Safety*In*Engineering

Common-Mode Failure Considerations in High-Integrity C&I Systems

Jim Thomson, February 2012

1. Introduction

This note aims to describe potential causes of Common-Mode Failure (CMF), how we can design C&I systems to prevent CMF, and how we can take possible CMF into account when doing plant risk assessments.

This note aims to cover both software and hardware systems and components.

Much of the basic thinking around CMF issues dates back to the 1970s and 1980s. In particular, two reports were published by the UK Atomic Energy Authority's Safety and Reliability Directorate which, to a significant extent, led subsequent thinking on this issue:

(i) *A Study of Common-Mode Failures*, SRD R146, GT Edwards and IA Watson, July 1979
(ii) *Defences against Common-Mode Failures in Redundancy Systems – A Guide for Management, Designers and Operators*, SRD R196, AJ Bourne, GT Edwards, DM Hunns, DR Poulter, IA Watson, January 1981

Arising from these reports and others, it was recognised that the avoidance of CMF was to a great extent an issue of quality assurance and quality control throughout the lifecycle of the C&I system. Subsequent international standards such as IEC 61508 *Functional safety of electrical/*

electronic/programmable electronic safety-related systems have developed this approach. IEC 61508 is based on:

- a lifecycle model for C&I systems (from conceptual design, through operation, to decommissioning)
- an assumption that the realistically-achievable reliabilities from redundant C&I systems are in some ways proportional to the degree of quality assurance and quality control employed throughout their lifecycles, and
- an assumption there are limits to the achievable reliabilities in non-diverse systems

2. What is Common-Mode Failure?

Common-Mode Failure can also be referred to as Common Cause Failure or Dependent Failure. Some people may say that there are subtle differences between these terms, but in my own view they are interchangeable. Let's keep it simple.

A precise definition of CMF was given in SRD R196 (ref ii): **"A Common-Mode Failure is the result of an event(s) which because of dependencies, causes a coincidence of failure states of components in two or more separate channels of a redundancy system, leading to the defined systems failing to perform its intended function."**

> *A well-known example of CMF is the Ariane 5 Launch Failure in 1996. This launch was the first of ESA's new Ariane 5 rocket launcher, which was a much bigger launcher than its predecessor Ariane 4. Thirty-seven seconds after launch from French Guiana on 4th June 1996, both the duty and the back-up Inertial Reference Systems (IRS's) failed, which led to launcher disintegration.*
>
> *The cause was a software fault in equipment which was unchanged from Ariane 4, but which was unsuitable for the changed flight trajectory of Ariane 5. There was inadequate analysis and simulation of the systems in Ariane 5. There were 2 IRS's with identical hardware and software. One was active and one was on hot stand-by. Because the flight trajectory was different from Ariane 4, the active IRS declared a failure due to a software exception (error message). The stand-by IRS then failed for the same reason.*
>
> *Actually, the affected software module only performed alignment of the inertial platform before launch – it had no function after launch. So, the error message was inappropriately handled, although the supplier was only following the contract specification.*
>
> *See http://www.youtube.com/watch?v=kYUrqdUyEpI&feature=related for a video of the launch failure.*
>
> *Conclusions:*
> *(i) The dual-redundant IRS system suffered CMF.*
> *(ii) There was a failure to review the software thoroughly for a new application (changing from Ariane 4 to Ariane 5), i.e. a Management of Change failure.*
> *(iii) The actual software error messages were generated from some unnecessary functionality, i.e. a software specification error.*

FIGURE 1: THE ARIANE 5 LAUNCHER AND THE LAUNCH FAILURE OF JUNE 1996

Other examples of CMF include the Uljin NPP common-cause software fault incident in 1999 www.safetyinengineering.com/FileUploads/Uljin%20NPP%20common-cause%20software%20fault_1312282222_2.pdf and, of course, the tsunami damage to Fukushima in 2011 which caused multiple CMFs and prevented all the post-trip cooling functions from operating at several reactors.

3. What Can Cause CMF?

A shortlist of possible causes of CMF to redundant channels in a system is shown in Table 1.

Table 1 Possible Causes of Common Mode Failure

	Source of CMF	Some possible causes of dependent failure
1	Specification or design failure	Failure to recognise within the specification the full range of circumstances in which the plant must operate
		Wrong/inadequate standards used
		Inadequate Management of Change (control of plant modifications)
		Common ageing processes on redundant channels
2	Construction/ installation/ inspection/ commissioning failure	Poor quality control of components and sub-systems during manufacture
		Lack of physical/electrical separation during installation
		Improper installation
		Commissioning testing: failure to test adequately all credible circumstances
3	Maintenance or operations failure	Failure to repair defective equipment in a timely manner
		Maladjustment of set-points, limit switches, etc
		Improper or inadequate maintenance or test procedures
		Failure to follow maintenance procedures
		Poor control of over-rides or interlock defeats
		Poor housekeeping
		Poor quality spare components
4	Environmental aspects	Temperature
		Humidity
		Vibration
		Stress
		Corrosion
		Contamination (abrasive material, chemical agent, etc)
		Radio frequency interference (RFI)
		Radiation
		Static charge
		Extreme weather (rain, snow, hail, ice, wind)
		Seismic event, tsunami
5	Other external and internal hazards	Fire
		Flood
		Explosion
		Air crash
		Terrorism

4. Defences against CMF

Although the scope of these failure mechanisms is very large, **there is no guarantee that the list of CMF causes given above is comprehensive**, since CMF is a catch-all, i.e. it includes “any other possible dependent failure mechanisms you haven’t considered”. Also, most of the above issues are underpinned by the employment of personnel with suitable qualifications, training and experience– ultimately it is the people who count. They have to be professional, disciplined, knowledgeable and engaged. They must also be able to differentiate between important and non-important issues.

Because the causes of CMF must include “dependent failure mechanisms you haven’t considered”, the defences against CMF must address both real, identifiable potential causes of CMF (e.g. fire, or lack of routine testing), and also more abstract, philosophical concerns. A very short list of some important defences against CMF is presented below:

a. Clear, robust quality assurance and quality control arrangements
b. Clear functional specifications (logic, environment, ergonomics)
c. Fail-safe design
d. Independent verification and validation (IV&V)
e. Testing at component, module, sub-system and system level
f. Clear traceability between functional requirements and testing, in both directions
g. Separation of control and protection
h. Physical separation between channels
i. Electrical separation between channels
j. Protection against fire and explosion
k. Flood protection
l. Seismic design as appropriate
m. Functional and equipment diversity *(in very high-integrity applications)*
n. A routine testing regime which effectively tests the functional requirements
o. Staggered testing so that channels are tested at different times

IEC 61508 *Functional safety of electrical/ electronic/programmable electronic safety-related systems* contains much more detailed descriptions of the 'techniques and measures' required to realise high-integrity C&I systems. These techniques and measures are in practice the same things as 'defences against CMF'.

A very brief summary of some of the techniques and measures prescribed in IEC 61508 is presented in Table 2 below.

Table 2 Techniques and Measures for the Design, Development and Operation of Safety Equipment

Techniques and measures required for the design, development and operation of safety equipment

Note: The following is a very high-level, brief checklist from IEC 61508 parts 2 and 3. IEC 61508 is a very complex standard, and reference should be made to the standard for the necessary detail. ***The degree to which each technique or measure has to be implemented depends on the SIL level required for the equipment.*** *Not all techniques and measures are required for all SILs. Definitions of terms are given in IEC 61508 part 7.*

Hardware	Software	ASICs and FPGAs
During design and implementation 1. Robust project management and documentation (throughout) 2. Structured specification, design 3. Observance of guidelines and standards 4. Functional testing, analysis 5. Operation and maintenance instructions, user- and maintenance-friendly 6. Interference testing 7. Fault insertion testing During operation 1. Program sequence monitoring and on-line monitoring or testing 2. Power supply monitoring and protection 3. Spatial separation 4. Ambient temperature protection 5. Modification protection	1. **Functional safety assessment**: checklists, truth tables, failure analysis, CCF analysis, reliability block diagrams 2. **Software requirements specification** – formal or semi-formal methods, traceability, software tools 3. Fault detection, error detecting codes 4. Diverse monitoring techniques 5. Recovery mechanisms or graceful degradation 6. Modular design 7. Trusted/verified software elements 8. **Forwards/backwards traceability at all stages** 9. Structured or semi-formal or formal methods, auto-code generation 10. Software tools 11. Guaranteed maximum cycle time, time-triggered architecture, maximum response time 12. Static resource allocation, synchronisation 13. Language selection, suitable tools 14. Defensive programming, modular approach, coding standards, structured programming 15. **Testing**: dynamic, functional, black box, performance, model-based, interface, probabilistic 16. Process simulation, modelling 17. **Modification/change control**: impact analysis, re-verification, revalidation, regression testing, configuration management, data recording and analysis 17. **Verification**: Formal proof, static analysis, dynamic analysis, numerical analysis	1. Structured description, VHDL design description and simulation, Boolean design description 2. Proven in use VHDL simulators and design environment 3. Functional testing on module and top levels, and embedded in system environment 4. Avoid asynchronous constructs, synchronised primary inputs 5. Design for testability; modularisation 6. Code guidelines adherence, code checker, defensive programming 7. Documentation of simulation results 8. Code inspection, walk-through 9. Validation of soft-cores 10. Internal consistency checks 11. Simulation of gate netlist to check timing constraints; static timing analysis of propagation delay 12. Verification of gate netlist 13. Check ASIC vendor requirements and constraints 14. Documentation of synthesis constraints, results and tools; use of proven in use tools and target libraries 15. Script based procedures 16. Test insertion and test pattern generation 17. Placement, routing, layout generation 18. Proven in use chip technology and manufacturing, QA, QC 19. Test coverage of manufacturing test; final verification and validation 20. Burn-in test

ASIC = Application-Specific Integrated Circuit

FPGA = Field-Programmable Gated Array

5. Diverse systems (such as Nuclear Reactor Protection Systems)

For the highest integrity applications, such as nuclear reactor protection systems (RPSs), there may be a need for a second, diverse system of detecting fault conditions and initiating a reactor shutdown. To be a fully and unambiguously diverse system:

a. The diverse RPS design should be developed by a different team, using independently-derived safety functional requirements;
b. The diverse RPS should be electrically and physically separated;
c. It should use different input sensors measuring diverse operating parameters;
d. Its signals should pass via separate routes and be processed by diverse types of logic solver;
e. Its final actuating devices (usually electrical breakers) should be from a different manufacturer;
f. Its means of shutdown should use different physical principles (e.g. boron injection vs. control rods).

In addition, there remains a non-disprovable concern that there may be a weakness to common-mode failure (CMF) **if both sets of logic solvers in two nominally-diverse systems are software-based**. This concern is related to the complexity of software systems, and the associated difficulties of verification and validation (V&V). In some undefined way, similarities in the software code design and production processes may yield the possibility of CMF – even if different software languages and operating systems are employed in the two systems. Because of this concern, it has become common in some countries to specify that the diverse protection system should be hard-wired.

6. Modelling CMF in probabilistic (quantitative) risk assessment

Conventional reliability assessments of random failure rates for hard-wired systems are based on measured failure rates for all the system's components and an assumption of 'perfect' routine testing (i.e. the routine testing detects all latent faults). This assessment approach can often yield unrealistically low predictions for actual systems failure rates. The system failure rates will in practice be dominated by common mode failures and not by random failures.

However, the application of probabilistic (or quantitative) risk assessment techniques means that there is a need to make judgments about the reliabilities of redundant systems, even when their failure rates are dominated by CMF. Two main approaches have been developed for modelling the effects of CMF in probabilistic (or quantitative) risk assessment:

i. The **cut-off method (or SIL method)** assumes that the reliabilities of a redundant multiple-channel system can be represented by a CMF 'cut-off' value, which is judged according to the perceived or assessed quality of the equipment, its design, manufacture, installation, operation and maintenance.
ii. The **Beta Factor method** assumes that the frequency of dependent failures between redundant channels is proportional to the assessed random failure rates of each redundant channel. The constant of proportionality is called the Beta factor.

6.1 The Cut-Off (SIL) Method

The cut-off method has, as its basis, assumptions that (a) the reliability of a redundant system is in some way proportional to the level of quality assurance and quality control (QA/QC) applied during its design, implementation, operation and maintenance, and (b) dependant upon the level of QA/QC, a "realistically achievable" system reliability can be assigned.

- The best achievable system reliability (the 'cut-off' level) may be (usually will be) worse than the value determined by reliability calculations.
- The correlation between QA/QC and cut-off system reliability is largely judgmental, because multiple-channel CMF events are rare, and their causes are manifold. Hence we cannot ever be sure about how QA/QC precisely affects achieved systems reliability. Nonetheless, the International Electro-technical Committee (IEC) has, in effect, made judgments about the correlation between QA/QC and cut-off reliability levels. These have been codified in the standard IEC 61508 *Functional safety of electrical/electronic/programmable electronic safety-related systems,* which prescribes a wide range of QA/QC measures that are needed to achieve 'Safety Integrity Levels' (SIL) for a redundant systems.
- Safety integrity Level (SIL) is therefore a surrogate for C&I systems reliability. SIL levels as follows are commonly used in the UK nuclear industry:
    - SIL 1 = 10^{-1} pfd or pa 'safety-related'
    - SIL 2 = 10^{-2} pfd or pa 'safety-related' or (sometimes) safety system
    - SIL 3 = 10^{-3} pfd or pa safety system
    - SIL 4 = 10^{-4} pfd or pa safety system

  Note: 'pfd' = probability of failure on demand, and 'pa' = per annum
- IEC 61508 recommends the use of 'techniques and measures' in varying degrees commensurate with the desired SIL. (See Table 2.) Each and every technique or measure is discussed in detail in IEC 61508 and recommendations are made about the appropriateness and the depth of each in order to achieve a particular SIL.

6.2 The Beta Factor Method

A measure of the effects of CMF on system reliability can be obtained by using the Beta factor, which is defined as **"the probability that, if a failure occurs in one channel of a redundant system, other channels will also fail due to a common cause"**. Hence, if the reliability of a single channel can be determined by calculation or otherwise, the CMF of the redundant system can be determined by multiplying the assessed single-channel reliability by the Beta factor.

Ref (i) quotes data suggesting Beta factors typically lie in the range 0.07 to 0.4. A detailed discussion of the Beta factor methodology can be seen in IEC 61508 *Functional safety of electrical/ electronic/programmable electronic safety-related systems*, edition 2 (2010), part 6, Annex D.

Personally, I have difficulties with Beta factors:

- In principle, I can see no reason at all why single-channel failure rates *should* be proportional to common-mode failure rates. They are different things altogether.
- Beta factor calculations can be used to produce spurious levels of accuracy for the reliability of redundant systems. Two or three significant figures have sometimes been claimed, quite

inappropriately. With simple SIL 'orders of magnitude' numbers you at least know that the figures are really just intelligent judgments, and nothing more precise.

6.3 Modelling Diverse Systems

If two separate protection systems have been installed in accordance with the principles set out in section 5 above, then any failure of one system should always be completely independent from a failure of the other system. Hence the probability of simultaneous failure both systems can be modelled in the probabilistic (quantitative) risk assessment as:

Probability of simultaneous failure of both diverse systems =

(Probability of failure of diverse redundant system 1) x (Probability of failure of diverse redundant system 2)

Any failure to meet the independence requirements set down in section 5 will to some extent compromise this conclusion.