A brief background on the history of CMF limits in civil Reactor Protection Systems

Jim Thomson, 23 June 2021

Probabilistic safety analysis (PSA) of nuclear power stations was first proposed by Farmer (1967). PSA began to be used widely in nuclear power station design following the WASH-1400 report (Rasmussen, 1975) into light water reactor safety. One issue that arose, however, was the maximum extent to which claims on control and instrumentation (C&I) could be made; that is, how could the PSA analysis allow for the possibility of dependent failures (or common-mode failure or CMF) between nominally independent systems? Without such limits, reliability claims for C&I systems could be multiplied together to yield numbers that were simply not credible. So, what levels (or CMF cut-offs) were credible?

The particular issue here is that *the claimed value for a CMF cut-off can have a large effect on the overall assessed plant numerical risk. However, the basis for any claimed CMF cut-off is by no means easy to establish – not least because very high integrity systems such as reactor protection systems, almost by definition, do not fail. Hence there is no database of relevant failures, so it becomes necessary to fall back on 'expert judgment', despite there being no clear basis for such judgment.* This has at times led to a 'Dutch auction' where the worst (lowest reliability) value put forward for CMF cut-off seems to control the discussion.

By the early 1980s, the Safety and Reliability Directorate (SRD) of the UK Atomic Energy Authority was able to propose guidelines on CMF (Bourne et al., 1981). These guidelines were written around an implicit assumption of hard-wired systems, and proposed maximum claims that could be made for redundant (multiple-channel) systems. These maximum claims (or CMF cut-offs), it was proposed, were to be based on largely qualitative criteria such as functional requirements definitions, design realisation aspects (including channel dependencies, design quality control, fail-safe design, manufacturing quality control, installation and testing quality control, maintenance and proof testing quality control, operational conditions and environmental controls, and potential external events), as well as quantitative measures such as assessed channel reliabilities. On this basis, the SRD report suggested a non-diverse or non-independent reactor protection system (RPS) might be limited to 10^{-2} to 10^{-3} pfd or pa failure rate. They also suggested that an RPS which incorporated diverse and independent sub-systems might achieve 10^{-5} to 10^{-6} pfd or pa.

The first nuclear power station in the UK (and perhaps worldwide?) to be designed from the start with dual, separate, independent multi-channel RPS's was the Prototype Fast Reactor (PFR) which first went critical in 1976. PFR's two RPS's incorporated diverse input sensors, diverse logic (relay and magnetic), and diverse actuation of reactor shutdown.

Heysham 2 and Torness (HYB/TOR) nuclear power stations were designed during the 1980s using PSA principles – a first in the UK - and lessons from the SRD report were incorporated. Their design included two diverse, separated and independent RPS's, one using relay logic and electromagnetic rod-drop, with the other using magnetic logic and nitrogen injection. In discussion with the regulator, somewhat less onerous CMF cut-off limits were used within the Heysham 2/Torness Pre-Construction Safety Report (PCSR) than those that had been proposed by SRD in 1981 (as discussed above); instead, a CMF limit was proposed, and agreed with the regulator, of not better than 10^{-5} pfd for simple, redundant, robust systems, with no known dangerous failure modes. This applied to the

magnetic logic RPS. In practice, GEC's 'Laddic' system (robust magnetic logic, now obsolete) has been the only technology that has ever been accepted into the higher-integrity (10^{-5} pfd) category by the UK regulator.

Other robust non-diverse systems were allowed to claim not better than 10^{-4} pfd (such as the relay-logic RPS).

The Heysham 2/Torness (HYB/TOR) projects occurred as software protection systems first began to see widespread use - the first draft guidelines into the use of Programmable Electronic Systems (PES) were published in 1988. These guidelines later became an input for IEC 61508 which was first published in the 1990s.

The draft PES Guidelines affected the end of HYB/TOR construction – extensive re-design and removal of some already-operational software-based equipment (non-RPS-related) was mandated by the regulator.

The basis for current UK civil nuclear licensing is found in two documents; Tolerability of Risk (TOR) (HSE, 1992) and the Safety Assessment Principles (HSE, revised 2006). Furthermore, a key licensing guide T/AST/046 (HSE, 2012 but currently under review) 'Technical assessment guide – computer based safety systems' plays a major role. T/AST/046 mandates a two-legged approach for high-integrity software based on 'production excellence' and 'independent confidence building'. *In practice, the UK regulator has never yet (2021) accepted a reliability claim for any software-based system of better than 10^{-3} pfd or pa* (although see below for EPR licensing where 10^{-4} seems to have been accepted). This is more-or-less consistent with the approach recommended by the Western European Nuclear Regulators Association (WENRA, 2010).

Software reliability claims became a major issue in the design and licensing of Sizewell B nuclear power station, which began power operation in 1995. The Sizewell B Primary Protection System (PPS) was claimed to have a reliability of 10^{-4}, but (as indicated above) the regulator only ever accepted a claim of 10^{-3} in the safety report. This was despite exhaustive and expensive independent verification and validation efforts. Hence, the safety report was only accepted on the basis of a sensitivity study which showed that Sizewell B risk remained within the tolerable, or ALARP, region even if a lower PPS reliability of 10^{-3} was assumed.

Development of standards for high-integrity RPS application has continued since the 1990s – notably IEC 61508, IEC 61513 and IEC 60880.

Of particular note is the recent experience with the EPR design in Finland, the UK and France.

The original proposal for UK-EPR included the following:

1. The EPR I&C consisted entirely of computer-based systems, Areva Teleperm XS (for the high-integrity protection functions) and Siemens SPPA-T2000 (for lower-integrity control functions). Furthermore, both these systems were originally developed by Siemens, so any claim for design diversity seemed weak.

2. The Siemens SPPA-T2000 system, which is a fairly low-integrity system designed to SIL 2 or equivalent standards, was being used to change parameters on the high-integrity Teleperm

XS system. In general, there was a high level of connectivity between two complex systems, although these systems were being claimed to be wholly independent of each other.

3. The Teleperm XS system was being claimed by the designers to have a reliability of 10^{-5} failures on demand. The SPPA-T2000 system was being claimed to have a reliability of 10^{-3}. Both of these reliability claims are at the very top end of what might be realistically achievable.

As a result of the Generic Design Assessment, the UK regulator requested significant changes in the C&I architecture. In particular,

- It was agreed that a non-computerised backup system would be implemented in order to provide protection and controls in case of total loss of C&I functions from the Teleperm XS and SPPA-T2000 platforms.

- It was agreed that one way communication would be implemented from the Teleperm XS system to the SPPA-T2000 system.

- It was agreed that the reliability claims would be reduced for the Teleperm XS (10^{-5} pfd to 10^{-4} pfd) and SPPA-T2000 (10^{-4} pfd to 10^{-2} pfd) systems.

A notable outcome of this review process in the UK is that **EPR designs in UK, Finland and France will now each have different I&C architectures**. All three countries are (or were, before Brexit) members of the European Union, so one might have expected common standards of regulation to apply. However, in each country the safety regulator has taken a different view of what constitutes 'best practice'. The UK position is as described above. In Finland, the safety regulator (STUK) has also requested a non-computerised backup RPS but in that country an FPGA-based system has been adopted. In France, however, the safety regulator (ASN) has more-or-less accepted the original architecture proposal with the proviso that more safety-related functions, which were originally to be in SPPA-T2000 systems, will now be in the high-reliability Teleperm XS system. The Chinese design will be the same as the French.

The key issue here is that it shows there is no absolute international consensus on best practice in C&I architecture and CMF cut-off claims. This is an issue that should be resolved, but unfortunately it is also an issue where national interests and pride can work against the achievement of consensus.

A further point of note is that there exists a forum for nuclear safety regulators called the Western European Nuclear Regulators Association where these issues could and should have been resolved. However, the French regulator is not presently a member.

Finally, it is worth noting that UK licensees have never yet used, nor has the UK nuclear regulator ever yet licensed the use of, high-integrity FPGA-based systems for use on civil nuclear power stations, although high-integrity FPGA-based systems have been used on US, Finnish, and Chinese plants (and perhaps also elsewhere).

References

Bourne, A.J., G.T. Edwards, D.M. Hunns, D.R. Poulter, I.A. Watson (1981), Defences against common-mode failures in redundancy systems SRD-196, UKAEA Safety and Reliability Directorate.

Farmer, F.R. (1967), Siting criteria, a new approach, IAEA SM-89/34, Vienna 1967.

HSE (1992), The Tolerability of Risk from Nuclear Power Stations, HMSO, 1992.

HSE (2006), Safety Assessment Principles for Nuclear Facilities, HMSO, 2006.

HSE (2012), T/AST/046 Issue 2, Technical assessment guide – computer based safety systems, HMSO 2012 (revision in preparation).

International Electro-technical Commission (2008), Functional safety of electrical/electronic/ programmable electronic safety-related systems, IEC 61508, 2nd edition.

International Electro-technical Commission (2001), Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems, IEC 61513.

International Electro-technical Commission (2006), Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions, IEC 60880, 2nd edition.

Rasmussen, N.C. (1975), Reactor Safety Study WASH-1400, US NRC.

WENRA (2010), Licensing of safety critical software for nuclear reactors: Common position of seven European nuclear regulators and authorised technical support organisations, WENRA, 2010.