Safety*In*Engineering

Nuclear Power Station Control and Instrumentation Safety Systems Architecture – An Overview

Jim Thomson, February 2012

1. Introduction

This note aims to set out the basis for good control and instrumentation (C&I[1]) safety systems architecture in NPPs. (Here, 'architecture' means the highest level of systems design.) It may seem surprising that anyone should feel the need to write this down; surely there are agreed standards for these things? Well, the answers to that question are various, including:

[1] C&I is confusingly called I&C in many countries. This can create difficulties when using Google.

- There are lots and lots of standards, of which some are consistent with each other, and some are not.
- The interpretation of these standards can be different in different counties; hence, for example, we had the recent rejection of a French design for NPP C&I safety system architecture by the UK's nuclear safety regulator, on the basis that the regulator had fundamental dislikes for some design features. (The regulator was correct. The design was subsequently amended and accepted.)
- Nuclear safety regulators can generate confusion by being too 'hands-on' in their approach. In some countries, regulators produce their own pseudo-standards which are, in effect, an overlay on other national and international standards. Also, in some countries, the safety regulators can so dominate the development process for C&I systems that the design engineer may feel he is guessing what regulatory caprices might be, rather than following sound principles. (I am not 'having a go' at the safety regulator here – they have a vital role to play.)

Exclusion: For the purposes of this note, I am deliberately avoiding any detailed discussion of the withstand capability against external and internal hazards, e.g. earthquake, flood, air crash, fire, etc.

1.1 Why are the architectures of safety systems different in nuclear, oil and gas, and aviation?

This may seem a stupid question, but it is worth thinking about. Some fundamental differences affecting C&I architectures between NPPs, oil and gas (O&G) facilities such as oil platforms and refineries, and civil aircraft, are as follows:

1. The hazard magnitudes may be significantly different (see also section 3). The potential hazards to the general public from NPPs – especially in terms of the risk of having to evacuate significant areas of land for many years – are in general greater than those for any other potential industrial hazards. (There are certain exceptions, e.g. Bhopal and potential dam failures, where the hazards are as bad, or worse than, nuclear power hazards.)
2. Also, in civil aviation, the persons at risk (the passengers) are accepting that they are taking on the risk by buying their tickets – we each do some sort of (probably subconscious) risk/benefit assessment[2]. (The same might be said for employees on, say, offshore O&G platforms.) There is therefore a difference between voluntary and involuntary acceptance of risk, and between risks where there is also benefit (e.g. salary) and where there is none. These factors – and others – ultimately mean that the reliability requirements are different for the C&I systems for nuclear plants, O&G plants, and aircraft.
3. Aircraft inevitably have to mix up control systems and protection systems, at least to some extent, whereas in both NPPs and in O&G facilities it is possible (and desirable) to separate control and protection. Modern digital aircraft systems have tended to become more 'integrated' – which means the separation between control systems, pilot display systems, and protection systems (which act to limit the flight envelope to safe areas) has become

[2] I wrote these words during a transatlantic flight.

more diminished. An example of problems that may arise has arguably been demonstrated in the Airbus A330 crash of 2009 (see www.safetyinengeering.com/case_studies).

1.2 Why is it important to get the C&I architecture right?

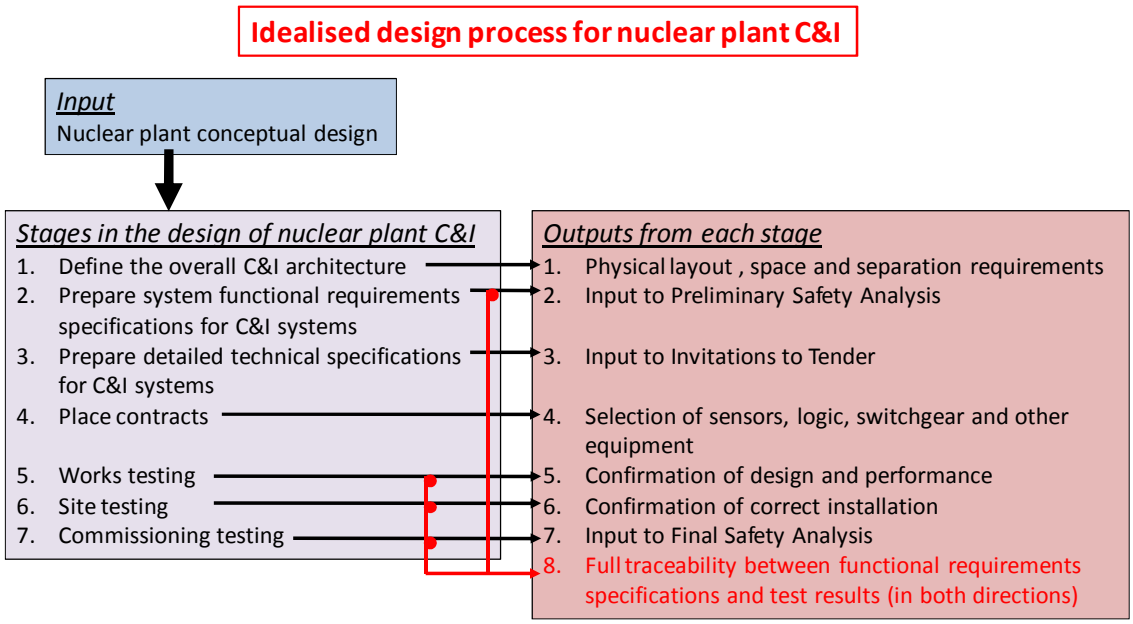
For new build nuclear power plants, the overall C&I architecture has to be frozen early in the design process. This is because:

(i) The C&I architecture includes the major protection systems and therefore defines much of the safety case.
(ii) The C&I architecture leads to definitions of space requirements and system separation requirements (for cubicles, switchgear, and cable routes) so that the civil structures can be designed.

Hence the programme for nuclear power station construction needs to address C&I architecture at an early stage. The typical order for C&I systems specification, design and implementation would be as follows:

a. Define the overall C&I architecture, including space and separation requirements
b. Prepare system functional specifications for C&I systems
c. Prepare detailed technical specifications for C&I systems
d. Place contracts
e. Works testing
f. Site testing
g. Commissioning testing

This is illustrated schematically below.



2. Deterministic considerations

'Deterministic' considerations for present purposes mean those considerations which are based on good engineering practice alone, as opposed to probabilistic risk considerations.

The fundamental deterministic considerations for good NPP C&I safety systems design can be summarised as follows:

a. Control and protection systems shall be separated.
b. Diverse reactor protection systems (RPSs) shall be fitted.
c. One of the diverse RPSs shall be hard-wired.
d. There shall be full traceability of the designs (forwards and backwards) from the derivation of all safety functional requirements through to their design, implementation and testing.

It always surprises me that this simple set of requirement does not appear clearly and explicitly in any international standard. Instead there is a plethora of large documents, which are very detailed and have been produced by considerable collaborative (sometimes international) efforts. The difficulty with these large international standards is that it can be challenging to differentiate the trees from the forest.

2.1 Some definitions

Control systems: In their broadest sense, these include sensors, plant status indications, logic systems, alarm systems, and auto-control systems. In NPPs with digital systems, 'control systems' are sometimes referred to as the DPS (Data Processing System), DPCS (Data Processing and Control System), or DCS (Digital or Distributed Control System). (The term DCS is more common in process industries and O&G than in NPPs.) The DPS/DPCS/DCS includes the Human-Machine Interface (HMI) – the computer screens in the Main Control Room - for the normal operation of the plant. The functions of the DPS/DPCS/DCS are self-evidently to control the plant parameters within normal limits, and to advise the operators of plant status, and to raise alarms when normal parameter ranges are exceeded.

Protection systems: These include sensors, logic, actuators, and the dedicated HMI for the protection systems. These systems play no active part in the normal operation of the plant whatsoever – their only role is to detect anomalous behaviour and initiate protection/mitigating actions, and keep the operator informed of what they are doing. Protection systems include both the Reactor Protection System (RPS) (q.v.) and the Engineered Safety Features Actuation System (ESFAS) (q.v.).

- Engineered Safety Features Actuation System (ESFAS): (This may also be called Post-Trip Sequencing and other names, depending on plant design.) This is the protection system which actuates a variety of functions after a reactor shutdown. The system objectives will be successful post-trip reactor cooling, and ensuring containment integrity. Its functions may include (depending on the NPP design) start-up of essential diesel generators, timed sequencing of loading up the generator loads, post-trip feedwater supply to steam generators, reactor coolant pumps, containment systems, etc. There may or may not be a requirement for a diverse ESFAS, although in some designs ESFAS actions are insufficiently

urgent to require a diverse automatic system – manual (operator) actions may suffice to actuate the engineered safety features.

- Logic solver: The equipment that decides, from the range of input signals received, whether to initiate a reactor trip or not. The logic is either software (microprocessor)-based or hard-wired (q.v.). The logic solver is part of the RPS (q.v.).
- Reactor Protection System (RPS): This system initiates rapid reactor shutdown when safe values of key plant parameters are exceeded. These parameters may include (depending on the NPP design) high neutron flux, high coolant temperature, low coolant flow, high coolant pressure, etc.

'Control and protection shall be separated': The systems should be electrically and physically separated to try to eliminate common-mode failures between control systems and protection systems. At no point should there be a direct electrical connection between a control system and a protection system. Any required electrical signal connection (e.g. communications) shall be via buffered links, e.g. opto-isolators. Electrical separation includes also the power supplies for the systems. In general, the power supplies should be sourced from different transformers, and the RPS should use guaranteed supplies. The systems shall also be physically separate, ideally with physical/fire barriers in between. These measures are necessary to prevent common-mode or common-cause failures.

Diversity: The objective of diversity is to try to eliminate the possibility of common-mode failures (CMFs). The requirement for a diverse RPS is fundamentally driven by probabilistic considerations (see section 3). The magnitude of the risks generally means that two completely independent routes to safe shutdown are required. The deterministic requirements of these diverse systems are that they must be independent not just in terms of physical and electrical separation, but also (so far as is reasonably practicable) in terms of their operating principles. Hence:

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

Redundancy: All protection systems will employ redundancy to some extent, and some control systems may also have redundancy. The extent of redundancy will depend on various factors including reliability requirements, maintenance requirements, and the single-failure criterion. (The *single failure criterion* is normally applied to protection systems – it means that no single failure of a system should cause a dangerous system failure.) A Primary RPS will usually use two-out-of-four (2oo4) logic. Some control systems may be 'duplex' (1oo2) where this is dictated by plant availability requirements.

Hard-wired: Hard-wired systems are those systems which do not employ digital (software-based) logic devices, sensors, displays or other components or sub-systems. Hard-wired logic solvers include

relay logic and magnetic logic. (Field-Programmable Gated Arrays (FPGAs) are considered by some to be another type of hard-wired logic element, although software is used in the design of FPGAs.)

Traceability: The design of complex control and protection systems needs to be done in a managed and careful way. It must progress carefully from safety analysis, via safety functional requirements specifications, to detailed designs, failure modes analysis, reliability analysis, module testing, integration testing, site acceptance testing and plant commissioning tests. To ensure that the testing programme does not lose sight of the original safety functional requirements, these requirements must be traced through to specific tests and back to the safety functional requirements in a transparent way.

Safety integrity Level (SIL) is a surrogate for C&I systems reliability, as used in IEC documents including IEC 61508. SIL levels as follows are commonly used in the UK nuclear industry:

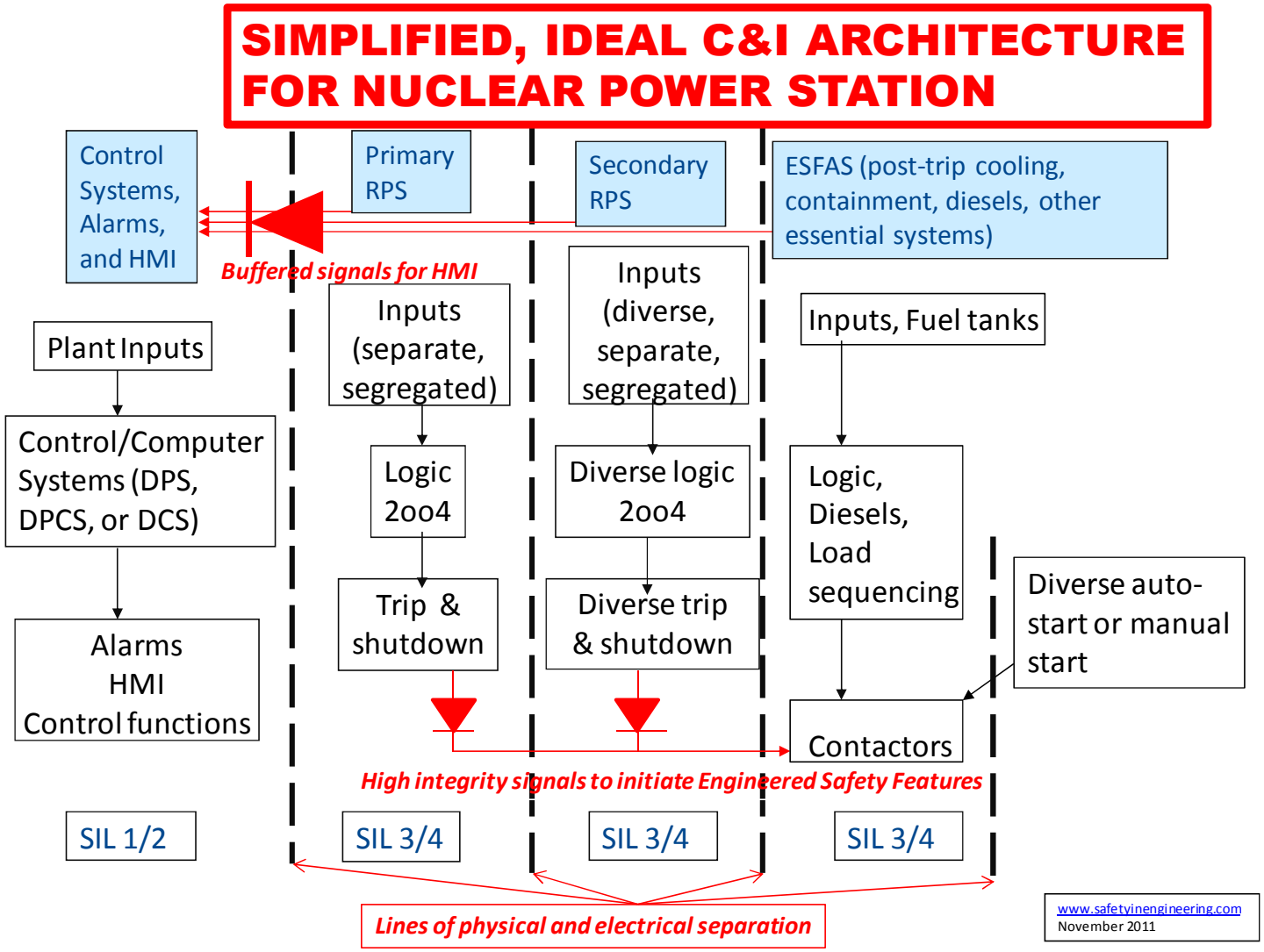
SIL 1 = 10^{-1} pfd or pa 'safety-related'
SIL 2 = 10^{-2} pfd or pa 'safety-related' or (sometimes) safety system
SIL 3 = 10^{-3} pfd or pa safety system
SIL 4 = 10^{-4} pfd or pa safety system

'pfd' = probability of failure on demand
'pa' = per annum

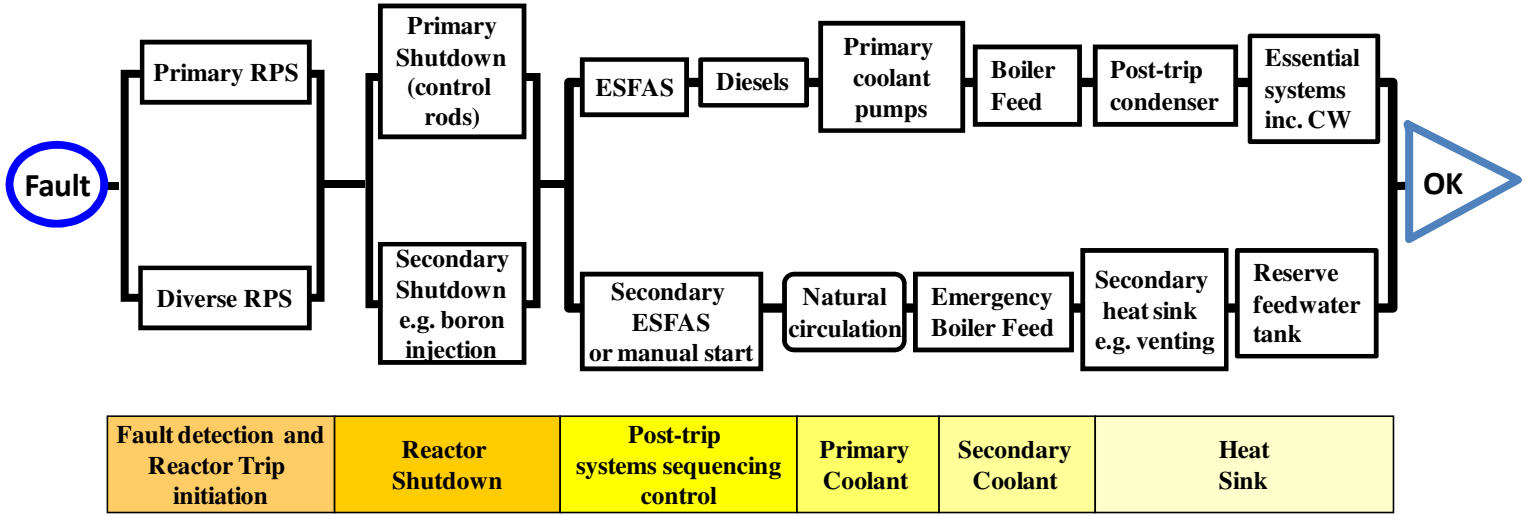
2.2 The 'ideal' NPP C&I safety systems architecture

Illustrations of idealised NPP C&I safety systems architectures are shown below. The diagrams are necessarily simplified, but one lesson I have learned painfully is that, when setting out on a C&I safety systems project, it is important that all engineers involved (design engineers, contractors and sub-contractors, safety regulators, client engineers, and future operators) have a simple mental model of the overall architecture that is to be implemented. This helps avoid major problems later in the project.

I emphasise that the drawings below are idealised and simplified. The realisation will always be different and more complex.


SIMPLIFIED, IDEAL C&I ARCHITECTURE FOR NUCLEAR POWER STATION
Control Systems, Alarms, and HMI
Primary RPS
Secondary RPS
ESFAS (post-trip cooling, containment, diesels, other essential systems)
Buffered signals for HMI
Plant Inputs
Inputs (separate, segregated)
Inputs (diverse, separate, segregated)
Inputs, Fuel tanks
Control/Computer Systems (DPS, DPCS, or DCS)
Logic 2oo4
Diverse logic 2oo4
Logic, Diesels, Load sequencing
Alarms HMI Control functions
Trip & shutdown
Diverse trip & shutdown
Diverse auto-start or manual start
Contactors
High integrity signals to initiate Engineered Safety Features
SIL 1/2
SIL 3/4
SIL 3/4
SIL 3/4
Lines of physical and electrical separation
www.safetyinengineering.com
November 2011

Reactor protection systems – diverse routes to cold shutdown



Notes:
1. This is an attempt to make a generic representation of diversity within reactor protection systems for all reactor types, so some simplification has been necessary. *Details will differ significantly according to the design of the power station,* especially with respect to post-shutdown cooling systems.
2. The diagram does not show redundancy – most (or all) of the above systems will also incorporate redundancy.
3. RPS = Reactor Protection System
4. ESFAS = Essential Safety Features Actuation System
5. Any route from 'fault' to 'OK' must be viable and meet reliability criteria.

www.safetyinengineering.com
November 2011

2.3 Short-term vs. long-term accident management systems

ESFAS is designed to deal with short-term post-trip requirements to ensure decay heat removal and containment. The experience of Three Mile Island and other accidents has been to show the need for clear plant status displays for long-term essential systems, over days and months. Limited-scope hard-wired displays for this purpose are usually referred to as Plant Accident Management Systems (PAMS).

3. Probabilistic (risk) considerations

3.1 Risk targets

In principle, the overall frequency of internally-induced reactor faults that could lead to major accidents is calculated as follows:

Σ{(Initiating event frequency) x (protection failure probability) x (diverse protection failure probability) }

= major accident fault frequency

The principal risk targets for nuclear reactors are typically set by three considerations:

i. Core-melt frequency (with a target of say 10^{-5} pa or better, calculated by summing all relevant possible fault sequences).
ii. The individual off-site risk to members of the public, which is calculated by summing the risk from all faults which lead to radiological release. The individual risk should be small compared to other risks – which typically means 10^{-6} pa for additional cancer risk to any individual living nearby arising from the summed frequency of all nuclear accidents.
iii. The societal risk from large nuclear accidents – those which could lead to large numbers of early deaths due to cancers (with resulting severe psychological and economic impact) - should be small. This typically means 10^{-6} pa for the summed frequency of all fault sequences that could lead to a large nuclear accident.

3.2 Alarms and HMI

The HMI (Human Machine Interface) encompasses displays, alarms and manual controls. Evidence shows that human reliability is not good in high-pressure situations with serious time constraints. For this reason, only weak reliability claims (~10^{-1} pfd) are ever made for operators in fault situations, and it is assumed they do not have to react quickly. Consequently there is little purpose in designing an extremely high reliability HMI, so it is normally just a SIL 1 system.

One key concern is that the HMI should not mislead operators into making a bad situation worse - for this reason, the *ergonomics* of plant displays deservedly gets a lot of attention.

Also, indication systems that show the status of post-trip cooling and containment systems (needed for monitoring the plant in accidents) need to have high integrity. Hence these systems often feature in special hard-wired displays in nuclear plant control rooms with SIL 2 or even SIL 3 reliabilities.

3.3 Auto-control systems

Auto-control systems can initiate faults if they fail. This can lead to plant down-time, and also to challenges on the protection systems, that is, they can cause 'initiating events' in fault sequences. It is therefore common to implement duplex control systems which can achieve SIL 2 reliability (10^{-2} pfd or pa).

3.4 Protection systems

The Primary RPS is the main system for ensuring reactor shutdown during faults. It is normally designed to the highest standards and is typically a SIL 3 or SIL 4 system. In modern nuclear plants, the Primary RPS is usually a digital (software-based) system. The design of digital RPSs is typically performed to international standards such as IEC 60880 or IEC 61508, and the systems will have claimed reliabilities in the 10^{-3} to 10^{-4} pfd range.

A fully-diverse Secondary RPS is normally fitted. The reliability required from the Secondary RPS will vary according to plant design, but it is typically in the 10^{-3} to 10^{-4} pfd range. However, some countries specify much lower reliability requirements for the Diverse RPS, even classifying it as a seismically-qualified 'Non-Safety' system.

The Primary ESFAS may, to some extent, be a distributed system, since the ESFAS controls a wide range of plant – diesel start-up, electrical breakers, sequencing equipment, valves, pumps, etc. The main logic will be high-integrity (typically in the 10^{-3} to 10^{-4} pfd range for a successful outcome), and the overall system may be highly redundant; for example, there may be a significant amount of excess diesel-generating capacity.

There may be a secondary ESFAS, or else the time constraints for operator action may allow claims for manual diverse actuation if the primary ESFAS fails.

3.5 The reliability of software-based systems

Reliability claims for software-based systems are fundamentally more difficult than those for non-software systems, for two main reasons.

First, for individual electrical, electronic or mechanical components, reliability claims are usually made on the basis of measured failure rates of a large number of similar components in other installations. For software-based systems, such an approach is not possible because the software will in general be unique for each application.

- *Software systems are usually assigned reliabilities according to their SIL values. (See the discussion on SILs in section 2.1 'Some definitions'.) International standards (e.g. IEC 61508, IEC 60880, IEC 62138) make assumptions that a software system's reliability is proportional to the level of quality assurance and testing that is used in the software production. This approach is entirely credible but also fundamentally unproveable: software failures will be dominated by non-stochastic (i.e. non-random) events such as inadequate specification. (This is unlike hard-wired systems where stochastic failure rates for components are well-supported by experience.)*

Second, software-based systems attain a complexity that is not practical for hard-wired systems. It is not unusual for a software-based safety system to have several thousand inputs and outputs (I/O).

- *For hard-wired systems, each safety function will generally be performed by a small number of components which are separate from other functions. It is therefore generally possible in hard-wired systems to prove the installed logic absolutely by doing both positive and negative testing, i.e. by testing that the desired combination of inputs always yields the correct output (positive testing) and that all undesired combinations of inputs will not generate any incorrect outputs (negative testing). However, for software-based systems with thousands of I/O, whose signals all ultimately go into the same processor, negative testing becomes impractical because the number of possible combinations of I/O increases to the point where the necessary test time becomes unfeasibly long. Also, software enables algorithms to be implemented in the logic, introducing another level of complexity.*

3.6 Software Diversity?

An issue that has caused debate and anguish – without necessarily providing a definitive verdict – is the question of whether or not it is possible to have two genuinely diverse protection systems if they are both software-based.

Remember that, for two high-integrity protection systems to be truly diverse, this ideally means that they need to be:

a. designed by two separate teams,
b. based on two separately-derived functional requirements specifications,
c. use different input process parameters,
d. use equipment sourced from different manufacturers (input devices, logic solvers, etc),
e. use different means of reactor shutdown,
f. be physically and electrically separated

However, 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.

4. Cyber-security

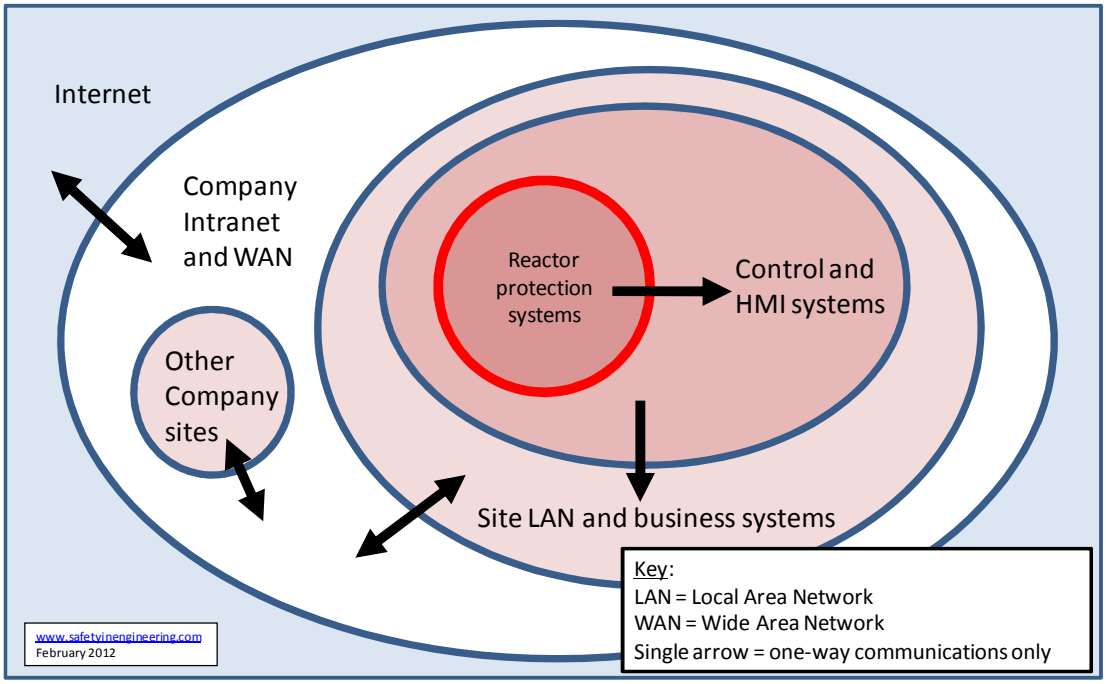
Stuxnet is a computer worm discovered in June 2010. It used ‘zero-day’ weaknesses in Windows to attack Siemens Simatic controllers at an Iranian uranium enrichment plant. Stuxnet was probably developed by a team of software engineers working for the Israeli government, possibly with US assistance. It was probably introduced and transmitted using memory sticks. This episode emphasised the importance of cyber-security in nuclear installations.

Fortunately, common-mode failure of multiple systems in nuclear power stations due to cyber-attack is difficult to envisage, because there are multiple levels of barriers to such attack:

(i) Separation between control and protection systems.
(ii) Administrative control over software changes.
(iii) The hard-wired diverse protection system will be resistant to any cyber-threat.

Plant operators, design engineers and regulators need to be vigilant to ensure that changes are not allowed to occur which may weaken the barriers between IT systems and control systems, or between control systems and protection systems. For example, it may be very convenient to create links between control systems and IT systems, to improve business information. It may also be very easy to use memory sticks to transfer data between the control systems and IT systems. Robust physical and administrative controls are required; these will probably include data encryption/decryption and virus checking for data transfer, when required.

Communication barriers and firewalls in nuclear power stations: protection systems, control and HMI systems, and IT systems



5. Selected further reading

1. IEC 61508, 2nd Ed, 2010: Functional safety of electrical/electronic/programmable electronic safety-related systems
2. IEC 61513, 2001: Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems
3. IEC 60880, 2nd Ed, 2006: Nuclear power plants – Instrumentation and control systems important to safety – Software aspects for computer-based systems performing category A functions
4. IAEA 1116 (NS-G-1.3), 2002: Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
5. IAEA 1495 (NP-T-3.12), 2011: Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants
6. IEEE 7-4.3.2, 2003: IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations