Evaluation of selected digital Instrumentation & Control architectures for nuclear power plants to determine compliance with the NNR position paper PP-0017 requirements

GG Swarts

21805032

A dissertation submitted in partial fulfilment of the requirements for the degree of Master of Engineering / Science in Mechanical and Nuclear Engineering at the University of the North-West

November 2014

Supervisor: Dr A Cilliers

ABSTRACT

Evaluation of selected digital Instrumentation & Control architectures for nuclear power plants to determine compliance with the NNR position paper PP-0017 requirements

The Instrumentation and Control (I&C) system is the central nervous-system of a nuclear power plant. New nuclear power plants being proposed to be built in this country all involve digital I&C systems, both safety related and non-safety related. The I&C systems of earlier Generation nuclear power plants are facing challenges with aging and obsolete analogue components. Technology has evolved in recent times and digital systems have replaced most analogue systems in other industries. Due to the safety and licencing requirements in the nuclear industry, the analogue and digital systems work concurrent in the protection and trip systems. The additional functionality of a digital I&C system will open up new possibilities to support operations as well as maintenance activities in the nuclear power plant.

For the I&C architectures and systems being evaluated by this study, the I&C architectures are based on existing digital platforms that were developed for nuclear power plants currently under construction in other countries.

The objective of this research project is to explain the development process of an I&C architecture, develop drivers and tactics from the National Nuclear Regulator (NNR) position paper PP-0017, evaluate and verify selected digital I&C architectures. The final objective is to synthesise a proposed digital I&C architecture in compliance with the requirements imposed by the NNR position paper PP-0017.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACKNOWLEDGMENTS

The author wishes to express sincere appreciation to the following:

My Lord and Saviour, Jesus Christ, “in whom are hidden all the treasures of wisdom and knowledge.” (Colossians 2:3)

My loving wife, Gloudina Swarts, whose encouragement and support enabled the fulfilment of this dream.

My study leader, Dr A. Cilliers, whose familiarity with the needs and ideas was helpful during the preparation of this research project. His valuable guidance and sound advice were also crucial in the success of this project.

Sasol as an employer and my manager, Sakkie Buys for granting me the opportunity to further my studies and education.

ABBREVIATIONS

ADD	Attribute-driven Design
ADDM	Attribute-driven Design Method
AOO	Anticipated Operational Occurrences
AP1000	Advanced Passive 1000
ASN	Nuclear Safety Authority
ATWS	Anticipated Trip Without Scram
CCF	Common Cause Failure
COTS	Commercial of the Shelf
C&I	Control and Instrumentation
DAS	Diverse Actuation System
DCS	Distributed Control System
DC&I	Digital Control and Instrumentation
DDS	Data Display and Processing System
DiD	Defence-in-depth
EDF	Électricité de France
EDG	Emergency Diesel Generators
ESF	Essential Safety Features
ESFAS	Essential Safety Features Actuation System
FPGA	Field Programmable Gate Array
GDA	General Design Assessment
HMI	Human Machine Interface

HSE	Health and Safety Executive
HIS	Human Interface System
IAEA	International Atomic Energy Agency
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
I&C	Instrumentation and Control
IT	Information Technology
KSF	Key Safety Function
LCO	Limiting Conditions of Operation
LOOP	Loss of Off-site Power
NC	Non-Categorised
NCSS	Non-Computerised Safety System
NI	Nuclear Installation
NNR	National Nuclear Regulator
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NUREG	US Nuclear Regulatory Commission Regulation
O&G	Oil and Gas
PACS	Priority and Actuation Control
PAMS	Plant Accident Management Systems
PAS	Process Automation System
PCC	Plant Condition Categories
PCSR	Pre-Construction Safety Report

PDC	Plan-Do-Check
PDDA	Preparation, Decision, Design, Assessment
PDFY	Probability of Dangerous Failure per Year
PFD	Probability of Failure on Demand
PICS	Process Information and Control System
PIPS	Process Instrumentation Pre-Processing System
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PPS	Primary Protection System
PS	Protection System
PSA	Probabilistic Safety Assessment
QDS	Qualified Display System
RAM	Control Rod Drive Mechanism
RCC-E	Rules of Design and Construction of Electrical Equipment
RCSL	Reactor Control, Surveillance and Limitation System
RPR	Reactor Protection System
RPS	Reactor Protection System
RR	Research Reactor
RRC	Risk Reduction Category
RSS	Remote Shutdown Station
SA	Severe Accident
SAP	Safety Assessment Principles
SAS	Safety Automation System

SBO	Station Blackout
SDOE	Secure Development and Operational Environment
SICS	Safety Information and Control System
SIL	Safety Integrity Level
SIS	Systems Important to Safety
SPS	Secondary Protection System
TAG	Technical Assessment Guides
TSC	Technical Support Center
UDG	Ultimate Diesel Generators
UK EPR	United Kingdom European Pressurized Reactor
US	United States
USNRC	United States Nuclear Regulatory Commission

DEFINITIONS

Anticipated operational occurrence. "Anticipated operational occurrences mean those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of power to all recirculation pumps, tripping of the turbine generator set, isolation of the main condenser, and loss of all offsite power."

Availability. "The fraction of time for which a system is capable of fulfilling its intended purpose. Reliability represents essentially the same information, but in a different form."

Bypass. "A device to inhibit, deliberately but temporarily, the functioning of a circuit or system by, for example, short circuiting the contacts of a relay."

Common cause failure. "Failure of two or more structures, systems and components due to a single specific event or cause. For example, a design deficiency, a manufacturing deficiency, operation and maintenance errors, a natural phenomenon, a human induced event, saturation of signals, or an unintended cascading effect from any other operation or failure within the plant or from a change in ambient conditions."

Defence-in-depth. "A hierarchical deployment of different levels of diverse equipment and procedures to prevent the escalation of anticipated operational occurrences and to maintain the effectiveness of physical barriers placed between a radiation source or radioactive material and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions."

Diversity. "The presence of two or more redundant systems or components to perform an identified function, where the different systems or components have different attributes so as to reduce the possibility of common cause failure, including common mode failure. Examples of such attributes are: different operating conditions, different working principles or different design teams (which provide functional diversity), and different sizes of equipment, different manufacturers, and types of equipment that use different physical methods (which provide physical diversity)."

Instrumentation and control. “Instrumentation means the monitoring of variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Control means the appropriate controls to maintain these variables and systems within prescribed operating ranges.”

Loss of coolant accidents. “Loss of coolant accidents mean those postulated accidents that result from the loss of reactor coolant at a rate in excess of the capability of the reactor coolant makeup system from breaks in the reactor coolant pressure boundary, up to and including a break equivalent in size to the double-ended rupture of the largest pipe of the reactor coolant system.”

Nuclear power plant. “A nuclear power unit means a nuclear power reactor and associated equipment necessary for electric power generation and includes those structures, systems, and components required to provide reasonable assurance the facility can be operated without undue risk to the health and safety of the public.”

Physical separation. “Separation by geometry (distance, orientation, etc.), by appropriate barriers, or by a combination thereof.”

Redundancy. “Provision of alternative (identical or diverse) structures, systems and components, so that any one can perform the required function regardless of the state of operation or failure of any other.”

Single failure. ‘‘A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure.”

Definitions from IAEA (2011).

CHAPTER 1: INTRODUCTION

If you ask electricity or chemical producers what their main requirements are for I&C systems in power and chemical plants and for enterprise management, you will almost always get the same answer. The correct information at the adequate time and the right place is what they expect and that for minimum investment and maintenance costs.

For private and personal use we would seem to have the answer: the Internet. But in the past few years this has also started to be used in the I&C sector in general and in the field of power plant and chemical industry. Almost all I&C suppliers now offer expansions and upgrades to existing systems to enable remote use of at least part of the locally available functions. The communication structures used here are similar with those of the Internet.

The I&C architecture and systems including the plant operations personnel in the control room is the "central nervous system" of a nuclear power plant. The I&C system senses physical and process parameters by using various components, integrate the information, do calculations, monitor selected aspects of the plant's health and make automatic adjustments to plant operations. To ensure safety, the system will also respond to failures and off-normal events. In summary, according to IAEA (2011), the purpose of the I&C system at a nuclear power plant is to enable and ensure efficient, safe and reliable power generation.

Progress in electronics and information technology has created incentives to replace traditional analogue I&C systems in nuclear power plants with digital I&C systems. The benefits of a digital I&C architecture are obvious. Firstly, it matches the mainstream of the IT world and enables integration of plant-wide communication. This is an absolute requirement for information provision in energy markets. Secondly, this also yields additional benefits for system and equipment maintenance and management. Digital systems offer better plant performance and additional diagnostic capabilities.

Analogue components will gradually become obsolete in the shift to digital components and systems. As a result, the nuclear industry will modernize existing analogue I&C systems to digital I&C systems, as well as implementing new digital I&C systems in new plants. Digital I&C systems have posed new challenges for the industry and regulators.

1.1 The problem statement

Digital I&C technology has been used widely in other industries (e.g. petrochemical), but has been adopted slowly in the nuclear industry. Digital I&C architecture and systems will be a radical change from traditional nuclear power plant analogue I&C architecture and systems. According to IAEA (2011) the nuclear power industry is slow to apply new technologies, especially digital and software systems, due to the need for safety assurance. This occurred due to the lack of confidence in the reliability of digital programmable devices and systems, as well as the challenging and complex licensing process of digital I&C systems. Digital I&C systems raise unique or additional issues to which analogue I&C systems are not subjected and the application of digital I&C systems generate some key safety and security issues. In the nuclear industry the following are some major issues associated with the application of digital I&C systems:

- the defence-in-depth principle,
- common cause failures,
- digital communication and networks,
- cyber security, and
- safety assessment in the licensing process.

The purpose of this study is to analyse and evaluate two selected I&C architectures – the UK EPR reactor I&C architecture from EDF and AREVA and the AP1000 reactor I&C architecture from Westinghouse. The evaluation outcome and characteristics of these two I&C architectures are then interpreted and verified against the drivers and tactics, as identified and developed from the NNR position paper PP-0017, to determine and demonstrate compliance with the NNR's requirements of safety and performance. The best practices and characteristics from the selected I&C architectures and the NNR requirements are used to finally synthesise a proposed digital I&C architecture.

1.2 Objectives of the study

The objectives of this study are therefore the following:

- Identify and develop drivers and tactics from the NNR position paper PP-0017.

- Analyse and evaluate the EPR architecture to determine the characteristics and shortcomings. These characteristics are verified against the NNR requirements to determine compliance.

- Analyse and evaluate the AP1000 architecture to determine the characteristics and shortcomings. These characteristics are verified against the NNR requirements to determine compliance.

- Use the best practices and characteristics from both architectures as well as the NNR requirements to synthesise a proposed digital I&C architecture.

1.3 The need for the study

Most of the current nuclear power plants are facing challenges in several I&C areas with aging and obsolete components and systems. All new nuclear power plants will be equipped with digital I&C architectures and systems. The increased functionality of a digital I&C system will open up new possibilities to better support operations and maintenance activities in the nuclear power plant.

1.4 Delimitations

This study is not attempting to analyse and to evaluate all the different existing and available architectures.

This study is limited to the conceptual level of the architectures and not attempting to evaluate the details or the individual components in the different architectures.

1.5 The outline of the study

The study is outlined as follow:

Chapter 1 gives a basic introduction on the requirements for I&C systems in nuclear power plants. The concept of digital I&C architecture and systems is introduced together with some general benefits. The problem statement and study objectives are also given in this chapter.

Chapter 2 explains the differences between the Control and the Protection systems for a nuclear power plant. The high level functional overview of the I&C functions are also described in this chapter as well as the safety classification of I&C functions and systems.

Chapter 3 starts with an investigation into the major issues associated with the application of digital I&C systems. A method is provided to develop an I&C architecture based on selected architectural drivers and tactics. This chapter is concluded with a simplified and ideal I&C architecture for nuclear power plants.

Chapter 4 provides the drivers and tactics, used for the design and implementation of digital I&C architectures and systems for nuclear installations, developed and identified from the NNR position paper PP-0017.

Chapter 5 reports on the technical assessment of the EDF and AREVA UK EPR I&C architecture. This chapter presents an overview of the architecture as well as the summarised findings of the I&C assessment of the Pre-Construction Safety Report.

Chapter 6 reports on the technical assessment of the Westinghouse Electric Company AP1000 I&C architecture. This chapter presents an overview of the architecture as well as the summarised findings of the I&C assessment of the Pre-Construction Safety Report.

Chapter 7 evaluates and verifies the assessment results of both the UK EPR architecture and the AP1000 architecture against the drivers and tactics as identified and developed from the NNR position paper PP-0017.

Chapter 8 synthesise a proposed digital I&C architecture based on the drivers and tactics as developed from the NNR position paper PP-0017 together with the best practices and characteristics from the EPR and AP1000 architectures.

Chapter 9 offers a conclusion and recommendations for this research project and suggestions for future research to be done.

2.1 Generation of control systems

In the late 1960s, electronic computers made their debut in power and petrochemical plants. The first application on these computers was a sequence-of-event recorder and display.

The next generation of electronic computing in power and petrochemical plants was introduced at the end of the 1980s. This generation used local networks that enabled a client / server architecture. This structure and architecture is still in use in most I&C systems today.

After the introduction of the Internet, the third generation of I&C systems and architecture was developed as an extension of the client / server architecture. The resulting system architecture would come to be known as “web-enabled”. It is also a fact that this third generation of I&C systems and architecture is still made up of a number of different subsystems and components. This will lead to increased maintenance costs and integration complexity in the long run.

The latest trend in petrochemical as well as in power plant I&C systems is a system structure called “web-based”, also known as the fourth generation of I&C architectures. Rainer (2006) explained that the cornerstone here is the basic architecture of the Internet with its three tiers: the presentation, the processing, and the data tier. Figure 1 shows the development of the different generations over the last fifty years.

It can be stated that the I&C architectures described here for the third and fourth generations support the trend towards increased and optimised centralization.

Rainer (2006) stated that in the energy markets an additional factor that is becoming increasingly significant in addition to the standard considerations of high reliability and a long lifetime for I&C systems is not merely the input of the maximum amount of data but far rather the input of the right information and thereby the important information into the decision-making process in good time and at the right point.

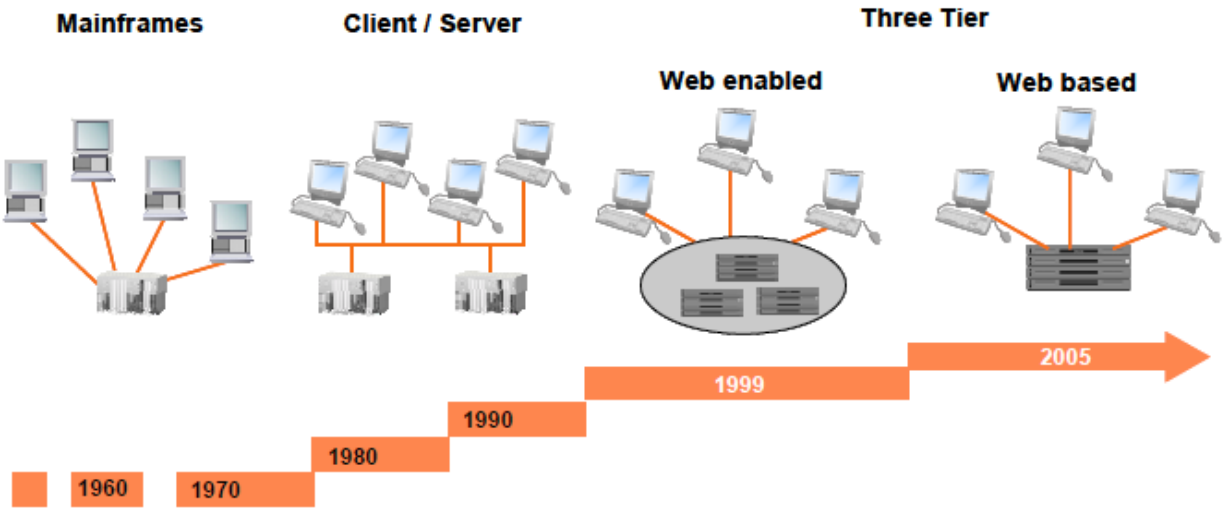

Figure 1: High level overview of I&C main functions (Rainer, 2006).

With the quick development of digital I&C systems, the analogue I&C systems in nuclear power plants will be replaced with digital I&C systems. Safety assessments remain an important factor with the shifting away from analogue to digital systems. However, the complex and different characteristics as well as interconnectivity of these systems make such assessments very difficult. The biggest difference between digital and analogue systems is in the I&C architecture. Analogue systems do not share hardware elements between redundant channels. The replication of the needed number of independent redundant channels provides the desired level of system reliability.

Digital systems rely mostly on electronic semi-conductor components and software to process and transmit multiple signals and information. Due to the differences in system architectures between analogue and digital, the failure characteristics are also different. In analogue I&C systems, the system failure occurs due to degradation and aging of components in the system.

2.2 Control and protection systems

The control and protection system in a nuclear power plant has a safety related function. According to the NRC, Criteria 13, “the I&C system shall be provided to monitor variables over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to ensure adequate safety, including those variables and systems that can affect the

fission process, the integrity of the reactor core, the reactor coolant pressure boundary and the containment and its associated systems". Comper (2003) explained that appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

I&C system is provided to control and monitor the neutron flux, control rod positions, temperatures, pressures, fluid flow and levels so as to ensure that adequate safety can be maintained. Instrumentation is provided in the reactor coolant system, steam and power system, the containment, safety systems, radiological waste systems and other auxiliaries and support systems. Parameters that must be provided for the operators under normal operating and accident conditions are displayed in the control room in proximity to the pertinent control devices for maintaining the indicated parameter in the proper range. The quantity and type of process instrumentation provided ensures safe and normal operation of all systems over the full operating range of the unit. The reactor control system is designed to maintain automatically a programmed average temperature in the reactor coolant during steady-state operation and to ensure that plant conditions do not reach reactor trip settings as the result of a transient caused by load change.

A wide spectrum of measurements is displayed for operator information, many of which are processed to provide alarms. These measurements provide notification and allow correction of conditions having the potential of leading to accident conditions. Typical indication measurements are rod positions, rod deviation, insertion limit, rod bottom, rod control system failure, in-core flux and temperature, protection system faults and protection test mode. Pressurizer pressure, level and reactor coolant system are monitored and alarmed to ensure that the reactor coolant system pressure is maintained within design operating limits. Containment pressure is monitored and alarmed to enable the operator to operate the containment vacuum system as needed to maintain the design operating pressure inside the containment. (Comper, 2003)

2.3 Protection and trip systems

According to the USNRC, Criteria 20, the protection and trip system shall be designed to automatically initiate the operation of appropriate systems, including the reactivity control systems, to ensure that the specified acceptable fuel design limits are not exceeded as a result of anticipated operational occurrences and to sense accident conditions and to initiate the operation of systems and components that are important to safety.

The reactor protection and trip system equipped with appropriate redundant channels (3 channels, 2-out-of-3 logic) is capable of coping with transients where insufficient time is available for manual corrective action. The design basis is in accordance with international standards. The reactor protection and trip system will automatically initiate a reactor trip when any variable monitored by the system or combination of monitored variables exceed the predefined set-points. The set-points provides for an envelope within which a safe operating conditions with adequate margin for uncertainties to ensure that design limits are not exceeded. Reactor trip is initiated by removing power to the rod drive mechanisms of all the full-length rod control assemblies. The reactor protection and trip systems also include the safety features actuation systems which automatically initiate emergency core cooling and other protection and emergency functions when sensing accident conditions. Redundant analogue channels measuring diverse variables are used. Manual actuation of protection systems may be performed when enough time is available for operator action.

According to Comper (2003), a circuit that is diverse from the reactor trip system automatically initiates a reactor trip through the opening of the RAM breakers and initiates a turbine trip under conditions indicative of an Anticipated Trip Without Scram (ATWS).

2.4 Functional overview of the I&C architecture

The I&C architecture and systems can be characterised by making use of a high level functional overview. This will give a high level view that focus on plant-wide systems as well as the objectives of these systems. IAEA (2011) stated that this high level functional overview addresses the following – sensory, communications, monitoring, display, control and trip. This high level functional overview is also outlined in Figure 2 below.

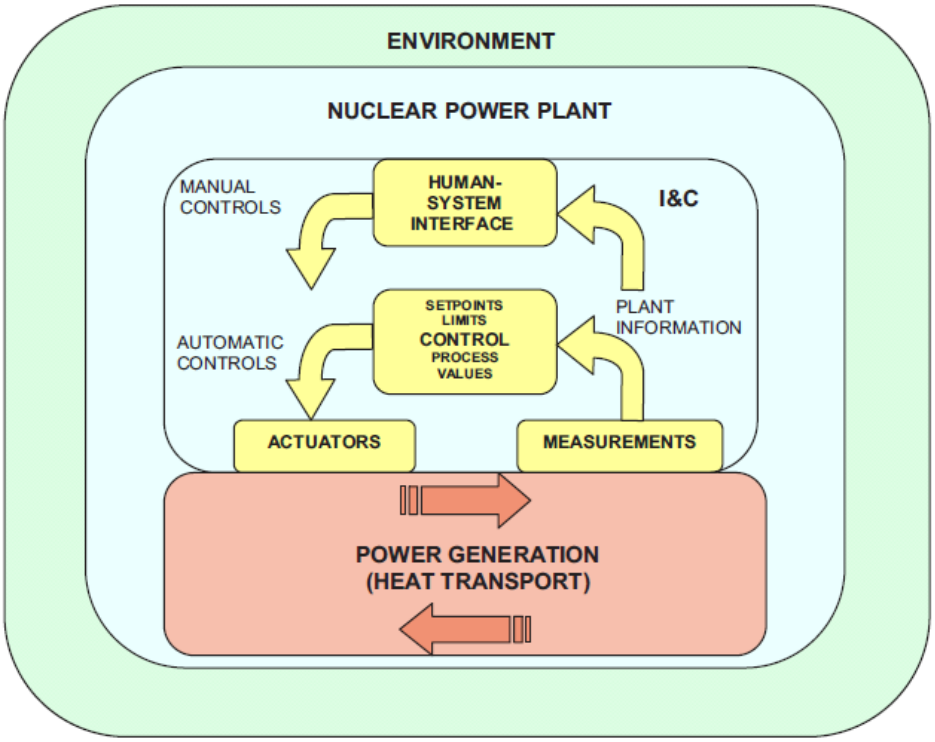

Figure 2: High level overview of I&C main functions (IAEA, 2011).

A block and flow diagram of a general I&C function is shown in Figure 3 below. The sensor is used to measure the physical or process parameter. This measured signal is then normalised by making use of a signal conditioner. Signal processing is the more complex part of the diagram. It involves scaling, linearization, or filtering of the normalised signal and the calculation of the deviation between this and the designed set point.

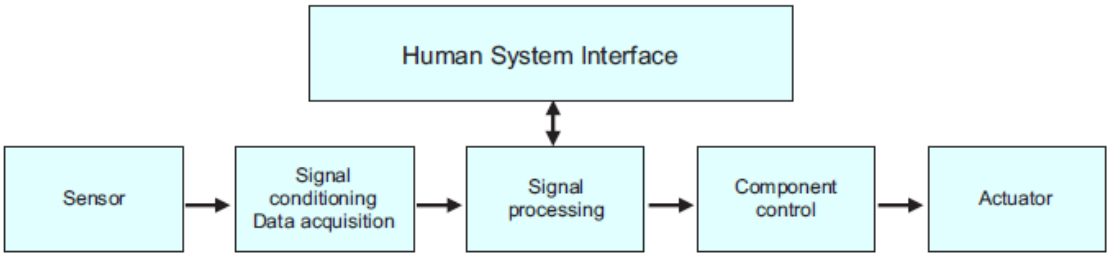

Figure 3: Block diagram of a typical I&C function (IAEA, 2011).

The I&C function will now be looked at from a physical point of view. In terms of signal processing and how control is performed, analogue and digital I&C systems are hugely different. This will be demonstrated with the assistance of Figure 4. Analogue voltages and current together with analogue electronics are used in analogue I&C systems. Digital I&C systems do the processing of the signals and control by means of digital processors containing software. The parameters are represented using binary (0 and 1). Thus, from a physical point of view the differences are significant, but functionally both solutions are similar.

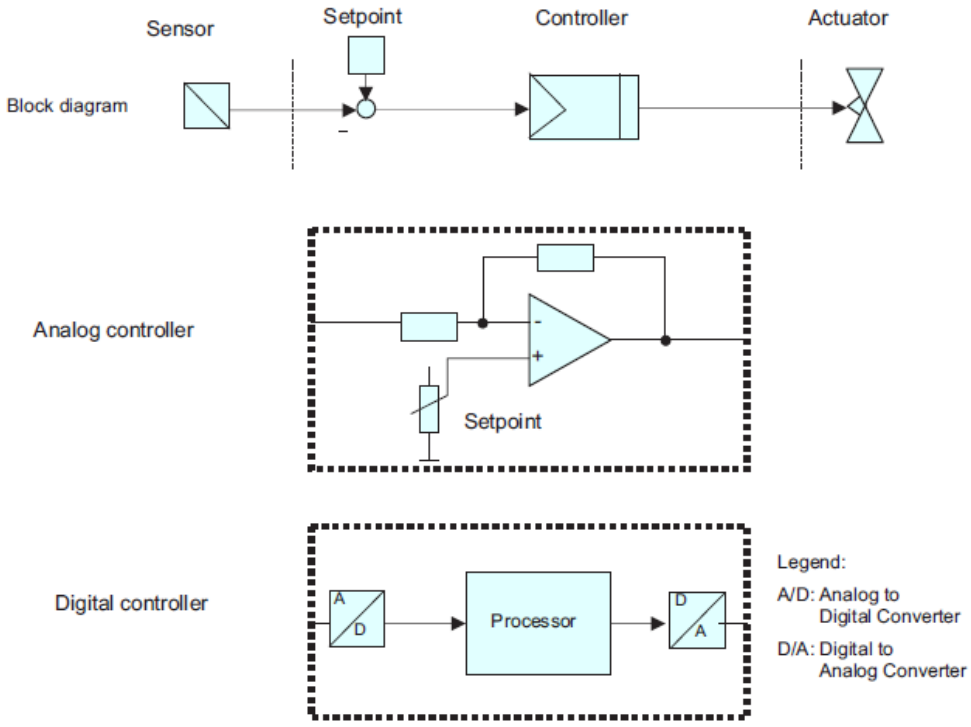

Figure 4: Analogue versus digital I&C systems (IAEA, 2011).

The configuration as shown in Figure 3 can now also be characterised as physical I&C components – the field devices (e.g. sensors, actuators, etc.) are the interface with the processes. The interconnection and communication between the field devices and the computational elements are accomplished with field communication (e.g. hard wired). The computational elements are the control and protection system, which also provides data acquisition. The computational elements can range in various forms from relay-based logic through to distributed control systems. The high-level

communication provides interconnection between the different systems as well as with the human-system interface (HSI). The HSI provides the display and interaction mechanism for the plant operating personnel.

Figure 5 is a simplified functional overview of the nuclear power plant I&C architecture. This functional overview must ensure a safe and reliable plant, even during failure conditions. To get an understanding of the system, the I&C functional overview must be subdivided according to its main functions as follow:

- Sensors – the interface with the process to take measurements continuously of the variables.
- Operational control and monitoring – process the data, optimize plant performance and manage plant operation.
- Safety system – to keep the plant in a safe operating condition and to shutdown the plant safely in the case of failure.
- Communication systems – to accommodate data and signal transfer (wires, fibre optics, etc.).
- Operators – human system interface; provide information to operating personnel and provide interaction with the I&C system.
- Actuators – this is devices (e.g. valves) to adjust the physical processes.

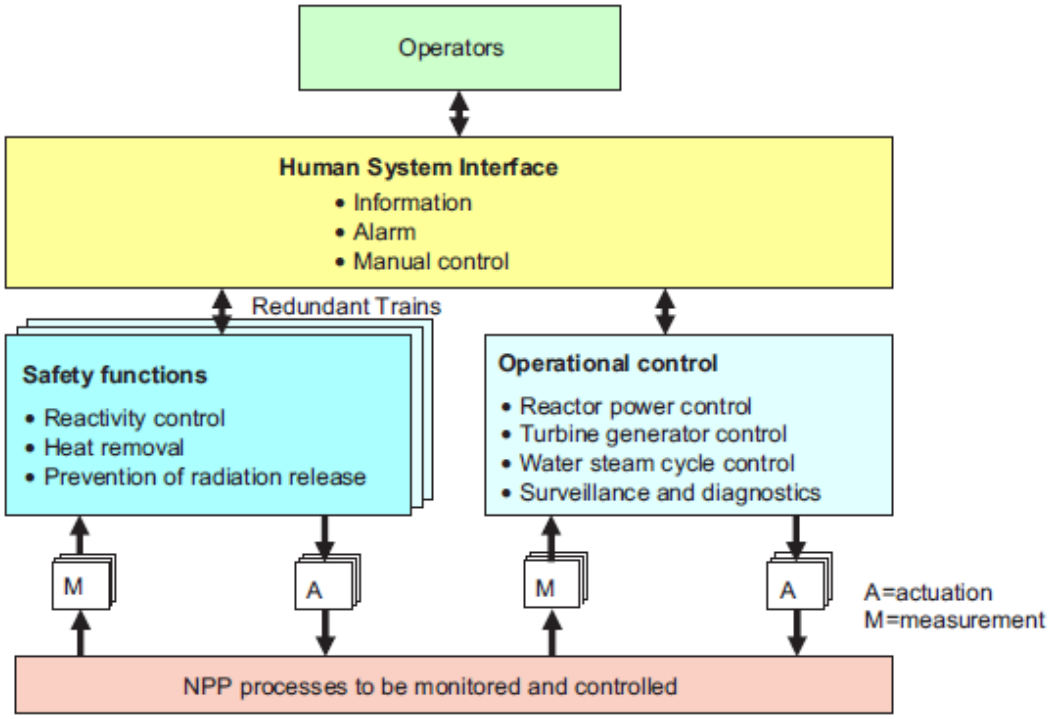

Figure 5: Functional overview of NPP I&C architecture (IAEA, 2011).

There has been tremendous development and advances in digital electronics and communication networks. Most of these new developments and technologies have been applied to digital I&C systems, which include hardware and software. Numerous upgrade projects have demonstrated that digital I&C technology can provide improvements in several aspects.

2.5 Safety classification of I&C functions and systems

The safety classification of I&C functions is usually performed using a combination of deterministic methods, probabilistic methods and engineering judgement. Once the I&C functions are classified, systems and components are assigned to classes according to the highest level function that they must perform. Typical nuclear power plant safety functions in which I&C systems have a significant role are: reactor trip, emergency core cooling, decay heat removal, emergency power supply, containment heat removal, etc.

Safety related I&C functions are those that are not directly safety functions but are otherwise important to safety such as functions that maintain the plant within a safe operating envelope under normal conditions, support radiation protection for plant workers, or add defence-in-depth to the plant's response to accidents. Examples of safety related I&C functions are: reactor power control, fire detection, radiation monitoring, display of information for planning emergency response, etc.

Non-safety I&C functions are those that are not necessary to maintain the plant within a safe operating envelope. Examples of non-safety I&C functions are: feedwater re-heater control, demineralizer control, intake and discharge screen control.

The IAEA Safety Standard Series NS-G-1.3 (2002) provides more information on the classification of I&C systems important to safety. According to IAEA (2011), there is many other classification schemes in common use as illustrated in Table 1.

Table 1: A comparison of different classification systems (IAEA, 2011).

National or international standard	**Classification of the importance to safety**				
IAEA NS-R-1	Systems Important to Safety				Systems Not Important to Safety
	Safety		Safety Related		
IEC 61226 Functions Systems	Systems Important to Safety				Unclassified
	Cat. A Class 1	Cat. B Class 2	Category C Class 3		
Canada	Category 1		Category 2	Category 3	Category 4
France N4	1E	2E	SH	Important to Safety	Systems Not Important to Safety
European Utility Requirements	F1A (Auto.)	F1B (Auto. and Man.)	F2		Unclassified
Japan	PS1/MS1*		PS2/MS2	PS3/MS3	Non-nuclear Safety
Rep. of Korea	IC-1		IC-2		IC-3
Russian Federation	Class 2		Class 3		Class 4 (Systems Not Important to Safety)
Switzerland	Category A		Category B	Category C	Not important to safety
UK Functions Systems	Cat. A Class 1	Cat. B Class 2	Category C Class 3		Unclassified
USA and IEEE	Systems Important to Safety				Non-nuclear Safety
	Safety Related, Safety, or Class 1E		(No name assigned)		

*PS: prevention system, MS: mitigation system

3.1 Different architectures for different industries

Some fundamental differences affecting I&C systems and architectures between nuclear power plants, petrochemical facilities, and civil aircraft are as follow:

- The hazard magnitudes are significantly different. The potential hazards to the general public and the environment from a nuclear power plant – especially in terms of the risk of having to evacuate and cleaning up areas for many years – are greater than those for any other potential industrial hazards.

- In civil aviation the persons at risk (the passengers) are accepting that they are taking on the risk by buying the tickets. In our day-to-day activities, we each do some sort of risk and benefit assessment. The acceptance of risk is a difference between voluntary and involuntary, and between risks where there is also benefit (e.g. increased salary) and where there is none. These factors, together with others, mean that the reliability requirements are different for the I&C systems and components for NPPs, petrochemical industry, and civil aviation.

- Civil aviation inevitably has to combine and interconnect control (non-safety) systems and protection (safety) systems. In both nuclear power plants and petrochemical industry it is desirable to separate control and protection systems.

3.2 Basic principles for safety

According to IAEA (2003), an important concept in the design of NPPs is the plant design basis which contains the basic philosophy of how the plant is intended to function in different conditions. The plant design basis is in practice a set of written explanations of how a system, structure, and components are supposed to function under certain operational conditions. This document is of great importance in creating an understanding of the requirements for I&C systems.

One of the most significant basic design principles through which safety is incorporated into the NPPs is defence-in-depth. Defence-in-depth involves the provision of diverse and independent barriers that

protect against the identified and known threads. A further application of the defence-in-depth principle leads to the application of diversity, separation and redundancy in systems and components to provide protection from random and unknown failures. For digital I&C systems the possibility that a common cause failure can undermine protection is one of the major issues discussed in the process of licensing a nuclear installation.

IAEA (2003) explained that the design of I&C systems and architectures is based on a top-down process, with subsequent step-wise refinements during the process. A second feature of the design process is a combination of synthesis and analysis. A design is proposed using a process of synthesis by matching available design characteristics against requirements to be fulfilled. The proposed design is then analysed in a validation process with certain assumed failures. This will then determine the consequences and compare it with defined acceptance criteria. If a design is acceptable, it can be further developed to a more detailed level.

3.3 Safety and security issues

The application of digital I&C technologies raise unique or additional issues to which analogue-based I&C systems used in the existing power plants are not subjected. These applications generate some key safety and security issues. The following are some major issues associated with the application of the digital I&C systems in the nuclear industry:

- the defence-in-depth principle,
- protection against common cause failures,
- digital communication and networks, and
- cyber security.

3.3.1 The defence-in-depth principle

The primary means of preventing and mitigating the consequences of accidents is with the defence-in-depth principle. The defence-in-depth principle is implemented through the combination of a number of independent and diverse levels of protection that would have to fail before harmful effects

could be caused to the public or to the environment. IAEA (2000a) identifies five lines of defence-in-depth that must be included in an NPP design:

- Prevent system failures and deviations from normal operations.
- Detect and intercept deviations from normal operating conditions to prevent anticipated operational occurrences from escalating to accident conditions.
- Control the consequences of accident conditions.
- Confine radioactive material in the event of severe accidents.
- Mitigate the consequences of radioactive release.

In traditional I&C designs, different systems often supported each of the lines of defence (see Figure 6). Strong independence must be provided between safety systems and safety-related systems. There is commonality among safety systems, but individual signals are processed by separate equipment. Engineered safety features actuation systems and reactor trip systems use different actuation logics, predominant failure modes of equipment are understood, and functions are designed to fail-safe when these types of failures happened. Signal and functional diversity are provided so that shared data would not jeopardize multiple lines of defence.

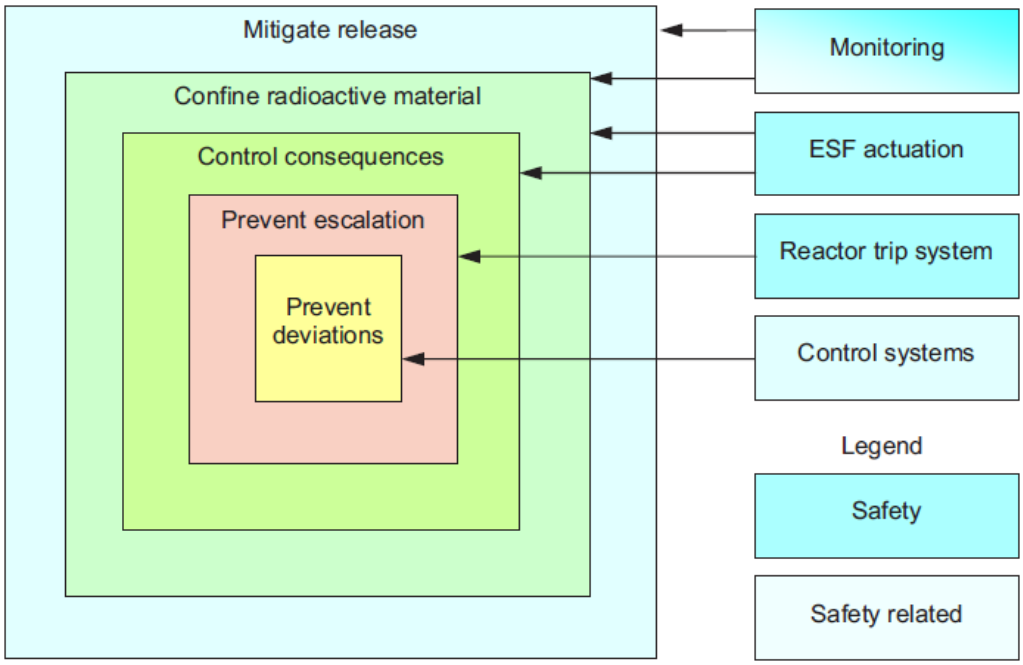

Figure 6: Typical I&C system relationship to plant defence in depth (IAEA, 2011).

The design of computer-based I&C systems must face new issues which, if not properly dealt with, may jeopardize independence between lines of defence or independence between redundant elements within a line of defence. The architectures of most computer-based I&C systems is fundamentally different from that of traditional I&C systems. In computer-based systems one or a few computers sometimes process all signals for one channel of both reactor trip and engineered safety features actuation functions. Furthermore, these components must process not only one signal that could induce a failure, but many. Therefore, a failure of an individual component affects not one, but many functions and may degrade operation of the I&C supporting two or more lines of defence. The scope of failures in computer-based systems may therefore be greater than in traditional systems unless the computer-based system is carefully designed to avoid this and analysed to identify potential vulnerabilities and confirm that they have been appropriately addresses. If such failures are limited to one of multiple redundant channels, each line of defence remains intact.

3.3.2 Protection against common cause failures

The use of defensive design measures and diversity is the general response to protect against common cause failures in I&C systems. Defensive design measures attempt to avoid systematic faults or preclude concurrent triggering conditions. Diversity uses dissimilarities in technology, function, designs, implementation, and so forth to prevent the potential for common failures. Common cause failure in I&C systems, according to IAEA (2011), results from:

- the triggering of a single systematic fault, or
- causally related faults by a single specific event.

IAEA (2011) also explained that a systematic fault affects all components of a specific type (hardware or software). A triggering mechanism is a specific event or condition that activates a faulted state and causes a system or component failure. The triggering mechanism may be related to environment, time, data, or hardware. Thus, a systematic failure is related in a deterministic way to a certain cause. The failure will always occur when the fault is challenged by the triggering mechanism.

In redundant systems, latent faults (such as software defects) are systematically incorporated in all redundant channels or divisions. Once triggered, the latent faults can become software failures that lead to common cause failure. Such failures can cause one or two possible conditions:

- outputs that change status (or values),
- outputs that fail “as-is”.

The first condition involves a spurious actuation of a safety function and is readily apparent. An “as-is” common cause failure is not revealed until there is a demand for a safety action. For a potentially unsafe common cause failure to occur due to a systematic fault, a number of conditions must be met as shown in Figure 7.

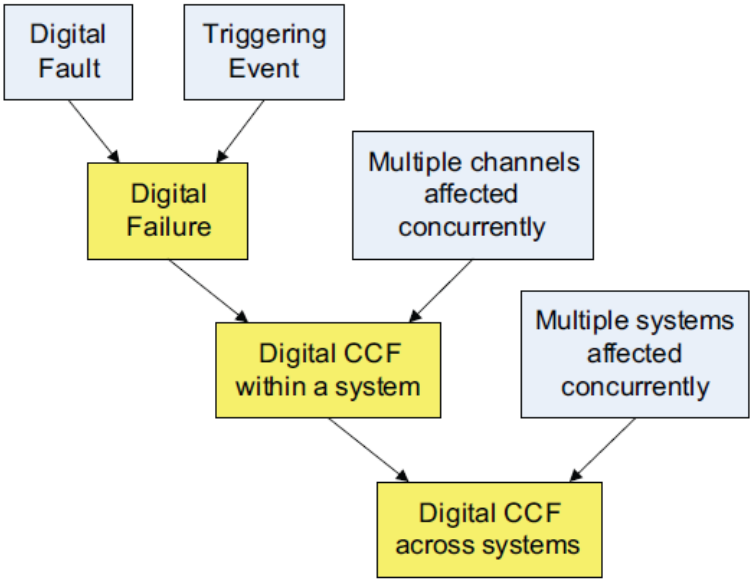

Figure 7: Conditions required creating a digital CCF (IAEA, 2009a).

To affect multiple systems, the systems must share the same fault(s) and be susceptible to the same trigger.

To reduce the potential for common cause failure in I&C systems, defensive design measures can be employed to avoid systematic faults or preclude the concurrent triggering conditions. Diversity is a complementary approach. The challenge for digital systems is to determine what combinations of defensive measures and / or diversity are effective and sufficient to adequately address common cause failure vulnerability. For digital I&C systems in NPPs, a diversity and defence-in-depth analysis should be conducted to demonstrate that vulnerabilities to common cause failures are adequately addressed. Quality assurance during all phases of software development, control, and validation and verification is critical to minimise the possibility of CCFs. (IAEA, 2009a)

3.3.3 Digital communication and networks

Often there is a need to share information between safety-related systems and safety systems, between systems supporting different plant lines of defence (for example where control and protection functions need information on the same parameter), or between redundancies within safety systems (for example, to vote redundant channels in making trip decisions). When this is done,

precautions are needed to prevent failures from propagating via the connections. In traditional I&C systems these connections were simple, point-to-point connections carrying individual signals.

The use of computers in NPPs has provided the opportunity for high level digital communication via a network between computers within a single safety channel, between safety channels, and between safety and non-safety computer systems. However, the digital communication network raises issues such as independence for inter-channel communication, and communication between non-safety and safety systems. Improper design of this communication ability could result in the loss of redundant or diverse computers' ability to perform one or more safety functions and thereby inhibit the safety system from performing its function.

The safety function processor through its instruction sequence should not be affected by any message or signal from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence. The main purpose of interdivisional communications should be the transmission of minimal messages, such as packed trip data words. Data that do not enhance the safety of the system should not be transmitted or received inter-divisionally. Communication architectures should have buffering systems to ensure there is no direct communication to the main safety processors, to enhance the ability of the safety processors to perform their safety functions without undue interference. Electrical isolation and consideration of functional dependencies are not sufficient to assure independence when a computer-to-computer communication is involved. Communication faults should not adversely affect the performance of required safety functions in any way. For proper independence of the safety system from non-safety equipment, physical, electrical and communication isolation should be ensured.

Other digital communication and networks also include the following - communication between control systems and IT systems as shown in the following Figure.

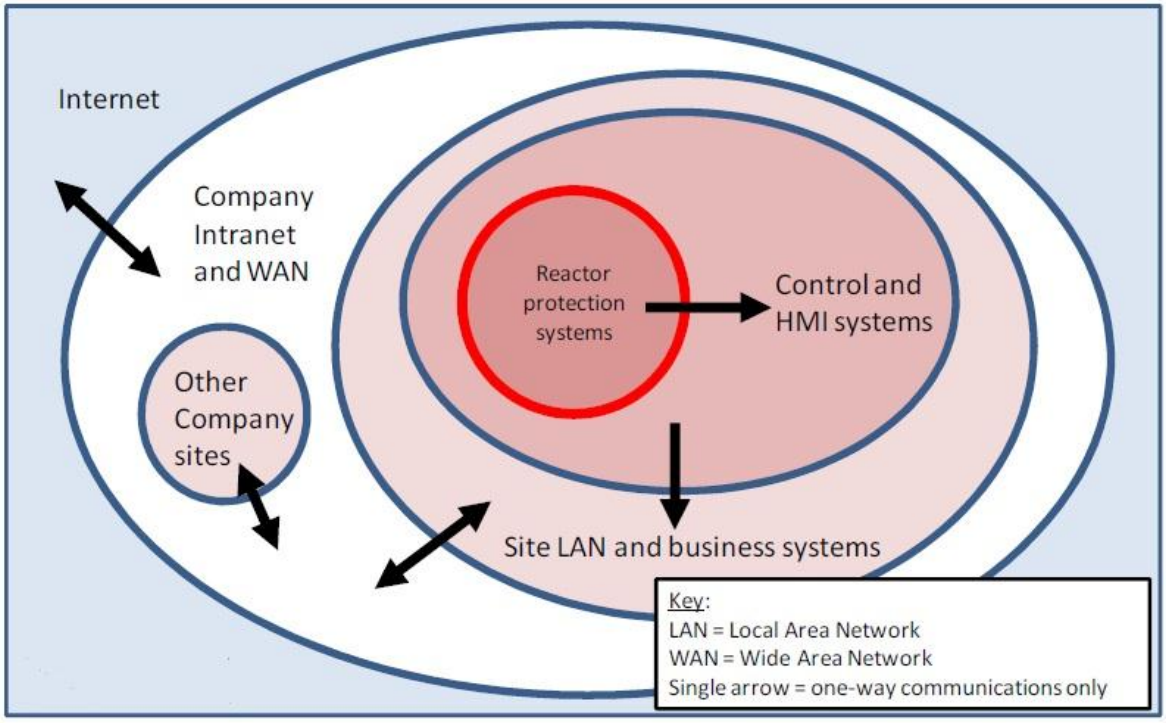

Figure 8: Communication barriers and firewalls in NPPs (Thomson, 2012).

It may be very convenient and easy to create communication links between control and / or protection systems and the IT systems, to improve business information communication and exchange. It may also be easy to use mobile memory mediums to transfer data between the control and / or protection systems and the IT systems. Robust physical protection and governance are required, and these will also include data encryption / decryption and virus checking.

3.3.4 Cyber security

The increasing prevalence of digital I&C systems and general IT-technology offers several benefits but also introduces new vulnerabilities and may open up facilities to security threats. Cyber-attacks could be associated with information theft, a disgruntled employee, a hacker, organised crime, a nation state, or a terrorist organization. Attacks may lead to loss of confidentiality (e.g. unauthorised access to information), loss of integrity (e.g. modification of information, software), or loss of availability (e.g. preventing data transmission and / or shutting down systems).

As an example, Stuxnet is a computer worm discovered in June 2010 at an Iranian uranium enrichment plant. It used “zero-day” weaknesses in Windows to attack Siemens Simatic controllers. It was probably introduced and transmitted using mobile memory media. This incident emphasised the importance of cyber security in nuclear installations as well petrochemical industries. (Thomson, 2012)

The digital I&C development process should address potential security vulnerabilities systematically at each stage of the digital I&C system life cycle. Cyber security should be a fundamental component of I&C design and specification. Especially computers used in protection / safety and safety-related systems must be well protected.

The tools for protecting against threats and building barriers include both technical tools, such as intrusion detection, virus scanners, firewalls, encryption and access control, (e.g. password and biometric identification) as well as administrative tools such as the application of a well-designed security policy, security zones, security management systems, periodic awareness training, and the development of a security culture. There are current regulations, guidance, and standards for I&C safety system design that have a close relationship with cyber security. Cyber security vulnerability might be significantly reduced if such regulations, guidance and standards are followed rigorously.

3.4 Architectural approach to design of digital I&C systems

Digital I&C systems can on a basic functional level be separated into hardware and software. On a higher level most software in digital I&C systems have made a distinction between system software and application software.

The architecture requirements for digital I&C systems are dependent on the safety role as one of the quality attributes of a particular I&C system. For example, I&C systems providing the nuclear power plant reactor protection role are normally implemented by using four way redundant trains of equipment and sub-systems, with each train or sub-system performing the same protection function. The four way redundant trains or sub-systems require complete independence (physical separation) of the trains to provide defence against internal and external hazards. A voting logic system (e.g. 2-out-of-4) is used to implement the required safety or protection function such as reactor trip.

To enable the functionality of the voting logic for the initiation of the safety and trip functions across the multiple trains, it is a requirement to have communication channels across the trains to transfer the relevant information to the voting logic. This requirement for cross communication to enable the voting logic has an impact on the physical plant and building layout and on the physical implementation required to maintain the defence against hazards.

I&C systems with a lower safety role (e.g. turbine control) than reactor protection do not require the same levels of redundancy. This is due to less stringent requirements for defence against potential hazards and failure.

The general I&C architecture selected is based on multiple nodes that communicate with each other using gateways. Redundant data communication channels are required to ensure that functional integrity is maintained in cases of failures. Divisions are sometimes introduced between the nodes and the data communication channels to reflect, for example, different safety categories or plant sub-systems.

A generally known approach to improve the reliability of I&C systems or nodes is the use of hot standby systems or nodes. This type of configuration allows a secondary standby system or node to switch into operation if the primary duty system or node fails. This approach provides a significant higher overall reliability of the I&C architecture.

3.5 Development of the architecture

The overall I&C architecture has to be frozen early in the design process for new build nuclear power plants. This is because the I&C architecture leads to definitions of building space requirements and physical system separation requirements (for cabinets, switchgear, and separate cable routes) so that the civil structures can be designed.

Hence the planning program for nuclear power plant design and construction needs to address I&C architecture and systems at an early stage.

It is recommended that the I&C systems should be designed, implemented and integrated with latest digital technology. It is also necessary to develop a generalised I&C architecture as a model for most

I&C systems and also ensuring that the I&C systems with digital technology complies with the necessary requirements of safety and performance.

The trend is to design I&C systems with digital-based components. The digital I&C architecture describes the I&C systems and communication channels at a high level, which is not easy with analogue I&C systems. Reflecting the characteristics quality attributes of existing analogue I&C systems into the digital I&C architecture and systems is a key activity in developing the I&C architecture. The issues in developing the digital I&C architecture are summarized by Wojcik (2006) as follow:

- The architecture should satisfy nuclear safety requirements.
- Required functions and / or systems should be well deployed in the architecture.
- Signal and communication interfaces should be well represented in the architecture.
- Architectural abstraction shall be well understandable and assessable.

3.5.1 Process to develop the architecture

IEEE (2000) defines an I&C architecture as “the organizational structure of a system or component, a system as a collection of components organised to accomplish a specific function or set of functions, and system architecture as the structure and relationship among the components of a system”. From this definition, architecture is associated with the structure of a system and the relationship among components, presents a high level description of what to build, and results from the earliest design decisions.

Wojcik (2006) has developed the architectural-based development method into an attribute-driven design (ADD) method. In the ADD method (ADDM), the architecture is driven by architectural drivers that are defined by Bass (2003) as quality attribute requirements that drive the construction of architecture, which are the combination of functional, quality and business requirements that shape the architecture. Typical examples of architectural drivers are of availability, maintainability, usability, testability, security, modifiability, and performance. Wojcik (2006) also explained that in order to develop the I&C architecture satisfying the drivers, architectural tactics need to be determined or

developed. Tactics are defined by Bass (2003) as design decisions that influence the control of quality attribute responses. A combination of tactics grouped with the drivers determines the strategy of developing digital I&C architectures. According to Wojcik (2006), architectural tactics are fine-grained design approaches used to achieve the quality attribute requirements. For example, availability is achieved with tactics that are shown in the following Figure.

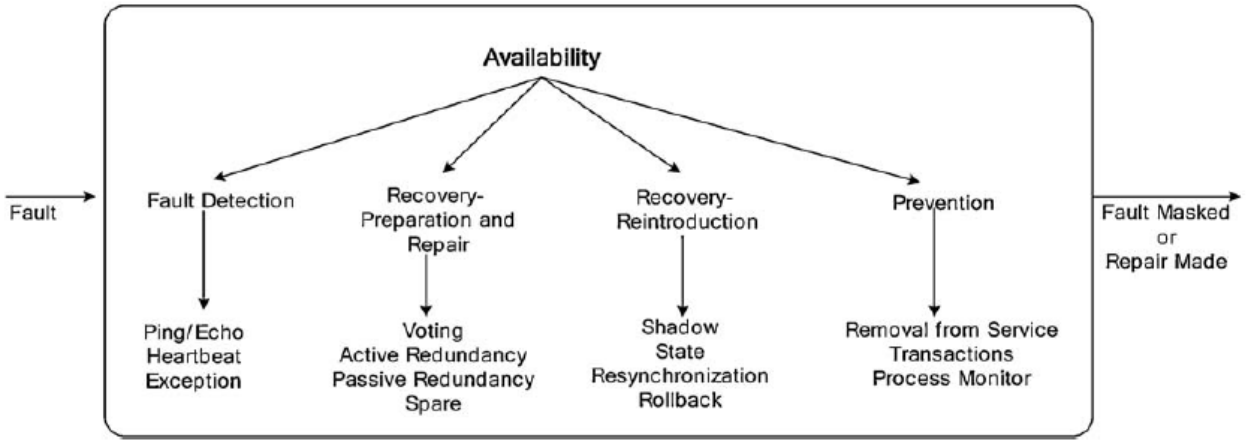

Figure 9: Tactics to achieve the availability of a system (Bass, 2003).

In Figure 9, availability is related to the detection of a fault, the recovery and repairing of the system or component from the fault, dealing with a case in which a system or components fails again after being recovered, and to prevent a fault. Figure 9 introduces tactics that are required in order to achieve the specified availability of a system. There are more tactics available to increase the availability.

Wojcik (2006) explained that the ADDM is a systematic approach that is a methodical approach repeated and learnable through a step-by-step procedure. It follows a recursive process that decomposes a system or system elements by applying architectural tactics that satisfy its driving quality attribute requirements. Wojcik (2006) provided the following 7 steps for the attribute-driven design method:

- Step 1 – Confirm there is sufficient requirements information.

- Step 2 – Choose an element of the system to decompose.
- Step 3 – Identify candidate architectural drivers.
- Step 4 – Choose a design concept that satisfies the architectural drivers.
- Step 5 – Instantiate architectural elements and allocate responsibilities.
- Step 6 – Define interfaces for instantiated elements.
- Step 7 – Verify and refine requirements and make them constraints for instantiated elements.

These steps are repeated until the I&C architecture satisfies all the architectural drivers. Although the ADDM was developed from the software engineering discipline, it contains a property which is applicable to I&C engineering discipline in producing an initial I&C architecture. Since the ADDM is a systematic approach it is reasonable to use this method for developing the I&C architecture. It is noted from Wojcik (2006) that the ADDM essentially follows a Plan-Do-Check (PDC) cycle. According to Wojcik (2006) the PDC is cyclically repeated until all objectives are met and the ADDM is also cyclically repeated until all significant architectural drivers are met. Wojcik (2006) also explained the ADDM in terms of the PDC as follow:

- Plan step – quality attributes and design constraints are considered to select which types of elements will be used in the architecture.
- Do step – elements are instantiated to satisfy quality attribute requirements as well as functional requirements.
- Check step – the resulting design is analysed to determine whether the requirements are satisfied.

Because the ADDM is motivated from the PDC cycle, it enable us to establish a process for developing the digital I&C architecture. The cyclic concept of the PDC and the attribute-driven design concept of the ADDM are used to establish the next process. The process presented by Wojcik

(2006) for developing the I&C architecture is called PDDA (Preparation, Decision, Design, Assessment), as shown in Table 2.

Table 2: Comparison of PDC, ADD and PDDA (Yong, 2011).

PDC	ADD	PDDA	
Steps	Steps	Steps	Activities
Pan	1	Preparation	Analyze the existing I&C systems, establish architectural goals, and determine architectural drivers
	2	Decision	Determine tactics that are applicable to the I&C architecture and satisfy the drivers and determine primitive architecture
	3		
Do	4		
	5	Design	Allocate functions and systems, design signal interfaces via communication or hardwire, and build the architecture by applying tactics
	6		
Check	7	Assessment	Evaluate the architecture

The PDDA is an iterative process to design the I&C architecture until all the requirements are met.

3.5.2 Developing the architecture based on PDDA process

3.5.2.1 Preparation

In the preparation step the following activities are performed: analysing the existing I&C systems and components (for an upgrade), establishing architectural goals, and determining I&C architectural drivers. (Wojcik, 2006)

Wojcik (2006) also gave the following examples of architectural goals: the use of a distributed control system (DCS) concept, the use of digital communication networks, and the compliance with nuclear safety and performance requirements.

There are many architectural drivers, as an example, a single failure criterion is determined as an architectural driver.

A single failure criterion is considered by Wojcik (2006) as the most important safety requirement. 10CFR50 App. A defines it as follow: “A single failure means an occurrence which results in the loss of capability of a component to perform its intended safety functions. Multiple failures resulting from a single occurrence are considered to be a single failure”. According to IEEE (1998) a nuclear power plant shall be designed to continuously perform required safety functions even if a single failure occurs. This is a first criterion of safety systems. The single failure criterion is selected as a first quality attribute for the I&C architecture.

For developing the DCS-based I&C architecture, the determinism, which is related to a deterministic timing, is considered by Wojcik (2006) as a second important requirement. The deterministic timing is defined by NUREG-0800 Ch. 7 BTP-14 as follow: “Timing is deterministic if the time delay between stimulus and response has a guaranteed maximum and minimum”. Since software is so flexible, DCS-based I&C systems are prone to violate the deterministic timing and the time delays caused by software cannot always be guaranteed. Wojcik (2006) stated that credit of safety to the systems cannot be given if the systems are not guaranteed to provide their functions in a deterministic manner.

3.5.2.2 Decision

In this step, the following activities are performed: determining tactics and determining primitive DCS-based I&C architectures. (Wojcik, 2006)

Tactics for meeting the single failure criterion are given in Figure 9. Tactics of fault detection and fault recovery in Figure 9 are selected, and more tactics are added for the criterion, as shown in Figure 10. The tactics in Figure 10 are based on the practices of a general NPP’s design.

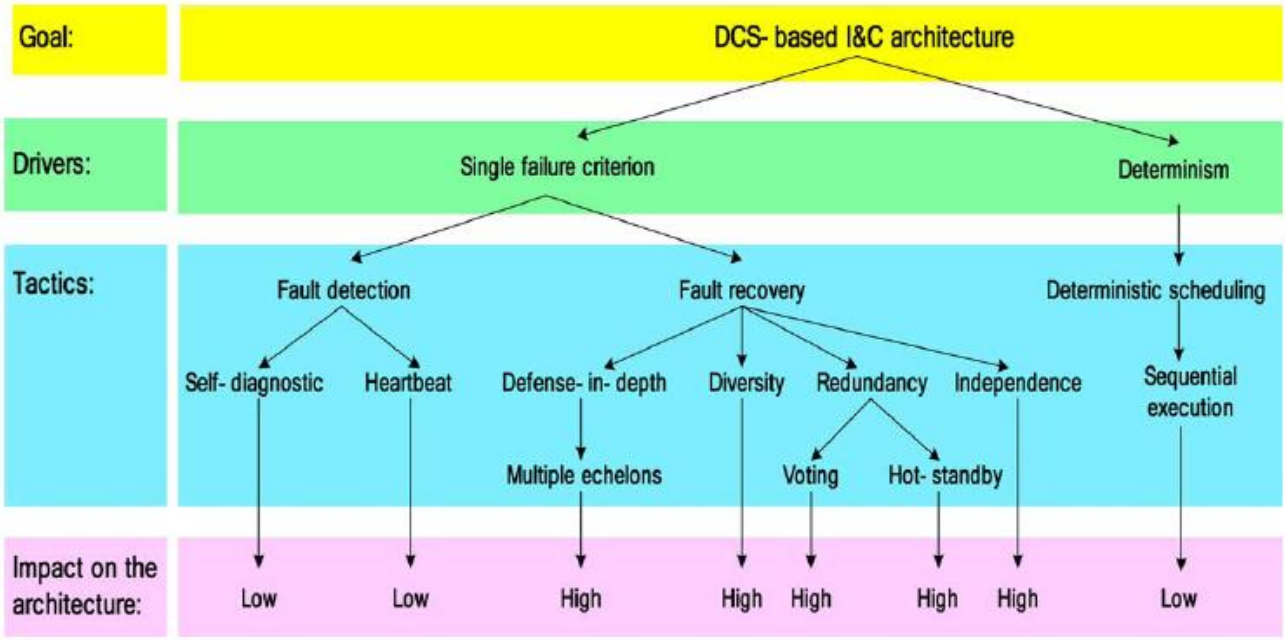

Figure 10: Selected architectural drivers and tactics (Yong, 2011).

A self-diagnostic is used to detect a fault that occurs inside a system. A heartbeat is used to detect a redundant counterpart's fault. The heartbeat is used to detect a fault that occurs in a source system that sends data. To achieve the fault detection to a maximum extend, both the self-diagnostic and heartbeat should be used complementary. According to Wojcik (2006), the impact of the self-diagnostic and heartbeat on the architecture is low since the self-diagnostic is implemented inside a system, and a means of data transmission is adequate to implement the heartbeat.

Defence-in-depth, according to US NRC (1994), is used to maintain the function of I&C systems with four echelons of control systems, reactor protection systems, engineered safety feature actuation systems, and monitoring and indicating systems. The impact of the defence-in-depth on the architecture is high due to additional systems or components. Diversity is used to prevent the common mode failures that are subject to occur when all the I&C systems or components are designed and manufactured with the same hardware and software.

The availability of a system can be increased by applying adequate redundancy. The redundancy should be applied differently to the non-safety systems and to the safety systems. Dual nodes are

required to achieve a minimum redundancy. The degree of redundancy of a safety I&C system is one of the main factors contributing to fault tolerance. The different configurable systems with their associated capabilities can be seen in the following Figure.

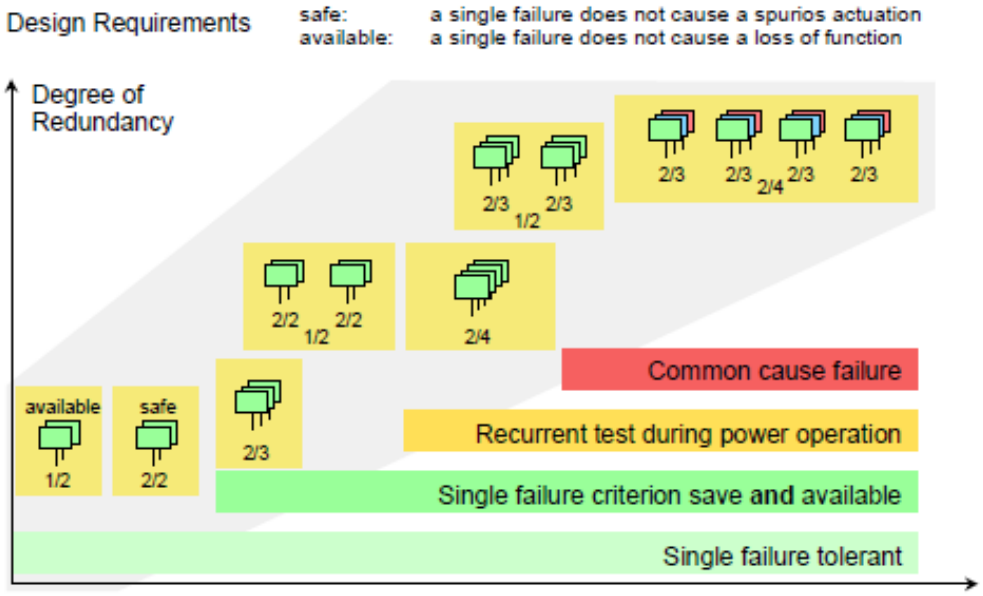

Figure 11: Selected architectural drivers and tactics (Prehler, 2001).

Hot-standby redundancy, in which the primary and secondary nodes run simultaneously, is commonly applied to the non-safety control systems. The primary and secondary nodes receive identical inputs simultaneously but only the primary is responsible for releasing outputs. The secondary node performs the same functions as the primary node, except for the output. The primary node sends a heartbeat to the secondary node periodically. When the secondary node does not receive a heartbeat from the primary node, the secondary node takes the output privilege from the primary node. According to Swaminatha (2005) the hot-standby cannot mask an incorrect result but the 2-out-of-3 voting logic can. Swaminatha (2005) also stated that the 2-out-of-3 voting logic is a minimum redundancy to filter an incorrect output resulted from the triple redundant components. This minimum voting logic is applied to the safety and protection systems that have critical logics to actuate a reactor trip.

Independence and logical separation is used to protect safety and trip systems from non-safety control systems. The safety and trip systems should not be interrupted by the non-safety control systems. The safety and protection functions required during and following any design basis events must be successfully accomplished.

Determinism is related to deterministic execution of instructions or functions, which is mainly concerned with a real-time system. The most important characteristic is that the real-time system should guarantee the repeatability of correct execution of functions within a minimum and maximum time limit. A sequential execution guarantees deterministic execution. With sequential execution, the execution time and priority of each task are pre-determined and fixed during operation. This solution is not required for all the I&C systems. It is proposed by Swaminatha (2005) that the safety systems should have the sequential execution, and the non-safety systems allow a task's pre-emption. Determinism is a matter of implementation inside a system and software related, the impact of the determinism tactic on developing the I&C architecture is low.

Finally, a primitive I&C architecture is shown in Figure 12. The safety and protection systems are shown with red colour and the non-safety control systems with blue colour. The systems and nodes are connected to communication networks that are divided into the safety and non-safety networks. The safety and non-safety networks are different and should be isolated from each other. The gateway is used to establish a safe communication connection between the two networks. The I&C architecture is developed by applying the selected tactics to the primitive I&C architecture.

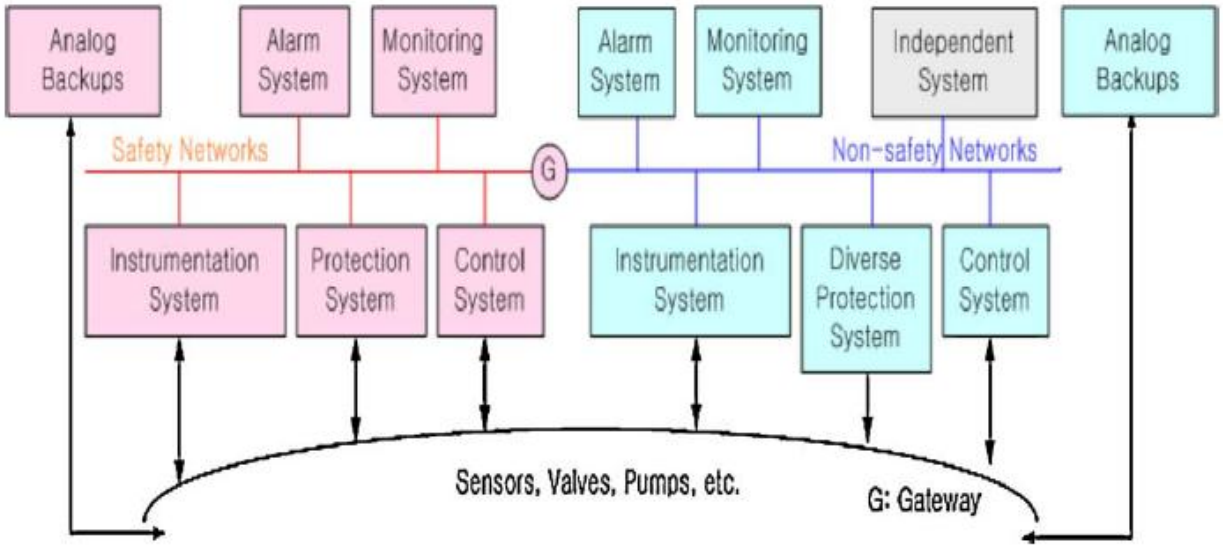

Figure 12: Primitive architecture (Yong, 2011).

3.5.2.3 Design

In this step the following activities are performed according to Wojcik (2006): assigning the I&C systems to the functional groups based on the primitive architecture, designing the networks, and developing the overall I&C architecture and system blocks applying the tactics.

A more detailed architecture is developed by applying the selected tactics in two parts: safety and non-safety. Voting logic is mainly applied to the safety and protection systems and the hot-standby tactic to the non-safety systems.

The network design in safety and protection systems is required in accordance with safety and performance requirements. According to Wojcik (2006), the network design adheres to the following criteria: utilizing the advantage of data communication, keeping safety channel independence, guaranteeing the flow of safety signals, and keeping independence between the different levels of safety systems. After defining the data transmission methods, the detailed architecture of safety I&C systems is developed. The safety systems are normally designed with quadruple redundant systems, which are four channelized systems. A protection or trip function is determined by a 2-out-of-4 voting logic. When one channel or train is out of service, the protection or trip function is determined by a 2-out-of-3 voting logic. This tactic ensures high availability.

The non-safety system is all about the performance. According to Wojcik (2006), the network design adheres to the following criteria: integrating the systems and maintaining diversity. After defining the communication channels and data transmission method, the detailed architecture of non-safety I&C systems is developed. As previously noted, the hot-standby tactic is applied to the non-safety systems and network design.

3.5.3 Deterministic considerations

According to Thomson (2012), the deterministic considerations for present purposes mean those considerations which are based on good engineering practices alone, as opposed to probabilistic risk considerations. Thomson (2012) summarised the following fundamental deterministic considerations for I&C safety and protection systems:

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

This simple set of requirements does not appear clearly and explicitly in any international standard. Instead, there is a mountain of large documents, which are very detailed and have been produced by considerable efforts. As Thomson (2012) stated – “the difficulty with these large international standards is that it can be challenging to differentiate the trees from the forest”.

3.5.4 Simplified and ideal I&C system architecture

Illustration of an idealised NPP I&C systems and architecture are shown below in Figure 13. The diagram is necessarily simplified – it is important that all engineers involved with the design (design engineers, safety regulators, client engineers, maintenance engineers, and future operators) have a understanding of the I&C architecture that is to be implemented.

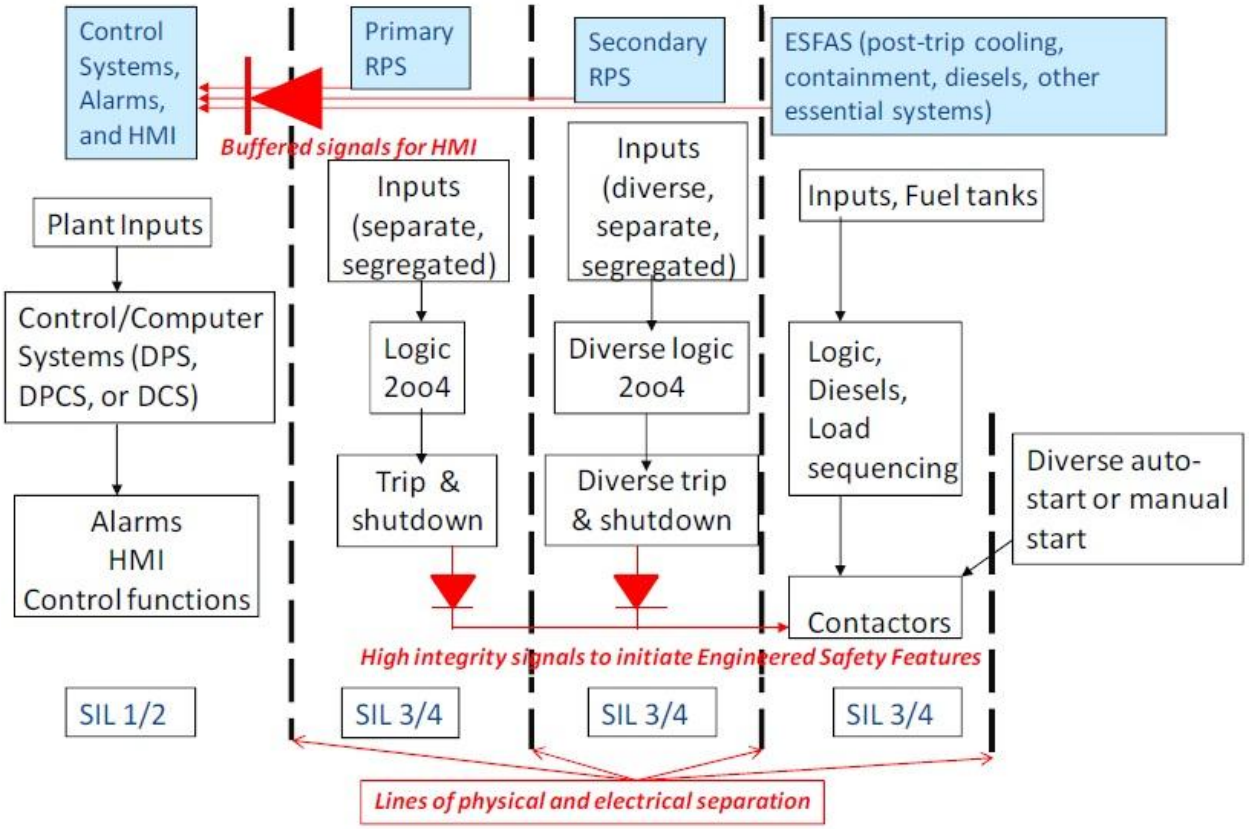

Figure 13: Simplified & Ideal I&C architecture for NPP (Thomson, 2012).

3.5.4.1 Short and long term accident management systems

Thomson (2012) stated that ESFAS (Essential Safety Features Actuation System) is designed to deal with short-term post-trip requirements to ensure decay heat removal and containment protection. The experience of Three Mile Island accident and other nuclear installation accidents have shown the need for local and remote plant status displays for long-term essential systems.

Thomson (2012) also added that 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 I&C system must be high-integrity (typically in the 10^{-3} to 10^{-4} PFD range), and the overall and related systems may be highly redundant; for example, there may be a significant amount of diesel-generating capacity.

According to Thomson (2012), 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.

3.5.4.2 Alarms and HMI

The HMI (Human Machine Interface) encompasses graphical displays, alarms, hardwired warning lights, and manual controls. Evidence from Thomson (2012) showed that human reliability is not good in high-pressure situations with serious time constraints. For this reason, Thomson (2012) claimed that only weak reliability claims (10^{-1} PDF) are ever made for operators in fault situations, and it is assumed that they do not have to react quickly. There is little purpose in designing a highly reliable HMI. The HMI is normally a SIL 1 system. The HMI should not mislead operators into making a bad situation worse. The ergonomics of plant displays and the operator's environment should get a lot of attention.

Display systems that indicate the status of post-trip systems and equipment need to have high integrity and reliability. These systems often feature in special hard-wired displays with SIL 2 or higher reliabilities.

3.5.4.3 Control and protection system

Control and protection systems can initiate faults if they fail. This can lead to spurious plant trips, and also challenges on the protection systems. Thomson (2012) explained that they can cause "initiating events" in fault sequences. It is therefore recommended by Thomson (2012) to implement duplex control systems which can achieve SIL 2 reliability (10^{-2} PDF).

3.5.4.4 Protection and trip system

The reactor protection and trip system is the main system for ensuring reactor shutdown during failures and faults. It should be designed to the highest standards and is typically a SIL 3 or SIL 4 system. The protection and trip system is usually a software-based system and the design should be performed to international standards such as IEC 60880 or IEC 61508. This will result in a system with reliabilities in the 10^{-3} to 10^{-4} PDF range.

A fully diverse secondary reactor protection and trip system is normally fitted. The reliability required from the secondary reactor protection and trip system will vary according to plant design. The reliability required is typically in the 10^{-3} to 10^{-4} PDF range. However, some countries specify lower

reliability requirements for the diverse reactor protection and trip system. Some countries classify it as a seismically-qualified “non-safety” system.

According to the National Nuclear Regulator (2013), the main objective of the National Nuclear Regulator (NNR) is to provide for the protection of persons, property, and the environment against nuclear damage through the establishment of safety standards and regulatory practices. In accordance with these nuclear safety standards and regulatory practices, the NNR regulates the nuclear installations (NIs) in South Africa.

Quality attribute requirements, which mean architectural drivers, are of availability, maintainability, testability, security, and performance as explained by Bass (2003). In order to design and develop the digital I&C architecture satisfying the selected drivers, architectural tactics need to be determined or developed.

4.1 Tactics and drivers from the NNR Position Paper PP-0017

In this section the tactics are determined and developed from the NNR position paper PP-0017 (National Nuclear Regulator, 2013) and also grouped into the two different drivers – single failure criterion and determinism.

4.1.1 Driver: Single failure criterion

4.1.1.1 Tactic: Redundancy, Independence, and Diversity

NNR[1] "In new NIs, which will undoubtedly be fitted with DC&I systems as primary, the DC&I systems may also be integrated with analogue C&I systems in certain critical applications as backup."

NNR[2] "In general, the RPS must be capable of automatically recognising plant conditions that fall outside specified limits and initiate prompt action to put the plant in a safe condition (e.g. shut down of the reactor) in a manner that minimises the possibility of false indications causing unwanted reactor protection action, but reliably acts upon recognition of valid protection conditions. This is typically done by having several independent protection

channels with a scheme to confirm the validity of the sensed unsatisfactory condition, e.g. 2-out-of-4 signals, taken twice."

NNR[3] "The RPS should also allow for testing without causing unwanted or unnecessary protective action; while not preventing a valid signal from initiating protective action. In addition, the RPS must provide for operator initiation of protective action."

NNR[4] "The system must provide for various types of reactor trips (scrams) that cause the prompt and rapid insertion of certain or all control rods partially or fully depending on the situation. The system should be fail-safe such that functional failures put the plant in a safe condition."

NNR[5] "In addition, it may be necessary to prevent certain plant conditions that could result in large and rapid reactivity additions for which trips or scrams are not sufficient to prevent exceeding thermal limits before power is turned. Such preventive measures may include automatic interlocks that won't allow certain actions that could cause reactivity addition accidents."

NNR[6] "There should be measures for reliability through defence-in-depth, including redundancy and diversity in the various RPS functions."

NNR[7] "The protection system shall be separate from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impacted."

4.1.1.2 Tactic: Defence-in-depth

NNR[8] "In addition, it is expected that there will always be provisions for manual operator backup and override in certain applications, such as reactor shutdown."

NNR[9] "The principle of defence-in-depth must be applied as appropriate."

NNR[10] “C&I systems involved with accident prevention would include operational plant process control systems, process variable indication, nuclear instruments, display, alarm and recording functions (e.g. safety parameter display system), reactor protection system interlocks, and any other pre-accident automatic protective actions. It could be argued that automatic and manual reactor shutdown functions are accident-preventive measures for pre-accident, but unsafe plant conditions in which prompt reactor shutdown is directly necessary to prevent core damage.”

NNR[11] “One of the major concerns with DC&I is the increased failure probability inherent with complexity and the increased vulnerability to distributed-fault or common-cause failures (CCFs). One of the chief means to prevent and mitigate the effects of CCF in DC&I, especially software-related CCF, is DiD.”

NNR[12] “To that end, the RPS may be responsible for automatic alarms or warnings to operators of plant conditions that are trending in an unsafe direction and/or have exceeded limits within those that cause automatic protective actions, to allow the operators to assess the situation and take corrective action before it becomes necessary for the RPS to initiate protective action.”

4.1.1.3 Tactic: Diversity

NNR[13] “Diversity is a way to reduce the potential effects of CCF (e.g. incorporation of inherent diversity in the design of the instrumentation and control systems, or by the use of a diverse backup system). It is recognised that there are varying degrees of diversity.”

4.1.1.4 Tactic: Defence-in-depth and diversity

NNR[14] “Unanticipated CCFs or distributed faults are more likely in digital systems than in analogue systems. Therefore, it is also more important to ensure that digital technology is applied in a manner that addresses functional DiD, functional diversity, and system diversity features.”

NNR[15] “Each safety system in a nuclear plant must operate regardless of failures from within or outside the safety system.”

4.1.1.5 Tactic: Independence

NNR[16] "Communications between computers in different safety divisions should have no detrimental effect on the safety division in question due to any failure or error in communications either from or to another division."

NNR[17] "Broadcast communication is an acceptable approach for the communication independence between computers in different safety divisions."

NNR[18] "Architectures utilising a central hub or router where communications from multiple safety divisions are transmitted across a single channel should be prohibited."

NNR[19] "A priority function should be a safety function. Devices that perform safety functions may be actuated by both safety systems and systems of lower safety class provided that the completion of safety actions cannot be interrupted by commands, conditions, or failures outside the function's own safety division."

NNR[20] "These provisions regarding interconnection of protection and control systems limit two-way communication between safety and non-safety systems. International industry consensus standards indicate such communication pathways are acceptable provided that:

a. failure of the communication system does not impair the safety function, and

b. the safety function does not rely on non-safety system inputs to operate."

NNR[21] "Applicants should demonstrate that proposed mixed-channel displays and controls and operation of safety devices by means of non-safety controls or of controls in other channels maintain the required independence and isolation of redundant safety systems."

NNR[22] "In particular, authorisation holders shall protect digital computer and communication systems and networks associated with the following categories of functions, from those cyber-attacks:

a. safety-related and important-to-safety functions

b. security functions

c. emergency preparedness functions, including offsite communications, and

d. support systems and equipment, which, if compromised, would adversely impact safety, security, or emergency preparedness functions.

Authorisation holders should further protect such systems and networks from those cyber-attacks that would act to modify, destroy, or compromise the integrity or confidentiality of data or software; deny access to systems, services, or data; and impact the operation of systems, networks, and equipment."

NNR[23] "In particular, there shall be provided in existing or new nuclear installations the capability for independent, manual shutdown of the reactor in NPPs and RRs, and other potentially hazardous processes in other types of nuclear installations."

4.1.1.6 Tactic: Independence, and Defence-in-depth

NNR[24] "Communication computers performing functions of a higher safety category should be adequately isolated from communication computers performing functions of a lower safety category (including non-classified functions)."

4.1.1.7 Tactic: Fault detection (Self-diagnostic, etc.)

NNR[25] "In addition, like other DC&I systems important to safety, the RPS should have surveillance, diagnostics, and prognostic functions that continuously monitor system performance (process and data) to detect and recognise system failures and / or known failure precursors in order to alert operators, or under certain conditions, take corrective action, in a timely manner."

4.1.2 Driver: Determinism

4.1.2.1 Tactic: Sequential execution

NNR[26] "Devices (e.g. processors) that perform safety functions should perform no communication handshaking or interrupts that could disrupt deterministic safety function processing."

4.1.2.2 Tactic: Deterministic design practice

NNR[27] "Design of digital systems for the highest classification shall be as simple as practical."

NNR[28] "All unnecessary complexity shall be avoided both in the functionality of the system and in its implementation."

NNR[29] "Implementation of cyber security features should not adversely impact the performance (including response time), effectiveness, reliability or operation of safety functions."

NNR[30] "Implementation of cyber security features directly in the safety system should be avoided when practical."

NNR[31] "The automatic inputs to the RPS are typically direct reactor plant parameters – conditioned signals from plant instruments and nuclear instruments, or specialised combinations and/or comparisons of parameters that are better indicators of the plant's proximity to thermal limits."

NNR[32] "Additional diversity, redundancy and independence, however, also increase a system's complexity and raise the possibility that the additional complexity may pose a larger risk of human errors in design, operation, and maintenance than the common cause failure they were intended to avoid. To compensate, one way to simplify the design, manufacture and use of digital I&C systems is to use prequalified 'commercial of-the-shelf' (COTS) hardware and software components that have been thoroughly tested and evaluated for nuclear power plant applications (dedication, including seismic and environmental qualification)."

NNR[33] "It is important to establish a Secure Development and Operational Environment (SDOE) for digital safety systems. The establishment of a SDOE refers to:

(1) measures and controls taken to establish a secure environment for development of the digital safety system against undocumented, unneeded and unwanted modifications; and

(2) protective actions taken against a predictable set of undesirable acts (e.g. inadvertent operator actions or the undesirable behaviour of connected systems) that could challenge the integrity, reliability, or functionality of a digital safety system during operations.

These SDOE actions may include adoption of protective design features into the digital safety system design to preclude inadvertent access to the system and/or protection against undesirable behaviour from connected systems when operational."

CHAPTER 5: ASSESSMENT OF THE EDF AND AREVA UK EPR I&C ARCHITECTURE

This EPR I&C architecture assessment cover topics of technical relevance to the I&C systems including the I&C architecture. This chapter presents the summarised outcomes of the I&C technical assessment of the EDF and AREVA Pre-Construction Safety Report (PCSR) (EDF and AREVA, 2009a) undertaken as part of Step 3 and Step 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. The goal of the assessment is to reach an informed judgement on the adequacy of the architecture. The assessment is based on the Flamanville 3 I&C systems and architecture.

5.1 Overview of the architecture

The overall architecture of the I&C system is given in the following Figure.

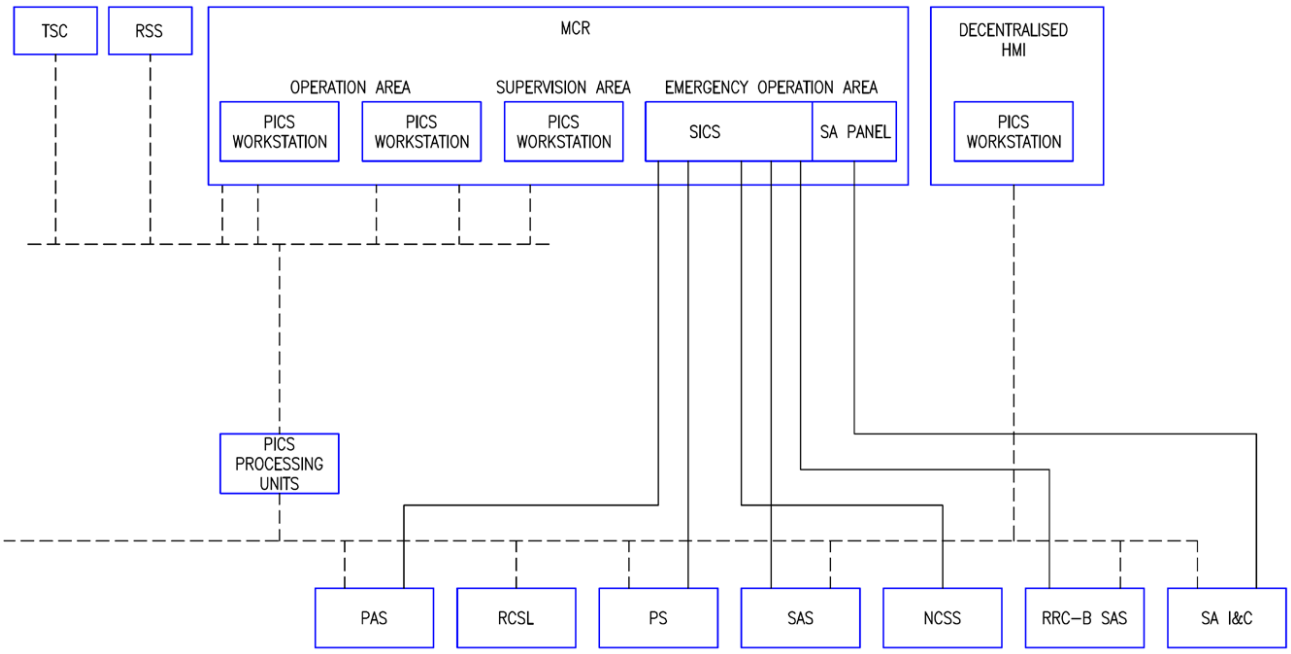

Figure 14: EPR I&C Architecture (EDF and AREVA, 2009a).

EDF and AREVA (2009a) structured the I&C architecture into the following different functional levels:

Level 0: Process interfaces

Consisting of:

- Instrumentation including the measuring elements and signal conditioners up to the automation system, as well as the Process Instrumentation Pre-Processing System (PIPS).

- Switchgear units and actuators as well as the Management of Priority and Actuation Control System (PACS).

Level 1: Automation systems

Including:

- Class 1 protection systems (Reactor Protection System (RPR)).

- Class 2 systems (Safety Automation System (SAS), Reactor Control, Surveillance and Limitation System (RCSL) and Non-Computerised Safety System (NCSS)).

- Class 3 systems (Process Automation System (PAS), RRC-B Safety Automation System (RRC-B SAS) and Severe Accident I&C System (SA I&C).

- Data acquisition, automation processes, monitoring and control in specific Class 3 or NC I&C systems (e.g. turbine, alternator, etc.).

Level 2: Monitoring and control of the unit

This is typically the data processing related to the Human Machine Interface (HMI) for the monitoring and control of processes implemented in:

- Process Information and Control System (PICS) (Class 3), and

- Safety Information and Control System (SICS) (Class 1).

There are also the following additional interfaces:

- the Inter WorkStation Console (PIPO) (Class 1),
- the Qualified Display System (QDS) (Class 1) which is the HMI unit of the RPR,
- the Inter-Panel Signalisation Panel (PSIS) (Class 2), and
- the Severe Accident (SA) Panel (Class 3) which is a dedicated area within the MCS [SICS] panel.

Level 3: Non-real-time applications

Level 3 applications are non-real-time applications, for example the Data Acquisition System.

5.1.1 Description of the I&C system architecture

EDF and AREVA (2009a) provided the following simplified I&C system descriptions:

PAS: The main role of the PAS is the monitoring and control of the plant in all normal operating conditions. The PAS also performs sufficient monitoring and control of sub-functions related to risk reduction.

RCSL: The RCSL processes Category B, Category C and non-categorised I&C Functions related to core control and monitoring.

These include:

- the core control functions, and
- the automatic Limiting Conditions of Operation (LCO) functions and limitation functions for reactor core parameters and for the reactor coolant circuit requiring control rod actuation.

RPR [PS]: The RPR [PS] monitors the safety parameters in all Plant Condition Categories (PCC), and for all initiating events, and enables:

- the automatic Category A protection and safety I&C functions,

- the automatic Category A control I&C Functions of the safety support systems, and
- the manual Category A I&C functions.

SAS: The functions performed by the SAS are:

- manual and automatic post-accident I&C functions necessary to bring the plant from the controlled state to the safe shutdown state (Category B),
- I&C functions related to Class 2 support systems which do not change their status during an event (safety support systems such as ventilation), and
- Category B I&C functions preventing radioactive release.

The elements of the SAS, performing the I&C functions related to the support systems, are organised in sub-systems incorporating the necessary protection against external effects (e.g. functional isolation, local controls, etc.).

The SAS is a Class 2 digital system.

NCSS: The NCSS provides protection and control in case of total loss of computerised (e.g. SPPA-T2000 and TXS platforms) I&C functions.

To meet the required overall reliability figures for I&C safety systems an additional, diversified and non-computerised safety system (NCSS) has been introduced to ensure that the I&C systems reliabilities are such that the design complies with the HSE SAPs recommendations.

The NCSS provides the functions to reach and maintain a stable state.

The NCSS is a Class 2 system.

RRC-B SAS: The RRC-B SAS is dedicated to severe accident Risk Reduction Category B (RRC-B) functions (with the exception of the Loss of Off-site Power (LOOP) severe accident scenario, which is managed by the Severe Accident I&C system (SA I&C), see below) and performs the Category C seismically qualified I&C Functions that contribute to the following safety functions:

- primary circuit depressurisation,
- Hydrogen control (mitigation),
- containment depressurisation and heat removal, and
- radiological source term monitoring.

The RRC-B SAS is a Class 3 digital system.

SA I&C: SA I&C provides the necessary control and communication in the event of a severe accident coupled with, or due to, a total loss of power (LOOP) plus loss of Emergency Diesel Generators (EDG) plus loss of Ultimate Diesel Generators (UDG) in the case of Station Blackout (SBO).

The SA I&C performs three main I&C Functions:

- acquires and processes signals,
- displays data (on the SA Panel on SICS), and
- acquires manual commands from the SA Panel on SICS.

The sensors used for SA I&C Functions are routed through different PIPS cubicles from those only used in other systems. They must meet some additional specific qualification requirements over and above the general safety requirements linked to classification. PIPS cubicles used to support SA I&C will also have a 12 hour battery back-up.

The SA I&C is a Class 3 digital system.

5.2 Safety case overview

EDF and AREVA provided a number of documents setting out its I&C safety case. The main document that describes the I&C systems and architecture is EDF and AREVA (2009a). The I&C provisions claimed by EDF and AREVA (2009a) include those that would be expected of a modern nuclear reactor such as:

- safety and reactor shutdown systems (e.g. Protection Systems),
- control and monitoring systems (e.g. Process Automation System (PAS) and Process Information and Control System (PICS)),
- control room and a backup control room via the Remote Shutdown Station (RSS), and
- communication systems for signal and information transfer within and external to the power plant.

From EDF and AREVA (2009a) it can be noticed that the UK EPR makes use of two different I&C platforms, Teleperm XS (e.g. Protection Systems and Reactor Control, Surveillance and limitation (RCSL) system) and Siemens SPPA T2000 (e.g. PAS, PICS and Safety Automation System (SAS)).

According to EDF and AREVA (2009a) an important aspect of the safety demonstration is the classification of Systems Important to Safety (SIS) and the application of appropriate design standards. EDF and AREVA (2009a) also stated that the UK EPR I&C design concept reflects French custom and practice, and is largely based on French standards (e.g. RCC-E) and French regulatory requirements. Four function (i.e. F1A, F1B, F2 and NC) categories and equipment (i.e. E1A, E1B, E2 and NC) classes are used.

5.3 SAP assessment

Particular attention was given by EDF and AREVA (2009a) to the items considered having relevance to system and architectural design. A report on the adequacy of EDF and AREVA's safety case argumentation was produced by the TSC (NII GDA, n.d.a). As a result of the argumentation assessment it is concluded that:

- Safety Categorisation and Classification – The UK EPR 4 levels of categorisation (F1A, F1B, F2 and NC) and classification (E1A, E1B, E2 and NC) do not align with HSE's SAPs (HSE, 2008a) or BS IEC 61226:2005.
- Defence-in-Depth – The allocation of safety functions to I&C systems conforms to the defence-in-depth concept, aligning with the 5 levels referred to in IAEA Safety Standard NS-

R-1 (IAEA, 2000a). However, use is made of only two digital platforms (i.e. Teleperm TXS and SPPA-T2000). A failure of one digital platform due to Common Cause Failure (CCF) may result in the loss of more than one level of defence.

- Redundancy – The level of equipment redundancy within the PAS and SAS requires further clarification.

- Diversity – Functional and equipment diversity is used across the two digital platforms Teleperm XS and SPPA-T2000.

- Protection Systems Independence – It should be demonstrated that faults in other systems will not impact on the PS safety function and that the communications are outwards from the PS.

- Reliability – The PCSR PSA gives 1×10^{-5} pfd and 1×10^{-4} pfd for the common 'Processing (non-specific)' parts of the E1A (Teleperm XS) and non-E1A (SPPA-T2000) systems respectively. These reliability claims are either beyond or at the normal limits for computer based safety systems (HSE, 2008b) and insufficient justification of these claims is provided.

- Failure to Safety – The fail-safe principle as applied to I&C systems is not well covered in the PCSR.

- Computer Based SIS – Further clarification is required as to how the independent confidence building and production excellence legs (HSE, 2008b) are addressed.

According to EDF and AREVA (2009a), EDF and AREVA are to provide more detailed information on the production excellence and confidence building activities applied to computer based SIS. Discussions are ongoing with regard to the use of statistical testing to support the Protection Systems reliability claim.

5.4 I&C system level architecture assessment

The technical assessment revealed that the I&C architecture is complex with reliance on only two computer and software based systems (developed by the same Company). There is also a high

degree of inter-connectivity between the different systems. Independence between the safety (Class 1) and safety related systems (Class 2/3) appear to be significantly compromised.

A particular concern to EDF and AREVA (2009a) is that the lower safety class systems appear to have write access to higher safety class systems. The usual practice of only allowing one-way communication from a safety related system to systems of a lower safety class is not applied in the UK EPR design.

Other significant concerns identified by EDF and AREVA (2009a) include:

- substantiation of the reliability claims for the computer based SIS that use the Teleperm XS and SPPA-T2000 platforms (e.g. PS, Safety Automation System (SAS) and PAS),
- the absence of a safety Class 1 display system,
- no Class 1 manual controls or indications either in the Main Control Room or Remote Shutdown Station, and
- EPR function categories / equipment class assignments do not appear to align with UK expectations as defined in BS IEC 61226:2005.

The reliability claims for the I&C systems (i.e. 10^{-5} PFD for the Teleperm XS Protection System and 10^{-4} PFD for the Siemens SPPA -T2000 platform that provides reactor protection) will prove very difficult if not impossible to substantiate. The claim on the Teleperm XS Protection System is beyond the normal limit for reliability claims (i.e. 10^{-4} PFD) as stated in nuclear sector standards and guidance (IAEA, 2000b) including that of the safety advisory group to France's regulatory body (GPR and German experts, 2000). The claim for the Siemens SPPA-T2000 platform is at the limit.

EDF and AREVA (2009a) stated that EDF and AREVA undertook a sensitivity study that looked at the potential for using less demanding reliability values for the computer based I&C platforms. The sensitivity study concluded that there is unlikely to be any margin for reducing the claimed I&C system reliabilities to more credible values without significantly increasing EDF and AREVA's risk estimates to levels which are close to or in excess of the Basic Safety Levels (HSE, 2008a).

It was also noted from EDF and AREVA (2009a) that the claim on the computerised Primary Protection System (PPS) when standing alone was 10^{-4} PFD and for the most frequent faults the claim for the combination of the PPS and hardware based Class 1 Secondary Protection System (SPS) was 10^{-7} PFD. From this it can be seen that EDF and AREVA are claiming two orders of magnitude better reliability for the combination of two computer based systems (i.e. 10^{-9} PFD) one of which (i.e. the Siemens SPPA-T2000 platform) was according to HSE (2009b) not developed to nuclear sector protection system standards such as IEC 60880 or IEC 60987.

EDF and AREVA (2009a) advised that the provision of a hardware back up protection system (as employed in Olkiluoto 3) might be a possible way forward on some of the concerns identified above. The implementation of a hardware backup system on Olkiluoto 3 and a Class 1 display system on US EPR suggests that the implementation of such systems is reasonably practicable and necessary for a plant designed to meet modern international safety standards and requirements.

In addition to the UK EPR architecture review, the TSC undertook a detailed review of the UK EPR I&C architecture (NII GDA, n.d.b). The objective of this review was to consider the overall I&C system and architecture looking at safety design features, namely:

- defence-in-depth and CCF,
- independence and diversity,
- provision for automatic and manual safety actuation, and
- appropriateness of equipment type / class.

EDF and AREVA (2009a) stated that the TSC work involved defining a list of reactor-independent essential and desirable architecture characteristics needed to comply with relevant standards and guidance. In selecting the characteristics consideration was given to HSE SAPs (HSE, 2008a), TAGs (HSE, 2008b) and (HSE, 2009a) and nuclear sector I&C standards (IEC, 2001).

The main conclusion of the TSC report (NII GDA, n.d.b) on the I&C architecture of the UK EPR is that the submission made by EDF and AREVA for the overall I&C architecture of the UK EPR reactor does not demonstrate that the UK EPR I&C architecture is in accordance with many of the relevant

principles, standards and guidance. The main concerns and observations arising from the TSC's review (NII GDA, n.d.b) include:

- overall specification of the I&C architecture design including the interface requirements between different systems,
- complexity and inter-connectivity of the I&C architecture,
- classification of certain safety systems and safety-related systems,
- reliability and diversity claims for the I&C systems,
- write access to Class 1 systems from lower class systems, and
- absence of key information in the PCSR.

The work described in NII GDA (n.d.b) was carried out on the basis of the April 2008 PCSR (EDF and AREVA, 2008). The TSC assessed the impact of the June 2009 UK EPR PCSR revision (EDF and AREVA, 2009a) and determined that the revision has not introduced significant changes to the I&C architecture compared to that described in EDF and AREVA (2008). The major concerns still remain, e.g. inputs into the Class 1 system from non-Class 1 sources.

The biggest change in EDF and AREVA (2009a) is the introduction of the RRC-B SAS and the provision of more information on the RRC-B Severe Accident I&C. The SAS has been renamed the Plant SAS and a dedicated SAS communications bus has been incorporated.

EDF and AREVA provided further substantiation of the UK EPR I&C design and a commitment in Letter EPR00180R (EDF and AREVA, 2009b) to undertake a number of modifications to the UK EPR I&C architecture as currently submitted in EDF and AREVA (2009a) to address the main areas of concern. The main commitments are summarised below and further details are contained in EDF and AREVA (2009b):

- One way communication will be implemented from the PS to the lower classified systems (should any exceptions be identified then they will be justified on a case-by-case basis).

- All signals transmitted between the Safety Information and Control System (SICS) and the PS will use a F1A (Class 1) path.

- A non-computerised backup system (1 x 10^{-3} PFD) will be implemented in order to provide protection and controls in case of total loss of I&C functions from the Teleperm XS and SPPA-T2000 platforms.

- Reduction of the reliability claims for the Teleperm XS (1 x 10^{-5} PFD to 1 x 10^{-4} PFD) and SPPA-T2000 (1 x 10^{-4} PFD to 1 x 10^{-2} PFD) platforms.

EDF and AREVA (2009b) also indicated that the non-computerised backup system will include the implementation of automatic functions and facilitate operator actions (after 30 minutes) as necessary to achieve a controlled state of the plant and to maintain it in a safe state for the long term. The functions of the system need to be defined through a functional analysis based on PSA studies to ensure that HSE SAP (HSE, 2008a) risk targets are met. The automatic functions will be implemented in the four I&C divisions using a 2-out-of-4 voting logic. The manual controls will be directly hardwired to the switchgear of the actuators. Actuation will either be initiated from the main control room (from SICS) or at the switchgear level (i.e. depending on time available as justified by human factor's analysis). EDF and AREVA (2009b) also explained that the UK EPR makes use of a Priority and Actuation Control System to resolve demands for component actuation from devices of different safety class.

EDF and AREVA have proposed a way forward in Letter EPR00180R (EDF and AREVA, 2009b) that provides the basis for proceeding to the next step of the GDA process. The provision of the following address the major concerns: non-computer based backup system, one way communication from the PS to lower classified systems, Class 1 information and manual controls, and reduction of reliability claims for the computer based systems.

5.5 Diversity of systems implementing reactor protection

A review of the diversity of the systems responsible for the reactor protection was undertaken by the TSC. The systems included by NII GDA (n.d.b) in the diversity review were the PS (Teleperm XS)

and SAS / PAS (Siemens SPPA-T2000). These systems were selected because they perform the UK EPR protection functions.

The approach adopted by the TSC included consideration of various forms of diversity, including:

- functional and equipment diversity (including diversity of platform),
- diversity of verification and validation,
- diversity of physical location (segregation),
- software diversity,
- data diversity / signal diversity,
- diversity of design / development, and
- diversity of specification.

The main finding of the TSC's report (NII GDA, n.d.b) on the diversity of systems responsible for reactor protection functionality is that the submission made by EDF and AREVA for adequacy of the diversity between the primary and secondary protection systems, does not demonstrate accordance with many of the relevant principles, standards and guidance used in the review. A full list of the TSC's main observations can be found in HSE (2009b). The main concerns from NII GDA (n.d.b) are:

- excessive reliability claim for the diverse protection systems taken together,
- lack of evidence of platform diversity,
- lack of evidence of diversity within systems in the same safety group when high reliability is needed, and
- absence of key information in the PCSR.

In addition, the changes proposed by NII GDA (n.d.b) to the UK EPR architecture and reliability claims will have a significant impact on the conclusions of the TSC's diversity review.

5.6 Summarised assessment

As a result of the I&C assessment the conclusion is that:

- A number of significant concerns were identified by EDF and AREVA (2009a) in relation to the adequacy of the UK EPR architecture, namely:

    i. substantiation of the reliability claims for the computer based Systems Important to Safety (SIS) that use the Teleperm XS and SPPA T2000 platforms,

    ii. complexity and interconnectivity of the architecture, and independence of systems, and

    iii. absence of Class 1 displays and manual controls.

- EDF and AREVA (2009a) also stated that the PCSR and supporting documentation cover the main I&C systems and provisions that would be expected in a modern nuclear reactor but the safety case argumentation and identification of evidence needs improvement.

EDF and AREVA have proposed a way forward in EDF and AREVA (2009b) that provides a basis for proceeding to the next step of the GDA process, which includes provision of a non-computer based backup system, one way communication from the protection system to lower classified systems, Class 1 information and manual controls, and reduction of reliability claims for the computer based SIS.

CHAPTER 6: ASSESSMENT OF THE WESTINGHOUSE AP1000 I&C ARCHITECTURE

This chapter presents the summarised outcomes of the I&C technical assessment of the Westinghouse Electric Company (WEC) AP1000 Pre-Construction Safety Report (PCSR) (WEC, 2009b) undertaken as part of Step 3 and 4 of the Health and Safety Executive's (HSE) Generic Design Assessment (GDA) process. The goal of the assessment is to reach an informed judgement on the adequacy of the architecture.

6.1 Overview of the architecture

The AP1000 I&C architecture and systems presented in this chapter provides control and protection against unsafe reactor operation. It also initiates selected protective and trip functions to mitigate the consequences of design basis initiating events and protect against the loss of the Key Safety Functions (KSFs).

The I&C architecture is arranged in a hierarchical manner. Above the communication network are the systems and nodes whose purpose is to provide the interface between the plant operators and the I&C systems. Below the communication network are the systems and nodes that perform the emergency trip, protection, and control functions. These are the PMS, the PLS, the in-core instrumentation system, the special monitoring system and the DAS.

The operations and control centres system consists of parts of the PMS, PLS, DAS and DDS, along with the control console structures.

The following Figure, which is adapted from Figure 2.1 of AP1000 Instrumentation and Control Defence-in-Depth and Diversity Report (WEC, 2003), provides a simple graphical representation of the I&C architecture.

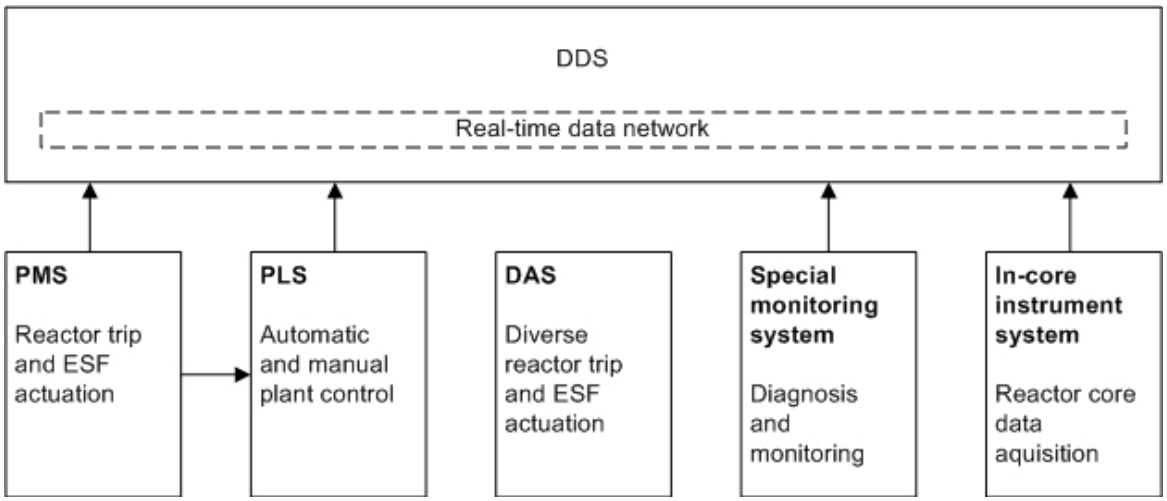

Figure 15: High-level AP1000 I&C Architecture (WEC, 2003).

A more detailed overview of the I&C architecture is shown in the following Figure.

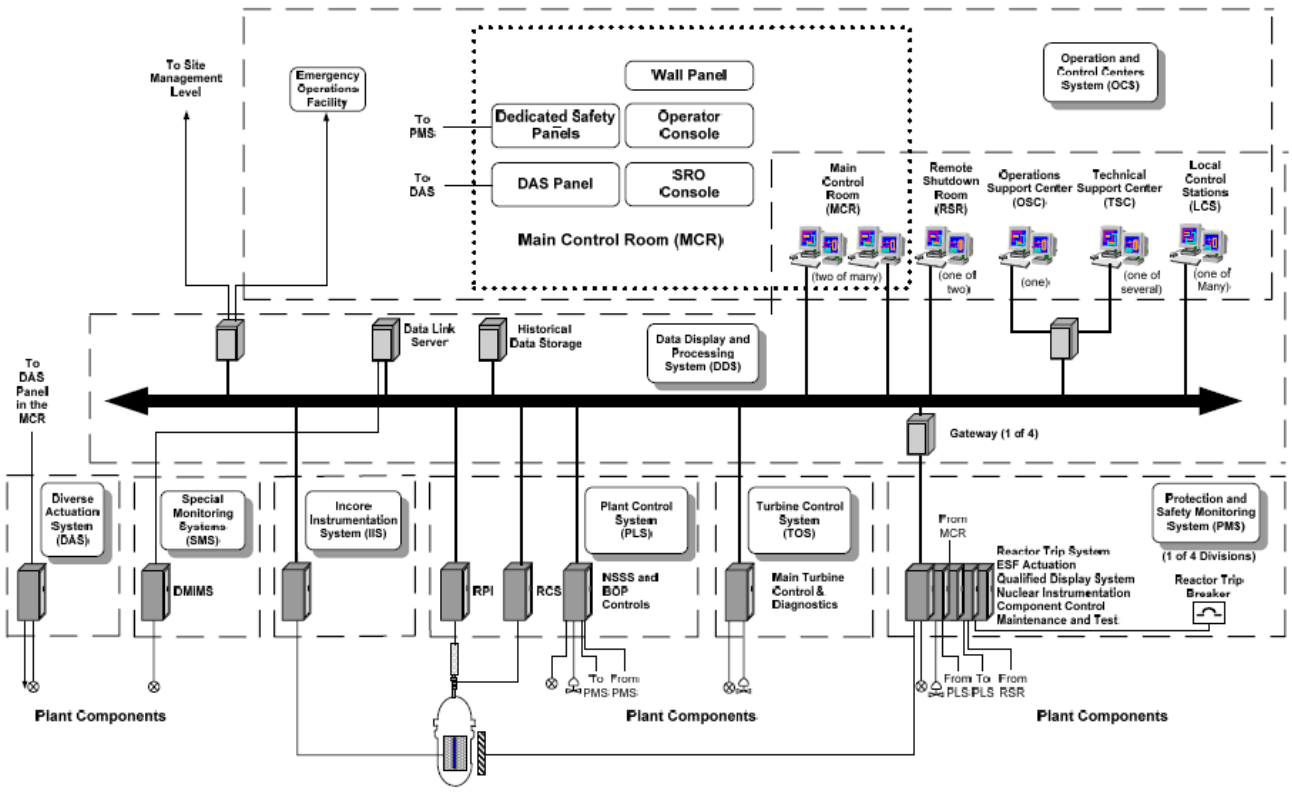

Figure 16: AP1000 I&C Architecture (Albert, 2011).

The following sub-sections provide summarised I&C system descriptions from WEC (2009b):

6.1.1 Plant control system

The PLS provides control of the plant during start-up, power operation, and shutdown conditions. The PLS integrates the automatic and manual control of the reactor, reactor coolant, and various reactor support processes. According to WEC (2009b), the PLS provides control over the following reactor system functions:

- rod control,
- pressuriser pressure and level control,
- steam generator water level control,
- steam dump (turbine bypass) control, and
- rapid power reduction.

In addition, the PLS provides control over a number of supporting duty systems, as listed in Table 7.7-3 of WEC (2009a).

The PLS provides automated control of reactor and other supporting systems in response to changes in operating limits as well as load changes. The PLS also provides the capability for manual control of nuclear power plant. Redundant systems are used in some applications to increase the availability and single-failure tolerance.

The control system is capable of manoeuvring the plant through certain transients. This manoeuvring is done without the need for manual intervention and without violating plant protection or component limits.

It was noted from WEC (2009b) that the control system permits manoeuvring the nuclear power plant through the transients without actuation of the following:

- steam generator safety valves,

- steam generator power operated relief valves, and
- pressuriser safety valves.

In addition, these valves are not actuated during a normal plant trip.

6.1.2 Protection and safety monitoring system

The AP1000 architecture provides instrumentation and systems to sense possible accident situations and initiate ESFs for the mitigation. WEC (2009b) stated that the occurrence of a fault or failure, such as loss of coolant, requires a reactor trip plus actuation of one or more of the ESFs. It is also clear from WEC (2009b) that this combination of events prevents or mitigates damage to the core and reactor coolant system components, and provides containment integrity.

The I&C systems performing reactor protection and ESF actuation functions, their related instruments, and the reactor trip switchgear are four-way redundant as per subsection 7.1.1 of WEC (2009a). WEC (2009b) explained that this redundancy permits the use of bypass logic so that a division or individual channel out of service can be accommodated by the operating portions of the protection system reverting to a 2-out-of-3 logic from a 2-out-of-4 logic. The redundancy and voting logic also mean that a single faulty instrument cannot spuriously actuate an ESF.

The variables monitored for reactor protection and ESF actuation as well as limits, ranges, accuracies and typical response times for the reactor protection and ESF variables are listed in WEC (2002).

Inputs used for reactor trip are derived from signals that are direct measurements of the desired variables as per subsection 7.2.2.2.4 of WEC (2009a). Two exceptions are listed in WEC (2009b), over-temperature and over-power, which cannot be directly measured:

- The over-temperature ΔT trip set-point is calculated from pressuriser pressure, reactor coolant temperature, and nuclear axial power shape. The set-point is compared against the measured ΔT power signal.
- Over-power ΔT is calculated from reactor coolant temperature and the nuclear axial power shape in the core. This value is compared against the measured ΔT power signal.

The process variables that do affect these parameters can be measured and they are used to continuously calculate the set-points.

A single failure in the PMS or the reactor protection divisions does not prevent a reactor trip, even when a reactor protection channel is bypassed for test or maintenance. Conformance of the equipment to this requirement is also discussed in WEC (2002). In addition to the redundancy of equipment, diversity of reactor trip functions is also incorporated. For example, reactor trip may occur on power range high neutron flux, over-temperature, over-power, pressuriser high pressure or pressuriser high water level.

A single failure in the PMS does not prevent the actuation of the ESFs when the monitored condition reaches the pre-set value that requires the initiation of an actuation signal as per subsection 7.3.2.2.2 of WEC (2009a). The single failure criterion is met even when one system of the ESF is being tested, as discussed in subsection 7.1.2.9 of WEC (2009a), or when there is a bypass condition during test or maintenance of the PMS.

6.1.3 Diverse actuation system

The DAS provides a diverse backup to the PMS. This backup is included to reduce the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and postulated common mode failure in the protection and control systems.

The PMS is designed to prevent common mode failures between itself and the PLS. However, in the low probability case where a common mode failure does occur, the DAS provides diverse protection. The DAS functional requirements are based on an assessment of the protection system instrumentation common mode failure probabilities combined with the event probability as per subsection 7.7.1.11 of WEC (2009a).

The DAS operates with two actuation logic modes, automatic and manual. WEC (2009b) explained that the automatic actuation logic mode functions to logically combine the automatic signals from the two redundant automatic subsystems in a 2-out-of-2 basis. The 2-out-of-2 logic is implemented by connecting the outputs in series. Outputs and actuation signals are in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual,

2-out-of-2 redundancies reduces the probability of inadvertent actuation as described in subsection 7.7.1.11 of WEC (2009a).

The manual actuation system operates in parallel to independently actuate the final devices, and is made possible by hard-wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the normal path through the PMS cabinets and the DAS automatic logic.

To support the diverse manual actuations, instrument outputs and information are displayed in the main control room in a manner that is diverse from the protection system. The instrument sensor output displayed in the main control room is repeated at the DAS instrumentation cabinet. According to subsection 7.7.1.11 of WEC (2009a), the indications that are provided from at least two sensors per function are:

- Steam generator water level – for reactor trip and passive residual heat removal actuations, and for overfill prevention by manual actuation of the automatic depressurisation system valves.

- Hot leg temperature – for passive residual heat removal actuation.

- Core exit temperature – for automatic depressurisation system actuation and subsequent initiation of in-containment refuelling water storage tank injection and also containment hydrogen igniter actuation.

- Pressuriser level – for core makeup tank actuation and reactor coolant pump trip.

- Containment temperature – for containment isolation and passive containment cooling system actuation.

- Rod control motor generator voltage – for reactor and turbine trip.

WEC (2009b) also stated that the automatic actuation signals provided by the DAS are generated in a functionally diverse manner from the PMS signals. Diversity is achieved by the use of different systems, different hardware implementations, and different software, where software is used.

Subsection 7.7.1.11 of WEC (2009a) contains a full description of the separation between the DAS and the PMS.

It is also stated that the DAS uses sensors that are separate from those being used by the PMS and the PLS. This prohibits failures from propagating to the other systems through the use of shared instruments or equipment.

The DAS manual and automatic control is independent of the PMS system. From the architecture it can also be seen that the DAS system is a standalone system that is not connected or interlocked with the PMS system. According to WEC (2009b) no actuation interfaces are shared between the DAS and the PMS except for motor-operated valves. The actuation devices of the DAS and the PMS systems are isolated to avoid adverse interactions between the two systems. This type of isolation also prevents the failure of an actuation device in one system from propagating a failure into the other system.

It is also important to note from WEC (2009b) that the DAS and the PMS use independent and separate power sources and internal power supplies.

6.2 Safety case overview

Westinghouse provided a number of documents setting out it's I&C safety case and the addressed SAPs. The submission that describes and explains the I&C architecture and systems is the Design Control Document, WEC (2009a). The I&C provisions claimed by WEC (2009a) include those that would be expected of a modern nuclear reactor such as:

- safety systems (e.g. reactor shutdown systems such as the Protection and Safety Monitoring System (PMS) and Diverse Actuation System (DAS),
- plant control and monitoring systems (e.g. the Plant Control System (PLS) that performs functions such as reactor power control),
- main control room with backup via the remote shutdown workstation, and
- communication systems for information transfer within and external to the plant.

Westinghouse explained that the description of the PMS is based on the Common Q platform and it is noted that this platform has been generically approved by the United States (US) Nuclear Regulatory Commission (NRC). Westinghouse also claimed that the DAS is to be based on Field Programmable Gate Array (FPGA) technology using a process approved by the US NRC for a non-reactor protection application.

The classification of systems important to safety and the application of appropriate design standards is an important aspect of the safety demonstration. According to WEC (2009b) the AP1000 I&C design concept reflects US custom and practice, and is largely based on US I&C standards (e.g. Institute of Electrical and Electronics Engineers (IEEE) standards) and US NRC requirements. Two system classifications are used (i.e. safety-related IEEE Class 1E and non-safety related).

6.3 SAP assessment

Particular attention was given by WEC (2009b) to those SAPs considered to have particular relevance to system and architectural design. A detailed report on the adequacy of the Requesting Party's safety case argumentation was produced by the TSC (NII GDA, n.d.c). As a result of the SAP argumentation assessment, it is concluded that:

- The SAP Roadmap provided by WEC in WEC (2008) does not readily identify all the relevant information within the DCD or PCSR and contains some information that should be in the safety case.

- The DCD and the PCSR do not always reference the available evidence that supports the claims (e.g. references to the W-CAP documentation).

- The I&C design is not yet complete (e.g. DAS) and this has limited the depth of assessment.

- Safety Categorisation and Classification – The AP1000 two levels of categorisation and classification (i.e. Safety Related and non-Safety Related) do not align with HSE's SAPs (HSE, 2008a) or BS IEC 61226:2005 (IEC, 2005).

- Standards – Further clarification is required in relation to the standards used by WEC and their alignment to nuclear sector international standards.

- Defence-in-Depth – Further clarification is required in relation to the allocation of safety functions to I&C systems (i.e. alignment to the 5 levels of defence-in-depth referred to in IAEA Safety Standard NS-R-1 (IAEA, 2000a)). However, use is made of two digital platforms (i.e. ABB AC160 and Ovation) and a FPGA based system. The PMS uses the ABB AC160 platform, the PLS is based on the Ovation platform and the DAS is to be implemented using an FPGA.

- Diversity – Equipment diversity is used across the two digital platforms PMS (ABB AC 160) and PLS (Ovation), and the DAS (FPGA based). Further clarification is required on the extent of functional diversity.

- Failure to Safety – Further clarification is required on the fail-safe principle as applied to I&C systems.

One of the main concerns in WEC (2009b) for the DAS system not being safety-related requires further clarification given the significant safety-related functions (Category A) such as reactor protection that it performs. Westinghouse has stated in the Westinghouse Letter WEC00087 (WEC, 2009c) that the functions the DAS implements are Category A in alignment with the Final Draft International Standard IEC 61226 Edition 3 (published as IEC 61226:2009). Westinghouse also stated that the PMS provides the principle means of fulfilling the function, and the DAS provides a significant contribution to fulfilling the function. Therefore, the DAS is implemented in a Class 2 system. WEC (2009b) confirmed that this may be acceptable provided the DAS reliability target is confirmed to be no better than 1×10^{-2} PFD and the safety groups (of which the DAS is a part) implementing the Category A functions are shown to be adequate.

6.4 I&C System level architecture assessment

The assessment did not reveal any major concerns that could become regulatory issues. One area of concern was the reliability claims on the PMS and PLS.

The TSC produced a detailed report on the AP1000 I&C architecture (NII GDA, n.d.d). The main objective of the work was to consider the overall I&C architecture and systems looking at safety design features in the WEC AP1000 submission, namely:

- defence-in-depth and failure mode management including Common Cause Failure (CCF),
- independence and diversity,
- provision for automatic and manual safety actuation, and
- appropriateness of equipment type / class.

It was noted from WEC (2009b) that the TSC work involved defining a list of reactor-independent essential / desirable system architecture characteristics needed to comply with relevant standards and guidance. In selecting the characteristics consideration was given to HSE SAPs (HSE, 2008a) technical assessment guides HSE (2009a) and HSE (2008b) and nuclear sector I&C standards, i.e. IEC (2001).

The TSC concluded that the AP1000 I&C architecture is in accordance with many of the relevant nuclear sector principles, standards and guidance documents. However, the TSC identified areas where further clarification and substantiation are required, the more significant of which include:

- overall specification of the I&C architecture design including the interface requirements between different systems,
- reliability claims for the I&C systems (PMS, DAS and PLS),
- categorisation and classification of systems (in particular DAS categorisation),
- analysis of the adequacy of safety groups (e.g. addressing coverage of Postulated Initiating Events (PIEs), reliability, CCF and single failures etc.),
- DAS FPGA design (including alignment with HSE ND's special case procedure for complex hardware),
- interconnectivity of systems on and off site,
- segregation of I&C systems to ensure a lower class system cannot frustrate the correct operation of a higher class system, and

- classification and provision of turbine control and safety display systems.

WEC (2009b) stated that the reliability claims for key I&C systems challenge the accepted claim limits for I&C systems (PMS 1 x 10^{-5} PFD and PLS 1 x 10^{-5} probability of dangerous failure per year (PDFY)). Westinghouse has undertaken a sensitivity study (IEC, 2007) to investigate the impact on plant risk of using more modest reliability claims for the I&C systems. Westinghouse's view is that the sensitivity study demonstrates that the plant risk is not unacceptable with more modest reliability claims (e.g. PMS 1 x 10^{-3} PFD).

Westinghouse has explained that its submissions (e.g. PCSR and DCD) are based on the categorisation and classification approach used in the US (WEC, 2009c) and that the categorisation can be mapped into the approach defined by the IAEA, SAPs and nuclear sector standards, i.e. IEC (2005). Westinghouse stated in WEC (2009b) that the categorisation will be completed in accordance with its Quality Assurance Procedures as the design is finalised. Westinghouse has provided a summary of its methodology including a provisional definition of AP1000 I&C functions based on IEC 61226 (IEC, 2005) categories and system class in accordance with IEC 61513 (IEC, 2001).

The limited detailed design information available (in particular for the DAS) has limited the depth of the assessment (e.g. DAS fail-safe behaviour). WEC (2009b) stated that the protection functionality of the DAS is to be implemented in FPGA technology. HSE (2009c) considers FPGA technology as "complex hardware technology and that the application development process has much in common with traditional software development".

The interconnectivity of systems on and off site has been reviewed by WEC (2009b). Westinghouse committed to undertake an assessment of computer security using appropriate standards during the next step of the internal assessment. WEC (2009b) also explained that the AP1000 design makes use of a Component Interface Module (CIM) to resolve demands for component actuation from devices of different safety class (e.g. PMS and PLS). According to WEC (2009b), further clarification is being sought as to the adequacy of this arrangement, in particular, that the PLS cannot frustrate correct operation of the PMS (e.g. actuations when demanded). The segregation as well as physical separation of I&C systems also requires further demonstration.

WEC (2009b) explained that Westinghouse is to qualify the Safety / Qualified Data Processing System (QDPS) display system internal communications bus (currently the AF100 bus) to Class 1 standards and when the qualification is complete it will be applicable to the AP1000. This will enable the safety Class 1 displays and controls to the operator.

The I&C architecture includes the main I&C systems that would be expected in a modern nuclear reactor. While the AP1000 I&C architecture is not unacceptable further assessment is required. WEC (2009b) also stated that the sensitivity review of the PMS, PLS and DAS reliability figures may lead to the need to review the I&C architecture. Additionally, further clarification is required in relation to DAS class and its contribution to the safety groups that implement Category A (e.g. reactor protection) functionality.

6.5 Diversity of systems implementing reactor protection

A review of the diversity of the systems responsible for the reactor protection was undertaken by the TSC. The I&C safety systems included by NII GDA (n.d.d) in the diversity review were the PMS and DAS. These systems perform the AP1000 protection functions.

The TSC produced a report on the diversity of the PMS and DAS (NII GDA, n.d.e). The approach adopted by the TSC included consideration of various forms of diversity, including:

- functional and equipment diversity (including diversity of platform),
- diversity of verification and validation,
- diversity of physical location (segregation),
- software diversity,
- data diversity / signal diversity,
- diversity of design / development, and
- diversity of specification.

The TSC's report (NII GDA, n.d.e) on the diversity of systems responsible for reactor protection concludes that WEC appears to claim full diversity between the PMS and DAS, but the DAS design is not complete enough to support a full diversity analysis. The documentation does not provide sufficient depth in areas such as diversity argumentation and evidence, analysis of common cause failures between PMS and DAS, analysis of the diversity within the safety groups providing the Category A functionality (including the contribution of the PMS and DAS to the safety groups), coverage of functional and equipment diversity, independence and segregation, maintenance and test, and use of diverse verification and validation.

6.6 Summarised assessment

As a result of the I&C assessment the conclusion is that:

- The PCSR and supporting documentation address the main I&C systems and provisions that would be expected in a modern nuclear reactor but the safety case argumentation and identification of evidence needs improvement.

- While the AP1000 I&C architecture is not unacceptable further assessment of the sensitivity of the PMS and DAS reliability figures is necessary and this may lead to the need to review the I&C architecture.

- Further substantiation is required to support the classification of the DAS, its contribution to the safety groups that implement Category A (reactor protection) functionality and adequacy of the diversity between the DAS and PMS.

- The DAS design is also incomplete.

No I&C related Regulatory Issues have been identified and the readiness of Westinghouse to address technical issues is encouraging according to WEC (2009b). Overall, on I&C grounds, there is no reason why the WEC AP1000 should not proceed to the next step of the GDA process.

CHAPTER 7: VERIFICATION OF THE ASSESSMENT RESULTS

In this chapter the assessment results of both the UK EPR reactor and the AP1000 reactor architectures are verified and tabled against the drivers and tactics as identified and developed from the NNR position paper PP-0017 (National Nuclear Regulator, 2013).

7.1 Single failure criterion driver

In this section the single failure criterion driver and its associated tactics are used to verify the UK EPR and AP1000 I&C architectures.

Table 3: Assessment verification results for the single failure driver.

Chapter 4 reference	**Compliance**		**Comments and Remarks**
	EPR	**AP 1000**	
Tactic: Redundancy, independence, and diversity			
NNR[1]	Yes	Partial	EPR: An additional, diversified and non-computerised back-up safety system (NCSS) has been introduced. AP1000: The DAS provides a diverse backup to the PMS, but is based on FPGA technology. It requires further clarification due to the non-safety related classification of the DAS system as well the absence of detailed design information.

NNR[2]	-	Yes	EPR: No data available from the selected literature. AP1000: The equipment and their related instruments and switchgear performing reactor trip and ESF actuation are 4-way redundant. The redundancy and voting logic also mean that a single faulty sensor cannot spuriously actuate an ESF.
NNR[3]	-	Yes	EPR: No data available from the selected literature. AP1000: A single failure in the PMS or the reactor trip actuation division does not prevent a reactor trip, even when a reactor trip channel is bypassed for test and maintenance.
NNR[4]	Partial	Partial	EPR: Further clarification is also required as to how the independence is addressed. The adequacy of diversity of systems implementing reactor protection functionality does not demonstrate accordance with many of the relevant principles, standards and guidance. The fail-safe principle in not well covered in the PCSR. AP1000: Diversity between the DAS and PMS is achieved by the use of different hardware, and different software. Further clarification is required on the fail-safe principle as applied to the systems.
NNR[5]	-	-	EPR: No data available from the selected literature. AP1000: No data available from the selected literature.
NNR[6]	Yes	Yes	EPR: There are measures for reliability, but the PCSR PSA reliability claims for the I&C systems will prove very difficult to substantiate. There is unlikely to be any margin for reducing the reliabilities to be more credible values without significantly increases AREVA's risk estimates to levels which are close to or in excess of the Basic Safety Levels. More details in Chapter 5 for the proposed solution. AP1000: There are measures for reliability, but the reliability claims for important systems challenge the accepted claim limits for I&C systems. The view of Westinghouse is that a sensitivity study demonstrates that the plant risk is not unacceptable with more modest reliability claims.

NNR[7]	Partial	Yes	EPR: It should be demonstrated that faults in other systems will not impact the PS safety function and that the communications are outward from the PS. The assessment revealed that the I&C architecture is overly complex and a high degree of connectivity between systems. PA1000: A single failure in the PMS does not prevent an actuation of the ESFs. The PMS is also designed to prevent common mode failures between itself and the PLS. As mentioned elsewhere, diversity between the DAS and PMS is achieved. The DAS uses sensors that are separate from those being used by the PMS and PLS. The DAS and PMS use independent and separate power sources. See Chapter 6 for more details.
Tactic: Defence-in-depth			
NNR[8]	Yes	Yes	EPR: The non-computerised backup system will facilitate operator actions and manual controls. AP1000: The PLS provides the capability for manual control of plant systems and equipment. The DAS can also operate in manual actuation mode. The manual actuation mode operates in parallel to independently actuate final devices and the sensor output displays in the control room are also diverse from the other display functions.
NNR[9]	Partial	Partial	EPR: The allocation of safety functions to I&C systems conforms to the defence-in-depth concept, aligning with the 5 levels referred to in IAEA Safety Standard NS-R-1. However, use is made of only two platforms. A failure of one platform due to CCF may result in the loss of more than one level of defence. AP1000: Further clarification is required in relation to the allocation of safety functions to I&C systems (i.e. alignment to the 5 levels of defence-in-depth referred to in IAEA Safety Standard NS-R-1.
NNR[10]	Partial	Partial	EPR: Refer to NNR[9]. AP1000: Refer to NNR[9].

NNR[11]	Partial	Partial	EPR: Refer to NNR[9]. AP1000: Refer to NNR[9].
NNR[12]	Yes	Yes	EPR: The PAS performs sufficient monitoring and control of sub-functions related to risk reduction. The non-computerised backup system will include the implementation of automatic functions and facilitate operator actions as necessary to achieve a controlled state of the plant. AP1000: The PLS provides the capability for manual control of plant systems and equipment. Special monitoring systems are also provided.
Tactic: Diversity			
NNR[13]	Partial	Partial	EPR: Functional and equipment diversity is used across the digital platforms and the non-computerised safety system. But, adequacy of the diversity between the primary and secondary protection system, does not demonstrate accordance with many of the relevant principles, standards and guidance. AP1000: Equipment diversity is used across the digital platforms and the DAS system. Further clarification is required on the extend of functional diversity. Further detailed substantiation is also required to demonstrate the adequacy of the diversity between the systems implementing reactor protection functionality (i.e. the DAS and PMS).
Tactic: Defence-in-depth and diversity			
NNR[14]	Partial	Partial	EPR: Refer to NNR[9] and NNR[13]. AP1000: Refer to NNR[7], NNR[9], and NNR[13].
NNR[15]	-	-	EPR: No data available from the selected literature. AP1000: No data available from the selected literature.

Tactic: Independence			
NNR[16]	Partial	Partial	EPR: It should be demonstrated that faults in other systems will not impact the PS safety function. The complexity and inter-connectivity of the I&C systems is a concern. All signals transmitted between the SICS and the PS will use a F1A (Class 1) path. AP1000: DAS is a standalone system that is not connected or interlocked with PMS. The actuation devices are also isolated so as to avoid adverse interactions between the systems. Further clarification and substantiation is required regarding the interconnectivity of systems on and off site.
NNR[17]	Yes	Yes	EPR: Makes use of a Priority and Actuation Control System to resolve demands for component actuation from devices of different safety classes. AP1000: Makes use of a Component Interface Module (CIM) to resolve demands for component actuation from devices of different safety classes.
NNR[18]	-	-	EPR: No sufficient data available from the selected literature. AP1000: No sufficient data available from the selected literature.
NNR[19]	Partial	Yes	EPR: The manual controls are proposed to be directly hardwired to the switchgear of the actuators. Actuation to be initiated from the control room (from SICS) or at the switchgear level. Refer to NNR[7] for more details. AP1000: The actuation signals provided by the DAS are generated in a functionally diverse manner from the PMS signals. Also, refer to NNR[7] for more details.
NNR[20]	Partial	Partial	EPR: The proposal is to implement one way communication from the PS to the lower classified systems. Refer to NNR[16] for additional details. AP1000: Refer to NNR[16] for details.

NNR[21]	Partial	Partial	EPR: Refer to NNR[16] for details. AP1000: Refer to NNR[16] for details.
NNR[22]	-	-	EPR: No sufficient data available from the selected literature. AP1000: No sufficient data available from the selected literature.
NNR[23]	Yes	Yes	EPR: The manual controls are proposed to be directly hardwired to the switchgear of the actuators. Actuation will either be initiated from the main control room (from SICS) or at the switchgear level. AP1000: The manual actuation mode operates in parallel to independently actuate the final devices, and is made possible by hard-wiring the controls located in the main control room directly to the final loads in a way that completely bypasses the normal path through the PMS cabinets and the DAS automatic logic.
Tactic: Independence and defence-in-depth			
NNR[24]	Partial	Yes	EPR: Refer to NNR[7] for details. AP1000: Refer to NNR[7] for details.
Tactic: Fault detection (self-diagnostics, etc.)			
NNR[25]	-	-	EPR: No data available from the selected literature. AP1000: No data available from the selected literature.

7.2 Determinism driver

In this section the determinism driver and its associated tactics are used to verify the UK EPR and AP1000 I&C architectures.

Table 4: Assessment verification results for the determinism driver.

Chapter 4 reference	Compliance		Comments and Remarks
	EPR	**AP 1000**	
Tactic: Sequential execution			
NNR[26]	-	-	EPR: No data available from the selected literature. AP1000: No data available from the selected literature.
Tactic: Deterministic design practice			
NNR[27] to NNR[33]	-	-	Not included in the scope of this verification and evaluation.

7.3 Summarised table

In this section the single failure criterion driver and its associated tactics (NNR[1] to NNR[25]) are summarised without the comments and remarks to give an overview when comparing the EPR and AP1000 I&C architectures.

Table 5: Summarised assessment verification results for the single failure driver.

	NNR[1]	NNR[2]	NNR[3]	NNR[4]	NNR[5]	NNR[6]	NNR[7]	NNR[8]	NNR[9]
EPR	Yes	-	-	Partial	-	Yes	Partial	Yes	Partial
AP1000	Partial	Yes	Yes	Partial	-	Yes	Yes	Yes	Partial

	NNR[10]	NNR[11]	NNR[12]	NNR[13]	NNR[14]	NNR[15]	NNR[16]	NNR[17]
EPR	Partial	Partial	Yes	Partial	Partial	-	Partial	Yes
AP1000	Partial	Partial	Yes	Partial	Partial	-	Partial	Yes

	NNR[18]	NNR[19]	NNR[20]	NNR[21]	NNR[22]	NNR[23]	NNR[24]	NNR[25]
EPR	-	Partial	Partial	Partial	-	Yes	Partial	-
AP1000	-	Yes	Partial	Partial	-	Yes	Yes	-

CHAPTER 8: PROPOSED ARCHITECTURE

In this chapter the architectural drivers and tactics, developed from the NNR position paper PP-0017 (National Nuclear Regulator, 2013), together with the best practices and characteristics from both the architectures are used for the development of a proposed digital I&C architecture and systems for nuclear installations.

Two different architectural drivers were identified in Chapter 4; single failure criterion and determinism. In order to develop the proposed I&C architecture satisfying the single failure criterion driver, the following architectural tactics are applied:

a. The digital I&C architecture is integrated with analogue I&C systems in critical and reactor safety related applications as backup, to address NNR[1].

b. Having several independent protection channels with a scheme to confirm the validity of the sensed unsatisfactory condition, e.g. 2-out-of-4 signals and / or systems taken twice, to address NNR[2] and NNR[3].

c. The protection systems provided for manual operator initiation of protective actions, to address NNR[3].

d. The system must provide for various types of reactor trips (scrams), to address NNR[4].

e. Reliability and mitigating the effects of CCF in digital I&C systems through defence-in-depth, including redundancy and diversity (functional & system) in the various protection systems, to address NNR[6], NNR[9], NNR[11], NNR[13] and NNR[14].

f. To comply with the minimum Basic Safety Levels; the I&C architecture is required to have a reliability of 10^{-4} PFD or better for the protection and trip system, and a reliability of 10^{-3} PFD or better for the control & protection system, to address NNR[6].

g. The protection system is separate from the control system, to address NNR[7].

h. Manual operator backup and override in certain applications, such as reactor shutdown, to address NNR[8] and NNR[23].

i. Communications between computers and nodes in different safety divisions should have no detrimental effect on the safety division – independence, to address NNR[16].

j. No central hub or router where communications from multiple safety divisions are transmitted across a single channel are allowed, to address NNR[18].

k. Systems performing functions of a higher safety category are adequately isolated from systems performing functions of a lower safety category, to address NNR[24].

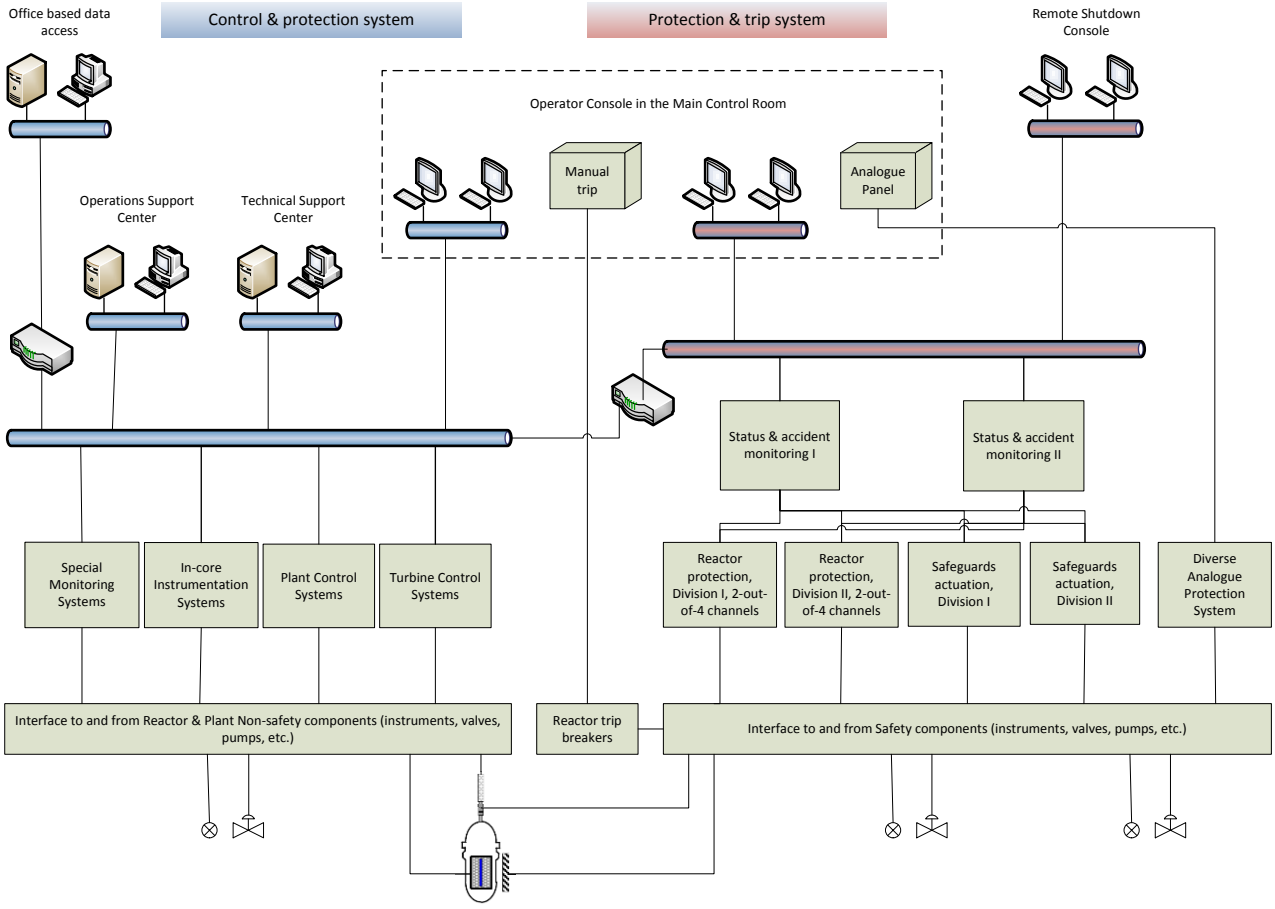

Figure 17: Proposed digital I&C architecture and systems for nuclear installations.

CHAPTER 9: CONCLUSION AND RECOMMENDATIONS

9.1 Conclusion of the research project

The global nuclear energy sector is experiencing a significant increase in the need of digital I&C systems at nuclear power plants to enable and ensure efficient, safe and reliable power generation. This research project has therefore initiated an investigation into the development of I&C architectures, development of the architectural drivers and tactics, evaluation of selected I&C architectures, and finally synthesising a proposed digital I&C architecture.

The application of the defence-in-depth principle in the design of I&C architectures leads to the application of diversity, separation and redundancy in systems and components to provide protection from random and unknown failures. By limiting failures to one of multiple redundant systems, each line of defence remains intact. The potential for common cause failures in I&C systems can also be reduced by employing defensive design measures as well as diversity.

The use of computers in nuclear power plants has provided the opportunity for digital communication via networks between nodes and also offers several benefits to the plant. To protect the I&C architecture, robust physical protection and governance are required, including data encryption / decryption and virus checking. Cyber security vulnerabilities are significantly reduced by following regulations, guidance and standards rigorously.

Two important architectural drivers and associated tactics used for the design and implementation of I&C architectures and systems for nuclear installations, were identified and developed from the NNR position paper PP-0017. A point of interest is that the NNR position paper PP-0017 is making use of UK EPR terminology, while the AP1000 architecture is more compliant to the NNR requirements.

Based on the architectural tactics, the technical assessment and evaluation of the selected digital I&C architectures resulted in the following main conclusions:

For the UK EPR I&C architecture a number of significant concerns were identified in relation to the adequacy and compliance of the I&C architecture; namely, excessive reliability claims for the systems, complexity and interconnectivity of the architecture, independence of systems as well as the absence of manual controls and Class 1 displays. EDF and AREVA have proposed a way forward which includes provision of a non-computer based backup system, one way communication from the protection system to lower classified systems, Class 1 information and manual controls, and reduction of reliability claims for the computer based SIS.

For the AP1000 I&C architecture no I&C related Regulatory issues have been identified and Westinghouse's readiness to address technical issues is encouraging. A number of concerns were identified in relation to the adequacy and compliance of the AP1000 architecture; namely, further assessment of the sensitivity of the PMS and DAS reliability figures is necessary, classification as well as the incomplete design of the DAS system.

From the technical assessment and evaluation, the characteristics of both architectures were verified against the NNR requirements (architectural tactics and drivers) to determine compliance. The compliance verification are summarised in the following table.

Table 6: Summarised assessment verification results for the single failure driver.

	NNR[1]	NNR[2]	NNR[3]	NNR[4]	NNR[5]	NNR[6]	NNR[7]	NNR[8]	NNR[9]
EPR	Yes	-	-	Partial	-	Yes	Partial	Yes	Partial
AP1000	Partial	Yes	Yes	Partial	-	Yes	Yes	Yes	Partial

	NNR[10]	NNR[11]	NNR[12]	NNR[13]	NNR[14]	NNR[15]	NNR[16]	NNR[17]
EPR	Partial	Partial	Yes	Partial	Partial	-	Partial	Yes
AP1000	Partial	Partial	Yes	Partial	Partial	-	Partial	Yes

	NNR[18]	NNR[19]	NNR[20]	NNR[21]	NNR[22]	NNR[23]	NNR[24]	NNR[25]
EPR	-	Partial	Partial	Partial	-	Yes	Partial	-
AP1000	-	Yes	Partial	Partial	-	Yes	Yes	-

From the selected literature and the evaluation and verification results, it is observed that both the UK EPR and the AP1000 I&C architectures are not fully compliant with the NNR requirements.

The research project concluded with a digital I&C architecture that was synthesised and developed from the best practices and characteristics of the selected I&C architectures. This proposed I&C architecture is also compliant with selected NNR requirements.

9.2 Recommendations for further studies

The following recommendations are made with regard to a follow-up study:

- Analyse and evaluate other available digital I&C architectures, e.g. Russian VVER.
- An investigation into the determinism driver for the different I&C architectures.
- Detailed investigation into the systems for the proposed digital I&C architecture.

CHAPTER 10: BIBLIOGRAPHY

Albert, W., 2011, *Overview of Data Communication in the AP1000 I&C System*, Nuclear Energy for New Europe, September 2011, 1208.

Bass, L., 2003, *Software Architectures in Practice*, 2nd edition, Addison-Wesley.

Comper, J., 2003, *Reactor Coolant System*, KPS.

EDF and AREVA, 2008, *UK EPR Pre-Construction Safety Report*, UK EPR-0002-011 Issue 00, April 2008.

EDF and AREVA, 2009a, *UK EPR Pre-Construction Safety Report*, UK EPR-0002-132 Issue 02, June 2009.

EDF and AREVA, 2009b, *Letter EPR00180R, RI-UKEPR-002 – C&I architecture issues*, TRIM Ref. 2009/386051.

GPR and German experts, 2000, *Technical Guidelines for the design and construction of the next generation of nuclear pressurized water plant units*, 19 and 26 October 2000.

HSE, 2008a, *Safety Assessment Principles for Nuclear Facilities*, Rev. 1, January 2008.

HSE, 2008b, *Technical Assessment Guide. Computer Based Safety Systems*, T/AST/046, Issue 2, ND BMS, June 2008.

HSE, 2009a, *Technical Assessment Guide. Safety Systems*, T/AST/003, Issue 4, ND BMS, 10 June 2009.

HSE, 2009b, *Step 3 Control and Instrumentation Assessment of the EDF and AREVA UK EPR*, Division 6 Assessment Report No. AR 09/038-P.

HSE, 2009c, *Step 3 Control and Instrumentation Assessment of the Westinghouse AP1000*, Division 6 Assessment Report No. AR 09/037-P.

IAEA, 2000a, *Safety of Nuclear Power Plants: Design*, IAEA Safety Standards Series No. NS-R-1, IAEA, Vienna, Austria.

IAEA, 2000b, *Software for Computer Based Systems Important to Safety in Nuclear Power Plants*, IAEA Safety Standards Series No. NS-G-1.1, IAEA, Vienna, Austria.

IAEA, 2002, *Instrumentation and Control Systems Important to Safety in Nuclear Power Plants*, IAEA Safety Standards Series No. NS-G-1.3, IAEA, Vienna, Austria.

IAEA, 2003, *Maintaining the Design Integrity of Nuclear Installations throughout their Operating Life*, INSAG-19, Vienna, Austria.

IAEA, 2009a, *Protecting against common cause failures in Digital I&C Systems of Nuclear Power Plants*, Vienna, Austria.

IAEA, 2009b, *Implementing Digital Instrumentation and Control Systems in the Modernization of Nuclear Power Plants*, Vienna, Austria.

IAEA, 2011, *Core Knowledge on Instrumentation and Control Systems in Nuclear Power Plants*, Nuclear Energy Series No. NP-T-3.12, IAEA, Vienna, Austria.

IEC, 2001, *Nuclear power plants – Instrumentation and control for systems important to safety – General requirements for systems*, BS IEC 61513:2001.

IEC, 2005, *Nuclear Power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions*, BS IEC 61226:2005.

IEC, 2007, *Nuclear power plants – Instrumentation and control important to safety – Hardware design requirements for computer-based systems*, 21 Control and Instrumentation Sensitivity Cases, Rev. 0, BS IEC 60987:2007,UKP-GW-GL-744, December 2008.

IEEE, 1998, *IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations*, Std. 603, IEEE, USA.

IEEE, 2000, *Authoritative Dictionary of IEEE Standards Terms*, Std. 100, IEEE, USA.

International Nuclear Safety Advisory Group (INSAG), 2003, *Maintaining the Design Integrity of Nuclear Installations Throughout their Operating Life*, INSAG-19, IAEA, Vienna.

Littlewood, B., 2008, *Guidance on means to achieve system diversity: DISPO6 view*, Ver. V1.0 PP_DISPO6_01, October 2008.

National Nuclear Regulator, 2013, *Design and Implementation of Digital Control and Instrumentation for Nuclear Installations*, PP-0017, Rev. 0, December 2013, South Africa.

NII GDA, n.d.a, *Technical Review – C&I SAP Compliance Assessment for EDF/AREVA UKEPR*, 36331/35856R, Issue 1.7.

NII GDA, n.d.b, *Technical Review – C&I System Architecture Safety Assessment for UK EPR*, S.P1440.57.11, Issue 2.0.

NII GDA, n.d.c, *Technical Review – C&I SAP Compliance Assessment for AP1000*, S.P1440.41.60, Issue 1.1.

NII GDA, n.d.d, *Technical Review – C&I Systems Architecture Functional Safety Review Report for Westinghouse AP1000*, 36331/35796R, Issue 1.4.

NII GDA, n.d.e, *Technical Review – C&I Diversity Aspects of C&I Category A Functional Systems Design Assessment for AP1000*, 36331/35867R, Issue 1.7.

US NRC, 1994, *Method for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems*, NUREG/CR-6303, December 1994, USA.

US NRC, 2007, *Appendix A to Part 50 – General Design Criteria for Nuclear Power Plants*, 10CFR50.

US NRC, n.d., *Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems*, NUREG-0800 Ch. 7 BTP-14, Rev. 5, USA.

Prehler, H., 2001, *Advanced I&C Systems for Nuclear Power Plants Feedback of Experience*, International Conference, Nuclear Energy in Central Europe, Germany.

Rainer, M., 2006, *Continuous Availability for Power Plant Automation*, Instrument & Controls Division, Siemens Power Generation.

Swaminatha, P., 2005, *Design aspects of safety critical instrumentation of nuclear installations*, Int. J. Nucl. Energy Sci. Technol. 2/3, 254 – 263.

Thomson, J., 2012, *Nuclear Power Station Control and Instrumentation Safety Systems Architecture – An Overview*, Safety in Engineering.

WEC, 2002, *Safety Criteria for the AP1000 Instrumentation and Control Systems*, WCAP-15776, April 2002.

WEC, 2003, *AP1000 Instrumentation and Control Defence-in-Depth and Diversity Report*, WCAP-15775, Rev. 2, March 2003.

WEC, 2008, *Safety Assessment Principles Roadmap for AP1000 Design*, UKP-GW-GL-710, Section C, Rev. 2, July 2008.

WEC, 2009a, *AP1000 European Design Control Document*, EPS-GW-GL-700, Rev. 1, December 2009.

WEC, 2009b, *AP1000 Pre-Construction Safety Report,* UKP-GW-GL-732, Rev. 2.

WEC, 2009c, *Westinghouse Letter WEC00087 - C&I Step 3*, UN REG, TRIM Ref. 2009/343656, August 2009.

Wojcik, R., 2006, *Attribute-Driven Design (AAD)*, Ver. 2.0, CMU/SEI-2006-TR-023, SEI CMU, USA.

Yong, S., 2011, *Developing architectures for upgrading I&C systems of an operating nuclear power plant using a quality attribute-driven design method*, Nuclear Engineering and Design, 241, 5281 – 5294, Republic of Korea.