IAEA TECDOC SERIES

IAEA-TECDOC-1848

IAEA-TECDOC-1848

Criteria for Diverse Actuation Systems for Nuclear Power Plants

IAEA
International Atomic Energy Agency

CRITERIA FOR DIVERSE ACTUATION SYSTEMS FOR NUCLEAR POWER PLANTS

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT VINCENT AND THE GRENADINES
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWAZILAND
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

IAEA-TECDOC-1848

CRITERIA FOR DIVERSE ACTUATION SYSTEMS FOR NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2018

Marketing and Sales Unit, Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
fax: +43 1 2600 29302
tel.: +43 1 2600 22417
email: sales.publications@iaea.org
http://www.iaea.org/books

For further information on this publication, please contact:

Safety Assessment Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
June 2018

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Criteria for diverse actuation systems for nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2018. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1848 | Includes bibliographical references.
Identifiers: IAEAL 18-01167 | ISBN 978–92–0–103518–9 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Electronic equipment. | Nuclear power plants — Safety measures. | Actuators.

FOREWORD

Common cause failures within the protection system might result in unacceptable consequences for certain combinations of common cause failures and postulated initiating events, especially in the case of programmable digital protection systems. When this situation is encountered, a diverse actuation system is often provided to back up the reactor protection system.

There is a general agreement that a diverse actuation system can effectively cope with the consequences of specific initiating events in conjunction with a postulated common cause failure of a reactor protection system. There are, however, different approaches to the safety classification, and to the use of analogue or programmable digital components with different attributes in the design of a diverse actuation system so as to mitigate the consequences of common cause failures of the reactor protection system. The design criteria for a diverse actuation system vary among countries and a consensus on an adequate level of diversity has not yet been established.

This publication provides specific details for utility engineers, operators, researchers, managers and personnel responsible for all aspects of design and implementation of instrumentation and control systems of diverse actuation systems for nuclear power plants. This publication will also aid Member States to support assessment of diversity in instrumentation and control architecture as a defence against common cause failures.

The IAEA wishes to thank all participants and their Member States for their valuable contributions. The IAEA officer responsible for this publication was A. Duchac of the Division of Nuclear Installation Safety.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

Specific Safety Requirements publication on Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR 2/1, Requirement 24 [1] states: "The design of equipment shall take due account of the potential for common cause failures (CCF) of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability."

The IAEA has published new safety guide SSG-39 on the Design of instrumentation and control (I&C) systems for nuclear power plants [2]. This safety guide provides recommendations on the design of I&C systems to meet the requirements established in [1]. Reference [2] provides guidance for the overall I&C architecture in support of the concept of defence in depth applied in the design of the plant systems and in establishing defence in depth for the I&C system itself as protection against common cause failure.

Common cause failures within the protection system might result in unacceptable consequences for certain combinations of common cause failures and postulated initiating events.

This publication describes a philosophy where the diverse actuation system (DAS) backs up safety functions performed by the primary protection systems. The term 'diverse actuation system' used in this publication is not the only term that could be used to describe such systems. Depending on Member States, other terms may include 'Secondary Protection System', 'Additional Protection System' and 'Non-Computerised Safety System'. The defining feature of such systems is that they are of a diverse design from that of the reactor protection system. A justification for this second system (the DAS) may be based upon deterministic and/or probabilistic analyses of initiating events, and therefore it may only backup a subset of the functions performed by the primary protection system to address CCF coincident with the more frequent postulated initiating events (PIEs).

Diverse actuation systems have been implemented as a backup to the primary protection systems at existing plants, as well as new nuclear power plant designs to increase the reliability of safety functions in case of CCF in protection systems, in particular in programmable digital protection systems. Current practices in Member States show that there are, however, different approaches to the safety classification, and to the use of analogue or digital components with different attributes in the design of a DAS so as to mitigate the consequences of common cause failure of the reactor protection system.

Design criteria for a diverse actuation system vary among countries and a consensus on adequate level of diversity has not been established yet (see Annex III of Ref. [2]). These variations result from different regulatory requirements or meeting the specific customer needs for the architecture of I&C systems of a nuclear power plant.

Specific considerations for the implementation of diverse actuation functions in an I&C system architecture are provided in the following subsections.

In the frame of this publication, the equipment and subsystems accommodating the diversely implemented functions are addressed as 'Diverse Actuation System' although in practice, this may comprise functions spread over several individual I&C systems.

1.2. OBJECTIVE

The purpose of this publication is to identify, based on current practices in Member States, common criteria for the design and implementation of a diverse actuation system as a backup system to a reactor protection system to implement safety functions.

1.3. SCOPE

This publication identifies and discusses criteria for the design of a diverse actuation system at nuclear power plants. The advantages and disadvantages of these criteria may vary for different types of reactors.

The critical areas include:

- Assessment of the attributes of diversity in I&C system architecture;
- Safety classification;
- Design criteria;
- Current technological options for the diverse actuation system;
- Use of manual actions and displays for diverse actuation.

This publication intends to provide specific details for utility engineers, operators, researchers, managers, and personnel responsible for all aspects of design and implementation of I&C systems. This publication will also aid Member States to support assessment of diversity in I&C architecture as a defence against common cause failures.

1.4. STRUCTURE

This publication contains seven main Sections and nine annexes.

Section 1 introduces the topic, objective, scope and structure of the document. Section 2 provides overall considerations of diverse actuation in I&C system architecture. Section 3 discusses the criteria for diverse actuation systems. Section 4 discusses technology options that can be applied for a diverse actuation system. Section 5 discusses the use of manual actions for diverse actuations. Section 6 provides an introduction to the annexes which show several examples of current practices on implementation of diverse actuation systems. Section 7 contains summary and conclusions.

References in this publication provide links to important documents, codes, standards and other guidance publications relevant to the design of I&C systems in NPPs.

Annexes to this publication provide examples of current practices in Member States on design and implementation of diverse actuation systems at new and existing nuclear power plants.

2. CONSIDERATION OF DIVERSE ACTUATION IN I&C SYSTEM ARCHITECTURE

2.1. DEFENCE IN DEPTH

Defence in depth in nuclear power plants consists of a hierarchical deployment of levels of equipment and procedures to maintain the effectiveness of the physical barriers placed between radioactive materials and workers, the public and the environment.

The defence in depth concept protects the three main barriers to release of radioactive material, the fuel, the reactor coolant system and the containment. A combination of inherent design features, active systems and administrative controls are provided to accomplish the 3 fundamental safety functions that protect the barriers to release. The design features, systems, and administrative controls are designed to implement the defence in depth strategy required by [1]. Many of the systems depend upon I&C systems for their proper operation. The I&C systems do not themselves provide defence in depth for the plant, but they have to support the plant defence in depth design.

2.2. CONCEPT OF PLANT STATES

The earlier concepts of the plant states as described in earlier IAEA publications NS-R-1 and SSR 2/1 comprised normal operation (NO), anticipated operational occurrences (AOO) and design basis accidents (DBA). Design basis accidents are defined by postulated initiating events considered in the design. Events other than postulated initiating events, fell into category of beyond design basis accidents. Beyond design basis envelope was not precisely defined and the safety demonstration focused on a few specific issues such as the anticipated transients without scram (ATWS) and a station blackout (SBO).

An updated concept of the plant states has been introduced in the SSR 2/1, Rev.1 [1]. Accident conditions considered in the design now comprise the design basis accidents and design extension conditions (DEC). The design extension conditions are postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. DEC is split into two categories; (i) without significant fuel degradation, also called DEC-A and (ii) with core melting, called DEC-B.

2.3. I&C SUPPORT FOR THE PLANT STATES

This section describes the typical role and functions across the plant states in accomplishing defence in depth and the measures provided with I&C systems to avoid the failure of one level of defence causing the failure of other levels.

2.3.1. I&C systems for normal operation

Architectural design across the plant states assigns the overall I&C functions to individual systems to controls complexity and limit the propagation of failures between systems. The architectural design has to ensure that the I&C does not jeopardize the independence between defence in depth provided at the plant level.

The I&C functions for normal operation are to:

— Control plant operations within the range of steady state operations;
— Support surveillance and in-service inspection programs in monitoring the condition of plant systems, structures and components.

I&C systems that control operations typically performs category 3 functions and are classified according to guidance provided in Ref. [3]. I&C systems that support surveillance, in-service inspection and condition monitoring are typically not safety classified but are still important to the early identification of failures or degradation of systems or fission product barriers.

2.3.2. I&C systems for anticipated operational occurrences

The I&C function for anticipated operational assurances (AOO) is to limit the effects of abnormal operation and failures so that the plant can be returned to normal operation as soon as possible. These I&C functions are typically category 1 and 2 functions, and are classified according to guidance provided in Ref. [3].

The I&C functions for AOO are to:

— Control the effects of abnormal operation;
— Prevent failures of equipment and fission product barriers.

2.3.2.1 Control of abnormal operation

Controlling the effects of abnormal operation include controlling the effects of abnormal operation of both plant equipment and the I&C itself.

Normal control systems are designed to detect deviations from normal conditions and initiate actions to return conditions to normal. For deviations and failures that can result in fast changes to plant conditions automatic actions are normally provided. Furthermore, the main control room human–machine interface (HMI) displays the plant parameters and alarms deviations from normal levels so that operators are aware of deviations and provide manual controls so that operators can manually control the abnormal operation. Where deviations or failures result in slow changes to plant conditions, automatic control may not be needed.

I&C systems for AOO typically include systems that:

- Control reactor power;
- Control normal operation of the primary and secondary circuits;
- Control decay heat removal during transition from power operation to shut down;
- Control decay heat removal during shutdown;
- Transfer between power supply between off-site sources and isolate faulted electrical equipment.

It is also important that the abnormal operation of the I&C systems themselves be controlled. This is typically accomplished by designing I&C control systems such that neither their normal operation nor failure can put the plant in a condition that is beyond the assumptions of the plant safety analysis or beyond the capability of Level 3 systems to mitigate (as shown in Fig. 1). Where this goal cannot be accomplished by system design, interlock systems may be employed to separately prevent the unsafe states or additional functions may be provided at level two to detect and act upon the effects of control system maloperation or failure.

Some plants also include interlock systems to prevent the plant from being placed in disallowed conditions. Examples of such interlocks include systems to:

- Prevent connections between high and low pressure piping when the pressure on the high side exceeds the design pressure of the low side piping;
- Limit the reactivity worth of any single control rod; and
- Prevent control rod configurations that would result in unacceptable flux distributions in the reactor core.

Abnormal I&C operations also include internal events that degrade the operators' ability to bring the plant to a safe state from the control room. For this eventuality a supplementary control room is provided for which the reactor can be placed and maintained in a shutdown state.

2.3.2.2 Detecting failure in plant systems

I&C systems have a role in detecting failure in other plant systems and in detecting failure in the I&C itself. The HMI displays and alarms discussed above are a significant source of information for alerting operating staff to failure of plant equipment or to plant conditions that need further investigation by field operators or maintenance staff.

I&C usually also includes functions to detect degradation of systems that contain radioactive material. These functions are important to provide operators with prompt and quantitative information to take corrective action before the barriers to fission product release are unacceptably degraded. I&C systems that support these functions typically include:

- Fuel failure monitoring systems;
- Reactor coolant system leak detection systems;
- Radiation monitoring systems.

I&C systems include a number of means for alerting operating staff to failures. These include:

- Design such that failures are self-revealing;
- Self-diagnostic functions;
- Automated testing, and
- Provisions and procedures for manual testing and inspection.

I&C systems normally incorporate more than one of these means. The means of failure detection provide the capability to detect any failure within an acceptable time period.

2.3.2.3 Safety classification

Most I&C functions for AOO are safety related. In some cases, interlock functions are safety classified. Some functions provided to monitor for failures in plant equipment or I&C systems may be classified as not important to safety. Nevertheless, the items that implement these functions will have the same safety classification as the monitored system unless the items that perform the monitoring function are fully isolated from the items that perform the safety function.

2.3.2.4 Independence

I&C equipment that contributes to defence in depth Level 1 and Level 2 are functionally diverse from the plant systems that they control.

Wherever possible I&C systems are designed so that their failures are safe and self-revealing or revealed by indications from other, unaffected functions. Such means of detecting failures of I&C systems are inherent in the design and thus independent of equipment failure. The maintenance staff using independent equipment performs periodic tests. Independence from environmental effects expected in plant operational states is achieved by confirming that items important to safety are capable of withstanding the normal and abnormal environmental conditions expected during operation. Items performing level 1 and 2 are not designed to tolerate exposure to unlikely internal hazards.

A remote shutdown facility or system is provided to allow safe shutdown capability that is independent of events that can disable the capability to achieve this from the main control room. Events considered include those that require evacuation from the main control room and those that may cause failure of needed control room displays and controls.

2.3.3. I&C systems for design basis accident

The I&C function for DBA is to prevent core damage in the event of a postulated initiating event including events that represent failures of I&C system at both normal operation and AOO.

I&C functions for DBA are to:

- Initiate, and control as necessary, the operation of engineered safety feature system;
- Provide information and controls for operators to take pre-planned actions related to accident mitigation and to achieve and maintain safe shutdown following an accident; and
- Provide information determining the status of the plant in accident conditions.

I&C systems for DBA typically include:

- The plant protection system (reactor trip and engineered safety feature actuation);

- Accident monitoring system;
- Systems that isolate emergency power supplies from off-site sources;
- Systems that control the startup, loading and operation of emergency power sources.

2.3.3.1 Safety classification

I&C functions for DBA are category 1 functions and are classified as safety according to guidance provided in Ref. [3]. The design of safety systems employs additional integrity strategies over and above those applied for all systems important to safety. These additional strategies include compliance with the single failure criterion, independence, application of more rigorous development processes, more rigorous qualification, more extensive on-line and periodic testing.

In plants that employ passive engineered safety features the emergency alternating current power systems, sources, and their controls might be classified in lower safety class (see guidance in Ref. [3]).

2.3.3.2 Independence

I&C systems that contribute to level 3 are diverse from the I&C systems that operate at levels 1 and 2. They are also designed to be independent of systems that operate at levels 1 and 2 by providing physical separation, electrical isolation, communications independence and functional independence from systems of lower safety classification. Level 3 systems are designed and rigorously qualified to be resistant to the effects of common environments including environments created by design basis accidents, other internal events and external events. Extra redundancy, physical separation, and electrical isolation are also sometimes provided so that I&C failures caused by a localized conditions will leave intact fully functional safety systems that continue to meet the defined reliability requirements.

2.3.3.3 Common cause failure of the reactor protection systems

In some Member States, a diverse backup system is provided to cope with the effects of common cause failure of the main reactor protection system in combination with postulated initiating events as defence in depth Level 3 function.

2.3.4. I&C systems for design extension conditions

I&C functions for DEC are to further reduce the likelihood of core damage and the magnitude of radioactive releases in the event of a severe accident.

The existence of a severe accident implies that plant systems supporting defence in depth levels 1, 2 and 3 have failed to accomplish their safety objectives. Nevertheless, some of these systems may be available for use in different modes to support core cooling or the protection of containment integrity.

The I&C functions for DEC are to:

- Monitor the main characteristics of plant status;
- Support operations to maintain the core subcritical;
- Support restoration of heat removal from the core and spent fuel;
- Support protection of containment integrity; and
- Support activities to delay further plant deterioration.

In some Member States, a diverse backup system may be provided to cope with the effects of common cause failure and postulated initiating events as DEC-A function.

Installed plant instrumentation has an important role in providing information about plant status, but these instrumentation sources may be supplemented with information from portable measurements, direct operator observation or analysis of air, gas and liquid samples.

The I&C may also be needed to start pumps and to align valves that are located in areas that may be inaccessible to operators under severe accident conditions. Manual control circuits from the control room or other operator-accessible locations have an important role in DEC.

2.3.4.1 Safety classification

Systems used at level 4 are classified according to their primary function. They may be classified as safety, safety related or not important to safety. According to guidance provided in Ref. [3], any function that is designed to provide a backup of a function categorized in safety category 1 and that is required to control design extension conditions without core melt, belongs to category 2 function.

2.3.4.2 Independence

For the most part independence between functions will be that provided for their normal functions.

Accident monitoring instrumentation and remote controls identified as critical for severe accident management is typically directly connected from sensor to display and from operator control to the final actuation device. Provisions are made for connecting temporary power for these functions.

2.3.5. I&C systems for mitigation of radiological consequences

Actions for mitigation of radiological consequences take place outside of the plant, but plant and off-site I&C has a role in providing some of the information needed to decide what actions are to be taken.

I&C functions for mitigation of radiological consequences are to:

- Support the determination of the source term that is available for release if containment or confinement structures leak;
- Monitor releases at planned discharge points;
- Monitor the activity in an array of sources outside of the plant;
- Monitor the plant atmospheric conditions that are needed to predict the dispersion of radioactive material.

Information of this type usually is needed in the control room, on-site emergency centre and off-site emergency centre.

2.3.5.1 Safety classification

Plant radiation monitoring systems are normally classified as safety related. Some measurements may be classified as safety for their role in responding to design basis accidents.

Off-site instrumentation is normally classified as not important to safety.

2.3.5.2 Independence

Installed instrumentation for monitoring radiation levels within the plant and at planned release points are normally part of the instrumentation provided for levels 2, 3 and 4 of defence in depth. Procedures are normally available to independently obtain the needed information from other sources such as portable detectors, passive dosimeters, analysis of samples, estimation based upon the reading of non-plant sensors, or predictions of severe accident models.

Table 1 provides examples of the I&C support for the plant defence in depth concept. It is recognized that the role and functions of I&C systems in accomplishing defence in depth that described in the section provide examples and may vary across the Member States.

TABLE 1. I&C SUPPORT FOR THE PLANT STATES

Plant state	Objective (From SSR 2/1, Rev.1, [1])	Essential means (From SSR 2/1, Rev.1s, [1])	Applied to plant I&C systems	Safety classification (From SSG-30, [3])
NO	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Comprehensive design bases for all I&C systems, reliable normal control systems	Class 3
AOO	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Systems to prevent certain unsafe operating modes, Testing and self-diagnostic provisions for I&C, design limitation on control system failure modes, I&C support to condition monitoring of plant systems	Class 2 and 3
DBA	Control of accidents within the design basis	Engineered safety features and accident procedures	Reactor protection system, diverse system* for the reactor protection system failures	Class 1
DEC	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of design extension conditions	Complementary measures and accident management	Diverse system** for the reactor protection system failures, design provisions for DEC (e.g. manual controls for SAM systems, accident monitoring instrumentation)	Class 2 and 3***

* Some Member States (e.g. associate to WENRA) consider a postulated initiating event combined with CCF of the reactor trip or engineered safety features actuation system (ESFAS) as a Level 3 function, consequently a diverse system is placed in Level 3.

** Some Member States (e.g. following the US regulatory framework) consider a postulated initiating event combined with CCF of the reactor trip or ESAFS as a Level 4 function, consequently a diverse system is placed in Level 4.

*** Some Member States do not consider design provisions for DEC as important to safety.

2.4. CONSIDERATION OF DIVERSITY

The design of reactor protection system is significantly more complicated than the systems that they control. Furthermore, the programmable digital systems may depend upon software that is common to every division of the safety actuation. This common software may be in the applications program, operating system or development systems. This commonality poses the risk that identical common faults will be introduced into all divisions of an I&C system and that these faults will be executed simultaneously if all divisions receive sufficiently similar inputs.

The high level of complexity, and the concern about software commonality result in the inability to demonstrate that the I&C systems will not be the dominant cause of common cause failure to initiate reactor protection system. To address this issue the protection systems are analysed to identify vulnerabilities to common cause failure that could result in unacceptable radiological consequences.

Reference [2] states that “the overall I&C architecture should not compromise the implementation of defence in depth and the diversity strategies of the design of the plant”. It also provides guidance on the overall I&C architecture in support of the concept of defence in depth applied in the design of the plant systems and in establishing defence in depth for the I&C system itself as protection against common cause failure. The functions allocated to the I&C systems include those functions that provide information and control capabilities relevant to operation of the plant in the various modes of operational states and in accident conditions.

In many NPPs, programmable digital I&C systems are interconnected and more complex to analyse (and, thus, safety assurance is more difficult to demonstrate than was the case for earlier generations of I&C systems). Analysis to identify conditions that might compromise the defence in depth or the strategy for diversity of the plant design is one of the means of investigating the vulnerability of I&C safety systems to common cause failure. In order to perform the analysis, it is necessary to understand the role of each individual I&C system in the defence in depth concept of the overall I&C architecture.

Backup of protection functions may be implemented as a dedicated stand-alone system, or via assignment of a set of I&C functions to I&C systems introduced in the architecture for other primary purposes providing adequate independence, defence in depth and diversification. In any case, the approach used to specify the functions, and to specify and implement the systems has to follow the approach necessary for any kind of I&C systems. This starts with the identification of the mission of the system(s) involved and then goes down to the implementation based on the specified criteria.

What is specific for DAS is that diversification to the reactor protection system has to be provided, and decided systematically. Section 3 lists the areas which need to be addressed in the design as ‘criteria’ and puts emphasis on those areas which are specific for DAS, especially the diversity criteria. The idea of implementing diversity within the reactor protection system is also possible.

Compliance of the design with the relevant design criteria needs to be demonstrated in the licensing process. This is typically done through analyses, justifications and other evidences. The evidences are generally of the same nature as for any other safety classified I&C systems, in line with the safety class, and comprise documents such as equipment qualification files, accuracy and response time analysis, test planning and test result documentation, failure mode and effects analysis, reliability analysis.

A specific case is the justification of the adequacy of the diversification of the DAS from the main protection system. Typical analyses to be considered include:

- CCF analysis for the individual I&C system, to justify which CCF mechanisms are addressed by the diversification within the primary protection system or DAS respectively, in order to justify the exclusion of certain types of CCF if these are managed without the need for any further diversification;
- Diversity / defence in depth analysis may complement this, to justify that an adequate set of functions has been selected, and that the implementation provides adequate diversity;
- Interface analyses, either integrated or prepared as separate documents, will justify the independence between systems, absence of unintended interfaces or justification that the implemented interfaces are consistent with the required independence.

Some of these analyses may be prepared on the basis of the individual I&C systems, and others are preferably prepared as common analyses for the complete I&C architecture, to address the proper interaction between systems within the defence in depth concept.

2.5. SIMPLICITY IN THE DESIGN

Simplicity is not a measurable or clearly defined characteristic of an I&C system so there is little guidance in Member States and international standards organizations that specifically addresses the aspect of simplicity for I&C systems, or in particular, programmable digital I&C systems. Consequently, no acceptable degree of simplicity has been established for I&C systems. However, measures need to be taken to avoid unnecessary complexity in the design of a DAS and its interfaces.

Complex programmable digital I&C systems challenge the demonstration of conformance with the fundamental design principles in safety I&C systems, such as independence, diversity and defence in depth, redundancy, and determinism (predictability and repeatability). Added complexity associated with the performance of functions not directly related to the main system functions may introduce potential design errors or additional hazards. For example, on-line self-testing and self-diagnostics functions, which are routinely incorporated in a programmable digital I&C system, could improve system availability and reliability, but could also add complexity to the system design.

A balanced approach is usually adopted between the potential risks associated with adding new functionality to I&C system and the benefits that those additional functions provide (see para 2.56 – 2.65 of Ref. [2]). When faced with several design options on how to carry out a safety function, the simpler design options need to be selected to accomplish the function and address potential hazards with the most confidence and clarity.

Simplicity attributes have to be considered in the design of the DAS and also in its implementation. Examples of simplicity attributes include limitation to only the necessary safety functions, a minimum number of inputs and outputs, few configuration parameters, high testability and software architecture with minimal interrupts. These attributes could help contribute to simplicity in the design of the DAS.

A consideration of simplicity for the design of the DAS needs to be made in combination with other fundamental design principles such as redundancy, independence, defence in depth, diversity, and determinism (predictability and repeatability).

2.6. OPTIONS FOR ARCHITECTURAL SOLUTIONS

There are many different country specific requirements and plant design solutions adopted for diverse actuation provisions to mitigate potential common cause failure of the reactor protection system. However, the objective for a chosen architecture is to assure the independence of protection system divisions, and the independence of the different levels of defence in depth applied at the plant.

Figure 1, which is a modified figure from Ref. [4], shows an illustrative example of a highly simplified and hypothetical I&C architecture design that has been subject to some modification away from an idealized structure of completely independent plant states.

Figure 1 shows the elementary layers of I&C, each having functional and communication capabilities, starting at the bottom from the plant sensors and actuators, through the I&C systems that provide automation of the process and safety functions in the centre, and up to the supervisory control and information systems used by operations and maintenance staff to control and monitor the plant.

Reading across the Fig. 1 it shows the I&C system support in the plant states. Different countries may have varying expectations on the exact requirements for I&C systems that are deployed to prevent escalation of plant conditions as a result of anticipated operational occurrences or accident conditions. The I&C layers show functions across the plant states for normal control of the plant; prevention and surveillance features; reactor protection and safety functions, together with complementary safety features to mitigate core melt; management of severe accidents; and to support planning of emergency response.

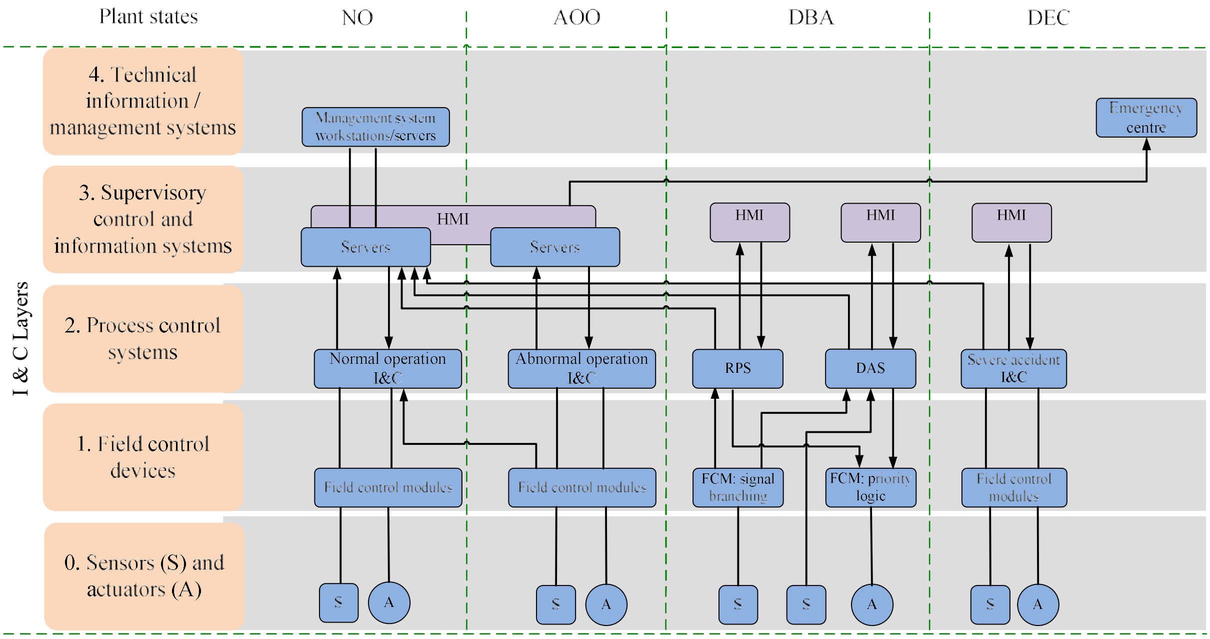


FIG. 1. An overview of plant states and typical I&C layers[1].

Key: S = Sensor; A = Actuator; FCM = Field control module; RPS = reactor protection system; DAS = diverse actuation system.

The task and scope of the additional safety features of the DAS are to control postulated common cause failure events of the reactor protection system. This is a typical objective for a DAS or a strategy to provide diversity within the DBA, and it has consequently to be systematically diversified from or within the reactor protection system so as to reduce CCF vulnerabilities to an acceptable level. The DAS may also be diverse from the control system dependent on the safety analysis of a particular initiating event.

In the example illustrated in Fig. 1, the diverse actuation functions are shown as implemented as an apparently dedicated stand-alone system called DAS. Some Member States may prefer such an approach using a simple non-computer based system to mitigate potential common cause failure of a reactor protection system. However, this is not the only possible approach, and the same objective is sometimes achieved by assigning diverse and independent functions to other I&C systems that are provided at other levels for different primary purposes.

Figure 1 also shows primary reactor protection system and DAS apparently sharing the same sensors and actuators, and this does not mean to be a recommended or the only possible approach. In a theoretical case each primary reactor protection system and DAS could have its own instrumentation, its own human–machine interface (HMI), and be designed with no data communication with each other so as to be independent as far as practicable. However, practical limits are often encountered at the plant level, and pragmatic solutions may be necessary as I&C systems at different levels of defence in depth may control the same process components. Such solutions need to consider the overall plant safety concepts and country specific regulatory requirements and to be appropriately

[1] This figure has been adapted from NE Series publication NE-T-3.xx Approaches for overall instrumentation and control architectures of nuclear power plants (in preparation).

analysed and justified, while recognizing that there may be diminishing benefits in adding more I&C systems if ultimately the same plant process and mechanical components are being controlled.

It is also necessary to be clear about what potential failure events are considered to be credible as this determines what the DAS is intended to address. If the potential concern is CCF of the reactor protection system then the I&C automation layer (see Fig. 1) may be the most important area for diversification. The field control modules (e.g. priority logic) may also be the target for diversification, particularly if based on programmable digital technology, as they provide a common means to control the plant from several levels of defence in depth. Similarly, if the concern is that a particular postulated initiating event might not be detected by the reactor protection system (e.g. a postulated latent functional fault in the requirements specification), then it may be necessary to ensure that the DAS has a diverse means of detecting the event in order to enhance the defence in depth protection. In such cases it may not be possible to share sensors, unless the protection system already has diverse means of detecting the event, when it may be possible to share one or more of the diverse signals. Of course, a DAS might be intended to address any combination of these concerns, or others, and it is important to define the objectives and boundaries of the DAS while taking into account any requirements for strong independence that may apply in particular countries.

3. CRITERIA FOR DIVERSE ACTUATION SYSTEMS

3.1. BASIS FOR THE DESIGN

Annex III–11 of Ref. [2] recognises that it is not uncommon for safety assessments to find that common cause failures within a programmable digital protection system might result in unacceptable consequences for certain combinations of common cause failures and postulated initiating events. When this situation is encountered, a diverse actuation system is often provided to backup the reactor protection system against selected multiple failure events.

Paragraph 4.32 of Ref. [2] states that “an analysis should be done of the consequences of each postulated initiating event within the scope of safety analysis in combination with the common cause failures that would prevent a protection system from performing the necessary safety functions”. However, the scope, approach and acceptance criteria for the analyses as expected by regulatory bodies may vary among Member States.

Some examples of differences are discussed in Annex III–8, 9 and 10 of Ref. [2] and the choice of failure events to be addressed in the design might consider factors such as: the frequency of the event; the consequences of the event; margin to cliff edge effects; the time available for necessary human actions; and the objective regarding core damage frequency (CDF). Some examples of design choices that have been taken in consideration are provided in the annexes of this publication.

The diverse actuation system may provide a diverse means in the implementation of one or more of the three fundamental safety functions: (1) Control of reactivity; (2) Removal of heat from the nuclear fuel; (3) Confinement of radioactive material. In particular, the postulated failures to be protected by the diverse actuation system may include ATWS which may need to be considered as they could be dominant accident sequences for some types of reactors. However, no postulated initiating event in combination with a common cause failure is allowed to lead to unacceptable conditions. Therefore, the provision of a DAS, or diversity within the primary reactor protection system, is consistent with the reinforcement of the defence in depth and may provide an additional protection to prevent escalation to design extension conditions.

3.2. SCOPE OF FUNCTIONS AND ARCHITECTURE OPTIONS

The scope of functions and the design of the DAS within the plant I&C architecture depend mainly on the safety regulations that are in force in the country of the NPP. In advanced stages of NPP construction it is more difficult to add a DAS so it is important to reach an agreement about what kind of DAS is necessary at an early stage of the NPP construction. Constraints also exist in case a DAS is needed as part of refurbishment project at existing NPPs.

The scope of the DAS will be developed on the following aspects:

- Identification of the necessary and agreed set of I&C functions assigned to DAS, as outlined in Section 3.1;
- Selection of the architecture, i.e. design of DAS as a stand-alone system, implementation within other I&C systems, or a mix thereof.

The I&C functions that may be diverse are defined and categorized according to their safety significance [4]. The diverse I&C functions can be assigned to various I&C systems, or to a stand-alone DAS. It is possible that different solutions may be adopted for particular initiating events and dependent on what postulated failure the diversely implemented function(s) is intended to mitigate. The set of functions to be implemented and the architectural choice is strongly influenced by the postulated CCF scenarios that are the targets of the diversification:

- What is the set of plant transients and accidents to be mitigated?
- Do the field devices used by the reactor protection system provide adequate diversification or CCF exclusion, so that they can be shared with the DAS, or are a dedicated set of field devices required?
- Does signal conditioning provide adequate robustness or has it to be diversified?
- Does prioritization of actuator control provide adequate robustness or has it to be diversified?
- Is the focus of diversification on signal processing, i.e. can the diversification be restricted to signal processing only?
- Can diversity within the system achieve the CCF reduction goal without adding architectural complexity?

In the example illustrated in Fig. 1, DAS is implemented at the defence in depth Level 3 namely for coping with some PIEs and simultaneous CCF of reactor protection systems (i.e. process control layer) that could result in either ATWS or a failure to actuate engineered safety features. The independence between the reactor protection systems and DAS needs to be considered.

There may be additional aspects of diversification outside I&C that have to be included in the selection of the architecture, such as considerations for the diversification of other support systems. Especially in retrofit projects, the resolution of separation issues that could not be solved by changes to the reactor protection system may also be factored into the design of a DAS. This could lead for example to requirements for the separation of cableways and penetrations, and possibly also to requirements for physical separation between the main reactor protection system and the DAS.

With these aspects, there is a wide range for the scope of the DAS. This may go from a very small to a very large scale. The extreme cases would be:

- Either a rather limited DAS with a subset of protection functions only, sensors practically completely shared with the reactor protection system, or diversification limited to the signal processing.
- Or a large DAS with the functional scope close to the reactor protection system, and a large set of dedicated sensors. This might possibly include installation in dedicated rooms, use of diversified support systems, and implementation of diversified priority logic.

3.3. SAFETY CLASSIFICATION

The IAEA Safety Guide SSG-30, Ref. [3] provides recommendations and guidance on how to meet Requirement 22 in Ref. [1] for the identification of structure, systems and components (SSCs) important to safety and for their classification on the basis of their function and safety significance.

Paragraph 4.4 of Ref. [3] states that “a complete set of engineering design rules should be specified to ensure that the SSCs will be designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained to appropriate quality standards. To achieve this, the design rules should identify appropriate levels of capability, reliability (dependability) and robustness. The design rules should also take due account of regulatory requirements relevant to safety classified SSCs.”

Furthermore, Paragraph 3.15 of Ref. [3] states that “any function that is designed to provide a backup of a function categorized in safety category 1 and that is required to control design extension conditions without core melt” should be assigned to safety category 2.”

Beyond the guidance provided by the IAEA, there exists a large body of national and international standards that give more detailed recommendations about design methodologies and system characteristics that support compliance with Ref. [3]. In particular, two standards development organizations are responsible for most of the internationally used standards for instrumentation and control (I&C) in nuclear power plants: the International Electrotechnical Commission (IEC), Subcommittee 45A, and the Institute for Electrical and Electronic Engineers (IEEE), Nuclear Power Engineering Committee. Each organization has developed a large number of standards. Both organizations produce standards that respond to the common principles underlying the requirements of Ref. [1] and the recommendations of Ref. [2]. For example, the International Electrotechnical Commission in Ref. [5] defines three safety categories A, B and C, while the Institute of Electrical and Electronics Engineers Ref. [6] only distinguishes between safety and non-safety system classes.

It is mentioned in Section 2.1 that “design criteria for a diverse actuation system vary among countries and a consensus on adequate level of diversity has not been established yet” (see Annex III of Ref. [2]). These variations result from different regulatory requirements or meeting the specific customer needs for the architecture of I&C systems of nuclear power plants. This however results in inconsistent engineering design requirements for systems provided specifically as diverse backup to reactor protection systems.

The World Nuclear Association and in particular its Cooperation in-Reactor Design Evaluation and Licensing (CORDEL) Digital Instrumentation & Control Task Force has published a report on Safety Classification for I&C Systems in Nuclear Power Plants – Current Status and Difficulties in Ref. [7]. What this report identifies as the most challenging concern is “insufficiently comprehensive local regulations … This leads to the application of international codes and standards which are different to local requirements in order to fill the gaps.”

Owing to the above difficulties, a single harmonized classification scheme is currently not used among all Member States. Depending on Member State requirements, the same or a lower safety classification than the reactor protection system may be assigned to a DAS.

3.4. CONSIDERATION OF COMMON CAUSE FAILURE

Requirement 24 of SSR-2/1 (Rev. 1) [1] states: “The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.”

Common cause failures are multiple failures that arise due to a single specific event or cause or from propagation of a fault from one system or redundant equipment to another consequential failure. Common cause failure in I&C systems might happen because of human errors, errors in the development or manufacturing process, errors in maintenance, errors in software tools used in development, propagation of failures between systems or components, or inadequate specification of, qualification for, or protection against, internal or external hazards [2].

Common cause failures may occur simultaneously or over a period of time, and their impact could be that a system is no longer able to perform one or more of its safety functions when required, or alternatively may cause a spurious action by the system which may impact the plant.

Some common cause failures may arise from clear causes that can be analysed, but others, especially those in programmable digital protection systems, may be much harder to analyse explicitly due to a lack of clear data or identifiable causes.

Analysis of defence in depth and diversity is one of the means of investigating the vulnerability of I&C safety systems to common cause failure. Reference [2] provides recommendations on how to apply diversity in the I&C systems in order to cope with CCF as follows:

- Paragraph 6.58 states that a decision to use diversity or not to use diversity in accomplishing the fundamental safety functions under design basis accident conditions should be justified.
- Paragraph 6.59 states that where diversity is provided to cope with the potential for common cause failure, the use of more than one type of diversity should be considered.
- Paragraph 6.61 states that where diversity is provided, it should be demonstrated that the choice of the types of diversity used achieves the common cause mitigation that is claimed.
- Paragraph 6.62 states that it is not always necessary to apply diversity in separate systems. For example, functional diversity and signal diversity might be applied within a single system.

In order to address above recommendations, an analysis is performed to determine which failure mechanisms are postulated and which kind of diversification can be applied to cope with. Various options to address the CCF vulnerabilities and assesses the effectiveness, disadvantages and complexities associated with the options, can be considered.

Reference [8] gives an example of how CCF analysis could be performed to assess the defence in depth and diversity of the proposed I&C system and to demonstrate whether CCF vulnerabilities are adequately addressed. The objective of the analysis provided in Ref. [8] is to identify vulnerabilities to three system failure types:

1) A plant transient is induced by the instrumentation system for which the reactor trip or ESF function is needed, but may not occur, because of an interaction between levels of defence.
2) Undetected failures that cause protective equipment not to respond to a plant transient or design basis accident.
3) Anomalous readings (e.g. accident conditions may have modified instrument response). Since these failures are unpredictable by definition, a strategy dictated by experience is to ensure sufficient signal diversity that alternate means of detecting significant events exist.

The analysis proceeds by dividing the I&C system into blocks to reduce design details to an abstraction level that is consistent with the goals of the analysis. A block is defined as ‘a physical subset of equipment and software for which it can be credibly assumed that internal failures, including the effects of software errors, will not propagate to other equipment or software.’ Failure propagation modes are divided into two classes: ‘physical (e.g. electrical) and logical (e.g. by corrupted data or corrupted interactions caused by software design faults).’ The degree of diversity between blocks, subsystems, or items of equipment is assessed with respect to diversity attributes in order to argue whether one block is either diverse or not diverse from another.

For convenience in assessment, Ref. [8] separates diversity into six attributes, similar, but not identical to Ref. [2]: Design diversity; Equipment diversity; Functional diversity; Human diversity; Signal diversity; Software diversity. Vulnerabilities are considered to be adequately addressed if specific conditions related to plant integrity and radiological release criteria are met.

Reference [9] describes another method for CCF analysis within the I&C architecture that includes similar steps as described above.

These publicly available reports in Refs [2], [8] and [9] provide examples of methodologies to analyse CCF vulnerabilities within the I&C architecture. The safety acceptance criteria applied are relevant to specific reactor types in a particular national context.

3.5. OPERATING EXPERIENCE CONCERNING CCF

As mentioned in Ref. [4], the introduction and potential overuse of diverse features and functions can also have disadvantages such as an increase in overall complexity of the I&C architecture, increased risk of spurious actuations (see also Ref. [10], Annex G.6.) and increased complexity of the operating procedures which raises the potential for human errors.

Reference [11] states that "the experience of CCF occurrences in NPPs shows that the following types of causes are dominant; (i) latent faults which are related to faults in the requirement specifications …, (ii) latent fault which are introduced during maintenance …, (iii) the triggering of latent faults during maintenance activities…".

Recent study in Ref. [12] shows that potential CCF events were dominated by non-software issues. Life cycle management and human performance issues were more prevalent. This study also indicates that the faults often appears not due to failure of I&C systems, but from failure to understand fundamental plant design requirements that leads to CCF and that might simultaneously affect even diverse systems.

The limited information available to date, such as that provided in the above references, has not identified any direct link between the use of programmable digital safety I&C and the occurrence of failures which (under some circumstances) could potentially lead to common cause failures. However, by their nature these are extremely rare failures and a comprehensive and statistically rigorous analysis linking implementation technology to the likelihood of CCF based on operating experience has yet to be performed.

3.6. TYPES OF DIVERSITY

3.6.1. General

Paragraph 6.60 of Ref. [2] provides an overview of the different types of diversity:

- Design diversity;
- Signal diversity;
- Equipment diversity;
- Functional diversity;
- Diversity in the development process;
- Logic diversity.

Following the analysis described in Section 3.4, the adequate types of diversity can be selected for the design of a DAS. This selection will consider the strong points and potentially negative consequences of each type of diversification.

The analysis considers not only that a certain type of diversification mitigates against certain types of faults which could potentially lead to coincident CCF of multiple systems, it also evaluates the likelihood of particular types of faults existing in multiple components within the overall design and considers, if such faults did exist, their potential to give rise to multiple coincident failures (i.e. CCF):

- If postulated systematic faults are sensitive to a common triggering event;
- If there are credible barriers to prevent fault-propagation;
- If rapid development of multiple failures can be excluded.

Errors and deficiencies to which diversity is expected to reduce the vulnerability are as follows:

- Errors in the functional requirements;
- Design errors: incorrect specification or implementation of software algorithms; incorrect coding;
- Inadequate specification of hardware boards and electrical circuitry;
- Manufacturing errors: systematic errors in the manufacturing of electronic components; electronic boards, cabinet wiring, and plant level cabling;
- Maintenance errors: triggering system failures by erroneous maintenance actions.

It has to be noted that addressing these errors may lead to very different design solutions. While some of the items given may be addressed by adequate robustness / simplicity of the characteristics of the reactor protection system, others may be considered as critical and need to be addressed by diversity in the DAS. This means that the defined set of criteria for diversification allows for a certain range of approaches. The finally selected design of the DAS is reviewed to confirm that certain types of failures of the primary protection system due to systematic deficiencies can either be excluded, have acceptable consequences or are managed by the DAS.

The following subsections provide a discussion of types of diversification aspects and their relative strength and side effects.

3.6.2. Design diversity

Design diversity is achieved using different design approaches to solve the same problem or a similar problem. It can be considered as an overarching approach which includes several of the other types of diversification. Design diversity comprises the use of different architectures and different technologies. Use of different technologies for the reactor protection system and the DAS would be the strongest form of design diversity.

Globally, it provides defences against systematic faults intrinsic to the design of an I&C system itself. It is effective:

- To resolve issues created by errors in the design concept;
- To avoid common implementation errors (for hardware and software);
- To minimize common errors in sizing of allocated resources.

By itself, it may be less effective in other areas, for example:

- To mitigate common maintenance errors (as different maintenance approaches / procedures are enforced);
- To correct errors in the functional requirements for the I&C systems.

3.6.3. Signal diversity

Signal diversity is achieved by systems in which a safety action may be initiated based upon different plant parameters. It is a powerful approach to mitigate faults outside the technology of the I&C system and also implementation errors in the I&C system itself, as it enforces different types of sensors, different algorithms and thus different exposure of the software execution to signal trajectories. Signal diversity is effective:

- To reduce issues due to errors in the specification of functional requirements;
- To address certain implementation errors (e.g. in the implementation of functional algorithms);
- To address design or specification errors of the related sensors / transmitters;
- To address certain maintenance errors (because different signals imply different setpoints and thresholds to be maintained separately).

Independently from the DAS, signal diversity is traditionally applied to some level already in the reactor protection systems in many plant designs, e.g. in subsystems of the reactor protection system. Consequently for plant designs with a DAS, it may be convenient to assign one of the diverse signals to the DAS.

Signal diversity solutions may add additional hardware and associated mechanical connections and failure points. The maintenance associated with the additional hardware adds cost and personnel radiation exposure.

3.6.4. Equipment diversity

Equipment diversity is achieved by hardware that employs different technological characteristics, e.g. analogue equipment versus programmable digital equipment, solid state equipment versus electromagnetic equipment, or computer based equipment versus programmable logic equipment. Equipment diversity can also be implemented within a single technology, e.g. software-based technology, relying on central processing unit types of different designs, with different instruction sets. A different aspect of equipment diversity is manufacturing diversity.

Equipment diversity may thus be seen as a special approach of ‘design diversity’. It is effective in similar areas and also:

- To address systematic manufacturing faults;
- To enforce diversity in software components (as far as these are tailored for a given hardware type / family, programming because the central processing unit is by nature different from programmable logic equipment, so that common implementation errors are excluded).

Equipment diversity is not effective to address errors in the specification of functional requirements (as essentially the implementation aspects are addressed).

3.6.5. Functional diversity

Functional diversity is achieved by systems that take different actions to achieve the same safety outcome.

It is very effective to resolve issues due to errors in the specification of functional requirements and to address certain implementation errors (e.g. in the implementation of functional algorithms) and certain maintenance errors. Functional diversity is typically implemented together with signal diversity.

3.6.6. Diversity in the development process

Diversity in the development process can be achieved by using different design organizations, different management teams, different design and development teams, and different implementation and testing teams [2]. Generally, it is not considered a diversification approach on its own. It will be considered as complementary to other diversification approaches (e.g. functional diversity, signal diversity, design diversity, equipment diversity).

It is beneficial to further reduce risk of errors in the implementation of diverse systems. When equipment diversity is chosen as the approach for a DAS, it could be an adequate practice to impose also a certain diversity in the development process, e.g. through selection of a dedicated, independent design team. However, the efficiency of the approach does not have to be overestimated, unless there are also restrictions on the complexity of the design, or other diversification elements. This is because experience shows that designers tend to make similar errors, and simplicity will help to reduce the likelihood of errors.

'Diversity' for the verification and validation team seems to be consensus, as practically all standards for computer based safety systems impose adequate independence for the verification and validation teams, to ensure an independent, unbiased view on the development results.

3.6.7. Logic diversity

Paragraph 6.60 of Ref. [2] states logic diversity is "achieved by use of different software or hardware description languages, different algorithms, different timings of logical functions, and different sequencing of logical functions." Logic diversity is similar to design diversity and equipment diversity where errors are dealt with at the implementation level of the logic and at the coding level. It is an option when hardware diversity is not imposed, and signal diversity / functional diversity do not exist.

Logic diversity is efficient to address assumed errors in the use of a given tool set to produce functionally equivalent algorithms that are different in implementation.

3.7. DESIGN CRITERIA

The criteria described in this section are generally applicable to the I&C systems important to safety and follow recommendations provided in Ref. [2]. Applicability of each criterion specifically for the DAS design is discussed below.

3.7.1. Redundancy

The degree of redundancy provided for any diverse actuation system need not necessarily be the same as for the primary reactor protection system and specific requirements for redundancy within the DAS are not always provided. However, there may be good architectural and integrity reasons why the two systems may have the same degree of redundancy. Architectural reasons could relate to the need to interface to redundant process trains for actuation, while for integrity reason the reliability requirements placed on a diverse actuation system may be similar to the reactor protection system (certainly in respect of the potential for spurious actuation which is likely to be just as onerous for the plant as spurious actuation of the reactor protection system).

The safety classification of the system may also impose redundancy criteria on the system such as the need to be able to tolerate a single random failure, and potentially also during maintenance of one of the redundant divisions. If such a single failure tolerance criterion is imposed, then it needs to be considered whether it relates only to the performance of the systems safety functions, or whether it also applies to the avoidance of spurious actuations.

3.7.2. Setpoints and response time

Trip set points used to initiate safety actions are selected to ensure that the required actions occur before the monitored variable reaches its analytical limit and those safety settings are calculated using a methodology to allow sufficient margin to account for potential measurement biases, channel biases, uncertainties and any changes that may occur over time. The additional factor to be taken into account for diverse actuation is that its set points have to be determined to ensure that the reactor protection system actuates before the diverse actuation system while still providing adequate protection as this approach will assist plant operators to understand what is happening. The requirements for accuracies and response times for diverse actions will be defined on the basis of the results of plant safety analysis in the same way as for other I&C systems.

3.7.3. Priority

Priority between the main reactor protection system and the DAS needs to be clearly defined. Priority between the DAS and normal operation control systems also needs to be clearly defined. The signal coming from the DAS will normally have higher priority than that from the operation control systems but this may not always be the case when the two systems have the same classification.

Priority evaluation has to consider different failure modes of primary reactor protection system and DAS for each individual function. For example, the evaluation involves failure to actuate mode, spurious / adverse actuation, as well as a contradictory actuation demand e.g. in the ESFAS. Priority evaluation has also to consider how to manage the priority function between the DAS and the reactor protection system when the action is not unequivocally safety oriented. Priority evaluation has to determine for each individual function the correct priority between manual and automatic actions.

3.7.4. Accuracy and repeatability

Safety functions are required to be performed within defined response times and accuracies under all of the conditions of operation for which they are required. Thus, the design of a DAS has to provide deterministic behaviour such that for any particular sequence of inputs from the plant and for all specified operating conditions and all possible conditions of data loading, it will predictably issue the same outputs within a defined response time range.

3.7.5. Independence

Independence is established to prevent a failure, an internal hazard or an external hazard from affecting redundant elements of safety systems. Failure processes that are considered include: failures resulting from design basis accidents, exposure to the same hazards, electrical connections between systems or between redundant divisions, data exchange between systems or between redundant divisions, and common errors in design, manufacturing, operations or maintenance [2].

The criteria for independence include measures such as physical separation, electrical isolation, functional and communication independence.

Physical separation protects against common cause failure due to the effects of internal hazards. Internal hazards of concern include fire, missiles, steam jets, pipe whip, chemical explosions, flooding and failure of adjacent equipment [2].

Electrical isolation and functional independence (including communications independence) prevent the propagation of faults from one system to another. The primary objective is normally to prevent failure of a system in a lower safety class from propagating to a system in a higher class, and in particular, to the reactor protection system. As a consequence, isolation devices between systems are normally part of the higher classified system and have to be appropriately qualified.

As a DAS is provided specifically to mitigate protection system CCF, it is also important in this case that a primary protection system failure does not propagate to the DAS, and this may affect the design of isolation features if there are any connections between the two systems.

Functional independence is supported by the architectural design and careful treatment of data that are shared between functions. Functional independence is a means of achieving isolation of a system from another system. Functional independence can also be used as a means of achieving isolation between redundant equipment [2].

If data communication is used, measures are provided to ensure that any failure in the DAS will not adversely impact the reactor protection systems and vice versa. Furthermore, measures need to be provided to ensure that any failure in the lower classified systems will not adversely impact the DAS through the data communication link. System interface and suitability analysis can be conducted to evaluate potential hazards resulting from data communication among different systems.

3.8. RELIABILITY CRITERIA

Diverse actuation systems, such as any other NPP system or equipment designed for fulfilment of safety functions. The DAS reliability needs to be commensurate with its safety significance [1].

Regarding mode of operation, DAS is a typical I&C system that is intended to actuate ‘on demand’. In such a case, important characteristics of reliability are:

- Probability of failure on demand;
- Probability of spurious actuation;
- Failure coverage by self-diagnostics.

3.8.1. Probability of failure on demand

For this characteristic, the target for DAS may be less strict as compared with the reactor protection system as the expected frequency where the DAS is called upon is very low.

3.8.2. Probability of spurious actuation

For this characteristic, the target for DAS may be equivalent to the reactor protection system.

3.8.3. Failures coverage by self-diagnostics

High availability can be provided by a combination of periodic testing, self-diagnosis (of specific failure modes) and prompt corrective maintenance. High failure coverage by self-diagnostic reduces the burden for frequent periodic testing.

3.9. QUALIFICATION CRITERIA

Recommendations on equipment qualification, which are applicable for I&C systems important to safety, where a diverse actuation system belongs to, are provided in paras 6.77 to 6.134 of Ref. [2].

The DAS equipment needs to be qualified according to applicable rules for the selected safety class for the seismic and environmental conditions, as well as electromagnetic interference (EMI) and radiofrequency interference (RFI) that could exist during the events to which the DAS equipment is assumed to be exposed.

3.10. TESTING, DIAGNOSTICS AND MAINTENANCE

Requirement 29 of Ref. [1] states that ”Items important to safety for a nuclear power plant shall be designed to be calibrated, tested, maintained, repaired or replaced, inspected and monitored as required to ensure their capability of performing their functions and to maintain their integrity in all conditions specified in their design basis”.

Diverse actuation systems are important to safety, so their design normally permits periodic testing and calibrations. These include testing channels independently for failures and losses of redundancy, and in testing all layers comprising sensors, conditioning, logic, actuators and any controls or displays.

Particular issues that may need to be considered in relation to a diverse actuation system include:

- Testing and maintenance – In some cases (e.g. based on probabilistic requirements) it may be prudent to prevent the reactor protection system and the diverse actuation system from being tested or maintained at the same time. If this principle is adopted, then it will need to be determined if it is prevented by administrative controls or by engineered interlocks (e.g. permissives).
- Monitoring and diagnostics – It may be acceptable for the reactor protection system and the diverse actuation system to be monitored by the same system or through the same interface, as long as adequate provision is made to ensure the independence of the safety systems is ensured (e.g. electrical isolation and one-way communications). It may still be the case that diverse health monitor alarms are required, though these may often not be diverse for the two systems, but rather the health of both systems is displayed via two diverse routes (e.g. via normal operational displays and via safety panel alarms).
- Calibration – Care has to be taken so that the method and equipment used for calibration of the reactor protection system and the diverse actuation system do not introduce a potential for common cause failure affecting both otherwise diverse systems. Such maintenance activities may often threaten the independence between redundant channels within a system, but they could also challenge the independence of the reactor protection and diverse actuation systems if adequate precautions are not taken.

3.11. SUPPORT SYSTEMS

3.11.1. Power supply

Diverse actuation systems are typically connected to uninterruptible power supplies that provide the systems with power within the tolerances specified by the design basis for the I&C systems. DAS can be powered directly from direct current power sources in order to minimize the need for inverters, motor-generators or power transfer devices in the electrical power system.

Reference [13] provides recommendations for electrical power supplies and associated distribution systems for instrumentation and control systems. This reference specifies the performance and the functional characteristics of the electrical supply systems recommended for the I&C systems important to safety of a nuclear power plant. Guidance is also given on the possible use of these supplies for other I&C systems.

3.11.2. Heating, ventilation and air-conditioning

Independence within the overall I&C architecture is intended to prevent the propagation of failures between systems, and to avoid, where practical, exposure of multiple systems to the same sources of common cause failure. Examples of such sources of common cause failure include failure of common support service systems [2]. It is generally the case that any heating, ventilation and air-conditioning (HVAC) systems necessary to ensure DAS systems remain within their specified range of operating conditions.

A diversity of HVAC is generally not required since both, the main protection system and the DAS, in many cases share the same HVAC system. For instance a potential safety justification might be based on arguments that satisfactory defence against loss of HVAC is applied between the safety divisions and a possibility of a common cause failure mechanism affecting all divisions simultaneously is thus sufficiently diminished. Thus all safety divisions cannot be affected by the same common cause failure mechanism, even though one division of the reactor protection and diverse actuation systems may be affected simultaneously. In such cases the justification is between the divisions rather than between the reactor protection and diverse actuation systems.

3.12. QUALITY ASSURANCE

Paragraph 4.4 of Ref. [3] states that “a complete set of engineering design rules should be specified to ensure that the SSCs will be designed, manufactured, constructed, installed, commissioned, operated, tested, inspected and maintained to appropriate quality standards”. The quality requirements for the DAS have to take due account of regulatory requirements relevant to its assigned safety classification.

The management system applicable for a diverse actuation system, including quality requirements is provided in IAEA Safety Standards Series Nos GSR-Part 2, Leadership and Management for Safety Ref. [14], GS-G-3.1, Application of the Management System for Facilities and Activities Ref. [15], and GS-G-3.5, The Management System for Nuclear Installations Ref. [16].

In some Member States, an augmented quality assurance program is required for the DAS, if it is not classified as a safety system. This is because of the differences in safety classification scheme. This means that the DAS has to meet quality assurance requirements between those for safety and non-safety systems.

3.13. CYBER SECURITY CONSIDERATION

The diverse actuation system will be included within the scope of the overall plans for security, and in particular with respect to cyber security. The required safety and security measures have to be designed and implemented in an integrated manner so that they do not compromise each other in order to satisfy Requirement 8 of Ref. [1].

Diverse actuation systems that rely on hardwired technology typically offer fewer potential cyber security vulnerabilities than systems that use programmable digital technology. If programmable digital technology is used, then para 9.42 of Ref. [2] states that the design should take into account best practices in terms of cyber security. In summary, risks that may arise from potential security threats and vulnerabilities and that could affect the diverse actuation system will need to be appropriately managed. Certain hardware programmable devices (HPD) that are one-time programmable also offer fewer potential security vulnerabilities than traditional computer based systems.

3.14. HAZARD ANALYSIS

Hazard analysis in I&C systems is a process to assess an I&C system throughout its development life cycle to identify hazards (i.e., threats and causes), and, at the same time, specify requirements and constraints to eliminate, prevent or control those potential hazards.

A hazard analysis can be conducted by examining the DAS system, its subsystems, components and interfaces with other systems. The inter-relationships within the DAS and its interactions with other systems, subsystems and components need also to be analysed to identify unintended or unwanted DAS system operation, as well as the impairment or loss of the ability to perform its specified functions. Paragraphs 2.56 through 2.65 in Ref. [2] provide general recommendation to perform the hazard analysis for the plant I&C systems.

4. TECHNOLOGY OPTIONS FOR DIVERSE ACTUATION SYSTEMS

4.1. MAIN TECHNOLOGIES USED FOR NPP I&C

A diverse actuation system is either based on electrical and/or electronic and/or programmable electronic technologies. This section describes basic technology options but not specific instrumentation principles Fig. 2 shows the relationship between the terms that are used to describe the different families of technologies.

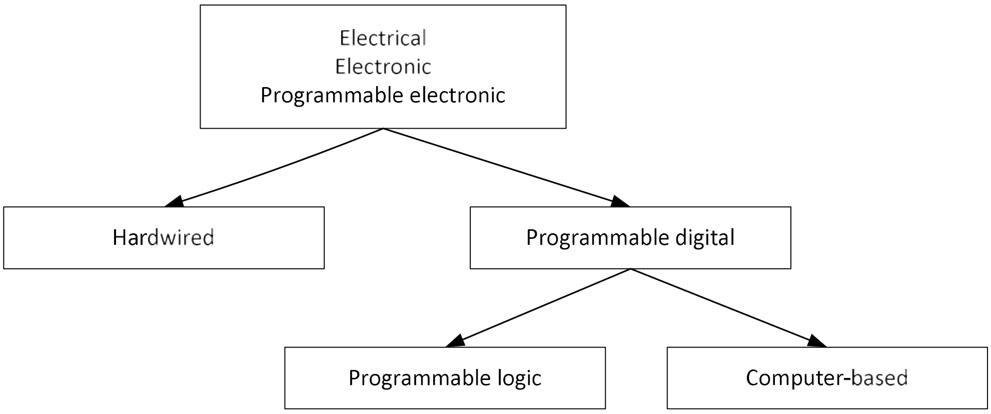


FIG. 2: Relationships between the technology related terms

Electrical and/or electronic and/or programmable electronic technologies can be subdivided into hardwired technology on one side and programmable digital technology on the other side.

Hardwired technology relies on relays, analogue electronic or discrete digital logic. It is described in more detail in Section 4.1.1.

Programmable digital technology relies on programmable logic or software instructions to accomplish function. It is further subdivided into programmable logic technology and computer based technology.

Programmable logic technology relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable. It is described in more detail in Section 4.1.2.

Computer based technology relies on software instructions running on microprocessors or microcontrollers. It is described in more detail in Section 4.1.3.

Finally, Section 4.2 presents the advantages and disadvantages of each family of technology regarding the implementation of a DAS.

4.1.1. Hardwired

Hardwired technology is a family that groups several different principles that are used to implement both logic and analogue I&C functions in NPP.

4.1.1.1 Pneumatic logic

Pneumatic systems are still in use and may be appropriate under certain circumstances, e.g. where electrical power is not necessary. Pneumatic systems are relatively simple and ‘relatively’ fail safe. Pneumatic components may be prone to mechanical failure.

4.1.1.2 Relay

Relay systems are relatively simple (at least when they are small). They are relatively inexpensive, and are immune to most forms of electromagnetic interference (EMI) and can be built for many different voltage ranges. However, relays are susceptible to a vibrations and seismic effects.

4.1.1.3 Solid state

The logic solver functions are performed by standardized electronic function blocks, which mainly include AND gates, OR gates, logic inverters and timers.

Solid state systems are hardwired, much like relays. Considering the merits and demerits of solid state systems they are comparable with relay based systems with the advantage that they have no mechanical moving parts and they are much smaller. The modules must be wired into the logic configuration that is required for the system.

Solid state system might be implemented using discrete components (transistors, capacitors and resistors) or using integrated circuits which contain several gates and are much more compact (e.g. Quad 2-input NAND-gate).

4.1.1.4 Programmable array logic (PAL)

PALs are small-size devices typically organized in OR/AND gate array in order to implement logic equations having the form of sum of products such as: output = (A and B and not C) or (not B and not C) or (D).

PALs are made specific by configuring connections, typically by blowing fuses or in some cases by configuring re-programmable switches.

The AND-gate structure is programmable, i.e. the product expression before programming is: (A and not A and B and not B and C and not C, etc.), where each term corresponds to one configurable connection. According to the functional requirement, the unneeded terms are removed to produce logic expressions A and not C.

The OR-gate structure is fixed: the inputs of the 'OR' are a fixed number of such programmable products, e.g. (A and not C) or (A and not B) or (D).

Low-level languages such as PALASM are typically used to configure PALs: the designer inputs the logic equations to be implemented and the tool translates them into a map of connections. No behavioural description such as in Hardware Description Language is possible with such languages.

PALs typically provide a few inputs and outputs (e.g. 10 inputs, 8 outputs) and they are equivalent to a few hundred gates at most. Due to this limited size they are considered hardwired technology and not programmable logic technology.

4.1.1.5 Magnetic logic

Magnetic logic is digital logic made using the non-linear properties of wound ferrite cores. Magnetic logic represents 0 and 1 by magnetizing cores clockwise or anticlockwise.

Examples of magnetic logic include core memory. Also, AND, OR, NOT gates and clocked shift logic gates can be constructed using appropriate windings, and the use of diodes.

Magnetic logic is inherently fail safe, i.e. the self-testing nature of the basic circuit means it will always fail safe, without the need for additional test or diagnostic circuits. The logical signal status, which reflects the 'safe' condition of critical process parameters, is represented by pulse-trains. In this way all the circuits remain dynamic continuously, during normal operation. Logic functions are processed by bi-stable magnetic core elements. Magnetic logic systems have the advantage of no moving parts which reduces the potential for random mechanical failures to impair reliability.

4.1.1.6 Analogue

Analogue functions may be implemented using discrete components (transistor, capacitors and resistors) or using more compact integrated circuits which contain several predefined blocks such as an operational amplifier.

Analogue functions may also be implemented using mechanical or pneumatic parts.

Analogue modules are usually needed for closed loop control and also to transform analogue signal into logic signal according to a chosen threshold.

4.1.1.7 Capabilities of hardwired technology

Logic functions (Boolean algebra + memories and timers) may be implemented in so called 'hardwired technology' using pneumatic logic, relay, solid state, PAL or magnetic logic.

Analogue functions may be implemented in so called hardwired technology using discrete components (transistor, capacitors and resistors), mechanical parts, pneumatic parts or more compact integrated circuit.

No calculation (fixed point or floating point) can be performed in practice using hardwired technology[2].

4.1.1.8 Susceptibility to CCF

Susceptibility to CCF for hardwired technology is generally considered less significant because of the relatively low complexity of the functionalities that may be implemented.

However, it does not mean that CCF can always be ruled out only because hardwired technology is used. A case by case analysis is typically necessary to conclude about the susceptibility to CCF of any particular design. Operating experience for relays has to be reviewed to avoid previously identified CCF vulnerabilities.

4.1.2. Programmable logic

Programmable logic technology is a family that groups several types of integrated circuit that consists of logic elements with an interconnection pattern, parts of which are user programmable.

Some circuits may be programmed by the user after manufacturing. The semiconductor industry typically distinguishes the following types of such circuits from the simplest to the most complex:

- Programmable Logic Device (PLD);
- Complex Programmable Logic Device (CPLD);
- Field Programmable Gate Array (FPGA).

There are three different ways to store the inter-connection pattern also called the 'configuration' of the circuit:

- Anti-fuse which does not require power supply and is programmable only once.
- Flash which does not require power supply and is re-programmable several times.
- Static random-access memory (SRAM) which requires a power supply and is re-programmable many times. SRAM requires external components to permanently store the configuration of the circuit such as an electrically erasable programmable read-only memory (EEPROM) or flash memory.

Some circuits have to be programmed during manufacturing:

- Application-Specific Integrated Circuit (ASIC).

[2] Computers can be built using discrete components as it was done in the early days of computer but this is not realistic for use in NPPs.

The industry further distinguishes semi-custom ASIC and full-custom ASIC where the latter offer more performances and flexibility at much higher design and manufacturing costs. There is no significant difference in the design principles between the full-custom ASIC and Integrated Circuit available off-the-shelf on the market.

Circuits that may be programmed by the user after manufacturing as well as semi-custom ASIC are typically developed with hardware description languages (HDL) and related software tools used to implement the requirements in a proper assembly of the pre-developed micro-electronic resources. These circuits are named HDL Programmed Devices[3].

4.1.2.1 Capabilities of programmable logic technology

Logic functions (Boolean algebra + memories and timers) as well as analogue functions can be implemented in programmable logic technology.

Calculations (fixed point or floating point) can be performed using programmable logic technology but it is typically more difficult than with computer based technology. This is because fixed point calculations require an arithmetic and logic unit (ALU) and floating point calculations require a floating point unit (FPU) that are not available natively in HDL.

For doing calculations with programmable logic technology several possibilities exist:

- Implement in HDL an ALU or an FPU (may be done in practice for simple ALU but hardly realistic for a full FPU);
- Use pre-developed ALU or FPU provided in HDL (synthesized or not);
- Use a blank integrated circuit that natively offers ALU and/or FPU in hardware.

Note that complete microprocessors may be implemented in programmable technology either in HDL (soft core) or embedded in the hardware of the blank integrated circuit.

4.1.2.2 Susceptibility to CCF

Susceptibility to CCF does not depend on the programmable logic technology itself but on how the technology is used to implement I&C functions.

If the programmable logic technology is used to implement simple logic functions that can be exhaustively tested (including internal states) in practice, then a case could be made that such design is not susceptible to CCF in multiple divisions due to latent design errors.

As the extremely opposite case, if the programmable logic technology is used to implement a microprocessor (embedded in hardware or in soft core), then the susceptibility to CCF is as significant as for computer based technology.

4.1.3. Computer based

Computer based technology relies on software instructions running on microprocessors or microcontrollers.

[3] The name HDL Programmed Devices originates from IEC 62566 “Development of HDL programmed integrated circuits for systems performing category A functions”.

The typical design process is to write the computer program in computer language, such as the C programming language[4], and to use a compiler tool set (i.e. compiler, assembler, linker) to produce the executable code that can run on the microprocessors or microcontroller.

4.1.3.1 Capabilities of computer based technology

Logic functions (Boolean algebra + memories and timers) as well as analogue functions can be implemented in computer based technology.

Calculations (fixed point and/or floating point) can be performed easily using computer based technology. This is because most of the modern microprocessors and microcontrollers natively include both the ALU and floating point unit (FPU) that are required. This is also because almost every computer language naturally offers a wide range of calculation operators on both integer and real floating types.

4.1.3.2 Susceptibility to CCF

Susceptibility to CCF is generally considered significant because of the high complexity of the functionalities that may be implemented.

Even when computer based technology is used to implement simple logic functions, the resulting computer programme can hardly be tested exhaustively in practice (including internal states) so CCF cannot be ruled out.

4.2. PROS AND CONS ASSOCIATED WITH EACH TECHNOLOGY OPTION

Table 2 summarizes advantages and disadvantages of technology options as discussed in Section 4.1.

TABLE 2. PROS AND CONS OF THE TECHNOLOGY OPTIONS

	Hardwired technology	Programmable logic technology	Computer based technology
Logic functions	Yes	Yes	Yes
Analogue functions	Yes	Yes	Yes
Fixed point calculation	No	Yes, Arithmetic & Logic Unit has to be implemented	Yes
Floating point calculation	No	Yes, with difficulty as a floating point unit is needed	Yes
Modifiability	Low	Low for anti-fuse / High for flash and SRAM	High
Self-diagnostics capabilities	Low	High	High
Obsolescence	Low	Medium / High (depending on whether specific native blocks provided by the vendor are used or not)	Medium / High (depending on whether the code is portable or not)
Susceptibility to CCF	Low	High*	High*
Cyber security demonstration effort	No	High**	High**

[4] C Programming language is standardized in ISO/IEC 9899

* Observed high reliability but difficult to demonstrate

** Demonstration effort strongly depends on the architecture of the configuration means, e.g. centralized (e.g. engineering station) or distributed (e.g. by configuring devices individually).

In some Member States, use of programmable logic and computer based technology may lead to considerable licensing uncertainty. However, the use of such technologies may also enable more precise protection functions to be implemented that can enhance nuclear safety.

It is to be noted that concerning programmable logic and computer based technologies, the pros and cons associated with factors such as obsolescence, susceptibility to CCF and cyber security demonstration effort are more dependent on the way the technology is used and for which kind of I&C functions than on the technology itself.

5. USE OF MANUAL ACTIONS FOR DIVERSE ACTUATIONS

5.1. PRINCIPAL CONSIDERATIONS

Paragraph 7.22 of Ref. [2] states that “The operator should be allowed sufficient time to evaluate the status of the plant and to complete the required actions. The associated timing analysis should take into account the time available and time required for each operator action necessary. The timing analysis determines the safety margin and as the safety margin decreases, the uncertainty in estimating the difference between these times should be appropriately considered.”

The footnote to the first sentence observes that “For new designs or significant modifications, it is advisable to design the plant such that during the first 30 min of a design basis accident, operator actions are not necessary to maintain plant parameters within the established limits.”

Para Annex III–15 of Ref. [2] states that “generally, manual actuation may be accepted as a diverse backup for the protection system but the conditions under which manual actuation may be credited vary. The range of accepted national practices includes the following:

- Manual action may be credited if the action is not needed in less than 30 min and human factors analysis has confirmed that a proper decision can be taken and implemented within that time;
- Manual action may be credited if the action is not needed in less than 20 min;
- Manual action may be credited for actuation of engineered safety features, but not for reactor trip;
- Manual action may be credited without restriction.”

Annex III–16 of Ref. [2] states that “while the above illustrates the range of practices among regulatory bodies, a regulatory body may take a different approach based upon the specific situation proposed.”

5.2. FUNCTIONAL ANALYSIS AND ASSIGNMENT

Manual actions may be credited for responding to events in which the safety function subject to a CCF is required only after a time period as specified in the safety analysis. The time available to perform the actions will be based on analysis of the plant response to the PIEs using realistic assumptions.

Manual action of safety functions can be performed on a system, division or component level, which depends on the design and human factors considerations. Manual actions need to be based upon, and ultimately included within, the emergency operating procedures (EOPs).

If a manual action in a DAS system is used as a diverse means or as part of the diverse means to accomplish the safety function, it needs to be demonstrated to be both feasible and reliable, given the time available and the ability of operators to perform the credited actions reliably. The demonstration can be achieved by a process consisting of human factors engineering (HFE) analysis, preliminary validation, integrated system validation on a full-scale simulator, and long term monitoring of operator ability to reliably perform the manual operator actions.

Generally, the HFE analysis demonstrates that the time available to accomplish the required manual actions is greater than the time required for the operator(s) to perform them correctly and reliably.

5.3. HUMAN-MACHINE INTERFACE

5.3.1. General

The HMI design has to address the controls for the manual actions. It has to provide indications that show the need for manual actions, and displays to evaluate the fulfilment of safety functions. The design of the human–machine interface for diversely implemented functions will have to be consistent with the HMI concept decided for the plant I&C architecture. Aspects to consider are:

- The assignment to the main control room, supplementary control room or other local control stations;
- Integration into the human–machine interface or provision of separate, dedicated controls and indicators;
- Association of controls and related indications;
- Consistency across different human–machine interfaces considering differences of the technology used.

5.3.2. Location of the human–machine interface

Manual actions that require short response times need controls to be located in the main control room (MCR).

For manual actions that do not require high coordination effort (e.g. across multiple components or equipment trains), and where the functional requirements allow for rather long response times, local controls may be adequate. This could be implemented in a dedicated local control station, or via local controls on switchgear cubicles in electrical equipment rooms. This approach may take credit from local controls specified already for use during commissioning or for maintenance during plant outages, and allows avoiding overhead for cable routeing and decoupling that could be necessary in case of a centralized arrangement.

The alarms and displays indicating the need for manual actions in any case will have to be arranged in the main control room, as well as the indications necessary to evaluate the successful execution (via check backs, binary status indicators and analogue displays).

Loss of the MCR has a low probability and is generally not considered in combination with the postulated CCF of the reactor protection system. Therefore implementation of additional controls for diverse manual actuation is generally not required for the supplementary control room.

5.3.3. Integration or separation of DAS-related controls and indicators

Modern plant designs typically comprise computerized human–machine interfaces, supporting plant control through computer based I&C systems. Diversified manual controls and supporting diversified indications will then be implemented either through dedicated conventional controls and indicators, wired to the corresponding parts of DAS, or comprise a computer based human–machine interface.

The control room design has to accommodate the various types of equipment (conventional push buttons, diversified computerized terminals). The choice to allocate them to dedicated control panels or integrate them with other controls and indications has to be made considering the complete inventory of controls / indicators and the conditions of use. A trade-off has to be made between human factors considerations and separation.

Typically, conventional indicators and controls linked to I&C systems in different places of the I&C architecture can be easily grouped in common control room panels; the allocation of the indicators and controls to different I&C systems is then hidden to the operator (unless there is dedicated identification of the HMI equipment, indicating the independence from other equipment). This facilitates easy use and transition between controls related to DAS and to other I&C systems. Concurrent use of controls linked to the reactor protection system and the DAS may be needed:

- For the operation of permissives when transitioning between plant states, where similar actions are required for the permissives of the reactor protection system and the corresponding functions of the DAS;
- When commands are memorized and need to be reset to allow the operator to regain control for long term manual actions.

Monitoring of the successful execution of actions of the reactor protection system, of automatic or manual diversely implemented functions may rely on the same set of indications for the plant's safety parameters provided they are not dependent on the reactor protection systems.

Adequate arrangements have also to be made when different HMI technologies are to be used (conventional displays and controls together with computer based HMI), considering concurrent use, frequency of operations and response time.

Designs which include the integration of computerized HMI equipment for diversely implemented manual actions have to account for similar CCF concerns, and this may lead to designs which avoid data communication between computerized HMI systems that could potentially propagate failures between such systems.

To find adequate solutions to these conflicting considerations, the DAS-related HMI equipment is ideally taken into account right from the beginning of the development of the control room concept.

6. CURRENT DESIGN SOLUTIONS AND DESIGN PROVISIONS

The annexes provide several examples of design solutions for implementation of a DAS which illustrate the range of various concepts and different scopes. All these examples describe a design solution that vendors developed for a specific reactor type. The annexes provide simplified descriptions of various DAS designs that are indicative only.

Each example provided in the annexes includes information on the following topics:

- Scope of functions;
- Place in the I&C architecture;
- Safety classification;
- Diversity criteria;
- Redundancy;
- Human–machine interface.

Annex I describes a design of diverse actuation system that has been applied for EPR reactor design in Olkiluoto-3. Diverse automatic actuation functions are implemented in the hardwired backup system (HBS). This comprises the automatic functions of reactor trip and actuation of ESFAS in a situation of postulated loss of the protection system. The technology used for processing the logic function is based on programmable logic devices (PLD).

Annex II describes a design of diverse actuation that has been applied for EPR reactor design in Flamanville-3. There is no specific I&C system that is called the diverse actuation system, however, functions are diversely implemented to cope with the postulated CCF of the reactor protection system as well as postulated CCF of the full safety automation system. Functions are diversely implemented by using two different platforms (TELEPERM-XS and SPPA-T2000 control systems) that are both computer based.

Annex III provides a solution for the US-APWR DAS design. A diverse actuation system is based on a non-safety diverse instrumentation and control system. It provides monitoring, control and actuation of safety and non-safety systems[5] required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the programmable digital safety system and programmable digital control system. The diverse actuation system includes an automatic actuation function, human–machine interface at the diverse panel, and interfaces with the programmable digital safety system and programmable digital control system.

Annex IV provides a solution used in the US-AP 1000 design. A diverse actuation system is a non-safety system that provides an alternate means of initiating a reactor trip, actuating selected engineered safety features, and providing plant information to the operator. The diverse actuation is included to support the AP1000 risk goals by reducing the probability of a severe accident that potentially results from the unlikely coincidence of postulated transients and common cause failure in the protection and safety monitoring system. The diverse actuation system receives signals directly from dedicated sensors. It contains redundant signal processing units that use hardware that is different or diverse from the hardware and software used in the protection and safety monitoring system.

Annex V provides a solution used in the Japanese ABWR reactor design. The Japanese I&C system for the ABWR has implemented programmable digital technology in the reactor protection system. This has been done considering the high reliability of programmable digital technology and rigorous application of verification and validation engineering methods. This is supported by positive operating experiences of programmable digital I&C performance for fossil plants and in nuclear non-safety grade control systems. The concept of diverse actuation has been implemented based on an independent manual backup I&C system. This together with other safety backup functions designed for safe plant shutdown (i.e. alternate rod insertion function and standby liquid control system) are provided to ensure diversity of the reactor protection system.

Annex VI provides a solution that has been implemented in the Russian VVER 1200 reactor design at Unit-6 of Novovoronezh NPP (commissioned in 2016). Diversification is essentially addressing the postulated failures of the processing part of the programmable digital reactor protection system. In that case, sensors are shared between the reactor protection system and the diverse actuation system. The DAS consists of two redundant, physically separated equal subsystems, each with a 2 out of 3 voting logic. The DAS design is based on hardwired technology that is significantly diverse from computer based technology used in the reactor protection system. Also the DAS development and V&V processes as well as involved developers and manufacturers were different.

Annex–VII describes a diverse actuation system that was installed, tested, commissioned and placed into service at the UK Sizewell B NPP in 1995. The diverse actuation system is termed the secondary protection system (SPS) at Sizewell B. The main reactor protection system at the station is termed the primary protection system (PPS). The primary role of the SPS is to provide the functions in a manner

[5] The USA uses a classification scheme with only two classes; safety and non-safety class. However for certain non-safety equipment, for example diverse actuation system, the augmented quality is applied for a product selection and a design solution.

diverse to those functions provided by the PPS against the most frequent PIEs. It actuates signals to the reactor trip switchgear and to the engineered safety features equipment, interlock signals to various plant components and controls, and provides manual actuation of engineered safety features.

Annex–VIII describes computerized diverse shutdown systems for CANDU reactors. Each CANDU reactor is designed with two diverse and independent shutdown systems. The shutdown systems are designed to limit radioactive release to the public by shutting down the reactor in the event of an accident. Either shutdown system is capable of shutting down and maintaining the reactor in the shutdown state for all design basis events.

Annex–IX describes the design of the diverse actuation system for the APR1400 reactor. The DAS is designed to mitigate the effects of potential CCF of programmable digital safety I&C systems including the plant protection system and engineered safety features-component control system (ESF-CCS). The DAS consists of the diverse protection system (DPS), the diverse manual engineered safety features (ESF) actuation (DMA) switches, and the diverse indication system (DIS).

In summary, all nine annexes provide a design solution for diverse actuation systems applied at the new and existing reactor designs.

Currently, there are a number of I&C retrofits going on or planned in Member States. The implementation of diverse actuation systems, as described above, may not be easily achievable for those retrofits when it was not part of the original design. When a diverse actuation system is considered as part of the I&C retrofits project, the regulatory requirements, especially the radiological release criteria applied for a diverse actuation system basically determines the design criteria and attributes, such as safety classification, functionality, independence and separation (electrical, physical). It depends on a specific I&C architectural design and technological solution (platform) to meet both the regulatory requirements and provide for an optimal way to address potential common cause failures in the reactor protection system.

7. SUMMARY

A diverse actuation system is often provided to backup the reactor protection system when analysis shows that common cause failures within the primary protection system might result in unacceptable consequences for certain combinations of common cause failures and postulated initiating events.

There is a general agreement that a diverse actuation system may effectively mitigate the consequences of specific initiating events in conjunction with a postulated common cause failure of a reactor protection system. There are, however, different approaches to the safety classification, the use of hardwired or programmable digital components with different attributes in the design of a diverse actuation system so as to mitigate the consequences of common cause failures of the reactor protection system.

This publication discuses Member States practices that may be considered for the design of diverse actuation systems, which include:

- The attributes of diversity in the I&C system architecture;
- The methods applied to enhance the level of diversity;
- The safety classification;
- The design criteria for diverse actuation systems;
- Current technological options for the diverse actuation system.

Furthermore, this publication discusses options for safe and reliable use of manual actions and displays for diverse actuation, including the design of the human–machine interface for diverse actuation functions that have to be consistent with the HMI concept decided for the plant I&C architecture.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1) IAEA, Vienna (2016).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of I&C Systems for Nuclear Power Plants, SSG-39, IAEA, Vienna (2016)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, IAEA Safety Standards Series No. SSG-30, IAEA, Vienna (2014).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Architectural Approaches in the Design of Nuclear Power Plant Instrumentation and Control Systems, IAEA Nuclear Energy Series No. NP-T-X.XX, Vienna (in preparation)

[5] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants - Instrumentation and Control Systems Important to Safety – Classification, IEC 61226:2009, IEC, Geneva (2009)

[6] INSTITUE OF ELECTRICAL AND ELECTRONIC ENGINEERS, Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603-2009, New York, (2009)

[7] WORLD NUCLEAR ASSOCIATION, Safety Classification for I&C Systems in Nuclear Power Plants - Current Status & Difficulties, Report No. 2015/008, London (2015)

[8] LAWRENCE LIVERMORE NATIONAL LABORATORY, Methods for Performing Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, Livermore (1994)

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Protecting against Common Cause Failures in Digital I&C Systems of Nuclear Power Plants, Nuclear Energy Series No. NP-T-1.5, IAEA, Vienna (2009)

[10] INTERNATIONAL ELECTROTECNICAL COMMISSION, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer based systems performing category A functions, IEC 60880 STD. Geneva (1986).

[11] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear power plants - Instrumentation and control systems important to safety - Requirements for coping with common cause failure (CCF), IEC 62340:2007, IEC, Geneva (2007)

[12] ELECTRIC POWER RESEARCH INSTITUE, Severe Nuclear Accidents: Lessons Learned for Instrumentation, Control and Human Factors. EPRI, Palo Alto, CA (2015)

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Electrical Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-34, IAEA, Vienna (2016)

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series No. GS-G-3.1, IAEA, Vienna (2006).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards Series No. GS-G-3.5, IAEA, Vienna (2009).

ANNEX I (EPR OLKILUOTO-3)

DIVERSE ACTUATION SYSTEM FOR EPR AT OLKILUOTO-3

I–1. SCOPE AND FUNCTION

For the Olkiluto-3 (OL-3) EPR^{TM} design, a hardwired backup system has been included in the design to address the licensing risks linked to the implementation of an I&C architecture relying exclusively on digital I&C systems. As a result, a set of I&C functions has been implemented on hardwired technology to backup the computerized TELEPERM XS (TXS)-based reactor protection system (PS) and the computer based post-accident functions for the OL-3 EPR design.

Diverse automatic actuation functions are implemented in the hardwired backup system (HBS). This comprises the automatic functions of reactor trip and actuation of ESFAS in a situation of postulated loss of the protection system. The HBS is able to cope with design base conditions category 2 (i.e. anticipated operational occurrences) and frequent design base conditions category 3 (i.e. frequent DBA) postulated initiating events.

The I&C functions implemented in the HBS rely on sensors and signal conditioning shared with the protection system. Processing of analogue signals is made in analogue circuits such as amplifiers and comparators for set point processing. Binary signals are processed in logic modules implementing standard logic gating (AND-gate, OR-gate, Flip-flops) and majority voting such as 2-out-of-4. Command outputs are sent to the devices initiating reactor trip and to the electronic priority modules controlling the actuators for ESFAS functions.

The technology used for processing the logic function is based on PLDs. For the different types of logic functions such as timers, flip-flops, elementary logic gates, several types of logic modules have been developed, each with a specific, factory-installed programming. The HBS functions are implemented by wiring analogue and binary modules in line with the required I&C functionality, considering also requirements regarding maintenance (e.g. sensor lock-out), periodic testing and self-monitoring and status indication in the control room. With this, although programmable logic technology is used, the HBS is considered hardwired, and diverse to the computerized protection system. The HBS equipment is installed in standard TXS cabinets, equipped with redundant power supply, fusing and cabinet monitoring equipment.

Also the functions for post-accident monitoring, long term post-accident manual actions and control of the related safety systems are addressed by the use of hardwired technology for the Safety information and control system (SICS). These safety classified functions for monitoring and manual control are implemented by hardwired controls, analogue indicators and alarm tiles integrated in conventional control consoles and panels using mosaic-technology. They basically include an individual channel for each sensor and actuator.

Generally, the indicators of SICS share sensors with other I&C systems, such as the protection system and the HBS, and rely on the same type of signal conditioning and distribution modules as these other I&C systems. Actuator control is generally through mosaic desktiles, directly wired to the electronic priority modules controlling the assigned actuators.

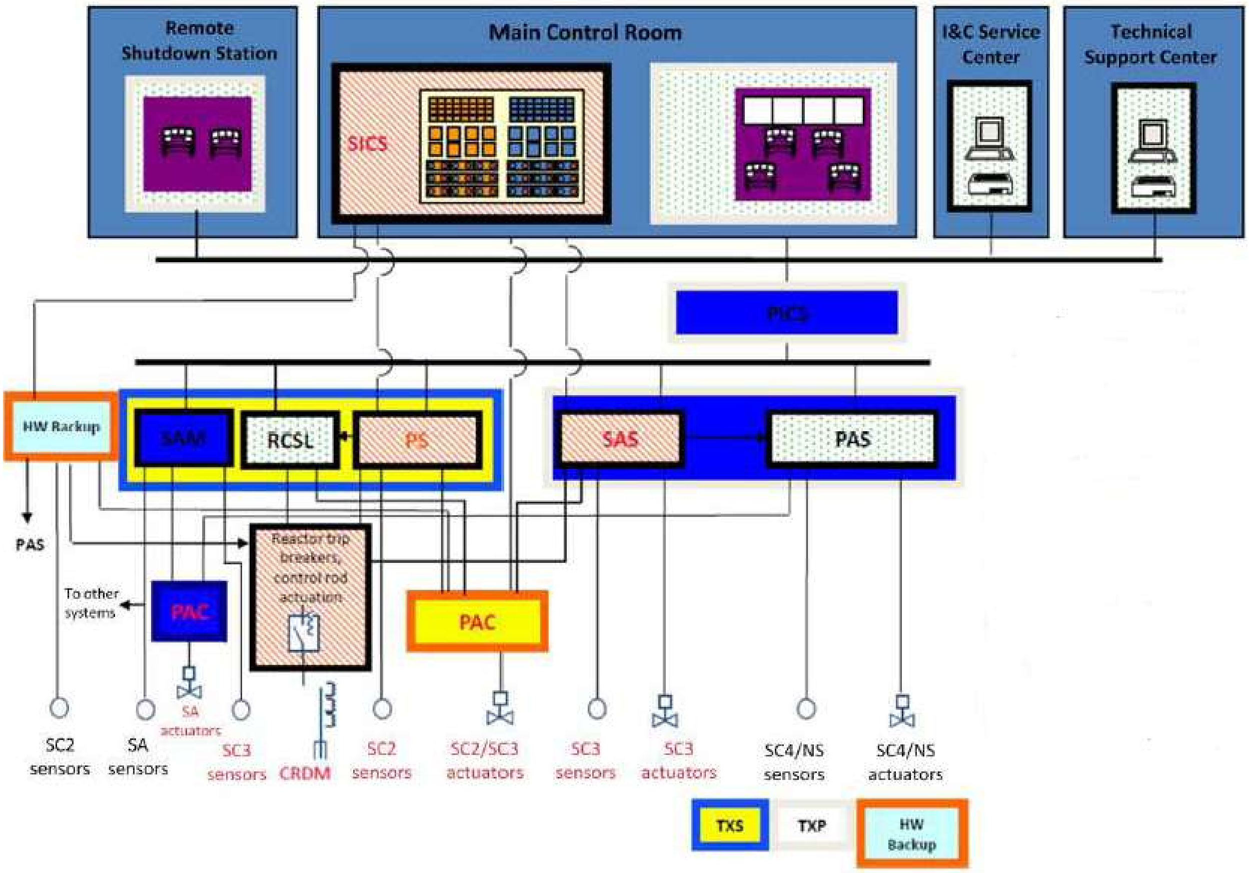


FIG. I–1. A simplified block diagram containing I&C systems and their distribution in the OL-3 design (Reproduced courtesy of Framatome).

Key: SICS = Safety information and control system, PICS = Process information and control system, RCSL = Reactor control, surveillance and limitation system, PACS = Priority actuation control system; PS = protection system, SAS = safety automation system; PAS = Process automation system; CRDM = Control rood drive mechanism, SAM = Severe accident management instrumentation.

I–2. PLACE IN THE I&C ARCHITECTURE

Figure I–1 shows in a simplified way the overall I&C architecture that is implemented in OL-3 EPR design. The figure illustrates which functions are performed by which system, and which technology is used for the implementation of each I&C function. A colour coding of each block represents a specific technology (e.g. TELEPERM XS, SPPA T2000 and hardwired backup) used for data acquisition, signal processing and formation of actuation signals.

Most of the safety classified sensors are shared between several I&C systems via a dedicated signal conditioning modules and signal multipliers (not shown in the figure) which also ensure the decoupling.

Actuators which are shared by several systems such as PS, HBS and SICS are controlled by priority and actuator control modules (assigned to the PACS), managing the priority between the different commands and providing check back and status information of the actuators. Protection system, HBS, RCSL, SICS are interfaced with wired connections for command signals and check backs; with the process / safety automation system, commands and check backs are exchanged via bus connections.

I–3. SAFETY CLASSIFICATION

The classification of OL-3 I&C systems follows the classification approach provided in YVL2.1[6] standard. HBS and SICS are classified in SC3 according to YVL2.1[7]. This corresponds to safety class 2 as defined in IEC 61513.

I–4. DIVERSITY CRITERIA

The OL-3 I&C architecture design has been verified by CCF and diversity analysis.

On the level of the safety classified I&C systems, CCF analyses confirmed that the systems are designed with adequate state-of-the art robustness and resilience to minimize the risk of common cause failures.

On the level of the I&C architecture, the CCF and diversity analysis confirmed that there is an adequate set of diversified functions to mitigate the design basis accidents, considering functional diversity wherever feasible and equipment diversity for the programmable equipment of the protection system and of the hardwired backup system. Equipment diversity has also been credited for the related field instrumentation.

A detailed justification has been produced to establish that the computerized TELEPERM XS equipment of the protection system and the TELEPERM XS equipment used in the HBS are sufficiently diverse respectively sufficiently simple and robust so that coincident systematic failures affecting both systems can be ruled out.

Two types of modules for the electronic priority and actuator control are used, with adequate diversity to ensure the protection against CCF in the PACS level.

I–5. REDUNDANCY

The diverse functions performed by HBS are contained in four redundant divisions, in line with the assignment of redundant actuators to the four divisions. The four divisions are installed in four physically separated I&C rooms, from which two I&C rooms are bunkered.

The I&C rooms of every division accommodate cabinets from all I&C systems, i.e. HBS cabinets are installed together with cabinets of PS, RCSL, SAS etc. including the cabinets for signal conditioning and priority and actuator control assigned to the same division.

The SICS controls and indicators in the panels in the main control are wired to the signal conditioning and actuator control equipment in the I&C rooms, consistent with the assignment of the sensors and actuators to the divisions.

I–6. HUMAN–MACHINE INTERFACE

The process information and control system PICS is the integrated, computerized human–machine interface system for monitoring and control of the plant in all situations. PICS also includes status indications and alarms from the self-monitoring of the hardwired backup system, as needed for maintenance and diagnostics. PICS comprises computerized operator workstations in the main control room, with large set of displays supporting all operator tasks.

[6] Nuclear power plant systems, structures and components and their safety classification, The safety guide of STUK, Finland.

[7] YVL2.1 defines three safety classes applicable for I&C, with Safety Class 2 (SC2) as the highest and SC4 as the lowest safety class.

When the PICS is unavailable, operators will transfer to the panels of the SICS, which allows to bring the plant to safe conditions. The SICS consists of hardwired panels also arranged in the main control room. It comprises analogue indicators and light emission diode (LED) status/alarm indicators driven by signal conditioning and self-monitoring devices. Desk tiles consist of pushbuttons and check back indicators (LED) that are driven by the priority and actuator control.

PS and HBS have their own status displays in PICS. Controls to the PS and HBS are implemented in SICS as hardwired push buttons.

ANNEX II (EPR FLAMANVILLE-3)

DIVERSE FUNCTIONS FOR FLAMANVILLE-3 EPR

II–1. SCOPE AND FUNCTION

In the EPR Flamanville 3 I&C architecture (see Figure II–1), the protection system (PS) provides the reactor automatic protection functions that are necessary to reach the controlled state (see definition in IAEA SSR 2/1) following any design basis initiating event. The safety automation system (SAS) at level 1 'system automation' and the Safety information and control system (SICS) at level 2 'supervision and control' provide the displays and manual commands that are necessary for post-accident operation following any design basis initiating event. They allow transitioning the plant from the controlled state to a safe state. Automatic functions are provided so that no manual actions are necessary in the first 30 minutes following any initiating event.

In the EPR Flamanville 3 I&C architecture, functions are diversely implemented to cope with:

- The postulated CCF of the full reactor protection system (PS);
- The postulated CCF of the full safety automation system (SAS).

CCF of the full SICS is not postulated because it is composed of independent and simple indicators for displays and buttons for commands all based on hardwired technology.

For the postulated CCF of the full PS, the functions diversely implemented cover DBC-2 and frequent DBC-3 events. The setpoints for these functions are set higher than for the PS so that the PS will always act first.

For the postulated CCF of the full SAS, the diverse automatic and manual functions implemented cover DBC-2, DBC-3, DBC-4 and DEC-A events.

II–2. PLACE IN THE I&C ARCHITECTURE

In the EPR Flamanville 3 I&C architecture, the PS is implemented using the TELEPERM XS platform which is computer based. The SAS is implemented using the Siemens SPPA T2000 platform which is also computer based. The SICS is composed of independent and simple indicators for displays and buttons for commands all based on hardwired technology.

As it can be seen on Figure II–1, there is no I&C system that is called diverse actuation system (DAS) in the EPR Flamanville 3 I&C architecture. The diverse functions identified are mainly implemented among I&C systems introduced in the architecture for other primary purposes.

The diverse functions that cope with the postulated CCF of the full PS are implemented in the SAS based on the SPPA T2000 platform.

The diverse functions that cope with the postulated CCF of the full SAS are implemented in the PS supplemented by the Hard kernel system (HKS), both based on the TELEPERM XS platform. The HKS is a small I&C system (5 cabinets) which has been introduced in the architecture specifically to embed diverse functions.

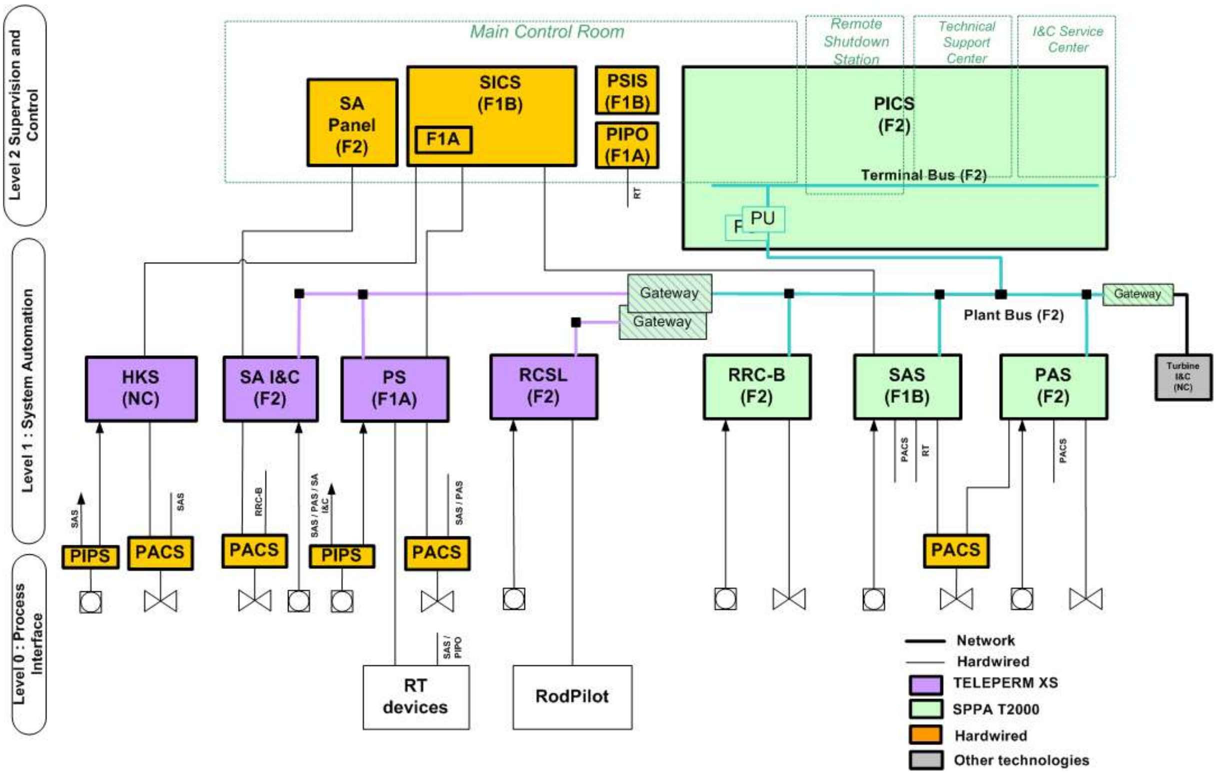


FIG. II–1. I&C architecture for EPR FLAMANVILLE 3 (Reproduced courtesy of Framatom).

Key: HKS = Hard kernel system, PICS = Process information and control system, RCSL = Reactor control, surveillance and limitation system, PS = protection system, SAS = safety automation system; SA Panel = Severe accident panel, SICS = Safety information and control system, PAS = Process automation system; PACS = Priority actuation control system, PIPS = Process instrumentation pre-processing system, RRC-B = Risk reduction category B, SA I&C = Severe accident I&C.

II–3. SAFETY CLASSIFICATION

The diverse functions that cope with the postulated CCF of the full PS are categorized safety category F2 which is equivalent to IEC 61226 safety category C. They are also seismically classified. The SAS which implements these functions is F1B safety classified which is equivalent to IEC 61513 safety class 2. The SAS is also seismically qualified.

The functions diversely implemented to cope with the postulated CCF of the full SAS are partly categorized in the safety category F2 and partly non-safety classified. The PS which implements the first part of these functions is F1A safety classified which is equivalent to IEC 61513 safety class 1. The HKS which implements the second part of these functions is not safety classified.

Indeed, the initial proposal to cope with the postulated CCF of the full SAS was based only on the use of the PS with a scope limited to design base condition category 2 (DBC-2) and frequent DBC-3 events. However, the qualification of the SPPA T2000 platform which was originally built for industrial process control was challenging. To mitigate the risk that the qualification of the SPPA T2000 does not succeed, the scope of the diverse functions was expanded to cover DBC-2, DBC-3, DBC-4 (e.g. loss of coolant accident, rod ejection, main steam line break) and DEC-A events (same events as the SAS) which require the addition of the HKS I&C system.

Later, the qualification of the SPPA T2000 has been completed successfully so the HKS is no longer necessary in the safety justification of the EPR Flamanville 3 and this is the reason why it is not safety classified. The HKS has been kept as an additional system for the robustness of the architecture.

II–4. DIVERSITY CRITERIA

The SAS diversely implements the functions that are necessary to cope with the postulated CCF of the full PS. SAS is implemented using the SPPA T2000 platform which relies on computer based technology. The PS, supplemented by the HKS, diversely implements the functions that cope with the postulated CCF of the full SAS. PS and HKS are implemented using the Teleperm XS platform which relies on computer based technology.

A detailed justification has been produced to establish that the SPPA T2000 platform and the Teleperm XS platform are sufficiently diverse so that the simultaneous CCF of both platforms can be ruled out.

The following types of diversity have been justified for the diversified functions:

- Signal diversity;
- Equipment diversity within a single technology;
- Functional diversity;
- Diversity in development process;
- Logic diversity.

Signal diversity and functional diversity allows coping with the risk of CCF at the level of the sensors and at the level of the actuators without the need to introduce dedicated and diverse sensors or actuators.

CCF of the priority logic used when the same actuators received orders from different I&C systems is not postulated because priority logic is implemented using simple devices all based on hardwired technology (relay based).

II–5. REDUNDANCY

The diverse functions that cope with the postulated CCF of the full PS are implemented using a fourfold redundant structure.

There is no redundancy requirement for the diverse functions that cope with the postulated CCF of the full SAS. Consequently, there is no redundancy in the structure of the HKS and the diverse functions included in the PS are generally not redundant.

II–6. HUMAN–MACHINE INTERFACE

At level 2 ‘supervisory and control’, PS, SAS and HKS are all connected to a single system, the SICS. CCF of the full SICS is not postulated because it is composed of independent and simple indicators for displays and buttons for commands all based on hardwired technology.

SICS indicators for displays and buttons for commands are the same when the plant is operated for post-accident operation using the SAS or the PS+HKS. In case of a CCF in the SAS, a commutator allows to switch SICS indicators and buttons from the SAS to the HKS.

There is consequently no additional human–machine interface for the diversified functions.

The manual reactor trip is implemented in hardwired technology by directly connecting the reactor trip buttons in the main control room to the reactor trip breakers and trip contactors.

ANNEX III (US-APWR)

DIVERSE ACTUATION SYSTEM FOR US-APWR

III–1. SCOPE AND FUNCTION

The diverse actuation systems (DAS) for the US-APWR provides monitoring, control and actuation of safety and non-safety systems required to cope with abnormal plant conditions concurrent with a CCF that disables all functions of the digital protection and safety monitoring system (PSMS) and computer based plant control and monitoring system (PCMS). The DAS includes automatic actuation functions, human system interface (HIS) functions located at the diverse HSI panel (DHP), and interfaces with the PSMS and PCMS. The DAS for the US-APWR design also includes the ATWS mitigation functions. In addition, the DAS in US-APWR is designed to prevent spurious actuations due to postulated earthquakes and postulated fires.

Within the DAS, manual actuation is provided for systems to maintain all critical safety functions. For accident conditions with insufficient time for manual operator action, the DAS provides automatic actuation of the required plant safety functions needed for accident mitigation. Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP located in the MCR.

The DAS for the US-APWR utilizes a hardwired technology (analogue circuits, solid state logic processing devices, relay circuits) that is diverse and independent from the computer based MELTAC® digital I&C platform used for the PSMS and PCMS. Conventional hardwired logic devices and relays for automatic actuation are installed in four diverse automatic actuation cabinets (DAACs) which are located in physically separated Class 1E electrical rooms. DAACs are qualified as Seismic Category II to cope with seismic events.

III–2. PLACE IN THE I&C ARCHITECTURE

The DAS is a separate, dedicated system with interfaces with the safety related process inputs and outputs of the safety logic system (SLS), which are isolated within these safety related systems. In addition, hardwired safety related logic within the SLS (not affected by a CCF) ensures that control commands originating in the DAS or SLS, which correspond to the desired safety function, always have priority. Therefore, there is no adverse interaction of the DAS with safety functions and no erroneous signals resulting from CCF in the SLS that can prevent the safety function.

Detailed functions and architecture of the DAS are designed based on various design bases, for example:

- Selection of postulated initiating events which need to be considered concurrent with CCF;
- Acceptance criteria for plant safety considering CCF;
- Allowable operator action based on operating procedure for CCF;
- Reliability and availability goals to achieve plant design objectives;
- Conformance to various plant abnormal conditions including fire and earthquake.

Integration of the diverse actuation system in the overall I&C architecture of US-APWR is shown in Fig. III–1.

III–3. SAFETY CLASSIFICATION

The DAS is the non-safety diverse instrumentation and control system for the US-APWR. However, as the DAS is a system important to plant safety, it has to meet requirements for an augmented quality assurance program.

III–4. DIVERSITY CRITERIA

The DAS design consists of conventional equipment that is diverse and independent from the MELTAC computer based platform utilized for the PSMS and PCMS, so that a beyond design basis CCF in these digital systems will not impair the DAS functions.

Sensors selected for the DAS input are interfaced from within the PSMS or PCMS input modules. These input modules utilize analogue distribution modules and isolation modules that connect the input signals to the DAS prior to any digital processing. Therefore, a software CCF within the PSMS or PCMS does not affect the DAS automation function or the display of plant parameters on the DHP. The DHP consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms.

The DAS receives inputs from qualified analogue isolation devices located in the reactor protection system (RPS) or directly from plant components. The DAS provides outputs which interface to the SLS power interface modules via qualified isolation devices located in the SLS or directly to plant components. Once actuated, either manually or automatically, the DAS signals are latched at the system level. This ensures all DAS functions actuate to completion. The DAS latches can be reset from the defeat switch located on the operator console. In addition, the DAS hardware for ATWS mitigation functions is diverse from the RT hardware used in the PSMS.

Each DAAC provides for automatic actuation of critical systems, which are required to be actuated within the first 10 minutes of an event. The defence-in-depth and diversity coping analysis provides justification for manual operator actions credited after 10 minutes.

III–5. REDUNDANCY

The DAS design includes internal redundancy to prevent spurious actuation of automatic and manual functions due to a single component failure. Within each DAAC, input signals are compared to their set point values and if the monitored value exceeds its set point, a partial trip/actuation signal is generated. Reactor trip (RT) signals and/or ESF actuation signals are generated from each DAAC through voting logic (2-out-of-4).

The numbers of channels required for each automatic actuation function are based on the following considerations:

- No single failure spuriously actuates the DAS;
- Bypass of a single channel does not cause the DAS automatic function to be inoperable, prevent credited manual actions or prevent monitoring critical safety functions.

The DAS actuation signals from four DAAC subsystems are configured at their destination using a voting logic to execute actuation of RT and ESF systems. The DAS actuation signals are isolated from the PSMS and interfaced to the separate subsystems in each DAAC.

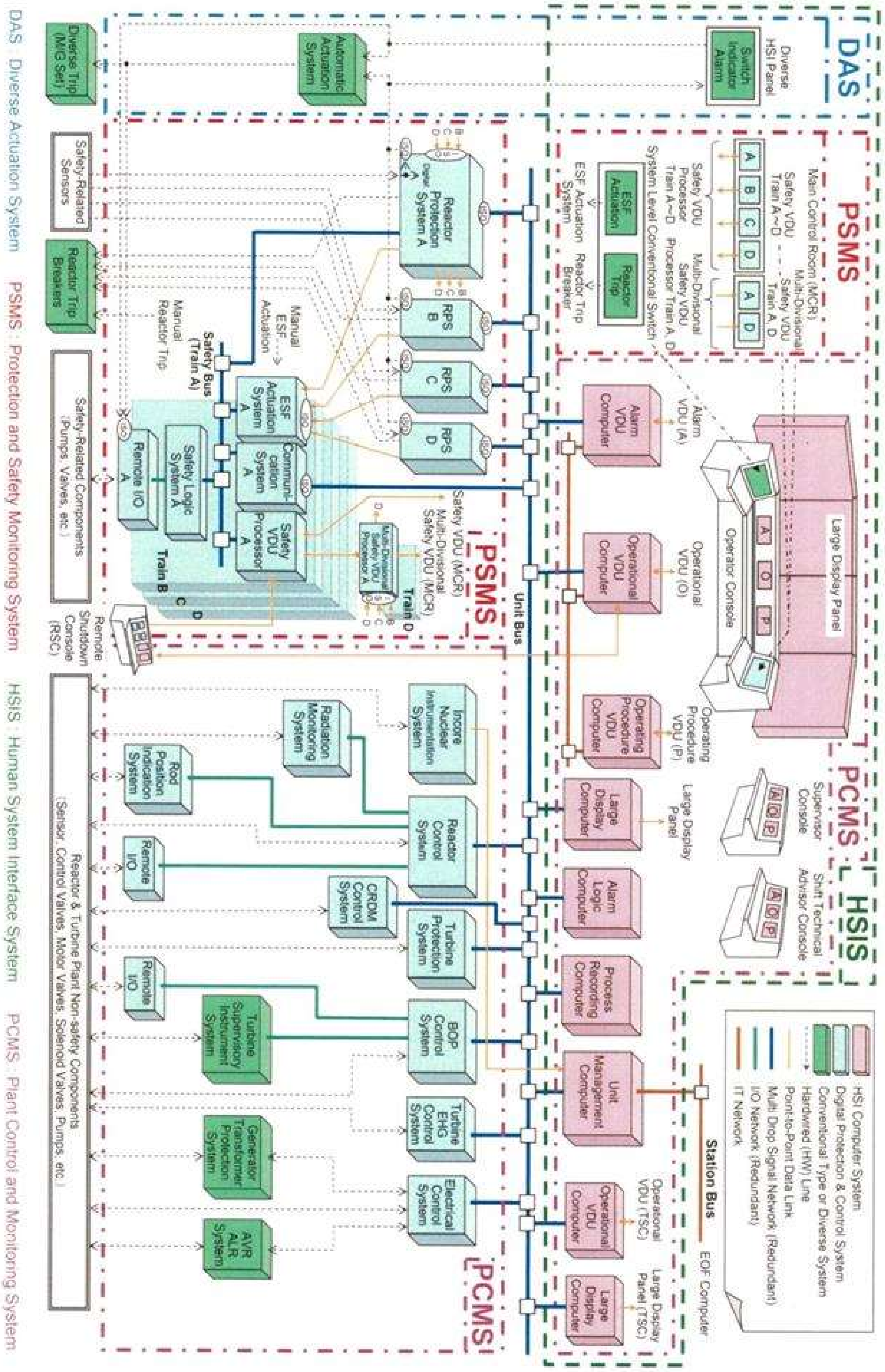
III–6 HUMAN–MACHINE INTERFACE

Key parameter indications, diverse audible and visual alarms, and provisions for manual controls are located in a dedicated independent DHP in the main control room easily accessible by plant operators. The DHP consists of conventional hardwired switches, conventional indicators for key parameters of all critical safety functions, and audible and visual alarms.

The DHP equipment is used for manual control and actuations credited in the defence-in-depth and diversity coping analysis. The actuation status of each safety related system actuated from the DHP can be confirmed by monitoring the safety function process parameters displayed on the DHP. The

DHP is powered by a Class 1E UPS and located in the MCR. Also, the DHP is seismically qualified as Category II.

The inhibition switch can be manually actuated during the plant startup and cooldown operations to prevent actuation of the DAS when it is not needed. This is an administratively controlled operating bypass.



DAS
Diverse HSI Panel
Switch Indicator Alarm
Automatic Actuation System
Diverse Trip (M/G Set)
PSMS
Main Control Room (MCR)
Safety VDU Train A~D
A
B
C
D
Multi-Divisional Safety VDU Train A, D
A
D
Safety VDU Processor Train A~D
Multi-Divisional Safety VDU Processor Train A, D
System Level Conventional Switch
ESF Actuation
Reactor Trip
ESF Actuation System
Reactor Trip Breaker
Reactor Protection System A
RPS B
RPS C
RPS D
Safety-Related Sensors
Reactor Trip Breakers
Manual ESF Actuation
Manual Reactor Trip
Safety Bus (Train A)
ESF Actuation System A
Communication System A
Safety VDU Processor A
Safety Logic System A
Remote I/O A
Train B
C
D
Multi-Divisional Safety VDU Processor A
Train D
Safety VDU (MCR)
Multi-Divisional Safety VDU (MCR)
PSMS
Unit Bus
Safety-Related Components (Pumps, Valves, etc.)
Remote Shutdown Console (RSC)
Alarm VDU Computer
Alarm VDU (A)
Operational VDU Computer
Operational VDU (O)
Operator Console
Large Display Panel
A
O
P
Operating Procedure VDU Computer
Operating Procedure VDU (P)
PCMS
HSIS
Supervisor Console
Shift Technical Advisor Console
Large Display Computer
Large Display Panel
Alarm Logic Computer
Process Recording Computer
Unit Management Computer
Operational VDU Computer
Operational VDU (TSC)
Large Display Computer
Large Display Panel (TSC)
EOF Computer
Station Bus
HSI Computer System
Digital Protection & Control System
Conventional Type or Diverse System
Hardwired (HW) Line
Point-to-Point Data Link
Multi Drop Signal Network (Redundant)
I/O Network (Redundant)
IT Network
Incore Nuclear Instrumentation System
Radiation Monitoring System
Rod Position Indication System
Reactor Control System
Remote I/O
CRDM Control System
Turbine Protection System
Remote I/O
Turbine Supervisory Instrument System
BOP Control System
Turbine EHG Control System
Generator Transformer Protection System
Electrical Control System
AVR ALR System
Reactor & Turbine Plant Non-safety Components (Sensor, Control Valves, Motor Valves, Solenoid Valves, Pumps, etc.)
PCMS
DAS : Diverse Actuation System
PSMS : Protection and Safety Monitoring System
HSIS : Human System Interface System
PCMS : Plant Control and Monitoring System

FIG. III–1. I&C architecture for US-APWR (Reproduced courtesy of Mitsubishi Heavy Industries, Ltd).

REFERENCES TO ANNEX III

[III–1] MITSUBISHI HEAVY INDUSTRIES, Ltd, US-APWR Design Control Document (DCD), Rev. 4, Tokyo (2013).

[III–2] MITSUBISHI HEAVY INDUSTRIES, Ltd, Defence-in-Depth and Diversity, MUAP-07006-NP-A, Rev. 2 (Non-Proprietary), Tokyo (2009).

[III–3] MITSUBISHI HEAVY INDUSTRIES, Ltd, Defence-in-Depth and Diversity Coping Analysis, MUAP-07014-NP, Rev. 5 (Non-Proprietary), Tokyo (2011).

ANNEX IV (US AP-1000)

DIVERSE ACTUATION SYSTEM FOR U.S. AP1000

IV–1. SCOPE AND FUNCTIONS

In the U.S. AP1000 standard design, the diverse actuation system (DAS) is a non-safety related system that provides an alternate means of initiating reactor trip, actuating selected engineered safety features, and providing plant information to the operator. The DAS is included to support the U.S. AP1000 risk goals by reducing the probability of a severe accident which potentially results from the unlikely coincidence of postulated transients and common cause failure (CCF) in the safety related protection and safety monitoring system (PMS). Although the PMS is designed to prevent CCFs, however, in the low probability case where a CCF does occur in the PMS, the DAS provides diverse protection and indication. The specific functions performed by the DAS are selected based on the probabilistic risk assessment (PRA) for the U.S. AP1000.

In the U.S. AP1000 DAS, the automatic actuation function is accomplished by two redundant logic subsystems on a two-out-of-two voting logic basis. Input signals are received from the sensors by an input signal conditioning block, which consists of one or more electronic modules. This block converts the signals to standardized levels, provides a barrier against electromagnetic and radiofrequency interference, and presents the resulting signal to the input signal conversion block. The conversion block continuously performs analogue to digital signal conversions and stores the value for use by the signal processing block. The automatic actuation signals provided by the DAS are generated in a functionally diverse manner from the PMS actuation signals. The CCF of sensors of a similar design is also considered in the selection of these functions.

The signal processing block polls the various input signals, evaluates the input signals against stored setpoints, executes the logic when thresholds are exceeded, and issues actuation commands. The resulting output signals are passed to the output signal conversion block, whose function is to convert logic states to parallel, low-level dc signals. These signals are passed to the output signal conditioning block. This block provides high level signals capable of switching the traditional power plant loads, such as breakers and motor controls. It also provides a barrier against electromagnetic and radiofrequency interferences.

The selection of setpoints and time responses determines that the automatic functions do not actuate unless the PMS has failed to actuate to control plant conditions. Any subsequent return to operation requires deliberate operator action. Capability is provided for testing and calibrating the channels of the DAS.

Actuation interfaces are shared between the DAS and the PMS. The DAS actuation devices are isolated from the PMS actuation devices, so as to avoid adverse interactions between the two systems. The actuation devices of each system are capable of independent operation that is not affected by the operation of the other. The DAS is designed to actuate components only in a manner that initiates the safety function. This type of interface also prevents the failure of an actuation device in one system from propagating a failure into the other system. The DAS and the PMS use independent and separate uninterruptible power supplies.

The U.S. AP1000 DAS is designed to provide protection under all plant operating conditions in which the reactor vessel head is in place and non-Class 1E UPS power is available. The automatic actuation processors, in each of the two redundant automatic subsystems of the DAS, are provided with the capability for channel calibration and testing while the plant is operating. To prevent inadvertent DAS actuations during on-line calibration, testing activities or maintenance, the normal activation function is bypassed. Testing of the DAS is performed on a periodic basis.

IV–2. PLACE IN THE I&C ARCHITECTURE

Figure IV–1 below shows the instrumentation and control (I&C) architecture for the U.S. AP1000 standard design. The non-safety related real time data network, which horizontally divides Figure IV–1 into the upper and lower portions, is a high speed, redundant communications network that links systems of importance to the operator. The lower portion of the figure includes the plant protection, control and monitoring functions. The upper portion of the figure depicts the control rooms and data display and processing system. At the lower right hand side is the safety related protection and safety monitoring system (PMS). Safety related systems are connected to the communications network through gateways and qualified isolation devices so that the safety related functions are not compromised by failures elsewhere. Plant protection, control and monitoring systems feed real time data into the network for use by the control room, the data display and processing system. The PMS performs the reactor trip functions, the engineered safety features (ESF) actuation functions, and the qualified data processing functions. The data display and processing (plant computer) system is implemented in a distributed architecture. The main control room is implemented as a set of compact operator consoles featuring colour graphic displays and soft control input devices. As shown in Figure IV–1, the diverse actuation system is implemented as a stand-alone system with its own dedicated sensors.

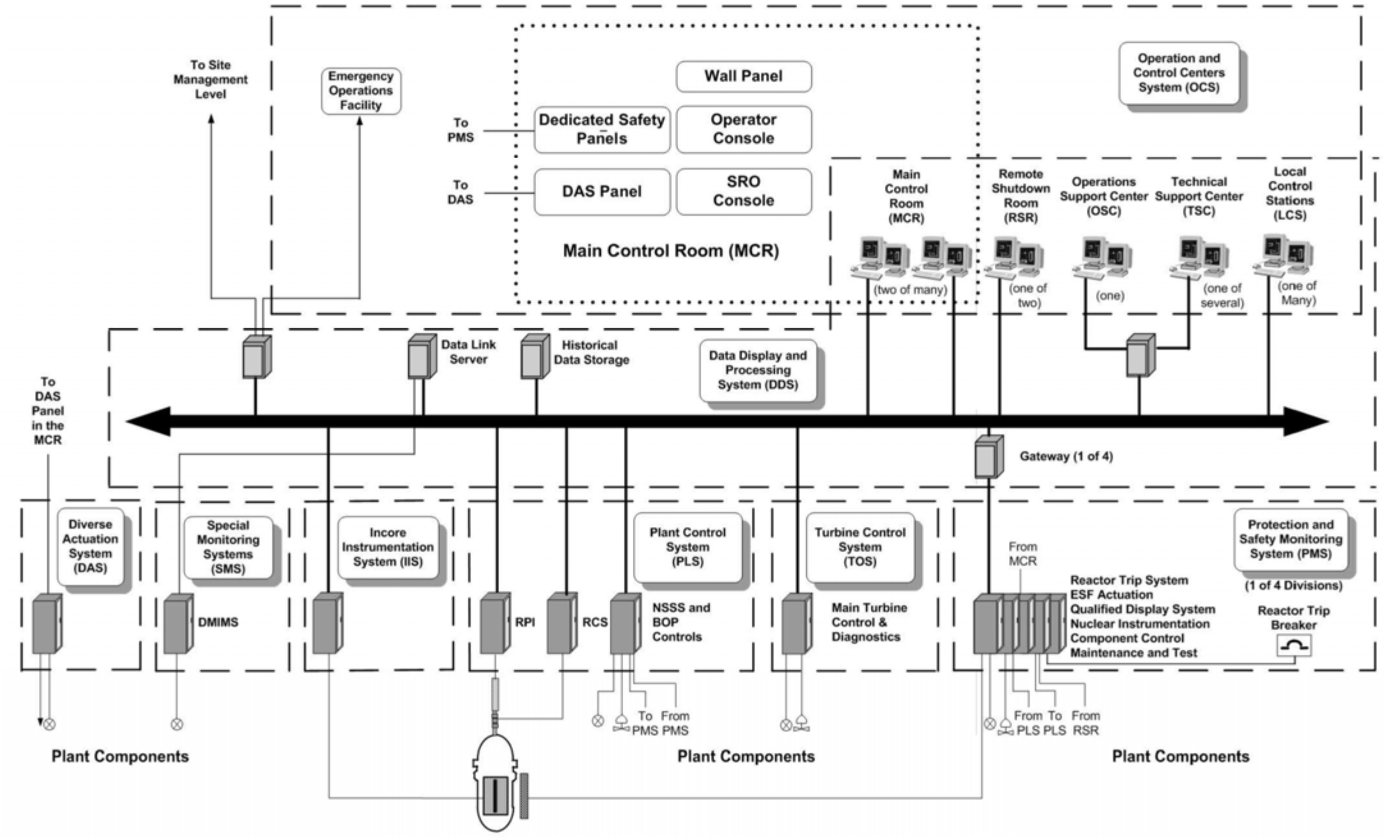


FIG. IV–1. U.S. AP1000 I&C architecture (Open source).

IV–3. SAFETY CLASSIFICATION

The diverse actuation system in the U.S. AP1000 standard design is classified as non-safety related and is implemented as a dedicated diverse system with its own dedicated field sensors to provide a backup means of initiating reactor trip and actuating selected engineered safety features. The DAS also provides plant information to the operators. Because the DAS is an important to safety system in the U.S. AP1000 design although it has non-safety related classification, it has to meet requirements for an augmented quality assurance program in Ref. [IV–1].

IV–4. DIVERSITY CRITERIA

Diversity for the U.S. AP1000 standard design is a principle in instrumentation of sensing different variables, using different technology, using different logic or algorithms, or using different actuation means to provide different ways of responding to postulated plant conditions. U.S. NRC NUREG/CR-6303 in Ref. [IV–2] segregates the types of diversity into six different areas: human, design, software, functional, signal and equipment. These six diversity criteria are used in the design of the DAS for the U.S. AP1000 standard reactor system.

- Design Diversity: The design diversity for the U.S. AP1000 standard design is achieved by utilizing different technology and platform for the DAS and PMS. The DAS is based on a field programmable gate array (FPGA) technology while the PMS uses a microprocessor technology. Because of different technologies and associated architectures, the design is different and diverse between the DAS and the PMS.
- Human Diversity: The human diversity is achieved by assigning people, who are not assigned to the PMS safety system, to be responsible for the design and fabrication of the DAS. The use of independent review is also required and specified in the design, verification, and validation programs for the AP1000 I&C systems and the DAS.
- Software Diversity: The software diversity between the DAS and the PMS is achieved by using different algorithms, logic, program architecture, executable operating system, and executable software/logic.
- Signal Diversity: The signal diversity between the DAS and the PMS is achieved by using dedicated sensors for the DAS, while the signals, which are used to produce reactor trips and engineered safety features (ESF) actuations in the PMS, are from different types of sensors from those used for the DAS.
- Function Diversity: The DAS uses the 2-out-of-2 voting logic for reactor trip and ESF actuation functions while the PMS employs the two-out-of-four voting logic for the reactor trip functions and most ESF actuation functions. The DAS provides a reactor trip function by tripping the non-safety rod drive motor-generator set field breakers, which is diverse from the reactor trip switchgear used for reactor trip functions in the PMS.
- Equipment Diversity: As mentioned in the above design diversity, different technologies are used for the DAS and the PMS, so the equipment for the DAS used to provide the signal input, conditioning and automatic actions is diverse from the equipment used for related functions in the PMS. The DAS displays and signal conditioning equipment are also different from those used for the PMS. The DAS power supplies, controller circuitry and selected peripheral components such as relays are also diverse from those used for the PMS.

IV–5. REDUNDANCY

For the U.S. AP1000 DAS design, there are two actuation logic modes: automatic and manual. The automatic actuation logic mode operates to logically combine the automatic signals from the two redundant automatic subsystems in a two-out-of-two redundant voting logic. The combined signal operates a power switch with an output drive capability that is compatible, in voltage and current capacity, with the requirements of the final actuation devices. The two-out-of-two voting logic is implemented by connecting the outputs in series. The manual actuation mode functions in parallel to independently actuate the final actuation devices. Actuation signals are output to the final field loads in the form of normally de-energized, energize-to-actuate signals. The normally de-energized output state, along with the dual, two-out-of-two redundancy reduces the probability of inadvertent actuation. The DAS is designed so that, once actuated, each mitigation action goes to completion.

The automatic actuation processors, in each of the two redundant automatic subsystems of the DAS, are provided with the capability for channel calibration and testing while the plant is operating. To prevent inadvertent DAS actuations during on-line calibration, testing activities or maintenance, the normal activation function is bypassed. Testing of the DAS is performed on a periodic basis.

IV–6. HUMAN–MACHINE INTERFACE AND MANUAL ACTIONS

In the U.S. AP1000 DAS design, the manual actuation function is implemented by hard-wiring the controls located in the main control room (MCR) directly to the final loads in a way that completely bypasses the normal path through the PMS cabinets, and the DAS automatic logic. In addition, a redundant method is provided at the DAS squib valve control cabinet to (1) open stage 4 automatic depressurization system valves, (2) initiate in-containment refueling water storage tank injection, (3) initiate containment recirculation, and (4) initiate in-containment refueling water storage tank drain to containment.

To support the diverse manual actuations, sensor outputs are displayed in the MCR in a manner that is diverse from the PMS display functions. The instrument sensor output displayed in the MCR is repeated at the DAS instrumentation cabinet.

REFERENCES TO ANNEX IV

[IV–1] NUCLEAR REGULATORY COMMISSION, Quality Assurance Guidance for ATWS Equipment That Is Not Safety Related, Generic Letter 8-06, Washington D.C., (1986).

[IV–2] WESTINGHOUSE, Advanced Passive 1000 (AP1000) Design Control Document (DCD), Rev. 19, June 21, Pittsburg, (2011).

[IV–3] NUCLEAR REGULATORY COMMISSION, Method for Diversity and Defence-in-Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, Washington D.C., (1994).

ANNEX V (ABWR)

AN EXAMPLE OF THE DIVERSE ACTUATION OF ABWR PLANT

V–1. SCOPE AND FUNCTION

The first ABWR plants, Kashiwazaki-Kariwa NPP No.6 and 7 (KK-6/7) of Tokyo Electric Power Company (TEPCO) Holdings, Incorporated, have been in commercial operation for more than 20 years. The instrumentation and control (I&C) system design includes diverse actuation, as does every Japanese ABWR.

This Annex provides an overview of the safety features that are diverse from the RPS (Reactor Protection System) and related mechanisms of Japanese ABWR I&C systems. For ease of understanding, the description does not include the reactor core recirculation flow control system which also enables control of reactivity.

ABWR reactor scram is achieved by Fine Motion Control Rod Drives (FMCRDs). FMCRD has two drive mechanisms of a motor drive and a hydraulic drive. Ordinal control rod withdraw or insertion for reactivity control is performed with the motor drive, however, quick control rod insertion for scram is carried out with the hydraulic drive.

The I&C system for the Japanese ABWR has adopted computer based technology for the Reactor Protection System (RPS) and safety grade systems. This approach is based on the high reliability of this technology experienced for fossil fuel fired plants, nuclear non-safety grade control systems and nuclear subsystems, together with the use of rigorous Verification and Validation (V&V) and engineering methods.

The design does not necessarily require another scram system to detect and protect against CCF of the digital RPS, but a concept similar to that of a diverse actuation system (DAS) has been implemented. Typical ABWR I&C features which are available for diverse shutdown are: ARI (alternate rod insertion), Manual Scram, and SLCS (standby liquid control system: neutron absorption material injection).

Though not required for safety, instrumentation and controls for the ARI provide a means to mitigate the consequences of ATWS events. Upon receipt of an initiation signal (based on either high reactor dome pressure or low reactor water level from the Recirculation Flow Control System), the Rod Control and Information System (RCIS) controls the FMCRD motors such that all operable control rods are driven to their full-in position. This provides a method, diverse from the Hydraulic Control Units, for scramming the reactor.

Basically, manual backup I&C systems are provided with a hardwired technology to cope with any occurrences of unexpected plant emergencies which require plant operator judgement and RPS or ESF initiation. These manual systems and computer based automatic system can individually activate the same safety facilities.

There are many safety backup I&C systems provided such as a High Pressure Core Flooder for core cooling and a Main Steam Isolation Valve for rector isolation. Though these I&C system contribute to cope with CCF, they were not originally provided. Therefore, explanation about them is omitted from this ANNEX V.

V–2. PLACE IN THE I&C ARCHITECTURE

Figure V–1 shows the overall architecture concept for ABWR I&C system. Figure V–2 shows an example of diverse actuation system in ABWR plant.

The basic design of the overall I&C architecture is a hierarchical layer structure: a supervisory plant layer, a system control layer and a plant equipment layer. Four computer based RPS units are designed within the system control layer.

The RPS is a classified safety grade system (PS1/MS1, which is the highest safety classification used in Japan), and is independent of other plant control systems. Each of the divisions is also independent of the other divisions of the RPS. The process signals of the RPS are unidirectionally transmitted to non-safety grade systems via optical data transmission.

V–2.1. Scram detection

Redundant sensor signals are independently transferred to 4 channels of the SSLC (safety system logic control) in which scram status is detected by 2 out of 4 logic. SSLC is an integrated computer based unit name designed for safety system control. Depending on the applied safety function, the mnemonic name is expressed as follows: SSLC-RPS and SSLC-ESF. Each SSLC outputs the scram signal to the hardwired relay circuits with reference to other plant condition signals. The hardwired relay circuit in which the manual scram signal is combined is used for voting the reactor scram initiation.

Two outputs such as A1 and B1 of hardwired relay circuits are respectively assigned to each solenoid of one scram pilot valve to ensure the scram initiation signal. As the scram pilot solenoids are normally energized according to the failsafe design, reactor scram can be executed only when both solenoids of a scram pilot valve are de-energized.

V–2.2. Mechanical diversity

As control rod (CR) drive mechanism is designed to be separated into the CR portion and the motor drive unit, the CR is quickly inserted into the reactor core in the event of a scram. Also the motor drive unit is controlled to move the CR all the way to the full insertion position if CR is not already fully inserted. This behaviour is called Scram follow-In and is controlled by the RCIS (rod control and information system) which is designed as a non-safety grade system.

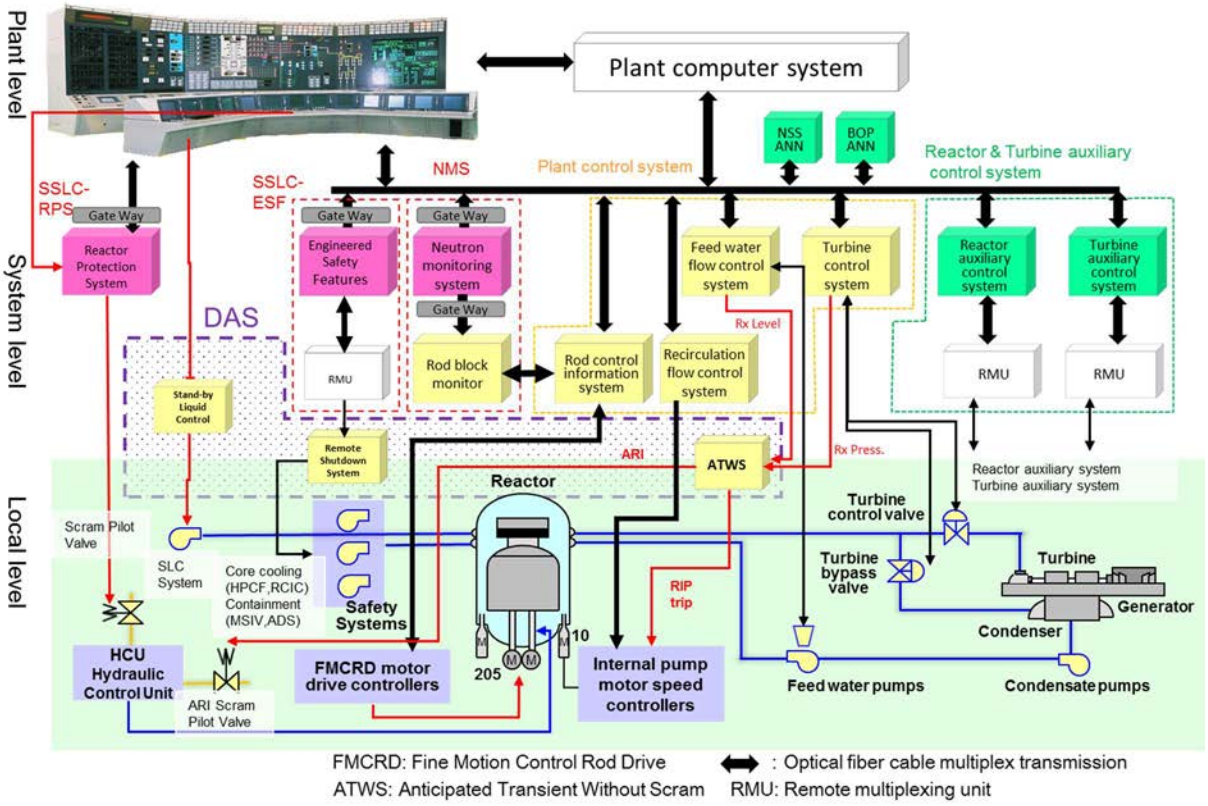
V–2.3. ATWS measures

A further diversity for the reactor scram mechanism is designed and implemented on the ABWR plant as a measure for ATWS.

The ATWS control system determines the occurrence of ATWS by detecting the sensor signals independent of those of the RPSs. To stop the reactivity of the reactor core, the RIPs (recirculation internal pumps) are tripped and the CRs are scrammed by the initiation of ARI scram valves. To realize rapid CR insertion into the reactor core, the ARI scram valves are equipped independently of the scram mechanism and backup scram mechanism. Also, the motor drive is controlled to the full-in position by the RCIS. This motor drive control activated by ARI signal is called Run-In.

V–2.4. Standby liquid control system

The standby liquid control system (SLCS) is designed to stop the reactivity of reactor fuel by injection of neutron flux absorption materials. Hardwired circuit and key controlled manual switch are provided to initiate the SLCS.



Plant level
System level
Local level
Plant computer system
NSS ANN
BOP ANN
Reactor & Turbine auxiliary control system
SSLC-RPS
Gate Way
Reactor Protection System
SSLC-ESF
NMS
Plant control system
Engineered Safety Features
Neutron monitoring system
Feed water flow control system
Turbine control system
Reactor auxiliary control system
Turbine auxiliary control system
DAS
RMU
Rod block monitor
Rod control information system
Recirculation flow control system
Rx Level
Stand-by Liquid Control
Remote Shutdown System
ARI
ATWS
Rx Press.
Reactor auxiliary system
Turbine auxiliary system
Reactor
Scram Pilot Valve
SLC System
Core cooling (HPCF,RCIC)
Containment (MSIV,ADS)
Safety Systems
Turbine control valve
Turbine bypass valve
Turbine
Generator
Condenser
RIP trip
10
205
HCU Hydraulic Control Unit
ARI Scram Pilot Valve
FMCRD motor drive controllers
Internal pump motor speed controllers
Feed water pumps
Condensate pumps
FMCRD: Fine Motion Control Rod Drive
ATWS: Anticipated Transient Without Scram
: Optical fiber cable multiplex transmission
RMU: Remote multiplexing unit

FIG. V–1 An example structure of overall I&C architecture for ABWR plant, Ref. [V–1](Reproduced courtesy of HITACHI-GE).

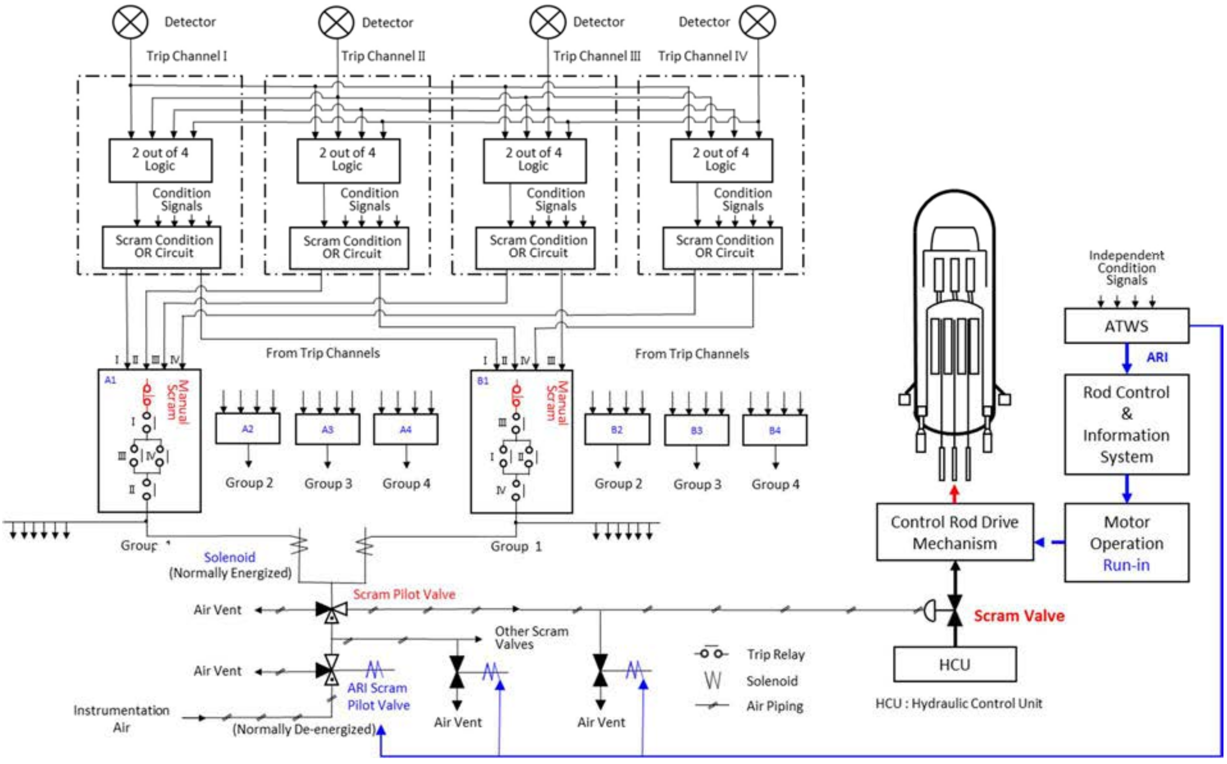


FIG. V–2 An example of diverse actuation system of ABWR Plant, Ref. [V–2]](Reproduced courtesy of HITACHI-GE).

V–3. SAFETY CLASSIFICATION

The safety classification for each feature which is able to be used for diverse actuation depends on the class of the system on which the feature is implemented.

Concerning the potential common cause failure of computer based RPS, Japanese regulation for nuclear power plants requires a computer based RPS to be equipped with backup features which are realized based on another principle or method (see Table V–1). Japanese nuclear regulation also requires the implementation of ATWS measures and SLCS injection features according to the concept of DiD.

TABLE V–1. SAFETY CLASSIFICATION FOR DIVERSE ACTUATION FEATURES

Feature as DAS	Safety classification	Note
Manual scram	Safety	Hardwired system, See FIG. V–2
ATWS	Non-Safety	ATWS: Hardwired system
		RCIS: digital duplex system
		RFCS: digital Triplex system
SLCS	Safety	Hardwired system

V–4. DIVERSITY CRITERIA

The criteria for diversity of computer based RPS (as shown in Table V–2) are: V&V (Verification and Validation) of computer based RPS and ESF are carried out. Other safety features based on different principles are implemented [V–4].

The ABWR I&C system utilizes the diversity of the FMCRD mechanisms (hydraulic drive and motor drive) and also implements diverse I&C systems (ATWS and SLCS).

TABLE V–2. DETECTION AND METHOD OF DIVERSE ACTUATION FEATURES

Diverse Feature	Detection	Action.
Manual scram	Plant operators	To de-energize scram solenoids with hardwired circuit
ATWS	Input signal for activation: 2 out of 3 for reactor pressure (EHC) 2 out of 3 for reactor water level 3 (RFCS Narrow range) 2 out of 4 for reactor water level 2 (ESF Wide range)	To energize ARI solenoids for reactor scram and recirculation pump trip. RCIS controls motor drives of FMCRDs for Run-In according to ARI signal
SLCS	Plant operators	To initiate the SLCS with hardwired circuit

V–5. REDUNDANCY

A hardwired single channel system is applied as it is shown in Table V–3 as follows:

TABLE V–3. REDUNDANCY DESIGN OF DIVERSE FEATURES

Diverse Feature	Redundancy	Note
Manual Scram	Single hardwired system	See FIG. V–2
ATWS	Single hardwired system	Input signals are independent of a scram system
SLCS	Single hardwired system	

V–6. HUMAN–MACHINE INTERFACE

Diverse hardwired manual controls and displays are provided to allow plant operators to act according to their judgement to cope with any plant emergency situation including any CCF of the computer based RPS and ESFs. The displays cover the essential measurements such as reactor level, reactor pressure, isolation valve statuses, etc.

Also, these parameters are displayed on the wide display panel in the main control room to share the plant status. Two push-button channels are provided for manual Reactor scram and ARI scram to protect against single failures, and scram is achieved only when these two channel switches are pushed at the same time. The switch signals are directly hardwired to break the protection relay circuit unit in the same group independently of the automatic protection.

The human–machine interfaces provided for each diverse actuation features it are shown in Table V–4 as follows:

TABLE V–4 HUMAN–MACHINE INTERFACE PROVIDED FOR DIVERSE FEATURES

Feature as DAS	Human-machine interface	Note
Manual Scram	Two manual push buttons (A and B) are installed in the centre of the main console	Simultaneous switching activates reactor scram
ATWS	Two twist release type push buttons (A and B) are installed in the centre of main console. Detection of ATWS status is alerted on the large annunciator ‘ATWS’ on the wide display panel behind the main console. All rod positions are displayed on the full core rods display panel and in the LCD screens	Simultaneous switching activates ARI scram
SLCS	A key release type switch is installed in the left side of main console. The conditions of Injection pump, tank and valves are displayed by lamps	This switch enables the actuation of duplicated systems of SLCS pumps and valves

BIBLIOGRAPHY TO ANNEX V

[V–1] HITACHI-GE, Conceptual figure of overall I&C architecture for ABWR power plant unit, the modified material of Hitachi-GE commercial, nuclear regulation authority (NRA) Japan, (2017).

[V–2] TEPCO, Instrumentation and Control System Appendix VIII, Application to the Reactor Establishment Permission (Construction of Units 6 and 7) of Kashiwazaki-Kariwa Nuclear Power Station, modified by NRA, (2017).

[V–3] NUCLEAR REGULATIONS AUTHORITY, The interpretation for the NRA ordinance on technical standards for commercial power reactors facilities, Japan, (2013).

ANNEX VI (NVNPP-6)

DIVERSE ACTUATION SYSTEM IMPLEMENTED AT RUSSIAN VVER 1200

A diverse actuation system (DAS) described in this Annex was installed, tested and commissioned at Novovoronezh NPP Unit-6 in 2016. This section is reproduced with some modifications based on the permission of Moscow factory ‘FIZPRIBOR’, Ltd.

VI–1. SCOPE AND FUNCTION

The Novovoronezh NPP diverse actuation system is based on a hardwired logic platform (HLP) designed and manufactured by FIZPRIBOR. It provides a diversely implemented protection functions to the reactor protection system, which is based on a computer based platform.

Protection functions are implemented using non-programmable hardware components, i.e. discrete logic chips. HLP hardware is designed to meet the following requirements:

- Testability of technical solutions during the development phase;
- Checkability of hardware during operation;
- Predictability of hardware behaviour in case of failure.

Implementation of protection functions using hard wired technology allows to:

- Exclude software reliability from consideration;
- Exclude the effect of information security aspects on the protection function;
- Perform reliability calculations for the DAS (including for the common cause failures).

VI–2. PLACE IN THE I&C ARCHITECTURE

The regular reactor protection system (RPS) consists of two independent subsets (‘kits’) (Fig. VI–1). Each kit is based on three-channel architecture with 2 out of 3 voting. One RPS kit is sufficient to perform reactor protection. Both RPS kits use identical equipment. Each RPS kit is backed up with the corresponding DAS kit to implement diversity.

A simplified diagram shown in Fig. VI–2 illustrates a generation of protection signal on a temperature measurement circuit. The signal processing is implemented by analogue to digital conversion unit (ADC).

The signal processing is designed to meet the following requirements:

- Input of signal from both the linearized (sensors with unified current output) and the non-linearized (thermocouples, resistance temperature detectors, non-linearizing converters) signal sources;
- Input of signal of different ranges (scales);
- Non-linear signal processing (linearization of signal from thermocouples, resistance temperature detectors, cold-junction compensation, level correction, saturation temperature compensation), signal thresholding;
- Signal filtering for interference elimination, including the 50 / 60 Hz interference;
- Selection of the signal operating range and the type of its non-linear processing (characteristic function) individually for each analogue input during device configuration;
- Analogue signal input accuracy 0.2% of the signal range or better.

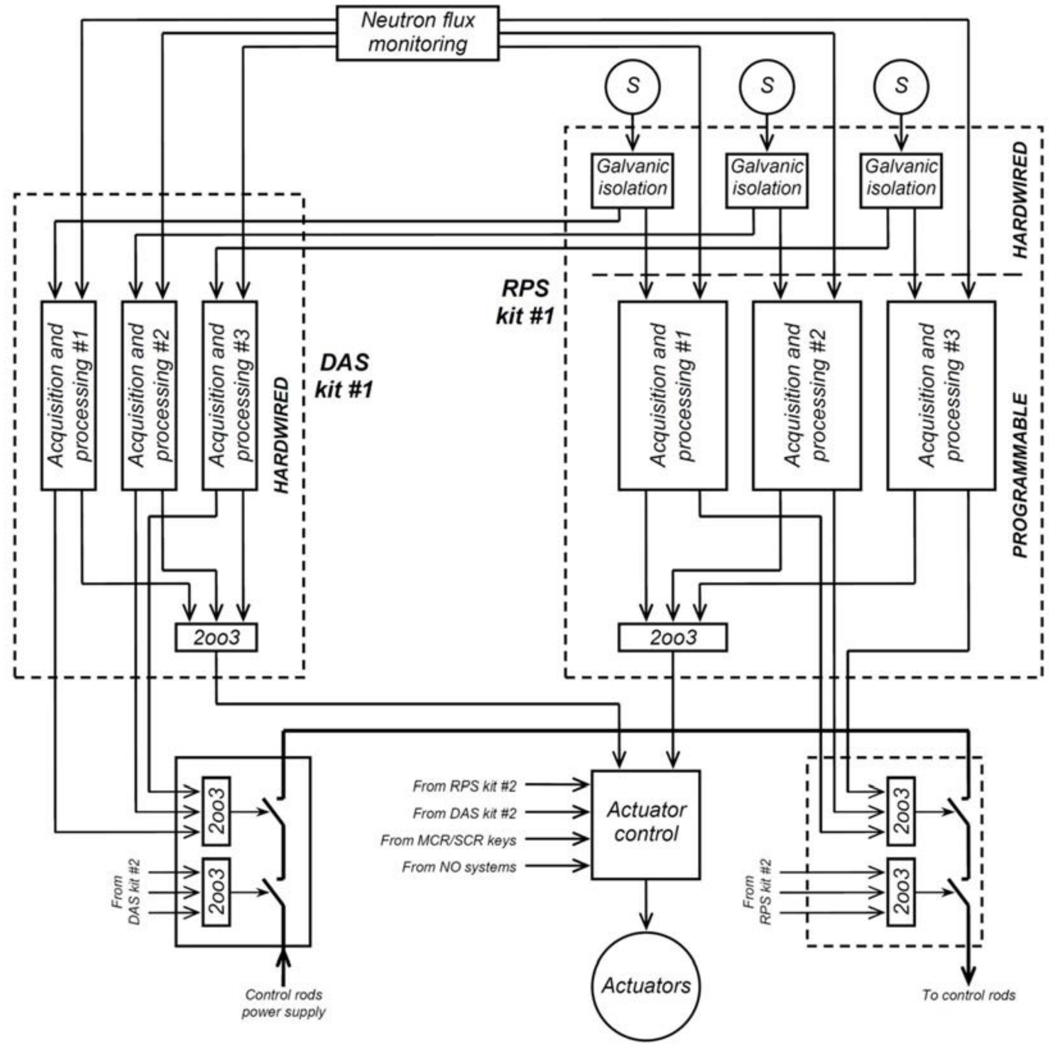


FIG. VI–1. Reactor protection and diverse actuation systems (Reproduced courtesy of FIZPRIBOR)

Key: S = sensors; RPS = reactor protection system; DAS = Diverse actuation system; MCR/SCR = main and supplementary control rooms; NO = normal operation.

The ADC output code is transmitted to the memory chip as an address. The value at the memory chip output uniquely corresponds to each input code i.e. the ADC code. The values stored in memory are the result of non-linear processing of the input signal for each ADC code. During normal operation the memory chip is read only: writing to EEPROM is hardware-locked.

VI–3. SAFETY CLASSIFICATION

According to the main regulatory document for NPPs NP-001-15 (replacement for OPB-88/97) DAS is assigned to the safety class 3 which is roughly equivalent to IEC 61226 safety category B. The highest class for I&C equipment in Russia is class 2.

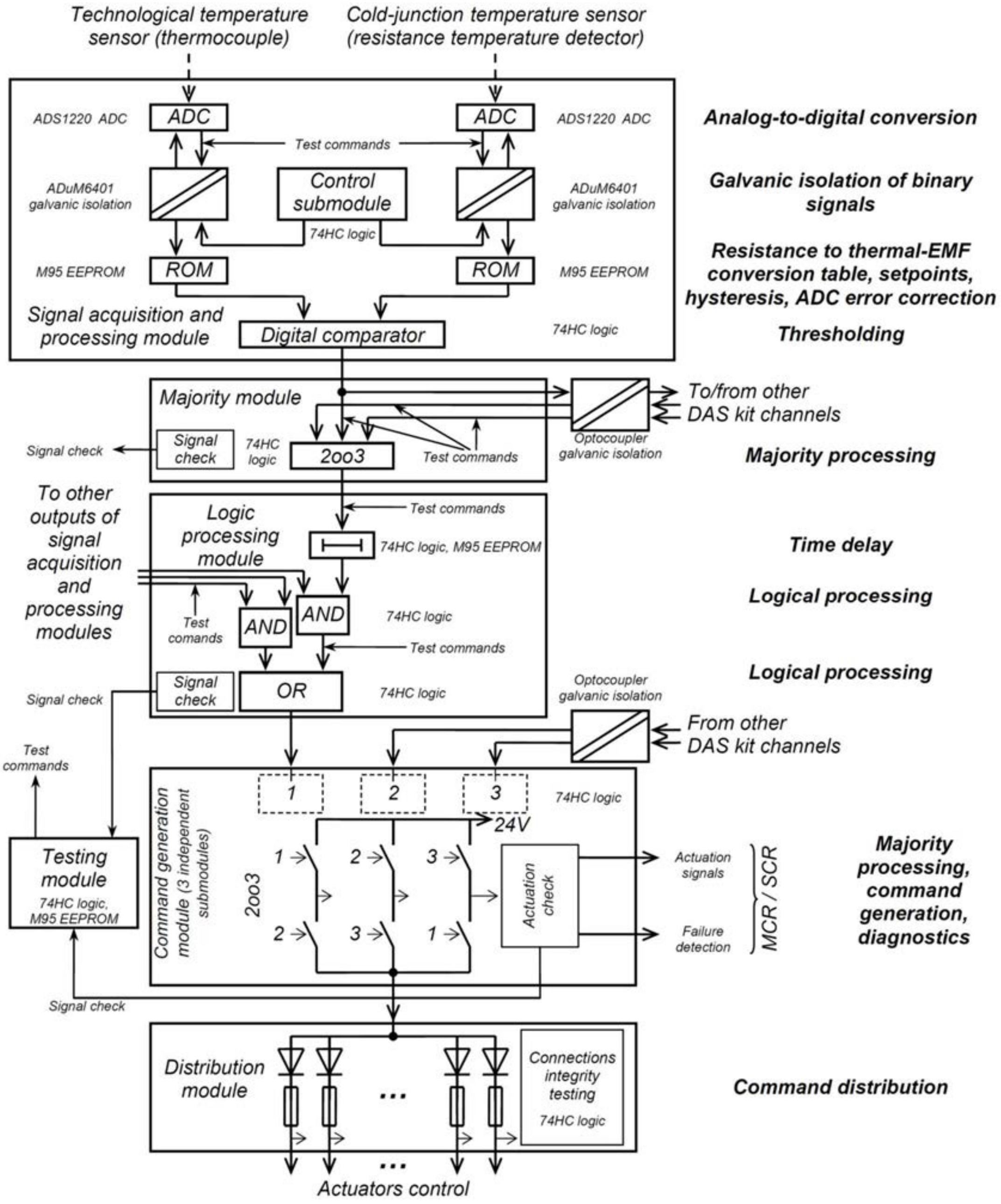

Technological temperature sensor (thermocouple)
Cold-junction temperature sensor (resistance temperature detector)
ADS1220 ADC
ADC
ADC
ADS1220 ADC
Analog-to-digital conversion
Test commands
ADuM6401 galvanic isolation
Control submodule
ADuM6401 galvanic isolation
Galvanic isolation of binary signals
74HC logic
M95 EEPROM
ROM
ROM
M95 EEPROM
Resistance to thermal-EMF conversion table, setpoints, hysteresis, ADC error correction
Signal acquisition and processing module
Digital comparator
74HC logic
Thresholding
Majority module
To/from other DAS kit channels
Signal check
Signal check
74HC logic
2oo3
Test commands
Optocoupler galvanic isolation
Majority processing
To other outputs of signal acquisition and processing modules
Logic processing module
Test commands
74HC logic, M95 EEPROM
Time delay
Logical processing
Test comands
AND
AND
74HC logic
Test commands
Logical processing
Signal check
Signal check
OR
74HC logic
Optocoupler galvanic isolation
From other DAS kit channels
Test commands
1
2
3
74HC logic
24V
Testing module
74HC logic, M95 EEPROM
Command generation module (3 independent submodules)
2oo3
1
2
3
2
3
1
Actuation check
Actuation signals
Failure detection
MCR / SCR
Majority processing, command generation, diagnostics
Signal check
Distribution module
...
Connections integrity testing
74HC logic
Command distribution
...
Actuators control

FIG. VI–2. An example of a block diagram for generating a protection function (Reproduced courtesy of FIZPRIBOR)

Key: - → analogue signals; ⟶ binary signals; ADC = analogue to digital convertor; ROM = read only memory; MCR/SCR = main and supplementary control rooms; NO = normal operation.

VI–4. DIVERSITY CRITERIA

A computer based platform (HLP) used in DAS provides the highest possible equipment diversity comparing to programmable protection systems. HLP hardware related to protection functions is implemented using non-programmable hardware components – discrete logic chips.

The following principles were used when finding circuit solutions and selecting electronic components for the implementation of the protection function:

- The functionality of the module and its parts is sufficient to implement the required function; the device behaviour in case of individual elements failure should be predictable;
- The functionality of the module and its parts is fixed and determined for all external signal values;
- The functionality of the module and its parts is testable via regular interfaces using stand-alone tools (such as oscilloscope) during the development phase and using regular diagnostic tools during operation;
- Cyclically working units are reset to initial state at the beginning of each cycle.

According to the mentioned above principles the use of programmable logic devices (PLDs), including small scale integration PLDs and FPGA was avoided for the following reasons:

- To prepare, load and test PLD firmware a software is used; the absence of critical errors in this software can hardly be confirmed.
- Due to the macro cells redundancy PLD failure can cause not only the loss of individual PLD cells but also the connection of previously unused cells to the circuit (including the memory elements - flip-flops) as well as the generation of previously absent connections. As a result PLD behaviour in case of failure is unpredictable.
- The testing of PLD-based circuit where only inputs and outputs are available is difficult even during the development phase because in the case of a large number of inputs and outputs it gets difficult to test all combinations of input signals. If flip-flops are used as memory elements or counters the testing gets even more difficult, since the current status of outputs depends not only on the current status of inputs but also on their previous statuses.
- PLD configuration is uploaded/downloaded via the service (debug) interface. Validation of the loaded PLD configuration by proofreading does not confirm the operability of PLD macro cells and PLD standard interfaces.

DAS algorithms are also diverse to RPS algorithms.

VI–5. REDUNDANCY

Each DAS subset consists of three redundant acquisition and control channels with 2oo3 command voting (Fig. VI–1). Voting modules for actuator commands are internally redundant (Fig. VI–2). Voting scheme for control rods power removal is implemented externally by wiring 6 solid state relays. Two DAS kits impose additional 1oo2 system redundancy.

VI–6. HUMAN–MACHINE INTERFACE

DAS is completely automatic and has no manual actuation capability. After the actuation DAS is automatically reset when its input signals return to their normal state.

Hardwired signal outputs are implemented to enable the DAS status monitoring at main / supplementary control room (MCR / SCR) panels' indicators.

Redundant programmable networks for data archiving and displaying are also implemented. DAS modules contain microcontroller units (MCU) for data acquisition (Fig. VI–3).

The data from the hardwired logic is transferred to the MCU via protected unidirectional buffers. The hardwired logic and the MCU have separate power supply circuits. This ensures the independence of the hardwired logic from the programmable logic even in case of malfunction.

The information from MCUs is collected by redundant industrial computers (concentrators).

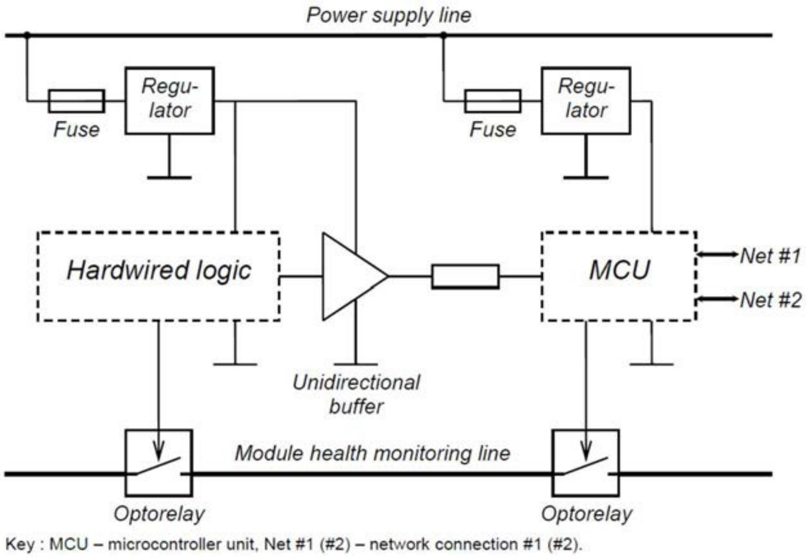


FIG. VI–3. Hardwired / programmable logic independence (Reproduced courtesy of FIZPRIBOR)

ANNEX VII (SIZEWELL B)

DIVERSE ACTUATION SYSTEM IMPLEMENTED AT UK SIZEWELL B

A diverse actuation system as described in this Annex was installed, tested, commissioned and placed into service at the UK Sizewell B NPP since 1995. This section is based on documentation kindly provided by EDF Energy.

VII–1. SCOPE OF FUNCTIONS

The diverse actuation system is termed the Secondary Protection System (SPS) at Sizewell B. The main reactor protection system at the station is termed the Primary Protection System (PPS).

The primary role of the SPS is to provide the following functions in a manner diverse to those functions provided by the PPS:

- Protection against the most frequent design basis initiating faults;
- Actuating signals to the reactor trip switchgear and to the Engineered Safety Features (ESF) equipment as appropriate in response to detected faults;
- Interlock signals to various plant components and manual controls required to reduce the frequency of specified fault sequences; and
- System level manual actuation of ESFs.

VII–2. PLACE IN THE I&C ARCHITECTURE

The Sizewell B Reactor Protection System (RPS) comprises the PPS and SPS, each providing automatic protection from unsafe states arising from faults within the design basis. The systems operate as two diverse and independent protection systems, each with its own set of plant sensors, logic equipment and reactor trip actuation (switchgear for the PPS and reactor trip contactors for the SPS). Each system also actuates the Engineered Safety Features (ESF's) where required, in order to mitigate the fault consequences. The SPS provides claimed protection against all of the frequent (> 10^{-3} pfd) initiating faults in the station fault schedule.

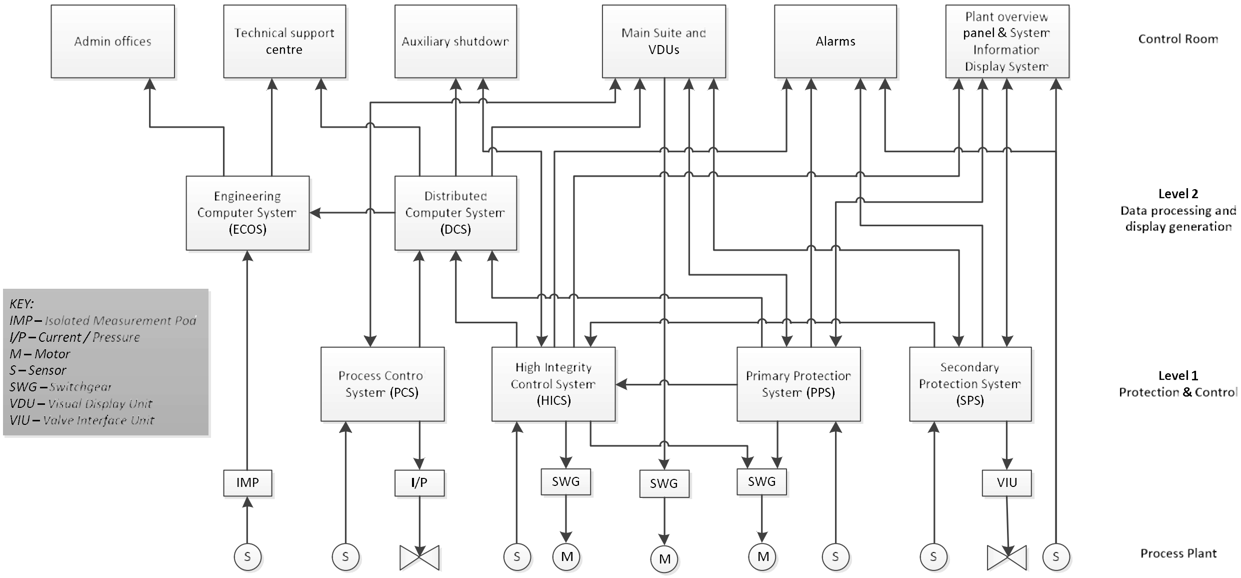

Admin offices
Technical support centre
Auxiliary shutdown
Main Suite and VDUs
Alarms
Plant overview panel & System Information Display System
Control Room
Engineering Computer System (ECOS)
Distributed Computer System (DCS)
Level 2
Data processing and display generation
KEY:
IMP – Isolated Measurement Pod
I/P – Current / Pressure
M – Motor
S – Sensor
SWG – Switchgear
VDU – Visual Display Unit
VIU – Valve Interface Unit
Process Control System (PCS)
High Integrity Control System (HICS)
Primary Protection System (PPS)
Secondary Protection System (SPS)
Level 1
Protection & Control
IMP
I/P
SWG
SWG
SWG
VIU
S
S
S
M
M
M
S
S
S
Process Plant

FIG. VII–1: Sizewell B I&C Architecture [based on Ref. VII-1] (Reproduced courtesy of EDF Energy)

VII–3. SAFETY CLASSIFICATION

The SPS is a high integrity protection system, and was qualified to the highest safety requirements (Category 1), similarly to the PPS.

The overall reliability targets for the RPS (the combined reliability of the PPS and the SPS together) were based on various reliability numerical targets for on-site radiologic dose, off-site radiologic dose, off-site fatalities, etc. as set out in the national regulator's Safety Assessment Principles (www.onr.org.uk). The bounding reliability claim for a SPS nuclear safety function was in the order of $1*10^{-4}$ pfd.

VII–4. DIVERSITY CRITERIA

A range of measures were adopted with the aim of ensuring that the possibility of common cause failure of the PPS and the SPS would be as low as reasonably practicable, including:

- Use of diverse technologies for the PPS and SPS implementation platforms;
- Physical separation of PPS and SPS equipment;
- Different companies selected to supply the PPS and SPS;
- Functional diversity - where PPS and SPS were used to detect the same fault, either different variables or different measurement techniques of the same variable were used, wherever practicable;
- Different essential supply power distribution boards were used to provide electrical power to the PPS and SPS;
- Diverse sensor and actuation device suppliers were used, wherever practicable.

VII–5. REDUNDANCY

- The key design principles and features of the SPS are as follows:
- The SPS is a four train system;
- Each SPS train has two subsystems to perform the functions of initiating reactor trip and actuating ESF plant as follows:
    - SPS Reactor Trip System;
    - SPS ESF Actuation System
- Actuation demands from each SPS train are combined together using two-out-of-four (2oo4) voting logic.

The technology platform used to implement the SPS is based upon simple conventional electronic components, e.g. electronic trip amplifiers, 'laddic' modules (multi-aperture ferrite devices i.e. magnetic logic) for the voting logic and pulse to direct current (DC) converters as power interface devices. This design was chosen to be diverse from the design of the computer based PPS. This equipment had been used in a variety of forms on previous generations of United Kingdom nuclear power plants.

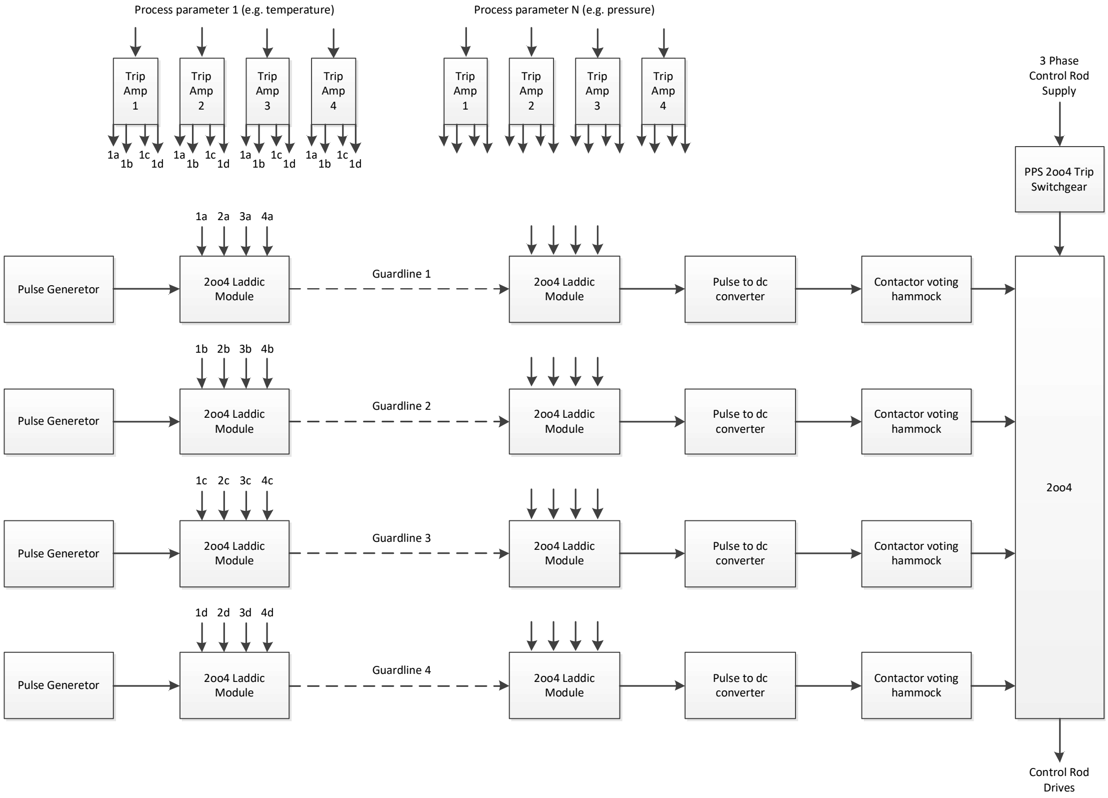


FIG. VII–2: Sizewell B SPS Guardline Arrangement [based on Ref. VII-2], (Reproduced courtesy of EDF Energy).

VII–6. HUMAN–MACHINE INTERFACE

The SPS provides hardwired indications on the MCR overview panel for essential measurements, alarms and SPS status indications.

A limited number of controls are also provided to the operator in the control rooms and are linked to the SPS to provide basic manual functions such as reactor trip, ESFAS actuation and neutron flux range vetoes.

REFERENCES TO ANNEX VII

[VII–1] Description of Sizewell B Nuclear Power Plant, G Meyer & E Stokke, 1997, NKS/RAK-2(97)TR-C4

[VII–2] The engineering specification, design and implementation of the Sizewell B Reactor Secondary Protection System, C Percival & D Bradbury, 1992 International Conference on Electrical and Control Aspects of the Sizewell B PWR

ANNEX VIII (CANDU)

EXAMPLE OF DIVERSE COMPUTERIZED SHUTDOWN SYSTEMS FOR CANDU

VIII–1. SCOPE AND FUNCTION

This section is based on documentation in Ref. [VIII–1], kindly provided by OPG/CEI.

CANada Deuterium Uranium (CANDU) reactors are a form of Pressurized Heavy Water Reactor that were originally designed and built in Canada by Atomic Energy of Canada Limited. The CANDU reactor utilizes heavy water (D_2O) as the moderator inside the reactor core (known as the calandria), as well as for the coolant, which is separate from the moderator. The increased neutron economy due to the use of heavy water provides for the use of natural uranium as the fuel in the CANDU reactors. As of September 2017, there are 31 operating CANDU reactors globally, 19 of which are located in Canada, with the remaining reactors operating in Argentina, China, India, Pakistan, Romania and South Korea.

The Canadian Standards Association (CSA) has published a series of standards (N-standards) that provide an interlinked set of requirements for the management of nuclear facilities and activities. Ref. VIII–2 stipulates requirements for the shutdown systems of nuclear power plants, and is one of the sets of standards that establishes design, procurement, installation, commissioning, operation, testing and maintenance requirements of the shutdown systems. The shutdown systems terminate the fission chain reaction in the event of an accident. Ref. VIII–2 requires that at least two separate, independent and diverse means of shutdown are provided for protection against common cause failures. The standard includes specific requirements for physical separation and functional independence between the two shutdown systems, as well as separation and independence between the shutdown systems and process systems.

Each CANDU reactor is designed with two diverse and independent shutdown systems, Shutdown System Number One (SDS1) and Shutdown System Number Two (SDS2). The shutdown systems (See Fig. VIII–1) are designed to limit radioactive release to the public by shutting down the reactor in the event of an accident. Either shutdown system is capable of shutting down and maintaining the reactor in the shutdown state for all design basis events.

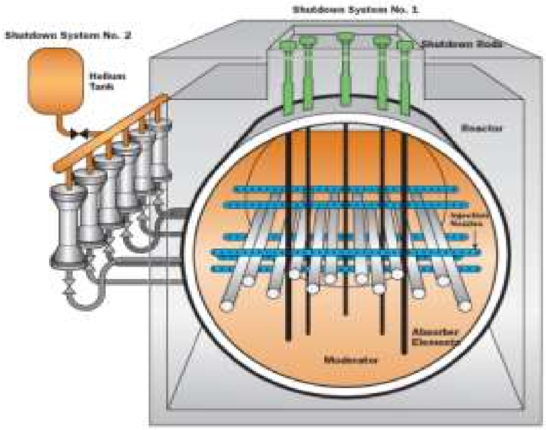


FIG. VIII–1. CANDU Shutdown Systems (Reproduced courtesy of OPG/CEI)

As an example, the Darlington Nuclear Generating Station is a Canadian nuclear power station located 80 km east of Toronto. The Darlington station comprises four CANDU nuclear reactors and has total output of 3,512 $MW_{(e)}$ when all units are on-line. The facility has been in operation since the early 1990s and was the first nuclear plant in the world to implement two fully computerized safety shutdown systems.

The fully computerized reactor shutdown systems provide a number of advantages:

- Replace a large portion of the conventional instrumentation and logic used in the active trip chain for shutdown systems used on previous stations;
- Perform additional functions such as dynamic compensation of the in-core flux detectors;
- Capability to use complex trips (setpoints depend on power level);
- Reduced operator load for testing and calibration;
- Increased safety reliability achieved by early fault detection through monitoring functions;
- Improved ergonomics of the computerized shutdown system also leads to better production reliability through features such as ‘Margin to Trip’ display and annunciation;
- Reduced and de-cluttered panel space in the Main Control Room (MCR);
- Improved storage of setpoints and overall resilience to drift effects compared to conventional analogue comparators.

VIII–2. PLACE IN THE I&C ARCHITECTURE

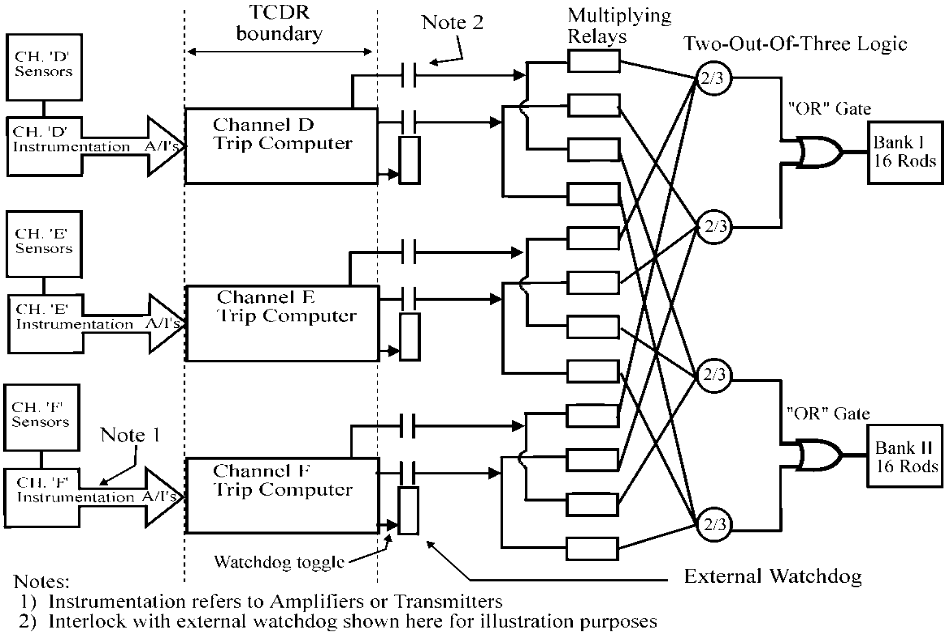
In the CANDU approach to reactor safety, the systems in the plant are categorized as either Process or Special Safety Systems. Process Systems are those required for normal operation, and the Special Safety Systems are those provided to limit any release of radioactivity that may follow failures in the process systems. The Shutdown Systems (SDS1 and SDS2) are two of the four special safety systems designed for the typical CANDU reactor and are independent of the reactor regulating and other process control systems. The other Special Safety Systems are the Emergency Coolant Injection System, and the Containment System.

The special safety systems are separated into two groups, Group 1 and Group 2, to provide protection against common cause events which impair a number of systems or damage a localized area of the plant. Group 1 includes most of the systems required for normal operation of the plant as well as two special safety systems, including SDS1. Group 2 systems may be actuated and monitored remotely to ensure that the required shutdown capabilities are maintained in the event that the Main Control Room (MCR) is damaged or uninhabitable. SDS2 is included in Group 2. The systems in each group are fully capable of performing the essential safety functions of reactor shutdown, decay heat removal, control and monitoring. The systems in each group are designed to be as independent of each other as practical to prevent common cause events from affecting systems in both groups.

Each shutdown system instrumentation and trip decision logic is triplicated and implemented by using three independent channels (D, E, F for SDS1 and G, H, J for SDS2). The three channels for each system have completely independent and physically separated power supplies, trip parameter sensors, instrumentation, Trip Computers and annunciation to mitigate against the impact of a single failure and to support testing and maintenance activities.

The design of SDS1 and SDS2 includes the following major elements: Sensors, Instrumentation (including amplifiers and transmitters), Trip Computer, Multiplying Relays and Two-Out-Of-Three decision mechanism. Figure VIII–2 shows the major elements of SDS1 and the three-channel arrangement. The Trip Computer Design Requirements defines the boundary of the channelized Trip Computers.

Each channelized Trip Computer is housed in separate instrument cabinet in order to satisfy the channel separation requirements. Racks containing channelized equipment are separated by a minimum distance of 1 m.



Notes:
1) Instrumentation refers to Amplifiers or Transmitters
2) Interlock with external watchdog shown here for illustration purposes

FIG. VIII–2. SDS1 General Block Diagram (Reproduced courtesy of OPG/CEI)

VIII–3. SAFETY CLASSIFICATION

Both SDS1 and SDS2 are designated as special safety systems and the trip functions are categorized as Category A functions and implemented using Class 1 systems.

VIII–4. REDUNDANCY AND RELIABILITY

Shutdown systems have a reliability target greater than 99.9% (i.e., unavailability requirement of less than 10^{-3} years per year for each system and 10^{-6} total for both shutdown systems). This is achieved by applying governing quality assurance through all phases of the life of the shutdown system, especially during the design phase. Shutdown system reliability is demonstrated by the use of computer-aided Safety Related System Tests (SRSTs). The SRSTs are performed at regular, predefined intervals based on the unavailability target for the system.

Trip Computer software is demonstrated to be reliable by strict compliance to the Safety Critical Software Engineering Standard, Ref. VIII–3] that is based on the original version of Ref. VIII–4 and has been kept up to date with improvements made to the standard. The Safety Critical Software Engineering Standard describes an integrated engineering approach for designing safety critical software. This includes systematic requirements specification and verification using mathematical functions, Hazards Analysis and Reliability Qualification. The cumulative effect of the software engineering tasks ensures that the software meets the highest degree of quality, robustness and reliability.

VIII–5. DIVERSITY CRITERIA

The two shutdown systems are of diverse designs to prevent common mode design errors (including CCF due to latent software design errors) and hardware failures from disabling both shutdown systems. The following table provides a summary of the diverse elements present in the design of CANDU shutdown systems. The diversity elements implemented in the CANDU design methodology can be logically grouped into Functional and Design diversity type. The diverse elements and corresponding methods are further described in more detail in the Table VIII–1 and in the following sections .

TABLE VIII–1. THE DIVERSE ELEMENTS AND CORRESPONDING DIVERSITY METHODS

Type	Diverse element	Method
Functional	Shutdown mechanism (VIII–5.1)	– Shutoff rods for SDS1 and poison injection for SDS2.
	Trip Parameters (VIII–5.2)	– Independent Trip Parameters
Design	Signal (VIII–5.3)	– Physically separate set of sensors monitored; – In-core flux detectors supplied by different manufacturers
	Actuation (VIII–5.4)	– Trip logic differences between SDS1 and SDS2
	Equipment (VIII–5.5)	– Different manufacturers are used for the Trip Computers; – Diverse processors and Trip Computer system architecture; – Diverse programming languages used to implement trip logic
	Design Process (VIII–5.6)	– Different approaches for software implementation; – System-specific development and verification procedures and design standards
	Design Teams (VIII–5.7)	– Independent development, verification and validation teams for SDS1 and for SDS2

VIII–5.1. Shutdown mechanism

Functional independence of the two shutdown systems is achieved by the adoption of two different shutdown mechanisms. SDS1 employs neutron absorbing 'shutoff' rods, made of elements such as cadmium. SDS2 trips the reactor by injecting a liquid poison solution (such as gadolinium nitrate) into the moderator from the side of the reactor core. In the more recent, CANDU6 design, the 2-out-of-3 voting logic for SDS1 is implemented using hardwired relay logic, while the 2-out-of-3 voting for SDS2 is performed by the poison injection valve logic.

VIII–5.2. Trip parameters

In the CANDU design, each shutdown system monitors a set of trip parameters that provides complete trip coverage for postulated initiating events requiring action by the shutdown system. Trip coverage is provided for each initiating event by two or more trip parameters, with one trip parameter being considered the primary and the other trip parameters considered secondary. The complete set of trip parameters (including both primary and secondary parameters) is monitored by each shutdown system and as a result each shutdown system is capable of independently initiating a reactor trip if an event is detected.

VIII–5.3. Signal

Each shutdown system relies on independent input signal instrumentation (including taps/tubing and transmitters and amplifiers). The In-core flux detectors for SDS1 and SDS2 are supplied by different manufacturers and have different performance characteristics. The SDS1 detectors are over-prompt, while the SDS2 detectors are under-prompt.

The in-core detectors for SDS1 are mounted vertically from the top of the reactor and the SDS1 ion chambers are mounted horizontally from the side of the reactor. The ion chambers and in-core detectors for SDS2 are horizontally mounted from the same side of the reactor as the poison injection nozzles. This arrangement ensures spatial separation between the SDS1 and SDS2 components that are mounted on the reactor.

VIII–5.4. Actuation

The trip voting logic for SDS1 is characterized as ‘general coincidence’ since any parameter beyond its trip limit will place the SDS1 channel in a ‘tripped’ state for the purpose of two-out-of-three voting to release the shutoff rods into the reactor core. The trip voting logic for SDS2 is characterized as ‘local coincidence’ since the same parameter must be beyond its trip limit on at least two of three SDS2 channels to release the gadolinium nitrate ‘poison’ into the reactor core.

Because of the diverse shutdown methods used, output actuation devices for the two shutdown systems are also diverse. SDS1 shut off rods are held at the top of the reactor core by mechanical clutches which are inserted into the reactor core via gravity and spring force. SDS2 output devices shutdown the reactor by opening fast-acting air activated valves that use helium to inject liquid poison into the reactor core.

VIII–5.5. Equipment

Within the constraints of equal quality and reliability, similar components in the two systems are supplied by different manufacturers, including diverse computer system architecture and CPUs used.

For example, in CANDU6 design, SDS1 Trip Computer platform is a safety certified PLC, while the SDS2 Trip Computer platform is an industrial computer that does not use an operating system. The Trip Computer logic is also implemented by using diverse programming languages, such as a graphical programming language for one system and a procedural language for the other.

VIII–5.6. Design process

While the design processes for both systems meet the Safety Critical Software Engineering Standard, CE-1001-STD, different approaches for software implementation exist for the two computerized shutdown systems, supported by system-specific development and verification procedures and design standards. Key attributes of each development process include systematic software design and code verification, hazards analysis and reliability qualification testing. Reliability qualification testing is performed at the end of the development process and provides additional confidence of the quality of the safety critical software.

VIII–5.7. Design Teams

Software Engineering team diversity is preserved consistent with requirements in the Safety Critical Software Engineering Standard, Ref. VIII–2. Independent development, verification and validation teams for SDS1 and for SDS2 are in place. For each system, independence of design and verification or validation personnel is maintained to the extent required to help ensure an unbiased verification and validation process.

VIII–6. HUMAN–MACHINE INTERFACE

For SDS1 and SDS2, a set of four manual channel trip pushbuttons which are independent of software are located in the MCR panels. The first three pushbuttons are channelized to allow the operator to place a single channel in a safe (tripped) state during maintenance. Manually tripping two or more channels will cause the two-out-of-three relay voting logic to trip the reactor. A fourth push-button is mechanically connected to the other three pushbuttons such that pushing the fourth button has the same effect of tripping all three channels at once.

To achieve high performance reliability, the SDS1 and SDS2 Trip Computers are designed to be as simple as possible and to implement only the functions necessary to support reactor shutdown. Other more complex functions such as the display of shutdown parameters in the Main Control Room and Safety Related System Tests (SRST) are implemented by the Display/Test Computers and Monitor Computer subsystems. The Display/Test and Monitor Computer systems implement the Shutdown System Human–Machine Interface (HMI) functions.

The HMI equipment comprises the MCR and Unit Secondary Control Area (USCA) panels, a unit operator's console and various window annunciations and computerized alarms. Figure VIII–3 shows the SDS1 and SDS2 operator interface in the MCR.

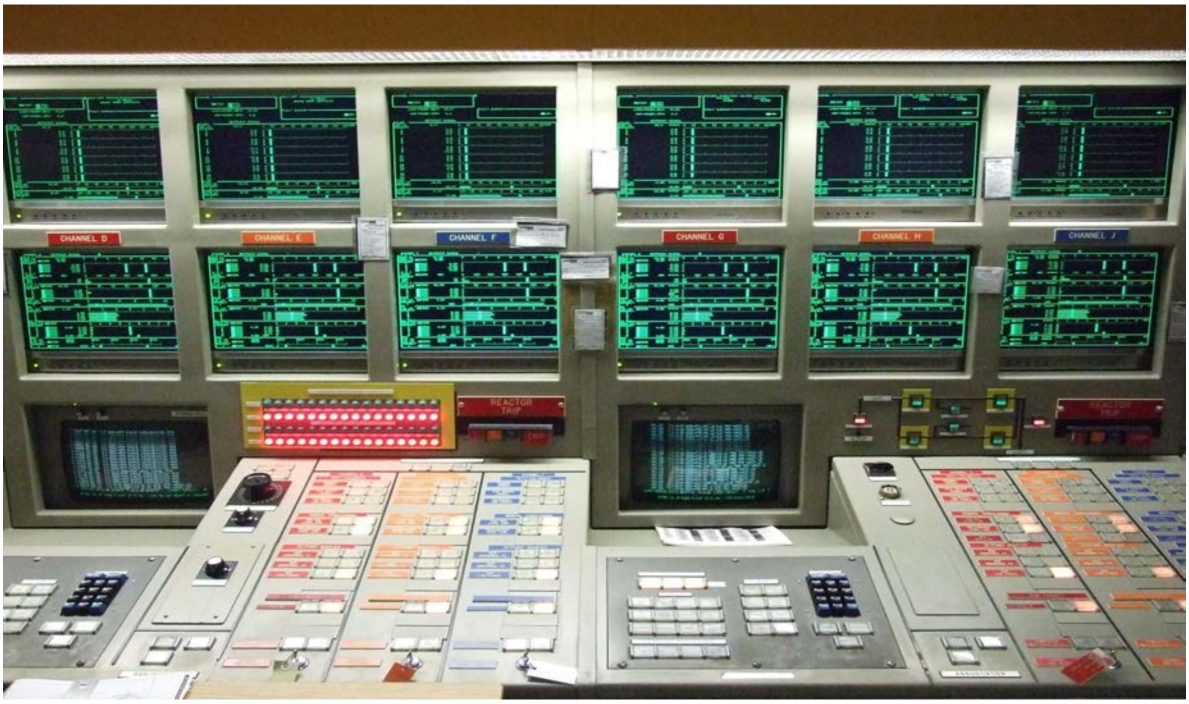


FIG. VIII–3. Shutdown System User Interface in Main Control Room (Reproduced courtesy of OPG/CEI)

REFERENCES TO ANNEX VIII

[VIII–1] DARLINGTON NUCLEAR GENERATING STATION, Digital Computer Control Systems and Shutdown Systems – A Design Engineer's Notebook, Safety Control Systems Conference 2008 – IDC Technologies, Henry Kernius and Paul Woo, Canada (2008).

[VIII–2] CANADIAN STANDARDS ASSOCIATION, Requirements for the Shutdown Systems of Canada Nuclear Power Plants, CSA N290.1, Canada (2013).

[VIII–3] CANDU COMPUTER SYSTEMS ENGINEERING CENTRE OF EXCELLENCE, Standard for Software Engineering of Safety Critical Software, CE-1001-STD, Canada (1999).

[VIII–4] INTERNATIONAL ELECTROTECNICAL COMMISSION, Nuclear power plants - Instrumentation and control systems important to safety - Software aspects for computer-based systems performing category A functions, IEC 60880 STD. Geneva (1986).

ANNEX IX (APR1400)

DIVERSE ACTUATION SYSTEM FOR APR1400

IX–1. SCOPE AND FUNCTION

In APR1400 design, diverse actuation system (DAS) is designed to mitigate the effects of potential CCF of computer based safety I&C systems including the plant protection system (PPS) and engineered safety features-component control system (ESF-CCS). The DAS consists of the diverse protection system (DPS), the diverse manual engineered safety features (ESF) actuation (DMA) switches, and the diverse indication system (DIS). The DAS design provides sufficient diversity and defence-in-depth to tolerate the following beyond design basis events:

- ATWS, which is defined as an AOO followed by failure of the reactor trip portion of the PPS;
- An AOO or a postulated accident (PA) concurrent with a software CCF that prevents the safety I&C systems from performing their required functions.

A reactor trip, turbine trip, auxiliary feedwater actuation and safety injection actuation functions are included in the DPS. The DPS reactor trip provides a simple and diverse mechanism to decrease the risk from the ATWS events and mitigates the effects of a postulated software CCF of the computer based computer logic within the PPS and ESF-CCS, concurrent with a steam line break inside containment. The DPS turbine trip is automatically initiated whenever the DPS reactor trip conditions are met. The DPS auxiliary feedwater system actuation provides additional reasonable assurance that an ATWS event could be mitigated if it occurred. The DPS safety injection system actuation assists the mitigation of the effects of a large break loss of coolant accident event with a concurrent software CCF within the PPS and ESF-CCS. The DPS automatic trip/actuation setpoints are specified to provide reasonable assurance that the PPS initiates an automatic trip/actuation signal prior to the DPS if a postulated software CCF has not degraded the PPS.

The DMA switches permit the operator to manually actuate ESF systems from the main control room (MCR) after a postulated CCF of the PPS and ESF-CCS. The DMA switches provide the safety injection system signal, main steam isolation signal, containment isolation actuation signal, containment spray actuation signal, auxiliary feedwater system actuation signal. The DMA switches are hardwired to the component interface module through the isolation devices and are independent and diverse from the safety system.

The DIS provides functions to monitor critical variables following a postulated software CCF of safety I&C systems. The displayed parameters are selected on the following bases:

- A subset of the accident monitoring instrumentation parameters;
- The inadequate core cooling monitoring parameters;
- A subset of the parameters needed for the operator to place and maintain the plant in a safe shutdown condition.

IX –2. PLACE IN THE I&C ARCHITECTURE

The APR1400 I&C systems consist of the safety protection and safety monitoring systems, non-safety control & monitoring system, diverse actuation systems and human–machine interfaces in the MCR and remote shutdown room as shown in Fig. IX–1. The safety I&C systems are implemented on programmable logic controllers (PLCs) and there are also a limited number of hardware switches to meet the safety system design criteria in Ref. [IX–1]. Major functions of control, alarm and indication of the non-safety I&C systems are implemented on a distributed control system (DCS) based common platform. The DCS supports component level control, automatic process control and high level group control. The DCS is designed in a redundant and fault-tolerant architecture to achieve high reliability such that a failure of a single component does not cause a spurious plant trip. The non-safety systems implemented in the DCS are the information processing system (IPS), power control system, and process–component control system (P-CCS) including nuclear steam supply system process control system.

The DPS and DIS are implemented on a FPGA-based logic controller (FLC), which is diverse from the common safety PLC platform. The DIS display is implemented on a non-safety flat panel display (FPD) that is independent from the IPS and diverse from the common safety PLC platform. The DMA switches are implemented by conventional switches, connected to the lowest level of component control.

For the defence against a postulated CCF in the protection system platform, the following major defence echelons are designed into the APR1400 I&C systems:

- Control and monitoring systems;
- PPS and ESF-CCS;
- Diverse actuation system (DPS, DIS and DMA switches).

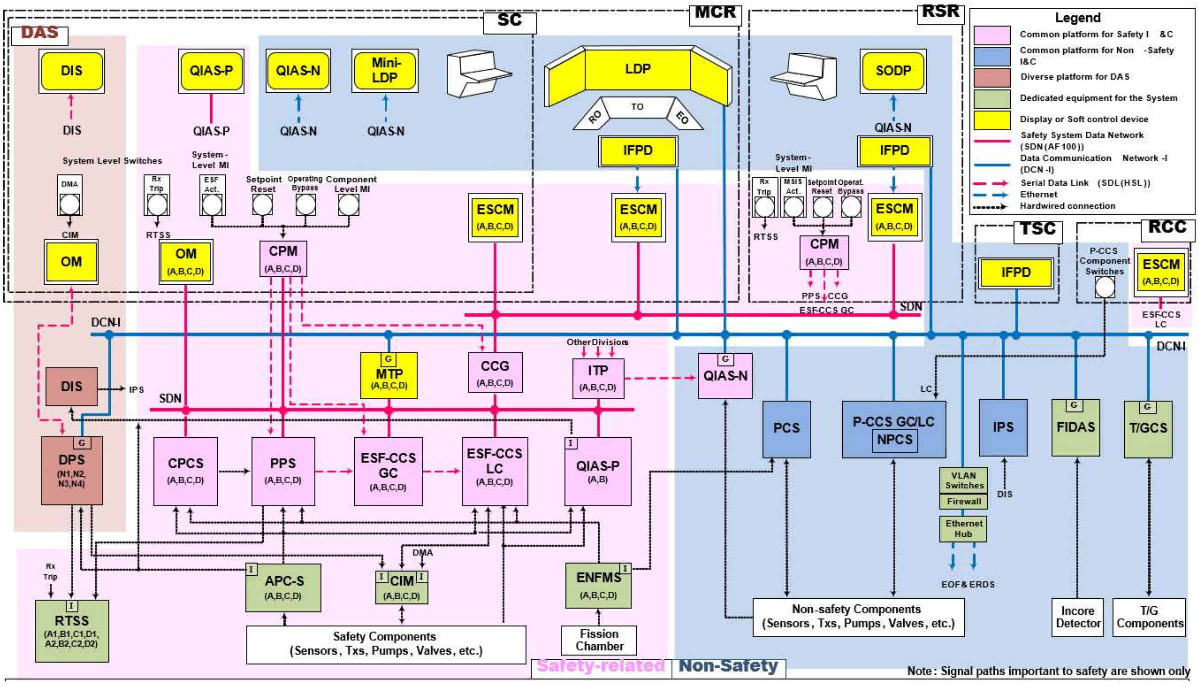


FIG. IX–1. An example of APR1400 I&C system architecture (Reproduced courtesy of KHNP)

IX –3. SAFETY CLASSIFICATION

The DPS is the non-safety system designed with augmented quality, as defined by U.S. NRC Generic Letter 85-06. The configuration of FPGA associated with the DPS is designed as important to safety (ITS), as described in the Software Program Manual of APR1400.

The DMA switches provide the non-safety functions. The DMA switches are designed with Class 1E qualified hardware and are seismically qualified. The DMA switches are energized using Class 1E power.

The DIS is the non-safety system designed with augmented quality. The software associated with the DIS is identified as ITS as described in the Software Program Manual of the APR1400.

IX –4. DIVERSITY CRITERIA

The APR1400 DAS has sufficient diversity features using the guidelines in Ref. [IX–2]. The analysis results of diversity attributes of DPS are as follows:

Design Diversity – Diverse equipment platform based on different technology is applied to the DPS compared with the PPS. The PPS uses the PLC technology for the digital logic processing, whereas the DPS uses the FPGA logic controllers (FLC) technology for the digital logic processing. In addition, system architectures are diverse between the PPS and the DPS. Therefore, design diversity is provided between the PPS and the DPS.

Functional diversity – The reactor trip mechanism of the DPS is diverse from that of the PPS. The PPS use the under voltage trip mechanism, whereas the DPS use the shunt trip mechanism. Therefore, functional diversity is provided between the PPS and the DPS.

Signal diversity – There is no signal diversity between the PPS and the DPS. The safety class sensors and the auxiliary process cabinet-safety (APC-S) are shared by both the PPS and the DPS. The sensors and APC-S are analogue equipment. Therefore, the sensor equipment is not affected by the software CCF.

Software diversity – The PPS uses the software for PLC for the digital logic processing, whereas the DPS uses the hardware description language (HDL) for the FLC. Therefore, software diversity is provided between the PPS and the DPS.

Equipment diversity – The diverse equipment platform from different manufacturer is applied to the DPS compared with the PPS. The PPS uses the PLC platform for the digital logic processing, whereas the DPS uses the FLC platform. Therefore, equipment diversity is provided between the PPS and the DPS.

Human diversity – The DPS is designed and tested by different engineers of different design and test team from the PPS design and test team. Therefore, human diversity is provided between the PPS and the DPS.

IX –5. REDUNDANCY

The DPS is composed of four channels with one cabinet per channel, and each DPS cabinet is located in a separate room. The DPS is implemented with a 2-out-of-4 voting logic to ensure a single failure within the DPS does not (a) cause a spurious actuation, and (b) preclude an actuation. Each DPS channel can be tested manually without causing component actuation during plant operations.

The DIS is a single channel of non-safety equipment to meet the requirements of Ref. [IX–3], Point 4 position for the safety I&C systems. It receives analogue inputs from signal splitters/isolators in the APC-S as well as in the qualified indication and alarm system – P (QIAS-P) channel A via hardwired interface and displays them on the non- safety DIS FPD at the MCR safety console.

IX –6. HUMAN–MACHINE INTERFACE

The DIS and DMA switches provide means for the operator to take manual actions necessary for the mitigation of AOOs and postulated accidents analysed in transient and accident analysis concurrent with software CCF in safety systems, to place the plant in a safe shutdown condition, and to monitor and maintain the critical safety functions. The DIS and DMA switches are also designed for all credited manual operator actions. The DIS and DMA switches are designed, verified and validated in accordance with the human factors engineering program.

Operator response is necessary to accomplish subsequent recovery actions following each event. Diversity in the plant equipment and software provides reasonable assurance that adequate instrumentation and controls are available for the timely diagnosis and mitigation of design basis events with a concurrent postulated software CCF in the PPS and ESF-CCS.

REFERENCE TO ANNEX IX

[IX–1] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE Std 603, New York, (1991).

[IX–2] LAWRENCE LIVERMORE NATIONAL LABORATORY, Methods for Performing Diversity and Defence in Depth Analyses of Reactor Protection Systems, NUREG/CR-6303, Livermore (1994).

[IX–3] NUCLEAR REGULATORY COMMISSION, Guidance for Evaluation of Diversity and Defence-In-Depth in Digital Computer Based Instrumentation and Control Systems, Branch Technical Position 7-19, Washington D.C. (2007)

DEFINITIONS

The following definitions apply for the purposes of this TECDOC.
Further definitions are provided in the IAEA Safety Glossary:
Terminology Used in Nuclear Safety and Radiation Protection (2016 Edition),
IAEA, Vienna (2016):

diverse actuation system: A system which implements protection functions in a diverse way to cope with common cause failures that are postulated in the reactor protection system.

Note: A diverse actuation system may be implemented as a dedicated stand-alone system, or via assignment of a set of protection functions to I&C systems introduced in the architecture for other primary purposes.

programmable digital item: Item that relies on software instructions or programmable logic to accomplish function (IEC 45A/1103/DC).

Note: The main kinds of programmable digital items are computer based items and programmable logic items.

programmable logic item: Item that relies on logic components with an integrated circuit that consists of logic elements with an inter-connection pattern, parts of which are user programmable (IEC 45A/1103/DC).

Note: A programmable logic item is a kind of programmable digital item.

computer based item: Item that relies on software instructions running on microprocessors or microcontrollers (IEC 45A/1103/DC).

Note 1: A computer based item is a kind of programmable digital item.

Note 2: This term is equivalent to software-based item.

hardwired item: Item that relies on relays, on analogue electronic or on discrete digital logic (IEC 45A/1103/DC).

Note: Hardwired items are also usually called conventional items.

HDL programmed device: Integrated circuit configured (for NPP I&C systems), with Hardware Description Languages and related software tools (IEC 45A/1103/DC).

Note 1: Hardware descriptions languages (HDL), and related tools (e.g. simulator, synthesizer) are used to implement the requirements in a proper assembly of pre-developed micro-electronic resources.

Note 2: The development of HDL programmed device can use pre-developed blocks.

Note 3: HDL programmed devices are typically based on blank Field Programmable gate Arrays (FPGA) or similar programmable integrated circuits.

Note 4: HDL programmed device is a kind of programmable logic item.

ABBREVIATIONS

ATWS	Anticipated transient without scram
ABWR	Advanced Boiling water reactor
CANDU	CANada Deuterium Uranium
CCF	Common cause failure
CDF	Core damage frequency
CORDEL	Cooperation in-Reactor Design Evaluation and Licensing
COTS	Commercial off-the-shelf
CPLD	Complex programmable logic device
CSA	Canadian Standards Association
DAS	Diverse actuation system
DBC	Design basis condition
DEC	Design extension condition
DiD	Defence in depth
DMA	Diverse Manual Actuation
DHP	Human system interface panel
EMI	Electromagnetic interference
EEPROM	Electrically Erasable Programmable Read-only Memory
EOP	Emergency operating procedure
ESF	Engineered safety feature
EDF	Electricite de France
EPR™	European Power Reactor
EPRI	Energy Power Research Institute
ESFAS	Engineered Safety Features Actuation System
FPGA	Field programmable gate array
HDL	Hardware descriptions languages
HFE	Human factors engineering
HMI	Human–machine interface
HPD	Hardware programmed device
HVAC	Heating ventilation and air-conditioning
IAEA	International Atomic Energy Agency
I&C	Instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
LED	Light emission diode
MCR	Main control room
MELTAC®	Digital I&C platform
NPP	Nuclear power plant
NRA	Nuclear regulation authority
PACS	Priority actuation control system
PICS	Process information and control system
PALASM	Hardware description language
PA	Postulated accidents
PE	Programmable electronic
PIE	Postulated initiating event
PLD	Programmable logic device
PMS	Protection and safety monitoring system
PPS	Primary protection system
PRA	Probabilistic risk assessment
PS	Protection system
RASU	Rusatom Automated Control Systems
RFI	Radio frequency interference
RPS	Reactor protection system
RT	Reactor trip
SA	Severe accident

SAM	Severe accident management
SBO	Station blackout
SDS	Shut down system
SICS	Safety indication and control system
SPS	Safety protection system
SRAM	Static random-access memory
STUK	Radiation and Nuclear Safety Authority
TXS	TELEPERM-XS control system
SPPA	SPPA-T2000 Control System
SPS	Secondary protection system
UPS	Uninterruptible power supply
US	United States
U.S. NRC	United States Nuclear Regulatory Commission
USCA	MCR and unit secondary control area
V&V	Verification and validation
WENRA	Western European Nuclear Regulators Association
WNO	World Nuclear Association

CONTRIBUTORS TO DRAFTING AND REVIEW

Andropov, E.	FIZPRIBOR, Ltd, Russian Federation
Bindu, S.	IGCAR, India
Burzynski, M.	NewClear Day, Inc., United States of America
Dimitrov, I.	Ontario Power Generation, Canada
Duchac, A.	International Atomic Energy Agency
Johnson, G.	Livermore, United States of America
Karasek, A.	CEZ, a.s., Czech Republic
Kim, Y.G.	KHNP Central Research Technology Institute, Korea, Republic of
Khochansky, M.	FIZPRIBOR, Ltd, Russian Federation
Hessler, Ch.	Framatome, Germany
Hojny, V.	State office for nuclear safety, Czech Republic
Chen, R.	China Nuclear Power Engineering Co., Ltd, China
Pickelmann, J.	Framatome, Germany
Richer, N.	Electricite de France, France
Rounding, A.	Amec Foster Wheeler, United Kingdom
Sivokon, V.	Rusatom Automated Control Systems (RASU), Russian Federation
Tate, R.	Office for Nuclear Regulation, United Kingdom
Zhao, J.	Nuclear Regulatory Commission, United States of America
Utsumi, M.	Mitsubishi Heavy Industries, Ltd, Japan
Qu, H.	Shanghai Nuclear Engineering Research and Design Institute, China
Watanabe, N.	Nuclear Regulation Authority, Japan
Xing, A.	Candu Energy Inc., Canada
Yllera, J.	International Atomic Energy Agency
Zeng, Z-Ch.	Canadian Nuclear Safety Commission, Canada

Technical Meeting

Vienna, Austria, 11–14 July 2017

Consultancy Meetings

Vienna, Austria, 10–14 October 2016

Vienna, Austria, 20–24 February 2017

Vienna, Austria, 25-29 September 2017

ORDERING LOCALLY

In the following countries, IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

CANADA

Renouf Publishing Co. Ltd

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: www.renoufbooks.com

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com Web site: www.rowman.com/bernan

CZECH REPUBLIC

Suweco CZ, s.r.o.

Sestupná 153/11, 162 00 Prague 6, CZECH REPUBLIC
Telephone: +420 242 459 205 • Fax: +420 284 821 646
Email: nakup@suweco.cz • Web site: www.suweco.cz

FRANCE

Form-Edit

5 rue Janssen, PO Box 25, 75921 Paris CEDEX, FRANCE
Telephone: +33 1 42 01 49 49 • Fax: +33 1 42 01 90 90
Email: formedit@formedit.fr • Web site: www.form-edit.com

GERMANY

Goethe Buchhandlung Teubig GmbH

Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 874 015 • Fax: +49 (0) 211 49 874 28
Email: kundenbetreuung.goethe@schweitzer-online.de • Web site: www.goethebuch.de

INDIA

Allied Publishers

1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 4212 6930/31/69 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: www.alliedpublishers.com

Bookwell

3/79 Nirankari, Delhi 110009, INDIA
Telephone: +91 11 2760 1283/4536
Email: bkwell@nde.vsnl.net.in • Web site: www.bookwellindia.com

ITALY

Libreria Scientifica "AEIOU"

Via Vincenzo Maria Coronelli 6, 20146 Milan, ITALY
Telephone: +39 02 48 95 45 52 • Fax: +39 02 48 95 45 48
Email: info@libreriaaeiou.eu • Web site: www.libreriaaeiou.eu

JAPAN

Maruzen-Yushodo Co., Ltd

10-10 Yotsuyasakamachi, Shinjuku-ku, Tokyo 160-0002, JAPAN
Telephone: +81 3 4335 9312 • Fax: +81 3 4335 9364
Email: bookimport@maruzen.co.jp • Web site: www.maruzen.co.jp

RUSSIAN FEDERATION

Scientific and Engineering Centre for Nuclear and Radiation Safety

107140, Moscow, Malaya Krasnoselskaya st. 2/8, bld. 5, RUSSIAN FEDERATION
Telephone: +7 499 264 00 03 • Fax: +7 499 264 28 59
Email: secnrs@secnrs.ru • Web site: www.secnrs.ru

UNITED STATES OF AMERICA

Bernan / Rowman & Littlefield

15200 NBN Way, Blue Ridge Summit, PA 17214, USA
Tel: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd

812 Proctor Avenue, Ogdensburg, NY 13669-2205, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 2600 29302 or +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

International Atomic Energy Agency
Vienna
ISBN 978–92–0–103518–9
ISSN 1011–4289