IAEA Nuclear Energy Series

No. NP-T-3.19

Basic Principles

Objectives

Guides

Technical Reports

Instrumentation and Control Systems for Advanced Small Modular Reactors

IAEA

International Atomic Energy Agency

IAEA NUCLEAR ENERGY SERIES PUBLICATIONS

STRUCTURE OF THE IAEA NUCLEAR ENERGY SERIES

Under the terms of Articles III.A and VIII.C of its Statute, the IAEA is authorized to foster the exchange of scientific and technical information on the peaceful uses of atomic energy. The publications in the **IAEA Nuclear Energy Series** provide information in the areas of nuclear power, nuclear fuel cycle, radioactive waste management and decommissioning, and on general issues that are relevant to all of the above mentioned areas. The structure of the IAEA Nuclear Energy Series comprises three levels: **1 — Basic Principles and Objectives**; **2 — Guides**; and **3 — Technical Reports**.

The **Nuclear Energy Basic Principles** publication describes the rationale and vision for the peaceful uses of nuclear energy.

Nuclear Energy Series Objectives publications explain the expectations to be met in various areas at different stages of implementation.

Nuclear Energy Series Guides provide high level guidance on how to achieve the objectives related to the various topics and areas involving the peaceful uses of nuclear energy.

Nuclear Energy Series Technical Reports provide additional, more detailed information on activities related to the various areas dealt with in the IAEA Nuclear Energy Series.

The IAEA Nuclear Energy Series publications are coded as follows: **NG** — general; **NP** — nuclear power; **NF** — nuclear fuel; **NW** — radioactive waste management and decommissioning. In addition, the publications are available in English on the IAEA Internet site:

http://www.iaea.org/Publications/index.html

For further information, please contact the IAEA at PO Box 100, Vienna International Centre, 1400 Vienna, Austria.

All users of the IAEA Nuclear Energy Series publications are invited to inform the IAEA of experience in their use for the purpose of ensuring that they continue to meet user needs. Information may be provided via the IAEA Internet site, by post, at the address given above, or by email to Official.Mail@iaea.org.

INSTRUMENTATION AND CONTROL SYSTEMS FOR ADVANCED SMALL MODULAR REACTORS

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
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
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 NUCLEAR ENERGY SERIES No. NP-T-3.19

INSTRUMENTATION AND CONTROL SYSTEMS FOR ADVANCED SMALL MODULAR REACTORS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2017

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

Printed by the IAEA in Austria
July 2017
STI/PUB/1770

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Instrumentation and control systems for advanced small modular reactors / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2017. | Series: IAEA nuclear energy series, ISSN 1995–7807 ; no. NP-T-3.19 | Includes bibliographical references.
Identifiers: IAEAL 17-01102 | ISBN 978–92–0–101217–3 (paperback : alk. paper)
Subjects: LCSH: Nuclear power plants — Instruments. | Nuclear reactors — Control. | Nuclear reactors — Design and construction.
Classification: UDC 621.039.56 | STI/PUB/1770

FOREWORD

One of the IAEA's statutory objectives is to "seek to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world." One way this objective is achieved is through the publication of a range of technical series. Two of these are the IAEA Nuclear Energy Series and the IAEA Safety Standards Series.

According to Article III.A.6 of the IAEA Statute, the safety standards establish "standards of safety for protection of health and minimization of danger to life and property". The safety standards include the Safety Fundamentals, Safety Requirements and Safety Guides. These standards are written primarily in a regulatory style, and are binding on the IAEA for its own programmes. The principal users are the regulatory bodies in Member States and other national authorities.

The IAEA Nuclear Energy Series comprises reports designed to encourage and assist R&D on, and application of, nuclear energy for peaceful uses. This includes practical examples to be used by owners and operators of utilities in Member States, implementing organizations, academia, and government officials, among others. This information is presented in guides, reports on technology status and advances, and best practices for peaceful uses of nuclear energy based on inputs from international experts. The IAEA Nuclear Energy Series complements the IAEA Safety Standards Series.

Small modular reactors (SMRs) are being developed in a number of Member States to address the spiralling energy demand by adding incremental capacity with moderate financial commitment for countries or regions with smaller grids or even none. Developers of SMR technologies aim for significant cost reduction through modularization and for shorter construction schedules than those more typical for large nuclear power plants. With lower upfront capital cost, SMRs have the potential to offer better affordability for developing countries. In a broader view of applications, SMR concepts and sizes are being promoted as being better suited for partial or full dedicated use in non-electrical applications such as seawater desalination, hydrogen production and heat for industrial processes, which can result in significantly improved thermal efficiency that translates into better return on investment. Many SMRs under development are designed to have an electrical capacity of less than 300 MW(e) to address target markets.

It is becoming clear that in order to increase operational efficiency and safety, SMR developers are using significantly more automation in plant systems. Designers are moving towards the use of more complex control systems with significantly more sensory instruments to assist in operational monitoring and decision making. In some cases, local automation for smaller SMRs is being proposed that would reduce, or even remove, the need for local operator presence. This means that instrumentation and control (I&C) capabilities in nuclear facilities are migrating towards those that are more typical of conventional industrial sectors (e.g. aerospace, transport and conventional power generation) but are challenging more traditional regulatory requirements and guidance in the nuclear sector. Compared to current reactors in operation, some advanced SMRs would operate differently and would also need new I&C approaches. The more compact system configuration can present significant challenges for the placement of I&C components for monitoring, control actuation and diagnostic measurements. In incorporating the lessons learned from the Fukushima Daiichi accident, I&C systems important to the safety of SMRs will also have to be addressed.

Numerous guidance and reports in I&C design, engineering and technology of nuclear power plants have been published by the IAEA since the 1980s. These publications have, however, not addressed the specific challenges in I&C for advanced SMRs.

In response to recommendations by a number of Member States, this publication discusses the issues and challenges relating to the design, qualification, licensing, implementation, operations and maintenance of I&C systems and human system interfaces for SMRs.

The publication is intended to address a wide audience, including newcomer countries considering nuclear power programmes that would utilize SMR technologies, nuclear regulatory authorities, plant owner organizations and reactor designers.

This publication was produced by a committee of international experts and advisors from numerous countries. The IAEA wishes to thank all participants and their Member States for their valuable contributions, in particular the chairman of the report preparation meetings, R. Wood (United States of America). The IAEA officers responsible for this publication were J. Eiler and M.H. Subki of the Division of Nuclear Power.

EDITORIAL NOTE

This publication has been edited by the editorial staff of the IAEA to the extent considered necessary for the reader's assistance. It does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

Although great care has been taken to maintain the accuracy of information contained in this publication, neither the IAEA nor its Member States assume any responsibility for consequences which may arise from its use.

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this book and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION

This section describes the distinction between instrumentation and control (I&C) systems for conventional, large reactors compared to those for advanced small modular reactors (SMRs). For the purposes of this publication, small reactors include designs providing for the equivalent of 300 MW(e) or less in power generation capacity. Modular refers to at least one of the following two characteristics: (i) design of the nuclear island as a module suitable for factory fabrication and ready for transport and installation; or (ii) implementation of multiple modules (i.e. reactor units) at a plant site. The designation of these reactors as ‘advanced’ refers to the distinction between these designs and conventional designs that dominate the worldwide commercial fleet.

1.1. BACKGROUND

The IAEA provides support to the development and deployment of SMRs through the project Common Technologies and Issues for SMRs. SMRs have the specific characteristics to match the spiralling energy demand by adding incremental capacity with moderate financial commitment for countries and regions with smaller grids. The considerable development work on SMR design concepts generally aims to provide increased benefits in the areas of safety and security, non-proliferation, waste management, and resource utilization and economy, as well as to offer a variety of energy products and flexibility in design, siting and fuel cycle options. Specifically, SMRs address deployment needs for smaller grids and lower rates of increase in demand. The technology aims for significant cost reduction through modularization, which further improves the construction schedule. With lower upfront capital cost, SMRs offer better affordability for developing countries. In the area of wide applications, SMR concepts and sizes are better suited for partial or full dedicated use in non-electrical applications such as seawater desalination, hydrogen production and heat for industrial processes, which will result in significantly improved thermal efficiency that translates into better return on investment. Most current SMRs have the electric capacity of less than 300 MW(e).[1] This power range offers flexibility in generation locations and it contributes to grid stability. Current IAEA activities on SMRs include the following:

- Formulating a roadmap for technology development incorporating safety lessons learned from the Fukushima Daiichi accident;
- Reviewing newcomer countries’ technical requirements, addressing standardization issues, use of proven technology and economic competitiveness;
- Tackling regulatory, licensing, infrastructure and business issues.

One of the important technical areas associated with the specificity of designs, and operational and process characteristics is the design and implementation of I&C systems. The I&C systems of a nuclear power plant provide the capability to control and regulate the plant systems manually and automatically during normal plant operation, and provide protection against unsafe plant operation. The systems also provide initiating signals to actuate safety functions, which are assigned to mitigate the consequences of faulted conditions and ensure safe shutdown.

Compared to current large reactors in operation, some advanced SMRs will operate differently, many will employ higher levels of automation, and some will need new I&C approaches. Many water cooled SMRs are integral pressurized water reactors (iPWRs) with modularization, in which the primary coolant system components are placed inside the reactor vessel, in the same compartment with the reactor core and control rod drive mechanism (CRDM). This type of primary system configuration requires sensor access requirements that are different from those of loop type light water reactors (LWRs). Some iPWR concepts adopt natural circulation, and several concepts adopt forced convection using horizontally or vertically mounted coolant pumps into the reactor vessel. The location of the primary pump within the reactor vessel limits accessibility for diagnostic measurements.

[1] According to the classification adopted by the IAEA, small reactors are reactors with an equivalent electric power of less than 300 MW(e) and medium sized reactors are reactors with an equivalent electric power of 300–700 MW(e).

In addition, many advanced SMRs use a non-water coolant, such as fast reactors cooled by liquid metals, including sodium, lead and lead–bismuth eutectic, and also gas cooled reactors operating at higher temperatures. For those non-water cooled SMRs, the process measurement instrumentation needs to be both chemically compatible with the coolant and tolerant of the higher temperature. There have also been recent design and technology developments for both land based, marine based and factory fuelled transportable SMRs. Examples of proposed marine based SMRs include barge mounted floating power units and sea-floor moored power units remotely operated from a coastal command and control room. Specific I&C issues and operational challenges of these submarine SMR units need to be understood and anticipated.

Several advanced SMR concepts are planned to be deployed as multi-module plants (i.e. 2–12 modules per plant unit, with a power output of 10–300 MW(e) per module). The impact of shared resources and systems requires the implementation of more sophisticated controls to address, among others, the specific dynamic behaviour.

In incorporating the lessons learned from the Fukushima Daiichi accident, there is a greater emphasis on the design of I&C systems as part of the defence in depth strategy.

The resolution of technical issues and challenges of I&C specific to the characteristics of advanced SMRs will enable deployment. This publication provides technical information on I&C issues associated with specific operation and process characteristics of SMRs that result from the fundamental differences to large reactors currently in operation. The publication explores innovation in I&C design and technology that can enhance operability, reliability, safety, maintainability and economic competitiveness of SMRs.

1.2. OBJECTIVE

The objective of this publication is to assist Member States active in SMR development in understanding current knowledge, practices, design and architecture, implementation, operating and maintenance related aspects with I&C systems in advanced SMRs, as well as exploring the challenges and issues that need to be resolved in the initial phases of design and implementation. This publication emphasizes the key cross-cutting technological issues associated with I&C systems and human system interfaces that arise from the specific behaviour and operational characteristics of advanced SMRs.

1.3. SCOPE

This publication addresses I&C issues associated with the specific design, process and operation characteristics of SMRs that result from fundamental differences with the plant systems in large reactors in current operation. The publication describes aspects that may need to be addressed in requirements and guidance. However, the publication is formulated to minimize overlap with areas common with large power reactors, which are already described in existing IAEA publications. Examples of potential differences include the following:

- Integration of an SMR into a hybrid energy supply system;
- Strategies for multi-unit control;
- Highly automated plant operations to enable optimal plant staffing;
- Communications between an SMR and a control and monitoring facility located away from the reactor unit;
- Long life sensors and actuators used in confined vessels subject to extreme environments;
- I&C used in transportable and factory fuelled sealed reactor modules;
- Effects of extensive load following on reactor control;
- Control strategies and I&C architecture;
- New uses for instrumentation;
- New sensors and other field components;
- Simulation, human factors and human system interface;
- Testing and calibration;
- I&C function under operation and accident conditions;
- Regulatory issues associated with I&C.

This publication is intended for all personnel involved in the design, manufacture, qualification, licensing, operation, and maintenance of I&C for SMRs. Users of this publication include the following:

- Member States with a plan for nuclear power plant deployment, particularly those adopting SMRs;
- Reactor designers, manufacturers and vendors;
- Governmental authorities involved in issues and technologies relating to I&C for SMRs;
- Research organizations;
- Technical support organizations;
- Utilities, owner/operators and other stakeholders.

Guidance provided here, describing good practices, represents expert opinion but does not constitute recommendations made on the basis of a consensus of Member States.

1.4. STRUCTURE

Section 2 outlines SMR operation, process and functionality characteristics. It describes specific items for SMRs such as their objectives, a listing of design concepts, the need to balance safety and economics, the economic impact of I&C, and potential regulatory issues with I&C approaches for SMRs.

Section 3 describes distinctive features and issues for I&C systems and human system interfaces that arise from the specific behaviour and operational characteristics of advanced SMRs. The section discusses the fundamental control strategy and architecture, specific equipment designs (i.e. new sensors, I&C components in harsh environments and accident instrumentation), human system interface issues, and operations and maintenance (O&M) specificities (including diagnostics and prognostics) with I&C for SMRs. The section also outlines regulatory issues with SMRs, new tools for modelling and simulation, human factors and human system interface, multi-unit management, hardware and software characteristics (i.e. wireless, and digital versus analogue), testing and calibration of sensors, testing for normal operation and accident conditions, and licensing.

Section 4 summarizes the key challenges and the best practices recommended by experts. The Annex compiles short reports on the status of I&C design development for SMRs in Member States.

2. GENERAL SMR OBJECTIVES AND CHARACTERISTICS AFFECTING I&C

2.1. OVERVIEW OF SMR OBJECTIVES

The high level goal of SMR development is to extend the benefits of nuclear power to markets that cannot use a conventional nuclear power plant. SMRs can also provide characteristics, features and capabilities not available with conventional large scale nuclear power plants. Specifically, these designs aim to capitalize on their relatively small size to achieve economic and performance objectives that can encourage expanded implementation of nuclear reactors. Objectives that are common to many SMR concepts include the following [1, 2]:

(a) Enhanced safety and security;
(b) Innovative fabrication and installation logistics;
(c) Adaptability of plant output;
(d) Operational flexibility;
(e) Affordability.

There are several characteristics found in many SMR design concepts that either inherently contribute to, or facilitate, enhanced safety and security. A favourable safety consequence of lower power capacity for an individual SMR unit is a reduced inventory of radionuclides. Consequently, the source term to be treated in safety analyses is smaller and the site boundary and emergency planning zone can potentially be reduced in size compared to conventional large reactors. SMR concepts seek to eliminate, by design, accident vulnerabilities that impact existing nuclear power plants (e.g. a large break loss of coolant accidents for iPWRs or rod ejection events for designs employing internal CRDMs). In addition, the dynamic behaviour of some SMR concepts (e.g. high heat capacity and large thermal inertia, low pressure operation and natural circulation for passive decay heat removal) can provide inherent safety response characteristics to accommodate passively abnormal and accident conditions. Passive safety design options include a minimum reactivity margin, robust fuel (e.g. accident tolerant or high integrity fuel with a high margin to failure), passive reactivity control and reactor shutdown, and passive decay heat removal [1]. Security can be promoted through design and installation approaches, such as providing whole life cores that do not require on-site refuelling or embedding the nuclear island deeply below grade.

For most SMR concepts, the reduced size of many major components and the modularization of the nuclear island (e.g. integral configuration of the reactor coolant system) help to achieve cost savings and plant construction efficiencies through innovative fabrication and installation logistics. Advanced manufacturing techniques mean that complete reactor modules can be assembled on-site rather than the traditional approach of constructing the nuclear island from separate elements (i.e. ‘stick build’). Manufacturing the nuclear island module in a stable, well controlled factory environment can promote construction efficiency, enhance quality and facilitate pre-service inspection. The establishment of manufacturing conventions for SMR modules supports standardization of the nuclear island and can result in economy of replication. Given that many SMR concepts involve compact designs incorporating significantly smaller vessels, transport options (e.g. barge, rail and road) of the main components, or even the complete nuclear island module, are greatly expanded over the limited options for large nuclear power plants (e.g. barge transport to coastal or large waterway sites). More varied transport options not only reduces cost and schedule risk but also permits greater flexibility in siting (inland sites or remote locations).

The smaller thermal power capacity and, in some cases, high temperature operation make SMRs adaptable to many energy applications; foremost is electricity generation. The small power output means SMR units can support small or micro grids with modest power demand or reinforce large grids by, for example, replacing ageing fossil fired power plants, which are typically small power sources themselves. With micro grids, SMR units can provide highly reliable and secure electric power. The inherent self-regulation and resilience to external events (e.g. station blackout, load rejection or loss of heat sink) possible for many SMR design concepts can substantially contribute to grid stability.

In addition to the more traditional electric power role of nuclear power plants, non-electrical product streams can be supported by SMRs. These applications include district heating, desalination, hydrogen production and industrial process heat supply. The energy conversion systems at the SMR plants can either comprise, or include, secondary heat transfer systems to channel high temperature coolants or high quality steam for industrial processes. Hybrid energy applications are possible where, in addition to electricity generation, some portions of the thermal output of an SMR unit is used to support generation of alternative energy products such as methanol via steam methane reforming or hydrogen via high temperature steam electrolysis. The production of diverse product streams can be implemented through dedicated generation on an SMR unit basis or reconfiguration of SMR units within a plant to support different products, depending on demand. Also notable is the potential application of SMR power production when used in conjunction with renewable energy.

The nature of an SMR makes possible various types of operational flexibility and applicability. The reduced source term and relatively low thermal output of an individual SMR unit expands the options for siting, which enable co-location with process heat and power customers and a reduction in the required water to support waste heat rejection. An SMR can serve as a stable energy source for remote, isolated or underdeveloped locations (e.g. polar, island and arid regions). Their small size also make them suitable for floating platforms (e.g. barges), which could be relocated to alternative sites as power demand evolves.

With regard to electricity generation, the roles of an individual SMR unit range from serving as a base load lynchpin of a micro grid to contributing on demand as a power peaking resource on a large grid. Base load operation is customary for nuclear power plants; however, SMRs can be more readily designed to follow load demand. Some SMR concepts can be inherently load following, while others can implement the capacity to bypass their full steam load. It might also be possible to transition SMR output among multiple hybrid energy product streams (e.g. electricity production at peak demand times transitioning to process heat for methane production at low demand times).

SMRs can offer enhanced availability (i.e. increased capacity factors) through an extended operation cycle (i.e. significantly longer intervals between refuelling outages). Extended operation cycles can be achieved through a lower power density core configuration. For very low power SMRs (~10 MW(e)), developers propose running a sealed and factory fuelled core to full depletion over a long period of time and then replacing the entire core vessel with a new core vessel, thereby eliminating the need for on-site refuelling and the associated postulated events.

With regard to operational flexibility at the plant level, power capacity can be scaled. In situations where small incremental additions are needed to satisfy slow growth in load demand, an SMR plant is a credible option. However, facilities comprising individual units or pairs suffer from a loss of economy of scale, which can be achieved by large nuclear power plants with gigawatt levels of power output from one or two units. Other economies such as the economy of multiples (or replication) may be needed to compensate for this loss. In this scenario, multiple SMR modules on the site achieve a large scale power output. These multiple units can be installed and commissioned in phases to add plant power capacity incrementally to match load demand growth.

Another approach is the economy of sharing, in which non-safety (primarily supporting or auxiliary) systems or other infrastructure elements can be shared as long as overall safety of the facility is not adversely impacted. One of the most significant resources for which sharing might be feasible is the control room. The distinct operation of each SMR unit distinguishes a multi-unit plant operation from the conventional approach: it involves coordinated management of the operation of each unit to satisfy customer demand, which can include the grid and interconnected industrial users of process heat.

Affordability is essential for economic competitiveness. The financial aspects of building a plant include total project cost and investment risk, upfront costs and day to day costs, and the impact depends on capital outlay, construction time and time to return on investment. The reduced number of components required for simplified designs and the smaller structures can significantly reduce the capital costs of SMRs compared to large reactors (i.e. economy of small). Efficiencies from factory fabrication and on-site assembly can reduce construction costs (i.e. economy of replication). Incremental commissioning of individual units in phases means an early return on investment from the first units. Sharing infrastructure and supporting systems (i.e. economy of sharing) can also reduce the capital costs of the plant. However, if the units at the plant are added incrementally, then this needs to be taken into account from the outset of design. In addition, consideration needs to be given to the impact of co-located construction and phased commissioning to ensure that safe, effective operation of in-service units is not affected by the installation and startup of new units.

The day to day costs for a nuclear power plant are primarily capital recovery, plant management and fuel. Financial costs are amortized over a fixed period of time, so these costs depend on the upfront financing available. Fuel costs tend to be stable and, in contrast with other energy sources, they are a minor component of the operational costs. Plant management is the most significant controllable contributor to costs. A primary component arises from O&M activities, which greatly depends on staffing size and plant availability. Coordinated supervision of multiple units with shared or reduced staff can manage these ongoing costs. Automation can be used to achieve the desired operational and staffing efficiencies (i.e. economy of automation). However, increased automation and optimizing the number of staff members cannot compromise the high level of safety assurance necessary for a nuclear power plant. Consequently, the economic gains for O&M costs can only be achieved if a sound technical basis for an acceptable safety case can be demonstrated.

2.2. OVERVIEW OF SMR CONCEPTS

Various SMR design concepts are under development, and many types use different reactor configurations and fuel, which results in control characteristics unique to each design. These specificities impose different constraints and conditions with regard to how certain operational performance parameters are measured, the actuation elements by which control actions are accomplished, and the environments that the sensors and actuators must withstand. Table 1 provides the representative global SMR concepts sorted first by their coolant and then by their deployment or development status or design maturity (see Abbreviations for the terms used). More information about many of the design concepts can be found in the Annex, and generic information and status about SMR concepts can be found in the Advanced Reactor Information System database.[2]

TABLE 1. REPRESENTATIVE GLOBAL SMR CONCEPTS

Design	Type	Technology developers	Modules per plant	Total plant MW(e)
		Water cooled		
CAREM-25	iPWR	CNEA, Argentina	1	27
SMART	iPWR	KAERI, Republic of Korea	1	100
mPower	iPWR	B&W Generation mPower, USA	2	360
NuScale	iPWR	NuScale Power, USA	12	540
ACP100	iPWR	CNNC/NPIC, China	2	200
IRIS	iPWR	IRIS Consortium/Polimi, Italy	1	325
VBER-300	iPWR	OKBM Afrikantov, Russian Federation	1	300
Westinghouse SMR	iPWR	Westinghouse Electric, USA	1	225
SMR-160	iPWR	Holtec, USA	1	160
AHWR300-LEU	HWR	BARC, India	1	300
		Marine based		
KLT-40S	FPU, TNPP	OKBM Afrikantov, Russian Federation	2	70
Flexblue	Seabed moored	DCNS, France	1	160
		Gas cooled		
HTR–PM	HTGR	INET, Tsinghua University, China	2	210
EM^2	HTGR	General Atomic, USA	1	240
PBMR	HTGR	Eskom PBMR, South Africa	1	165
		Liquid metal cooled fast spectrum		
SVBR-100	LMFR	AKME-engineering, Russian Federation	1	101
BREST-OD-300	LMFR	RDIPE, Russian Federation	1	300
PRISM	LMFR	GE Nuclear Energy, USA	4	1244
4S	LMFR	Toshiba, Japan	1	10–30

[2] See http://aris.iaea.org

2.3. UNIQUE SMR DESIGN CHARACTERISTICS THAT IMPACT I&C

Most SMR designs were based on past R&D on similar but older technology. However, the operating characteristics of a new design may not be clear. There is a significant amount of documented operational experience for past prototypical and first of a kind designs developed and built as early as the late 1950s: for example, IAEA-TECDOC-1691, Status of Fast Reactor Research and Technology Development [3], presents many of the control challenges and solutions implemented for fast reactors. This operational experience is valuable to designers and operators of future SMR designs that build on these design concepts; however, new designs have to be carefully compared to their predecessors to understand how and where this operational experience is actually applicable to the new design. Subtle changes in design can result in significant changes in operating characteristics that can render past operational experience less useful to supporting the modern safety case: a significant reduction in the reactor size of early prototypes can completely change the control approach. This requires designers to supplement past R&D results with new findings.

The knowledge about a reactor's operational characteristics has a significant influence on the approach taken to develop a supporting I&C system to ensure the overarching architecture is in place to operate the design safely, reliably and economically. Most design concepts are for very simple and predictable operational behaviour with I&C used to supplement operations (e.g. reduced staff) or improve plant availability (e.g. support predictive maintenance). As a result, the I&C design process is iterative[3] and needs to be refined as greater operational knowledge is gained through plant design, R&D insight and simulation exercises. Basic principles of nuclear I&C design and safety analysis already exist in publications by the IAEA, national regulators, and national and international codes and standards organizations.

With industry's desire to achieve greater levels of automation, particularly in the face of more simple designs using passive and inherent features, there is a need to understand better the contribution of increased automation to the complexity of the overall architecture and hence understanding failure modes in the safety analysis. It is true that some approaches to automation of I&C systems have been proven in other sectors, but safety analysis still needs to be conducted to gain additional confidence that those approaches can perform as planned under the various postulated external and human induced conditions that can occur at a nuclear facility. The adoption of new processes tends to occur slowly in the nuclear sector because of the additional effort needed to demonstrate this confidence, and vendors of technology do not wish to expend resources for a small market. The primary concern with new digital I&C equipment is complexity, which leads to questions of software reliability and the potential for common cause failure of digital equipment.

2.4. MEASUREMENT CHARACTERISTICS SPECIFIC TO ADVANCED SMRs

Existing nuclear grade sensors and transmitters, including smart sensors that are capable of self-diagnostics, are based on conventional sensing technologies that have been understood for over a century. Sensing technologies such as fibre optic sensors, ultrasonic flow meters, and wireless sensors have been fully developed for industrial applications and can have limited roles in nuclear power applications — with the exception of ultrasonic flow sensors, which are not yet qualified for use in primary process measurements.

In some cases, SMR designs will have design characteristics approaching those proposed for Generation IV designs and will draw on R&D by groups such as the Generation IV International Forum. The greatest challenges faced by SMR developers will be adapting measurement processes to operate in significantly more cramped or inaccessible spaces, with more limited access for maintenance. Instrumentation has to be rugged enough to handle not only the high temperatures (and high pressures in some advanced reactor designs) but also the long term effects of the coolant on the sensor interface. Corrosive and high temperature coolants will affect the operative lifespan of process instrumentation and affect measurement uncertainty. Current in situ and hands on calibration and response time testing techniques might need to be revised to accommodate these characteristics. This will drive designers to seek more robust measuring systems, together with methods to detect and adjust to degradations to maintain operation and to ensure that plant operation continues within its allowed operating envelope. To address this,

[3] The modern terminology for this iterative I&C design is called the I&C lifecycle approach and is continuous over the lifecycle of the facility.

process measuring techniques and sensors are emerging that could help diversify I&C architecture for advanced reactors. However, these new methods will need to be evaluated and qualified for use in the primary system of advanced SMRs. The following subsections highlight some of the key challenges SMR designers will face for each SMR type.

2.4.1. Integrated pressurized water reactors

2.4.1.1. Measurement issues associated with internal steam generators

Helical coil steam generators (HCSGs) being considered for use in various SMR designs differ from conventional nuclear steam generators in that the reactor coolant is on the shell side of the steam generator and the feedwater/secondary steam system flows inside the tubes of the steam generator. HCSGs are common in fossil fired power plants but have minimal nuclear operating experience. Upadhyaya et al. [4] report that since feedwater/steam flow occurs inside the tubes, the liquid inventory in each tube is smaller than for the shell side, which makes both liquid level and location of the water–steam phase change very difficult to measure. The small internal diameter of the tubes introduces very rapid dynamic behaviour in the face of small changes in reactor power. This can cause transients that make tube dryout difficult to measure and control, and it means that in order to prevent tube dryout, a highly responsive tube side feedwater flow control is required. This precludes the use of conventional level measurements in favour of a flow based (mass flow management) measurement approach that compares steam flow with feedwater flow. The precision of the measurement of steam flow is heavily influenced by the devices that measure steam temperature and pressure. In the secondary sides of more conventional nuclear power plants, the greater precision of level measurement of feedwater inventory offsets the uncertainties associated with steam flow measurement. For HCSGs, the challenge vendors face will be to reduce significantly the uncertainties of the steam flow measurement instruments to offset the reduced certainties of feedwater flow data.

On account of the geometry of the annular riser and concentric downcomer, flow measuring devices that rely on the pressure differential across some obstruction cannot be used (e.g. orifice plates, flow nozzles and Venturi flow meters). Furthermore, design documentation for several iPWRs indicates that taps are not expected to be used in the lower section of the vessel below the top of the core to avoid introducing potential accident scenarios. This constrains the use of differential pressure transmitters along the length of the vessel for both flow and level measurements.

Traditional differential pressure based level measurement is based on two taps, in which an upper vessel tap is used to provide a reference pressure and a lower vessel tap provides a pressure equal to the reference pressure plus the height and density of the liquid above the lower tap. The integral vessel configuration makes this very challenging. It is expected that digital technology can be used to provide compensation for the unique configuration, but this equipment needs to be verified and qualified for use. Even with the appropriate compensations, this type of level measurement could be problematic for integral primary system concepts due to the design philosophy of avoiding an external penetration below the top of the core. If the coolant level decreases below the height of the lower tap, then both taps will sense only the reference pressure, the differential pressure will be zero, and the actual level from that point and below will be unknown. This condition is not be typical and might only be found during a severe accident situation. However, based on previous lessons of the Three Mile Island accident and the Fukushima Daiichi accident, these are important considerations.

Measurement of HCSG flow induced vibrations is challenged by two key factors: (i) space for the current probes competes with the needs of other in-vessel instruments; and (ii) probes will be located in the flowing reactor coolant and are therefore subject to reactor coolant system (RCS) environmental degradation mechanisms (e.g. the chemical and radioactive environment).

The nature and impact of long term degradation of the tube bundles has to be determined and addressed, particularly with the added effects of radiation exposure and longer intervals between physical inspections of the hardware. This may require additional instruments to be installed to measure the key indicators of degradation.

Another technical challenge is the detection of reactor coolant leaks into the secondary systems. Although the use of HCSGs can significantly reduce the likelihood of the steam generator tube rupturing (i.e. higher pressure is on the outside of the tubes), issues such as fretting or corrosion could result in small pinholes forming, which could enable the primary coolant to slowly leak into the secondary systems. As these leaks are likely to be small, their detection could prove difficult and may require chemical analysis. On the other hand, large incursions of RCS water into the secondary side (major tube failure) will likely be detected through a discrepancy in mass flow.

2.4.1.2. Internal control rod drive mechanisms

There are two primary areas where internal CRDMs present challenges to designers: (i) reliability during reactor operation; and (ii) maintenance related issues during reactor outages. During reactor operation, and particularly in the face of longer intervals between outages, detection and monitoring of degradation of internal CRDM components is a challenge. It will require some materials and reliability testing given the high temperature, pressure and radiation environment inside the reactor pressure vessel. Under certain operating conditions, the chemical environment could also subcomponents of the mechanisms (e.g. affecting levels of friction). In addition, electrical cables need to pass through the reactor pressure vessel flange to operate the CRDMs and to indicate the control rod positions. This requires qualification activities to investigate the long term impacts on the cables such as degradation of insulation — failure analysis can impact safety analysis results. Every failures always needs to result in a predictable state that does not compromise nuclear safety. Current design concepts planning to use internal CRDMs include the Generation mPower reactor and the Westinghouse SMR [5].

2.4.1.3. Internal pressurizers

The pressurizer in an iPWR is a located at the top of the reactor pressure vessel. Its short, wide geometry, unlike the longer vessel typically found in loop type reactor configurations, presents challenges to sensing and responding to pressure and inventory volume transients. Occasional, rapid RCS pressure and inventory fluctuations require more sensitive and responsive instruments. The linear geometry of iPWRs means that pressure perturbations in the reactor vessel are transmitted immediately and directly to the pressurizer space (unlike loop style pressurizers, which sit at a distance on a hot leg from the reactor and experience a pressure wave delay). This could result in a cyclic feedback response by the pressure control system that might be difficult to control. Baffles act as pressure transient suppressors in the reactor vessel to dampen the intensity of such perturbations, thereby reducing the need for the pressurizer control systems to react.

Since the pressurizer is located within a normally inaccessible space inside containment/confinement, instruments cannot be readily inspected and maintained and need to be designed more robustly for longer periods of operation between outages.

2.4.1.4. Primary coolant flow measurement issues

One of the unique technical challenges with iPWRs is the measurement of the primary coolant flow given the complex flow paths of integral vessel design. Without the availability of long, straight flow paths or opportunities for flow restrictions (e.g. orifices) and pressure taps, it is a challenge to enable conventional flow measurements. Clayton and Wood [6] report that:

> “As the primary flow measurements place the highest value on measurement reliability and response time as opposed to absolute accuracy, alternate instrumentation approaches appear useful such as applying pumping power signature diagnostics coupled with neutron noise analysis as a primary flow measurement.”

Some ideas for inferential measurements include correlation of pressure or temperature measurements, inferential models using a thermocouple string and inferential measurements using pump power measurements. These methods and others need to be evaluated for accuracy, uncertainty and practicality.

2.4.1.5. Measurement issues in natural circulation: Low flow conditions and low pressure startup

Some of the iPWR designs adopt natural circulation in their primary coolant system (e.g. CAREM, NuScale and AB6-M). While natural circulation eliminates the need for a reactor coolant pump, the reactors require a specific, rational startup procedure to prevent neutronic and thermal-hydraulic instabilities in lower pressure startup. Measurement devices for detecting various types of instability (e.g. geysering, density wave oscillation and pressure wave oscillation) are necessary. The only reactor operated in natural circulation is the Dodewaard reactor in the Netherlands. The only certified natural circulation reactors are the economic simplified boiling water reactor and CAREM, which is under construction.

2.4.1.6. Measurement issues with reactor coolant system coolant levels during accident conditions

In the event of a severe accident in which all safety measures to keep adequate coolant levels above the top of the core have failed, other level measurement methods using ultrasonic technologies or sensor thermal response can be used to supplement the conventional methods. The decision to employ such supplemental methods should ideally be made as part of a risk informed, defence in depth approach. Thermal level measurement is possible using heated resistance temperature detectors (RTDs) or thermocouples for inferred level measurements.

2.4.1.7. Directly mounted reactor coolant pumps: Flow measurement and vibrations

Many SMR designs feature integrated reactor coolant pumps mounted directly to, or within, the reactor vessel to eliminate the need for external coolant loop piping and hence to reduce significantly the risk of a large loss of coolant accident (LOCA). From an I&C perspective, however, this significantly restricts the designer's options for measuring instrumentation placement, owing to lack of space. Instruments for individual pump RCS flow measurement have to be installed near the pump flange, where critical welds exist. The lack of available space for instrument taps also presents challenges for positioning pump temperature and vibration monitoring instruments. Where horizontal pumps and motors are used, the measurement of vibration becomes more important on account of the increased stresses on the pump bearings.

These challenges require an integrated approach to instrument design that economizes on available space near the base of the pump while providing the necessary data. Westinghouse, for example, has developed a vibration integrity monitoring system for AP-1000 RCS pumps to gather as much useful data as possible given the space constraints [7]. Applications of this type would likely be equally useful for iPWR concepts.

2.4.1.8. Lower plenum: In-core instrumentation

Typical existing pressurized water reactors (PWRs) utilize penetrations in the lower plenum for temperature measurement and moveable neutronic instrumentation. For an iPWR that proposes to use a similar approach, there are two technological issues to be resolved:

(a) There is significantly less room on the lower plenum for instrument penetrations, which means instruments may have to share penetrations.
(b) The lower plenum interspace between the lower plenum and the core support plate is larger than what is typically found in PWRs in order to facilitate RCS flow.

This means that any instrument probes not only have to be thinner to fit through the penetrations, but also longer. This results in probes that would be more subject to lateral forces that can warp or otherwise deform the probe. The instruments themselves would then need to be designed to fit inside these smaller penetrations. Designers would need to develop not only thinner and longer probes but also make them stronger.

2.4.2. Liquid metal cooled reactors

Although each type of liquid metal coolant introduces unique complications to I&C implementation, liquid metals generally utilize opaque coolants that make maintenance and inspection of components inside the coolant loop difficult. In addition, the relatively high melting points for liquid metals necessitate the use of heaters following reactor shutdown to avoid coolant solidification. Thermal cycling and associated expansion and contraction add repetitive stresses to instrumentation and interface processes that can adversely affect the sensor reliability over an extended period of exposure.

2.4.2.1. General comments about lead based reactors

Molten lead based reactors have a significant amount of naval operating experience, primarily of Russian origin, with lead–bismuth eutectic as the favoured coolant. Lead–bismuth eutectic has a much lower melting point than pure lead or sodium, does not expand or contract significantly when solidifying or melting, and does not react with water or air. However, lead based coolants are corrosive to structural materials. The degree of damage to structural elements can be monitored and controlled, but this unique complication necessitates the development of new I&C systems not currently found in conventional LWRs.

Corrosion of structural steels is directly related to the oxygen content in the coolant. In order to protect the structural materials from corrosive liquid lead, a stable oxide layer must be sustained. Insufficient oxygen content leads to dissociation of the protective oxide coating on the structural element and corrosion will occur. In contrast, excessive oxygen addition will result in slagging that disturbs thermal and hydraulic characteristics of the flow which is also undesirable. Therefore, it is important to develop a system that can both monitor and control the oxygen content in the coolant. There is currently research being done in the United States of America to address the issue of oxygen content in liquid metal. A solid phase oxygen controlling system was developed at the University of Nevada specifically for lead and lead–bismuth eutectic in order to mitigate corrosion concerns in nuclear applications [8]. In addition to the US research, studies on lead–bismuth eutectic are also being conducted in the Republic of Korea with the lead–bismuth cooled 300 MW(e) PEACER (Proliferation-Resistant Environment-Friendly, Accident-Tolerant, Continuable and Economical Reactor), at Seoul National University [9].

The effects of corrosion and slagging are not limited to degraded structural integrity. Corrosion or slag buildup on thermowells or pressure sensing lines can compromise I&C temperature, pressure, level, and flow signal accuracy, dynamic response time and reliability. However, if properly instrumented with flow meters and temperature sensors, it may be possible to identify locations in the plant that are subject to greater levels of corrosion. Although lead coolant flow rates are expected to be low, controlling the flow rate of the coolant will also help to alleviate the effects of corrosion.

2.4.2.2. General comments about sodium cooled fast reactors

In particular, the unique operating conditions and characteristics for sodium cooled fast reactors (SFRs) introduce specific challenges to existing instrumentation technology. For example, components in SFRs have to be designed for reliable operation at high temperatures (>500°C), have a fast response in order to maintain stable reactor control, and provide diagnostic capability in case of inadvertent reactivity addition. Sodium's most significant disadvantage is its reactivity with water and air. Leaks are extremely dangerous and require immediate action to avoid large scale damage to plant systems.

Pressure sensing lines, the primary process to sensor interface for pressure, level and flow transmitters, carrying sodium coolant can also be susceptible to leaking and need to be subjected to on-line monitoring (OLM) techniques capable of detecting blockages or other anomalies during normal operating conditions. Robust SFR designs incorporate an inert gas cover around components in contact with the liquid sodium coolant. The gas cover provides protection in the event of a leak. Hence, it would be desirable to develop instrumentation to monitor the inert cells for leaks to provide early warning of a breach in the primary boundary before significant propagation occurs.

Some SFRs are pool type designs that incorporate the primary intermediate coolant heat exchanger inside the pool of primary sodium coolant. From this heat exchanger, which is submerged in the coolant pool inside the reactor, pipes run out of the reactor to transport the intermediary coolant to a steam generator. Any instrumentation installed in the pool will be subjected to temperatures in the range of 500–600°C for extended periods of time. Thermocouples can easily handle temperatures in this range; however, they have poor long term stability and are typically less accurate than RTDs. Owing to the nature of their installation in a pool type design, exercising the option of frequent sensor replacement might not be feasible. In contrast, RTDs have excellent long term stability but might not withstand the continuous exposure to temperatures on the upper end of the measurement range of the RTD. Sufficient sensor diversity, measurement redundancy and use of in situ calibration methods might be adequate to provide reliable temperature data between refuelling intervals.

Additional operating characteristics and concerns for SFRs include a dynamically sensitive reactor due to the shorter neutron life time and magnitude of delay coefficient (relative to a traditional LWR), the potential for positive reactivity insertion by voids in the coolant, core motion that can lead to reactivity issues based on a high leakage fraction of fast neutrons, and high local power densities which necessitate optimal coolant heat transfer. These characteristics stress the importance of reactor diagnostic and control technologies as well as fast response instrumentation, control and protection systems. These technologies may be required to ensure reactor protection and thus improve the safety of the SFRs.

2.4.2.3. IAEA publications on I&C for fast reactors

Section 7 of IAEA Nuclear Energy Series No. NP-T-1.9, Design Features and Operating Experience of Experimental Fast Reactors [10], discusses a number of key parameter monitoring issues, which are listed below and are therefore not discussed further in this publication:

(a) Oxygen monitoring.
(b) Hydrogen monitoring.
(c) Carbon monitoring.
(d) Monitoring inert cells for sodium leaks.
(e) Contributors to coolant impurities.
(f) Challenging coolant impurities (polonium and slag in lead based designs).
(g) Coolant freezing.
(h) On-line diagnostics of neutron flux for core reactivity insertion from:
    - Voids;
    - Flow irregularity;
    - Anomalous core motion.

Measurement technologies and approaches for fast reactors are discussed at length in Ref. [11], which also contains some discussion on tools for OLM.

It is worth noting that significant operating experience exists in other industries that use liquid metals for manufacturing processes; however, such experience has to be reconciled with the impacts of radioactive exposures and the need for higher control certainty typically required for nuclear applications. A significant amount of experimental work has been, and continues to be, conducted by both private companies and national nuclear laboratories to understand nuclear related effects on these technologies. Significant operating experience also exists within the nuclear industry; however, intellectual property rights means vendors normally tightly control specific solutions to problems.

2.4.2.4. Impacts of liquid metal coolants on I&C sensing devices

In the presence of dense and often chemically reactive fluids, measuring devices need to be designed to mitigate against the following effects:

(a) Erosion and chemical ablation: This effect alters the physical dimensions of measuring devices and therefore affects the calibration over time.
(b) Slow deformation due to stresses generated by changes in flow intensity: Bending actions, for example, can alter electrical characteristics of a device resulting in a slow drift of input signal.
(c) Deposition and clogging: For example, pressure sensing taps are particularly susceptible, leading to an erosion of quality of the pressure signal.
(d) Electrical effects of flowing metallic fluids: These result from flow based friction and static electricity.

The effects can all influence an instrument’s performance and in-service life span. The design goal is both to demonstrate and maintain the design function of these instruments for their full in-service life. This is accomplished through in-service monitoring of the components and mitigation of degradation through design. One method of mitigation is to design the component mechanism to withstand degradation effects and another is to compensate, either mechanically or electronically, as the component wears. The method chosen depends on the safety classification of the components, their accessibility, risks encountered during maintenance and the cost.

2.4.2.5. Flow measurement in metallic fluids

Traditional methods of measuring fluid flow in water cooled reactors use mechanical flow measuring devices, inference by pressure differential, ultrasonic and, more recently, optical measurements. In many cases, these methods are very problematic in liquid metal environments because of clogging and the fluid's density, opacity and chemistry.

The high electric conductivity of liquid metals can be used to measure fluid flow, and examples include electromagnetic flow meters and miniaturized permanent magnetic probes for local velocity measurements. SMR designers are attempting to apply these approaches to their designs.

Sodium flow would typically be measured at the pump outlet and at the outlet of the fuel subassemblies to detect flow blockage. Monitoring flow is vital to protecting the plant from events such as pump seizure, pump trip, off-site power failure and pipe rupture, which result in a sudden reduction in flow and rise in core temperature. Flow reductions are exacerbated by the high core power densities of the fast flux reactor design. Permanent magnet flow meters are widely used for sodium flow measurements. However, they are not well suited for use in high radiation environments because of damage to the magnets.

2.4.2.6. Detecting local instances of fuel solidification: Lead cooled

Although reactor vessels for lead cooled reactors are designed to minimize instances of local lead freezing, flow characteristics of the coolant under different operating parameters means that some freezing cannot be precluded. Local freezing can introduce complications that range from altered flow characteristics in the core to flow restrictions and plugged instruments. Mechanisms need to be developed to detect early freezing phenomena: for example, temperature measuring devices installed around the outside of the reactor core could detect changes in thermal conductance that indicate the thickening of walls due to lead freezing.

2.4.3. Gas cooled reactors

2.4.3.1. General comments about gas cooled reactors

High temperature gas cooled reactors (HTGRs) are expected to employ helium as the primary coolant and operate at temperatures in the range of 800–1000°C and pressures greater than 7 MPa. These advanced reactors can utilize tristructural isotropic (TRISO) fuel particles, which are specifically designed not to crack under the extremely harsh conditions in an HTGR core. Either a pebble bed or a prismatic block core configuration is possible for these designs [12].

HTGRs are expected to operate with a low power density compared to liquid metal reactors or PWRs. The dynamic response of the reactor power and temperature interactions are expected to be slow, which is good for reactor control and safety. However, it is anticipated that, given the low power densities, low heat conduction from the core to the coolant and the high operating temperatures of this type of design, the following conditions apply:

— Large core volume;
— Large temperature difference across the core;
— High coolant velocity.

All of these factors (as well as prior operating experience) indicate that HTGRs may well experience an increased likelihood of instability from component vibration, thermal stress and non-uniformities in thermal power distribution at the core outlet. Variations in temperature, density and pressure of the gas coolant coupled with the high velocities can all lead to 'striping' or modulation of the thermal power distribution at the HTGR core outlet. Thus, the challenge for the HTGR design will be obtaining accurate and representative temperature and flow measurements. These variations in thermal power measurements can also result in challenges to plant control and stability.

Significant temperature non-uniformities at the HTGR core outlet can result from non-uniformities of power density and thermal conductivities across the core as well as incomplete mixing at the core outlet. Temperature non-uniformities could affect the accuracies of nuclear instrumentation calibrations, which are based on calculations of reactor thermal power output. These non-uniformities can also affect reactivity controls, which are typically based on maintaining a stable core outlet temperature in load following conditions. Additional complications arise with flow measurements owing to variations in coolant density and pressure. Therefore, it is expected that specialized flow and spatial and gradient temperature measurements in the high temperature environment need to be investigated and evaluated by the HTGR designers of I&C systems.

Since there is no activation of helium, activation based transit time measurements are not feasible. However, the non-uniform variation in thermal output of the HTGR could make the helium coolant a candidate for cross-correlation or other transit time technologies based on the inherent thermal fluctuations in the gas coolant flow. Additional development is needed to assess the placement and configuration of temperature sensors, the time needed to process temperature and flow signals to obtain an accurate calculation of the flow velocity, associated uncertainties and relevant failure mechanisms.

Within the HTGR core, a large temperature gradient places significant stress on structural components and on any instrumentation that might be installed in the process. Gas coolants have relatively low thermal conductivities and densities, and therefore require high flow rates to provide sufficient heat transfer. This high flow rate can generate flow induced vibrations that further disrupt sensors installed perpendicular to the coolant flow. The combination of adverse flow conditions and high temperature gradients make obtaining in-core measurements difficult. Large temperature gradients change the coolant's density and therefore affect the accuracy of flow sensors that rely on pressure at two points along the coolant path. In the event that the gas is not well mixed, stratification and streaming issues complicate temperature measurements. Thermal stratification can yield erroneous temperature readings because conventional temperature sensors like RTDs and thermocouples are only sensitive at their probe tips. They cannot determine the temperature profile along the length of the probe. Research is being conducted in the United States of America to develop an ultrasonic thermometer that can do this and could be a suitable candidate for gas cooled reactor temperature measurements in highly stratified locations [13].

There are two reactor concepts for HTGRs: TRISO concepts which are broken down further into pebble based fuel and prismatic block configuration; and solid pin designs with graphite based moderator blocks similar to the prismatic design. I&C systems might need to interact not only with conventional or gas cooled secondary loops but also tertiary coolant loops. Two main power conversion designs are proposed: Brayton and Rankine direct helium power turbines and via steam generator/conventional power turbines.

For the Chinese High Temperature Reactor–Pebble-Bed Module (HTR–PM) twin unit configuration, the I&C systems will need to consider the I&C systems of two reactor units communicating with a combined single steam and single power turbine. In fact, the design can be configured to have up to six reactor units feeding a single power turbine. Combining reactors to work in combination with one another presents challenges to control systems, which have to take measurements from multiple units. Normally, three specific systems in the HTGR systems structure define the I&C needs:

- Plant control system;
- Data and instrumentation system;
- Investment protection system.

Due to the modular HTGR safety philosophy, systems such as the backup reactor cooling system and associated instrumentation are referred to as investment protection systems and instrumentation. It initiates backup cooling to protect reactor equipment in events which could reduce service life or cause a long term outage.

2.4.3.2. Detection of failed fuel

When using solid moderators (either prismatic or pebble based), any rubbing of moderator components against one another — either due to refuelling, transport (for factory sealed transportable designs) or thermal effects — can result in slow erosion of the moderator elements and hence dust, which circulates through the reactor systems. In TRISO fuel arrangements, such erosion mechanisms can potentially release very small amounts of fuel particles from the moderator matrix, which will need to be monitored and contained within the reactor vessel. With the reactor coolant operating at high pressure, this presents a small increase in risk of a release in the event of containment failure. As a result, solutions need to be developed for in-core monitoring of moderator erosion.

2.4.3.3. In-core instrumentation

HTGRs have fuel that is specifically designed to survive very high temperatures during normal operation and transients. The reactor parameters under these conditions need to be monitored at all times. Hence, the instruments have to be designed to operate and not degrade under these higher temperatures including those temperatures that could result in fuel degradation.

In addition, HTGRs that use pebbles in a refuelable configuration have specific in-core instrumentation that is different from more traditional gas cooled designs because they have to cope with the movement of fuel pebbles during operation.

2.4.3.4. Coolant leak detection

Gas as a reactor coolant medium requires the RCS pressure boundary to be especially leaktight particularly in consideration of possible releases during loss of containment events. Since gas is a compressible fluid, pressure detection methodologies do not work well for detecting leaks. This means that leak detection requires extremely precise chemical detection methods such as 'sniffers'. Designers will be challenged to determine the best positions to place such instruments and the leak detection thresholds to be used. Detection accuracies will likely need to be well above readily available commercial detectors.

Helium gas can be particularly difficult to work with because of the very small molecular size, which enables it to escape easily through the smallest flaws in welds and gaskets. A helium leak detector, also known as a mass spectrometer leak detector, can locate and measure the size of the leak, but it requires local placement of probes to measure partial pressure. In the large, controlled space around a reactor vessel, such a system could only be used with a probe placed at a distance to detect that a leak exists, but the location of the leak would need to be determined manually during an outage. The helium leak detector or concentration monitor would need to be placed in an elevated area, accessible when the reactor is at power to allow for maintenance activities. Although operational experience exists from past prototypes of helium cooled designs such as Fort St. Vrain, United States of America, the first modern SMR design likely to address this issue with state of the art detection systems will be the Chinese HTR–PM.

2.4.3.5. Measurement of gas flow

Gas flow measurement is a mature technology in many industries, including the nuclear sector. The main issue will be to ensure those technologies implemented into various SMR designs will be sufficiently reliable when used in applications difficult to access. In addition, such instruments will need to be robust at the very high gas temperatures experienced during normal operation. Such systems would likely need to provide some measure of flow indication to operators during accident conditions (compressors running or shutdown) to assess whether coolant flow is through the core.

2.4.3.6. Detection of air ingress into reactor coolant system gas

The gas typically chosen for a HTGR RCS has to be as chemically inert as possible and has also to prevent the risk of fuel combustion. Air ingress into the RCS represents a significant risk of onset of fuel combustion and fires in the reactor vessel and can only be measured indirectly as a result of loss of reactor vessel containment (depressurization). The immediate response to an air ingress event is to trip the reactor and to depressurize the RCS. This issue is well known within the HTGR sector and experiences are well documented (see Ref. [14]).

2.4.3.7. Detection of water vapour in reactor coolant system gas

Steam and water ingress events are assumed to be primarily caused by steam generator tube leaks or breaks, but leaks in other water cooled heat exchangers in the primary system are also possible. Water ingress into the RCS represents an increased risk of the following:

- A significant positive reactivity risk because the water vapour acts as a moderator;
- Increased source term due to water interaction with fuel (release of noble gases);

- Oxidization of graphite;
- Water interactions with plated out activation products that subsequently resuspend them into the RCS environment.

Once moisture is detected, it is important to immediately trip the unit to stop helium circulation (to reduce moisture ingress) and to isolate and empty the leaking steam generator. Ball et al. [15] report that:

> "Moisture monitoring will likely be performed either with a mechanical resonance or capacitive-type gauge connected to a gas sampling tube (to lower the gas temperature and pressure) or preferably by an online, infrared absorbance spectrometer….
>
> "In general, the hot graphite of the core is expected to react with all of the trace oxygen, moisture, and carbon dioxide in the coolant to form carbon monoxide and hydrogen. The hydrogen, in turn, could react with cooler graphite to form CH_4. The moisture detection system needs to be sensitive to ~1 ppm of moisture, and periodic off-line analysis of primary coolant contamination helps to keep track of the reactions occurring during normal operation.
>
> "The recent HTGR moisture ingress evaluation notes that ppm levels of moisture could be a chronic problem at HTGRs, but indicates that further research and development (R&D) is advised to estimate the effects on core materials and lifetimes. However, with a properly functioning helium cleanup system, even the large amount of moisture that can potentially be present in new fuel or reflector block loadings can be removed relatively rapidly (hours).
>
> "Water-steam leaking into a helium environment will have an acoustic signature as the steam flow induces vibration in the leaking crack. The intensity and frequency of the acoustic signature will vary if the crack enlarges and the steam flow increases over time. The leak's acoustic signal can be detected by attaching a high-temperature strain gauge to the surface of the primary piping near the SG and reading out the strain gauge at a few tens of kilohertz.
>
> "A rise in the loop tritium level resulting from flushing the chemisorbed tritium from the core graphite would be observable in the helium cleanup system. In the most likely form of the helium cleanup system, a side stream of primary coolant would be oxidized by flowing it over a copper oxide bed to form tritiated water. Next, the tritiated water would be adsorbed onto a microporous synthetic zeolite filter, referred to as a molecular sieve dryer. The filter would be removed from the flow path and heated to drive off the water. Finally, the water would be condensed in a cold trap and analyzed for tritium content most likely by use of a scintillation cocktail. The tritium collection process inherently takes time; tritium would not be detected until the filter is exchanged and analyzed, likely some hours after the water ingress begins. However, tritium detection may be a useful indicator of small-to-moderate water ingresses."

2.4.3.8. Helium purification system

Fission products and noble gases that escape the fuel particles need to be removed from the RCS gas system to reduce the potential source term in the event of a containment breach. As a result, gas purification systems require instruments to detect fission products and noble gases. Fission product detection in a gas is a proven technology used in many nuclear reactor designs, and these products would normally be removed from the RCS using scrubbers (also proven). Technology for detecting noble gases is also proven; however, removing the gases remains difficult because they cannot be filtered or chemically extracted.

2.4.3.9. Fuel handling system and burnup measurement I&C for pebble bed reactors

Pebble bed reactors that recirculate fuel using an on-line refuelling system require measurement capabilities, also known as on-line fuel burnup measurement, to determine whether individual pebbles are spent and are to be removed or to return fuel to the reactor. Burnup measurement also allows plant operations to separate and remove damaged or broken spheres. Instruments are also required for safeguards purposes to accurately count pebbles for inventory control.

2.4.3.10. Reserve shutdown system (pebble bed system)

Some HTGR designs propose a reserve shutdown system that utilizes small absorber spheres that are dropped into the core from a holding container. Measuring devices are needed to confirm the remaining number of spheres in the poised container.

2.4.4. Molten salt reactors

2.4.4.1. General comments about molten salt reactors

Past experience with molten salt reactors (MSRs) is limited to work in the 1960s and 1970s at Oak Ridge National Laboratory, United States of America. The challenge for instrumentation for MSR flow and temperature measurements will be the characteristics of the molten salt coolant. Instrumentation requirements are reliable and accurate measurement of coolant flow and temperature. Instrumentation would be required in pipes and tanks, whose temperatures can reach as high as 700°C. Activation based flow measurements utilizing gamma emission are also feasible.

The challenge with materials used for measurements is the corrosive nature of molten salts. A number of candidate materials have been selected for study to determine which will be best for MSRs. For example, thermowells need to be qualified to withstand the higher temperatures and corrosiveness of the molten salt coolant. If the material limitations of pressure sensors are too great to overcome, alternative methods of pressure measurement need to be explored. Since the operating pressure of an MSR is low, the most important pressure measurements in the plant are for level and flow of the coolant. On account of the refractive properties of molten salt, light can pass through it quite easily. For both level and flow, optical instruments could be used to make precise and accurate measurements without substantially obstruction. The instruments already exist; the challenge for optical measurements is the inclusion of viewpoints into the reactor core. Strategically placed mirrors in the process fluid could gather information about level and flow in the core. This development in optical instrumentation would provide a new type of level and flow measurement not found in the current generation of operating plants.

Much of the existing literature for MSRs that discusses specificities of I&C was written over forty years ago (see Ref. [16]). There is very little modern literature on this subject, which makes it a significant challenge to understand what a modern control system architecture would look like. Fortunately, many other industries use molten salts in processes, so many of the instruments to measure both physical and chemical parameters are proven. This is important because unlike measurement systems for traditional solid fuel reactors, many of the key sensing instruments for an MSR would be devoted to chemical measurements and inventory control. With regard to the chemistry of the carrier salts, additional precautions are required to prevent corrosion and chemical attack of RCS components, and to prevent the generation of additional radiological risks, such as tritium (in impure lithium salts). R&D activities for future designs would need to confirm satisfactory operation and precision in a radiological environment, particularly in the purification systems.

2.4.4.2. Safeguards: Monitoring the inventory of liquid fuels

Although the fissile inventory of MSR fuels is expected to be lower than what is typically used in traditional reactors, a technology has yet to be developed to ensure safeguards are maintained and fissile materials are not being diverted out of the carrier salts. Early consultation with the IAEA is necessary to ensure such systems are developed, tested and implemented in a schedule commensurate with the deployment of the first modern MSRs.

2.5. ISSUES COMMON TO ALL DESIGN TYPES

2.5.1. Remote safeguards measurement capabilities for hard to access facilities

SMRs can be deployed in locations that make safeguards verification very challenging to inspectors, for example:

(a) Subsurface marine facilities, for example Flexblue (see Section A–4) and SHELF designs): These facilities would be located deep down on the seabed and, access would be limited to the main control room (MCR) and emergency response centre, located onshore at a distance from the plants but connected by cable.
(b) Small plants located at very remote sites: These facilities can range from surface (i.e. barge mounted) power plants, which would operate at sea, to very small power reactor facilities servicing an off-grid mine or community.

In both examples, the location of the facility presents challenges to safeguards inspectors, who have to travel to the site to perform their activities. Vendors are encouraged to consult with the IAEA early to determine possible alternative methods to monitor safeguards. For example, remote encapsulated camera systems may be adequate for continuously monitoring the facility, and satellite surveillance could also augment manual inspections.

2.5.2. Measurement of changes to internal configuration following module transport

Following shipment from a manufacturing and testing facility to a site, the construction and commissioning organization normally confirms that the component meets acceptance criteria set by the customer. This typically includes an assessment of any changes in geometry to key internal components as a result of the transport. Components can be sensitive to mechanical vibrations (seismic) and changes in temperature and humidity. Changes in tolerances could impact future plant operation. For example, corrosion or warping can impact the speed at which safety systems operate. In extreme cases, latent stresses might exist that could lead to future component failure. This is particularly important with factory fuelled transportable designs which arrive at the site in a sealed state and cannot be opened for visual inspections. With a sealed design, methodologies are required to confirm that components and systems remain within the original factory acceptable tolerances.

2.5.3. In-core flux mapping

The compact design of SMRs makes the placement of instruments such as flux mapping detectors technically challenging. Thus, detectors will need to be more compact to fit within the available space, and will need to be robustly designed and validated.

2.6. OPERATIONAL CHARACTERISTICS SPECIFIC TO ADVANCED SMRs

2.6.1. Autonomous operation with remote intervention capabilities

A number of developers of very low SMR technology (~10 MW(e)) are exploring techniques that can be adopted to make very small local (on-site) designs fully autonomous, controlled from a remote location tens to thousands of kilometres away. The MCR would still be thought of as an extension of the reactor facility, in which operators behave exactly as they do in a conventional nuclear power plant. The main difference would be that communications would be conducted from outside the security zone of the actual facility. It would therefore require a special, secured communication link between the MCR and the facility.

The most likely application would be in very remote regions that currently rely on off-grid generation sources for power (i.e. diesel generators). A owner/operator could choose it on account of the lower cost of personnel and support staff on the site, since the revenue from generation would be quite low. Operators with a fleet of these small facilities would look at centralizing and sharing control of the facilities, minimizing the number of staff needed on-site to skeleton maintenance staff. Furthermore, the absence of personnel reduces hazards from a fitness for duty perspective that exist in a central operation centre near a populated area. Although most I&C issues specific to remote operation concern the communications link between the central MCR and the remote site facility, others concern advanced human factors engineering (HFE) and extensive use of automation considerations, which need to be addressed during the I&C architecture design stage to enable operators to monitor and control multiple facilities remotely and simultaneously.

2.6.2. Integrated operation of multiple units

SMRs can be implemented in a power park configuration of multiple units to satisfy evolving levels of power demand. As demand grows, additional capacity can be added through phased commissioning of more units. In addition to economical expandability, Clayton and Wood [6] report that a multi-unit plant has the advantage of only losing a small percentage of its power output should an individual unit be out of service due to a planned outage or unplanned trip. Unlike most existing multi-unit nuclear power plants, management of a multi-unit SMR plant is more likely to involve integrated operation of the units through shared systems and a common control room. In fact, some SMR design concepts include configurations based on shared energy conversion systems (e.g. turbine generators) coupled to two or more reactors. The degree of operational integration within the plant can range from simple coordination of load allocation among separate units to co-located control room and workstations with some sharing of staff and equipment to single operator supervision of multiple units.

Clayton and Wood [6] report that modern nuclear power plants have moved towards greater automation of individual unit operation but still rely on human interaction for supervision, system management and operational decisions. This operational approach is acceptable for large nuclear plants because of the ability to defray personnel costs against the significant per unit power output [6]:

> "In contrast, SMR objectives for reduced staffing imply highly automated plant control with greatly reduced reliance upon on-site highly skilled staff for interactive operational control under normal conditions and immediate intervention for event management.
>
> "Highly automated intelligent control involves more than simple automation of routine functions. It implies the detection of conditions and events, determination of appropriate response based on situational awareness, adaptation to unanticipated events or degraded/failed components, and reevaluation of operational goals. To enable [multi-unit] plant operations based on a reduced staff, the control system for a SMR must be capable of fulfilling these higher level supervisory and decision functions. The automation and intelligence incorporated in the SMR control system can range from automated control systems that perform simple transition among predefined operational strategies and functional configurations based on detection of triggering events, to nearly autonomous control systems that can perform control, detection, decision, reconfiguration, and self-maintenance independently based on human permissives.
>
> "Highly automated, intelligent control capabilities have not been demonstrated for nuclear power plant operations and there is limited experience in other application domains….
>
> …….
>
> "Demonstration of the technology required to effectively operate a grouping of small reactors as a single plant is needed. Development of multi-modular plant management and supervisory control should address strategies for coordinated use of shared systems and managed transitions among plant configurations (e.g., phased commissioning of units or flexible system arrangements for selection among co-generation options)."

2.6.3. Multiple end product or reconfigurable energy conversion systems

Clayton and Wood [6] describe that “the provision of multiple product streams enables effective utilization of the energy content of the heat generated by the reactor.” Essentially, this implies reconfigurable energy conversion systems (i.e. balance of plant, BOP), and [6]:

> “For example, the lower end waste heat can be used to support district heating, desalination, or low-grade industrial process heat applications. High temperature heat can be used for product generation such as hydrogen production to provide an alternate use when the full output of the plant is not needed for power production. Essentially, the plant could be reconfigured to meet demand. For example, electrical power could be the exclusive product during high demand periods and some units could be switched to hydrogen production during overnight, low demand periods. Integrated process diagnostics and advanced control to anticipate downstream upsets and response to dynamic coupling of different production systems (e.g. turbine-generator for electricity, thermal systems for desalination or hydrogen production) enables automatic reconfiguration of balance of plant.”

Providing for these capabilities requires more extensive instrumentation of BOP systems and the introduction of automatic controls for traditionally manual actions. Other benefits of automating the transition among product streams include the avoidance of operational disruptions (i.e. obviating the need for shutdowns or runbacks during the transition) and minimization of the required on-site staffing to effect the realignment of systems. In grids with intermittent power sources (e.g. solar and wind), dynamically reconfigurable SMR plants can load follow based on grid demand by switching end use of full power modules rather than tracking grid demand through reactor power manoeuvres.

2.7. MAINTAINABILITY CHARACTERISTICS SPECIFIC TO ADVANCED SMRs

Maintainability is discussed at length in IAEA Safety Standards Series No. SSG-39, Design of Instrumentation and Control Systems for Nuclear Power Plants [17]. Maintainability for I&C is the characteristics of design, installation and operation that allows structures, systems and components (SSCs) to be kept within their performance limits or to be restored to their performance limit envelop within an acceptable amount of time. Maintainability includes ease of surveillance and ease of replacement or repair.

Upadhyaya et al. [18] report that: “For reliable and economic long-term operation of Small Modular Reactors (SMR), it is imperative that continuous in-situ monitoring of critical equipment must be developed and incorporated in the reactor design phase.” Design specific issues include the following (several of which are highlighted in Ref. [19]):

(a) Extended fuel life will increase the time between maintenance and surveillance opportunities. Therefore, there is a need for reliable monitoring of critical component status and health during operation. This is commonly termed on-line monitoring (OLM) because the components are monitored while the reactor is in service.

(b) The desire for fault tolerance is extremely important, in particular for export reactors for which the infrastructure of the receiving country might not be as advanced as current nuclear countries. Fault tolerance commonly requires a fault detection and identification system, which is used to supplement fault tolerance designed into the systems.

(c) Remote deployment might use semi-autonomous operations that would require reliable knowledge of the plant condition both to make control decisions and to intervene off-site.

(d) Economics will also drive the use of advanced condition monitoring and health determination methods. A reduced maintenance force will need to rely on enhanced condition monitoring information to improve safety and reliability.

(e) New plant types, components, I&C technologies and operations (such as deep load following) can also benefit from enhanced condition monitoring.

(f) Some components, such as internal components in integral primary system designs, might not be accessible for conventional monitoring and maintenance practices, so automated OLM methods might be necessary.

United States Department of Energy (DOE) workshops on OLM and SMRs [20] further emphasize the need for the development of continuous, non-invasive approaches for reactor surveillance. Upadhyaya et al. [18] report that:

> "These technologies contribute to smart condition-based maintenance, reduced human resources, remote monitoring of reactor components, and autonomous operation. In SMR designs, the pressure vessel incorporates most of the critical equipment used for power generation. Examples of such plant components include: motors, coolant circulation pumps, motor-operated valves, control rod drive mechanisms (CRDM), in-core instrumentation, and reactor internal structures."

2.7.1. Extended operation cycles

An extended operation cycle (intervals between refuelling outages) can increase capacity factors for a facility while allowing more flexibility around scheduling for planned maintenance outages. As a result, several SMR developers are looking to ensure extended operation cycles are possible by designing core configurations to utilize slower fuel burnup in lower power densities. However, extending the operation cycle creates challenges for I&C systems by increasing the time between inspection and maintenance outages. This is particularly important for sensing devices and actuators that have to perform to specification over an extended period of time in very harsh environments, in which in situ devices are exposed to aggressive degradation mechanisms. Degradation of sensors and actuators can result in unintended, or even unsafe, control system behaviour. For example, flow and temperature probes used in lead and lead–bismuth designs can be exposured to very aggressive corrosion and erosion mechanisms.

Supporting extended operation with longer periods between inspection and maintenance requires effective surveillance, diagnostics and prognostics (SDP) for condition monitoring and health determination. Confirmation of component health through in situ condition assessment can serve to justify extended inspection and calibration intervals without the imposition of operational restrictions (e.g. higher safety margins). In addition, condition monitoring and health determination can provide the basis for early identification and management of equipment degradation, even to the point of incipient failure detection. However, the effectiveness of condition monitoring techniques, especially quantifiying uncertainty, needs to be demonstrated to ensure the efficacy of such methods.

The reliability models for I&C systems support claims of safe operation and provide information for the safety analysis process, and they will need to present suitable demonstrations that degradation mechanisms are well understood and that materials used for in situ devices perform with high confidence (commensurate with the safety importance of the device) between maintenance intervals. It is likely that these demonstrations will include evidence of suitable materials testing under experimental conditions in which such data do not already exist. For actuators that remain in a static condition, without being exercised, for long periods of time, designers and operators need to consider periodic testing under actual operating conditions to demonstrate reliability criteria are being met.

2.7.2. Cost effective maintenance and asset management

The implementation of SMRs in remote locations or in newcomer countries where the nuclear power infrastructure and indigenous technical expertise are limited (or developing) will increase the importance of optimized maintenance and effective asset management to utilize available resources most efficiently. Unlike a large scale nuclear power plants, where a sizable maintenance staff and periodic preventive maintenance approach are economically sustainable given the significant power output, SMR plants need to optimize their staffing demands and to perform maintenance activities more closely to an 'as needed basis' to achieve competitive O&M costs. Specifically, condition assessment can support identification and characterization of degradation (e.g. fouling, drift, mechanical wear and relaxation of restraints), and health determination can enable management of performance and scheduling of mitigative action. Thus, the maintenance burden can be more effectively managed by only performing required actions and by predicting better when they should be scheduled. SDP enable condition monitoring and health determination of SSCs, both for active assets (e.g. pumps, valves and turbines) and passive assets (e.g. reactor internals, heat exchangers, steam generators, vessels and piping).

An aspect of maintenance and asset management of greater significance for many SMR designs is the need to monitor the condition of inaccessible components (such as steam generators or internal rod drives for integral or pool type designs). If such equipment cannot be monitored in situ or on-line, it might have to be inspected manually at regular intervals. This would incur higher costs, lead to more frequent and longer outages, require more on-site staff, and likely increase the level of exposure for plant personnel. The harsh in-vessel environment and potentially complex configurations might require new measurement capabilities for on-line and in situ monitoring, and new development in advanced diagnostic and prognostic techniques.

2.8. ECONOMIC CONSIDERATIONS AFFECTING I&C USAGE

I&C technology can contribute to the economic competitiveness of SMRs through its impact on upfront capital costs for plant implementation and its effect on the day to day costs of plant management [6]. Clearly, any economic considerations have to be balanced against the need to ensure safety. The upfront cost contribution is primarily dependent on the number and complexity of I&C systems and components to be designed, implemented, licensed and installed. While inherent response behaviour and passive safety characteristics can reduce the requirements for active controls and protection, I&C systems do not generally scale with size. Clayton and Wood [6] report that therefore:

> "Although costs associated with I&C systems are typically not a significant contributor to capital expenses for nuclear power plants [e.g. in the order of 5%], they may constitute a proportionally larger fraction of capital costs for SMRs [e.g. 15–20%]. Essentially, costs for sensors, cable runs, controls and interface equipment may not be as sensitive to savings resulting from reduced unit size, especially if multi-modular plants require independent, dedicated control rooms for each unit. Thus, there is benefit to ensuring that more highly integrated system architectures utilizing modern technologies are employed. Traditional I&C architectures were based on segregated or 'stove-piped' systems and required extensive cable runs….
>
> "The greatest capital cost contribution from I&C systems arises from cable installation."

System architectures for modernization of existing plants and current designs for new plants involve greater integration and more common communication interconnections (e.g. shared wires through multiplexing or networking). Adoption of wireless communication and local powering of instruments can increase the cost savings for equipment and installation through reduced signal and power cable requirements.

As discussed in Ref. [6], the most significant, controllable, day to day cost for a nuclear power plant is plant management. This cost element greatly depends on staffing size and plant availability, and the primary contributor involves O&M activities.

The reduced upfront costs and potential for expedited construction time for an SMR are clearly attractive as a manageable investment compared to a large nuclear power unit. However, the capital requirements remain substantial compared to other power sources such as natural gas or renewable energy. Consequently, SMRs will need to achieve cost effective plant management to ensure economic competeviteness: the value of building an SMR is compromised if the O&M costs per MW(e) are substantially higher than a large nuclear power plant. Therefore, efficient, effective operational approaches and strategic maintenance are necessary to ensure economic competitiveness.

Since I&C technologies provide the foundation for what is the equivalent of the central nervous system of a nuclear power plant, the I&C architecture and its constituent systems can have a significant role in controlling O&M costs through its impact on plant availability, efficiency of power conversion, and staffing requirements. Clayton and Wood [6] report that:

> "For example, the operation of a nuclear power plant is labor intensive. The O&M staff at a plant consists of operator teams for each shift at each unit and the maintenance staff can involve a large number of technicians and specialists. The current industry average for O&M staff is roughly one person per every two megawatts of generated power. SMR designs must be able to meet or improve on this ratio to be cost competitive, independent of the number of reactor modules needed to achieve a comparable power output. Meanwhile, the maintenance staff requirements for an individual reactor module may decrease due to a simplified design but the volume of work might increase as the number of systems to be serviced increase proportionally

> with the number of units on site. Additionally, the workload could also be affected by an increase in the percentage of time each year spent with one or more units at the plant in outage as multi-modules rotate refueling. New advances in I&C capabilities provide the possibility of much deeper knowledge of the status and condition of a nuclear power plant, which can be exploited to improve the effectiveness and efficiency of plant personnel. The industry success over the past couple of decades in reducing plant O&M staffing levels by roughly a factor of four is primarily the result of lessons learned coupled with improved I&C technology and functionality. Continued improvement in I&C systems and applications, coupled with the operational characteristics of SMR designs, can support further enhancements in O&M performance.
>
> "Ensuring high availability depends on avoiding unnecessary plant or unit trips and minimizing the outage time for refueling and maintenance. The first condition is supported by highly reliable automated control systems that are fault tolerant and sufficiently robust to handle an extensive range of plant transients. For highly automated intelligent control systems, the robustness that can be achieved may include anticipating (and avoiding) accident conditions and responding to off-normal or degraded conditions (e.g., plant component degradation or failure) through power runbacks and adjustments in control goals or methods. The former characteristic requires a detailed understanding of the dynamic behavior of the SMR, the availability of diagnostic information on the plant state, and robust control capabilities that integrate the knowledge of plant state with decision driven intelligent control. The latter characteristic also requires state knowledge as well as condition information for components and equipment to enable robust supervisory control that can respond to events and conditions by adjusting demands and/or adapting the control strategy.
>
> "Plant availability is also influenced by fuel cycle demands. Most SMR designs promote extended refueling intervals. The LWR-based designs typically anticipate 3–4 year cycles by eliminating the mid-cycle shuffling of fuel assemblies. More advanced concepts with high conversion ratio designs anticipate core lifetimes of 20–30 years. In those cases, the outage frequency will be driven by inspection and maintenance needs. Thus, there is a need to have a well-founded understanding of the condition of plant components and equipment and a basis for detecting incipient failure (to avoid scrams and unplanned outages). Minimizing maintenance demands can be facilitated by intelligent integrated I&C systems that support plant-wide diagnostics and prognostics. In addition to improving plant availability, optimized maintenance also has the prospective benefit of reducing staff demands so that staff reduction goals for SMRs can be achieved.
>
> "Automated, intelligent control can contribute to improved efficiency of power production by ensuring that control actions closely and rapidly track load demands. Additionally, improved knowledge of plant state can be facilitated through highly reliable, accurate sensors and possibly innovative measurement techniques (e.g., more direct measurement of key parameters, drift free first principle measurements, analytic measurement based on data fusion). With improved state knowledge and tighter control, operating margins can be reduced and more power can be generated."

2.9. REGULATORY CONSIDERATIONS

All of the issues discussed in this publication have regulatory significance for the installation and operation of SMRs; of which some can become regulatory 'show stoppers', which need to be resolved prior to deployment. Experts strongly recommend early engagement (i.e. prior to licensing or certification) to avoid later delays.

Many regulators have been proactive in looking ahead to review and licensing challenges associated with SMRs. For example, the United States Nuclear Regulatory Commission (NRC) has identified several potential policy, licensing and key technical issues in its notices and staff interactions (see Section 3) [21]:

- Use of probabilistic risk (safety) assessment in licensing SMRs;
- Implementation of the defence in depth philosophy for advanced reactors;
- Appropriate requirements for operator staffing for small or multi-unit facilities;
- Operational programmes for small or multi-unit facilities;
- Installation of reactor modules during operation for multi-units;

— Industrial facilities using nuclear generated process heat;
— Security and safeguards requirements for SMRs;
— Off-site emergency planning requirements for SMRs.

Not all Member States have a licensing or certification process for SSC areas such as I&C platforms or systems. However, licensing I&C systems for SMRs will necessarily involve understanding and adaptating to various regulatory regimes among the potential international user base.

In many countries, existing regulatory requirements for SMRs were either written with specific reactor technologies in mind (narrow scope regulations) or were never designed to deal with significant changes to technological approaches. Because all SMRs introduce a number of novel approaches to regulatory discussions, this would result in challenges during regulatory reviews of licensing safety cases. This is particularly true for regulatory guidance, codes and standards, and review guidance for regulatory staff. While fundamental safety principles should be applicable to SMRs, the exact methods used to demonstrate adherence to those principles might not be formally established at each regulatory body, especially for SMRs based on less commercially used technologies such as liquid metal or high temperature gas.

Early interaction with regulators will be important to identify areas that may challenge SMR review and licensing. The timelines required for necessary (or desired) changes in regulations can vary greatly depending on the State owing to variations in the legal structures for regulation. The governing legislation for nuclear regulation in many countries might not recognize SMRs as a different category of reactor, so desired flexibility for special attributes of SMR designs can rely upon the nature of existing requirements (i.e. prescriptive versus risk informed or performance based).

Many countries have regulatory mechanisms in place for a proponent to apply risk informed insights when addressing regulatory requirements. These risk informed insights are used to develop technical and regulatory cases (via a graded approach) that demonstrate that the intent of regulatory requirements have been addressed in the design. The intent is to ensure that the mitigation measures put in place are for the potential consequences of accidents and malfunctions. In some regulatory jurisdictions, for example, demonstrated inherent stability of the core under all operating conditions might be used to support a case for a single shutdown system. These conclusions will need to be supported with suitable evidence such as results from validated codes or results from quality assured research and testing. For I&C architectures, risk informed design becomes more challenging, for example when considering sharing of signals under new operating models or developing control software.

Although this publication examines a number of important I&C issues, it does not provide significant insights on how these issues are being resolved with real world engineering efforts. With vendors and engineers under significant pressure to maintain control over intellectual property, technology developers are naturally hesitant to share insights on solutions to these technology problems. From a regulatory perspective, this introduces challenges as the final solutions to key issues cannot be discussed or debated until either the certification or licensing review, and this means the risk of delays during licensing increases significantly. This point further underscores the need for early and more transparent prelicensing engagement with regulatory bodies.

3. DISTINCTIVE I&C FEATURES AND ISSUES

This section expands on the generic issues discussed in Section 2. It is structured to consider the following key subject areas important to those who design, operate and maintain I&C SSCs for these types of facility:

(a) Approach to design: Section 3.1 explores how design needs to be conducted to integrate I&C technology effectively into the overall plant design.
(b) I&C architecture, technology and equipment: Section 3.2 discusses specific design considerations, features and technologies and their implications to SMRs.
(c) Fabrication and site integration: Section 3.3 examines issues around design and testing of modules.

(d) Concepts important for operation: Section 3.4 describes the environment in which SMRs will likely operate and the issues associated.

(e) Maintenance: Section 3.5 focuses on key maintenance issues and technologies available to address them.

3.1. APPROACH TO DESIGN

3.1.1. Following a systematic systems engineering approach

I&C approaches used for traditional nuclear power plant designs might not be scalable to SMRs because operating characteristics can differ substantially. Hence, there needs to be increased emphasis on SMR vendors to perform and document proficient systems engineering and analysis during the design process. A good example of a systematic lifecycle approach to I&C system design is described in ISO/IEC 15288:2008, Systems and Software Engineering: System Life Cycle Processes [22]:

> "This International Standard concerns those systems that are man-made and may be configured with one or more of the following: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials and naturally occurring entities.
>
> "When a system element is software, the software life cycle processes documented in ISO/IEC 12207:2008 [23] may be used to implement that system element.
>
> …….
>
> "This International Standard applies to the full life cycle of systems, including conception, development, production, utilization, support and retirement of systems…
>
> …….
>
> It also applies to a complete stand-alone system [such as I&C systems for SMRs] and to systems that are embedded and integrated into larger more complex and complete systems."

A system engineering approach needs to include the systems involved in the end use of the design (e.g. systems for electricity generation, steam for industrial processes, and desalination) because they might impact design, operation and maintenance of I&C systems that control and protect the reactor. Early interaction of I&C design staff with other design disciplines in the SMR design process can optimize I&C systems under various operating states. In addition, early identification and documentation of interface requirements and interface design details between I&C systems and other reactor systems can minimize challenges often experienced during integration of systems. Developing an early understanding of these interfaces can facilitate a valuable understanding of the intersystem behaviours.

One of the areas that may be underexplored by commonly used analyses is examination of intersystem behaviour, including I&C system interfaces. Although many analysis techniques examine systems failures and their effects on plant status, erratic and undesirable systems behaviours and their effects on connected systems and ability to create transient conditions in the facility might not be thoroughly analysed. Traditional analysis techniques need continue to be used to assist in understanding reactor behaviour. However, additional architectural analyses may be necessary to understand intersystem interactions. The NRC reports that (*footnote omitted*) [24]:

> "A hazard analysis (HA) is a process for examining an instrumentation and control (I&C) system throughout its development life cycle to identify hazards (i.e., factors and causes), and I&C requirements and constraints to eliminate, prevent, or control those hazards. HAs examine safety-related I&C systems, subsystems, and components and their interrelationships and their interactions with other systems, subsystems, and components to identify unintended or unwanted I&C system operation including the impairment or loss of the ability to perform a safety function.

> "…Experience with complex systems in general and with digital systems for critical functions in diverse application sectors in particular…has revealed that current hazard analysis techniques such as fault tree analysis (FTA) and failure modes and effects analysis (FMEA), by themselves, do not assure the discovery of (or absence of) system-internal hazards rooted in system development activities. In contrast, a hazard analysis should facilitate a more focused I&C system review and should help to ensure traceability among regulatory requirements, architectural considerations, and system requirements to enable a more effective, and efficient I&C licensing review."

An SMR vendor needs to produce documentation sufficient to demonstrate that hazards of concern have been identified, as well as the system requirements and constraints to eliminate, prevent or mitigate them. These system requirements and constraints should ideally assist a technical assessor in confirming that the hardware and software for I&C architecture are robust against postulated events, system failures and undesirable behaviours. Systems engineering and analysis documentation produced as a result of this effort needs to support compliance with regulatory requirements for I&C systems. Some specific examples of interfaces between I&C and various reactor systems (and reactor support systems) are provided in the Annex.

3.1.1.1. Balancing reliability, simplicity and situational knowledge

As depicted in Fig. 1, design of an overall I&C architecture involves a carefully planned balance of three key areas coupled with an effective human factors engineering (HFE) programme plan developed at the earliest stages of the design activities.

One of the key design goals of SMR vendors (as requested by utilities) is to seek, via design, a reduction in O&M costs by minimizing the necessary staff complement needed to operate and maintain the facility. Reducing the complement of field operators and maintainers means that plant operators and maintenance support staff will need greater plant situational information to make the necessary operational and maintenance decisions. This can be achieved by building a greater degree of automation into the overall plant architecture. To accomplish this, plant I&C systems will need extra equipment (e.g. sensors, transmitters, actuators and processing systems) to perform the tasks that staff have traditionally performed.

Arguably, the most reliable I&C system are designed simply: more automation increases the complexity and thereby introduces the potential for new failure modes. Some of these might not be easy to detect or analyse in

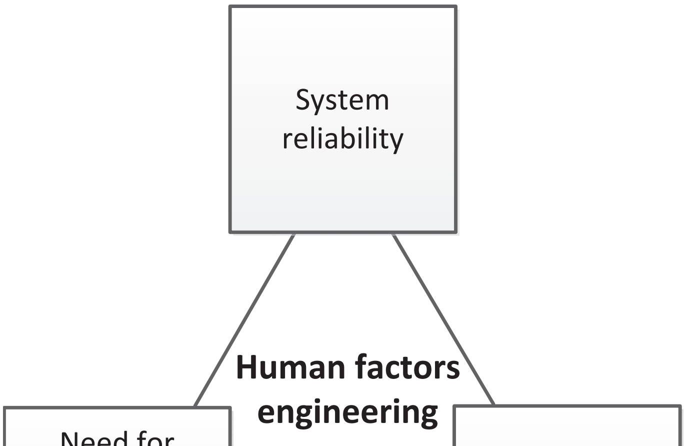

System reliability
Human factors engineering
Need for operator and maintainer situational information
Simplicity

FIG. 1. Optimization through human factors engineering.

safety analysis. Reduced reliability of key plant systems not only impacts plant availability but also affects the safety analysis, which in turn affects the plant safety case (i.e. increased regulatory impact).

As a result, the introduction of automation to reduce the need for plant staff should not be considered only from a plant O&M cost perspective. Rather, automation needs to be considered as part of an overall plant and system reliability programme that considers costs and burden on safety analysis work, and ensures reliability is maximized. In the extreme case of very low power SMR concepts being proposed for remote regions, some vendors believe that on-site O&M staff are not necessary. Although this is technologically feasible, it will likely face public opposition. The plant I&C architecture would need to be extremely robust and reliable, particularly when access to remote monitoring and control of the facility is cut off for period of time.

3.1.1.2. Using systems engineering to plan locations of equipment

More automation means an increased use of sensors and actuators (including integrated electronics) in field locations to gather the necessary information to promote situational awareness and to provide necessary control feedback. With hundreds of process variables available for measurement in a nuclear power system, the selection of optimum sensor locations poses a unique problem [25]. Li [26] reports that:

> "Sensor placement design is a critical component of a fault diagnostic system…. Whenever a process encounters a fault, the effect of the fault is propagated to some or all the process variables. The main objective of fault diagnosis is to observe these fault symptoms and determine the root causes of observed behavior. The ability of the sensor network to detect and discriminate failure modes and anomalous conditions is crucial for the efficiency of the fault diagnostic system."

Given the size constraints and extreme environments of many SMR concepts, the design of an efficient equipment placement strategy will assist in the quick and accurate identification of equipment and process faults. Li [26] continues:

> "The solution to the problem of sensor placement may be broadly broken down into two tasks: (1) fault modeling or prediction of cause–effect behavior of the system, generating a set of variables that are affected whenever a fault occurs, and (2) use of the generated sets to identify sensor locations based on various design criteria…. The fault propagation or cause–effect behavior is derived on the basis of a qualitative model that is used to represent the process."

As a result, it is very important that a systems engineering approach to design be used to optimize the placement of instruments and I&C hardware. This approach can then be used when deciding on alternative design approaches for I&C placement to cope with harsh conditions and space restrictions, such as:

- Reducing component size;
- Designing a longer component life span;
- Using multifunction components where appropriate and permissible;
- Using a type of component that can be placed in a different location.

The systems engineering approach also has to consider inspection and maintenance tasks because space constraints can adversely affect their execution, resulting in increased failures. Space constraints can require new inspection and maintenance tools to be developed.

3.1.1.3. Ensuring I&C component performance under degraded conditions in challenging environments

A systems engineering approach to design becomes more critical for I&C systems being proposed for SMRs because of the expected conditions in which the components will function. The goal of designers is to predict, understand and mitigate the effects of degradation of I&C systems and components to ensure safe operation and stable performance can be achieved over long periods of time with minimal to no maintenance.

I&C components (e.g. sensors, transmitters and actuators), in particular for systems important to safety, are expected to perform to a high degree of reliability under all operating conditions, harsh environments (e.g. high pressure, high temperature, high radiation, corrosive and erosive, and chemical deposition) which can arise during accidents. It is also important to consider that SMR proponents are consciously planning designs that have longer intervals between outages. Although all I&C components degrade over time, they should maintain functionality and take into account degraded accuracy.

Where component locations become restricted, difficult to access or subject to harsh conditions, which is the case for many SMR concepts, there is a need to predict the performance of the components to ensure adequate lifetime performance in the absence of maintenance. This is particularly important for components which have moving parts (e.g. relays, valves and pressure transmitters) or chemical based actuators (e.g. a small explosive charge in a squib valve).

Type testing is an approach that can be used in concert with a systems engineering approach. In a type test, a representative sample of equipment is be subjected to a series of tests, simulating the effects of significant ageing mechanisms during normal operation and subsequently subjected to design basis event testing that simulates the installed equipment service and expected environments. A successful type test demonstrates that the equipment can perform the intended safety function(s) for the required operating time before, during, and/or following the design basis event, as appropriate. The results of type testing of multiple components in a system can be used to predict overall system behaviours and characteristics.

3.1.1.4. Tools to support I&C design

Design and verification tools are key in confidence building for both software and hardware based I&C systems. As a minimum, tools should be able to model best estimate plant response as well as providing design basis modelling when they are used for both design basis calculations and operator interface modelling. New I&C approaches for SMRs will need to be supported by models and tools that are properly verified and validated. When using existing models and tools, both the tools and associated uncertainties need to be evaluated for any discrepancies between the traditional understanding of nuclear power plant I&C behaviours and those for SMR design concepts. For example, different core and primary system configurations lead to different plant behaviours, which could result in a specific tool being rendered invalid.

Plans for verification and validation of tools need to be part of the systems engineering approach to design. The plans also need to include any test facilities required to support verification and validation. In many cases, SMR concepts are novel enough that extensive test facilities and mock-ups need to be established very early in the design process. Plans for software verification and validation need to meet applicable criteria, for example such as those found in Institute of Electrical and Electronics Engineers (IEEE) and International Electrotechnical Commission (IEC) standards (see the discussion in Ref. [27], which should be fully applicable to SMRs).

Verification and validation records need to be maintained for the lifetime of each specific I&C system because these records provide evidence that all planned activities have been performed, results recorded, and anomalies investigated and resolved. This evidence supports the safety case of each facility. If necessary, the records can also be made available to third parties for audit and review. Records need to demonstrate clearly the traceability of all verification and validation work to the relevant source documentation.

3.1.2. Design of control rooms

Some SMR designers propose operating models that either have multiple units or modules in a facility sharing a common control room or one operator (or operational team) supervising multiple modules simultaneously. HFE will most likely dominate the safety discussion of these proposals. As a result, human system interaction and human factors will be key considerations in I&C systems design of multi-unit SMR plants.

Many industries already provide excellent guidance and frameworks for defining system functionalities based on operational requirements and human factors. SMR designers are exploring how these guidelines can be used for nuclear power applications. In addition, various organizations have developed guidelines to support the design of nuclear plant control rooms and digital human system interfaces. These guidelines provide the technical bases for meeting plant safety and operational requirements, improving cost effective plant and human performance, and reducing the likelihood of human errors. For multi-unit SMR plants, the control room and workstation are technically and financially important, and require extensive R&D. There is ongoing effort in design, analysis and simulation of control rooms and workstations for multi-unit SMR plants, with the goal of optimizing operational costs while meeting plant safety requirements.

Design considerations include the integration of automation addressing multiple units, new information systems, new operating procedures and any other aspect that changes the human–system interaction. Control room and workstation layouts and alarm management are two very important human factor features of an I&C system design for a multi-unit nuclear power plant. Alarm management in a multi-unit control room can be more complicated from a human factors perspective and can face significant challenges — not only alarms caused by each unit itself but also alarms caused by other units. An effective alarm management strategy will significantly enhance the operator's ability to reduce the consequence of an emerging abnormal occurrence.

Multi-unit control rooms for multiple reactor facilities already exist for large scale generating stations. For example, Fig. 2 depicts a four unit MCR at a four unit Canada deuterium–uranium (CANDU) facility. There is already a precedent for the safe operation of multiple units out of one control centre, and it should be noted that secondary control areas are not in shared facilities.

Factors that lead to successful and safe plant operation under multi-unit MCRs include the following:

(1) The MCR minimum complement is captured and documented in the safety case of the facility for all operating conditions and must be met as a licence condition. The minimum complement is subject to regulatory oversight. Compliance activities by the regulator look for documented evidence of the minimum complement in the safety case through areas such as safety analysis, licensee's review of organizational performance and review of events.

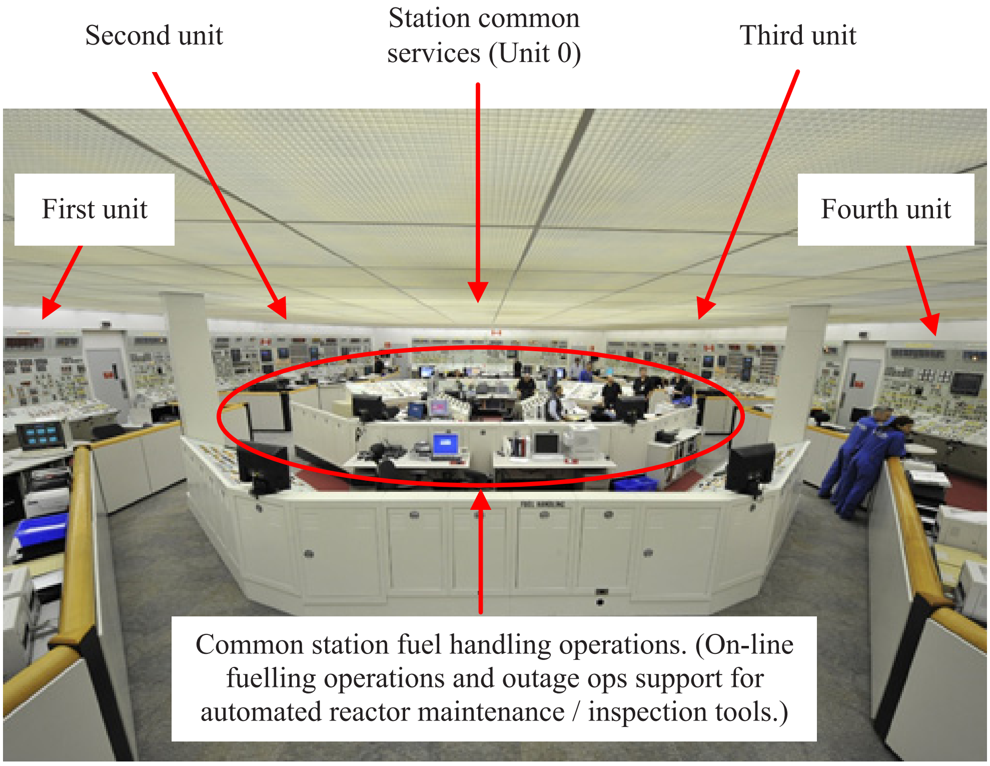

Second unit
Station common services (Unit 0)
Third unit
First unit
Fourth unit
Common station fuel handling operations. (On-line fuelling operations and outage ops support for automated reactor maintenance / inspection tools.)

FIG. 2. CANDU four unit main control room.

(2) The strong conduct of an operations programme[4] that controls not only access to the MCR by plant personnel but also the behaviour of staff in the MCR:
   (i) All work control activities (including managing work protection) by plant support and maintenance personnel is managed outside the MCR in a work control area. Access to the unit authorized nuclear operator and supporting MCR is limited to personnel that have specific and direct business with MCR staff (e.g. briefings prior to unit test evolutions). There are enough staff members on all MCR unit panels to permit some qualified MCR operator to assist incident units during an event when requested. These are rehearsed under simulator training exercises.
   (ii) MCR interactions between staff of separate units are minimized unless there is a clear need to communicate relevant interunit interaction information between units. For example, major test evolutions on plant common systems (Unit 0 MCR) might involve specific tasks by individual unit operational staff.
   (iii) Coordinated efforts between units are conducted under a clear and briefed communications protocol.
   (iv) MCR staff and associated field staff are, as a rule, dedicated to a unit in order to prevent operational errors between units (e.g. equipment adjusted on the wrong unit) and to follow differences in unit configurations resulting from maintenance and operational evolutions.

(3) A well maintained plant documentation programme: In a multi-unit facility, documentation is generally unit specific unless it is clearly certain that the configurations are identical across all units.

(4) Strong control of unit by unit and plant wide configuration.

(5) Many systems that support the MCR air (heating, ventilation, air conditioning, fire protection and emergency breathing) need to be designed with a very high reliability target to avoid a station wide event if a major event (e.g. fire and earthquake) were to occur. The safety case of the facility is required to consider the impacts of such MCR events and is required to have mitigation strategies in place in the event of the loss of MCR systems or it becoming uninhabitable. This is partially covered through backup control rooms, additional plant protective systems and associated emergency operating procedures.

In the aftermath of the Fukushima Daiichi accident, nuclear power plant designers are moving back to dedicated unit MCR architectures; however, some SMR designers, such as NuScale, are exploring ways to propose safety cases not only with shared control rooms but even with operational staff monitoring and controlling multiple modules simultaneously. Some reasons for doing this include the following:

(a) Economics: Business models for these types of design cannot generate sufficient revenue from generation to support a large station complement. This is frequently an argument mistakenly put before regulators who have a sole mandate to ensure safe operation rather than economic viability.

(b) Claims that the design will result in significantly simplified operation owing to:
   (i) Very predictable and operator friendly operational characteristics (inherent stability of core, slow event transition time and preclusion of fuel damage in an event);
   (ii) Fewer unit SSCs to be monitored and manipulated during operation;
   (iii) Passive safety system behaviour, leading to significant time before operator intervention;
   (iv) Improved automation;
   (v) Improvements in operator interfaces that increase situational awareness and reduce the need for operator intervention.

HFE R&D will play a very large role in understanding how safe operation under a multiple and shared unit operating scenario can be achieved in a safety case. Results of HFE research and analysis are needed to understand and support safety arguments by examining:

- Processes used to optimize not only the numbers of direct operator interfaces, but types of interface used (e.g. which indicators have to be available under which operating conditions). This affects not only the size of

[4] The Institute of Nuclear Power Operations (INPO) and the World Association of Nuclear Operators (WANO) have numerous publications that address important attributes and characteristics of a good conduct of operations and conduct of maintenance programmes.

the MCR systems but also minimizes distracting or superfluous information during specific operational states or transitional states.
- Methods by which an operator can better visualize multiple parameter operating margins in real time to understand where operation is occurring in relation to limiting conditions of operation.
- The effects of multi-unit monitoring and control by an operator (i.e. how to avoid confusions between units).
- The effects of extensive automation on the operator's ability to maintain a strong understanding of unit behaviour.
- The effects of technology on the operator's attention to the plant situation (e.g. boredom leads to complacency).

3.1.3. Using I&C systems to supplement physical protection

Physical protection of the facility and its key systems is already a major part of the I&C design process. One of the main goals being pursued in the design of SMRs is the reduced need for security staffing to ensure physical protection of the facility. Optimized staffing is a significant economic factor in SMR deployment. One of the approaches proposed is the introduction of specific I&C systems to supplement physical protection, which would be used:

(a) To alert the operator and security staff to potential or attempted intrusions (to initiate a physical response);
(b) To initiate protective actions (i.e. locking doors and disabling systems) that deny or delay access to plant systems;
(c) To prevent unauthorized removal of materials from the facility or, in the case of transportable nuclear power plants, unauthorized removal of the facility.

Many of these approaches remain under development and will be subject to regulatory approvals both from a security perspective and from an overall plant safety case perspective. As a result, security and I&C designers will need to collaborate during the design phase to ensure that the use of I&C is consistent with design and regulatory requirements for physical security.

For remote operations, the absence of a traditional complement of on-site personnel might necessitate use of I&C technology to detect security events and to manage the reactor's transition to a defensible and safe state.

3.1.4. Additional I&C considerations for transportable nuclear power plants

The major features of most SMR concepts are the modular design and construction methods, which includes the ability to transport completed modules from the manufacturer to the site. Some SMR concepts go further by proposing to ship a complete, sealed and fully fuelled unit from the factory. Any potential damage or other physical changes that can occur to the module during transport need to be considered. This is important for not only fragile I&C systems, such as flux detectors and relay systems, but also modern solid state devices if they have not been designed with transport conditions in mind, such as:

- Shocks and vibrations;
- Extreme temperatures, changes in temperatures and humidity effects (including potential for corrosion);
- Effects from static, external electromagnetic interference and radio frequency interference;
- Pressure effects (with changes in elevation).

Designers need to understand the possible bounding environmental conditions that could occur during transport and which often depend on the location, climate and the methods of transport. Any damage that occurs during transit needs to be anticipated, as on-site repair of a sealed module might not be possible. Designers thus need to focus on preventing damage. In addition, methods and tools for evaluating the condition of the equipment need to be developed for both pre- and post-delivery to test any effects of transport.

3.1.5. Codes and standards

The current suite of codes and standards might be sufficient for design and regulation of certain types of SMR, but this can only be determined on a case by case basis. Any gaps in the codes and standards can increase regulatory uncertainty. Therefore, SMR proponents seeking significant departure from existing standards need to consider pursuing SMR specific (or even technology specific or design specific) codes and standards.

There is a strong interest by industry to pursue harmonized codes and standards for SMRs, in particular to facilitate export throughout the world. However, this is a long term goal that will require significant international collaboration and consensus.

3.1.6. Role of simulators in design, verification and validation

The development of control strategies represents a crucial part of the design process, since the nuclear reactor is a part of an integrated plant to be connected to the grid. Design specific system behaviour can mean that any historical experience or operational data may either be unavailable or need to be proven relevant. As a result, a number of SMR designers integrate engineering and operational training simulators into the overall design process, including the design of the I&C architecture. This is driven by the need to acquire sufficient knowledge of the new systems. Once the system dynamic behaviours are understood more clearly, the design process then feeds engineering data back into the simulator in an iterative fashion to further enhance the design. HFE can also be performed parallel to these activities, leading to a more useful I&C architecture. This process can run several iterations before the final design. Some SMR concepts propose multi-unit operation and control room configurations. Simulator systems help designers to understand the human interface with I&C equipment and to optimize the systems to reduce human error.

By using simulators in the design process, both commissioning and early operation of first of a kind plants benefit from operators having a very strong understanding of the I&C design's performance characteristics and mechanical system behaviour.

3.2. I&C ARCHITECTURE, TECHNOLOGY AND EQUIPMENT

There are international activities to formalize a common understanding of safety design principles. For example, the Multinational Design Evaluation Programme (MDEP), a cooperative effort of a group of nuclear regulators with a common interest in the same new reactor technologies, includes activities to explore generic regulatory issues for specific nuclear power plant technologies. A working group within the programme has reached a consensus with regard to the overall I&C architecture of a plant (i.e. the organization of I&C systems important to safety). This common position [28] addresses the safety design principles and supporting information with regard to the overall I&C architecture for the demonstration of safety. It outlines the following key principles to be considered in the design and implementation of I&C components and systems:

- Defence in depth;
- Consideration of common cause failures;
- Independence;
- Diversity;
- Compliance of safety groups with the single failure criterion;
- Reliability;
- Complexity.

Although the common position [28] was expressly written with large nuclear power plant designs in mind, the principles can be applied to SMRs and research reactors and by regulators in their regulatory frameworks.

3.2.1. Simplification as an architectural goal

The methods and processes used to design I&C architecture for SMRs are fundamentally the same as those used for larger plants. I&C architecture is likely to adopt distributed control system concepts similar to those used for modern large nuclear power plants. A possible exception is for very low power SMRs (i.e. stationary or transportable designs, 10–25 MW(e)), which might employ a central computer system model. In this case, control of the nuclear island systems would be combined with the distributed control systems from other modules attached to the nuclear island (e.g. packaged turbine generator and secondary steam control systems). The reason for this possible re-centralization of computer functions stems from the compact size of proposed designs, where distances between sensors, actuators and processors are very small. In addition, this centralized system allows for a simpler and more easily defensible connection to a remote monitoring and control centre.

The NRC addresses the concept of simplicity in design specific review standards for SMRs. Simplicity of design seeks to maximize reliability of systems, which contributes to overall plant safety. Simplicity also reduces the effort needed to predict failure modes and related postulated initiating events, thereby reducing the complexity of both safety analysis and human factor assessments.

3.2.2. Architectural models for controlling reactors and balance of plant

3.2.2.1. Multi-unit control strategies

There are three architectural models representative of concepts under consideration for SMR facilities (see Fig. 3):

(a) Traditional model: An MCR controls a single nuclear steam supply system (NSSS) to a single secondary side system (e.g. turbine and process steam plant). This model is used by most existing facilities.

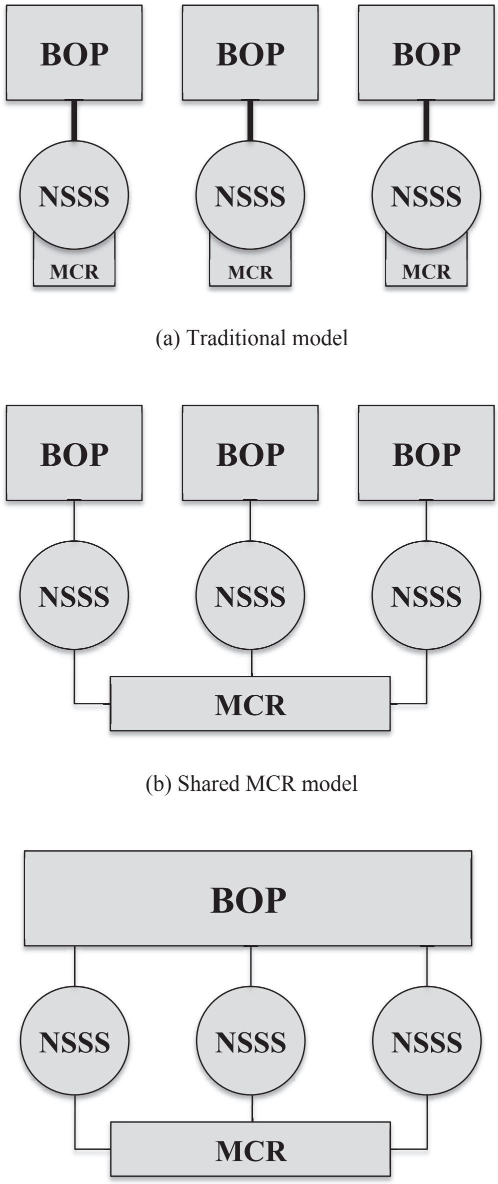
(b) Shared MCR model: A multi-unit MCR, with each unit controlled from a single independent I&C system. This model is used in Canadian multi-unit plants.

(c) Shared MCR and BOP model: A multi-unit MCR with each NSSS unit controlled from a single, independent I&C system but each interfaced with a common BOP I&C system. This model is currently not used; however, it is being proposed for some SMRs, such as the Chinese HTR–PM, which will connect two or more NSSS systems to a single turbine and steam plant.

This section focuses on the shared MCR and BOP models (see Section 3.1.2 for information on the traditional MCR model). Sharing BOP systems provides significant benefits, both in terms of capital cost and personnel utilization because these systems are not associated with a single reactor unit. With such a configuration, there is a strong coupling between the multiple SMR units and the BOP which, when presented with unbalanced load operation, can affect safe, smooth and steady operation of the reactors. In order to reduce the strong coupling between the multiple SMR units by the multi-use and unbalanced load operation, an advanced coordinated control strategy is needed. Some possible new coordinated control strategies are being studied and include the use of decoupling control, optimum control, non-linear adaptive control and intelligent control methods. All approaches seek to obtain better control performance of multi-unit SMR plants. Whichever approach is used, a new, integrated I&C system needs to be developed to mitigate effects on the reactor while providing stable control of the BOP under changing loads.

An important aspect when implementing such an architectural model is the need to leverage the capabilities of modern integrated I&C systems to ensure that operators have timely information about plant status in a concise and organized fashion, and can quickly and easily issue commands. These systems also make it possible to fulfil the data availability expectations of the new generation of power plants, such as supplying real time performance information to the owner, and ensuring that remote emergency response centres have access to plant status data in real time.

When considering a multi-layered I&C system architecture of multi-unit SMR plants, there will be commonalities between BOP systems and reactor systems at some levels. However, systems important to safety will generally remain independent and unit specific. When developing common system architectures via this



(a) Traditional model

(b) Shared MCR model

(c) Shared MCR and BOP model

Note: BOP — balance of plant; MCR — main control room; NSSS — nuclear steam supply system.

FIG. 3. Three models under consideration for SMR facilities.

novel approach, particular attention will need to be paid to design for computer security[5] provisions. In particular, some additional control layers may need to be made more unidirectional in nature and additional configuration management measures may need to be instituted. A multi-layered I&C system architecture can offer the following advantages:

(a) Each functional layer provides complementary control and monitoring capabilities that assure independent backup of the multi-unit plant operation and protection functions.

[5] Throughout this publication, 'computer security' will be used to cover the security of all computers and all interconnected systems and networks. The terms IT security and cybersecurity are, for the purpose of this publication, considered synonyms of computer security and are not used.

(b) The layered architecture allocates complex data management and display processing to the plant management layer, while making the control and protection systems as simple as possible.

(c) The highly distributed nature of the system network is flexible enough to allow upgrades of system components as additional units are added to the facility (e.g. new module construction).

There are certainly technical challenges to be addressed to ensure a safe and economical design. In particular, the design of the I&C systems of multi-unit SMR plants will need to leverage rigorous engineering methodologies and proven automation technologies to address plant monitoring, control and protection systematically.

3.2.2.2. I&C terminal points in the safety case

Unlike nuclear power plant designs that are primarily designed for electricity generation, many SMR concepts are being developed for non-electrical generation. This can blur the traditional line between the plant systems and the connection to end use (e.g. the switchyard). Other grid scenarios can also impact the terminal point for I&C architecture. The SMR designer needs to use a system engineering approach to understand and document clearly I&C terminal point boundaries in the safety case, based on insights from signal analysis, understanding of devices being used, safety analysis and safety classification work. Examples of different architectural scenarios are discussed below.

The generation of high quality process steam for industrial processes is one of the main potential uses of SMRs — in some cases even allowing for parallel electrical generation (e.g. cogeneration, see Fig. 4).

Cogeneration is quite common and has generally been a strategy used for fossil fired plants, which have been able to interface well with secondary uses because many of the codes and standards are shared between the facility producing the steam and the facility using it. With a nuclear facility, licensing requires the development and maintenance of a more formally documented safety case. The safety case will show that a systematic safety analysis programme is in place to assist in demonstrating that safety requirements will be met when the facility is operated. Insights of safety analysis, whether deterministic or probabilistic, influence the safety classification (and associated code classification) of nuclear plant systems, particularly for systems important to the ultimate safety of the plant.

It is important for the designer to understand where the safety case of the nuclear facility ends (i.e. terminal points of nuclear I&C systems) and how the process side I&C systems interface or influence the nuclear island I&C systems. Terminal points may also exist in the software.

For hard piped systems such as heat transfer interfaces (heat exchangers) between the nuclear island and process side, defining terminal points of the nuclear safety case is relatively straightforward. With I&C systems,

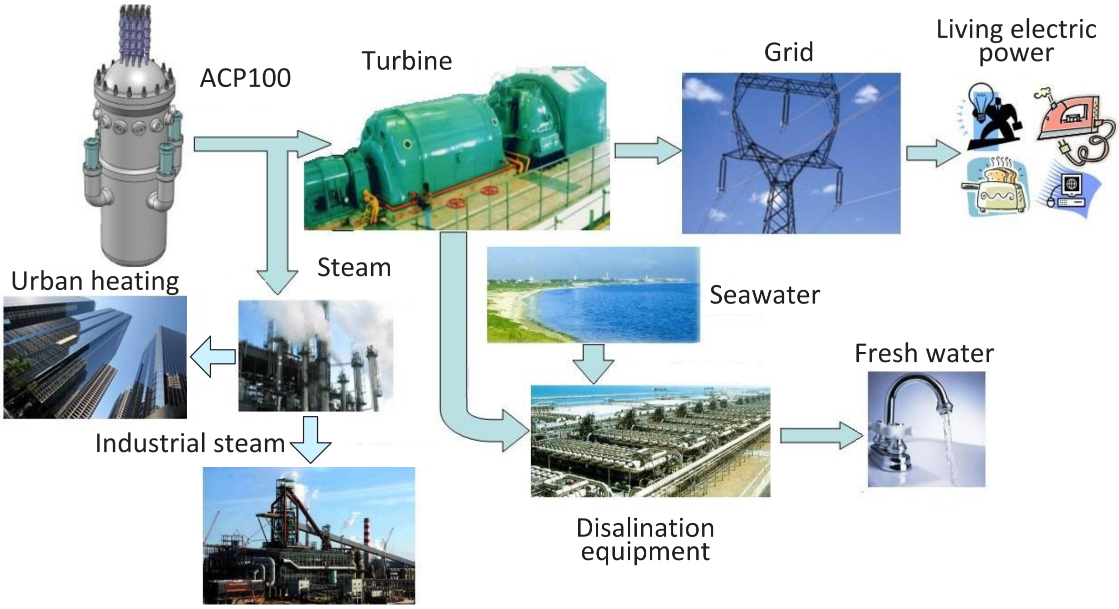


FIG. 4. NPIC/CNNC ACP100 unit (China) used as a cogeneration plant.

however, where process signals or field instrument data need to be fed back to control heat generated by the reactor, these interfaces and how the equipment and signals interact are more complex and safety case boundaries can depend on the system.

For current nuclear power plant arrangements, the terminal points and jurisdiction of the grid operator varies from country to country (and even within states and provinces). When developing the safety case for a facility, the jurisdictional boundaries between the plant systems and the grid operator need to be understood and documented clearly in both plant O&M documents and supporting safety analyses. Grid operators also need to be aware of their jurisdictional boundaries, have their own procedures for detecting and mitigating transients and be able to communicate with the plant operator in real time to share transmission and generation data so that both sides can make informed and coordinated decisions. Some SMR designers might seek to develop and implement software based communication means to automate some of the decision making between the grid and the plant control systems.

Operating scenarios for most SMR based facilities will have the same jurisdictional boundaries as larger nuclear power plants. For some SMR operating scenarios, however, the concept of the grid can be different from what is conventionally understood. For example, smaller SMRs can be built and operated to support an islanded grid such as a mining project in a remote region not connected to a regional grid. In this instance, the grid becomes an extension of the power plant and there is a greater need to understand how grid events can be detected and mitigated by the plant. Existing islanded grids used for industrial processes, such as mines, can experience extreme load swings over short periods of time as major pieces of mining equipment are started or stopped. If not controlled rapidly, these swings can cause damage to BOP systems, which in turn impact reactor operation. Under these conditions, I&C systems for monitoring and controlling the grid will need to be factored into the safety case through safety analysis. This can affect the safety classification used for such devices and control software dependent on the inherent characteristics of the plant systems to mitigate transients. The degree of involvement of the nuclear regulator in grid related discussions is ultimately based on the safety case of the plant.

Where an SMR is used for cogeneration, detection of a transient on the electrical distribution system can trigger a response to divert additional steam to the cogeneration side of the plant to prevent a reactor power transient (maintaining heat sink capabilities). If this mitigation is part of the safety approach for maintaining fuel integrity, the transient detection devices and software will likely need a high level of assurance that it will function to mitigate the transient.

For SMRs designed for pure process support (steam production) and no electricity production, interfaces with customers using steam need to be treated the same as that for the grid. Again, involvement by the nuclear regulator (rather than the involvement of the regulator of the industry receiving the steam) will depend on the safety case of the reactor facility. The safety case is informed by the robustness of the reactor facility to transients from the process steam side.

3.2.2.3. Communications among I&C systems

For most SMR design concepts, issues around communications within an I&C architecture will be more or less the same as those for a modern nuclear power plant. Remotely monitored and operated designs might be an exception, and proposals are being developed to establish wired and wireless communication between the remote MCR and the facility’s autonomous control systems. Communication connections can be accomplished through the following:

- In-plant cables (for internal plant system communication signals);
- Wireless equipment (for internal plant system communication signals where wired connections are impractical)[6];
- Direct long cable for shore connection of a marine based, submersible SMR;
- Radio or acoustic links as an emergency backup system (Flexblue);
- Encrypted satellite communications.

[6] It may be difficult to provide a secure boundary for I&C systems using wireless communications. Wireless communications can suffer from reduced reliability as well as being easy to detect, jam and intercept from beyond the secure boundary. Encryption provides for confidentiality and can support integrity but generally reduces availability.

Communications within the architecture need to be designed with levels of defence in depth that take advantage of diversity and redundancy where necessary to achieve very low unavailability targets or failure rates. This is required to mitigate partial or total loss of communications for either short or long periods of time. Typically, designers propose to address this by increasing the autonomous control intelligence of the architecture, so the plant can maintain or achieve a safe state under a prolonged loss of communication. Of course, this approach also requires the designer of the reactor technology to ensure inherent safety and security features are built into the overall design to permit autonomous control to a very high level of confidence.

3.2.2.4. Remote communication and control

Remote operation and monitoring of complex mission critical systems is gradually becoming commonplace in many industries outside the nuclear sector. Good examples and associated lessons learned can be found in:

- Aerospace (satellites, probes, remote operated aircraft and drones);
- Commercial aviation (fly by wire — remote operation to a lesser degree);
- Large, complex telescopes in remote locations;
- Hydroelectric dam projects;
- Mining equipment;
- Health sciences (telepresence surgical systems).

The general concept is that the operator does not locally control the facility systems but instead issues commands to the controlling computers of the facilities. These computers (which could be part of a distributed computing system) determine whether plant conditions permit the requested command — using sensors (and control logics), which are frequently triplicated for redundancy and defence in depth. This allows for control systems to vote on plant conditions based upon these sensors and to determine whether the conditions allow for the requested control change. However, a human command can override this voting process by using a specific bypass built into the hardware or software.

From a safety perspective, a remote control room is an extension of the on-site plant. The decision to have staff present on-site would be driven by the following:

(a) Public opinion based on safety and security perceptions (acceptance of unstaffed facilities);
(b) Reliability of the on-site control architecture;
(c) Reliability of the communications connection between the remote control room and the site;
(d) Computer security requirements and regulation;
(e) Other on-site O&M needs (i.e. the need to support ongoing operations through maintenance activities).

The key to the successful development of such systems involves extending the HFE programme beyond the analysis of human–machine interfaces and into the analysis of how software is developed and quality assured. Human sensory inputs and behaviour in the field are being replaced by software architecture; hence, human interfaces in software development need to be cognizant of the effects on nuclear safety and the roles of human error in software development. Application of computer security principles to the human interfaces during software development is another important consideration.

Special consideration will need to be paid to computer security incidents that have the potential to adversely impact the safety and security of the facility. The adverse scenarios from worst to best cases are:

- Function is indeterminate.
- Function has unexpected behaviours or actions.
- Function fails.
- Function performs as expected (i.e. fault tolerant).

An example of an incident having limited impact would be the loss of communications between the remotely located control room and the facility's autonomous systems. This incident is normally handled from a safety standpoint. One way to do this is to ensure communications between the control room and operating facility are highly reliable. Long distance communication solutions for such applications would likely need to incorporate many current principles of good I&C design. The communication links would need to consider redundancy, diversity and survivability for the environments in which they would be expected to traverse. In addition, some long distance communication solutions have different communication speeds. The latency that can be relied upon between the remote control room and the reactor would need to be factored into plant design decisions and analyses for which operator awareness and action would be required.

From a safety standpoint, an SMR designer adopting a remote operation concept would need to establish early in the design process the desired system behaviour upon detection of any communication problems. The reactor facility will need to be able to detect the loss of communication and, for many reactor applications, pursuit of an automatic safe shutdown is likely to be the conservative response. A coordinated approach between I&C and other reactor systems would be required to establish the correct path to a safe shutdown and maintenance in a safe shutdown condition, without operator involvement. SMR design also needs to ensure the ability to respond to other irregularities (e.g. corrupted or intermittent messages) in communication from the remote control room. Furthermore, the risk of corrupted or intermittent messages might increase with the use of wireless technology.

From a security standpoint, an SMR designer would need to take into account situations where the function is indeterminate (e.g. complete compromise, remote code execution and defeat devices) or the function has unexpected behaviours or actions (e.g. the control system may be in a non-conforming condition, incapable of performing its design function). These situations do not result in the system failing or becoming unavailable and are generally not covered by the considerations taken for safety. SMRs need to be designed to prevent, detect, and respond to, potential malicious activities that intercept, modify or hijack communication from the remote control room.

Under certain circumstances, immediate shutdown of the reactor in response to a loss of communications with a remote control room might not be desirable. The State's regulatory structure might not support continued operation of a reactor in this fashion (i.e. without operator oversight). Early interaction with a regulator would be necessary to address this. Many parameters would need to be considered: the power of the reactor; the existence of proven passive safety features (i.e. can the reactor reliably shut down by itself or is the shutdown sequence too complex); the ability to re-establish communications; and the consequences of a sudden loss of power to the local community. A computer security analysis can help to ensure that proven passive safety features cannot be overcome through compromise of the control systems.

The security of long distance communication links will also be a special consideration for remote operation. In current practice, where control rooms and their I&C connections to reactor systems are all at the same level of physical security, many computer security attack vectors can be minimized or eliminated. Using communication links that are not under the direct control of the facility operator will result in communications that are more susceptible to security threats (including physical and cyber-attacks). An SMR operator would need to consider how such communication links could be protected and the potential consequence that could result were these communication links to be compromised. The use of public communication infrastructures to relay command and control information would prohibit the implementation of a robust security architecture, as these communication infrastructures would be assigned to the lowest (i.e. least secure) security levels. This could necessitate the implementation of automatic fail-safe and fail-secure systems immune to cyber-attack (e.g. analogue), thereby reducing the potential for severe consequences.

3.2.2.5. Use of wireless technology

The field of communications is rapidly evolving, and wireless technology is already being introduced for personnel and limited data communication within plant sites. It is developing reliable characteristics that make them suitable for I&C architecture. The IEC published Ref. [29] to better understand the implications of wireless technology in nuclear facilities. Due to the potential for SMRs in remote locations, the designs are more likely to demand the use of wireless technology to obtain necessary data. Therefore, the contents of Ref. [29] are applicable and may be beneficial to consider during the design of wireless systems. One of the key technical points from Ref. [29] is that further work is required to assess the effects of strong radiation fields (during accidents and malfunctions) on wireless communications.

Computer security measures need to permit the safe and secure use of wireless technology, as wireless signals can be susceptible to jamming, interception and malicious compromise. These measures need to take into account the potential for wireless transmissions to extend beyond the physically protected area (e.g. exclusion area) allowing for interception, while malicious signals from outside the protected area may be received by the SMR.

For very small reactor facilities in remote locations, the control architecture can include a control facility far from the facility. The experience of other industries with a need for similarly high reliability has to be considered.

3.2.2.6. Computer security considerations

A robust computer security architecture needs to form the basis of the computer security plan. Technical guidance for computer security architecture is described in IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [30]. Technical considerations for computer security of I&C systems at nuclear facilities have been drafted and is published in the IAEA Nuclear Security Series [31].

Computer security for SMRs will also need to give special attention to: (i) the use and application of wireless technology inside the facility; and (ii) the adequacy of computer security measures between the remote control location and SMRs (e.g. satellite communications can be easily identified, intercepted and jammed, and are generally detectable over a large area).

A number of Member States have developed requirements for computer security and related architecture. In most cases, the requirements have not yet been documented in either codes and standards or requirements. In Canada, for example, a standard [32] has been developed that addresses requirements to be applied to develop, implement and sustain a computer security programme for reactor facilities, ranging from research reactors to full scale nuclear power plants. The requirements are designed to be independent of reactor technology and interpreted, where possible, in a manner commensurate with the potential risks to the facility. Requirements and guidance for remote operation were also considered in the standard.

3.2.2.7. The use of I&C in the overall architectural strategy for supporting maintenance and reliability

Many industries are exploring ways to use advanced I&C technologies in maintenance activities, particularly in concert with reliability centred maintenance programmes. The primary reason is to maximize process availability (i.e. minimize unplanned failures), but it also reduces overall maintenance costs. SMR operating business models seek to ensure maintenance efficiencies are maximized to achieve both aims.

On account of the safety implications, it is important to select I&C technology strategically. Although there are likely benefits to the addition of such components and systems, they should not contribute in any way to a decline in safety performance of the systems they are supporting. In some cases, maintenance real time information may need to be segregated from operational real time information. Segregation needs to be considered as part of HFE. The behaviour of such systems, both software and hardware, needs to be analysed under all anticipated conditions to understand any potential effects (positive and negative) on the facility safety analysis. In addition, if the maintenance activity is considered to have a safety impact, regulatory requirements might also need to be factored into system design and operation.

3.2.3. Developing robust control strategies for unconventional dynamic behaviours in SMRs

Clayton and Wood [6] report that some SMR concepts, such as iPWRs and other advanced designs, use unconventional process system components that do not have well established performance characteristics. Therefore, innovative measurements and methods might be needed for diagnoses of performance and determination of condition. In addition, specific dynamic behaviour characteristics of some SMR concepts pose unique control challenges that need to be addressed in the design of automatic control systems. In addition [6]:

> "Some SMR concepts involve sharing resources and systems among units to further reduce the upfront costs. This degree of sharing can range from minor support or auxiliary systems (e.g., emergency coolant tanks, control stations, backup electrical power, etc.) to major primary or secondary systems (e.g., turbine-generators coupled with two or more units). Depending on the nature and degree of sharing among modules, there may be significant dynamic coupling that must be taken into account within the operational controls for the plant. The impact of shared resources and systems may only require supervisory coordination of demands or may result in more sophisticated control implementations to address unique dynamic behavior. However, these

> control considerations are uncommon in nuclear power operational experience and should be demonstrated. In addition, the regulatory implications of shared systems must be evaluated.”

3.2.4. Developing diagnostic strategies for monitoring unconventional components in SMRs

Unconventional process system components that do not have well established performance characteristics might require additional monitoring:

(a) To support the in-service inspection programme;
(b) To develop operational experience (to support the plant safety case);
(c) To detect, record and monitor degradation or other phenomena.

Clayton and Wood [6] find that:

> “With the array of bundled helical tubes, flow-induced vibrational effects have to be investigated and addressed through control approaches utilizing surveillance and diagnostics information. Finally, the nature and impact of long-term degradation of the tube bundles has to be determined and addressed.”

3.2.5. Using I&C for radiation protection in SMR designs

I&C used in radiation protection strategies is generally a mature technology and is not likely to require significant improvements to be implemented in SMR facilities. The fundamental design philosophies for radiation protection remain the same as for larger facilities but also consider novel approaches to field inspections and maintenance of SSCs and refuelling.

Advanced SMR designs that are not water cooled can require special instruments to be located in key areas where design specific radionuclides might exist during normal operating conditions and accidents: for example, risks from ^{210}Po can exist in lead cooled reactors, requiring special methods of detection and particular alarms. Additional consideration is to be made for accidents during the transport of factory fuelled designs.

3.2.6. Sharing full scope simulators by multiple power utilities utilizing the same technology

The economic case for an on-site simulator becomes more prohibitive the smaller the SMR — even if the simulator itself is rather simple. Some SMR designers of are exploring a single simulator that is shared by multiple customers, within the same country or between countries. Such an approach depends on a number of factors:

(a) How the simulator is used within the overall site specific training programme for operations staff. Some vendors propose bulk generic training at the central simulator, with only specific training to be done on-site.
(b) Although there is a strong desire to build and operate standardized plants, different plants will have differences in SSC configurations (either specified by the customer or possibly by licensing specifications as a result of site characteristics) that need to be reflected in the simulator controls and software.
(c) Even if plant designs are standardized, differences in plant vintages, equipment vintages and software versions between sites mean that plant configurations will never be completely identical.
(d) Operational practices vary between countries and even companies. For example, how systems and equipment status is displayed on MCR panels often depends on local practices and norms.
(e) The role of the simulator as an operations support for a utility during a major plant event needs to be clear. If the utility has plans to run rapid simulations during an event to test alternative approaches late in a rare accident scenario, the simulator needs to be available as a tool as part of on-site emergency planning.

In (a)–(c), the use of a shared simulator requires a highly reconfigurable architecture that can reflect the operating behaviours and characteristics of each site and cultures of the operating organizations. This can prove to be a significant hurdle, for example if there are different software versions at each facility. The maximum number of units that a shared simulator can realistically support also needs to be considered.

3.2.7. I&C equipment

3.2.7.1. Sensors

Clayton and Wood [6] report that (see also Section 2.4) small and medium reactors have different process measurement needs than large LWRs:

> "For example, no currently available fission chambers are capable of operating near-core in a very high-temperature gas-cooled reactor (VHTR), thus necessitating neutron flux measurement being located away from the core. Similarly, diagnostic measurements are different for reactors with different coolants. The ultrasonic imaging required to verify proper component or fuel element placement below the surface of liquid sodium remains commercially unavailable."

They report that a prior investigation of instrumentation needs for iPWR was conducted [33] and [6]:

> "It was determined that measurement of certain key parameters can best be accomplished using in-vessel sensors that require development and demonstration. These in-vessel measurement capabilities include flux/power, primary flow, reactor coolant system temperatures, primary water inventory, steam generator water inventory, and steam generator stability."

(a) Neutron flux measurement

Some SMRs will not be able to employ current equipment used in nuclear power plants for neutron flux measurement owing to space restrictions or environmental compatibility presented by certain equipment designs. For some SMR concepts, a "highly ruggedized neutron detector capable of withstanding high temperature and high radiation needs to be developed with the associated radiation hardened electronics" [6]. For others, traditional or modified ion chambers will likely be sufficient.

(b) Level and flow measurement

For liquid metal and molten salt coolants, extensive flow and level measurement experience exists from conventional industries that use these substances. States that have experience with these coolants have also accumulated operational experience with these measurement technologies in either experimental prototype or full scale nuclear facilities. As a result, future designs of these types will evolve the instrumentation to improve reliability and accuracy.

For gas cooled technologies, this is also true for flow measurement technologies in other industries, and they can be considered to be mature. However, experience with the application of flow measurement techniques to gas cooled reactors is not extensive and demonstration of the environmental compatibility (e.g. radiation and high temperature), reliability and accuracy for nuclear applications is required. Clayton and Wood [6] find that for iPWRs:

> "Also, since the pressurizer is integral to the reactor vessel and vessel penetrations are restricted, conventional PWR-type temperature-compensated differential pressure based level measurements are not feasible. The lack of an external primary coolant loop for an IPSR [integral primary system reactor] also alters the nature of the heat balance measurements across the core."

There is also a challenge to measuring reactor flow in iPWRs because flow restrictions and pressure taps are undesirable. It is the premise of considerable R&D efforts that flow measurements in the integral vessel design (as well as other advanced concepts) can be made using indirect parameters such as pump speed or pump current. Flow measurements can also be made directly using transit time flow measurement technologies. These technologies have been used successfully at Comanche Peak Nuclear Power Station, United States of America, and Sizewell B, United Kingdom [34].

These types of flow measurement can be verified by thermal heat balance calculations obtained from cross-calibration measurements of primary temperatures and secondary process flow and temperatures. This cross-checking would not be much different than that routinely used for precision calorimetric performed in today's conventional nuclear power plants. The premise is that the reactor thermal power can be determined from precise measurements made on the secondary side of the plant and from primary coolant RTDs. Given the thermal power calculated from the feedwater and steam parameters and the primary temperature measurements, the primary coolant mass flow rate can also be calculated.

(c) Temperature measurement

For liquid metal, gas cooled and molten salt coolants, temperature measurement operational experience (conventional and nuclear) is mature. Future designs of these types will thus evolve the instrumentation to improve reliability and accuracy.

For iPWRs, traditional, mature technologies can be used; however, there is a desire to find ways to reduce the need for regular calibration. As a result, if the sensors are to be placed outside the vessel, sampling scoops would need to be used, such as with the bypass manifolds in conventional PWRs to bring the process water to the location where the temperature could be measured. However, all of these solutions have drawbacks.

In addition, the lack of an external primary coolant loop for an iPWR presents issues for temperature measurement. Clayton and Wood [6] find that:

> "For example, obtaining accurate measurements from long lead wire thermocouples will be challenging. … The longer fuel cycles and service intervals envisioned for SMRs provide a strong incentive to develop drift free, first principles measurement technologies. In conventional PWRs, the coolant temperature measurement instrumentation is calibrated during each refueling outage. Technologies such as Johnson noise thermometry that are immune to the progressive deterioration of the sensing element are important to a successful, cost effective SMR deployment."

Mature commercial technologies already exist for optical measurement of temperature. However, the effects of radiation on optical measurement devices have so far only been tested in research reactors. Issues such as radiation darkening reduce the effectiveness of fibre optic components.

3.2.7.2. Actuators

(a) Internal reactivity device actuator

All SMR concepts plan to embed actuators that operate reactivity mechanisms within a compact containment structure that would not normally be accessible to humans when the unit is at power, for example:

(i) For the mPower reactor iPWR concept, the CRDMs are located within the reactor vessel between the integral steam generators and the reactor core.
(ii) For the NuScale reactor iPWR concept, the CRDMs are located outside the integrated reactor module but inside a highly compact steel containment module kept under vacuum conditions.
(iii) Some more compact fast reactor concepts consider the use of rotatable reflectors, which would require actuators to be mounted directly to the reactor vessel.

The common factor is that, unlike nuclear power plant designs, which have larger volume containment structures, the more compact volumes of SMRs expose the actuators to more aggressive environments during both normal operation and accident conditions and includes:

- Higher temperatures (including potential for combustion level temperatures in the core in an HTGR);
- Rapid changes to atmospheric pressures in accident conditions (and in some cases in a reactor trip);
- Closer proximity to radiation fluence;
- Exposures to chemical attack.

The life cycle engineering processes and reliability approach used by the vendor will need to assess these hazards and their corresponding degradation effects and to consider them in design mitigation strategies. One such approach is environmental qualification. With such confined and inaccessible actuators, in situ inspection and maintainability issues become significant and designers need to consider both condition monitoring sensors and more rugged construction.

Strategies being used by various vendors to supplement their design activities include more aggressive testing specifications. In some cases, this can require engineering judgement to be applied beyond existing environmental qualification standards. All leading SMR vendors are currently conducting R&D on these types of actuator, but very little information about results is available in the public domain.

(b) Canned motor pumps

Smaller canned motor pumps are extensively used in non-nuclear industries as well as marine nuclear applications and are considered to be mature. The largest canned motor pump is used in the AP-1000, and the CAP-1400 will likely be larger. As a result, there will likely be operating experience available from which SMR designers can learn. The smaller pumps being proposed for certain SMRs, however, will need to consider the placement of diagnostic instruments in more confined conditions.

(c) Electromagnetic pumps

Electromagnetic pumps have no moving parts and are used extensively by non-nuclear industries for liquid metal and molten salt applications [35]. One SMR in particular, the Toshiba 4S, incorporates electromagnetic pumps in its RCS; however, operational experience is currently limited to prototype pumps.

3.2.7.3. Electronics in smart devices

So called smart devices will be very useful to automate data gathering and health monitoring. Their amenability to networking can also support reductions in cables, as bus networks could be used in place of point to point wiring. A further application could be the use of information as an input into a supervisory control system to enable automatic decision making. However, as with any nuclear power plant application, considerations such as communications reliability, computer security and potential vulnerability to common cause failure all need to be addressed.

Because of space limitations, the electronics contained in smart devices in SMRs could be exposed to harsher environments than more traditional nuclear power plants. Clayton and Wood [6] report that: “High doses of ionizing radiation cause significant changes in the characteristics of semiconductor electronic devices”, leading to operational uncertainties and premature failures. With the longer fuel cycles proposed for SMRs, this will present maintenance challenges. Moreover [6]:

> “Radiation exposure complicates the utilization of COTS [commercial off the shelf] semiconductor components. Radiation tolerance is rarely if ever required for applications outside of military, aerospace, and nuclear industry applications. Without detailed process knowledge, radiation tolerance is impossible to simulate. Radiation tolerance can change without notice whenever the manufacturer makes minor process changes.
>
> “Fortunately, there are a variety of nonexclusive techniques that can be implemented to overcome the lack of commercially available radiation tolerant, high temperature electronic devices. These techniques include (1) the addition of localized shielding for sensitive components, (2) moving the sensitive components further from the reactor where technically feasible, (3) design Application Specific Integrated Circuits (ASICs) using silicon-on-insulator (SOI) techniques, (4) design ASICs using modern complementary metal–oxide semiconductor (CMOS) processes, and (5) fault tolerant circuit design techniques.”

3.3. FABRICATION AND SITE INTEGRATION

3.3.1. Manufacturing and factory pre-commissioning testing

Across numerous industries, there is clear evidence that factory manufacturing of modules as part of modular construction results in the following:

- — Higher quality and more consistent products;
- — Lower manufacturing costs;
- — Reduced times for transport, field assembly, construction and commissioning;
- — Reduced construction and commissioning costs.

It is important to understand that modular engineering requires very close coordination between various module vendors to ensure that the modules can precisely integrate when installed and commissioned at the site. In some cases, the transport of modules can actually become significantly more complex and subject to technical issues at the receiving site.

Modular manufacturing and construction is now a matter of course for large, complex civil engineering endeavours in shipbuilding, aerospace and telecommunications. Although a number of nuclear power plant developers are actively capturing value from these methodologies to reduce both time and cost of construction and commissioning, SMR vendors require these methodologies to be used to be economically viable and to satisfy customer demand for projects which are on time and on budget. Indeed, with SMRs, the desire is to have fewer modules in a facility yet make them easily transportable to any site around the world.

As is typical for manufacturing modules in other industries, I&C elements for most systems are installed in the module and pre-commissioned at the factory prior to shipment to the site for installation and final commissioning. One such example is the reactor vessel assembly module for all SMRs. The most extreme case would be a factory sealed, transportable nuclear power plant in which I&C elements — including sensitive in-core instrumentation — would be in place before the plant were transported to the site for installation, integration testing and commissioning. These reactor modules are designed to be sealed and inaccessible for the core life, which is in the range of 5–35 years. At the end of the operating cycles, some I&C elements may be needed to provide key indications during transport back to the factory for refuelling, refurbishment or decommissioning.

The need for factory acceptance and pre-commissioning testing is driven by two primary factors:

(a) It is part of the licensee's acceptance criteria: Information is needed to meet installer criteria to demonstrate that the systems are ready for installation and integration testing.

(b) The licensee wants to shorten on-site testing and to ensure that technical issues are resolved at the factory, before shipment: This helps to reduce on-site issues, delays and resulting costs.

The site commissioning organization will need not only results but also detailed technical information from the module vendor to plan on-site inspection and commissioning tests to be performed upon receipt of the module (see Section 3.3.2). As a result, factory acceptance and pre-commissioning tests need to document clearly the following in accordance with the quality requirements of the licensee:

- — Processes and procedures used, including relevant codes and standards;
- — Test boundaries and performance criteria;
- — Assumptions used in factory acceptance and pre-commissioning tests;
- — Benchmark conditions and as left equipment states or status.

Areas that can involve additional system integration tests include testing systems for post-shipment effects or potential damage due to shock, temperature and humidity.

3.3.2. Site receipt, installation and commissioning

As is normal for any nuclear construction project, receipt inspections of all module elements need to be performed post-receipt at the site and in accordance with the licensee’s quality assurance programme. Inspections include any necessary tests of I&C elements to confirm they have not been adversely affected by transport. This requires the receiving inspectors to have the necessary technical information from the vendor to determine whether the systems are within the parameters of the as shipped state. When certain I&C elements are inaccessible (i.e. embedded), the inspectors require the necessary protocols and test procedures by which to ascertain system integrity in the absence of physical inspection methods. This requires a measure of transparency by vendors to share design information.

Once installed on-site, all elements of ‘pre-tested’ modules are then integrated and tested under the facility commissioning programme. This practice is currently used in many nuclear power plant projects. Hence, there already is relevant operational experience being documented from which SMR designers and constructors can capitalize. This approach places an emphasis on the commissioning organization’s need to understand the roles, scope and depth of the factory pre-commissioning tests as part of the overall site integration and pre-commissioning testing programme. It is important for the commissioning organization to use a systems engineering approach to understand the strengths and limitations of the factory pre-testing programmes and processes. This knowledge is used to determine where commissioning might need to be adjusted to take these limitations into account. As mentioned above, this requires access to detailed design information to ascertain where conditions have changed significantly enough to warrant additional or modified commissioning testing.

3.4. CONCEPTS IMPORTANT FOR OPERATION

3.4.1. Provisions for deep load following and fast runback

All grid systems require some generation to be able to operate flexibly and to allow generation to change to match variations in demand. Countries with a grid system interconnected to other countries will also need to operate flexibly to control power flows across the interconnectors to other networks as demand varies. Many SMR designers are required by potential customers to provide deep load following capabilities as part of the utility’s overall energy mix balancing strategy. One such strategy is presented in Fig. 5, which shows an SMR operating in a hybrid mode with renewables. This is particularly important for very small grids or remote grids where loads fluctuate rapidly. Some SMR concepts, in particular transportable nuclear power plants will need to operate for significant periods of time on very small local grids, which is approaching an operating state called ‘islanding mode’.

New nuclear units generally have greater load following capability than those found in the current fleet. However, because of the effect of thermal transients during load changes (e.g. fuel and pressure vessels), they will have restrictions in their technical specifications that limit the magnitude or speed of load variation and the number of load cycles.

Fast runbacks are generally a reactor protective measure initiated in response to plant or grid transients. It is used to ensure reactor availability and to prevent reactor poison out. This protective strategy assists the operator in reducing stressful transient effect on the lifespans of plant SSCs.

Depending on the design characteristics of the reactor, a fast runback can be a measure used for deep load following, for example if a facility is generating in concert with local renewable power generation. To improve load following and the use of fast runback in SMR technologies, it is sometimes necessary to design alternative control strategies to adjust promptly the set point for the electrical energy provided to the grid, according to the load demands: for example, to limit the thermal transients on the plant during the load following operational mode, one measure might be to develop multiple input/output control strategies, in which several control actions could be performed on the plant to regulate not only the power production but the temperature field as well.

In some cases, it may not be possible to rely on a proportional integral derivative based strategy in which the different actuators tend to control the different output variables independently, providing set points which can also cause disturbance on the other system controlled variables. In those cases, the adoption of feedback single input/output control loops might not yield acceptable performance.

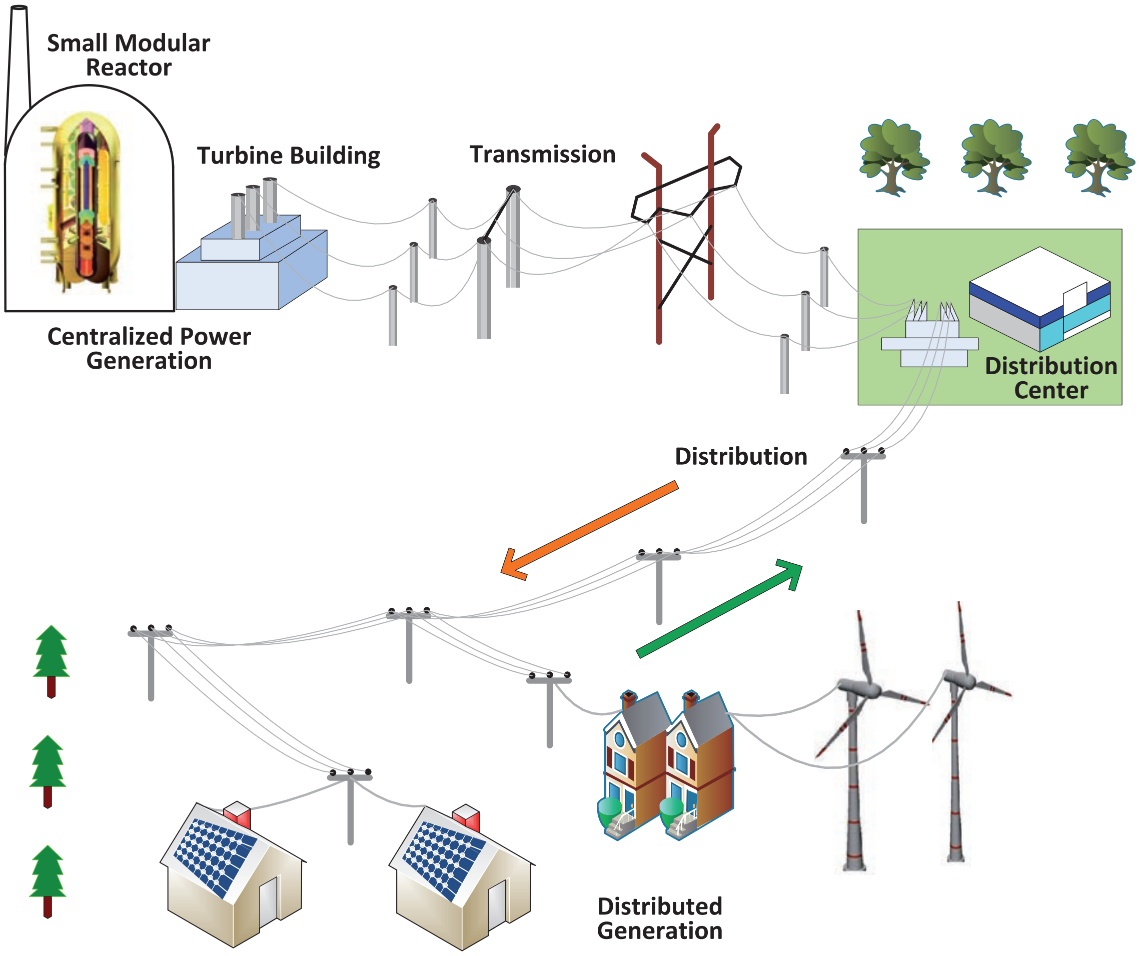


FIG. 5. Distributed generation and the consequent possibility of reversal of the traditional power flow from the high tension to the medium voltage line.

3.4.2. Integrated supervisory control

Integrated, intelligent and autonomous supervisory control architecture has been investigated in many industries for some time [36]. Some SMR concepts explore an integration of control with SDP in a semi-autonomous fashion both to enhance the operation of the plant and to reduce the operation burden on plant staff. This approach has an overarching supervisory control strategy, with the SDP as one portion. The integrated architecture combines robust and resilient decision algorithms to enhance the operational safety and performance of SMRs through the detection, diagnosis and mitigation of anticipated faults and transients. As Jin et al. [37] report:

> "The objective of robust control is to minimize the sensitivity of plant operations to exogenous disturbances and internal faults while achieving a guaranteed level of performance with a priori specified bounds of uncertainties. On the other hand, the role of resilient control is to enhance plant recovery from unanticipated adverse conditions and faults as well as from emergency situations by altering its operational envelope in real time. In this paper, the issues of real-time resilient control of nuclear power plants are addressed for fast response during emergency operations while the features of the existing robust control technology are retained during normal operations under both steady-state and transient conditions."

The goal is to have an integrated fault tolerant and resilient system for control and for transient mitigation that incorporates the following technology features:

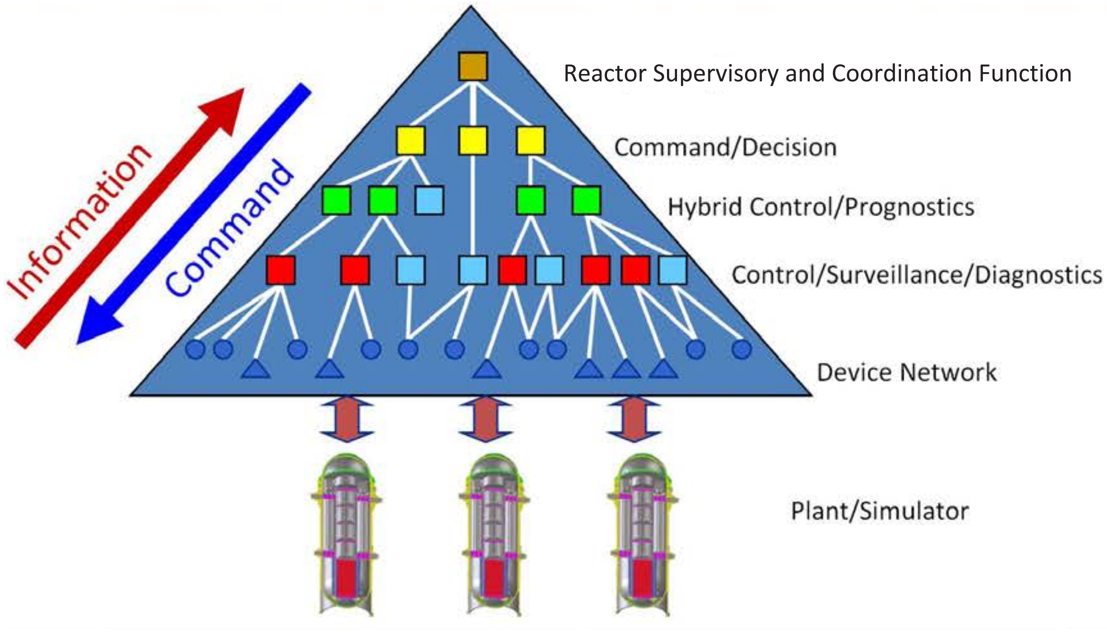
(a) Fault monitoring and diagnosis of instrumentation, devices, equipment and systems;

(b) Robust and resilient control strategies that mitigate faults and reconfigure the plant for safe and reliable continued operation.

Figure 6 is an example block diagram of a supervisory control system architecture for multiple modules with embedded fault diagnostics. As Ref. [38] reports:

> "This approach provides the framework for autonomous control while supporting a high-level interface with operations staff who can act as plant supervisors. The final authority for decisions and goal setting remains with the human but the control system assumes expanded responsibilities for normal control action, abnormal event response, and system fault tolerance. The autonomous control framework allows integration of controllers and diagnostics at the subsystem level with command and decision modules at higher levels."

Some current plants incorporate some of these design features; however, not at the degree expected for SMRs. For example, the first computer controlled (automated reactor regulating system) CANDU units were at the Pickering A station in 1971 (four 540 MW(e) units). Since then, the controls have gone through a series of upgrades, some of which incorporate additional functionality. The system currently has the ability to detect some abnormal conditions, such as heat transport pump shutdown or aberrant steam generator water levels. When abnormal specific conditions are identified, the control system automatically takes corrective or compensatory actions such as reducing power or shutting down the reactor. The setback (slow linear decrease) and step back (fast decrease) routines respond to abnormal condition signals and take action to restore the station to the normal operating domain.


Information
Command
Reactor Supervisory and Coordination Function
Command/Decision
Hybrid Control/Prognostics
Control/Surveillance/Diagnostics
Device Network
Plant/Simulator

Source: Based on fig. 4 of Ref. [38].

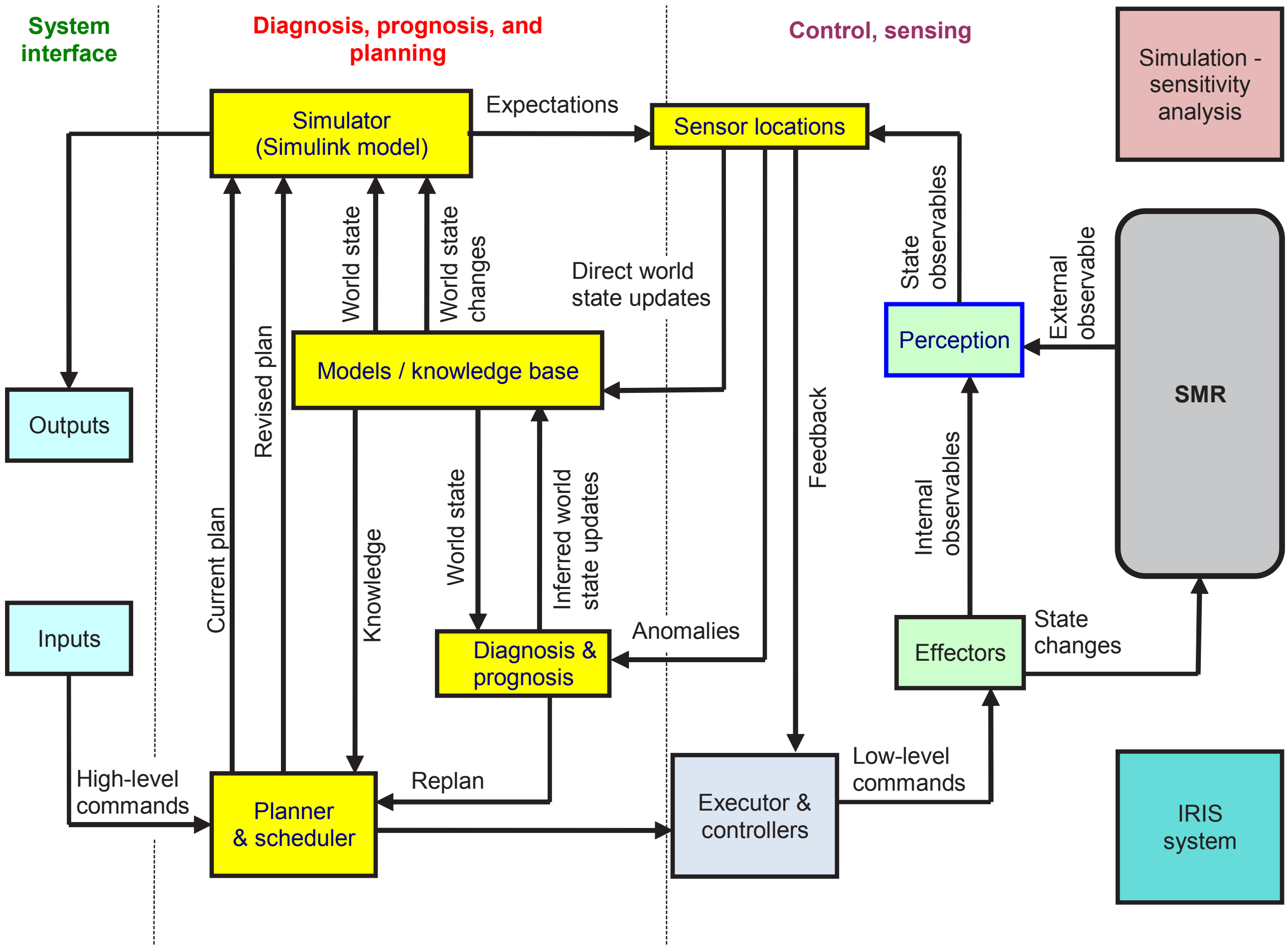
FIG. 6. Supervisory control architecture for multimodular nuclear power plants.

Figure 7 presents an implementation scheme for a supervisory control algorithm with integrated SDP.

The integrated robust and resilient control architecture has been studied by several research groups in several countries. Jin et al. [37] present a solution developed for the IRIS reactor under the DOE grant Advanced Instrumentation and Control Methods for Small and Medium Reactors with IRIS Demonstration [39] and they report:

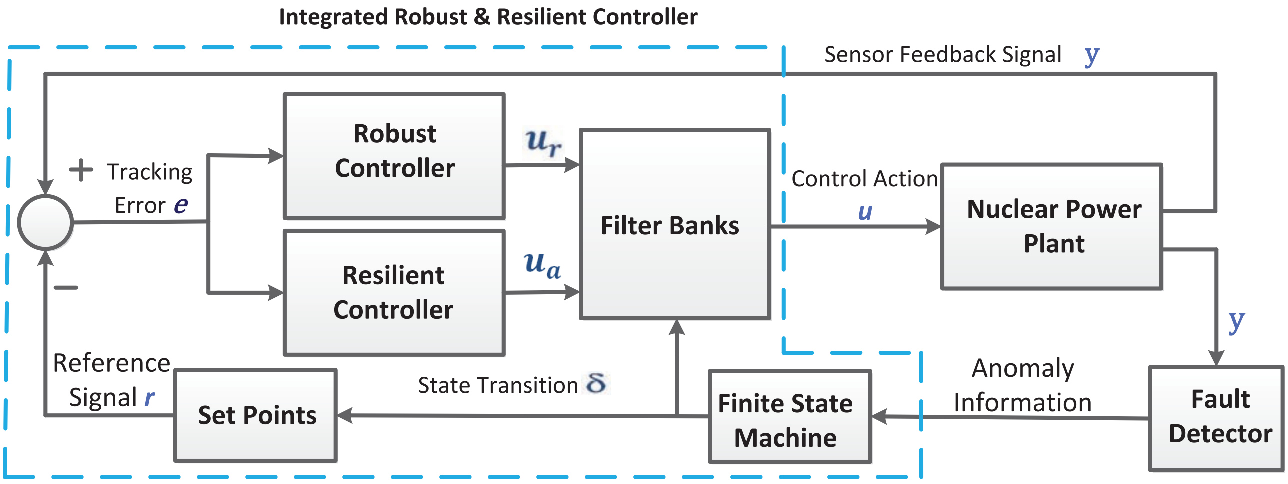
> “[Figure 8] depicts the layout of an integrated robust and resilient control system that includes the robust controller, resilient controller, fault detector, finite state machine (FSM), a set of reference points, and a filter bank for bumpless transfer. The fault detector is extrinsic to both robust and resilient controllers.”

The integration of control with SDP will require detailed analysis of the system interactions to avoid unintended consequences. This is of utmost importance when developing a safety case for regulatory approval.



Source: Based on fig. 1.3 of Ref. [39].

FIG. 7. Integration of advanced instrumentation and controls modules for SMRs.



Source: Based on fig. 4 of Ref. [37].

FIG. 8. Layout of the integrated robust and resilient control system.

3.5. MAINTENANCE

Effective maintainability will be crucial to both the availability and economic competitiveness of SMRs. In fact, load following SMRs might experience accelerated degradation of SSCs, which will make maintainability a more important consideration. Maintainability will be challenging when:

(a) Components are inaccessible (e.g. components inside iPWR reactor vessels).
(b) Components are in extreme environmental conditions (such as in molten lead or salt cooled systems).
(c) Facilities have small on-site maintenance teams or are located remotely from maintenance resources.

There is much information detailing proven maintainability methods that can be used to mitigate these issues and to plan for effective maintenance programmes. For example, the Reliability Information Analysis Center is a United States Department of Defense chartered laboratory with a technical focal point for information, data, analysis, training and technical assistance in engineering fields. On the topic of design for maintainability, some major considerations include accessibility, reparability, modularity, standardization, testability and simplicity.

Advanced techniques for design for maintainability can include collaboration between maintenance personnel and designers and virtual reality test facilities [40]. The National Aeronautics and Space Administration (NASA) has also developed best practices [41].

3.5.1. Impacts of longer operating intervals on maintenance

3.5.1.1. Surveillance, diagnostics and prognostics

There have been many programmes and projects focused on using SDP on nuclear power plant components, sensors and structures to improve safety, reliability and efficacy of both maintenance and operation. The results of many of these programmes can be directly applied to SMR designs [42]. For example, the US DOE Light Water Reactor Sustainability Programme [43] seeks to develop “technologies and other solutions that can improve the reliability, sustain the safety, and extend the life of the current reactors.” Furthermore [43]:

> “It has two facets with respect to long-term operations: (1) manage the aging of plant systems, structures, and components so that nuclear power plant lifetimes can be extended and the plants can continue to operate safely, efficiently, and economically; and (2) provide science-based solutions to the industry to implement technology to exceed the performance of the current labor-intensive business model.”

The IAEA has also had several programmes dedicated to documenting the state of the art and best practices of OLM. A publication on OLM for improving performance in nuclear power plants was issued in 2008 [44], and, more recently, a 2013 publication focused on advanced SDP techniques in monitoring SSCs in nuclear power plants [45]. Although these IAEA publications do not focus on SMRs, the methods and technologies explored are directly applicable.

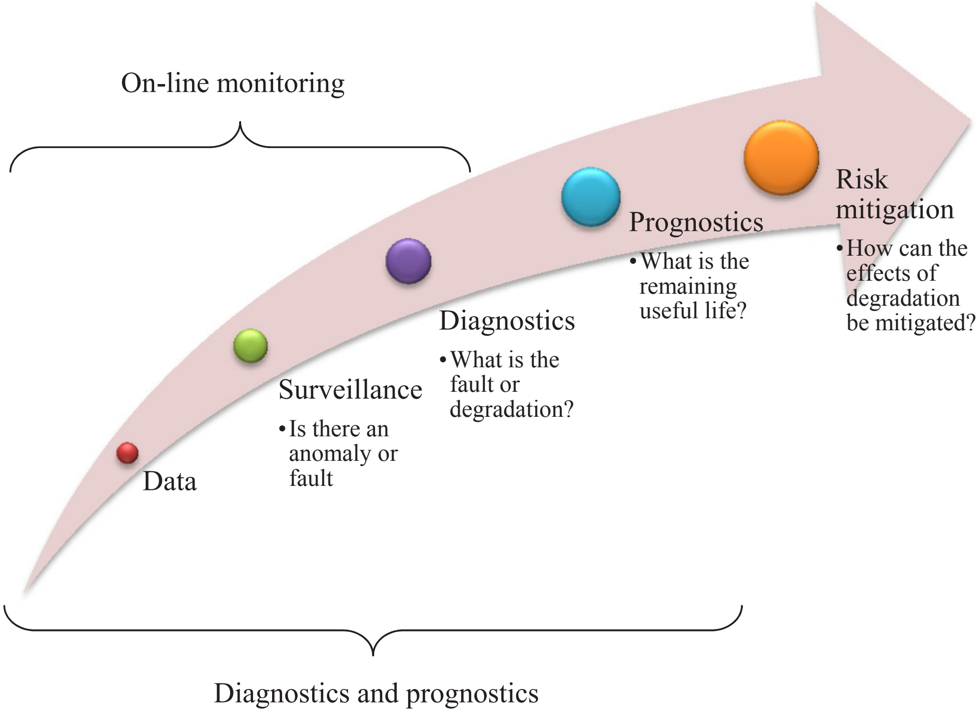
SDP include the methods used to perform on-line, continuous or periodic health monitoring of SSCs. SDP systems comprise several modules that solve specific tasks. As shown in Fig. 9, data collected from the SSC of interest are used for surveillance purposes [45]:

> "Surveillance [i.e. monitoring] usually consists of analysing collected data to detect small changes that are related to SSC degradation. The onset of degradation manifests itself as a fault, defined as an abnormal deviation in the condition of at least one piece of equipment or at least one process variable. When a fault is detected, a diagnostic module is activated to identify and characterize the fault. This is important because different faults progress to failure in different ways and therefore require different prognostic models. Once the fault is identified, a prognostic model is activated, which uses information such as current and past environmental and usage conditions, past and current operational sensor data, and historical failure data for similar components, to predict an item specific probability of failure distribution."

A 2012 Pacific Northwest National Laboratory report [46] reviews the use of prognostics and health management in technologies and applications for nuclear power plants and related technology currently applied in the field or under development in other technological application areas.

Jardine et al. [47] present one of the most complete works on condition based maintenance. It provides a summary and review of recent R&D in diagnostics and prognostics. It is organized in three stems: data acquisition, data processing and maintenance decision making; with an emphasis on algorithms, models and technologies.

Although several of these publications do not focus explicitly on SMRs, they do discuss technologies and implementations that impact SMR needs for SDP. These technologies promote early degradation detection to enable appropriate mitigation actions which will improve safety and reliability and potentially reduce serious consequences.


On-line monitoring
Data
Surveillance
• Is there an anomaly or fault
Diagnostics
• What is the fault or degradation?
Prognostics
• What is the remaining useful life?
Risk mitigation
• How can the effects of degradation be mitigated?
Diagnostics and prognostics

Source: Based on fig. 1 of Ref. [45].

FIG. 9. A typical on-line monitoring surveillance system.

3.5.1.2. Instrument calibration

Many SMRs will have extended refuelling intervals to maximize production and to minimize opportunities for proliferation of materials. These longer intervals will challenge maintenance and replacement of sensors. In most countries, however, current regulations require sensor calibration be checked against a traceable standard. Therefore, a safety case can be made to lengthen monitoring intervals and to develop methods for on-line calibration monitoring proven to meet safety requirements.

The Electric Power Research Institute (EPRI) conducted a drift study in which instrument calibration data were collected from 18 nuclear plants [48]. The study provides evidence that sensor drift is not time dependent, indicating that additional work needs to be done to demonstrate sensor calibration periods to be extended. This is particularly important for new sensor designs, which will need to be proven. On-line sensor calibration monitoring had been successfully implemented and technical issues are discussed in Refs [44, 49–58]. The NRC reports that [51]:

> "The EPRI Instrument Monitoring and Calibration (IMC) Users Group was formed in 2000 with an objective to demonstrate OLM technology in operating nuclear power plants for a variety of systems and applications. A second objective is to verify that OLM is capable of identifying instrument drift or failure. The On-Line Monitoring Implementation Users Group was formed in mid 2001 to demonstrate OLM in multiple applications at many nuclear power plants and has a four-year time frame."

A review of the lessons learned from these implementations is documented in Hines and Davis [59]. All of the knowledge collected for nuclear power plants in the above publications and activities is fully applicable to SMRs.

There are some key issues and challenges to the implementation of these methods in SMRs. In many cases, operating experience will not be available to support design, commissioning and operation related activities. This can result in licence conditions being implemented for first of a kind plants until sufficient operating experience data are available to test the designs — including sensor performance during extended maintenance intervals. Clearly, capabilities to detect sensor drift will prove useful in supporting O&M programmes for SMRs.

3.5.2. Maintenance simulator and augmented (virtual) reality

SMR operators are, for reasons of economics, likely to propose sharing personnel and tools involved in complex inspection and maintenance tasks. This will probably mean that operators will expect vendors to facilitate the training and qualification of maintenance staff.

Designers of I&C related tools specifically need to consider adaptability of the tool to differences in systems between facilities (whether by vintage, design or simply differences in each plant). This means that the facility operator needs to have configuration information to inform maintenance staff about the current system status. This can involve documenting and understanding the following:

(a) Differences in codes and standards used for I&C in the licensing basis of the facility;
(b) Differences in specific plant I&C SSCs (likely due to vintage);
(c) Differences in software and firmware versions;
(d) Differences in system operating approach because of site specific safety needs;
(e) Interfaces between I&C systems to be maintained and ancillary devices and software added by the operator to support O&M.

All of these differences need to be reflected in maintenance simulators used by staff to train and prepare for deployment to a specific facility.

3.5.3. New I&C tools to monitor life cycle issues specific to SMR

Some specific technical issues unique to SMRs can benefit from the use of I&C strategies. Most SMR concepts will need to address at least one of the following issues through R&D or other technical and regulatory research, prior to the detailed design phase in order to prepare a complete and comprehensive licensing basis or deployment.

3.5.3.1. Ageing management of civil structures

Many SMR designs will be using subsurface civil structures (likely concrete based) to improve facility robustness and to increase resistance to security threats to make a case for reducing security staff. Most likely, structural integrity will need to be demonstrated not just for an operating lifespan of up to 60 years but also for a safe storage stage until decommissioning is completed. Under a worst case scenario, this could mean a monitored lifespan of up to 100 years.

Subsurface structures are subject to a number forces and degradation mechanisms such as:

(a) Ground pressures, which increase with depth;
(b) Buoyancy forces, which change over time, depending on groundwater conditions and gradual local geological forces;
(c) Effects of exposure to groundwater (both saline and fresh) combined with soil and rock chemistry, which attacks cement, weakening it structurally.

Unlike the civil structures of a typical nuclear power plant, SMR subsurface structures are, by their nature, difficult (or impossible) to inspect from outside using traditional methods. An alternative could be to take periodic core samples from inside for analysis, which is similar to a coupon concept for assessing radiation effects on pressure vessels.

For nuclear power plants, a traditional approach might be to implement periodic non-destructive examinations and visual inspections or simply to anticipate these effects and use more concrete to build thicker structures with a higher margin to failure over time. However, this method might add unnecessary cost to the construction of SMRs if alternative technical approaches to detecting degradation can be used.

Other approaches used in alternative industries include instrumented concrete for detecting water in-leakage or chemical degradation, and long life load cells for measuring changes in forces or deflection over time. SMR designers need to investigate alternative technologies — and the codes and standards associated with them — to improve their civil structure ageing management strategy.

3.5.3.2. Health monitoring and maintenance of embedded reactivity control device assemblies

Both integrated vessel SMRs and factory sealed transportable SMRs will utilize reactivity control devices whose actuators and related I&C and electrical systems are embedded within the reactor module assembly. For example, most iPWRs utilize embedded control rod drive assemblies. Sealed, non-water cooled designs utilize technologies ranging from control rod drive assemblies to adjustable reflectors.

In all the designs, reactivity control drive assemblies will be closer to the reactor core and within a confined space. This exposes I&C components to a number of degradation mechanisms, including:

(a) Higher radiation doses, which can result in changes in material properties of various subcomponents (e.g. cables and motors) over time, leading to speed variations;
(b) Higher temperatures;
(c) Exposure to harsh pressure and chemical environments in the face of structural failure events within the vessel.

Regardless of the technology used and the fact that these devices will likely be hardened to withstand these harsh environments, maintenance will present significant access difficulties, including potential disassembly of portions of the reactor module. With sealed transportable designs, this may mean the entire reactor assembly will need to be returned to the factory for repair. This has obvious consequences to the availability of the facility (and economic case) to perform its function. Thus, there is a need for the operator and its maintenance organization to monitor and understand the margin to failure of these systems to better predict when calibration or maintenance will be necessary. To accomplish this, certain parameters will need to be instrumented to provide the operator with the diagnostic information needed to assess the margin to failure of the device. This will require the development of hardened sensors, not only for pressure and temperature measurements but also to assess the chemical environment to which the devices are exposed. Such sensor technologies may not yet exist, but R&D will need to be factored into the facility safety case if specific failure mechanisms could potentially impact the safety of the facility.

3.5.3.3. Material degradation in sealed vessels

Somewhat related to accessibility is the ability of operators to monitor and measure any significant material degradation within the reactor module assembly. Degradation mechanism includes the following:

(a) Pressure cycle and radiation effects on structures and components (e.g. embrittlement and cracking).
(b) Chemistry effects: This is a key area for lead and lead–bismuth reactors, in which oxygen control is needed to maintain protective oxide layers on structures and components (e.g. pump impellers).
(c) Effects of erosion: Key for liquid metal reactors.

Similar to the I&C components, this will also require hardened sensors and R&D to be factored into the facility safety case.

4. CONCLUSION

When examining an SMR concept from an I&C design perspective, the technical discussion becomes less based on reactor size and function but rather on addressing technical challenges introduced by the specific operational and maintenance characteristics of each concept. The I&C architectures and specific technical approaches of SMRs represent a significant step in expanding the role of I&C systems to further enhance safety, significantly improve O&M and hence reduce O&M costs. Many of the approaches and technologies being examined have been proven in other industrial settings, some of which demand similar levels of reliability as that required for nuclear applications. However, nuclear applications also introduce unique technical and HFE challenges that will need to be addressed to test these approaches in nuclear environments and within a defence in depth approach. Key challenges include the following:

(a) Any expansion of the role of I&C architecture in facility O&M (e.g. increased automation for SMRs) needs to be reconciled with fundamental nuclear safety principles. This means that the operating organization, and in particular operators themselves, will play a key role in facility oversight and require unambiguous situational awareness and the ability to ensure safety at all times. The complexity of the I&C architecture will complicate the safety analysis; hence, simplicity is a key design principle. Economic considerations such as lifecycle O&M costs need to take these principles into account.
(b) Similarly, expanding the role of I&C architecture in facility O&M will require a robust HFE approach that considers not only the traditional human–machine interfaces but also the contribution of human errors into the design of automation, which will replace or supplement human decision making. This is especially true for supervisory control systems, whose technical maturity has not yet been adequately demonstrated in nuclear power applications from a safety context. Vendors will need to confirm HFE processes are integrated in their supply chains.
(c) With alternative end uses such as cogeneration, integration with renewables and remote grid applications, I&C systems of SMRs will become more integrated with the I&C systems of the end use processes. It is important for designers to understand how the I&C of the energy conversion process systems can influence, or interface with, the I&C systems of the nuclear island. Terminal points for regulation of the design might not always be clear and might exist in software based systems. The location of regulatory terminal points establishes the difference between whether an event occurring in the energy conversion process is an internal plant event or an external event. This also influences how computer security is addressed in the design provisions.

(d) Space and accessibility constraints, harsh environments, longer intervals between facility outages and the desire for more information to optimize O&M, including dose considerations, place significant challenges on I&C designers to develop both highly reliable and cost effective solutions. New reactor configurations and coolant types can require new types of sensor and condition monitoring equipment, and new, more dynamic control strategies.

(e) Shared MCR facilities, whether individual SMR units controlled by multiple operators or a single operator across multiple units, will require extensive HFE. Significant experience exists in other industries (e.g. the petrochemical industry). There is also extensive operational experience for multi-unit control rooms in nuclear power plants, and designers need to build on this experience. It is important to note that the activity of plant operation is the focus of licensing by regulatory authorities. Where an MCR or secondary control room is planned to be located remotely from a facility in concert with local autonomous operation, the I&C systems will be considered by regulatory authorities to be an engineered extension of the facility's site I&C architecture. Thus, communication means has to be carefully considered as part of the design approach.

(f) The application of I&C technology can supplement physical protection, but it needs to be developed and demonstrated for SMRs in the face of design basis threats that vary from site to site.

(g) Factory fuelled and sealed transportable nuclear power plants can require additional I&C for use in transit. I&C systems will need to be hardened to survive the rigors of transport and the means will need to be developed to confirm I&C systems can perform their design function unaffected by hazards encountered during transport.

Many of the SMR designs under development, and in particular non-water cooled concepts, share similar — if not the same — technical challenges with larger, Generation IV style concepts. All draw lessons learned from R&D and operational experience derived from early prototype facilities as well as contemporary R&D being conducted by individual vendors, national laboratories, technical institutes and groups such as the Generation IV International Forum. Verification and validation results, both past and present, have to be evaluated for relevance to specific cases. In particular, scalability and applicability have to be examined when considering multi-unit operation models and alternative facility uses beyond power generation. In addition, different SMR configurations will have different dynamic characteristics, so any unresolved issues and technical gaps will result in regulatory challenges and subsequent delays during licensing.

The technical knowledge base around issues and possible solutions is growing quite large. Although some information is publicly available, it can be very difficult to locate for I&C designers and utilities — the ultimate users of the technology. Many possible solutions to challenging problems is generally inaccessible to I&C designers because of intellectual property rights, and many developers were reluctant to share significant insights and technical details for this publications. Best practices recommended by experts include the following:

(1) Centres of knowledge should ideally make information more readily available to facilitate the early development of harmonized engineering approaches. This can greatly help both the revision of existing codes and standards and the development of new ones. Consolidating information and making it more accessible will also enable earlier participation of regulators and, more importantly, utilities in developing requirements on I&C approaches for specific applications.

(2) Utilities interested in SMRs need to engage more visibly and actively with existing industry organizations focused on operational excellence (e.g. World Association of Nuclear Operators, WANO) to set user requirements for I&C systems, including economic considerations. Utility requirements need to embed fundamental requirements for developers to demonstrate the use of proven systems engineering approaches, such as the I&C lifecycle approach.

(3) Utilities play a central role in a site commissioning programme, so they need to provide early feedback on requirements for commissioning to be performed on-site versus factory testing and pre-commissioning. Site commissioning and operating organizations (who are accountable for the project) will need access to design information (e.g. for site acceptance tests and safety analyses).

(4) Industry organizations such as WANO, in concert with utilities and developers, need to engage early with the IAEA and nuclear regulatory forums such as the OECD/NEA Committee on Nuclear Regulatory Activities to encourage regulators to develop common positions with regard to requirements for I&C architectures and strategies in the presence of new approaches.

(5) Engineering and operational simulators are extremely useful for SMR developers in the design, validation and verification of I&C systems and related human–machine interactions. Designers need to expand this good practice and showcase their efforts to the industry at large. Regulators should consider integrating this good practice into requirements and guidance for I&C design.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends, IAEA-TECDOC-1451, IAEA, Vienna (2005).

[2] INGERSOLL, D.T., Deliberately small reactors and the second nuclear era, Prog. Nucl. Energy **51** (2009) 589–603.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Fast Reactor Research and Technology Development, IAEA-TECDOC-1691, IAEA, Vienna (2012).

[4] UPADHYAYA, B.R., ZHAO, K., WOOD, R.T., INGERSOLL, D.T., Thermal-hydraulic analysis of a helical coil steam generator for level monitoring, Trans. Am. Nucl. Soc. **88** (2002) 283–284.

[5] CARELLI, M.D., INGERSOLL, D.T., Handbook of Small Modular Nuclear Reactors, Woodhead Publishing, Cambridge (2014).

[6] CLAYTON, D.A., WOOD, R.T., “The role of instrumentation and control technology in enabling deployment of small modular reactors”, Nuclear Plant Instrumentation, Control and Human–Machine Interface Technologies (Proc. 7th American Nuclear Society Int. Topical Mtg, Las Vegas, 2010), ANS, LaGrange Park, IL (2010) CD-ROM.

[7] WESTINGHOUSE ELECTRIC COMPANY, Nuclear Automation: Vibration Integrity Monitoring System, NA-0020, Westinghouse Electric Company, Cranberry Township, PA (2012).

[8] MA, J., TRABIA, M., JIANG, Y., MOUJAES, S., Solid-phase Oxygen Control System, Mechanical Engineering Faculty Publications, Univ. Nevada, Las Vegas, NV (2005).

[9] JEONG, S.H., BAHN, C.B., CHANG, S.H., CHOI, S.Y., HWANG, I.S., “Oxygen sensor development for LBE System”, Proceedings of the Spring Meeting of the Korean Nuclear Society, 2005, KNS, Seoul (2005).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Features and Operating Experience of Experimental Fast Reactors, IAEA Nuclear Energy Series No. NP-T-1.9, IAEA, Vienna (2013).

[11] OECD NUCLEAR ENERGY AGENCY, Handbook of Lead–Bismuth Eutectic Alloy and Lead Properties, Materials Compatibility, Thermal-hydraulics and Technologies, NEA No. 6195, OECD, Paris (2007).

[12] NUCLEAR REGULATORY COMMISSION, TRISO-coated Particle Fuel Phenomenon Identification and Ranking Tables (PIRTs) for Fission Product Transport Due to Manufacturing, Operations, and Accidents, NUREG/CR-6844, Vol. 1: Main Report, Office of Nuclear Regulatory Research, Washington, DC (2004).

[13] DAW, J., REMPE, J., TAYLOR, S., CREPEAU, J., WILKINS, J., “Ultrasonic thermometry for in-pile temperature detection”, Nuclear Plant Instrumentation, Control and Human–Machine Interface Technologies (Proc. 7th American Nuclear Society Int. Topical Mtg, Las Vegas, 2010), ANS, LaGrange Park, IL (2010) CD-ROM.

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of High Temperature Gas Cooled Reactor Performance: Benchmark Analysis Related to the PBMR-400, PBMM, GT–MHR, HTR-10 and the ASTRA Critical Facility, IAEA-TECDOC-1694, IAEA, Vienna (2013).

[15] BALL, S.J., HOLCOMB, D.E., CETINER, S.M., HTGR Measurements and Instrumentation Systems, ORNL-TM-2012/107, Oak Ridge National Laboratory, Oak Ridge, TN (2012).

[16] TALLACKSON, J.R., MOORE, R.L., DITTO, S.J., Instrumentation and Controls Development for Molten-Salt Breeder Reactors, ORNL-TM-1856, Oak Ridge National Laboratory, Oak Ridge, TN (1967).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna (2016).

[18] UPADHYAYA, B.R., MEHTA, C., LOLLAR, V., HINES, J.W., Remote monitoring of equipment in small modular reactors, Chem. Eng. Tran. **33** (2013).

[19] HOLCOMB, D.E., et al., Instrumentation, Controls, and Human–Machine Interface Technology Development Roadmap for Grid-appropriate Reactors, ORNL-GNEP-LTR-2008-041, Oak Ridge National Laboratory, Oak Ridge, TN (2008).

[20] BALDWIN, T., TAWFIK, M., BOND, L. (Eds), Report from the Light Water Reactor Sustainability Workshop on On-line Monitoring Technologies, INL/EXT-10-19500, Idaho National Laboratory, Seattle, WA (2010).

[21] NUCLEAR REGULATORY COMMISSION, Potential Policy, Licensing, and Key Technical Issues for Small Modular, SECY-10-0034, US Govt Printing Office, Washington, DC (2010).

[22] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Systems and Software Engineering: System Life Cycle Processes, ISO/IEC 15288:2008, ISO, Geneva (2008).

[23] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION, Systems and Software Engineering: Software Life Cycle Processes, ISO/IEC 12207:2008, ISO, Geneva (2008).

[24] NUCLEAR REGULATORY COMMISSION, “Instrumentation and controls: Hazard analysis”, 7.0 Appendix A, Design-Specific Review Standard for NuScale SMR Design,
www.nrc.gov/docs/ML1535/ML15355A295.html

[25] UPADHYAYA, B.R., LI, F., PERILLO, S.R.P., HINES, J.W., Load-following, co-generation, and sensor placement strategy for small modular reactors, Int. J. Nucl. Safety Simul. **2** (2011).

[26] LI, F., Dynamic Modeling, Sensor Placement Design, and Fault Diagnosis of Nuclear Desalination Systems, PhD Thesis, Univ. Tennessee, Knoxville, TN (2011).

[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Verification and Validation of Software Related to Nuclear Power Plant Instrumentation and Control, Technical Report Series No. 384, IAEA, Vienna (1999).

[28] MULTINATIONAL DESIGN EVALUATION PROGRAMME, Common Position on Safety Design Principles and Supporting Information for the Overall I&C Architecture, DICWG No. 9, OECD, Paris (2015).

[29] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants: Instrumentation and Control Important to Safety — Use and Selection of Wireless Devices to be Integrated into Systems Important to Safety, IEC TR 62918, IEC, Geneva (2014).

[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[31] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (in preparation).

[32] CANADIAN STANDARDS ASSOCIATION, Cyber Security for Nuclear Power Plants and Small Reactor Facilities, CSA N290.7, CSA, Mississauga, Ontario (2014).

[33] WESTINGHOUSE ELECTRIC COMPANY, Instrumentation Needs for Integral Primary System Reactors (IPSRs), STD-AR-05-01, WEC, Pittsburgh, PA (2005).

[34] RIGGSBEE, E., RITCHEY, C., HASHEMIAN, A., "Evaluation of I&C design for SMRs", Nuclear Plant Instrumentation, Control and Human–Machine Interface Technologies (Proc. 9th American Nuclear Society Int. Topical Mtg, Charlotte, 2015).

[35] NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, Liquid-metal Pump Technologies for Nuclear Surface Power, NASA-TM-2007-214851, NASA, Hanover, MD (2007).

[36] ANTSAKLIS, P.J., PASSINO, K.M., "Introduction to intelligent autonomous control systems with high degrees of autonomy", Introduction to Intelligent and Autonomous Control (ANTSAKLIS, P.J., PASSINO, K.M., Eds), Kluwer Academic Publishers, Boston, MA (1992) 1–26.

[37] JIN, X., RAY, A., EDWARDS, R.M., Integrated robust and resilient control of nuclear power plants for operational safety and high performance, IEEE Trans. Nucl. Sci. **57** (2010) 807–817.

[38] OAK RIDGE NATIONAL LABORATORY, Definition of Architectural Structure for Supervisory Control System of Advanced Small Modular Reactors, ORNL/TM-2013/320, ORNL, Oak Ridge, TN (2013).

[39] HINES, J.W., et al., Advanced Instrumentation and Control Methods for Small and Medium Reactors with IRIS Demonstration, Vols 1–7, DE-FG07-07ID14895/UTNE/2011, Univ. Tennessee, Knoxville, TN (2011).

[40] PENG, G., XIN, H., GAO, J., CHENG, D., A visualization system for integrating maintainability design and evaluation at product design stage, Int. J. Adv. Manuf. Tech. **61** (2012) 269–284.

[41] NATIONAL AERONAUTICS AND SPACE ADMINISTRATION, Recommended Techniques for Effective Maintainability, NASA-TM-4628, NASA, Washington, DC (1994).

[42] UNITED STATES DEPARTMENT OF ENERGY, Nuclear Energy Research and Development Roadmap: Report to Congress, DOE, Washington, DC (2010).

[43] UNITED STATES DEPARTMENT OF ENERGY, Light Water Reactor Sustainability Program: Integrated Program Plan, INL/EXT-11-23452, Rev. 5, Office of Nuclear Energy, Washington, DC (2017).

[44] INTERNATIONAL ATOMIC ENERGY AGENCY, On-line Monitoring for Improving Performance of Nuclear Power Plants, Part 1: Instrument Channel Monitoring, IAEA Nuclear Energy Series No. NP-T-1.1, IAEA, Vienna (2008).

[45] INTERNATIONAL ATOMIC ENERGY AGENCY, Advanced Surveillance, Diagnostic and Prognostic Techniques in Monitoring Structures, Systems and Components in Nuclear Power Plants, IAEA Nuclear Energy Series No. NP-T-3.14, IAEA, Vienna (2013).

[46] COBLE, J.B., RAMUHALLI, P., BOND, L.J., HINES, J.W., UPADHYAYA, B.R., Prognostics and Health Management in Nuclear Power Plants: A Review of Technologies and Applications, PNNL-21515, Pacific Northwest National Laboratory, Richland, WA (2012).

[47] JARDINE, A.K.S., DAMING, L., BANJEVIC, D., A review on machinery diagnostics and prognostics implementing condition-based maintenance, Mech. Syst. Signal Process. **20** (2006) 1483–1510.

[48] ELECTRIC POWER RESEARCH INSTITUTE, Guidelines for Instrument Calibration Extension/Reduction, Rev. 1: Statistical Analysis of Instrument Calibration Data, TR-103335-R1, EPRI, Palo Alto, CA (1998).

[49] NUCLEAR REGULATORY COMMISSION, On-line Testing of Calibration of Process Instrumentation Channels in Nuclear Power Plants, NUREG/CR-6343, Office of Nuclear Regulatory Research, Washington, DC (1995).

[50] ELECTRIC POWER RESEARCH INSTITUTE, On-line Monitoring of Instrument Channel Performance, TR-104965-R1 NRC SER, EPRI, Palo Alto, CA (2000).

[51] NUCLEAR REGULATORY COMMISSION, Technical Review of On-line Monitoring Techniques for Performance Assessment, Vol. 1: State-of-the-art, NUREG/CR-6895, Office of Nuclear Regulatory Research, Washington, DC (2006).

[52] NUCLEAR REGULATORY COMMISSION, ibid., Vol. 2: Theoretical Issues (2007).

[53] NUCLEAR REGULATORY COMMISSION, ibid, Vol. 3: Limiting Case Studies (2008).

[54] ELECTRIC POWER RESEARCH INSTITUTE, On-Line Monitoring of Instrument Channel Performance, Vol. 1: Guidelines for Model Development and Implementation, TR-1003361, EPRI, Palo Alto, CA (2004).

[55] ELECTRIC POWER RESEARCH INSTITUTE, ibid., Vol. 2: Model Examples, Algorithm Descriptions, & Additional Results, TR-1003579.

[56] ELECTRIC POWER RESEARCH INSTITUTE, ibid., Vol. 3: Applications to Nuclear Power Plant Technical Specification Instrumentation, TR-1007930.

[57] ELECTRIC POWER RESEARCH INSTITUTE, Guideline for On-line Monitoring of Nuclear Power Plant Instrument Channel Performance, TR-1022988, EPRI, Palo Alto, CA (2011).

[58] HUMBERSTONE, M., WOOD, B., HENKEL, J., HINES, J.W., An adaptive model for expanded process monitoring, Nucl. Technol. **173** (2011) 35–45.

[59] HINES, J.W., DAVIS, E., Lessons learned from the US nuclear power plant on-line monitoring programs, Prog. Nucl. Energy **46** (2005) 176–189.

Annex

STATUS REPORTS

This Annex comprises brief technical descriptions of salient features of several small modular reactor (SMR) concepts, with an emphasis on their instrumentation and control (I&C) systems architectures. A review of the advanced SMR R&D programme of the United States Department of Energy (DOE) can be found in Wood [A–1].

A–1. WESTINGHOUSE SMR (UNITED STATES OF AMERICA)

The Westinghouse SMR is a 200 MW(e) class integral pressurized water reactor (iPWR) concept with all primary components located inside the reactor vessel. The reactor core is a partial height conversion of the 17 × 17 fuel assembly. The control rod drive mechanism (CRDM) utilizes latch assemblies, interfaces with fuel and uses controls based on existing designs. The CRDM also uses a three coil magnetic jack. The eight reactor coolant pumps are three phase, horizontally mounted axial flow pumps. The reactor produces 225 MW(e) and 800 MW(th). The I&C system for the Westinghouse SMR is the OVATION based digital control system. This innovative, compact design incorporates the safety features and principles of the AP-1000. The I&C system is critically important with respect to the reliability and availability of the plant during normal operations and postulated design basis events. Westinghouse has embraced the continuing innovation in digital computer and graphic display technologies in the design of the I&C systems for the Westinghouse SMR as an integrated reactor design, while leveraging experience with proven I&C technology approved for use by the United States Nuclear Regulatory Commission (NRC) and currently being deployed in the AP-1000 plants under construction in several countries.

A–1.1. Fundamental design principles of the I&C system

The I&C system is designed to provide protection for safe reactor operation in all operating modes. The functional performance requirements, design bases, system descriptions and safety evaluations have been designed on the basis of the following fundamental principles:

(a) Independence: The I&C system addresses the independence requirements of General Design Criteria 13, 21, 22 and 24 of 10 CFR 50 [A–2], in addition to section 5.6 of IEEE 603-2009 [A–3]. The I&C design exhibits independence between redundant portions of a single safety system as well as between safety systems and associated systems. All aspects of independence, such as physical, functional, electrical and communications, are addressed in the design.

(b) Redundancy: Redundancy is used in the I&C systems to achieve system reliability goals and conformity with single failure criterion. The Westinghouse SMR design plans demonstrate they satisfy single failure criterion described in NRC Regulatory Guide 1.53 [A–4] and IEEE 603-2009 [A–3].

(c) Determinism: The I&C system output is designed to be predictable and repeatable. Input signals and system characteristics result in output signals through known relationships among the system states and responses to those states. The system produces the same outputs for a given set of input signals (and sequence of inputs) within well defined response time limits to allow timely completion of credited actions. Furthermore, the output of digital I&C and data communications systems are predictable and repeatable. Safety applications are being designed to conform to the performance and timing requirements for safety systems contained in IEEE 603-2009 [A–3].

(d) Simplicity: Simplicity is a principle design consideration for I&C systems for the Westinghouse SMR. Complexity is only added to the design of the I&C systems when required to enhance plant performance or safety.

A–1.2. I&C architecture for the Westinghouse SMR[1]

Figure A–1 illustrates the planned I&C architecture for the Westinghouse SMR. The lower portion of the figure includes the plant protection, control and monitoring functions. The protection and safety monitoring system (PMS) provides detection of off-normal conditions and actuation of appropriate safety related functions necessary to achieve and maintain the plant in a safe shutdown condition. The plant control system (PLS) controls non-safety related components in the plant that are operated from the main control room (MCR) or remote shutdown workstation. The diverse actuation system (DAS) is a non-safety related, diverse system that provides an alternative means of initiating reactor trip and actuating selected engineered safety features (ESFs). Each of these control and protection systems is based on those approved for use by the NRC in the AP-1000 plant design.

The non-safety related, real time data network, which horizontally divides Fig. A–1, is a high speed, redundant communications network that links systems of importance to the operator. Safety related systems are connected to the network through gateways and qualified isolation devices so that the safety related functions are not compromised by failures elsewhere. The plant protection, control and monitoring systems feed real time data into the network for use by the control room and the data display and processing system. The data display and processing (plant computer) system is implemented in a distributed architecture. The working elements of the distributed computer system are graphics workstations.

The upper portion of the figure depicts the control rooms and data display and processing system. The MCR is implemented as a set of compact operator consoles featuring colour graphic displays and soft control input devices. The graphics are supported by a set of graphics workstations that take their input from the real time data network.

A–1.3. I&C systems summary level description for the Westinghouse SMR[2]

The I&C systems comprised the PMS, PLS, DAS, operation and control centres system (OCS), data display and processing system, and the in-core instrumentation system. The control systems share a common hardware design and implementation philosophy. They are also functionally integrated to enhance responsiveness during plant transients.

The PMS provides detection of off-normal conditions and actuation of appropriate safety related functions necessary to achieve and maintain the plant in a safe shutdown condition. The system controls safety related components in the plant that are operated from the MCR or remote shutdown workstation. The PMS monitors key variables related to equipment mechanical limitations, and variables directly affecting the heat transfer capability of the reactor. Some limits, such as the over temperature ΔT set point, are calculated in the plant protection subsystem from other parameters because direct measurement of the variable is not possible.

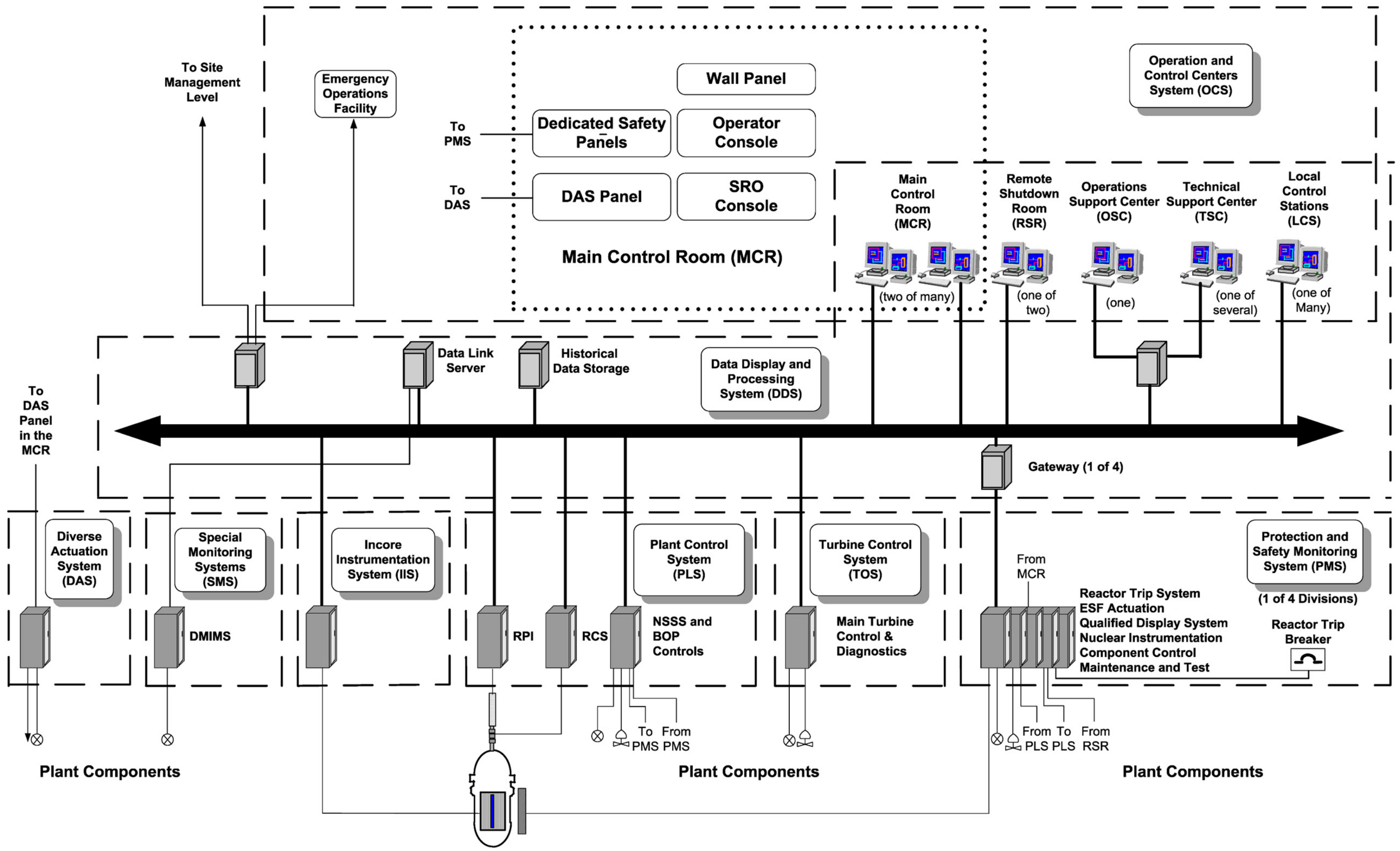
The PLS contains non-safety related control and instrumentation equipment to change reactor power, control pressurizer pressure and level, control feedwater flow, and perform other plant functions associated with power generation. The PLS provides automatic regulation of reactor and other key system parameters in response to changes in operating limits (load changes), while also providing the capability for manual control of plant systems and equipment.

The DAS, a non-safety I&C system diverse from the PMS, provides an alternative means of initiating reactor trip, actuating selected ESFs, and providing plant information to the operator. The PMS design includes features and its development and verification processes include measures to minimize the likelihood of common mode failures. However, in the low probability case where a common mode failure does occur, the DAS provides diverse protection.

The OCS includes the MCR, the technical support centre, the remote shutdown room, emergency operations facility, local control stations and associated workstations for these centres. The boundaries of the OCS for the MCR and the remote shutdown workstation are the signal interfaces with the plant components. These interfaces are via the PMS processor and logic circuits, which interface with the reactor trip and ESF plant components, the PLS processor and logic circuits, which interface with the non-safety related plant components, and the plant real time data network, which provides plant parameters, plant component status, and alarms. The control systems regulate the operating conditions in the plant automatically in response to changes in plant conditions and load demand. The first function of the ISS is to provide information to generate a three dimensional flux map of the

[1] This section is based on Ref. [A–5].

[2] This section is based on Ref. [A–5].



Source: Figure 7.1-1 of Ref. [A–5].

FIG. A–1. I&C architecture for the Westinghouse SMR.

reactor core. This map is used to calibrate ex-core detectors used by the PMS, verify that the core is operating within allowable power distribution limits, verify core design calculations and optimize core performance. The second function is to provide the PMS with core exit thermocouple signals required for post-accident monitoring.

A–1.4. Modular design and wireless technology in the Westinghouse SMR

Modularization of the Westinghouse SMR will enable integration of I&C systems within the plant construction modules so that many communication and control functions can be easily tested in the factory setting. Wiring within the modules can also be completed at the factory, allowing for significant simplifications in the routing of cables and runways in the field. While integrated tests are still required, the risk of encountering issues will be decreased and site acceptance test procedures will be less complicated.

A–1.5. Summary

The current I&C design for the Westinghouse SMR incorporates multiple innovative features that retrieve plant diagnostic information to support accident analysis and response planning and actions. Digital I&C systems with modern HFE promote greater operator understanding of plant status, easier automation of plant control, and rapid repair and replacement of any failed system components.

A–2. ACP100 (CHINA NATIONAL NUCLEAR CORPORATION, CHINA)

The ACP100, an iPWR that generates 310 MW(th) or about 100 MW(e), is being developed by the China National Nuclear Corporation (CNNC). It has four reactor coolant pumps connected to the reactor pressure vessel by short pipes. Sixteen once through steam generators are located in the reactor pressure vessel. Unlike other iPWR type SMRs, the pressurizer of ACP100 is located outside of the reactor vessel. The Nuclear Power Institute of China (NPIC) applies diversity in the design of I&C system through: (i) different hardware and software platforms for 1E and N1E I&C; (ii) the reactor protection system (RPS) with functional diversity; and (iii) diverse protection systems to cope with the common mode failure of the RPS. The ACP100 adopts passive safety system and integrated reactor design technology. The I&C system design for ACP100 will be based on the defence in depth concept, compliance with the single failure criterion and diversity.

A–2.1. Preliminary schemes of the main I&C systems of the ACP100 NSSS

A–2.1.1. General system configuration

The I&C systems of the ACP100 NSSS include the reactor nuclear instrumentation system, RPS, DAS, reactor control system, rod control and rod position monitoring system, reactor in-core instrumentation system, loose parts and vibration monitoring system and other process control systems (see Fig. A–2).

A–2.1.2. General control scheme

Liao et al. [A–6] report that:

> “The general control scheme for NSSS of the SMR is the automatic control combined with the manual control. The control systems of the NSSS have an automatic control range from 0 to 100% Full Power (FP), except for the RPC [reactor power control system] and FWC [steam generator feedwater control system], where the manual scheme is applied below 20% FP instead of the automatic scheme. The NSSS is operated at the corresponding power level according to the different load level. During the load following mode, the primary control principle is to maintain the main steam pressure and the average temperature of the reactor coolant at the specific constant respectively. According to the control system design, the reactor is capable of returning to the equilibrium condition automatically through the load variations transient in steps of ±10% FP or in continuous ramps with a gradient of ±5% FP/min.”

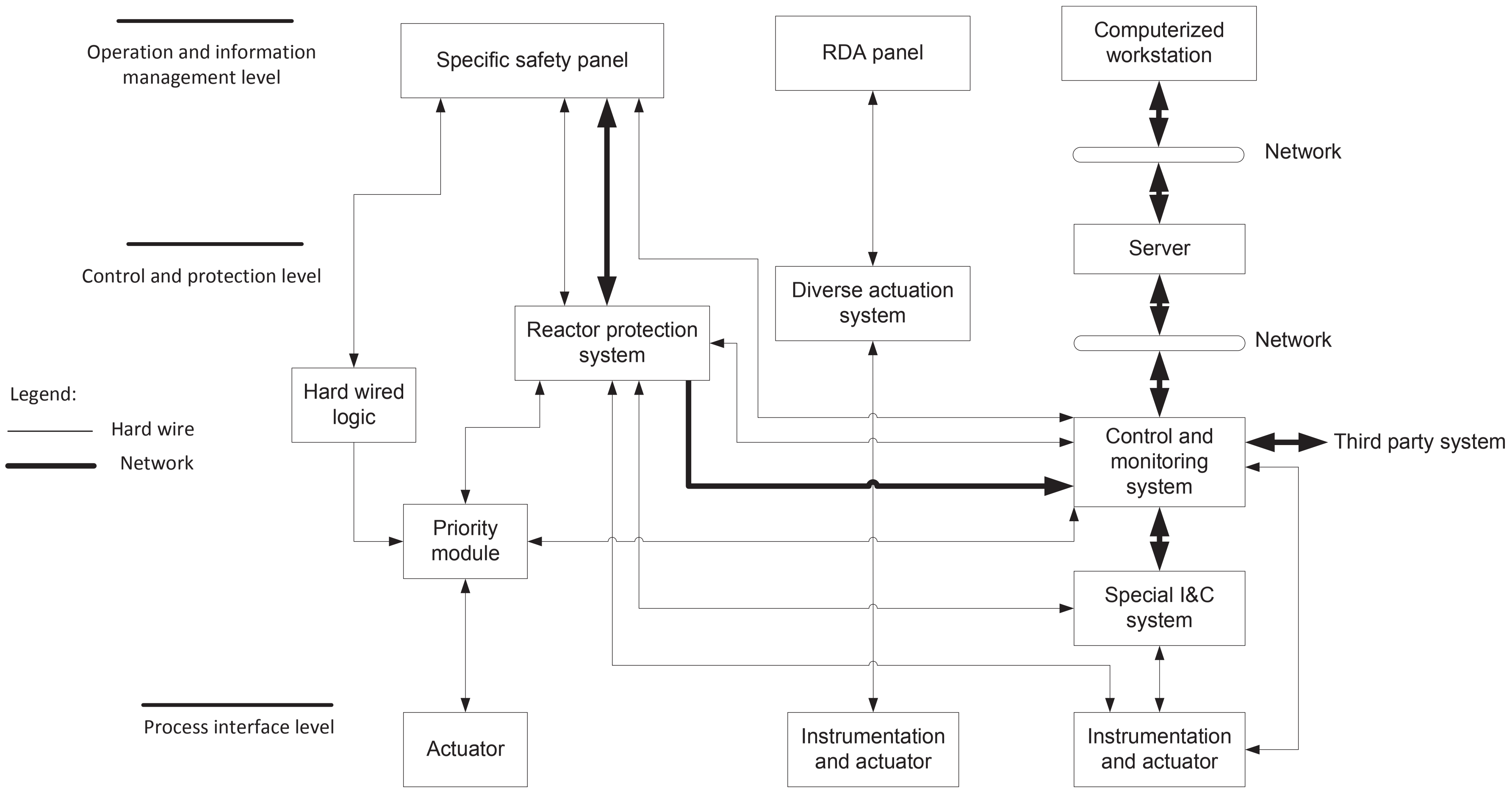


FIG. A–2. ACP100 I&C overall architecture.

A–2.2. Preliminary scheme of the systems

A–2.2.1. Reactor nuclear instrumentation system

The system uses information from three separate types (each type includes four independent channels) of instrument channel with a source range (10^{-9}–10^{-3}% FP), intermediate range (10^{-6}–100% FP) and power range (10^{-6}–200% FP) to provide three separate protection and monitoring levels.

A–2.2.2. Steam generator feedwater control system

Liao et al. [A–6] report that:

> “The functionality of the OTSG [once through steam generator] feed water control system is to maintain a fixed setpoint of the OTSG’s secondary side pressure and to make the feed water flow accommodate the load requirements by regulating the OTSG’s feed water flow.
>
> “During 0 to 20% FP, the feed water flow is controlled manually. [B]ypass control valves are used to adjust the feed water flow manually through the startup feed water line and the startup feedwater pump. During the 20% FP to 100% FP, the feed water flow is regulated automatically through the main Feed Water Pump (FWP), main Feed Water Valve (FWV) and the main feed water line.”

A–2.2.3. Reactor power control system

Liao et al. [A–6] report that:

> “The reactor power control (RPC) system includes two control channels: the temperature channel and the power mismatch channel. The temperature channel receives the average temperature measurement computed and adjusted from the core inlet and outlet temperature measurements, and compares it with the reference temperature (a fixed setpoint) and corrective signal is generated. The error between these two signals is the primary control signal of the RPC system. The power mismatch channel is a forward channel. This channel receives the nuclear power signal and the total feed water flow of the secondary side and adds their error to the temperature error signal. The final error signal is processed by the rod speed program, and then produces the control rod travel speed signal and two direction logic signals.”

A–2.2.4. Reactor in-core instrumentation system

The self-powered neutron detector and the thermocouple are integrated to the neutron and temperature detectors assembly. The standard signals are sent to the control cabinet through the internal network for displaying, storing and calculation. The design of in-core temperature measurement subsystem complies with the redundant principle (see Fig. A–3).

A–2.2.5. Diverse actuation system

The DAS is a non-safety system that provides a diverse backup to the reactor protection. Diversity between DAS and RPS is achieved by using different architectures, different hardware implementations and different software (see Fig. A–4).

A–2.2.6. Reactor protection system

The RPS of the ACP100 has a configuration of four redundant divisions. The functions of reactor trip and ESF actuation are completed by the four redundant protection divisions. Four redundant measurements, using four separate sensors, are made for each variable used for reactor trip (see Fig. A–5).

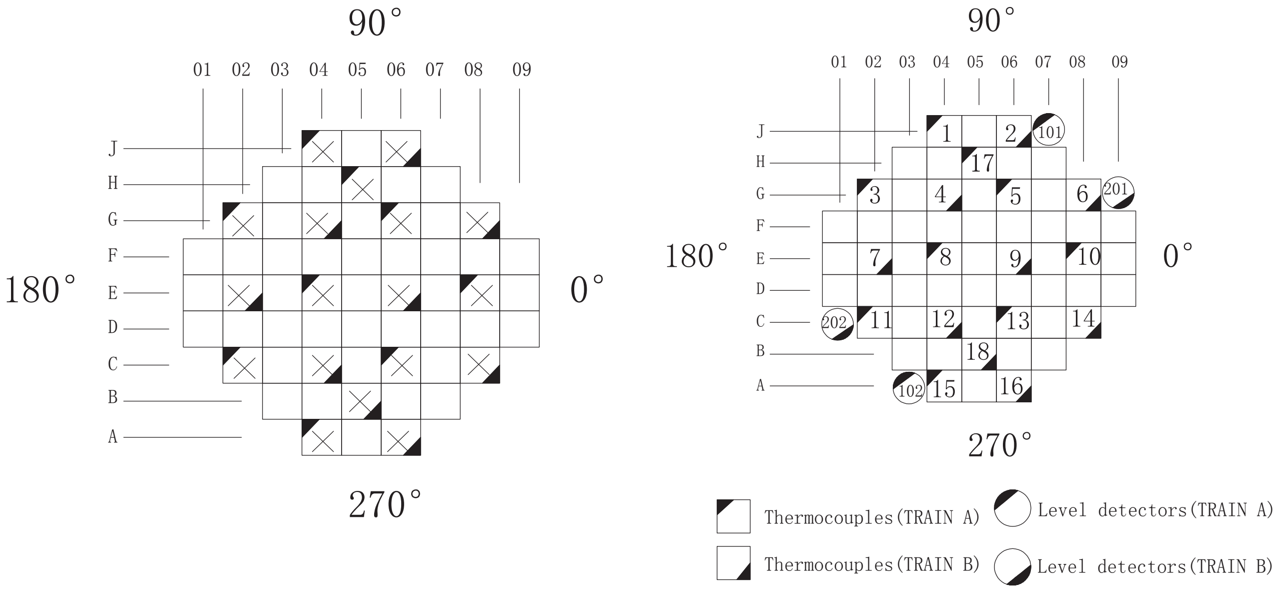


FIG. A–3. Layout of the detectors of the reactor in-core instrumentation system (courtesy of China National Nuclear Corporation).

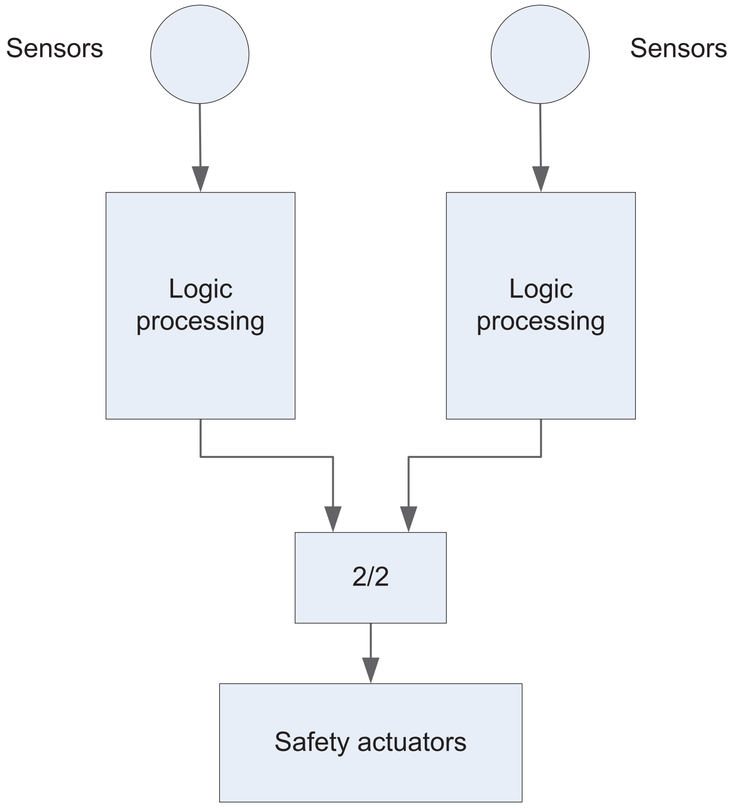


FIG. A–4. Diverse actuation system architecture.

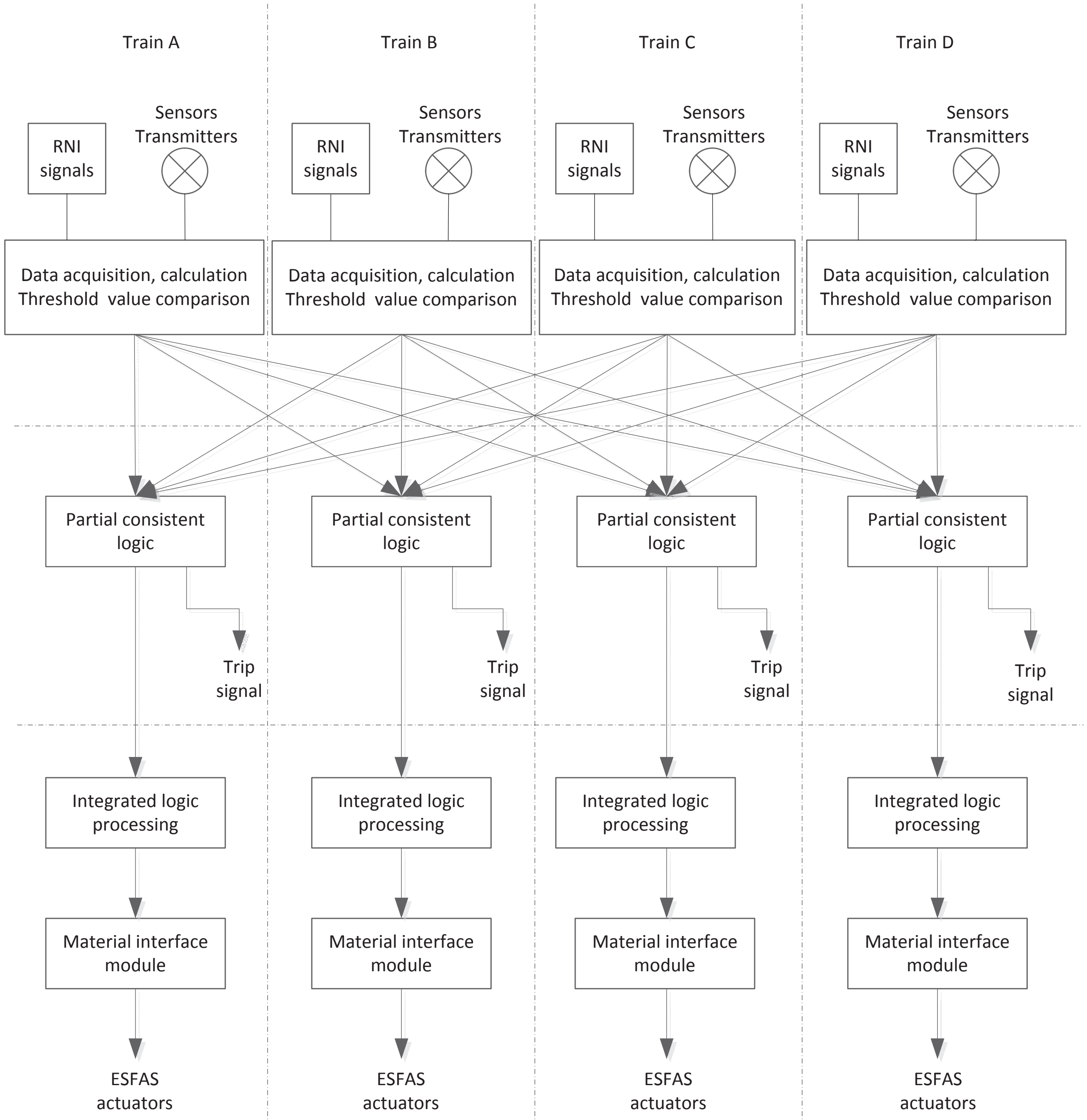


FIG. A–5. ACP100 Reactor protection system architecture (courtesy of China National Nuclear Corporation).

A–2.3. Summary

The ACP100 is being designed to use passive safety technology and integrated reactor technology and has high intrinsic safety. The standard design of the I&C system meets the control and operation requirements of the CNNC. The parameters of the control systems, MCR design and electricity supply plan have been optimized during the preliminary design for demonstration projects.

A–3. AHWR300-LEU (BHABHA ATOMIC RESEARCH CENTRE, INDIA)

AHWR300-LEU is a 300 MW(e), vertical, pressure tube type, heavy water moderated and boiling light water cooled natural circulation reactor designed in India. The fuel is designed to generate 65% of energy out of ^{233}U, which is bred in situ from thorium. Advanced heavy water reactor (AHWR) I&C systems include various equipment to perform display, monitoring, control, protection and safety functions. The general design concepts include redundancy, diversity, physical separation of channels, fail-safe behaviour, fault tolerance, testability and maintainability, and are extensively employed to maximize availability while ensuring safety. Microcontroller, computer based, triple modular redundant systems and triplicated hardwired systems are implemented with on-line testing facilities. The computer based systems are connected via redundant communication networks. The dual redundant server computers collect the process data from the systems. Dedicated, distributed data acquisition and analysis systems provide display and logging of data.

To maintain the system inventory feed water is fed to steam drums and the coolant circulation in the primary system is achieved by two-phase natural circulation. The main heat transport (MHT) system thus ensures that the fuel integrity is protected and radiological consequences are kept as low as reasonably achievable.

The safety goal for the AHWR is to achieve objectives for next generation nuclear reactor systems, such as reducing the probability of severe accidents and radioactivity release to near insignificant levels. Several innovative and passive technologies have been incorporated for normal reactor operation, decay heat removal, emergency core cooling and confinement of radioactivity to achieve this (see Fig. A–6).

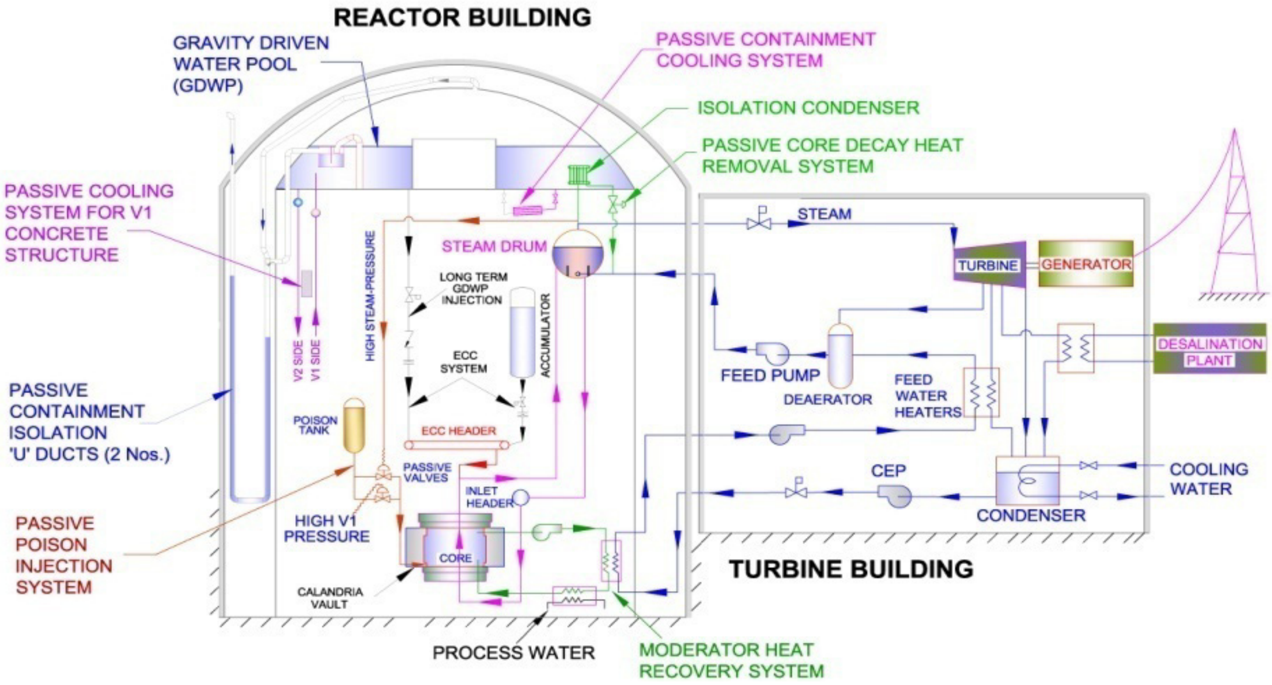


FIG. A–6. Advanced heavy water reactor (courtesy of Bhabha Atomic Research Centre).

A–3.1. I&C system architecture of the AHWR

The I&C systems of the AHWR use modern electronic technology. The design objectives met by the philosophy of defence in depth and redundancy have resulted in I&C systems of high reliability and availability, which meet stringent safety and operational requirements.

The I&C systems of the AHWR perform functions essential for the safety of the reactor in all operation modes. To enhance the reliability the process and I&C systems are divided into two diverse groups, in which the systems are classified as safety systems, safety related systems and systems not important to nuclear safety. Each group can perform safety functions independently. The MHT is well instrumented to monitor and control inventory, temperature, pressure and coolant chemistry. The safety systems are equipped with independent sensors and triplicated logic to meet single failure criterion and actuators.

A–3.2. Technological challenges

The driving force for natural circulation is proportional to the density difference, which is generally characterized by low driving pressure differences and hence low flow rates in natural circulation loops. The main design requirement of the AHWR is to maintain adequate thermal and stability margin. Hence, the channel flow and channel power monitoring instrumentation becomes very important for channel safety and integrity. Measurement of channel quality or void fraction is essential to obtain channel power. The technological challenges in this reactor are:

(a) To design and develop novel devices suitable for precise measurement of bidirectional low velocity flow;
(b) To develop sensors for void measurements and an algorithm to compute channel quality;
(c) To identify the occurrence of stagnation channel breaks;
(d) To trip the reactor if any of these parameters exceeds the safe limit.

A–3.3. R&D and experiments for demonstrating I&C systems of the AHWR

Development of instrumentation sensors for the measurement of low velocity, natural circulation, bidirectional flows and direct measurement of two-phase parameters such as void fraction, its distribution, two-phase flow and channel thermal power output is essential and a complex task. Prototype sensors and instrumentation systems are being developed and tested in a scaled experimental facility called an integral test loop (ITL), which simulates the MHT system of the AHWR for their performance evaluation.

A–3.3.1. Development of a bidirectional Venturi flow sensor

A novel, bidirectional Venturi flow sensor (see Figs A–7 to A–11) with optimum and equal converging/diverging cone angles has been designed and developed to monitor flow in all 452 coolant channels and a flow monitoring algorithm has been created. The sensor performance validation for reactor conditions is in progress in ITL. The salient features of this sensor are bidirectional flow measurement/flow reversal identification, good measurement sensitivity at low flow velocities, reasonably constant discharge coefficient for wide range of Reynolds numbers and low permanent pressure loss across the device.

A–3.3.2. Development of two-phase instrumentation

Developmental work on an electrical impedance based void sensor called Rotating electric field admittance probe and two-phase mass flux measurements using a pitot tubes assembly and traversing beam gamma ray densitometer and experimental qualification has been conducted. To compare the different methods, these sensors are planned to be qualified in the AHWR scaled experimental facility at high pressure and high temperature conditions.

A–3.3.3. Technique for channel power measurement

As these sensors need to be qualified for reactor applications, a technique has been created for channel power computation from two-phase pressure drop (ΔP) measurements in the vertical tail pipes of the AHWR. The differential pressure measured is used to obtain the density of the steam water mixture leaving the fuel channels and in turn void fraction in the pipe section. Knowing the quality, operating pressure and channel inlet temperature, the

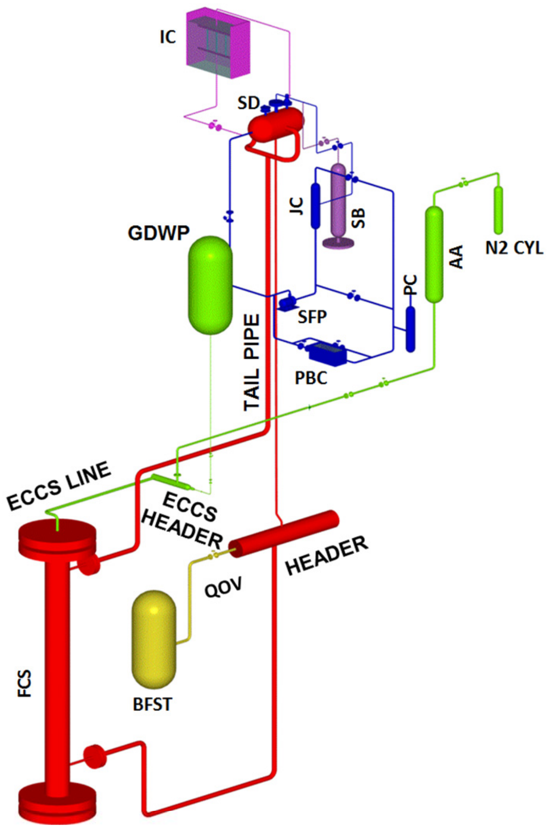


FIG. A–7. Integral test loop (courtesy of Bhabha Atomic Research Centre).

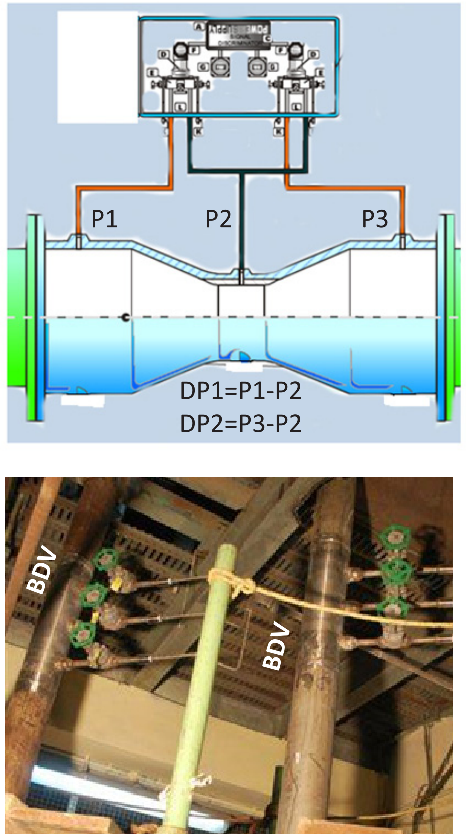


FIG. A–8. Bidirectional Venturi installed in an integral test loop (courtesy of Bhabha Atomic Research Centre).

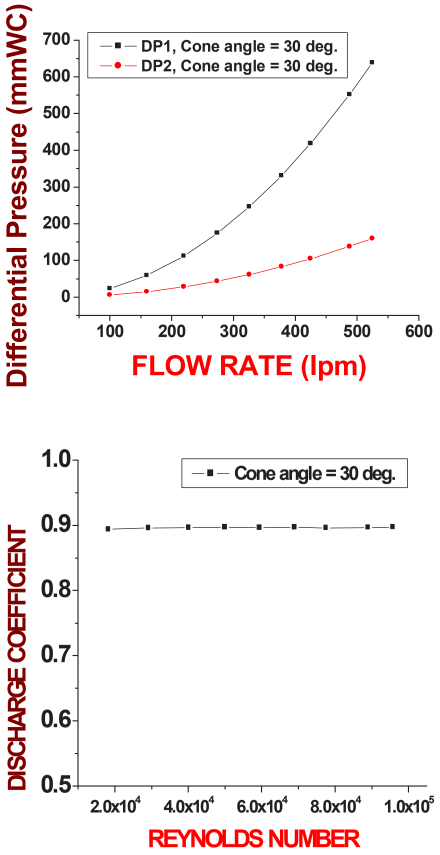


FIG. A–9. Experimental characteristics.

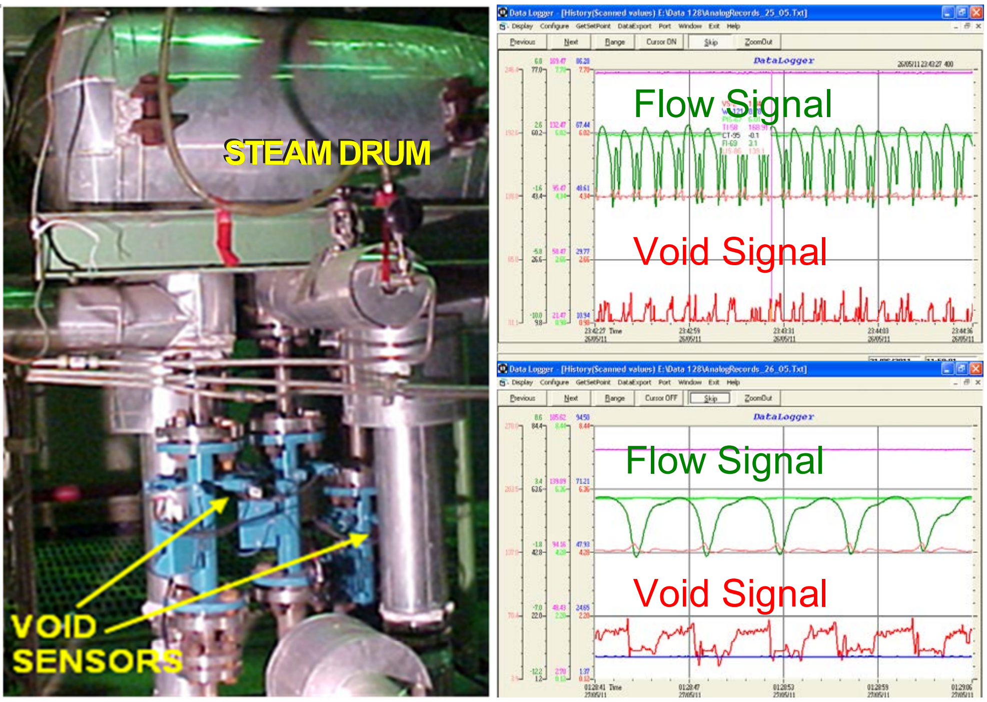


FIG. A–10. Steam water experimental facility and sensor response (courtesy of Bhabha Atomic Research Centre).

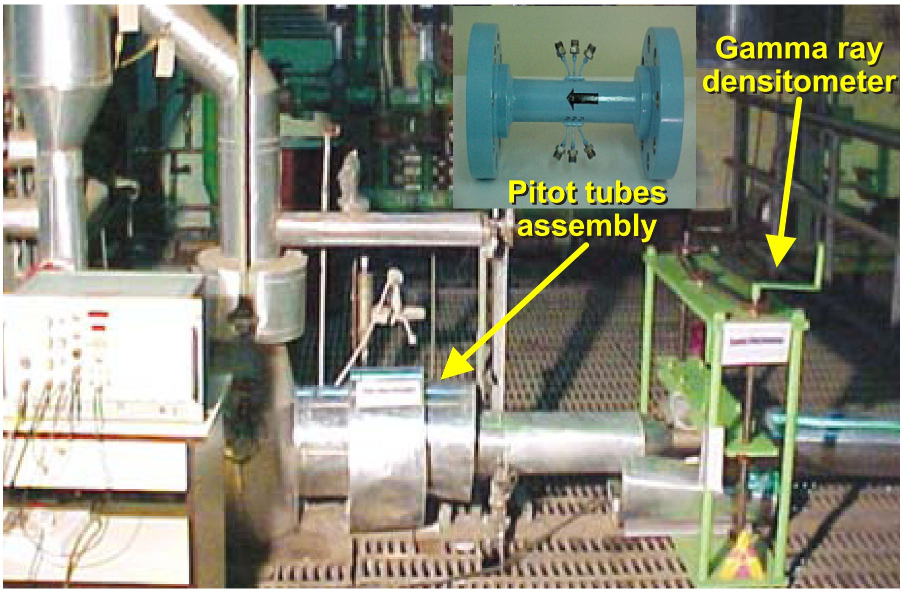


FIG. A–11. Pitot tubes assembly and gamma ray densitometer in experimental setup (courtesy of Bhabha Atomic Research Centre).

enthalpy at the core outlet and inlet can be calculated. Power in channel is estimated using the measured channel mass flow rate and channel inlet/outlet enthalpy.

A–3.3.4. Channel stagnation break identification

Small break loss of coolant accident (LOCA) detection is important for boiling pressure tube type reactors, since channel stagnation is expected if the break in one feeder is of a particular size. Consequences such as fuel overheating in that channel can be avoided if there is a trip on channel low flow. However, implementing low flow trips in all 452 channels is a very difficult task. Hence, steam leak detection becomes necessary to detect this

LOCA of various sizes. For prompt action following small break LOCA, a steam leak detection system has been developed to detect any leak inside the reactor vault. The detection technique is reliable and plays a very important role in ensuring the safety of the reactor. To identify this channel stagnation break occurrence, acoustic sensors to capture pressure variations and transients are provided in the reactor vault. The signals from these acoustic sensors, flow measurements in inlet feeders and void fraction measurements in tail pipes generate the reactor trip signal.

A–3.4. Summary

The channel flow, channel power and channel stagnation break identification are the important monitoring instrumentation for channel safety. All 452 channels in the AHWR are instrumented with in-house developed bidirectional Venturi flow meters for monitoring the forward flow and identifying any flow reversal during defuelling or refuelling. A robust technique of steam leak detection has been developed by acoustics method for channel stagnation break identification.

A–4. FLEXBLUE (DCNS, FRANCE)

Flexblue is a French, marine based, transportable reactor concept that is planned to be moored on the sea-floor to produce 160 MW(e). The plant will be run remotely from a shore control room, with no operator on board. Periodically, operators will access the submarine unit to maintain Flexblue during short time sessions. Studies have considered between two to six reactors, possibly with a shared control room. The Flexblue I&C system implements redundancies of trains, different levels of defence, especially on communication systems, technological diversification and the principle of reactor unit I&C autonomy.

The calculated accidental dose rate due to irradiation is strictly negligible, and a human external approach is possible. A submarine SMR has inherent, specific technical requirements that require dedicated I&C systems.

The Flexblue I&C system will be operated from a remote control room. The DCNS human factors approach permits the reduction of the operating team and the mutualization of the control room. DCNS has designed a robust I&C system based on its experience in the naval industry especially nuclear submarines. Ongoing studies include finding feasible technical solutions to the automation of maintenance operations, and remote control maintenance or reengineering of the equipment to eliminate the need for maintenance.

Safety studies have led to the consideration of different accident scenarios; the analysis of which has resulted in robust I&C system architecture. The I&C system of Flexblue implements redundancies of trains, different levels of defence especially for communication systems, technological diversification and the principle of reactor unit I&C autonomy.

A–4.1. Module autonomy

The main principles of I&C system of Flexblue are based on module autonomy, which is assured by having all the systems supporting the safety functions in the module. During incident or accident conditions, the reactor can be operated from both the local control room and the local remote shutdown station.

A–4.2. Simplification in operation and safety

The nuclear plant unit is exclusively operated from the MCR on the shore. The safety is improved with four operating areas in incident conditions: the MCR, the main remote shutdown station, the local control room and the local remote shutdown station. The Flexblue concept includes the possibility of multi-unit operations from a single control room in order to run a cluster of modules. Multi-unit operations drastically reduce the operating crew size (one operator per module).

A–4.3. Technological diversity

I&C and communications systems are based on different technologies, following the safety levels in conformity with IEC standards. Several possible solutions to allocate the classes of functions to the controllers are considered with different diversification schemes. The I&C system of Flexblue includes a diversified operating station, which enables safety function commands in cases of technological failure at the nominal station.

A–4.3.1. Decentralized I&C system

A decentralized I&C system means that tests and qualification can be conducted skid by skid. The maintenance is also more convenient and allows modular building and a better optimization of each system. Functions at the highest safety level need to be separated within redundant trains, which requires the centralization by train of the equipment which support these functions. The different buses and communication systems also require centralization.

A–4.3.2. Human factors approach

A strong human factors approach is necessary to manage the challenges of the tele-operation, including the management of a cluster of modules and the optimization of maintenance and operating crew size. A human factors analysis on the implementation of tele-operation includes activities such as maintenance on the module and work–time management.

A–4.3.3. Links between the shore and module

The communications system contains different levels, with a nominal communications system through submarine cables. An emergency communications system works via radio links, and ultimately via an acoustic link.

A–4.3.4. Maintenance, repair and operations

The current focus is on identifying functions which need local operations (on the site of production). For each identified operation, the feasibility of the automation or tele-operation is estimated, and solutions include system automation by I&C equipment, innovation or technological adaptation of existing applications (e.g. submarine feedback).

A–4.4. Summary

The two main challenges are the limitation of human interventions (automation) and the increase of reactor availability. The I&C system of Flexblue is highly reliable and allows the control room to be shared among several reactors, which makes it cost effective. Moreover, the autonomy of the safety functions of the I&C system located inside the module, its diverse technologies and the robustness of the communication systems all improve the overall safety of the reactor. Optimized I&C systems used in submarine SMRs can provide newcomer countries (and established ones) safe and cost effective solutions.

A–5. mPOWER (BABCOCK & WILCOX NUCLEAR ENERGY GENERATION MPOWER, UNITED STATES OF AMERICA)

The mPower SMR, designed by Babcock & Wilcox Nuclear Energy Generation mPower, United States of America, is an iPWR designed to generate an output of 180 MW(e). It adopts internal steam generators, an in-vessel CRDM, and horizontally mounted, canned motor pumps for its primary cooling circuit. The system is being designed with a high level of plant automation, including control for startup, shutdown and load following modes.

When more than one SMR unit is deployed at the same site, utilization of a single control centre is necessary to increase operational efficiency and to realize the full economic benefit of the small modular model. Control centre consolidation allows an overall reduction in the number of licensed operators required to run the plant without compromising safety, and also positively impacts capital cost as a result of reducing construction requirements. In addition, the sharing of balance of plant (BOP) systems provides significant benefits, both in terms of capital cost and personnel utilization. It is practical to separate their control functions from those of the SMR units into a single shared partition of the I&C system, so long as the functional independence of the units is maintained and plant safety is not compromised. New and evolving regulations are causing utilities to increase their focus on protecting critical digital systems. Thus, the I&C system design has not only to provide technical security controls, but it also has to be an integral part of the plant's computer security program.

A–5.1. mPower reactor assembly

The mPower reactor is an iPWR, in which the primary systems, pressurizer, pumps and steam generator are contained within the reactor vessel as one assembly (see Fig. A–12). The most notable architectural feature of mPower is the number of systems that are housed completely within the containment vessel. Not only the reactor core and control rods, but the control rod drive, steam generator and pressurizer are all integral to the reactor assembly. By housing the control rod drives within the reactor vessel, the drive mechanism can have a gravity driven, fail-safe design, so that all rods will drop into the core if electrical power fails. It also eliminates the possibility of a control rod ejection accident, since no part of the control rod drive system extends through a pressure boundary. Figure A–13 depicts a layout for an mPower two-unit site, with the turbine building adjacent to the corresponding cluster of underground containments.

One significant challenge of modularity is operator staffing. Although it is technically possible to design control systems that can operate the plant essentially autonomously, current NRC regulations require a reactor operator, a senior reactor operator and a supervisor for each reactor. This rule was established by the NRC for the current fleet of large nuclear plants. As the result, the required operator staffing level for multi-unit SMR plants might be higher than that of a large reactor plant with the same power capacity. The rationale behind staffing

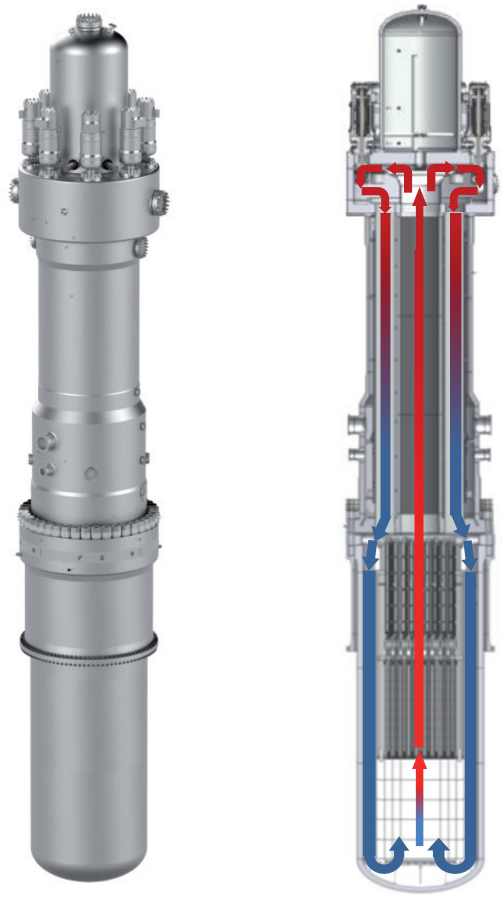


FIG. A–12. mPower SMR assembly (courtesy of Babcock and Wilcox Nuclear Energy).

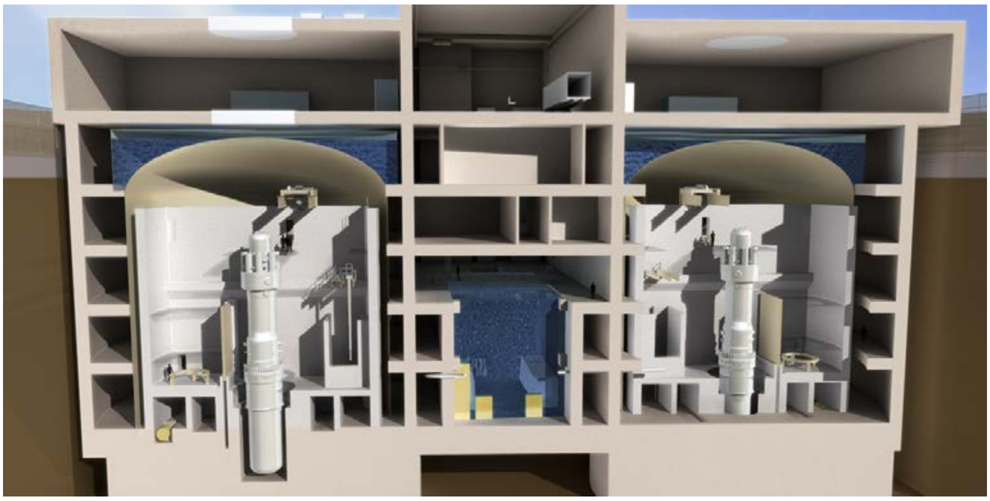


FIG. A–13. A two-unit SMR nuclear power plant (courtesy of Babcock and Wilcox Nuclear Energy).

regulations will need to be revisited by the NRC as mPower and other SMR plants with more capable I&C systems are brought into operation.

A–5.2. I&C system architecture

For a multi-unit mPower plant, the functional subsystems are grouped into four separate layers. The first layer is the inner most layer, which comprises the safety related portion of the system responsible for reactor protection and engineered safeguards features. The second layer comprises the main power generation control functions. The third layer contains the common system control functions for shared systems that are common to multiple units. The fourth or outer most layer performs the display, alarming and historical trending functions required by the plant operators. Figure A–14 demonstrates the functional architecture of the system with the four independent layers (each shown in different colour) separated by electrical isolation, which clearly distinguishes the physical separation of the monitoring, control and protection functions.

A–5.2.1. Data management (green)

This layer comprises the display, alarming and trending functions and consists of multiple data servers, workstations and video displays via a redundant communication network. This system is primarily responsible for collecting, processing, trending, storing and displaying all plant information required to assess the current performance of the plant and trend data for future maintenance actions.

A–5.2.2. Power generation (yellow)

This layer comprises the power generation control systems and consists of process controllers and input/output modules, data servers and video displays connected to a robust and redundant real time communication network. This portion of the system is responsible for the processing, controlling and displaying of all plant systems required for normal operation and shutdown of the nuclear reactor and its supporting systems.

A–5.2.3. Common equipment (blue)

For a multi-unit mPower plant, there can be a number of common supporting equipment to service all of the units at the same site. The utilization of the common equipment among the different units allows resource sharing, which reduces the operating costs of the plant. For the plant depicted in Fig. A–14, the common equipment layer provides the software and hardware necessary to control the equipment common to both Units 1 and 2. The

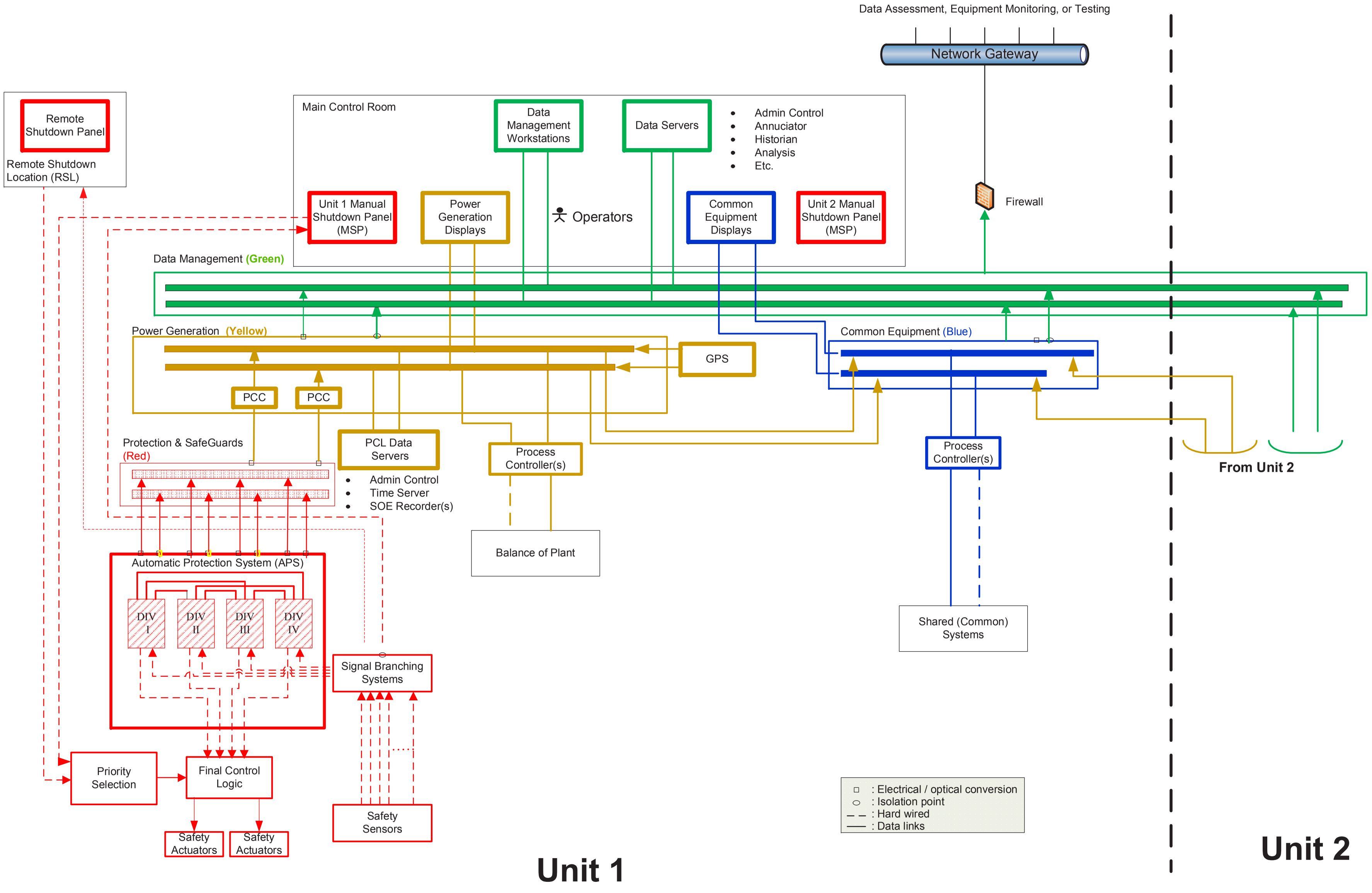


FIG. A–14. Representative I&C system architecture for a multi-unit SMR plant.

common equipment layer receives data from the power generation layers of the two units and provides data to the data management via one way, optically isolated links.

A–5.2.4. Protection and safeguards (red)

The inner most layer performs reactor protection and engineered safeguards functions and is an additional and separate layer that continuously monitors plant variables. It is responsible for automatically shutting down the plant if it detects that the plant management and control systems have not kept the plant within a predefined set of conditions. Furthermore, it will start any other required systems to mitigate the detected problem and place the plant in a safe state. The plant protection system has the following important characteristics:

(a) A physically separate system that generally does not share hardware and software with the plant management and control systems;
(b) Environmentally qualified for the harshest anticipated operating and accident conditions, including extreme natural hazards;
(c) Designed to shut down the reactor, trip the turbine generator, start the cooling water system, and go to preset conditions that are safe for the plant to maintain for extended periods;
(d) Designed to be single failure proof.

The four layers are separated by electrical isolation and physical separation providing separated monitoring, control and protection functions. Data communication through the layers is unidirectional from the inner most system outward and is implemented with one way communication between the layers. This will facilitate NRC certification of the design by clearly separating the safety, control and monitoring roles of the system elements. The highly distributed nature of the system network provides inherent scalability to allow future expansion of system components. A general description of the I&C system architecture is as follows:

- Each functional layer provides complementary control and monitoring capabilities that ensure independent backup of the plant operation and protection functions.
- Information flows from the bottom up so that the operators have full access to all plant status data while assuring that lower control and protection layers cannot be compromised by any single failure. This layered architecture also ensures that functions with lower criticality do not interfere with plant protection functions.
- The layered architecture allocates complex data management and display processing to the plant management layer while making the control and protection systems as simple as possible.
- Operational data are assessed and presented to plant operators at the outer most layer using automated tools, displays and annunciator functions for quick identification of potential problems in the plant control and protection systems.
- Manual control and plant safety system actuations bypass the automatic control and protection logic to ensure that the safe plant operation is always executed by the plant operators.
- Hardwired controls provide an independent backup means in the event of communication network faults. If network communications are lost, the necessary indicators and commands are available via hardwired meters and switches.

Each significant control and safety feature of the plant ensures that diversity and defence in depth principles are fully met. Defence in depth is based on multiple, independent, concentric barriers implemented by layering the plant I&C subsystems to mitigate the effects of a postulated common cause failure.

A–5.3. Human factors engineering issues

Human system interaction and human factors are key considerations in the design of digital I&C systems. The design objective is to reduce incompatibilities between the characteristics of the system and the characteristics of the people who operate and maintain it. Design considerations include the integration of plant automation, new information systems, new procedures, and any other aspect that changes the human–machine interaction. Control room and workstation layouts and plant alarm management methodology are two very important human factor features of an I&C system design.

A–5.4. Control room and workstation design

For multi-unit SMR plants like the mPower, the control room (or workstation) design has important technical and financial implications, and it requires extensive study and development. There is an ongoing effort in design, analysis and simulation of control rooms and workstations for SMR plants to optimize operational costs while meeting plant safety requirements.

A–6. SMART (KOREA ATOMIC ENERGY RESEARCH INSTITUTE, REPUBLIC OF KOREA)

The system-integrated modular advanced reactor (SMART) is an integral type reactor containing major components such as a pressurizer, steam generators and reactor coolant pumps in a single reactor pressure vessel. SMART has eight modular type once through steam generators, which comprise helically coiled tubes, four canned motor reactor coolant pumps and four channel control rod position indicators. This integrated arrangement enables the elimination of large bore piping, resulting in an inherent elimination of large break LOCAs. The eight modular once through steam generators produce superheated steam under normal operating conditions. The small inventory of the secondary side (tube side) water in each steam generator prohibits a return to power following a steam line break accident. Four reactor coolant pumps with a canned motor inherently prevent loss of coolant associated with a pump seal failure. The in-vessel pressurizer is designed to control the system pressure at a nearly constant level during all design basis events.

The in-vessel pressurizer is designed to control the system pressure at a near constant level during entire design basis events. The low power density design with a slightly enriched UO_2 fuelled core ensures a thermal margin of greater than 15%, which can accommodate any anticipated transient event. Reactivity control during normal operation is achieved using soluble boron and control rods, and burnable poison rods are introduced for a flat radial and axial power profile, which results in an increased thermal margin of the core. A man–machine interface system (MMIS) is used to provide control, protection and monitoring functions for SMART during normal, abnormal and accident conditions. The MMIS of SMART consists of I&C systems and a control room. The MMIS is designed with a layered structure based on full digital and information processing technology and communication network scheme. The features of an I&C system include the following:

- Alarm and indication system;
- Information processing system;
- Core protection system;
- RPS;
- ESF actuation control system;
- NSSS and BOP control systems, sensors and instrumentation;
- Radiation monitoring system;
- Automatic seismic trip system;
- Integrity monitoring system.

A–6.1. Sensors and instrumentation systems

The high reliability and performance of instrumentation systems is achieved using advanced features such as digital signal processing, remote multiplexing, signal validation and fault diagnostics, and sensing signal sharing.

The ex-core neutron flux monitoring systems comprise four safety channels and two startup channels. The neutron detectors of the four safety channels are installed in reactor vessel. The signals from the safety channels are shared for reactivity control system. The in-core instrumentation system comprises 29 detector assemblies, which are developed as mini type for SMART, with four stacked, rhodium self-powered detectors, one background detector and one set of K type thermocouples for each.

The core cooling monitoring system calculates the following:

- The core exit temperature, using thermocouples;
- The reactor water level, using nine stacked, heated and unheated, junction thermocouples;
- The subcooled margin, using pressurizer pressure sensors and resistance temperature detectors for steam generator in/out temperatures.

The primary integrity monitoring system consists of the following:

- The acoustic emission monitoring system for finding the location of leakage of the pressurizer safety valves, the reactor coolant pumps and the penetrations at the reactor vessel side;
- The loose part monitoring system at the primary coolant loops;
- The reactor coolant pump monitoring system.

A–6.2. Main control room

The SMART compact control room (or workstation) is designed to be operated by one person under normal plant conditions. The MCR is a key facility when dealing with any emergency situations, so it is designed to ensure that plant personnel successfully perform their tasks according to the proper operating procedures to maintain the plant in a safe condition. To achieve this, HFE process and principles are applied and verified using the full scope dynamic mock up. The three types of seated, compact workstations are:

(a) The safe shutdown workstation, which also contains a set of hardwired switches for manual actuation of ESF equipment and reactor trip;
(b) The main monitoring and control workstation;
(c) The auxiliary monitoring and control workstation and a large display panel installed in the MCR.

To resolve the human performance issues, elastic tiled alarm display method and alarm reduction method (prioritization and suppression) are adopted. Operators can easily do their motor tasks efficiently through soft control technology with a touch screen. A remote shutdown panel in the remote shutdown room provides hot standby operation when the MCR is not available due to fire or sabotage.

A–6.3. Information processing design

The information level in SMART comprises an alarm and indication system and an information processing system. The purpose of the information level is to provide the plant operating staff with various supervisory monitoring aids and to enable them to enhance plant operability and to lead the plant to safe states by adopting the primary and hot standby redundant concept for data processing servers and distributed graphic processing clients through a standard network. Safety parameters, functions and alarms are presented in a hierarchy and information is well organized with the optimized navigation concept. The availability of the information level is more than 99.5% by adopting the primary and hot standby redundant concept for data processing servers and distributed graphic processing clients through a standard network. The heartbeat interconnection between the primary and hot standby processor is used to detect a failure so that bumpless operating is achieved. The information processing system provides monitoring functions for the operational status of SMART:

(a) Critical function monitoring, as part of the safety parameter display system, is used to provide the monitoring functions in accordance with:
    - Core reactivity;
    - Core heat removal;
    - Reactor coolant inventory;
    - Reactor coolant pressure;
    - Reactor coolant system heat removal;
    - Pressure and temperature of the reactor building;

- Isolation of the reactor building;
- Release of radioactive materials and effluent gas.

(b) SMART core monitoring system, as a diverse function from SMART core protection system (SCOPS) monitors:
- Power operation limits of the departure from nuclear boiling and the local power density;
- Azimuth tilt;
- Axial offset;
- Power limit.

A–6.4. Protection and control system

The two major systems of the protection system are the RPS and the ESF actuation system. The basic structure of the system, which is responsible for performing the main functions, comprises four redundant trip channels, which are modularized by specific functions and segmented for functional diversity, and uses full digital technology with a designated safety communication network. It also adopts an embedded operating system (i.e. the scheduler, including the watch dog timer function, is developed). The digital protection system automatically shuts down the reactor whenever conditions reach the safety set points, and actuates the engineered safety systems to mitigate any consequences of an accident. SCOPS provides an alternative means to shut down the reactor. The safety grade I&C systems of SMART are designed with the newly developed safety grade platform, based on a digital signal processor with a system bus. The platform features a hard real time characteristics and an on-line periodic test for idle time. Control grade diverse means are additionally provided to prevent anticipated transient without scram.

The control systems comprise a power control system, secondary control system and process control system. The power control system performs reactor regulating control and CRDM control. The secondary control system includes the main steam pressure control system, feedwater control and turbine control system. The process control system manages various pumps and valves that are needed to maintain the normal operating condition of SMART. The control systems adopt module based design and standardized equipment to improve maintainability. To improve availability and reliability of the control systems, hot standby and duplex (redundancy) structures are also introduced into each system. Furthermore, safety and non-safety soft controllers with touch panels are designed to perform the control actions reliably. In summary:

(a) SCOPS is the hard, real time, computer system and provides:
- Reactor trip signal;
- Control rod driving mechanism withdrawal inhibit signal;
- Auxiliary trip;
- Reactor monitoring;
- Core element assembly position display.

(b) The RPS generates:
- Trip signals at a high log power;
- Variable overpower;
- Low and high pressurizer pressure;
- High and low main steam pressure;
- Reactor building high pressure;
- Low feedwater flow;
- Low reactor coolant pump flow;
- Loss of power for the reactor coolant pump;
- High local power density;
- Low departure nucleate boiling region;
- Reactor manual trip.

(c) The ESF control system comprises:
- Segmented group controllers;
- Loop controllers;
- Component interface modules;

— Multiplexers for minimum inventory switches;
— Maintenance and test panels.

(d) The power control system comprises:
— Reactor power control system;
— Control rod driving mechanism control system using insulated gate bipolar transistor technology;
— Reactor power cutback system.

(e) The process control system comprises:
— Diverse protection system;
— Pressurizer pressure control system;
— Pressurizer level control system;
— Chemical and volume control system;
— BOP control system.

A–6.5. Data communication system

The distributed control system (DCS) provides highly reliable data exchanges between intra and intersystems. The DCS architecture developed for SMART is based on the communication network technology. The design concepts include status based transmission, deterministic architecture, full separation and isolation, hard real time features, and adaptation of verifiable technologies. The safety DCS uses a dedicated communication protocol of the equipment, and the non-safety communication uses industrial standardized protocols. Each data communication system is redundant with a fault tolerant architecture to enhance the system availability and reliability.

The safety system signals which feed the non-safety systems are isolated using fibre optic cables, and data flow is unidirectional from safety to non-safety systems. Non-safety systems are not able to transmit any signals or data. The safety systems maintain their communication independence from the non-safety systems. The DCS is characterized with the following design features:

(a) Fixed access controls using time division multiplexing and switching methods;
(b) Fibre optic transmission medium;
(c) Separation and isolation between transmissions and receive paths;
(d) Point to point link architecture;
(e) More than 10 Mbps for each link connection;
(f) Critical fault management.

A–6.6. Technical requirements

A–6.6.1. Redundancy

In SMART, each safety system, including the core protection system, RPS and the ESF actuation control system, comprises four channels to meet the single failure criteria.

A–6.6.2. Defence in depth

SMART provides successive physical barriers against the release of radioactive material. Inherent and passive safety features, safety systems and ESFs prevent the possibilities of an abnormal event and mitigate the progress of the event if one arises.

A–6.6.3. Diversity

The diverse protection system provides the alternative trip means to meet the requirements of an anticipated transient without scram.

A–6.6.4. Data communications

The data communication system provides a communication means to MMIS. The systems of all levels are connected through a network for reliable data transmission and a lower cost for cables. The data communication system comprises the safety data communication system and the non-safety data communication system.

A–6.6.5. Computer security

Cyber-attacks have an adverse effect on the safety of a nuclear plant. Therefore, MMIS requires computer security measures that efficiently provide protection from a cyber-threat, and the computer security design needs to be considered during all development processes in MMIS.

A–6.6.6. Qualification of digital technologies

Hardware qualification conditions are a harsh environment and a mild environment. Every safety MMIS system and component installed in a harsh environment is tested, analysed and reported. Software qualification of SMART MMIS uses the software development life cycle, which includes planning, requirement analysis, design, implementation, integration and testing and installation, operation and maintenance stages. The software program manual is issued during the early stage of development.

A–7. HTR–PM (INSTITUTE OF NUCLEAR AND NEW ENERGY TECHNOLOGY, TSINGHUA UNIVERSITY, CHINA)

As one of the most popular Generation IV nuclear energy system, high temperature gas cooled reactors (HTGRs) have outstanding inherent safety features. The concept of a modular high temperature gas cooled reactor (MHTGR), first proposed by Reutler and Lohnert [A–7] at the end of the 1970s, is attractive because of its inherent safety features and potential economic competitiveness (for a review of joint projects by industry and research institutions and universities, see Refs [A–8, A–9]). China began research work on a pebble bed HTGR at the end of 1970s. After the Government of China approved a pebble bed test reactor in 1992, the 10 MW high temperature reactor (HTR-10) was designed and constructed by the Institute of Nuclear and New Energy Technology (INET), Tsinghua University, and it achieved full power in January 2003 [A–10].

Many studies have demonstrated that the multimodular approach offers a solution to retain both the inherent safety of HTGRs and sound economies of scale. Its use of many small reactors in conjunction with several shared turbines permits a simpler core design while, at the same time, at least partially retaining economies of scale by increasing the number of modules. Therefore, after the operation of HTR-10, the High Temperature Reactor–Pebble-Bed Module (HTR–PM) project was proposed and actively supported by the Government of China to build an MHTGR demonstration plant [A–11, A–12]. Taking advantage of the multimodular concept of MHTGRs, the HTR–PM is designed by INET in a double modular configuration and is under construction [A–12]. This configuration means that two 250 MW(th) NSSSs are connected to one 200 MW(e) turbine generator system (see Fig. A–15).

A–7.1. Partition and architecture of the I&C system

The I&C system of the HTR–PM has a safety and a non-safety system. The safety I&C system comprises the RPS and ESF actuation system of individual NSSS modules; and the non-safety I&C system is shared by all NSSS modules. The non-safety I&C system has layered structures and the following three layers:

(a) Detection and execution: The first layer comprises the sensors and actuators of the individual NSSS modules and BOP.

(b) Control: The second layer is the control system of the power generation process. This layer comprises process controllers and input/output modules, data servers and video displays connected to a robust and redundant real time communication network. This part of the I&C system is responsible for the processing, controlling

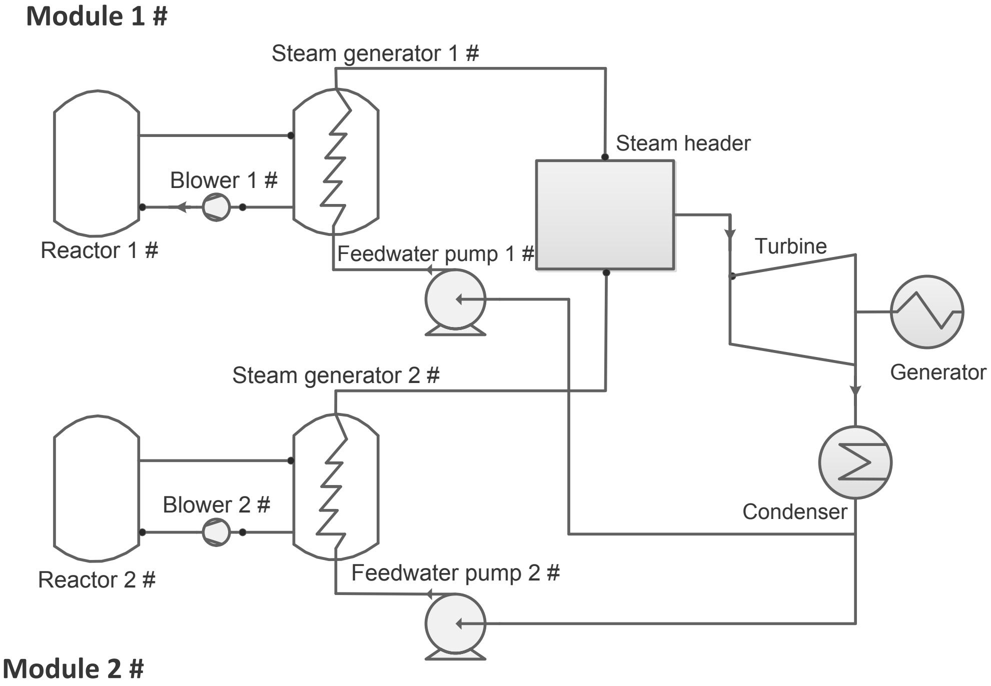


FIG. A–15. Diagram of the HTR–PM with double modules and one turbine generator.

and displaying of all plant systems required for normal operation and shutdown of the nuclear reactor and its supporting systems. The system receives data from safety I&C systems via one way isolated links.

(c) Human–machine interface: The third layer performs the display, alarming and historical trending functions required for plant operation. This layer comprises multiple data servers, workstations and video displays via a redundant communication network.

A–7.2. Main control room and operator staffing

When more than one NSSS module is deployed at the same site, utilization of a single control room can increase operational efficiency and realize the full economic benefit of a multimodular nuclear power plant. For the HTR–PM, a design of double NSSS modules and one BOP sharing a single MCR has been adopted. In sharing an MCR, each NSSS module is monitored and controlled by one operator. A total of four operators in the MCR is required for the HTR–PM: two reactor operators, a BOP operator and a supervisor.

A–7.3. Coordinated control strategy

On account of the strong coupling between two NSSS modules and one turbine of the HTR–PM when they are in the unbalanced load operation, an advanced coordinated control strategy needs to be developed to overcome this complex control challenge. Issues in the control of PWR type, multimodular reactor plants are discussed in Kim and Bernard [A–13], who emphasize the difference of operation strategies between single and multi-reactor systems. As for the HTR–PM, the MHTGR type nuclear power plant, the operation characteristics are significantly different from PWR type nuclear power plants. Thus, the traditional control strategy for multimodular PWRs can hardly be a suitable coordinated control strategy for the HTR–PM.

Based on analysis of the complicated, dynamic characteristics of the HTR–PM, some new coordinated control strategies have recently been studied, such as decoupling control, optimum control, non-linear adaptive control and intelligent control methods. Corresponding to the layered structures of non-safety I&C system, a layered control structure of the HTR–PM is proposed (see Fig. A–16).

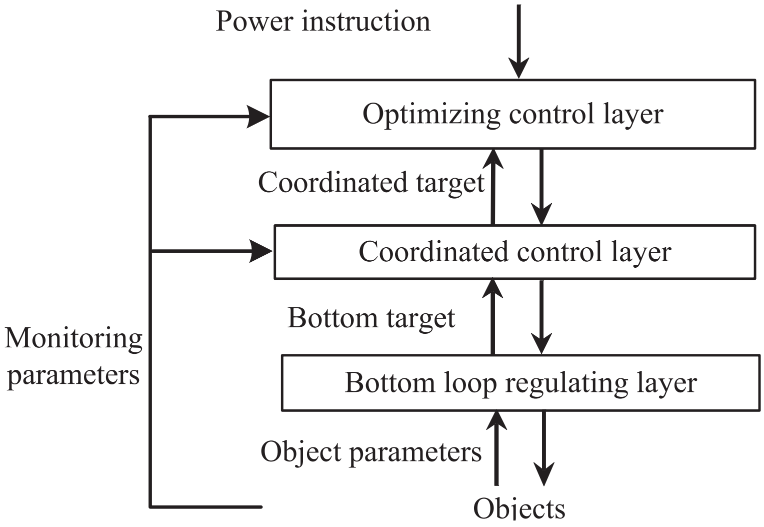


FIG. A–16. The control strategy with layered structure of the HTR–PM.

The three layers include the following:

(a) Bottom loop regulators act as the subcontrollers for the cascade controllers in the coordinated control layer. The three single loop, proportional–integral–derivative designed include the nuclear power regulator, helium flow regulator and feed water flow regulator.
(b) Coordinated controllers implement a decoupling control strategy to solve the tight coupling control variable inside a modular reactor. The three cascade controllers designed include the hot helium temperature controller, steam temperature controller and reactor thermal power controller.
(c) Optimizing controllers implement multivariables and multi-objectives to solve the complex coupling characteristics between modules. According to the functions, the optimizing control layer is partitioned as load instruction centre, state distinguishing unit and assistant operation service unit.

A–8. SVBR-100 (AKME-ENGINEERING, RUSSIAN FEDERATION)

The lead–bismuth cooled fast reactor (SVBR-100) is an innovative design based on existing Russian reactors with liquid metallic coolant (see Fig. A–17). Its main features include the following:

(a) High level of inherent self-protection and passive safety and significant simplification of the design of the reactor as well as the entire nuclear power plant;
(b) Possibility to operate with different types of fuel in different fuel cycles (period of operation without refuelling is not less than 7–8 years);
(c) Compact design and maximum factory readiness;
(d) Possibility of creating module based structured nuclear power plants with power multiplying by adding reactors.

A–8.1. Main design elements and parameters

The main design elements include a reactor integral arrangement in a robust vessel, surrounded by the safety body, and hydraulic connections of coolant among primary circuit equipment formed by the reactor vessel and internals elements, without pipelines and furniture (see Fig. A–18).

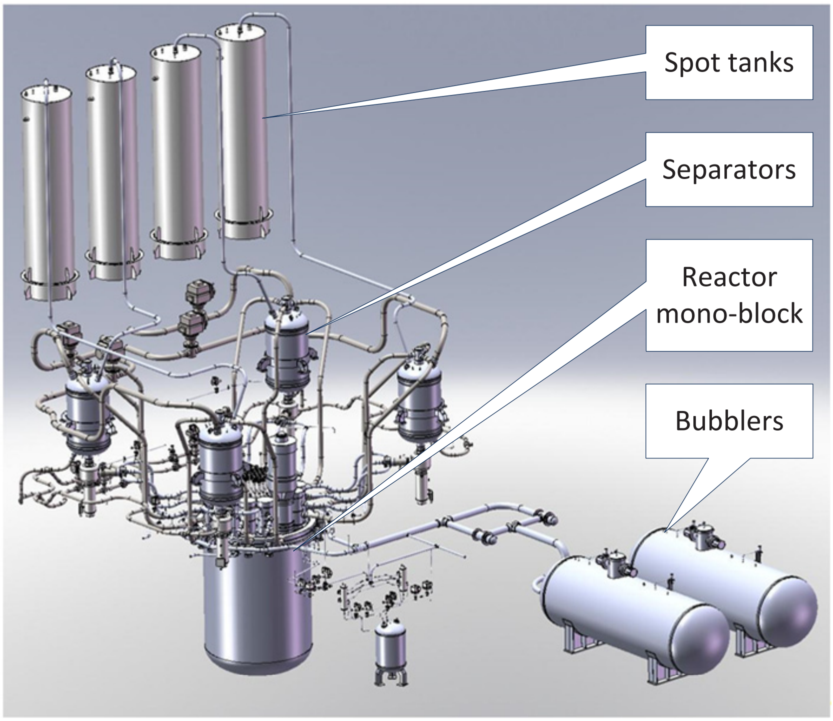


FIG. A–17. Simplified diagram of the SVBR-100.

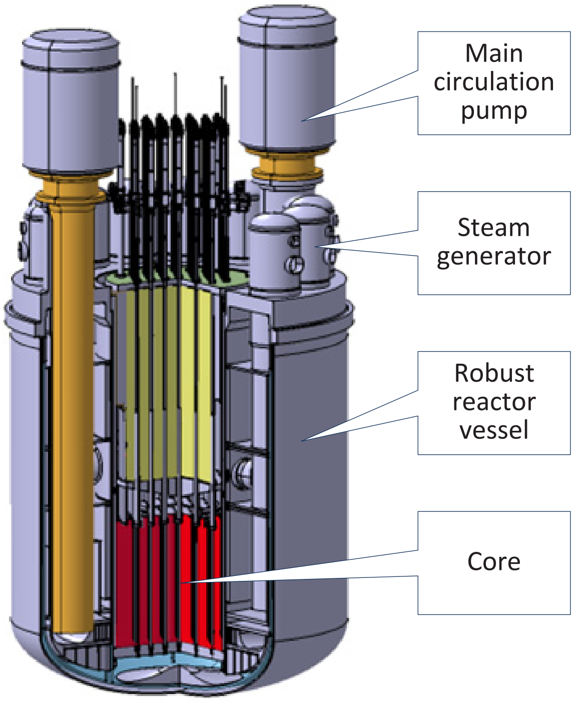


FIG. A–18. The SVBR-100 monoblock design.

The main process parameters are the following:

- Thermal power: 280 MW;
- Steam generation rate: 580 t/h;
- Steam pressure: 6.7 MPa;
- Coolant temperature at inlet/outlet: 345/495°C;
- Time period between refuelling: 7–8 years.

A–8.2. Main principles and characteristics

The main principles of the design include the following:

- Distributed I&C system with several levels of hierarchy and defence in depth;
- Soft control of nuclear power plant technological systems;
- Large screen and reserve zone in the MCR;
- Principles such as diversity, reliability and physical separation providing a high level of functional reliability, including protection against common cause failures;
- Well developed diagnostic functions;
- Self-diagnostic of I&C programmable devices.

Design characteristics include the following:

- Regulation of coolant flow rate by changing rotation speed of the main coolant pump, depending on reactor power for maintaining constant coolant heat up;
- Full scope diagnostic system of the nuclear power plant;
- I&C operability during 7–8 years of continuous nuclear power plant operation;
- New tasks of neutron flux monitoring while core refuelling;
- Highly reliable reactor control at startup and operation;
- Load follow operation in the deep range (100–50–100%).

More information is available in Refs [A–14, A–15].

A–9. IRIS (IRIS INTERNATIONAL CONSORTIUM, ITALY)

IRIS is an iPWR concept to produce 335 MW(e) and 1000 MW(th). The concept was initially developed by a Westinghouse led consortium, and Politecnico di Milano, Italy, is continuing the development effort. The small reactor is light water cooled and forced circulation in its primary cooling circuit. Due to its integral configuration, a variety of accidents are either eliminated or their consequences and probability of occurring are greatly reduced by the design (i.e. with no intervention of either active or passive systems). In fact, 88% of class IV accidents (i.e. the possibility of radiation release) are either eliminated or downgraded. This provides a high level of defence in depth.

A–10. CAREM (NATIONAL ATOMIC ENERGY COMMISSION, ARGENTINA)

CAREM-25 is a water cooled small reactor designed by the National Atomic Energy Commission (Comisión Nacional de Energía Atómica, CNEA) to generate 27 MW(e) and 100 MW(th) with minimal operator control. Its primary cooling circuit is fully contained in the reactor vessel, thus eliminating the possibility of a LOCA. Heat removal from the core is performed by natural convection, which drives the primary flow and excludes the need for primary coolant pumps. Its startup pressurization is achieved by balancing vapour production and condensation in the vessel. CAREM-25 differs from other integral concepts by not having any active device controlling the system pressure. Therefore, the linked phenomena in operation of the plant cause it to behave differently from conventional LWRs.

A–11. NUSCALE (NUSCALE POWER, UNITED STATES OF AMERICA)

NuScale is an SMR concept developed in the United States of America for a plant that can comprise 1–12 independent reactor modules, each capable of producing a net electric power of 45 MW(e). Each module includes an iPWR operated under natural circulation, primary flow conditions. A NuScale module adopts a set of internal helical coil steam generators. Each reactor is housed within its own high pressure containment vessel, which is submerged under water in a stainless steel lined concrete pool. The current design proposes one operator controlling four reactor modules. Comprehensive HFE and human system interface studies are underway to determine the optimum number of reactors that can be effectively and safely controlled by a single operator.

A–12. KLT-40S (OKBM AFRIKANTOV, RUSSIAN FEDERATION)

KLT-40S is a PWR developed in the Russian Federation for a floating nuclear power plant. It is based on the commercial KLT-40 marine propulsion plant and is an advanced variant of reactor plants that power nuclear icebreaker ships. The floating nuclear power plant with a KLT-40S reactor can be manufactured in shipyards and can then be delivered to the customer fully assembled, tested and ready for operation. The reactor has a modular design with the core, steam generators and main circulation pumps connected with short nozzles. The reactor has a four loop system with forced and natural circulation, a pressurized primary circuit with canned motor pumps and leaktight bellow type valves, a once through coiled steam generator and passive safety systems.

A–13. VBER-300 (OKBM AFRIKANTOV, RUSSIAN FEDERATION)

VBER-300 is a medium sized, Russian power reactor that generates 325 MW(e) and 917 MW(th) for land based nuclear power plants and nuclear cogeneration plants, as well as for floating nuclear power plants. The VBER-300 design is a result of the evolution of modular marine propulsion reactors. The thermal power increase is due to an increase in mass and overall dimensions, while the reactor’s appearance and main design solutions are kept as close as possible to those of marine propulsion reactors. Reactivity control is managed by rod insertion and boron dilution. VBER-300 has two independent safety trains for both active and passive emergency safety and residual heat removal systems.

REFERENCES TO THE ANNEX

[A–1] WOOD, R.T., “US Department of Energy instrumentation and controls technology research for advanced small modular reactors”, Progress of Nuclear Safety for Symbiosis and Sustainability: Advance Digital Instrumentation, Control and Information Systems for Nuclear Power Plants (YOSHIKAWA, H., ZHANG, Z., Eds), Springer, Tokyo (2014).

[A–2] NUCLEAR REGULATORY COMMISSION, Domestic Licensing of Production and Utilization Facilities, 10 CFR 50, Appendix A to Part 50.

[A–3] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations, IEEE 603-2009, IEEE, Piscataway, NJ (2009).

[A–4] NUCLEAR REGULATORY COMMISSION, Application of the Single-Failure Criterion to Safety Systems, Regulatory Guide 1.53, Rev. 2, Office of Nuclear Regulatory Research, Washington, DC (2003).

[A–5] NUCLEAR REGULATORY COMMISSION, Westinghouse AP1000 Design Control Document Rev. 19, ML11171A500, Tier 2 Ch. 7: Instrumentation and Controls,
www.nrc.gov/docs/ML1117/ML11171A500.html

[A–6] LIAO, L., YOU, K., CHEN, Z., The automatic control design and simulation of reactor control system in small modular reactor, Nucl. Safety Simul. **5** (2014) 23–28.

[A–7] REUTLER, H., LOHNERT, G.H., Advantages of going modular in HTRs, Nucl. Eng. Des. **78** (1984) 129–136.

[A–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Current Status and Future Development of Modular High Temperature Gas Cooled Reactor Technology, IAEA-TECDOC-1198, IAEA, Vienna (2001).

[A–9] KADAK, A.C., MIT pebble bed reactor project, Nucl. Eng. Technol. **39** (2007) 95–102.

[A–10] XU, Y., HTGR advances in China, Nucl. Eng. Int. **50** (2005) 22–25.

[A–11] ZHANG, Z., YU, S., Future HTGR developments in China after the criticality of the HTR-10, Nucl. Eng. Des. **218** (2002) 249–257.

[A–12] ZHANG, Z., SUN, Y., Economic potential of modular reactor nuclear power plants based on the Chinese HTR–PM project, Nucl. Eng. Des. **237** (2007) 2265–2274.

[A–13] KIM, K.K., BERNARD, J.A., Considerations in the control of PWR type multimodular reactor plants, IEEE Trans. Nucl. Sci. **41** (1994) 2686–2697.

[A–14] ANTYSHEVA, T., BOROVITSKY, S., SVBR-100: New Generation Power Plants for Small and Medium-Sized Power Applications (2011), www.iaea.org/NuclearPower/Downloadable/Meetings/2011/2011-07-04-07-08-WS-NPTD/2_RUSSIA_SVBR_AKME-eng_Antysheva.pdf

[A–15] SIVOKON, V., KONOPLEV, N., Russian Nuclear Power Development: Main Achievements and NPPs I&C Issues (2013), www.iaea.org/NuclearPower/Downloadable/Meetings/2013/2013-05-22-05-24-TWG-NPE/day-1/17.russia_presentation.pdf

ABBREVIATIONS

4S	Super-Safe, Small and Simple
ACP	Advanced China Power
AHWR	advanced heavy water reactor
BARC	Bhabha Atomic Research Centre
BOP	balance of plant
CANDU	Canada deuterium–uranium
CAREM	Central Argentina de Elementos Modulares
CNEA	National Atomic Energy Commission (Comisión Nacional de Energía Atómica)
CNNC	China National Nuclear Corporation
CRDM	control rod drive mechanism
DAS	diverse actuation system
DOE	United States Department of Energy
EM^2	Energy Multiplier Module
ESF	engineered safety features
FP	full power
FPU	floating power unit
GE	General Electric
HFE	human factors engineering
HTGR	high temperature gas cooled reactor
HTR–PM	High Temperature Reactor–Pebble-Bed Module
HWR	heavy water reactor
I&C	instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
INET	Institute of Nuclear and New Energy Technology
iPWR	integral pressurized water reactor
IRIS	International Reactor Innovative and Secure
ISO	International Organization for Standardization
KAERI	Korea Atomic Energy Research Institute
LEU	low enriched uranium
LMFR	liquid metal fast reactor
LOCA	loss of coolant accident
LWR	light water reactor
MCR	main control room
MHT	main heat transport
MHTGR	modular high temperature gas cooled reactor
MMIS	man–machine interface system
MSR	molten salt reactor
NRC	United States Nuclear Regulatory Commission
NSSS	nuclear steam supply system
NPIC	Nuclear Power Institute of China
O&M	operations and maintenance
OECD	Organisation for Economic Co-operation and Development
OECD/NEA	OECD Nuclear Energy Agency
OKBM	Afrikantov Experimental Design Bureau for Mechanical Engineering
OLM	on-line monitoring
PBMR	pebble bed modular reactor
PLS	plant control system
PMS	protection and safety monitoring system
Polimi	Politecnico di Milano

PRISM	Power Reactor Innovative Small Modular
PWR	pressurized water reactor
RCS	reactor coolant system
RDIPE	Research and Development Institute of Power Engineering
RPS	reactor protection system
RTD	resistance temperature detector
SDP	surveillance, diagnostics and prognostics
SFR	sodium cooled fast reactor
SMART	system-integrated modular advanced reactor
SMR	small modular reactor
SSCs	structures, systems and components
SVBR	lead–bismuth cooled fast reactor
TNPP	transportable nuclear power plant
TRISO	tristructural isotropic
VBER	water modular power reactor

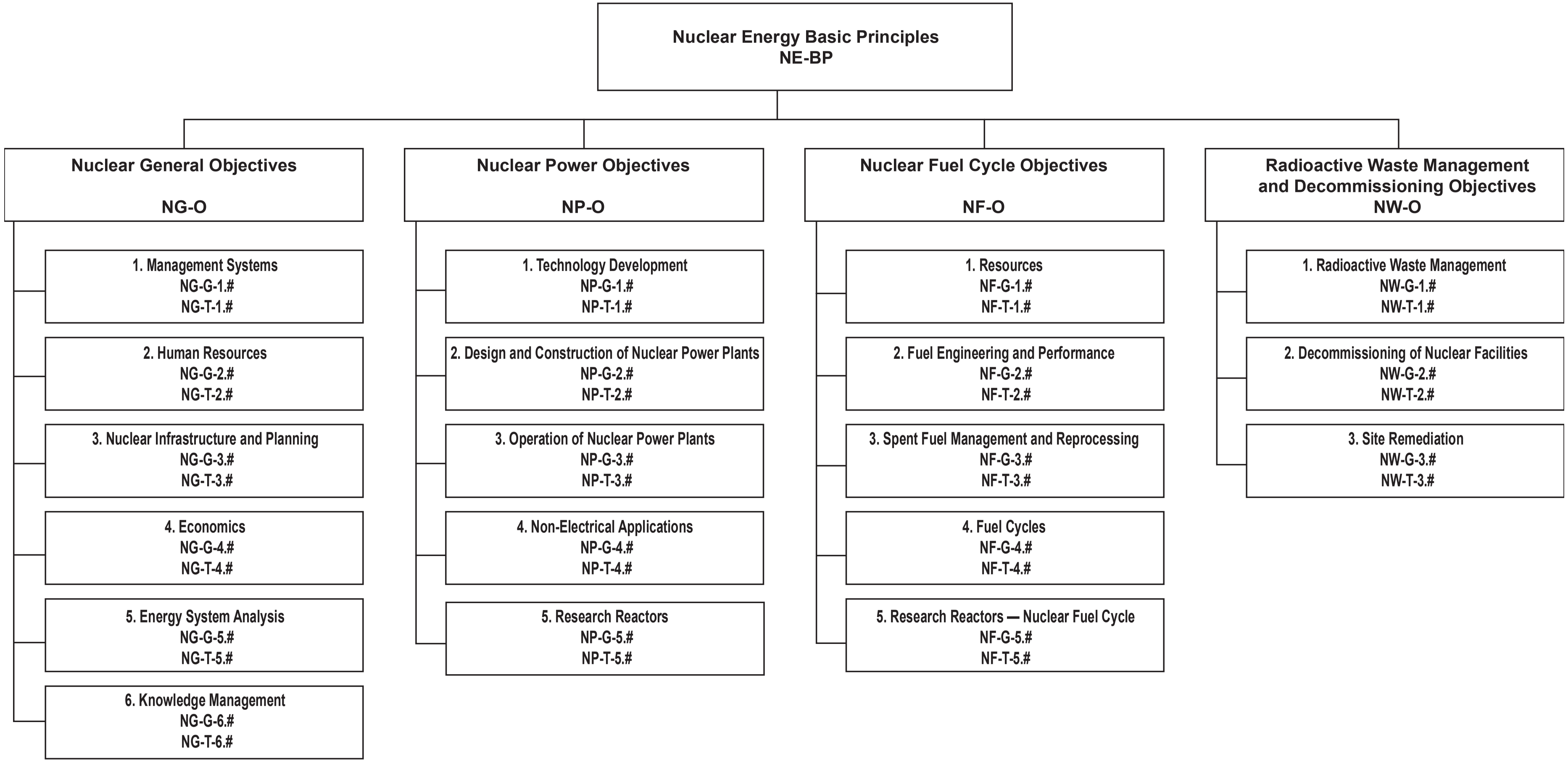
CONTRIBUTORS TO DRAFTING AND REVIEW

Arnholt, B.K.	Babcock and Wilcox mPower, United States of America
Ashcraft, J.M.	Nuclear Regulatory Commission, United States of America
Boyer, S.	DCNS, France
Chen, Z.	Nuclear Power Institute of China, China
Das, P.	Bhabha Atomic Research Centre, India
De Vos, M.	Canadian Nuclear Safety Commission, Canada
Eiler, J.	International Atomic Energy Agency
Fittipaldi, A.	National Atomic Energy Commission, Argentina
Glockler, O.	SunPort SA, Switzerland
Hines, W.	University of Tennessee, United States of America
Holcomb, D.	Oak Ridge National Laboratory, United States of America
Huang, X.	Tsinghua University, China
Jilani, G.	International Atomic Energy Agency
Koo, I.S.	Korea Atomic Energy Research Institute, Republic of Korea
Mossman, T.	Nuclear Regulatory Commission, United States of America
Park, J.Y.	Korea Atomic Energy Research Institute, Republic of Korea
Paserba, K.	Westinghouse Electric Corporation, United States of America
Ponciroli, R.	Politecnico di Milano, Italy
Rajalakshmi, R.	Bhabha Atomic Research Centre, India
Ricotti, M.	Politecnico di Milano, Italy
Riggsbee, E.	Analysis and Measurement Services, United States of America
Sivokon, V.	Rosenergoatom, Russian Federation
Subki, M.H.	International Atomic Energy Agency
Upadhyaya, B.	University of Tennessee, United States of America
Wood, R.	Oak Ridge National Laboratory, United States of America
Zahid, M.	International Atomic Energy Agency

Technical Meeting
Vienna, Austria: 21–24 May 2013

Consultants Meetings
Vienna, Austria: 19–22 November 2013, 5–9 May 2014, 16–20 March 2015

Structure of the IAEA Nuclear Energy Series


Nuclear Energy Basic Principles
NE-BP
Nuclear General Objectives
NG-O
1. Management Systems
NG-G-1.#
NG-T-1.#
2. Human Resources
NG-G-2.#
NG-T-2.#
3. Nuclear Infrastructure and Planning
NG-G-3.#
NG-T-3.#
4. Economics
NG-G-4.#
NG-T-4.#
5. Energy System Analysis
NG-G-5.#
NG-T-5.#
6. Knowledge Management
NG-G-6.#
NG-T-6.#
Nuclear Power Objectives
NP-O
1. Technology Development
NP-G-1.#
NP-T-1.#
2. Design and Construction of Nuclear Power Plants
NP-G-2.#
NP-T-2.#
3. Operation of Nuclear Power Plants
NP-G-3.#
NP-T-3.#
4. Non-Electrical Applications
NP-G-4.#
NP-T-4.#
5. Research Reactors
NP-G-5.#
NP-T-5.#
Nuclear Fuel Cycle Objectives
NF-O
1. Resources
NF-G-1.#
NF-T-1.#
2. Fuel Engineering and Performance
NF-G-2.#
NF-T-2.#
3. Spent Fuel Management and Reprocessing
NF-G-3.#
NF-T-3.#
4. Fuel Cycles
NF-G-4.#
NF-T-4.#
5. Research Reactors — Nuclear Fuel Cycle
NF-G-5.#
NF-T-5.#
Radioactive Waste Management and Decommissioning Objectives
NW-O
1. Radioactive Waste Management
NW-G-1.#
NW-T-1.#
2. Decommissioning of Nuclear Facilities
NW-G-2.#
NW-T-2.#
3. Site Remediation
NW-G-3.#
NW-T-3.#

Key

BP:	Basic Principles
O:	Objectives
G:	Guides
T:	Technical Reports
Nos 1-6:	Topic designations
#:	Guide or Report number (1, 2, 3, 4, etc.)

Examples

NG-G-3.1:	Nuclear General (**NG**), Guide, Nuclear Infrastructure and Planning (topic **3**), **#1**
NP-T-5.4:	Nuclear Power (**NP**), Report (**T**), Research Reactors (topic **5**), **#4**
NF-T-3.6:	Nuclear Fuel (**NF**), Report (**T**), Spent Fuel Management and Reprocessing (topic **3**), **#6**
NW-G-1.1:	Radioactive Waste Management and Decommissioning (**NW**), Guide, Radioactive Waste (topic **1**), **#1**

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 978–92–0–101217–3
ISSN 1995–7807