IAEA Nuclear Energy Series

No. NP-T-3.16

Accident Monitoring Systems for Nuclear Power Plants

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.

ACCIDENT MONITORING SYSTEMS FOR NUCLEAR POWER PLANTS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA
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
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, ISLAMIC REPUBLIC OF
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
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
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-3.16

ACCIDENT MONITORING SYSTEMS FOR NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2015

COPYRIGHT NOTICE

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
February 2015
STI/PUB/1676

IAEA Library Cataloguing in Publication Data

Accident monitoring systems for nuclear power plants. — Vienna : International Atomic Energy Agency, 2015.
p. ; 30 cm. — (IAEA nuclear energy series, ISSN 1995–7807 ; no. NP-T-3.16)
STI/PUB/1676
ISBN 978–92–0–110414–4
Includes bibliographical references.

1. Nuclear power plants — Safety measures. 2. Nuclear power plants — Accidents. 3. Nuclear reactor accidents. 4. Emergency management. I. International Atomic Energy Agency. II. Series.

IAEAL 15–00955

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.

During the Fukushima Daiichi accident, in 2011, the instrumentation provided for accident monitoring proved to be ineffective for a combination of reasons that appeared to include a loss of power, evaporation of liquid in sense lines, failure of sensors due to environmental conditions, instrument ranges that were not suitable for monitoring plant conditions and a lack of alternative data for use in validating instrument readings.

Lessons learned from the accident point to the importance of accident management systems, including the availability of instrumentation systems that can monitor relevant plant parameters in the reactor and inside containment during and after a severe accident. These parameters are needed to support the execution of severe accident management guidelines to mitigate the consequences of such accidents and to disseminate information to external technical support staff. Furthermore, parameters collected during severe accident conditions could allow for prediction of the accident evolution, implementation of recommended mitigating actions and coordination of rescue actions, as well as informing other appropriate organizations.

Criteria for accident monitoring instrumentation has largely been based upon experience from the accident at the Three Mile Island nuclear power plant, in 1979. These criteria had to be re-evaluated in the light of the Fukushima Daiichi accident, relevant insights from R&D programmes and the need for extended coverage of severe accident phases in accident management.

This publication provides a common international technical basis to be considered when establishing the various criteria for accident monitoring instrumentation to support operation under design basis and design extension conditions in nuclear power plants. The information in this publication is useful to support new plant designs as well as modification of existing nuclear power plants.

This publication comprehensively covers all relevant aspects of accident monitoring in nuclear power plants. The critical issues discussed reflect the lessons learned from the Fukushima Daiichi accident, involve accident management and monitoring strategies for nuclear power plants, the selection of plant parameters for monitoring plant status, the establishment of performance, design, qualification, display and quality assurance criteria for designated accident monitoring instrumentation, and design and implementation considerations. This publication also covers technology requirements and techniques for monitoring instrumentation.

This publication was produced by a committee of international experts and advisors from numerous countries. These contributors are listed at the end of the publication. The IAEA wishes to thank all participants and their Member States for their valuable contributions. The IAEA officers responsible for this publication were G. Johnson and A. Duchac of the Division of Nuclear Installation Safety and J. Eiler 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.

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

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.

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

1.1. BACKGROUND

The Fukushima Daiichi accident in March 2011 highlighted the need to re-examine criteria for instrumentation provided to monitor accident parameters in nuclear power plants. This re-evaluation was required to respond to lessons learned from accident experience and to extend the applicability of criteria to design extension conditions (DEC).

The IAEA has established an Action Plan on Nuclear Safety in response to the Fukushima Daiichi accident. One of the action items of this plan was to provide guidance to Member States on post-accident and severe accident monitoring systems. Historically, the terms 'post-accident monitoring' and 'accident monitoring' have both been used to mean the same concept. Accident monitoring is used in this publication because its use acknowledges that accident conditions can span a long period of time from the initiation of the event to the return to a controlled state. The major international standards organizations have also adopted this terminology.

This publication was prepared in response to this action item to reflect current knowledge, experience and best practices in this area and is based on the results of a series of consultants and technical meetings.

1.2. OBJECTIVE

The objective of this publication is to provide a comprehensive overview of instrumentation for monitoring accident conditions in land based, stationary nuclear power plants designed for electricity generation or for other heat production applications (e.g. district heating or desalination), for both new plant designs and enhancements to existing plants. It describes the basic principles of accident monitoring, the selection of plant parameters for monitoring plant status, criteria to be considered during the design of accident monitoring instrumentation, the methodology for implementing accident monitoring systems and areas where improvements, including new methodologies or technologies, may be needed.

This publication is intended for all personnel involved in the design, manufacture, qualification, licensing, operation and maintenance of accident monitoring systems in nuclear power plants.

1.3. SCOPE

This publication deals with monitoring instrumentation and the associated instrumentation support systems for preventive and mitigative accident management. The monitoring systems support on-site staff in making decisions for the management of design basis accidents (DBAs) and DEC. Severe accidents are included in DEC.

The publication covers instrumentation that is directly used to implement accident management strategies and also instrumentation that may be used to validate or back up the directly used instrumentation. Such instrumentation may include permanently installed instruments that are designated for use in accident monitoring, portable instruments, instruments that are installed but not normally in service and instruments provided to monitor temporary equipment.

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 1 introduces the topic by addressing the motivation for the preparation of this publication, as well as the objective and scope of the publication, including the intended audience.

Section 2 provides an overview of accident management, characteristics of accident conditions, accident management and monitoring strategies, operator aids and existing guidance.

Section 3 summarizes the information needed to support accident management, the selection of plant parameters and the sources of information for accident monitoring.

Section 4 discusses the establishment of criteria for accident monitoring instrumentation. It describes in detail the various types of criteria including performance, design, qualification, display and quality assurance.

Section 5 describes design and implementation considerations for accident monitoring instrumentation in existing plants and new plant designs. These considerations involve coping with severe environmental conditions, as well as maintenance, testing and training issues.

Section 6 discusses technology needs to support the implementation of accident monitoring systems. It also identifies areas where future research may be desirable to improve the technology for accident monitoring systems and instrumentation.

Section 7 provides a summary based on the body text of the publication.The Appendix describes the independence of accident monitoring functions considering component operation or failure, and internal and external hazards.

The references in this publication list important documents, codes, standards and other guidance published to cover the accident management and monitoring area. Annexes I and II contain Member State experiences with the design, development, implementation and application of accident monitoring instrumentation. The glossary provides definitions of terminology in use within the nuclear instrumentation and control (I&C) area. A list of abbreviations used in this publication is then given, followed by a list of contributors.

2. ACCIDENT MANAGEMENT FOR NUCLEAR POWER PLANTS

2.1. OVERVIEW

Accident monitoring instrumentation provides the information that operators and other emergency response personnel need to manage accident conditions. Before accident monitoring needs can be defined, it is first necessary to understand the characteristics of accident conditions and accident management strategies.

The IAEA design specific safety requirements for the systems, structures and components (SSCs) of nuclear power plants identifies accident conditions as deviations from normal operation that are less frequent and more severe than anticipated operational occurrences, and which include DBAs and DEC [1].

DBAs result in conditions for which a facility is designed in accordance with established design criteria and conservative methodology. DEC are not considered for DBAs, but are considered in the design process of the facility in accordance with best estimate methodology. In many cases, the effects of DEC will be bound by those of DBAs, but some DEC will result in significant fuel degradation. This subset of DEC is called severe accidents.

Accident management is a set of actions envisaged to respond to, or recover from, an accident situation. This is done by using plant systems, or, if applicable, portable equipment with appropriate connections. Accident management can be split into two parts:

(a) Preventive accident management integrates actions and measures needed to prevent significant core damage and terminate the progress of core damage once it has started. Preventive accident management deals with DBAs and those DEC which do not result in significant fuel degradation, and is usually accomplished by plant operation staff using emergency operating procedures (EOPs) in the main control room (MCR), but is generally limited to actions taken before core damage occurs.

(b) Mitigative accident management, often called severe accident management, is primarily devoted to maintaining the integrity of the containment as long as possible, minimizing releases of radioactive material and achieving a long term stable state when the fuel has started to degrade beyond the level of damage accepted for DBAs and those DEC which do not result in significant fuel degradation. Mitigative accident management deals with severe accidents and is usually performed by technical support centre (TSC) staff using severe accident management guidelines (SAMGs).

Both preventive and mitigative strategies may call for operation of equipment anywhere within the plant and the use of equipment that is not normally a part of the plant, including equipment brought from off-site. The two methods of accident management deal with events that have significantly different characteristics requiring different types of response which place different requirements on the accident monitoring systems.

2.2. CHARACTERISTICS OF ACCIDENT CONDITIONS

The IAEA defines two main plant states, operational states and accident conditions, in IAEA Safety Standards Series No. SSR-2/1, Safety of Nuclear Power Plants: Design [1]. Operational states comprise normal operation and anticipated operational occurrences, the latter of which are deviations from normal operation that are expected to occur at least once during the operational lifetime of a facility. Table 1 summarizes the differences between the plant states.

While plants are designed to withstand DBAs, their actual capability to cope with accidents is usually considerably greater than that credited in the safety analysis. This is mainly because only certain systems have been credited to respond by the safety analysis. The use of other, non-credited, systems can greatly enhance the plant's capability. The increased capability is furthered if systems are also allowed to operate outside their intended range of operation (non-conventional use of systems). It is therefore necessary to monitor all of a plant's capabilities to fulfil the safety functions, which may include hook-ups of non-dedicated systems and temporary components.

Two categories of DEC are considered: accident conditions that are not considered DBAs and do not result in significant fuel degradation; and accident conditions that are more severe than DBAs and involve significant fuel degradation. This latter type of DEC is termed a 'severe accident'.

The characteristics of these different types of accident condition are further described below. The list of external events may differ, and the magnitude of such events varies, based on the incurred risks.

2.2.1. Design basis accidents

DBAs are selected following a rigorous screening process. DBAs encompass a wide spectrum of internal and external events that were considered in the design to represent and bound the range of events that might happen during a plant's lifetime. They are categorized according to their probability of occurrence and are used to define the design basis, including the provision of safety systems for dealing with these events, the performance criteria needed for safety systems and other items important to safety that are necessary to mitigate the consequences of an accident and return the plant to a safe state. A primary safety objective of the plant design is to demonstrate by means of the safety analysis that all DBAs can be managed in such a way that they have acceptable radiological impacts on-site and off-site (i.e. to be within the authorized limits).

EOPs are developed to provide the plant operators with directions for responding to DBAs and DEC that do not result in significant fuel degradation. Accident management then focuses on understanding the state of the plant and ensuring that the appropriate preplanned actions (both automatic and manual) are taken.

2.2.2. Design extension conditions

Requirement 20 in SSR-2/1 [1] addresses a part of the beyond DBA scenario problem including severe accidents by prescribing that a set of DEC be considered in plant design.

DEC are derived for the purpose of improving the safety of nuclear power plants. The objective is to enhance plant capabilities in such a way that plants can withstand accidents that are more severe than DBAs without unacceptable radiological consequences, by either preventing such events or mitigating their consequences. Therefore, if deemed appropriate, DEC could lead to the decision of adding alternative safety features to compensate for the deficiency of some essential systems or components. Ideally, such features should have the capability of fulfilling their intended safety functions under the anticipated environmental conditions that could prevail for DEC.

TABLE 1. SUMMARY OF PLANT STATES AND THEIR CHARACTERISTICS

<table>
<tr><td rowspan="3">Plant states</td><td colspan="2">Operational states</td><td colspan="3">Accident conditions</td></tr>
<tr><td rowspan="2">Normal operation</td><td rowspan="2">Anticipated operational occurrences</td><td rowspan="2">Design basis accidents</td><td colspan="2">Design extension conditions</td></tr>
<tr><td>Without significant fuel degradation</td><td>Severe accidents</td></tr>
<tr><td>Safety objectives</td><td colspan="2">Prevent any significant damage to items important to safety or which lead to accident conditions</td><td colspan="2">Prevent significant fuel degradation and keep releases within acceptable limits</td><td>Terminate fuel damage
Maintain the integrity of the containment for as long as possible
Minimize on-site and off-site releases and their adverse consequences</td></tr>
<tr><td>Accident management strategy</td><td>None needed</td><td colspan="3">Preventive</td><td>Mitigative</td></tr>
<tr><td>Credited plant equipment</td><td>All plant equipment,except as allowed by operating limits and conditions</td><td colspan="2">Safety systems</td><td colspan="2">All available</td></tr>
<tr><td>Operating procedures</td><td>Normal operating procedures</td><td>Abnormal operating procedures</td><td colspan="2">Emergency operating procedures (emergency response procedures and function restoration procedures)</td><td>Severe accident management guidelines</td></tr>
<tr><td>Typical decision making responsibility</td><td colspan="2">Plant operators</td><td colspan="2">Plant operator with assistance of shift technical advisors</td><td>Emergency response managers with assistance of plant operators</td></tr>
<tr><td>Expected environmental conditions</td><td colspan="2">Normal</td><td colspan="2">Harsh</td><td>Severe</td></tr>
</table>

DEC without significant fuel degradation are of relatively low frequency. These DEC may vary from one site to another and may include:

(a) Operational states or accidents coincident with a common cause failure (CCF) (e.g. loss of ultimate heat sink or station blackout);
(b) Events occurring during low frequency states of the plant (e.g. leak in the reactor cooling system when the reactor pressure vessel (RPV) is open);
(c) Events due to external hazards beyond the design basis (e.g. Fukushima Daini).

Owing to the low probability of these DEC, the response generally does not need to address the single failure criterion. Preventive accident management strategies and EOPs may be sufficient to respond to certain DEC, but when significant fuel damage occurs, the circumstances are treated as severe accidents.

2.2.2.1. Design extension conditions in spent fuel pools

Safety analysis accounts for the quantity of fission products as well as sources for combustible gases stored in spent fuel pools (SFPs). The phenomena that could affect the fuel in the core may apply to the fuel elements in the SFP. However, there are significant differences that have influences on the strategies for coping with these phenomena:

(a) In the SFP area, there are generally fewer fission product barriers (owing to the lack of containment around the SFP). The releases of gases and radioactivity that would result from a significant number of clad failures would lead to releases that would negatively affect site activities.
(b) The reduced decay heat in the fuel in the SFP leads to more time before reaching fuel failures, facilitating the application of preventive strategies. However, in cases of fuel pool structural failures, this delay may be small due to rapid draindown scenarios.

Although strategies for spent fuel storage have the main goal of preventing fuel damage and are thus of preventive type, the important time delay available generally does not require exact procedures, and it may be acceptable to apply guidance type documents. Therefore, SFP strategies may constitute a part of SAMGs, or a mixture of EOPs and SAMGs.

2.2.3. Severe accidents

One of the main assumptions of DBA is that SSCs always maintain the adequate capability needed to fulfil their intended safety functions. As a consequence, DBAs do not result in fuel degradation. However, severe accidents typically generate much worse conditions for which the design of SSCs may not be adequate.

The effects of severe accidents are more severe than those of DBA. Thus, safety systems may not be capable of preventing degradation of reactor fuel in the reactor or in spent fuel storage.

Inadequate evaluation of the magnitude and frequency of occurrence of some external events could result in external hazards exceeding design basis conditions. For example, for river sites underestimating the magnitude and the probability of occurrence of landslides in dams situated upstream of the plant could lead to severe challenges to some essential buildings and the systems they shelter.

A severe accident may lead to a substantial release of fission products inside or outside the reactor coolant system (RCS). Severe accidents may also be associated with internal or external hazards that cause loss of important systems, jeopardize the integrity of fuel in spent fuel storage, affect other units and facilities on the site, and display misleading or confusing instrument readings.

To optimize the management of an accident, the operating staff need to understand the mechanisms of reactor accidents and assess how plant systems can be used to control a developing situation. They need to make use of all the available plant systems under accident conditions, not only dedicated safety systems, but also the possible use of non-safety systems under DEC. Use of both dedicated safety and non-safety systems outside of their intended range of operation is to be anticipated under DEC.

When plant operators or emergency response staff recognize that the plant is in a severe accident state, a transition is made from preventive to mitigative accident management strategies. The plant conditions that signify the existence of a severe accident need to be clearly specified and monitored based on well defined and documented criteria.

The basic aims of severe accident management are to terminate the progress of fuel damage, to keep the containment integrity as long as possible, and to minimize on-site and off-site radioactive material releases. Halting the progress of fuel damage also helps prevent failure of the RPV or the calandria. Severe accident management strategies are discussed further in Section 2.3.

Accident progression during a severe accident can involve two phases, the in-vessel phase and the ex-vessel phase, with fundamental differences in the challenges to safety functions and the magnitude of radioactivity release. For both phases, the phenomena involved need to be identified and understood. An example of the possible fuel damage sequence and associated in-vessel phenomena for a water cooled reactor type follows:

— Overheating of the fuel and cladding;
— Onset of exothermic oxidation of the cladding, accompanied by production of hydrogen;
— Damage to and melting of the fuel cladding;
— Rapid increase in hydrogen production, with a possible challenge to containment integrity owing to deflagration or detonation;
— Melting of the cladding, fuel and core materials and downward relocation of the corium;
— Interaction of the molten corium with the residual water in the RPV or calandria;
— Potential response caused by a molten corium–water reaction;
— Heating of the RPV or calandria by the molten corium.

At the last stage, the possibility of RPV or calandria failure should be considered. If attempts to arrest the accident progression at this point are not successful, vessel melt-through will occur, and the ex-vessel phase of the accident will commence.

During the ex-vessel phase, a variety of phenomena may challenge the containment integrity. These phenomena include:

(a) Damage to the containment owing to high pressure ejection of the corium (direct containment heating).
(b) Hydrogen combustion (deflagration/detonation), with hydrogen produced during the in-vessel phase and later during the ex-vessel phase by core–concrete interaction (which may also produce carbon monoxide, which is also combustible) or a molten corium–water reaction. Apart from the threat of global combustion, there is a danger of local deflagrations or detonations, which can generate missiles that may challenge the containment integrity.
(c) Energetic molten corium and water interaction (steam explosion).
(d) Core–concrete interactions, which directly jeopardize the integrity of the containment due to base mat melt-through.
(e) Long term pressurization or temperature increases, ultimately leading to failure of the containment.
(f) Bypass of the containment, for example through a damaged steam generator due to tube creep rupture, or through some other pathway, for example an interfacing system loss of coolant accident (LOCA).

2.2.4. Procedures and guidelines

Procedures and guidelines direct the control room staff and other emergency response personnel in terminating the progress of accidents and in mitigating their consequences.

For DBAs, plant specific EOPs are developed to make best use of the systems available to terminate the progression of an accident by protection of fission product barriers.

A procedure comprises a step by step list of required actions and responses that have to be followed verbatim. These procedures have to be followed in the specified order, and in accordance with other ‘rules of usage’ in which the procedure users (usually the reactor operators) are highly trained. A procedure is therefore a highly structured means of specifying a well defined series of actions to be taken and is based on the values of individual variables or combinations of variables and available mission time.

Symptom based procedures (sometimes called function restoration procedures) are also used to confirm that fundamental safety functions are being maintained. These contain actions to be taken based on the values of directly measurable plant variables and available mission time. In a symptom based procedure, the user (operator) is not required to know the initiating event or sequence of events that caused the accident, as well as plant conditions that are not directly measurable, in order to apply the procedure.

SAMGs are the guidelines used for severe accidents and are typically meant for use by the TSC staff or equivalent support or crisis teams. The term guideline here is used to describe a fairly detailed set of instructions that describe the tasks to be executed on the plant, but which are less strict and prescriptive than the procedures found in the EOPs. Manuals or handbooks provided to support SAMGs contain a description of the tasks to be executed and their background reasoning.

SAMGs take plant specific details into account. These vary significantly between different types of reactor (e.g. reactor type, fuel type, coolant type and pressure, size and strength of the containment, number and capability of trains of safety equipment) and also between different reactors of the same type.

The SAMGs may suggest actions that may not be appropriate for EOPs because of potential negative effects, operational and phenomenological uncertainties and the predominantly long term nature of these actions.

During DEC, some actions that are straightforward in accidents without fuel damage might have significant potential drawbacks when the fuel has started to melt. For example, water injection onto overheated fuel can lead to a significant release of hydrogen into the RCS and containment. Furthermore, uncertainties in physical phenomena can be significant and need to be adequately credited for deriving reasonable mitigative strategies. Consequently, decision makers are often faced with the need to weigh the pros and cons of performing an action before deciding on the strategy for minimizing the effects of the event.

SAMGs normally contain a description of both the positive and negative potential consequences of proposed actions, including quantitative data, where available and relevant, and contain sufficient information for the plant staff to reach an adequate decision on the actions to take during the evolution of the accident.

Generally, a guideline differs from a procedure in the following ways:

(a) Verbatim compliance with a guideline is not normally required.
(b) The order of the actions specified in a guideline may be altered based on the judgement of the trained guideline user.
(c) The actions to be taken may depend upon evaluation of plant conditions by the user as specified in the guideline. These actions will include the available alternatives (based on plant equipment availability at the time), and will also include the option of not implementing a particular action.
(d) Use of SAMGs generally requires additional evaluation by personnel located in the local TSC or potentially through a national crisis organization.

In addition, when using EOPs, responsibility and decision making belong to control room staff, while when using SAMGs, the responsibility and decision making may be transferred to the TSC staff.

Decisions will be based on the user's evaluation using the SAMGs. It is also important to keep the long term perspective in mind; otherwise, the short term measures and actions may cause unnecessary problems or irreparable damage for the long term handling of the plant.

2.3. ACCIDENT MANAGEMENT STRATEGIES

2.3.1. Preventive accident management

Preventive accident management is devoted to taking actions for restoring core cooling to preventing fuel damage, preventing damage to spent fuel for maintaining fuel integrity and keeping radioactive releases within authorized limits. It is aimed at bringing the plant to a controlled state when safety functions can be fulfilled satisfactorily, or restoring essential safety functions if some have been lost. In some scenarios, the spent fuel may also be at risk of being damaged. In such cases, preventive accident management may need to deal with maintaining cooling to spent fuel stores.

Preventive accident management deals with plant conditions in which physical phenomena are well established, consequences of recommended actions are predictable — at least qualitatively — and plant parameter evolution can be adequately monitored. Furthermore, plant safety systems are expected to be available, and many non-safety systems will also be available if supporting systems (e.g. power supply) continue to function.

In the preventive domain, accident management is in most plants directed by the shift supervisor using procedures that normally consist of descriptive steps, as the plant status will be known from the available instrumentation and the consequences of actions can be predetermined by appropriate analysis. The direction for the preventive domain, therefore, takes the form of procedures, usually called EOPs, and is prescriptive in nature. EOPs cover both DBAs and DEC that do not result in significant fuel degradation. The EOPs address all events considered credible on the basis of possible initiating events and possible complications during the evolution of the event that could be caused by additional hardware failures, human errors or events from outside.

2.3.2. Mitigative accident management

Mitigative accident management mitigates the consequences of DEC. It is aimed at terminating damage to the fuel, maintaining the integrity of the containment for as long as possible and minimizing on-site and off-site releases and their adverse consequences. In some scenarios, the spent fuel may also be damaged. In such cases, mitigative accident management may also need to deal with restoring cooling to one or more spent fuel stores. IAEA Safety Standards Series No. NS-G-2.15, Severe Accident Management Programmes for Nuclear Power Plants [2], provides a more extensive discussion of mitigative accident management.

Essential elements to be assessed are the status of fission product barriers, actual or imminent fuel damage and challenges to RPV or calandria and containment integrity. If, through an analysis of variable trends, it is evaluated that containment integrity is not likely to be maintained, substantial benefits will be gained by delaying or preventing a catastrophic containment failure (e.g. actuating temporary containment venting). These benefits include the extension of time available to the operating staff to restore or replace failed safety systems and implement the emergency plan.

In the mitigative domain, uncertainties may exist in the status of fundamental safety functions, the status of plant systems and equipment and in the outcome of actions. Consequently, the guidance for the mitigative domain (SAMGs) is not prescriptive in nature, but rather it proposes a range of potential mitigative actions and should ideally allow for additional evaluation and alternative actions.

The SAMGs address the full spectrum of credible challenges to fission product boundaries due to severe accidents, including those arising from multiple hardware failures, human errors or events from outside, and possible physical phenomena that may occur during the evolution of a severe accident (such as steam explosions, direct containment heating and hydrogen burns).

The wide variety of situations that can happen in a DEC scenario, the uncertainties associated with relevant phenomena and potential conflicting priorities for a decision maker responsible for managing the accident require more creative approaches for developing efficient mitigative strategies.

During the initial phases of DEC, the SAMGs will be implemented under the direction of the shift supervisor. Because of the complexity of response and uncertainties involved, command and control will normally be transferred at some point to emergency response personnel who have more resources to evaluate strategies that are most likely to accomplish the goals of mitigative accident management. In many Member States, this role is performed by the staff in the TSC.

2.4. ACCIDENT MONITORING STRATEGIES

Accident monitoring systems need to provide operators and TSC staff with the information that they need to develop an integrated understanding of the status of the reactor, containment and SFP in a manner that allows for the greatest understanding of the nature of the accident, the status of the integrity of the barriers to fission product release, and the potential magnitude and pathways for such a release. Accident monitoring systems should ideally be composed of instruments that are specifically designated for the purpose. In general, the designated instruments is to be permanently installed and provide direct information necessary for accident management wherever the command and control of the accident is expected to occur (e.g. control room or TSC).

Since the EOPs and SAMGs depend on the ability to estimate the magnitude of several key plant parameters, the plant parameters needed for both preventive accident management measures and mitigative accident management measures are to be identified.

Implementation of EOPs and SAMGs require different management strategies, and they also require different strategies for accident monitoring. The design philosophy of accident monitoring systems need to address the different demands and requirements for a DBA and DEC. EOPs presume a controlled situation after a certain period of time. Conversely, the progress of DEC is more difficult to predict and can end with more serious consequences, potentially progressing far enough to require the evacuation of the plant and some of the surrounding environment.

This section summarizes the information needs and design criteria applicable to instrumentation that supports the two different strategies. Section 3 gives details about the selection of accident monitoring parameters. Section 4 describes the criteria for designated accident monitoring channels.

2.4.1. Accident monitoring instrumentation for preventive accident management

Preventive accident management deals with foreseen events that are relatively well defined. The plant is designed such that safety systems will remain functional during events. Furthermore, many non-safety systems may be expected to continue to operate. Therefore, monitoring systems used for preventive accident management are composed of qualified instruments that have a defined range over the anticipated mission time.

To implement preventive accident management procedures, the accident monitoring systems need to provide the plant operators with the information that they require:

(a) To take preplanned manual actions needed to bring the plant to a controlled state;
(b) To assess the status of the plant's fundamental safety functions;
(c) To assess the status and function of plant safety systems;
(d) To determine whether there is a potential for breach, or an actual breach of fuel clad, the RCS or the containment;
(e) To understand the status of other plant systems so that appropriate decisions can be made as to their use;
(f) To estimate the magnitude of any potential or actual radioactive release.

2.4.2. Accident monitoring instrumentation for mitigative accident management

Mitigative accident management deals with unforeseen events that may evolve differently than expected by the plant designers. Some plant systems may remain operable, but it is difficult to predict which ones the operators can depend upon. Experience at Fukushima Daiichi demonstrated the need to provide instruments that are designated for severe accident monitoring and that are robust enough to survive environmental conditions that may be created by severe accidents. Nevertheless, conditions created by severe accidents may produce unforeseen damage or degradation in even the best suited instruments (sensors, cabling, terminations, signal processing electronics or transducers). Furthermore, some instrumentation may need to operate for a long time without the possibility of replacement. Therefore, the qualification for accident monitoring instruments need to be taken into account. Alternative instrumentation needs to be identified where the primary instrumentation is not available or not reliable.

Consequently, monitoring for severe accidents needs to be composed of systems that are designated for severe accident use, pre-identified sets of other existing instrumentation that might be useable to provide information in the event that portions or all of the normal monitoring system fails, and non-instrumented information sources that may be used to gather the required information. Hence, use of instrumentation that is qualified for the expected environmental conditions is the preferred method to obtain the necessary information.

Severe accident monitoring needs to provide the information that operators and TSC staff need:

(a) To detect the need to transition from EOPs to SAMGs;
(b) To execute the SAMGs;
(c) To assess the state of the fuel and the containment;
(d) To determine when a controlled state has been reached.

Operators and TSC staff need to be trained on the identification and use of these designated instruments to support SAMG implementation.

2.4.2.1. Designated severe accident monitoring

Designated severe accident instruments monitor variables that have been identified to be needed to support implementation of SAMGs. These should ideally be able to monitor and display the measured variables:

(a) For the full range of predicted conditions with margins;
(b) With sufficient precision to understand trends of the variable over the full course of time for which information is needed;
(c) Within the conditions that result for the duration of the mission time.

Where it may not be possible to accomplish all needs with a single range of measurements, instrument channels with different ranges will be needed. Consideration is to be given to the range of the channel, not just the range of the sensor. As an example, thermocouples often use a display range that is less than the range of the sensor. Such an approach may be acceptable if provision is made for alternative readout or for rescaling the display.

Under severe accident conditions, it is often less important to know when a variable reaches a specific value, and more important to be able to identify when it increases or decreases and at what rate of change. Hence, the required accuracy of the instrument depends on the intended use of the associated variable.

2.4.2.2. Temporary and portable instrumentation

Portable instrumentation may sometimes be the only means for obtaining information on plant variables. These may be included among designated instrumentation to support implementation of EOPs and SAMGs.

For implementation of SAMGs, the use and evaluation of signals from temporary or portable instrumentation may provide a means for attaining signal diversity and for confirming the accuracy of the designated SAMG instrumentation.

Portable instruments may also be useful to gather data when the duration of the accident or the environment leads to failure of designated instruments. The possibility that portable instruments may be needed to detect the achievement of a controlled state should be considered.

2.4.2.3. Other available instruments

Other available instruments that are not designated for the purpose of severe accident monitoring may provide data that can be used to derive qualitative or quantitative information needed for severe accident management.

Instruments not designated as severe accident instruments may be useful when these instruments have sufficient capabilities to provide adequate information in case of severe accidents. The instruments not designated for severe accidents may be limited in their time of use and selected on the basis of their precise location (e.g. dose rate at a given location).

Existing plant instruments need to be evaluated to identify those that can provide the information needed for severe accident management if the designated instruments fail.

The identified instruments need to be evaluated to determine whether they are suitable for use (e.g. have the necessary performance and that they would not provide information that may mislead operators) and can be expected to survive in the environmental conditions that may be created by severe accidents.

In some cases, it may be relatively easy to address issues that render an existing instrument unsuitable for severe accident monitoring. For example, procedures might be developed to extend the range of instrument readout or for providing power to the instrument if its normal power supply fails.

Where information is not available through direct measurement, it might be obtained alternatively from indirect sources or derived using operator aids. An example of such an indirect measurement is the use of pressure measurement in a connected residual heat removal loop or safety injection system to infer RCS pressure when the direct RCS pressure measurement is not available. Alternative means for the functioning of instruments during a station blackout is also to be considered, as well as the potential for instrument destruction during a severe accident.

Operator aids are needed to help operators understand the capabilities of these instruments. Such guidance should ideally include direction for recognizing failed instruments and for conducting checks to obtain reasonable assurance that the information given by the instrument can be used and the process to be implemented for deriving the final information needed for managing the accident.

2.4.2.4. Other information sources

Other information sources that do not depend upon plant instrumentation may also be available. An example is analysis of containment gas samples to determine the concentration of ^{137}Cs, ^{129}I and ^{85}Kr to confirm subcriticality. Other information obtainable by post-accident sampling systems and by direct operator observation may also support implementation of SAMGs. Where such techniques are planned, they need to be considered when establishing the monitoring instrumentation to support mitigative accident management.

2.4.3. Operator aids

Designing a set of individual indications to cover each functional area and leaving the development of an integrated picture up to the operators and analysts on the day of the event is not an optimal approach to accident mitigation. For both DBAs and DEC, the design of accident monitoring systems needs to be coordinated with the design of operator aids that will assist the operators and accident management staff to determine plant status, decide on actions to be taken and monitor the plant response to those actions. Operator aids for accident monitoring systems should ideally help the data users to assess the operability, determine the validity of instrument readings, estimate the value of accident monitoring parameters based upon the available data and use the available information in assessing plant conditions.

Users of accident monitoring data need to be provided with information about the reliability, expected limits to operability and survivability of both designated and other available accident monitoring channels so that they can recognize conditions that may be impairing the reliability of the readings. For each accident monitoring channel, the operator aids should ideally include information such as:

(a) Instrument tap, sensor, transmitter, signal processing and readout locations;
(b) Instrument channel range and any provisions available for extending the measurement range;
(c) Channel uncertainties when exposed to the environmental conditions which may exist when the instruments are needed (e.g. conditions during normal operation, anticipated operational occurrences, DBA and DEC);
(d) Plant power source including means available to power the channel from different sources;
(e) Limitations of the measurement (e.g. reading depends upon an assumed liquid density) and provisions available to compensate for these limitations (e.g. provisions to adjust the readings for off-calibration conditions);
(f) Environmental limitations for instrument channel components.

Data validation might include, as appropriate, interchannel comparison and comparison with diverse variables with a known relationship to the variable in question. Assessment of operability might include, for example, the use of checklists to help recognize suspicious behaviour on the part of a channel or a set of channels and diagnostic methods that can be used by plant instrument technicians.

Making best estimates of variable readings may include aids for combining readings from redundant or diverse instruments, calculations or nomograms that help users adjust instrument readings based upon plant conditions (e.g. to revised vessel level measurements based upon estimate temperature and pressure (density) of the contained fluid) or calculations or tables for relating an indirect measurement to the value of the variable of interest.

Aids to assessing plant conditions might include checklists for assessing the status of critical safety functions, descriptions of the interrelationship between variables, charts or displays that can show the current status and trends of a collection of key variables.

Ideally, operator aids will be available and implemented in computer systems. Safety parameter display systems are commonly used to assist the operators in preventive accident mitigation. Nevertheless, it needs to be kept in mind that complex electronic systems are vulnerable to failure (e.g. owing to loss of power). Therefore, operators need to have access to, and to be trained in, the use of non-electronic aids.

2.5. EXISTING ACCIDENT MONITORING INSTRUMENTATION GUIDANCE

Nuclear power plants currently have some form of accident monitoring instrumentation systems that are based on existing accident monitoring design criteria. These systems are largely designed using guidance that was developed in the early years of the nuclear industry, and then modified as necessary to include the impact of lessons learned through major nuclear plant upsets and accidents that occurred in the 1979–1986 time frame. For example, guidance for accident monitoring criteria for light water reactor technology plants is largely influenced by the principles inherent within their licensing bases (late 1960 vintage plants through to the mid-1990s), as modified by lessons learned from the accident at the Three Mile Island Unit 2 (TMI-2), in 1979, and the Chernobyl accident, in 1986. Ideally, the design criteria contained in existing guidance should now be augmented with criteria derived for the monitoring of severe accidents and DEC in light of lessons learned from the Fukushima Daiichi accident, which occurred in 2011.

Immediately following the accident at TMI-2, US industry experts convened as a group under the auspices of the American Nuclear Society (ANS). Their members drafted ANS Standard 4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors [3]. This effort resulted in a useful means for addressing accident monitoring instrumentation design in light of the functions that need to be implemented by plant operators and emergency responders in the event of an accident. ANS Standard 4.5-1980 provided a functionally based methodology for categorizing the various types of accident monitoring instrument based on the functions served and type of information provided, in a manner that allowed for the identification of the qualification requirements and duration requirements that need to be considered in the design of these instruments.

US Nuclear Regulatory Commission (NRC) Regulatory Guide 1.97, Revision 2 [4] endorsed the use of the criteria depicted within ANS Standard 4.5-1980, and provided guidance for applying these criteria for meeting US regulations. Subsequently, the Institute of Electrical and Electronics Engineers (IEEE) convened to develop IEEE Standard 497, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations [5], which also adopted the same grouping based upon accident monitoring functions. Additionally, IEEE Standard 497 provided design standard requirements for qualifying such instrumentation to meet the harsh environmental conditions expected to be present during the course of a nuclear plant accident. Later revisions of US NRC Regulatory Guide 1.97 endorsed the use of IEEE Standard 497 and its subsequent revisions.

The current version of IEEE Standard 497 was released in November 2010, just four months before the Fukushima Daiichi accident occurred. However, this event changed not only the general view on safety systems for nuclear power plants but also unveiled, in particular, the importance for reliable monitoring instrumentation suited to operate under such adverse conditions of a severe accident. This prompted the Nuclear Power Engineering Committee of the IEEE to initiate the next update of IEEE Standard 497, which is currently in progress.

Historically, the International Electrotechnical Commission (IEC) has not had a system standard for accident monitoring instrumentation design criteria. However, IEC Standard 61226 [6] identifies the instrument functions, classifies them and defines the applicable requirements, and IEC Standard 60964 [7] defines requirements applicable to the human–system interface in the control room. The IEC also has standards dealing with specific functions that have a role in accident monitoring, such as monitoring of the radiation, containment and core cooling. It has been proposed that the IEC join with the IEEE for issuing a dual logo standard on accident monitoring systems for nuclear power plants based on a version of the IEEE Standard 497 that is now being revised. A small expert group of individuals from both organizations investigated the feasibility of this proposal in 2012 and did not come across any significant points of disagreement.

German standard KTA 3502 [8], from the Nuclear Safety Standards Commission (Kerntechnischer Ausschuss, KTA), addresses accident monitoring instrumentation. The current version of KTA 3502 was released in 2012. This standard establishes requirements for accident monitoring equipment for DBAs in non-mobile light water reactors. It does not refer to the monitoring instrumentation of the reactor protection systems, for nuclear remote surveillance systems, nor for instrumentation solely dedicated for normal operation. KTA has also published several standards dealing with monitoring of radioactive releases.

The Electric Power Research Institute (EPRI) TR-102371 [9] provides guidance on identifying the capabilities of instruments that might be used as other available instruments and the development of operator aids for such instruments. EPRI TR-103412 [10] provides additional guidance on the identification of severe accident information needs, identification of severe accident environmental and process conditions, and evaluation of the capabilities of other available instruments.

One shortcoming identified with existing guidance is that early licensing policy and guidance had placed a greater emphasis on the use of such instrumentation for operators to use for the mitigation of DBAs (prevention of fuel damage), with less emphasis on guidance for developing instrumentation the operators can use to mitigate the radiological releases from fuel damage events.

At the same time, the fidelity of models of accident progression has steadily increased to the point where best estimate modelling of the effects of accident progression can be used to estimate the consequences of fuel damage events to a much higher degree of accuracy than that afforded by the studies in the early 1970s.

3. SELECTION OF PLANT PARAMETERS FOR ACCIDENT MONITORING

3.1. INFORMATION REQUIREMENTS

Accident monitoring instrumentation needs to provide the necessary information to support making operational decisions during implementation of EOPs and SAMGs. Examination of the EOP and SAMG strategies would identify the appropriate parameters. Furthermore, all major transitions within and between accident mitigating procedures or guidelines correspond directly to changes in information needs for plant operators and TSC staff.

Accident monitoring parameters also need to be selected with the goal of supporting the emergency response plan decision making process. Important parameters to monitor for emergency response are contained in IAEA Safety Standards Series No. GS-R-2, Preparedness and Response for a Nuclear or Radiological Emergency [11], and IAEA Safety Standards Series No. GS-G-2.1, Arrangements for Preparedness for a Nuclear or Radiological Emergency [12]. Selection of accident monitoring parameters should consider the status of the fission product barriers and the possible onset of degradation of the fission product barriers. This would also include the condition of the fuel.

Plant status parameters to be monitored to support accident management and emergency response actions are necessary for several purposes:

(a) Implementing EOPs to prevent extensive fuel cladding damage. Such information includes those parameters required to assess plant safety function status as well as those variables that assess the performance of safety systems and support systems relied upon to reach this objective.
(b) Implementing SAMGs to mitigate accident progression and to bring the plant into, and to maintain it, in a controlled state, even in the long term phase of the accident.
(c) Assessing the potential magnitude of fission product releases and monitoring such releases together with meteorological conditions for feeding information to teams in charge of emergency planning and evacuation concepts, among other things.
(d) Assessing environmental conditions relevant for monitoring the control room as well as TSC habitability or access to selected plant areas in order to perform local actions.
(e) Resolving ambiguities in displayed information.

3.2. IDENTIFICATION OF VARIABLES MONITORED BY DESIGNATED ACCIDENT MONITORING CHANNELS

The critical set of information needed to specify appropriate design criteria for accident monitoring instrumentation includes the breadth of accident scenarios that need to be considered and the key assumptions to be considered when postulating either DBA or DEC scenarios to ensure that the nature of the postulated event has been accurately characterized. Many variables will support both preventive and mitigative accident management. The different characteristics of the DBA and DEC may, however, impose different design criteria on the instrumentation that monitors these variables. Nevertheless, instrumentation can often be designed to meet both sets of criteria.

Much of the needed information may be found in the plant's accident mitigation procedures. These procedures are generally derived from safety studies and analyses. They take into account the result of design basis studies and insights from probabilistic safety analyses or DEC studies, as necessary. In particular, these studies enable the identification of which operator actions are necessary, the plant parameters on which they will be based, and the systems and components that will be involved in the scenario under consideration. For a DEC scenario, information may be needed to identify actions which are to be avoided to prevent occurrence of energetic phenomena which could further challenge fission product barrier integrity (e.g. do not spray if hydrogen concentration is too high). These same studies provide information that points to the plant variables on which decisions will be based, for any particular accident management strategy. The development of procedures and selection of monitoring variables will often be an iterative process to take account of instrument capabilities.

The following subsections describe criteria for identifying the variables to be measured and displayed. Annexes I and II give examples of the monitored variables from Japan and the Republic of Korea, respectively.

3.2.1. Parameters to support preventive accident management

Accident monitoring that supports preventive accident management need to monitor the plant variables which give operators the information they need to accomplish the following.

3.2.1.1. Take preplanned manual actions needed to bring the plant to a controlled state

These will be variables the operators need in order to take preplanned manual actions that are necessary for safety systems to perform their safety functions and for which no automatic control is provided. These parameters will typically be identified in the EOPs, abnormal operating procedures or plant licensing basis.

3.2.1.2. Assess the status of the plant's fundamental safety functions

The fundamental safety functions are control of reactivity, removal of heat from the reactor and from spent fuel storage, and confinement of radioactive material including shielding against radiation, control of planned radioactive releases and limitation of accidental radioactive releases. These parameters will typically be identified in the functional restoration procedures or the EOPs.

3.2.1.3. Determine whether there is a potential for breach, or an actual breach, of barriers to radioactive release

Typically, the barriers of interest are the fuel clad, the RCS and the containment. Variables are to be selected to provide the most direct indication of the integrity of fission product barriers with a capability for monitoring beyond the normal operating range. These variables are typically identified in the plant licensing basis, design basis documents for fission product barriers or EOPs.

3.2.1.4. Understand the status of plant systems so that appropriate decisions can be made as to their use

These will be parameters that:

(a) Indicate the performance of safety features and support features that are needed to mitigate DBAs;
(b) Indicate the performance of other systems needed to bring the plant to a controlled state;
(c) Indicate the status of safety systems and their support features;
(d) Support the determination of emergency action levels.

These parameters will be typically identified in the EOPs, abnormal operating procedures, functional restoration procedures or plant licensing basis.

3.2.1.5. Estimate the magnitude of any impending radioactive release

These variables will include those that monitor the:

(a) Magnitude of release through identified pathways;
(b) Environmental conditions (e.g. wind speed and direction) used to determine the effect of release of radioactive material through the identified pathways;
(c) Radiation levels and radioactivity in areas surrounding the plant;
(d) Radiation levels and radioactivity in the MCR, in all personnel assembly points and in other areas of the plant where access may be needed for plant recovery.

3.2.2. Parameters to support mitigative accident management

Accident monitoring that supports mitigative accident management needs to provide the safety information required to appropriately respond to plant conditions as the accident progresses. This information is to enable plant operators and emergency response staff:

(a) To terminate or limit further fuel degradation, if possible;
(b) To maintain the integrity of the containment for as long as possible;
(c) To minimize on-site and off-site releases and their adverse consequences;
(d) To provide information for off-site management of the emergency;
(e) To measure radiation levels and radioactivity in areas surrounding the plant;
(f) To measure radiation levels and radioactivity in the MCR and other areas of the plant where access may be needed for plant recovery.

3.3. IDENTIFICATION OF OTHER AVAILABLE INSTRUMENTS

The process for identifying the other instruments that may be available for severe accident management should ideally start with an evaluation of plant instrumentation capabilities for currently operating plants and plants under construction, or proposed system capabilities for nuclear power plants in the development phase. Such evaluation should ideally include a review of plant instrumentation to identify instrument channels that may fulfil the severe accident information needs discussed above, identification of the severe accident process and plant environmental conditions that may affect the survivability of the instrumentation, evaluation of the instrument suitability for implementing SAMGs and evaluation of the instrument ability to survive severe accident conditions.

Based on the environmental and performance requirements, other instrument channels can be assessed to identify instrumentation likely to be available for use in measurement of variables during accident progression. This characterization could also appropriately cross-connect available information with the objective of detecting whether some systems or components can be relied upon for accident management depending on the nature of the initiating event. An example could be a component that has the capability for operating at high temperature, pressure humidity and radiation, among other things, but which has limited resistance to seismic loading. Such a component could be used in a wide variety of accident conditions, unless the accident initiation has resulted from an earthquake. In such cases where the instrumentation identified may be useable only in certain scenarios, the limitations are to be noted in the operator aids. In some cases, it may be necessary to provide aids that assist the operators to infer the necessary information from the available instrumentation or to identify utilization methods that operators may apply to compensate for limitations of instrument channels. Examples of the latter might include use of alternative power sources, rescaling of instrument channels for severe accident conditions or use of portable meters to measure instrument outputs when the normal signal processing or display components are under or over ranged.

An iterative process may be introduced to address this. For instance, the calculated environmental conditions may introduce limits in the duration of use of some existing components or instrumentation, and suggest potential modifications within the accident mitigation guidance to account for these limitations. These proposed modifications may require new calculations to check whether the new strategy is valid. Then, when new equipment designs are

proposed to address these situations, such equipment may also have technological limits that need to be addressed (e.g. owing to extremes in radiation levels present), which would necessitate further adaptations to the strategy.

At the end of this process, a reasonable mapping of what is likely to have adequate reliability for use in severe accident management need to be obtained. The next phase could be a gap analysis based on the above mentioned mapping. The objective of this phase might be to evaluate whether what has been anticipated for accident management can properly work. An example of such an evaluation could be assessing whether adequate instrumentation exist for the specific range of conditions present when a particular component or a system needs to be actuated for a prescribed accident management strategy to be used for a particular range of physical conditions. At the end of the process, a reasonable assessment of existing or contemplated plant capabilities should ideally be available and used in a decision making process. Examples of such decisions are:

(a) Whether the instrumentation that is already available is adequate for purpose;
(b) Whether there are some gaps in information available to the operators, but if those gaps can be compensated for, in part or in total, through the use of alternative existing components or instrumentation;
(c) Whether additional testing or analysis of instrument performance is needed to obtain a better understanding of component or instrument channel capabilities;
(d) Whether upgrades in instrument channels are needed.

The above described analysis needs to be plant specific; consequently, conclusions as to what actions are appropriate could differ from one plant to another. Ideally, a clear, well documented and repeatable process should be defined and then implemented.

An important aspect of this process is obtaining quantitative information that is used for defining anticipated ranges (including uncertainties for adverse conditions) of variables for all phases of accident progression and define set points or characteristic values needed for making important management decisions (e.g. for exiting EOPs or transferring accident management responsibility). This information could encompass physical variable ranges as well as timing, as the root cause of accidents with qualitatively similar progression can be very diverse, and their consequences could significantly differ.

4. ESTABLISHING CRITERIA FOR DESIGNATED ACCIDENT MONITORING INSTRUMENTATION

4.1. INTRODUCTION

This section describes the characteristics that designated accident monitoring instrumentation require to ensure that the needed information will be functionally appropriate and sufficiently reliable during DBA and DEC. The criteria described in this section apply to designated instrumentation identified for use for preventive accident management and mitigative accident management, as identified in Section 3.2. The criteria described in this section do not apply to other available instrumentation (non-designated instrumentation) for severe accident management. The identification of other available instrumentation and the process for confirming their suitability for use in implementing SAMGs and its survivability in severe accidents conditions as identified in Section 3.3.

In the context of this publication, instrumentation is grouped based on its accident monitoring function with regards to when it is expected to be used (i.e. EOPs or SAMGs) and for what purpose (i.e. monitoring safety functions, monitoring safety systems or monitoring radiological releases). Table 1, in Section 2, illustrates the relationship between functional states, accident management approaches and instrumentation, and Table 2 illustrates how the instrumentation will be grouped for discussion in this publication.

TABLE 2. DESIGNATED ACCIDENT MONITORING INSTRUMENTATION COMPOSITION

<table>
<tr><td colspan="4">EOP instrumentation</td><td>EOP and SAMG instrumentation</td><td>SAMG instrumentation</td></tr>
<tr><td colspan="3">EOP instrumentation for monitoring safety functions</td><td rowspan="2">EOP instrumentation for monitoring systems important to safety</td><td rowspan="2">Instruments for monitoring parameters to transition from EOPs to SAMGs and radiological release</td><td rowspan="2">SAMG instrumentation for monitoring safety functions</td></tr>
<tr><td>EOP instrumentation for taking preplanned manual action</td><td>EOP instrumentation to assess status of safety functions</td><td>EOP instrumentation used to detect potential or actual breach of barriers</td></tr>
</table>

Note: Systems important to safety include ‘safety systems’ and ‘safety related items’. EOP — emergency operating procedure; SAMG — severe accident management guideline.

Unless otherwise stated, the discussion given below applies to instrumentation in all functional groups. Where an instrument belongs to more than one functional group, the topics discussed for all of the applicable functional groups need to be addressed. If partition of the instrumentation is needed for a given topic below, the instrumentation will first be divided into instrumentation used for implementation of EOPs and instrumentation used for implementation of SAMGs. Still further segregation may be necessary for certain topics below. When this is the case, the instrumentation will be grouped into four subdivisions:

(a) EOP instrumentation used for monitoring fundamental safety functions (as described in Requirement 4 of SSR-2/1 [1]);
(b) EOP instrumentation used for monitoring systems important to safety;
(c) Instrumentation used for monitoring radiological releases;
(d) SAMG instrumentation used for monitoring safety functions.

EOP instrumentation for monitoring safety functions is sometimes further divided into EOP instrumentation for taking preplanned manual actions, EOP instrumentation used to assess the status of safety functions and EOP instrumentation used to detect potential or actual breaches of barriers.

4.2. ESTABLISHING PERFORMANCE CRITERIA

Analyses are to be used to determine the characteristics that accident monitoring instruments need during the accidents in which they are intended to operate. Such analyses will identify requirements in line with what is needed for the implementation of procedures and guidelines used during accidents conditions. When confirming that the instrumentation has the required characteristics, consideration needs to be given to loads and stressors on the accident monitoring components during the event, and these loads and stressors are to be addressed in documentation. When selecting instrumentation, compromise between different characteristics of instrumentation could be necessary (e.g. an instrument with an excellent response time could have less suitable duration of operation or it could be difficult to replace under severe accident conditions). These performance features are further described in the performance criteria below.

4.2.1. Information from procedures and modelling

Performance criteria for the instrumentation are largely based on the information requirements of the plant accident management procedures and guidelines and the expected behaviour of the accident monitoring parameters under accident conditions (e.g. extreme values or rates of change). The expected behaviour is predicted based upon modelling of the events which the procedures and guidelines are established to address. Accident management procedures and guidelines usually state conditions where operator control actions are necessary, where operators need to confirm the operation of automatic systems or where a transition needs to be made from EOPs to SAMGs. The uncertainty that can be tolerated in the display of variables that indicate these conditions and the differing instrumentation performance needed for DBA and DEC need to be considered when determining the performance criteria of the instrumentation.

4.2.2. Range

When determining the accident monitoring instrumentation range, consideration should ideally be given to all analysed events, including events managed by both EOPs and SAMGs, for which the instrumentation is expected to function. The range of instrumentation used to implement EOPs is to cover, with appropriate margins, the predicted full range of the variables. Typically, margins need to be provided to ensure the instrumentation remains on scale when analytical uncertainties in the predicted range and harsh environment measurement errors are considered.

The range of instrumentation channels provided to determine whether there is a potential for breach, or an actual breach, of barriers to radioactive release needs to be extended to also cover the expected limits of the variables that are predicted when a breach of a fission product boundary is expected. For example, the pressure

instrumentation provided to detect a potential for breach of containment should ideally span the range of predicted containment failure conditions from subatmospheric to overpressure, including margins that are sufficient to account for uncertainties in these values.

Instrumentation used to implement SAMGs are to consider fuel degradation and fuel damage and be sufficient to cover, with margins as appropriate, the predicted limits of the variables that the instrumentation monitors.

Instrumentation may have different range requirements based on intended functions as discussed in the accuracy discussion below. When determining the instrumentation range, the instrumentation accuracy requirements should also be considered. In some cases, it may be necessary that the measurement of a variable will need instrumentation with different ranges to support different accident management functions.

4.2.3. Accuracy

Specific accuracy requirements are to be specified for each accident management function. Accuracy requirements for instrumentation need to consider their intended functions and how the information provided by the instrumentation is to be used. In general, instruments can be separated into two categories: those that are intended to determine the value of a variable (or status of the variable) and those that are to be used to determine the trend of a variable.

Instrumentation for implementation of EOPs has to fulfil accuracy requirements which are derived from the plant's design. If instrumentation is used to determine procedural actions, the accuracy needs to be sufficient to make a clear determination of the condition the procedure is evaluating.

For instrumentation used during SAMG implementation, trending is frequently more important, although a specific value may still be needed. Accuracy requirements for these trending instruments would only need to be sufficient to allow users to determine whether the value is increasing, decreasing or staying roughly the same. Where redundant instrumentation is provided, accuracy needs to be sufficient so that measurement uncertainties will not cause trend information to be ambiguous.

It is possible that a variable may need to be measured with high accuracy during EOP implementation and need less accuracy during SAMG implementation. In these situations, different accuracy requirements may be specified for the instrumentation for EOP and SAMG uses.

4.2.4. Response time

When determining the response time for analogue and digital instrumentation, the instrument's intended function needs to be considered. Timely information is needed, but it should be understood that displayed information will lag behind actual conditions for various reasons.

During implementation of SAMGs, information of higher importance is related to the event progression, which is monitored with the trends of variables. For this reason, instrumentation used for implementation of SAMGs may not need short response times. The response times are nevertheless to allow for trends to be identified and established.

For digital systems, the variable update rate may dominate response times. For example, update rates of the order of once per second are normally sufficient for instrumentation directly read by the operator. Where accident monitoring data is used by computers that may assist operator understanding or by transient logging systems that need to capture evidence of rapid events, these uses may dictate the response time requirements.

4.2.5. Duration of operation

Accident monitoring instrumentation needs to be capable of performing functions over the duration required to enable plant operators to appropriately respond to such accidents according to guidelines and procedures. When determining the accident operating duration, the instrument's intended function needs to be considered.

Instrument channels that the operators need to take preplanned manual actions are to remain operable for at least as long as the latest time when the operator action may be necessary.

Instrumentation channels that are used to assess the status of fundamental safety functions are to remain operable for the longest predicted duration for implementation of EOPs in which the associated safety function is challenged.

Instrumentation channels that are used to detect the potential for breach, or actual breach, of a barrier to radioactive release and to estimate the magnitude of any impending release are to remain operable for the predicted maximum time to bring the plant to a controlled state following implementation of EOPs. Some Member States have selected 100 days as a conservative duration of operation for these instruments.

Instrumentation channels that are used to understand the status of plant systems are to remain operable until the associated systems are no longer necessary for EOP implementation.

Owing to the potential long term monitoring of a severe accident and continued monitoring following a severe accident, some instrumentation used for implementing SAMGs would need to consider long durations of operation (i.e. in the order of years). Designated severe accident instrumentation may not need to be shown to survive for the full duration of the accident and the post-accident monitoring period, as long as the alternative means meet the necessary performance criteria. Instrumentation used for long term accident monitoring following a severe accident need not be shown to operate during the severe accident if it can be installed following the termination of the event. Accident monitoring instrumentation may not need to be shown to survive the full duration of operation if it can be repaired or replaced within an acceptable out of service time.

The required duration of operation for accident monitoring will normally be based upon accident analysis and is usually documented in the plant's licensing basis documents.

4.3. ESTABLISHING DESIGN CRITERIA FOR HIGH FUNCTIONAL RELIABILITY

Accident monitoring functions need to have been designed for reliability. By reliable, it is meant that the indications are to be available in the required locations, continue to meet performance requirements, make sense and can be trusted (e.g. no erratic behaviour resulting from partial failure). Functional reliability is a characteristic both of individual instrument channels and groups of channels that provide a given function or give information about a specific variable. All individual channels need to be reliable. No channel can be free of failure, consequently, multiple instrument channels are needed for monitoring the most critical variables, and efforts to minimize the potential for common cause failure (CCF) of these channels are necessary. Design analysis needs to confirm that a design incorporates appropriate features that are known to promote high reliability, such as redundancy, compliance with the single failure criterion, testability, fail-safe design and rigorous qualification. A combination of qualitative analysis, quantitative analysis and testing is usually needed to demonstrate reliability. Designated accident monitoring instrumentation is to comply with the recommendations for instrumentation and control (I&C) systems given in IAEA Safety Standards Series No. NS-G-1.3, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants [13].

4.3.1. Safety classification

Designated accident monitoring instrumentation is to comply with the recommendations for safety classifications given in IAEA Safety Standards Series No. SSG-30, Safety Classification of Structures, Systems and Components in Nuclear Power Plants [14].

Instrumentation designated for monitoring safety functions during the implementation of EOPs and SAMGs needs to have certain characteristics that represent a higher level of safety. EOP instrumentation used for monitoring of systems important to safety and instrumentation for monitoring radiological release need not meet the higher level of safety, but is still to comply with criteria applicable to all systems important to safety. Application of higher safety classification levels for instrumentation designated for use during implementation of SAMGs does not preclude the use of instrumentation with a lower safety classification if the use of those instruments becomes necessary during an event.

4.3.2. Application of the single failure criterion

EOP instrumentation for monitoring safety functions are not to be lost as a result of random component failures, non-detectable failures or conditions that are caused by the accident that causes the need for the information.

Consequently, these functions are to be designed to meet the single failure criterion. That is, the design is to ensure that the required information will remain available in the presence of the following:

— Any single detectable failure of an accident monitoring component;
— Any undetectable failures;
— All failures caused by a single failure;
— All failures and spurious system actions that cause, or are caused by, the DBA requiring the accident monitoring function.

The application of the single failure criterion to accident monitoring systems should also consider the failure of support features (collections of equipment that provide services such as cooling, lubrication and power supply) that an accident monitoring instrumentation channel requires to function.

CCFs due to maintenance, testing and incorrect functional design are not considered because specific CCFs cannot be predicted. Such failures are dealt with in different ways, such as quality assurance for design, manufacturing, construction, operation and diversity.

Undetectable failures are failures that cannot be detected by systematic testing, alarm or anomalous indication. These failures are normally precluded by good design for testability.

Failures that are caused by the DBA are normally addressed by some combination of separation, protection from or design to withstand the effects of the DBA.

Normally, compliance with the single failure criterion also involves assuming removal from service or bypassing of part of the safety system for testing or maintenance that is allowed by plant operating limits and conditions. This is not necessary when applying single failure to accident monitoring because of the relatively low probability of an event for which accident monitoring is required while a system is out of service and the possibility for rapidly restoring bypassed channels. The duration for which one or more accident monitoring channels is allowed to be out of service needs to be limited by plant operating limits and conditions.

The single failure criterion is not applied to:

(a) Instrumentation provided for monitoring systems important to safety during implementation of EOPs because the status of systems can be inferred by the status of fundamental safety functions.
(b) Instrumentation used for monitoring radiological releases because portable instruments can be used to make measurements. Additionally, instrumentation provided for measuring off-site releases are part of on-site and off-site sensor networks; hence, the failure of a single instrument does not result in an unacceptable loss of data.
(c) Instrumentation for monitoring safety functions during implementation of SAMGs because of the low probability of the failure of the instrumentation coincident with the event. It is desirable, nevertheless, to design these instruments to be robust and reliable so that operators and technical support staff are likely to have plant information upon which to base decisions.
(d) Instrumentation needed only for DEC without significant fuel degradation, because they have a low frequency that makes the combination of the accident with failure of instrumentation improbable. However, the information needed to manage these conditions is frequently the same as those used in DBAs, for which the single failure criterion fully applies.

4.3.3. Redundancy

Redundancy is a method to ensure that operators have the necessary information even if an instrument channel fails. Redundancy may be provided by identical instrumentation, diverse instrumentation or measurements of diverse variables. If failure of a single accident monitoring instrument can result in ambiguity about the value or trend of the variable, an additional channel, or additional channels, is to be provided to allow users to resolve the ambiguous indication. If diverse instrumentation or diverse variables are used to achieve redundancy, aids are to be provided to help the users interpret the information.

SAMG instrumentation for monitoring safety functions may have long mission times and may be exposed to very severe environments. Therefore, redundancy is to be provided unless the single channel can be repaired or replaced within an acceptable out of service time.

Instrumentation for monitoring of safety functions during implementation of EOPs will normally be redundant as a result of compliance with the single failure criterion.

Instrument channels that are used to understand the status of plant systems need not be redundant because the information provided to them can be readily deduced from the instrumentation used to monitor safety functions.

Instrument channels that are used to estimate the magnitude of any impending radioactive release do not need to be redundant because portable instrumentation can be used to take measurements. Instrumentation used for monitoring radiological releases is redundant by design. Additionally, instrumentation provided for measuring off-site releases is part of a network of sensors; hence, the failure of a single instrument does not result in unacceptable loss of data.

4.3.4. Prevention and tolerance of common cause failure

Ideally, identified CCF vulnerability should not have the potential for denying operators the information and variables that they need to control and mitigate accident conditions.

EOP instrumentation for monitoring safety functions and SAMG instrumentation is to be analysed to identify vulnerabilities to CCF. The assessment should consider any CCF of information presented on designated accident monitoring displays as a result of software errors in digital processing of the instrument readings and CCFs of instrument channels. CCF of instrument channels may result, for example, from environmental conditions, unusual process conditions and unexpected events, or failures of instrumentation, cabling, electrical terminations, sensing lines or necessary support systems (e.g. electrical power).

If analysis identifies CCF vulnerability, consideration is to be given to modifying the design, or to the provision of diverse instrumentation or diverse measurements that are not subject to the identified vulnerabilities. Presenting operators and technical staff with diverse indications increases the likelihood that the best accident management decisions possible are made.

For SAMG instrumentation for monitoring safety functions, diversified features to address vulnerabilities to CCF may include other designated accident monitoring instrumentation, other available instrumentation, temporary instrumentation or other data sources.

4.3.5. Independence

The ability of designated accident monitoring instrumentation to provide information needed for monitoring of safety functions during implementation of EOPs or for monitoring of safety functions during implementation of SAMGs should ideally be unaffected by the failure or operation of I&C components that are not part of the accident monitoring system and unaffected by the effects resulting from the postulated initiating events in which the safety functions need to be monitored. Redundant accident monitoring channels should ideally be unaffected by the failure or operation of the other channels forming the redundancy.

Designated accident monitoring channels may provide inputs to other I&C functions provided that the above criteria are met and provided that other plant safety systems are unaffected by the failure or operation of the accident monitoring function.

The various functions of accident monitoring support different levels of the defence in depth concept that is described in SSR-2/1 [1], which requires that levels of defence in depth be independent as far as is practicable. The Appendix illustrates the application of the above principles to achieve independence between accident monitoring functions that support different levels of defence in depth.

For instrumentation used during the implementation of EOPs and SAMGs, means for achieving independence from the failure or operation of components include physical separation, electrical isolation, functional independence and independence from the effects of communications errors.

Electrical isolation devices and features used to provide communication independence for the above functions should be sufficient to protect the channel functions from credible failures external to the channel.

Means for achieving independence from the effects of the initiating event include location of accident monitoring components outside of the area affected by the initiating event and protection from the effects, including environmental conditions. Equipment qualification and diversity may also support independence. These topics are discussed in Section 4.4. Sometimes, a combination of such features is used. For example, if a component is located near a high pressure pipe, physical protection may be needed to protect against missiles or jet impingement from

a pipe break, and the equipment may be designed and environmentally qualified to withstand the high temperature, high humidity and corrosive atmosphere created by the pipe break. Otherwise, it needs to be demonstrated that this component is not required in the case of this pipe break. Generally, a combination of features is employed to achieve the independence goals.

4.3.6. Data validation

Failures or unexpected behaviours of accident monitoring instrument channels may result in the operator being presented with ambiguous indications. Means for validating readings of designated accident monitoring instrumentation need to be provided and documented to provide users with the most valid information available. Methods for validating the readings of accident monitoring instrumentation include range checking, comparison of redundant instrumentation, comparison of readings for variables with a known relationship to each other, comparison with the readings of other available instrumentation, comparison with information from non-instrumented sources (e.g. operator observations or analysis results) and instrument channel health monitoring. Sometimes, more than one of these methods may be needed to validate an instrument. For example, range checking can detect certain invalid readings, but cannot confirm that an on-scale reading is valid.

Validation of the readings of EOP instrumentation used for monitoring safety functions should ideally be possible using instrumentation that meets the same criteria as applied to designated accident monitoring instrumentation performing these same functions. Normally, this may be accomplished by comparing the readings of redundant channels. If different readings by redundant channels do not allow a conclusion about a variable value, other designated instrumentation meeting the same criteria should ideally be available to allow resolution of the ambiguous reading. Often, the ability to resolve ambiguity is provided by having three independent channels measuring the same variable.

Validation of the readings of SAMG instrumentation for monitoring safety functions should be possible using other designated SAMG instrumentation, other available instrumentation, temporary instrumentation or other data sources.

Cross-channel checks alone might not be sufficient to validate designated accident monitoring instrumentation for monitoring of safety functions during severe accidents. Experience has shown that unexpected plant configurations and environmental conditions may result in CCFs of instrumentation. Provisions for validity checks against other related variables and against other available instrumentation are to be established and documented.

Sufficient time needs to be allowed for validation when it is performed by the operator. Operator aids need to be available to help operators validate the readings of designated accident monitoring instrumentation. Electronic operator aids (e.g. computer systems) may be used, but for instrument readings that provide information needed for monitoring of safety functions during EOP implementation or for monitoring of safety functions during a severe accident, non-electronic backup methods are necessary.

4.3.7. Power supply

Most measurement devices need power to operate, and virtually all control room displays require power, even if the associated sensor is self-powered. The electrical supply to accident monitoring channels that need external power needs to be reliable enough to give reasonable assurance that accident monitoring systems can operate as expected for the duration of the accident.

EOP instrumentation for monitoring safety functions need to be powered from safety classified sources that meet the criteria given in IAEA Safety Standards Series No. NS-G-1.8, Design of Emergency Power Systems for Nuclear Power Plants [15]. The criteria of NS-G-1.8 [15] are intended to prevent the power supplies from being incapacitated by the initiating event, in particular in the case of an external initiating event (coupled with dependent events when appropriate), by environmental conditions prevailing during an accident or by failure of power from off-site sources, the plant's main generator or other units. Power needs to be provided from uninterruptable sources unless analysis shows that short interruptions are acceptable.

Where a power supply is necessary for SAMG instrumentation, provisions need to be made to allow these instrument channels to operate from separate standalone power supplies. These separate standalone power supplies are to be independent of the normal and dedicated backup power supplies. Provisions need to be made in advance

to replenish any consumable items needed by the standalone power sources (e.g. electrical charge, filters or fuel). Sufficient consumables need to be readily available to allow for delays in resupplying from outside sources.

4.3.8. Calibration

Designated accident monitoring instrument channels need to be calibrated. Provisions need to be made for calibration of accident monitoring instrument channels at a frequency that ensures that the channels are accurate enough to perform their function. The calibration interval assumed in establishing calibration variables (e.g. expected drift over the time between calibrations) need to account for the EOP implementation duration unless recalibration is possible under accident conditions. Instrumentation needs to be calibrated over the range of use during accident conditions. When calibration requires specific facilities (e.g. calibration of radiation monitors), appropriate arrangements are to be envisaged.

Instrument channel calibration may be affected by accident conditions. Therefore, means need to be provided to allow the calibration to be validated during accidents. If this validation needs the intervention of staff in the area with degraded environmental conditions, analysis should ideally show that the conditions where the staff need to work in will be tolerable for the duration necessary to complete the needed calibrations.

It may be preferable that the design provides means to calibrate accident monitoring instrument channels during accident conditions such as:

(a) Locating sensors and electronics in areas that will remain accessible to maintenance staff during the events for which they are required to operate;
(b) Basing the calibration on the sum of the normal calibration interval and the accident duration;
(c) Selecting instrumentation that does not require periodic calibration;
(d) Calibrating by comparison with other information that has a known relationship to the display channel;
(e) Automating calibration features.

4.3.9. Testability

Periodic testing plays an important role by reducing the time before failure of an instrument channel is detected and corrected. Complete failure of a channel is often quickly recognized by plant operators, who frequently need to check the indication of accident monitoring channels. Testing is necessary to detect more subtle failures such as excessive drift or indication biases. A periodic test programme needs to be established for designated accident monitoring instrument channels. The scope, method and frequency of testing needs to be justified as being consistent with functional and availability requirements.

Means for checking the operability of designated accident monitoring instrument channels are to be documented. Means for confirming operability include:

— Observing the effects of conditions that cause the monitored variable to change;
— Substituting a known and changing signal for the normal sensor input;
— Cross-checking between channels that have a known relationship with each other;
— Automating on-line diagnostics of the channel.

If on-line diagnostics are the only means provided to confirm operability of an instrument channel, the on-line diagnostics are to meet the same requirements as the channel itself.

4.3.10. Direct versus indirect measurement

In most circumstances, direct measurement of a variable of interest will be more reliable and more accurate than indirect measurement (i.e. inferring the value of a variable from readings of variables that have a known relationship to the variable of interest). Some variables of interest, however, cannot be measured directly. Measurement of the maximum linear heat generation rate of fuel rods in the core is an example. To the extent practicable, designated accident monitoring instrumentation needs to directly measure plant variables.

Designated accident monitoring instrumentation may also make measurements by indirect means such as a calculation based upon multiple measurements or determination of the value of a variable based upon measurement of other data with a known relationship to the desired variable. Ideally, the use of indirect measurements should be justified, the possibility of misinterpretation of the indirect measurement should be addressed and operator aids should be available to help operators interpret the indirect measurements.

4.3.11. Control of access and computer security

Unauthorized physical or electronic access to accident monitoring channels increases the possibility of damage or modification of the channels. Experience shows that such damage and modification is usually unintentional, but the possibility of malicious acts needs to be considered, especially for digital systems. Access to accident monitoring instrumentation is to be limited to prevent unauthorized access and to reduce the possibility of error. Areas of particular concern are access to set point adjustments, test points, controls for removing a channel from service, calibration adjustments, analogue connection points, data connections for digital systems, and configuration data because of their importance to preventing degraded system performance owing to potential errors in operation or maintenance. Under severe accident conditions, personnel unfamiliar with plant systems and entering a site for remediation can unintentionally jeopardize plant systems.

Effective methods include appropriate combinations of administrative measures, electronic access control and physical security (e.g. locked enclosures, locked rooms or alarms on enclosure doors). Guidance on physical security for nuclear power plants is given in:

— IAEA Nuclear Security Series No. 4, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage [16];
— IAEA Nuclear Security Series No. 8, Preventive and Protective Measures against Insider Threats [17];
— IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [18].

IAEA Nuclear Security Series No. 17, Computer Security at Nuclear Facilities [19], provides guidance on computer security for digital systems used in electronic access control.

The methods used for controlling both physical and electronic access to digital elements of designated accident monitoring instrument channels need to be justified as providing the required security without interfering with the performance of safety functions.

Data from designated accident monitoring instrument channels may be transmitted to plant locations outside the control room and to locations outside the plant (e.g. emergency operations facility). The designated accident monitoring instrument channels are not to be adversely affected by connections such as, for example:

— Failure, operation or maloperation of equipment in these locations;
— Failure, operation or maloperation of the communication paths to these locations;
— Activities of personnel in these locations.

4.3.12. Maintenance and repair

Effective and well planned maintenance reduces the failure rate of electronic systems. When failure of an instrument channel is detected, the ability to rapidly diagnose the problem and start the repair makes an important contribution to channel reliability. Accident monitoring systems need to be designed such that they can be maintained, repaired, replaced and adjusted with appropriate periodicity, either during normal plant operation or at shutdown, and, when possible, repaired during an accident. Although repair and replacement may be desirable during and following an accident, it may not always be possible because of the location and environment in the area around the damaged equipment. Therefore, the accident monitoring systems needs to be designed to avoid or minimize the repair activity and time at the harsh environmental locations during an accident.

Before designing for repair, factors such as delay for making the system operational and environmental conditions for repair including access to buildings if appropriate need to be carefully analysed. Personal radiation protection under accident conditions (e.g. using airline respirators and protection suits) can greatly hinder

the work of operators or other technical staff. The decontamination procedures of personnel and equipment also need to be envisaged. When the possibility of repair has been chosen for the accident monitoring system or part of it, a guidance document detailing all operations to be made (i.e. access to system locations, assessment of environmental conditions and detailed repair scenarios, among other things) need to be established, and operators are to be periodically trained to provide reasonable assurance that repairs can be done in a timely manner.

Some SAMG instrumentation for monitoring safety functions may be expected to fail during service because of extreme environmental conditions or exceptionally long required operating duration. In these cases, a clear strategy for obtaining the necessary information after failure needs to be developed. This may include use of alternative instrumentation, use of non-instrument data sources or provisions to replace failed instrumentation. Provisions for replacement should consider accessibility to work locations, ease of replacement and provisions for recalibration.

4.3.13. Support features

Failure or incorrect operation of support features can result in failure or incorrect operation of accident monitoring channels. Electrical power is an example of such support features, but other supporting features such as compressed air supplies and cooling systems may be important in certain cases. Support features, whose failure or maloperation could adversely affect the ability of designated accident monitoring instrumentation to perform the functions, need to meet all applicable requirements of the associated accident monitoring instrumentation. Where a support feature depends upon replenishment of consumables (e.g. filters, compressed air, fuel or electrical charge), design provisions are to ensure necessary access to replace these items, an appropriate inventory of replacements needs to be maintained on-site, and procedures need to be in place to carry out replacement under accident conditions.

Other support features that are not required for operability of accident monitoring channels are to be designed so that their operation, failure or maloperation cannot degrade the capability of accident monitoring channels. SAMG instrumentation for monitoring safety functions needs to have a minimum dependence on support features.

4.3.14. Use of portable instrumentation

Portable instrumentation may be used as designated accident monitoring instrumentation. In such cases, the instrumentation used, means for communicating the data and the means for analysing data are to meet the requirements applicable to the accident monitoring functions that are supported. The instrumentation is:

(a) To be readily available to trained plant staff under accident conditions;
(b) To be periodically tested and calibrated;
(c) To be stored in a manner that protects them from internal and external hazards;
(d) To be stored together with sufficient supplies of consumables (e.g. batteries or filters) to keep them in service until resupply is assured.

Design provisions are to be implemented to facilitate the use of this equipment (including limitations on use under environmental conditions such as radiation field) and particularly reduce delays for implementation. The use of portable monitors requires a well established system of documentation of measurements performed on a site.

A use of innovative methods (e.g. robots or unmanned aerial vehicles) under challenging environmental conditions need to be analysed.

4.4. ESTABLISHING QUALIFICATION CRITERIA

Equipment qualification includes functional qualification, qualification for the effects of internal events, electromagnetic qualification and qualification for the effects of external events. Qualification for the effects of internal events, external events and electromagnetic environments aims to ensure that these events do not result in CCFs of accident monitoring functions.

Functional qualification is considered in the discussion of quality assurance in Section 4.6.

4.4.1. Hazards to be considered

EOP and SAMG instrumentation for monitoring safety functions is to remain available when exposed to the effects of any internal and external hazards that could credibly initiate or result from the accidents for which they are needed. Environmental hazards to be considered include:

(a) Environmental effects of accidents:
  (i) Temperature (including high and low temperature areas and fires);
  (ii) Pressure (including high sustained pressures and impulse pressures, e.g. a shock wave or impact);
  (iii) Moisture (including relative humidity and submergence);
  (iv) Radiation field (including contamination);
  (v) Vibration (including high and low frequencies);
  (vi) Chemical exposure (including process spray, smoke or gas);
  (vii) Combined effects of these parameters.
(b) Electromagnetic effects:
  (i) Ambient radiated electromagnetic field as a function of frequency;
  (ii) Conducted electromagnetic field as a function of frequency;
  (iii) Credible voltage surges that need to be endured.
(c) Seismic effects:
  (i) Seismic spectrum at the equipment location;
  (ii) Shock waves and vibration from impacts (internal and external).

The following publications of the IAEA Safety Standards Series discuss internal and external hazards and the measures for qualifying or protecting against these hazards:

— IAEA Safety Standards Series No. NS-G-1.5, External Events Excluding Earthquakes in the Design of Nuclear Power Plants [20];
— IAEA Safety Standards Series No. NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants [21];
— IAEA Safety Standards Series No. NS-G-1.7, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants [22];
— IAEA Safety Standards Series No. NS-G-1.11, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants [23].

4.4.2. Protection against hazards

Accident monitoring functions are to be protected, to the greatest extent possible, against CCFs that may result from internal or external events. Protection usually takes the form of barriers or physical separations such that a single event cannot disable a monitoring function. For example, protection against the effects of an internal missile may be achieved by protecting the equipment with a barrier, or by physically separating redundant instrumentation so that the failures that result from the missile will not disable the monitoring functions.

When protection is provided for instrumentation for monitoring of safety functions during implementation of SAMGs, it should be considered that the consequences of a hazard may be more severe or further reaching than the hazard consequences associated with a DBA. For example, the effects of an external hazard that exceeds the plant design basis may be much more severe than the effects considered for a DBA.

4.4.3. Determination of hazard environments

It is not always feasible to fully protect equipment only through the use of barriers or physical separation. This is normally the case for environmental effects caused by accident conditions, electromagnetic effects and seismic effects. Where protection alone is insufficient, qualification of equipment for the hazard environments is necessary.

Both magnitude and duration of exposure to the environmental variables should be considered when assessing equipment performance under and after environmental exposure. Normally, equipment is not qualified for specific locations, but for values that bound the effects in the area where it is located. The effects of environmental conditions on the instrument readings should ideally be estimated by taking into consideration the local environmental conditions, which can deviate from global conditions. Instrumentation that is qualified under global conditions may not function properly under local conditions. The expected failure modes and resultant instrument indications (e.g. off-scale high, off-scale low or floating) for instrumentation failures in severe accident conditions that are beyond the design basis need to be identified.

Methods for determining the hazard environments caused by internal and external hazards that are considered in the design bases are to be well established and documented. These hazards are not as well defined for severe accidents. Sources of information for estimating the environmental effects caused by severe accidents include:

— Source term estimation;
— Severe accident modelling;
— Experience from previous severe accidents.

Accident progression modelling codes may be used to determine the environmental conditions that may affect the survivability of instrument channels and the performance requirements (e.g. range and mission time) required for severe accident monitoring channels. Although many efforts have achieved considerable qualitative and quantitative accident progression modelling results, it is difficult to claim that such results allow for formal code validation in the strict sense. Some physical phenomena are not readily amenable to scaling, and, more generally, the only references available for global comparison of real situations to code simulations are limited, and give global rather than local variables. The results of such codes can provide qualitative predictions, and the quantitative results should be considered as having been determined with a degree of uncertainty. However, even though the quantitative results have uncertainty, engineering judgement can be used to estimate the approximate degree of uncertainty. Thus, the code operator is either to have a broad knowledge regarding severe accident phenomena, computer code characteristics and limitations, and potential plant specific design improvement limitations, or else ensure that the code operator is working closely with personnel who do have such knowledge. In all cases, a high degree of carefully considered engineering judgement is required.

Prediction of severe accident environments and performance requirements will need to consider a range of core states (e.g. fuel cladding is oxidized but intact; fuel is badly damaged but still in the reactor vessel; significant quantities of core debris are outside the reactor vessel) and a range of containment conditions (e.g. containment intact; containment intact but challenged by conditions such as insufficient heat removal, hydrogen accumulation or core–concrete interaction; containment integrity is lost, but fission products are still passing through the containment; containment is bypassed). The prediction will also need to evaluate a range of scenarios such as loss of coolant accident (LOCA) with failure of the emergency core cooling system (ECCS), extended loss of the ultimate heat sink, extended station blackout and loss of all alternating current and direct current power sources.

4.4.4. Qualification to withstand hazards

Accident monitoring instrumentation is to be designed to withstand expected seismic conditions and qualified in accordance with NS-G-1.6 [21], and designed and qualified for the electromagnetic environment in accordance with the guidance of NS-G-1.3 [13]. Accident monitoring instrumentation that may experience harsh environmental effects resulting from accident conditions need to be designed to withstand these conditions and qualified by type tests to demonstrate that they will remain operable in the worst case postulated accident environment (with a margin) in which the instrumentation is needed. Processes for qualifying instrumentation to withstand the environmental effects of design basis internal and external hazards are well established and will usually include type testing for instrumentation that will be subjected to harsh environments. See, for example, IEEE Standard 323 [24] and IEC Standard 60780 [25] for environmental effects of accidents, IEC Standard 62003 [26] for electromagnetic effects, and NS-G-1.6 [21] and IEC Standard 60980 [27] for seismic effects. These approaches may also be applied to instrumentation that supports monitoring of severe accidents.

It may not always be possible to type test instrumentation used for monitoring safety functions during severe accidents. Owing to the extreme environmental variables associated with severe accidents, it may sometimes be impractical or even impossible to test instrumentation for severe accident conditions. Approaches to deal with this situation include:

(a) Use of extremely robust instrumentation that is not likely to be damaged by the expected conditions;
(b) Relocate, where possible, instrumentation to a location where exposure to severe environmental conditions can be limited;
(c) Use of portable instrumentation stored away from the expected severe environmental conditions;
(d) Analysis of instrumentation to assess its capability to withstand conditions that exceed the qualification conditions;
(e) Separate testing for the most severe environmental variables (e.g. high temperature testing without simultaneously simulating associated pressure and humidity environments);
(f) Testing to failure of the instrumentation for given environmental variables.

Instrumentation used during implementation of SAMGs that is not type tested for the full range of postulated accident conditions needs to be tested for conditions that are as close as practicable to the postulated severe accident conditions. Such testing needs to be supplemented by a survivability analysis performed for the anticipated severe accident environments using information obtained from failure testing. The survivability analysis would be used to determine environmental constraints for the reliable use of the instrument data.

4.5. ESTABLISHING DISPLAY CRITERIA

Display criteria for accident monitoring instrumentation should consider operator tasks and information needed during and after an accident. These criteria have been historically undervalued in conventional design considerations for control room layouts. Simple and effective displays for operators and emergency personnel should consider the level of stress and confusion that can exist during accident management situations. Ensuring that operators in the control room or technical staff in the TSC (or other alternative command and control locations) can efficiently identify and communicate critical information during accident conditions increases the likelihood that an optimal decision will be reached.

The display characteristics for accident monitoring need to be determined on the basis of an analysis of the functions required to respond to an accident and analysis of the tasks required of the operator to implement those functions. Display characteristics need to be identified to include range, accuracy, display format (e.g. status, value or trend), units and response time consistent with the performance characteristics discussed in Section 4.2. The following considerations are also to be accounted for in the design of the display.

4.5.1. Human factors

The likelihood of human error increases during accident situations because of the increased stress associated with the event, so accident monitoring displays need to be designed through application of accepted human factor methods and principles. These include illumination, size, geometry, layout, available content, suitable format and standardization of the displays, and should consider the task to be performed with the information provided by the display. The various types of data available to the operator need to be grouped based upon the tasks and not on the sources of data. Staffing assumptions, operating experience reviews, functional requirements analysis and task analysis provide the bases for identifying the human–system interface requirements for accident monitoring.

4.5.2. Anomalous indications

Ideally, accident monitoring instrumentation should not cause indications on displays (i.e. meters, annunciators, recorders or video display units) to give anomalous readings which may misinform plant operators or be potentially confusing. To the extent practicable, additional displays need to be provided for EOP and SAMG

instrumentation for monitoring safety functions so they can be used to validate or confirm that the information provided is not anomalous.

4.5.3. Continuous versus on demand display

At least one of the redundant display segments for accident monitoring instrumentation used for EOP and SAMG instrumentation for monitoring safety functions needs to be either a validated digital display or a dedicated analogue display. Because of the potential loss of normal and backup power during a severe accident, this display needs to be able to operate self-powered or from portable power supplies for the instrumentation used for monitoring safety functions during implementation of SAMGs.

Displays for EOP monitoring for systems important to safety and for monitoring radiological releases may be accessible on demand.

4.5.4. Trend or rate information

Trend displays are to be utilized to display plant and system status information in a graphical manner where the user is required to visually scan and compare sets of data, identify changing patterns, detect deviations from normal values, determine rate of change, monitor slow changes in variables and predict trends.

If direct or immediate trend or rate information is essential, the trend information needs to be continuously available on dedicated trend displays and selectively available on another redundant trend display. Since trend data are necessary during implementation of SAMGs, these criteria would apply directly to SAMG instrumentation, but may also apply to EOP instrumentation when trending is procedurally required.

The display needs to have the capability of providing sufficient data to allow the trend to be established. Trend displays should ideally be capable of showing data collected during time intervals that are consistent with the expected rate of change in plant conditions.

Trend graphs on a computer based display device need to display data in a manner that is sufficient to provide the information needed to make decisions related to the procedure or guidance being implemented. The graph will always indicate the normal or safe operational ranges, along with current values for the plant variables. The number of variables indicated on a single trend graph needs to be limited to avoid complexity and confusion.

4.5.5. Display identification

Operators and TSC staff need to be able to quickly determine which instruments are the primary instruments to be used during accident and severe accident conditions. Control room indication of EOP and SAMG instrumentation for monitoring safety functions need to be continuously available and uniquely identified as accident monitoring instrumentation with a characteristic designation so that the operator can easily discern information intended for use under accident conditions. Since control decisions for the implementation of SAMGs might not be done from the control room, the severe accident instrument displays also need to be uniquely identified in the TSC or other alternative command and control locations. Bold insignia, such as highlighted instrument bevels or backdrops of various colours, are examples of highlighting methods for panel mounted displays.

On a multivariable video display containing both accident monitoring and non-accident monitoring instrumentation displays, EOP and SAMG instrumentation for monitoring safety functions are to be uniquely identified within the display.

4.5.6. Display location

Control room indication of accident monitoring system displays needs to be placed in locations that are appropriate for their functions. The basis for display locations need to include functional task analysis results and accepted human factor principles, including time to access the display and the accessibility of the display location.

To the extent practicable, the same displays used for normal plant operation need to be used for on demand accident monitoring displays. It may be necessary that the severe accident management information be displayed on a different display device than that of the normal and design basis event related displays.

For SAMG instrumentation, provisions to remotely monitor essential variables should be considered. The potential for loss of access to the control room or remote shutdown panel should ideally be assumed when determining design requirements for severe accident monitoring systems. Communication systems for transmitting data or verbal information are to be reliable and secure.

Accident monitoring displays in the TSC and any other alternative command and control locations need to be placed in a similar configuration to the control room displays, to provide familiarity with the display layout in both locations and to be continuously updated during normal operation so that there is no lag in providing information to the TSC staff and in the transition of the event command and control from the control room to the TSC (or other alternative command and control locations) once the accident transition point is reached.

4.5.7. Information ambiguity

Displays provided for the sole purpose of resolving information ambiguity do not need to be of the same type as the primary instrumentation and can be available on demand. Information ambiguity needs to be addressed by the data validation methods described in Section 4.3.6.

4.5.8. Recording

Recording is to be provided during implementation of EOP and SAMG instrumentation used for monitoring safety functions. Recording also needs to be provided for instrumentation used to monitor radiological releases (other than where portable instrumentation is used).

Accident monitoring data records need continuously to be updated, stored and accessible on demand. Recording may be performed using digital or analogue means. Recording devices may consist of non-safety related equipment. Recording need to be operable before, during and after an accident, and to have provisions for being powered from supplies that are independent of the plant power supplies (see Section 4.3.7). Playback of the recordings needs to be available on demand.

4.5.9. Digital display signal validation

If signal validation is used, the validity of the indication needs to be provided as part of the display, for example, through the use of unique colour coding.

4.6. ESTABLISHING QUALITY ASSURANCE CRITERIA

Accident monitoring instrumentation need to be developed and maintained in accordance with a nuclear quality assurance programme that complies with appropriate guides, such as:

— IAEA Safety Standards Series No. NS-R-3, Site Evaluation for Nuclear Installations [28];
— IAEA Safety Standards Series No. NS-G-3.1, External Human Induced Events in Site Evaluation for Nuclear Power Plants [29];
— IAEA Safety Standards Series No. SSG-18, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations [30].

Requirements, design and development activities for accident monitoring systems and components need to be documented in sufficient detail to support verification and validation, regulatory review, manufacture, installation, commissioning, operation and modification. This documentation is to be maintained under a change and configuration management programme.

The components of accident monitoring systems are to be type tested to demonstrate compliance with the requirements related to monitoring for EOP implementation. Although type testing is the preferred method for demonstrating that accident monitoring instrumentation is qualified for DBA conditions, additional methods may be used for qualification when justifiable. Accident monitoring components and systems are to be tested during system commissioning and periodically during operation to demonstrate satisfactory performance and that

functionality is not degraded by faults. Periodic testing methods need to detect failures of redundant measurement channels and need to be performed frequently enough to provide reasonable assurance that independent failure of redundant components will not disable an accident monitoring function.

Instrumentation used for implementation of SAMGs may be subject to environmental extremes and operation times that make type testing impractical. In these cases, the equipment used within accident monitoring systems needs to be type tested to demonstrate compliance with the requirements under conditions that are as close as practical to severe accident conditions. These tests need to be supplemented by other methods to assess the capability of components to perform in more extreme environments.

The development of novel or complex designs are to be subject to additional levels of verification and validation.

5. DESIGN AND IMPLEMENTATION CONSIDERATIONS FOR ACCIDENT MONITORING INSTRUMENTATION

This section presents aspects of the implementation of the accident monitoring system designed on the basis of the criteria outlined in Section 4 above. Also included are certain aspects of using this system, including training of staff and testing.

5.1. DIFFERENCES FOR NEW AND EXISTING PLANTS

The integration of an accident monitoring system can be accomplished much more easily for a new plant compared to retrofit application at an existing plant. If design and performance criteria are taken into consideration from the start, additional sensors, containment penetrations, raceway and sheltered locations for transducers and data processing units can be entered into the early design phase.

If a new or modified accident monitoring system has to be installed at an existing plant, the duplication of measurement channels for several systems might not be possible. For instance, the installation of additional nozzles for pressure measurements at the reactor pressure vessel (RPV) or penetrations through the containment wall might not be practicable. In these cases, data required for the accident monitoring system may have to be branched off from existing measurement channels. This should ideally be accomplished without endangering the licensing basis of the reactor because the sensor signals may affect other aspects of the safety I&C. The following potential constraints for a retrofit installation at an existing plant need to be analysed when starting with the design of an accident monitoring system:

(a) Already existing instrumentation for operational or safety I&C purposes that is needed for monitoring several selected variables;
(b) Already existing instrumentation that is used for monitoring purposes and that is to be integrated into the accident monitoring system;
(c) Location of the sensors and cable routeing for new instrumentation.

The concept of the accident monitoring system can be established after these fundamental constraints are addressed. Such arrangements can comply with the criteria given in Section 4 if the necessary independence, resistance to CCF and (where applicable) the single failure criterion. The Appendix gives an example of how accident monitoring channels may share common measurement channels without introducing significant dependencies between the various instrumentation functions.

5.2. DESIGN CONSIDERATIONS

To comply with the performance and design criteria above, the location and robustness of the instrument components need to be considered. To the extent possible, physical protection and separation from the harsh environment are to be provided if they can be performed without sacrificing the ability of the instruments to collect the required data or jeopardizing the robustness of barriers to fission product release. If physical protection is not practical, the design of the equipment should consider the robustness of each of the components. The design will have a direct impact on the availability and validity of the data needed from the instrument.

'Accident proof' equipment for sensors, cabling and transducers is to be used for accident monitoring. The locations for the sensors, the cable routeings and the locations for the transducers are to be selected in the most favourable and sheltered manner to allow for a long survival time in case of accident. Since the course of DEC may not be known in advance, failure of even well placed and robust equipment cannot be excluded.

One of the most important auxiliary support features of the accident monitoring system is the power supply, including standalone, independent, power supplies for SAMG instrumentation. Such a power supply might take the form of a small portable power supply, which will provide the required power to the systems installed at the site for a defined time period, for instance three to ten days. A battery power supply or a combined power generator solution with backup batteries could be applied for this purpose. Such supplies need to be independent of the plant power system (i.e. independent of the plant and off-site power sources and also independent of the plant electrical distribution system).

When planning the installation of the instrumentation, consideration is to be given to easy access for testing, repair and replacement, even under accident conditions.

5.3. CONSIDERATIONS FOR COPING WITH SEVERE ENVIRONMENTAL CONDITIONS

5.3.1. Radiation release and other environmental effects created by accidents

Fission products are released from the fuel during an accident, but measurement of the magnitude of such releases in the containment is difficult. Such releases are problematic for components and instrumentation situated inside the containment, as well as for evaluating potential external consequences.

Radiation exposures to equipment inside the containment during DEC are expected to be much higher, in many places, than those resulting from DEC that can be terminated without extended degradation of the fuel cladding. Although the relative differences in radiation exposures are not expected to be the same in all areas of the plant, they are expected to be considered as part of the environmental conditions required for instrumentation. All instrumentation used for implementation of SAMGs needs to be designed and installed to withstand local anticipated conditions. Design for survivability may be done either through selecting instrumentation that has intrinsic resistance, by type testing, or through protecting instrumentation that has less resistance. Alternatively, design for accessibility to replace the equipment should be considered.

Appropriate attention is to be paid to other environmental conditions (e.g. high pressures, temperatures or moisture), consequential effects of radiation exposures (e.g. radiolysis), manufacturing specifics (e.g. materials) or installation provisions (e.g. shielding), which could lead to partial degradation of some information, to make sure that they do not unacceptably alter the quality of the anticipated information.

The following may help to improve the quality and reliability of instrumentation response:

(a) Avoid installing instrumentation in areas where it is unnecessarily exposed to high radiation levels. Different locations with less demanding environmental conditions may help obtain adequate accuracy conditions.
(b) When optimizing instrumentation location, credit plant layout specifics and operational constraints. Installation can be installed in a limited number of places, and such locations are to be screened to eliminate those that would make some routine activities difficult (e.g. inspection, minimal testing and access to other components, among others).
(c) Check whether the range of operation of instrumentation to be used is adequate for the contemplated range of plant degradation.

(d) Use environmentally qualified cables, cable terminations and termination procedures in harsh environment areas, even for instrument loops where the sensors and transmitters have not been qualified.
(e) Assess contemplated instrumentation qualification and survivability, for the range of contemplated environments.
(f) When additional data are required to assess component behaviour in a degraded environment, define an appropriate process for getting some data. In particular, if further tests are needed to assess further resistance, evaluate practicable paths.
(g) When possible, contemplate the use of proven technology, in particular, radiation resistant technology.
(h) When available instrumentation (already installed or commercially available) does not give sufficient confidence that the instrument response is adequately reliable, explore ways to obtain more reliable information:
  (i) Evaluate whether the required accuracy is reasonable in the anticipated situation and whether simpler information (e.g. trends) would allow more robust implementation of contemplated guidelines.
  (ii) Evaluate direct use of other available instrumentation or cross-connection of existing information. In such cases, develop comprehensive supporting documents that help to minimize the risk of misinterpretation of readings by control room operators or TSC personnel.
(i) Recognize the fact that global reliability of accident management instrumentation is given by the weakest link of the system (e.g. cabling, cable terminations or data collection systems).
(j) When assessing radiological releases, attention needs to be paid to the spatial distribution of releases on-site as well as off-site.

5.3.2. Combustible gases

Combustible gases can be generated as a result of radiolysis, cladding oxidation (i.e. zirconium and steel) and chemical reactions during core–concrete interaction after vessel melt-through. Combustible gases pose significant challenges to component integrity, including information systems. Even if detonation is prevented in the containment by use of an inert atmosphere, recombiners or igniters, hydrogen may accumulate in the containment. Because of potential containment leakage, a risk of explosion in surrounding rooms exists. This risk is to be evaluated and considered in the design of the instrumentation. Accident monitoring instrumentation needs to be located or protected such that the combustion or heat from the recombination of combustible gases does not lead to a loss of accident monitoring functions.

Combustible gases are not expected to be evenly distributed. This creates two issues for consideration. First, information provided to plant operators may not be representative, unless the design of the monitoring system has taken into consideration the potential uneven distribution of combustible gases. A typical example is hydrogen concentration when the containment atmosphere cannot be mixed. The measurement may be valid if the sampling location has been evaluated as being representative of gross hydrogen concentration (e.g. the multiunit Canada deuterium–uranium (CANDU) stations can have four to six reactor units connected to the same containment). Second, the bulk of the containment volume is not necessarily the only zone of interest for equipment protection. Other zones of the containment building (e.g. some cubicles) or other buildings may shelter instrumentation considered important for managing some complex situations. Such zones or buildings need to be identified and evaluated to obtain reasonable assurance that the contemplated instrumentation, as installed, is likely to perform as expected in degraded conditions.

Information that can be used for specifying appropriate ranges of combustible gas monitoring instrumentation includes:

— Precalculated prevailing combustion regimes (inert or slow/fast deflagrations);
— Precalculated threats to the containment by combustion loads;
— Precalculated hydrogen release into the containment and mixing in the containment regions;
— Precalculated carbon monoxide concentration during the core–concrete interaction.

Combustible gas monitoring usually relies on some form of gas sampling. Performance of the instrumentation is adversely affected by:

(a) Water and aerosol plugging of instrument lines or probes because of steam condensation, potentially leading to strongly biased results;
(b) Radioactive contamination in sampling lines and sampling systems;
(c) Changes in the resistivity of signal cables due to radiation, moisture and temperature;
(d) High temperatures at the analyser locations.

Diversity and separation should be considered to cope with CCF. Consideration needs to be given to use of intrinsic safety and explosion proof designs.

5.3.3. Accident sampling system

An accident sampling system or other adequate sampling facility could be considered for use in taking regular samples from plant systems. The accident sampling system is capable of obtaining representative reactor coolant and containment air and fluid samples that support accurate analytical results for the parameters of interest. If an accident sampling system does not exist, other approaches are to be adopted for fuel damage evaluation and for estimation of the inventory of fission products released into the containment.

Specifications of the radiological and chemistry parameters to be monitored may include:

(a) For primary coolant and sump sampling:
  (i) Gross activity;
  (ii) Gamma spectrum;
  (iii) Boron content;
  (iv) Dissolved hydrogen (applies only for primary coolant);
  (v) Dissolved oxygen (applies only for primary coolant);
  (vi) pH.
(b) For containment air sampling:
  (i) Hydrogen (and other combustible gas) content;
  (ii) Oxygen content;
  (iii) Gamma spectrum.

Use of a containment sampling system constitutes a potential containment bypass path. Design of this system is to include measures to reduce the risk of significant containment leaks when using the system, particularly during DEC.

5.4. MAINTENANCE AND TESTING

Instrumentation is to be designed to enable periodic testing and maintenance. Test and maintenance programmes need to be planned to minimize the time during which accident monitoring channels are out of service. The operability of instrument monitoring channels are to be confirmed frequently during normal operation, but the need to remove instrument channels for this is to be avoided to the extent practical. This might be accomplished, for example, by frequent checking of the behaviour of channels, and periodically checking the consistency between redundant and diverse channels. Prognostic and diagnostic analysis of instrument channel readings may also be a useful tool. Recalibration of the sensors might require dismantling of the sensors and, thus, it may be preferable to do so during a plant shutdown when it is possible without degrading reliability.

5.5. TRAINING

Plant operators are to be trained in the characteristics and use of designated, portable and other available accident monitoring instruments so that they are prepared to correctly interpret and properly use the accident monitoring information. The operators need to be able to realize, based on the indications provided by the accident monitoring instrumentation, changes in accident progression at the earliest moment to enable timely implementation of appropriate measures. Training should consider the use of both electronic and non-electronic operator aids to improve the effectiveness and success of the performed measures under the time pressure constraints of a real accident.

Personnel implementing SAMGs are to undergo training similar to that for plant operators to interpret the indications from the accident monitoring instrumentation. Users of information from accident monitoring systems and other available instruments are to be trained in the capabilities, limitations (including mission time), survivability and failure behaviours of the instrumentation. This training can be performed by use of adequate simulators and postulated scenarios for the MCR, the emergency control room and a remote observation room or similar location.

6. TECHNOLOGY NEEDS FOR ACCIDENT MONITORING

The objective of this section is to give a perspective of what is at stake when developing, or assessing the performance of, instrumentation systems that can be used in the long term phase of an accident, including fuel melt situations. The following will be dealt with, to various degrees:

(a) Challenges resulting from extensive fuel degradation from an instrumentation perspective (from the sensor to the output);
(b) Improved modelling for predicting plant conditions during DEC scenarios;
(c) Increase of instrumentation inventory and locations to determine the most extreme conditions (e.g. by considering the installation of additional sensors at suitable positions);
(d) Use of severe accident modelling to establish necessary parameter ranges, mission times and environmental conditions which equipment needs to withstand.

6.1. BACKGROUND

Analyses of plant behaviour during severe accidents such as TMI-2, Chernobyl or Fukushima Daiichi have shown that instrumentation system capability was an issue. In some cases, the existing instrumentation was basically adequate. Therefore, it was shown that extending the existing safety system capability was sufficient. In other cases, such as the Fukushima Daiichi accident, it was found that plant operators faced completely unanticipated situations, with multiple units being affected. In addition, some areas of the plant that were not originally considered to lead to significant challenges had degraded to a level that required significant mitigative actions. Depending upon the location of the monitoring instrumentation, mission times, parameters to be monitored and the severity of the accident, instrumentation systems may face widely different challenges.

6.2. SPECIFIC CONSIDERATIONS FOR SEVERE ACCIDENT MANAGEMENT GUIDELINE INSTRUMENTATION

Specific requirements are imposed upon the instrumentation during severe accident scenarios, which require consideration of the following:

(a) Upgrade of instrumentation systems to increase their robustness and resilience;
(b) Improved modelling and simulation tools for severe accidents incorporating new information gained from recent incidents;
(c) Development programmes to evaluate the benefits that could be gained from the application of new technologies or the creative use of existing robust technologies.

Some of these may be difficult to address, and developing a fully consistent approach is not always possible. Major challenges that may present themselves when addressing severe accidents include:

— Monitoring reactivity after any fuel relocation;
— Monitoring the coolant inventory;
— Monitoring the level of radioactivity released from the fuel and ultimately to the containment system;
— Measuring the concentration of combustible gas, in particular hydrogen;
— Monitoring the removal of decay heat from different areas of the nuclear system (nuclear steam supply system and spent fuel pool (SFP));
— Monitoring the containment integrity.

Instrumentation needed, or contemplated to be used for, severe accident management is to be defined considering the above challenges or risks, and be designed and installed to provide reasonable assurance that they will perform as intended.

6.2.1. Reactivity monitoring instrumentation

Under DEC, fuel reactivity is to be monitored. Fuel reactivity could become more difficult to evaluate if a fuel melt results in relocation of the fuel. In-core detectors provide useful indications during normal operation. However, during an accident scenario that results in extensive fuel melt, these in-core detectors may no longer provide adequate information.

In current plants, ex-core neutron monitors (wide range, intermediate range and source range) are used for normal operation and DBAs. For DEC, the following should be considered:

(a) Capability for monitoring the reactivity of relocated fuel for an extended period of time;
(b) Neutron monitoring equipment may be exposed to environmental conditions that are significantly more severe than those contemplated in the plant design basis;
(c) Neutron monitoring calibration changes resulting from DEC may lead to greater uncertainty and misinterpretation of reactor conditions.

At a minimum, there needs to be an evaluation of the range of accident conditions in which the available or contemplated instrumentation will remain operable. Further investigation is also recommended to evaluate the response of ex-core detectors when the fuel is relocated, in-vessel or ex-vessel. Such an investigation is to determine whether vessel melt-through could be detected using an ex-core detector.

If monitoring of reactivity cannot be accomplished with the available instrumentation, alternative means need to be developed for gaining reasonable assurance that a return to criticality can be detected. Indirect measurements could be considered, for example the measurement of radiation fields at key measuring points close to the fuel could help an operator to at least assess the reactivity of the fuel and the relocation of the fuel, as appropriate. In this respect, evaluation of radiological mapping (i.e. maps of radiation field) as a function of an accident scenario could be a useful tool.

The contemporary method to determine the concentration of fission products (e.g. caesium, iodine or xenon) is analysis of the isotopes present. The composition of the containment atmosphere, in particular its content of radioactive aerosols, iodine and noble gases, yields an indication about the condition of the fuel after DEC. When indirect methods are used, the applicability of such methods under accident conditions needs to be evaluated as a function of the accident scenario.

Evaluations of the fuel during DEC also need to take into account scenarios involving reactivity within the SFP.

6.2.2. Decay heat removal verification

Verification of decay heat removal from the fuel is important. Where accident progression cannot be stopped before significant fuel melt has occurred, assessing adequate heat removal becomes an issue. The difficulty increases further when the fuel begins to melt and relocate to other zones of the reactor, or, in the worst case, outside the reactor vessel. In addition, the removal of decay heat from the SFP may become a challenge, as learned from the Fukushima Daiichi accident.

6.2.2.1. Heat removal from the core

Evaluating heat removal capability when the core is covered can be achieved by measuring the thermodynamic conditions of the coolant. This requires measurement of the coolant level, temperature and pressure in the RPV. Several methods can be used for the measurement of temperature and pressure, but the correct assessment of the level in the RPV can be problematic under DEC. However, additional or alternative information may be required if the fuel is significantly melted because the above measures may not be sufficient to determine the degree of fuel cooling taking place. Other factors may require taking into account, for example the level in the reactor pit in the case of in-vessel retention strategy, sump level or core catcher temperature for the ex-vessel retention strategy. Dependable means for monitoring core cooling after the core has relocated may not have been considered for existing plants.

The measurement of the water level inside the RPV is a challenging task, due to the harsh conditions, including high radiation doses. Prior to the accident at TMI-2 in March 1979, the total mass inventory of the coolant inside the RPV was determined by the water level inside the pressurizer.

During the accident at TMI-2, the levels inside the pressurizer and the RPV were decoupled after saturation conditions were reached inside the RPV and steam voids penetrated the reactor coolant system (RCS). The recognition of this effect prompted the development of new systems and instrumentation for the measurement of the water level within the RPV. At that time, differential pressure instruments and heated junction thermocouples were recognized to have shortcomings, but were used because practical considerations ruled out other alternatives. Alternative RPV water level measurement methods need to be revisited.

6.2.2.2. Status and location of the core

Currently, there is no indication from which the status and location of the core may be determined. During DEC, one or more of the following states might exist:

(a) The core might be intact;
(b) The core might have experienced cladding failure or fuel melt, but still retains a coolable geometry;
(c) The core might no longer be coolable, but is still in place;
(d) The core might be relocating to the bottom of the vessel;
(e) A significant amount of fuel might have relocated within the vessel and remains molten;
(f) A significant amount of fuel might have relocated within the vessel and has solidified;
(g) A significant amount of fuel might have relocated to the containment and is still molten, but is not producing significant core–concrete interactions;
(h) A significant amount of fuel might have relocated to the containment and is still molten, and is producing significant core–concrete interactions;
(i) A significant amount of fuel might have relocated to the containment and has solidified;

(j) A significant amount of fuel might have relocated outside of the containment and is still molten;
(k) A significant amount of fuel might have relocated outside of the containment and has solidified.

Monitoring technologies would be useful to provide operators and accident managers with this information so that they can optimize mitigative accident management strategies (i.e. by applying the right strategies during each stage of the accident progression).

Knowledge that these states are imminent and exist is useful. An example of detecting imminent core damage may be monitoring for the presence of iodine to determine whether a gap release has occurred while the core is still coolable. This information would help operators decide when termination of the drywell spray is appropriate.

6.2.2.3. Spent fuel pool instrumentation

The Fukushima Daiichi accident provided evidence that reliable indication of the water level and temperature in SFPs is needed for monitoring and mitigating complex plant situations. These will determine whether or not an adequate heat removal capability is being maintained in the SFP.

Some existing pools rely upon minimal instrumentation or utilize visual devices only. Many others use instrumentation that is not designed to operate after exposure to internal or external hazards such as seismic events or structural collapse.

The requirements for SFP instrumentation are the same as those for all other instrumentation systems. The system needs to withstand environmental conditions to which they are expected to be exposed, and it also needs to provide an indication that can be relied upon for accident management purposes. Protection is to be provided against the effects of the hazards (e.g. mechanical, thermal loading and irradiation).

Examples of currently available technologies are:

(a) Bubblers: These require an air compressor to operate. The capability of the compressor during accident scenarios needs to be maintained.
(b) Differential pressure sensors: These require the installation of a nozzle in the SFP and an impulse line that could be a cause of SFP leakage. Specific installation requirements are necessary to minimize the risk of leakage.
(c) Heated thermocouples: These consist of two thermocouples, a heater for each thermocouple and a protection tube made out of stainless steel. The instrument follows the same principles as that used in the RPV water level application. Because two thermocouples are required to determine water level, the loss of a thermocouple will result in the loss of level measurement. Specific installation requirements are necessary to minimize the risk of mechanical damage.
(d) Radar systems: Two types are currently available:
    (i) Through-air radars: The emitted radar signal is transmitted through a hollow tube ending with a horn at the water surface level. The run time of the signal from the emitter to the receiver unit is used to derive the SFP water level.
    (ii) Guided wave radar: The radar signal is run through a metal guide tube or wire that is submerged in the pool water. The run time of the signal is used to derive the SFP water level.

    Both systems use a low frequency C-band radar that can penetrate foam and strong agitation and is thus particularly suitable for severe environmental conditions. Specific installation requirements are necessary to ensure the protection of the emitter and the receiver electronics from radiation exposure and from mechanical or seismic loads.
(e) Magnetic float switches: These slide in a guide tube and open or close reed contacts installed in series in the sensor unit attached to the floater tube. Specific installation requirements are necessary to minimize the risk of mechanical damage.
(f) Video cameras: The use of radioactivity resistant video cameras to view the SFP may be useful for providing a visual indication of pool level and fuel condition. The depth of the field of view may be impaired by steam in the SFP.

If cooling of the pool fails for an extended period of time, high temperatures may occur. The result of high temperatures may be the loss of inventory. The loss of inventory may be because of boil-off or the occurrence of mechanical problems (e.g. high stresses in concrete structures subjected to large temperature differentials or high stresses in the pool liner causing leaks at the welds).

Pool temperature is to be measured. Direct temperature measurement within the SFP is preferred to measurement in the cooling loop to avoid the loss of information in the event of the loss of the SFP cooling system. Direct temperature measurement also gives an indication of the accessibility of the SFP area.

6.2.3. Containment integrity monitoring

Monitoring containment integrity is an integral part of accident management. Containment pressure alone may not be sufficient for assessing containment integrity. The availability of a containment vessel level measurement (as opposed to a level switch located high in the containment) may help to detect degraded integrity in the lower regions of the containment, but may not detect leakage in the upper regions. Consequently, the need for other forms of monitoring is to be evaluated based upon the knowledge of the containment weak points and ultimate strength. The analysis of the containment needs to include the recirculation lines.

Instrumentation for containment water level may use the same technology that was outlined in Section 6.2.2.3. It may be practical to locate the instrumentation outside the containment.

Further improvements in technologies may be required to monitor parameters suitable for determining containment integrity, such as:

— Measuring hydrogen concentration for diagnosis of the structural integrity;
— Analysis of gaseous fission products inside the containment.

An alternative to direct measurement of combustible gas concentration would be to measure the temperature of the recombiner plates. This measurement provides a status of the recombination activity and uses very robust sensors (thermocouples) that ensure good reliability. Because this is a sampling technique, it also requires aids to be correctly interpreted to evaluate the risk of detonation and to determine which recombiners are to be instrumented.

6.2.4. Improved modelling of severe accidents

An accident simulation model is to be used to model the progression. These models need to support the determination of instrument range requirements (including margins), instrument mission times, environmental conditions (including uncertainties) and operator training.

There are a number of severe accident modelling methods. All suffer from limitations in modelling techniques, uncertainties in the representation of the phenomena and limited experimental data to support validation. Continued improvement of severe accident modelling techniques is needed so that these analyses can better inform the design of accident monitoring instrumentation.

6.2.5. Wireless instrumentation

The use of wireless instrumentation may also be considered for accident monitoring, but technical issues (e.g. failure of communications, corruption of data and security of transmitted data) need to be taken into account. Methods similar to those used by military communication systems may be required to satisfy security requirements.

6.2.6. Robots

Robots equipped with radiation resistant monitoring instrumentation, including video cameras, may be useful to allow for the investigation of potentially contaminated areas. Various models of robots are available, mainly for military purposes. These robots may be suitable for accident monitoring with some modifications.

7. SUMMARY AND CONCLUSIONS

The Fukushima Daiichi accident highlighted the importance of accident monitoring instrumentation during the progression of accident scenarios at a nuclear power plant. Existing strategies for accident monitoring, which were developed before the Fukushima Daiichi accident, need to be re-evaluated. Generally, existing accident monitoring systems were designed for DBAs but not for DEC. When designing accident monitoring instrumentation at new nuclear power plants or when performing enhancements of existing nuclear power plants, lessons learned need to be taken into account. The accident management strategies should consider the importance of monitoring the SFP in addition to the reactor.

Accident management strategies have been developed in many Member States on the basis of an understanding of accident behaviour as well as of plant capabilities to deal with accidents. The objectives of the strategies are specified in EOPs and SAMGs, and are related to the basic safety functions (e.g. to protect the fuel integrity by maintaining subcriticality and restoring cooling, protect the integrity of the RCS, protect the containment integrity and minimize radioactive releases). A critical step in developing accident management strategies is the establishment of monitoring criteria, which use identifiable parameters, for decision making. Accident monitoring systems then need to provide information about these parameters to enable the operators to implement accident management strategies.

Selection of designated instruments for accident monitoring is based on those that are deemed necessary to provide the parameters required to accomplish the goals of the EOPs and SAMGs. The selection of designated instruments is not to preclude the use of other available instruments.

Designated instruments need to be capable of performing their functions in the environment required and for the time frame required. An appropriate monitoring system composed of robust and suitable instrumentation powered by independent and reliable power supplies is required for this purpose. The variables are to be displayed in a clear and reliable manner that allows the operators and TSC staff to efficiently accomplish the goals of the EOPs and SAMGs.

When designing new, or upgrades to existing, accident monitoring systems, considerations need to include installation requirements that address the adverse effects of severe accidents on accident monitoring instrumentation such as the presence of combustible gases and the potential degradation of reactor coolant and containment atmospheric sampling capabilities.

Further technology development is desirable to improve accident monitoring in certain areas. These include improved methods for monitoring subcriticality and core cooling over the long term, development of systems for monitoring water inventory and temperature in SFPs, means to recognize the level of damage sustained by the fuel and its location, improved containment integrity monitoring and improvements in severe accident modelling for the purpose of determining the required accident monitoring instrument performance and environmental compatibilities.

The integration of a monitoring system suitable for both DBAs and DEC into a comprehensive accident management strategy needs to be considered at nuclear power plants and to be based upon lessons learned.

Appendix

INDEPENDENCE OF ACCIDENT MONITORING FUNCTIONS

A.1. INTRODUCTION

Accident monitoring systems support levels 3, 4 and 5 of the defence in depth concept as described in SSR-2/1 [1], Paragraphs 2.12–2.14. Requirement 7 of SSR-2/1 [1] states: "The levels of defence in depth shall be independent as far as is practicable." The Appendix discusses how the design and qualification criteria given for designated accident monitoring instruments in Sections 4.3 and 4.4 achieve independence between the accident monitoring equipment that supports the different defence in depth levels.

A.1.1. Definition of independence

Functions are independent if the equipment necessary to perform a function is unaffected by:

— Operation or failure of other equipment;
— Occurrence of effects resulting from the postulated initiating event for which it is required to function.

Note that complete segregation between different levels of defence in depth is not needed to provide independence. It is sufficient that provisions are made to confine faults and to protect equipment such that sufficient equipment is available to perform the required function in the presence of a fault and the conditions resulting from the postulated initiating events.

A.2. INDEPENDENCE FROM COMPONENT OPERATION OR FAILURE

A.2.1. Instrument channels

Many of the variables used for monitoring safety functions under DBA conditions may be used for plant control, plant protection and DEC management. The same instrument channels can be used to support all four functions under the conditions described in Section 4.3.2.

For DBAs, it is reasonable to assume that failures will be limited to one channel of measurement. Thus, compliance with the single failure criterion is sufficient to ensure that safety function monitoring under DBA conditions will be independent of failure of equipment in the protection and control functions. Under the criteria in Section 4.3.2, the necessary information needs to remain available after all instrument failures that cause, or are caused by, the DBA plus a single failure of an additional component. If failure of a channel that is used for control can cause the DBA, this channel needs to be assumed failed concurrent with a single random failure. In such a case, the accident monitoring is to be at least a three channel system, and many designs provide four channels.

The possibility of very severe environmental conditions and long operating durations makes it difficult to satisfy all points of the single failure criterion for severe accident monitoring functions. The provision of redundancy will mitigate this to some extent (see Section 4.3.3).

The possibility cannot be discounted that severe accident conditions may cause CCF of sensors or transmitters. To cope with this possibility, other available instruments are identified, and operator aids are prepared to allow continued monitoring of severe accidents, even if the designated instruments become unavailable. With such provisions, channels may be shared between defence in depth levels 1–4.

Under severe accident conditions, signal processing electronics may present an unnecessary power drain, limit the range of instrument readout (as occurred with thermocouple readings at both TMI-2 and Fukushima Daiichi) and impede diagnosis of instrumentation problems. Consequently, provisions need to be made in the control room for a simple display of instrument readings and for access to sensor or transmitter outputs. This further reduces the influence of signal processing on the availability of information for monitoring severe accidents.

During DBAs, the status of safety systems can be inferred from the information about safety functions. Therefore, failure of a single sensor will not affect the ability to monitor safety systems. Consequently, independence from other functions is not necessary.

Radiological monitoring points are generally part of networks of sensors that use different instrument channels than those used for the other accident monitoring functions. Therefore, independence between levels of defence in depth is not an issue. There may be a small number of shared sensors for monitoring specific release points. These may be shared with other accident monitoring, control or protection functions. The loss of individual data points is not usually critical to deciding emergency response.

A.2.2. Display and analysis

At least one set of displays for EOP instrumentation needs to meet all reliability and qualification requirements that are applied to the instrument channels; thus, redundant displays will be needed. This does not preclude presentation of the information on another single display or in another location. It is also encouraged to provide this information for use by electronic operator aids such as a safety parameter display system. The displays may be qualified computer driven displays or simple qualified displays (e.g. meters). A set of displays that meets the single failure criterion is sufficient to ensure the availability to monitor EOP variables even if the displays are also used to allow operators to perform control and protective functions. If qualified displays receive inputs from equipment of lower safety class, electrical isolation and physical separation need to be provided as necessary to ensure that failures in the lower class systems will not prevent the display of information needed for EOPs.

It is to be assumed that computer based displays may fail under severe accident conditions. Therefore, simple qualified displays (e.g. meters) of severe accident monitoring channels need to be available to support independence of these functions from the monitoring of EOP variables. Electronic operator aids can be very helpful, but unless the electronic aids for EOP instrumentation are designed to the same criteria as the accident monitoring channels, it is not to be assumed that the electronic aids will be available. When the availability of electronic operator aids cannot be ensured, operator aids that do not depend upon power (e.g. paper based aids) are to be available.

When signals for EOP or SAMG instruments are sent outside of the accident monitoring channels, they need to be electrically isolated and physically separated such that failure or operation of the common displays do not affect the accident monitoring system displays.

A.2.3. Power

The power supplies for EOP instrumentation may be shared with power supplies for control functions, protection functions and severe accident monitoring functions. Since the power supply for monitoring EOP variables will need to meet the single failure criterion, sufficient provisions need to exist to ensure that failure of a channel will not affect other channels, as discussed in Section A.2.1.

It is to be assumed that plant power supplies for accident monitoring instruments may fail under severe accident conditions and that some time will be needed to repair or to replace consumable items. Consequently, to achieve independence from other defence in depth levels, severe accident monitoring functions are to be designed with the capability to be powered independently from the plant power system and from instrument channels that are not needed for monitoring severe accidents. If SAMG instruments need power, there are to be provisions to power them from alternative power sources, as discussed in Section 4.3.7. Examples of such sources include batteries installed in the instruments, standby batteries, standby battery inverter sets and portable alternating current generators. If the alternative power sources are not located near the instrument loop supplies, they are to be protected from the consequences of severe accidents and natural phenomena, and need to be either connected to the instrumentation in a similarly protected way or can be easily moved to the location of the instrumentation. Means to replenish consumables needed for operation of the alternative power supplies need to be readily available in sufficient quantity to allow continued operation of severe accident monitoring until a time when restoration of normal power or replenishment of consumable stores can be assured. Consumables might include, for example, electric charges, fuel, filters and lubricants.

Instruments for radiological monitoring under DEC may be powered in the same way as instruments for monitoring under DBAs. If this power fails, measurements may continue to be made using portable instruments or inferred from the readings of the network of field instruments, which are usually powered from other sources.

A.2.4. Support features

Support features need to meet the same criteria as the highest level instrument function that they are required to support. In this case, the independence provisions for support features are the same as for the accident monitoring instruments.

It should be considered that support systems may fail under severe accident conditions and that they may be difficult to access for repair or for the replenishment of consumable items that they depend upon. Consequently, to maintain independence of SAMG instruments from other functions, the SAMG instruments are, as far as practicable, not to depend upon support features.

Where support features are needed for severe accident instruments, they should ideally be able to operate independently from plant utilities (e.g. water, compressed air and electrical power). Means to replenish consumables needed for operation of the support systems need to be readily available in sufficient quantities to allow continued operation of severe accident monitoring until a time when restoration of normal power or replenishment of consumable stores can be assured.

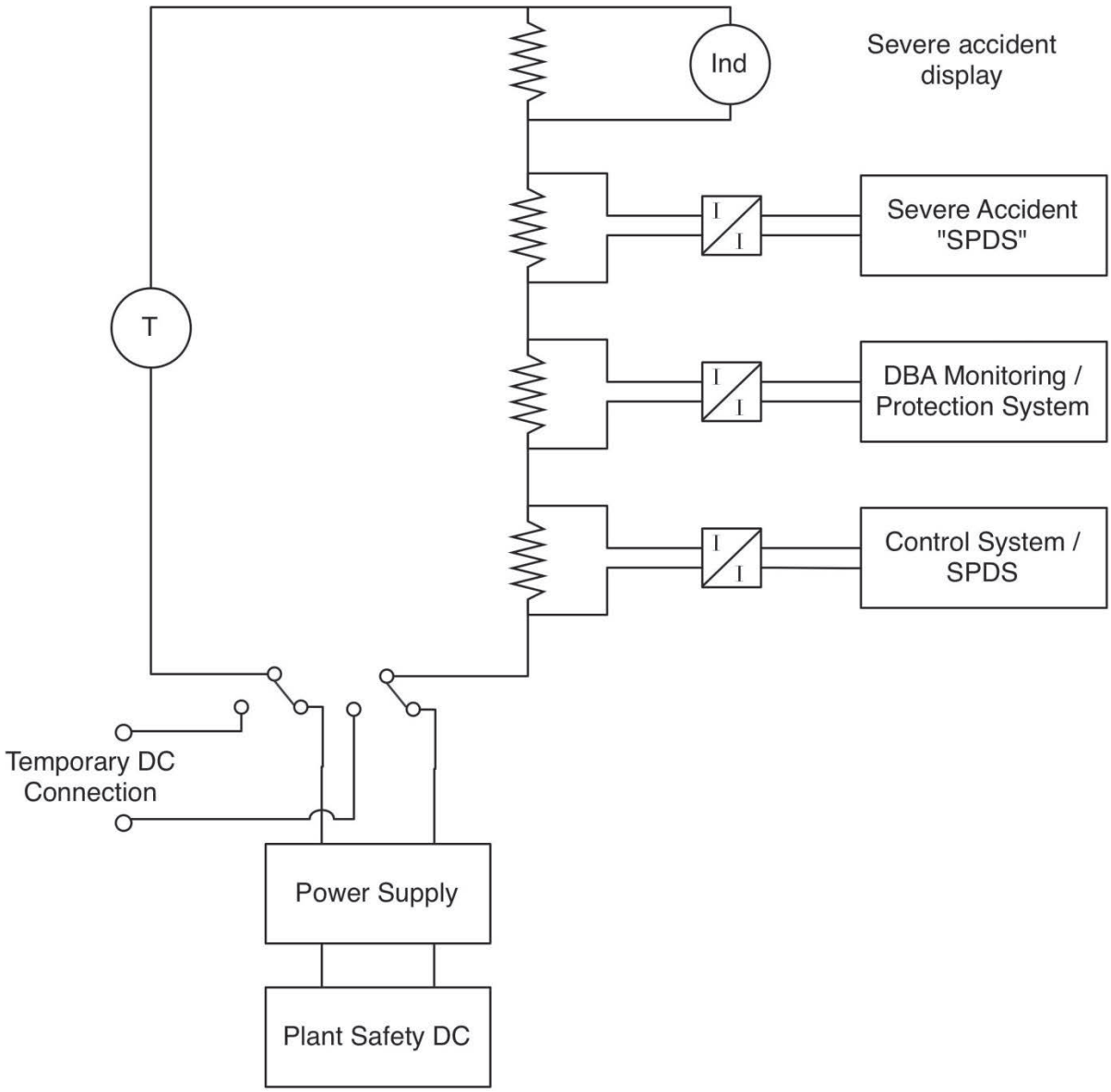
A.2.5. Isolation

If the same instrument channel is used to support functions at different levels of defence in depth, the functions is to be electrically isolated from each other. Figure 1 gives an example of such a system.

A.3. INTERNAL AND EXTERNAL HAZARDS

Ideally, monitoring functions supporting EOP or SAMG implementation should continue to be available following the exposure to hazards that may cause, or result from, the events to which they respond. This is usually accomplished by a combination of protection of equipment from the hazards, physical separation and electrical isolation of redundant equipment so that the necessary functionality remains available even if some channels are damaged and qualification to ensure the equipment withstands the hazard. If these features ensure that the monitoring will remain available during the worst conditions, they will remain available in the presence of lesser hazards. Therefore, no further action is necessary to ensure independence between the different monitoring functions.

The effects of DEC may be more widespread than those of DBAs. It is therefore possible that hazards associated with DEC result in CCF of instruments that are considered independent for DBAs. This possibility needs to be considered, and preventive or mitigative measures need to be provided. These measures include, for example, provision of additional instruments that will not be exposed to common hazards, provision of diverse instruments that will not be affected by common hazards, provisions for repair of damaged instruments, alternative cable routeings or the use of other available instruments.



Note: DBA — design basis accident; DC — direct current; I/I: galvanic isolator; Ind — indicator; SPDS — safety parameter display system; T — transmitter.

FIG. 1. Example instrument channel that supports functions at defence in depth levels 1–4.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna (2009).

[3] AMERICAN NUCLEAR SOCIETY, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors, ANS Standard 4.5-1980, ANS, La Grange Park, IL (1980).

[4] NUCLEAR REGULATORY COMMISSION, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, Regulatory Guide 1.97, Rev. 2, US Govt Printing Office, Washington, DC (1983).

[5] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, IEEE Standard 497-2010, IEEE, Piscataway, NJ (2010).

[6] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions, Standard 61226, IEC, Geneva (2009).

[7] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Control Rooms – Design, Standard 60964, IEC, Geneva (2011).

[8] KERNTECHNISCHER AUSSCHUSS, Accident Measuring Systems, Safety Standard 3502 (11/2012), KTA, Salzgitter (2012).

[9] ELECTRIC POWER RESEARCH INSTITUTE, Instrument Performance under Severe Accident Conditions: Ways to Acquire Information from Instrumentation Affected by an Accident, TR-102371, EPRI, Palo Alto, CA (1993).

[10] ELECTRIC POWER RESEARCH INSTITUTE, Assessment of Existing Plant Instrumentation for Severe Accident Management, TR-103412, EPRI, Palo Alto, CA (1993).

[11] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-R-2, IAEA, Vienna (2002).

[12] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, Arrangements for Preparedness for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GS-G-2.1, IAEA, Vienna (2007).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).

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

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Emergency Power Systems for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.8, IAEA, Vienna (2004).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Engineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage, IAEA Nuclear Security Series No. 4, IAEA, Vienna (2007).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Preventive and Protective Measures against Insider Threats, IAEA Nuclear Security Series No. 8, IAEA, Vienna (2008).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

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

[20] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.5, IAEA, Vienna (2003).

[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.6, IAEA, Vienna (2003).

[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.7, IAEA, Vienna (2004).

[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Internal Hazards other than Fires and Explosions in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-1.11, IAEA, Vienna (2004).

[24] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS, IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations, IEEE Standard 323-2003, IEEE, Piscataway, NJ (2003).

[25] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Electrical Equipment of the Safety System — Qualification, Standard 60780, IEC, Geneva (1998).
[26] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Nuclear Power Plants – Instrumentation and Control Systems Important to Safety – Requirements for Electromagnetic Compatibility Testing, Standard 62003, IEC, Geneva (2009).
[27] INTERNATIONAL ELECTROTECHNICAL COMMISSION, Recommended Practices for Seismic Qualification of Electrical Equipment of the Safety System for Nuclear Generating Stations, Standard 60980, IEC, Geneva (1989).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. NS-R-3, IAEA, Vienna (2003).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-3.1, IAEA, Vienna (2002).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, WORLD METEOROLOGICAL ORGANIZATION, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSG-18, IAEA, Vienna (2011).

Annex I

SUMMARY OF LESSONS LEARNED IN JAPAN FROM SEVERE ACCIDENTS: R&D PROGRAMME FOR SA-KEISOU IN JAPAN

I–1. BACKGROUND

Instrumentation systems in a nuclear power plant are very important for monitoring plant conditions for safe operation and shutdown. The severe accident at the Fukushima Daiichi nuclear power plant in March 2011 caused several severe situations such as failure of the plant power supply for many monitoring instruments, core damage and hydrogen explosion, among other things. Many of the functions of the instrumentation systems were lost. Monitoring the plant's conditions then became harder to perform.

In the event that an accident similar to the one at the Fukushima Daiichi nuclear power plant were to occur in the future, measurements of the important variables, such as reactor water level or reactor pressure, are to be ensured. The development of SA-Keisou[1] is needed to monitor these important variables, which contribute to preventing the escalation of an event into a severe accident, mitigating the consequences of a severe accident, achieving a safe state for the plant and confirming that the plant continues to be in a safe state over the long term.

I–2. OBJECTIVE

Through the R&D programme, the specific requirements for SA-Keisou will be prepared. If a severe accident were to occur in the future, SA-Keisou could contribute to the suppression of the accident by measuring the important variables (e.g. water level and pressure), thus enabling plant operators to take appropriate preventive or mitigative actions at the right times during the accident progression to mitigate public exposure to released radionuclides. SA-Keisou focuses on the development of severe accident monitoring systems. This programme can also enhance technical levels in the nuclear industry in Japan and can promote safety and utilization of nuclear power plants. Applications of the post-accident monitoring systems corresponding to the Three Mile Island Unit 2 (TMI-2) accident and design basis accidents (DBA), among other things, have already been studied in Japan.

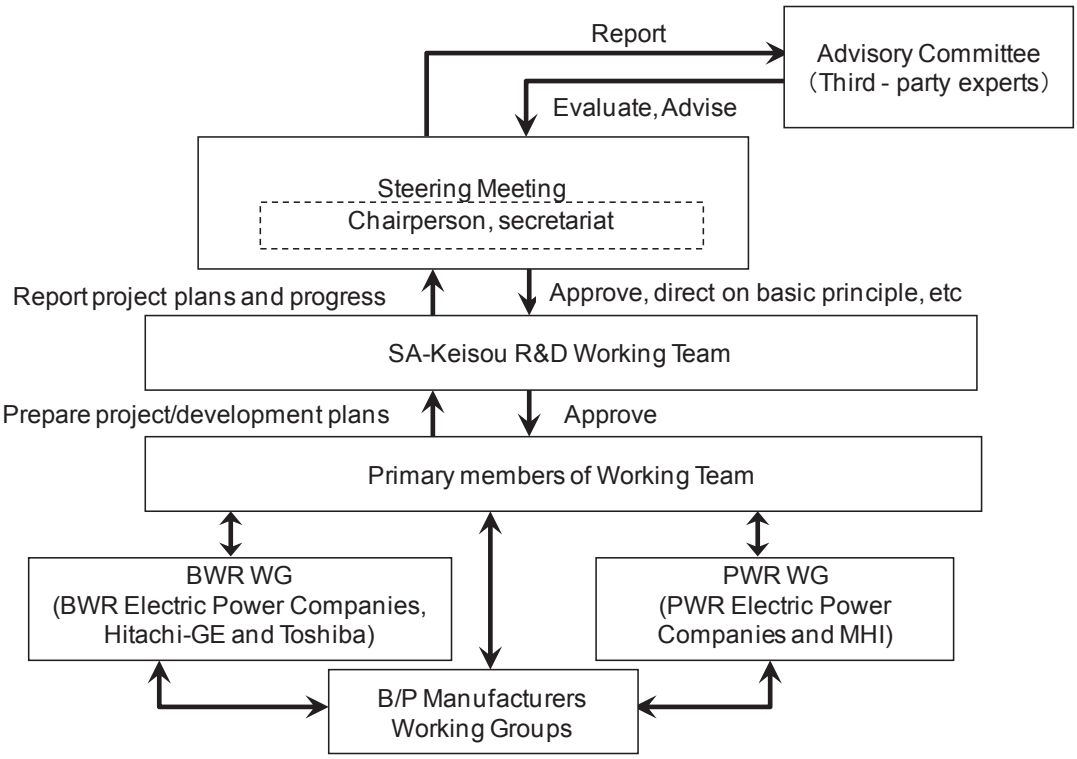
I–3. ESTABLISHING ORGANIZATION OF SA-KEISOU R&D

The general outline of an organization of SA-Keisou R&D is shown in Fig. I–1. This R&D is carried out as a subsidy project programme by the Ministry of Economy, Trade and Industry, a ministry of the Government of Japan. It is necessary that the Government, electric power companies, plant manufacturers and third party experts work together to develop SA-Keisou.

I–4. RESEARCH AND DEVELOPMENT PLAN

An outline of the R&D programme is shown in Fig. I–2.

[1] In English, SA-Keisou means severe accident — instrumentation and monitoring systems.



Note: B/P — balance of the plant; BWR — boiling water reactor; MHI — Mitsubishi Heavy Industries; PWR — pressurized water reactor; WG — working group.

FIG. I–1. Organization of SA-Keisou R&D.

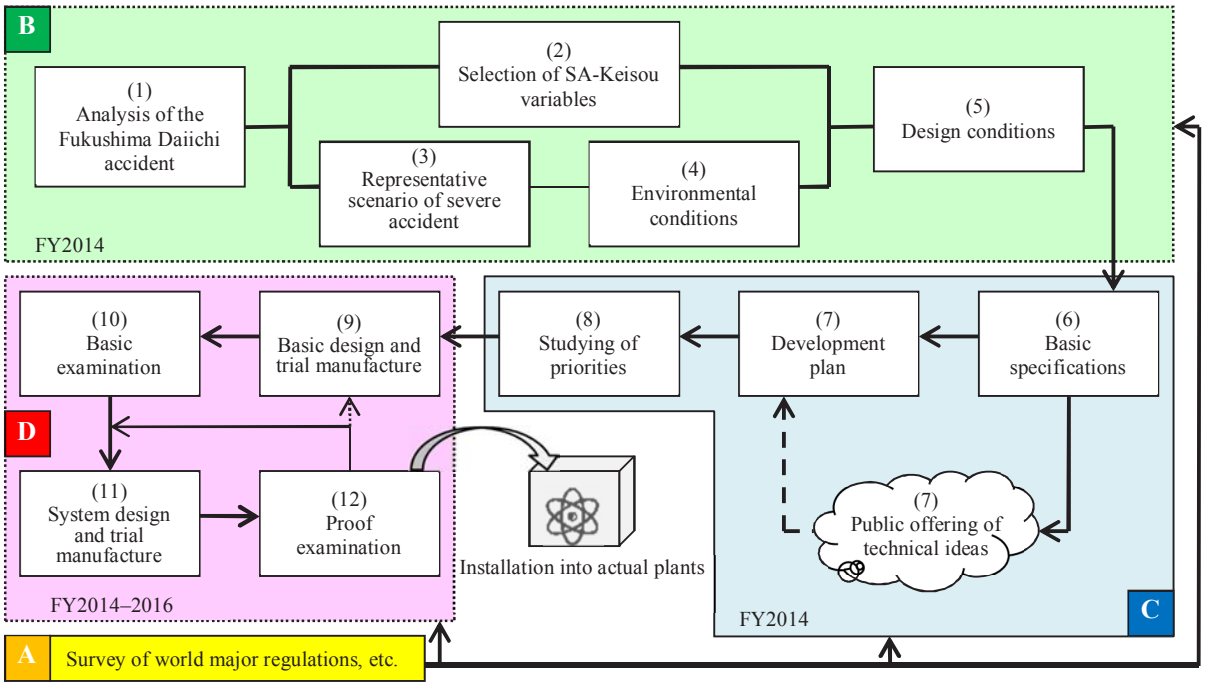


FIG. I–2. Outline of the R&D programme.

I–5. SELECTION OF MEASUREMENT VARIABLES FOR SA-KEISOU

I–5.1. Selection process for candidate measurement variables

The purpose of SA-Keisou is to develop the instrumentation systems required to provide plant operators with the information they need to mitigate the progression of a severe accident. However, the selection of variables to be measured is not determined unambiguously, but rather through an evaluation process. Therefore, SA-Keisou variables are selected in two steps. In the first step, potential SA-Keisou variables deemed to be potentially effective are tentatively identified as 'candidate' variables. In the second step, the final SA-Keisou variables are chosen from the candidate variables using the selection method outlined in Section I–5.3. Any remaining unselected candidate variables may be implemented in the future through the development of new technology. The selection process of SA-Keisou variables and the concepts are shown below and in Fig. I–3.

I–5.1.1. Listing of SA-Keisou candidate variables

The candidate variables are first listed for selection as the SA-Keisou variables. The candidates are identified from an analysis of the current accident management guidelines (AMGs), a survey of world major codes, regulations and standards, and an analysis of the Fukushima Daiichi accident.

I–5.1.2. Selection and classification of SA-Keisou variables

The 'final' measurement variables chosen (SA-Keisou variables) are then selected from the candidate variables. To be chosen, two points of view are considered. The first is whether the identified measurement variables are able to support achievement of the mitigation strategy for a severe accident or not. The second is whether the measurement variables have the potential to measure with appropriate accuracy and response time. In addition, the plant conditions resulting from the accident progression are identified and classified to assist with establishing instrumentation system design criteria. The SA-Keisou variables selected with the measurement purpose that is appropriate to the plant condition are classified by importance (i.e. main variables, alternatives and supporting variables).

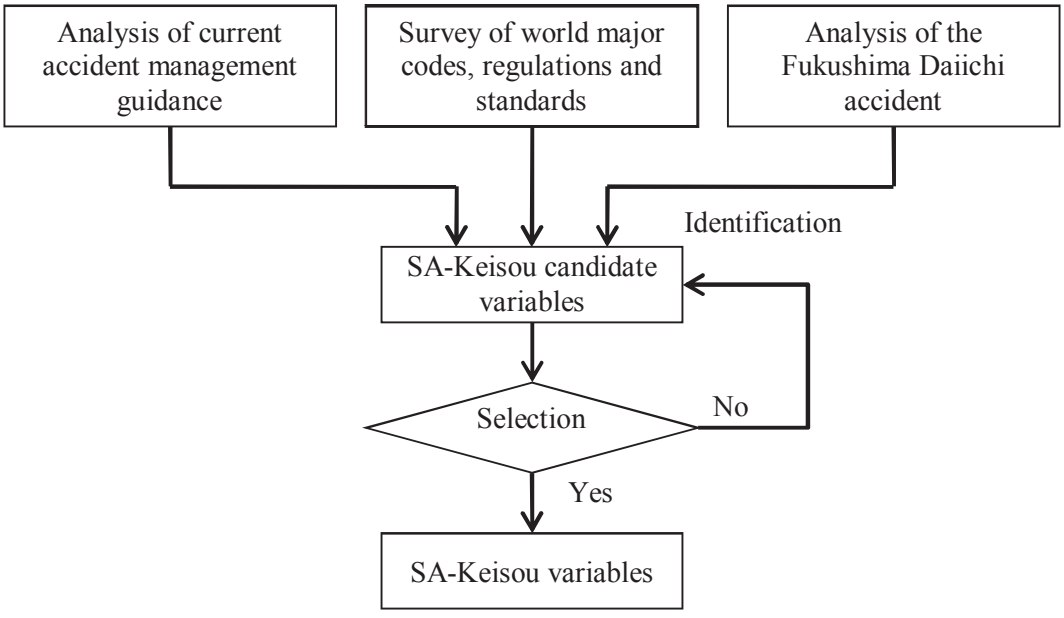
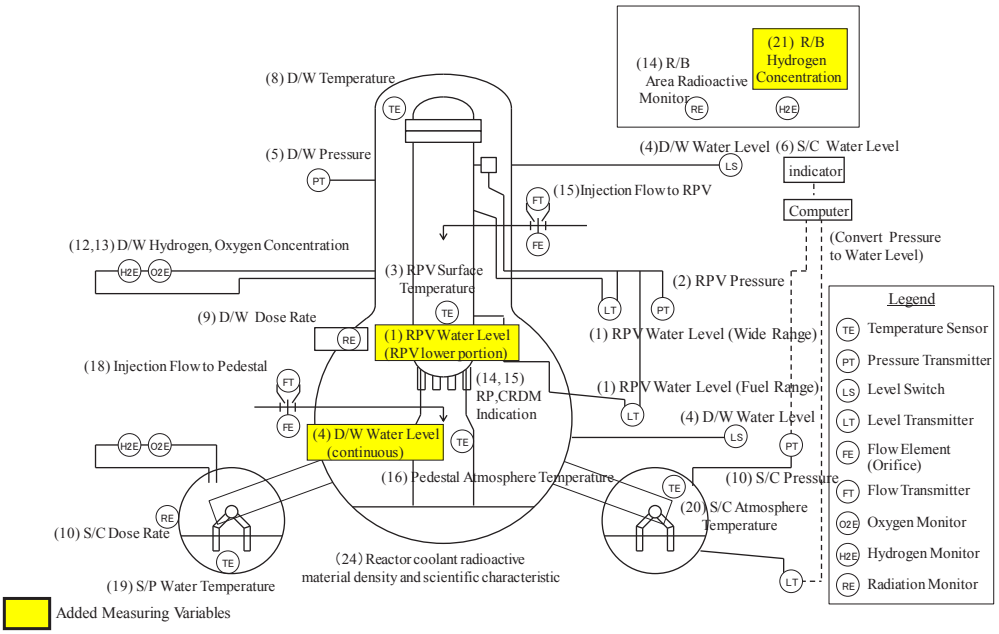


FIG. I–3. Selection process of SA-Keisou variables.

I–5.2. Identification of SA-Keisou candidate variables

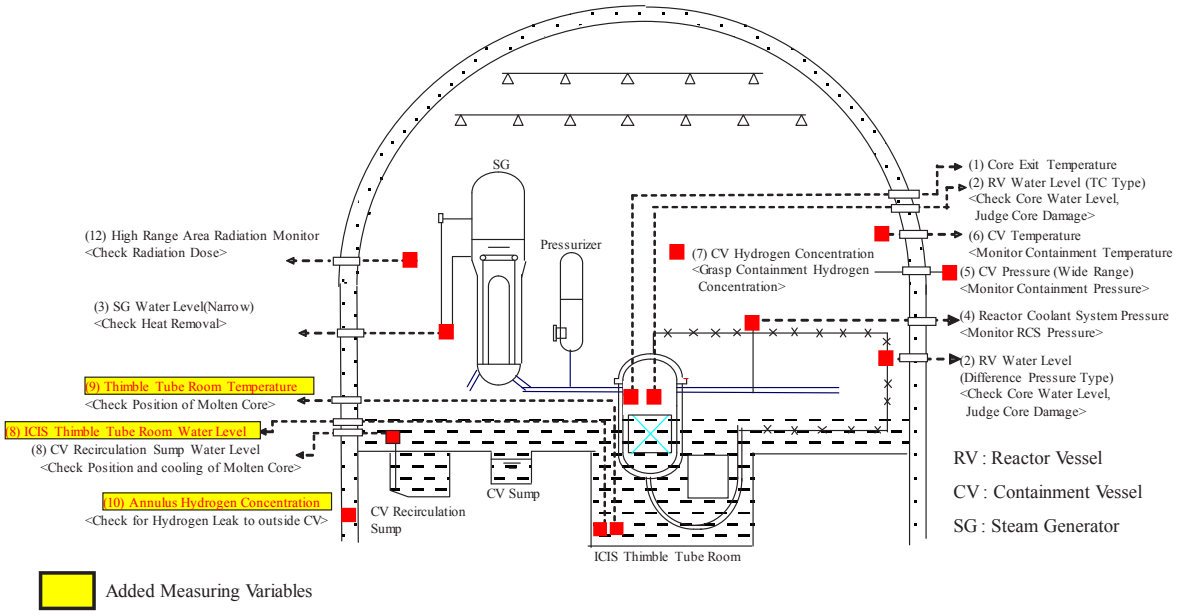
I–5.2.1. Results of the identification of SA-Keisou candidate variables

The identification of SA-Keisou candidate variables is accomplished based on analysis of the current AMG, world major codes, regulations and standards, and an analysis of the Fukushima Daiichi accident, as shown in Figs I–4 and I–5.



Note: CRDM — control rod drive mechanism; D/W — drywell; R/B — reactor building; RP — rod position; RPV — reactor pressure vessel; S/C — suppression chamber; S/P — suppression pool.

FIG. I–4. Example of SA-Keisou candidate variables for BWRs.



Note: ICIS — in-core instrumentation system; RCS — reactor coolant system; TC — thermocouple.

FIG. I–5. Example of SA-Keisou candidate variables for PWRs.

Tables I–1 and I–2 show the SA-Keisou candidate variables for boiling water reactor (BWR) and pressurized water reactor (PWR) plants, respectively.

TABLE I–1. SA-KEISOU CANDIDATE VARIABLES FOR BWRs

No.	Variables	Selection reason	Remarks (for measurement purposes)
1	RPV water level	A, C	Confirm core cooling conditions, etc.
2	RPV pressure	A, C	Confirm operation of injection to core, etc.
3	RPV surface temperature	A, C	Confirm integrity of reactor pressure boundary (RPV), etc.
4	D/W water level	A, B, C	Confirm operation of PCV vent, etc.
5	D/W pressure	A, B, C	Confirm operation of PCV vent, etc.
6	S/C water level	A, C	Confirm operation of PCV vent, etc.
7	S/C pressure	A, B, C	Confirm operation of PCV vent, etc.
8	D/W temperature	A, B, C	Confirm operation of PCV spray, etc.
9	D/W dose rate	A, B, C	Confirm fuel boundary damage and meltdown, etc.
10	S/C dose rate	A, B, C	Confirm fuel boundary damage and meltdown, etc.
11	D/W, S/C hydrogen concentration	A, B, C	Confirm hydrogen initiation and concentration within PCV, etc.
12	D/W, S/C oxygen concentration	A, B, C	Confirm hydrogen initiation and concentration within PCV, etc.
13	D/W, S/C water vapour concentration	D	Confirm hydrogen initiation and concentration within PCV, etc.
14	R/B area radiation monitor	A, C	Confirm emission of fission products from PCV, etc.
15	Injection flow to RPV	A, C	Confirm core cooling conditions, etc.
16	Pedestal atmosphere temperature	A, C	Confirm damage of reactor pressure boundary (RPV), etc.
17	Number of signal losses of RPV instruments and equipment	A, C	Confirm integrity of reactor pressure boundary (RPV)
18	Injection flow to pedestal	A, C	Confirm cooling of core debris, etc.
19	Suppression pool water temperature	A, B, C	Confirm operation of PCV spray, etc.
20	S/C atmosphere temperature	A, B, C	Confirm operation of PCV spray, etc.
21	R/B hydrogen concentration	C	Confirm integrity of PCV
22	R/B oxygen concentration	D	Confirm operation of flammable gas control system

TABLE I–1. SA-KEISOU CANDIDATE VARIABLES FOR BWRs (cont.)

No.	Variables	Selection reason	Remarks (for measurement purposes)
23	R/B water vapour concentration	D	Confirm operation of flammable gas control system
24	Reactor coolant radioactive material density and scientific characteristics	B, C	Confirm fuel boundary damage and meltdown
25	Radioactive material density inside PCV	D	Confirm fuel boundary damage and meltdown
26	Water source tank level	A	Confirm operation of PCV spray, etc.
27	Safety relief valve exhaust pipe temperature	A	Confirm operation of depressurizing of RPV
28	Core temperature	B, D	None
29	Neutron flux	B	None

Note: A — variable identified based on accident management guidelines; B — variable identified based on overseas reactor plant knowledge; C — variable identified based on analysis of the Fukushima Daiichi accident; D — variable identified based on other reasons; D/W — drywell; PCV — primary containment vessel; R/B — reactor building; RPV — reactor pressure vessel; RV — reactor vessel; S/C — suppression chamber.

TABLE I–2. SA-KEISOU CANDIDATE VARIABLES FOR PWRs

No.	Variables	Selection reason	Remarks (for measurement purposes)
1	Core exit temperature	A	Confirm core damage, etc.
2	RV water level	A	Confirm condition of core cooling, etc.
3	SG water level (narrow range)	A	Confirm submergence condition of SG tube, etc.
4	Reactor coolant pressure/RCS pressure	A	Confirm operation of depressurizing of primary system
5	Containment pressure/CV pressure (wide range)	A	Confirm CV damage, etc.
6	Containment temperature/CV temperature	A	Confirm CV damage, etc.
7	Containment hydrogen concentration/CV hydrogen concentration	B	Confirm hydrogen initiation and combustion in CV, etc.
8-1	Reactor cavity water level/ICIS thimble tube room water level	B	Confirm cooling condition of core debris, etc.
8-2	Containment recirculation sump water level/CV recirculation sump water level	A	Confirm operation of injection to containment
9	Reactor cavity temperature/ICIS thimble tube room temperature	B	Confirm core debris fall to lower RV, etc.
10	Annulus hydrogen concentration	C	Confirm CV damage, hydrogen initiation and concentration within CV, etc.

TABLE I–2. SA-KEISOU CANDIDATE VARIABLES FOR PWRs (cont.)

No.	Variables	Selection reason	Remarks (for measurement purposes)
11	Monitoring post	A	Confirm emission of FP from CV, etc.
12	High range area radiation monitor	A	Confirm core damage, etc.
13	Exhaust high range gas monitor	A	Confirm emission of FP from CV, etc.
14	Main steam line radiation monitor	A	Confirm SG heat transfer pipe damage, etc.
15	Refuel water storage tank water level	A	Confirm operation of injection to primary system, operation of injection to CV, etc.
16	Neutron flux	A	Confirm CV damage, core debris fall to lower RV, etc.
17	CCW surge tank pressure (wide range)	A	Natural convection cooling inside CV
18	CCW flow	A	Natural convection cooling inside CV
19	Fire service water accumulated flow/integrated flow	A	Confirm cooling of core debris, etc.
20	Injection flow	C	Confirm core cooling condition, cooling of core debris, etc.
21	Auxiliary feedwater flow	C	Confirm SG heat transfer pipe damage, etc.
22	Reactor coolant radioactive material density and scientific characteristics	B, C	Confirm core damage, etc.

Note: A — variable identified based on accident management guidelines; B — variable identified based on overseas reactor plant knowledge; C — variable identified based on analysis of the Fukushima Daiichi accident; CCW — component cooling water; CV — containment vessel; FP — fission products; ICIS — in-core instrumentation system; RCS — reactor coolant system; RV — reactor vessel; SG — steam generator.

I–5.2.2. Identification of SA-Keisou candidate variables based on world major codes, regulations and standards for BWRs

(a) Subjects of evaluation

The BWR SA-Keisou candidate variables identified from world standards and guidance are listed in Table I–1 based on a survey of Refs [I–1 to I–4].

(b) Survey results

The need for measurement of core subcriticality and other ‘new’ variables was found to be a condition which needed to be monitored at the severe accident. The design considerations for such measurements were then identified. The direct or indirect variables which satisfy the design considerations were listed as the SA-Keisou candidate variables.

I–5.2.3. Identification of SA-Keisou candidate variables based on world major codes, regulations and standards for PWRs

The PWR SA-Keisou candidate variables based on selected standards for PWRs are shown in Tables I–3 and I–4.

TABLE I–3. SA-KEISOU CANDIDATE VARIABLES BASED ON 10 CFR 50 FOR PWRs

	10 CFR 50	Current measures of Japanese plants
10 CFR 50.34(f)(2)(xvii)	"Provide instrumentation to measure, record and readout in the control room: (A) containment pressure, (B) containment water level, (C) containment hydrogen concentration, (D) containment radiation intensity (high level), and (E) noble gas effluents at all potential, accident release points. Provide for continuous sampling of radioactive iodines and particulates in gaseous effluents from all potential accident release points, and for onsite capability to analyze and measure these samples."	Measured as the following variables: (a) Containment pressure; (b) Recirculation sump water level; (c) Post-accident hydrogen monitor[a] (local indication); (d) Containment high range area monitor; (e) Each monitor.
10 CFR 50.34(f)(2)(xviii)	Provide instruments in the control room: — Primary coolant saturation meter; — Coolant level in the reactor vessel.	The variables shown in the left column can be monitored in the MCR.
10 CFR 50.34(f)(2)(xix)	"Provide instrumentation adequate for monitoring plant conditions following an accident that includes core damage."	Post-accident monitoring instrumentation is utilized even after the core damage. Wide range pressure instruments can withstand pressure up to the containment limit pressure.
10 CFR 50.44(b)(4)(ii)	"Equipment must be provided for monitoring hydrogen in the containment. Equipment for monitoring hydrogen must be functional, reliable, and capable of continuously measuring the concentration of hydrogen in the containment atmosphere following a significant beyond design-basis accident for accident management, including emergency planning."	Hydrogen concentration is measured with PASS. Continuous measurement in beyond design basis condition is not assured.
	Result	
Containment hydrogen concentration monitoring in the MCR needs to be further discussed.		

Source: See Ref. [I–2].
Note: MCR — main control room; PASS — post-accident sampling system.
[a] Hydrogen concentration in the containment cannot be monitored in the MCR.

TABLE I–4. SA-KEISOU CANDIDATE VARIABLES BASED ON FINNISH YVL 1.0 (PWRs)

	Finnish YVL 1.0	Current measures of Japanese plants
Section 3.6 Monitoring and control	"Monitoring equipment shall be designed for the nuclear power plant to manage and monitor the progress of severe accidents and to give data about (1) the possible re-criticality of the reactor or its debris (2) the threat of a reactor pressure vessel melt-through (3) the location of the reactor debris (4) other factors possibly endangering containment integrity. "The measurement systems designed for accident monitoring and management shall maintain operability even in the event of a single failure. "The measurement systems shall be capable of measuring accurately enough over the entire range within which the measured parameters vary during operational conditions or accidents. As far as possible, the measurements shall be so planned that the operators will easily see if the measurement fails or the measurement range is exceeded."	(1) Detection of re-criticality at SA is not considered; (2) RV failure can be detected with the RCS pressure; (3) Not applicable. (4) "Other factors possibly endangering containment integrity" can be monitored with the containment pressure and temperature. Redundancy has not been provided for the instrumentation systems established as measures for accident management. Backup variables are specified for each main monitoring variable.
	Result	
	Detection of re-criticality, monitoring of molten core position, and redundancy need to be further discussed. In the Finish Stress Test Report, re-criticality is detected with intermediate range neutron flux before RV failure and with rate of increase in containment pressure after RV failure. For molten core position monitoring, addition of ICIS thimble tube room temperature instrumentation system may be utilized.	

Source: See Ref. [I–3].
Note: ICIS — in-core instrumentation system; RCS — reactor coolant system; RV — reactor vessel; SA — severe accident.

I–5.2.4. Analysis of the Fukushima Daiichi accident and its results

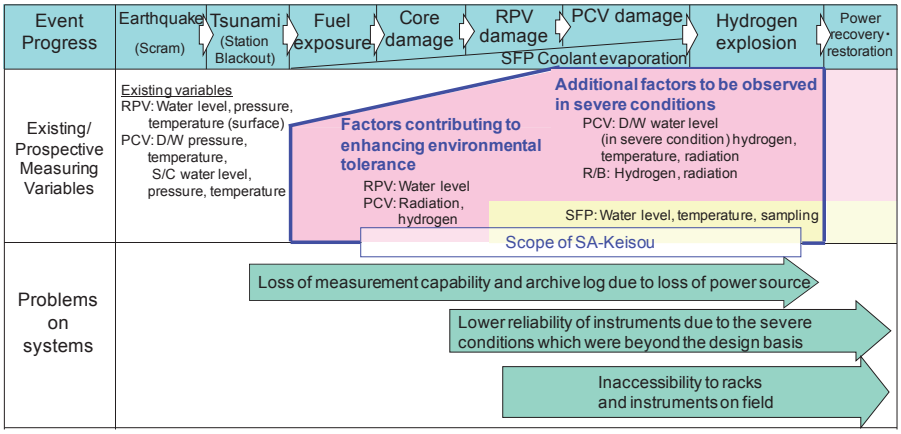
(a) Identification of SA-Keisou candidate variables based on analysis of the Fukushima Daiichi accident sequence

Through an analysis of the Fukushima Daiichi accident, a set of new measurement variables has been identified that has the potential to support severe accident mitigation strategies. Furthermore, an analysis of the accident provides information that enables better identification of the environmental conditions that can result from a severe accident, which can be used to strengthen the environmental resistance of accident monitoring instrumentation.

The sequence of the accident and the existing and prospective variables to be monitored are shown in Fig. I–6.

(b) Summary of SA-Keisou candidate variables for BWRs resulting from the Fukushima Daiichi accident analysis

A summary of the variables identified from the accident and a listing of SA-Keisou candidate variables for BWRs are shown in Table I–5. The main measurement variables resulting from Fukushima Daiichi accident analysis are shown in Fig. I–7.



Note: D/W — drywell; PCV — primary containment vessel; R/B — reactor building; RPV — reactor pressure vessel; S/C — suppression chamber; SFP — spent fuel pool.

FIG. I–6. Sequence of the Fukushima Daiichi accident and existing and prospective variables to monitor.

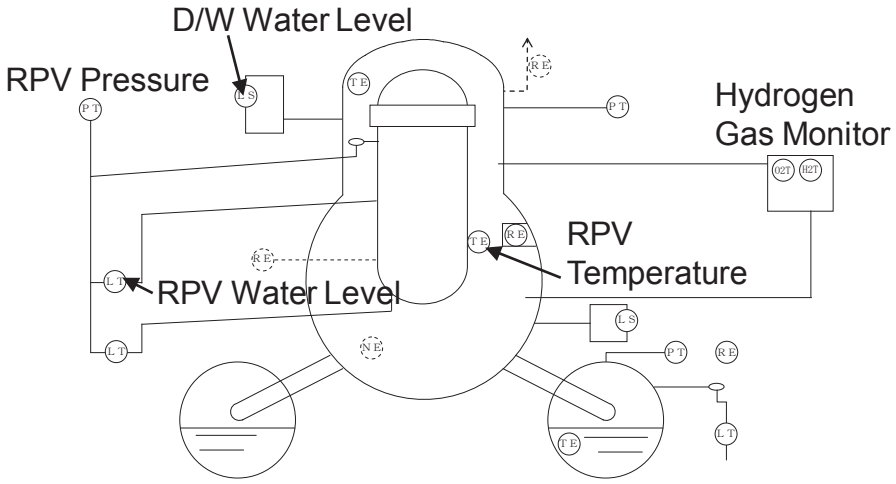
TABLE I–5. SUMMARY OF SA-KEISOU CANDIDATE MEASUREMENT VARIABLES RESULTING FROM ANALYSIS OF THE FUKUSHIMA DAIICHI ACCIDENT FOR BWR PLANTS

Main variables	Summary of the accident	Problems and items to consider in SA-Keisou
RPV water level	PCV temperature elevation due to RPV boundary failure → instrumentation reference leg water level decreased Before calibration (at plant water filling), the indication on the display was higher than the actual level After calibration (at plant water filling), the indicated water level was lower than the lower limit of the measurement range Although measurement of the water level at the lower portion of the RPV was desired, the instrumentation system did not exist	A method for recovery of reference leg water level at SA Instrumentation diversity to avoid CCF Necessity of instrumentation for the lower portion of the RPV water level
D/W water level	Although measurement of the D/W water level was desired, the instrumentation system did not exist (only a float type level switch was installed)	Installation of instrumentation for D/W water level (continuous)
R/B hydrogen concentration (gas monitor)	A large amount of hydrogen was generated in the RPV during the accident due to the water–zirconium reaction The generated hydrogen which was released to the PCV during depressurization of the RPV escaped to the R/B as the PCV pressure elevated, and it accumulated in the upper portion of the R/B, resulting in a hydrogen explosion A hydrogen gas monitor had not been installed because measurement of hydrogen concentration in the R/B was not assumed to be necessary	R/B was not equipped with any instrumentation system for hydrogen concentration analysis, and the probability of hydrogen explosion had not been predicted → necessity of installation of instrumentation for hydrogen gas monitoring
RPV water sampling analysis (radionuclide analysis, pH, etc.)	This system was intended to check the degree of fuel damage The system was not operable owing to the loss of the emergency power supply and the related losses of functions of the utilities, such as the cooling water system and the instrumentation air system, which are necessary for system operation	Isolation valve open/close was inoperable Measurement was not possible after fuel damage (water level too low) No water at the nozzle (jet pump flow) Cooling water feeding system at SA Sampling method without pump and re-examination of the layout plan

TABLE I–5. SUMMARY OF SA-KEISOU CANDIDATE MEASUREMENT VARIABLES RESULTING FROM ANALYSIS OF THE FUKUSHIMA DAIICHI ACCIDENT FOR BWR PLANTS (cont.)

Main variables	Summary of the accident	Problems and items to consider in SA-Keisou
SFP instrumentation (water level, temperature)	Instrumentation systems for water level and temperature were necessary to monitor stability of the SFP cooling system Each system had only one measurement point; measurement in the direction of the depth was not included in the measurement range	Since the existing level instrumentation was a float type level switch, water level measurement during the level decrease was not possible à necessity of installation of instrumentation for wide ranges of water levels Since the temperature instrumentation was installed to detect only the upper portion of the pool water, measuring the pool water temperature during the water decrease was not possible a necessity of installation of instrumentation to monitor water temperature
SFP water sampling analysis (radionuclide analysis, pH, etc.)	Pool water was expected to be analysed to detect for fuel damage caused by hydrogen explosion in the building, lack of cooling water or corrosion owing to seawater injection (except for Unit 1) The existing sampling system could not be utilized because of the difficulty in entering the area of the system, owing to the high level of radiation	Necessity to lay out the rack outside the secondary containment

Note: CCF — common cause failure; D/W — drywell; PCV — primary containment vessel; R/B — reactor building; RPV — reactor pressure vessel; SA — severe accident; SFP — spent fuel pool.



Note: D/W — drywell; RPV — reactor pressure vessel.

FIG. I–7. Main measurement variables for a BWR identified from analysis of the Fukushima Daiichi nuclear power plant.

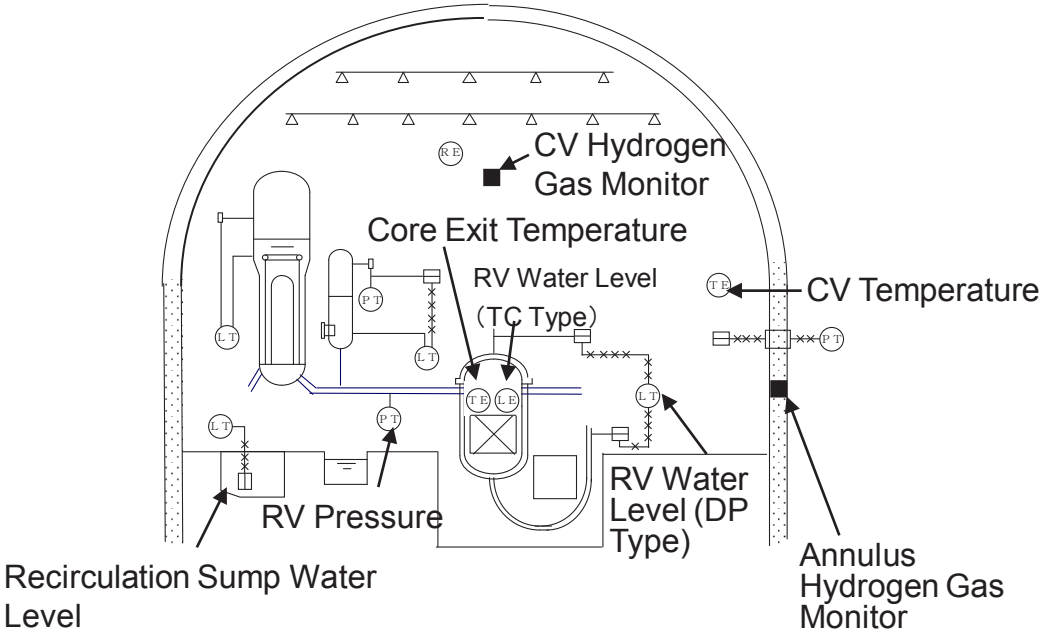
(c) Summary of the Fukushima Daiichi accident and listing of SA-Keisou candidate variables for PWRs resulting from the accident analysis

A summary of the variables identified from the Fukushima Daiichi accident and a listing of SA-Keisou candidate variables for PWRs are shown in Table I–6. The main measurement variables resulting from the accident analysis are shown in Fig. I–8.

TABLE I–6. SUMMARY OF SA-KEISOU CANDIDATE MEASUREMENT VARIABLES RESULTING FROM ANALYSIS OF THE FUKUSHIMA DAIICHI ACCIDENT FOR PWR PLANTS

BWR measurement variables	PWR measurement variables/methods	Analysis results/items to consider in PWR based on lessons learned
RPV water level	Differential pressure type RV water level (thermocouple type in some plants)	By installing seal sensors, hermetically seal the reference water to prevent the fill water in capillary tubes from evaporating Possibly substitute core exit temperature instruments to check core damage
D/W water level	Recirculation sump water level	Continuous indication Evaluation of environmental effects
D/W hydrogen gas monitor	CV hydrogen gas monitor (analysis by sampling measurement)	Additional installation of a hydrogen gas monitor which can measure hydrogen concentration directly inside the CV
R/B hydrogen gas monitor	Not present for the annulus	Additional installation of annulus hydrogen gas monitor

Note: BWR — boiling water reactor; CV — containment vessel; D/W — drywell; PWR — pressurized water reactor; R/B — reactor building; RPV — reactor pressure vessel; RV — reactor vessel.



Note: CV — containment vessel; DP — differential pressure; RV — reactor vessel; TC — thermocouple.

FIG. I–8. Main measurement variables for a PWR resulting from analysis of the Fukushima Daiichi nuclear power plant.

I–5.3. Final selection and classification of variables for SA-Keisou

In this section, a description is provided as to how the final selection of measurement variables was developed from the candidate variables. To establish an appropriate set of design requirements, the candidate variables for SA-Keisou were considered in the following order. First, a set of specific plant states appropriate to various stages of accident progression was defined. Second, the environmental conditions (typical scenarios of severe accidents) appropriate to each stage were identified. Finally, the variables for SA-Keisou were selected and classified.

I–5.3.1. Definition of plant states

In the AMG, the initiating event of the accident is not identified. The emergency operating procedures have been structured to enable the plant operators to respond to the plant symptoms that can lead to damage of the core, reactor pressure vessel (RPV) and reactor containment vessel (CV). A similar process is then applied to emergency procedures applicable to unidentified accident events. In the future, it is expected that severe accident management guidelines will be formulated based on the same organizational guidelines. For this reason, a set of plant states corresponding to the various stages of accident progression was identified and classified to enable a coherent evaluation of equipment performance in light of its ability to survive the applicable conditions. This classification of severe accident plant states is called severe accident classification. When the plant states were classified, the concept of defence in depth within the IAEA standards was adopted [I–5].

(a) Classification of severe accident plant states (severe accident classification)

The AMG provides guidance for implementing management strategies for the prevention and mitigation of damage to the RPV and subsequent damage to the reactor CV. In the AMG, the proposed accident management strategy is described as early water injection after core damage, which could lead to damage of the RPV and subsequent damage to the reactor CV. Furthermore, because the reactor CV was damaged during the Fukushima Daiichi accident, the analysis study focused on the maintenance of the soundness of the reactor core state, and the maintenance of the integrity of the RPV state and reactor CV state. A set of severe accident plant states is defined as follows:

(i) SA1: The reactor core is damaged, but the core fuel remains inside the RPV (RV).
(ii) SA2: An RPV (RV) failure has occurred, and the core fuel is outside the RPV (RV).
(iii) SA3a: A PCV (CV) failure has occurred (assuming the success of the accident management action and the success of water injection within 24 h after the scram).
(iv) SA3b: A PCV (CV) failure has occurred (assuming the failure of the accident management action and the failure of the ability to inject water within 24 h after the scram, but after that water injection is successful).

The various plant states that exist after damage of an RPV (SA3) were divided into two stages from the point of view of the defence in depth. One was SA3a, including accidents of the type that occurred at the Fukushima Daiichi nuclear power plant, and the other was SA3b, corresponding to various events which are considered to be beyond SA3a. Plant substates SA3a and SA3b were distinguished in terms of whether the accident management strategy was successful or not. To support this analysis, these plant substates were classified in terms of whether water injection 24 h after the scram was successful or not.

Note that this study is intended for the identification of accident monitoring instrumentation design criteria required for support of mitigation of the accident progression, and not for long term accident management strategies following the experiences of SA1, SA2, SA3a or SA3b plant states. For example, even if the temperature of the PCV (CV) may be low enough to re-enable equipment operability, entrance to the PCV (CV) to replace inoperable equipment is still restricted, owing to the high radiation environment.

(b) Correspondence with the defence in depth concept of IAEA standards

From the viewpoint of the concept of defence in depth, IAEA defence in depth level 4 corresponds to the state in which the equipment is intended for an event that is beyond design basis accidents (DBAs), but does not damage the PCV (CV), preventing a major release of radioactive materials (i.e. SA1 or SA2). In addition, IAEA defence in depth level 5 corresponds to the state where the PCV (CV) is damaged and a major release of radioactive materials occurs (i.e. SA3a or SA3b).

(c) Correspondence with specific severe accident events

An evaluation of the classification of plant states in this annex and an evaluation based on the sequence of specific severe accident events are different. The AMG provides guidance for operation procedures corresponding to the state of the plant, including consideration of the IAEA defence in depth levels 4 and 5 in an indefinite event.

There is an urgent need to implement novel instrumentation systems as soon as possible which are able to handle an accident event that is not anticipated. However, it will take a great deal of time to evaluate each accident event that has not been considered previously, but there is a demand to increase the margin of safety as soon as possible. Therefore, a correspondence of beyond DBA conditions is required with a certain defence in depth level coverage in each of the post-DBA substates.

With the above considerations, 'a low probability but big impact accident', such as an interface system loss of coolant accident (LOCA), was classified into SA3b (i.e. PCV (CV) damage and AMG mitigating strategy failure). A procedure addressing accident convergence has not been established yet, but the instrumentation system for monitoring such an accident sequence needs to be designed to accomplish its function at each of the above described severe accident conditions that occur in each successive accident progression state. The definitions of severe accident classification states are shown in Table I–7.

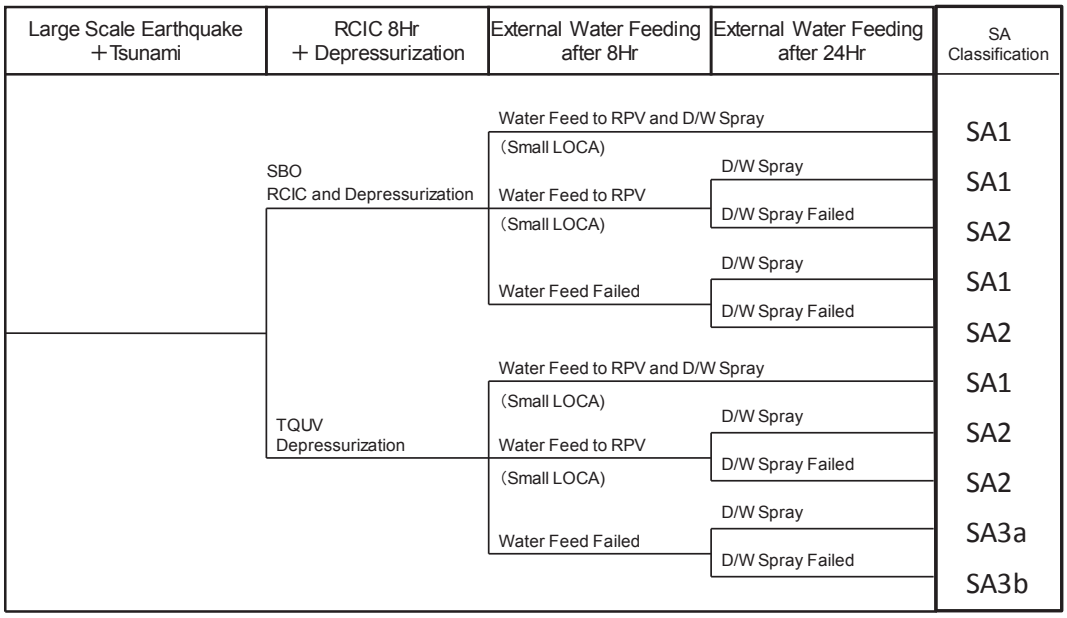
TABLE I–7. DEFINITIONS OF SEVERE ACCIDENT CLASSIFICATION STATES

SA classification state	SA1	SA2	SA3a	SA3b
Fuel condition/fuel position	Meltdown/within RPV (RV)	Debris/RPV (RV) or PCV (CV)	Debris/RPV (RV) or PCV (CV)	Debris/RPV (RV) or PCV (CV)
Core condition	Damaged	Damaged	Damaged	Damaged
RPV (RV) condition	Sound	Damaged	Damaged	Damaged
PCV (CV) condition	Sound	Sound	Damaged	Damaged
Water injection	Success	Success	Success	Failure
IAEA defence in depth level	Level 4	Level 4	Level 5	Level 5
SA regulation defence in depth level	4-1		4-2	5

Note: CV — containment vessel; PCV — primary containment vessel; RPV — reactor pressure vessel; RV — reactor vessel; SA — severe accident.

I–5.3.2. Determination of environmental conditions: Representative scenario during a severe accident

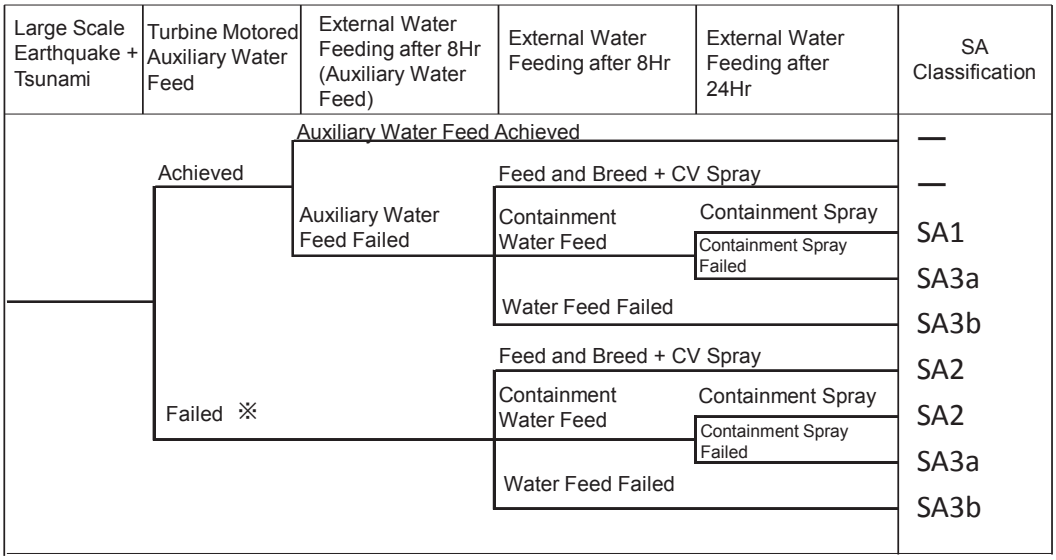
The representative severe accident scenario is evaluated to determine the environmental conditions applicable to SA-Keisou. The environmental conditions are determined for each of the severe accident classifications (SA1, SA2, SA3a and SA3b) based on the representative severe accident scenario. Representative scenario and severe accident classification examples are shown in Figs I–9 and I–10.



TQUV: anticipated transient combined with failure of HPCI, RCIC, and LPECCS

Note: D/W — drywell; HPCI — high pressure coolant injection; LOCA — loss of coolant accident; LPECCS — low pressure emergency core cooling systems; RCIC — reactor core isolation cooling; RPV — reactor pressure vessel; SA — severe accident; SBO — station blackout.

FIG. I–9. Representative scenario and severe accident classification examples for a BWR plant.



※Turbine driven auxiliary water feed failure leads to Core Damage and RV Damage in few hours. Mitigation of accident progression by auxiliary water feed cannot be expected.

Note: CV — containment vessel; RV — reactor vessel; SA — severe accident.

FIG. I–10. Representative scenario and severe accident classification examples for a PWR plant.

I–5.3.3. Selection of final SA-Keisou variables

To select the final set of measurement variables for SA-Keisou, the following criteria were used for confirming plant state and equipment operation:

(a) Variables that enable the accomplishment of accident management strategies to prevent RPV (RV) damage;
(b) Variables that enable the accomplishment of accident management strategies to prevent PCV (CV) damage;
(c) Variables that enable the accomplishment of accident management strategies to suppress off-site radioactive releases when the RPV (RV) or PCV (CV) are damaged.

The measurement variables required for confirming plant state and equipment operation are then selected. The following concerns are considered for this selection process:

— Selection of variables enabling the accomplishment of the specific measurement purpose for each stage of the severe accident;
— Selection of variables that enable such measurements with the required accuracy and response time.

The selection of the measurement variables will be implemented according to an updated AMG which will be prepared based on the evaluation of the Fukushima Daiichi nuclear power plant. The final variable selection is to be revised after the renewed AMG is issued. If other measurement variables are candidates in this development, their needs are to be considered according to the same selection approach.

I–5.3.4. Classification of SA-Keisou variables

For severe accident monitoring instrumentation, variables are required to provide information to the plant operator to assess plant conditions and to permit manual actions. The measurement variables for the instrumentation system for severe accident are classified as follows:

(a) Variables that enable confirmation of the plant condition:
  (i) Main variables: These variables are required for measurement purposes such as monitoring and operation. The main variables are shown with the symbol '◎'. In the case that measurement is carried out using multiple variables, a group of these variables is defined as a main variable. These variables are shown with the symbol '★'.
  (ii) Alternative variables: These variables are substitutes for the main variables and carry out the same measurement purposes. These variables are shown with the symbol '●'.
  (iii) Supporting variables: These variables are required for providing supplemental information for measurement purposes. These variables are shown with the symbol '○'.
(b) Variables that enable appropriate equipment operation:
  (i) Variables required for initiating operation and confirming successful operation: These variables are used to judge the initiation of equipment operation and confirm successful operation. These variables are shown with the symbol '▲'.
  (ii) Variables required for confirming successful operation: These variables are not used to assess the initiation of the equipment operation, but are used to confirm the success of the operation. These variables are shown with the symbol '△'.
(c) Variables available for comprehending the plant condition: These variables are shown with the symbol '◇'.

I–5.3.5. Results of selection and classification of SA-Keisou variables

The SA-Keisou classification matrices for BWR and PWR plants are shown in Tables I–8 and I–9, respectively. These tables show the variables for severe accident classification depending on plant conditions, including environmental conditions and measurement purposes such as monitoring accident progress and confirming proper system operation. The variables are assigned to each measurement purpose such as monitoring

TABLE I–8. SA-KEISOU CLASSIFICATION MATRIX FOR BWRs

(SA classification) Plant condition	(SA1) Core damage→Meltdown/RPV integrity is maintained/PCV integrity is maintained	(SA2) Meltdown/RPV is damaged/PCV integrity is maintained	(SA3a) Meltdown/RPV is damaged/PCV is damaged	(SA3b) Meltdown/RPV is damaged/PCV is damaged
Environmental condition in PCV: ・Maximum temperature ・Pressure ・Humidity ・Radiation	・171°C ・0.31 MPa ・Steam ・5×10^6 Gy/6 months	・300°C ・1.0 MPa ・Steam ・5×10^6 Gy/6 months	・700°C ・1.0 MPa ・Steam ・5×10^6 Gy/6 months	・1000°C ・1.0 MPa ・Steam ・5×10^6 Gy/6 months
Environmental condition outside PCV: ・Maximum temperature ・Pressure ・Humidity ・Radiation	・66°C ・3.4 kPa ・100% ・3×10^5 Gy/6 months	・66°C ・0.01 MPa ・Steam ・3×10^5 Gy/6 months	・100°C ・0.01 MPa ・Steam ・2×10^6 Gy/6 months	・100°C ・0.01 MPa ・Steam ・2×10^6 Gy/6 months
Required duration of performance	Over 3 days			

Measurement purpose/performance		Monitoring					Operation confirmation						Monitoring				Operation confirmation					Monitoring					Operation confirmation						Monitoring
		Possibility of boundary damage and confirmation of event initiation	Cooling function	Containment function									Possibility of boundary damage and confirmation of event initiation	Cooling function	Containment function								Possibility of boundary damage and confirmation of event initiation	Cooling function									Cooling function
No.	Variables	Confirm fuel boundary damage and meltdown	Confirm core cooling condition	Confirm integrity of reactor pressure boundary (RPV)	Confirm integrity of PCV	Confirm hydrogen initiation and concentration within PCV	Injection to core	Depressurize RPV	Injection to pedestal	Make-up to water source tank	PCV spray	PCV vent	Confirm damage of reactor pressure boundary (RPV)	Confirm cooling of core debris	Confirm integrity of PCV	Confirm hydrogen initiation and concentration within PCV	Injection to core	Injection to pedestal	Make-up to water source tank	PCV spray	Injection to reactor well	PCV vent and filtered vent	Confirm PCV damage	Confirm emission of FP from PCV	Confirm hydrogen initiation and concentration within PCV	Confirm cooling of core debris	Injection to core	Injection to pedestal	Make-up to water source tank	PCV spray	Control combustible gas concentration within R/B	Confirm cooling of core debris outside RPV
1	RPV water level	○	◎	○		○	▲	▲	▲				○																		
2	RPV pressure		●	★			▲	▲					★																		
3	RPV surface temperature		●	○			▲	△	▲				○	○			▲									○	▲				
4	D/W water level			○(3)					▲(3)		▲	▲	○(3)	◎(3)				▲(3)		▲		▲				◎(3)		▲(3)		▲		
5	D/W pressure			★	★	○		△			▲	▲	★	○	★	○				▲		▲	★		○	○				▲		
6	S/C water level								△		▲	▲						△		▲		▲						△		▲		
7	S/C pressure				★	○		△			▲	▲			★	○				▲		▲	★		○					▲		
8	D/W temperature			★	★						▲		★	○	★					▲	▲(4)		★			○				▲		◇(2)
9	D/W dose rate	◎	○	○								▲	○									▲										
10	S/C dose rate	◎	○									▲										▲										
11	D/W, S/C hydrogen concentration	○	○	○		◎					▲	▲	○	○		◎				▲		▲			◎	○				▲		
12	R/B area radiation monitor				★										★								★	◎								
13	Injection flow to RPV(1)		○				△		▲		▲			○			△	△		△						○	△	△		△		
14	Pedestal atmosphere temperature			★	★				▲		△		★	●	★			▲		▲			★			●		▲		▲		◇(2)
15	Injection flow to pedestal(1)								△					○				△								○		△				
16	S/P water temperature							△			▲									▲										▲		
17	S/C atmosphere temperature				★						▲				★					▲			★							▲		◇(2)
18	R/B hydrogen concentration				○										○								○	○							▲	
19	Water source tank level						▲	▲	▲	▲	▲						▲	▲	▲	▲	▲						▲	▲	▲	▲		
20	SRV exhaust pipe temperature							△																								
21	No. of signal loss of RPV instruments and equipment			○									○																			

RPV: Reactor pressure vessel
D/W: Drywell
S/C: Suppression chamber
R/B: Reactor building
S/P: Suppression pool
SRV: Safety relief valve
FP: Fission products
PCV: Primary containment vessel
SA: Severe accident

◎: Main variables required for accomplishing measurement purposes
★: Variables required for accomplishing measurement purpose in combination with other variables
▲: Variables required for initiating operation and confirming success of operation
△: Variables required for confirming success of operation
●: Alternative variables for main variables
○: Supporting variables which provide supplemental information for measurement purposes
◇: Available variables for comprehending plant condition

Note: (1) Nos 13 and 15 are preferable to be measured at injection flow line in front of RPV/PCV, but if injection flow line is established, outlet flow of resource is supposed to be supplementally confirmed as a dependent variable (alternative variable); (2) Resistance (critical value) is evaluated as instrumentation systems; (3) Pedestal; (4) Drywell head atmosphere temperature. This table may change in the future.

TABLE I–9. SA-KEISOU CLASSIFICATION MATRIX FOR PWRs

(SA classification) Plant condition	(SA1) Core damage→Meltdown/RV integrity is maintained/CV integrity is maintained	(SA2) Meltdown/RV is damaged/CV integrity is maintained	(SA3a) Meltdown/RV is damaged/CV is damaged	(SA3b) Meltdown/RV is damaged/CV is damaged
Environmental condition in CV: ・Maximum temperature ・Pressure ・Humidity ・Radiation	・190°C ・0.414 MPa ・100% ・Under existing PAM condition	Same as SA3a condition	・200°C ・1.6 MPa ・100% ・2MGy/year (annular space is under 5MGy/year)	・300°C ・Atmosphere pressure ・100% ・2MGy/year (annular space is under 5MGy/year)
Environmental condition outside CV: ・Maximum temperature ・Pressure ・Humidity ・Radiation	・Atmosphere temperature ・Atmosphere pressure ・– ・–	Same as SA3a condition	・Depending on location ・Atmosphere pressure ・– ・Depending on location	・Depending on location ・Atmosphere pressure ・– ・Depending on location
Required duration of performance	Over 80 hours			

Measurement purpose/performance	Monitoring: Possibility of boundary damage and confirmation of event initiation	Monitoring: Cooling function		Monitoring: Containment function				Operation confirmation						Monitoring: Possibility of boundary damage and confirmation of event initiation	Monitoring: Cooling function			Operation confirmation								Monitoring: Possibility of boundary damage and confirmation of event initiation	Monitoring: Cooling function			Operation confirmation	Monitoring: Possibility of boundary damage and confirmation of event initiation	Monitoring: Cooling function		
No. Variables	Confirm core damage	Confirm condition of core cooling	Confirm submergence condition of SG tube	Confirm integrity of RV	Confirm integrity of CV	Confirm hydrogen initiation and combustion in CV	Confirm integrity of SG tube	Depressurize primary system	Injection to primary system	Feed water to SG	Make-up to water source tank	Injection to containment	CV spray	Confirm RV damage	Cooling condition of core debris	Confirm integrity of CV	Confirm hydrogen initiation and combustion in CV	Injection to primary system (4)	Make-up to water source tank(4)	Injection to containment(4)	CV spray(4)	Natural convection cooling within CV	Filtered vent(4)	Confirm CV damage	Confirm hydrogen initiation and combustion in CV	Confirm emission of FP from containment	Cooling condition of core debris	Same as(4)	Confirm CV damage	Confirm hydrogen initiation and combustion in CV	Confirm emission of FP from containment	Confirm cooling condition of core debris	Same as (4)	Confirm CV damage	Confirm hydrogen initiation and combustion in CV	Confirm emission of FP from containment	Confirm cooling condition of core debris
1 Core exit temperature	◎	★							▲									▲																	
2 RV water level	○	●																																	
3 SG water level (narrow range)			◎				○			▲																									
4 Reactor coolant pressure/RCS pressure		★		★(1)				▲	▲					★(1)																					
5 Containment pressure/CV pressure (wide range)				★(1)	★	○		△					▲	★(1)	○	★	○				▲	▲	▲	★					◇						
6 Containment temperature/CV temperature				★	★								▲	★	○	★					▲	▲		★			○		◇			◇			
7 Containment hydrogen concentration/ CV hydrogen concentration	○	○				◎							▲		○		◎				▲	▲			◎		○			◇					
8–1 Reactor cavity water level/ ICIS Thimble Tube Room water level(2)				○								▲	▲	○	◎					▲	▲	▲	▲				◎								
8–2 Containment recirculation sump water level/ CV recirculation sump water level(2)												△																							
9 Reactor cavity temperature/ ICIS Thimble Tube Room temperature				★	★							▲	▲	★	●	★				▲	▲			★			●								
10 Annulus hydrogen concentration					○	○										○	○							○	○	○			◇	◇					
11 Monitoring post(3)					★											★								★		◎			◇		◇				
12 High range area raditation monitor	◎	○																																	
13 Exhaust high range gas monitor					★											★								★		◎									
14 Main steam line radiation monitor							◎																			○									
15 RWST water level									▲		▲	▲	▲					▲	▲	▲	▲														
16 Neutron flux				○																															
17 CCW surge tank pressure (wide range)																																			
18 CCW flow																																			
19 Fire service water accumulated flow/Integrate flow												△	△		○					△	△						○								
20 Injection flow(5)		○							△			△	△		○			△		△	△						○								
21 Auxiliary feed water flow			○							△																									

CV: Containment vessel
RWST: Refuel water storage tank
CCW: Component cooling water system
FP: Fission products
PAM: Post-accident monitoring
RV: Reactor vessel
RHR: Residual heat removal
SA: Severe accident
ICIS: In-core instrumentation system

◎: Main variables required for accomplishing measurement purposes
●: Alternative variables for main variable
★: Variables required for accomplishing measurement purpose in combination with other variables
○: Supporting variables which provide supplemental information for measurement purposes
▲: Variables required for initiating operation and confirming success of operation
△: Variables required for confirming success of operation
◇: Available variables for comprehending plant condition

Environment resistance is required in accordance with survey results of 2011

Environment resistance is required with limiting duration required for SA operation

Note: (1) Confirm containment pressure instead of reactor coolant pressure after RV damage (because reactor coolant pressure quickly becomes same pressure as containment pressure after RV damage). Therefore, environment resistance of reactor coolant is included to verify condition of PAM; (2) Reactor cavity water level overlaps with existing measurement range of recirculation sump water level. Existing recirculation sump water level measurement utilizes diaphgram seal sensor and because it is thought that it is likely to be influenced by variation of environmental condition, reactor cavity water level is measured by applying equipment such as thermocouple type; (3) Monitoring post is surveyed including that it is excluded from development object because it is located outside CV and it is possible to apply equipment such as portable type. In addition, it is not limited to monitoring post if it can measure dose rate outside CV; (4) SA2 operation is conducted on SA3a condition continuously; (5) CV spray flow, RHR flow, filling flow and high pressure injection flow (in review). This table may change in the future.

and operation confirmation in SA1, SA2, SA3a and SA3b. The number of these variables is limited so as to not cause substantial burden to the plant operators during the time they are needed.

I–6. DESIGN CRITERIA FOR SA-KEISOU

I–6.1. Required design items

The required design items of SA-Keisou are shown in Table I–10. The development of SA-Keisou is accomplished by consideration of the items in this table.

TABLE I–10. REQUIRED DESIGN ITEMS

Required design items	Main variables	Alternative variables	Supporting variables	Variables required for initiating operation and confirming success of operation	Variables required for confirming success of operation
Reliability (redundancy and diversity)	✓	✓	X	✓	X
Separation and independence	✓	X	X	✓	X
Environmental qualification	✓	✓	X	✓	X
Seismic qualification	✓	✓	X	✓	X
Power supply	✓	✓	X	✓	X
Testability	✓	✓	✓	✓	✓
Range	✓	✓	✓	✓	✓
Accuracy	✓	✓	X	✓	X
Quality assurance	✓	✓	X	✓	X
Indication and record	✓	✓	X	✓	X
Flooding protection	✓	✓	X	✓	X
Fire protection	✓	✓	X	✓	X

Note: This table may change in the future.
✓: apply.
X : do not apply.

I–6.2. Details of required design items

I–6.2.1. Reliability (redundancy and diversity)

It is important to have enough reliability and simplification for SA-Keisou. The following considerations need to be given to:

(a) Not requiring system redundancy for one measurement variable;
(b) Providing diversity in the selection of measurement variables: in principle, multiple variables are to be selected for one measurement purpose;
(c) Providing redundant measurements where doing so will not reduce plant reliability.

I–6.2.2. Independence

The defence in depth level of the main variables, which are categorized as level 4, need to be designed to have independence from level 3 variables. The definitions of levels 3 and 4 are consistent with the defence in depth level identified in IAEA Safety Standards Series No. SSR-2/1, Safety of Nuclear Power Plants: Design [I–5].

To the degree appropriate, the redundant equipment needs to be independent and separate. The main variables should ideally be designed to have an independence from the equipment of level 3. The level 3 equipment which is shared with the alternative variables needs to meet the qualifications (seismic and environmental) and power supply requirements for SA-Keisou.

I–6.2.3. Environmental qualification

SA-Keisou is to be designed to have environmental resistance, including temperature, pressure and radiation. Conditions of temperature, pressure and radiation under severe accident environments are to be set with consideration to severe accident classification and arrangement location.

I–6.2.4. Seismic qualification

The seismic qualification of class S in Japan are required. The typical facilities of class S are equipment and pipes of the reactor coolant pressure boundary.

I–6.2.5. Power supply

SA-Keisou needs to be capable of being powered by independent plant power systems.

I–6.2.6. Testability

SA-Keisou is to be designed to have periodic testing capabilities when the reactor is in operation or in shutdown.

I–6.2.7. Measurement range

SA-Keisou is to be designed to have a measurement range that is fit for purpose.

I–6.2.8. Accuracy

SA-Keisou is to be designed to have the required measurement accuracy.

I–6.2.9. Quality assurance

Quality assurance, such as design control, is to be conducted in accordance with JEAG 4121-2009 Application Guide to Quality Assurance Code for Safety in Nuclear Power Plants — Operation Phase of Nuclear Power Plants [I–6].

I–6.2.10. Indication and record

Severe accident monitoring instrumentation are be designed to provide continuous monitoring display in the main control room, and recording capability is to be provided.

I–6.2.11. Flooding protection

If internal flooding and external flooding occur, the required flooding protection is to be taken to accomplish the function of SA-Keisou.

I–6.2.12. Fire protection

SA-Keisou is to be designed so that non-combustible and fire retardant materials are used wherever practical.

I–7. SCHEDULE

The R&D schedule of SA-Keisou is shown in Table I–11.

TABLE I–11. RESEARCH AND DEVELOPMENT SCHEDULE

R&D plan contents	Fiscal year 2011	Fiscal year 2012	Fiscal year 2013	Fiscal year 2014
Defining requirements for instrumentation systems				
Selection of parameters required for severe accidents				
Setting environmental conditions, etc., for severe accidents				
Defining requirements				
Settling of primary development plan				
Public offering of technical ideas				
Setting basic specifications on instrumentation systems				
Study of development plan on instrumentation systems				
Investigation of priority of development plan				
Development of severe accident instrumentation systems				
Design and prototype production of instrumentation systems				
Basic test and analysis of instrumentation systems				
Qualification tests on instrumentation systems				
Drawing up standards and guidelines for severe accidents				
Investigation of overseas standards				
Drawing up standards and guidelines				

I–8. SUMMARY

Development of SA-Keisou is needed to monitor important variables that enable plant operators to implement accident management strategies for mitigation of severe accidents at nuclear power plants. Selection of measurement variables for SA-Keisou, including additional variables, is accomplished based on an analysis of current AMG, world major codes, regulations and standards, and the Fukushima Daiichi accident. The measurement variables for SA-Keisou have been determined.

To enable the classification of severe accident monitoring instrumentation, plant conditions after core damage are classified into the following:

(a) SA1: The reactor core is damaged, but the core fuel remains inside the RPV (RV).
(b) SA2: There is an RPV (RV) failure and the core fuel is outside the RPV (RV).
(c) SA3a: There is a PCV (CV) failure (assuming the success of the accident management action and the success of the water injection within 24 h after the scram).
(d) SA3b: There is a PCV (CV) failure (assuming the failure of the accident management action and the failure of water injection within 24 h after the scram; however, after that water injection is successful).

Variables for severe accident monitoring instrumentation are further grouped into the following.

(a) Variables that enable confirmation of the plant condition:
  (i) Main variables: These variables are required for accomplishing measurement purposes. In the case that the measurement purpose is accomplished by multiple variables, a group of these variables is defined as a main variable.
  (ii) Alternative variables: These variables are substitutes for the main variables and carry out the same measurement purposes.
  (iii) Supporting variables: These variables are required for providing supplemental information for measurement purposes.
(b) Variables that enable appropriate equipment operation:
  (i) Variables required for initiating operation and confirming success of the operation: These variables are used to judge the initiation of the equipment operation and confirm the success of the operation.
  (ii) Variables required for confirming successful operation: These variables are not used to assess the initiation of the equipment operation, but are used to confirm the success of the operation.

Independence between instrumentation supporting responses to levels 3 and 4 of the defence in depth concept should be considered.

The design criteria of severe accident monitoring instrumentation for SA1, SA2, SA3a and SA3b are shown. The variables for severe accident classification depending on plant conditions, including environmental conditions and measurement purposes such as monitoring and operation confirmation, are also shown in SA-Keisou classification matrices.

REFERENCES TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. NS-G-2.15, IAEA, Vienna (2009).
[I–2] NUCLEAR REGULATORY COMMISSION, Domestic Licensing of Production and Utilization Facilities, Code of Federal Regulations, 10 CFR 50, US Govt Printing Office, Washington, DC (2011).
[I–3] RADIATION AND NUCLEAR SAFETY AUTHORITY, Finnish Regulations YVL 1.0, STUK, Helsinki (1996).
[I–4] NUCLEAR REGULATORY COMMISSION, Proposed Orders and Request for Information in Response to Lessons Learned from Japan's March 11, 2011, Great Tohoku Earthquake and Tsunami, SECY 12-0025, US Govt Printing Office, Washington, DC (2012).
[I–5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1, IAEA, Vienna (2012).
[I–6] JAPAN ELECTRIC ASSOCIATION, Application Guide to Quality Assurance Code for Safety in Nuclear Power Plants — Operation Phase of Nuclear Power Plants, JAEG 4121-2009, Japan (2009).

Annex II

POST-ACCIDENT MONITORING IN PRESSURIZED HEAVY WATER REACTOR NUCLEAR POWER PLANTS — CANDU 6: WOLSONG UNITS 2/3/4

II–1. INTRODUCTION

The basic concept for post-accident monitoring (PAM) in the Canada deuterium–uranium (CANDU) 6 nuclear power plants in operation in the Republic of Korea is similar to other types of nuclear power plant. When design basis accidents (DBAs) occur, the safety systems actuate to provide mitigating actions, such as reactor shutdown, emergency core cooling and containment isolation. During and after a DBA, the operators need information to guide their responses.

The purpose of PAM instruments is to provide information to assist the control room operators after an accident:

(a) To evaluate the plant conditions and identify the nature or course of the accident;
(b) To confirm that the appropriate safety systems have performed or are performing their required actions;
(c) To monitor the plant characteristics to follow the effects of the accident;
(d) To determine the appropriate actions to be performed and monitor the results of the actions.

PAM is fulfilled by using various instruments, displays and indicators on the control panels in the main control room (MCR) or the panels in the secondary control area (SCA). Thus, an independent and separate system for the sole purpose of PAM is not adopted in the Wolsong 2/3/4 nuclear power plants. Control room operators are to watch the indicators or monitor displays located in the corresponding system panels because they are already accustomed to the display locations during normal operation. Basically, maximum use of the instrument loops of plant process, safety and safety related systems is expected for accident monitoring rather than installing a dedicated PAM system.

Therefore, when an emergency operating procedure is conducted by plant operators after reactor shutdown is initiated, they naturally use the safety instrument channels or non-safety channels in the control room to proceed with the diagnosis and response actions in accordance with the procedure.

II–2. FUNCTIONS AND PERFORMANCE OF POST-ACCIDENT MONITORING INSTRUMENT CHANNELS

The PAM instrument channels have the following three functions:

(a) To provide the information necessary to verify reactor shutdown, reactor heat removal and protection of barriers against the release of radioactivity to the environment;
(b) To provide information to the MCR and some of it to the SCA;
(c) To provide suitable annunciation to ensure the support of required operator actions.

II–2.1. Design bases

Instrumentation channels for PAM have been selected and designed based on the following considerations for plant safety:

— Initiating events/accidents for which monitoring is necessary;
— Safety systems designed to protect the initiating events and limit the consequences;

— Operator actions to be conducted after accidents;
— Plant characteristics and parameters related to post-accident actions.

II–2.1.1. Design basis accidents

The PAM related instruments or equipment have been designed and qualified to ensure they have the capabilities to meet monitoring requirements for the following DBAs:

(a) Loss of coolant accident (LOCA).
(b) Loss of feedwater.
(c) Main steam line break.
(d) LOCA + loss of emergency core cooling system (ECCS).
(e) LOCA + loss of class IV electric power.
(f) Single calandria tube accident (see Fig. II–1):
    — Stagnation feeder break;
    — Pressure tube rupture;
    — Channel flow blockage;
    — End fitting failure;
    — LOCA + site design earthquake;
    — Design basis earthquake (DBE).

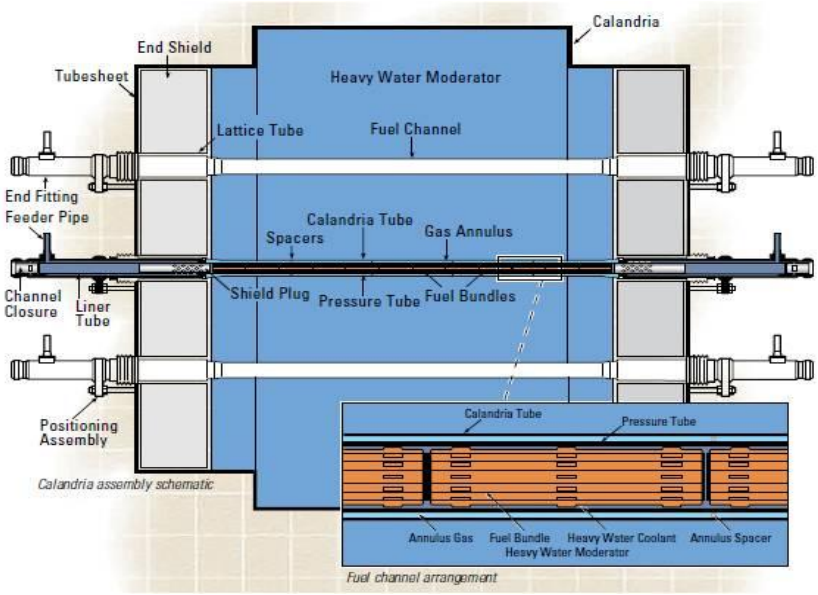


FIG. II–1. Structure of calandria and fuel channel.

II–2.1.2. Safety and safety related systems required during accidents

Safety systems and safety related systems required to operate during DBA sequences are considered in the PAM parameter selections. If a system is essential to prevent or mitigate an accident, the status or value indicating that the system is properly working needs to be confirmed as a part of the PAM. The systems credited to be used in DBA situations and the PAM parameters indicating their system status or output signals are as follows:

(a) Shutdown systems No. 1 and No. 2 (SDS1 and SDS2): Reactor power level and rate;
(b) ECCS: Flow, pump status, recirculation temperature and sump level;

(c) Containment system: Dousing tank level, containment isolation status, hydrogen igniter status, pressure and temperature;
(d) Heat transport system (HTS): Inlet and outlet header pressure/temperature, liquid relief valve (LRV) status, pressurizer level, deuterium oxide (D_2O) storage tank level, shutdown cooling system (SDCS) pump status and SDCS heat exchanger in/out temperature;
(e) Moderator system: Moderator level and temperature;
(f) Emergency water supply (EWS) system: Pump header pressure and flow rate;
(g) Emergency power supply (EPS) system: Bus status and supplying voltage;
(h) Main steam system: Steam generator (SG) pressure and level, main steam safety valve status;
(i) Feedwater system: Flow rate and deaerator level;
(j) Post-LOCA instrument air (PLIA): Compressor status;
(k) Post-accident air sampling monitor: Fuelling machine vault activity.

II–2.1.3. Operator actions in accident conditions

Operator actions credited or required during DBAs define which minimum set of information is provided by PAM signals to support the actions. Many actions are common to different DBAs. These operator action groups form a basis and rationale in selection and information grouping for PAM display strategies. Representative operator actions during DBAs in CANDU 6 plants are:

— Initiate high pressure emergency core cooling;
— Start the EWS and EPS;
— Secure the heat sink;
— Open the main steam safety valves;
— Operate the SDCS;
— Depressurize the containment;
— Conduct cooldown by the SG;
— Maintain the SG level.

II–2.1.4. Plant characteristics under accidents

The plant characteristics and safety features of CANDU plants, which are different from pressurized water reactors or boiling water reactors, are also important factors in selecting PAM variables and implementing them in the MCR and/or SCA. For example, the two independent coolant loops in CANDU plants are isolated from each other and from the pressurizer when a LOCA accident occurs. Four LRVs are used for overpressure protection of the coolant system during the time when the pressurizer is isolated. Failing to open the LRVs causes the same behaviour as during a LOCA. LRVs in the impaired loop need to be closed and LRVs in the intact loop may be opened during the LOCA or DBE. Therefore the LRV status is designated as one of the PAM variables as a performance verification parameter. In addition, the D_2O storage tank level is used as key information for detecting small LOCAs.

II–2.2. Post-accident monitoring parameters

Because the main barriers for protection from radiological releases are (i) fuel cladding, (ii) HTS (i.e. the reactor coolant system) and (iii) containment, most of the PAM parameters are selected to identify the conditions that indicate a threat to the integrity of the barriers.

Fuel cladding melting needs to be prevented by adequate cooling, which depends on reactor power, coolant circulation and the heat sink. The HTS boundary can be failed by overheating or by mechanical breaks. The containment integrity can be monitored by radioactivity measurements inside/outside the reactor building (R/B).

This subsection describes the main PAM variables used in the Wolsong 2/3/4 CANDU 6 plants.

II–2.2.1. Reactor power and rate

Verification of reactor shutdown can be performed by checking whether the nuclear fission of the reactor core is subcritical or not. 'Log power' and 'log rate' provide a continuous indication of the degree of subcriticality of the reactor core and the trend of the neutron flux from the core. The displays in the MCR are provided by SDS1 (channels D and F) and SDS2 (channels G and J) for redundancy. The indication in the SCA is provided by SDS2 (channels G and J).

II–2.2.2. Primary heat transport system parameters

The temperature and pressure of the HTS are the key parameters for ensuring that the residual heat from the reactor core is being removed by the circulation of coolant water after reactor shutdown. The PAM parameters associated with the HTS are:

— Reactor outlet header temperature;
— Reactor outlet header pressure;
— Reactor inlet header temperature;
— Header to header differential temperature;
— LRV status, among other things.

II–2.2.3. Heat transport system inventory parameters

In the event of a small LOCA, the inventory of the HTS will decrease at a rate that depends on the break size. Therefore, information on the HTS inventory is required to support the plant operators to recognize the occurrence of a small LOCA and arrange for an alternative source for a heat sink. The following two PAM parameters provide the appropriate indications for small LOCAs (or leaks):

— Pressurizer level;
— D_2O storage tank level.

II–2.2.4. Steam and feedwater related parameters

The residual heat from the fuel is primarily removed by the SGs when the reactor coolant is circulating. The PAM parameters related to the heat sink from the SGs are:

— SG pressure;
— SG level;
— Main steam safety valve status;
— Feedwater flow;
— Deaerator level.

II–2.2.5. Emergency core cooling system parameters

Since LOCA is one of the most significant accidents threatening the fuel, the ECCS is provided as a safety system to inject cooling water into the reactor when a LOCA occurs. Therefore, it is necessary for the operators to be assured that emergency cooling water is being supplied to the HTS by observing the following PAM parameters:

— ECCS recirculation flow;
— ECCS pump status;
— ECCS recirculation water temperature;
— R/B sump water temperature;
— ECCS sump water level.

II–2.2.6. Containment system parameters

Integrity of containment (i.e. within the R/B), which is the last barrier to radiological releases, can be monitored via the following PAM parameters:

— Dousing tank water level;
— R/B isolation valve status;
— R/B temperature;
— R/B radioactivity.

II–2.2.7. Moderator system parameters

In case of physical contact between the pressure and calandria tubes resulting from a LOCA event, moderator heavy water can become another heat sink for the reactor. The PAM parameters for the moderator system are:

— Moderator level;
— Moderator temperature.

II–2.2.8. Post loss of coolant accident instrument air system

In CANDU 6 nuclear power plants, the secondary instrument air system, called the PLIA system, is equipped to avoid a pressure rise in the R/B resulting from in-flow of instrument air when the containment is isolated after a LOCA. The PLIA system, which employs a smaller compressor than the normal instrument air system, draws air from the containment to deliver compressed air to instruments inside the containment via dedicated instrument air lines. The PAM parameter for the PLIA system is:

— Operational status of the PLIA system.

II–2.2.9. Emergency power supply system parameters

In the event that all normal station power supplies (i.e. classes 1, 2, 3 and 4) are not available, such as following a DBE, the EPS system provides electrical power from seismically qualified diesel generators to equipment that is essential for long term reactor cooling and monitoring. The systems to be supplied with electrical power by the EPS system are, among other things, ECCS pumps, ECCS and EWS valves, hydrogen igniters, PAM parameters, necessary heating and lighting. The EPS is started by operators in the SCA. The PAM parameter for the EPS system is:

— Status and voltage of the power bus.

II–2.2.10. Emergency water supply system parameters

The EWS provides an alternative source of cooling water for decay heat removal when all or a part of the normal water supply is unavailable. It uses three pumps in an emergency water and power supply building to provide water to SGs, the HTS (for make-up purposes) and the ECCS heat exchanger secondary side. The PAM parameter is provided by the EWS:

— Opening of EWS valves and water flow.

II–2.2.11. Shutdown cooling system parameters

The purpose of the SDCS is to provide cooling water to the HTS for decay heat removal when the reactor is shut down. The SDCS can be used as a heat sink for cooling the reactor core via the unimpaired loop in the

event of LOCA, or for alternative cooling in the case of loss of feedwater or steam line breaks. The following PAM parameters indicate the status of the SDCS:

— Pumps suction/discharge pressures;
— Heat exchanger inlet/outlet temperatures.

II–2.2.12. Gaseous effluent monitor activity and rate

The gaseous effluent monitoring system (i.e. a stack monitor) provides information on radioactive gases released from the R/B. The PAM parameters measured by the gaseous effluent monitoring system are:

— Particulate concentration;
— Iodine-131 concentration;
— Noble gas concentration.

II–2.2.13. Containment activity

The post-accident air sampling and monitoring system is used to monitor the radiation level in the air in the R/B after an accident and R/B isolation. It monitors environmental conditions inside the R/B so that the operators can decide whether to vent the R/B and whether the R/B is accessible. The post-accident air sampling and monitoring system provides:

— Concentrations of radioisotopes in the R/B atmosphere.

II–2.3. Components comprising post-accident monitoring instruments

The PAM instruments can be divided into the following three basic components:

— Sensing devices;
— Signal transmission devices;
— Display devices.

Most sensing devices and signal transmission devices are located in the field where the PAM parameters are to be detected. The display devices are located in the MCR and/or SCA.

II–2.3.1. Sensing devices

The sensing devices are composed of an element that is in contact with the actual process entity being measured and a transmitter or an amplifier that generates an electrical signal proportional to some attribute of the entity.

The types of attribute (process parameters) monitored in the Wolsong 2/3/4 nuclear power plants include:

— Neutron flux power (log N);
— Log rate;
— Radioactivity;
— Pressure;
— Temperature;
— Level;
— Flow;
— Current;
— Voltage;
— Position status.

Among the above process parameters, pressure, differential pressure, flow and level transmitters are the most common types of sensing device which are based on pressure measurements. The transmitters exploit a diaphragm type element connected to the process by means of instrument tubing to pressure taps on a tank or pipe. The role of instrument tubing is to deliver the pressure of the process to the sensing elements which are mounted at distance in a proper place for instrument maintenance and protection.

The temperatures are measured by resistance temperature detectors mounted in thermowells on tanks or pipes. A resistance to current converter converts resistance value to 4–20 mA signals or 0.9–4.5 V signals. The position status for valves is sensed by limit switches attached to the valve body. Radioactivity is provided by on-line radiation monitoring analysers. Neutron flux is measured using ion chambers.

II–2.3.2. Transmission devices

The typical transmission method for the measured signals is to use 4–20 mA current signals for noise immunity. Signal connections between the MCR and SCA are buffered by using signal isolating devices in current to current converters.

II–2.3.3. Display devices

PAM parameters are shown in either display monitors, panel meters, electromechanical indicators or indicating lights. The display monitors are driven by a digital control computer system.

II–2.4. Design performances of post-accident monitoring components

(a) Seismic: The PAM instruments that are required for monitoring during and after site design earthquakes or DBEs are qualified seismically in accordance with adequate safety design guides. Those instruments can survive to provide the PAM parameters in case of postulated seismic events.
(b) Environmental: The PAM instruments are tested or demonstrated to ensure that the instrument channels will remain operational during and following the accidents in which they are supposed to perform measurements.
(c) Reliability: The availability of instrument channels for a PAM parameter is better than 99.0%. This availability is achieved by periodic testing and reliable design of each measurement system. The PAM parameter instrumentation satisfies a single failure criterion.
(d) Testing capability: The functionality of PAM instrument channels can be checked or tested on power at any time. Although entire sensor to display testing is preferable, if it is impractical, alternative methods such as cross-comparison are used.

II–3. OPERATION STRATEGIES

II–3.1. Normal operation

Because the CANDU 6 plants do not have an independent PAM system and PAM channels have at least two redundant channels, operators compare the redundant indications of each parameter throughout the MCR panels to check their functionality.

II–3.2. Post-accident operation

In an accident situation, operators are to check the appropriate indications in the MCR because they take actions in accordance with emergency operating procedures. Therefore, operators access the PAM display devices of each system in which the parameter to be monitored is presented.

When the MCR is not habitable, the operators are to use the SCA to monitor the accident related parameters.

II–4. LOCATION OF POST-ACCIDENT MONITORING INDICATORS AND DISPLAYS

PAM parameter displays are located on their respective system panels. However, some PAM parameters in the SCA are displayed on the same panel. Nine digital control computer monitors mounted in the control room panels and one monitor in the operator desk can also be used to provide displays of any PAM parameters. The PAM parameters indicated in the SCA include:

— Reactor power and log rate;
— Reactor outlet header temperature and pressure;
— Core differential pressure;
— Pressurizer level;
— SG pressure level;
— ECCS recirculation flow and temperature;
— ECCS pump status;
— R/B water level;
— Dousing tank level;
— R/B isolation status;
— R/B pressure and temperature;
— Hydrogen igniter status;
— Moderator temperature;
— PLIA status;
— EPS bus voltage;
— EWS pump status and flow.

II–5. CONCLUSION

In the Wolsong 2/3/4 CANDU 6 nuclear power plants, PAM is basically fulfilled by using various instruments, displays and indicators on the control panels in the MCR or the panels in SCA. When the MCR is unavailable, the SCA provides most of the parameters for long term PAM.

GLOSSARY

accident conditions. Deviations from normal operation that are less frequent and more severe than anticipated operational occurrences, including design basis accidents and design extension conditions.

accident management. The taking of a set of actions during the evolution of a beyond design basis accident to prevent the escalation of the event into a severe accident, to mitigate the consequences of a severe accident and to achieve a long term controlled state. The second aspect of accident management (to mitigate the consequences of a severe accident) is also termed severe accident management.

anticipated operational occurrence. An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

controlled state. A plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to implement provisions to reach a safe state.

design basis accident. An accident causing accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits.

design extension conditions. Accident conditions that are not considered for design basis accidents, but that are considered in the design process of the facility in accordance with best estimate methodology, and for which releases of radioactive material are kept within acceptable limits. Design extension conditions could include severe accident conditions.

parameter. A physical plant condition that may be directly measurable or may be inferred through a set of plant variables.

qualification. The demonstration and documentation of the ability of the equipment to perform its functions under applicable service conditions.

severe accident. Accident conditions more severe than a design basis accident and involving significant fuel degradation.

severe accident management. See **severe accident** and **accident management**. By extension, accident management for a severe accident includes the taking of a set of actions during the evolution of the accident to mitigate degradation of the fuel.

variable. A quantity or data item, typically measured directly by an instrumentation channel, whose value can change.

ABBREVIATIONS

AMG	accident management guideline
ANS	American Nuclear Society
BWR	boiling water reactor
CANDU	Canada deuterium–uranium
CCF	common cause failure
CV	containment vessel
DBA	design basis accident
DBE	design basis earthquake
DEC	design extension conditions
ECCS	emergency core cooling system
EOP	emergency operating procedure
EPRI	Electric Power Research Institute
EPS	emergency power supply
EWS	emergency water supply
HTS	heat transport system
I&C	instrumentation and control
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
KTA	Kerntechnischer Ausschuss (Nuclear Safety Standards Commission)
LOCA	loss of coolant accident
LRV	liquid relief valve
MCR	main control room
NRC	United States Nuclear Regulatory Commission
PAM	post-accident monitoring
PCV	primary containment vessel
PLIA	post-LOCA instrument air
PWR	pressurized water reactor
R/B	reactor building
RCS	reactor coolant system
RPV	reactor pressure vessel
RV	reactor vessel
SAMG	severe accident management guideline
SCA	secondary control area
SDCS	shutdown cooling system
SFP	spent fuel pool
SG	steam generator
SSCs	systems, structures and components
TMI	Three Mile Island
TSC	technical support centre

CONTRIBUTORS TO DRAFTING AND REVIEW

Arita, S.	Hitachi-GE Nuclear Energy Ltd, Japan
Barbaud, J.Y.	Électricité de France — SEPTEN, France
Campion, M.	AMEC, United Kingdom
Cowdrey, C.B.	Nuclear Regulatory Commission, United States of America
Duchac, A.	International Atomic Energy Agency
Eiler, J.	International Atomic Energy Agency
Hong, Z.	Shanghai Nuclear Engineering Research and Design Institute, China
Hostetter, G.	Tetra Tech, United States of America
Hunt, P.	Bruce Power Inc., Canada
Hwang, I.K.	Korea Atomic Energy Research Institute, Republic of Korea
Janzekovic, H.	Slovenian Nuclear Safety Administration, Slovenia
Johnson, G.	International Atomic Energy Agency
Koenig, W.	AREVA NP GmbH, Germany
Lee, A.	Candu Energy Inc., Canada
Peko, D.	Department of Energy, United States of America
Rahn, D.L.	Nuclear Regulatory Commission, United States of America
Slanina, M.	VUJE, Slovakia
Solovjanov, O.	Westinghouse Electric Co., Belgium
Vidard, M.L.	MVI Consulting, France

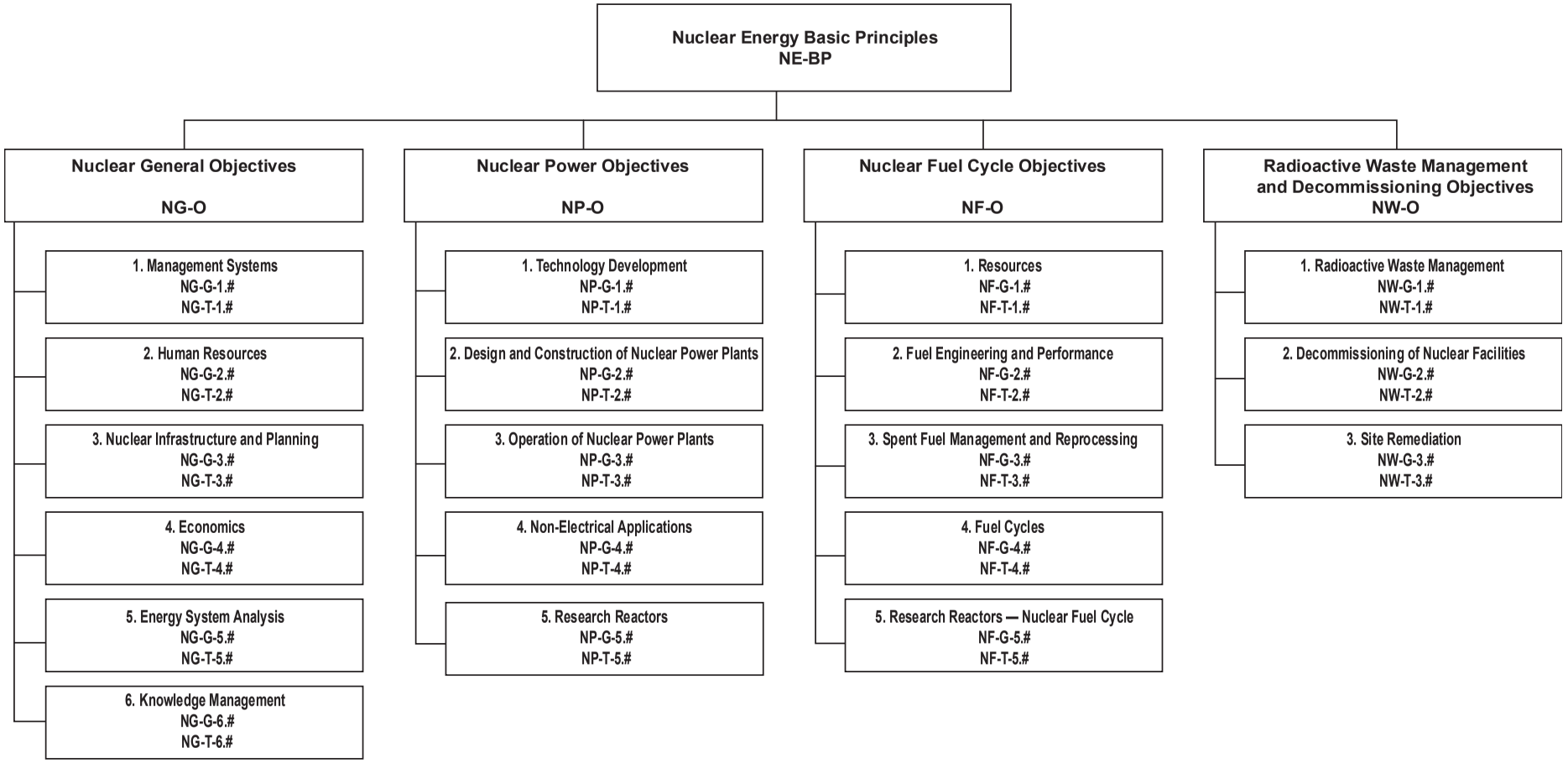
Technical Meeting

Hwaseong-si, Republic of Korea: 6–9 May 2013

Consultants Meetings

Tokyo, Japan: 3–7 September 2012
Vienna, Austria: 18–22 March 2013, 2–6 December 2013

Structure of the IAEA Nuclear Energy Series



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**

IAEA
International Atomic Energy Agency

No. 23

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.

AUSTRALIA
DA Information Services
648 Whitehorse Road, Mitcham, VIC 3132, AUSTRALIA
Telephone: +61 3 9210 7777 • Fax: +61 3 9210 7788
Email: books@dadirect.com.au • Web site: http://www.dadirect.com.au

BELGIUM
Jean de Lannoy
Avenue du Roi 202, 1190 Brussels, BELGIUM
Telephone: +32 2 5384 308 • Fax: +32 2 5380 841
Email: jean.de.lannoy@euronet.be • Web site: http://www.jean-de-lannoy.be

CANADA
Renouf Publishing Co. Ltd.
5369 Canotek Road, Ottawa, ON K1J 9J3, CANADA
Telephone: +1 613 745 2665 • Fax: +1 643 745 7660
Email: order@renoufbooks.com • Web site: http://www.renoufbooks.com

Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

CZECH REPUBLIC
Suweco CZ, spol. S.r.o.
Klecakova 347, 180 21 Prague 9, CZECH REPUBLIC
Telephone: +420 242 459 202 • Fax: +420 242 459 203
Email: nakup@suweco.cz • Web site: http://www.suweco.cz

FINLAND
Akateeminen Kirjakauppa
PO Box 128 (Keskuskatu 1), 00101 Helsinki, FINLAND
Telephone: +358 9 121 41 • Fax: +358 9 121 4450
Email: akatilaus@akateeminen.com • Web site: http://www.akateeminen.com

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: fabien.boucard@formedit.fr • Web site: http://www.formedit.fr

Lavoisier SAS
14 rue de Provigny, 94236 Cachan CEDEX, FRANCE
Telephone: +33 1 47 40 67 00 • Fax: +33 1 47 40 67 02
Email: livres@lavoisier.fr • Web site: http://www.lavoisier.fr

L'Appel du livre
99 rue de Charonne, 75011 Paris, FRANCE
Telephone: +33 1 43 07 50 80 • Fax: +33 1 43 07 50 80
Email: livres@appeldulivre.fr • Web site: http://www.appeldulivre.fr

GERMANY
Goethe Buchhandlung Teubig GmbH
Schweitzer Fachinformationen
Willstätterstrasse 15, 40549 Düsseldorf, GERMANY
Telephone: +49 (0) 211 49 8740 • Fax: +49 (0) 211 49 87428
Email: s.dehaan@schweitzer-online.de • Web site: http://www.goethebuch.de

HUNGARY
Librotrade Ltd., Book Import
PF 126, 1656 Budapest, HUNGARY
Telephone: +36 1 257 7777 • Fax: +36 1 257 7472
Email: books@librotrade.hu • Web site: http://www.librotrade.hu

INDIA
Allied Publishers
1st Floor, Dubash House, 15, J.N. Heredi Marg, Ballard Estate, Mumbai 400001, INDIA
Telephone: +91 22 2261 7926/27 • Fax: +91 22 2261 7928
Email: alliedpl@vsnl.com • Web site: http://www.alliedpublishers.com

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

JAPAN
Maruzen Co., Ltd.
1-9-18 Kaigan, Minato-ku, Tokyo 105-0022, JAPAN
Telephone: +81 3 6367 6047 • Fax: +81 3 6367 6160
Email: journal@maruzen.co.jp • Web site: http://maruzen.co.jp

NETHERLANDS
Martinus Nijhoff International
Koraalrood 50, Postbus 1853, 2700 CZ Zoetermeer, NETHERLANDS
Telephone: +31 793 684 400 • Fax: +31 793 615 698
Email: info@nijhoff.nl • Web site: http://www.nijhoff.nl

SLOVENIA
Cankarjeva Zalozba dd
Kopitarjeva 2, 1515 Ljubljana, SLOVENIA
Telephone: +386 1 432 31 44 • Fax: +386 1 230 14 35
Email: import.books@cankarjeva-z.si • Web site: http://www.mladinska.com/cankarjeva_zalozba

SPAIN
Diaz de Santos, S.A.
Librerias Bookshop • Departamento de pedidos
Calle Albasanz 2, esquina Hermanos Garcia Noblejas 21, 28037 Madrid, SPAIN
Telephone: +34 917 43 48 90 • Fax: +34 917 43 4023
Email: compras@diazdesantos.es • Web site: http://www.diazdesantos.es

UNITED KINGDOM
The Stationery Office Ltd. (TSO)
PO Box 29, Norwich, Norfolk, NR3 1PD, UNITED KINGDOM
Telephone: +44 870 600 5552
Email (orders): books.orders@tso.co.uk • (enquiries): book.enquiries@tso.co.uk • Web site: http://www.tso.co.uk

UNITED STATES OF AMERICA
Bernan Associates
4501 Forbes Blvd., Suite 200, Lanham, MD 20706-4391, USA
Telephone: +1 800 865 3457 • Fax: +1 800 865 3450
Email: orders@bernan.com • Web site: http://www.bernan.com

Renouf Publishing Co. Ltd.
812 Proctor Avenue, Ogdensburg, NY 13669, USA
Telephone: +1 888 551 7470 • Fax: +1 888 551 7471
Email: orders@renoufbooks.com • Web site: http://www.renoufbooks.com

United Nations
300 East 42nd Street, IN-919J, New York, NY 1001, USA
Telephone: +1 212 963 8302 • Fax: 1 212 963 3489
Email: publications@un.org • Web site: http://www.unp.un.org

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

IAEA Publishing Section, Marketing and Sales Unit, International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22488 • Fax: +43 1 2600 29302
Email: sales.publications@iaea.org • Web site: http://www.iaea.org/books

14-51441

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA
ISBN 978–92–0–110414–4
ISSN 1995–7807