IAEA
International Atomic Energy Agency

SAFETY REPORTS SERIES

No. 46 (Rev. 1)

Assessment of Defence in Depth for Nuclear Power Plants

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available on the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

ASSESSMENT OF DEFENCE IN DEPTH FOR NUCLEAR POWER PLANTS

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

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

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

SAFETY REPORTS SERIES No. 46 (Rev. 1)

ASSESSMENT OF DEFENCE IN DEPTH FOR NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2024

COPYRIGHT NOTICE

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
tel.: +43 1 2600 22529 or 22530
email: sales.publications@iaea.org
www.iaea.org/publications

Printed by the IAEA in Austria
June 2024
STI/PUB/2008
https://doi.org/10.61092/iaea.dbwn-89a9

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Assessment of defence in depth for nuclear power plants / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2024. | Series: safety reports series, ISSN 1020–6450 ; no. 46 (Rev.1) | Includes bibliographical references.
Identifiers: IAEAL 23-01623 | ISBN 978–92–0–144923–8 (paperback : alk. paper) | ISBN 978–92–0–145023–4 (pdf) | ISBN 978–92–0–145123–1 (epub)
Subjects: LCSH: Nuclear power plants — Safety measures. | Nuclear reactors — Safety measures. | Nuclear power plants — Design and construction.
Classification: UDC 621.039.58 | STI/PUB/2008

FOREWORD

The concept of defence in depth has evolved from the original idea of using multiple physical barriers against releases of radioactive materials to incorporating a combination of barriers and complementary means of providing the barriers with consecutive and independent levels of protection. Defence in depth is an overall safety philosophy that encompasses the entire lifetime of a nuclear power plant (NPP), including siting, design, manufacture, construction, commissioning, operation and decommissioning. Defence in depth is applied by means of organizational, behavioural or design related safety measures, and it represents a focal point for the IAEA's safety related activities.

In the late 1990s, the IAEA recognized a need for more specific guidance on the implementation and assessment of defence in depth in NPPs. To address this need, in 2005 the IAEA published Safety Reports Series No. 46, Assessment of Defence in Depth for Nuclear Power Plants. The Safety Report introduced an assessment method (objective trees) that was designed to facilitate the assessment of an NPP's conformance to the concept of defence in depth and was primarily applicable to existing NPPs. Since its publication, the method described in the Safety Report has been used in a number of practical applications.

The present publication is a revision of Safety Reports Series No. 46 that takes into account developments since the publication of the original Safety Report, including significant enhancements of the international safety requirements for NPPs. It also incorporates operating experience and lessons learned from previous applications of the method.

The publication describes the updated version of the original method for assessing the comprehensiveness of defence in depth and demonstrates the overall improvement in assessment results when it is used. For assessment of comprehensiveness, five levels of defence in depth are considered. To ensure that safety objectives are met at each level of defence in depth, the integrity of relevant fission product barriers is fulfilled by the safety functions. A set of challenges to the performance of safety functions and the mechanisms leading to these challenges are specified by the method. Finally, a comprehensive list of safety provisions, which contribute to preventing these mechanisms from occurring, is specified. These provisions encompass the inherent safety features, equipment, procedures, personnel availability, personnel training and safety culture aspects. The challenges, mechanisms and provisions for all levels of defence in depth are presented in the assessment method in the form of objective trees.

The assessment method is intended to be used predominantly by the operating organization, and thus covers the responsibility of the operating organization for all stages of the NPP's lifetime, from siting to the cessation of operation, as well as external factors important to safety that can be influenced

by the operating organization. Nevertheless, the method provides useful practical guidance for any other user requiring a comprehensive assessment of defence in depth, including regulatory bodies and technical support organizations providing services either to the regulatory body or to the operating organization.

The on line supplementary file for this publication, which can be found on the publication's individual web page at https://doi.org/10.61092/iaea.dbwn-89a9, provides a full set of objective trees for the purpose of practical assessment of the defence in depth capabilities of NPPs.

The IAEA is grateful to the experts from ČEZ and the Japan Nuclear Safety Institute who contributed to this publication. The IAEA officers responsible for this publication were A. Duchac and and J. Luis Hernández of the Division of Nuclear Installation Safety.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The primary means of preventing accidents in a nuclear power plant (NPP) and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth. Defence in depth is defined in the IAEA Nuclear Safety and Security Glossary [1] as:

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

Paragraph 3.31 of IAEA Safety Standards Series No. SF-1, Fundamental Safety Principles [2], refers to defence in depth as the primary means of preventing and mitigating the consequences of accidents.

Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. Defence in depth is an overall safety philosophy that encompasses all safety activities, including the siting, design, manufacture, construction, commissioning, operation and decommissioning of NPPs. Defence in depth is based on multiple barriers, and a variety of means (provisions) to protect these barriers is an essential strategy to ensure the nuclear safety of NPPs.

Defence in depth ensures that the fundamental safety functions are maintained with sufficient margins to compensate for equipment failures, uncertainties, incomplete knowledge of accident initiation and progression, and human errors. If one level of defence fails, the subsequent level of defence comes into play.

The safety provisions associated with defence in depth can be of different natures: organizational, behavioural and design measures, including properly selected site characteristics, inherent safety features, safety margins, active and passive systems, operating procedures and operator actions, more general organizational measures and safety culture aspects. The levels of defence are intended to be individually robust and independent to the extent reasonably practicable, in particular between Levels 3 and 4.

The International Nuclear Safety Advisory Group (INSAG) introduced the concept of basic safety principles, including defence in depth, in INSAG-3, published in 1988. The concept of defence in depth was elaborated in INSAG-10 [3], published in 1996. INSAG-12 [4] was published in 1999 as a revision of INSAG-3 to take into account subsequent developments of and refinements to nuclear safety principles for NPPs. In this revision, INSAG recognized the benefits of excellence in operational and human performance by promoting behaviour that supports the safety and reliability of NPPs throughout the entire operating organization. The emphasis was placed upon reinforcing the right behaviour in all aspects of management, operation, maintenance and design modification, rather than exclusively upon the results and outcomes of the work.

Subsequent to the issuance of the INSAG reports, the concept of fundamental safety principles was incorporated into SF-1 [2], published in 2006. Finally, the concept of defence in depth for NPPs was established in the IAEA safety requirements publications, most recently in paras 2.12 to 2.14 and Requirement 7 of SSR-2/1 (Rev. 1) [5].

Safety Reports Series No. 46, Assessment of Defence in Depth for Nuclear Power Plants[1], published in early 2005, described a practical assessment method ('objective trees') for assessing the comprehensiveness of the defence in depth capabilities of an NPP (mainly of an existing NPP). However, significant enhancements of international safety requirements, including defence in depth, have since taken place, in particular after the Fukushima Daiichi accident.

Other sources of information were also reviewed for applicable updates to the assessment method of objective trees. Among these, the following IAEA publications were considered:

— IAEA Safety Standards Series No. SSR-1, Site Evaluation for Nuclear Installations [6];
— IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), Safety of Nuclear Power Plants: Commissioning and Operation [7];
— IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant [8];
— IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant [9].

The Western European Nuclear Regulators Association (WENRA), which aims to develop a harmonized approach to nuclear safety within its member countries, published its approach for updating the assessment method

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants, Safety Reports Series No. 46, IAEA, Vienna (2005).

of defence in depth in its report WENRA Safety Reference Levels for Existing Reactors — Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident [10].

The present publication updates the method of objective trees that was previously described in Safety Reports Series No. 46, which it supersedes. The updated method also features improved user friendliness based on experience gained from previous method applications. This publication presents the results of the overall improvement of the method for assessing the comprehensiveness of defence in depth at all levels of defence.

1.2. OBJECTIVE

The objectives of this publication are as follows:

— To update the method of objective trees and provide a comprehensive overview of the concept of defence in depth, considering the enhancement of international safety requirements, including those resulting from the lessons learned from the Fukushima Daiichi accident;
— To present the results of the overall improvement of the method for assessing the comprehensiveness of defence in depth at all levels of defence, taking into consideration the updated IAEA Safety Standards, in particular SSR-2/1 (Rev. 1), Safety of Nuclear Power Plants: Design [5];
— To provide a method for the systematic identification of the required safety provisions for siting, design, construction, commissioning and operation that are needed for assessing the comprehensiveness and quality of defence in depth at the plant.

The target audience of this Safety Report is operating organizations, regulatory bodies and their technical support organizations, consultants and advisory bodies.

Guidance and recommendations provided here in relation to identified good practices represent expert opinion but are not made on the basis of a consensus of all Member States.

1.3. SCOPE

This publication applies to both new and, with engineering judgement, existing NPPs. The publication also applies to spent fuel transported or stored in pools outside the reactor coolant system (RCS) on the reactor site. The method

described in this publication could also be adapted for other types of reactors, such as small modular reactors.

The publication addresses the assessment methods applicable to various stages of the lifetime of an NPP, including siting, design, construction, commissioning and operation. Decommissioning, because of its specific features and significantly different ways of ensuring safety, will not be specifically considered in the application of this assessment method, although many aspects are implicitly covered as a part of the design and operational provisions.

The five levels of defence in depth are covered in the present publication. For given objectives at each level of defence, a set of challenges are identified, and several root mechanisms leading to the challenges are specified. Finally, to the extent possible, a comprehensive list of safety provisions, designed to prevent these mechanisms from occurring, is provided. These safety provisions, which encompass the inherent safety features, equipment, procedures, staff availability, personnel training and safety culture aspects of the levels of defence in depth, are considered.

For an easier and more user friendly application of this assessment method, an overview of all of the challenges, mechanisms and safety provisions for all levels of defence is illustrated in the form of 'objective trees'.

The assessment method described in this publication is not meant to replace other evaluations that are required by national or international standards. Rather, it is intended to provide an additional tool to help assess the comprehensiveness and implementation of defence in depth in an NPP. Guidance and recommendations provided here in relation to identified good practices represent expert opinion but are not made on the basis of a consensus of all Member States.

1.4. STRUCTURE

Section 2 addresses the concept of defence in depth and the importance of fulfilling the safety functions to achieve the safety objectives for the different levels of defence. Section 3 provides a detailed description of the approach to making an inventory of the defence in depth capabilities of a plant. Section 4 describes the process (or the steps) for the use of the method. Section 5 discusses the potential applications of the method for practical tasks, based on experience from the use of the method.

Appendix I provides a discussion of the safety functions derived from the fundamental safety functions for the purpose of this publication. Appendix II[2]

[2] Appendix II is published in full as an online supplementary file to accompany this publication. Appendix II of this publication summarizes the content of the supplementary file.

summarizes the objective trees that graphically represent how, for each relevant SP, the safety objectives of the different levels of defence can be achieved by establishing defence in depth provisions at different stages of the lifetime of the plant.

Annex I describes a possible approach that demonstrates the process of the practical elimination of plant event sequences leading to early or large radioactive releases as a complementary component to the assessment of defence in depth. Finally, Annex II provides the justification for modifications of the objective trees originally contained in the superseded publication.

2. THE CONCEPT OF DEFENCE IN DEPTH

2.1. GENERAL CONSIDERATIONS

The Safety Fundamentals SF-1 [2] established one fundamental safety objective and ten safety principles that provide the basis for requirements and measures for the protection of people and the environment against radiation risks and for the safety of facilities and activities that give rise to radiation risks. The fundamental safety objective applies to all stages in the lifetime of an NPP, including siting, design, manufacture, construction, commissioning and operation, as well as decommissioning. This includes the associated transport of radioactive material and the management of spent nuclear fuel and radioactive waste.

Principle 8 (Prevention of accidents) of SF-1 [2] states: "All practical efforts must be made to prevent and mitigate nuclear or radiation accidents."

Specifically, para. 3.30 of SF-1 [2] states:

> "The most harmful consequences arising from facilities and activities have come from the loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or other source of radiation. Consequently, to ensure that the likelihood of an accident having harmful consequences is extremely low, measures shall be taken:
>
> — To prevent the occurrence of failures or abnormal conditions (including breaches of security) that could lead to such a loss of control;
> — To prevent the escalation of any such failures or abnormal conditions that do occur;
> — To prevent the loss of, or the loss of control over, a radioactive source or other source of radiation."

Furthermore, para. 2.12 of SSR-2/1 (Rev. 1) [5] states:

> "The primary means of preventing accidents in a nuclear power plant and mitigating the consequences of accidents if they do occur is the application of the concept of defence in depth… This concept is applied to all safety related activities, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. This is to ensure that all safety related activities are subject to independent layers of provisions so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth throughout design and operation provides protection against anticipated operational occurrences and accidents, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant."

The concept of defence in depth applies to all activities important to safety, whether organizational, behavioural or design related, and whether in full power, low power or various shutdown states. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability.

Defence in depth is provided by an appropriate combination of the following measures:

- An effective integrated management system of the design and operating organizations (see GSR Part 2 [11] and the associated Safety Guides for relevant provisions);
- Adequate site selection (see SSR-1 (Rev. 1) [6] and the associated Safety Guides for relevant provisions);
- Robust design and engineering practices ensuring appropriate implementation of design principles, adequate safety margins, and protection against hazards (see SSR-2/1 (Rev. 1) [5] and the associated Safety Guides for relevant provisions);
- Comprehensive operational procedures and practices, as well as accident management procedures (see SSR-2/2 (Rev. 1) [7] and the associated Safety Guides for relevant provisions).

The specific design of several successive independent fission product barriers for the confinement of radioactive material may vary, depending on the radioactivity of the material and on the possible deviations from normal operation

that could result in the failure of some barriers. The number and type of barriers that confine the fission products are dependent on the technology that has been adopted for the reactor. For the NPPs under consideration, these barriers include the fuel matrix (not always listed as a separate barrier), the fuel cladding, the pressure boundary of the RCS and the reactor containment.

The concept of defence in depth as applied to NPPs is generally divided into five levels. If one level fails, the subsequent level comes into play. Table 1 summarizes the objectives of each level and the corresponding provisions that are essential for achieving them. The objectives of different levels of defence (criteria of success) described in Table 1 are specified in para. 3.5 of SSG-88 [12].

The IAEA's definition of the levels of defence might have different interpretations, mainly in relation to Level 3 and Level 4. The IAEA Safety Guide on Design Extension Conditions and the Concept of Practical Elimination in the Design of Nuclear Power Plants (SSG-88) provides guidance on the interpretation of the two main approaches [12].

Paragraph 3.31 of SF-1 [2] states:

> "Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. ...The independent effectiveness of the different levels of defence is a necessary element of defence in depth."

TABLE 1. LEVELS OF DEFENCE IN DEPTH *(reproduced from Ref. [12])*

Level of defence	Objective	Essential design means	Essential operational means	Level of defence
Approach 1				Approach 2
Level 1	Prevention of abnormal operation and failures	Robust design and high quality in construction of normal operation systems, including monitoring and control systems	Operational limits and conditions and normal operating procedures	Level 1

TABLE 1. LEVELS OF DEFENCE IN DEPTH *(reproduced from Ref. [12]) (cont.)*

Level of defence		Objective	Essential design means	Essential operational means	Level of defence
Approach 1					Approach 2
Level 2		Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures and/or emergency operating procedures	Level 2
Level 3	3a	Control of design basis accidents	Safety systems	Emergency operating procedures	Level 3
	3b	Control of design extension conditions to prevent core melting	Safety features for design extension conditions without significant fuel degradation[a]	Emergency operating procedures	Level 4
Level 4		Control of design extension conditions to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melting[b] Technical support centre	Severe accident management guidelines	
Level 5		Mitigation of the radiological consequences of significant releases of radioactive substances	On-site and off-site emergency response facilities	On-site and off-site emergency plans and procedures	Level 5

[a] Such safety features are understood as additional safety features for design extension conditions, or as safety systems with an extended capability to prevent the consequences of severe accidents (see para. 5.27 of SSR-2/1 (Rev. 1) [5]).

[b] Such safety features are understood as additional safety features for design extension conditions, or as safety systems with an extended capability to mitigate the consequences of severe accidents or to maintain the integrity of the containment (see para. 5.27 of SSR-2/1 (Rev. 1) [5]).

The levels of defence are intended to be individually robust and independent to the extent reasonably practicable, particularly between Levels 3 and 4. The safety objective of defence in depth is to ensure that a single failure, whether an equipment failure or a human failure, at one level of defence, or a combination of failures at more than one level of defence, does not propagate to jeopardize subsequent levels of defence in depth. The individual robustness and independence of different levels of defence are crucial to meeting this objective.

The objective of Level 1 is the prevention of abnormal operation and system failures. If there is a failure at this level, an initiating event takes place. This can happen either if the defence in depth provisions at Level 1 were not effective or if a certain mechanism was not considered in establishing the defence in depth provisions at Level 1. Level 2 will detect these failures, to avoid or to control the abnormal operation. If Level 2 fails, Level 3 ensures that the fundamental safety functions will be performed mainly by the activation of specific safety systems or safety features with a view to limiting the possible consequences of design basis accidents (DBAs) or of design extension conditions (DECs) without significant fuel degradation. If Level 3 fails, Level 4 limits accident progression by means of safety features for DECs with core melting and accident management provisions in order to prevent severe accident conditions with external releases of radioactive material and to mitigate the consequences of such accidents if they were to occur.

The objective of Level 5 is the mitigation of the radiological consequences of significant external releases through the on-site and off-site emergency response. The provisions of Level 5, depending on the national regulations and the classification of the emergency, are not fully controlled by the operating organization, since local, regional or State authorities play an important role in the execution of off-site emergency plans.

The role of the operating organization is to establish on-site emergency response facilities and to contribute to off-site emergency response facilities to meet Requirement 67 of SSR-2/1 (Rev. 1) [5], which states:

> "The nuclear power plant shall include the necessary emergency response facilities on the site. Their design shall be such that personnel will be able to perform expected tasks for managing an emergency under conditions generated by accidents and hazards."

Furthermore, para. 6.42 of SSR-2/1 (Rev. 1) [5] states:

> "Information about important plant parameters and radiological conditions at the nuclear power plant and in its immediate surroundings shall be provided to the relevant emergency response facilities[23]. Each facility shall be provided with means of communication with, as appropriate, the control

room, the supplementary control room and other important locations at the plant, and with on-site and off-site emergency response organizations.

[23] Emergency response facilities are addressed in IAEA Safety Standards Series No. GSR Part 7, Preparedness and Response for a Nuclear or Radiological Emergency [13]. For nuclear power plants, emergency response facilities (which are separate from the control room and the supplementary control room) include the technical support centre, the operational support centre and the emergency centre."

A simplified flow chart, which presents the logic of defence in depth, is shown in Fig. 1. A success path is defined for each level of defence in depth. According to the philosophy of defence in depth, if the provisions of a given level of defence fail to control the evolution of an event sequence, the subsequent level of defence will come into play.

A deterministic approach to defence in depth does not explicitly consider the probabilities of occurrence of the challenges or mechanisms (an explanation of these terms will be further discussed in Section 3.1), nor does it include the quantification of the probabilities of success associated with the performance of features and systems for each level of defence. In NPPs, this deterministic approach is complemented by probabilistic safety analysis (PSA) considerations (e.g. safety goals, quantification of levels of defence in depth) to help demonstrate that the concept of defence in depth is met and is maintained for the entire lifetime of the plant. A plant specific PSA complying with the specific regulatory requirements, conformance to consensus standards and appropriate controls may be considered in the assessment of risk insights when complementing the deterministic safety analysis of the plant conforming to the concept of defence in depth.

2.2. FULFILMENT OF THE FUNDAMENTAL SAFETY FUNCTIONS

Fulfilment of the fundamental safety functions maintains the safety of an NPP by avoiding the failure of fission product barriers or by mitigating the consequences of a radioactive release in the case of a fission product barrier becoming compromised. In this context, Requirement 4 of SSR-2/1 (Rev. 1) [5] states:

"Fulfilment of the following fundamental safety functions for a nuclear power plant shall be ensured for all plant states: (i) control of reactivity; (ii) removal of heat from the reactor and from the fuel store; and (iii) confinement

of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases."

The fundamental safety functions are essential to the concept of defence in depth as a measure of the appropriate implementation of defence in depth through the related safety functions and safety provisions of the NPP, as indicated by the underlying relevant safety principles. The purpose of the defence in depth

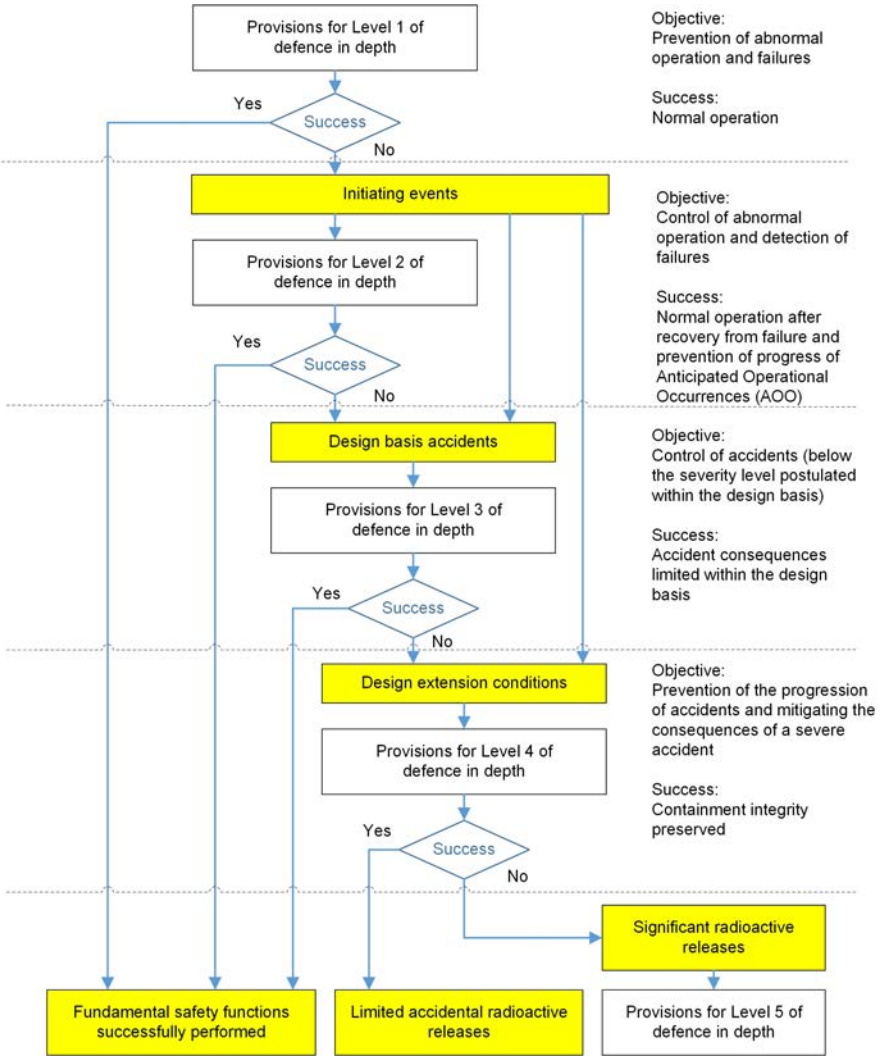

FIG. 1. Flow chart for the concept of defence in depth.

provisions is to protect the barriers and to mitigate the consequences if the barriers against the release of radioactive material are compromised.

Possible challenges to the fundamental safety functions are dealt with by the safety provisions established at a given level of defence in depth, which may include inherent safety characteristics, safety margins, active and passive systems, procedures, operator actions, organizational measures and safety culture aspects. Identification of all possible mechanisms that may result in challenges to the fulfilment of a fundamental safety function is performed for each level of defence in depth. These mechanisms are used to determine the set of initiating events (i.e. challenges to a fundamental safety function) that can lead to deviations from normal operation.

To facilitate structuring of the safety provisions, each of the fundamental safety functions is further subdivided into several derived or subsidiary safety functions. The subdivision of fundamental safety functions, as used in the framework of this methodology, is presented in more detail in Appendix I. The independent fulfilment of fundamental safety functions or derived safety functions at all levels of defence in depth underlies the concept of defence in depth. In addition, safety functions establish the conditions and limits for maintaining the integrity of the associated barriers against the release of radioactive material.

2.3. PRACTICAL ELIMINATION

The concept of practical elimination is recalled in para. 2.11 of SSR-2/1 (Rev. 1) [5], which states: "Plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated'…" This is an objective of the design, but as indicated in this paragraph, off-site protective measures might still be required by the responsible authorities. In relation to the concept of defence in depth, para. 2.13 of SSR-2/1 (Rev. 1) [5] also states: "Event sequences that would lead to an early radioactive release or a large radioactive release are required to be 'practically eliminated'."

With regard to design, 'practical elimination' is normally considered to refer only to those plant event sequences leading to or involving significant fuel degradation, such as a 'severe accident', for which the confinement of radioactive materials cannot be reasonably achieved. These plant event sequences have to be considered in the design for the implementation of the 'practical elimination' concept, either by demonstrating their physical impossibility or, with a high level of confidence, that they are extremely unlikely to occur by implementing safety provisions in the form of design and operational features.

IAEA Safety Standards Series No. SSG-88, Design Extension Conditions and Application Concept of Practical Elimination in the Design of Nuclear Power

Plants [12], provides recommendations on the implementation of the requirements in SSR-2/1 (Rev. 1) [5] that are related to the concept of defence in depth and the practical elimination of plant event sequences leading to early or large radioactive releases. The recommendations in relation to the concept of defence in depth are focused on design aspects, particularly on those aspects associated with DECs. This safety guide provides a high level safety assessment method related to these design aspects. The role of deterministic safety analyses in the demonstration of practical elimination is addressed in IAEA Safety Standards Series No. SSG-2 (Rev. 1), Deterministic Safety Analysis for Nuclear Power Plants [14].

Annex I of this publication provides a description of an approach to the demonstration of practical elimination that is based on the assessment of provisions that would generally include engineering judgement, deterministic safety analyses and PSAs.

3. APPROACH TO TAKING INVENTORY OF THE DEFENCE IN DEPTH CAPABILITIES OF A PLANT

3.1. DEFENCE IN DEPTH AND ACCIDENT MANAGEMENT

Paragraph 3.32 of SF-1 [2] states:

"Defence in depth is provided by an appropriate combination of:

- An effective management system with a strong management commitment to safety and a strong safety culture.
- Adequate site selection and the incorporation of good design and engineering features providing safety margins, diversity and redundancy, mainly by the use of:
  - Design, technology and materials of high quality and reliability;
  - Control, limiting and protection systems and surveillance features;
  - An appropriate combination of inherent and engineered safety features.
- Comprehensive operational procedures and practices as well as accident management procedures."

Paragraph 3.33 of SF-1 [2] states:

> "Accident management procedures must be developed in advance to provide the means for regaining control over a nuclear reactor core, nuclear chain reaction or other source of radiation in the event of a loss of control and for mitigating any harmful consequences."

3.2. DESCRIPTION OF THE ASSESSMENT APPROACH

This section describes the reference approach for examining the completeness and quality of implementation of the concept of defence in depth in a systematic way. The approach is based on the following basic assumptions:

- Safety is ensured by implementing safety provisions at all five levels of defence.
- Each of the levels is individually robust.
- Each level has its relevant safety objectives ensured by integrity of the relevant barriers.
- Fundamental safety functions and more detailed (derived) safety functions for maintaining the integrity of fission product barriers are identified.
- Safety functions can be challenged by different mechanisms affecting their performance.
- The safety provisions of different kinds are implemented to prevent mechanisms affecting the safety functions.
- Requirement 7 of SSR-2/1 (Rev. 1) [5], "The levels of defence in depth shall be independent as far as is practicable", is applied.

The identification of mechanisms that affect the performance of fundamental safety functions, as well as safety provision options for avoiding such an impact for each level of defence in depth, is an essential task in the development of the method framework for taking an inventory of the defence in depth capabilities of a plant. In developing the method framework, it is useful to summarize the following:

(a) Defence in depth involves multiple barriers against the release of radioactive material, as well as several levels of defence, including design, organizational and behavioural measures (provisions).
(b) Each level of defence in depth has specific objectives, including the protection of relevant barriers and the essential means of this protection. To ensure achievement of the objective of each level of defence in depth, all

fundamental safety functions (and derived or subsidiary safety functions) relevant to this level need to be performed.

(c) Challenges to the objectives are generalized mechanisms (groups of mechanisms), processes or circumstances (conditions) that may have an impact on the intended performance of safety functions. The nature of the challenge is characterized by the specific safety principle that contributes to the achievement of the objective through the performance of safety functions. Challenges are caused by groups of mechanisms having similar effects (consequences).

(d) Mechanisms are more specific processes or situations whose consequences might create challenges to the performance of safety functions.

For each mechanism, it is possible to identify a number of provisions, such as inherent plant safety characteristics, safety margins, system design features and operational measures, including human behaviour, that can support the performance of the safety functions and prevent the mechanism from taking place.

For each level of defence, a framework for taking an inventory of the defence in depth capabilities assesses all challenges and mechanisms and identifies possible provisions for achieving the objectives as indicated by the relevant safety principles.

The framework described above may be graphically depicted in terms of an objective tree, as shown in Fig. 2. At the top of the tree, there is the level of defence in depth that is of interest, followed by the objectives to be achieved, including the barriers to be protected against the release of radioactive material. Below this, there is a list of fundamental safety functions or derived safety functions that need to be maintained to achieve both the objectives and the protection of the barriers of the level of defence under consideration. For instance, the objective for Level 2 is to control abnormal operation and to detect failures as well as to ensure the continued integrity of the first three barriers (i.e. the fuel matrix, the fuel cladding and the pressure boundary of the RCS) through the performance of fundamental safety functions and derived safety functions. For Level 3, the objective is to control accidents within the design basis. For these accidents, it is required to limit damage to the first two barriers to avoid consequential damage to the pressure boundary of the RCS and any subsequent damage to the reactor containment.

The performance of fundamental safety functions and derived safety functions can be affected by challenges that are placed on a lower level (below the level of safety functions) in the objective tree. On the next lower level of the tree, several mechanisms are listed that can give rise to challenges. Under each of the mechanisms, there is a list of possible provisions that could be implemented in order to prevent the mechanisms from occurring and to prevent challenges to

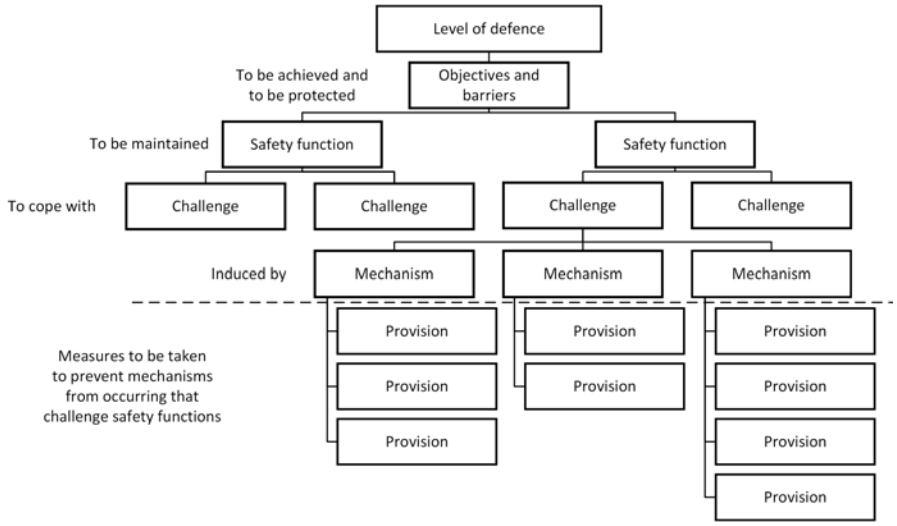

FIG. 2. Structure for defence in depth provisions at each level of defence.

the safety functions from arising. The list of provisions can be long, since there are many different approaches, and combinations of approaches, to preventing mechanisms from occurring. Not all of the provisions need to be implemented at the same time, since they may be interchangeable. The individual provisions can be further subdivided into smaller items or steps towards implementation, such as performing the analysis, organizing independent verification and ensuring compliance with the acceptance criteria.

The graphical depiction of links between safety objectives and safety provisions in the form of an objective tree helps to identify weaknesses in the implementation of the concept of defence in depth and supports the questioning attitude essential for nuclear safety. The method of using objective trees is understood not only as a comprehensive assessment tool for defence in depth, but also as a way of thinking about nuclear safety in very broad circumstances.

The following example, applicable to pressurized water reactors, may further illustrate the approach described above. One of the safety functions relevant for Levels 1–3 of defence in depth is the prevention of unacceptable reactivity transients. This safety function can be challenged by the insertion of positive reactivity. Several mechanisms may lead to such a challenge, including control rod ejection, spurious control rod withdrawal, control rod drop or misalignment, erroneous startup of a circulation loop, release of absorber deposits in the reactor core, incorrect refuelling operations or inadvertent boron dilution. For each of these mechanisms, a number of provisions may be made to

prevent its occurrence. For example, control rod withdrawal can be prevented, or its consequences mitigated, by the following provisions:

(a) Design margins minimizing the need for automatic control;
(b) An operating strategy with most of the control rods out of the core;
(c) Monitoring of the control rod position;
(d) Limited speed of control rod withdrawal;
(e) Limited worth of the control rod groups;
(f) A negative feedback reactivity coefficient;
(g) A reliable and fast safety shutdown system;
(h) Early detection of the positive reactivity insertion.

The main goal of the method presented in this publication is to take an inventory of the defence in depth capabilities (i.e. the safety provisions implemented) during any stage of the lifetime of the plant. Its essential attributes are therefore the completeness of the list of mechanisms, grouped into generalized challenges endangering the fulfilment of safety functions, and the sufficient comprehensiveness of the list of safety provisions aimed at preventing those mechanisms from taking place. Taking a top down approach, in other words, starting with the objectives of each level of defence and progressing down through the challenges and mechanisms to the provisions, is an appropriate way to develop the most comprehensive objective trees.

3.3. SPECIFICATIONS OF THE PROVISIONS

The defence in depth capabilities of a plant are established by means of the provisions that prevent mechanisms, or combinations of mechanisms, from occurring that might challenge the performance of the safety functions. The list of safety provisions can be drawn up as comprehensively as possible. A combination of IAEA Safety Standards, INSAG-12 [4] and expert judgement can be used to support an all-inclusive selection of the main challenges, mechanisms and provisions for each safety function to be performed. A graphical depiction of the elements of defence in depth and safety culture over the lifetime of a plant has been devised, as shown in Fig. 3, which was reproduced from INSAG-12 [4].

Across the horizontal axis of Fig. 3, the stages of the lifetime of a plant are listed, beginning with siting and design, continuing with construction and operation, and ending with plant decommissioning. (Decommissioning is beyond the scope of the present publication.) The levels of defence in depth are shown along the vertical axis of the figure. These levels begin at the top, with the first level involving the prevention of abnormal events, progressing through levels

devoted to recovery from abnormal events of increasing levels of severity and concluding with the level of defence aimed at mitigating the radiological consequences of the most severe and most unlikely accidents. In Fig. 3, the major features (elements) are listed that contribute to defence in depth during the NPP's lifetime. Each of the elements is representative of a specific safety principle discussed in detail in INSAG-12 [4]. The lines connecting the safety provisions indicate the interrelations among the principles.

The safety principles described in INSAG-12 [4] are commonly shared safety concepts that indicate how to achieve safety objectives at different levels of defence in depth. The safety provisions cannot guarantee that plants will be free of risk. Nonetheless, INSAG-12 [4] has stated that, if the principles are adequately applied, the defence in depth concept could be considered properly implemented. It is therefore considered that the safety provisions provide a reasonable basis for the comprehensiveness of the provisions. Since the publication of INSAG-12 [4], the safety provisions are fully reflected in the latest revision of the IAEA Safety Standards. In fact, the requirements and recommendations provided in the current standards go beyond the expectations of INSAG-12 [4] in several instances.

Figure 3 also indicates how to assign individual safety provisions to different levels of defence in depth. Assignment of safety provisions to a certain level of defence in depth means that non-compliance with such a safety principle can adversely affect achievement of the objectives, particularly for a given level.

The first step in assigning safety provisions to individual levels of defence is shown in Fig. 3. A preliminary assignment is carried out as a horizontal band selected from the safety provisions in Fig. 3, located within the boundaries of the different levels of defence. Of course, the complex nature of some of the principles cannot be fully reflected by a one dimensional projection of this kind. Furthermore, the boundaries of the levels are not strict, and some overlapping among levels exists. Similar boundary overlapping exists for different plant lifetime stages, such that compliance with safety provisions in each lifetime stage requires the given safety provision to maintain the implementation of safety provisions from the previous stage. Thus, some flexibility in assigning safety provisions to different levels of defence in depth is needed while maintaining the comprehensiveness of implementation.

The second step in the assignment of safety provisions is shown in Fig. 4, which is reproduced from INSAG-12 [4] and presents the physical barriers and levels of protection in defence in depth. The message conveyed by Fig. 4 is that any violation of general safety provisions, such as design management, quality assurance or safety culture, can adversely affect multiple levels of defence at the same time. Specific safety provisions that usually address the performance of various hardware components are typically assigned to different levels of defence.

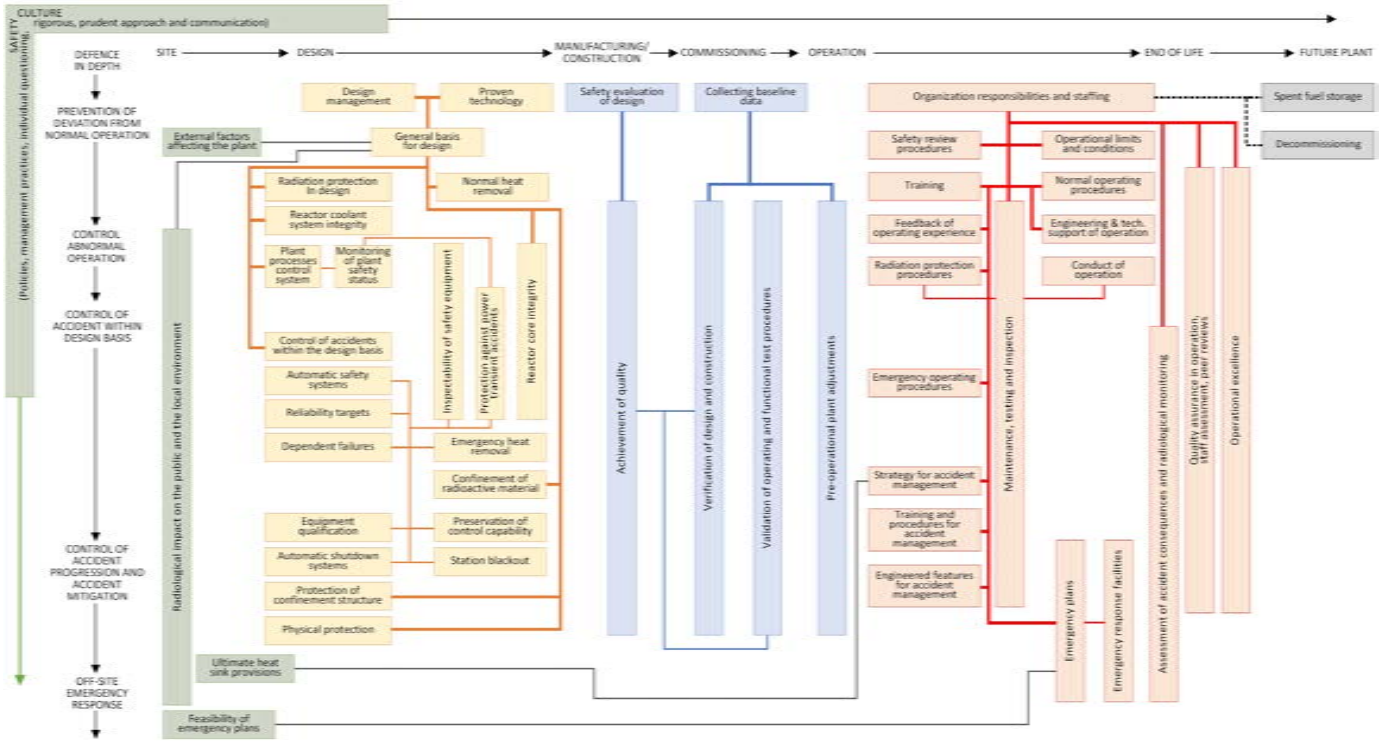

FIG. 3. Schematic presentation of the specific safety principles of INSAG-12, showing their coherence and their interrelations [4].

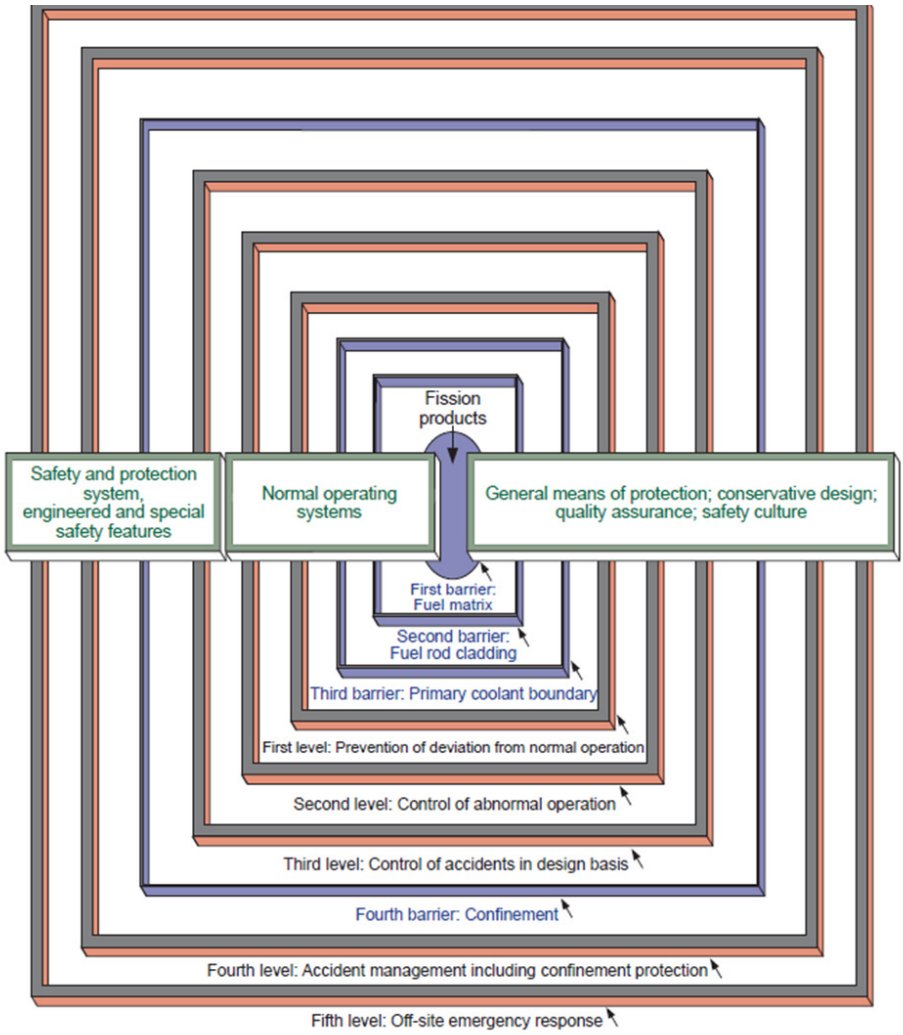

FIG. 4. The relationships between physical barriers and levels of protections in defence in depth [4].

The third step in the assignment of safety provisions to individual levels of defence is provided by the explanatory text on the safety provisions themselves in INSAG-12 [4] and the derived requirements for siting, design and operation in SSR-1 [6], SSR-2/1 (Rev. 1) [5] and SSR-2/2 (Rev. 1) [7].

The summary results of the assignment of the safety provisions are given in Table 2. The numbering of the safety provisions given in Table 2, as well as their grouping into siting, design, manufacture and construction, commissioning, operation, accident management and emergency preparedness, are taken directly from INSAG-12 [4]. However, the defence in depth level for each safety principle was partly revised based on the findings and lessons learned after INSAG-12 [4] was issued. Specifically, the defence in depth levels for safety principles 136, 168, 174, 177, 182, 217, 233, 240, 242, 265, 272, 284, 290, 296 and 339 in INSAG-12 [4] were revised.

It can be seen from Table 2 that many safety principles have a bearing on more than one level of defence. For example, 'achievement of quality' (SP249) has an impact across Levels 1–4, since it affects the reliability of all the engineering provisions that are in place to provide the defences at those levels.

The concept of defence in depth relies on a high degree of independence among the levels of defence in depth (see INSAG-10 [3] and SSR-2/1 (Rev. 1) [5]). In practice, however, some sort of interdependence among the levels of defence exists because of the pervading nature of several of the safety principles. Consequently, full independence of the levels of defence in depth cannot be achieved. This is due to several factors and constraints, such as a potential common exposure to the effects of external hazards or internal hazards, an unavoidable sharing of some items important to safety and human factors.

A robust independence among systems whose simultaneous failure would result in conditions having harmful effects on people and the environment is therefore essential. In this context, para. 4.13A of SSR-2/1 (Rev. 1) [5] states: "In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems." In addition, para. 5.29 (a) of SSR-2/1 (Rev. 1) [5] states (footnote omitted) that "features that are designed for use in, or that are capable of preventing or mitigating, events considered in the design extension conditions … shall be independent, to the extent practicable, of those used in more frequent accidents."

In some cases, the assignment of safety principles to levels of defence in depth in Table 2 reflects differences in current national practices. For instance, in some countries, normal operating procedures (SP288) cover both normal and abnormal operational modes. In other countries, abnormal operational modes are covered by emergency operating procedures (EOPs) (SP290); the same EOPs are

TABLE 2. ASSIGNMENT OF SAFETY PRINCIPLES (SPs) TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH [4]

Stage of the plant lifetime	No. of SP	Title of the SP	Levels of defence					No. of objective tree
			1	2	3	4	5	
Siting	136	External factors affecting the plant	●	●	●	●		1
	138	Radiological impact on the public and the local environment	●	●	●	●	●	2
	140	Feasibility of emergency plans					●	62
	142	Ultimate heat sink provisions	●	●	●	●		3
Design	150	Design management	●	●	●	●		4
	154	Proven technology	●	●	●	●		5
	158	General basis for design	●	●	●	●		6
	164	Plant process control systems	●	●				7, 8
	168	Automatic safety systems			●	●		9
	174	Reliability targets	●	●	●	●		10
	177	Dependent failures			●	●		11
	182	Equipment qualification			●	●		12
	186	Inspectability of safety equipment	●	●	●	●		13
	188	Radiation protection in design	●					14
	192	Protection against power transient accidents	●	●	●			15, 16
	195	Reactor core integrity	●	●	●			17, 18
	200	Automatic shutdown systems			●	●		19, 20

TABLE 2. ASSIGNMENT OF SAFETY PRINCIPLES (SPs) TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH [4] (cont.)

Stage of the plant lifetime	No. of SP	Title of the SP	Levels of defence					No. of objective tree
			1	2	3	4	5	
	203	Normal heat removal	●	●				21
	205	Startup, shutdown and low power operation	●	●	●	●		22
	207	Emergency heat removal			●	●		23, 24
	209	Reactor coolant system integrity	●	●				25
	217	Confinement of radioactive material		●	●	●		26, 27, 28
	221	Protection of confinement structure			●	●		29, 30
	227	Monitoring of plant safety status	●	●	●	●		31, 32
	230	Preservation of control capability	●	●	●	●		33
	233	Station blackout				●		34
	237	Control of accidents within the design basis			●			35
	240	New and spent fuel storage	●	●	●	●		36
	242	Plant physical protection	●	●	●	●		37
Manufacture and construction	246	Safety evaluation of design	●	●	●	●		38
	249	Achievement of quality	●	●	●	●		39
Commissioning	255	Verification of design and construction	●	●	●	●		40

TABLE 2. ASSIGNMENT OF SAFETY PRINCIPLES (SPs) TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH [4] (cont.)

Stage of the plant lifetime	No. of SP	Title of the SP	Levels of defence					No. of objective tree
			1	2	3	4	5	
	258	Validation of operating and functional test procedures	●	●	●	●		41
	260	Collecting baseline data	●	●	●	●		42
	262	Pre-operational plant adjustments	●	●	●	●		43
Operation	265	Organization, responsibilities and staffing	●	●	●	●		44
	269	Safety review procedures	●	●	●	●		45
	272	Conduct of operations	●	●	●	●		46, 47
	278	Training	●	●	●			48
	284	Operational limits and conditions	●					49
	288	Normal operating procedures	●					50
	290	Emergency operating procedures		●	●	●		51
	292	Radiation protection procedures	●	●	●	●		52
	296	Engineering and technical support of operations	●	●	●	●		53
	299	Feedback of operating experience	●	●	●	●		54
	305	Maintenance, testing and inspection	●	●	●	●		55
	312	Quality assurance in operation	●	●	●	●		56

TABLE 2. ASSIGNMENT OF SAFETY PRINCIPLES (SPs) TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH [4] (cont.)

Stage of the plant lifetime	No. of SP	Title of the SP	Levels of defence					No. of objective tree
			1	2	3	4	5	
Accident management	318	Strategy for accident management				●		57
	323	Training and procedures for accident management				●		58
	326	Engineered features for accident management				●		59
Emergency preparedness	333	Emergency plans				●	●	61, 62
	336	Emergency response facilities				●	●	60, 61
	339	Assessment of accident consequences and radiological monitoring				●	●	62

also applicable for accidents within the design basis and to some extent (before significant fuel degradation) for DECs, as well.

A certain amount of subjectivity in the assignment of safety provisions cannot be avoided. However, this subjectivity is not detrimental to the comprehensiveness of the objective trees, since safety provisions represent only one of various sources of information for the development of the approach.

Among the 53 safety principles assigned to the five levels of defence in Table 2, there are:

— Three exclusive to Level 1;
— Three common to Levels 1 and 2;
— Three common to Levels 1–3;
— One exclusive to Level 3;
— Twenty-six common to Levels 1–4;
— Two common to Levels 2–4;
— Six common to Levels 3 and 4;
— Four exclusive to Level 4;

— Three common to Levels 4 and 5;
— One common to Levels 1–5;
— One exclusive to Level 5.

3.4. OBJECTIVE TREES

The objective trees are presented in Appendix II for all levels of defence on the basis of the approach described in this publication. Annex II provides some additional guidance and clarification, in particular an explanation of the reason(s) for updating the objective trees.

The purpose of an objective tree is to provide a comprehensive list of the safety provisions that, when selected, will negate the associated mechanisms. Note that some safety provisions are individually capable of preventing the mechanisms from occurring, whereas others need to be complemented by additional safety provisions. This means that not all safety provisions associated with a given mechanism are implemented in parallel. Therefore, the insights offered by this approach could help determine at which level of defence in depth the safety provisions are required to be implemented, including any need for modified or additional provisions.

The provisions offered in the objective trees were mainly derived from the safety principles in INSAG-12 [4] and the IAEA Safety Standards, with considerations of additional engineering judgement based on internationally recognized safety practices. The various types of provisions include inherent plant safety features, systems, procedures, availability and training of personnel, safety management and safety culture measures. To provide reasonably practical support, the provisions are often formulated in technically more specific wording, compared with the general wording in the IAEA Safety Standards.

For safety principles that are common to multiple levels of defence, several ways of presenting the objective trees are used. If a substantial difference in the provisions for different levels is identified, a separate objective tree is developed for each respective level of defence in depth. Otherwise, the same objective tree can simply be used for each of the relevant levels of defence in depth. For such cases, the objectives and means at different levels of defence are different, and the same objective tree applies to different plant systems.

Even though the safety provisions and connected challenges and mechanisms are clearly linked to the levels of defence in depth in Table 2 and to the objective trees in Appendix II, the provisions for given mechanisms could be relevant only for some levels of defence in depth. A qualified decision needs to be made by the user when assessing the implementation of provisions.

In using the method, the impacts of mechanisms on the performance of safety functions are first analysed with adequate tools (e.g. deterministic safety analyses, PSAs, engineering judgement), even if this is not always explicitly expressed in the provisions. The evaluation of the importance, selection and implementation of an appropriate measure always needs to be based on the results of such an analysis.

4. USE OF THE METHOD

Users of the method presented in this publication are expected to review and compare provisions for defence in depth that are identified in the objective trees with the existing defence in depth capabilities of their plant.

The method for checking the comprehensiveness of defence in depth is applied in the reverse direction to the way in which the method is developed. That is, instead of the top down process used for the development of the objective trees, a bottom up process for assessing objective trees is used, including the following steps:

— Comparing the provisions in the objective trees with the provision capabilities of the plant;
— Judging the level of implementation of each provision;
— Considering whether implementation of another provision is needed in parallel with the given one to reach the intent of the provision;
— Considering optional provisions and judgement of whether the absence of a provision leads to a weakness in defence in depth;
— Judging whether a mechanism can be considered to be prevented from occurring;
— Judging whether a challenge can be considered to be prevented from affecting the fulfilment of a safety function.

The objective trees provide the rationale for the bottom up method, starting with the assessment of individual provisions. For each provision, the user will evaluate the level of its implementation. If the implementation of provisions is satisfactory, then the relevant mechanism can be considered to have been prevented from occurring. Deviations are discussed and justified either by compensatory features specific to the plant or by further provisions that conform to the concept of defence in depth for the plant.

This Safety Report is not intended to present stand-alone guidance. To obtain a full explanation of the provisions, it is necessary to consult the supporting publications compiled in the reference list. The method described in this Safety Report is flexible enough to allow its expansion to include additional specific provisions and mechanisms identified in national standards or relating to specific plant types. During the review, the operating organization (together with the regulatory body) needs to determine whether specific standards are mandatory or only optional; this is strongly dependent on the regulations of each State. It is the responsibility of the operating organization to select a proper set of provisions and to consider modified or additional provisions to avoid mechanisms that challenge safety functions, in order to ensure that the concept of defence in depth is met and the national regulations are fulfilled.

The method described in this Safety Report indicates, from a qualitative point of view, what kind of provisions can be implemented to avoid the occurrence of mechanisms that challenge safety functions. However, the method neither gives preference to individual provisions nor specifies the way to implement or quantify the efficiency of a provision. The user determines the adequacy of individual provisions. For the omission of a provision, a detailed justification is necessary. This method helps in identifying dependences of principles that might affect defences at more than one level and safety principles that are linked to each other. These dependences indicate for the reviewer where further attention is needed for the identification of the affected levels of defence in depth and where additional work is necessary to achieve independence among the different levels of defence in depth.

The proposed approach is deterministic in nature and can also be used for safety assessment of an NPP without a PSA. However, a plant specific PSA can be used to support the judgement on the adequacy of the defence in depth and the logical structure of the defences, provided that the PSA is sufficiently broad in scope, contains a sufficient level of detail and conforms with current regulatory requirements and consensus standards. In addition, PSA risk metrics could facilitate a better understanding of the interrelations among the various safety provisions and challenges.

Decisions on whether to implement a missing or incomplete provision require full consideration of the safety implications and priorities (e.g. within the framework of licensing activities, periodic safety reviews). It is the responsibility of the operating organization to set up a programme for the implementation of corrective measures in accordance with the national regulations and international standards. Apart from additional costs, the introduction of new equipment and programmes to implement an additional provision for defence in depth can also introduce additional complexity to the operation of a plant and additional potential failure modes. This approach does not consider the side effects of

increased complexity and operational difficulties caused by the implementation of additional defence in depth measures.

5. POTENTIAL APPLICATIONS

Defence in depth remains the essential strategy to ensure nuclear safety for both existing and new NPPs. The method presented in this publication offers a tool to facilitate the assessment of the comprehensiveness of defence in depth in a systematic manner. It has been developed with reliance upon the fundamental safety principles and the IAEA Safety Standards, which identify the most important measures (provisions) to be implemented to assure that the concept of defence in depth is met for NPP installations.

The applications experienced until now demonstrate that the screening method is based on a sound concept and can be effectively used by NPPs. The method helps to identify missing or weak provisions. Visualization in the form of objective trees supports understanding of the importance of individual provisions and the interrelations among provisions and mechanisms. Self-assessment review contributes to reviewers taking a questioning attitude, in accordance with the principles of safety culture. The updating of the method by incorporating current safety requirements and improving user friendliness provides a good basis for broader use of the method.

The method described in this Safety Report is the only currently known practical method enabling a user to perform a comprehensive screening, provide credible evidence of the defence in depth implementation at an NPP and formulate valid conclusions.

Based on lessons learned, the following applications of the method may be considered:

— Bottom up qualitative assessment of the availability of identified provisions in any specific NPP, combined with expert judgements of the sufficiency of provisions for preventing challenges to safety functions from taking place;
— Use of selected lists of provisions as reminders for the verification of availability of necessary measures in specific safety reviews, including different IAEA safety review missions;
— Verification of the comprehensiveness of safety assessment criteria in periodic safety reviews by comparing the criteria with the list of provisions identified in the objective trees;

— Assessment of the severity of deficiencies in safety levels identified in periodic safety reviews by indicating the challenges to performance of safety functions, the levels of defence in depth affected and the available provisions possibly compensating for the deficiencies;
— Identification of measures for safety upgrading of a given NPP to eliminate identified gaps;
— Demonstration of progress in the safety upgrading of a given NPP by increasing the number of implemented safety provisions (possibly illustrated by plots);
— Demonstration of a comprehensive consideration of defence in depth in the plant safety analysis reports;
— Use of the objective trees for training of NPP personnel to support their comprehensive consideration of the concept of defence in depth in day to day operations.

The method does not include any quantification of the level of defence in depth at a plant or any prioritization of the provisions of defence in depth. It is intended only for assessment, that is, for determining both the strengths and weaknesses for which the provisions have been considered. There are no strict criteria for what is considered a sufficient level of implementation of individual provisions. The level of detail and completeness of the evaluation is at the discretion of the user of the assessment approach.

Appendix I

FUNDAMENTAL SAFETY FUNCTIONS AND SAFETY FUNCTIONS

As mentioned in Section 2.2, safety functions are subdivisions of the fundamental safety functions, including those necessary to prevent accident conditions, or escalation of accident conditions, and those necessary to mitigate the consequences of accident conditions. They can be accomplished, as appropriate, using structures, systems and components (SSCs) provided for normal operation, those provided to prevent anticipated operational occurrences (AOOs) from leading to accident conditions, or those provided to mitigate the consequences of accident conditions, as well as with prepared personnel actions.

The following set of safety functions[3] has been identified as appropriate to develop the objective trees:

(a) Preventing unacceptable reactivity transients;
(b) Maintaining the reactor in a safe shutdown condition after all shutdown actions;
(c) Shutting down the reactor as necessary to prevent AOOs from leading to DBAs and to shut down the reactor to mitigate the consequences of DBAs;
(d) Maintaining sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant pressure boundary;
(e) Maintaining sufficient reactor coolant inventory for core cooling in and after all postulated initiating events considered in the design basis;
(f) Removing heat from the core[4] after a failure of the reactor coolant pressure boundary in order to limit fuel damage;
(g) Removing residual heat in appropriate operational states and accident conditions with the reactor coolant pressure boundary intact;
(h) Transferring heat from other safety systems to the ultimate heat sink (UHS);
(i) Ensuring necessary surveillance, maintenance and services (such as electrical, pneumatic, hydraulic power supplies, lubrication) as a support function for a safety system[5];

---

[3] There may be other possibilities for subdividing the fundamental safety functions, depending on the national regulations in States.

[4] This safety function applies to the first step of the heat removal system(s). The remaining steps are encompassed in safety function (8).

[5] This is a support function for other safety systems when they must perform their safety functions.

(j) Maintaining acceptable integrity of the cladding of the fuel in the reactor core;
(k) Maintaining the integrity of the reactor coolant pressure boundary;
(l) Limiting the release of radioactive material from the reactor containment in accident conditions and conditions following an accident;
(m) Limiting the radiation exposure of the public and site personnel in and following DBAs and DECs, including severe accidents that release radioactive materials from sources outside the reactor containment;
(n) Limiting the discharge or release of radioactive waste and airborne radioactive material to below prescribed limits in all operational states;
(o) Maintaining control of environmental conditions within the plant for the operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety;
(p) Maintaining control of radioactive releases from irradiated fuel transported or stored outside the RCS, but within the site, in all operational states;
(q) Removing decay heat from irradiated fuel stored outside the RCS but within the site;
(r) Maintaining sufficient subcriticality of fuel stored outside the RCS but within the site;
(s) Preventing the failure of, or limit the consequences of failure of, a SSC whose failure would cause the impairment of a safety function;
(t) Maintaining the integrity of the reactor containment in accident conditions and conditions following an accident;
(u) Limiting the effects of the release of radioactive materials on the public and the environment.

The set of safety functions can be grouped with respect to the fundamental safety functions (see Section 2.2) as follows:

— Safety functions related to fundamental safety function (i) “control of reactivity”: safety functions (1), (2), (3), (18).
— Safety functions related to fundamental safety function (ii) “removal of heat from the reactor and from the fuel store”: safety functions (4), (5), (6), (7), (8), (17).
— Safety functions related to fundamental safety function (iii) “confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases”: safety functions (10), (11), (12), (13), (14), (16), (20), (21).

There are also three special safety functions related to all three fundamental safety functions: safety functions (9), (15), (19).

The set of safety functions established in Safety Reports Series No. 46 was found to be adequate for the updated methodology, as well.

Established safety functions (with shorter versions of the text) and their grouping in accordance with the above descriptions are graphically depicted in Fig. 5.

FIG. 5. Overview and grouping of safety functions used in the present report (SF: safety function; FSF: fundamental safety function; LOCA: loss of coolant accident).

Appendix II

CONTENT OF THE ONLINE SUPPLEMENTARY FILE

Appendix II is available as an online supplementary file on the publication's individual web page at https://doi.org/10.61092/iaea.dbwn-89a9.

Appendix II provides a full set of objective trees (shown in objective trees 1−62) for the purpose of practical assessment of the defence in depth capabilities of NPPs.

The objective trees in Appendix II graphically represent how, for each relevant SP, the safety objectives of the different levels of defence can be achieved by establishing defence in depth provisions at different stages of the plant lifetime. Each of the captions to the objective trees indicates the levels of defence, to which the provisions contribute to fulfilling the objectives. Next in the caption, the corresponding safety principles are given as a commonly shared safety concept, stating how the safety objectives at relevant levels of defence can be achieved. Each objective tree itself starts with an indication of the fundamental safety functions to be performed in order to achieve the objectives for the given safety principles; it is then followed by the challenges that might have an impact on the performance of safety functions and the mechanisms leading to individual challenges and finally by a list of the provisions to be implemented to avoid occurrence of the mechanisms. Annex II provides explanatory text for each objective tree and references to relevant IAEA Safety Standards.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary, Non-serial Publications, IAEA, Vienna (2022), https://doi.org/10.61092/iaea.rrxi-t56z

[2] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006), https://doi.org/10.61092/iaea.hmxn-vw0a

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG Series No. 10, IAEA, Vienna (1996).

[4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev.1, INSAG Series No. 12, IAEA, Vienna (1999).

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

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Installations, IAEA Safety Standards Series No. SSR-1, IAEA, Vienna (2019).

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

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, Action Plan on Nuclear Safety Series, IAEA, Vienna (2014).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, Action Plan on Nuclear Safety Series, IAEA, Vienna (2012).

[10] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, WENRA Safety Reference Levels for Existing Reactors — Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident, WENRA (2014).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016), https://doi.org/10.61092/iaea.cq1k-j5z3

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Extension Conditions and Application the Concept of Practical Elimination in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-88, IAEA, Vienna (2024), https://doi.org/10.61092/iaea.la1m-dy8m

[13] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015), https://doi.org/10.61092/iaea.3dbe-055p

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2 (Rev. 1), IAEA, Vienna (2019).

Annex I

APPROACH TO DEMONSTRATION OF PRACTICAL ELIMINATION OF PLANT EVENT SEQUENCES LEADING TO EARLY OR LARGE RADIOACTIVE RELEASES

This annex provides a description of an approach to the demonstration of 'practical elimination' that is based on the assessment of provisions using engineering judgement, deterministic safety analyses and probabilistic safety analyses (PSAs). A description of the concept of practical elimination involves only those events or sequences of events leading to or involving significant fuel degradation, that is, a 'severe accident', for which the confinement of radioactive materials cannot be reasonably achieved. These plant event sequences have to be considered in the design for practical elimination, which should either make them physically impossible or extremely unlikely to occur with a high level of confidence.

Paragraph 7.70 of IAEA Safety Standards Series No. SSG-2 (Rev. 1) [I–1] provides guidance on demonstrating practical elimination:

> "Demonstration of 'practical elimination' of the possibility of conditions arising that could lead to an early radioactive release or a large radioactive release should include, where appropriate, the following steps:
>
> (a) Identification of conditions that potentially endanger the integrity of the containment or allow bypassing of the containment, resulting in an early radioactive release or a large radioactive release.
> (b) Implementation of design and operational provisions in order to 'practically eliminate' the possibility of those conditions arising. The design of these provisions should include sufficient margins to cope with uncertainties.
> (c) Final confirmation of the adequacy of the provisions by deterministic safety analysis, complemented by probabilistic safety assessment and engineering judgement."

More comprehensively, IAEA Safety Standards Series SSG-88 [I–2] provides guidance on how to demonstrate the practical elimination of plant event sequences leading to an early or large radioactive release; this guidance was used as a basis for the approach described below. For each plant event sequence considered for practical elimination, an assessment is performed to demonstrate the acceptability of the design or to define additional design provisions to be

implemented. A demonstration is provided that it is physically impossible for the condition to arise, or that the condition is considered extremely unlikely to occur with a high level of confidence.

To help ensure that the demonstration of practical elimination is manageable[1], the whole set of individual plant event sequences that might lead to unacceptable radiological consequences should be grouped to form a limited number of bounding cases or types of accident condition. The following five general types of plant event sequence should be considered, depending on their applicability for specific designs [footnotes omitted]:

(a) Plant event sequences that could lead to prompt reactor core damage and consequent early containment failure, such as the following:
    (i) Failure of a large pressure retaining component in the reactor coolant system (RCS);
    (ii) Uncontrolled reactivity accidents.
(b) Plant event sequences that could lead to early containment failure, such as the following:
    (i) Highly energetic direct containment heating;
    (ii) Large steam explosion;
    (iii) Explosion of combustible gases, including hydrogen and carbon monoxide.
(c) Plant event sequences that could lead to late containment failure[2], such as the following:
    (i) Basemat penetration or other damage to the integrity of the containment during molten corium–concrete interaction;
    (ii) Long term loss of containment heat removal (e.g. failure of the containment heat removal system);
    (iii) Explosion of combustible gases, including hydrogen and carbon monoxide.
(d) Plant event sequences with containment bypass, such as the following:
    (i) A loss of coolant accident (LOCA) with the potential to drive the leakage outside of the containment via supporting systems (i.e. a LOCA in an interface system);
    (ii) Plant event sequences producing a consequential containment bypass (e.g. an induced steam generator tube rupture);

---

[1] There are no specific objective trees on the assessment of practical elimination.

[2] These conditions need to be analysed during the identification of situations to be practically eliminated. Nevertheless, consequences associated with the first two points of (c) could generally be mitigated with the implementation of reasonable technical means.

(iii) Plant event sequences with core melt, which include spent fuel pool sequences for plants that have a spent fuel pool located inside the containment, and in which the containment is open[3] (e.g. in the shutdown state).

(e) Significant fuel degradation in a spent fuel pool[4].

The practical elimination from consideration of plant event sequences that could lead to large or early releases has to be demonstrated by deterministic considerations supported by probabilistic considerations, considering the uncertainties due to limited knowledge of some physical phenomena. It is a decision of the regulatory body to establish what are or are not acceptable targets to support the demonstration of practical elimination [I–2].

All plant locations and buildings where nuclear fuel is stored are considered in the identification process, including the irradiated fuel storage.

It may be useful to classify accident scenarios, taking into account the progression of an initiating event and the resulting consequences that need to be avoided. Three types of scenario can be considered:

— Type I: Scenarios with an initiating event that leads directly to severe fuel damage and early failure of the confinement function.
— Type II: Severe accident scenarios with phenomena that induce early failure of the confinement function.
— Type III: Severe accident scenarios that result in late failure of the confinement function.

The approach to the demonstration of practical elimination could consist of the following steps:

---

[3] Currently, the technology used for equipment hatches is generally not fast enough to ensure reclosure and restoration of the containment integrity. Therefore, any significant, rapid fuel degradation mechanism in shutdown operating modes with an open containment needs to be considered for practical elimination.

[4] Most plant designs used in various States locate the spent fuel pool outside of the containment, given the slow kinetics of accidents likely to lead to severe damage of the fuel assemblies stored in the spent fuel pool. The timescales enable the implementation of on-site or off-site prevention or protective measures. This option is considered to be the best choice in the decision making process compared with the additional costs and operational constraints of locating the spent fuel pool in the reactor building. However, this does mean that any occurrence of significant fuel degradation in the pool would directly lead to a large radioactive release. Therefore, any plant event sequence with significant degradation of the fuel assemblies stored in the spent fuel pool needs to be considered for practical elimination.

— Step 1: Identification of the conditions (challenges) to be practically eliminated.
— Step 2: Whenever possible, demonstration of practical elimination based on physical impossibility according to the laws of nature.
— Step 3: Identification and implementation of design provisions for prevention of the challenges.
— Step 4: Identification and implementation of operational provisions (procedures) for prevention of the challenges.
— Step 5: Deterministic safety analysis and engineering judgement of the effectiveness of the provisions.
— Step 6: Whenever appropriate and feasible, PSA showing a very low probability of failure of the implemented design and operational provisions.

Where a claim is made that a condition that needs to be practically eliminated is physically impossible, it is necessary to demonstrate that the inherent safety characteristics of the system or reactor type ensure that the condition, by the laws of nature, cannot occur and that the fundamental safety functions (see Requirement 4 of IAEA Safety Standards Series No. SSR-2/1 (Rev. 1) [I–3]) are fulfilled.

Where a claim is made that a condition that needs to be practically eliminated is extremely unlikely to arise, it is necessary to demonstrate this with a high level of confidence. Although probabilistic targets can be set (e.g. frequencies of core damage or radioactive releases), the demonstration of practical elimination cannot only be approached probabilistically. Insights gained from PSA need to be used to support deterministic safety analyses and engineering judgement for the demonstration of practical elimination. Also, meeting a probabilistic target alone is not a justification to exclude the analysis and possible implementation of additional reasonable design or operational measures to reduce the risk. Thus, a low probability of occurrence of a plant event sequence with core damage is not a reason for not protecting the containment against the conditions generated by such a plant event sequence. In fact, design extension conditions (DECs) with core melting need to be postulated in the design, in accordance with Requirement 20 of SSR-2/1 (Rev. 1) [I–3].

It is also noted that the concept of practical elimination applies to plant event sequences of internal origin; in the case of external hazards, the concept of adequate margins is used.

Table I–1 presents examples of design and operational measures available to minimize the likelihood of conditions that could lead to early or large radioactive releases.

TABLE I–1. EXAMPLES OF DESIGN AND OPERATIONAL MEASURES FOR PRACTICAL ELIMINATION OF EARLY OR LARGE RADIOACTIVE RELEASES

Challenge	Mechanism	Design and operational measures to prevent the mechanisms
Prompt reactor core damage and consequent early containment failure	Failure of a large component in the RCS	• Most suitable composition of materials selected • Metal component or structure as defect free as possible • Metal component or structure tolerant of defects • Mechanisms of growth of defects known • Design provisions and suitable operation practices in place to minimize thermal fatigue, stress corrosion, embrittlement, pressurized thermal shock, overpressurization • Effective in-service inspection and surveillance programme in place during manufacturing and operation
	Uncontrolled reactivity accidents	• Identification of situations leading to fast insertion of reactivity • Analysis of challenges and consequences for fast reactivity insertions • Core design ensuring subcriticality under any plant conditions • Effective fast shutdown systems • Procedures to prevent potentially risky operating modes
Severe accident phenomena that could lead to early containment failure	Core meltdown at high pressure (direct containment heating)	• Reliable means to ensure opening of existing depressurization (relief, safety) valves of the RCS • Diverse system to depressurize the RCS • Additional barriers to minimize corium dispersion (e.g. ledges, walls or indirect paths)
	Large steam explosion	• Using dry cavity • Adjustment of timing of cavity/drywell flooding • In-vessel retention by external reactor pressure vessel (RPV) cooling • In-vessel retention by internal RPV flooding • Decoupling of reactor cavity from containment envelope • Provisions for releasing steam from the cavity • Increased temperature of coolant for cavity flooding

TABLE I–1. EXAMPLES OF DESIGN AND OPERATIONAL MEASURES FOR PRACTICAL ELIMINATION OF EARLY OR LARGE RADIOACTIVE RELEASES (cont.)

Challenge	Mechanism	Design and operational measures to prevent the mechanisms
Severe accident phenomena that could lead to early containment failure (cont.)	Hydrogen explosion	• Large containment volume • Installation of igniters and/or recombiners • Containment inertization by nitrogen (permanently) or steam (temporarily) • Mixing of containment atmosphere • Filtered venting to reduce pre-burning pressure and number of gases
	Containment boundary melt through	• Flooding of reactor cavity or drywell • Additional barrier against corium for cavity doors and sumps, etc., to maintain corium cooling • In-vessel retention by external RPV cooling • In-vessel retention by internal RPV flooding • Insulator layers to eliminate or delay interaction • Corium spreading on cooled large area or core catcher
	Slow overpressurization of containment	• Large thermal capacity of the containment • Installation of adequately robust internal spray system • Installation of external spray system • Installation of adequately robust fan cooler system • Installation of sump cooling system • Installation of suppression pool cooling system • Installation of any other containment heat removal system • Installation of igniters and/or recombiners • Installation of filtered venting system
	Containment failure due to fast overpressurization or mechanical damage due to vessel failure	• Ensure dry cavity at the time of RPV breach, with measures to prevent molten core–concrete interaction • In-vessel retention by external RPV cooling • In-vessel retention by internal RPV flooding • Adequate steam flow path from the cavity • Verification and strengthening of cavity bottom, if necessary

TABLE I–1. EXAMPLES OF DESIGN AND OPERATIONAL MEASURES FOR PRACTICAL ELIMINATION OF EARLY OR LARGE RADIOACTIVE RELEASES (cont.)

Challenge	Mechanism	Design and operational measures to prevent the mechanisms
Non-confined severe fuel damage	Severe accident with containment bypass through damaged steam generator or through interface system	• Prevention of interface system LOCA • Depressurization of the RCS • Identification of bypass route and possibilities for fission products retention • Development and application of primary to secondary leak management • Ensuring steam generator tubes flooded by secondary coolant
	Significant fuel failure in a storage pool	• Pool structure designed against all conceivable internal and external hazards that could damage its integrity • Avoiding siphoning of water out of the pool • Redundant lines for pool cooling that eliminate possibility of long lasting loss of cooling function • Reliable instrumentation for pool level monitoring • Appropriate reliable means to compensate for any losses of water inventory (e.g. spent fuel pool flooding from an external source)

REFERENCES TO ANNEX I

[I–1] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2 (Rev. 1), IAEA, Vienna (2019).

[I–2] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Extension Conditions and Application the Concept of Practical Elimination in the Design of Nuclear Power Plants, IAEA Safety Standards Series No. SSG-88, IAEA, Vienna (2024), https://doi.org/10.61092/iaea.la1m-dy8m

[I–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev. 1), IAEA, Vienna (2016).

Annex II

EXPLANATION AND JUSTIFICATION OF MODIFICATIONS OF OBJECTIVE TREES

This annex is intended to provide additional description of individual objective trees included in this Safety Report. Although the objective trees are intended to be self-explanatory to the extent possible, the explanatory text may help in understanding the scope and structure of individual objective trees and the interrelations among them. The following paragraphs may facilitate understanding of the structure of the objective trees and their usage.

Performing an evaluation by using the objective trees method ensures comprehensiveness of the evaluation, such that no aspect of defence in depth is omitted or ignored. The objective trees provide a comprehensive list of mechanisms that can cause non-performance of safety functions at different levels of defence and thus lead to the non-achievement of the safety goal, which is to protect people and the environment from harmful effects of exposure to ionizing radiation. For each mechanism, the objective trees contain a summary of possible measures (provisions) which, individually or jointly, can prevent the occurrence of the given mechanism. Although the aim in constructing the objective trees was to make the list of provisions as broad as possible (e.g. by using the IAEA Safety Standards, various technical guidance documents and professional experience), the list of provisions cannot be considered definitive.

The aim of the method is to show, on the basis of the IAEA Safety Standards or engineering judgement, what could be done to prevent the occurrence of a mechanism and what types of provisions can be considered to prevent the mechanism. The method does not stipulate the obligation to implement all provisions in parallel; one provision omitted or insufficiently implemented can be compensated, or even replaced, by other provisions. What is needed in the absence of a provision is a justification for accepting this fact. The method does not set priorities in the implementation of individual provisions, nor does it specify the method of implementation or quantify the effectiveness of the provision. The adequacy and sufficiency of the provisions has to be determined by the evaluator using his or her expert knowledge.

When constructing the objective trees, one of the principles is to assign to each of the mechanisms its own set of prevention provisions. In many cases, the same or similar provisions can contribute to preventing several mechanisms. This approach means that some of the provisions can be repeated in several places in the objective trees. Depending on other circumstances, the evaluation of

such provisions needs to be repeated in some cases or can be limited just to one single evaluation.

The provisions included in the objective trees can be of very different natures, and encompass organizational, behavioural and design measures, including properly selected site characteristics, inherent safety features, safety margins, active and passive systems, operating procedures and operator actions, more general organizational measures and safety culture aspects. Some provisions may require performing various kinds of assessments, including deterministic safety analyses or PSAs. In such cases, the provision becomes one of the successive steps in implementation rather than being the specific measure itself. The provisions are formulated in situations when the assessment or analysis is an important component in deciding whether and what kind of provisions would fit the given objective.

The evaluations focus on verification of whether the group of provisions associated with the given mechanism sufficiently excludes the application of that mechanism. It is therefore important that the individual provisions associated with one mechanism are evaluated as a group, respecting their relationships to other provisions that are relevant to a given mechanism. The use of a graphical interpretation of the links between mechanisms and provisions in the form of objective trees is intended to make the links between the individual elements of defence in depth more visible.

The basis for the subdivision of items into different objective trees was the set of safety principles included in INSAG-12 [II–1], and the name of the corresponding safety principle is indicated in the title of the objective tree. In addition to INSAG-12 [II–1], each objective tree includes reference to safety principles, as well as references to overarching safety requirements from the IAEA Safety Standards.

Each objective tree contains an explanatory text, which briefly describes the following information:

— Area: allocation of the objective tree to the plant lifetime (e.g. siting, design, operation);
— SP number: number of the relevant safety principle in INSAG-12 [II–1];
— SP text: title of the relevant safety principle;
— Defence in depth level: applicable level(s) of defence in depth;
— Objective tree number: ordinal number of the objective tree;
— Map: number of the objective tree followed by ordinal number of the mechanism in this objective tree (navigation of the mechanism in the whole system);
— Challenge text: text on the challenge to the performance of the safety functions;

— Mechanism number: ordinal number of the mechanism (counting started from the first objective tree);
— Mechanism text: text on the mechanism to the performance of the safety functions;
— Fundamental safety functions: fundamental safety function(s) affected;
— Safety functions: derived safety function(s) affected (only used if it is possible to differentiate them from the fundamental safety functions);
— Provision *i*: text on the *i*th provision to prevent the given mechanism from taking place; the ordinal number of the provision is no indication of the importance or priority of its implementation.

Objective tree 1. External factors affecting the plant (SP136)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 14, 16, 17, 30.

This objective tree includes the items (i.e. challenges, mechanisms, provisions) that are relevant for siting and may potentially affect the nuclear power plant (NPP), such as natural hazards and human hazards. Malevolent human actions are not considered site specific mechanisms. Such malevolent actions are covered by objective tree 37, under two relevant mechanisms: 'lack of vigilance' and 'design vulnerabilities to potential threats', where malevolent action is considered as one of the threats. In the objective tree, provisions are formulated individually for each mechanism. In addition to specific mechanisms dealing with specific hazards (such as earthquakes or fires), there are two general mechanisms intended to cover the remaining, not specifically listed hazards: one for natural and the other for human induced external hazards. There is also one general mechanism devoted to the comprehensive identification of natural hazards relevant for the given site. Not only individual natural hazards, but also their meaningful combinations, are considered in one of the mechanisms and associated provisions. A specific mechanism is devoted to potential interactions between the grid and the plant.

This objective tree deals with the site characteristics and not with the capabilities of the structures, systems and components (SSCs) to cope with the site induced loads. The assessment of the capabilities of SSCs is part of the design. When it is necessary to specify the margins for design of selected SSCs, this relates to the increased site specific loads for which the SSCs are required to function in order to prevent early or large radioactive releases. The provisions associated with siting also include the evaluation of feasibility of compensatory design or operational measures. Examples of such compensatory measures include cleaning sewage inlets, removing snow layers and preventing water from entering electric cabinets by temporary sealing. Examples of compensatory

measures for earthquakes can be dampers, strengthened structures, seismic monitoring and early shutdown of the reactor. It is recognized that the terms 'adequate margin' and 'sufficient margin' need to be used with care. An adequate margin is understood as a more substantial, larger margin necessary in the case of large uncertainties, like those associated with external hazards.

Objective tree 1 covers the determination of external hazards specific to the given site, their frequencies and intensities, and adequate margins depending on the level of uncertainty for the given hazard (including periodic reassessment of the site characteristics). Consideration of the site characteristics in the design of the plant is the subject of objective tree 11.

Objective tree 1 introduces the phrase "SSCs ultimately needed to prevent early or large radioactive releases". These are the SSCs necessary to mitigate the consequences of severe accidents with core melt. The design of these SSCs is expected to be particularly robust and to include margins to withstand loads and conditions generated by natural external hazards exceeding those derived from the site evaluation. A list of these SSCs is design dependent; however, in general the list includes at least (i) the containment structure; (ii) systems necessary to contain the molten core and to remove heat from the containment; (iii) systems to transfer the heat to the ultimate heat sink (UHS) in severe accident conditions; (iv) systems to prevent hydrogen detonations; (v) alternative power supplies (alternative to the emergency power supply); (vi) instrumentation and control systems to allow the functionality of the systems above; and (vii) control rooms.

Objective tree 2. Radiological impact on the public and the local environment (SP138)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 5, 13, 19, 20, 34, 67, 82.

In this objective tree, there are two groups of mechanisms, each consisting of three mechanisms and relevant for site characteristics. The first group of provisions is related to site characteristics important for the transport of radioactive materials via different exposure pathways. The second group of provisions is related to the determination or limitation of the radiological impact of different plant states, which is specified differently for Levels 1 to 2, for Level 3 and DEC-A (design extension conditions (DECs) without significant fuel degradation), and for severe accidents. For the second group of mechanisms, three different levels were put in one objective tree just because they were sufficiently simple to be placed in a single figure. Otherwise, the provisions for dissemination of radioactive materials differ for different levels of defence in depth because of the fact that the acceptance (dose) criteria, as well as the

methods for determination of radiological consequences (conservative versus best estimate), are different.

The first group of mechanisms, common to all levels of defence, is dealing with different pathways for the release of radioactive materials into the environment. Specific sets of provisions were developed for each of the three release pathways, air, water and food chain, with distinguishing provisions for different mechanisms. The other three mechanisms deal with site characteristics affecting the determination of the radiological effects of normal and abnormal plant operation, of design basis accidents (DBAs) together with DEC-A and of DEC-B (DECs with core melting, i.e. severe accidents) on people and the environment. Since site characteristics for different plant states can be generally considered in a different way, specific sets of provisions are developed for different plant states.

It is recognized that acceptable doses for the public have not been established as radiological acceptance criteria for DECs (and in particular for severe accidents with core melting) in all States. Although there is some flexibility in the way the criteria are defined (besides the dose, there can be also other methods of limitation, e.g. acceptable releases for some radioisotopes), the availability of some criteria, such as for severe accidents, is quite essential for safety analysis in accordance with the IAEA Safety Standards. If such criteria are not established by the regulatory body, it is up to the designer (or the operating organization) to set its own radiological targets. Radiation monitoring outside the plant buildings could also be included in this objective tree. Given that it is not so strongly dependent on the site characteristics, radiation monitoring for operational states is covered by objective tree 14 (partly also by objective tree 52) and for accident conditions by objective trees 60, 61 and 62.

Objective tree 3. Availability of UHS (SP142)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 53.

This objective tree contains only mechanisms belonging to two different stages in the lifetime of the plant, namely siting and design. The first mechanism addresses the potential loss of heat transport from the fuel to the UHS due to non-availability of the UHS itself, and the other three mechanisms (belonging to the plant design) address the potential loss of heat transport due to vulnerability of the heat transport system (HTS) to the UHS. This combination of lifetime stages reflects the fact that in INSAG-12 [II–1], the description of SP142 is also a mixture of siting and design related issues.

The effects of external hazards on damaging mechanisms acting on the UHS itself were considered, as well as damaging mechanisms acting on the HTS to the UHS. In the construction of this objective tree, the boundary considered between

the UHS and HTS is the coolant of the UHS and the coolant of the essential service water system, which means that the HTS starts with the essential service water system. As the UHS, two different options (the atmosphere or a large body of water such as the sea) were considered, although it was clear that only one of the options is normally used in many cases. As far as the vulnerability of the HTS is concerned, three mechanisms were identified, related to (i) the reliability of the system; (ii) the capacity of the system for most adverse conditions; and (iii) the vulnerability of the system to external hazards, including those beyond the design basis events. The mechanisms dealing with heat transfer phenomena in the HTS (evaporation, temperature increase) are addressed in the evaluation of the capacity of the systems. Since a great deal of discussion is usually devoted to the correct consideration of various provisions, it is underlined that the provisions are to be understood as options, not necessarily to be implemented in parallel.

The UHS, including the HTS to the UHS, belongs to the SSCs necessary for practical elimination of plant event sequences leading to early or large radioactive releases. Therefore, increased robustness of these SSCs is required to withstand external hazards more severe than those considered for design, derived from the hazard evaluation for the site. If the evaluation of existing means results in insufficient margins to such events, either the SSCs can be strengthened or diverse means for heat removal (e.g. cooling towers, cooling ponds) can be added to the existing means. However, the issue cannot be solved by redundancies, unless another redundancy is designed as diverse.

The IAEA Safety Standards do not prescribe what is a sufficient amount of coolant to be stored on the site.[1] The objective is to have enough coolant to ensure the heat removal function, with the possibility to refill the reserves. Diverse water sources may be considered, such as backup wells, nearby lakes or dams with transport capabilities, water distribution systems or robust underground tanks.

The list of provisions aimed at enhancing the reliability of the HTS function includes two provisions that seem to contradict each other: (i) interconnections among redundant trains with isolation capability, and (ii) enhancement of functional and physical separation among redundant trains. The separation of redundant trains is applicable for Level 3, whereas interconnections can be used for Level 4 (as indicated in the boxes of provisions). Provisions included in this objective tree are in general applicable for Levels 1 to 4 of defence (e.g. removal of decay heat from the fuel is ensured in all plant states). Nevertheless, some means for heat removal (i.e. feed and bleed from the reactor coolant system (RCS), heat removal from the containment by venting or dedicated spraying) are relevant only for DECs, as indicated in the boxes with these provisions.

---

[1] In some countries, the regulatory body specifies that the amount of coolant to be stored on the site needs to be sufficient for 30 days.

Objective tree 4. Design management (SP150)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 1, 2, 6, 9.

This objective tree deals with the overall control of the design process (management), understanding that this control is important for both the initial design of the plant and any subsequent design modifications. Levels 1 to 4 of the defence in depth can be affected by the design process, in the sense that the design influences the functional capability of all items important to safety, belonging to different levels of defence. The final objective of provisions in this objective tree is to prevent a potential degradation of the functional capability of items important to safety due to deficiencies in the design process. To the extent possible, the operating organization has to keep control over the process, although for some internal processes in the design organization, this control is performed indirectly. The mechanisms and associated provisions in this objective tree cover internal conditions in the design organization (qualification of the personnel, coordination of different groups, strong quality assurance), as well as maintaining the design integrity of the operating organization itself by establishing a special organizational unit with that responsibility. The objective tree is intended to be more specific in indicating the responsibility of the operating organization and less specific in the provisions devoted to activities in the design organization (the main provisions related to the design organization are still listed). It is assumed that the implementation of provisions related to the design organization will be ensured by the operating organization as the contractual obligation of the designer.

Objective tree 5. Proven technology (SP154)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 3, 9, 18.

Using proven technology, covered by this objective tree, has a large role in reinforcing confidence that items important to safety have been designed, tested, verified and qualified sufficiently for their intended function(s), in accordance with established and relevant national and international codes and standards, laws and regulations. More specifically, paras 4.14−4.16 of SSR-2/1 (Rev. 1) require the following for items important to safety:

— They are preferably of a design that has previously been proven in equivalent applications;
— They are of high quality and of a technology that has been qualified and tested;
— National and international codes and standards are applicable;

— For unproven designs, safety is demonstrated by appropriate research programmes and performance tests with specific acceptance criteria;
— Operating experience from other relevant applications is examined to support the design;
— A new design or new practice is adequately tested before being brought into service and is monitored in service to verify that the behaviour of the plant is as expected.

Among the provisions to comply with the expectations, in addition to hardware orientated provisions there are also possibilities for using analytical demonstration of the functional capability. The provisions recommended in this objective tree are intended to prevent an unexpected degradation of the functional capability of items important to safety by considering mechanisms causing:

— Unanticipated behaviour of the plant under normal or abnormal conditions;
— Undetectable failures of items important to safety;
— Unanticipated failure modes of items important to safety;
— Unanticipated limitations on the performance of the engineered safety features;
— Unanticipated degradation of the barriers.

When the codes and standards are properly selected, the items important to safety are generally considered to be of proven design, except in the case of using innovative design solutions.

Objective tree 6. General basis for design (SP158)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 6, 13, 14.

This objective tree is intended to summarize the provisions aimed at specification of the plant design basis or design envelope. Four kinds of challenges are considered:

— Inadequate design basis for normal operation;
— Inadequate design basis for internal and external hazards;
— Inadequate design basis for anticipated operational occurrences (AOOs) and accident conditions;
— Inadequate performance of items important to safety.

The challenges and mechanisms address the adequate specification of all plant states and hazard conditions (first three bullets), as well as adequate design

of items important to safety to function reliably under all conditions covered by the design. In this objective tree, the meaning of the term 'design basis' is the same as 'design envelope', which has been introduced recently in the IAEA Safety Standards. In accordance with IAEA-TECDOC-1791, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants [II–3], both terms mean a set of initiating events, internal and external hazards, as well as other conditions to be considered in the plant design. The features to enable the safe use of non-permanent equipment are considered to be part of the plant design envelope only under special conditions [II–3].

A determination of the design envelope starts with the identification of all plant states, from normal operation through AOOs and DBAs up to DECs. Loads originating from internal and external hazards can affect the performance of any of the plant states, and these loads form another, separate part of the design envelope. The next step in the formation of the plant design envelope is an analysis of all plant states, in accordance with SSG-2 (Rev. 1) [II–4], by realistic and conservative methods for AOOs, conservative methods for DBAs and realistic methods for DECs. The analysis is performed by using validated computer codes to determine bounding parameters corresponding to different plant states. For each relevant SSC, the design functions and associated envelope parameters are defined. The SSCs are safety classified, and engineering and design rules are established corresponding to the safety classification of the SSCs. The requirements on seismic design, environmental qualification, electromagnetic and radiofrequency interference, and quality are defined. The general design basis of SSCs also includes the availability and reliability of auxiliary systems and supporting systems (e.g. electrical power supply, instrumentation and control systems, fire protection systems, cooling, heating and ventilation systems, communication systems).

Eventually, both the safety analysis and the design are independently verified by the operating organization (or by another qualified body on behalf of the operating organization, e.g. a technical support organization). Although different parts of this process (i.e. selection of plant states, performance of the analysis and designing of the items important to safety corresponding to the design envelope) are described in separate sets of provisions, it is understood that, in many cases, there will be a need for several iterations between these two sets of provisions.

Objective tree 7. Plant process control systems (SP164)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 28, 59, 60, 61.

This objective tree applies to Level 1 of defence in depth. In combination with objective trees 8 and 9, it is intended to evaluate whether the plant systems required for the reactor power and all parameters of the RCS are maintained within the established limits. Three categories of systems are considered: the plant process systems (normal operation control systems), the limitation and trip systems, and the safety systems. In addition to adequate system design, it is evaluated whether each of the systems has sufficient capacity to reliably perform its (intended) safety function and whether it is reasonably independent from the systems belonging to other levels of defence.

This objective tree specifically addresses the process control systems for keeping plant parameters within normal operation limits, preferably without actuation of either the reactor trip or the safety systems. The operating range, which is the domain of normal operation, is bounded by values of the variables less extreme than the trip set points. Automatic controls are kept operational to keep parameters within prescribed ranges. This is ensured by adequate margins in the design, high reliability of the process control system, and proper setting and selectivity of initiating parameters of the protection devices.

Objective tree 8. Plant process control systems (SP164)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 28, 59, 60, 61.

This objective tree applies to Level 2 of defence in depth. It deals with the capacity, reliability and independence of the limitation and trip system. Independence among the different levels of defence in depth is considered, as far as reasonably practicable, an important attribute of defence in depth, although in some cases the functions of the limitation and trip system are combined with functions of the safety systems. Ideally, the limitation and trip functions are to be performed by a separate system. The settings of the plant variables ensure that equipment malfunction or failure would actuate an automatic protective action in a selective manner, such as a programmed power reduction, plant shutdown or automatic safety system. Trip set points are chosen in such a way that the limitation and trip systems work properly and would not allow the reaching of the safety limits and hence the actuation of the safety systems.

Objective tree 9. Automatic safety systems (SP168)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 16, 32, 42, 56, 61, 63, 64, 65, 74.

This objective tree deals primarily with Level 3 of defence in depth. It partially deals with Level 4 (DEC-A) of defence in depth, namely with safety

systems that are postulated not to be included in the list of multiple failures. The objective tree addresses the adequate capacity and reliability of safety systems. The safety systems need to be capable of shutting down and cooling down the plant, ensuring that the plant parameters and radioactive releases will be kept within the safety limits. Safety systems are required to be independent from Level 1 and Level 2 systems and, as far as reasonably practicable, also from Level 4 systems (fully for new plants, and to the extent possible for existing plants). The independence of Level 3 from Level 4 of defence in depth is an important factor necessary for compliance with the requirements of practical elimination of plant event sequences leading to early or large radioactive releases. This independence also ensures that the effective functioning of the safety systems is not adversely affected by interaction with other systems. In connection with this objective tree, safety systems require proper functioning of their support systems. This entails high reliability of support systems, equipment qualification, testing and maintaining a sufficient stock of consumables. Certain systems may require a different backup system for given safety functions (e.g. a common cause failure of the reactor protection system, station blackout); this provision is important for coping with DEC-A conditions.

Objective tree 10. Reliability targets (SP174)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 62.

Although the requirements for the reliability and testability of instrumentation and control systems apply primarily to safety systems and, thus, to Level 3 of defence in depth, the applicability of this objective tree was extended to all other levels of defence in order to indicate that adequate reliability is required for all items important to safety. Therefore, the mechanisms and provisions in this objective tree apply to items important to safety. Similarly, as in objective tree 9, it is understood that the reliability targets apply not only to the safety systems, but also to their support systems. In this objective tree, the provisions are subdivided into design and operational provisions affecting the reliability of items important to safety, assuming that the supporting systems are also essential components of the items important to safety. One of the three mechanisms deals with design provisions for ensuring reliability, and another with operational provisions for ensuring reliability. In addition, there is a third mechanism dealing with common cause failures among items important to safety, with reference to a specific objective tree. In accordance with TECDOC-1791 [II–3], it is assumed that, as far as non-permanent equipment is concerned, this equipment does not belong to the design envelope and, therefore, provisions included under all mechanisms in objective tree 10 do not apply to non-permanent equipment. However, features to enable the safe use of non-permanent equipment

for restoring the required function (e.g. power supply in station blackout, the capability to remove heat from the containment or from the spent fuel pool (SFP)) are considered in the design. Non-permanent equipment belongs to the equipment involved in accident management, as described in objective tree 59.

Objective tree 11. Dependent failure (SP177)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 19, 20, 21, 24, 25, 26, 27.

This objective tree applies mainly to Levels 3 and 4 of defence in depth. It addresses the challenges and all mechanisms that can lead to common cause failures of safety systems or safety features for DECs. To cover both the safety systems and the safety features for DECs, the term 'items important to safety' is used. In addition to specific internal failures resulting in common cause failures (e.g. loss of power, loss of support systems, systematic errors in design, construction, operation or maintenance), attention is paid to various internal and external hazards, which can simultaneously affect several systems. The list of hazards given in the text on mechanisms is meant to provide examples and is not a comprehensive checklist of items to be specifically evaluated for the given design or plant.

Objective tree 12. Equipment qualification (SP182)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 30.

Originally, this objective tree corresponded to Level 3 of defence in depth, but it was extended to also include Level 4. As with objective tree 11, the general identifier 'items important to safety' is used to cover both the safety systems and the safety features for DECs. It is understood that items important to safety include not only the safety systems and safety features for DECs, but also their support systems (without explicitly writing the term 'support systems' in the text on provisions). The underlying assumption is that the qualification of SSCs is established and preserved for the lifetime of the NPP to ensure that the equipment will be capable of performing its intended safety function(s) under the range of service conditions specified for the operational states and in accident conditions, as well as during external events not excluded by the design (e.g. seismic events, electromagnetic phenomena such as arcing and lightning).

Objective tree 13. Inspectability of safety equipment (SP186)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 29.

This objective tree addresses a potentially undetected degradation of the functional performance of items important to safety due to a lack of inspections, considering all items important to safety for all levels of defence. The provisions listed in this objective tree are intended to address issues originating from inadequate intervals between inspections, inadequate scope of inspections, limitations in inspections due to difficulties accessing items important to safety, inadequate performance of inspections or insufficiencies in taking corrective actions to resolve issues identified in the inspection throughout the lifetime of the plant. The provisions are written in such a way as to specify explicitly the provisions for performing inspections, the selection of methods, the evaluation of the results of inspections and the implementation of corrective actions.

Objective tree 14. Radiation protection in design (SP188)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 5.

This objective tree applicable for Level 1 of defence in depth addresses design features important to ensuring the radiation protection of the public (by limiting gaseous and liquid radioactive discharges), as well as the radiation protection of the plant personnel (by preventing their contamination by radioactive material and limiting direct exposure to radiation). The provisions also include other features, such as the design of radioactive waste treatment systems, filtration systems, ALARA measures and testing. The radiation protection of plant personnel and the public is also addressed in several other objective trees. The spread of radioactive substances to the environment potentially causing public doses is addressed in objective tree 2. The limitation of radioactive releases following AOOs, DBAs and DEC-A conditions is addressed in objective tree 27, and DEC-B conditions are addressed in objective tree 28. Radiation protection of the plant personnel during plant operation by the implementation of the radiation protection programme is addressed in objective tree 52. Protection of the plant personnel and the public, in the case of severe accidents, by the implementation of on-site and off-site emergency plans (as a part of the emergency response), is addressed in objective tree 62.

Objective tree 15. Protection against power transient accidents (SP192)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 16, 19, 45.

This objective tree addresses any of the mechanisms resulting in a challenge relating to the insertion of an excessive amount of reactivity, which can result in fuel damage due to the potential increase of reactor power. All mechanisms that either increase the amount of fissionable material or remove the neutron absorber

from the reactor core are considered, including control rod ejection, control rod withdrawal, control rod drop or misalignment, erroneous startup of a circulation loop, release of absorber deposits in the reactor core, incorrect refuelling operations and inadvertent boron dilution. For each of these mechanisms, there are a number of provisions to prevent its occurrence. This objective tree specifically deals with Levels 1 and 2 of defence in depth; therefore, the provisions reflect design and operational provisions aimed at preventing the occurrence or reducing the probability of the deviation, recognizing the occurrence of the event.

Objective tree 16. Protection against power transient accidents (SP192)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 16, 19, 45.

This objective tree corresponds to Level 3 of defence in depth. It addresses a similar challenge with the insertion of an excessive amount of reactivity that, because of the potential increase in reactor power, can lead to fuel damage and results from the same (or similar) mechanisms as in objective tree 15. In some of the mechanisms, the difference is the amount and speed of insertion of reactivity, which could lead to potentially more severe consequences. Compared with objective tree 15, there are two mechanisms that could potentially lead to accidents. The first mechanism is caused by inadvertent startup of the reactor at low coolant temperature or by an excessive cooldown of the reactor that is not sufficiently compensated for by the neutron absorber contained in the primary coolant. The second mechanism is a rapid insertion of reactivity by sudden injection of non-borated coolant to part of the core, causing recriticality and potential fuel damage.

The source of the non-borated coolant can be external (applicable mainly during the shutdown operating regime) or can result from the condensation of steam in the steam generator and the collection of non-borated coolant in the cold leg in certain loss of coolant accidents (LOCAs), followed by its subsequent rapid transport to the core. Such fast heterogeneous boron dilution is much more severe than slow homogeneous boron dilution by injecting coolant during plant startup. If such dilution would lead to very fast reactivity insertion (prompt criticality), such a scenario needs to be practically eliminated. The issue of potential recriticality after injection of a clean condensate into a partially degraded core (with molten control rods) is addressed under SP200 (automatic shutdown system). Among the provisions to mitigate the consequences of the accidents are inherent properties (reactivity feedback effects), actions by the safety systems ensuring shutdown of the reactor and operator actions to mitigate the consequences of the accident.

Objective tree 17. Reactor core integrity (SP195)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 43, 44, 45.

This objective tree deals with the potential damage of fuel due to various mechanical and chemical effects impacting the fuel during normal and abnormal operation: AOOs (Levels 1 and 2 of defence in depth). The mechanical effects of DBAs are addressed separately, in objective tree 18. This objective tree considers that mechanical effects can impact the reactivity control or the core cooling, or can cause direct fuel damage by mechanical loads. A variety of potential fuel damaging mechanisms of quite different natures could be considered; for example, axial forces acting on fuel assemblies (internal loads caused by springs, which are used in the upper core plate, preventing fuel assemblies from being pushed out from the reactor core) or the mechanical effects of earthquakes. As a separate mechanism, the potential fuel damage from chemical effects, such as corrosion and hydration, is considered. Provisions for preventing the mechanisms from causing fuel damage include mainly robustness and quality of fuel design, as well as various kinds of monitoring means (including monitoring of radioactivity of coolant) aimed at early identification of potential causes of the damage. Only mechanical and chemical effects are covered by this objective tree. Various thermal and burnup effects are covered separately by objective tree 21.

Objective tree 18. Reactor core integrity (SP195)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 43, 44, 45.

Similarly to objective tree 17 for normal and abnormal operation, this objective tree considers the potential mechanical effects of DBAs on reactor core integrity. In particular, the mechanical effects of LOCAs causing propagation of pressure waves in the reactor are considered. Other effects of DBAs, mainly thermal and associated effects (such as oxidation), are covered by objective tree 23.

Objective tree 19. Automatic shutdown systems (SP200)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 26, 61.

This objective tree applies to Levels 3 and 4 of defence in depth. It addresses the potential challenges caused by inadvertent insertion of reactivity after reactor shutdown (non-performance of the derived safety function (2)). The potential mechanisms involved include the removal of mechanical absorbers

from the reactor core, boron dilution or significant decrease of the coolant temperature. There is also one special mechanism for Level 4 of defence in depth, corresponding to potential recriticality due to injection of non-borated coolant to the partially degraded core.

Objective tree 20. Automatic shutdown systems (SP200)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 26, 61.

This objective tree reflects the same principle as objective tree 19. It also applies to Levels 3 and 4 of defence in depth, but addresses the potential challenge caused by inadequate means for shutting down the reactor (non-performance of the derived safety function (3)).

Objective tree 21. Normal heat removal (SP203)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 51, 53, 70.

This objective tree addresses the challenges associated with a potential degradation of decay heat removal from the fuel in the core during normal and abnormal operation (Levels 1 and 2 of defence in depth). The causes of the degradation of decay heat removal can be found in the reactor core, but also in the primary, secondary or tertiary cooling circuits (cooling towers and HTS to the UHS). This objective tree deals only with normal heat removal from the reactor core. Normal decay heat removal from the SFP is dealt with separately, in objective tree 36. The issues associated with the heat removal in normal and abnormal operation (Levels 1 and 2 of defence in depth) are combined in a common objective tree, since the means for decay heat removal are the same for both Levels 1 and 2 of defence in depth. The issues associated with the RCS integrity (selection of materials, in-service inspections, structural design of the RCS) are not included in this objective tree and are covered separately by objective tree 25. Therefore, only the structural design of the reactor internals is mentioned in this objective tree. The mechanisms and provisions in this objective tree are formulated assuming a pressurized water reactor design, which is more complex because of the existence of a secondary circuit. For a boiling water reactor design, an appropriate integration of provisions applicable to the primary and secondary circuits might be necessary.

Objective tree 22. Startup, shutdown and low power operation (SP205)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 8, 26, 27.

This objective tree addresses specific challenges resulting in deviations from normal operation associated with startup, shutdown and low power modes. Two kinds of challenges are considered: the first one reflecting the higher likelihood of failures during such operational modes, and the second one caused by a degraded capability of the plant to cope with deviations from normal operation (for example due to degradation of some fission product barriers). There is also one mechanism related to the specific evolution of postulated initiating events and accident scenarios, with provisions focused on the identification of events and accident scenarios relevant for non-power operational modes, the selection of acceptance criteria, the execution of deterministic safety analysis, the development of specific emergency operating procedures (EOPs) and severe accident management guidelines (SAMGs). During shutdown modes, some relaxation of safety barriers may be necessary but should be applied only when properly justified.

Objective tree 23. Emergency heat removal (SP207)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 33, 52.

This objective tree has been developed to cover challenges relating to a potential degradation of fuel cooling under DBAs and DEC-A conditions. This objective tree also applies to DEC-A conditions (part of Level 4 of defence in depth, DECs without core melting) to reflect the evolution of safety requirements since the publication of INSAG-12 [II–1]. The applicability of this objective tree is limited to decay heat removal from the fuel located in the reactor core during DBAs and DEC-A conditions. Decay heat removal from the SFP is covered by objective tree 36. The mechanisms and provisions are subdivided for failures in emergency heat removal during LOCAs, non-LOCA accidents, accidents due to loss of UHS, loss of power supply and loss of support systems. Potential damaging effects on nuclear fuel due to degraded heat removal are covered here, and one of the provisions for mitigating fuel damage is the use of accident tolerant fuel. As far as accidents due to loss of UHS are concerned, reference is made to objective tree 3. Accidents at non-power operational modes are covered separately in objective tree 22. Operator actions to restore core cooling under accident conditions are covered by the development and implementation of EOPs described in objective tree 51. Common cause failures potentially affecting core cooling are addressed separately in objective tree 11.

Objective tree 24. Emergency heat removal (SP207)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 33, 52.

This objective tree corresponds to Level 4 of defence in depth, DEC-B conditions (severe accidents). It deals with emergency heat removal from the fuel originally located in the core, but after core degradation and relocation, also in the reactor cavity or in the containment. The issue of imbalance between heat production and heat removal, with excessive heat production due to recriticality, is addressed in objective tree 19. The sources of heat generation in severe accidents are not only accumulated decay heat, but also other heat sources such as the heat generated by chemical reactions between metallic materials and the coolant. Similarly to objective tree 23, reference is made to objective tree 3 as far as accidents due to loss of UHS are concerned. Slow overpressurization due to steam generation is dealt with by objective tree 30.

Objective tree 25. Reactor coolant system integrity (SP209)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 47, 48.

This objective tree is relevant for Levels 1 and 2 of defence in depth. It addresses the challenges potentially affecting the integrity of the reactor pressure vessel (RPV) and the provisions implemented to eliminate such challenges. The objective tree includes the provisions necessary to ensure practical elimination of sudden rupture of large, pressurized components (in particular the RPV) as one of the challenges potentially leading to early or large radioactive releases. In addition to the design provisions covered by this objective tree, there are also operational provisions (mild operational modes) to practically eliminate rupture of the RPV (see Annex I). The mechanisms to be prevented by design include weaknesses in the design basis, selection of materials, fabrication methods, in-service inspections and tests.

Objective tree 26. Confinement of radioactive material (SP217)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 54, 55, 56, 57, 58.

This objective tree addresses potential releases to the environment due to releases from the RCS. Two pathways are considered: either releases to the containment and then to the environment, or releases bypassing the containment. The challenges due to releases to the containment are considered in two sequential steps: first, the releases from the RCS to the containment are considered, and

then the releases from the containment to the environment. This objective tree is relevant for Levels 2 and 3 of defence in depth. The reason for including Level 2 is the potential for very small releases, which would increase radioactivity in the containment, but since they may be compensated for by the normal make-up system, they do not belong to the category of DBAs. Releases from sources other than the RCS are discussed separately in objective tree 27. Because the release pathways and the associated phenomena are quite different for DBAs and DECs, it is considered appropriate to have two different objective trees, one for Level 3 and another for Level 4 of defence in depth.

Objective tree 27. Confinement of radioactive material (SP217)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 54, 55, 56, 57, 58.

This objective tree covers Level 2, Level 3 and partially Level 4 (DEC-A) of defence in depth. As already introduced, it deals with potential releases from various sources outside the RCS. Potential sources of radioactive releases are the SFP, radioactive waste treatment systems, spent fuel transport containers and on-site dry spent fuel storage. References are made to objective tree 36, where the mechanisms leading to fuel damage in the SFP or during transport are covered. The SFP is covered by objective tree 43, and wet spent fuel storage is covered by objective tree 36; both are the same facilities. Objective tree 27 deals to some extent with on-site dry spent fuel storage, in the case when such storage is a part of the same nuclear installation.

Objective tree 28. Confinement of radioactive material (SP217)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 54, 55, 56, 57, 58.

This objective tree is relevant for accident conditions more severe than DBAs and applies to Level 4 of defence in depth. It discusses various provisions reducing releases from the containment and releases bypassing the containment, mainly due to accidents in the SFP and primary to secondary leak. It is noted that a severe accident taking place in the SFP, which is located outside the containment, needs to be practically eliminated. If the SFP is located within the containment, large releases in the short term are eliminated by the containment function, provided that the integrity of the containment is maintained. The provisions for prevention or limitation of releases from the containment are given for different situations: (i) release from the RCS, (ii) release from the containment water, (iii) release from the internal SFP to the containment atmosphere, (iv) removal of fission products from the containment atmosphere and (v) limitation

of releases from the containment to the environment. One of the issues associated with potential releases from the containment is direct (unfiltered) leakage from the primary containment (called 'primary containment bypass'). This issue is relevant for double containments, in which a major part of the releases from the primary containment enters the containment annulus and afterwards is released to the environment through the filters. However, a small part of the release (called 'secondary containment bypass') can propagate directly to the environment through penetration and isolation devices, for example, thus bypassing the filters and determining radiological consequences. For all mechanisms leading to containment bypass, the provisions contributing to practical elimination of plant event sequences leading to early or large radioactive releases are listed.

Objective tree 29. Protection of confinement structure (SP221)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 58.

This objective tree deals with challenges exposing the integrity of the confinement (primarily the containment) structure, as a precondition for the successful confinement of radioactive material. This objective tree is associated with Level 3 of defence in depth and primarily with the mechanisms relevant for DBAs. However, besides the mechanisms exposing the containment integrity due to containment overpressurization and low subatmospheric pressure, the potential effects of internal and external hazards are also considered. For external hazards, reference is made to objective trees 1 (natural hazards) and 37 (human induced hazards). Potential damage due to inadequate containment testing and inspections is also considered. Random hazards are identified based on their probability, and malevolent human actions are taken into account based on broader considerations. The mechanism of damage by external hazards considered in this objective tree is particularly important because the containment belongs to the SSCs ultimately needed for the prevention of early or large radioactive releases, and therefore its robustness (adequate margins to withstand external hazards more severe than those considered for design, derived from the hazard evaluation for the site) is very important. This objective tree also deals with potential damage caused by low underpressure. Such a mechanism is relevant only for some special types of containments. For a standard full pressure containment, it is relevant only in the case of using containment filtered venting, with the partial release of non-condensable gases to the environment.

Objective tree 30. Protection of confinement structure (SP221)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 58.

This objective tree, similarly to objective tree 29, deals with the protection of the confinement structure, but specifically in connection with phenomena associated with a severe accident. This objective tree is applicable to Level 4 of defence in depth. The objective tree also considers the challenges to containment integrity originating in the SFP, if it is located in the containment, and the challenge of destruction of the containment by explosions outside it (e.g. the Fukushima Daiichi accident). As far as damage due to internal hazards is concerned, this objective tree considers only specific hazards originating from the phenomena associated with a severe accident (such as the mechanical impact of the RPV bottom cut-off, hydrogen or steam explosions in the reactor cavity). Containment damage by internal missiles or in-vessel steam explosions is not included in this objective tree. These types of damage are generally considered to be very unlikely. The safety provisions for DECs (equipment) at Level 4 are preferably independent from the safety systems used at Level 3. For existing plants, installation of safety provisions for DECs may not be feasible. In such cases, consideration is given either to system robustness or the enhancement of safety provisions to perform reliably under DECs.

Objective tree 31. Monitoring of plant safety status (SP227)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 59, 60, 62.

This objective tree applies to Levels 1 and 2 of defence in depth. It addresses all challenges resulting either from deficiencies in knowledge and understanding of plant safety status by operating personnel or from a lack of early warning of developing problems. The challenges can arise from the incomplete or inappropriate display of safety relevant information, or inadequate information or communication on identifying emerging problems.

Objective tree 32. Monitoring of plant safety status (SP227)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 59, 60, 62.

Similarly to objective tree 31, this objective tree addresses the challenges caused by deficiencies in knowledge or understanding of the plant's safety status in accident conditions. It applies to Levels 3 and 4 of defence in depth. The mechanisms potentially resulting in inadequate operator response in accident conditions include incompleteness of information, ambiguity of information and problems with communication among the plant personnel. Two special mechanisms address the issue of interdependencies among monitoring chains for different levels of defence and the issue of potential loss of plant information

due to the loss of instrumentation (with reference to objective tree 34 for station blackout).

Objective tree 33. Preservation of control capability (SP239)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2] Requirement 65, 66, 67.

This objective tree deals with potential mechanisms leading to loss of control room habitability due to various reasons (e.g. fires, penetration of toxic gases or other dangerous substances) or damage to the control room by external hazards or other external actions. This objective tree is applicable to all levels of defence in depth because the control room and control room personnel are the same for all plant states. This objective tree also includes specific provisions that are intended to ensure the habitability of the control room and its robustness against natural external hazards, including capability to survive conditions more severe than design basis external hazards, as a precondition for the practical elimination of plant event sequences leading to early or large radioactive releases. The possibility of a remote control location, if required, is mentioned here as well.

Objective tree 34. Station blackout (SP233)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 68.

This objective tree applies to Level 4 of defence in depth. It is developed to quite a high level of detail in order to reflect the importance of the issues associated with station blackout after the Fukushima Daiichi accident. Seven different mechanisms resulting in the challenge that items important to safety may become unavailable because of station blackout are considered, with more than 40 provisions listed to prevent these mechanisms from taking place. The provisions reflect the comprehensive information provided in IAEA-TECDOC-1770, Design Provisions for Withstanding Station Blackout at Nuclear Power Plants [II–6].

Objective tree 35. Control of accidents within the design basis (SP237)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 16, 19, 20.

This objective tree applies to Level 3 of defence in depth. It addresses general requirements placed on plant safety systems. The challenge in this objective tree deals with inadequate design of safety systems that could result in a delayed or inadequate response to postulated initiating events, leading to the progression of DBAs to DECs. Three sets of provisions are developed to prevent relevant mechanisms from occurring: provisions to ensure performance of

automatic actions of safety systems, provisions to ensure performance of manual actions in case of the failure of safety systems and provisions to ensure adequate characteristics of the safety systems. Equivalent provisions for engineered safety features and safety features for DECs (at Level 4 of defence in depth) are covered by objective trees 57−59.

Objective tree 36. Storage of fresh and spent fuel (SP240)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 80.

This objective tree is intended to address the issues associated with storing fresh and, in particular, spent nuclear fuel inside and outside the containment. This objective tree applies to Levels 1 to 4 of defence in depth. A list of provisions also covers the need to perform safety analyses in order to consider DECs without significant fuel degradation and to practically eliminate early or large radioactive releases. There are provisions for monitoring of the SFP inventory and removal of decay heat from irradiated fuel, as well as for enhanced robustness of the SFP and dry fuel storage against external hazards. This objective tree is devoted to those provisions that are important to preventing fuel damage in storage systems for fresh and spent nuclear fuel that are located inside the plant, but not necessarily inside the reactor building. The provisions of this objective tree are referred to in objective tree 27 because the prevention of radioactive releases (addressed in objective tree 27) is closely related to fuel damage, addressed in objective tree 36. Fresh mixed oxide fuel needs to be cooled in the storage pool because its surface temperature and surface dose rate are much higher than those of fresh UO_2 fuel.

Objective tree 37. Physical protection of the plant (SP242)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirement 17.

This objective tree applies to all levels of defence under the assumption that deficiencies in the physical protection of the plant can affect all levels. This objective tree does not comprehensively cover the whole area of physical protection; it primarily deals with interfaces between safety and security. Two challenges are identified in this objective tree: safety items being damaged by unauthorized activities (with two mechanisms, one dealing with lack of vigilance in preventing unauthorized access and the other dealing with deficiencies in design) and nuclear safety being potentially jeopardized by inadequate security measures. This objective tree therefore deals with the very important issue of existing interfaces between safety and security.

Objective tree 38. Safety evaluation of design (SP246)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 10, 42.

This is the first of the two objective trees covering the area of manufacturing and construction. This objective tree applies to Levels 1 to 4 of defence in depth. It deals with the role of the operating organization in independent verification of the design during manufacturing and construction of the plant as an important component of taking over its prime responsibility for safety. Specific provisions underline the fact that the independent verification of the design is performed by the operating organization for existing plants (in the case of plant modifications) or on behalf of the future operating organization for new plants. The operating organization is also responsible for early communication with the regulatory body and submission of the safety demonstration of the design in due time.

Objective tree 39. Achievement of quality (SP249)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 9, 11, 18.

This objective tree applies to Levels 1 to 4 of defence in depth. Its objective is to prevent degradation of the functional capability of items important to safety due to inadequate quality during the manufacturing or construction of the plant (including plant modifications). Although it is not always explicitly stated, this objective tree formulates the responsibility of the operating organization to ensure adequate quality of products and services delivered by external manufacturers or constructors. The terms ‘manufacturers’ and ‘constructors’ are more frequently used in this objective tree as an equivalent to the term ‘suppliers’ (of products and services). The operating organization ensures that all suppliers have adequate quality assurance programmes and plans to meet the expectations of the operating organization, by means of reviews and/or audits of manufacturers’ and constructors’ practices and documents.

Objective tree 40. Verification of design and construction (SP255)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 42.

This is the first of the four objective trees for the area of commissioning. It applies to Levels 1 to 4 of defence in depth because deficiencies in the verification of design and construction can result in a degraded plant performance due to as-built safety related and radiation protection items not complying with the design intent. Unlike objective tree 38 (which focuses on verification of the design before and during construction), this objective tree focuses on adequately developing the commissioning programme components, performing the commissioning tests and taking the necessary corrective actions to manage identified weaknesses.

Objective tree 41. Validation of operating and functional test procedures (SP258)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 25, 26.

The aim of this objective tree is to eliminate deficiencies in the validation of operating procedures and procedures for functional tests for all items important to safety. The objective tree applies to Levels 1 to 4 of defence in depth. The mechanisms deal with potential consequences that may impact on the equipment performance because of an insufficient scope of validation of normal operating procedures and procedures for functional tests during commissioning to demonstrate (by quality and scope of validation) that all items important to safety will function in accordance with the design intent.

Objective tree 42. Collection of baseline data (SP260)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 25, 31.

This objective tree applies to Levels 1 to 4 of defence in depth. It addresses the need to collect the initial data during commissioning and, particularly in the commissioning tests, set all parameters that are to be monitored during operation of the plant. Detailed diagnostic data are to be collected on components with special safety significance. Lack of baseline data could result later in an undetected degradation of functional performance of items important to safety (particularly fission product barriers).

Objective tree 43. Pre-operational adjustment of plant (SP262)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 15, 29; SSR-2/2 (Rev. 1) [II–5], Requirement 25.

This objective tree applies to Levels 1 to 4 of defence in depth. It addresses the need to confirm compliance of the as-built plant characteristics with the design intent and to record as-built plant parameters for future use. Inadequate tests during commissioning, without reflecting as-built plant characteristics in the plant data and procedures, could result in degraded plant safety performance caused by as-built processes and plant systems not being compliant with the design intent.

Objective tree 44. Organization, responsibilities and staffing (SP265)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 1, 5, 7.

This is the first of the objective trees belonging to the area of operation. The objective tree has a general part applicable to Levels 1 to 4 of defence in depth, reflecting the needs of the overall organization, responsibilities and staffing. In addition, it has two specific parts: one reflecting the adequacy of organization for normal operations, and the other reflecting the adequacy of organization for accident conditions. This objective tree is viewed in conjunction with other objective trees dealing with organizational matters, in particular objective trees 46 and 47 (Conduct of operations), objective tree 45 (Safety review procedures), objective tree 56 (Quality assurance in operation) and objective tree 54 (Feedback of operating experience).

Objective tree 45. Safety review procedures (SP269)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–5], Requirement 10; GSR Part 4 (Rev. 1) [II–7], Requirements 12, 22.

This objective tree applies to Levels 1 to 4 of defence in depth. It reflects the need for the operating organization to arrange for continuing surveillance and audit of the operational safety of the plant and for a routine process of safety management that covers all aspects of day to day operations and reports to the plant management. The safety reviews include a direct review by plant managers, as well as independent reviews performed by the internal independent oversight team. Among the available means of facilitating independent safety reviews, the IAEA Operational Safety Review Team missions and World Association of Nuclear Operators peer reviews are specifically mentioned. The review gives special attention to unusual plant configurations and conditions. This objective tree also addresses the need for adequate response to the regulatory requirements.

Objective tree 46. Conduct of operations — procedures (SP272)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 6, 7, 8.

This objective tree applies to all levels of defence in depth because ineffective conduct of operations can affect all levels of defence in depth simultaneously. This objective tree also addresses the operating procedures. The quality of operating procedures is addressed separately in objective trees 50−52 and 58. The current objective tree deals just with the correct use of the procedures. Reference is also made to the issue of a lack or degradation of safety culture, with a link to the dedicated objective tree 47.

Objective tree 47. Conduct of operations — safety culture (SP272)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 1, 3, 4, 7, 8, 27; GSR Part 2 [II–8], Requirements 1, 5.

Although this objective tree is placed under the safety principle 'Conduct of operations', it is specifically devoted to issues associated with the lack or degradation of safety culture. All five levels of defence are applicable to this objective tree. Sufficiently detailed provisions are formulated to ensure compliance with all key attributes of safety culture, as follows:

— Safety is a clearly recognized value;
— Leadership for safety is clear;
— Accountability for safety is clear;
— Safety is integrated into all activities;
— Safety is learning driven.

Objective tree 48. Training (SP278)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 4, 7, 18, 19.

This objective tree applies to Levels 1 to 3 of defence in depth. It deals first with general provisions for training, and then with special mechanisms and provisions for managers, control room operators and maintenance personnel. General provisions for training deal with the scope (technical content) and the execution (formal arrangements) of training. There is a separate objective tree, objective tree 58, devoted to special features of training for accident management.

Objective tree 49. Operational limits and conditions (SP284)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 28; SSR-2/2 (Rev. 1) [II–5], Requirement 6.

The applicability of this objective tree is assigned only to Level 1 of defence in depth because it addresses the limits and conditions for normal operation. The whole set of operational limits and conditions is defined for all operating modes, including limits for key plant variables, surveillance and testing requirements and requirements for minimum staffing. Three mechanisms are identified: inadequate scope, inadequate basis of operational limits and conditions, and violation of operational limits and conditions by the plant personnel.

Objective tree 50. Normal operating procedures (SP288)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirement 26.

This objective tree applies to Level 1 of defence in depth (in the existing system of objective trees, Level 2 is covered by objective tree 51). It comprehensively addresses all potential issues associated with normal operating procedures. The provisions included in this objective tree are intended to ensure an adequate scope, adequate quality and adherence to approved normal operating procedures.

Objective tree 51. Emergency operating procedures (SP290)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 19, 26.

This objective tree applies to Levels 2, 3 and 4 of defence in depth. It covers the whole process of development and implementation of EOPs. In this objective tree, abnormal operating procedures are also considered under EOPs. Individual mechanisms covered by this objective tree include the need to have a sufficient basis for development of EOPs, including relevant analytical support; compliance with adequate formal requirements applicable to the procedures; adequate technical scope and quality; and verification and validation. In this objective tree, a link is made to other safety principles (and objective trees) to cover the issue of adequate training on the use of EOPs. As described in SSG-54 [II–9], EOPs cover the preventive domain of accident management at DECs (i.e. before significant fuel degradation) and are complemented by SAMGs in the mitigatory domain (i.e. when significant fuel degradation is imminent or ongoing). The EOPs cover not only accidents originating in the RCS, but also events in the SFP and in the systems for treatment of radioactive waste. The set of preventive actions may also consider the safe use of non-permanent equipment.

Objective tree 52. Radiation protection procedures (SP292)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 19, 20, 26.

This objective tree applies to Levels 1 to 4 of defence in depth. It addresses the operating provisions to prevent radiation exposure of the plant personnel above the prescribed limits (in addition to design provisions addressed in objective tree 14). Overall coordination for all operating provisions is ensured by a comprehensive radiation protection programme. Effective implementation of the programme is under the control of specialized radiation protection personnel with adequate authority, provided with the necessary equipment and controlling

the compliance of all activities with relevant radiation protection procedures. Radiation protection procedures also cover monitoring the potential exposure of contractors, reporting radiation doses to the regulatory body and paying close attention to exposures potentially received during special operational activities, such as maintenance during outages.

Objective tree 53. Engineering and technical support of operations (SP296)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 67; SSR-2/2 (Rev. 1) [II–5], Requirement 19.

This objective tree applies to Levels 1 to 4 of defence in depth. It underlines the fact that, although the prime responsibility for safety rests with the operating organization, this responsibility can be effectively executed only with external engineering and technical support. Attention is paid to the internal capability of the operating organization to arrange and ensure the quality of the technical support provided by external organizations. Further on, the need for careful prioritization and planning of usually limited resources for technical support is addressed. Attention is also paid to the selection, auditing and verification of the quality of services and products in the area of nuclear safety, if delivered by external organizations. External support is not necessarily limited to a single country. In order to support the high quality engineering and technical support available in external organizations, it is advisable to directly or indirectly support relevant development programmes for external organizations.

Objective tree 54. Feedback of operating experience (SP299)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirement 24.

This objective tree applies to Levels 1 to 4 of defence in depth. It is intended to verify that effective feedback of operating experience is in place to ensure that events significant to safety are detected and evaluated in depth, that any necessary corrective measures to avoid the recurrence of events and to enhance safety are taken promptly and that information on the events is disseminated. The objective tree evaluates whether the feedback from the plant is implemented, as well as whether there is access to operating experience relevant to plant safety from other NPPs around the world.

Objective tree 55. Maintenance, testing and inspection (SP305)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 29; SSR-2/2 (Rev. 1) [II–5], Requirements 31, 32.

This objective tree applies to Levels 1 to 4 of defence in depth. It addresses the issues associated with inadequate performance of maintenance, testing and inspections during plant operation. The relevant challenge to be eliminated is a degraded functional capability of items important to safety. The mechanisms to be prevented from occurring include inconsistencies or delays in maintenance, testing, surveillance and inspections or problems caused by incorrectly performed activities. In the case of weaknesses in maintenance, testing or inspections, an undetected degradation of fission product barriers caused by various operational phenomena (e.g. irradiation, thermal cycling, wearing out) can occur. In cases of deficiencies in providing information about the status of maintenance works, the shift operators may not have precise information about the availability of the systems.

Objective tree 56. Quality assurance in operation (SP312)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirements 2, 3, 7, 9; GSR Part 2 [II–8], Requirements 1, 6.

This objective tree applies to Levels 1 to 4 of defence in depth. It addresses the issues associated with an inadequate quality assurance in the plant operation. It deals with weaknesses in the plant management, as well as in the quality of items important to safety. The relevant challenges to be eliminated are either unsatisfactory operational performance due to inadequate management, or degraded functional capability of items important to safety due to a lack of compliance with applicable quality requirements in operation. The importance of the operating organization using an integrated management system instead of simple quality assurance provisions is emphasized, in line with GSR Part 2 [II–8]. The mechanisms are therefore subdivided into mechanisms associated with different general issues of the management system. Nevertheless, there are still two mechanisms specifically addressing the quality assurance of the classified equipment. In addition, there are provisions associated with the keeping of key records important for the plant's operational history and activities associated with the maintenance of classified equipment.

Objective tree 57. Strategy for accident management (SP318)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 18, 19.

This objective tree is the first of the objective trees specifically dealing with accident management. It belongs to Level 4 of defence in depth and addresses the issue of the development of an overall strategy for accident management with the objective of eliminating the challenge of non-comprehensive or ineffective

accident management strategies. The individual strategies contain high level sets of actions aimed either at preventing the progression of an event into a severe accident (preventive strategies) or mitigating the consequences of a severe accident (mitigation strategies). Strategies for the development of accident management programmes comprise the following steps:

— Identification of plant vulnerabilities to find mechanisms through which critical safety functions may be challenged. In the event that these challenges are not mitigated, the core may be damaged, and the integrity of fission product barriers may be compromised.
— Identification of plant capabilities under challenges to critical safety functions and fission product barriers, including capabilities to mitigate such challenges in terms of both the equipment and the operating personnel.
— Development of suitable accident management strategies and measures, including hardware features, to cope with the vulnerabilities identified.
— Development of procedures and guidelines to execute the accident management strategies.

The objective tree considers the requirements established in SSR-2/2 (Rev. 1) [II–5] and the recommendations provided in SSG-54 [II–9] on accident management programmes for NPPs. The objective tree reflects the requirements on the systematic development of accident management strategies and on comprehensive analytical support for the development of strategies. The most important strategies are explicitly listed. The issue of multiunit sites is also specifically addressed. The development of strategies is important for the development of EOPs and SAMGs, as underlined by the respective provisions in objective tree 58. The provisions of this objective tree also apply to non-permanent equipment used for the execution of accident management actions under the conditions at defence in depth Level 4.

Objective tree 58. Training and procedures for accident management (SP323)

Relevant IAEA Safety Standards: SSR-2/2 (Rev. 1) [II–5], Requirements 7, 19.

This objective tree belongs to Level 4 of defence in depth and deals with all issues associated with the availability of procedures and guidelines, and the adequate training of personnel needed for the execution of accident management

actions. Accident management is understood as the set of actions taken during the evolution of DECs in order to:

— Prevent the escalation of the event into a severe accident;
— Mitigate the consequences of a severe accident;
— Achieve a long term safe state.

The challenges addressed by this objective tree include:

— Inadequate numbers and qualifications of personnel for accident management;
— Inadequate response of accident management personnel due to inadequate accident management procedures and guidelines (specifically EOPs and SAMGs);
— Inadequate response of accident management personnel due to weaknesses in accident management training.

The provisions for training include not only training of plant personnel, but also training of trainers. Training also covers accidents taking place in parallel on several units (multiunit accidents) and addresses the safe use of alternative and non-permanent (mobile) equipment. The term 'multifunctional simulator' is used to differentiate this tool from a full scope simulator. A multifunctional simulator is basically a laptop with special software for presenting the results of calculations. The provisions of this objective tree also apply to non-permanent equipment used for the execution of accident management actions under the conditions at defence in depth Level 4.

Objective tree 59. Engineered features for accident management (SP326)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 20; SSR-2/2 (Rev. 1) [II–5], Requirement 19.

This objective tree belongs to Level 4 of defence in depth and is applicable to the determination of provisions for the management of accidents that are more severe than DBAs, namely DECs, including severe accidents. The objective tree deals with general provisions to ensure the availability and reliable performance of equipment and instrumentation under DECs, without specifying the type of equipment or conditions. More detailed specifications of equipment and conditions are covered by previously discussed objective trees, specifically for residual heat removal and for the protection of containment integrity. This objective tree also addresses the provisions regarding the availability of adequate equipment for the management of multiunit accidents, which is either qualified

or sufficiently robust to withstand natural external hazards more severe than those considered for design (beyond design basis events) with adequate margins. Non-permanent equipment represents a very important contribution to the safety of the plant under DECs, particularly for an existing plant. The provisions of this objective tree partially apply also to non-permanent equipment used for the execution of accident management actions under DECs.

Objective tree 60. Emergency response facilities (SP336)

Relevant IAEA Safety Standards: SSR-2/1 (Rev. 1) [II–2], Requirement 67; GSR Part 7 [II–10], Requirements 24, 25, 26.

This objective tree belongs to Level 4 of defence in depth and deals specifically with the role of the technical support centre (TSC) in the emergency response organization. In accordance with GSR Part 7 [II–10] and SSG-54 [II–9], the TSC primarily provides support to the control room personnel, whereas other emergency response facilities are focused on the protection of people and the environment. The following properties of the TSC are reviewed:

— Adequate staffing and equipment;
— Habitability under the conditions induced by external hazards;
— Adequate information about the situation in the plant and its surroundings;
— Reliable communication means with the control rooms;
— Means for prediction of evolving accident conditions.

The TSC is considered an integral part of the emergency response organization, ensuring the consistency of TSC activities with the activities of the emergency response organization. The TSC plays an important role in emergency planning, since it communicates with and provides information to the emergency centre. Nevertheless, the coordination role in emergencies, as also reflected in the objective trees, is given to the emergency centres (see objective tree 61), where the responsibility for the overall coordination of the whole emergency response is usually placed.

Objective tree 61. Emergency plans (SP333)

- **Emergency plans (on-site) (SP333);**
- **Emergency response facilities (SP336).**

Relevant IAEA Safety Standards: GSR Part 7 [II–10], Requirement 23.

This objective tree applies to Level 5 of defence in depth. The objective tree deals with on-site emergency response facilities and arrangements influencing

the effectiveness of execution of the on-site emergency plan. Two different challenges are addressed by this objective tree:

— The execution of emergency plans is ineffective because of a lack of coordination within the emergency response organization;
— The execution of emergency plans is ineffective because of a lack of logistical support.

The objective tree deals with the role of emergency response facilities other than the TSC. In accordance with GSR Part 7 [II–10], the emergency response facilities are separate from the control room and supplementary control room, and include the TSC, the on-site emergency centre, the operational centre and optionally also the off-site emergency centre. In accordance with GSR Part 7 [II–10], three facilities can be combined: the TSC, the operational support centre and the emergency centre. The operational support centre is a space where personnel can stay when not performing the assigned actions (local actions, recovery actions). Sufficient capacity, habitability, conditions for resting and food reserves are the conditions to be provided. For the TSC, which belongs to Level 4 of defence in depth, a separate objective tree, objective tree 60, was developed. Other, previously listed elements of emergency response facilities belong to Level 5 of defence in depth. Two different functions of the emergency centre are covered by the objective tree: providing logistical support for the execution of emergency plans, and coordinating all activities of the on-site emergency response organization (including coordination of the TSC). The issue of the vulnerability of the emergency response facilities to post-accident conditions and external hazards is covered as an important factor to be verified.

Objective tree 62. Emergency plans (SP333)

- **Feasibility of emergency plans (SP140);**
- **Emergency plans (on-site) (SP333);**
- **Assessment of accident consequences and radiological monitoring (SP339).**

Relevant IAEA Safety Standards: GSR Part 7 [II–10], Requirement 23.

This objective tree applies to Level 5 of defence in depth and combines challenges belonging to two different areas: siting (from the viewpoint of the feasibility of emergency plans) and emergency preparedness (the execution of emergency plans and assessment of accident consequences and radiological monitoring). Three different challenges are addressed by the objective tree:

— Site characteristics unfavourable for the execution of emergency plans;
— Incorrect decisions by authorities due to delayed, misleading or incorrect information given by the operating organization;
— Inadequate on-site response to emergencies.

The objective tree focuses on the duty of the operating organization to execute on-site emergency plans. It also addresses the duty of the operating organization to provide necessary inputs for the execution of off-site emergency plans. Those actions belonging to the off-site emergency plans, which usually fall under the responsibility of the local or State authorities, are not covered in detail by this objective tree. Only those parts that can be affected by communication from the operating organization are covered. As far as on-site emergency plans are concerned, this objective tree focuses on the functions to be ensured, whereas the facilities needed for the execution of emergency plans on the site (i.e. emergency response facilities), including adequate staffing and communication means, are covered by objective trees 60 and 61.

REFERENCES TO ANNEX II

[II–1] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG Series No. 12, IAEA, Vienna (1999).

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

[II–3] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791, IAEA, Vienna (2016).

[II–4] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2 (Rev. 1), IAEA, Vienna (2019).

[II–5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards Series No. SSR-2/2 (Rev. 1), IAEA, Vienna (2016).

[II–6] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Provisions for Withstanding Station Blackout at Nuclear Power Plants, IAEA-TECDOC-1770, IAEA, Vienna (2015).

[II–7] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[II–8] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2, IAEA, Vienna (2016), https://doi.org/10.61092/iaea.cq1k-j5z3

[II–9] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-54, IAEA, Vienna (2019).

[II–10] FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL CIVIL AVIATION ORGANIZATION, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, INTERPOL, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, PREPARATORY COMMISSION FOR THE COMPREHENSIVE NUCLEAR-TEST-BAN TREATY ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, UNITED NATIONS OFFICE FOR THE COORDINATION OF HUMANITARIAN AFFAIRS, WORLD HEALTH ORGANIZATION, WORLD METEOROLOGICAL ORGANIZATION, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards Series No. GSR Part 7, IAEA, Vienna (2015), https://doi.org/10.61092/iaea.3dbe-055p

DEFINITIONS

The following definitions apply for the purposes of this Safety Report only.

Further definitions are provided in the IAEA Nuclear Safety and Security Glossary: Terminology Used in Nuclear Safety, Nuclear Security, Radiation Protection and Emergency Preparedness and Response, IAEA, Vienna (2022): https://doi.org/10.61092/iaea.rrxi-t56z

challenge: Generalized mechanisms, processes or circumstances (conditions) that may have an impact on the intended performance of safety functions. Challenges are caused by a set of mechanisms having consequences that are similar in nature.

mechanisms: Specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.

objective tree: A graphical presentation, for each of the specific safety principles belonging to the five levels of defence in depth, of the following elements from top to bottom: (1) objective of the level; (2) relevant safety functions; (3) identified challenges; (4) constitutive mechanisms for each of the challenges; (5) a list of provisions in design and operation for preventing the mechanism from occurring.

provisions: Measures implemented in design and operation, such as inherent plant characteristics, safety margins, system design features and operational measures contributing to the performance of the safety functions aimed at completely or partially preventing the mechanisms from occurring.

safety principle: A commonly shared safety concept stating how to achieve safety objectives at different levels of defence in depth.

ABBREVIATIONS

ALARA	as low as reasonably achievable
AOO	anticipated operational occurrence
DBA	design basis accident
DEC	design extension condition
DEC-A	design extension condition without significant fuel degradation
DEC-B	design extension condition with core melting
EOP	emergency operating procedure
HTS	heat transport system
INSAG	International Nuclear Safety Advisory Group
LOCA	loss of coolant accident
NPP	nuclear power plant
PSA	probabilistic safety analysis
RCS	reactor coolant system
RPV	reactor pressure vessel
SAMG	severe accident management guideline
SFP	spent fuel pool
SP	safety principle
SSC	structure, system and component
TSC	technical support centre
UHS	ultimate heat sink
WENRA	Western European Nuclear Regulators Association

CONTRIBUTORS TO DRAFTING AND REVIEW

Doutt, C.	Consultant, United States of America
Duchac, A.	International Atomic Energy Agency
Luis Hernandez, J.	International Atomic Energy Agency
Machacek, J.	ČEZ, a. s., Czech Republic
Messiga, J.P.	Autoridad Regulatoria Nuclear, Argentina
Misak, J.	ÚJV Řež, a. s., Czech Republic
Poulat, B.	Consultant, France
Samokhin, A.	Scientific and Engineering Center on Nuclear and Radiation Safety, Russian Federation
Takahashi, H.	Japan Nuclear Safety Institute, Japan
Tiberi, V.	Institut de Radioprotection et de Sûreté Nucléaire, France
Tuomisto, H.	Fortum, Finland

Technical Meeting

Temelin NPP, Czech Republic: May 2021 (virtual)

Consultants Meetings

Vienna, Austria: 24 November 2020 (virtual)

Vienna, Austria: 23–25 March 2021 (virtual)

IAEA
International Atomic Energy Agency

No. 27

ORDERING LOCALLY

IAEA priced publications may be purchased from our lead distributor or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA.

Orders for priced publications

Please contact your preferred local supplier, or our lead distributor:

Eurospan
1 Bedford Row
London WC1R 4BU
United Kingdom

Trade orders and enquiries:
Tel: +44 (0)1235 465576
Email: trade.orders@marston.co.uk

Individual orders:
Tel: +44 (0)1235 465577
Email: direct.orders@marston.co.uk
www.eurospanbookstore.com/iaea

For further information:
Tel. +44 (0) 207 240 0856
Email: info@eurospan.co.uk
www.eurospan.co.uk

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

Publishing Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530
Email: sales.publications@iaea.org
www.iaea.org/publications

This publication describes the updated version of the method for the assessment of comprehensiveness of defence in depth and demonstrates the overall improvement in assessment results when using it. For assessment of comprehensiveness, five levels of defence in depth are considered. To ensure that safety objectives are met at each level of defence in depth, the integrity of relevant fission product barriers is maintained by the safety functions. A set of challenges to the performance of safety functions and the mechanisms leading to the challenges are specified by the method. Finally, a comprehensive list of safety provisions, which contribute to preventing these mechanisms from occurring, is specified. These provisions encompass the inherent safety features, equipment, procedures, personnel availability, personnel training and safety culture aspects. The challenges, mechanisms and provisions for all levels of defence in depth are presented in the assessment method in the form of objective trees.

International Atomic Energy Agency
Vienna, 2024
www.iaea.org