

IAEA Safety Standards

for protecting people and the environment

Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants

Specific Safety Guide

No. SSG-3



IAEA

International Atomic Energy Agency



Documents

Document Sharing Hub

IAEA SAFETY 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 at 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 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.

OTHER SAFETY 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 and protection 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 **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**.

DEVELOPMENT AND APPLICATION
OF LEVEL 1 PROBABILISTIC
SAFETY ASSESSMENT FOR
NUCLEAR POWER PLANTS

Safety standards survey

The IAEA welcomes your response. Please see:
<http://www-ns.iaea.org/standards/feedback.htm>



Documents
Document Sharing Hub

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

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

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

IAEA SAFETY STANDARDS SERIES No. SSG-3

DEVELOPMENT AND APPLICATION OF LEVEL 1 PROBABILISTIC SAFETY ASSESSMENT FOR NUCLEAR POWER PLANTS

SPECIFIC SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2010

COPYRIGHT NOTICE

All IAEA scientific and technical publications are protected by the terms of the Universal Copyright Convention as adopted in 1952 (Berne) and as revised in 1972 (Paris). The copyright has since been extended by the World Intellectual Property Organization (Geneva) to include electronic and virtual intellectual property. Permission to use whole or parts of texts contained in IAEA publications in printed or electronic form must be obtained and is usually subject to royalty agreements. Proposals for non-commercial reproductions and translations are welcomed and considered on a case-by-case basis. Enquiries should be addressed to the IAEA Publishing Section at:

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

© IAEA, 2010

Printed by the IAEA in Austria
April 2010
STI/PUB/1430

IAEA Library Cataloguing in Publication Data

Development and application of level 1 probabilistic safety assessment for nuclear power plants : specific safety guide. — Vienna : International Atomic Energy Agency, 2010.

p. ; 24 cm. — (IAEA safety standards series, ISSN 1020-525X ; no. SSG-3)

STI/PUB/1430

ISBN 978-92-0-114509-3

Includes bibliographical references.

1. Nuclear power plants — Risk assessment. 2. Nuclear power plants — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL

10-00612

FOREWORD

The IAEA's Statute authorizes the Agency to establish safety standards to protect health and minimize danger to life and property — standards which the IAEA must use in its own operations, and which a State can apply to its nuclear and radiation related facilities and activities. A comprehensive body of safety standards under regular review, together with the IAEA's assistance in their application, has become a key element in a global safety regime.

In the mid-1990s, a major overhaul of the IAEA's safety standards programme was initiated, with a revised oversight committee structure and a systematic approach to updating the entire corpus of standards. The new standards that have resulted are of a high calibre and reflect best practices in Member States. With the assistance of the Commission on Safety Standards, the Agency is working to promote the global acceptance and use of its safety standards.

Safety standards are only effective, however, if they are properly applied in practice. The IAEA's safety services — which range in scope from engineering safety, operational safety, and radiation, transport and waste safety to regulatory matters and safety culture in organizations — assist Member States in applying the standards and appraise their effectiveness. These safety services enable valuable insights to be shared and I continue to urge all Member States to make use of them.

Regulating safety in nuclear and radiation related activities is a national responsibility, and many Member States have decided to adopt the IAEA's safety standards for use in their national regulations. For the Contracting Parties to the various international safety conventions, IAEA standards provide a consistent, reliable means of ensuring the effective fulfillment of obligations under the conventions. The standards are also used around the world by organizations that design, manufacture and apply nuclear and radiation related technologies in power generation, medicine, industry, agriculture, research and education.

The IAEA takes seriously the enduring challenge for operators and regulators everywhere — of ensuring a high level of safety in the use of nuclear and radioactive materials around the world. Their continuing utilization for the benefit of humankind must be managed in a safe manner, and the IAEA safety standards are designed to facilitate the achievement of that goal.

THE IAEA SAFETY STANDARDS

BACKGROUND

Radioactivity is a natural phenomenon and natural sources of radiation are features of the environment. Radiation and radioactive substances have many beneficial applications, ranging from power generation to uses in medicine, industry and agriculture. The radiation risks to workers and the public and to the environment that may arise from these applications have to be assessed and, if necessary, controlled.

Activities such as the medical uses of radiation, the operation of nuclear installations, the production, transport and use of radioactive material, and the management of radioactive waste must therefore be subject to standards of safety.

Regulating safety is a national responsibility. However, radiation risks may transcend national borders, and international cooperation serves to promote and enhance safety globally by exchanging experience and by improving capabilities to control hazards, to prevent accidents, to respond to emergencies and to mitigate any harmful consequences.

States have an obligation of diligence and duty of care, and are expected to fulfil their national and international undertakings and obligations.

International safety standards provide support for States in meeting their obligations under general principles of international law, such as those relating to environmental protection. International safety standards also promote and assure confidence in safety and facilitate international commerce and trade.

A global nuclear safety regime is in place and is being continuously improved. IAEA safety standards, which support the implementation of binding international instruments and national safety infrastructures, are a cornerstone of this global regime. The IAEA safety standards constitute a useful tool for contracting parties to assess their performance under these international conventions.

THE IAEA SAFETY STANDARDS

The status of the IAEA safety standards derives from the IAEA's Statute, which authorizes the IAEA to establish or adopt, in consultation and, where appropriate, in collaboration with the competent organs of the United Nations and with the specialized agencies concerned, standards of safety for protection

of health and minimization of danger to life and property, and to provide for their application.

With a view to ensuring the protection of people and the environment from harmful effects of ionizing radiation, the IAEA safety standards establish fundamental safety principles, requirements and measures to control the radiation exposure of people and the release of radioactive material to the environment, to restrict the likelihood of events that might lead to a loss of control over a nuclear reactor core, nuclear chain reaction, radioactive source or any other source of radiation, and to mitigate the consequences of such events if they were to occur. The standards apply to facilities and activities that give rise to radiation risks, including nuclear installations, the use of radiation and radioactive sources, the transport of radioactive material and the management of radioactive waste.

Safety measures and security measures¹ have in common the aim of protecting human life and health and the environment. Safety measures and security measures must be designed and implemented in an integrated manner so that security measures do not compromise safety and safety measures do not compromise security.

The IAEA safety standards reflect an international consensus on what constitutes a high level of safety for protecting people and the environment from harmful effects of ionizing radiation. They are issued in the IAEA Safety Standards Series, which has three categories (see Fig. 1).

Safety Fundamentals

Safety Fundamentals present the fundamental safety objective and principles of protection and safety, and provide the basis for the safety requirements.

Safety Requirements

An integrated and consistent set of Safety Requirements establishes the requirements that must be met to ensure the protection of people and the environment, both now and in the future. The requirements are governed by the objective and principles of the Safety Fundamentals. If the requirements are not met, measures must be taken to reach or restore the required level of safety. The format and style of the requirements facilitate their use for the establishment, in a harmonized manner, of a national regulatory framework. The safety requirements use ‘shall’ statements together with statements of

¹ See also publications issued in the IAEA Nuclear Security Series.

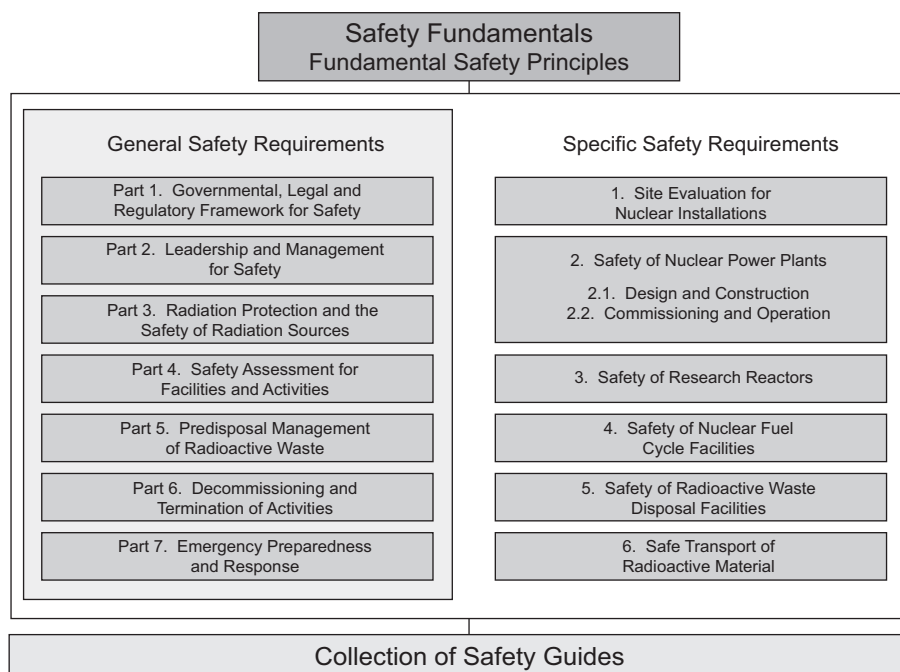


FIG. 1. The long term structure of the IAEA Safety Standards Series.

associated conditions to be met. Many requirements are not addressed to a specific party, the implication being that the appropriate parties are responsible for fulfilling them.

Safety Guides

Safety Guides provide recommendations and guidance on how to comply with the safety requirements, indicating an international consensus that it is necessary to take the measures recommended (or equivalent alternative measures). The Safety Guides present international good practices, and increasingly they reflect best practices, to help users striving to achieve high levels of safety. The recommendations provided in Safety Guides are expressed as ‘should’ statements.

APPLICATION OF THE IAEA SAFETY STANDARDS

The principal users of safety standards in IAEA Member States are regulatory bodies and other relevant national authorities. The IAEA safety

standards are also used by co-sponsoring organizations and by many organizations that design, construct and operate nuclear facilities, as well as organizations involved in the use of radiation and radioactive sources.

The IAEA safety standards are applicable, as relevant, throughout the entire lifetime of all facilities and activities — existing and new — utilized for peaceful purposes and to protective actions to reduce existing radiation risks. They can be used by States as a reference for their national regulations in respect of facilities and activities.

The IAEA's Statute makes the safety standards binding on the IAEA in relation to its own operations and also on States in relation to IAEA assisted operations.

The IAEA safety standards also form the basis for the IAEA's safety review services, and they are used by the IAEA in support of competence building, including the development of educational curricula and training courses.

International conventions contain requirements similar to those in the IAEA safety standards and make them binding on contracting parties. The IAEA safety standards, supplemented by international conventions, industry standards and detailed national requirements, establish a consistent basis for protecting people and the environment. There will also be some special aspects of safety that need to be assessed at the national level. For example, many of the IAEA safety standards, in particular those addressing aspects of safety in planning or design, are intended to apply primarily to new facilities and activities. The requirements established in the IAEA safety standards might not be fully met at some existing facilities that were built to earlier standards. The way in which IAEA safety standards are to be applied to such facilities is a decision for individual States.

The scientific considerations underlying the IAEA safety standards provide an objective basis for decisions concerning safety; however, decision makers must also make informed judgements and must determine how best to balance the benefits of an action or an activity against the associated radiation risks and any other detrimental impacts to which it gives rise.

DEVELOPMENT PROCESS FOR THE IAEA SAFETY STANDARDS

The preparation and review of the safety standards involves the IAEA Secretariat and four safety standards committees, for nuclear safety (NUSSC), radiation safety (RASSC), the safety of radioactive waste (WASSC) and the safe transport of radioactive material (TRANSSC), and a Commission on Safety Standards (CSS) which oversees the IAEA safety standards programme (see Fig. 2).

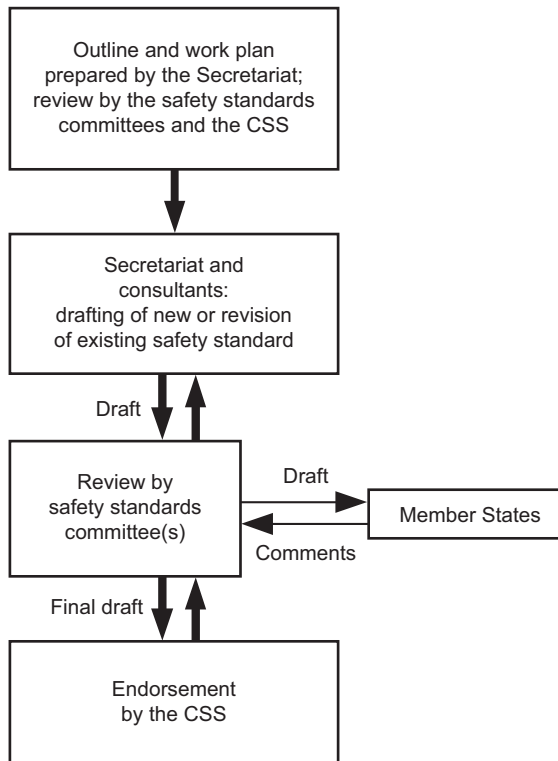


FIG. 2. The process for developing a new safety standard or revising an existing standard.

All IAEA Member States may nominate experts for the safety standards committees and may provide comments on draft standards. The membership of the Commission on Safety Standards is appointed by the Director General and includes senior governmental officials having responsibility for establishing national standards.

A management system has been established for the processes of planning, developing, reviewing, revising and establishing the IAEA safety standards. It articulates the mandate of the IAEA, the vision for the future application of the safety standards, policies and strategies, and corresponding functions and responsibilities.

INTERACTION WITH OTHER INTERNATIONAL ORGANIZATIONS

The findings of the United Nations Scientific Committee on the Effects of Atomic Radiation (UNSCEAR) and the recommendations of international

expert bodies, notably the International Commission on Radiological Protection (ICRP), are taken into account in developing the IAEA safety standards. Some safety standards are developed in cooperation with other bodies in the United Nations system or other specialized agencies, including the Food and Agriculture Organization of the United Nations, the United Nations Environment Programme, the International Labour Organization, the OECD Nuclear Energy Agency, the Pan American Health Organization and the World Health Organization.

INTERPRETATION OF THE TEXT

Safety related terms are to be understood as defined in the IAEA Safety Glossary (see <http://www-ns.iaea.org/standards/safety-glossary.htm>). Otherwise, words are used with the spellings and meanings assigned to them in the latest edition of The Concise Oxford Dictionary. For Safety Guides, the English version of the text is the authoritative version.

The background and context of each standard in the IAEA Safety Standards Series and its objective, scope and structure are explained in Section 1, Introduction, of each publication.

Material for which there is no appropriate place in the body text (e.g. material that is subsidiary to or separate from the body text, is included in support of statements in the body text, or describes methods of calculation, procedures or limits and conditions) may be presented in appendices or annexes.

An appendix, if included, is considered to form an integral part of the safety standard. Material in an appendix has the same status as the body text, and the IAEA assumes authorship of it. Annexes and footnotes to the main text, if included, are used to provide practical examples or additional information or explanation. Annexes and footnotes are not integral parts of the main text. Annex material published by the IAEA is not necessarily issued under its authorship; material under other authorship may be presented in annexes to the safety standards. Extraneous material presented in annexes is excerpted and adapted as necessary to be generally useful.

CONTENTS

1.	INTRODUCTION	1
	Background (1.1–1.8)	1
	Objective (1.9–1.11)	4
	Scope (1.12–1.16)	5
	Structure (1.17)	5
2.	GENERAL CONSIDERATIONS RELATING TO THE PERFORMANCE AND USE OF PSA (2.1)	6
	Scope of the PSA (2.2–2.4)	6
	Validation and review of the PSA (2.5–2.6)	7
	Living PSA (2.7–2.9)	8
	Reference values (safety goals or criteria) (2.10–2.20)	9
	Use of PSA in decision making (2.21–2.31)	12
3.	PROJECT MANAGEMENT AND ORGANIZATION FOR PSA ...	15
	Definition of objectives and scope of the PSA project (3.1–3.2)	15
	Project management for PSA (3.3–3.7)	16
	Selection of methods and establishment of procedures (3.8–3.9)	17
	Team selection and organization (3.10–3.12)	18
	Establishment of a quality assurance programme for PSA (3.13–3.14)	18
	General aspects of PSA documentation (3.15–3.22)	19
4.	FAMILIARIZATION WITH THE PLANT AND COLLECTION OF INFORMATION (4.1–4.3)	21
5.	LEVEL 1 PSA FOR INTERNAL INITIATING EVENTS FOR FULL POWER OPERATING CONDITIONS (5.1–5.2)	23
	General aspects of Level 1 PSA methodology (5.3–5.10)	23
	Initiating event analysis (5.11–5.39)	25
	Accident sequence analysis (5.40–5.68)	30
	Systems analysis (5.69–5.85)	36
	Analysis of dependent failures (5.86–5.91)	40
	Analysis of common cause failures (5.92–5.95)	41
	Human reliability analysis (5.96–5.113)	42

Other modelling issues (5.114–5.120)	46
Data required for a Level 1 PSA (5.121–5.139)	47
Quantification of the analysis (5.140–5.150)	50
Importance analysis, sensitivity studies and uncertainty analysis (5.151–5.160).	52
6. GENERAL METHODOLOGY FOR LEVEL 1 PSA FOR INTERNAL AND EXTERNAL HAZARDS	55
Introduction (6.1)	55
Analysis process (6.2–6.5)	56
Collection of initial information (6.6–6.7)	58
Identification of hazards (6.8–6.13)	59
Screening of hazards (6.14–6.25)	61
7. SPECIFICS OF LEVEL 1 PSA FOR INTERNAL HAZARDS	64
Introduction (7.1)	64
Bounding assessment and detailed analysis for Level 1 PSA for internal hazards (7.2–7.11)	65
Analysis of internal fire (7.12–7.65)	67
Analysis of internal flooding (7.66–7.92)	81
Other internal hazards (7.93–7.114)	88
8. SPECIFICS OF LEVEL 1 PSA FOR EXTERNAL HAZARDS	91
Introduction (8.1)	91
General aspects of bounding analysis for external hazards (8.2–8.14)	91
Parameterization of external hazards (8.15–8.28)	94
Detailed analysis of external hazards (8.29–8.32)	97
Frequency assessment for external hazards (8.33–8.58)	98
Fragility analysis for structures and components (8.59–8.80)	103
Integration of external hazards in the Level 1 PSA model (8.81–8.100)	107
Documentation and presentation of results (8.101–8.111)	111
9. LEVEL 1 PSA FOR LOW POWER AND SHUTDOWN MODES	114
General aspects of Level 1 PSA for low power and shutdown modes (9.1–9.3)	114

Specification of outage types and plant operational states (9.4–9.10)	115
Initiating events analysis (9.11–9.21)	118
Accident sequence analysis (9.22–9.30)	121
Systems analysis (9.31)	124
Analysis of dependent failures (9.32–9.35)	125
Human reliability analysis (9.36–9.45)	126
Data assessment (9.46–9.55)	128
Quantification of accident sequences (9.56–9.57)	130
Importance analysis, sensitivity studies and uncertainty analysis (9.58–9.60)	131
Documentation and presentation of results (9.61–9.71)	131
 10. USE AND APPLICATIONS OF PSA	 133
Scope of PSA for applications (10.1–10.5)	133
Risk informed approach (10.6–10.7)	135
Use of PSA for design evaluation (10.8–10.27)	136
Risk informed technical specifications (10.28–10.35)	140
Risk monitors (10.36–10.54)	141
Risk informed in-service inspection (10.55–10.64)	145
Risk informed in-service testing (10.65–10.69)	147
Graded quality assurance (10.70–10.75)	148
PSA based safety performance indicators (10.76–10.77)	150
PSA based event analysis (10.78–10.83)	150
Risk informed regulations (10.84–10.89)	151
 REFERENCES	 153
 ANNEX I: EXAMPLE OF A GENERIC LIST OF INTERNAL AND EXTERNAL HAZARDS	 155
 ANNEX II: EXAMPLES OF FIRE PROPAGATION EVENT TREES AND SEISMIC EVENT TREES	 165
 ANNEX III: SUPPORTING INFORMATION ON PSA FOR LOW POWER AND SHUTDOWN MODES	 167
 CONTRIBUTORS TO DRAFTING AND REVIEW	 185
BODIES FOR THE ENDORSEMENT OF IAEA SAFETY STANDARDS	189

1. INTRODUCTION

BACKGROUND

1.1. It is generally recognized that facilities and activities dealing with radioactive material provide many benefits, but at the same time give rise to radiation risks. The Safety Fundamentals, Fundamental Safety Principles [1], establish principles to ensure the protection of workers, the public and the environment, now and in the future, from the harmful effects of ionizing radiation. These principles emphasize the need to assess and control the inherent risk. In particular, Principle 5 of Ref. [1] (para. 3.22) on optimization of protection states:

“To determine whether radiation risks are as low as reasonably achievable, all such risks, whether arising from normal operations or from abnormal or accident conditions, must be assessed (using a graded approach) a priori and periodically reassessed throughout the lifetime of facilities and activities.”

1.2. Several IAEA Safety Requirements publications establish more specific requirements for risk assessment for nuclear power plants. The Safety Requirements publication on Safety of Nuclear Power Plants: Design [2] (para. 5.69) establishes that:

“A safety analysis of the plant design shall be conducted in which methods of both deterministic and probabilistic analysis shall be applied. On the basis of this analysis, the design basis for items important to safety shall be established and confirmed.”

It is also emphasized further in Ref. [2] (para. 5.73) that:

“A probabilistic safety analysis of the plant shall be carried out in order:

- (1) to provide a systematic analysis to give confidence that the design will comply with the general safety objectives;
- (2) to demonstrate that a balanced design has been achieved such that no particular feature or PIE¹ makes a disproportionately large or

¹ PIE: postulated initiating event.

significantly uncertain contribution to the overall risk, and that the first two levels of defence in depth bear the primary burden of ensuring nuclear safety;

- (3) to provide confidence that small deviations in plant parameters that could give rise to severely abnormal plant behaviour ('cliff edge effects') will be prevented;
- (4) to provide assessments of the probabilities of occurrence of severe core damage states and assessments of the risks of major off-site releases necessitating a short term off-site response, particularly for releases associated with early containment failure;
- (5) to provide assessments of the probabilities of occurrence and the consequences of external hazards, in particular those unique to the plant site;
- (6) to identify systems for which design improvements or modifications to operational procedures could reduce the probabilities of severe accidents or mitigate their consequences;
- (7) to assess the adequacy of plant emergency procedures; and
- (8) to verify compliance with probabilistic targets, if set."

1.3. Thus, probabilistic safety assessment (PSA) is considered to be an important tool for analysis for ensuring the safety of a nuclear power plant in relation to potential initiating events that can be caused by random component failure and human error, as well as internal and external hazards.

1.4. The Safety Requirements publication on Safety Assessment for Facilities and Activities [3] (para. 4.13) emphasizing the need for a comprehensive safety analysis states:

"The safety assessment has to include a safety analysis, which consists of a set of different quantitative analyses for evaluating and assessing challenges to safety in various operational states, anticipated operational occurrences and accident conditions, by means of deterministic and also probabilistic methods."

It is also stated in Ref. [3] (para. 4.55):

"The objectives of a probabilistic safety analysis are to determine all significant contributing factors to the radiation risks arising from a facility or activity, and to evaluate the extent to which the overall design is well balanced and meets probabilistic safety criteria where these have been defined."

Thus, a comprehensive PSA is required to investigate the safety of a nuclear power plant thoroughly.

1.5. PSA has been shown to provide important safety insights in addition to those provided by deterministic analysis. PSA provides a methodological approach to identifying accident sequences that can follow from a broad range of initiating events and it includes a systematic and realistic determination of accident frequencies and consequences. In international practice, three levels of PSA are generally recognized:

- (1) In Level 1 PSA, the design and operation of the plant are analysed in order to identify the sequences of events that can lead to core damage and the core damage frequency is estimated. Level 1 PSA provides insights into the strengths and weaknesses of the safety related systems and procedures in place or envisaged as preventing core damage.
- (2) In Level 2 PSA, the chronological progression of core damage sequences identified in Level 1 PSA is evaluated, including a quantitative assessment of phenomena arising from severe damage to reactor fuel. Level 2 PSA identifies ways in which associated releases of radioactive material from fuel can result in releases to the environment. It also estimates the frequency, magnitude and other relevant characteristics of the release of radioactive material to the environment. This analysis provides additional insights into the relative importance of accident prevention and mitigation measures and the physical barriers to the release of radioactive material to the environment (e.g. a containment building).
- (3) In Level 3 PSA, public health and other societal consequences are estimated, such as the contamination of land or food from the accident sequences that lead to a release of radioactivity to the environment.

1.6. Level 1 PSA, Level 2 PSA and Level 3 PSA are sequential analyses, where the results of each assessment usually serve as a basis for the PSA at the next level. Level 1 PSA provides insights into design weaknesses and into ways of preventing accidents leading to core damage, which might be the precursor of accidents leading to major releases of radioactive material with potential consequences for human health and the environment. Level 2 PSA provides additional insights into the relative importance of accident sequences leading to core damage in terms of the severity of the releases of radioactive material they might cause, and insights into weaknesses in measures for the mitigation and management of severe accidents and ways of improving them. Finally, Level 3 PSA provides insights into the relative importance of accident prevention and mitigation measures, expressed in terms of adverse consequences for the

health of both plant workers and the public, and the contamination of land, air, water and foodstuffs. In addition, Level 3 PSA provides insights into the relative effectiveness of aspects of accident management relating to emergency preparedness and response.

1.7. Level 1 PSAs have now been carried out for most nuclear power plants worldwide. In recent years, a trend has emerged for Level 2 PSAs or limited Level 2 PSAs (e.g. Level 2 PSAs in which the large early release frequency is estimated) to be carried out for many types of nuclear power plant. In addition, Level 3 PSAs have been carried out in several States.

1.8. This Safety Guide was prepared on the basis of a systematic review of relevant publications, including Refs [1–3], current and ongoing revisions of other Safety Guides, an International Nuclear Safety Advisory Group (INSAG) report [4] and other publications that address the safety of nuclear power plants.

OBJECTIVE

1.9. The objective of this Safety Guide is to provide recommendations for meeting the requirements of Ref. [3] in performing or managing a Level 1 PSA project for a nuclear power plant and using it to support its safe design and operation. This Safety Guide is applicable to existing nuclear power plants and to evolutionary designs of nuclear power plants, but may not be fully applicable to revolutionary designs. The recommendations provided in this Safety Guide aim to promote technical consistency among Level 1 PSA studies in order to provide reliable support for applications of PSA and risk informed decision making. A further aim of this Safety Guide is to recommend a standard framework that can facilitate a regulatory review or an external peer review of a Level 1 PSA and its various applications.

1.10. This Safety Guide also provides a consistent, reliable means of ensuring the effective fulfilment of obligations under Article 14 of the Convention on Nuclear Safety [5].

1.11. The recommendations presented in this Safety Guide are based on internationally recognized good practices. However, it is not intended to pre-empt the use of equivalent new or alternative methods. On the contrary, the use of any method that achieves the objectives of Level 1 PSA is encouraged. However, the framework for PSA outlined in this Safety Guide is expected to apply for the foreseeable future.

SCOPE

1.12. This Safety Guide addresses the necessary technical features of a Level 1 PSA and applications for nuclear power plants, on the basis of internationally recognized good practices. The scope of a Level 1 PSA addressed in this Safety Guide includes all operational conditions of the plant (i.e. full power, low power and shutdown) and all potential initiating events and potential hazards, namely: (a) internal initiating events caused by random component failures and human error, (b) internal hazards (e.g. internal fires and floods, turbine missiles) and (c) external hazards, both natural (e.g. earthquake, high winds, external floods) and of human-induced (e.g. airplane crash, accidents at nearby industrial facilities).

1.13. This Safety Guide is focused on the reactor core; it does not cover other sources of radioactive material on the site, e.g. the spent fuel pool. However, while considering Level 1 PSA for low power and shutdown modes (Section 9), the risk from the fuel removed from the reactor is also addressed.

1.14. The consideration of hazards arising from malicious actions does not lie within the scope of this Safety Guide.

1.15. In carrying out Level 1 PSA, the most common practice is to perform the analysis for the various hazards and operational modes in separate modules, having a Level 1 PSA for full power operating conditions for internal initiating events as a basis. This Safety Guide follows this approach.

1.16. The recommendations of this Safety Guide are intended to be technology neutral to the extent possible, and it is expected that the vast majority of the recommendations will be applicable to different types of nuclear power plant. However, examples, where deemed necessary, are mainly provided for light water cooled nuclear power plants. Interpretation or judgement may be necessary when applying some recommendations to other types of nuclear power plant.

STRUCTURE

1.17. Section 2 provides recommendations on the general issues concerning the performance and use of PSA, including the scope of the PSA, validation of the PSA and a living PSA. Section 3 provides key recommendations on project management and organization for PSA and general aspects of PSA documentation. Section 4 addresses the task of familiarization of the team

carrying out the PSA with the nuclear power plant. Sections 5–8 provide recommendations on the methodology of a Level 1 PSA for full power operating conditions for various initiating events and hazards. Section 5 provides recommendations on Level 1 PSA for internal initiating events. Section 6 summarizes key recommendations on the general aspects of Level 1 PSA for internal and external hazards, and Sections 7 and 8 address the specifics of Level 1 PSA for internal hazards and external hazards, respectively. Section 9 provides key recommendations for Level 1 PSA for low power and shutdown modes. Section 10 sets out key recommendations for applications of Level 1 PSA. Three annexes provide an example of a generic list of internal and external hazards, an example of a fire propagation event tree and a seismic event tree, and supporting information on PSA for low power and shutdown modes.

2. GENERAL CONSIDERATIONS RELATING TO THE PERFORMANCE AND USE OF PSA

2.1. This section describes some general issues relevant to the performance of PSA and the use of PSA results in practice. Though the scope of the Safety Guide is limited to consideration of Level 1 PSA, this section describes the issues from a broader perspective in order to provide a complete picture of the capabilities of PSA technology and its results. Some statements in this section do not represent explicit recommendations; rather, they provide supporting information to facilitate understanding of the context of other statements and recommendations provided in other sections of the Safety Guide.

SCOPE OF THE PSA

2.2. Paragraphs 2.2–2.4 provide recommendations on meeting Requirement 1 on a graded approach and Requirement 14 relating to the scope of the safety analysis for a PSA [3]. The scope of the PSA to be undertaken should be correlated with the national safety goals or criteria, if the latter have been set. At a high level, quantitative results of PSA are often used to verify compliance with safety goals or criteria, which are usually formulated in terms of quantitative estimates of core damage frequency, frequencies of radioactive releases of different types and societal risks and which therefore may necessitate performance of a Level 1 PSA, Level 2 PSA or Level 3 PSA, respectively. Safety

goals or criteria do not usually specify which hazards and plant operational modes have to be addressed. Therefore, in order to use the PSA results for the verification of compliance with existing safety goals or criteria, a full scope PSA involving a comprehensive list of initiating events and hazards and all plant operational modes should be performed unless the safety goals or criteria are formulated to specify a PSA of limited scope, or alternative approaches are used to demonstrate that the risk from those initiating events and hazards and operational modes that are not in the model does not threaten compliance with the safety goals or criteria.

2.3. If the PSA is carried out only to Level 1, then the reactor core is usually the focus of the analysis. If the PSA is carried out to Level 2 or Level 3, where the impact of radioactive releases has to be assessed, then the scope of the PSA may include contributions to risk arising from other radioactive material on the site, such as spent fuel and radioactive waste. Such sources of radioactivity outside the core should be included in the PSA whenever the intention is to address the total risk from the plant to members of the public near the site.

2.4. A major advantage of PSA is that it provides an explicit framework for the analysis of uncertainties in risk estimates. The identification of sources of uncertainty and an understanding of their implications on the PSA model and its results should be considered an inherent part of any PSA, so that, when the results of the PSA are to be used to support a decision, the impact of the uncertainties can be taken into account.

VALIDATION AND REVIEW OF THE PSA

2.5. Paragraphs 2.5 and 2.6 provide recommendations on meeting Requirement 18 on the use and validation of computer codes for a PSA and Requirement 21 on the independent verification of PSA [3]. PSA involves a number of analytical methods. These include the development of event tree and fault tree logic models used for analysis of accident sequences, the methods for solution of the logic models, the models of phenomena that could occur, for instance, within the containment of a nuclear power plant following core damage, and the models for the transport of radionuclides in the environment to determine their effects on health and the economy, depending on the scope of the analysis (Level 1, 2 or 3). Prior to their application, it should be demonstrated that these analytical methods provide an adequate representation of the processes taking place. The computer codes that support these analytical methods should be adequate for the purpose and scope of

the analysis and the controlling physical and logical equations should be correctly programmed in the computer codes (Ref. [3], para. 4.60).

2.6. It is a widely accepted practice for the organization conducting a PSA to commission an independent peer review of the PSA from an outside body, sometimes from a different State, to provide a degree of assurance that the scope, modelling and data are adequate, and to ensure that they conform to current, internationally recognized good practices in PSA. The experts involved in the review of the PSA should not be engaged in any activities relating to performance of the PSA under consideration and should represent an organization that is independent of the developer of the PSA.

LIVING PSA

2.7. Paragraphs 2.7–2.9 provide recommendations on meeting Requirement 24 on maintenance of the safety assessment for Level 1 PSA [3]. In the operating lifetime of a nuclear power plant, modifications are often made to the design of safety systems or to the way the plant is operated. Such modifications could have an impact on the level of risk associated with the plant. Additional statistical data on the frequencies of initiating events and the probabilities of component failure will become available during plant operation. Likewise, new information and more sophisticated methods and tools may become available, which may change some of the assumptions made in the analysis and hence the estimates of the risk given by the PSA. Consequently, the PSA should be kept up to date throughout the lifetime of the plant to ensure that it remains relevant for the decision making process. A PSA that undergoes regular periodical updating is termed a ‘living PSA’. In updating a PSA, account should be taken of changes in the design and operation of the plant, new technical information, more sophisticated methods and tools that become available and new plant specific data derived from the operation of the plant, e.g. data to be used for the assessment of initiating event frequencies or component failure probabilities. The updating of a PSA should be initiated by a specified process and the status of the PSA should be reviewed regularly to ensure that it is maintained as a representative model of the plant and fits the purpose it is intended for.

2.8. Data should be collected throughout the lifetime of the plant to check or update the analysis. Such data should include data on operational experience, in particular data on initiating events, data on component failures and unavailability during periods of testing, maintenance and repair, and data on human

performance. The results from the analysis should be periodically reassessed in the light of new data.

2.9. The development of a living PSA should be encouraged to assist the decision making process in the normal operation of the plant. Many issues, such as evaluation of the change in risk associated with a change to the plant or a temporary change in the allowed outage time of a component, can be supported by arguments derived from a PSA. Experience has shown that such a living PSA can be of substantial benefit to the operating organization and its use is generally welcomed by regulators.

REFERENCE VALUES (SAFETY GOALS OR CRITERIA)

2.10. Paragraphs 2.10–2.20 provide recommendations on meeting Requirement 4 for the purpose of conducting a PSA [3]. When the aim of the PSA is to identify significant contributors to risk or to choose between various design options and plant configurations, a reference value may not be necessary. However, when the aim of the PSA is to assist in reaching a judgement on whether (i) a calculated risk is acceptable, (ii) a proposed change to the design or operation of the plant is acceptable, or (iii) a change is necessary to reduce the level of risk, then probabilistic reference values should be specified to provide guidance to designers, operators, regulators and other interested parties in fulfilling their respective roles in the provision of safe nuclear power, on the level of safety desired or required for the plant. In some States, current practice is for reference values to be formulated as safety goals, with the implication that they represent orientation values whose achievement is to be aimed for. In other States, the reference values are criteria that specify strict limits for which compliance is required.

2.11. A PSA will yield numerical values relating to risk at various levels, depending on the consequences to be evaluated. Probabilistic safety goals or criteria may be set in relation to any or all of the following measures:

- (a) The probability of failure of particular safety functions or safety systems;
- (b) The frequency of core damage² (Level 1 PSA);
- (c) The frequency of a specific release (specified, for example, in terms of its quantity, isotopes, timing) of radioactive material from the plant or the

² For the concept of core damage, specific criteria have to be specified, as described in Section 5 of this Safety Guide. These criteria may be different for different reactor designs.

frequency of a release of radioactive material as a function of its magnitude (Level 2 PSA);

- (d) The frequency of occurrence of specific health effects to members of the public or the frequency of occurrence of particular environmental consequences (Level 3 PSA).

2.12. One possible framework for the definition of probabilistic safety criteria is given in Ref. [6], which defines a ‘threshold of tolerability’ above which the level of risk would be intolerable, and a ‘design target’ below which the risk would be broadly acceptable. Between these two levels there is a region where the risk would be acceptable only if all reasonably achievable measures have been taken to reduce the risk. Although this approach has been adopted in some States, it is more usual to find probabilistic safety criteria identified as targets, goals, objectives, guidelines or reference values for orientation. In addition, the numerical values for the levels of risk, which correspond to the threshold of tolerability and the design targets, differ from State to State.

2.13. For the probability of failure of safety functions or safety systems, the probabilistic targets can be set at the level of the safety function or safety system. Such probabilistic targets are useful for checking that the level of redundancy and diversity provided is adequate. Such targets will be specific to the plant design and therefore no recommendations on setting such targets can be provided here. In the safety assessment, it should be checked whether these targets have been met. If they have not, the design may still be acceptable provided that the higher level criteria have been met. However, particular consideration should be given to the safety systems in question to see whether any reasonably practicable improvements can be made.

2.14. On the basis of current experience with the design and operation of nuclear power plants, INSAG, in 1999, proposed numerical values that can be achieved for current and proposed designs of nuclear power plants.

2.15. INSAG (see Ref. [4]) has proposed the objectives for core damage frequency separately for existing plants and future plants.³

³ The objectives for core damage frequency in Ref. [4] are (a) 1×10^{-4} per reactor-year for existing plants and (b) 1×10^{-5} per reactor-year for future plants. It was not explicitly specified in Ref. [4] for which scope of PSA the numerical values are applicable. It is assumed that a full scope PSA is meant.

2.16. Core damage frequency is the most common measure of risk since most nuclear power plants have undergone at least a Level 1 PSA and the methodology is well established. In many States, numerical values of this type are used either formally or informally as probabilistic safety goals or criteria.

2.17. Large off-site release of radioactive material: A large release of radioactive material, which would have severe implications for society and would require off-site emergency arrangements to be implemented, can be specified in a number of ways, including the following:

- (a) As absolute quantities (in bequerels) of the most significant nuclides released;
- (b) As a fraction of the inventory of the core;
- (c) As a specified dose to the most exposed person off the site;
- (d) As a release incurring ‘unacceptable consequences’.

In some cases, criteria are specified that relate to the timing of the release, in particular whether the release occurs early or late. In such cases, the term ‘early’ needs to be defined.

2.18. The objectives have also been proposed by INSAG for a large off-site release of radioactive material requiring short term off-site response.⁴

2.19. Although there is no international consensus on what constitutes a large off-site release, similar probabilistic criteria have been specified in a number of States.

2.20. Health effects to members of the public: INSAG has given no guidance on targets for health effects for members of the public.⁵

⁴ The objective for large off-site releases requiring short term off-site response is 1×10^{-5} per reactor-year for existing plants. Reference [4] does not specify a numerical value for a large off-site radioactive release for future plants, but states the following qualitative objective: “Another objective for these future plants is the practical elimination of accident sequences that could lead to large early radioactive releases, whereas severe accidents that could imply late containment failure would be considered in the design process with realistic assumptions and best estimate analyses so that their consequences would necessitate only protective measures limited in area and in time.”

⁵ In some States, the target for the risk of death of a member of the public is taken to be 1×10^{-6} per reactor-year.

USE OF PSA IN DECISION MAKING

2.21. Paragraphs 2.21–2.31 provide recommendations on meeting Requirement 23 of Ref. [3] on the use of a Level 1 PSA. The PSA should be used during the lifetime of the plant to provide an input into decision making in combination with the results and insights of deterministic safety analyses and considerations of defence in depth.

2.22. PSA can provide useful insights and inputs for various interested parties, such as plant staff (management and engineering, operations and maintenance personnel), regulatory bodies, designers and vendors, for making decisions on:

- (a) Design modifications and plant modifications;
- (b) Optimization of plant operation and maintenance;
- (c) Safety analysis and research programmes;
- (d) Regulatory issues.

2.23. Where the results of the PSA are to be used in support of the decision making process, a formal framework for doing so should be established. The details of the decision making process will depend on the purpose of the particular PSA application, the nature of the decision to be made and the PSA results to be used. If numerical results from the PSA are to be used, reference values against which these results can be compared should be established.

2.24. The PSA should address the actual or, in the case of a plant under construction or when modifications are being undertaken, the intended design or operation of the plant, which should be clearly identified as the basis for the analysis. The status of the plant can be fixed as it was on a specific date or as it will be when agreed modifications are completed. This needs to be done to provide a clear target for completion of the PSA. Later changes can be addressed in the framework of a living PSA programme, as described in paras 2.7–2.9.

2.25. For a plant in the design stage, the results of PSA should be used as part of the design process to assess the level of safety. In this case, the insights gained from PSA should be considered in combination with the insights gained from deterministic analysis to make decisions about the safety of the plant. Decisions on the safety of the plant should be the result of an iterative process aimed at ensuring that national requirements and criteria are met, the design is balanced and the risk is as low as reasonably achievable.

2.26. In addition, the results of the PSA should be compared with the probabilistic safety goals or criteria if these have been specified in national

regulations or guidelines, etc. This should be done for all probabilistic criteria defined for the plant, including those that address system reliability, core damage, releases of radioactive material, health effects for workers, health effects for the public and off-site consequences such as land contamination and food bans.

2.27. The PSA should set out to identify all accident sequences that contribute to risk and to determine if there are weaknesses in the design or operation of the plant. The PSA can be used, for example, to assess the need for changes to reduce the safety significance of such weaknesses. If the analysis does not address all the contributions to risk (for example, if it omits external hazards or shutdown states), then conclusions drawn from the PSA about the level of risk from the plant, the balance of the safety systems provided and the need for changes to be made to the design or operation to reduce the risk may be biased.

2.28. The results of the Level 1 PSA should be used to identify weaknesses in the design or operation of the plant. Weaknesses can be identified by considering the contributions to the risk from groups of initiating events, the importance measures of the safety systems and the contributions of human error to the overall risk. Where the results of the PSA indicate that changes could be made to the design or operation of the plant to reduce risk, the changes should be incorporated where reasonably achievable, taking the relative costs and benefits of any modifications into account.

2.29. The results of the Level 2 PSA should be used to determine if sufficient provision has been made to prevent or mitigate the effects of postulated core damage sequences. In Level 2 PSA, it should be considered whether the containment is adequately robust and whether the protection systems such as hydrogen mixing and recombining systems, containment sprays and containment venting systems provide an adequate level of protection to prevent a large release of radioactive material to the environment. Furthermore, containment bypassing events such as a loss of coolant accident in interfacing systems should be addressed. In addition, Level 2 PSA should be used to identify and optimize accident management measures that could be carried out to mitigate the effects of the damaged core. This could include determining additional measures, for example, measures that could be taken to introduce water into the reactor containment.

2.30. When available, the results of Level 2 PSA and Level 3 PSA should be provided to civil authorities as a technical input for off-site emergency planning.

2.31. Section 10 provides detailed recommendations on specific applications of PSA for the regulatory body and for operating organizations. However, for the sake of convenience and continuity in covering the general aspects of PSA, a summary of the main recommendations relating to application of PSA is provided in the following:

- (a) The results of the PSA should be used in developing emergency procedures for accidents and to provide inputs into the technical specifications of the plant. In particular, the results of the PSA should be used to investigate the increase in risk after the removal from service of items of equipment for testing or maintenance and the adequacy of the frequency of surveillance or testing. The PSA should be used to confirm that the allowed outage times do not contribute unduly to risk and to indicate which combinations of equipment outages should be avoided.
- (b) The PSA should be used throughout the design and operation of the plant to assist in the decision making process on the safety of the plant:
 - (i) For a new plant, the PSA should be initiated in the conceptual design stage to check that the level of redundancy and diversity provided in the safety systems is adequate. The PSA should be continued through the more detailed design stage to assess more detailed design issues and should be used to support operation of the plant. In the design stage, an iterative process should be put in place to ensure that the insights gained from the PSA are fed back into the design process.
 - (ii) For an existing plant, the PSA should be carried out either as part of a periodic safety assessment or to support the safety case for proposed modifications. Although the requirements for the PSA remain the same, the data used may vary with the experience accumulated. Moreover, depending on the age of the facility, the remaining operational lifetime, the cost of proposed modifications and other related considerations, there will be differences in what changes could reasonably be implemented to reduce risk. Such considerations should take account of the possibility of plant life extension, irrespective of whether such a life extension has been applied for or is only being considered.
- (c) The PSA should be used to determine if the safety systems contain an adequate level of redundancy and diversity and if the overall design is balanced. As indications of a balanced design, the results of the PSA should show that:
 - (i) No particular feature of the design or of the group of initiating events makes a disproportionately large contribution to risk;
 - (ii) The achievement of an overall low level of risk does not rely on contributors that have significant uncertainty.

A lack of balance in the design is often an indication that there are opportunities for implementing reasonably practicable measures to reduce risk.

3. PROJECT MANAGEMENT AND ORGANIZATION FOR PSA

DEFINITION OF OBJECTIVES AND SCOPE OF THE PSA PROJECT

3.1. Paragraphs 3.1 and 3.2 provide recommendations on meeting Requirement 4 of Ref. [3] on purpose of the Level 1 PSA and Requirement 14 relating to the scope of a Level 1 PSA [3]. Determination of the objectives of the PSA together with its intended and potential uses is an important step to undertake prior to starting the process of performing a PSA. The scope of the PSA is defined by the analysis level (Level 1, 2 or 3), the initiating events and hazards considered, and the operational modes (i.e. full power, low power or shutdown states⁶) addressed. The scope of the PSA should be compatible with both the objectives of the study and the available resources and information, i.e. the necessary procedures and methods, personnel, expertise, funding and the time needed for the analysis. For example, if the objective of a PSA is to verify the risk arising from plant operation against specified safety goals, thus implying a complete risk assessment, a full scope PSA comprising a comprehensive listing of initiating events and hazards and all plant operational modes should be performed, and adequate resources should be provided for the analysis. In addition, other sources of radiation (e.g. the spent fuel pool) may need to be analysed, depending on the formulation of the safety goals.

3.2. It should be recognized that the intended applications of PSA may impose additional requirements on the scope of the PSA, on the modelling approaches and on the level of detail. If such additional requirements are taken into account at the planning stage of the PSA project, it will help to avoid inconsistencies in the results and insights obtained. For instance, if it is planned to use the PSA for the development of a severe accident management programme, a Level 2 PSA should be performed. As another example, if it is planned to use the PSA model as a basis for a risk monitor, the PSA model should be ‘symmetrical’ in terms of the modelling of initiating events. The common simplification of modelling an

⁶ PSA for low power and shutdown states is usually performed as part of the same study.

initiating event as always occurring in one particular train should not be used. For example, loss of coolant accidents should be modelled for each loop with an appropriate probability that a specific loop is affected (i.e. 1/2 for a two train plant, 1/3 for a three train plant) rather than a single event in one of the loops. More details on the features of PSA necessary for various applications of PSA are provided in Section 10.

PROJECT MANAGEMENT FOR PSA

3.3. Paragraphs 3.3–3.14 provide recommendations on meeting Requirement 5 of Ref. [3] on preparation for the safety assessment for Level 1 PSA and on meeting Requirement 22 of Ref. [3] on management of the safety assessment. Project management of the PSA depends strongly on the specific conditions in a State, namely:

- (a) The organizations participating in the PSA project;
- (b) The type and extent of the involvement of the participating organizations;
- (c) The objectives and the scope of the PSA study.

After the objectives and the scope of the PSA have been specified, the management scheme for the PSA project should be developed, including the selection of methods and establishment of procedures, the selection of personnel and the organization of the team that will perform the PSA, the training of the team, the preparation of a PSA project schedule, the estimation and securing of the necessary funds, and the establishment of quality assurance procedures and peer review procedures.

3.4. A PSA study is normally commissioned by one of the following:

- (a) The plant designer;
- (b) The operating organization of the plant;
- (c) The regulatory body.

The PSA can be performed by these groups or by consultants, research institutes, universities or a combination of these. In any case, the operating organization should always participate as a source of operational knowledge, as well as being a beneficiary from the insights obtained.

3.5. It is generally considered desirable to start the process of performing the PSA as early as possible in the lifetime of the plant. Design weaknesses or

procedural weaknesses that are recognized early can be corrected or improved less expensively than those that remain until the plant is in operation. While a PSA can be started in any of the stages in the lifetime of the plant, the PSA models and documentation should be maintained and regularly updated throughout the operating life of the plant to provide continued benefit.

3.6. The PSA study should consider a particular ‘freeze date’ for modelling the as built and as operated plant conditions. If it is known at the beginning of the PSA project that certain changes in plant design and operation will be implemented in the near term, before the PSA is finished, a decision should be taken at an early stage of the PSA as to whether these changes will be addressed in the PSA. If the decision is made to address the future changes, the freeze date should be determined accordingly and the PSA should take account of the status of the plant after the modifications.

3.7. The documentation for the PSA should be developed in a clear, traceable, systematic and transparent manner so that it can effectively support the review of PSA, applications of PSA and future PSA upgrades.

SELECTION OF METHODS AND ESTABLISHMENT OF PROCEDURES

3.8. Appropriate working methods and procedures should be established at the outset of the project so that there is a minimum of modification to these procedures during the project. Unnecessary iterations in methods and procedures may cause delays in the PSA project. General guidance for the methodological tools and approaches to analysis is given in the following sections of this publication. Once the working methods have been selected, the various procedural steps should be interfaced with the tasks of quality assurance and training to produce a detailed plan of the tasks, including a schedule for the project.

3.9. The resources in terms of the expertise of the specialists involved, human resources, computer time, calendar time and so on that will be necessary to complete a PSA depend greatly on the scope of the PSA, which is in turn governed by the overall objectives, and on the available expertise in the PSA team. Scheduling of the activities should be carried out following the establishment of detailed procedures and should account for the availability of personnel.

TEAM SELECTION AND ORGANIZATION

3.10. The members of the team that perform the PSA can be characterized by the organization they represent and the technical expertise they provide. Once the necessary personnel have been identified, lines of communication should be set up and specific tasks should be assigned. The training necessary should be determined and planned in accordance with the activities of the PSA. The task of team formation and training is closely associated with the corresponding tasks of quality assurance.

3.11. The expertise necessary to conduct a PSA should provide two essential elements: knowledge of the plant and knowledge of PSA techniques. This expertise can vary in depth, depending on the scope of the PSA, but the participation of the plant designer and the operating organization of the plant should be foreseen, if possible. More specifically, the necessary expertise relating to knowledge of the plant should be obtained from persons with extensive familiarity with the design and operation of the plant under normal and accident conditions.

3.12. A team that will perform a PSA for the first time should be provided with training to acquire the expertise necessary to complete the study successfully.

ESTABLISHMENT OF A QUALITY ASSURANCE PROGRAMME FOR PSA

3.13. The quality assurance⁷ programme for a PSA encompasses activities that are necessary to achieve the appropriate quality of the PSA and activities that are necessary to verify that the appropriate quality is achieved. For a PSA, appropriate quality means an end product that is correct and usable and one which meets the objectives and fulfils the scope of the PSA. The quality assurance programme should provide for a disciplined approach to all activities affecting the quality of the PSA, including, where appropriate, verification that each task has been satisfactorily performed and that necessary corrective actions have been implemented.

⁷ Instead of the term ‘quality assurance’, the term ‘management system’ is used in Ref. [7]. The term ‘quality assurance’ is left in this Safety Guide in order to comply with widely accepted current practices and terminology used in the area of PSA.

3.14. Quality assurance of the PSA should be viewed and established as an integral part of the PSA project and the quality assurance procedures should be an integral part of the PSA procedures. The quality assurance procedures should provide for control of the constituent activities associated with a PSA in the areas of organization, technical work and documentation. In their application to the technical work, quality assurance procedures are aimed at ensuring consistency between goals, scope, methods and assumptions, as well as accuracy in the application of methods and in calculations. Quality assurance procedures should include control of the documentation of the PSA. General requirements for control of documents are established in section 2 of Ref. [7].

GENERAL ASPECTS OF PSA DOCUMENTATION

Objectives and content of documentation

3.15. Paragraphs 3.15–3.22 provide general recommendations on meeting Requirement 20 on documentation for Level 1 PSA [3]. The primary objectives of the PSA documentation should be to fulfil the requirements of its users and be suitable for the specific applications of the PSA. Possible users of the PSA include:

- (a) Operating organizations of nuclear power plants (management and operating personnel);
- (b) Designers and vendors;
- (c) Regulatory bodies and persons or organizations providing them with technical support;
- (d) Other government bodies;
- (e) The public.

Some of these users, the public for example, might use, primarily, the summary report of the PSA, while others will use the full PSA documentation, including the computer model.

3.16. PSA documentation includes work files, computer inputs and outputs, correspondence, interim reports and the final report of the PSA. The documentation of PSA should be complete, well structured, clear and easy to follow, review and update. It should be presented in a traceable and sequential manner, i.e. the order of appearance of analysis in the final documentation should follow, as far as possible, the order in which it was actually performed. In addition, means should be provided for possible extensions of the analysis,

including integration of new topics, use of improved models, broadening of the scope of the PSA in question and its use for alternative applications. Explicit presentation of the assumptions, exclusions and limitations for extending and interpreting the PSA is also of critical importance to users.

3.17. The documentation should provide within the report (or by reference to available material) all necessary information to reconstruct the results of the study. All intermediate subanalyses, calculations, assumptions, etc., that will not be published in any external reports should be retained as notes, working papers or computer outputs. This is very important for reconstructing and updating each detail of the analysis in the future.

Organization of documentation

3.18. The final report of the PSA study should be divided into three major parts:

- (1) Summary report;
- (2) Main report;
- (3) Appendices to the main report.

3.19. The summary report should be designed to provide an overview of the motivations, objectives, scope, assumptions, results and conclusions of the PSA at a level that is useful to a wide audience of reactor safety specialists and that is adequate for high level review. The summary report is designed:

- (a) To support high level review of the PSA;
- (b) To communicate key aspects of the study to a wide audience of interested parties;
- (c) To provide a clear framework and guide for the reader or user prior to consulting the main report.

The summary report of a PSA should include a subsection on the structure of the report, which should present concise descriptions of the contents of the sections of the main report and of the individual appendices. The relation between various parts of the PSA should also be included in this subsection of the summary report.

3.20. The main report should give a clear and traceable presentation of the complete PSA study, including a description of the plant, the objectives of the study, the methods and data used, the initiating events considered, the plant modelling results and the conclusions. The main report, together with its appendices, should be designed:

- (a) To support technical review of the PSA;
- (b) To communicate key detailed information to interested users;
- (c) To permit the efficient and varied application of the PSA models and results;
- (d) To facilitate the updating of the models, data and results in order to support the continued safety management of the plant.

3.21. The appendices should contain detailed data, records of engineering computations, detailed models, etc. The appendices should be structured so as to correspond directly to the sections and subsections of the main report, as far as possible.

3.22. In addition to the general recommendations for documentation provided in this section, specific recommendations for documentation are provided in other sections of this Safety Guide, for example, for PSA for internal initiating events, for PSA for internal fire, for PSA for internal flooding, for PSA for external hazards and for PSA for low power and shutdown states.

4. FAMILIARIZATION WITH THE PLANT AND COLLECTION OF INFORMATION

4.1. This section provides recommendations on meeting Requirement 5 of Ref. [3] on preparation for Level 1 PSA. The PSA team should familiarize themselves with the design and operation of the plant, including the emergency procedures and the test and maintenance procedures. Information sources that may be used for familiarization with the plant include the following:

- (a) The safety analysis report for the plant;
- (b) Technical specifications for the plant;
- (c) System descriptions;
- (d) As built (as is) system drawings (piping and instrumentation diagrams);
- (e) Electrical line drawings, including circuit diagrams and trip criteria for the electrical bus protection system;
- (f) Control and actuation circuit drawings;
- (g) Normal operating procedures, emergency procedures, test procedures and maintenance procedures;

- (h) Analyses pertinent to the determinants of mission success criteria of systems;
- (i) Operational experience from the plant or from similar plants in the same State or other States, and reports and analysis of incidents;
- (j) Operator's logs;
- (k) Discussions with operating staff;
- (l) Plant operational records and reports of shutdowns;
- (m) Plant databases and/or the computerized management system for maintenance, if available;
- (n) Plant layout drawings;
- (o) Drawings of piping location and routing;
- (p) Drawings of cable location and routing;
- (q) Plant walkdown reports;
- (r) Regulatory requirements;
- (s) Other relevant plant documents.

The plant documents containing the information necessary for the analysis should be collected and made available to the PSA team. Depending on the scope of the PSA, more specific information may be required, for example, plant layout and topography of the site and surroundings for PSA for external hazards. Interaction with operating personnel who are not part of the PSA team might be necessary for clarification and additional information.

4.2. Currently, in many States, performance of a PSA is required as part of the safety analysis report. In this case, PSA documentation may refer to the corresponding sections of the safety analysis report, e.g. descriptions of systems. All references should be clearly provided so that the referred information can be easily found.

4.3. Plant familiarization is a key element of PSA for external and internal hazards. A thorough plant walkdown should be performed to verify information on hazard sources and plant features susceptible to damage due to the hazard. Specific guidance for plant familiarization for external and internal hazards should be provided.

5. LEVEL 1 PSA FOR INTERNAL INITIATING EVENTS FOR FULL POWER OPERATING CONDITIONS

5.1. This section provides recommendations on meeting Requirements 6–13 of Ref. [3] for Level 1 PSA for internal initiating events. This section provides recommendations on the technical issues that need to be addressed in carrying out a Level 1 PSA for internal initiating events caused by random component failures and human errors occurring at full power.

5.2. The recommendations on Level 1 PSA cover:

- (a) General aspects of Level 1 PSA methodology;
- (b) Initiating event analysis;
- (c) Accident sequence analysis;
- (d) Systems analysis;
- (e) Analysis of dependent failures;
- (f) Analysis of common cause failures;
- (g) Human reliability analysis;
- (h) Modelling of passive systems and computer based systems;
- (i) Data required for a Level 1 PSA;
- (j) Integration and quantification of the PSA model;
- (k) Sensitivity studies and importance and uncertainty analysis.

The general framework for analysis is illustrated in Fig. 1.

GENERAL ASPECTS OF LEVEL 1 PSA METHODOLOGY

5.3. The first step should be to define the overall approach and methodology to be used for the Level 1 PSA. The overall approach and methodology should be capable of modelling the fault sequences that could occur, starting from an initiating event, and should be capable of identifying the combinations of safety system failures, support system failures and human errors that could lead to core damage.

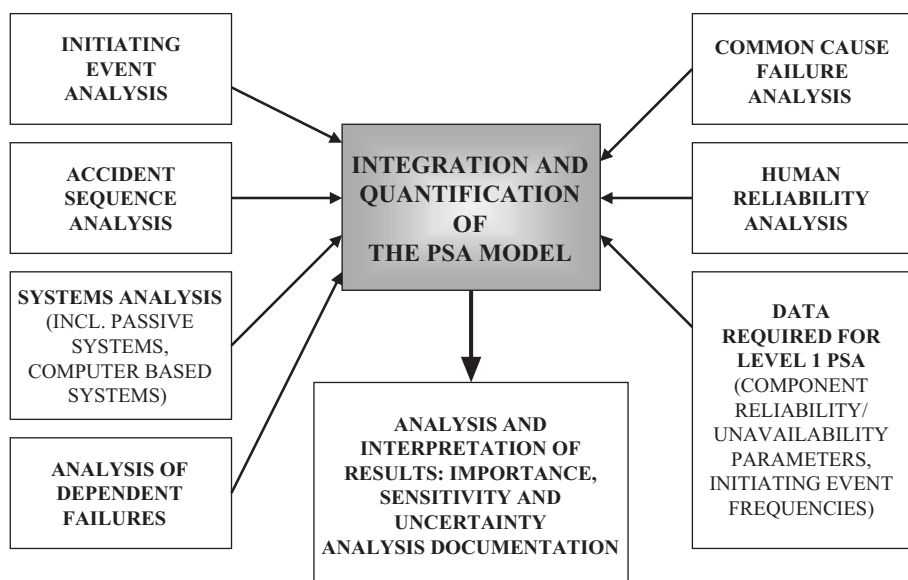


FIG. 1. General analysis framework of a Level 1 PSA for internal initiating events.

5.4. Several techniques can be used in performing a PSA. However, the usual approach is to use a combination of event trees and fault trees. The relative size (complexity) of the event trees and fault trees is largely a matter of preference of the team carrying out the analysis and also depends on the features of the software used.

5.5. One widely practised approach is to use a combination of event trees and fault trees often referred to as the fault tree linking approach. The event trees outline the broad characteristics of the accident sequences that start from the initiating event and, depending on the success or failure of the mitigating safety and safety related systems, lead to a successful outcome or to damage to the core (see paras 5.42 and 5.43), or to one of the plant damage states (required for the Level 2 PSA). The fault trees are used to model the failure of the safety systems and the support systems to carry out their safety functions.

5.6. Another approach that is widely used is to carry out the analysis using large event trees and small fault trees. In this approach, failures of safety functions, safety systems and support systems are modelled in the event trees. This approach is variously referred to as the large event tree approach, the linked event tree approach, or the event tree with boundary conditions approach. It is also

possible to carry out the analysis using event trees only or fault trees only. However, in the latter case, the high level fault tree structure is usually derived from, or based on, an event tree or set of event trees.

5.7. The overall aim should be to calculate a best estimate of the core damage frequency while avoiding the introduction of excessive conservatism wherever possible, since this may bias the results unnecessarily. Hence, the Level 1 PSA should be based on best estimate models, assumptions and data. However, some conservatism may be necessary where there is a high level of uncertainty, in order to avoid unjustifiable optimism.

5.8. The Level 1 PSA model produced should be capable of being used for the intended applications and of being updated for possible future applications.

5.9. The analysis should be carried out using a suitable computer code that has the following capabilities:

- (a) It should be capable of handling the very large and complex logic model of the nuclear power plant.
- (b) It should be capable of quantifying the PSA model in a reasonably short timescale.
- (c) It should be capable of providing the information necessary to interpret the Level 1 PSA, such as the core damage frequency, frequencies of cutsets (combinations of initiating events and failures and/or human errors leading to core damage), importance measures and results of uncertainty and sensitivity analyses.

5.10. The production of the Level 1 PSA is an iterative process and it should be carried out until an accurate, sufficiently detailed model has been produced.

INITIATING EVENT ANALYSIS

5.11. The starting point of the Level 1 PSA is the identification of the set of initiating events. An initiating event is an event that could lead directly to core damage (e.g. reactor vessel rupture) or that challenges normal operation and which requires successful mitigation using safety or non-safety systems to prevent core damage.

5.12. This section deals with the identification of internal initiating events that could arise during full power operation. The general methodology for

Level 1 PSA for internal and external hazards is presented in Section 6 and detailed recommendations are provided in Sections 7 and 8, respectively. Recommendations on issues specific to the identification of initiating events that could arise in low power and shutdown modes are provided in Section 9.

Identification of initiating events

5.13. A systematic process should be used to identify the set of initiating events to be addressed in the Level 1 PSA. This should involve a number of different approaches including:

- (a) Analytical methods such as hazard and operability studies or failure mode and effects analysis or other relevant methods for all safety systems to determine whether their failures, either partial or complete, could lead to an initiating event;
- (b) Deductive analyses such as master logic diagrams to determine the elementary failures or combinations of elementary failures that would challenge normal operation and lead to an initiating event;
- (c) Comparison with the lists of initiating events developed for the Level 1 PSAs for similar plants and with existing safety standards and guidelines;
- (d) Identification of initiating events on the basis of the analysis of operating experience from the plant under investigation and from similar plants;
- (e) Review of the deterministic design basis accident analysis and beyond design basis accident analysis and the safety analysis report.

5.14. The set of internal initiating events used as the basis for the Level 1 PSA should be as comprehensive as possible. It is recognized that it is not possible to demonstrate that all possible initiating events have been identified. However, by using a sufficiently comprehensive combination of the different approaches listed in para. 5.13, it is possible to gain confidence that the set of initiating events that has been identified for the plant is as comprehensive as possible.

5.15. In identifying initiating events, particular consideration should be given to any design features that are novel or distinctive to the plant in question as potential sources of new initiating events. This is particularly important for new nuclear power plants where there is little or no operating experience and special efforts should be made to identify unique initiating events, failure modes, accident sequences and dependencies that are particular to that design. The analytical techniques indicated in para. 5.13 (a) should be carried out for all the operating front line systems, support systems and standby systems to identify possible initiating events (or consequential failures that could constitute initiating

events) that could arise through failure to operate, partial failure to operate or inadvertent operation.

5.16. The major categories of initiating events that are included in the Level 1 PSA are events that threaten the safety functions, such as removal of heat from the reactor core, control of the primary coolant inventory, maintaining the integrity of the primary circuit and control of the reactivity of the core.

5.17. The set of initiating events identified should include partial functional failures or partial system failures as well as complete failures, for example, reduction of feed to steam generators or loss of feed to one steam generator as well as complete loss of all feed to all steam generators. This is important since initiating events involving partial failures could make a significant contribution to the risk.

5.18. The set of initiating events identified should include those that can occur during all the permissible modes of power operation of the plant, for example, operation with one of the coolant loops removed from service.

5.19. The set of initiating events should include events of very low frequency with potentially large consequences, for example, rupture of the reactor pressure vessel, or loss of coolant accidents in interfacing systems. Inclusion of loss of coolant accidents in interfacing systems is particularly important if the Level 1 PSA is intended to be used as the basis for a Level 2 PSA (and possibly a Level 3 PSA).

5.20. For sites with more than one nuclear power plant unit, the set of initiating events that can affect more than one of the units at the same time should be identified, for example, loss of off-site power. In addition, events that can arise in one of the units and lead to an initiating event in another unit should be identified, for example, for a Level 1 PSA for internal hazards, an initiating event in the unit being analysed could be caused by a strike from a missile generated by disintegration of a turbine in an adjacent unit.

5.21. The set of initiating events identified for the plant should be compared with that for similar plants, as stated in para. 5.13 (c), to ensure that all the relevant initiating events have been included. Where differences are identified, additional initiating events should be included or justification should be provided of why they are not relevant.

5.22. A review of the operating experience of the nuclear power plant (if it is already operating) and of similar nuclear power plants should be carried out to

ensure that any initiating events that have actually occurred are included in the set of initiating events addressed in the Level 1 PSA.

5.23. The causes of such initiating events should be identified and should be taken into account in the analysis. For initiating events that have a number of causes or where more than one failure would be necessary for the initiating event to occur, a common approach is to use a fault tree to model the initiating event.

Transients

5.24. The Level 1 PSA should be based on a comprehensive set of transients that can occur. Examples of the types of transient that can occur include the following:

- (a) Increase in reactor heat removal, e.g. opening of secondary relief valve(s) or a steam line break;
- (b) Decrease in reactor heat removal, e.g. loss of main feed or a feed line break;
- (c) Decrease in reactor coolant system flow rate, e.g. tripping of the reactor coolant pump, pump seizure or shaft break;
- (d) Anomalies in reactivity and power distribution, e.g. uncontrolled control rod withdrawal, control rod ejection or boron dilution;
- (e) Increase in reactor coolant inventory, e.g. inadvertent operation of the emergency coolant injection system;
- (f) Any event causing a reactor trip or immediate shutdown of the reactor.

5.25. The set of transients should include loss of off-site power as an internal initiating event. The initiating event involving loss of off-site power should be specified in terms of the frequency of occurrence and the duration of the loss of off-site power, which should take into account the likelihood of recovery of off-site power. This should be based on details of the design and operating experience in relation to the grid connections to the plant.

5.26. When losses of off-site power that could occur due to internal hazards (such as a fire in the plant) and external hazards (such as extreme environmental conditions or an earthquake) are modelled explicitly in a PSA for those hazards, the definition of the loss of off-site power for the model for internal initiating events should exclude these causes so as to avoid double counting in the Level 1 PSA.

5.27. The set of initiating events should also include failures of support systems, for example, electrical power systems, instrument air, cooling water systems, room cooling systems and the instrumentation and control systems. This is

particularly important where the failure of a support system could lead to a reactor trip and the support system in question also has a role to play after a reactor trip.

Loss of coolant accidents

5.28. A complete set of initiating events that can lead to a loss of coolant accident should be considered in Level 1 PSA.

5.29. The set of loss of coolant accidents identified should include all the different sizes and locations of breaks that can lead to a loss of primary coolant. Possible locations should be identified on the basis of the actual design and layout of the plant and the set of loss of coolant accidents should include failures of pipework and valves, in particular, relief valves.

5.30. The set of loss of coolant accidents that can result in the discharge of primary coolant outside the containment should be identified. This typically includes steam generator tube ruptures and loss of coolant accidents in interfacing systems where the primary coolant leakage from the break bypasses the containment and hence is not available for recirculation from the containment sump.

5.31. The set of loss of coolant accidents identified should be categorized and grouped according to the success criteria of the safety systems that must be operated to prevent core damage. For pressurized water reactors, loss of coolant accidents are usually categorized as large, medium or small, mainly on the basis of the performance required from the coolant injection systems to mitigate the loss of coolant accident. Depending on the plant design, a different set of equipment may be required to provide protection from very small loss of coolant accidents such as those involving failure of the reactor coolant pump seal.

Grouping of initiating events

5.32. In order to limit the analysis required for the Level 1 PSA to a manageable size, a grouping process should be carried out before proceeding to the accident sequence analysis.

5.33. If, in order to further limit the PSA model to a manageable size, some initiating event groups are screened from consideration for inclusion in the model, the screening criteria established should be consistent with the purpose of performing the PSA, so that significant contributors to risk are not excluded. If

screening is performed, it may still need to be revisited for specific PSA applications.

5.34. Initiating events should be arranged in groups in which all of the following properties of the initiating events are the same (or very similar):

- (a) The accident progression following the initiating event;
- (b) The success criteria for the mitigating systems;
- (c) The effect of the initiating event on the availability and operation of safety systems and support systems, including the presence of conditions for signals that will actuate protection actions or block actuation of systems;
- (d) The response expected from plant operators.

5.35. The success criteria for the mitigating systems used for a specific group of initiating events should be the most stringent criteria for all the individual events within the group.

5.36. Where initiating events with slightly different accident progressions and/or success criteria for the mitigating systems have been grouped together, the accident sequence analysis should provide a bound for all the potential accident sequences and consequences of these initiating events.

5.37. The grouping of initiating events should be done in such a way that undue conservatism is not introduced into the analysis.

5.38. Initiating events that could cause a containment bypass (e.g. steam generator tube rupture or loss of coolant accidents in interfacing systems) should not be grouped with other loss of coolant accidents where the containment would remain effective.

5.39. The Level 1 PSA documentation should include a list of all the initiating events that have been identified for the plant and should provide a description of each initiating event and sufficient information on the method used to identify it, e.g. hazard and operability studies, failure mode and effects analysis, master logic diagram or review of operating experience.

ACCIDENT SEQUENCE ANALYSIS

5.40. The next step in the analysis is to determine the response of the plant to each group of initiating events (as identified in accordance with the foregoing

procedure) that requires the operation of safety systems to carry out the safety functions to prevent core damage. Such safety functions typically include shutting down the reactor and keeping it subcritical, removal of heat from the reactor core, etc. (see para. 5.45).

5.41. The events that are identified in the accident sequences will relate to the success or failure of the safety systems and human actions taken in carrying out the safety functions required for the groups of initiating events. The end points of the accident sequence models will correspond either to a safe stable state where all required safety functions have been performed successfully or to core damage.

Core damage

5.42. A criterion (or criteria, if appropriate) should be developed for what constitutes core damage or a particular degree of core damage.⁸ For example, for light water reactors, it is often assumed that core damage occurs if any of the fuel parameters (such as the clad temperature) exceeds its design basis limit or a higher limit if this can be justified.

5.43. However, the specification of what constitutes core damage is often done by adopting an indirect criterion. For example, for a pressurized water reactor, core damage is assumed to occur following prolonged exposure of the top of the core or if a maximum specified cladding temperature is exceeded. If a significantly long time interval is required to cause core damage after exposure of the top of the core, then this should be taken into account in framing a realistic definition of core damage.

Safety functions, safety systems and success criteria

5.44. The accident sequence analysis should be carried out for each group of initiating events, as identified in paras 5.32–5.39.

5.45. The safety functions that need to be performed to prevent core damage should be identified for each initiating event group. The safety functions required

⁸ Several core damage states can be specified, depending on the degree of the damage, for example, in channel type reactors, damage to different numbers of channels is usually considered depending on the severity of the consequences. Another factor in specifying the degree of core damage can be timing, e.g. delayed core damage.

will depend on the reactor type and the nature of the initiating event and will typically include:

- (a) Detection of the initiating event and reactor trip;
- (b) Shutdown of the reactor and maintaining subcriticality;
- (c) Heat removal from the reactor core;
- (d) Maintaining the integrity of the primary circuit and the containment.

5.46. The safety systems and operator actions that will need to be available to perform each of these safety functions should be identified, along with the success criteria for the safety systems used in performing these safety functions.

5.47. The success criterion for each safety system should be defined as the minimum level of performance required to achieve the safety function, taking into account the specific features of each sequence. Where redundant trains of the safety system are involved, the success criteria should be defined as the number of trains that are required to operate. Where diverse safety systems are involved, the success criteria should account for the performance required from each of the diverse systems. This could include partial operation of each of the diverse systems as supported by the best estimate safety analysis.

5.48. The safety systems that would fail as a result of the initiating event should be identified and taken into account in specifying the success criteria. Examples of such cases are where the initiating event involves the failure of a support system, for example, the electrical power and cooling water systems, or where the initiating event produces a harsh environment in an area where safety related equipment is located. In either case, this can lead to failure of the required safety systems. Another example arises in the case of a large or intermediate loss of coolant accident in a pressurized water reactor where, if the break occurs in a cold leg, the flow would be lost from the trains of the emergency core cooling system connected to that leg; this would need to be recognized in defining the success criteria.

5.49. The success criteria should specify the mission times for the safety systems, that is, the time that the safety systems will need to operate so that the reactor reaches a safe, stable shutdown state and that will allow for long term measures to be put in place to maintain this state. In many cases, this has been taken to be 24 or 48 h for most initiating events. For new designs that provide the features to delay core damage, consideration of a longer mission time may be necessary.