

IAEA SAFETY STANDARDS SERIES

Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants

SAFETY GUIDE

No. NS-G-2.2



INTERNATIONAL
ATOMIC ENERGY AGENCY
VIENNA

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www.iaea.org/ns/coordinet

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA 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 in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related sales publications are the **Technical Reports Series**, the **Radiological Assessment Reports Series** and the **INSAG Series**. The IAEA also issues reports on radiological accidents and other special sales publications. Unpriced safety related publications are issued in the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series**, the **IAEA Services Series** and the **Computer Manual Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**.

OPERATIONAL LIMITS AND
CONDITIONS AND
OPERATING PROCEDURES FOR
NUCLEAR POWER PLANTS

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

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

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, 2000

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria
November 2000
STI/PUB/1100

SAFETY STANDARDS SERIES No. NS-G-2.2

OPERATIONAL LIMITS AND
CONDITIONS AND
OPERATING PROCEDURES FOR
NUCLEAR POWER PLANTS

SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2000

VIC Library Cataloguing in Publication Data

Operational limits and conditions and operating procedures for nuclear power plants : safety guide. — Vienna : International Atomic Energy Agency, 2000.

p. ; 24 cm. — (Safety standards series, ISSN 1020-525X ; no. NS-G-2.2)

STI/PUB/1100

ISBN 92-0-102000-7

Includes bibliographical references.

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

VICL

00-00252

FOREWORD

by **Mohamed ElBaradei**
Director General

One of the statutory functions of the IAEA is to establish or adopt standards of safety for the protection of health, life and property in the development and application of nuclear energy for peaceful purposes, and to provide for the application of these standards to its own operations as well as to assisted operations and, at the request of the parties, to operations under any bilateral or multilateral arrangement, or, at the request of a State, to any of that State's activities in the field of nuclear energy.

The following advisory bodies oversee the development of safety standards: the Advisory Commission for Safety Standards (ACSS); the Nuclear Safety Standards Advisory Committee (NUSSAC); the Radiation Safety Standards Advisory Committee (RASSAC); the Transport Safety Standards Advisory Committee (TRANSSAC); and the Waste Safety Standards Advisory Committee (WASSAC). Member States are widely represented on these committees.

In order to ensure the broadest international consensus, safety standards are also submitted to all Member States for comment before approval by the IAEA Board of Governors (for Safety Fundamentals and Safety Requirements) or, on behalf of the Director General, by the Publications Committee (for Safety Guides).

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA. Any State wishing to enter into an agreement with the IAEA for its assistance in connection with the siting, design, construction, commissioning, operation or decommissioning of a nuclear facility or any other activities will be required to follow those parts of the safety standards that pertain to the activities to be covered by the agreement. However, it should be recalled that the final decisions and legal responsibilities in any licensing procedures rest with the States.

Although the safety standards establish an essential basis for safety, the incorporation of more detailed requirements, in accordance with national practice, may also be necessary. Moreover, there will generally be special aspects that need to be assessed on a case by case basis.

The physical protection of fissile and radioactive materials and of nuclear power plants as a whole is mentioned where appropriate but is not treated in detail; obligations of States in this respect should be addressed on the basis of the relevant instruments and publications developed under the auspices of the IAEA.

Non-radiological aspects of industrial safety and environmental protection are also not explicitly considered; it is recognized that States should fulfil their international undertakings and obligations in relation to these.

The requirements and recommendations set forth in the IAEA safety standards might not be fully satisfied by some facilities built to earlier standards. Decisions on the way in which the safety standards are applied to such facilities will be taken by individual States.

The attention of States is drawn to the fact that the safety standards of the IAEA, while not legally binding, are developed with the aim of ensuring that the peaceful uses of nuclear energy and of radioactive materials are undertaken in a manner that enables States to meet their obligations under generally accepted principles of international law and rules such as those relating to environmental protection. According to one such general principle, the territory of a State must not be used in such a way as to cause damage in another State. States thus have an obligation of diligence and standard of care.

Civil nuclear activities conducted within the jurisdiction of States are, as any other activities, subject to obligations to which States may subscribe under international conventions, in addition to generally accepted principles of international law. States are expected to adopt within their national legal systems such legislation (including regulations) and other standards and measures as may be necessary to fulfil all of their international obligations effectively.

EDITORIAL NOTE

An appendix, when included, is considered to form an integral part of the standard and to have the same status as the main text. Annexes, footnotes and bibliographies, if included, are used to provide additional information or practical examples that might be helpful to the user.

The safety standards use the form 'shall' in making statements about requirements, responsibilities and obligations. Use of the form 'should' denotes recommendations of a desired option.

The English version of the text is the authoritative version.

CONTENTS

1.	INTRODUCTION	
	Background (1.1–1.3)	1
	Objective (1.4)	1
	Scope (1.5)	1
	Structure (1.6)	2
2.	SAFETY OBJECTIVE (2.1)	2
3.	THE CONCEPT OF OPERATIONAL LIMITS AND CONDITIONS AND THEIR DEVELOPMENT	2
	The concept of operational limits and conditions (3.1–3.7)	2
	Development of operational limits and conditions (3.8–3.16)	4
4.	SAFETY LIMITS (4.1–4.5)	5
5.	LIMITING SAFETY SYSTEM SETTINGS (5.1–5.4)	6
6.	LIMITS AND CONDITIONS FOR NORMAL OPERATION (6.1–6.9)	8
7.	SURVEILLANCE REQUIREMENTS (7.1–7.5)	10
8.	OPERATING PROCEDURES	10
	General (8.1–8.7)	10
	Particular aspects of emergency procedures (8.8–8.18)	11
	Procedures for operation in the commissioning phase (8.19–8.20)	14
9.	DEVELOPMENT OF OPERATING PROCEDURES (9.1–9.7)	14
10.	COMPLIANCE WITH OPERATIONAL LIMITS AND CONDITIONS AND OPERATING PROCEDURES (10.1–10.7)	15
	APPENDIX I: SELECTION OF LIMITS AND CONDITIONS FOR NORMAL OPERATION	19

APPENDIX II: DEVELOPMENT OF OPERATING PROCEDURES (OUTLINES)	28
REFERENCES	31
ANNEX: EXAMPLE TO EXPLAIN SOME TERMS USED	33
GLOSSARY	37
CONTRIBUTORS TO DRAFTING AND REVIEW	39
ADVISORY BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS	41

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide was prepared as part of the Agency's programme for establishing safety standards relating to nuclear power plants. The present Safety Guide supersedes the IAEA Safety Guide on Operational Limits and Conditions for Nuclear Power Plants which was issued in 1979 as Safety Series No. 50-SG-O3.

1.2. For a nuclear power plant to be operated in a safe manner, the provisions made in the final design and subsequent modifications shall be reflected in limitations on plant operating parameters and in the requirements on plant equipment and personnel. Under the responsibility of the operating organization, these shall be developed during the design safety evaluation as a set of operational limits and conditions (OLCs). A major contribution to compliance with the OLCs is made by the development and utilization of operating procedures (OPs) that are consistent with and fully implement the OLCs.

1.3. The requirements for the OLCs and OPs are established in Section 5 of the IAEA Safety Requirements publication Safety of Nuclear Power Plants: Operation [1], which this Safety Guide supplements.

OBJECTIVE

1.4. The purpose of this Safety Guide is to provide guidance on the development, content and implementation of OLCs and OPs. The Safety Guide is directed at both regulators and owners/operators.

SCOPE

1.5. This Safety Guide covers the concept of OLCs, their content as applicable to land based stationary power plants with thermal neutron reactors, and the responsibilities of the operating organization regarding their establishment, modification, compliance and documentation. The OPs to support the implementation of the OLCs and to ensure their observance are also within the scope of this Safety Guide. The particular aspects of the procedures for maintenance, surveillance, in-service inspection and other safety related activities in connection with the safe operation of nuclear power plants are outside the scope of this Safety Guide but can be found in other IAEA Safety Guides (see, for example, Refs [2] and [3]).

STRUCTURE

1.6. Section 2 indicates the relation between the fundamental safety objective and the OLCs. The concept and development of OLCs are introduced in Section 3. Sections 4 to 7 describe in some detail the characteristics of the types of OLCs, safety limits, limits on safety system settings, limits and conditions for normal operation, and surveillance requirements. Sections 8 and 9 address the question of OPs, including their development. In Section 10 guidance is provided on how to ensure compliance with OLCs and procedures, including reference to the need to retain records of such compliance. Appendix I presents a sample list of the items for which limits and conditions are generally established and Appendix II gives outlines for the development of OPs. In the Annex an example is provided to explain some terms used in the Safety Guide. A Glossary is included at the end.

2. SAFETY OBJECTIVE

2.1. To achieve the fundamental technical safety objective directed to the prevention of situations from arising which might lead to accident conditions, and the mitigation of the consequences of such accident conditions should they arise: “The operation of the installation must be controlled in accordance with a set of operational limits and conditions, derived from the safety analysis, which identify safe boundaries of operation. These limits and conditions must be revised as necessary in the light of experience from commissioning and operation. Minimum requirements must be set for the availability of staff and equipment... Operations must be carried out by adequately trained and authorized personnel in accordance with detailed, validated and approved procedures...” (Ref. [4], para. 510).

3. THE CONCEPT OF OPERATIONAL LIMITS AND CONDITIONS AND THEIR DEVELOPMENT

THE CONCEPT OF OPERATIONAL LIMITS AND CONDITIONS

3.1. The Agency’s Safety Requirements for Operation [1] state that OLCs shall be developed to ensure that plants are operated in accordance with design assumptions and intent. In order to achieve this requirement the plant safety analysis report should be developed in such a manner as to identify clearly the OLCs that must be met to

prevent situations from arising which might lead to accident conditions or to mitigate the consequences of accidents if they do occur.

3.2. The OLCs shall contain operational requirements for different operational states including shutdown [1]. These operational states should include starting up, power production, shutting down, maintenance, testing and refuelling. The OLCs should also define operational requirements to ensure that safety systems, including engineered safety features, perform the necessary functions in all operational states and also in design basis accidents (DBAs).

3.3. The technical aspects of the OLCs cover the limitations to be observed, as well as the operational requirements that structures, systems and components important to the safety of the nuclear power plant be able to perform their intended functions as assumed in the plant safety analysis report. Safe operation depends upon personnel as well as on equipment; OLCs should therefore also cover actions to be taken and limitations to be observed by operating personnel.

3.4. With regard to operating personnel, the OLCs include those principal requirements for surveillance and corrective or complementary actions that are necessary to supplement the functioning of equipment involved in maintaining the established OLCs. Some OLCs may involve combinations of automatic functions and actions by personnel.

3.5 The OLCs at the power plant should include the following items:

- (a) Safety limits,
- (b) Limiting safety system settings,
- (c) Limits and conditions for normal operation,
- (d) Surveillance requirements,
- (e) Action statements for deviations from the OLCs.

In addition, OLCs may include objectives for all or some of the most significant OLCs in order to justify their application, as well as a basis for their derivation. These items should be included in the documentation on OLCs to increase consciousness on the part of plant personnel of their application and observance.

3.6. It should be understood that OLCs form a logical system in which the elements listed in para. 3.5 are closely interrelated and in which the safety limits constitute the ultimate boundary of the safe conditions. An example explaining such an interrelationship is given in the Annex. The OLCs should be readily accessible to control room personnel. For this they should be collected in one document for control

room use. Control room operators should be highly knowledgeable of the OLCs and their technical basis.

3.7. Should a situation arise in which, for any reason, operating personnel do not understand the operational state or cannot ascertain that the power plant is being operated within operating limits, or the plant behaves in an unpredicted way, measures should be taken without delay to bring the plant to a safer state.

DEVELOPMENT OF OPERATIONAL LIMITS AND CONDITIONS

3.8. The OLCs shall be based on a safety analysis of the individual plant and its environment in accordance with the provisions made in the design [1]. The OLCs should be determined with due account taken of the uncertainties in the process of safety analysis. The safety analysis report and OLCs should be reviewed and amended where necessary on the basis of the results of commissioning testing. The justification for each of the OLCs should be substantiated by means of a written indication of the reason for its adoption and any relevant background information. These justifications should be readily available when necessary.

3.9. The initial OLCs should normally be developed in co-operation with the designers well before commencement of operation to ensure that adequate time is available for assessment and approval by the regulatory body.

3.10. Each OLC should have associated surveillance requirements that support the operating personnel in ensuring compliance with the OLC.

3.11. It is also essential that the OLCs be meaningful to the responsible operating personnel and be defined by measurable or directly identifiable values of parameters. Where directly identifiable values cannot be used, the relationship of a limiting parameter with the reactor power or another measurable parameter should be indicated by tables, diagrams or computing techniques as appropriate. The limit or condition should be stated in such a way that it is clear whether a breach has or has not occurred in any situation.

3.12. Clear presentation and avoidance of ambiguity are important contributors to reliability in the use of OLCs, and therefore advice on human factors should be sought at an early stage in the development of the documentation in which the OLCs will be presented to the operating personnel. The meaning of terms should be explained to help prevent misinterpretation.

3.13. Where modifications to the OLCs become necessary, the same approach as that described in paras 3.8–3.12 should be followed. All plant modifications should be reviewed to determine whether they necessitate modifications to the OLCs. Any modification to the OLCs should be subject to assessment and approval by the regulatory body as required.

3.14. When it is necessary to modify OLCs on a temporary basis, for example to perform physics tests on a new core, particular care should be taken to ensure that the effects of the change are analysed, and the modified state, although temporary, necessitates at least the same level of assessment and approval as a permanent modification. When a reasonable alternative approach is available, this should be preferred to a temporary modification of an OLC.

3.15. Periodic review of OLCs should be undertaken to ensure that they remain applicable for their intended purpose, and, where necessary, the OLCs should be modified in the light of operating experience and technological development. This periodic review should be carried out even if the plant has not been modified.

3.16. Consideration should be given to probabilistic safety assessment (PSA) applications in the optimization of OLCs. Probabilistic assessment methods together with operating experience may be used for justification and modification of OLCs.

4. SAFETY LIMITS

4.1. The concept of safety limits is based on the prevention of unacceptable releases of radioactive materials from the plant through the application of limits imposed on the temperatures of fuel and fuel cladding, coolant pressure, pressure boundary integrity and other operational characteristics influencing the release of radioactive material from the fuel. Established safety limits are to protect the integrity of certain physical barriers that guard against the uncontrolled release of radioactive material. The safety limits should be established by means of a conservative approach to ensure that all the uncertainties of safety analyses are taken into account. This implies that exceeding a single safety limit does not always lead to the unacceptable consequences mentioned earlier. Nevertheless if any safety limit is exceeded, the reactor should be shut down and normal power operation restored only after appropriate evaluation has been performed and approval for restarting has been given in accordance with established plant procedures.

4.2. The limits are chosen with the objective of maintaining the integrity of the fuel cladding and the integrity of the pressure boundary of the reactor coolant system

under all conditions, thus ensuring that there is no significant release of radioactive materials. An essential factor in maintaining the integrity of the fuel cladding is adequate cooling of the fuel. In this regard, the pressure boundary of the reactor coolant system should be kept intact. This prevents any loss of coolant and resulting reduction in the effectiveness of cooling.

4.3. Although the integrity of the containment is important in limiting the radiological consequences of an accident, loss of containment integrity does not of itself lead to damage to the fuel cladding. It is not therefore included in the safety limits but should be included under limits and conditions for normal operation (Section 6).

4.4. The temperatures of the fuel and fuel cladding should be limited to values that ensure that the design intent with respect to the extent of failures is achieved. The safety limits should usually be stated as the maximum acceptable values which ensure the integrity of the fuel cladding, with the conservatism mentioned in para. 4.1. Limits for local heat transfer rates for the fuel cladding should be defined and established to ensure that local fuel temperatures and fuel cladding temperatures do not rise to levels at which cladding failure could occur.

4.5. Safety limits for the pressure and temperature of the reactor coolant system should be stated in relation to their design values.

5. LIMITING SAFETY SYSTEM SETTINGS

5.1. There will be safety system settings for a range of parameters. These are the parameters included in safety limits as well as other parameters, or combinations of parameters, which could contribute to pressure or temperature transients. Exceeding some such settings will cause the reactor to be tripped to suppress a transient. Exceeding other settings will result in other automatic actions to prevent safety limits from being exceeded. Some other safety system settings are provided to initiate operation of engineered safety systems. These systems limit the course of anticipated operational occurrences in such a way that either safety limits are not exceeded or the consequences of postulated accidents are mitigated. The interconnection between safety system settings, safety limits and OLCs is illustrated in the Annex.

5.2. Established safety system settings should ensure automatic actuation of safety systems within parameter values assumed in the safety analysis report, despite the

possible errors that could occur adjusting the nominal set point. Appropriate alarms should be provided to enable the operating personnel to initiate corrective actions before safety system settings are reached.

5.3. The following are typical parameters, operational occurrences and protective system devices for which safety system settings are necessary. Note that the settings may be different in different plant states. For example, at a low operating temperature, the relief system for the reactor pressure vessel may necessitate lower pressure settings.

- (1) Neutron flux and distribution (startup, intermediate and operating power ranges);
- (2) Rate of change of neutron flux;
- (3) Axial power distribution factor;
- (4) Power oscillation;
- (5) Reactivity protection devices;
- (6) Temperatures of fuel cladding or fuel channel coolant;
- (7) Temperature of reactor coolant;
- (8) Rate of change of temperature of reactor coolant;
- (9) Pressure of the reactor coolant system (including cold overpressure settings);
- (10) Water level in reactor vessel or pressurizer (varying with plant state and differing with reactor type);
- (11) Reactor coolant flow;
- (12) Rate of change of reactor coolant flow;
- (13) Tripping of primary coolant circulation pump;
- (14) Intermediate cooling and ultimate heat sink;
- (15) Water level in the steam generator;
- (16) Inlet water temperature for the steam generator;
- (17) Outlet steam temperature for the steam generator;
- (18) Steam flow;
- (19) Steam pressure;
- (20) Settings provided to initiate steam line isolation, turbine trip and feedwater isolation;
- (21) Closure of isolation valve for the main steam line;
- (22) Injection of emergency coolant;
- (23) Containment pressure;
- (24) Settings provided to initiate startup of spray systems, cooling systems and isolation systems for the containment;
- (25) Dry well pressure;
- (26) Control and injection systems for coolant poison;
- (27) Radioactivity levels in the primary circuit;

- (28) Radioactivity levels in the steam line;
- (29) Radioactivity levels and levels of atmospheric contamination in the reactor building;
- (30) Loss of normal electrical power supply;
- (31) Emergency power supply.

5.4 The actions to be initiated as described in para. 5.1 for the items listed here may vary according to reactor type and design, or some of the settings may not be applicable. For particular reactor types, additional parameters may be described in the safety analysis report, for which safety system settings should be specified.

6. LIMITS AND CONDITIONS FOR NORMAL OPERATION

6.1. Limits and conditions for normal operation are intended to ensure safe operation; that is, to ensure that the assumptions of the safety analysis report are valid and that established safety limits are not exceeded in the operation of the plant. In addition, acceptable margins should be ensured between the normal operating values and the established safety system settings to avoid undesirably frequent actuation of safety systems. Figure A-1 in the Annex demonstrates a correlation between safety limits, safety system settings and limits for normal operation.

6.2. The limits and conditions for normal operation should include limits on operating parameters, stipulations for minimum amount of operable equipment, minimum staffing levels, prescribed actions to be taken by the operating staff in the event of deviations from the established OLCs and the time allowed to complete these actions. The limits should also include parameters important to safety, such as the chemical composition of working media, their activity contents and limits on discharges of radioactive material to the environment.

6.3. Operability requirements should state for the various modes of normal operation the number of systems or components important to safety that should be either in operating condition or in standby condition. These operability requirements together define the minimum safe plant configuration for each mode of normal operation. Where operability requirements cannot be met to the extent intended, the actions to be taken to manoeuvre the plant to a safer state, such as power reduction or reactor shutdown, should be specified, and the time allowed to complete the action should also be stated.

6.4. Given the higher associated risks during startup of the power plant after outages, the operability requirements for this mode should be more stringent than those

permitted for operational flexibility in power operation. Safety system equipment that is required to be operable for startup should be specified.

6.5. After an abnormal event, including a reactor trip, the cause of the event should be ascertained to the extent necessary to provide assurance that it is safe to resume operation or, in case of a trip, to restart the reactor. Procedures for determining the actions and evaluations to be carried out should be available. If OLCs have been exceeded, the cause should be investigated.

6.6. When it is necessary to remove a component of a safety system from service, confirmation should be obtained that the safety logic continues to be in accordance with design provisions. The performance of a safety function may be affected by process conditions or service system conditions that are not directly related to the equipment performing the function. It should therefore be ensured that such influences are identified and appropriate limits applied.

6.7. For the operability requirements for safety related equipment, the provisions in the design for redundancy, the reliability of the equipment and the period over which equipment may be inoperable without an unacceptable increase in risk should be taken into consideration.

6.8. The allowable periods of inoperability and the cumulative effects of these periods should be assessed in order to ensure that any increase in risk is kept to acceptable levels. Methods of PSA or reliability analysis should be used as the most appropriate means for this purpose. Shorter inoperability periods than those derived from a PSA may be stipulated in the OLCs on the basis of other information such as pre-existing safety studies or operational experience.

6.9. There is a discussion in Appendix I of those items for which limits and conditions for normal operation are generally necessary. It should be recognized that, for a particular plant design, other limits may be necessary to ensure that all parameters included in the design and in the safety analysis are adequately controlled.

7. SURVEILLANCE REQUIREMENTS

7.1. In order to ensure that safety system settings and limits and conditions for normal operation are met at all times, the relevant systems and components should be monitored, inspected, checked, calibrated and tested in accordance with an approved surveillance programme.

7.2. The surveillance programme should be adequately specified to ensure the inclusion of all aspects of the limits or conditions. The frequency of the surveillance procedures should be stated and should be based on a reliability analysis including, where available, a PSA and a study of experience gained from previous surveillance results or, in the absence of both, the recommendations of the supplier.

7.3. The surveillance requirements should be specified in procedures with clear acceptance criteria so that there are no doubts concerning system operability or component operability. The relationship between these criteria and the limit or condition being confirmed should be available in written form.

7.4. The surveillance requirements should also cover activities to detect ageing and other forms of deterioration due to corrosion, fatigue and other mechanisms. Such activities will include non-destructive examination of passive systems as well as of systems explicitly covered by limits and conditions for normal operation. If degraded conditions were to be found, then the effect on the operability of systems should be assessed and acted upon.

7.5. Further guidance concerning surveillance activities can be found in the IAEA Safety Guide on Surveillance of Items Important to Safety in Nuclear Power Plants [3].

8. OPERATING PROCEDURES

GENERAL

8.1. All safety related activities shall be performed in conformity with documents issued in accordance with approved administrative procedures. The availability and correct use of written OPs, including surveillance procedures, is an important contribution to the safe operation of a nuclear power plant. The IAEA Safety Requirements [1] state that “operating procedures shall be developed which apply comprehensively for normal, abnormal and emergency conditions ” (Ref. [1], para. 5.11).

8.2. The OPs for normal operation should be developed to ensure that the plant is operated within the OLCs and should provide instructions for the safe conduct of all modes of normal operation, such as starting up, power production, shutting down, shutdown, load changes, process monitoring and fuel handling. The OPs should be submitted to the regulatory body for assessment and approval if required.

8.3. Alarm response procedures should be developed in support of the main OPs. They should ensure timely and correct response to deviations from the limits of

steady state operation (Annex) and should ensure that the plant parameters are maintained within specified limits.

8.4. For anticipated operational occurrences and accident conditions, the OPs should provide instructions for the recovery. For design basis accidents (DBAs), these procedures to keep the plant state within specified limits may be event based or symptom based. For beyond design basis conditions, the instructions will be symptom based; that is, they will use parameters indicating the plant state to identify optimum recovery routes for the operator without the need for accident diagnosis.

8.5. When verbal and/or written instructions are used in operational practice at a nuclear power plant, administrative procedures should be in place to ensure that the verbal and/or written instructions do not diverge from the established OPs and do not compromise established OLCs. Any non-compliance should be notified to the regulatory body for prior approval.

8.6. Operating procedures should be verified and validated to ensure that they are administratively and technically correct, are easy for the operator to use and will function as intended. Special attention should be paid to ensuring that OPs are compatible with the environment in which they are intended to be used. The OPs should be validated in the form in which they will be used in the field.

8.7. The OPs should be periodically reviewed to ensure that they remain fit for their purpose and if necessary the procedures should be modified, verified, validated and approved, as required.

PARTICULAR ASPECTS OF EMERGENCY PROCEDURES

8.8. Emergency operating procedures (EOPs) may be developed as event oriented or symptom oriented. For DBAs, both approaches can be used, although symptom oriented procedures are preferable for the reasons stated in para. 8.12. For beyond design basis accidents, owing to the wide variety of conditions that may exist, symptom based EOPs and accident management guidance are preferable.

8.9. Event based EOPs specify operator actions on the basis of the determination of the event. For event based procedures, the decisions and measures to respond to accidents should be made on the basis of the state of the plant in relation to predefined events, which are considered in the design and safety analysis report. In using the event based approach, the operator must identify the specific DBA before the recovery and/or mitigatory operator actions have begun.

8.10. Event based EOPs should include at least the following:

- (a) Symptoms for the identification of the specific accident (such as alarms, operating conditions, probable magnitudes of parameter changes, characteristics of potential degradation of core cooling);
- (b) Automatic actions that will probably be taken as a result of the accident;
- (c) Immediate operator actions for the operation of controls or the confirmation of automatic actions;
- (d) Subsequent operator actions directed to returning the reactor to a normal condition or to provide for safe, extended and stable shutdown conditions.

8.11. Consideration should be given to the inherent limitations of event based procedures. These are:

- (a) Optimal recovery and/or mitigation is possible only after the proper identification of the type of event. Operators may be subject to the necessity to respond to unexpected events and may thus find themselves in situations for which they have had no specific training or for which there are no procedures to identify accurately the event that has occurred.
- (b) Only a finite number of events are analysed and accounted for in the Final Safety Analysis Report (FSAR), and unanalysed accidents beyond the design basis are outside the scope of the procedures.
- (c) Most event based procedures are oriented 'one way' and deal with only a limited number of combinations of events.
- (d) There are no links or transition points between different procedures; therefore, there is no predefined method for the operator to deal with multiple events (such as a steam line break in conjunction with a loss of coolant accident, or a loss of feedwater in conjunction with an anticipated transient with scram).

8.12. Symptom based EOPs can resolve some of the limitations of the event based approach by formally defining and prioritizing the major critical safety functions. In symptom based procedures, the decisions for measures to respond to events should be specified with respect to the symptoms and the state of systems of the plant (such as the values of safety parameters and critical safety functions). This allows the operator to maintain optimal operating characteristics without the need to be concerned with the continuing accident scenario. The method for monitoring plant parameters used in the symptom based approach is in accordance with the needs of the plant staff in severe accident conditions.

8.13. A comprehensive thermohydraulic analysis should be performed for the implementation of symptom based procedures. This analysis should ensure that the

generic set of operator actions in connection with the deterioration of each critical safety function is sufficient to withstand the most severe challenge to that safety function.

8.14. EOPs should be easy to distinguish from other plant procedures. A consistent format should be used throughout. The title of the procedure should be short and descriptive to enable the operator quickly to recognize the abnormal condition to which it applies.

8.15. Explanatory text should be avoided in EOPs, which should be limited to instructions for the operator to carry out an action or to verify the plant state. EOPs may contain supplementary background information to aid operators further in taking proper emergency actions, but this information should be separated from the main procedural actions. The instructions should include actions, where appropriate, to initiate the procedure for determining the emergency class of the accident conditions and beginning the corresponding emergency response actions. The instructions for these actions should be repeated whenever execution of an EOP or the AMG indicates a change in the severity of the event.

8.16. The EOPs or accident management guidance necessary to cope with beyond design basis accidents should be identified by a systematic analysis of the beyond design basis accidents and the plant's vulnerabilities to such accidents, and by the development of strategies to deal with these vulnerabilities.

8.17. Plant specific details should be taken into account in the identification and selection of the most suitable actions to cope with beyond design basis accidents. The accident management guidance for severe accidents should include the utilization of all possible means, safety related or conventional, in the plant or from neighbouring units or external, with the aim of preventing the release of radioactive material to the environment.

8.18. To ensure the effective use of accident management guidance, it should be carefully interfaced with the existing EOPs to provide continuity and to avoid any omissions or contradictions.

PROCEDURES FOR OPERATION IN THE COMMISSIONING PHASE

8.19. Construction, commissioning and operating groups co-exist in the commissioning phase, and a gradual transfer of responsibilities takes place from one group to the other, until the responsibility for the complete plant is taken over by the management

of the operating plant. During this time, operations should be performed by the operating group under the supervision of the commissioning group, in accordance with test procedures prepared for implementing the commissioning programme.

8.20. The test procedures should follow normal plant OPs to the extent practicable, in order to verify and, if necessary, amend such procedures. This process also provides an opportunity for operating personnel to become familiar with normal plant OPs and plant response to these procedures. More guidance on the procedures for operation in the commissioning stage can be found in the IAEA Safety Guide on Commissioning Procedures for Nuclear Power Plants [5].

9. DEVELOPMENT OF OPERATING PROCEDURES

9.1. In order to develop a set of procedures for use in operation, a planned and systematic process should be applied. This may be assisted by the use of a comprehensive writer's guide.

9.2. Each procedure should be sufficiently detailed for a qualified individual to be able to perform the required activities without direct supervision, but should not seek to provide a complete description of the plant processes involved.

9.3. The format of procedures may vary from plant to plant, depending on the policies of the operating organization, but should be developed in accordance with established quality assurance requirements and recommendations. Appropriate guidance is provided in an IAEA Safety Series publication on quality assurance [6], and particularly in Safety Guide No. 50-SG-Q13.

9.4. Persons with appropriate competence and experience shall be designated to draw up and verify procedures.

9.5. Techniques that take account of human factors, such as task analysis, should be used to develop safe, reliable and effective OPs in which account is taken of the layout of the control room, the general design of the plant, and staffing arrangements and operating experience at the plant concerned.

9.6. Guidance specific to the plant should be provided in the following areas:

(a) A clear definition of constraints specified in the safety analysis report and the OLCs;

- (b) Appropriate links between procedures to avoid omissions and duplication, and clear identification of entry and exit conditions;
- (c) Presentation to the operator in a manner conforming to good practice in relation to human factors, including clarity of objective and meaning, and use where appropriate of flow charts, diagrams and other aids to the operator;
- (d) The need for written explanations of the basis for the procedure, to assist the user and persons modifying the procedure in the future;
- (e) A verification and approval process that includes validation for the plant in question or for a simulation as relevant as practicable;
- (f) The use of event and symptom based procedures for dealing with anticipated operational occurrences and accident conditions, with the use of symptom based procedures for accident conditions beyond the design basis.

9.7. In addition, proper identification of the relevant sensors, alarms and actuators, especially with regard to post-incident or post-accident procedures, should be provided so as to ensure a safe transition to an adequately safe state. Further guidance on the approach to the development of OPs is provided in Appendix II.

10. COMPLIANCE WITH OPERATIONAL LIMITS AND CONDITIONS AND OPERATING PROCEDURES

10.1. The plant's management has the primary responsibility for ensuring compliance with the OLCs. To discharge this responsibility, relevant controls should be established in accordance with the IAEA Code on Quality Assurance and the associated Safety Guides [6]. A major contribution to compliance with OLCs is the provision of OPs consistent with the OLCs. Some OLCs may be directly stated in procedures or other documents, and if so this should be clearly indicated in the implementing document. For multiunit plants, OLCs should not be presented for more than one unit in a single document.

10.2. In order to help ensure compliance, all persons who have responsibilities in the application of OLCs should always have available a copy of the OLCs currently in force and should be adequately trained in their application. If possible, operational limits should be legibly indicated on instruments and displays so as to facilitate compliance. Similarly, the current OPs should be immediately available to the control room personnel and to others who need to use them or refer to them. Operating personnel should be adequately trained in the application of current procedures and

appropriate retraining should be planned and conducted when the OLCs and OPs are modified.

10.3. If it should occur that an OLC is not being met or a procedure cannot be followed, then this should be reported and the causes should be analysed. This may lead to the modification of an OLC or procedure in accordance with established procedures which allow for changes to be made in a controlled manner and approved, as required by the regulatory body. Results of routine or commissioning tests also necessitate analysis and consideration of the need for modifications to the OLCs and/or the OPs.

10.4. Methods of configuration management should be used when modifying OLCs or OPs to ensure that other documents remain consistent with the modified OLCs and OPs. In particular, there should be a mechanism to track from the safety analysis through the OLCs to the implementing procedures, in order to aid configuration control and to avoid the accidental deletion or retention of an OLC or its accidental application. See also IAEA Safety Guide No. 50-SG-Q2 on Quality Assurance [6].

10.5. There should be limits and conditions on staff numbers, notably in the control room (Appendix I). The OPs should be designed to be used by the staff available, in terms of both numbers and qualifications. The OPs should make clear who is responsible for their implementation. Where there is a need for oral communication, this should be conducted in accordance with approved protocols.

10.6. Records of plant operation and demonstrations of compliance with OLCs and OPs should be made and stored in accordance with IAEA Safety Guide No. 50-SG-Q3 on quality assurance [6]. Reports of non-compliance should be investigated to ensure that corrective action is implemented and to help prevent such non-compliance in future. Typical documents and records relating to this Safety Guide are as follows:

- (a) Operational records covering periods at each power level, including shutdown;
- (b) Records of the surveillance programme;
- (c) Records of the fuel inventory (new and used), fuel transfers, histories of fuel burnup and core verification;
- (d) Records of releases of gaseous and liquid radioactive materials to the environment, and of solid and liquid radioactive wastes accumulated on the site;
- (e) Records of pressure cycles and temperature cycles for the components of the system for primary heat transport;
- (f) Records of reviews of modifications made to OPs or plant equipment that were related to OLCs, or of the reviews of the modifications made to the OLCs;
- (g) Records of audits, their findings and corrective actions;

- (h) Reports of deviations from OLCs or procedures;
- (i) Reports of human errors or component failures in the safety systems that affected compliance with the OLCs;
- (j) Special or temporary operating instructions for deviations from normal operation, abnormal occurrences and experimental requirements;
- (k) Administrative procedures for the production and authorization of OPs, including special and temporary OPs.

10.7. Specific consideration should be given to configuring the documentation referred to in para. 10.6 so that the records relevant to the decommissioning stage may be readily identified and retrieved when necessary. For guidance on decommissioning, see Ref. [7]. See also IAEA Safety Guide No. 50-SG-Q14 on quality assurance [6].

Appendix I

SELECTION OF LIMITS AND CONDITIONS FOR NORMAL OPERATION

REACTIVITY CONTROL

Negative reactivity requirements

I.1. The minimum negative reactivity in the reactivity control devices available for insertion should be such that the degree of subcriticality assumed in the safety analysis report can be reached immediately after shutdown from any operational state and in any relevant accident conditions.

I.2. The necessary negative reactivity should be specified in terms of the information available to the reactor operator, such as control rod positions, liquid poison concentration or neutron multiplication factors.

I.3. To maintain the specified degree of subcriticality for an indefinite period of time after shutdown, additional means as provided in the design may be used, such as the use of boronated water or other poisons if the temperature, xenon concentration or other transient reactivity effects cannot be compensated for by normal reactivity control devices.

Reactivity coefficients

I.4. Where the safety analysis indicates the need, limits should be stated for the reactivity coefficients for different reactor conditions to ensure that the assumptions used in the accident and transient analyses remain valid through each fuelling cycle.

Rate of insertion for positive reactivity

I.5. Limits on the rate of insertion for positive reactivity should be stated. Compliance should be ensured either by means of reactivity system logic or by setting special limitations to be observed by operating personnel, in order to avoid reactivity related accident conditions which might lead to excessive fuel temperatures.

Monitoring the neutron flux in the reactor core

I.6. Instrumentation needs for adequate monitoring of the neutron flux for reactor power levels, including startup and shutdown conditions, should be stated. These may

include stipulations on the use of neutron sources for providing the necessary minimum flux level and on the sensitivity of neutron detectors.

Devices for reactivity control

I.7. Operability requirements for reactivity control devices, including requirements for redundancy or diversity as stated in the safety analysis report, and their position indicators should be stated for the various modes of normal operation. These operability requirements should specifically define the proper sequence and the actuation and insertion times for reactivity control devices. Operating times for reactivity control devices should be consistent with, or more conservative than, the design assumptions.

Reactivity differences

I.8. Limits on permissible reactivity differences between predicted and actual critical configurations of reactivity control devices should be stated, and conformance should be verified in the initial criticality phase after each major refuelling and at specified intervals. The cause of significant differences should be evaluated and the necessary corrective action should be taken.

Liquid poison systems

I.9. Concentration, storage and temperature limits affecting solubility should be stated for all liquid poison systems, and appropriate measures should be specified to ensure detection and correction of deviations from these limits. Operability requirements to ensure proper actuation and functioning of the systems should be stated, and the actuation and injection times should be defined.

Core

I.10. After any alteration to the core, the location of fuel and in-core components should be confirmed and verified in accordance with written procedures in order to ensure that every item is in the correct place.

Prevention of boron dilution

I.11. In light water reactors, particular attention should be paid to minimizing the possibility of a boron dilution event during shutdown operations. Limits and conditions on the boron concentration, neutron flux monitoring in the range of the source, isolation of unboronated water sources and emergency boronating systems should be stated.

REACTOR PROTECTION SYSTEM AND INSTRUMENTATION

Reactor protection system and instrumentation for other safety systems

I.12. Operability requirements should be stated for the reactor protection system and for instrumentation and logic for other safety systems, together with limits on response times, instrument drift and accuracy, where appropriate. Interlocks required by the safety analysis report should be identified and relevant operability requirements should be stated.

Instrumentation and control for remote shutdown

I.13. Where instrumentation and control for remote shutdown are provided for in the plant design in case of the possible loss of habitability of the main control room, the operability requirements for the essential parameters (such as temperature, pressure, coolant flow and neutron flux) should be stated to permit the plant to be shut down and maintained in a safe condition from a location or locations outside the main control room.

CORE COOLING

Temperature of the reactor coolant system

I.14. Limits on the coolant temperature (maximum or minimum) and rate of temperature change should be stated for the various modes of normal operation to ensure that specified safety limits of core parameters are not exceeded and that temperatures affecting coolant system integrity are maintained within appropriate bounds.

Pressure of the reactor coolant system

I.15. Limits on the permissible pressure of the reactor coolant system should be stated for the various modes of normal operation. For some purposes, for example in order to take account of limitations in the properties of materials, these operational limits should be stated in conjunction with other parameters such as temperature or coolant flow. In such cases, the relations should be clearly stated, and any curves or calculational techniques necessary to ensure that permissible conditions are not exceeded should be provided. Likewise, where applicable, special requirements should be stated. Limits should be selected so that the initial conditions assumed for the various accident analyses are not exceeded and the integrity of the primary coolant system is maintained.

Reactor power

I.16. Limits on the total reactor power should be established and defined in the safety analysis report, in order to ensure that the capacity of the core cooling systems is not exceeded.

Distribution of reactor power

I.17. The special logic for reactivity control, or control rod and/or absorber patterns, together with reactivity values for the control rods, should be stated where necessary in order to ensure that the specified limitations for permissible flux differences, power peaking factors and power distribution for various modes of normal operation are met. Proper control of flux distributions should ensure that the limiting fuel temperatures and heat flux and the initial conditions assumed in the accident analyses are not exceeded. If appropriate, proper calculational methods or measuring techniques should be provided to enable the reactor operator to confirm compliance.

Chemical quality of the reactor coolant

I.18. In addition to the limitations mentioned on pressure and temperature, limits should be stated for chemical quality of the reactor coolant; for instance, in water cooled reactors, the conductivity, the pH value, the oxygen content and the levels of impurities such as chlorine and fluorine are important.

Pressure safety valves and/or relief valves

I.19. Operability requirements should be stated for the number of safety valves and/or relief valves required for the reactor coolant system. For direct cycle boiling water plants, this system includes the steam system relief valves and safety valves. The pressure settings for valve actuation should be stated. Selection of these values should be such that system integrity is maintained in all operational states, including operation at low temperatures.

Moderator and cover gas system

I.20. As appropriate, limits for moderator temperature, chemical quality and contaminant levels should be stated. Limits for permissible concentrations of explosive gas mixtures in the cover gas should also be stated. In this regard, operability requirements for equipment for on-line process monitoring should be specified.

Steam generators

I.21. Operability requirements consistent with those described in the safety analysis report should be stated for steam generators. These requirements should include requirements for the operability of emergency feedwater systems and of safety valves and isolation valves of the steam system, as well as requirements for satisfactory water quality and specified limitations on water level and on the minimum capacity for heat exchange.

Leakage of the reactor coolant system

I.22. Leakage limits should be such that the coolant inventory can be maintained by normal make-up systems and that the system integrity can be maintained to the degree assumed in the safety analysis report. Specifications of maximum leakage from particular components important to safety, commensurate with their safety function, should be provided. In establishing leakage limits, consideration should be given to the permissible limits of contamination of the environment or of secondary systems by the leaking media. Operability requirements should be stated for the detection of, or for measuring systems for, leakage of reactor coolant. In general, leakages should be classified as identified (for example, leakages into collection systems such as those at pump seals, into the containment atmosphere or through the steam generator; these leakages should be measured in order not to mask the unidentified leakages) or unidentified leakages.

Reactor coolant radioactivity

I.23. Limits for the permissible specific activity of the reactor coolant should be stated in order to ensure the protection of personnel and the environment as well as to provide a measure of fuel integrity, as discussed in the safety analysis report. If on-line measurement of coolant activity is used to monitor the fuel cladding integrity in operation, the minimum provisions for the detection and, where appropriate, identification of failed or suspect fuel should be stated.

Ultimate heat sink

I.24. The ultimate heat sink is usually the river, lake or sea from which cooling water for equipment and condensers is drawn. In some cases dry or wet cooling towers are also used. Limitations on power production levels consistent with the cooling capabilities of these heat sinks should be specified.

Removal of decay heat at shutdown

I.25. Operations in the shutdown state may cause a restriction in the capability of the reactor cooling systems. Limits on decay heat levels should be stated for the commencement of certain operations such as reducing coolant levels or opening the reactor coolant system and containment boundaries. Additional limits and conditions should be specified to identify the necessary cooling systems to be operable in all shutdown states. In light water reactors, particular attention should be paid to the control and monitoring of water levels during shutdown operations to prevent the loss of the systems for removal of decay heat. Limits and conditions on allowable levels and necessary operable instrumentation should be provided.

Emergency core cooling systems

I.26. Operability requirements should be stated for the various systems used for emergency core cooling. These should include requirements on: equipment operability and environmental conditions; adequacy of the injection and circulation of coolant; integrity of piping systems; specified limitations on minimum quantities of fluids for all systems relied upon for emergency core cooling. These operability requirements should cover all the provisions necessary to cope with relevant accidents analysed in the safety analysis report. In particular, to ensure the continuous availability of these systems, operability requirements should also be stated for emergency power supply systems and other auxiliary systems, such as heating circuits used to prevent freeze-up of solutions, for equipment cooling systems and for ventilation systems. The long term capability of these emergency systems after the occurrence of a relevant accident should also be considered and specified to ensure that any release of radioactive substances to the environment is below acceptable limits.

CONTAINMENT SYSTEMS

I.27. Operability requirements for containment systems should be stated and should include the plant conditions for which containment integrity is not required. Permissible leakage rates should be specified, and the operability and condition of the following should be stated: isolation valves; vacuum breaker valves; actuation devices; systems for filtration, cooling, dousing and spraying; control and analysis systems for combustible gases; venting and purging systems; associated instrumentation. The OLCs specified should be such that the release of radioactive materials from the containment system will be restricted to those leakage paths and rates assumed in the accident analyses. Precautions for access control should be specified in order to ensure that the effectiveness of the containment system is not impaired.

OTHER SYSTEMS

Ventilation systems

I.28. If applicable, appropriate limits should be established on the operability of ventilation systems where such systems have been provided for the purpose of controlling airborne radioactive material within stated limits in support of a safety system.

Ventilation of secondary containment

I.29. If secondary containment is provided, it should be ventilated and kept at an appropriate absolute pressure as described in the safety analysis report, to ensure that any possible direct leakage will remain below the value assumed. Appropriate limits in terms of pressures or leakage rates should be stated.

Service systems

I.30. The reliable operation of many safety systems is dependent on the operation of service systems such as compressed air systems and service water systems. Limits and conditions for these service systems should be considered if they can have a major effect on plant safety.

Electrical power systems and other power sources

I.31. Requirements for the availability of the electrical power sources should be stated for all operational states. These include: off-site sources; on-site generators (diesels and gas turbines, including associated fuel reserves); batteries and associated control; protective, distribution and switching devices. The operability requirements should be such that sufficient power will be available to supply all safety related equipment necessary for safe shutdown of the plant, and for the mitigation and control of accident conditions. The operability requirements should determine the necessary power, redundancy of supply lines, maximum permissible time delays and necessary duration of the emergency power supply. Equivalent requirements should be stated for other power sources (for example, the pneumatic power system). Particular care should be taken to ensure that electrical supplies remain adequate in shutdown operations, when many systems and components will be out of service for maintenance.

Seismic monitors

I.32. Where applicable, operability requirements for seismic monitoring instrumentation should be stated. Settings should be established for alarms or for any corrective

action consistent with the safety analysis report. The number of devices specified should be sufficient to ensure that any necessary automatic action is initiated at the specified limits.

Movements of heavy objects

I.33. Limits and conditions should be provided to prevent the movement of heavy objects over, or adjacent to, areas where safety related systems or components could be damaged as a result of misuse or failure of the lifting equipment. It is likely that such limits and conditions will vary with the operational mode.

Fuel handling

I.34. Operational requirements for fuel and absorber handling should include limits on the amount of fuel which can be handled at one time and, if necessary, on the temperature and decay time of irradiated fuel. If appropriate, the requirements for operability of fuel handling equipment should be stated. Provision should be made for monitoring the core reactivity during fuel loading or refuelling operations to ensure that the reactivity requirements are met. The procedures and instrumentation required for such monitoring should be specified. To ensure that operations which might give rise to nuclear excursions or radiation hazards are not undertaken during fuel movements, requirements for communication between the fuel handling personnel and the operating personnel in the control room should be stated.

Storage of irradiated fuel

I.35. The conditions for storage of irradiated fuel should be stated and should include: the minimum cooling capability of the cooling system for spent fuel and the minimum water level above the fuel; a prohibition against storage of fuel in any position other than that designated for irradiated fuel; the minimum reserve capacity for storage; and the appropriate reactivity margins to guard against criticality in the storage area. Appropriate radiation monitoring should also be specified for the storage area for irradiated fuel.

Storage of new fuel

I.36. The criteria for new fuel storage should be stated. Any special measures to prevent criticality in new fuel during handling or storage should also be stated. When required, fuel enrichment should also be verified before insertion into the core.

Instrumentation for radiation monitoring

I.37. Operability requirements for radiation monitoring instrumentation, including monitoring of effluents, should be stated. These operability requirements should be such as to ensure that appropriate areas and release paths are adequately monitored in accordance with the requirements for radiological protection and the requirements of the regulatory body, and to ensure that an alarm or an appropriate action is initiated if the prescribed radiation limit or activity limit is exceeded.

Plant staffing

I.38. The plant personnel required to be on duty for the various operational states should be specified and shall be sufficient to implement the necessary emergency procedures. The minimum staffing required for the control room should be stated, including the necessary qualifications for their duties.

Fire protection systems

I.39. Requirements for the availability of fire protection systems should be stated for all operational states.

Appendix II

DEVELOPMENT OF OPERATING PROCEDURES (OUTLINES)

II.1. Plant operating procedures may be developed along the lines shown in Fig. II.1, following quality assurance principles.

II.2. The drafting of operating procedures (Box 1) should normally be done by the operating group. The main documents used as references should include:

- (a) Documents containing design assumptions and intentions;
- (b) Contractual documents from the contractors giving guidance on the operation of systems and components;
- (c) Commissioning documents (see the IAEA Safety Guide on the Commissioning Procedures for Nuclear Power Plants [5]);
- (d) Documents containing procedures from other plants of the same or similar types.

The operating group should ensure in any case that procedures are consistent with safety analysis reports, OLCs and any other regulatory requirements, as well as with the policy of the operating organization as contained in the plant manual.

II.3. Review of the first draft of the OPs, and in particular of the safety aspects (Box 2), should be performed by a suitably qualified person whose qualifications are at least equal to that of the drafter of the document. The reviewer should check that the draft does state that all features of the plant and its performance that are assumed as cornerstones in the safety analyses are required to be operable or to be complied with. The review should also consider the formal and editorial aspects of the document.

II.4. Comments on the draft should be requested from the operating staff and, as appropriate, from the designer and constructor (Boxes 3 and 3(a)).

II.5. After authorization by the Operations Manager (Box 4), the procedure should be validated by first attempting to apply it in the actual initial operation of each system or if necessary during simulated operation (Box 5). This validation should be performed, wherever possible, by personnel other than those responsible for the drafting and review. In those cases where only a simulated operation was carried out, the procedure should finally be validated by actual operation of the system as soon as this is possible.

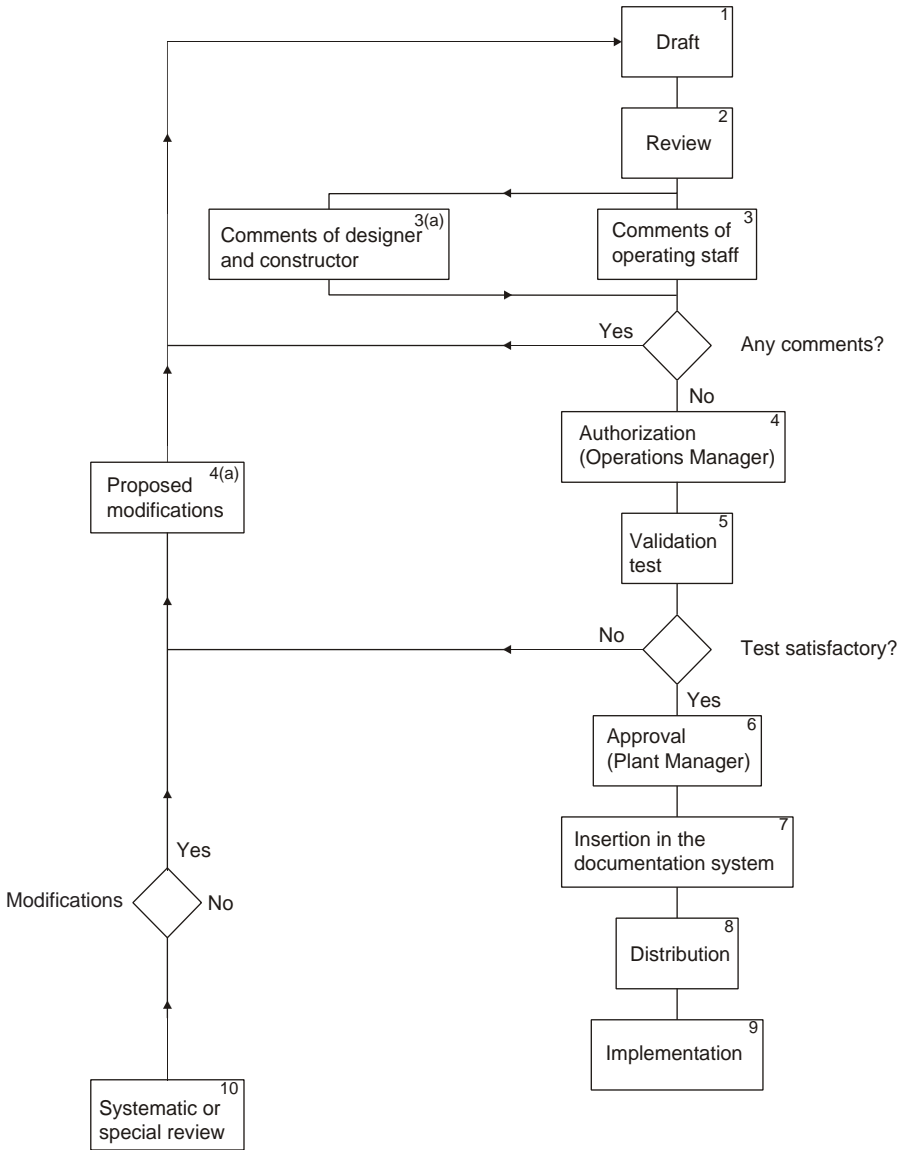


FIG. II.1. Flow diagram for the development of operating procedures.

II.6. If the validation test is satisfactory, the draft should be sent to the plant manager with the recommendation that it be approved and issued. If the draft is not satisfactory, it should be sent back to the drafter with proposed modifications (Box 4(a)).

II.7. The procedures should be approved and issued after it has been confirmed that no further modifications are considered necessary (Box 6). The procedures should then be entered into the documentation system, included in the plant manual, and treated in accordance with quality assurance principles (Box 7).

II.8. All procedures which have been approved should be distributed in accordance with written administrative procedures and made available for use in the control room (Boxes 8 and 9).

II.9. Reviews should be carried out at stated intervals (usually one or two years) or whenever necessary in the light of operating experience (Box 10).

II.10. Any modification to the procedures as a result of the above mentioned reviews should be made following the same flow of the arrangements as for the initial document.

REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Operation, Safety Standards Series No. NS-R-2, IAEA, Vienna (2000).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance of Nuclear Power Plants, Safety Series No. 50-SG-O7, IAEA, Vienna (1990).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Surveillance of Items Important to Safety in Nuclear Power Plants, Safety Series No. 50-SG-O8, IAEA, Vienna (1990).
- [4] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Commissioning Procedures for Nuclear Power Plants, Safety Series No. 50-SG-O4, IAEA, Vienna (1980).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).
- [7] INTERNATIONAL ATOMIC ENERGY AGENCY, Decommissioning of Nuclear Power Plants and Research Reactors, Safety Standards Series No. WS-G-2.1, IAEA, Vienna (1999).

Annex

EXAMPLE TO EXPLAIN SOME TERMS USED

INTRODUCTION

A-1. Figure A-1 explains and illustrates the interrelationship between a safety limit, a safety system setting and an operational limit.

A-2. For clarity, the example given in Fig. A-1 illustrates only the case in which the critical parameter of concern is the fuel cladding temperature.

A-3. It is assumed for the purposes of Fig. A-1 that a correlation has been established in the safety analysis report between a monitored parameter (in this case, coolant temperature) and the maximum fuel cladding temperature, for which a safety limit has been established. The safety analysis would show that actuation of the safety system by the monitored coolant temperature at the safety system setting should prevent the fuel cladding temperature from reaching the set safety limit beyond which releases of significant amounts of radioactive material from the fuel might occur.

RANGE OF STEADY STATE OPERATION

A-4. The monitored parameter should be kept within the steady state range by the control system or by the operator in accordance with the OPs.

ALARM SETTING EXCEEDED (CURVE No. 1)

A-5. The monitored parameters may exceed the steady state range as a result of load changes or imbalance of the control system, for example. If the temperature rise reaches an alarm setting, then the operator will be alerted and will take action to supplement any automatic systems in reducing temperature to the steady state values without allowing the temperature to reach the operational limit for normal operation. The delay in the operator's response should be taken into consideration.

OPERATIONAL LIMIT EXCEEDED (CURVE No. 2)

A-6. Limits for normal operation may be set at any level between the range of steady state operation and the actuation setting for the safety system, on the basis of the

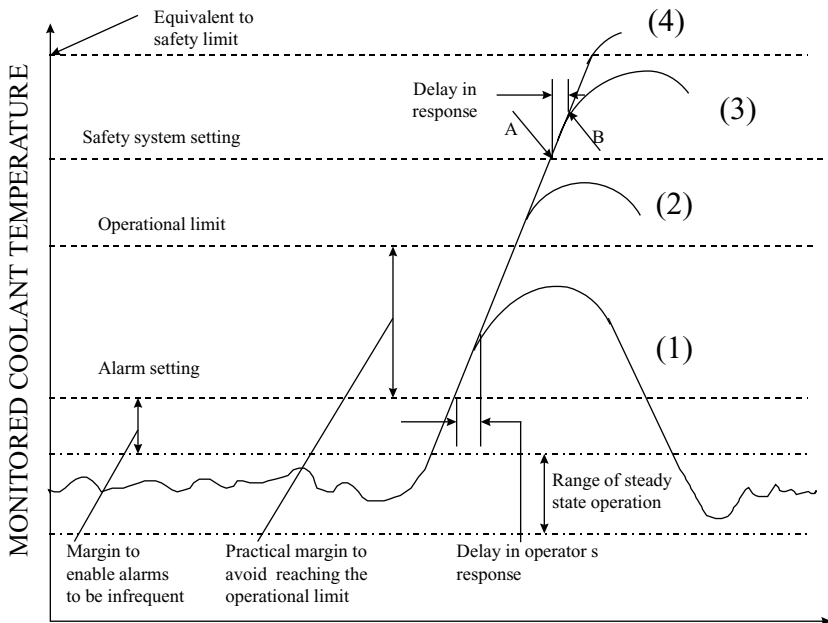
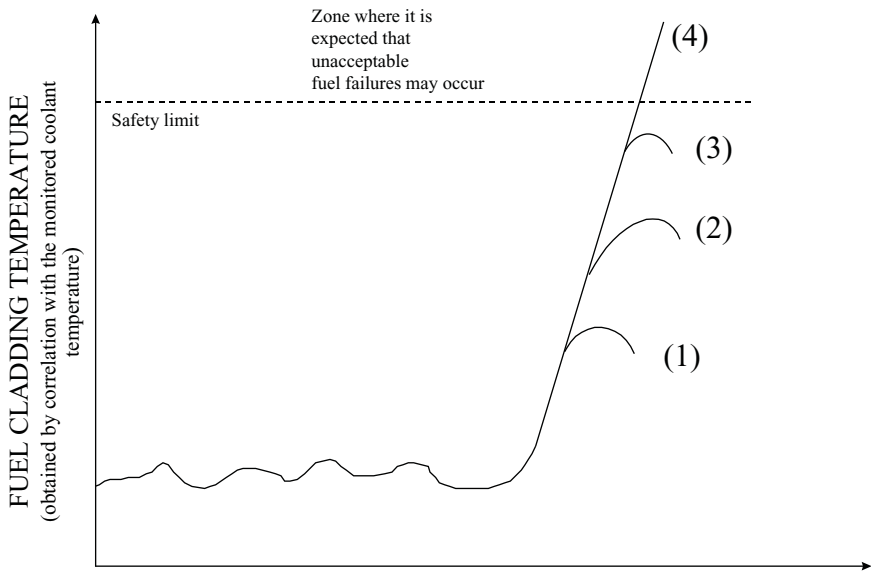


FIG. A-1. Interrelationship between a safety limit, a safety system setting and an operational limit.

results of the safety analysis. It is normal to have margins between alarm settings and operational limits in order to take account of routine fluctuations arising in normal operation. There may also be a margin between the operational limit and the safety system setting to allow the operator to take action to control a transient without activating the safety system. If the operational limit is reached and the operator is able to take corrective action to prevent the safety system setting being reached, then the transient will be of the form of curve 2.

SAFETY SYSTEM SETTING EXCEEDED (CURVE No. 3)

A-7. In the event of malfunction of the control system or operator error or for other reasons, the monitored parameter might reach the safety system setting at point A with the consequence that the safety system is actuated. This corrective action only becomes effective at point B owing to inherent delays in the instrumentation and equipment of the safety system. The response should be sufficient to prevent the safety limit being reached, although local fuel damage cannot be excluded.

SAFETY LIMIT EXCEEDED (CURVE No. 4)

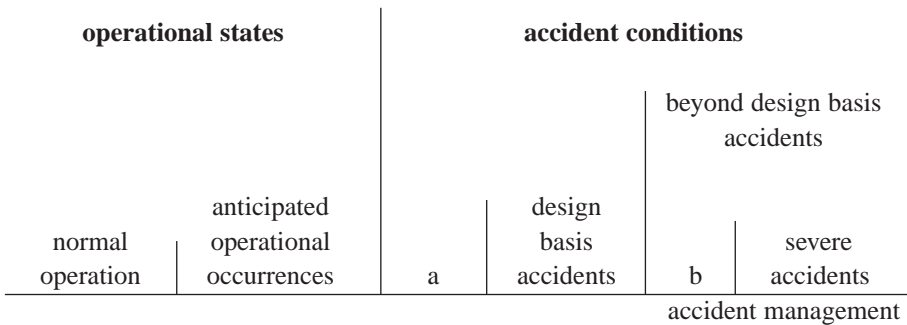
A-8. In the event of a failure that exceeds the most severe one that the plant was designed to cope with, or a failure or multiple failures in a safety system, it would be possible for the temperature of the cladding to exceed the value of the safety limit, and hence significant amounts of radioactive material could be released. Additional safety systems may be actuated by other parameters to bring other engineered safety features into operation to mitigate the consequences, and measures for accident management may be activated.

GLOSSARY

operating organization/operator. Any organization applying for authorization or authorized to operate a nuclear power plant and responsible for its safety.

operational limits and conditions. A set of rules setting forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the regulatory body for safe operation of a nuclear power plant.

plant states



a: Accident conditions which are not explicitly considered design basis accidents but which are encompassed by them.

b: Beyond design basis accidents without significant core degradation.

accident conditions. Deviations from normal operation more severe than anticipated operational occurrences, including design basis accidents and severe accidents.

accident management. The taking of a set of actions during the evolution of a beyond design basis accident:

- To prevent the escalation of the event into a severe accident;
- To mitigate the consequences of a severe accident;
- To achieve a long term safe stable state.

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

design basis accident. Accident conditions against which a nuclear power plant is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

normal operation. Operation within specified operational limits and conditions.

operational states. States defined under normal operation and anticipated operational occurrences.

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

safety limits. Limits on operational parameters within which the operation of a nuclear power plant has been shown to be safe.

safety system. A system important to safety, provided to ensure the safe shutdown of the reactor or residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents.

safety system settings. The levels at which protective devices are automatically actuated in the event of anticipated operational occurrences or accident conditions, to prevent safety limits being exceeded.

CONTRIBUTORS TO DRAFTING AND REVIEW

Brandejs, P.	State Office for Nuclear Safety, Czech Republic
Lange, D.	International Atomic Energy Agency
McIntyre, P.	Berkeley Power Station, United Kingdom
Straub, G.	TUV Energie und Systemtechnik GmbH, Germany
Taylor, R.	International Atomic Energy Agency
Vaišnys, P.	International Atomic Energy Agency

ADVISORY BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS

Nuclear Safety Standards Advisory Committee

Belgium: Govaerts, P. (Chair); *Brazil:* da Silva, A.J.C.; *Canada:* Wigfull, P.; *China:* Lei, Y., Zhao, Y.; *Czech Republic:* Stuller, J.; *Finland:* Salminen, P.; *France:* Saint Raymond, P.; *Germany:* Wendling, R.D., Sengewein, H., Krüger, W.; *India:* Venkat Raj, V.; *Japan:* Tobioka, T.; *Republic of Korea:* Moon, P.S.H.; *Netherlands:* de Munk, P., Versteeg, J.; *Russian Federation:* Baklushin, R.P.; *Sweden:* Viktorsson, C., Jende, E.; *United Kingdom:* Willby, C., Pape, R.P.; *United States of America:* Morris, B.M.; *IAEA:* Lacey, D.J. (Co-ordinator); *OECD Nuclear Energy Agency:* Frescura, G., Royen, J.

Advisory Commission for Safety Standards

Argentina: Beninson, D.; *Australia:* Lokan, K., Burns, P., *Canada:* Bishop, A. (Chair), Duncan, R.M.; *China:* Huang, Q., Zhao, C.; *France:* Lacoste, A.-C., Asty, M.; *Germany:* Hennenhöfer, G., Wendling, R.D.; *Japan:* Sumita, K., Sato, K.; *Republic of Korea:* Lim, Y.K.; *Slovak Republic:* Lipár, M., Misák, J.; *Spain:* Alonso, A., Trueba, P.; *Sweden:* Holm, L.-E.; *Switzerland:* Prêtre, S.; *United Kingdom:* Williams, L.G., Harbison, S.A.; *United States of America:* Travers, W.D., Callan, L.J., Taylor, J.M.; *IAEA:* Karbassioun, A. (Co-ordinator); *International Commission on Radiological Protection:* Valentin, J.; *OECD Nuclear Energy Agency:* Frescura, G.