Safety Reports Series
No. 46

Assessment of Defence in Depth for Nuclear Power Plants

IAEA
International Atomic Energy Agency

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, and also general safety (i.e. all these areas of safety). The publication categories in the series are **Safety Fundamentals, Safety Requirements** and **Safety Guides**.

Safety standards are coded according to their coverage: nuclear safety (NS), radiation safety (RS), transport safety (TS), waste safety (WS) and general safety (GS).

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 P.O. Box 100, A-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 e-mail 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 in other publications series, in particular the **Safety Reports Series**. Safety Reports provide practical examples and detailed methods that can be used in support of the safety standards. Other IAEA series of safety related publications are the **Provision for the Application of Safety Standards Series**, the **Radiological Assessment Reports Series** and the International Nuclear Safety Group's **INSAG Series**. The IAEA also issues reports on radiological accidents and other special publications.

Safety related publications are also issued in the **Technical Reports Series**, the **IAEA-TECDOC Series**, the **Training Course Series** and the **IAEA Services Series**, and as **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. Security related publications are issued in the **IAEA Nuclear Security Series**.

ASSESSMENT OF DEFENCE IN DEPTH FOR NUCLEAR POWER PLANTS

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

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

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

Printed by the IAEA in Austria
February 2005
STI/PUB/1218

SAFETY REPORTS SERIES No. 46

ASSESSMENT OF DEFENCE IN DEPTH FOR NUCLEAR POWER PLANTS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2005

COPYRIGHT NOTICE

IAEA Library Cataloguing in Publication Data

Assessment of defence in depth for nuclear power plants. — Vienna : International Atomic Energy Agency, 2005.
p. ; 24 cm. — (Safety reports series, ISSN 1020–6450 ; no. 46)
STI/PUB/1218
ISBN 92–0–114004–5
Includes bibliographical references.

1. Nuclear reactors — Safety measures. 2. Nuclear power plants — Design and construction. 3. Nuclear engineering — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL 04–00388

FOREWORD

Defence in depth is a comprehensive approach to safety that has been developed by nuclear power experts to ensure with high confidence that the public and the environment are protected from any hazards posed by the use of nuclear power for the generation of electricity. The concepts of defence in depth and safety culture have served the nuclear power industry well as a basic philosophy for the safe design and operation of nuclear power plants.

Properly applied, defence in depth ensures that no single human error or equipment failure at one level of defence, nor even a combination of failures at more than one level of defence, propagates to jeopardize defence in depth at the subsequent level or leads to harm to the public or the environment.

The importance of the concept of defence in depth is underlined in IAEA Safety Standards, in particular in the requirements set forth in the Safety Standards: Safety of Nuclear Power Plants: Design (NS-R-1) and Safety Assessment and Verification for Nuclear Power Plants (NS-G-1.2). A specific report, Defence in Depth in Nuclear Safety (INSAG-10), describes the objectives, strategy, implementation and future development in the area of defence in depth in nuclear and radiation safety. In the report Basic Safety Principles for Nuclear Power Plants (INSAG-12), defence in depth is recognized as one of the fundamental safety principles that underlie the safety of nuclear power plants.

In consonance with those high level publications, this Safety Report provides more specific technical information on the implementation of this concept in the siting, design, construction and operation of nuclear power plants. It describes a method for comprehensive and balanced review of the provisions required for implementing defence in depth in existing plants.

This publication is intended to provide guidance primarily for the self-assessment by plant operators of the comprehensiveness and quality of defence in depth provisions. It can be used equally by regulators and independent reviewers. It offers a tool that is complementary to other methods for evaluating the strengths and weaknesses of defence in depth in specific plants.

The IAEA staff members responsible for this publication were J. Höhn and J. Mišák of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

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

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

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

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The concept of defence in depth has been developed from the original idea of placing multiple barriers between radioactive materials and the environment. At present the concept includes a more general structure of multiple physical barriers and complementary means to protect the barriers themselves, the so-called levels of defence. It ensures that a high level of safety is reliably achieved with sufficient margins to compensate for equipment failures and human errors.

Defence in depth is implemented to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within nuclear power plants and events initiated outside plants. Defence in depth is an overall safety philosophy that encompasses all safety activities, including the siting, design, manufacture, construction, commissioning, operation and decommissioning of nuclear power plants.

Systematic assessments of the implementation of defence in depth are performed throughout the lifetime of a plant, and are typically conducted by different organizations. For assessment, engineering methods are used, combining qualitative analysis and quantitative methods. Computational analytical tools are typically used to evaluate the performance of the barriers and safety systems.

The concept of defence in depth is applied to a broad variety of safety related activities and measures, be they organizational, behavioural or design related. However, no single method is available for assessing the importance of these measures, which vary in nature. Whilst progress has been made recently in this area through the use of probabilistic methods, the deterministic approach is still primarily directed at evaluating design features only.

Therefore, there is a need for developing a comprehensive deterministic safety assessment approach, which should be able to consider the contributions of the various defence in depth provisions[1] to the overall safety aim of defence in depth.

[1] Provisions: measures implemented in design and operation such as inherent plant characteristics, safety margins, system design features and operational measures contributing to the performance of the safety functions aimed at preventing the mechanisms from occurring.

1.2. OBJECTIVE

The present publication describes a method for assessing the defence in depth capabilities of an existing plant, including both its design features and the operational measures taken to ensure safety. A systematic identification of the required safety provisions for the siting, design, construction and operation of the plant provides the basis for assessing the comprehensiveness and quality of defence in depth at the plant.

The five levels of defence in depth are covered in the present review. For given objectives at each level of defence, a set of challenges[2] is identified, and several root mechanisms[3] leading to the challenges are specified. Finally, to the extent possible, a comprehensive list of safety provisions, which contribute to preventing these mechanisms from occurring, is provided. A broad spectrum of provisions, which encompass the inherent safety features, equipment, procedures, staff availability, staff training and safety culture aspects, is considered.

For easier and more user friendly applicability, the method that is reviewed in this publication, including the overview of all challenges, mechanisms and provisions for all levels of defence, is illustrated in the form of 'objective trees'[4].

1.3. SCOPE

The assessment method that is reviewed in this publication is directly applicable to existing light water and heavy water reactors, and to spent fuel transported or stored in the pools outside the nuclear reactor coolant system on the site of these reactors. With some minor modifications, the method can also be used for other types of reactor such as reactors cooled with gas or with liquid

---

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

[3] Mechanisms: specific reasons, processes or situations whose consequences might create challenges to the performance of safety functions.

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

metal. In the future the method can be modified also for innovative or new reactor designs.

The assessment method is applicable to all stages of the lifetime of the plant, from design to operation. Siting aspects are in part covered. However, decommissioning has not been considered in the development of this assessment method.

The assessment method described in this publication is not meant to replace the other evaluations required by national or international standards. Rather, it is intended to complement regulatory evaluations and to provide an additional tool for a better appreciation of the defence in depth capabilities of a plant.

With a view to providing a clear interpretation of the term defence in depth and a better understanding of the completeness of this concept, the present publication contains a comprehensive review of the provisions for all levels of defence. However, this publication does not provide any guidance for evaluating the safety significance of omissions or for the prioritization of the defence in depth provisions.

1.4. STRUCTURE

Section 2 addresses the strategy of defence in depth and the importance of fulfilling the safety functions[5] (SFs) to achieve the objectives for the different levels of defence. Section 3 provides a detailed description of the approach for making an inventory of the defence in depth capabilities of a plant. Section 4 discusses the applications of the approach and how to use the approach for assessing defence in depth. Section 5 presents conclusions. A discussion of the SFs is presented in Appendix I. In Appendix II, the objective trees graphically represent how, for each relevant safety principle[6], the safety objectives of the different levels of defence can be achieved by establishing defence in depth provisions at different stages of the lifetime of the plant. A test application of the approach is summarized in Appendix III. Definitions are provided at the end of the book.

[5] Safety function: a specific purpose that must be accomplished for safety in operational states, during and following a design basis accident (DBA) and, to the extent practicable, in, during and following the plant conditions considered beyond the DBA.

[6] Safety principle: a commonly shared safety concept stating how to achieve safety objectives at different levels of defence in depth.

2. THE CONCEPT OF DEFENCE IN DEPTH

2.1. GENERAL CONSIDERATIONS

Three safety objectives are defined for nuclear installations in the IAEA Safety Fundamentals publication [1]. Safety objectives require that nuclear installations are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control. The general nuclear safety objective is supported by two complementary objectives, the radiation protection objective and the technical safety objective.

By observing a comprehensive set of safety principles [2], the operators of plants will achieve the nuclear safety objectives. In this process, the measures that are taken to keep radiation exposure in all operational states to levels as low as reasonably achievable, and to minimize the likelihood of an accident that might lead to loss of normal control of the source of the radiation, are essential. For nuclear power plants, the safety objectives are ensured by fulfilling the three fundamental safety functions (FSFs)[7] described in Section 2.2.

According to INSAG-10 [3], defence in depth consists of a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive material and workers, the public or the environment, during normal operation, anticipated operational occurrences (AOOs) and, for some barriers, accidents at the plant.

In general, several successive physical barriers for the confinement of radioactive material are in place within a plant. Their specific design may vary depending on the radioactivity of the material and on the possible deviations from normal operation that could result in the failure of some barriers. The number and type of barriers that confine the fission products are dependent on the technology that has been adopted for the reactor. For the reactors under consideration these barriers include the fuel matrix, fuel cladding, pressure boundary of the reactor coolant system, and the containment or confinement.

Defence in depth is generally divided into five levels [3]. Should one level fail, the subsequent level comes into play. Table 1 summarizes the objectives of each level and the corresponding means that are essential for achieving them.

[7] The three fundamental safety functions are: (1) control of the reactivity; (2) removal of heat from the fuel; (3) confinement of radioactive material and control of operational discharges, as well as limitation of accidental releases.

TABLE 1. LEVELS OF DEFENCE IN DEPTH [4]

Levels of defence in depth	Objective	Essential means for achieving the objective
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accidents within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

The levels are intended to be independent to the extent practicable. The general objective of defence in depth is to ensure that a single failure, whether an equipment failure or a human failure, at one level of defence, and even a combination of failures at more than one level of defence, does not propagate to jeopardize defence in depth at subsequent levels. The independence of different levels of defence is crucial to meeting this objective.

Figure 1 is a flow chart showing the logic of defence in depth. Success is defined for each level of defence in depth. According to the philosophy of defence in depth, if the provisions of a given level of defence fail to control the evolution of a sequence, the subsequent level will come into play.

The objective of the first level of defence is the prevention of abnormal operation and system failures. If there is a failure at this level, an initiating event takes place. This can happen either if the defence in depth provisions at Level 1 were not effective enough or if a certain mechanism was not considered in establishing the defence in depth provisions at Level 1. Then the second level of defence will detect these failures, to avoid or to control the abnormal operation. Should the second level fail, the third level ensures that the FSFs will be performed by activation of specific safety systems and other safety

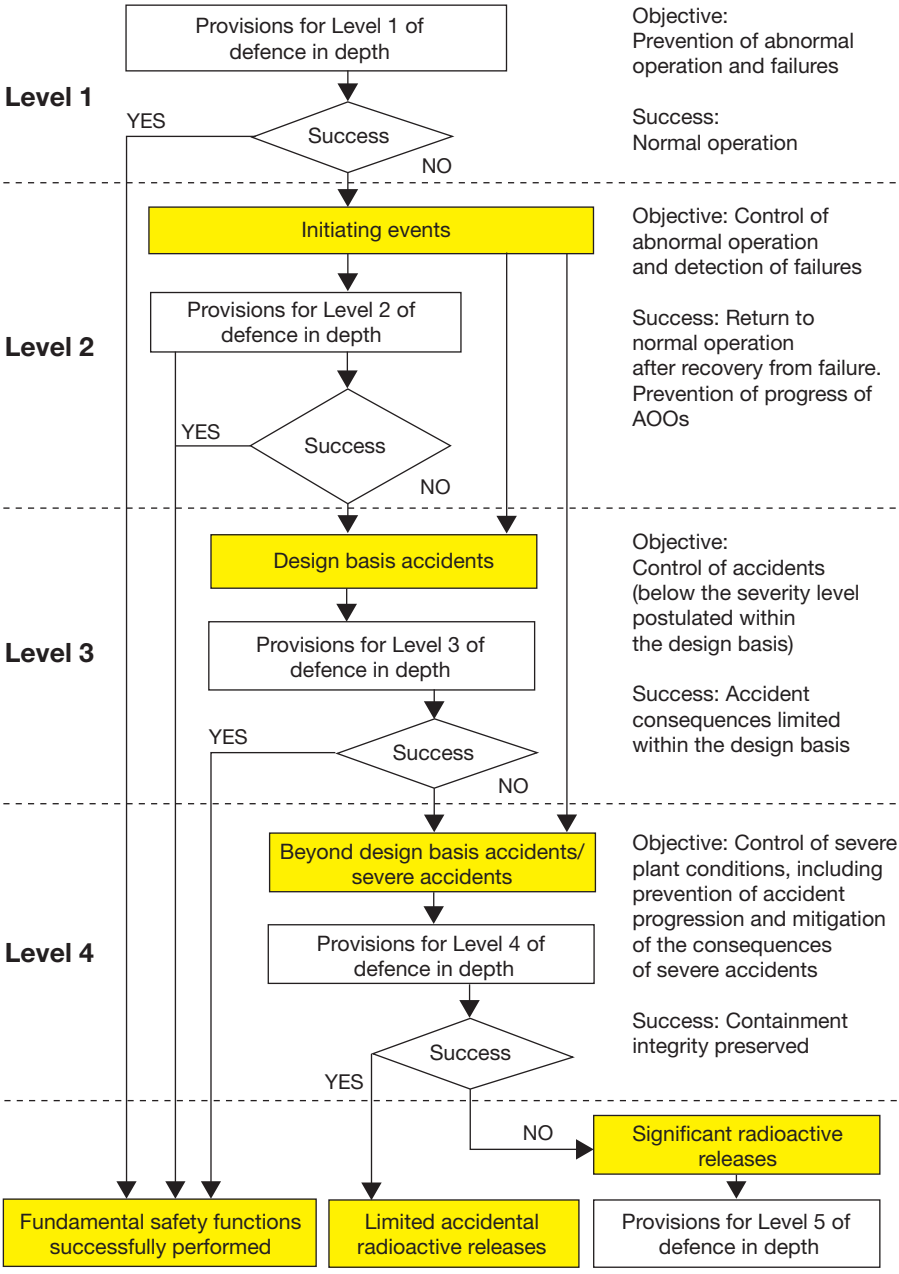


FIG. 1. Flow chart for defence in depth.

features with a view to limiting the possible consequences of design basis accidents (DBAs). Should the third level fail, the fourth level limits accident progression by means of accident management measures in order to prevent or mitigate severe accident conditions with external releases of radioactive material. The last objective (the fifth level of defence) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

A deterministic approach to defence in depth does not explicitly consider the probabilities of occurrence of the challenges or mechanisms (an explanation of these terms is given in Section 3.1) nor does it include the quantification of the probabilities of success associated with the performance of features and systems for each level of defence. However, in the future this deterministic approach can be further complemented by probabilistic safety analysis (PSA) considerations (system reliability, probabilistic targets, etc.), to provide an adequate level of safety ensuring a well balanced design.

2.2. FULFILMENT OF FUNDAMENTAL SAFETY FUNCTIONS

To ensure the safety of plants by avoiding the failure of barriers against the release of radioactive material and by mitigating the consequences of their failure, the following FSFs have to be performed in operational states, during and following DBAs and, to the extent practicable, in, during and following the considered plant conditions beyond the DBA [4]:

(1) Control of reactivity;
(2) Removal of heat from the core;
(3) Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

Henceforth in the present report, FSF (2) 'removal of heat from the core', as mentioned in Ref. [4], will be replaced by the more general FSF 'removal of heat from the fuel' to cover also the fuel removed from the core but that is still on the site of the plant and is a potential radioactive source.

The FSFs are essential for defence in depth and as a measure of the appropriate implementation of defence in depth through the various provisions for the design and operation of the plant, as indicated by the underlying relevant safety principles. The aim of the defence in depth provisions is to protect the barriers and to mitigate the consequences if the barriers against the release of radioactive material are damaged.

Possible challenges to the FSFs are dealt with by the defence in depth provisions established at a given level of defence, which include inherent safety characteristics, safety margins, active and passive systems, procedures, operator actions, organizational measures and safety culture aspects. All those mechanisms that can challenge the performance of the FSFs should be first identified for each level of defence. These mechanisms are used to determine the set of initiating events that can lead to deviation (initiation or worsening) from normal operation.

Each of the FSFs may be subdivided into several derived/subsidiary SFs, as presented in Appendix I. The list in Appendix I is based on Safety of Nuclear Power Plants: Design [4]. Some modifications to the list were necessary to allow a more general applicability of these SFs beyond the scope of Ref. [4]. Independence in the performance of the FSFs/SFs at all levels underlies the defence in depth concept. In addition, the performance of the SFs also establishes the conditions for maintaining the integrity of barriers against the release of radioactive material.

3. APPROACH FOR MAKING AN INVENTORY OF THE DEFENCE IN DEPTH CAPABILITIES OF A PLANT

3.1. DESCRIPTION OF THE APPROACH

The identification of what can have an impact on the performance of an FSF as well as of the variety of options that exist for avoiding this impact for each level of defence is an essential task in the development of the framework for making an inventory of the defence in depth capabilities of a plant. For developing the framework, it is useful to explain the following concepts:

(a) *Defence in depth* involves multiple barriers against the release of radioactive material as well as several levels of defence, which include organizational, behavioural and design measures (*provisions*).
(b) Each *level of defence* has its specific objectives, including the protection of relevant barriers and the essential means for this protection. To ensure achievement of the objective of each level of defence, all FSFs (and derived/subsidiary SFs) relevant for this level need to be performed.
(c) *Challenges* are generalized mechanisms, processes or circumstances (conditions) that may have an impact on the intended performance of SFs. The nature of challenges is characterized by the safety principle that contributes to the achievement of the objective through the performance

of SFs. Challenges are caused by a set of mechanisms having similar consequences.

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

For each of the mechanisms it is possible to find a number of provisions, such as inherent plant safety characteristics, safety margins, system design features and operational measures, which can support the performance of the SFs and prevent the mechanism from taking place.

A framework for making an inventory of the defence in depth capabilities should screen for each level of defence all the challenges and mechanisms, and identify possible safety provisions for achieving the objectives of each level of defence as indicated by the relevant safety principles.

The framework described above may be graphically depicted in terms of an 'objective tree', as shown in Fig. 2. At the top of the tree there is the level of defence in depth that is of interest, followed by the objectives to be achieved, including the barriers to be protected against release of radioactive material. Below this, there is a list of FSFs or derived SFs which need to be maintained to achieve both the objectives and the protection of the barriers of the level of defence under consideration. For instance, for Level 2 the objective is to control abnormal operation and to detect failures, as well as to ensure the

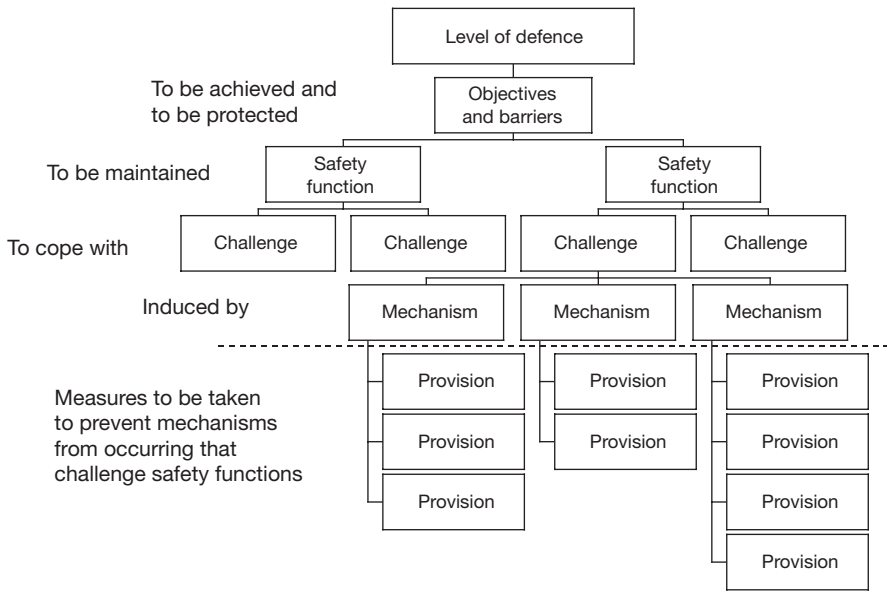


FIG. 2. Structure for defence in depth provisions at each level of defence.

continued integrity of the first three barriers (the fuel matrix, cladding and pressure boundary of the reactor coolant system) through performance of FSFs/SFs. For Level 3, the objective is to control accidents within the design basis. For these accidents it is required to limit damage of the first two barriers, to avoid consequential damage of the pressure boundary of the reactor coolant system and to avoid any damage of the reactor containment.

There might be an impact on the performance of FSFs/SFs by challenges which are placed on a lower level of the objective tree. On the next lower level of the tree there are several mechanisms listed that can give rise to the challenges. Under each of the mechanisms, there is a list of possible provisions that should be implemented in order to prevent the mechanisms from occurring and to prevent challenges to the SFs from arising.

The following example applicable to pressurized water reactors (PWRs) may further illustrate the approach described. One of the SFs relevant for Levels 1–3 of defence in depth is prevention of unacceptable reactivity transients. This SF can be challenged by insertion of positive reactivity. Several mechanisms lead to such a challenge, including control rod ejection, control rod withdrawal, control rod drop or misalignment, erroneous startup of a circulation loop, release of absorber deposits in the reactor core, incorrect refuelling operations or inadvertent boron dilution. For each of these mechanisms there are a number of provisions to prevent its occurrence. For example, control rod withdrawal can be prevented or its consequences mitigated by:

(1) Design margins minimizing the need for automatic control,
(2) An operating strategy with most of the rods out of the core,
(3) Monitoring of rod position,
(4) Limited speed of rod withdrawal,
(5) Limited worth of the control rod groups,
(6) A negative feedback reactivity coefficient,
(7) Conservative set points of the reactor protection system,
(8) A reliable and fast safety shutdown system.

The main objective of the method presented in this publication is making an inventory of the defence in depth capabilities, i.e. the provisions implemented during any stage of the lifetime of the plant. Its essential attribute therefore would be the completeness of the list of mechanisms grouped into generalized challenges endangering the fulfilment of SFs, and sufficient comprehensiveness of the list of safety provisions aimed at preventing those mechanisms from taking place. The top down approach, i.e. from the objectives of each level of defence down through challenges and mechanisms down to the

provisions, is considered an appropriate way to develop the objective trees in the most comprehensive way.

3.2. SPECIFICATION OF THE PROVISIONS

The defence in depth capabilities of a plant are established by means of the provisions that prevent mechanisms or combinations of mechanisms from occurring that might challenge the performance of the FSFs and SFs. It is important that the list of provisions is drawn up as comprehensively as possible. A combination of expert judgement, the IAEA reference report INSAG-12 [2] and two IAEA Safety Standards publications [4, 5] has been used to provide guidance on the comprehensive selection of the main challenges, mechanisms and provisions for each of the SFs to be performed. In Ref. [2] a graphical depiction of the elements of defence in depth and safety culture over the lifetime of a plant has been devised, as shown in Fig. 3, which is reproduced from Ref. [2].

Across the horizontal axis of the figure the stages of lifetime of a plant are listed, beginning with design, through construction and operation, and ending with plant decommissioning. Decommissioning is beyond the scope of the present publication. Along the vertical axis of the figure there are the levels of defence in depth. These levels begin at the top with the first level involving the prevention of abnormal events, progressing through levels devoted to the recovery from abnormal events of increasing levels of severity, and concluding with the level of defence aimed at mitigating the radiological consequences of the most severe and most unlikely accidents. Within the figure the major features (elements) are listed that contribute to defence in depth during the nuclear power plant lifetime. Each of the elements is representative of a specific safety principle discussed in detail in Ref. [2]. The lines connecting the safety principles in Fig. 3 indicate the interrelations among the principles.

The safety principles described in Ref. [2] are commonly shared safety concepts that indicate how to achieve safety objectives at different levels of defence in depth. The safety principles do not guarantee that plants will be absolutely free of risk. Nonetheless, INSAG [2] has stated that, if the principles are adequately applied, the nuclear power plants should be very safe. It is therefore considered that the safety principles provide a useful basis for the comprehensiveness of the provisions.

Figure 3 also indicates how to assign individual safety principles to different levels of defence in depth. Assignment of safety principles to a certain level of defence in depth means that non-compliance with such a safety

principle can adversely affect achievement of the objectives, in particular for a given level.

The first step for assignment is shown in Fig. 3. A preliminary assignment is done as a horizontal band selected from the safety principles in Fig. 3, located within the boundaries of the different levels of defence. Of course, the complex nature of some of the principles cannot be fully reflected by a one dimensional projection of this kind. Furthermore, the boundaries of the levels are not so clear and some overlapping between levels exists.

The second step for assignment is shown in Fig. 4, which is reproduced from Ref. [2], showing the physical barriers and levels of protection in defence in depth. The message conveyed by Fig. 4 is that any violation of general safety principles such as in design management, quality assurance or safety culture can adversely affect several levels of defence at the same time. Specific safety principles that usually address the performance of various hardware components are typically assigned to different levels of defence.

The third step for assignment of safety principles to individual levels of defence is provided by the explanatory text on the safety principles themselves in Ref. [2] and the derived requirements for design and operation in the IAEA Safety Standards [4, 5].

The results of the assignment of the safety principles are given in Table 2. The numbering of the safety principles given in Table 2, as well as their grouping into siting, design, manufacture and construction, commissioning, operation, accident management and emergency preparedness, are taken directly from Ref. [2].

It can be seen from Table 2 that many principles have a bearing on more than one level of defence. For example 'achievement of quality' (safety principle 249 (SP (249)) has an impact across Levels 1–4, since it affects the reliability of all the engineering provisions that are in place to provide the defences at those levels.

The concept of defence in depth relies on a high degree of independence between the levels of defence. In practice, however, some sort of interdependence between the levels of defence exists as a result of the pervading nature of several of the principles. Of course, formal assignment of one safety principle to several levels of defence in depth does not necessarily mean lack of independence between the different levels. This is because the same principle is typically applied to different systems, different manufacturers, different plant staffs and different plant conditions, and not necessarily the same weakness propagates through all of these groupings. However, since interdependence between different levels represents a serious weakening of the defence in depth concept, for each such indicated case a special

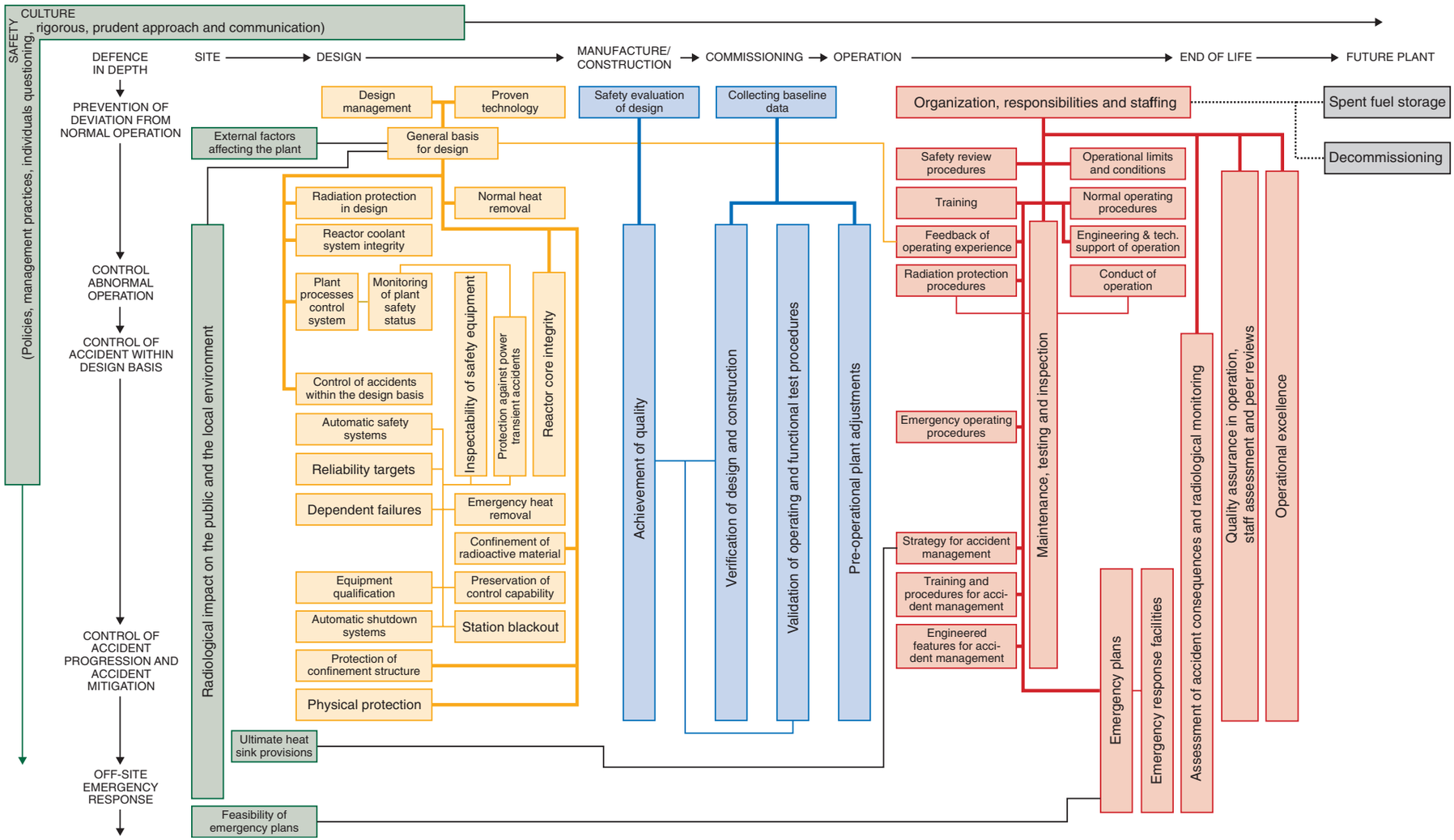


FIG. 3. Schematic presentation of the specific safety principles of INSAG, showing their coherence and their interrelations [2].

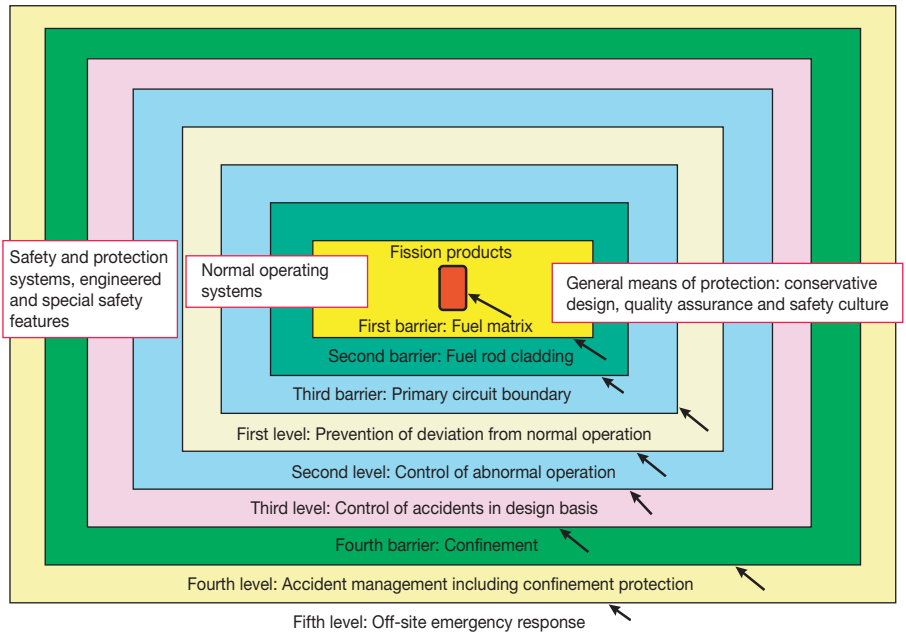


FIG. 4. Interrelationship between physical barriers and levels of protection in defence in depth [2].

consideration should be made to check all possible implications of potential deficiencies.

In some cases, the assignment of safety principles to levels of defence in Table 2 reflects differences in current national practices. For instance, in some countries, normal operating procedures (SP (288)) cover both normal and abnormal operational regimes. In other countries, abnormal operational regimes are covered by emergency operating procedures (EOPs)[8] (SP (290)); the same EOPs are also applicable for accidents within the design basis and to some extent (before significant core degradation) also for beyond design basis accidents (BDBAs).

Naturally, a certain amount of subjectivity in the assignment of safety principles cannot be avoided. However, this subjectivity is not detrimental to

[8] Emergency operating procedures: plant specific procedures containing instructions to operating staff for implementing preventive accident management measures. The EOPs typically contain all the preventive measures (for both DBAs and BDBAs).

the comprehensiveness of the objective trees, since safety principles represent only one of various sources of information for development of the approach.

3.3. OBJECTIVE TREES

The objective trees are presented in Appendix II for all the levels of defence based on the approach described. The trees themselves are self-explanatory, i.e. no additional text is provided to explain the challenges, mechanisms and provisions. Further guidance can be found in Refs [2, 4, 5].

The following remarks can be made on the formulation of provisions in the objective trees:

(a) Impacts of mechanisms should first be analysed with adequate tools, even if this is not always explicitly expressed in the provisions. The selection and implementation of an appropriate measure always needs to be based on the results of such an analysis. Lack of analysis can easily represent a source of weakening of defence in depth.

(b) The intention of objective trees is to provide a comprehensive list of the possible options for provisions. Not necessarily all of them are to be implemented in parallel. The plant operator, on the basis of the insights offered by this approach, is in a better position to decide upon the required level of implementation of the provisions, including any need for a modified or additional provision.

(c) The provisions offered in the objective trees were mainly derived from the IAEA and INSAG safety principles, the IAEA Safety Standards and on the basis of an additional engineering judgement from those experts who participated in the development of this publication. The various types of provision include: inherent plant safety features, systems, procedures, availability and training of staff, safety management and safety culture measures.

(d) For safety principles that are common to several levels of defence, several ways of presenting the objective trees are used. If a substantial difference in the formulation of provisions for different levels is identified, a separate objective tree is developed for each of the respective levels. Otherwise, the same objective tree can simply be used for each of the relevant levels. However, it should be clear for such cases that the objectives and means at different levels are different and that the same objective tree applies to different plant systems, i.e. the plant process systems, the control systems and the safety systems. To keep both the number and the structure of objective trees within reasonable limits,

TABLE 2. ASSIGNMENT OF SAFETY PRINCIPLES TO INDIVIDUAL LEVELS OF DEFENCE IN DEPTH

Phases of plant life	No. of SP	Safety principle (SP)	Level of defence				
			1	2	3	4	5
Siting	136	External factors affecting the plant	o				
	138	Radiological impact on the public and the local environment	o	o	o	o	o
	140	Feasibility of emergency plans					o
	142	Ultimate heat sink provisions	o	o	o	o	
Design	150	Design management	o	o	o	o	
	154	Proven technology	o	o	o	o	
	158	General basis for design	o	o	o	o	
	164	Plant process control systems	o	o			
	168	Automatic safety systems			o		
	174	Reliability targets			o		
	177	Dependent failures			o		
	182	Equipment qualification			o		
	186	Inspectability of safety equipment	o	o	o	o	
	188	Radiation protection in design	o				
	192	Protection against power transient accidents	o	o	o		
	195	Reactor core integrity	o	o	o		
	200	Automatic shutdown systems			o	o	
	203	Normal heat removal	o	o			
	205	Startup, shutdown and low power operation	o	o	o	o	
	207	Emergency heat removal			o	o	
	209	Reactor coolant system integrity	o	o			
	217	Confinement of radioactive material			o	o	
	221	Protection of confinement structure			o	o	
	227	Monitoring of plant safety status	o	o	o	o	
	230	Preservation of control capability	o	o	o	o	
	233	Station blackout			o	o	
	237	Control of accidents within the design basis			o		
	240	New and spent fuel storage	o	o			
	242	Physical protection of plant	o	o			

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

Phases of plant life	No. of SP	Safety principle (SP)	Level of defence				
			1	2	3	4	5
Manufacture and construction	246	Safety evaluation of design	o	o	o	o	
	249	Achievement of quality	o	o	o	o	
Commissioning	255	Verification of design and construction	o	o	o	o	
	258	Validation of operating and functional test procedures	o	o	o	o	
	260	Collection of baseline data	o	o	o	o	
	262	Pre-operational adjustment of plant	o	o	o	o	
Operation	265	Organization, responsibilities and staffing	o	o	o	o	o
	269	Safety review procedures	o	o	o	o	
	272	Conduct of operations	o				
	278	Training	o	o	o		
	284	Operational limits and conditions	o	o	o		
	288	Normal operating procedures	o				
	290	Emergency operating procedures	o	o	o	o	
	292	Radiation protection procedures	o	o	o	o	
	296	Engineering and technical support of operations	o	o	o	o	o
	299	Feedback of operating experience	o	o	o	o	
	305	Maintenance, testing and inspection	o	o	o	o	
	312	Quality assurance in operation	o	o	o	o	
Accident management	318	Strategy for accident management				o	
	323	Training and procedures for accident management				o	
	326	Engineered features for accident management				o	
Emergency preparedness	333	Emergency plans				o	o
	336	Emergency response facilities				o	o
	339	Assessment of accident consequences and radiological monitoring			o	o	o

similar provisions to avoid the occurrence of different mechanisms were sometimes condensed in the tree presentation (e.g. SP (136) in Appendix II).

In total 68 different objective trees have been developed for 53 specific safety principles assigned to the five levels of defence:

— Eleven trees exclusively for Level 1;
— Seven trees exclusively for Level 2;
— Two trees common to Levels 1 and 2;
— Three trees common to Levels 1–3;
— Eleven trees exclusively to Level 3;
— Nineteen trees common to Levels 1–4;
— One tree common to Levels 2–4;
— Five trees common to Levels 3 and 4;
— Eight trees exclusively for Level 4;
— One tree for Level 5, incorporating seven principles.

4. APPLICATIONS

Users of the method presented in this publication are expected to review and compare provisions for defence in depth identified in the objective trees with the existing defence in depth capabilities of their plant. The objective trees provide the rationale for the bottom up method, starting with the screening of individual provisions. Users should evaluate for each provision the level of its implementation. If the implementation of provisions is satisfactory, then the relevant mechanism can be considered as having been prevented from occurring. Deviations should be discussed and either justified by compensatory features specific to the plant or reconsidered for further strengthening of the defence in depth of the plant.

A large number of provisions are identified in the objective trees presented on the basis of the IAEA Safety Standards [1, 4, 5], relevant INSAG reports [2, 3] and good engineering practices. The present guidance is not intended to be a stand-alone document. Reference to the supporting publications mentioned is necessary to obtain a full explanation of the provisions. The method described is flexible enough to encourage expansion in order to include specific provisions and mechanisms identified in national

standards or relating to specific plant types. During the review, the plant operator or the regulator needs to determine whether particular standards are mandatory. In general, it is the responsibility of every plant operator to select a proper set of provisions and to consider modified or additional provisions in order to avoid mechanisms that challenge the SFs.

The method described in the present report indicates, from a qualitative point of view, what kind of provisions can be implemented to avoid the occurrence of mechanisms. However, the method described neither gives preference to individual provisions nor specifies the way to implement or quantify the efficiency of a provision. Indeed, the adequacy of provisions has to be determined by the user. In particular, for the omission of a provision, a detailed justification is necessary.

The objective of the proposed screening approach is deterministic in nature and the approach can also be used for safety assessment of a plant without a PSA or with an incomplete PSA. A plant specific PSA, sufficiently broad in scope and with a sufficient level of detail, can be used to support the judgement on the adequacy of the defence in depth and of the logical structure of the defences. In addition, a good quality PSA facilitates a deep understanding of the interrelation between the various defences and supports prioritization of provisions according to their contribution to risk reduction.

The guidance given in this report helps in identifying dependences of principles that might affect defences at more than one level and principles that are linked to other principles. These dependences indicate for the reviewer where further attention is needed for the screening of the affected levels of defence.

It is to be noted that decisions on whether or not to implement the missing or incomplete provisions need to be made after full consideration of the safety implications and priorities. It is definitely the responsibility of the plant staff to set up a programme for implementation of corrective measures or of the nuclear regulator to require corrective measures. Introduction of new equipment and programmes to implement an additional provision for defence in depth can also introduce (apart from additional costs) additional complexity to the operation of a plant and additional potential failure modes. There is no consideration in this approach of the side effects of increased complexity and operational difficulties caused by the implementation of additional defence in depth measures. The approach is not developed to identify new weaknesses in defence in depth introduced by implementing new modifications or provisions. A PSA study is an appropriate tool for such an evaluation.

By way of example, some results of the first test application of the method are provided in Appendix III. The screening of the defence in depth capabilities for WWER 440/V213 units at the Bohunice nuclear power plant was

performed for selected safety principles, which contributed to the achievement of safety objectives for Levels 3 and 4 of defence. The objective of this test application was to demonstrate that the approach is helpful and easily applicable to existing plants in order to screen systematically their defence in depth capabilities, and to identify strengths and weaknesses. The test application was carried out in a self-assessment mode by the plant operators. The results have been considered as a starting point for an in depth evaluation to qualify appropriate measures within the current plant upgrading programme.

5. CONCLUSIONS

Defence in depth is expected to remain an essential strategy to ensure nuclear safety for both existing and new plants. The method presented offers a further perspective that serves plant safety by screening the defence in depth capabilities of plants in a systematic manner. It has been developed in reliance upon basic safety principles [1, 2] and internationally agreed IAEA safety requirements [4, 5], which lay down the most important measures (provisions) to be implemented for assuring a sound and balanced defence in depth.

The approach does not include any quantification of the extent of defence in depth at a plant nor a prioritization of the provisions of defence. It is intended only for screening, i.e. for determination of both the strengths and weaknesses for which provision should be considered.

The screening approach, which uses objective trees, offers a user friendly tool for determining the strengths and weaknesses of defence in depth at a specific plant. The top down approach has been used for the development of objective trees, i.e. from the objectives of each level of defence down to the challenges and mechanisms, and finally to the provisions. A demonstration of defence in depth in a comprehensive and systematic way may provide reassurance for the plant operators that their safety strategy is sound and well balanced among the levels of defence. From a regulatory point of view, identification of deficiencies of defence in depth might be a valuable complement to traditional regulatory approaches.

There are no strict criteria on what is considered a sufficient level of implementation of individual provisions. The level of detail and completeness of evaluation is at the discretion of the user of the screening approach.

While the approach is primarily intended to facilitate self-assessment of defence in depth by plant operators, it can also be used by regulators or by

independent reviewers. A commitment by the operator to self-assessment is an essential feature of a good safety culture. The approach has been developed to be as complete as possible, but it is sufficiently flexible to allow inclusion of other mechanisms and provisions that are related to specific plant types or that are identified in national standards. In this respect, the approach might be very beneficial for checking the completeness and balance of any measures implemented for major safety improvement or modernization activities or for plant reorganizations.

This approach is also considered as an appropriate tool for presenting progress in strengthening defence in depth. Repeated screenings after a certain period of time are needed for this purpose. In particular, plant operators are encouraged to repeat in full the approach after completion of a major safety improvement programme or a substantial reorganization in the plant.

Feedback is welcome from users to the developers of the method for improving it. In this connection, the appropriateness of the mechanisms and challenges set in the objective trees needs to be verified. Comments on the text in the boxes of the objective trees are also welcome in order to address more precisely the relevant safety aspects. Special attention needs to be given to the objective trees of those safety principles that are applicable to more than one level of defence and to the need to make further appropriate distinctions between provisions belonging to different levels of defence.

BLANK

Appendix I

FUNDAMENTAL SAFETY FUNCTIONS AND SAFETY FUNCTIONS

Safety functions are subdivisions of the FSFs including those necessary to prevent accident conditions or escalation of accident conditions and those necessary to mitigate the consequences of accident conditions. They can be accomplished, as appropriate, using systems, components or structures provided for normal operation, those provided to prevent AOOs from leading to accident conditions or those provided to mitigate the consequences of accident conditions, and also with prepared staff actions.

The following set of SFs have been taken directly from Ref. [4] as appropriate to develop the objective trees in Appendix II:

(1) To prevent unacceptable reactivity transients;
(2) To maintain the reactor in a safe shutdown condition after all shutdown actions;
(3) To shut down the reactor as necessary to prevent AOOs from leading to DBAs and to shut down the reactor to mitigate the consequences of DBAs;
(4) To maintain sufficient reactor coolant inventory for core cooling in and after accident conditions not involving the failure of the reactor coolant pressure boundary;
(5) To maintain sufficient reactor coolant inventory for core cooling in and after all postulated initiating events considered in the design basis;
(6) To remove heat from the core[9] after a failure of the reactor coolant pressure boundary in order to limit fuel damage;
(7) To remove residual heat in appropriate operational states and in accident conditions with the reactor coolant pressure boundary intact;
(8) To transfer heat from other safety systems to the ultimate heat sink;
(9) To ensure necessary services (such as electrical, pneumatic, and hydraulic power supplies and lubrication) as a support function for a safety system[10];
(10) To maintain acceptable integrity of the cladding of the fuel in the reactor core;

[9] This SF applies to the first step of the heat removal system(s). The remaining step(s) are encompassed in SF (8).

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

(11) To maintain the integrity of the reactor coolant pressure boundary;
(12) To limit the release of radioactive material from the reactor containment in accident conditions and conditions following an accident;
(13) To limit the radiation exposure of the public and site personnel in and following DBAs and selected severe accidents that release radioactive materials from sources outside the reactor containment;
(14) To limit the discharge or release of radioactive waste and airborne radioactive materials to below prescribed limits in all operational states;
(15) To maintain control of environmental conditions within the plant for the operation of safety systems and for habitability for personnel necessary to allow performance of operations important to safety;
(16) To maintain control of radioactive releases from irradiated fuel transported or stored outside the reactor coolant system, but within the site, in all operational states;
(17) To remove decay heat from irradiated fuel stored outside the reactor coolant system but within the site;
(18) To maintain sufficient subcriticality of fuel stored outside the reactor coolant system but within the site;
(19) To prevent the failure or limit the consequences of failure of a structure, system or component whose failure would cause the impairment of an SF.

In order to distinguish better provisions aimed at limiting releases of radioactive material from the reactor containment (SF (12)) and provisions aimed at preventing loss of containment integrity, the following SF was added to the original set of SFs as given in Ref. [4]:

(20) To maintain the integrity of the reactor containment in accident conditions and conditions following an accident.

The SFs are intended as a basis for determining whether a structure, system or component performs or contributes to one or more SFs. They are also intended to provide a basis for assigning an appropriate gradation of importance to safety structures, systems and components that contribute to the various SFs. This means that the SFs are mostly related to the structures, systems or components. In the present report, the SFs are used in a more general sense, not necessarily related only to plant equipment but also to human factors such as personnel actions. In particular, there is no plant equipment directly considered at Level 5 of the defence in depth. Therefore, one more special SF has been added to the list in the framework of this report:

(21) To limit the effects of releases of radioactive materials on the public and environment.

The set of SFs can be grouped with respect to the FSFs as follows:

(a) SFs related to FSF (1) "control of the reactivity": SFs (1)–(3) and (18);
(b) SFs related to FSF (2) "removal of heat from the fuel": SFs (4)–(8) and (17);
(c) SFs related to FSF (3) "confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases": SFs (10)–(14), (16), (20) and (21).

There are also three special SFs related to all FSFs: SFs (9), (15) and (19).

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

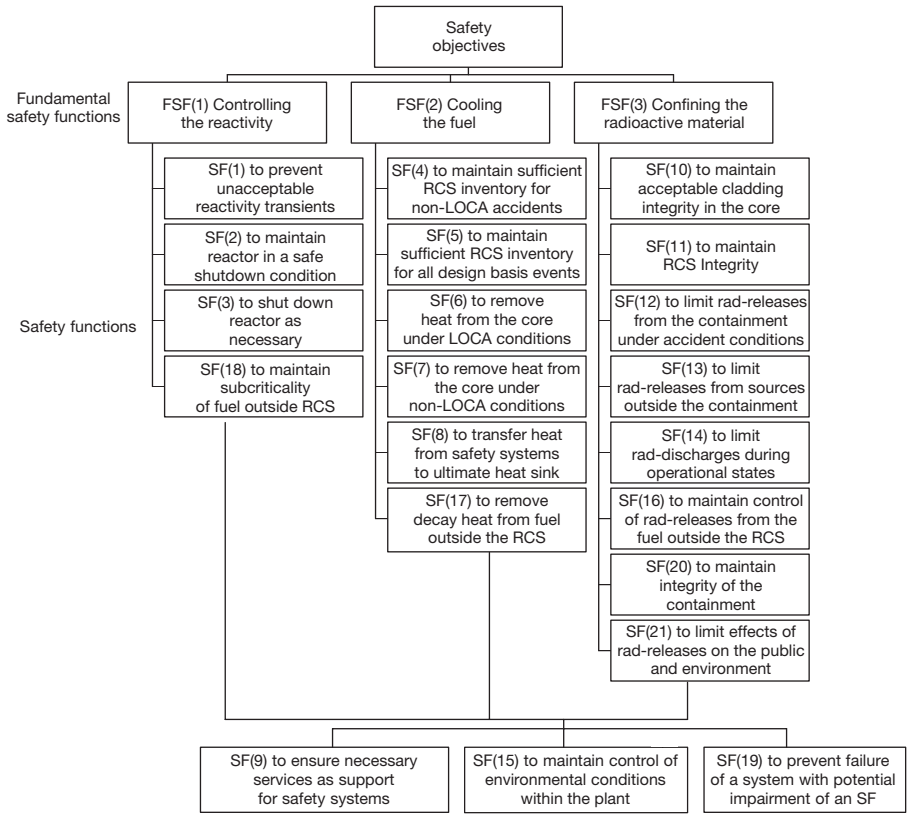


FIG. 5. Overview and grouping of SFs used in the present report (RCS, reactor coolant system; LOCA, loss of coolant accident).

Appendix II

OBJECTIVE TREES FOR ALL LEVELS OF DEFENCE IN DEPTH

The first five figures (Figs 6–10) in this Appendix are provided to remind the reader of the objectives to be achieved, including the barriers to be protected, through the performance of FSFs/SFs for each level of defence.

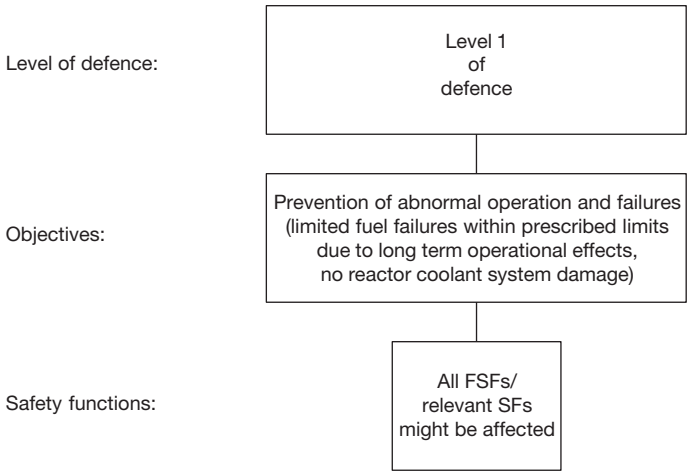


FIG. 6. Objectives to be achieved and barriers to be protected for Level 1 of defence in depth.

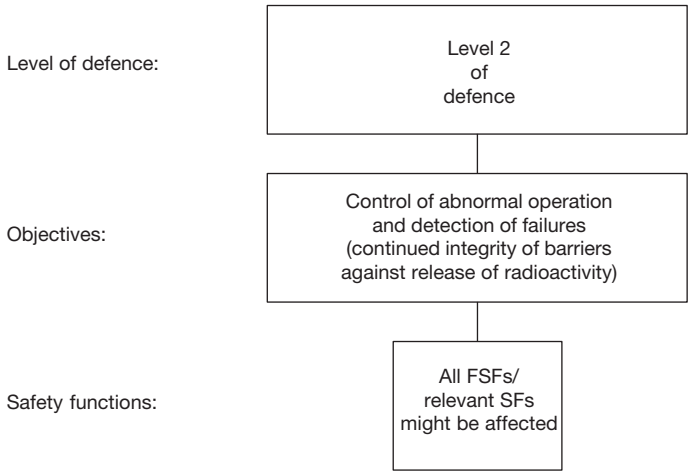


FIG. 7. Objectives to be achieved and barriers to be protected for Level 2 of defence in depth.

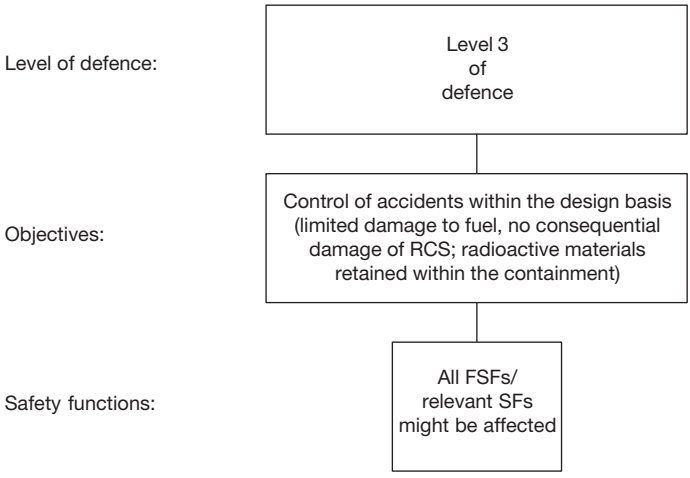


FIG. 8. Objectives to be achieved and barriers to be protected for Level 3 of defence in depth (RCS, reactor coolant system).

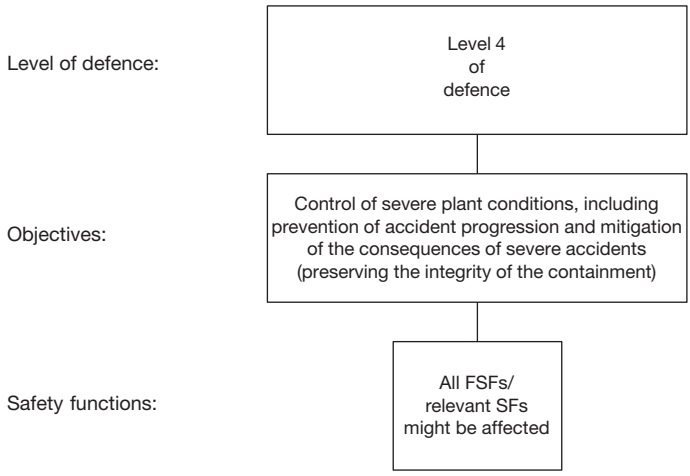


FIG. 9. Objectives to be achieved and barriers to be protected for Level 4 of defence in depth.

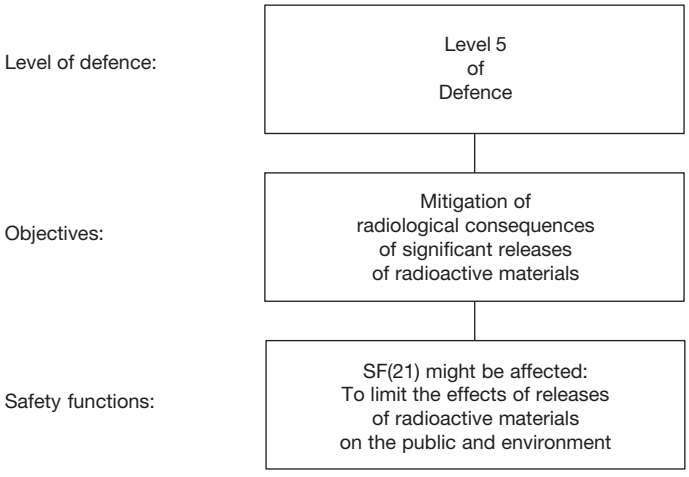


FIG. 10. Objectives to be achieved and barriers to be protected for Level 5 of defence in depth.

This Appendix goes on to provide a full set of objective trees (shown in Figs 11–78) for the purpose of practical screening of the defence in depth capabilities of plants. In each of the captions to the objective trees the levels of defence are indicated to which the provisions contribute to fulfilling the objectives. Next in the caption the corresponding safety principle(s) is given as a commonly shared safety concept(s), stating how the safety objectives at relevant levels of defence can be achieved. Each objective tree itself starts with an indication of the FSFs/SFs to be performed in order to achieve the objectives for the given safety principle(s); it is then followed by the challenges which might have an impact on the performance of SFs and the mechanisms leading to individual challenges, and finally a list of the provisions to be implemented to avoid occurrence of the mechanisms. In some objective trees, second order (more detailed) provisions are indicated by text without boxes (e.g. Fig. 15).

To keep the size of some of the objective trees within reasonable limits, their presentations for different SFs at the same level of defence are given on more than one page, e.g. SP (200) for Levels of defence 3 and 4, which are presented separately for SF (2) and SF (3) in Figs 33 and 34, respectively.

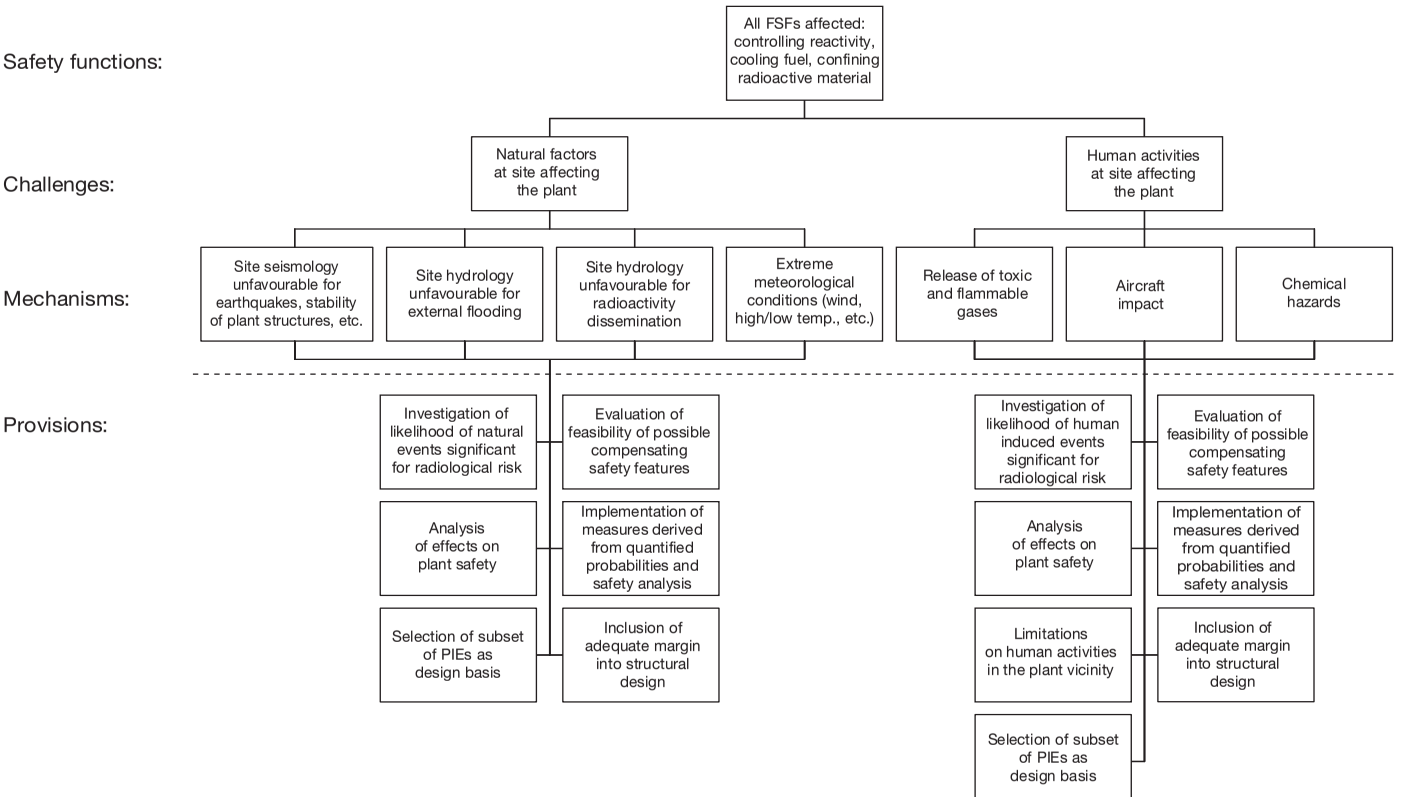


FIG. 11. Objective tree for Level 1 of defence in depth (PIE, postulated initiating event). Safety principle (136): external factors affecting the plant.

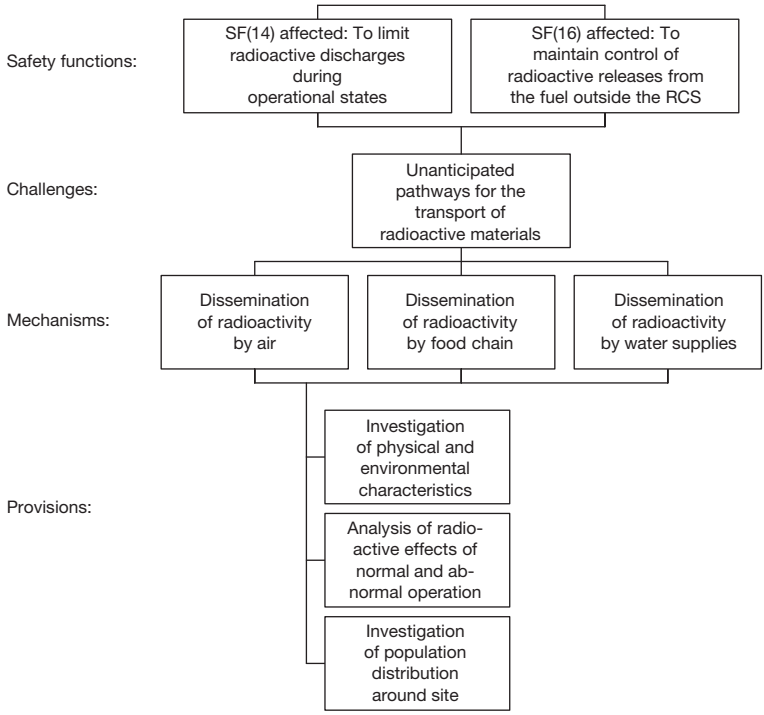


FIG. 12. Objective tree for Level 1 of defence in depth. Safety principle (138): radiological impact on the public and the local environment.

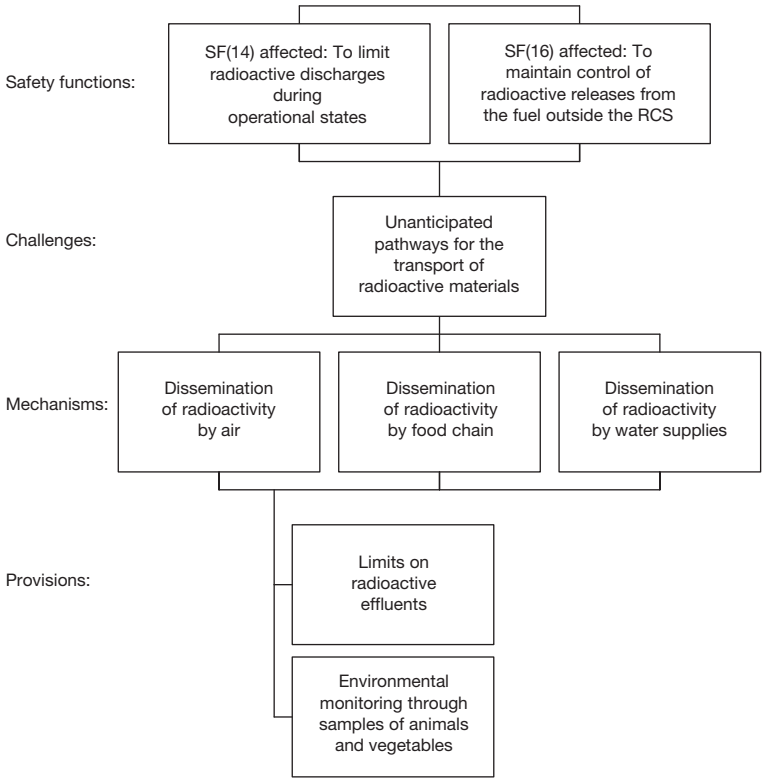


FIG. 13. Objective tree for Level 2 of defence in depth (RCS, reactor coolant system). Safety principle (138): radiological impact on the public and the local environment.

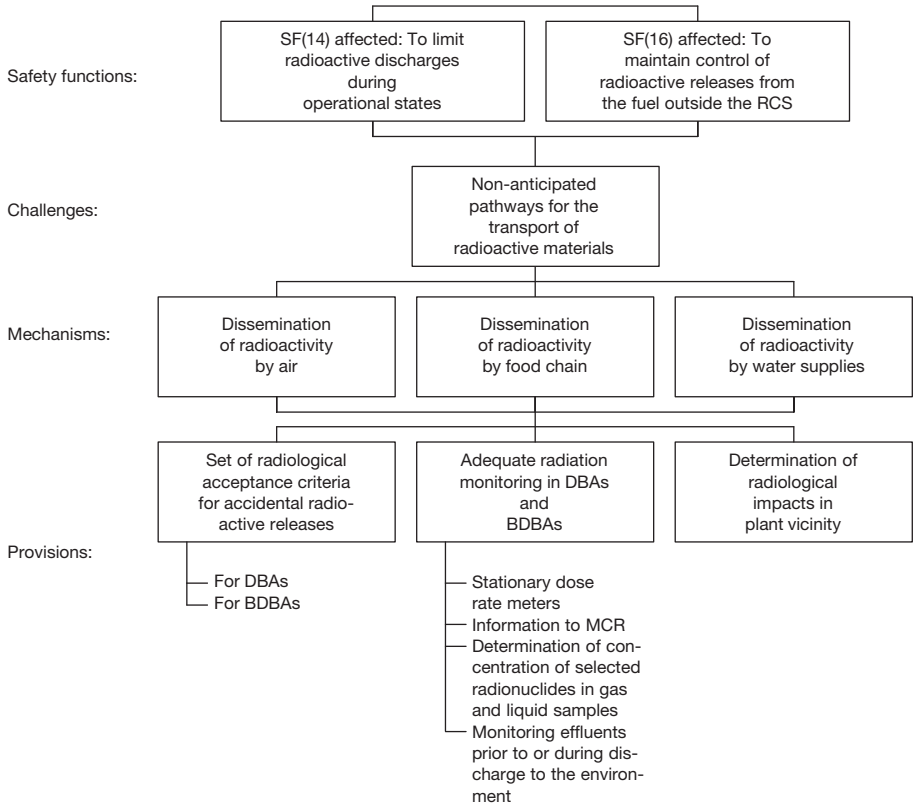


FIG. 14. Objective tree for Levels 3 and 4 of defence in depth (MCR, main control room). Safety principle (138): radiological impact on the public and the local environment.

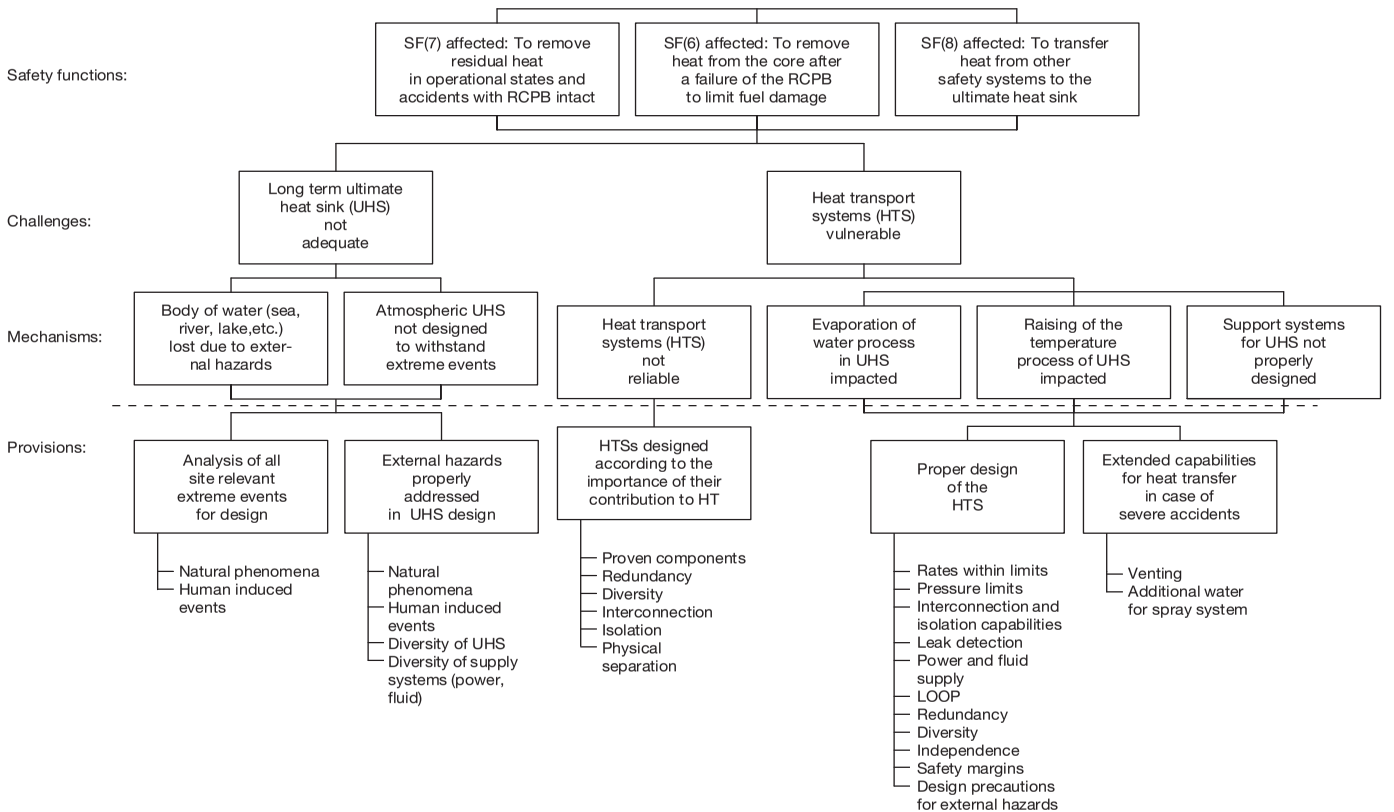


FIG. 15. Objective tree for Levels 1–4 of defence in depth (RCS, reactor coolant system; LOOP, loss of off-site power; UHS, ultimate heat sink). Safety principle (142): ultimate heat sink provisions.

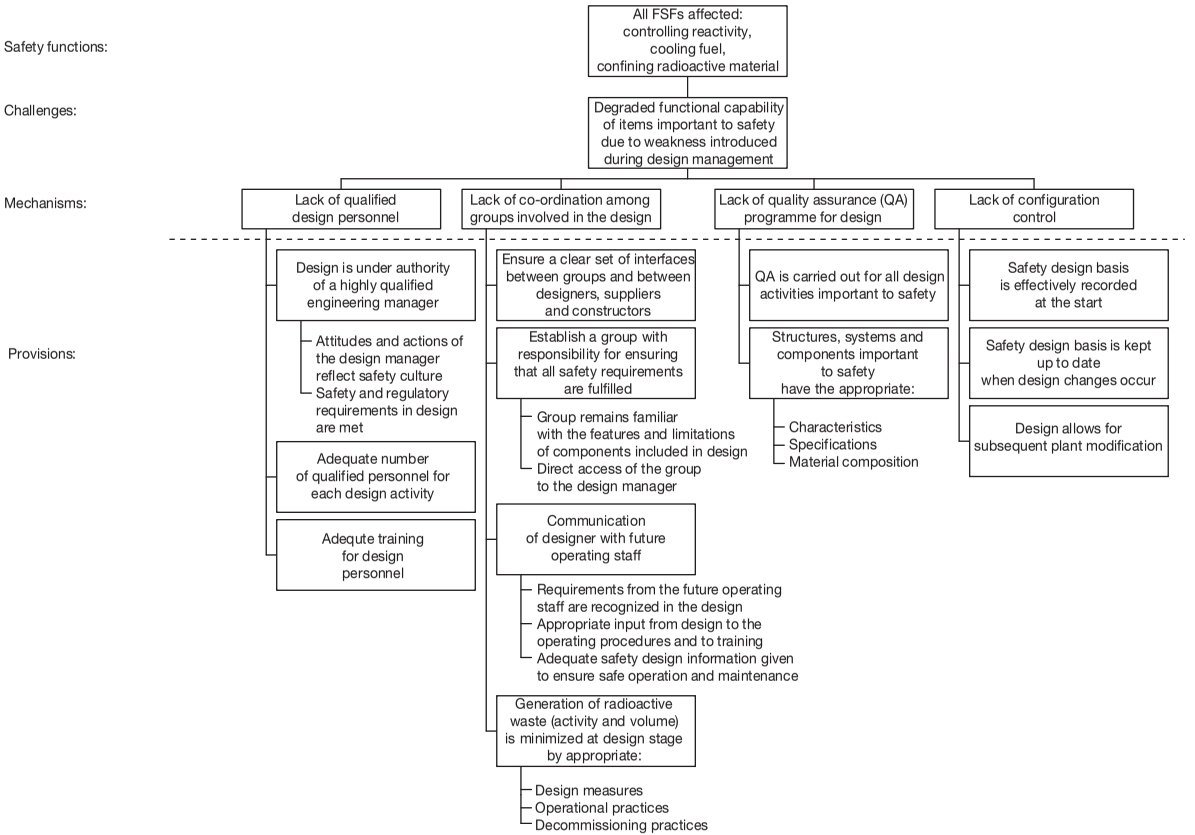


FIG. 16. Objective tree for Levels 1–4 of defence in depth. Safety principle (150): design management.

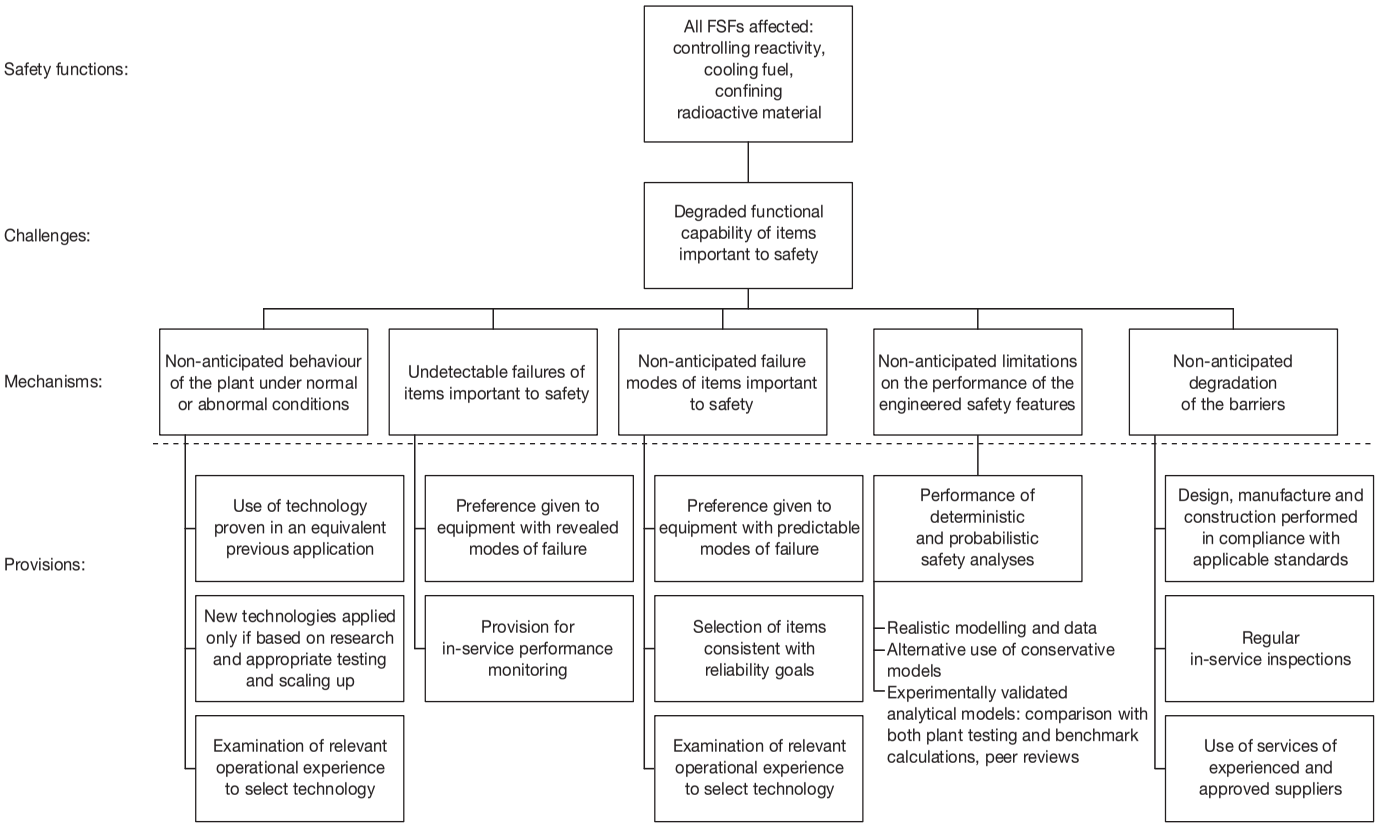


FIG. 17. Objective tree for Levels 1–4 of defence in depth. Safety principle (154): proven technology.

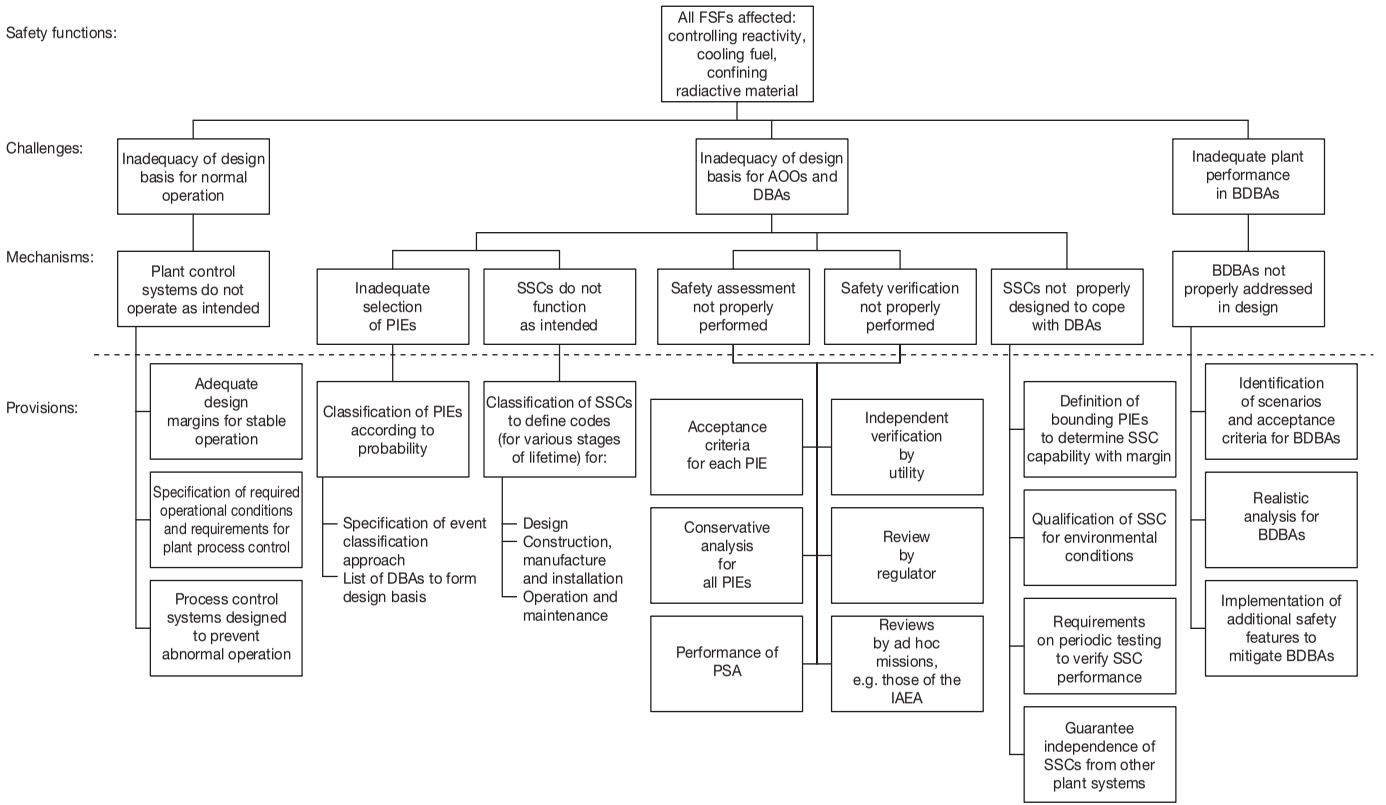


FIG. 18. Objective tree for Levels 1–4 of defence in depth (SSCs, structures, systems and components; PIE, postulated initiating event). Safety principle (158): general basis for design.

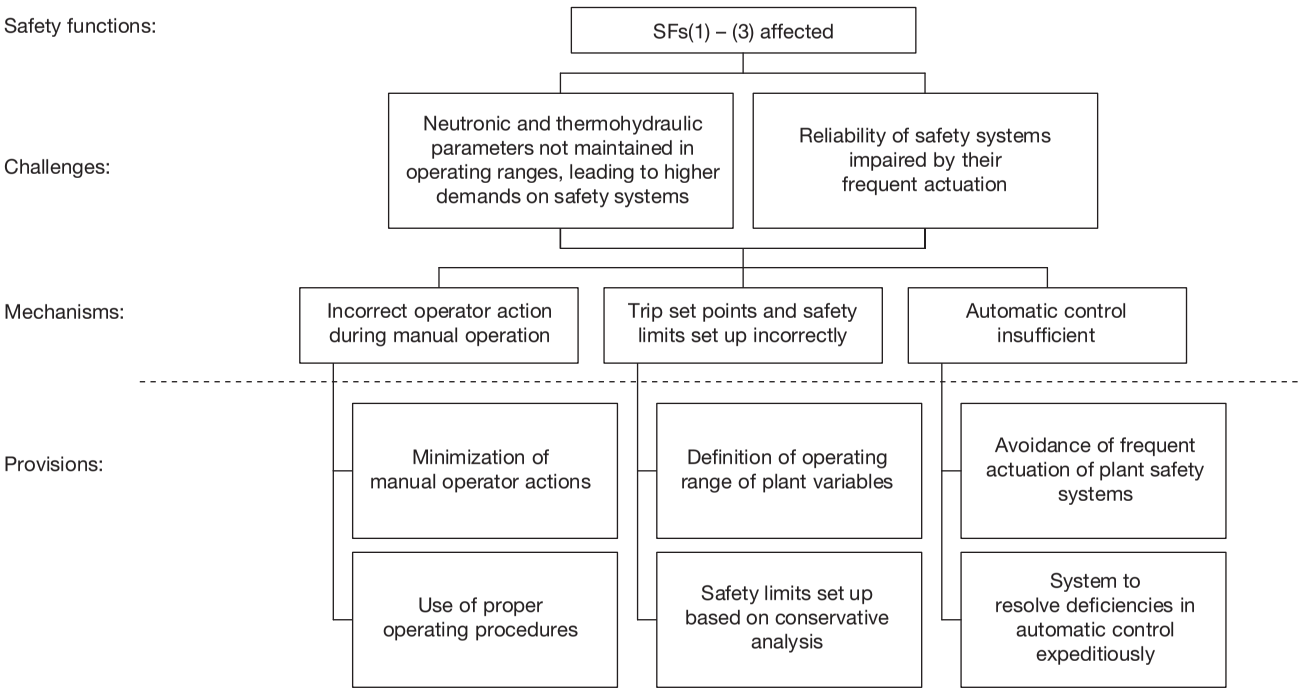


FIG. 19. Objective tree for Level 1 of defence in depth. Safety principle (164): plant process control systems.

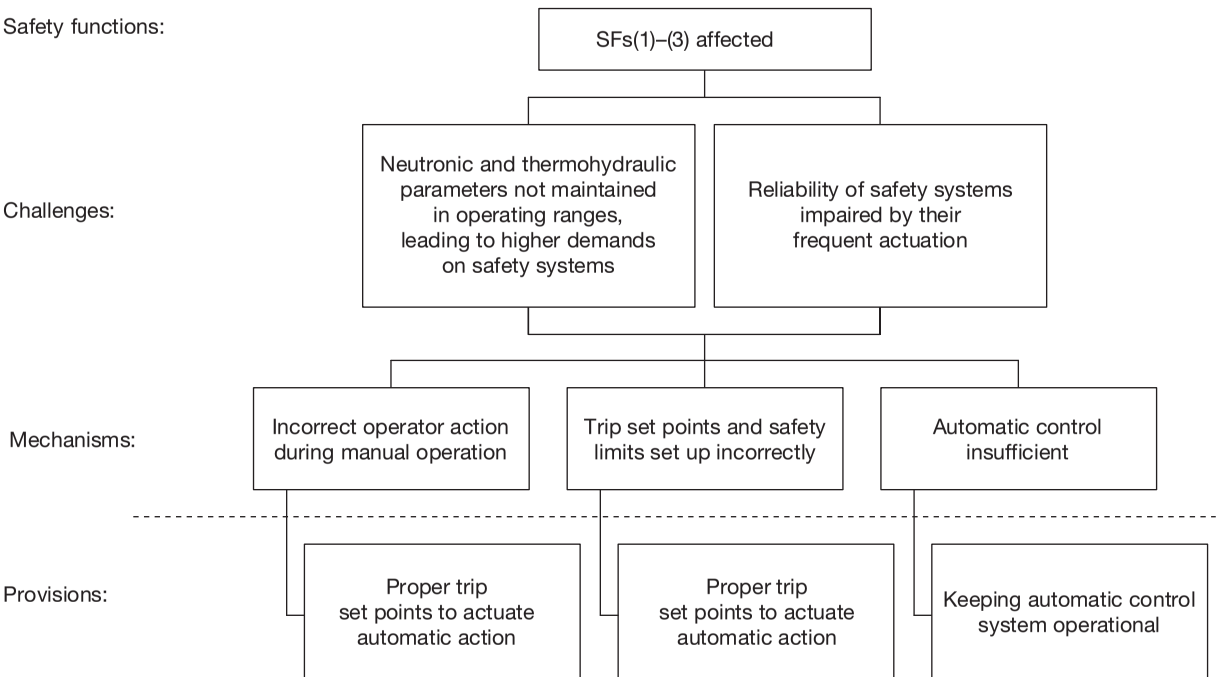


FIG. 20. Objective tree for Level 2 of defence in depth. Safety principle (164): plant process control systems.

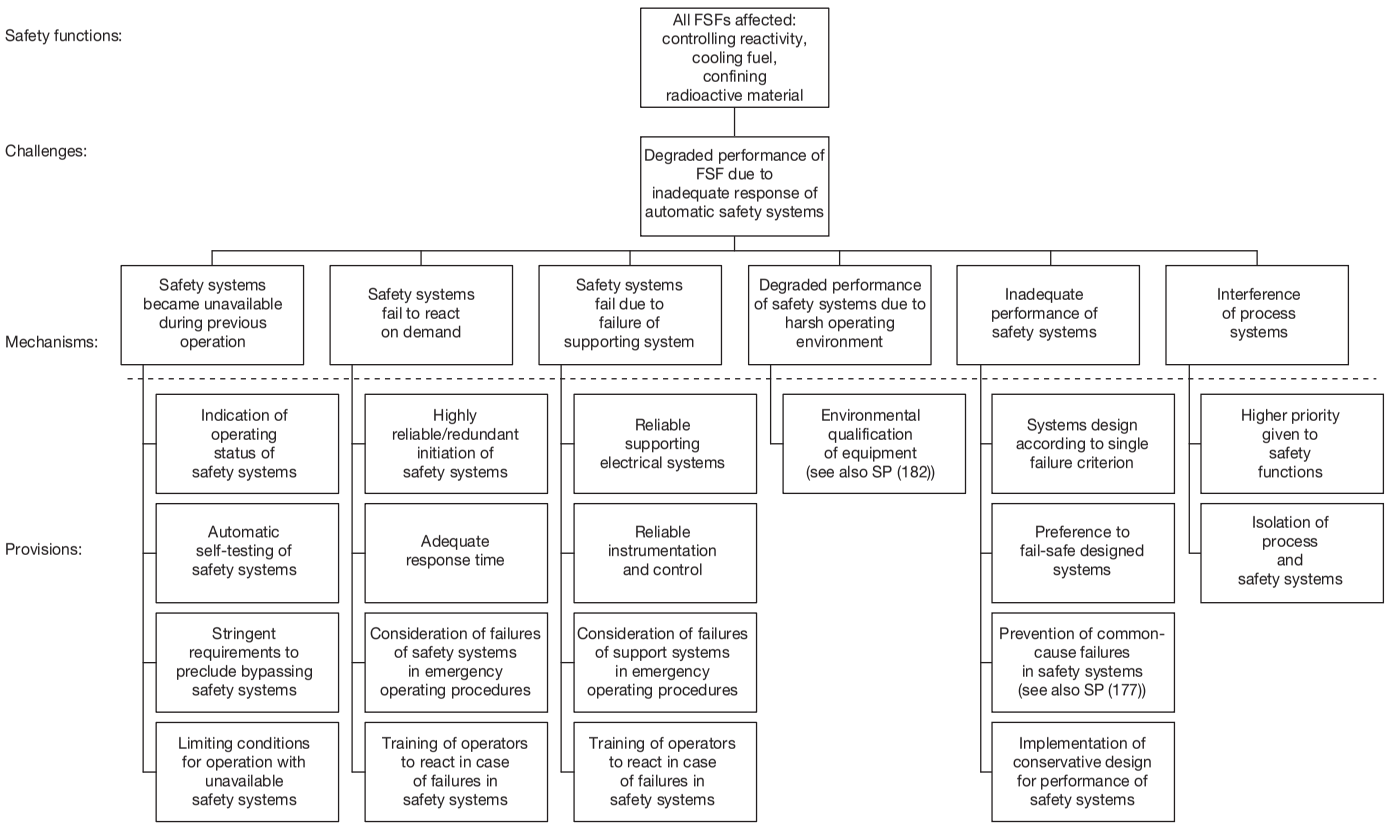


FIG. 21. Objective tree for Level 3 of defence in depth. Safety principle (168): automatic safety systems.

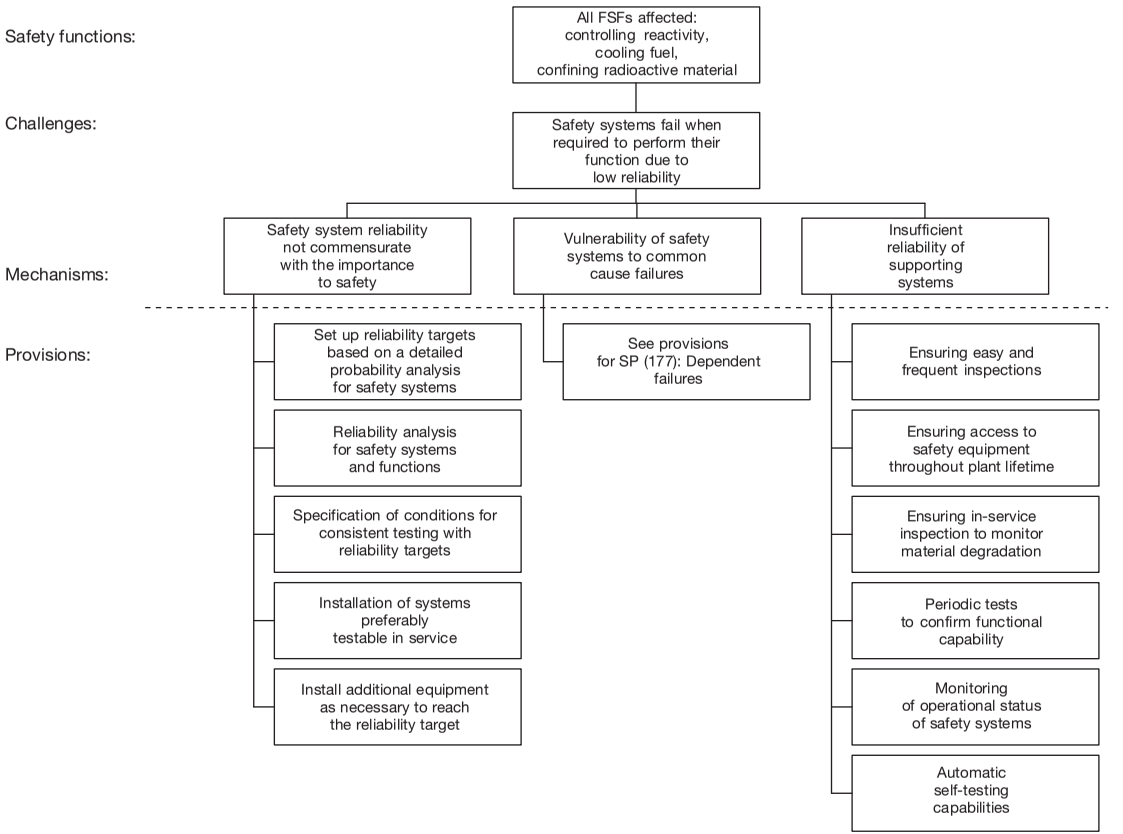


FIG. 22. Objective tree for Level 3 of defence in depth. Safety principle (174): reliability targets.

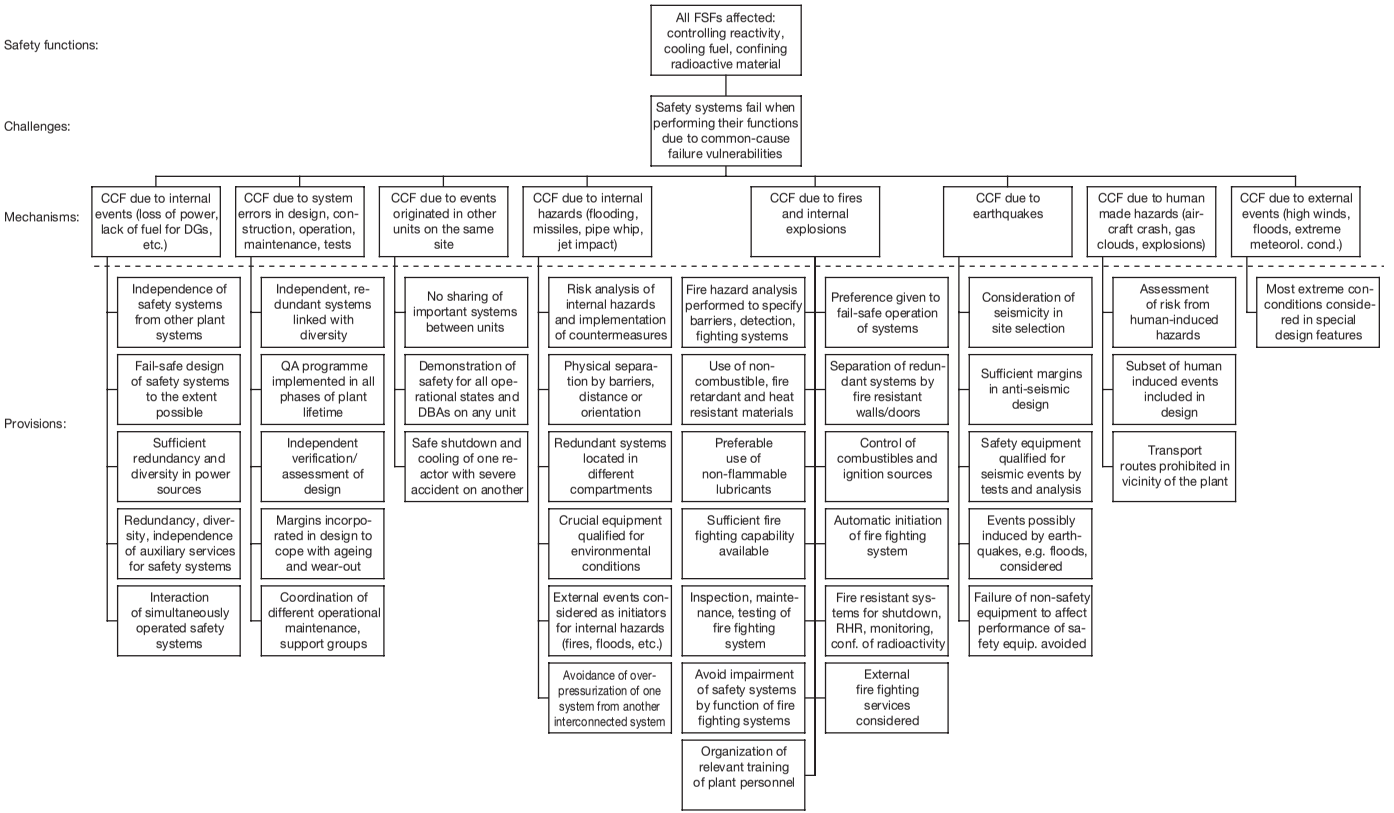


FIG. 23. Objective tree for Level 3 of defence in depth (CCF, common cause failure; DG, diesel generator; RHR, residual heat removal). Safety principle (177): dependent failures.

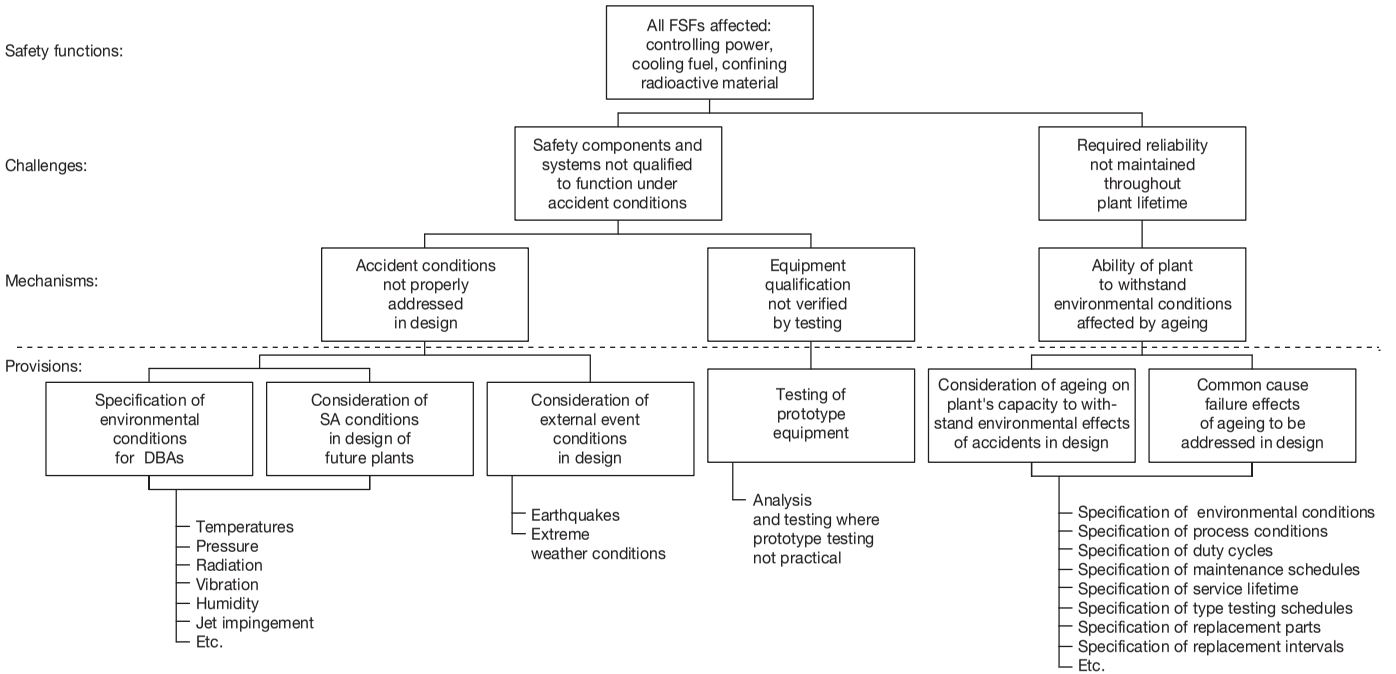


FIG. 24. Objective tree for Level 3 of defence in depth (SA, severe accident). Safety principle (182): equipment qualification.

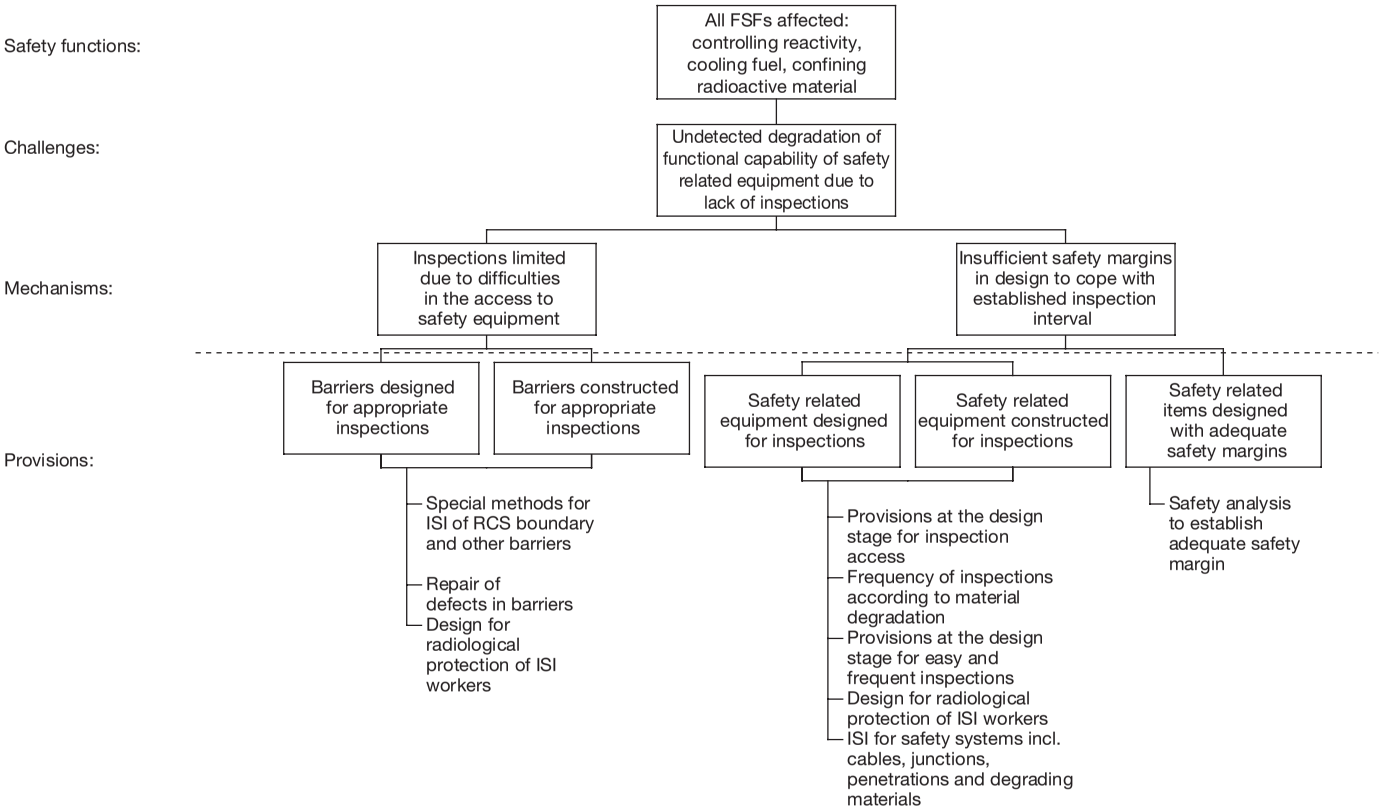


FIG. 25. Objective tree for Levels 1–4 of defence in depth (ISI, in-service inspection; RCS, reactor coolant system). Safety principle (186): ease of access of safety equipment for inspection.

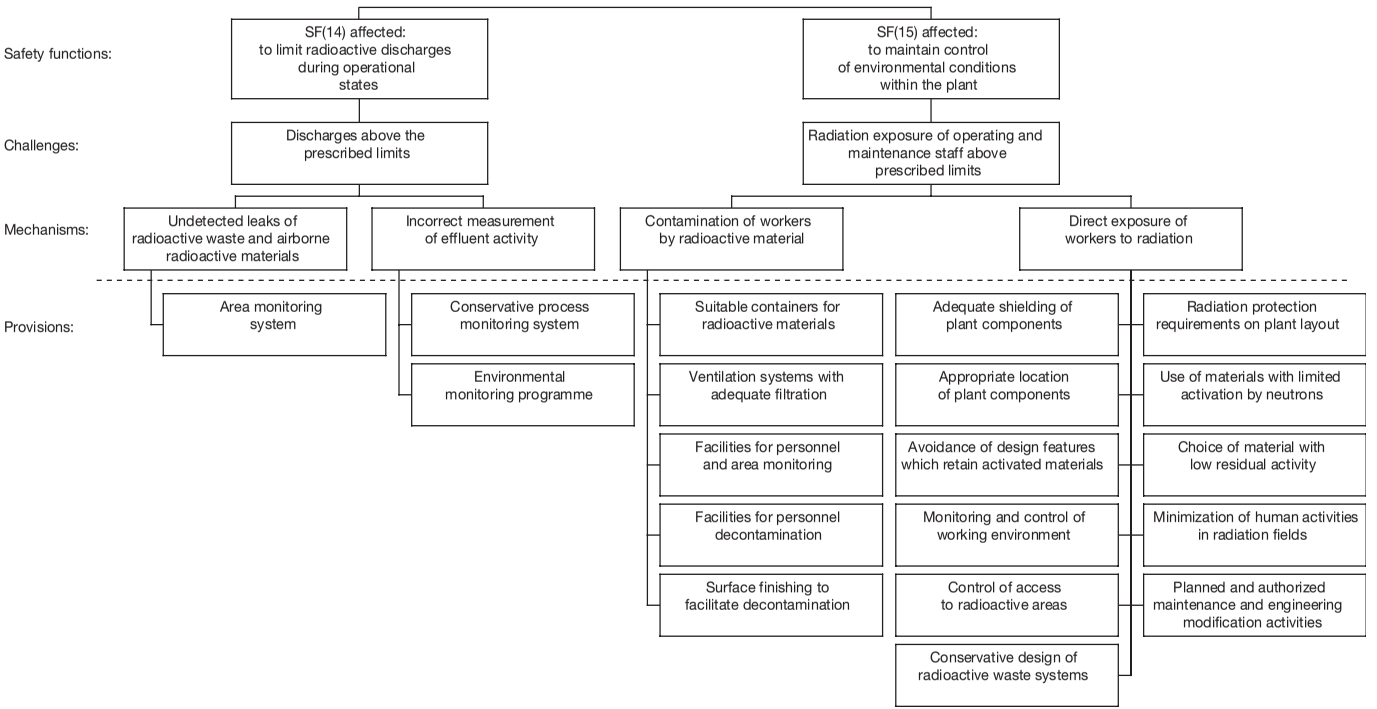


FIG. 26. Objective tree for Level 1 of defence in depth. Safety principle (188): radiation protection in design (see also SP (292)).

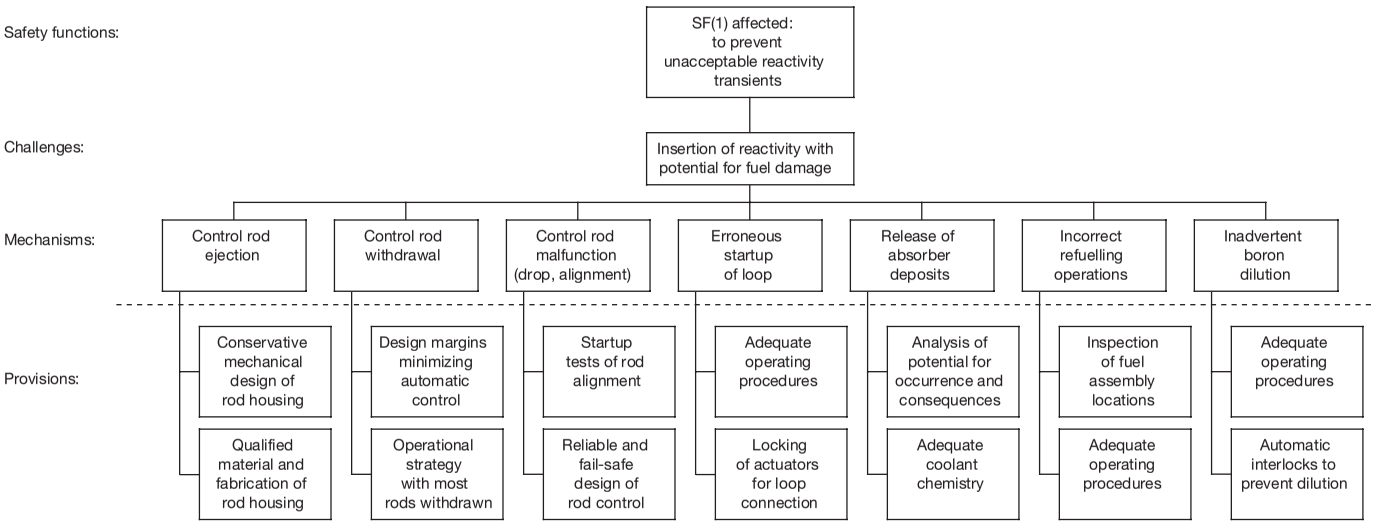


FIG. 27. Objective tree for Level 1 of defence in depth. Safety principle (192): protection against power transient accidents.

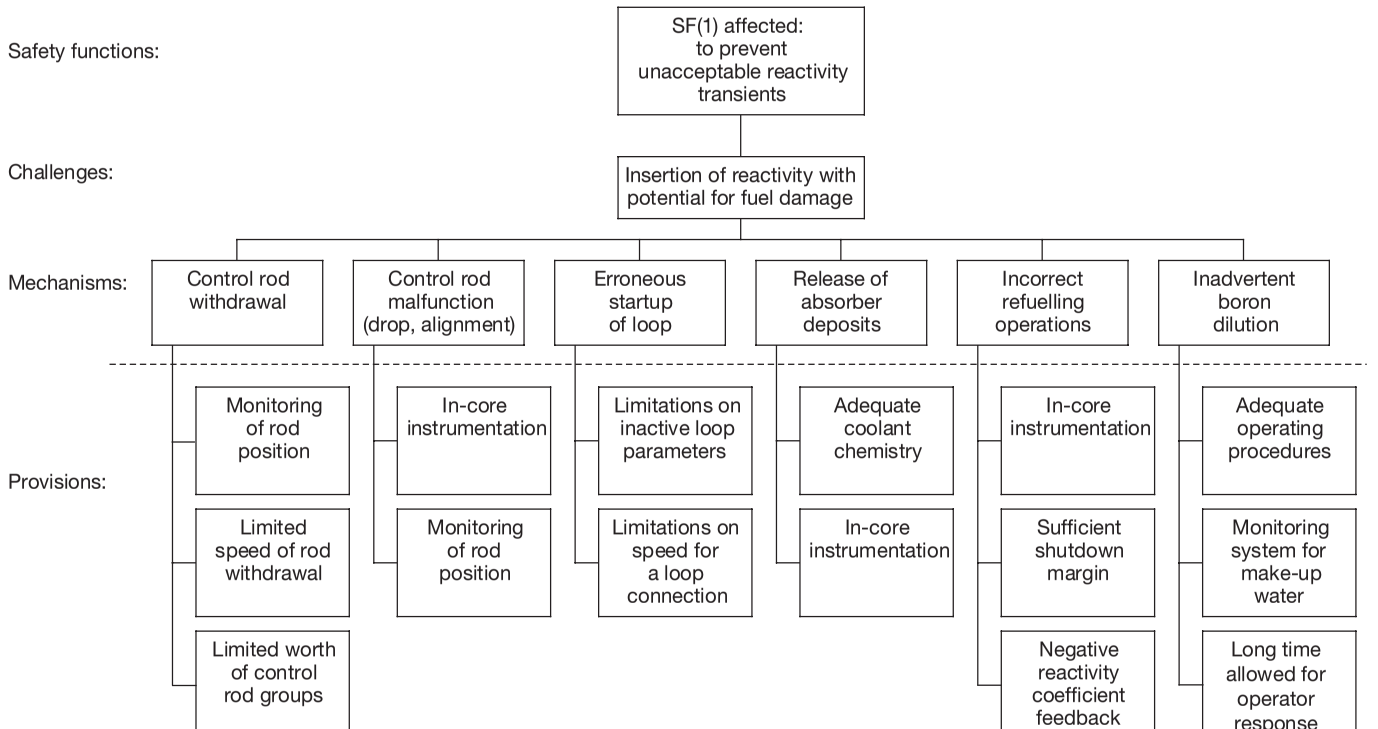


FIG. 28. Objective tree for Level 2 of defence in depth. Safety principle (192): protection against power transient accidents.

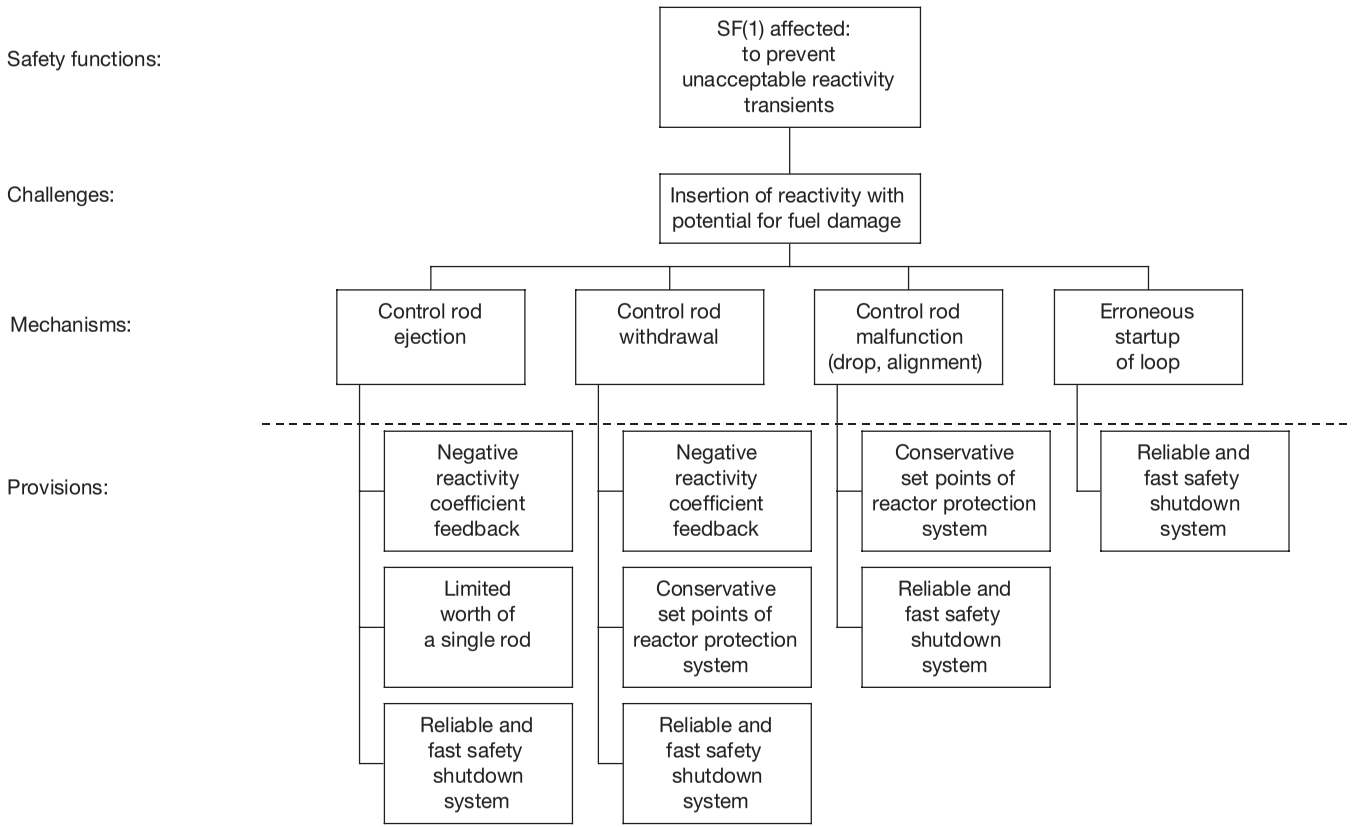


FIG. 29. Objective tree for Level 3 of defence in depth. Safety principle (192): protection against power transient accidents.

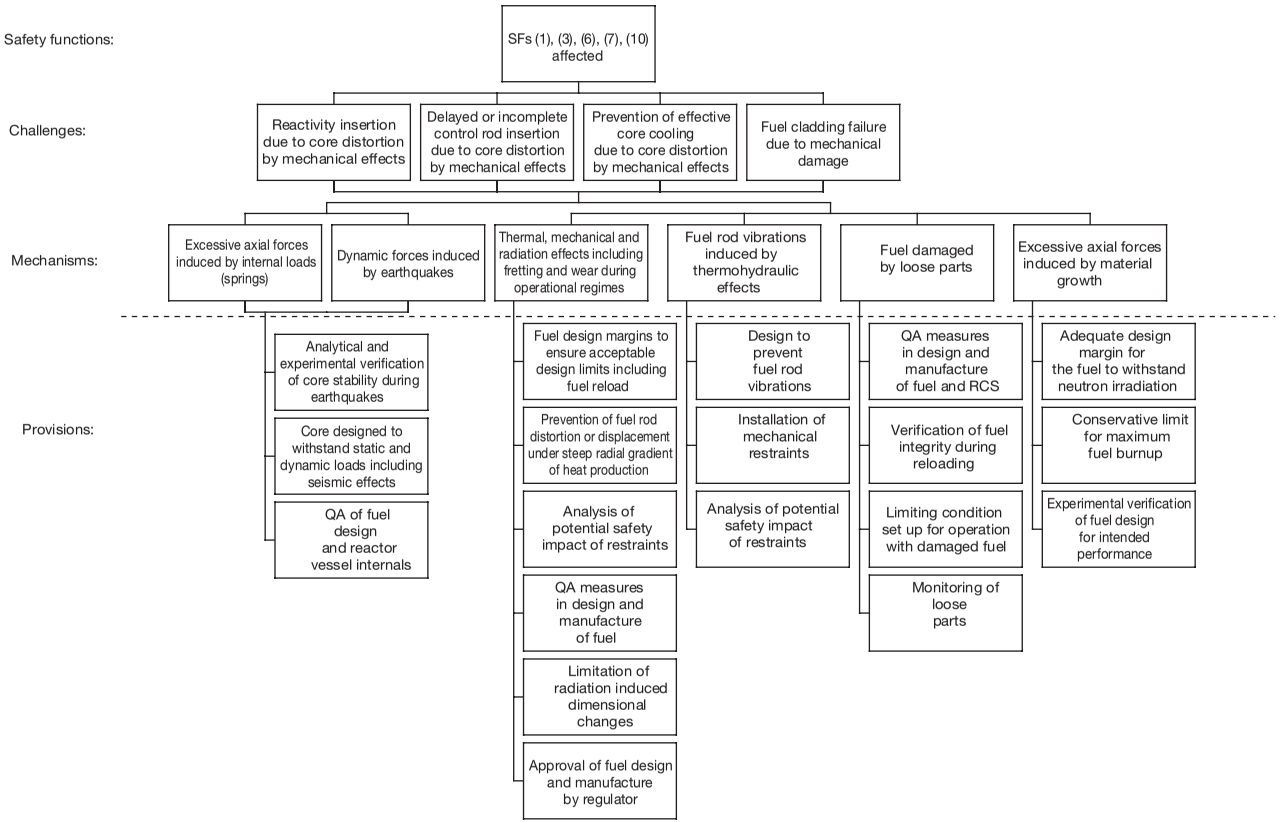


FIG. 30. Objective tree for Level 1 of defence in depth (QA, quality assurance; RCS, reactor core coolant). Safety principle (195): reactor core integrity.

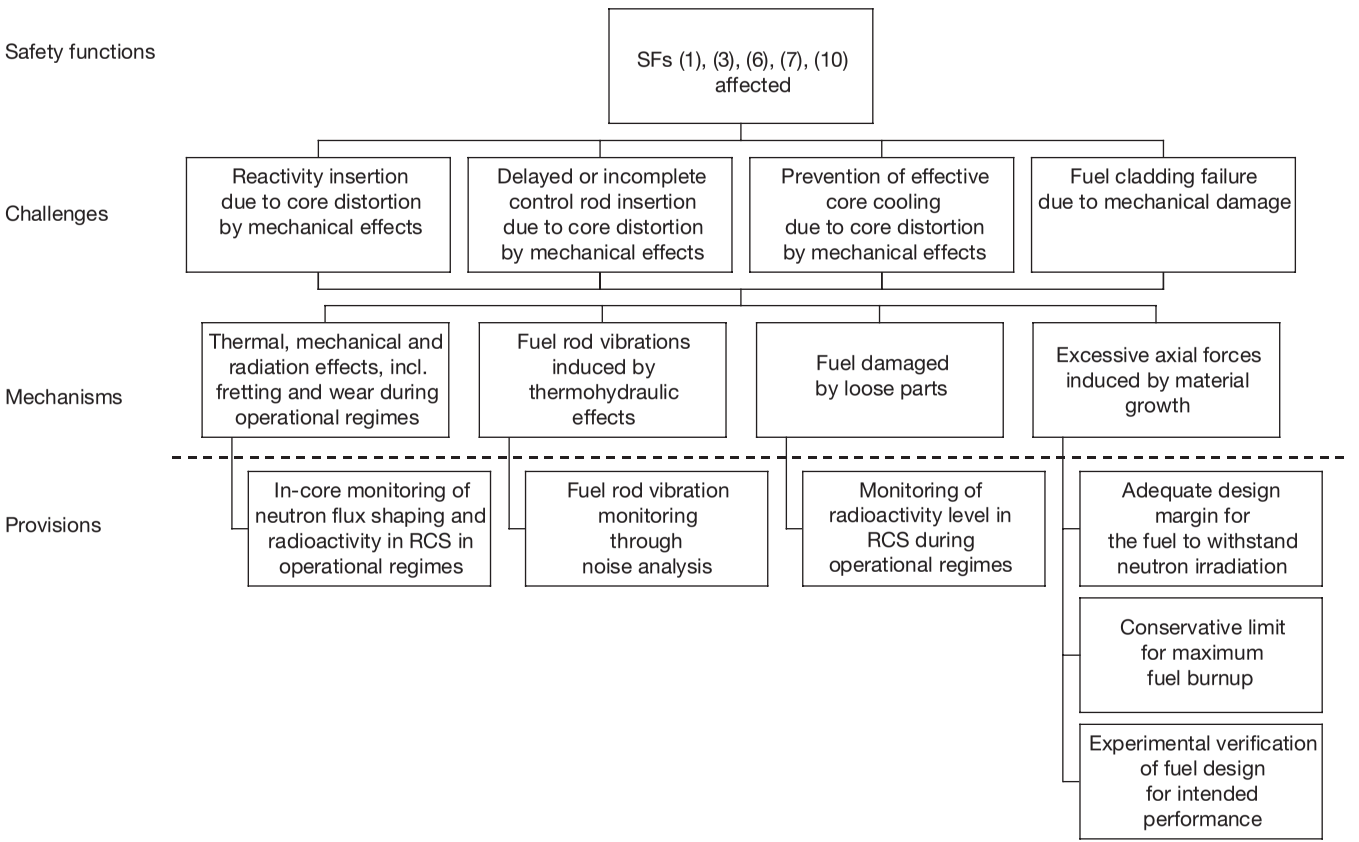


FIG. 31. Objective tree for Level 2 of defence in depth (RCS, reactor coolant system). Safety principle (195): reactor core integrity.

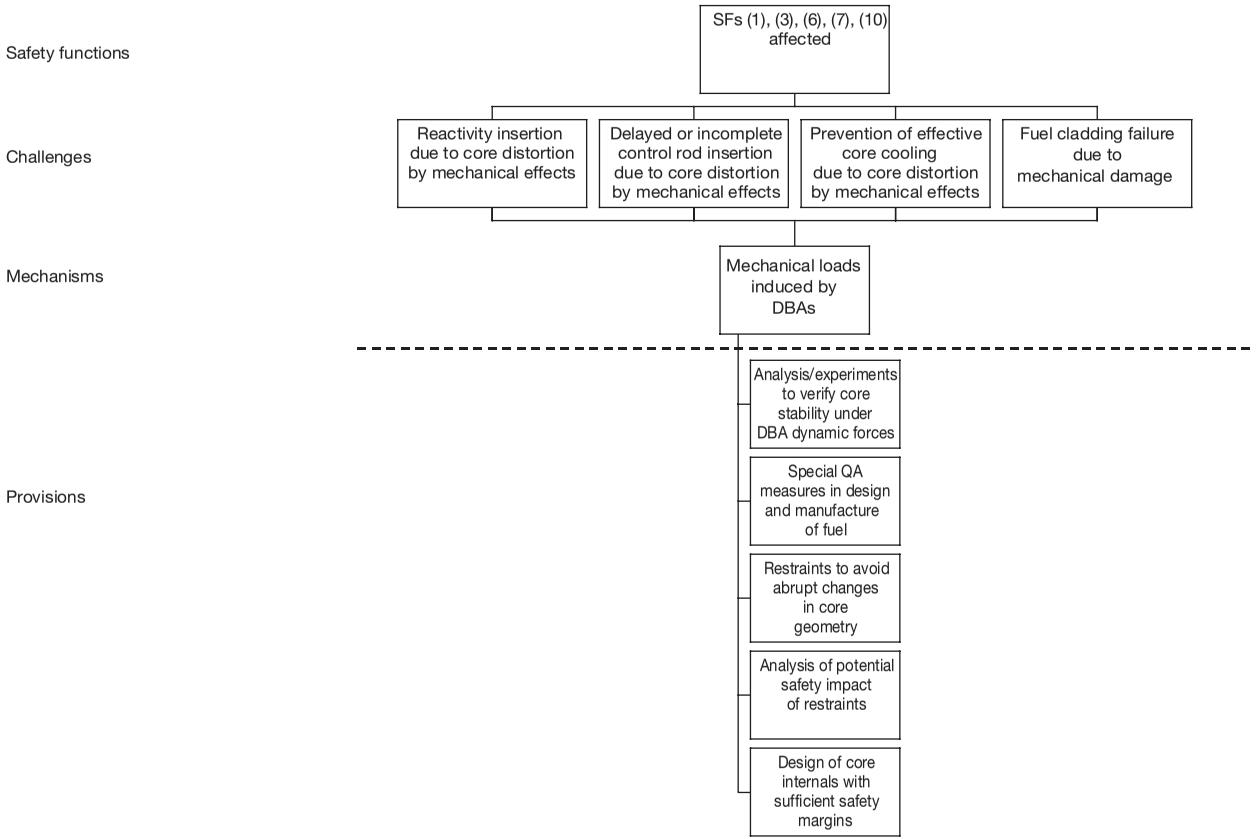


FIG. 32. Objective tree for Level 3 of defence in depth (QA, quality assurance). Safety principle (195): reactor core integrity.

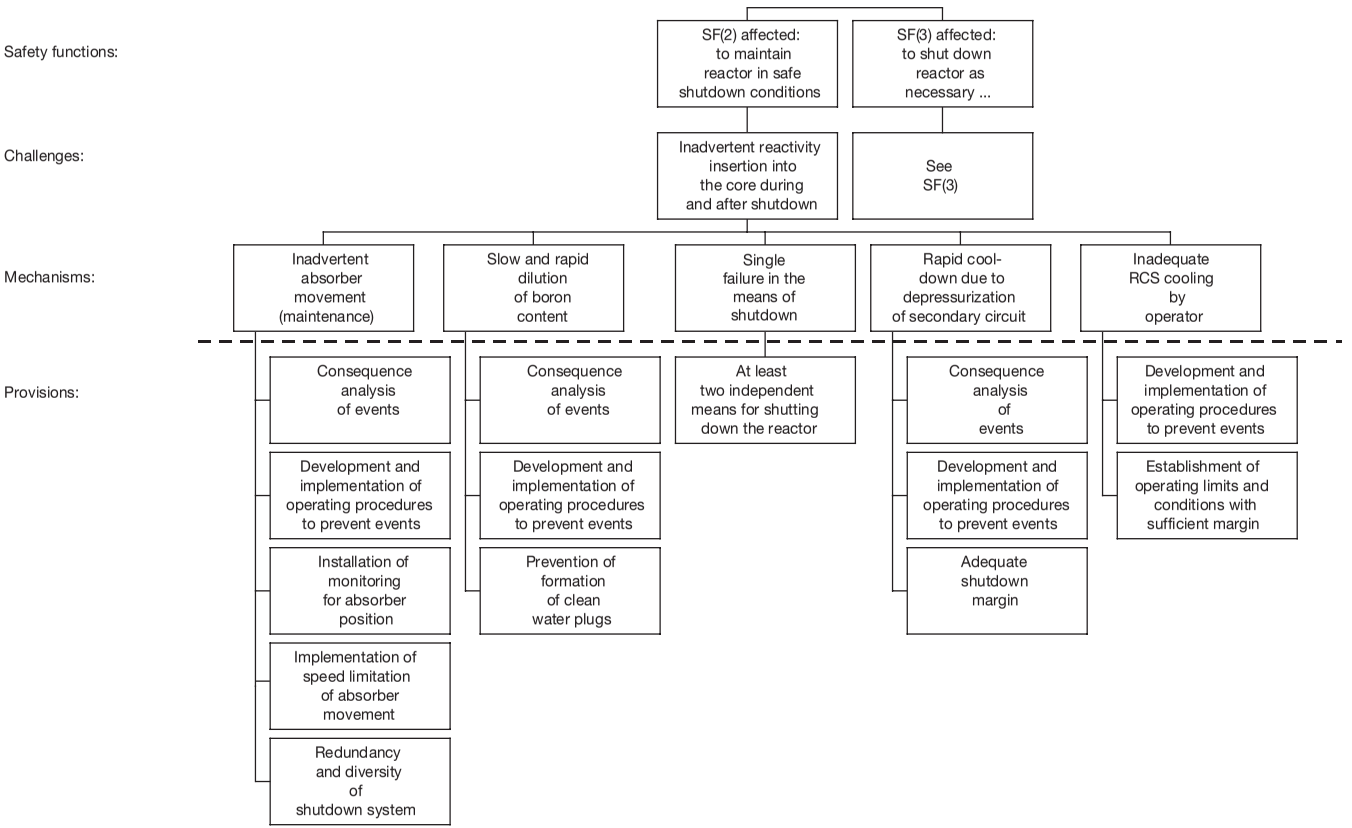


FIG. 33. Objective tree for Levels 3 and 4 of defence in depth (RCS, reactor core coolant). Safety principle (200): automatic shutdown systems, see also SF (2).

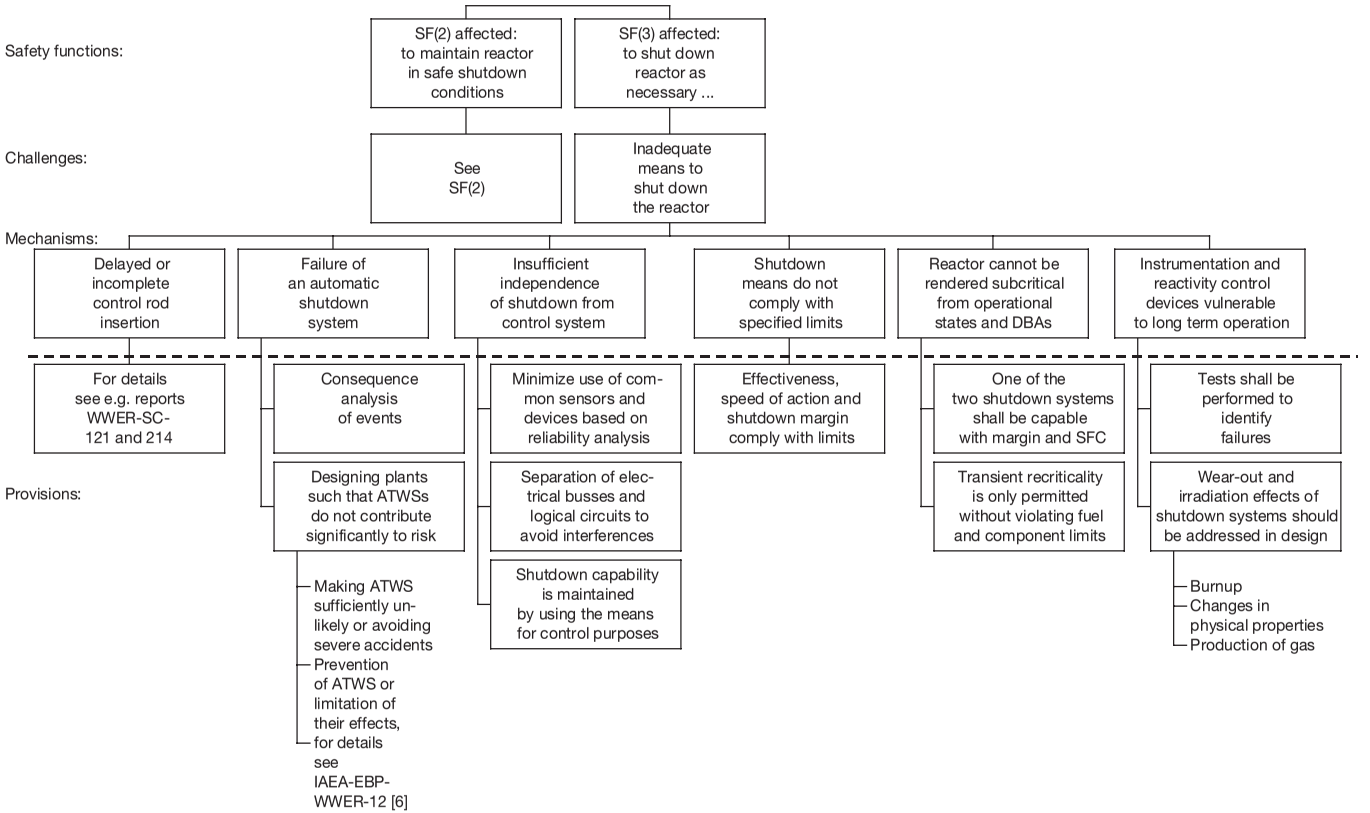


FIG. 34. Objective tree for Levels 3 and 4 of defence in depth (ATWS, advanced transient without scram; SFC, single failure criterion). Safety principle (200): automatic shutdown systems, see also SF (3).

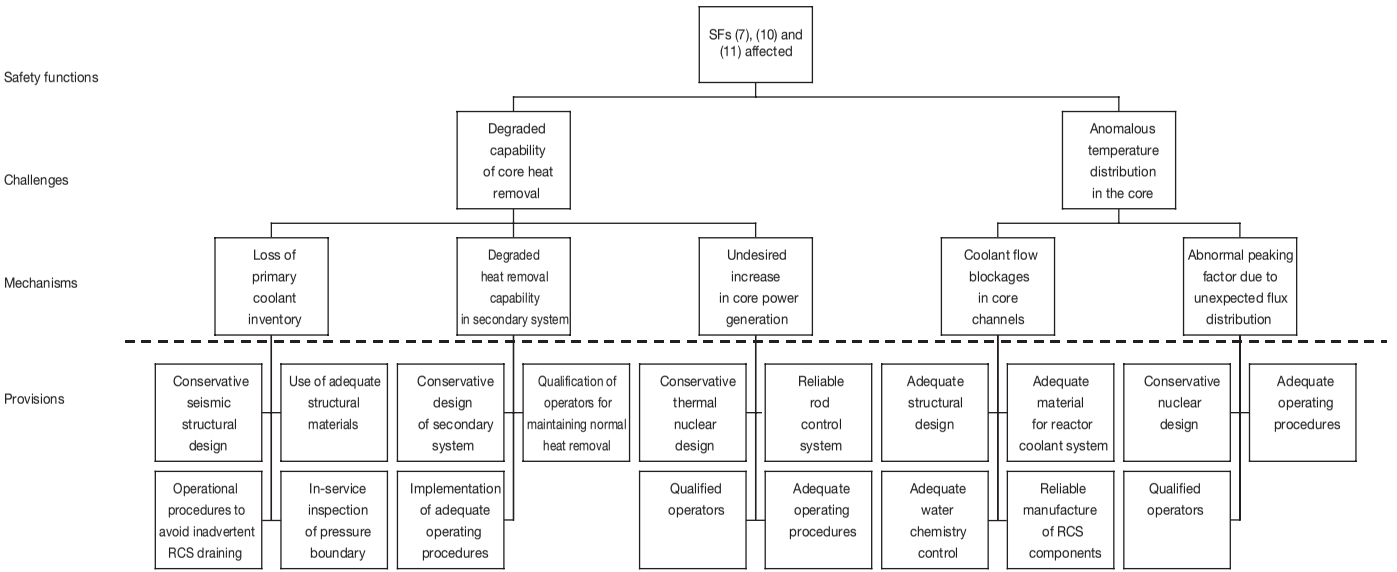


FIG. 35. Objective tree for Level 1 of defence in depth (RCS, reactor coolant system). Safety principle (203): normal heat removal.

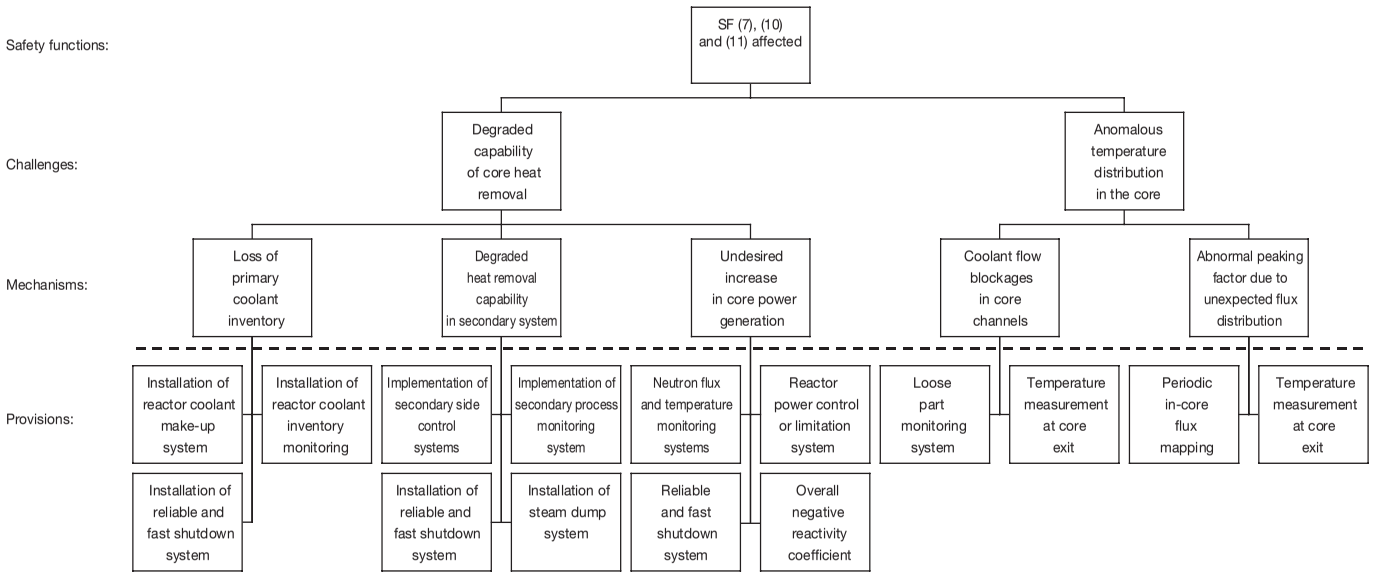


FIG. 36. Objective tree for Level 2 of defence in depth. Safety principle (203): normal heat removal.

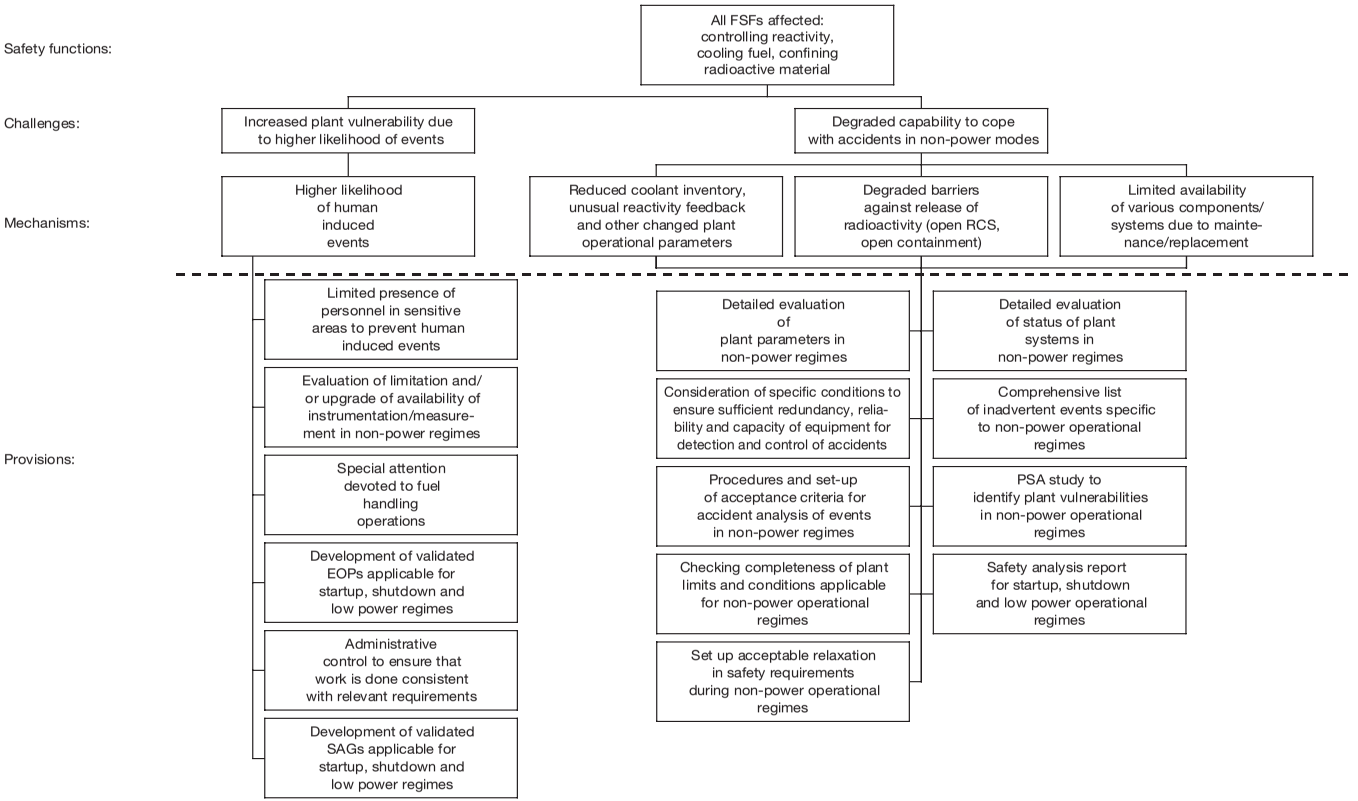


FIG. 37. Objective tree for Levels 1–4 of defence in depth (RCS, reactor coolant system; SAG, severe accident guideline). Safety principle (205): startup, shutdown and low power operation.

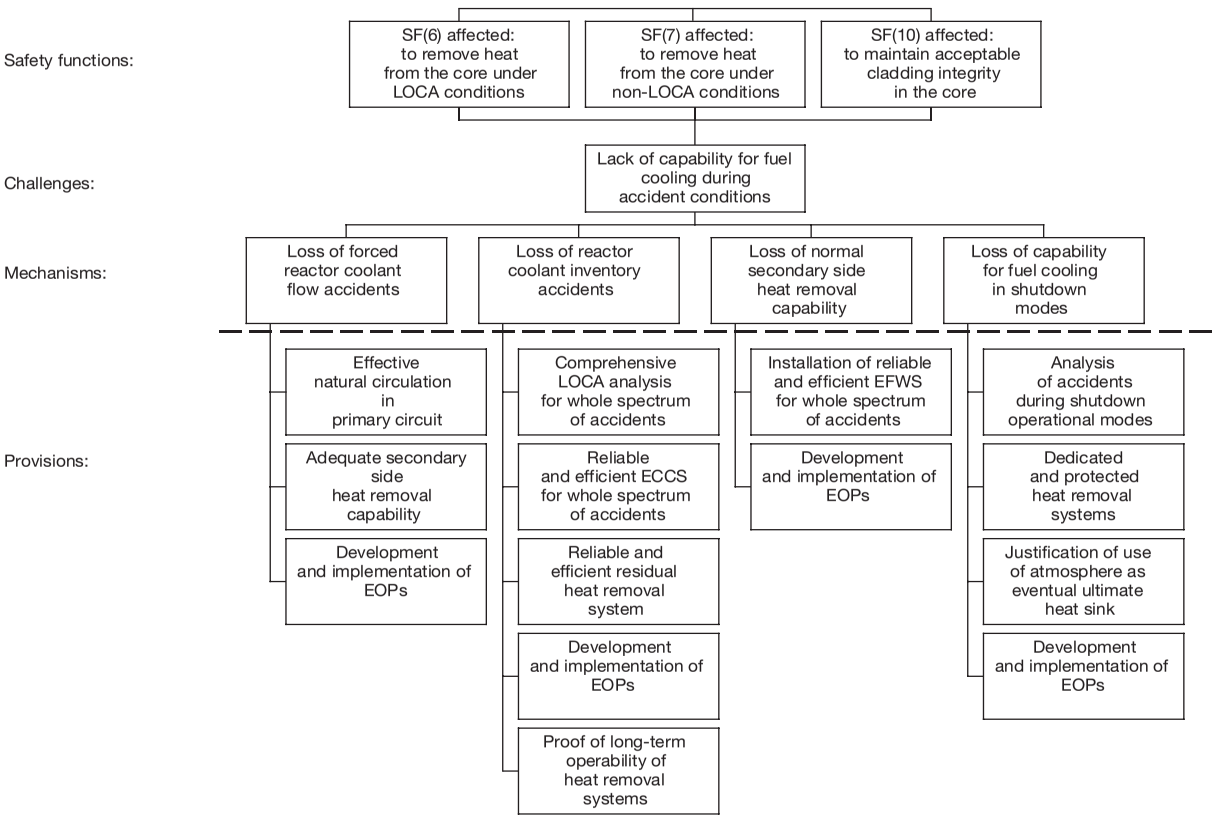


FIG. 38. Objective tree for Level 3 of defence in depth (ECCS, emergency core cooling system, EFWS, emergency feedwater system). Safety principle (207): emergency heat removal.

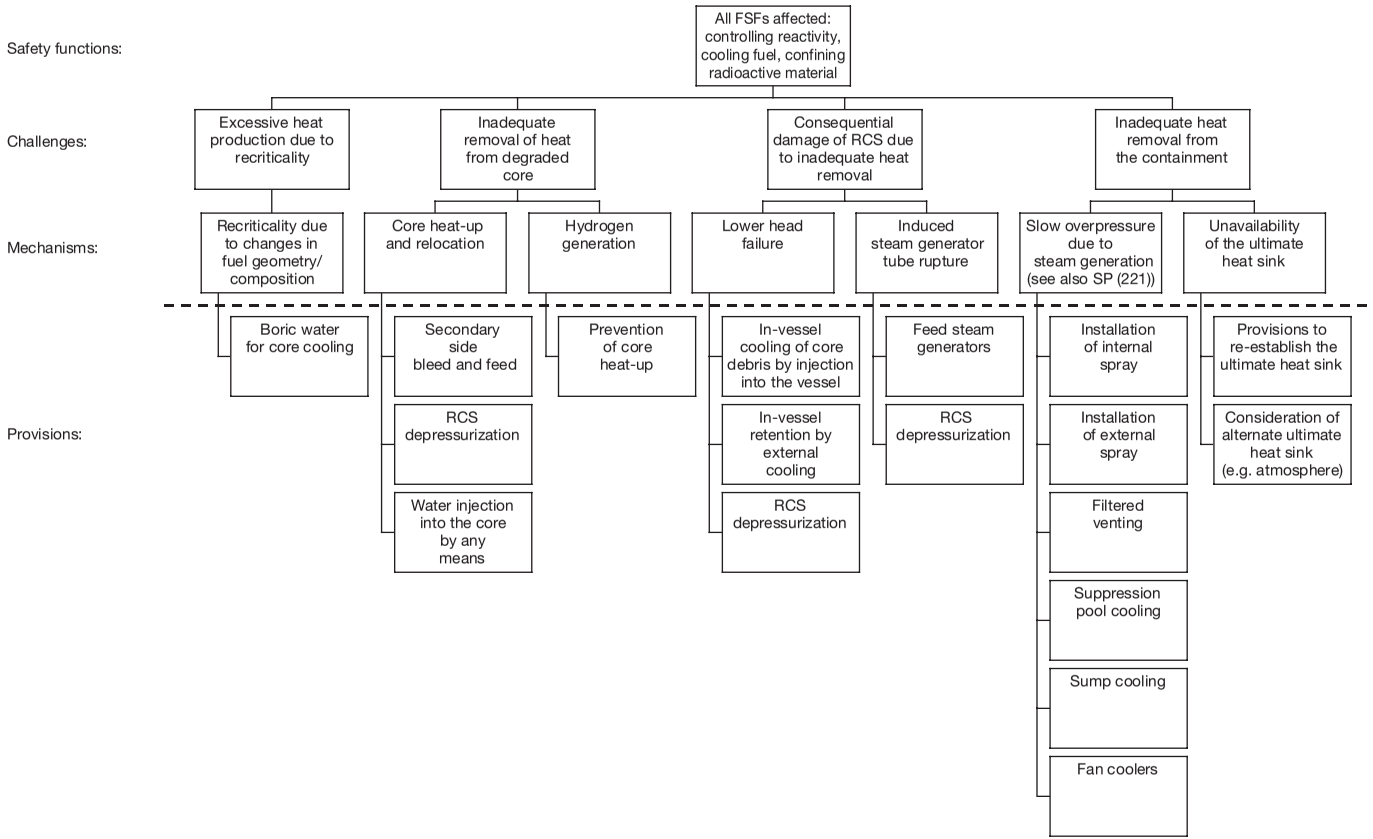


FIG. 39. Objective tree for Level 4 of defence in depth (RCS, reactor coolant system). Safety principle (207): emergency heat removal.

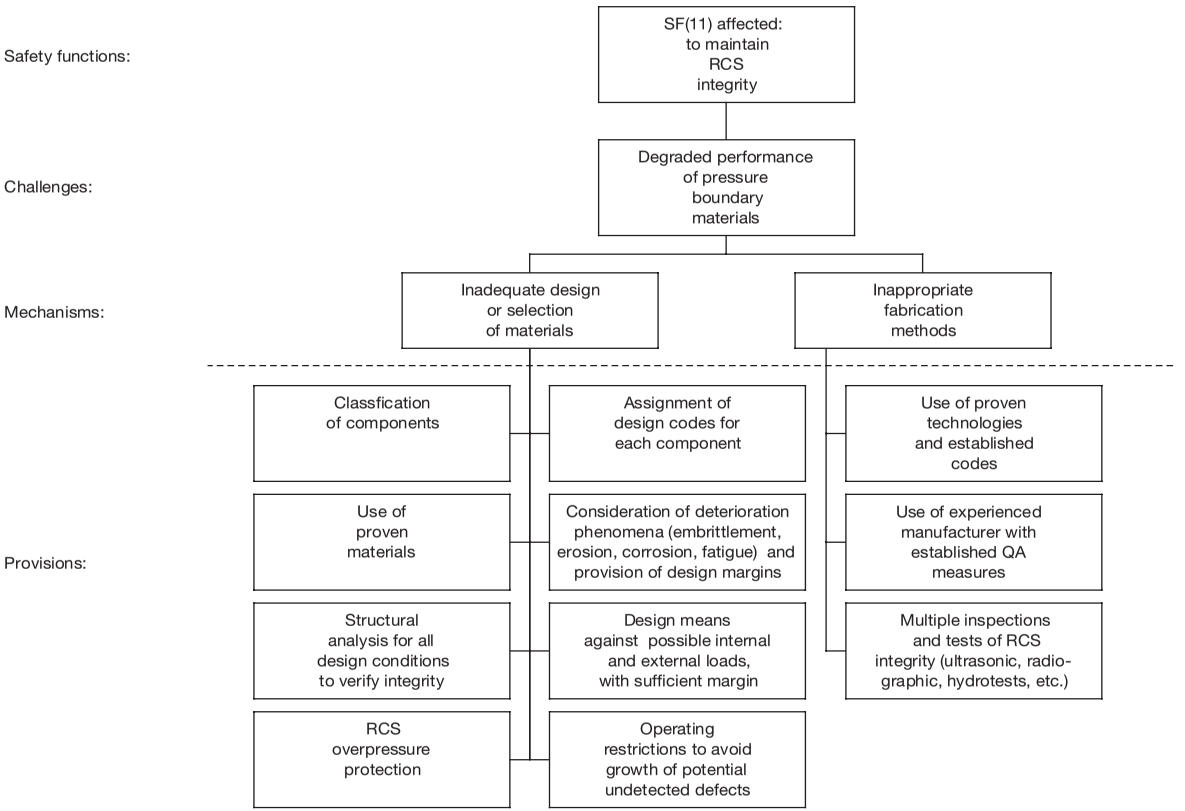


FIG. 40. Objective tree for Level 1 of defence in depth (RCS, reactor coolant system; QA, quality assurance). Safety principle (209): reactor coolant system integrity.

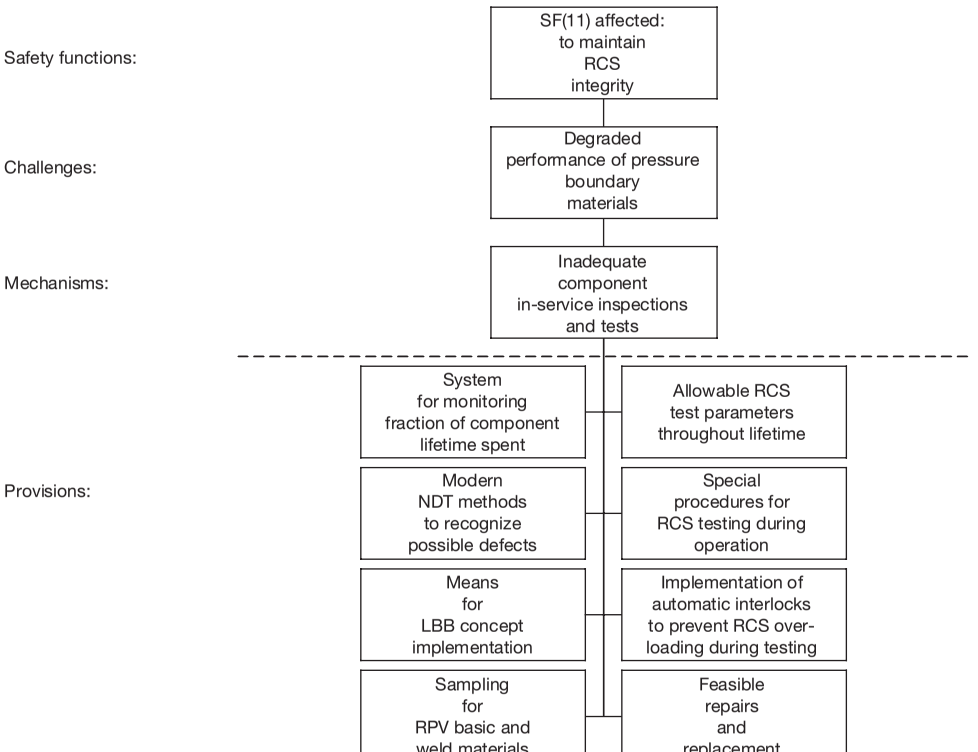


FIG. 41. Objective tree for Level 2 of defence in depth (NDT, non-destructive testing; LBB, leak before break; RPV, reactor pressure vessel; RCS, reactor coolant system). Safety principle (209): reactor coolant system integrity.

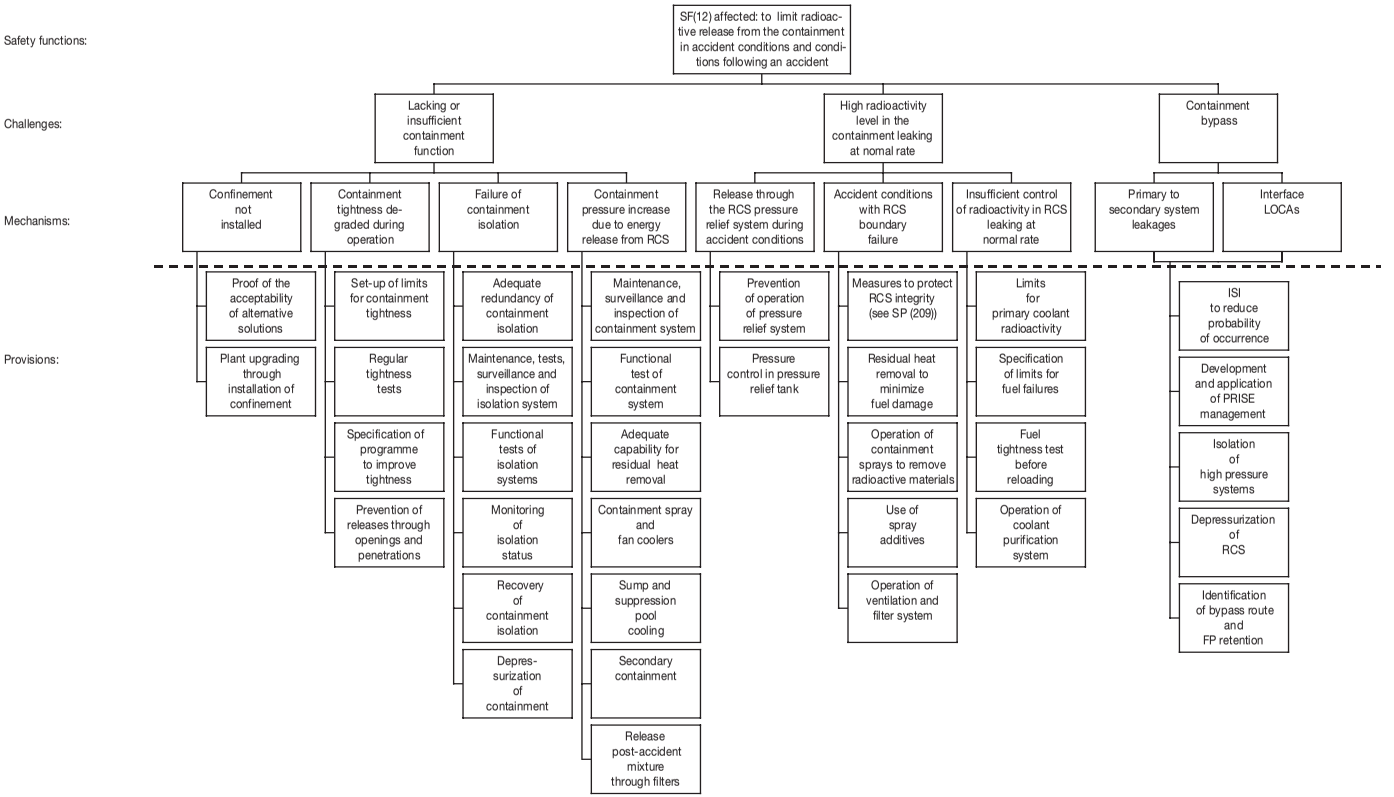


FIG. 42. Objective tree for Level 3 of defence in depth (RCS, reactor coolant system; LOCA, loss of coolant accident; ISI, in-service inspection; PRISE, primary to secondary leakage; FP, fission product). Safety principle (217): confinement of radioactive material (see also SF (12)).

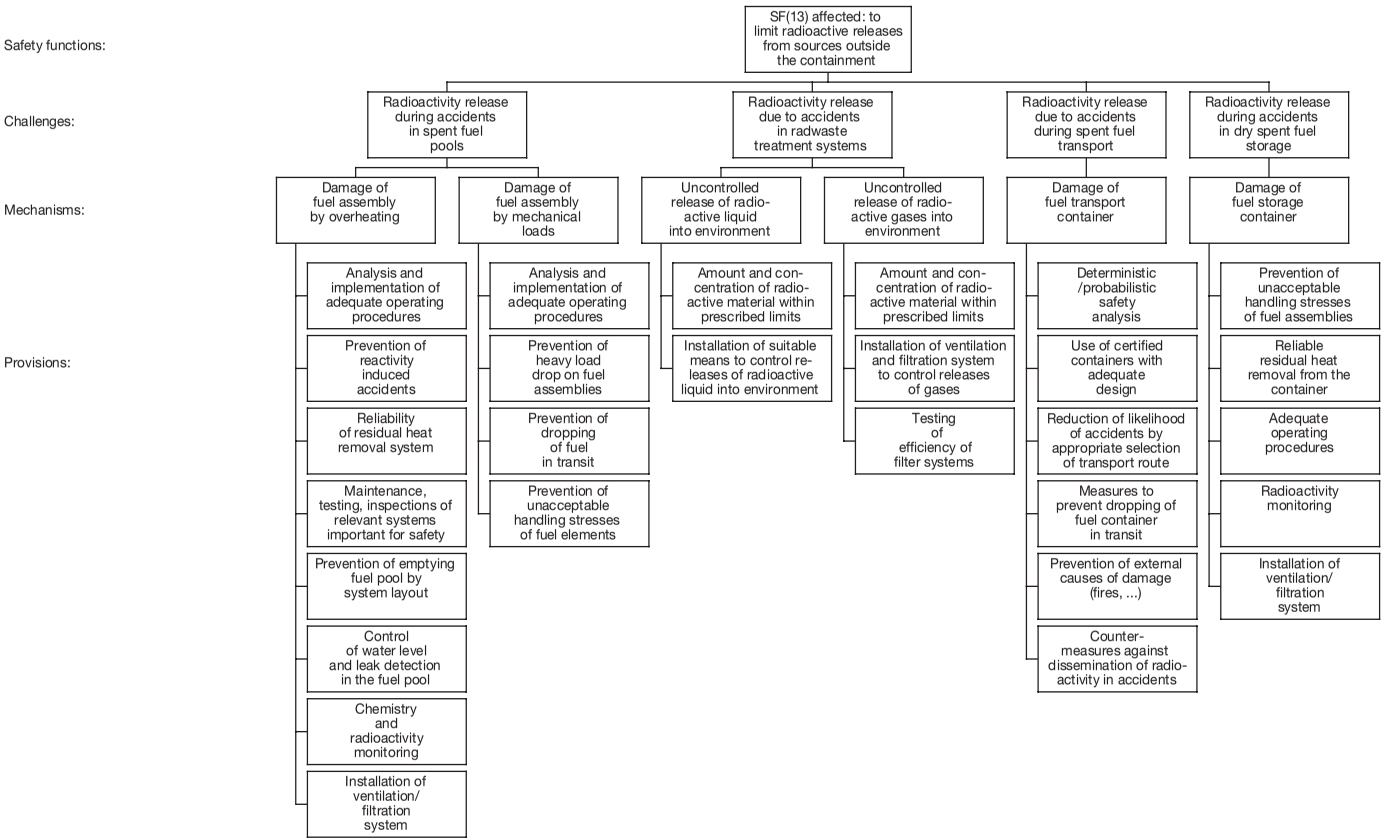


FIG. 43. Objective tree for Level 3 of defence in depth. Safety principle (217): confinement of radioactive material (see also SF (13)).

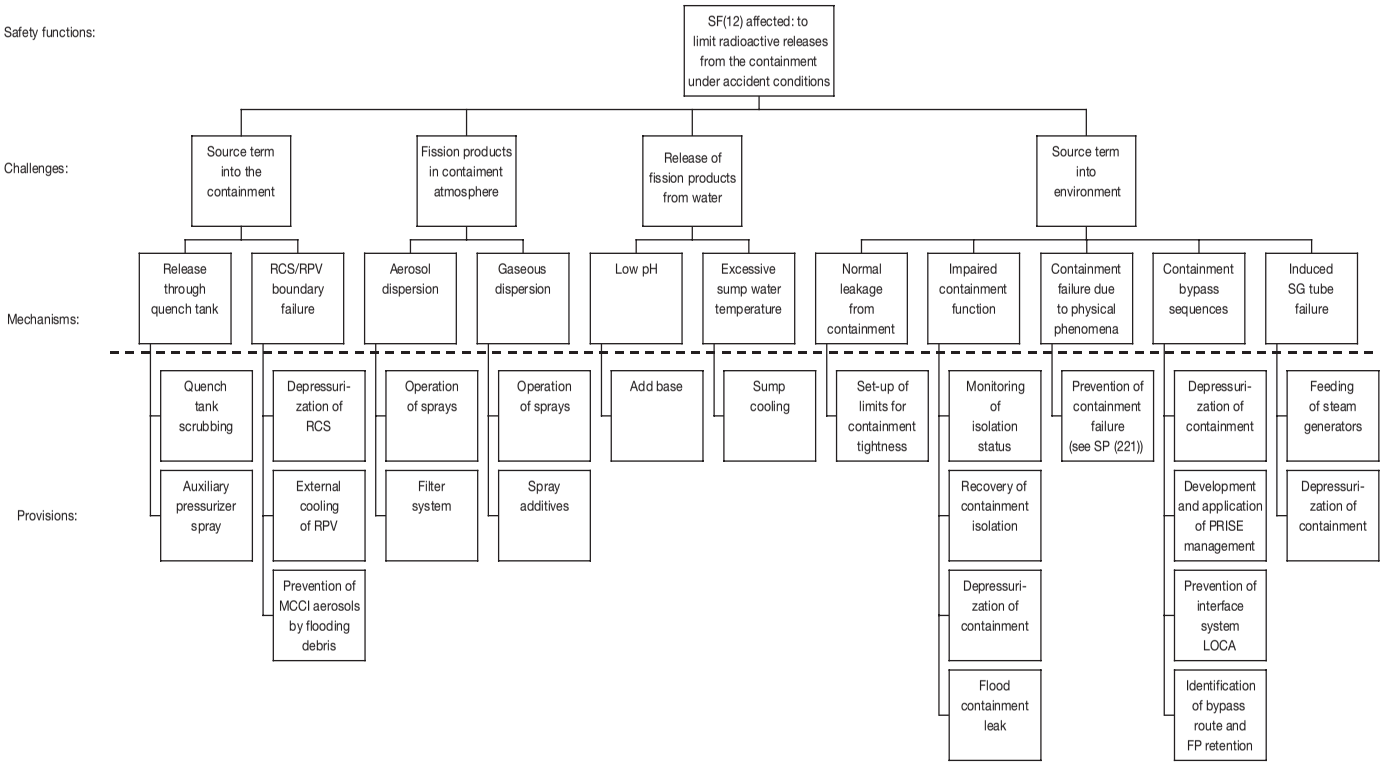


FIG. 44. Objective tree for Level 4 of defence in depth (RCS, reactor coolant system; RPV, reactor pressure vessel; MCCI, molten corium–concrete interaction; PRISE, primary to secondary leakage; LOCA, loss of coolant accident; SG, steam generator). Safety principle (217): confinement of radioactive material.

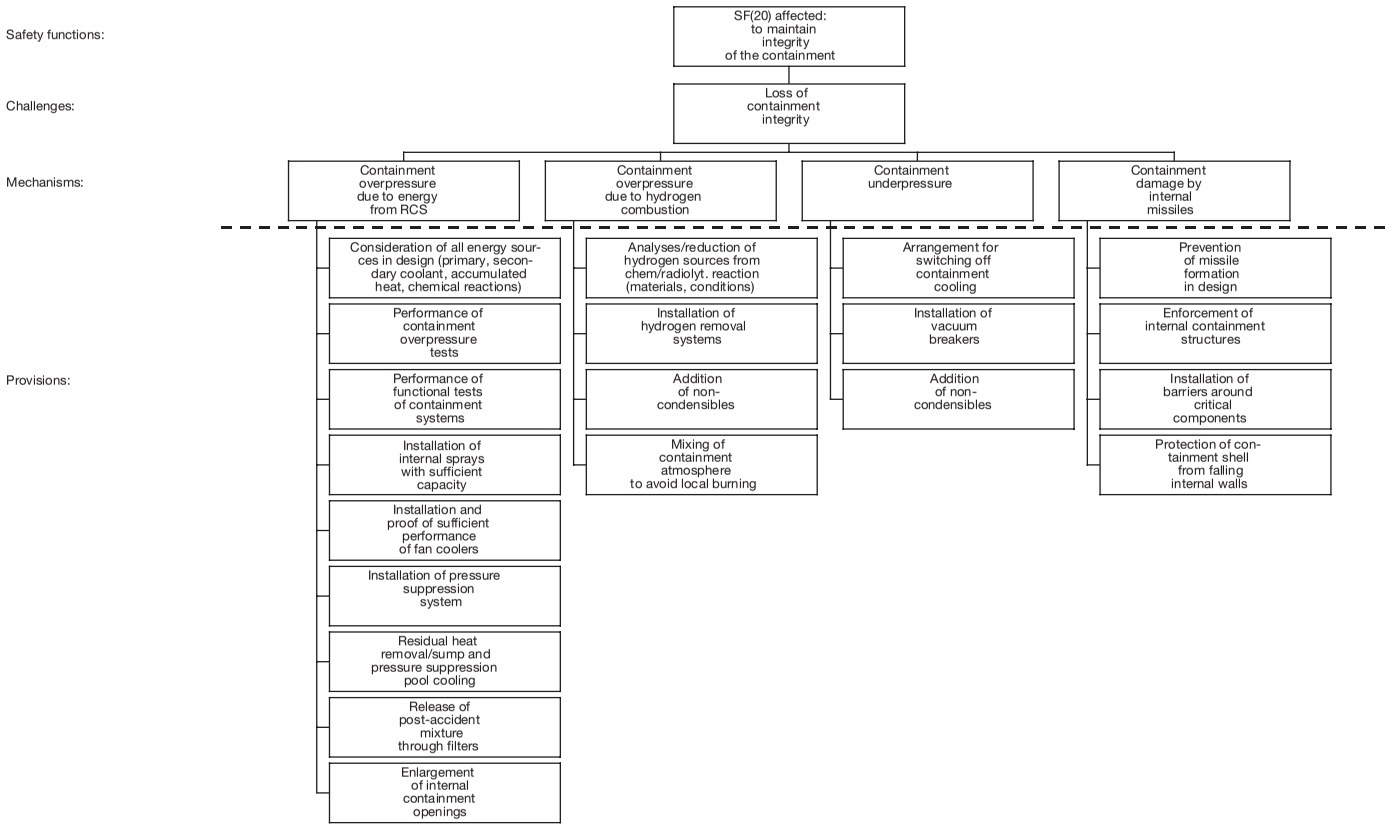


FIG. 45. Objective tree for Level 3 of defence in depth (RCS, reactor coolant system). Safety principle: protection of confinement structure (221).

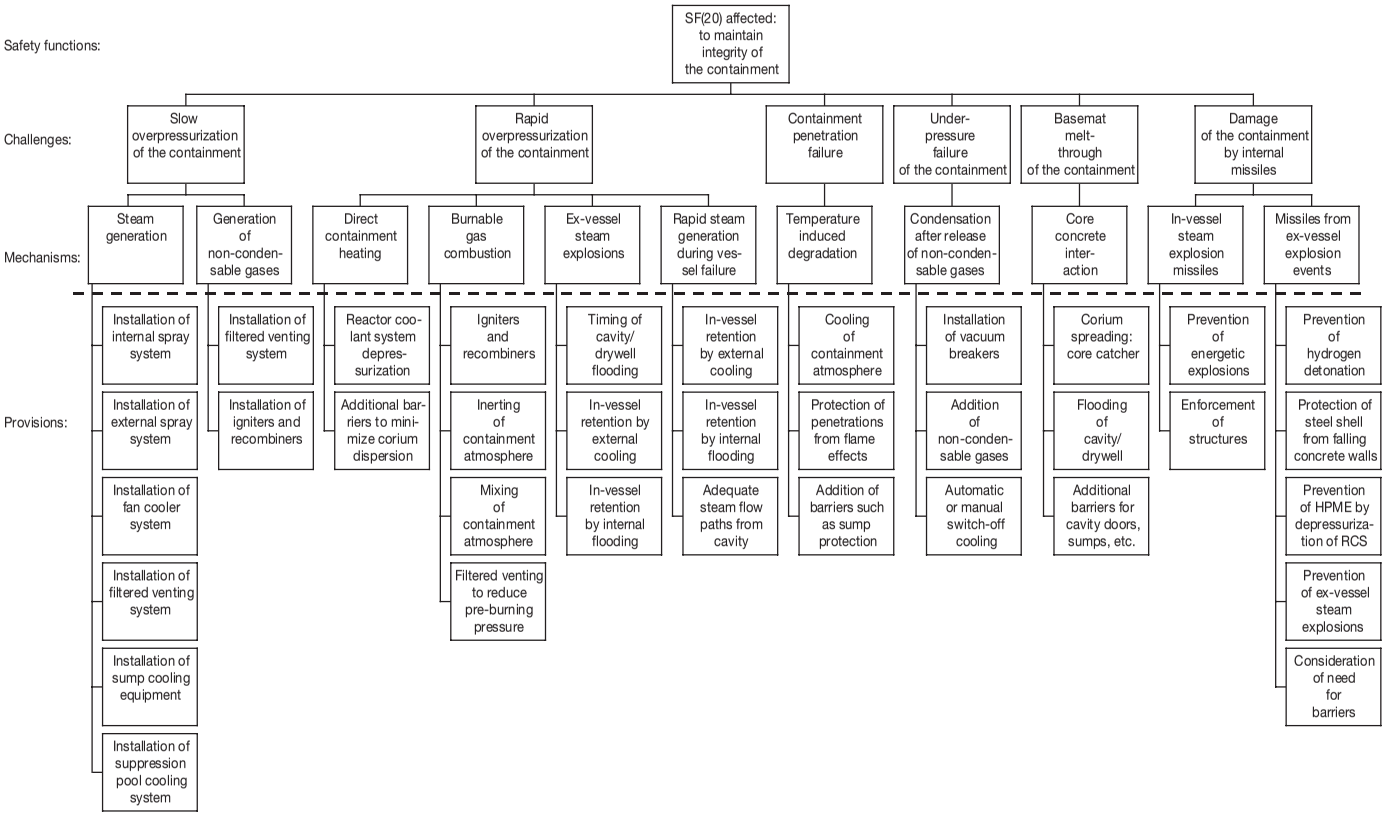


FIG. 46. Objective tree for Level 4 of defence in depth (HPME, high pressure melt ejection; RCS, reactor coolant system). Safety principle (221): protection of confinement structure.

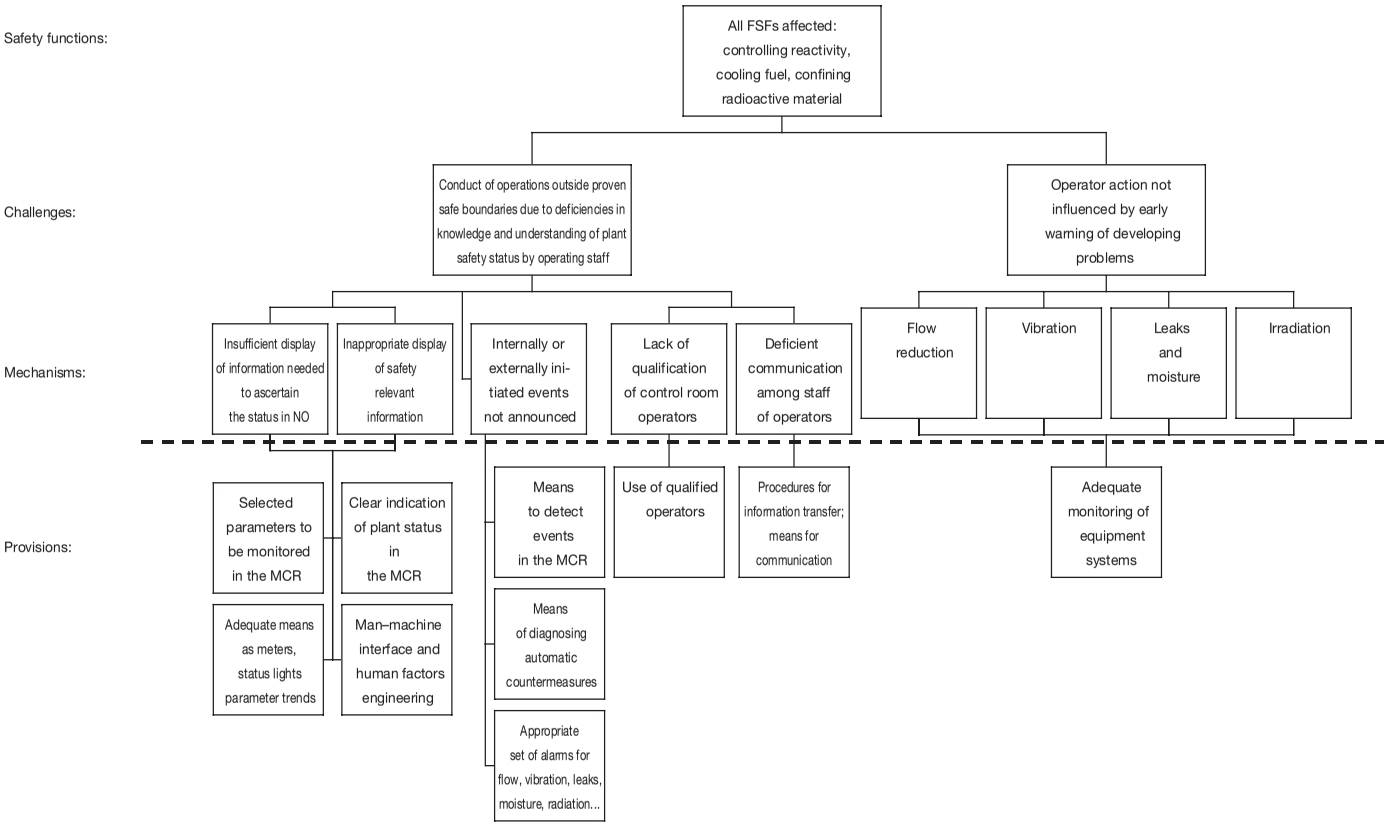


FIG. 47. Objective tree for Levels 1 and 2 of defence in depth (NO, normal operation; MCR, main control room). Safety principle (227): monitoring of plant safety status.

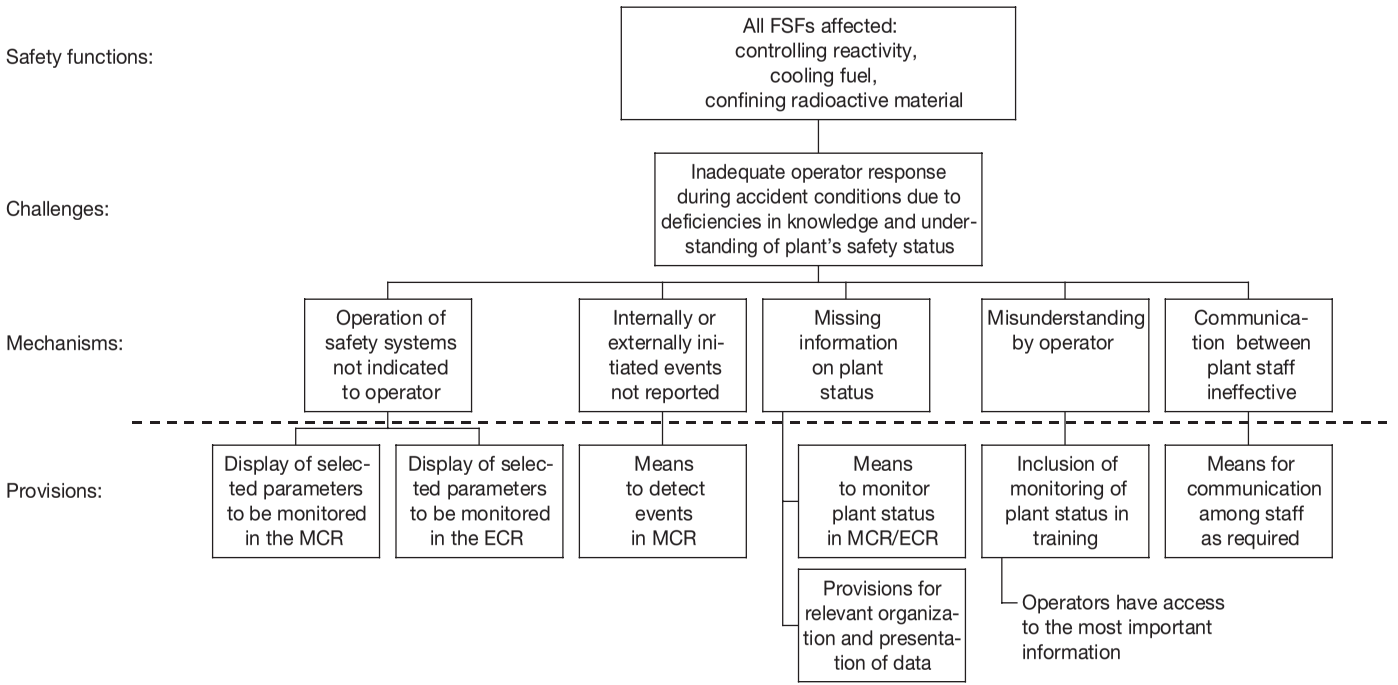


FIG. 48. Objective tree for Levels 3 and 4 of defence in depth (MCR, main control room; ECR, emergency control room). Safety principle (227): monitoring of plant safety status.

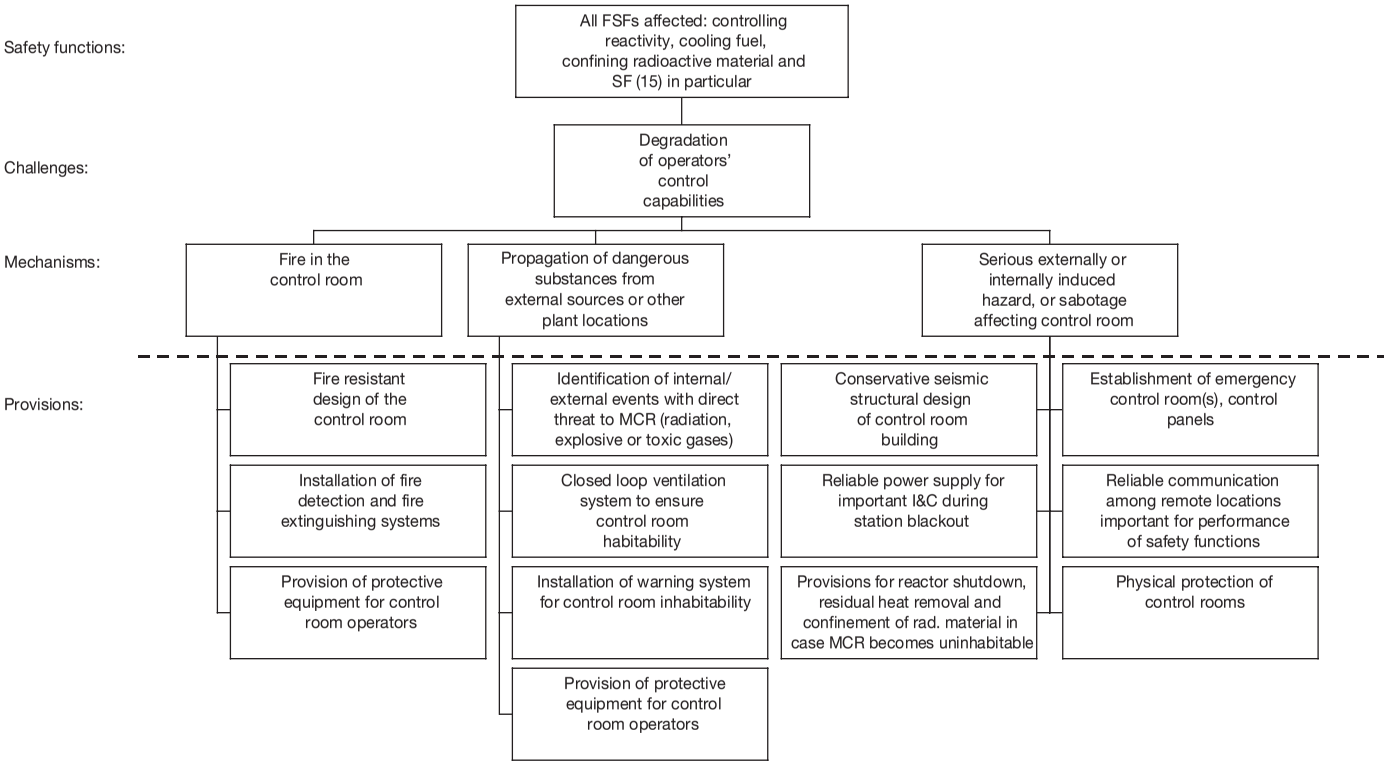


FIG. 49. Objective tree for Levels 1–4 of defence in depth (MCR, main control room; I&C, information and control). Safety principle: preservation of control capability (230).

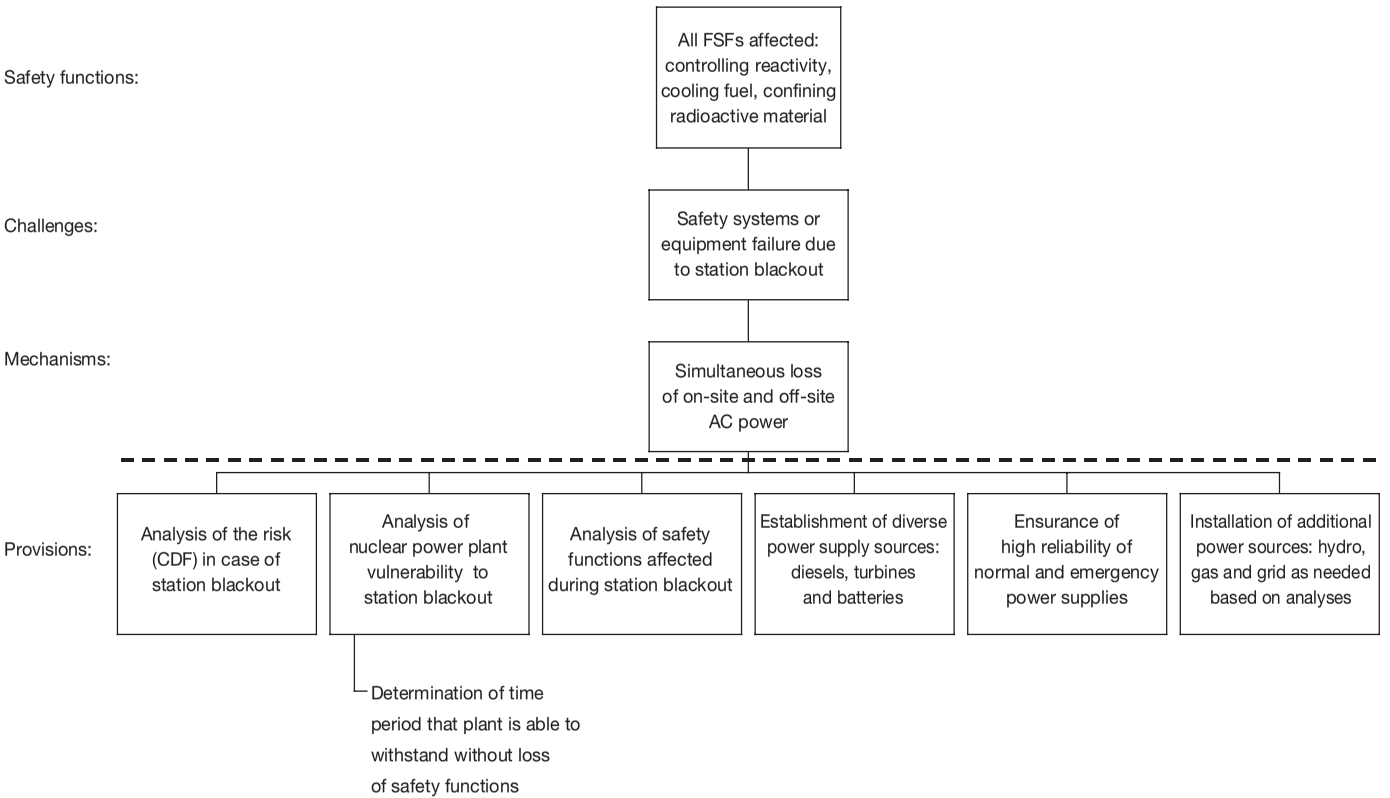


FIG. 50. Objective tree for Levels 3 and 4 of defence in depth (CDF, core damage frequency). Safety principle: station blackout (233).

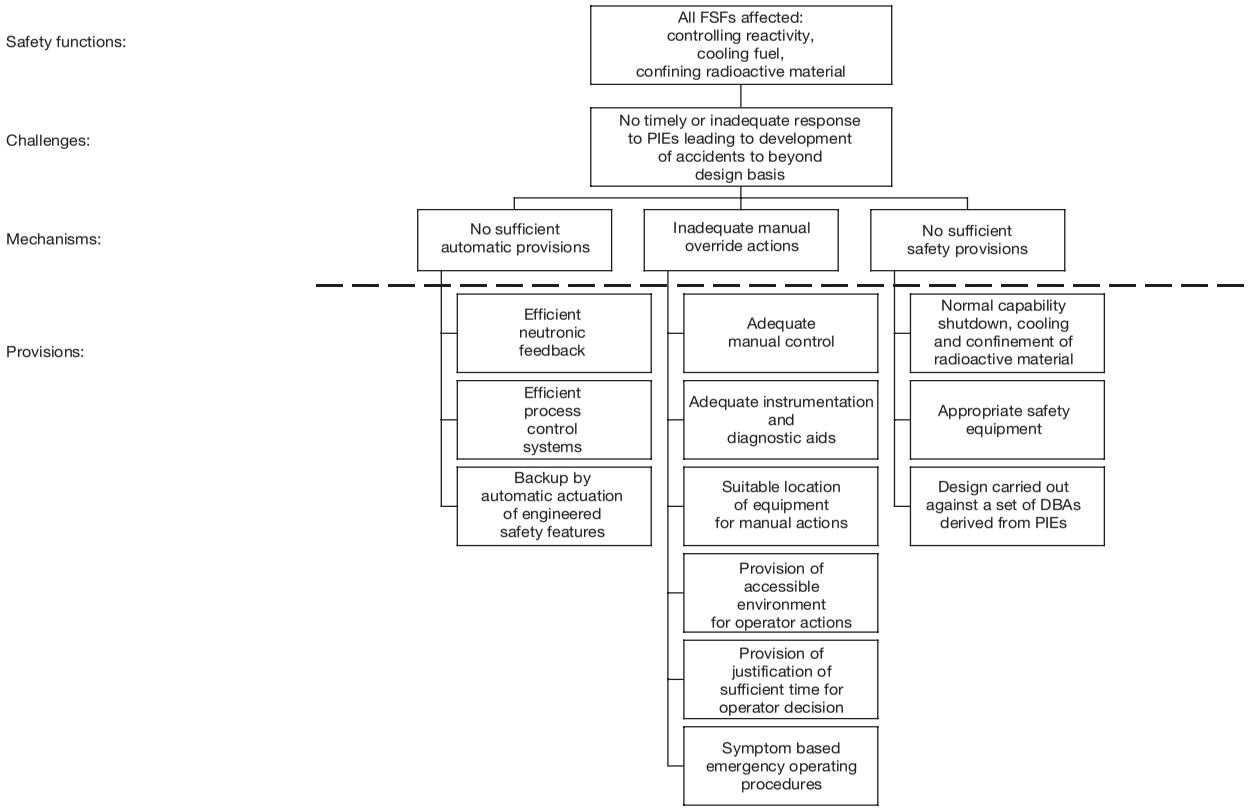


FIG. 51. Objective tree for Level 3 of defence in depth (PIE, postulated initiating event). Safety principle (237): control of accidents within the design basis.

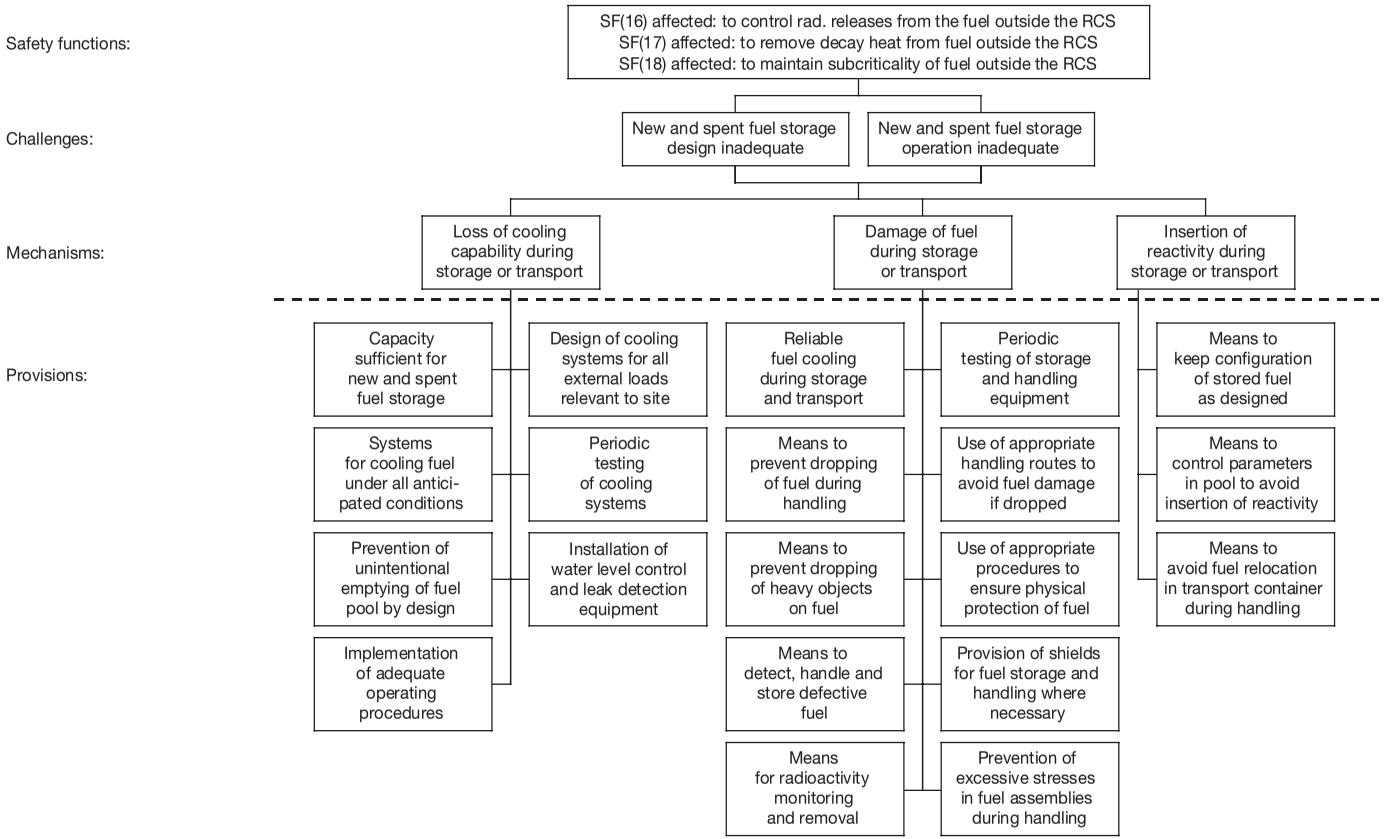


FIG. 52. Objective tree for Levels 1 and 2 of defence in depth (RCS, reactor coolant system). Safety principle (240): new and spent fuel storage.

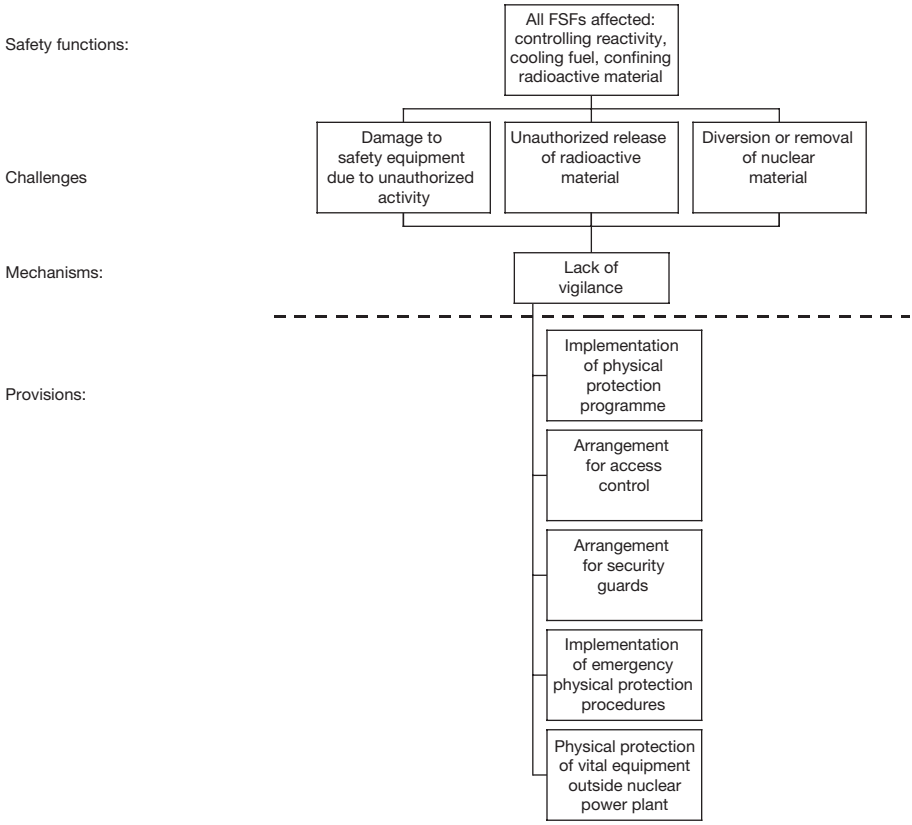


FIG. 53. Objective tree for Level 1 of defence in depth. Safety principle (242): physical protection of plant.

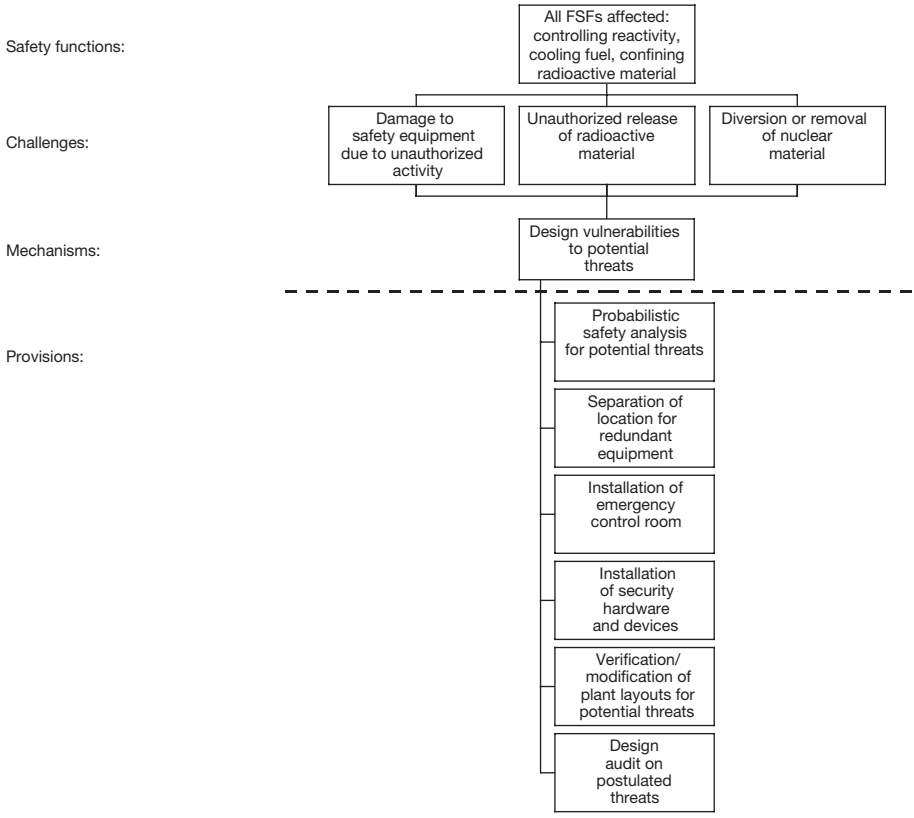


FIG. 54. Objective tree for Level 2 of defence in depth. Safety principle (242): physical protection of plant.

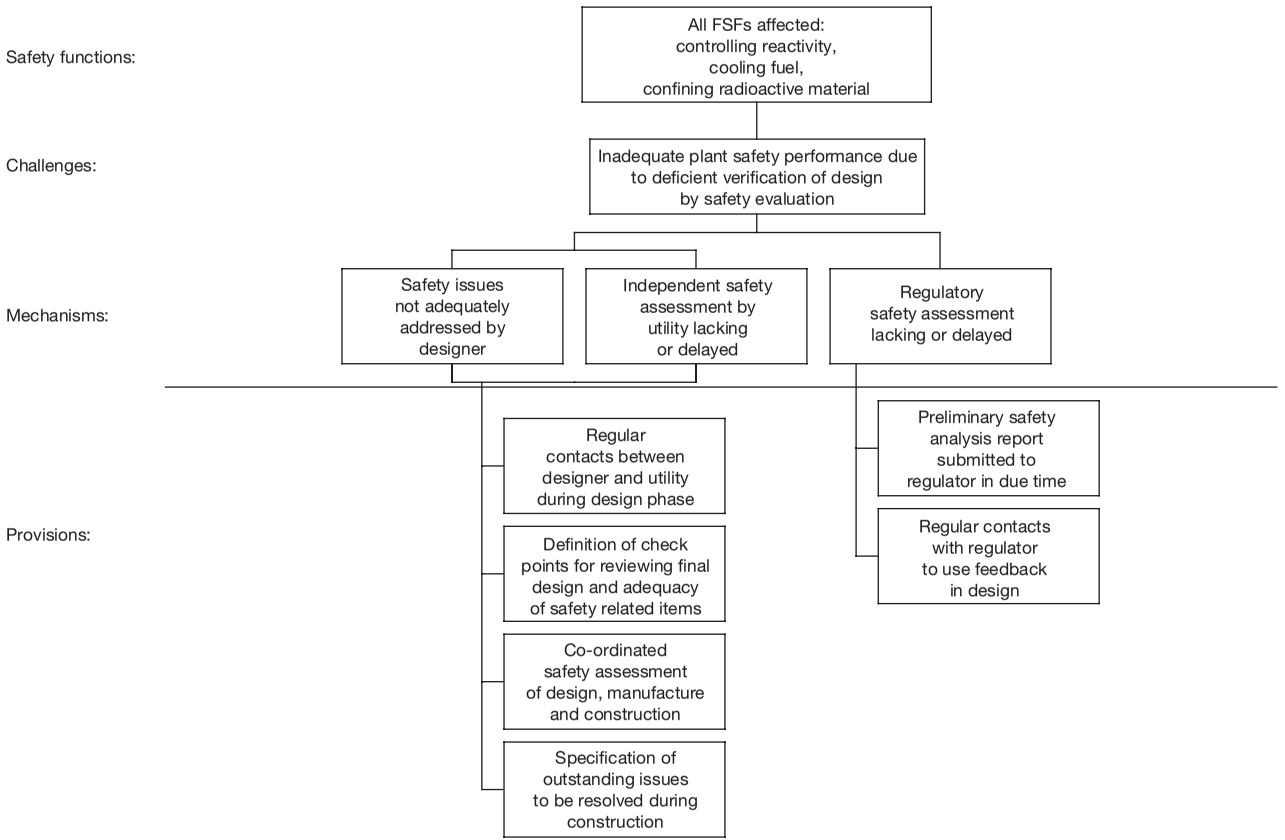


FIG. 55. Objective tree for Levels 1–4 of defence in depth. Safety principle (246): safety evaluation of design.

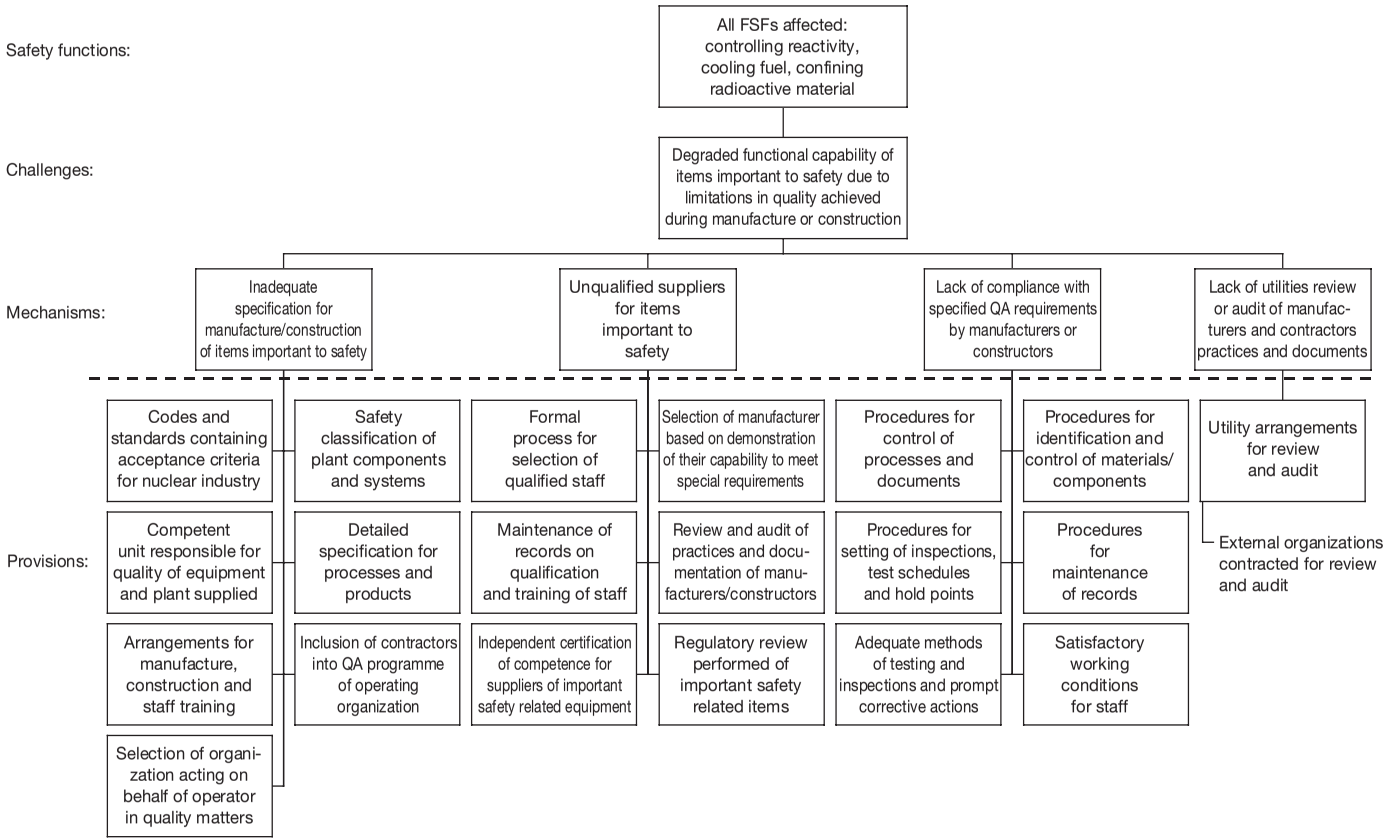


FIG. 56. Objective tree for Levels 1–4 of defence in depth. Safety principle (249): achievement of quality.

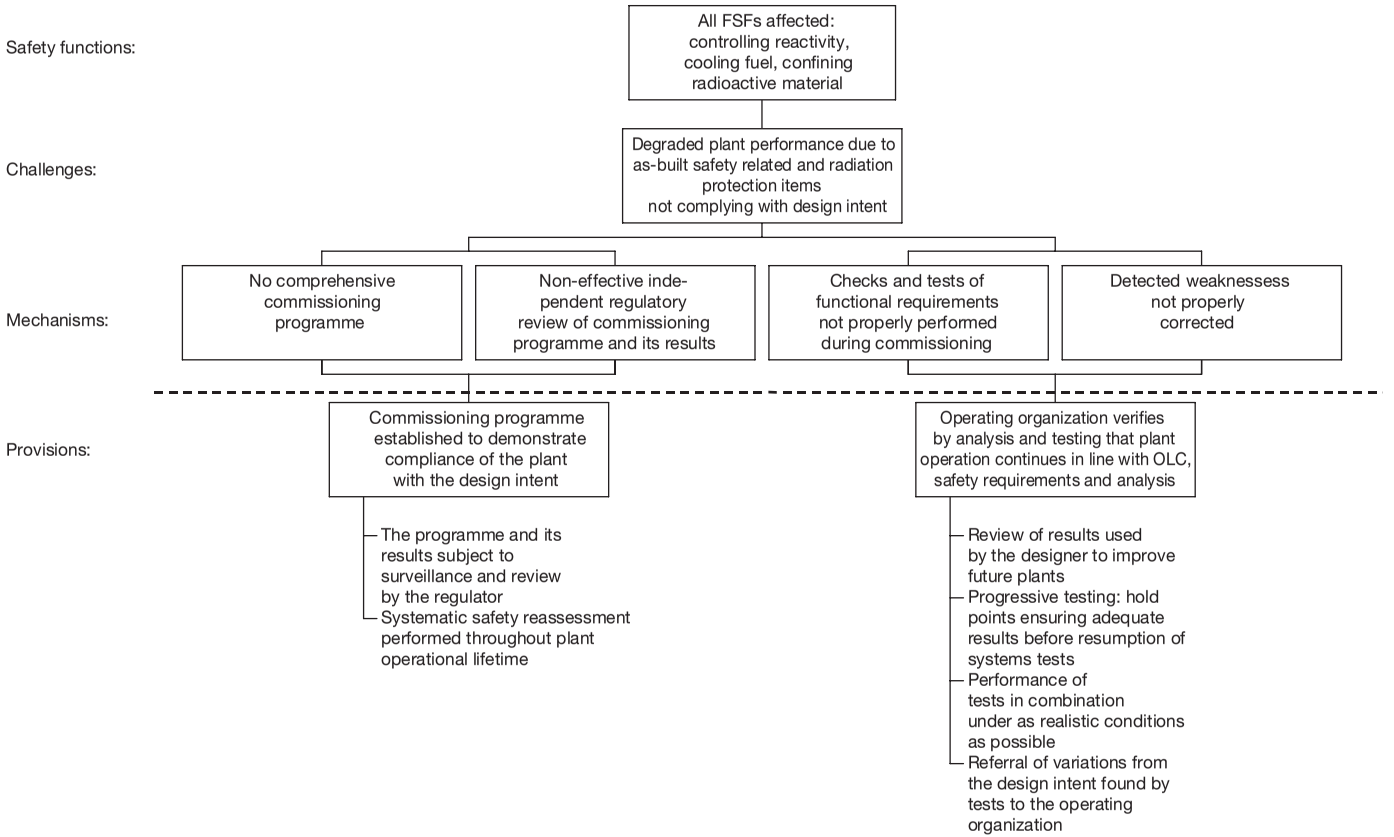


FIG. 57. Objective tree for Levels 1–3 of defence in depth. Safety principle (255): verification of design and construction.

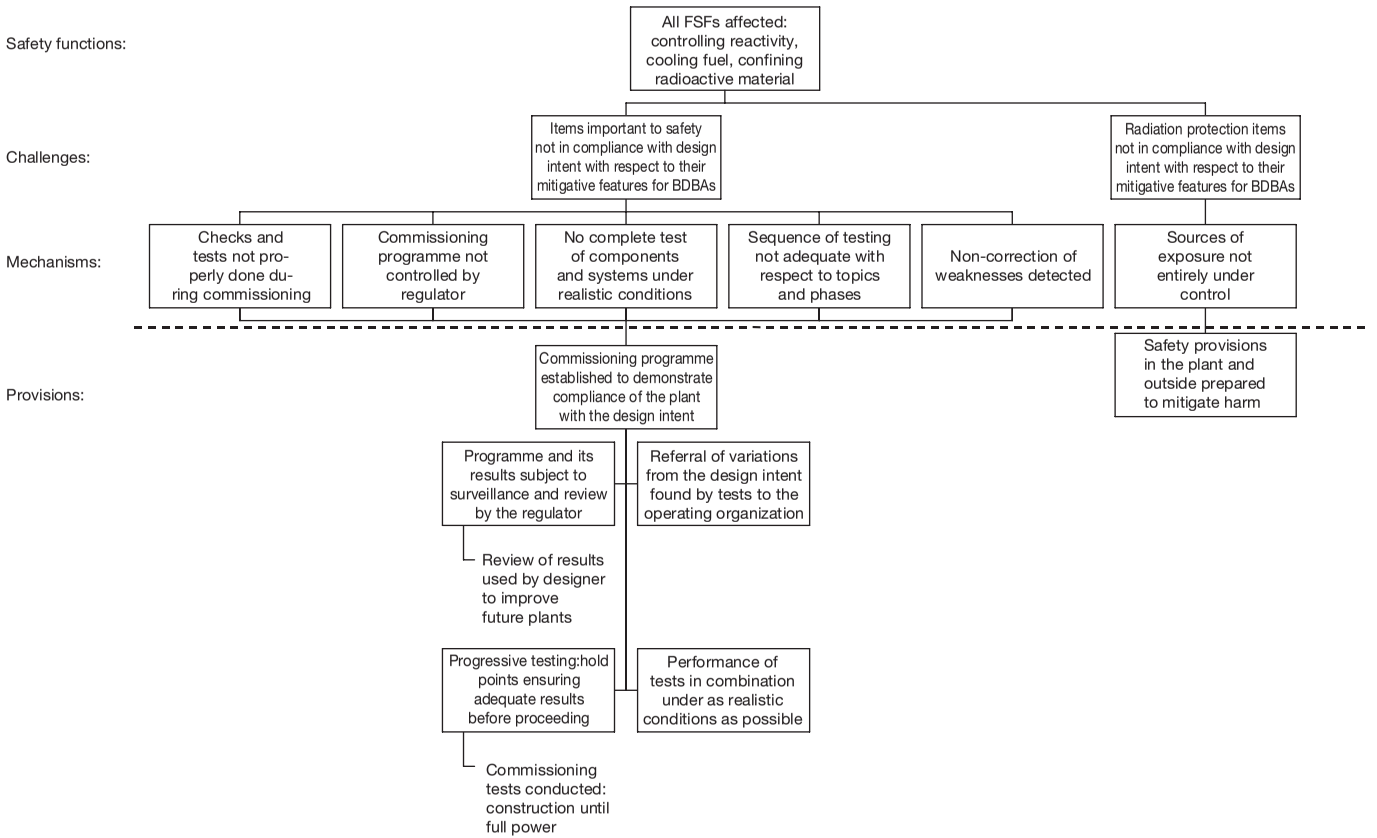


FIG. 58. Objective tree for Level 4 of defence in depth. Safety principle (255): verification of design and construction.

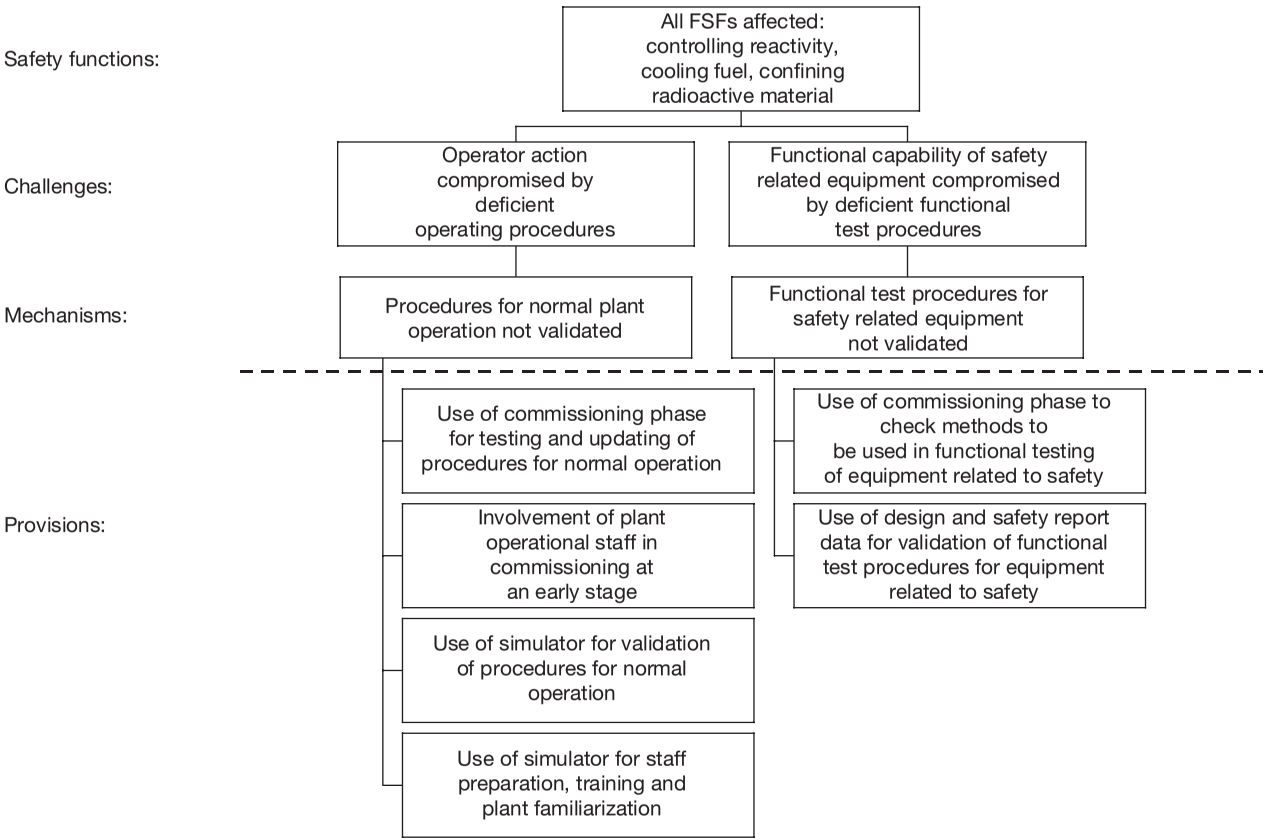


FIG. 59. Objective tree for Levels 1–4 of defence in depth. Safety principle (258): validation of operating and functional test procedures.

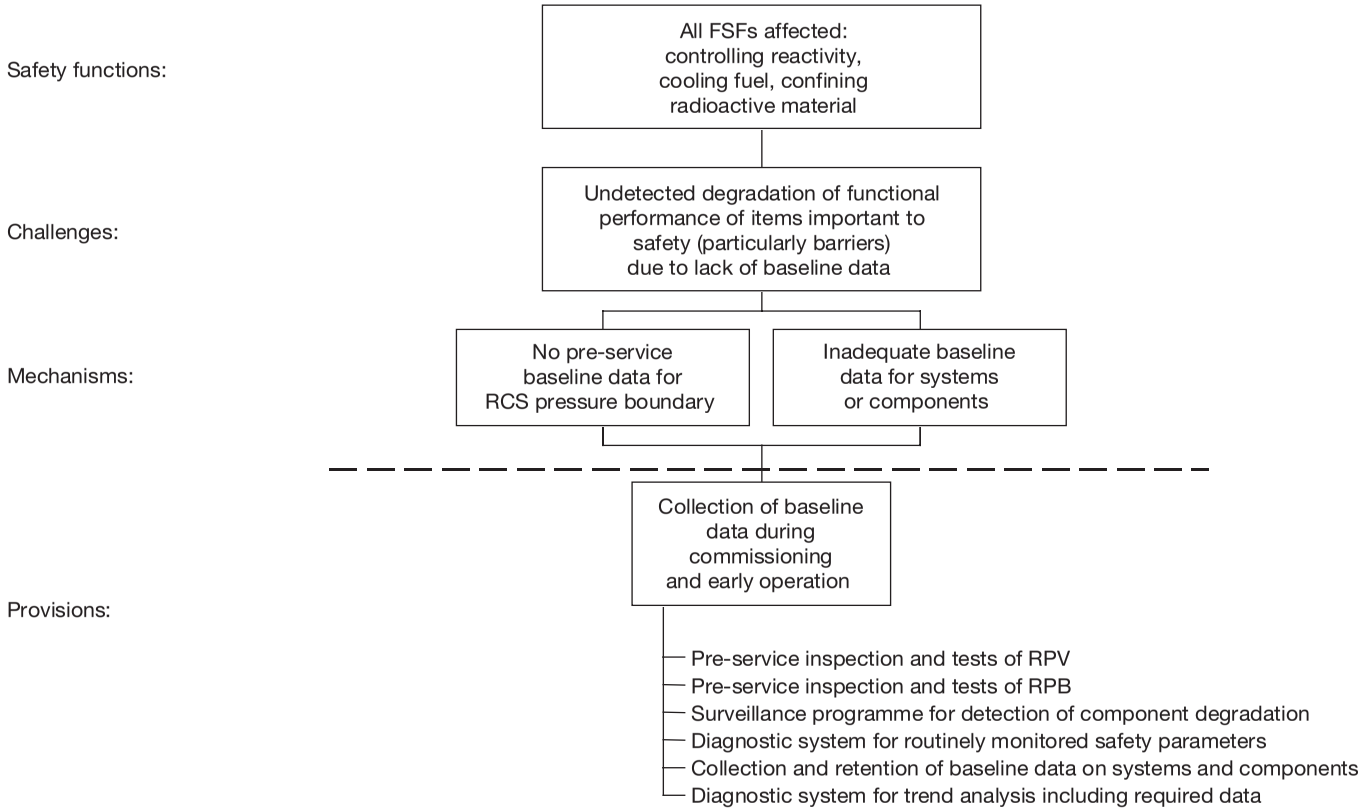


FIG. 60. Objective tree for Levels 1–4 of defence in depth (RCS, reactor coolant system; RPV, reactor pressure vessel; RPB, reactor pressure boundary). Safety principle (260): collection of baseline data.

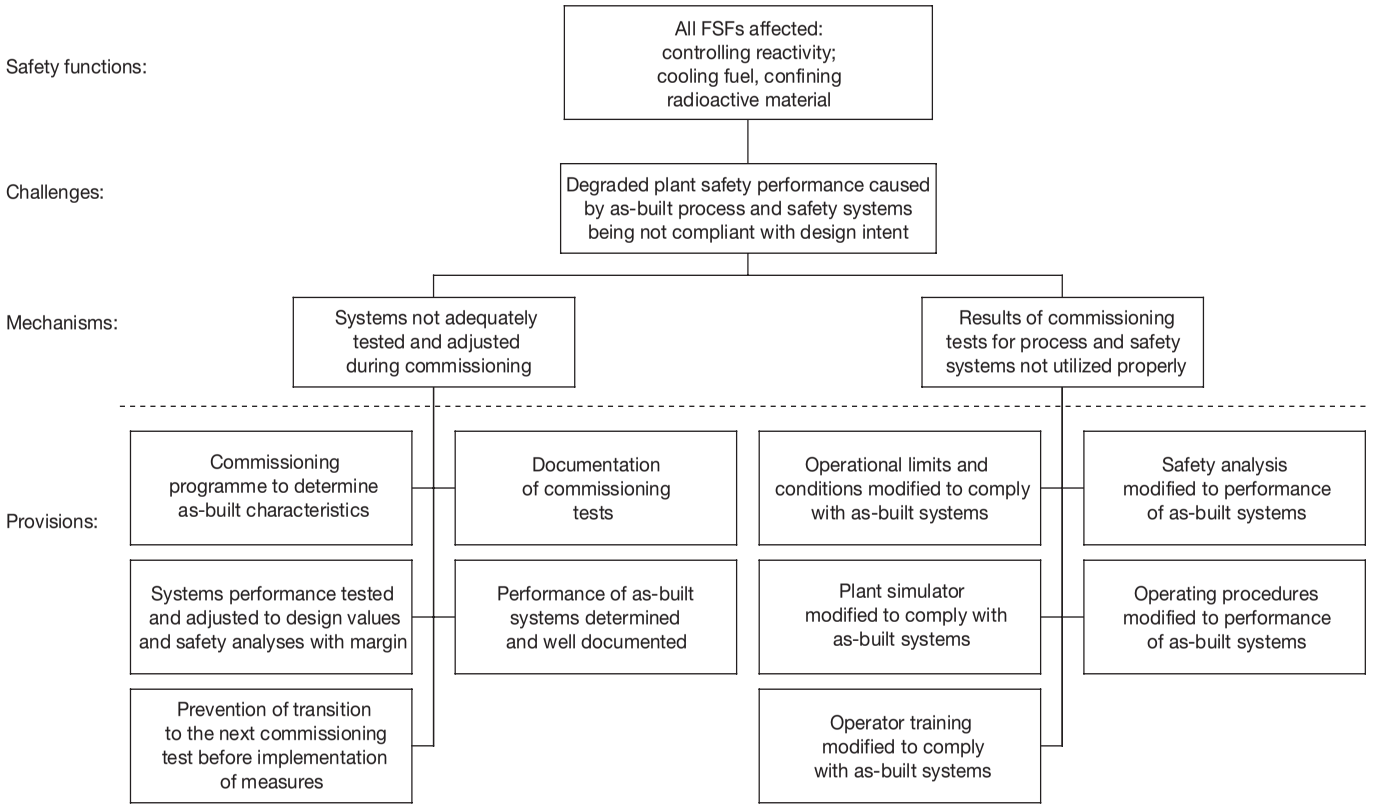


FIG. 61. Objective tree for Levels 1–4 of defence in depth. Safety principle (262): pre-operational adjustment of plant.

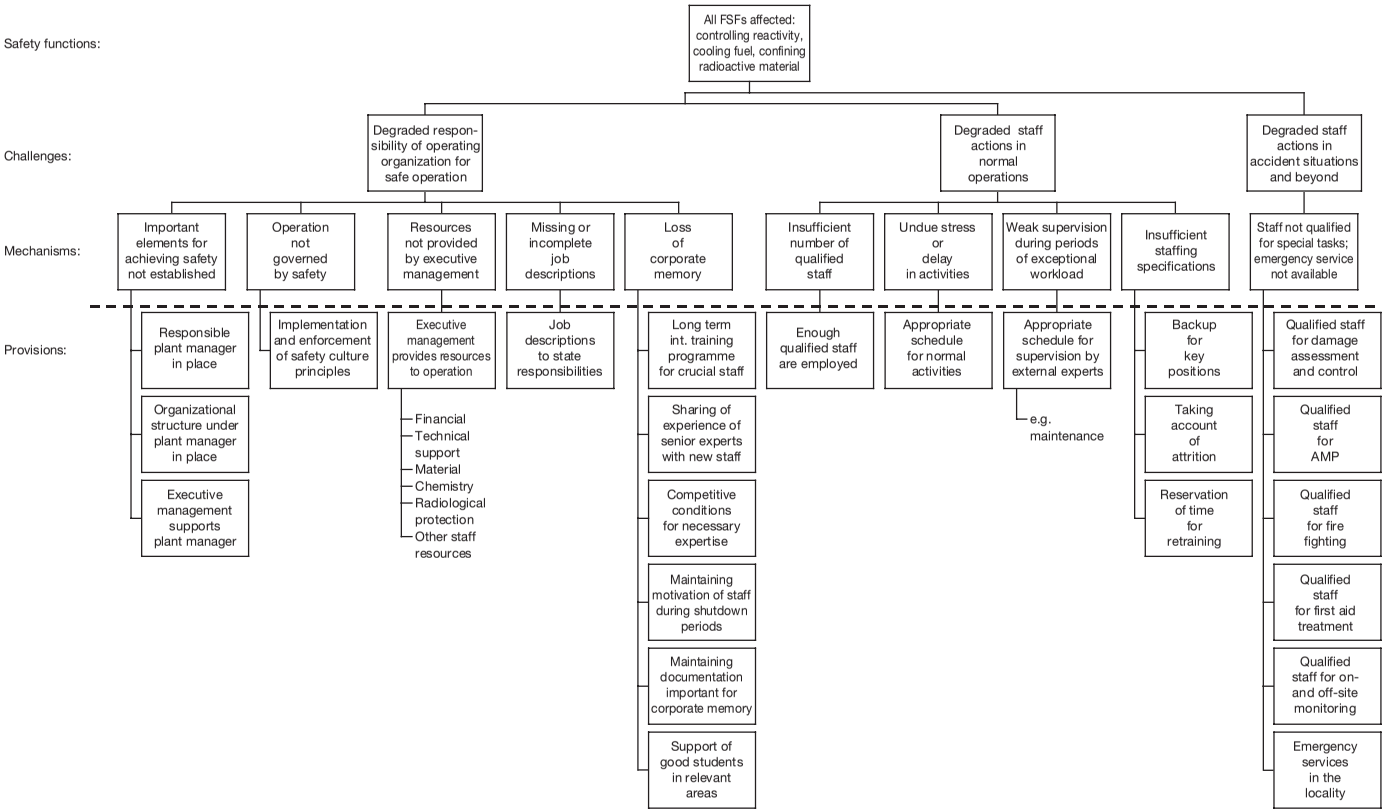


FIG. 62. Objective tree for Levels 1–4 of defence in depth (AMP, accident management programme). Safety principle (265): organization, responsibilities and staffing.

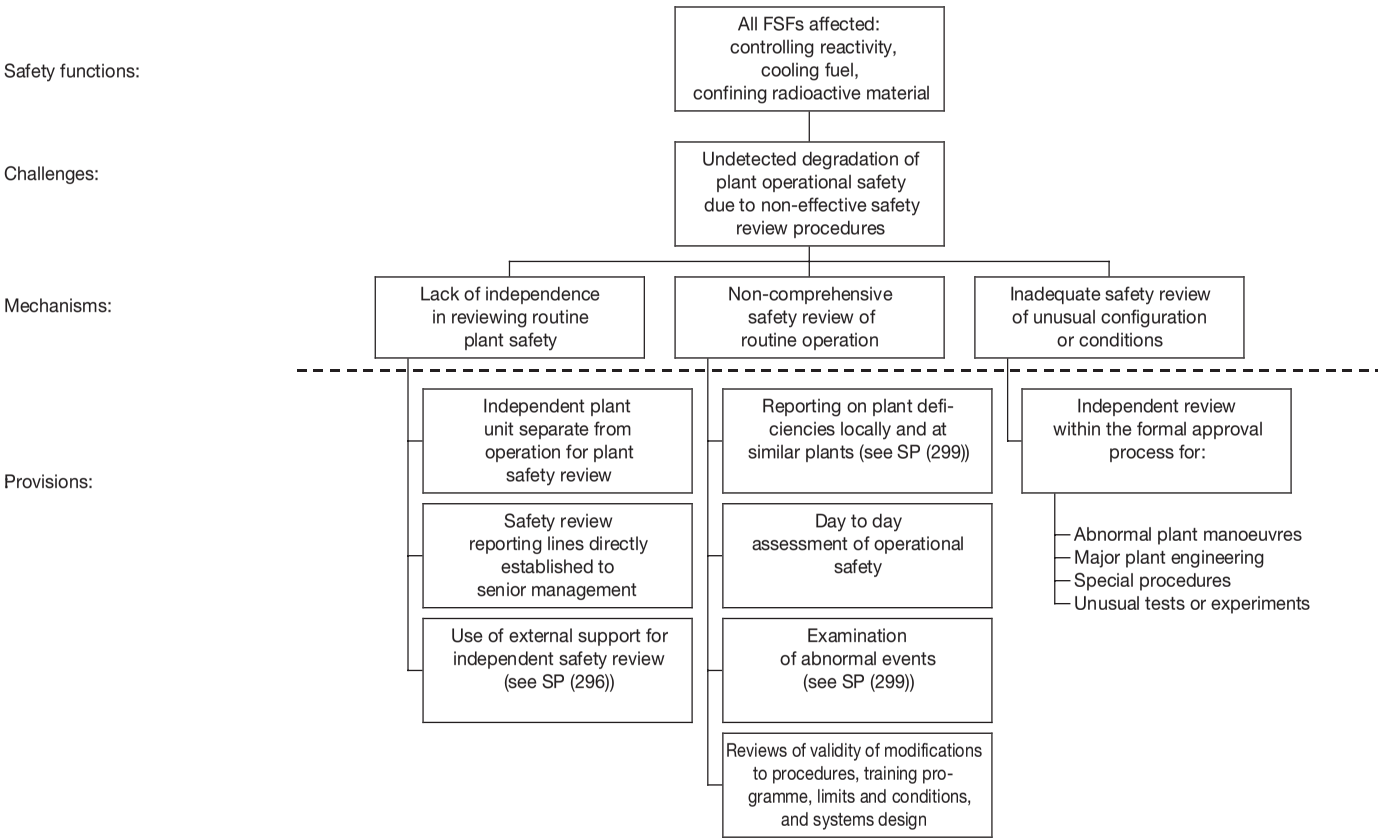


FIG. 63. Objective tree for Levels 1–4 of defence in depth. Safety principle (269): safety review procedures.

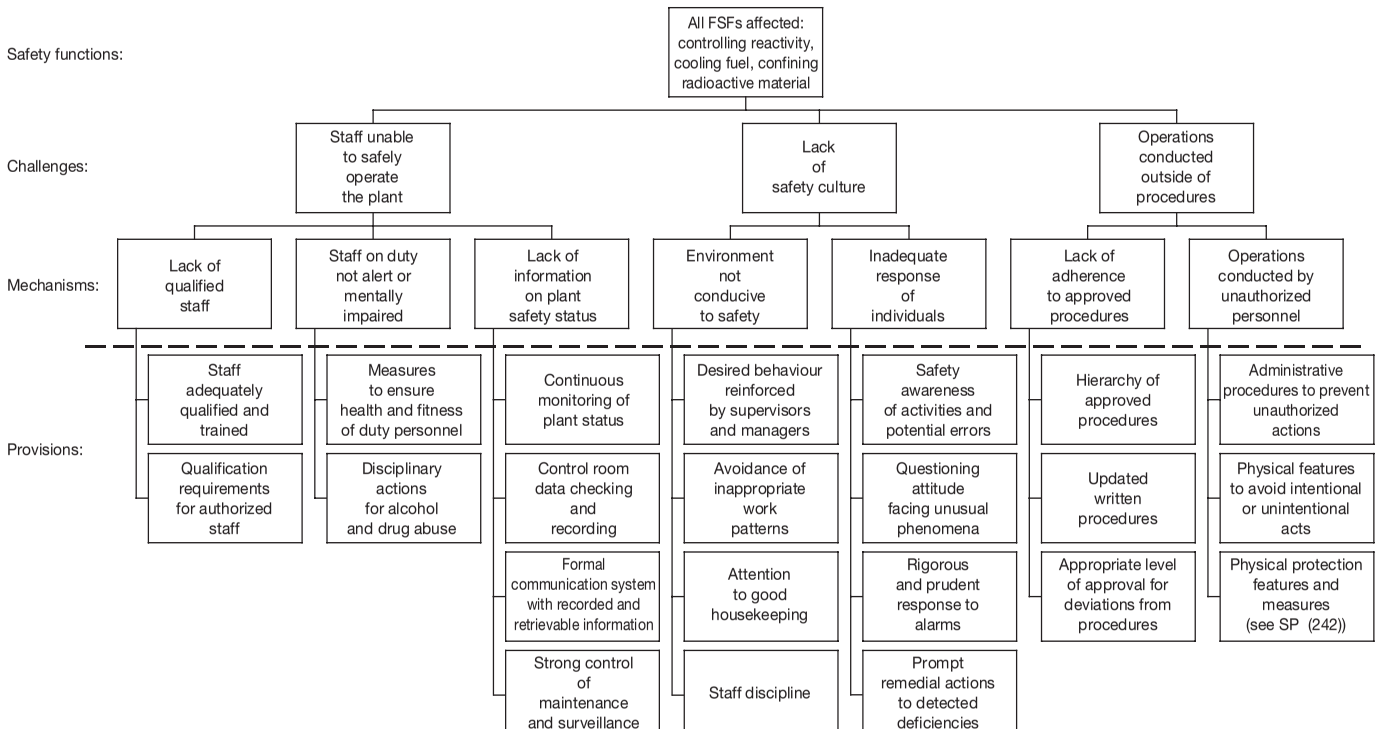


FIG. 64. Objective tree for Level 1 of defence in depth. Safety principle (272): conduct of operations.

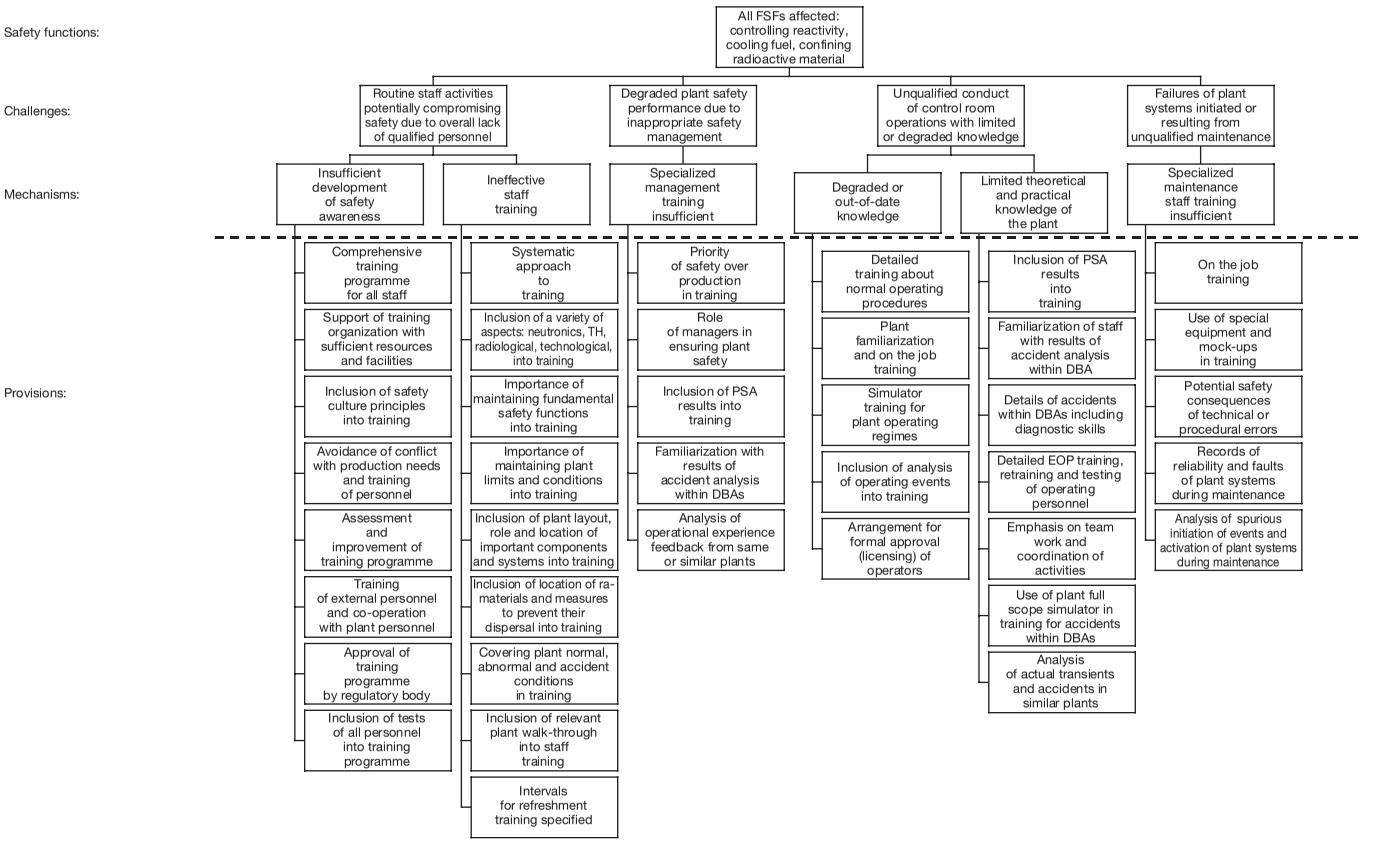


FIG. 65. Objective tree for Levels 1–3 of defence in depth (TH, thermohydraulic). Safety principle (278): training (see also SP (323)).

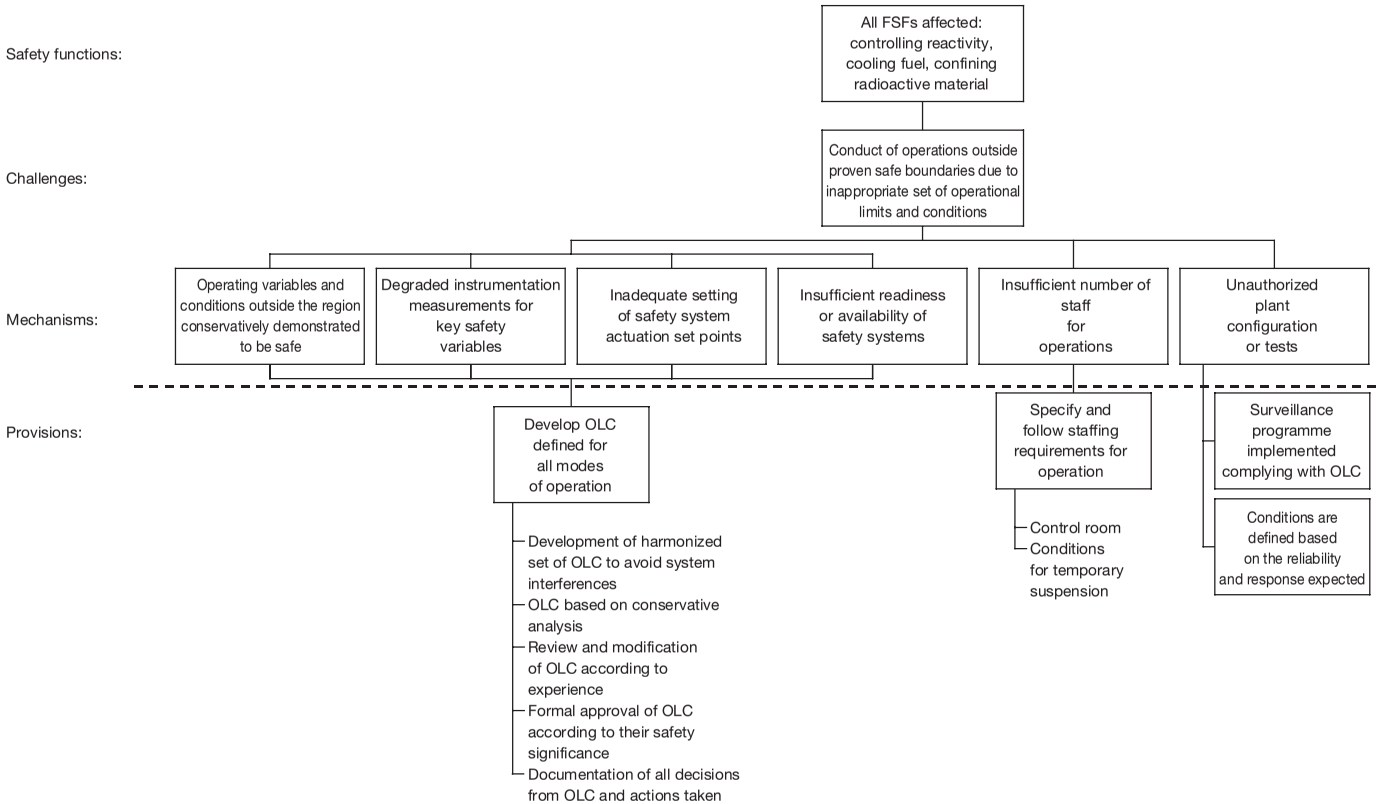


FIG. 66. Objective tree for Levels 1–3 of defence in depth (OLC, operational limits and conditions). Safety principle (284): operational limits and conditions.

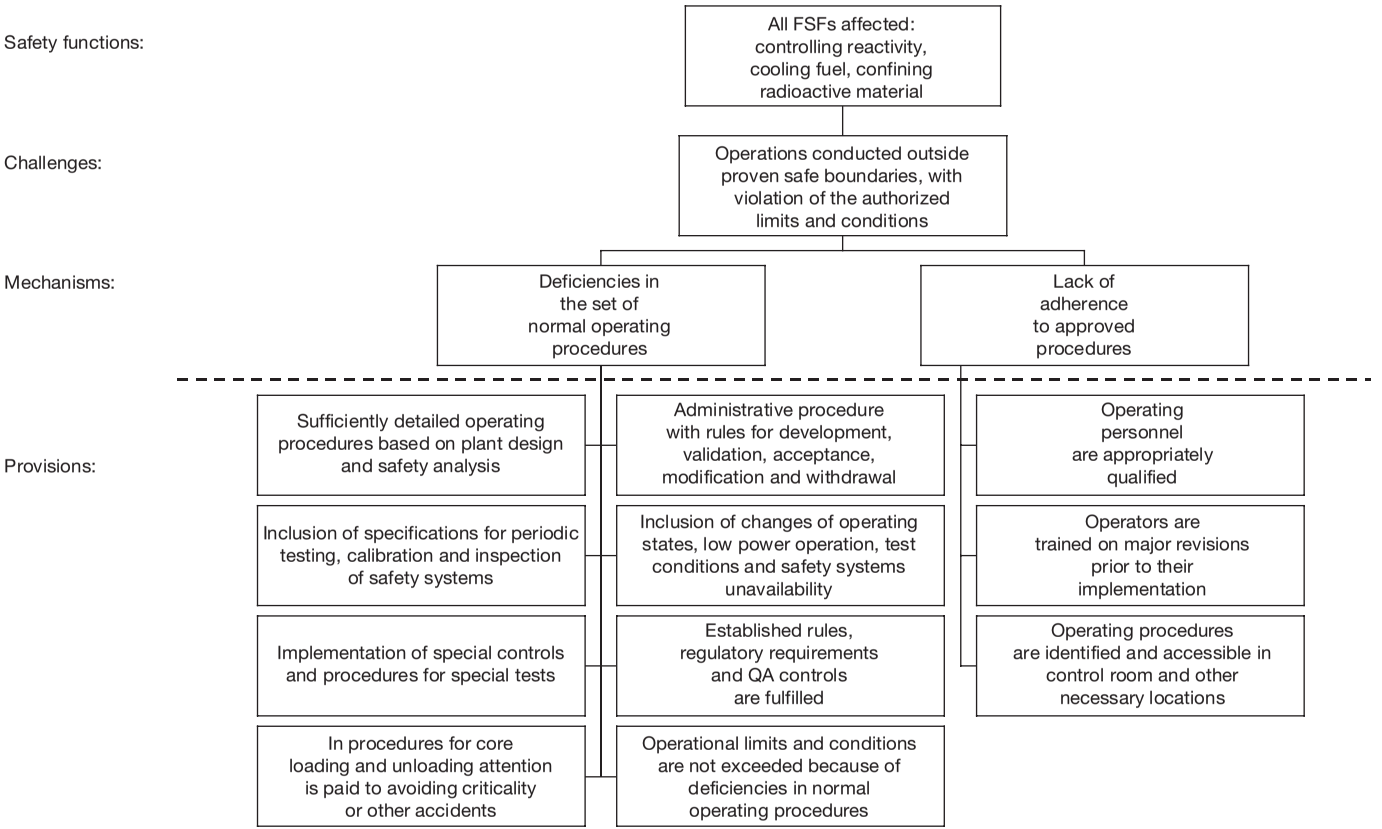


FIG. 67. Objective tree for Level 1 of defence in depth (QA, quality assurance). Safety principle (288): normal operating procedures.

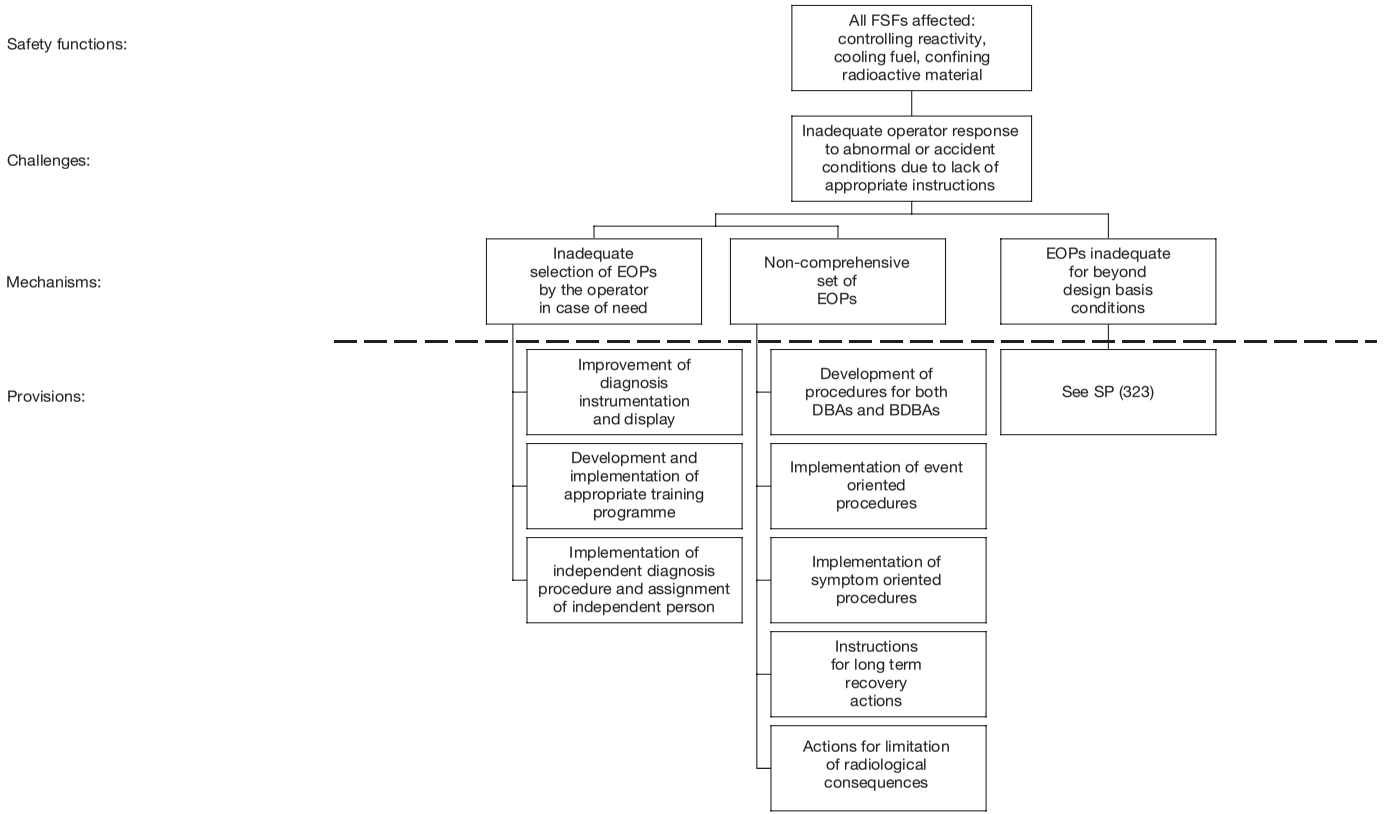


FIG. 68. Objective tree for Levels 2–4 of defence in depth. Safety principle (290): emergency operating procedures.

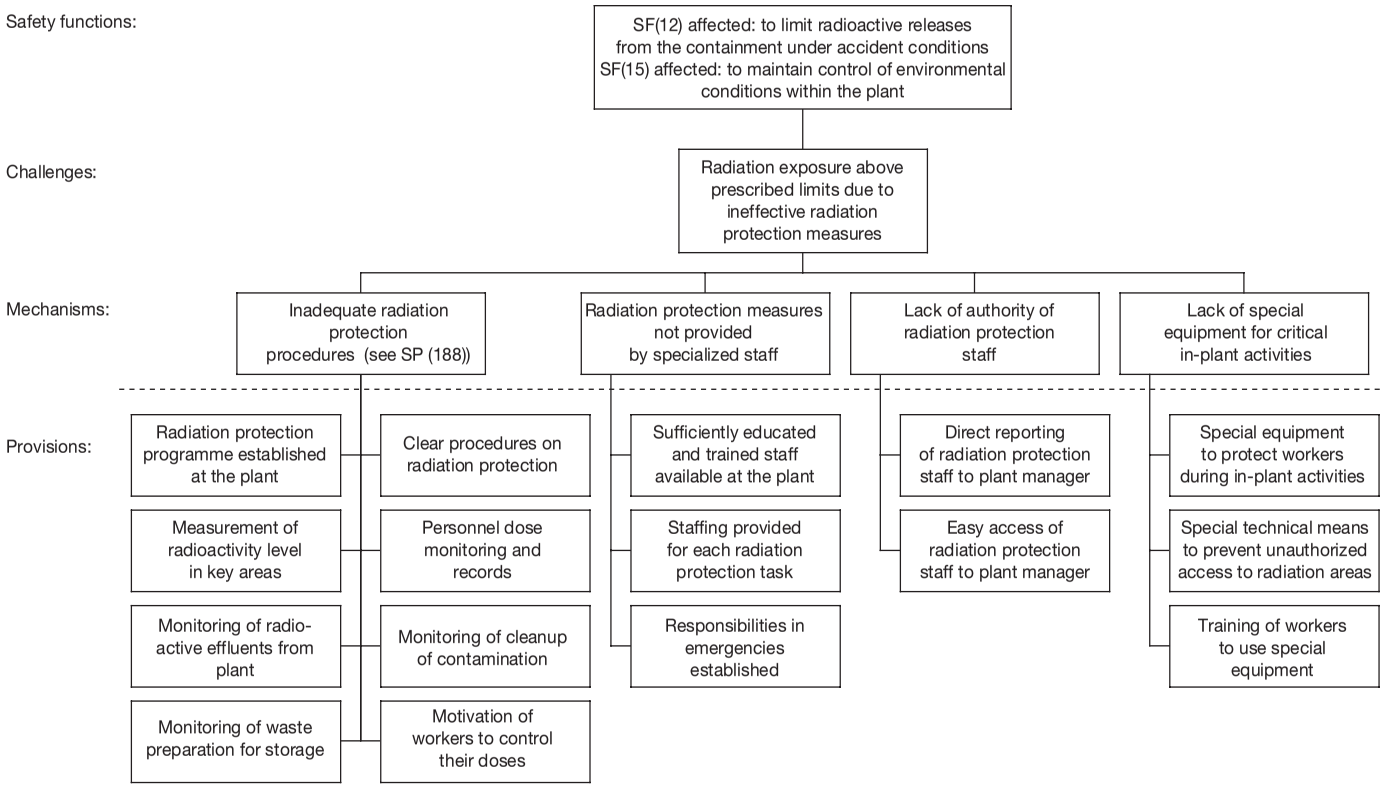


FIG. 69. Objective tree for Levels 1–4 of defence in depth. Safety principle (292): radiation protection procedures.

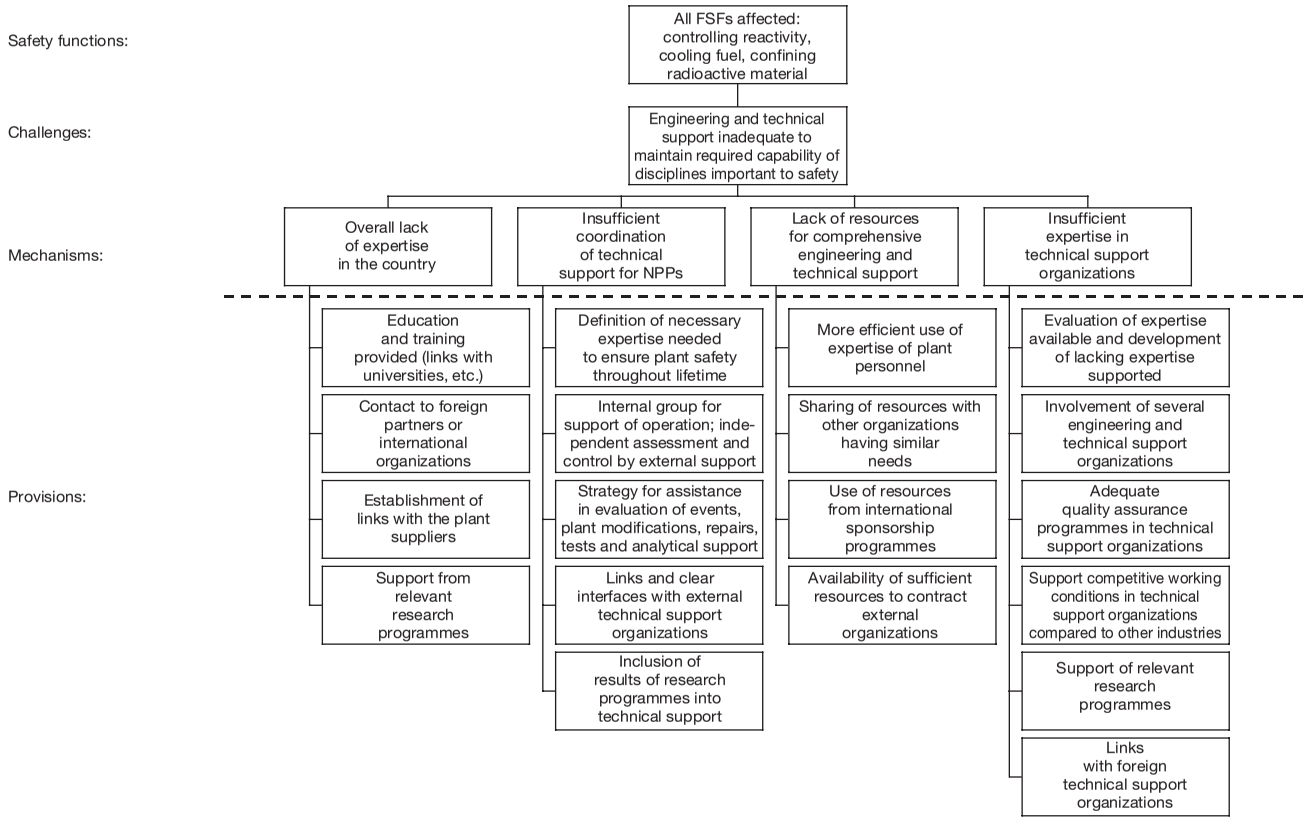


FIG. 70. Objective tree for Levels 1–4 of defence in depth (NPP, nuclear power plant). Safety principle (296): engineering and technical support of operations.

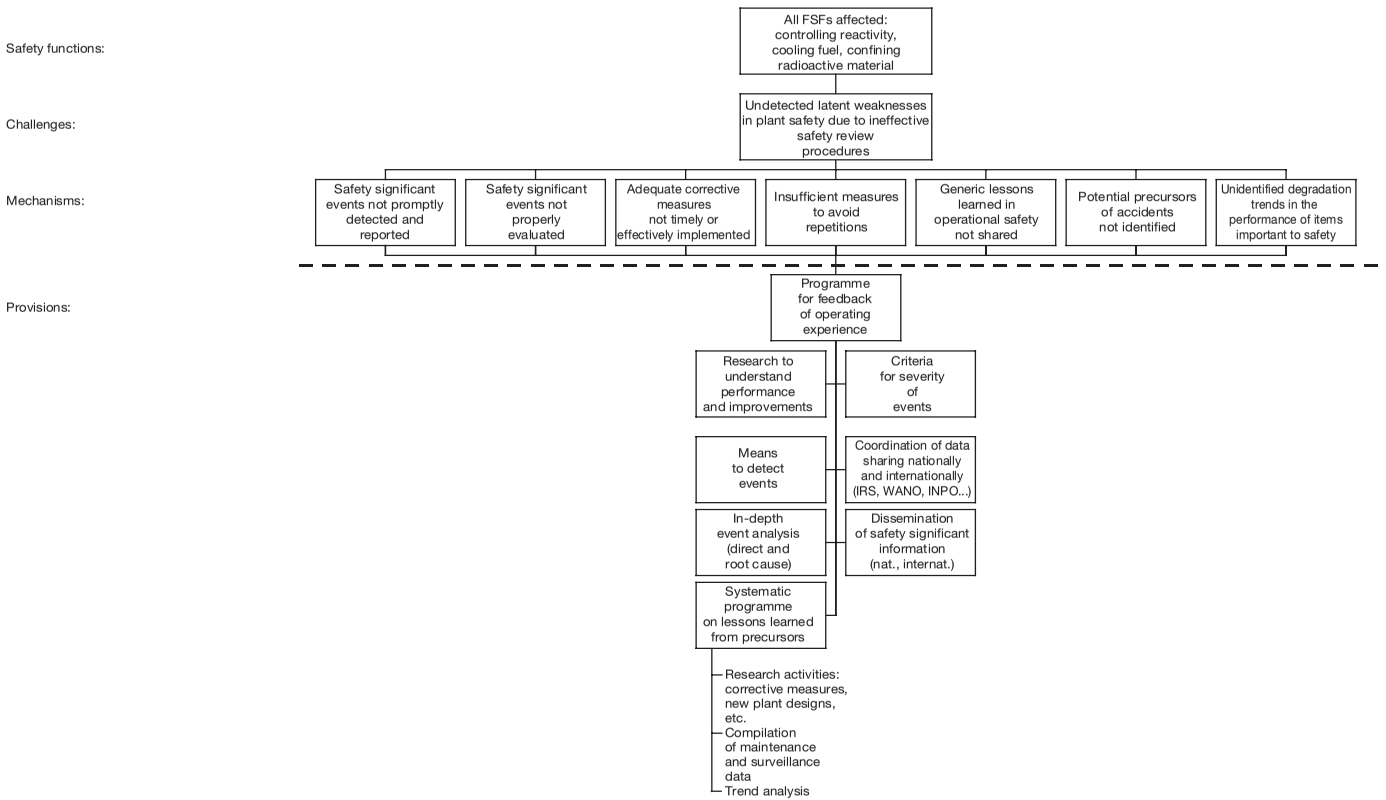


FIG. 71. Objective tree for Levels 1–4 of defence in depth (IRS, Incident Reporting System; WANO, World Association of Nuclear Operators; INPO, Institute of Nuclear Power Operations). Safety principle (299): feedback of operating experience.

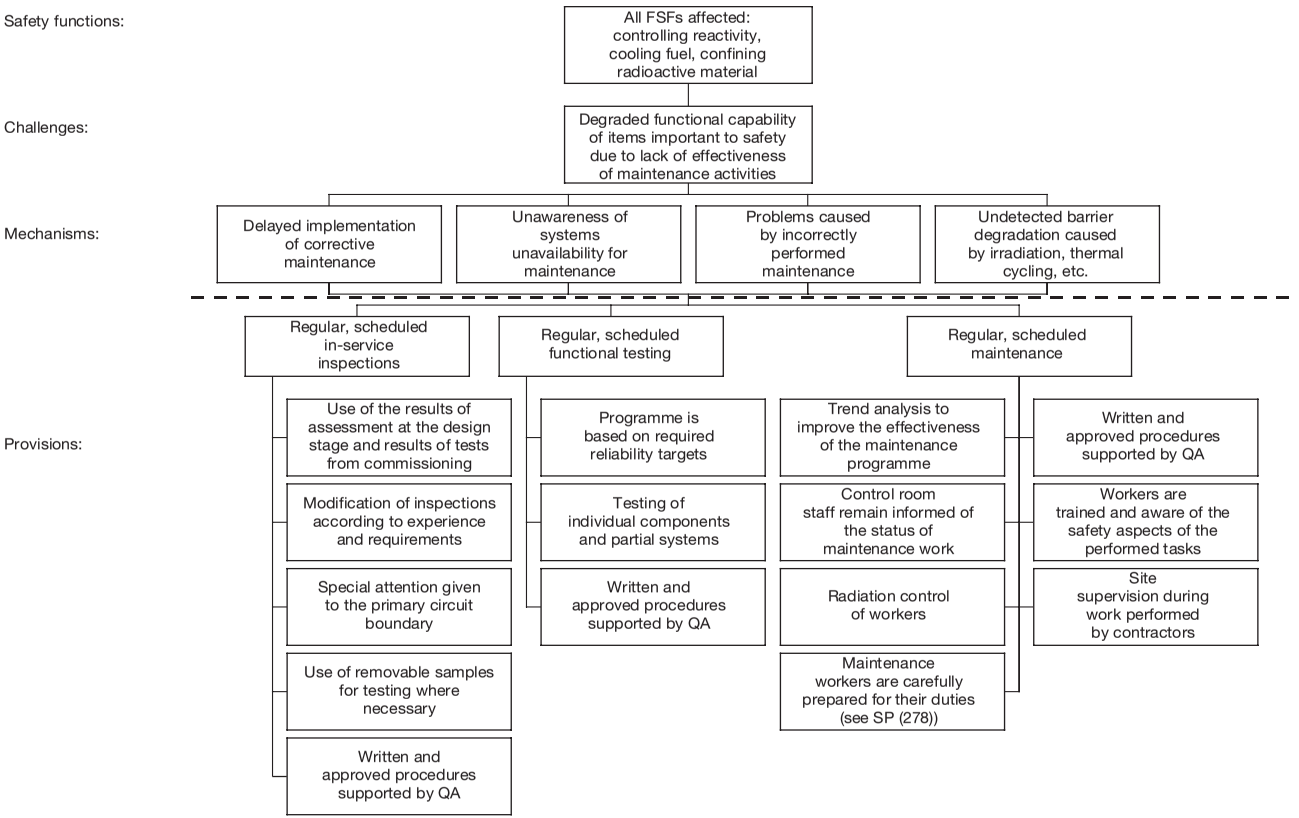


FIG. 72. Objective tree for Levels 1–4 of defence in depth (QA, quality assurance). Safety principle (305): maintenance, testing and inspection.

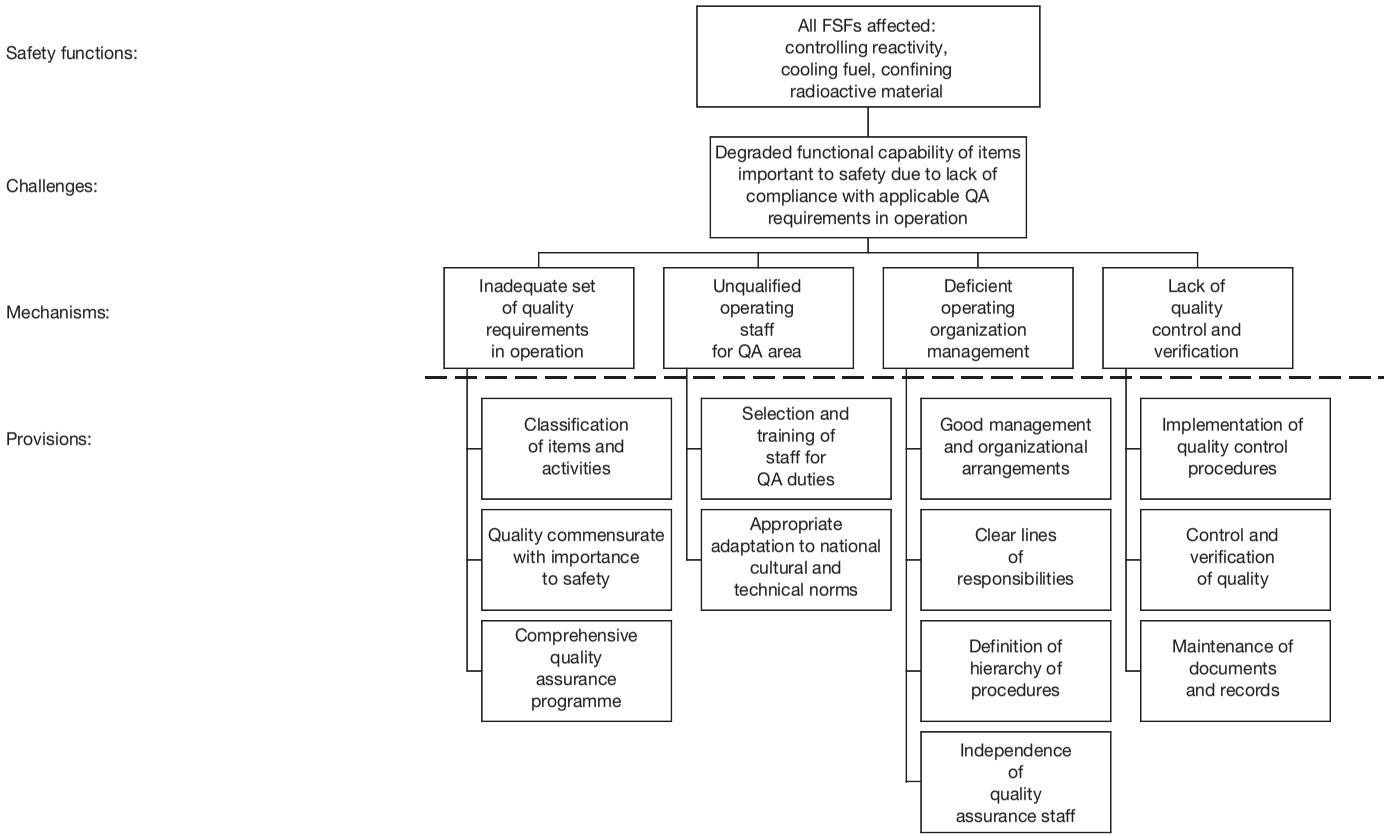


FIG. 73. Objective tree for Levels 1–4 of defence in depth (QA, quality assurance). Safety principle (312): quality assurance in operation.

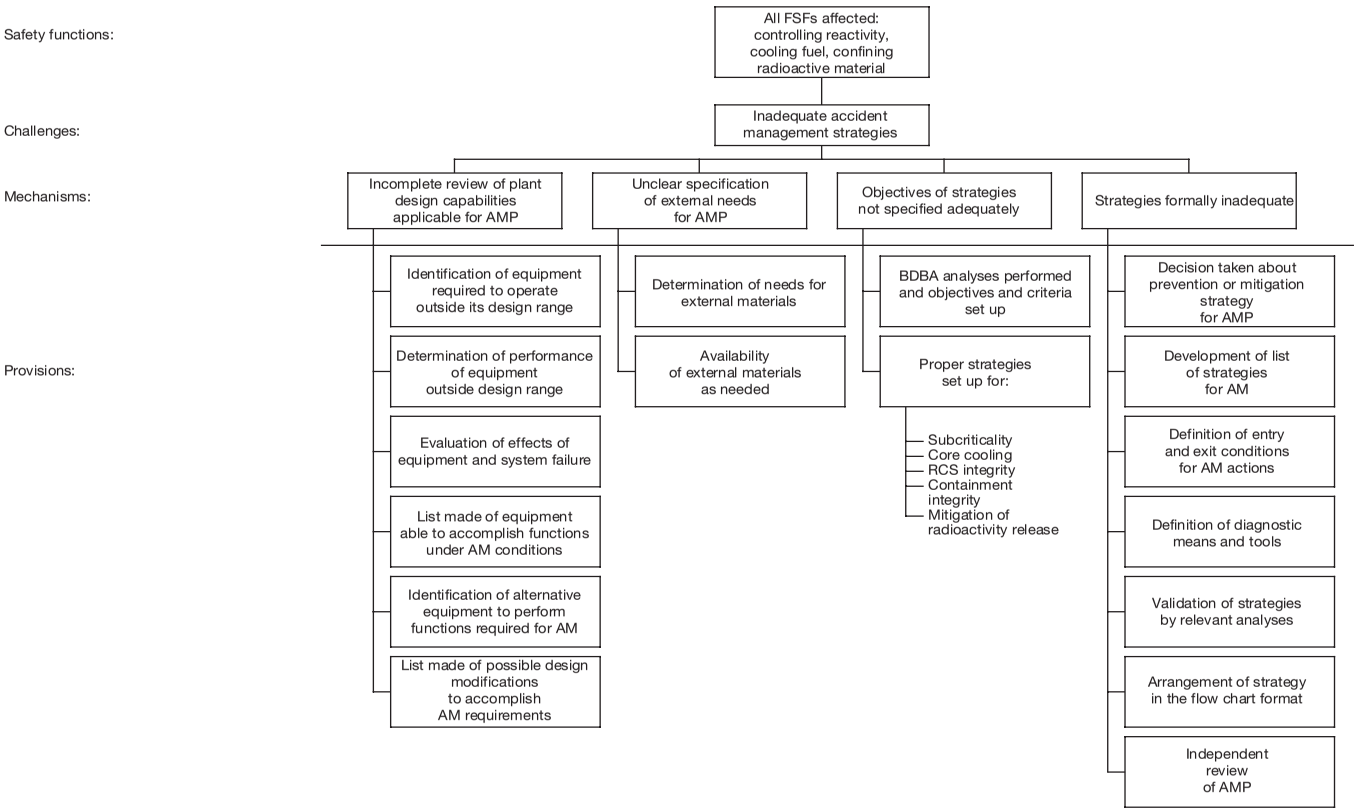


FIG. 74. Objective tree for Level 4 of defence in depth (AMP, accident management programme; AM, accident management; RCS, reactor coolant system). Safety principle (318): strategy for accident management.

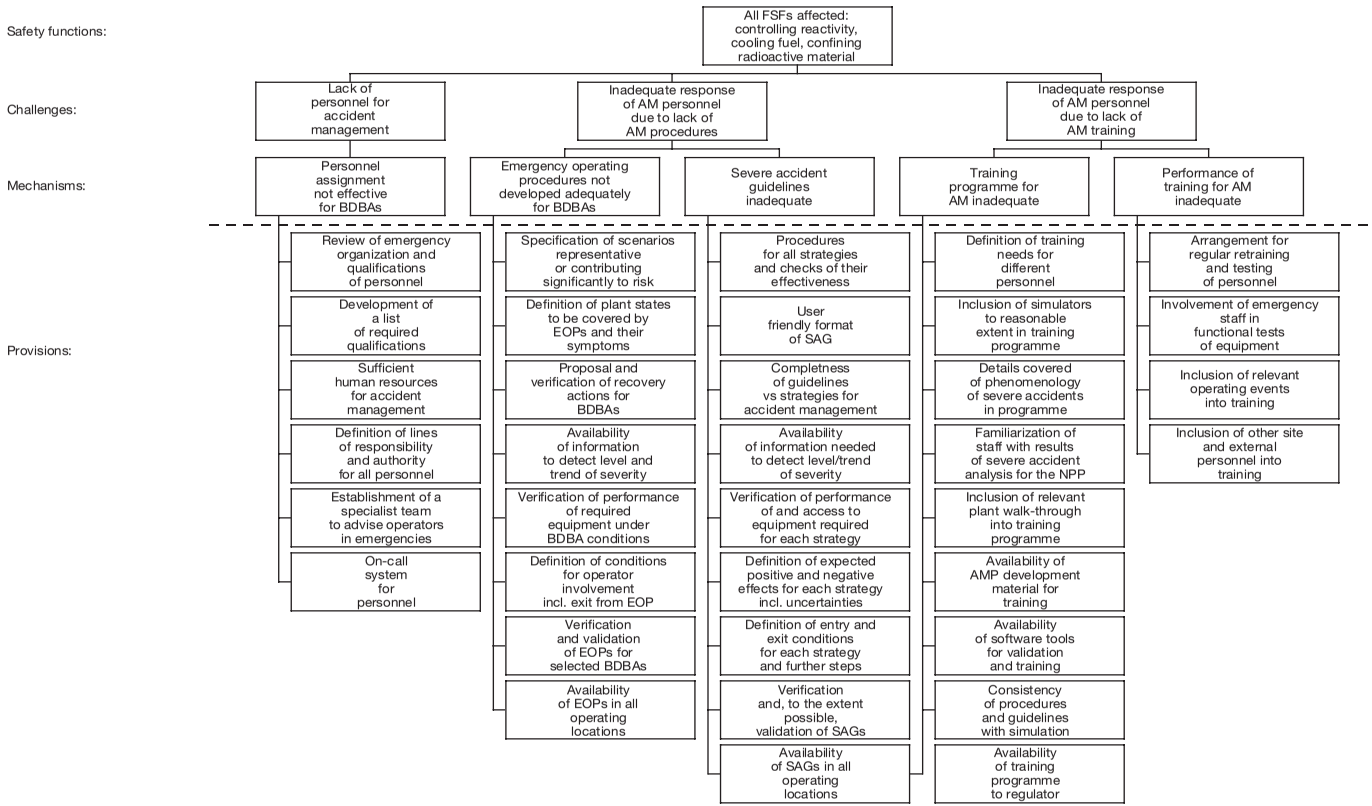


FIG. 75. Objective tree for Level 4 of defence in depth (AM, accident management; AMP, accident management programme; SAG, severe accident guidelines; NPP, nuclear power plant). Safety principle (323): training and procedures for accident management.

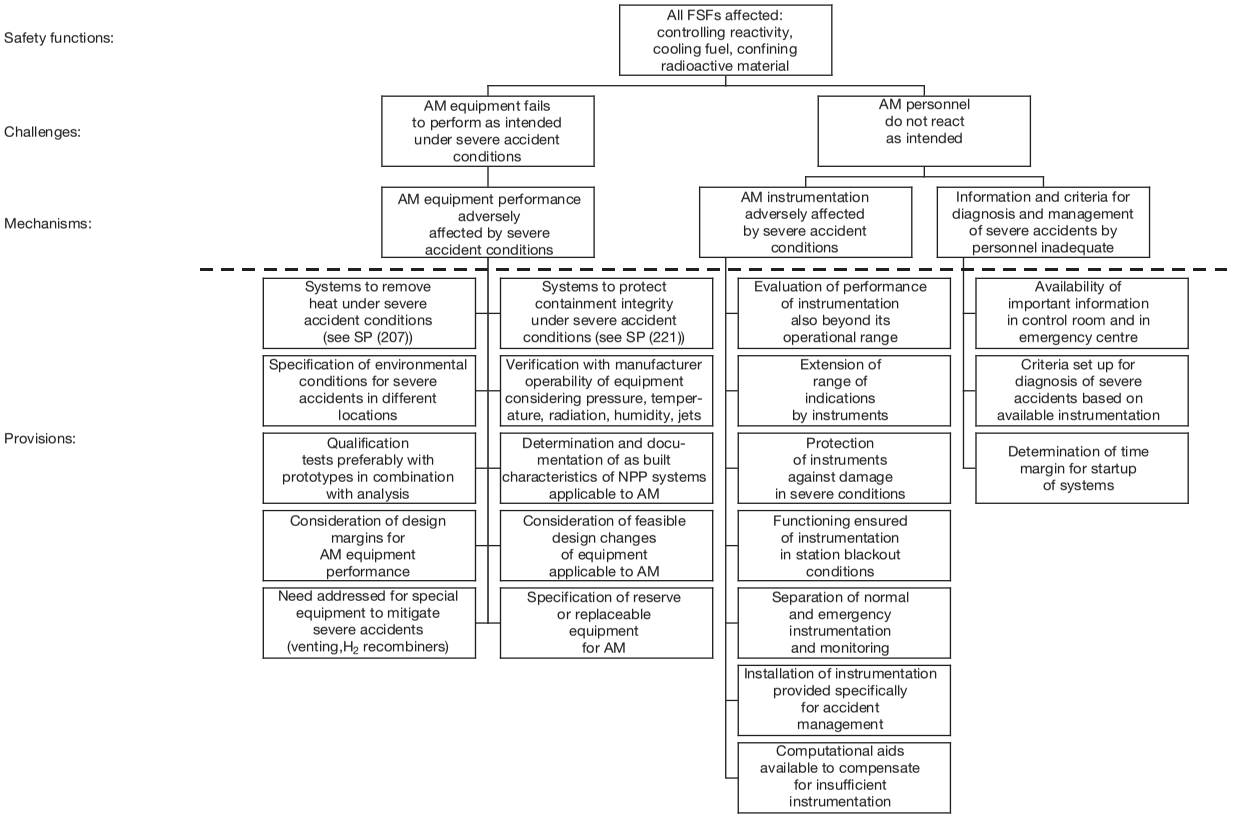


FIG. 76. Objective tree for Level 4 of defence in depth (AM, accident management; NPP, nuclear power plant). Safety principle (326): engineered features for accident management.

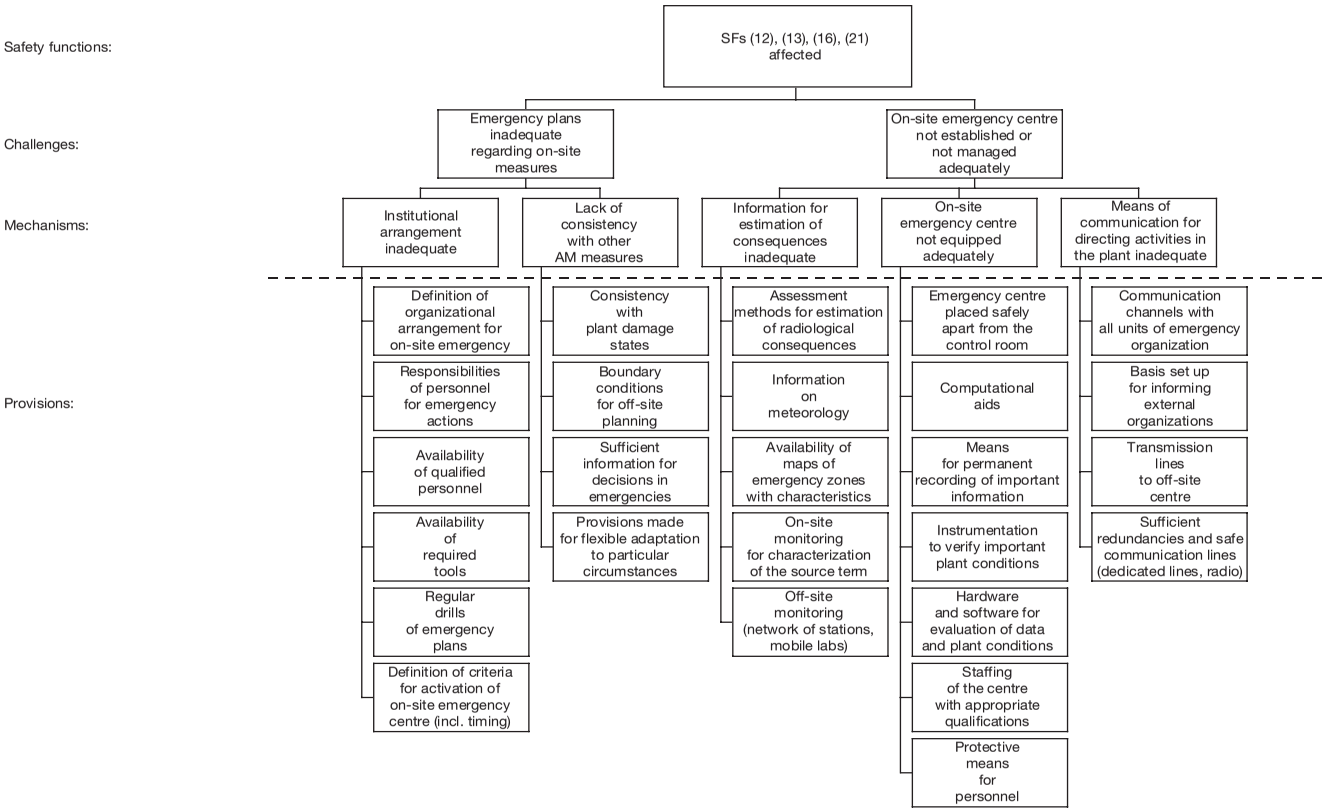


FIG. 77. Objective tree for Level 4 of defence in depth (AM, accident management). Safety principles: emergency plans (333), emergency response facilities (336).

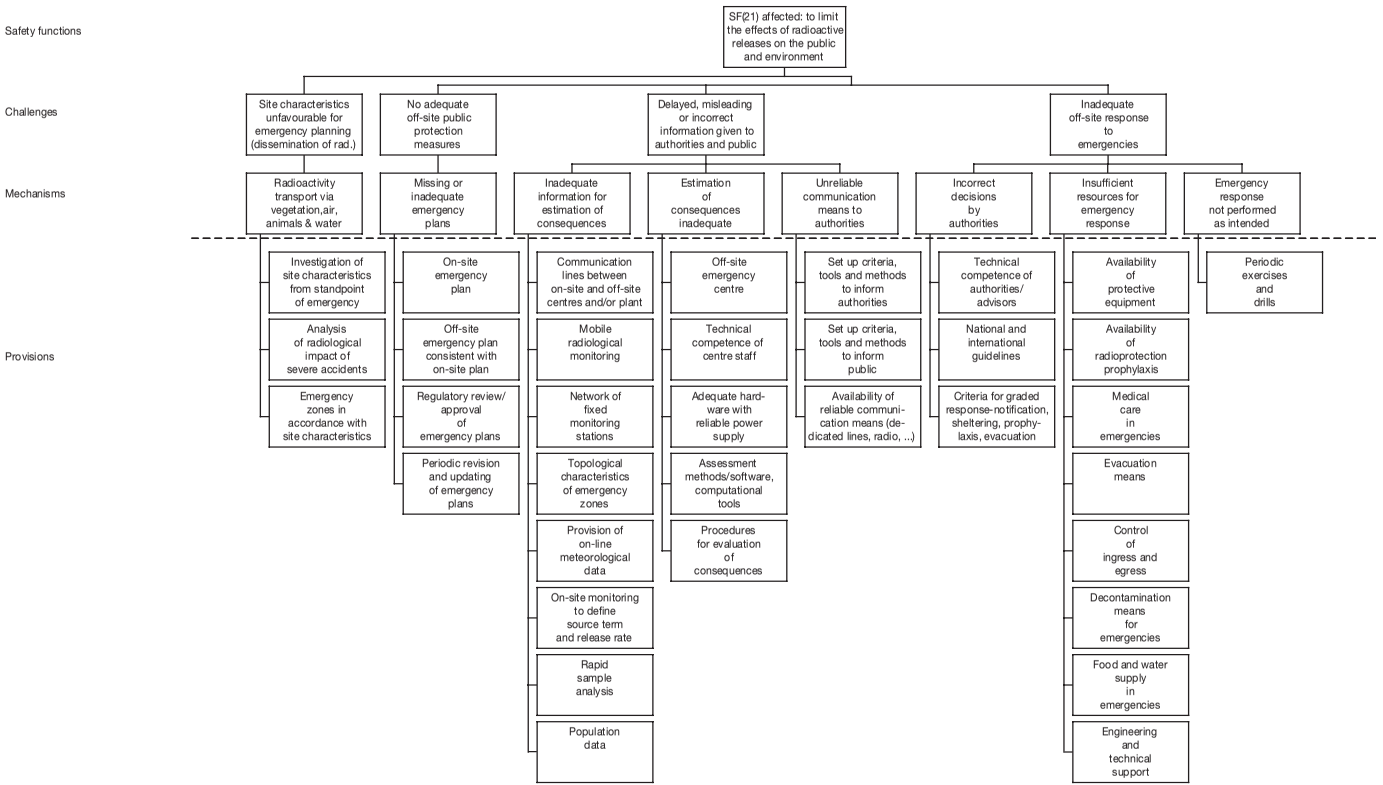


FIG. 78. Objective tree for Level 5 of defence in depth. Safety principles: radiological impact on the public and the local environment (138), feasibility of emergency plans (140), organization responsibilities and staffing (265), engineering and technical support of operations (296), emergency plans (333), emergency response facilities (336), assessment of accident consequences and radiological monitoring (339).

Appendix III

SCREENING OF DEFENCE IN DEPTH CAPABILITIES OF WWER 440/V213 REACTORS

The following partial test application was performed and provided by the Bohunice plant, Slovakia; it has not been reviewed by the IAEA.

III.1. OBJECTIVES OF THE REVIEW

A test application of the screening method has been performed by the staff of the Bohunice plant within the framework of the preparation of the safety upgrading programme for the V-2 plants. The Bohunice V-2 plant consists of two units equipped with WWER 440/V213 reactors. The units were commissioned in 1984 and 1985, respectively. A comprehensive description of the plant and its specific design features can be found in Ref. [7].

Since commissioning, the V-2 plants have been in stable routine operation. The operational record of the units is good. An upgrading programme for the plant has recently been developed. The safety concept (basic engineering) of the programme was at the time of the test application ready for regulatory review. The key features of the upgrading programme are:

(a) A safety upgrading based mostly on Ref. [8] was planned.
(b) Replacement of equipment for which no spare parts are available was planned.
(c) A power uprating of up to 107% of nominal power was considered.
(d) An extension of operational lifetime of up to 40 years was planned.

As the plant was in a preparatory phase for the upgrading programme, both the present status and some planned upgrading measures were considered in the review. An important objective was to verify that the upgrading programme covers all the safety issues identified.

III.2. SCOPE OF THE REVIEW

The scope of the review was limited to several selected safety principles related to Levels 3 and 4 of defence in the areas of siting and design, namely to the safety principles as follows:

— SP (142), ultimate heat sink provisions;
— SP (150), design management;
— SP (154), proven technology;
— SP (158), general basis for design;
— SP (168), automatic safety systems.

The plant Safety Analysis Report, updated in 1996, the operational documentation and the operational feedback database were used as background documents for the review. In addition, the results of a PSA Level 1 study developed for full power, low power and shutdown operational regimes were available for the review, as well as specific analyses of internal flooding and fires. Plant design documentation was also used to an appropriate extent. However, it should be emphasized that due to the limited scope and time available for the review, the objectives of the screening were more related to verification of the applicability of the approach than to evaluation of the safety status of the plant. Therefore, this section cannot be considered as a formal safety review of the plant.

III.3. COURSE OF THE REVIEW

As described in Sections 3 and 4 of the present publication, a bottom up approach was used for screening. Screening for each safety principle started from the bottom of the relevant objective tree. Implementation of provisions aimed at avoiding the occurrence of related mechanisms was evaluated as a first step. In a second step, conclusions were derived for all mechanisms based on the level of implementation of the provisions. Finally, during the third step, conclusions were formulated regarding sufficient prevention of challenges.

As stated above, the review was performed for five selected safety principles. However, with the aim of limiting the scope of the present report, only the review for SP (168) will be presented below as an example. The objective of this example is to illustrate the way and level of detail used for evaluation of the individual provisions.

III.4. EXAMPLE OF REVIEW FOR SAFETY PRINCIPLE (168) – AUTOMATIC SAFETY SYSTEMS

III.4.1. Review of provisions

III.4.1.1. Indication of operating status of safety systems

The operating status of safety systems is indicated in the main control room (MCR). The status of information and control (I&C) systems, in particular of the reactor trip system (RTS) and the emergency safety features actuation system (ESFAS), is indicated satisfactorily (several improvements have been implemented) given the technology used at the time of the construction of the plant. The status of all permissions disabling activation of the system is indicated, and an alarm on activation of one out of three measuring channels is provided. Loss of power supply to some parts of the system is indicated. Secondary devices (indicators and set point generators) have been improved to detect several kinds of failure. The alarm is activated on the front panel of the devices. The I&C shift foreman periodically checks the alarm status in the I&C compartments. Indication of the operating status in sufficient detail is included in the specification for the new reactor protection system (RPS), which will be installed as a part of the upgrading programme.

The status of electrical systems is also indicated satisfactorily except for the position of breakers. They can be set in a test position in which the component (pump) is not able to fulfil its SF. However, this position is not indicated in the MCR. That is why the test procedures are written in a very detailed way, ensuring that the component breaker remains in the operating position after the test. Independent checking of the status of the breakers is done in busbar cabinets during operation. Correction of this deficiency is included in the upgrading programme.

The status of the mechanical parts of the systems is indicated by means of valve positions and the indications of several other variables. The positions of manual valves are not detected and indicated. That is why periodic surveillance procedures are written in a detailed way that ensures proper valve (including manual) alignment after the test to ensure operability of the system. Independent and regular checking of valve positions, especially of manual valves, is done during operation.

III.4.1.2. Automatic self-testing of safety systems

A self-testing capability of the safety I&C equipment already existed in the original design. It is achieved by means of comparison of the prescribed status and the values obtained by measuring channels. Should the deviation

between the channels exceed a preset value, the alarm is activated in the MCR. However, some failures within the system could remain undetected. That is why the specifications for limits and conditions of the plant give time intervals for testing the operability of the systems. Detailed procedures are developed to test the systems and to detect any failure causing loss of an SF of the system. The PSA study of the systems showed that the existing combination of self-testing capability and periodic testing performed by the operators ensures sufficient reliability of the system.

Within the framework of the safety upgrading programme, replacement of safety I&C equipment (RTS and ESFAS) is being prepared. New up to date technology is assumed for implementation. The self-testing capability is one of the key features of the design of the new system.

A new self-testing capability is also being prepared for battery status evaluation, to detect a failure which could cause a battery to be unable to fulfil its design SF. This will be implemented within the upgrading programme.

III.4.1.3. Stringent requirements to preclude bypassing of safety systems

The only bypassing possibility exists in protection systems of the normal operation components. No bypassing capability exists in the design of the safety I&C systems. For the testing of the diesel generator loading sequencer the bypassing capability was implemented. It allows an automatic startup of the containment spray system pump during the test. A procedure and independent checking are used to control bypassing. In case of an omission, the bypass can cause early or spurious actuation of the pump, but successful startup of the pump cannot be endangered. However, the need for a reset capability for some ESFAS signals was identified in the course of development of the symptom based EOPs. This capability will be implemented in the new ESFAS.

A bypassing capability within the mechanical systems exists only for pilot valves of the pressurizer safety valves. Keys are used to block the pilot valve during the test or for isolation of a leaking valve. The usage of the keys is controlled by the test procedure and by the containment access administrative procedure.

III.4.1.4. Limiting conditions for operation with unavailable safety systems

Limits and conditions are developed according to NUREG-0452 (Rev. 3) [9] and to satisfy the requirements given in IAEA Safety Series No. 50-SG-O7[11].

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance of Nuclear Power Plants, Safety Series No. 50-SG-O7 (Rev. 1), IAEA, Vienna (1990).

Operability of the safety systems in specified operational modes is accordingly required. Operator actions are prescribed for operation when safety systems are unavailable. The time to accomplish the actions is specified. Allowed outage time for operation with an unavailable safety system is specified. The allowed outage time is specified on the basis of engineering judgement and taking into account the safety implications and ability to repair the unavailable component. An evaluation of the allowed outage time recently performed on the basis of a PSA showed that the specified time is very conservative and could be extended without increasing the risk.

III.4.1.5. Highly reliable/redundant initiation of safety systems

The existing RTS includes four levels of initiating signal. However, only one of them, first order reactor scram (AZ I) signals, is designed to perform the trip function. Some postulated initiating events are detected by two parameters, some by one parameter and some by using only third order reactor scram (AZ III) channels. The selection of initiation criteria does not guarantee fulfilment of the acceptance criteria when the single failure criterion is assumed.

Regarding the new RTS, the requirement exists to detect every postulated initiating event by two parameters. If two parameters are not available, the only parameter should be processed by two diverse logics and diverse sensors should be used in redundant trains.

For ESFAS, redundant initiation is used whenever practical. Safety functions not activated by two parameters should be performed by diverse safety systems independently of ESFAS.

The reliability requirements are defined according to the recommendations in INSAG-12 [2]. The Slovak regulations recommend failure rate targets for the reactor trip system of $<10^{-5}$ per demand and for the ESFAS system of $<10^{-3}$ per demand.

III.4.1.6. Adequate response time

The response times for all types of measuring channel of existing RPS (RTS and ESFAS) were measured in experiments. The results were used in modelling of system behaviour for safety analyses. The response time of one of the channels gave unsatisfactory results. That is why the set point of a particular variable was adjusted to compensate for inadequate response time and to meet the safety criteria. The logics of a particular signal will be modified in the new design of the RPS.

The experience with the Bohunice V-1 (two older V230 units at the same site) upgrading programme shows that even damping and hysteresis of existing electromechanical devices should be carefully evaluated. Appropriate measures should be implemented into a new technology. All these aspects have been taken into account in the V-2 upgrading programme.

III.4.1.7. Consideration of failures of safety systems in emergency operating procedures

When entering EOPs, operators are required to perform immediate actions to ensure basic conditions for successful implementation of the procedures. Afterwards they check for the symptoms of emergency conditions. Should emergency conditions be diagnosed, automatic actions are verified. This means that the safety system performance is checked. Any deviation in safety system performance is corrected manually.

The symptom based EOPs are written in a two column format. The left hand column provides an operator action and an expected plant response to the action. The right hand column is called 'Response Not Obtained' (RNO). The RNO column is used for an operator contingency action in case of a failure of the left hand column action (the operator could not perform the prescribed action or the plant response to the operator action was not as expected). This is systematically done throughout the procedure. A best estimate approach is used in analyses to support EOPs. Design basis accidents and BDBAs are covered by EOPs up to the significant core damage level. Possible failures of safety, safety related, support and normal operation systems and items are considered. The validation process for EOPs also considers validation of RNO operator actions. Emergency operating procedures are subject to the comprehensive maintenance programme. This means that the plant experience gained in training, analyses (both deterministic and probabilistic) and research, as well as the overall industry experience, are incorporated into the procedures.

III.4.1.8. Training of operators to react in case of failures in safety systems

Training sessions are designed to train the operators in usage of both columns of the EOPs. Operators are trained to react in the case of a failure of the system designed to cope with the accident, i.e. they are trained to react in the case of failures in the safety systems.

An additional diverse way to respond to failures in the safety systems is now described. An independent person (shift supervisor or safety engineer) periodically monitors the critical safety function (CSF) status trees. In the case of failures in safety systems and/or operator failures, significant deviation of

status of CSFs is expected. This deviation should be detected and appropriate function restoration procedures should be implemented to bring the plant back into safe conditions. The operators are trained in usage of the function restoration procedures.

III.4.1.9. Reliable electrical and ventilation support systems

The electrical power supply systems of all the safety systems are classified as safety system support systems in the upgrading programme. This means that the qualification criteria (e.g. environmental and seismic) used for the support systems are the same as those used for the safety systems themselves. Obsolete equipment (e.g. batteries and rechargers) was replaced by new equipment. The battery discharge time was increased to two hours. The trains of the supporting electrical systems are separated from each other and from the normal operation systems. Limited interconnections are allowed to ensure high reliability of the safety systems or plant availability. Detailed criteria for this kind of interconnection are being developed for the upgrading programme. A PSA was done for the electrical power supply systems. The high reliability of the systems was confirmed. However, some deficiencies were identified in the power supply for the feedwater valves. To improve the capability of the system to perform the SF, the power supply was rearranged from another train than that used in the original design.

The pending issues to be covered by the upgrading programme are completion of seismic qualification and improvements in fire resistance related to correcting the deficiencies identified in the separation of the cables of the safety trains.

III.4.1.10. Reliable instrumentation and control

The I&C systems designed for actuation of all safety systems are classified as safety systems. This means that the qualification criteria (e.g. environmental and seismic) applicable to safety systems are used. The decision was taken for several reasons to replace the existing RPS (RTS and ESFAS) with a new one. The safety concept (basic engineering) is complete. Detailed analyses of all the logics of the existing system and of the experience gained in the course of the EOP development, PSA studies, periodic safety analyses and operational experience were used in the development of the new concept. A preliminary PSA was done for the new configuration of the system. The results are satisfactory.

The heating, ventilation and air conditioning (HVAC) systems are designed as the normal operation systems. They will be requalified to safety

system support systems. Safety related functions will be identified and measures to satisfy criteria will be implemented (seismic resistance and emergency power supply).

III.4.1.11. Consideration of failures of support systems in emergency operating procedures

After entering EOPs the operators are required to take immediate steps to ensure that the basic conditions exist for successful implementation of the procedures. Then they check for symptoms of emergency conditions. Should emergency conditions be diagnosed, automatic actions should be verified. This means that the performance of the safety systems is checked, including the performance of the support systems. Any deviation in the performance of the support systems for the safety system should be corrected.

III.4.1.12. Training of operators to react in case of failures in support systems

Scenarios for training sessions are designed to train the operators in the usage of both columns of the EOPs. Operators are trained to react in the case of a failure of the system designed to deal with the accident. Thus they are trained to react in the case of failures in safety system support systems.

An additional diverse way to respond to failures in the support systems is the following. An independent person (a shift supervisor or safety engineer) periodically monitors the critical safety function status trees. In the case of failures in the safety system support systems the safety system also fails, and a significant deviation of status of the CSFs is expected. This deviation should be detected and appropriate function restoration procedures should be implemented to bring the plant back into safe conditions. The operators are trained in the usage of the function restoration procedures.

III.4.1.13. Environmental qualification of equipment

The safety I&C systems located inside the containment were environmentally qualified (see also SP (182)) for large break, loss of coolant accident conditions according to the original design. However, formal documentation from this qualification was not available. The parts of the system located inside the I&C rooms but outside the containment were not environmentally qualified. The valves of the safety systems located inside the containment were also not fully qualified. The plant launched a wide environmental qualification programme. In the first step the items to be environmentally qualified were identified. Environmental criteria were set up

for every room containing items to be qualified. Each item was evaluated according to these criteria. There were several types of conclusion. If the environmental qualification criteria were fully met, the item was accepted for future operation. If the criteria were not met, the item had to be either replaced by a new one or upgraded to meet the criteria. This activity started prior to development of the upgrading programme and the results are used in the upgrading programme.

III.4.1.14. Systems design according to the single failure criterion

The RTS is designed with (1 + 1) × 100% redundancy. There are three measuring channels within each redundancy for every parameter. A two out of three voting system is used to generate an output signal. Two parallel output relays are installed in every redundancy. Finally, there is a one out of two voting system of two redundancies. The system is designed to meet the single failure criterion. The only exception is the power supply system of control rod drives. There are four parallel lines with only one breaker in each of them.

The ESFAS system is designed with (1 + 2) × (1 + 1) × 100% redundancy. There are three measuring channels within each half-redundancy for every variable. A two out of three voting system is used to generate an output signal. Two parallel output relays are installed in every half-redundancy. Finally, there is a one out of two voting system of the two half-redundancies. Every redundancy is designed to actuate the safety features of a particular train in the safety systems. The system is designed to meet the single failure criterion.

The front line active safety systems are designed with (1 + 2) × 100% redundancy (high pressure safety injection system, low pressure safety injection system and containment spray system). The support systems (ESFAS, electrical emergency power supply system and service water system) are designed in the same manner. The passive safety system (hydro-accumulators) is designed with (2 + 2) × 50% redundancy. The secondary side active safety system (emergency feedwater system) and RTS are designed with (1 + 1) × 100% redundancy. In general, the single failure criterion is applied in the design of safety systems. However, the understanding and application of the single failure criterion has developed over the years. The Nuclear Regulatory Authority of the Slovak Republic issued a document with guidelines on the application of the single failure criterion. There is a project to apply this document to the upgrading programme. If necessary, several questions need to be clarified and items of equipment modified (e.g. the power supply system for the control rod drives and the steam generator fast acting isolation valves).

III.4.1.15. Preference for fail-safe designed systems

The fail-safe design of the reactor protection system means that in the case of its failure the reactor is tripped; spurious actuation of the system trips the reactor and puts it into safe conditions.

An essential part of the existing reactor trip system has been designed as a fail-safe system. Special measures were implemented to ensure reactor trip in the case of a failure causing loss of reactor trip capability. Nevertheless, several types of failure remain undetected. They cause a loss of individual measuring channel capability to generate a trip signal. Information and control personnel frequently check and test the system to ensure its high reliability.

The fail-safe feature is also specified as a requirement for the new RPS system. The possibility of undetectable failures will be significantly reduced.

However, it is more complicated to specify a safe action or position of the actuator in the case of an ESFAS. The steam line fast acting isolation valve (FAIV) is normally open and its safe action is to close in order to isolate the affected steam generator. Spurious actuation (closure) of the valve is the initiating event for a loss of secondary heat sink SF of a particular steam generator. It is a specific feature of the WWER 440 reactor that this function is important even in cold shutdown conditions, because steam generators are used as a secondary residual heat removal system. The ESFAS system is designed to keep the actuators in their installed positions in the case of a loss of power supply. Individual spurious actuations of some actions of the ESFAS system can occur due to some failures within the system and consequently some initiating events can take place. However, overall complex actuation of ESFAS actions is not expected in the case of a loss of power supply. On the other hand, the ESFAS system is not able to fulfil its SF in the case of an emergency and the operator is obliged to shut down the unit manually within the specified time. Thus, the ESFAS system is designed as a fail-safe system to the extent possible. The issue of undetected failures within the RTS is also applicable to the ESFAS system. Several types of failure remain undetected. They can cause the loss of individual measuring channel capability to activate an output signal. Information and control personnel frequently check and test the system to ensure its high reliability.

The fail-safe design principle will be applied in the new system to the extent possible. The possibility for undetectable failures will be significantly reduced.

III.4.1.16. Prevention of common cause failures in safety systems

There are two redundancies in the reactor trip system (see also SP (177)). They are independent of each other, of other safety systems and of other plant systems. Power supply sources of redundancies are also independent, as are the HVAC systems of redundancies. Redundant systems are located in physically separated compartments. However, sensors are not qualified for harsh environments. The original seismic qualification is not sufficient for newly obtained seismic input data.

ESFAS systems are installed in three redundancies. They are independent of each other, of the reactor protection system and of other plant systems. The power supply sources and HVAC systems of redundancies are independent. Redundancies are located in physically separated compartments. However, sensors are not qualified for harsh environments. Seismic qualification is not sufficient for new seismic input data. Two out of three of the redundancies can be affected by the consequences of high energy line breaks.

Another issue related to common cause failures is related to the initiation of specific events (see also SP (154), Proven technology, 'Revealed modes of failures', and SP (158), General basis for design, 'Development of list of DBAs', to form the design basis). For example, there was an operational event during operation at full power with a failure of one output ESFAS relay, which initiated actions corresponding to the main steam header break and closed the FAIVs of all the steam generators. The safety valves of the steam generators ensured the secondary heat sink function and the integrity of the steam generators. The reactor was tripped due to the high rate of main steam header pressure drop. This event was not considered in the original safety analysis report. Post-event analyses gave positive results; all safety criteria were met. However, this kind of event should be identified in the failure mode and the effect analysis, and in addition should be analysed within the scope of the DBAs. The design of the new ESFAS system must avoid this kind of failure.

III.4.1.17. Implementation of conservative design for performance of safety systems

At the system level all aspects of conservative design have already been considered. These include robustness of the items (components) of automatic safety systems and their sufficient capacity with adequate margins.

III.4.1.18. Higher priority given to safety functions

The priority of SFs over functions of normal operation was implemented in the original design of automatic safety systems. However, due to the new safety classification of functions and systems, some deficiencies were identified. Prioritization of SFs was identified as a new issue, which is to be ensured within the ESFAS system itself. Both types of priority will be considered in the upgrading programme.

The priority of automatic actions over manual operator actions was ensured in the original design. In the course of development of the new symptom based EOPs some operator actions were identified as significant. An example is the reduction of safety injection flow; the operator cannot take this action in the wide range of pressure below 8.3 MPa and temperature above 180°C. The safety signal reset capability is to be implemented when justified.

III.4.1.19. Isolation of process and safety systems

The original automatic safety systems are separated from normal operation systems. There are special sensors available for the reactor trip system, the ESFAS system, the normal operation control systems, the analog indicators in the main control room and the process information system. A common part of the sensors is an instrumentation line of particular redundancy. This is a very good solution from the point of view of safety. The disadvantages of this design are the large number of detectors and the high maintenance costs. These issues have become more important, as due to requirements regarding environmental qualification all safety sensors have to be replaced by new ones. The only detectors commonly shared by safety and normal operation systems are neutron flux power range ex-core detectors. The signals of these detectors from safety and normal operation systems are properly isolated.

Regarding the new design of safety systems it is proposed to reduce significantly the number of sensors and to allow multipurpose usage of sensors. An additional reduction of sensors will be achieved by integration of the reactor trip and ESFAS systems. Proven isolation devices will be used for the isolation of process systems from safety systems.

III.5. REVIEW OF MECHANISMS

III.5.1. Unavailability of safety systems during previous operation

All provisions are adequately implemented in existing systems. The quality of these provisions corresponds to the technology level used at the time of their construction. A combination of implemented provisions and checks by personnel in the field ensure satisfactory reliability of the system.

All provisions will also be implemented in the new system; however, with higher quality. A justified RESET capability will be implemented.

III.5.2. Failure of safety systems to react on demand

Selection of initiation criteria does not always guarantee fulfilment of acceptance criteria when the single failure criterion is assumed. The response time became adequate after an adjustment was made to the system. Emergency operating procedures and operator training are satisfactory regarding consideration of failures in the safety systems. Diverse initiation criteria will be implemented in the new reactor trip system.

III.5.3. Failure of safety systems due to failure of supporting systems

The supporting electrical systems are reliable. The supporting ventilation systems will be improved within the upgrading programme. Emergency operating procedures and operator training are satisfactory in the case of failures in the supporting systems to the safety system.

III.5.4. Degraded performance of safety system due to harsh operating environment

An environmental qualification programme was started several years ago. A list of equipment to be replaced and a list of equipment to be requalified have been developed. Measures will be implemented within the upgrading programme. Supporting ventilation systems will also be improved within the upgrading programme.

III.5.5. Inadequate performance of safety systems

The single failure criterion is applied in the design of the reactor trip and ESFAS system. A weak point is the power supply system of the control rods. The new system will be designed to meet fully the criterion.

The fail-safe criterion is not fully implemented for the reactor trip system but will be implemented in the design of the new system. The ESFAS system is designed as fail-safe to the extent possible; the same principle will be applied to the new system.

III.5.6. Interference of process systems

Priority of SFs over normal operation and over operator actions was implemented in the original design and will also be implemented in the new design. RESET capabilities will be implemented to allow justified controlled operator actions. It is expected that the number of interconnections between safety and normal operation systems will be higher in the new systems. Proven isolation devices will be implemented to allay safety concerns.

III.6. REVIEW OF CHALLENGES

III.6.1. Degraded performance of fundamental safety functions due to inadequate response of automatic safety systems

A decision on replacement of the original automatic safety I&C systems by new ones has been made. Areas identified for improvement are the following:

— Operating status indication,
— Self-testing capability,
— Diversity of initiating criteria,
— Supporting ventilation systems,
— Seismic and environmental qualification of equipment,
— Single failure criterion application,
— Fail-safe principle,
— Controlled operator intervention.

Deficiencies identified in the original system will be resolved in the new system, and the challenges of degraded performance of FSFs due to no timely or inadequate response of the automatic safety systems will be eliminated.

III.7. RESULTS AND LESSONS LEARNED FROM THE REVIEW

The test application of the screening method demonstrated that the approach is based on sound concepts and can be effectively used in plants. It can be considered a good method for the periodic safety review. It can also be used in a limited scope for review of the plant quality assurance programme, evaluation of plant modifications and evaluation of events or precursors. Because of the wide scope of the aspects reviewed, the approach can effectively support the questioning attitude as part of the plant safety culture.

When the review is being performed as a self-assessment, the level of satisfaction heavily depends on the plant safety culture and the desire for improvement. In any case the approach helps in identifying missing or weak provisions. The understanding of the importance of the provisions and of the interactions among the provisions or mechanisms is improved because of the complexity of the approach and its visualization in the form of objective trees.

For the Bohunice plant, the results of the screening were found to be in compliance with the recommendations of Ref. [8] and with the plant findings. Appropriate measures are planned for implementation within the upgrading programme. This is an important conclusion of this screening from the plant perspective. Screening was a starting point for a deeper evaluation of the areas needing improvement within the development of the safety concept of the upgrading programme. The test application contributed to the comprehensiveness of the plant upgrading programme.

The application also contributed to improvements of the screening method. For example, inclusion in the approach of the following modifications was proposed:

(a) The provision 'Periodic surveillance testing and in-field audits of safety systems' should be added to prevent the mechanism 'Safety systems become unavailable during previous operation'.
(b) The provision 'Install reliable supporting electrical systems' was originally concentrated on electrical systems only. It was recommended that this should be made broader to assume all kinds of supporting systems, not only electrical ones. A typical additional supporting system is the ventilation system. The importance of this system was confirmed by available PSA studies.

Owing to the large number of provisions, mechanisms and challenges, some coding system would be helpful for practical reasons in full scope applications. The coding system can be developed in a future version of this approach. Development of the electronic version of this approach with links to

various supporting documents is recommended, to provide correct and complete information from original documents in support of appropriate evaluation of particular provisions. This should provide the user with an easy cross-checking capability for the evaluated provisions, mechanisms and challenges, to assist in ensuring the consistency and quality of the screening document. The system should be flexible, to allow the user to establish links with the existing plant documentation.

BLANK

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, International Atomic Energy Agency, Vienna (1999).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, International Atomic Energy Agency, Vienna (1996).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Operation, Safety Standards Series No. NS-R-2, IAEA, Vienna (2000).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Anticipated Transients without Scram for WWER Reactors, IAEA-EPB-WWER-12, Vienna (1999).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Basis and Design Features of WWER-440 Model 213 Nuclear Power Plants, IAEA-TECDOC-742, Vienna (1994).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Issues and the Ranking for WWER 440 Model 213 Nuclear Power Plants, IAEA-EPB-WWER-03, Vienna (1996).

[9] NUCLEAR REGULATORY COMMISSION, Standard Technical Specifications for Westinghouse Pressurized Water Reactors, Rep. NUREG-0452 Rev. 3, Office of Standards Development, Washington, DC.

BLANK

DEFINITIONS

accident. Any unintended event, including operating errors, equipment failures or other mishaps, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

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; and
— 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 nor lead to accident conditions.

beyond design basis accident. Accident conditions more severe than a design basis accident.

design basis. The range of conditions and events taken explicitly into account in the design of a facility, according to established criteria, such that the facility can withstand them without exceeding authorized limits by the planned operation of safety systems.

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.

initiating event. An identified event that leads to anticipated operational occurrences or accident conditions and challenges safety functions.

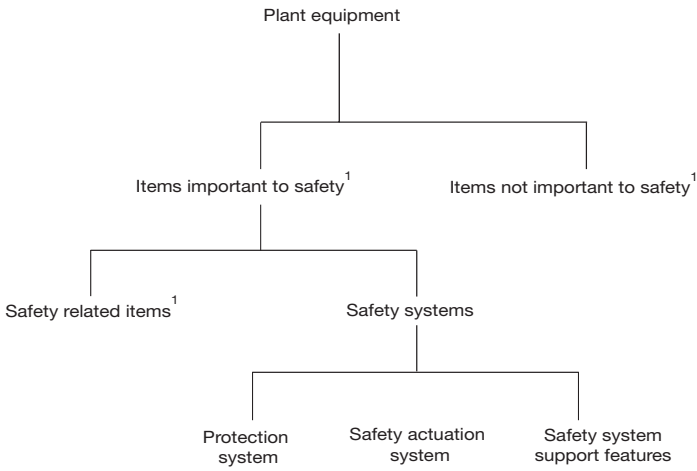
normal operation. Operation within specified operational limits and conditions. For a nuclear power plant, this includes starting, power operation, shutting down, shutdown, maintenance, testing and refuelling.

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 an authorized facility.

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

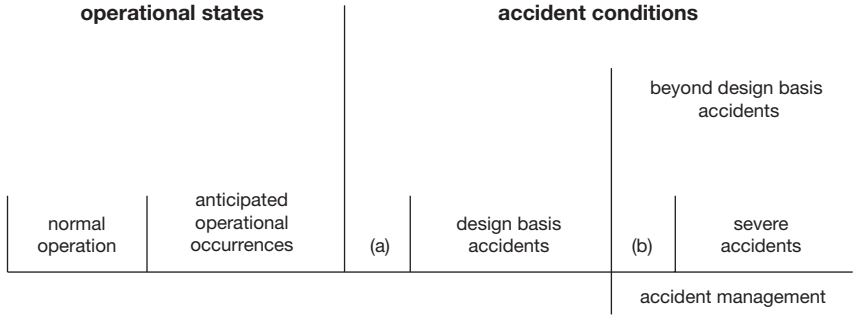
— Some States and organizations use the term operating conditions (for contrast with accident conditions) for this concept.

plant equipment.



[1] In this context, an 'item' is a structure, system or component.

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.

postulated initiating event. An event identified during design as capable of leading to anticipated operational occurrences or accident conditions. The primary causes of postulated initiating events may be credible equipment failures and operator errors (both within and external to the facility), and human induced or natural events.

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

validation. The process of determining whether a product or service is adequate to perform its intended function satisfactorily.

verification. The process of determining whether the quality or performance of a product or service is as stated, as intended or as required.

CONTRIBUTORS TO DRAFTING AND REVIEW

Aeberli, W.	Beznau NPP, Switzerland
Butcher, P.	AEA Technology, United Kingdom
Camargo, C.	Comissão Nacional de Energia Nuclear, Brazil
Fil, N.	Gidropress Experimental Design Bureau, Russian Federation
Höhn, J.	International Atomic Energy Agency
Lipár, M.	International Atomic Energy Agency
Mauersberger, H.	Nuclear&Technical Safety Services, Austria
Mišák, J.	International Atomic Energy Agency
Naňo, J.	NPP Bohunice, Slovakia
Powers, D.	Sandia National Laboratories, United States of America
Prior, R.	Nuclear Consultants International (PTY), South Africa
Tuomisto, H.	Fortum Engineering, Finland
Vayssier, G.L.C.M.	Nuclear Safety Consultancy, Netherlands
Vidard, M.	Electricité de France, France