UJV-14679
June 2018

Updating the Method of Objective Trees for Assessment of Defence in Depth for Nuclear Power Plants with Consideration of Recent Safety Requirements

Jozef Misak

Ústav jaderného výzkumu Řež a.s.

ACKNOWLEDGEMENTS

The report has been prepared in close cooperation and with significant contribution of the staff of engineering department of the Czech electric utility CEZ a.s. and of the Japan Nuclear Safety Institute (JANSI)

CONTENTS

Abstract 5

List of acronyms 6

1. INTRODUCTION 9
1.1. BACKGROUND 9
1.2. OBJECTIVE 11
1.3. SCOPE 12
1.4. STRUCTURE 12

2. THE CONCEPT OF DEFENCE IN DEPTH 14
2.1. GENERAL CONSIDERATIONS 14
2.2. FULFILMENT OF FUNDAMENTAL SAFETY FUNCTIONS. 18

3. APPROACH FOR MAKING AN INVENTORY OF THE DEFENCE IN DEPTH CAPABILITIES OF A PLANT 19
3.1. DESCRIPTION OF THE APPROACH 19
3.2. SPECIFICATION OF THE PROVISIONS 21
3.3. OBJECTIVE TREES 25

4. APPLICATIONS 30

5. CONCLUSIONS 33

Appendix I. FUNDAMENTAL SAFETY FUNCTIONS AND SAFETY FUNCTIONS 35

Appendix II OBJECTIVE TREES FOR ALL LEVELS OF DEFENCE IN DEPTH 38

ANNEX I. Summary of key lessons learned from the main reference documents used for updating the method 180

1. Modifications due to strengthening of IAEA Safety Requirements for siting 180

2. Modifications due to strengthening of IAEA Safety Requirements for design 180

3. Modifications due to strengthening of IAEA Safety Requirements for operation 181

4. Modifications due to post-Fukushima updating of WENRA reference levels for existing reactors 182

5. Modifications due to OECD/NEA lessons learned from Fukushima accident 191

6. Modifications due to recommendations from the post-Fukushima stress tests 198

8. Modifications due to recommendations from the post-Fukushima IAEA Expert Meetings 203

ANNEX II. Approach to demonstration of practical elimination of early or large releases 211

ANNEX III. Explanation and justification of modifications of objective trees in SR 46 216

REFERENCES 233

DEFINITIONS 234

ABSTRACT

This publication describes a screening method for assessment of comprehensiveness of defence in depth for both existing as well as for new nuclear power plants. The original method developed more than 10 years ago has been described in the IAEA Safety Report No. 46 - Assessment of defence in depth for nuclear power plants. Since development of the Safety Report significant enhancement in international safety requirements took place. For further use of the method it was necessary to update the method taking into account all new developments and also to improve its user friendliness considering experience from its previous applications.

The present publication describes an updated version of the method and presents the results of its overall improvements. For screening of comprehensiveness, usual five levels of the defence in depth are considered. For achieving safety objectives at each level, integrity of relevant physical barriers against releases of radioactivity shall be maintained which in turn require performance of fundamental safety functions. A set of challenges to performance of safety functions is identified, and several mechanisms leading to the challenges are specified. Finally, 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. The overview of all challenges, mechanisms and provisions for all levels of defence, is presented in the form of 'objective trees'.

The screening method is intended to be predominantly used by the operating organization. The method thus covers responsibility of the operating organization for all stages of the NPP life time from siting up to the end of operation as well as external factors important to safety which can be influenced by the operating organization.

LIST OF ACRONYMS

AC	Alternating Current
ALARA	As Low As Reasonably Achievable
AM	Accident Management
AOO	Anticipated Operational Occurrence
BDBA	Beyond Design Basis Accident
BWR	Boiling Water Reactor
CHF	Critical Heat Flux
DBA	Design Basis Accident
DC	Direct Current
DCH	Direct Containment Heating
DEC	Design Extension Condition
DEC-A	Design Extension Conditions without Fuel Melting
DEC-B	Design Extension Conditions with Fuel Melting
DiD	Defence in Depth
EC	European Commission
ECCS	Emergency Core Cooling System
ECR	Emergency Control Room
ENSREG	European Nuclear Safety Regulators Group
EOP	Emergency Operating Procedure
ESWS	Essential Service Water System
EU	European Union
FSF	Fundamental Safety Function
HPME	High Pressure Melt Ejection
HTS	Heat Transport System
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Advisory Group
IVR	In-Vessel Retention (of molten corium)
I&C	Instrumentation and Control
L	Level of Defence
LOCA	Loss of Coolant Accident

LWR	Light Water Reactor
MCR	Main Control Room
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
OECD	Organization for Economic Cooperation and Development
OT	Objective Tree
PCV	Primary Containment Vessel
PGA	Peak Ground Acceleration
PIE	Postulated Initiating Event
PSA	Probabilistic Safety Analysis
PSR	Periodic Safety Review
PTS	Pressurized Thermal Shock
PWR	Pressurized Water Reactor
QA	Quality Assurance
RCS	Reactor Coolant System
RHR	Residual Heat Removal
RL	Reference Level
RPV	Reactor Pressure Vessel
R&D	Research and Development
SAM	Severe Accident Management
SAMG	Severe Accident Management Guideline
SAR	Safety Analysis Report
SBO	Station Black-Out
SF	Safety Function
SFP	Spent Fuel Pool
SG	Steam Generator
SP	Safety Principle
SRS	Safety Report Series
SSC	System, Structure and Component
TSC	Technical Support Centre
TSO	Technical Support Organization
UHS	Ultimate Heat Sink

WENRA Western European Nuclear Regulators Association

1. INTRODUCTION

1.1. BACKGROUND

According to the IAEA Safety Glossary [1], defence in depth is "a hierarchical deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between a radiation source or radioactive materials and workers, members of the public or the environment, in operational states and, for some barriers, in accident conditions". Defence in depth is an overall safety philosophy that encompasses all safety activities, including siting, design, manufacture, construction, commissioning, operation and decommissioning of nuclear power plants (NPPs).

As confirmed recently by different forums, defence in depth based on multiple barriers and variety of means (provisions) to protect the barriers is an essential strategy to ensure nuclear safety for both existing and new NPPs. The safety provisions can be of different nature: organizational, behavioural and design measures, including properly selected site characteristics, inherent safety features, safety margins, active and passive systems, operating procedures and operator actions, more general organizational measures and safety culture aspects.

Defence in depth ensures that the fundamental safety functions (FSFs) are reliably achieved with sufficient margins to compensate for equipment failures and human errors. Should one level fail, the subsequent level comes into play.

For many years, defence in depth represents a focal point for IAEA safety related activities. The need for a practical tool aimed at facilitating assessment of comprehensiveness of defence in depth has been recognized by the IAEA at the end of 90's with the objective to contribute to more specific understanding of this very general term. All NPPs have physical barriers and means to protect the barriers, while their level of defence can be very different. It was also necessary to underline that the measures for protection of the barriers include much more than just NPP technological systems and procedures.

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 was available for assessing the importance of these measures, which vary in nature. Whilst progress has been made in this area through the use of probabilistic methods, the deterministic approach was primarily directed at evaluating design features only. Therefore, there was 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.

Among many IAEA documents related to defence in depth, there are two documents with special importance for the present publication. One of them is INSAG-12 (update of INSAG-3) - Basic Safety Principles for NPPs, published in 1999 [2], introducing the concept of basic safety principles (SPs), and Safety Reports Series No. 46 - Assessment of defence in depth for NPPs (SRS-46), published in early 2005 [3], which describes a practical screening method for assessing comprehensiveness of the defence in depth capabilities of a NPP (mainly of an existing plant), including both its design features and the operational measures taken to ensure safety. However, since development of SRS-46 during the period 1998-2004, significant enhancement in international safety requirements is including also enhancement of defence in depth took place both before, but in particular after the Fukushima accident. For further use of SRS-46, it was necessary to update the report by taking into account all new developments and also to improve its user friendliness considering experience with its previous applications. In particular, the following international documents were considered in updating the method of objective trees:

- Site Evaluation for Nuclear Installations, Specific Safety Requirements, NS-R-3, Rev. 1, IAEA, 2016 [4]
- Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1 Rev. 1, IAEA, 2016 [5]
- Safety of Nuclear Power Plants: Commissioning and Operation, Specific Safety Requirements, SSR-2/2, Rev. 1, IAEA, 2016 [6]
- IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA, 2013 [7]
- IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA, 2013 [8]
- WENRA Safety Reference Levels for Existing Reactors – Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident, September 2014 [9]
- Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Overview and Conclusions, ENSREG, April 2012 [10]
- Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Compilation of Recommendations and Suggestions from the Review of the European Stress Tests, ENSREG, July 2012 [11]

[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 completely or partially the mechanisms from occurring.

- Implementation of Defence in Depth at Nuclear Power Plants - Lessons Learnt from the Fukushima Daiichi Accident, OECD/ NEA No. 7248, 2016 [12]

Summary of key lessons learned from the above listed documents is presented in Annex I of this publication.

The present publication aims to update SRS-46 and presents the results of overall improvements of the methodology for screening comprehensiveness of the defence in depth at all levels of defence.

1.2. OBJECTIVE

The present publication describes an updated version of the 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 publication. 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' (OTs)[4].

The updated method described in this document is intended to be predominantly used by the operating organization, and therefore the provisions are focused on those which can be managed or at least influenced by the operating organization. The method covers responsibility of the operating organization for all stages of the NPP life time from siting up to the end of operation as well as external factors important to safety which can be to some extent influenced by the operating organization.

---

[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.

1.3. SCOPE

The assessment method that is presented in this publication is directly applicable to existing light water reactors (LWRs), 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 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 also 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 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

After this introduction, this publication has four other sections. In addition, there are two appendices and three annexes.

Section 2 addresses the strategy of defence in depth and the importance of fulfilling the safety functions (SFs)[5] 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 presents a number of ways how to use the approach for practical tasks. Section 5 presents conclusions.

A discussion of the SFs is presented in Appendix I. In Appendix II, the OTs 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. There are two formats of OTs. One of the formats uses the standard form of figures (as it was used in the

[5] Safety function: a specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions

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

original SRS-46), the other format uses EXCEL sheets, which are more easily adjustable for future updating of the methods. Nevertheless, there is relatively simple computerized way for conversion of EXCEL sheets into figures.

Summary of key lessons learned from the main reference documents used for updating the method is presented in Annex I to this publication. Annex II describes possible approach to demonstration of practical elimination of early or large releases. Finally, Annex III contains explanation and justification of modifications of OTs originally contained in SRS-46.

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 [13]. 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 SPs [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 NPPs, the safety objectives are ensured by fulfilling the three fundamental safety functions (FSFs)[7] described in Section 2.2.

According to INSAG-10 [14], 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 (RCS), and the containment.

Defence in depth is generally divided into five levels [14, 5]. 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. It is noted that Table 1 corresponds to currently valid IAEA approach, in which the border line between Level 3 and 4 of defence is placed between design basis accidents (DBAs) managed by the safety systems and design extension conditions (DECs), more severe than DBAs, managed by safety features for DECs. DECs are further subdivided into two subcategories. DEC-A are accidents not associated with severe fuel damage. DEC-B (severe accidents) are accidents associated with severe fuel damage, in case of LWRs understood as fuel melting.

[7] The three fundamental safety functions (or main safety functions) are: (a) Control of reactivity; (b) Removal of heat from the reactor and from the fuel store; (c) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

TABLE 1. LEVELS OF DEFENCE IN DEPTH [9]

Level of defence	Objective	Essential design means	Essential operational means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction of NO systems, including monitoring and control systems	Operational rules and normal operating procedures
Level 2	Control of abnormal operation and detection of failures	Limitation and protection systems and other surveillance features	Abnormal operating procedures/emergency operating procedures
Level 3	Control of design basis accidents (postulated single initiating events)	Engineered safety features (safety systems)	Emergency operating procedures
DEC-A	Control of design extension conditions to prevent core melt	Safety features for design extension conditions without core melt	Emergency operating procedures
Level 4 **DEC-B**	Control of DECs to mitigate the consequences of severe accidents	Safety features for design extension conditions with core melt. Technical Support Centre	Complementary EOPs/ severe accident management guidelines
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	On-site and off-site emergency response facilities	On-site and off-site emergency plans

The levels of defence are intended to be individually robust and independent to the extent practicable, in particular between Levels 3 and 4. 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 robustness and independence of different levels of defence is crucial to meeting this objective.

Figure 1 is a simplified 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 Level 1 is the prevention of abnormal operation and system failures. If there is a failure at this level, an initiating event takes place. This can happen either if the defence in depth provisions at Level 1 were not effective enough or if a certain mechanism was not considered in establishing the defence in depth provisions at Level 1. Level 2 will detect these failures, to avoid or to control the abnormal operation. Should Level 2 fail, Level 3 ensures that the FSFs will be performed by activation of specific safety systems and other safety features with a view to limiting the possible consequences of DBAs. Should Level 3 fail, Level 4 limits accident progression by means of safety features for DECs and accident management measures in order to prevent or mitigate severe accident conditions with external releases of radioactive material. The last objective (Level 5) is the mitigation of the radiological consequences of significant external releases through the on-site and 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. Nevertheless, this deterministic approach is complemented by probabilistic safety analysis (PSA) considerations (system reliability, probabilistic targets, etc.), to provide an adequate level of safety ensuring a well balanced design.

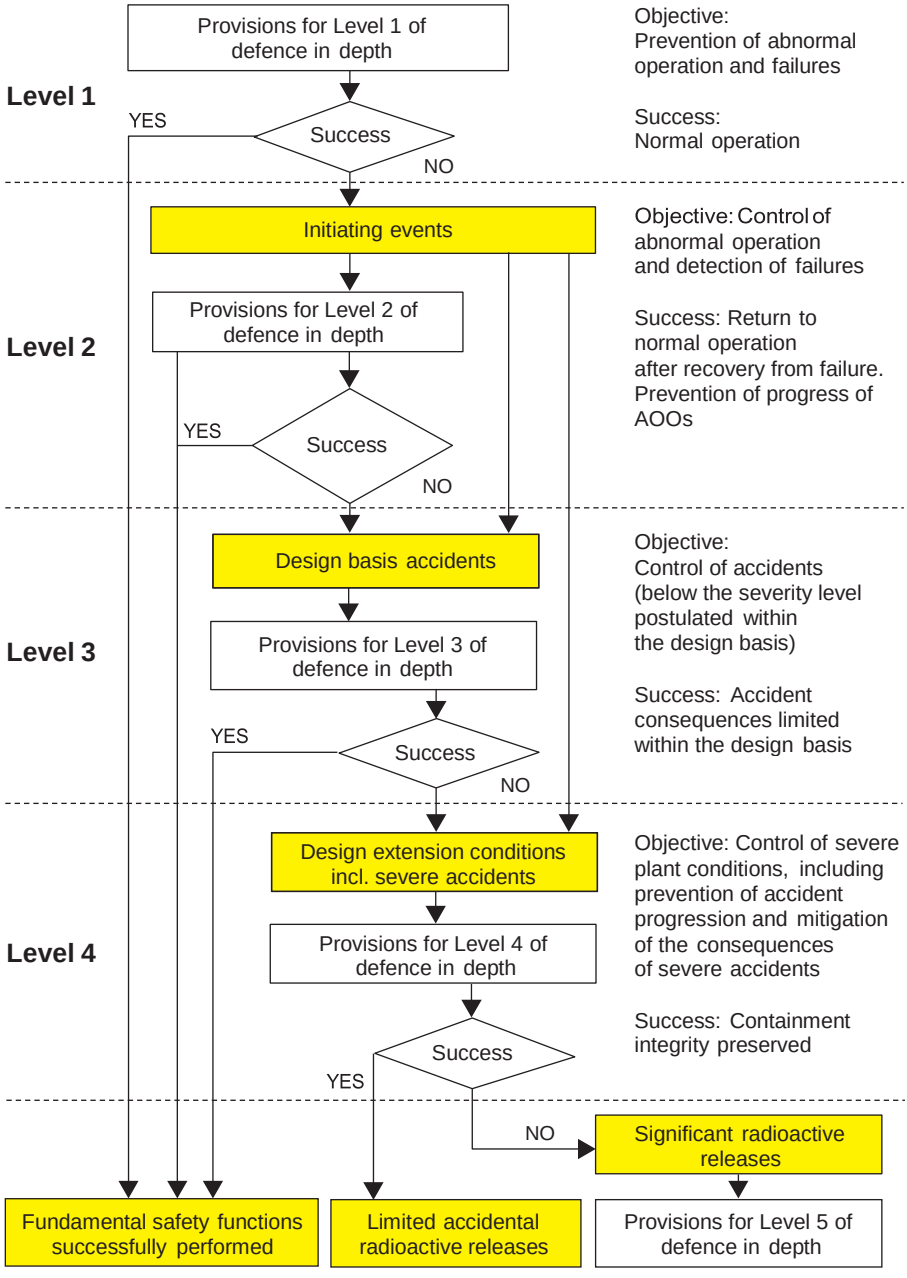


FIG. 1. Flow chart for defence in depth.

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 according to SSR-2/1, Rev. 1 [5]

(1) Control of reactivity;

(2) Removal of heat from the reactor and from the fuel store;

(3) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

FSFs have to be performed for all plant states, i.e. operational states, during and following DBAs as well as during and following the considered plant conditions more severe than the DBA, it means DECs, as stated in Requirement 4 of SSR-2/1, Rev. 1 [5]:

It is noted that removal of heat means not only heat removal from the reactor, but also from 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 as a measure of the appropriate implementation of defence in depth through the various safety provisions of the plant, as indicated by the underlying relevant SPs. 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. 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

SRS-46 [3] and this updated publication describe the reference approach for checking the completeness and quality of implementation of the concept of defence in depth in a systematic way. The bases for the approach are as follows:

- Safety must be ensured by implementing safety provisions at all five levels of defence in depth at any time;
- Each of the levels should be individually robust;
- Each level has its relevant safety objectives ensured by integrity of the barriers;
- For maintaining integrity of the barriers, the FSFs and more detailed (derived) SFs should be performed;
- SFs can be challenged by a number of mechanisms affecting their performance;
- To prevent mechanisms affecting the SFs, safety provisions of different kinds should be implemented;
- Provisions implemented at different levels of defence should be reasonably independent.

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 SP 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 including human behaviour, 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 SPs.

The framework described above may be graphically depicted in terms of an OT, 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 continued integrity of the first three barriers (the fuel matrix, cladding and pressure boundary of the RCS) 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 RCS and to avoid any damage of the reactor containment.

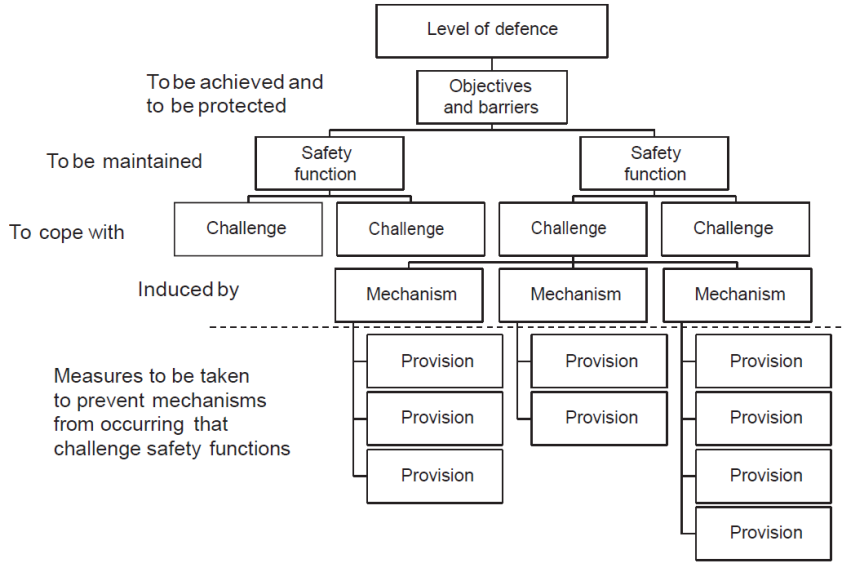


FIG. 2. Structure for defence in depth provisions at each level of defence.

There might be an impact on the performance of FSFs/SFs by challenges which are placed on a lower level of the OT. 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.

Graphical depiction of links between safety objectives and safety provisions as an objective tree helps to identify weaknesses in defence in depth and supports the questioning attitude essential for nuclear safety. Screening by means of OTs should be understood not only as a comprehensive tool for assessment, but also as a way of thinking on nuclear safety in very broad circumstances.

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 OTs 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 convenient that the list of provisions is drawn up as comprehensively as possible. A combination of expert judgement, the INSAG-12 report [2], IAEA Safety Standards and many other reference documents presented in Annex I have 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 NPP lifetime. Each of the elements is representative of a specific SP discussed in detail in Ref. [2]. The lines connecting the SPs in Fig. 3 indicate the interrelations among the principles.

The SPs described in Ref. [2] are commonly shared safety concepts that indicate how to achieve safety objectives at different levels of defence in depth. The SPs do not guarantee that plants will be absolutely free of risk. Nonetheless, INSAG-12 [2] has stated that, if the principles are adequately applied, the NPPs should be very safe. It is therefore considered that the SPs provide a useful basis for the comprehensiveness of the provisions. Since publication of INSAG-12, the SPs are already quite comprehensively reflected in currently available IAEA Safety Standards. In fact, in several occasions the requirements and the guidance of the Standards are formulated beyond the expectations of INSAG-12.

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

The first step for assignment of SPs to individual levels of defence is shown in Fig. 3. A preliminary assignment is done as a horizontal band selected from the SPs 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 SPs such as design management, quality assurance or safety culture can adversely affect several levels of defence at the same time. Specific SPs that usually address the performance of various hardware components are typically assigned to different levels of defence.

The third step for assignment of SPs to individual levels of defence is provided by the explanatory text on the SPs themselves in Ref. [2] and the derived requirements for siting, design and operation in the IAEA Safety Standards [4,5,6].

The revised results of the assignment of the SPs are given in Table 2. The numbering of the SPs 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]. However, the defence in depth level for each SP was partly revised based on the findings and lessons learned after INSAG-12 was issued. Specifically, the defence in depth level for SPs-136, 168, 174, 177, 182, 217, 233, 240, 242, 265, 272, 284, 290, 296, 339 among the SPs in Ref. [2] was revised.

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

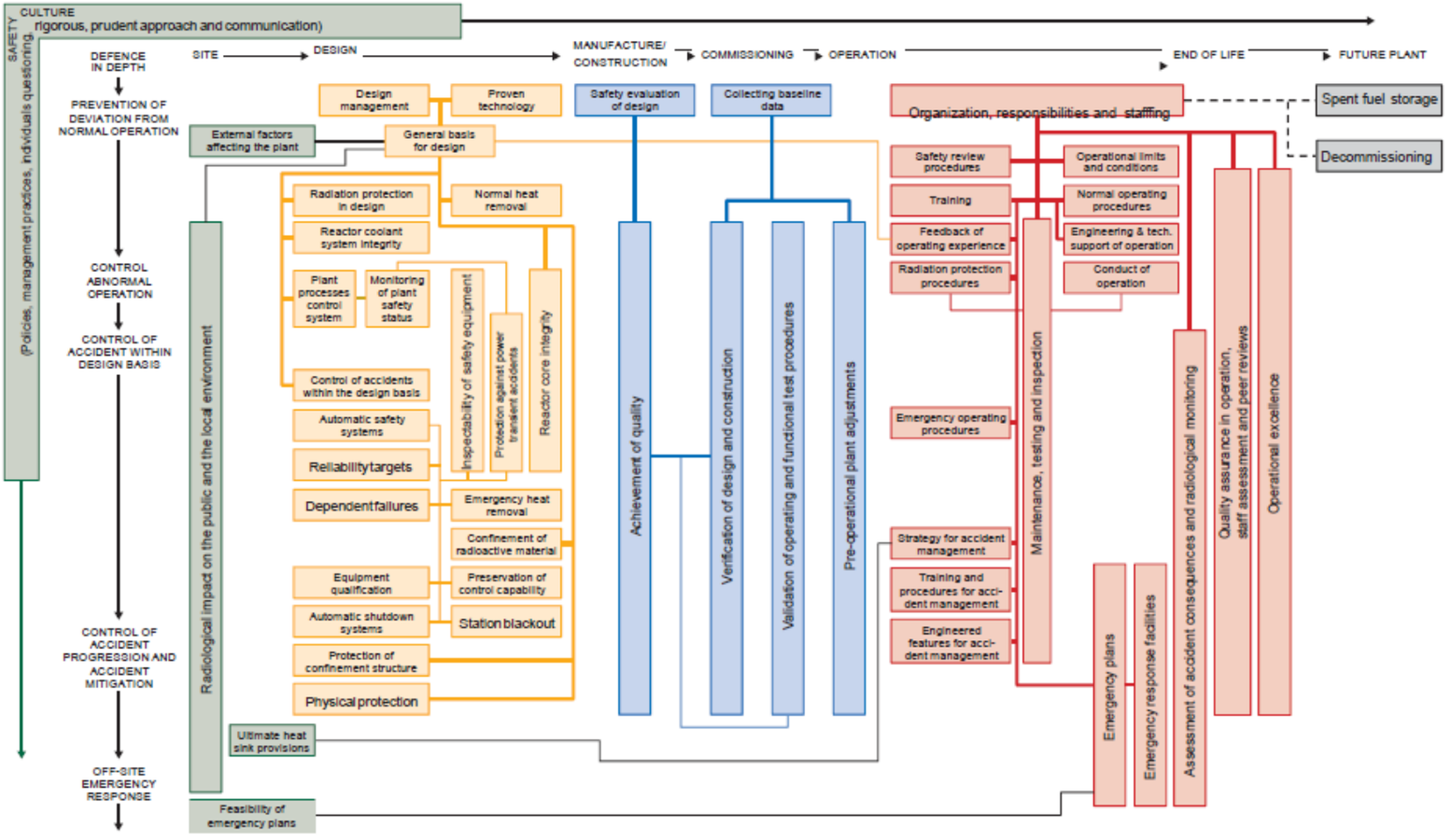


FIG. 3. Schematic presentation of the specific safety principles of INSAG, showing their coherence and their interrelations [2].

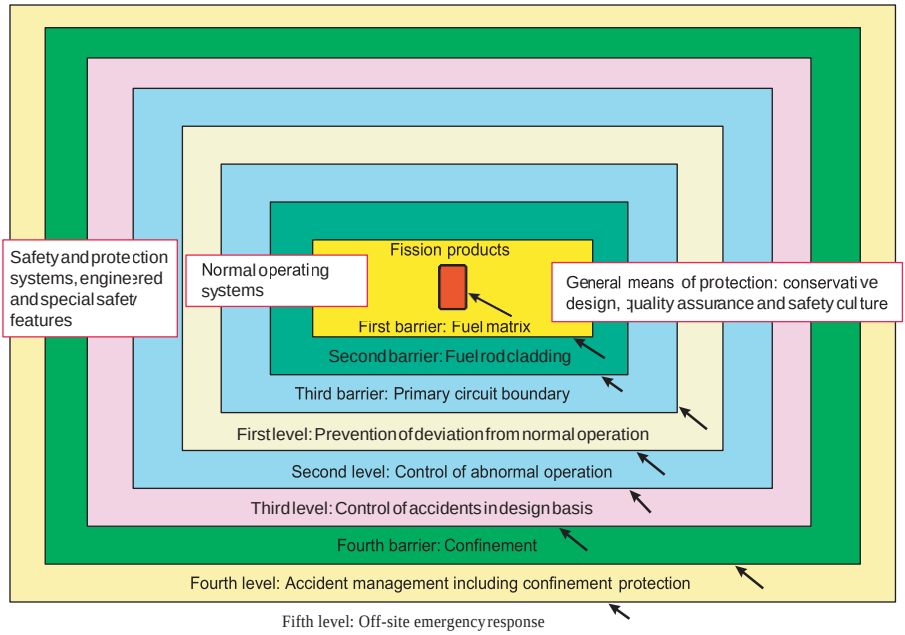


FIG. 4. Interrelationship between physical barriers and levels of protection in defence in depth [2].

In some cases, the assignment of SPs 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 DECs.

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

3.3. OBJECTIVE TREES

The OTs are presented in Appendix II for all the levels of defence based on the approach described. The trees themselves are intended to be self- explanatory, i.e. no additional text should be needed to explain the challenges, mechanisms and provisions. Nevertheless, Annex III contains some additional explanatory text whenever found useful, in particular explanation of the reasons for updating the OTs from their original

[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).

version contained in SRS-46 [3].

The following remarks can be made on the formulation of provisions in the OTs

(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 OTs is to provide a comprehensive list of the possible options for provisions. Some of the provisions are individually capable to prevent completely the mechanisms from occurring, while others need to be complemented by additional provisions. It means that not necessarily all provisions associated with a given mechanism 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 OTs were mainly derived from the IAEA and INSAG SPs, the IAEA Safety Standards, many other guidance documents 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. In order to provide reasonably practical guidance, the provisions are often formulated in more specific way compared to general wording of IAEA Safety Standards.

(d) For SPs that are common to several levels of defence, several ways of presenting the OTs are used. If a substantial difference in the formulation of provisions for different levels is identified, a separate OT is developed for each of the respective levels. Otherwise, the same OT 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 OT 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 OTs within reasonable limits, similar provisions to avoid the occurrence of different mechanisms were sometimes condensed in the tree presentation (e.g. SP (136) in Appendix II).

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

Phases of plantlife	No. of SP	Safety principle (SP)	Level of defence				
			1	2	3	4	5
Siting	136	External factors affecting the plant	o	o	o	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	o	
	174	Reliability targets	o	o	o	o	
	177	Dependent failures			o	o	
	182	Equipment qualification			o	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	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	
	237	Control of accidents within the design basis			o		
	240	New and spent fuel storage	o	o	o	o	
	242	Physical protection of plant	o	o	o	o	

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

Phases of plantlife	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	
	269	Safety review procedures	o	o	o	o	
	272	Conduct of operations	o	o	o	o	
	278	Training	o	o	o		
	284	Operational limits and conditions	o				
	288	Normal operating procedures	o				
	290	Emergency operating procedures		o	o	o	
	292	Radiation protection procedures	o	o	o	o	
	296	Engineering and technical support of operations	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

4. APPLICATIONS

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

Use of the method for checking comprehensiveness of defence in depth is done in a reverse way compared to development of the method. Instead of top down process used for development of the OTs the bottom up screening of OTs is used, including the following steps

- Comparison of provisions in the OTs with capabilities of the plant;
- Judgment of the level of implementation of each provision;
- Consideration of optional provisions and judgment whether an absence of a provision leads to the weakness in defence in depth;
- Judgment whether a mechanism can be considered as prevented to occur;
- Judgment whether a challenge can be considered as prevented to affect fulfillment of a SF.

The OTs 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.

The present guidance is not intended to be a stand-alone document. Reference to the supporting publications listed in the references 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 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 publication 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 publication 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. 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.

There were examples of application of the objective trees approach in the past and renewed interest in the approach is observed after the Fukushima Daiichi accident.

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

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

- Bottom-up qualitative assessment of availability of identified provisions in any specific NPP, combined with an expert judgments of sufficiency of provisions for preventing challenges to SFs to take place;
- Use of selected lists of provisions as reminders for verification of availability of necessary measures in specific safety reviews, including IAEA safety review missions;
- Verification of comprehensiveness of safety assessment criteria in periodic safety reviews (PSRs) by comparing the criteria with the list of provisions identified in the OTs;
- Assessment of severity of deficiencies in safety level identified in PSR by indicating the challenges to performance of SFs, levels of defence in depth

affected and available provisions possibly compensating the deficiencies;

— Identification of measures for safety upgrading of the NPP to eliminate identified gaps;

— Demonstration of progress in safety upgrading of a given NPP by increasing number of implemented safety provisions;

— Demonstration of a comprehensive consideration of defence in depth in the plant Safety Analysis Reports (SARs);

— Use of the OTs for training of NPP staff to support their comprehensive consideration of defence in depth in day by day operations.

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 in this document 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 SPs and internationally agreed IAEA Safety Standards, which lay down the most important measures (provisions) to be implemented for assuring a sound and balanced defence in depth.

The IAEA SRS-46 provided a feasible framework for assessment of comprehensiveness of implementation of defence in depth provisions, but due to relatively long time since its publication it needed updating and improvements of its user friendliness. The work described in this publication responded to the needs for overall improvements of the whole methodology for screening comprehensiveness of the defence in depth at all levels of defence.

Updating of the challenges, mechanism and provisions in the OTs took into account strengthening of international and national safety requirements and lessons learned, in particular those reflected in the IAEA Safety Standards, WENRA reference levels and safety objectives, OECD/NEA recommendations for strengthening of defence in depth, and any other post-Fukushima lessons learned, including results of the European and other stress tests.

In the updated method, the original basis of the approach by means of systematic assessment of provisions available to prevent mechanisms and challenges affecting safety functions potentially leading to the damage of the barriers against releases of radioactivity was maintained. The way of illustrating the links between safety objectives, barriers, safety functions, challenges, mechanisms and safety provisions by objective trees remained unchanged. In addition the objective trees are available also in the form of EXCEL sheets easy to be updated and converted into figures.

The updating also included adjustment of the balance between individual OTs, as well as improvements in formulation of all items in the OTs in order to ensure their validity, correctness and clarity.

The user friendliness of the method was improved by developing a computerized version of OTs, with sufficient flexibility for further corrections and modifications, with a possibility to associate various attributes to individual items of the objective trees and a possibility of easy updating the OT.

The method does not include any quantification of the level 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 OTs, 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.

APPENDIX I. FUNDAMENTAL SAFETY FUNCTIONS AND SAFETY FUNCTIONS

SFs 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 has been used in the SRS-46 found as appropriate to develop the objective trees:

(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 (PIEs) 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 accident conditions with the reactor coolant pressure boundary intact;

(8) to transfer heat from other safety systems to the ultimate heat sink (UHS);

(9) to ensure necessary services (such as electrical, pneumatic, hydraulic power supplies, 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;

(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;

---

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

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

(13) to limit the radiation exposure of the public and site personnel in and following DBAs and design extension conditions (DECs) including 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 material 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 RCS, but within the site, in all operational states;

(17) to remove decay heat from irradiated fuel stored outside the RCS, but within the site;

(18) to maintain sufficient sub-criticality of fuel stored outside the RCS 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 a SF;

(20) to maintain the integrity of the reactor containment in accident conditions and conditions following an accident;

(21) to limit the effects of release of radioactive materials on the public and environment.

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

- SFs related to FSF(1) "control of the reactivity": SFs (1), (2), (3), (18);
- SFs related to FSF(2) "removal of heat from the reactor and from the fuel store**":** SFs (4), (5), (6), (7), (8), (17);
- SFs related to FSF(3) **"**confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases**":** SFs (10), (11), (12), (13), (14), (16), (20), (21).

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

The set of SFs established in SRS-46 was found adequate for the updated methodology as well.

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

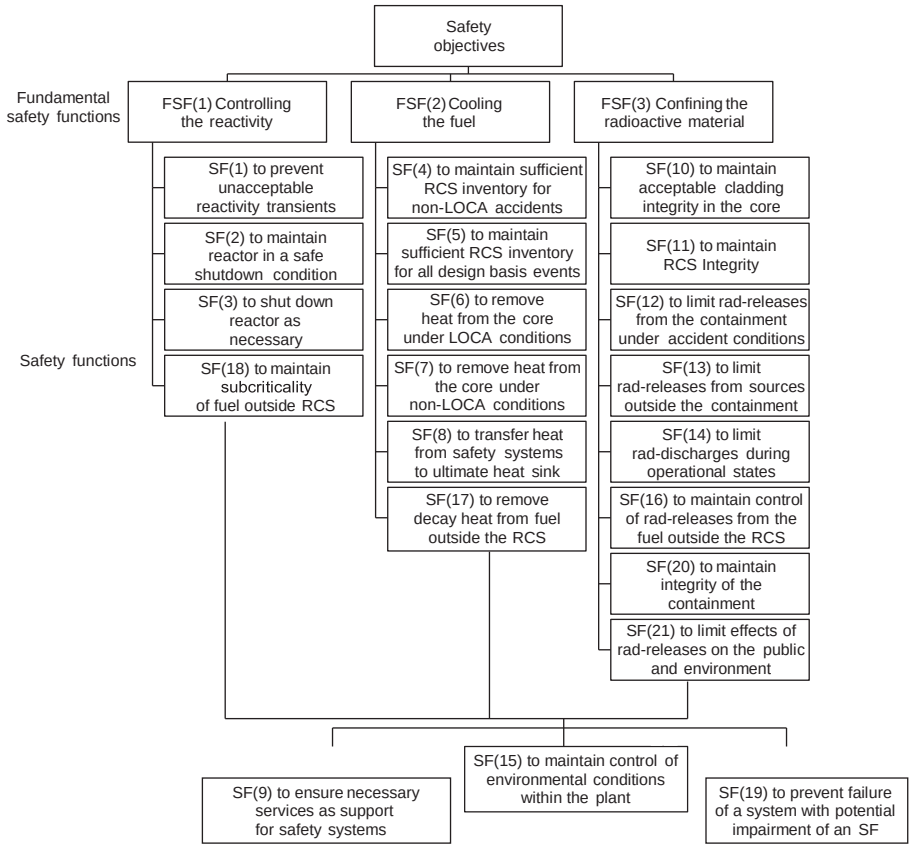


FIG. 5. Overview and grouping of SFs used in the present report (RCS, reactor coolant system; LOCA, loss of coolant accident).

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.

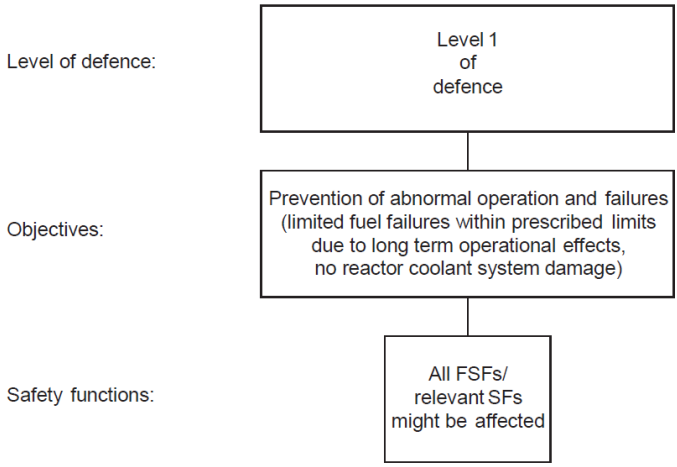


FIG. 6. Objectives to be achieved and barriers to be protected for Level 1 of defence in depth.

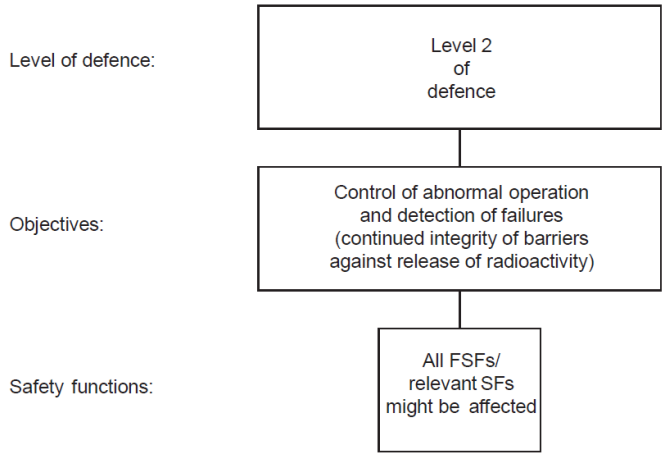


FIG. 7. Objectives to be achieved and barriers to be protected for Level 2 of defence in depth.

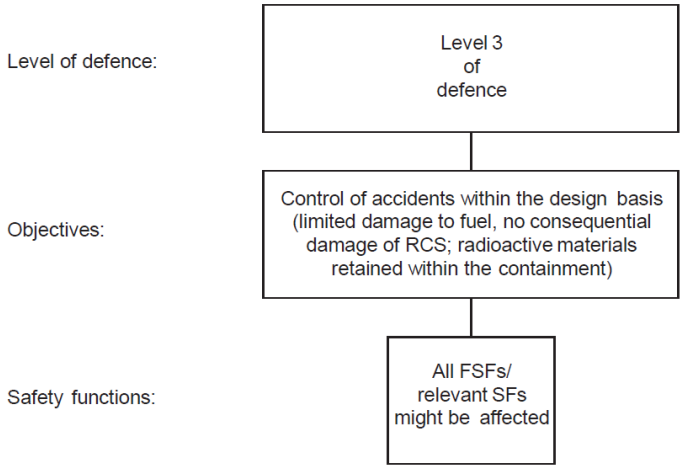


FIG. 8. Objectives to be achieved and barriers to be protected for Level 3 of defence in depth (RCS, reactor coolant system).

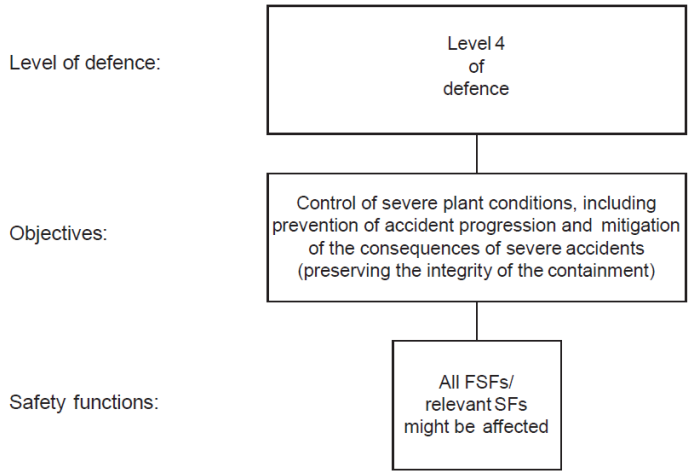


FIG. 9. Objectives to be achieved and barriers to be protected for Level 4 of defence in depth.

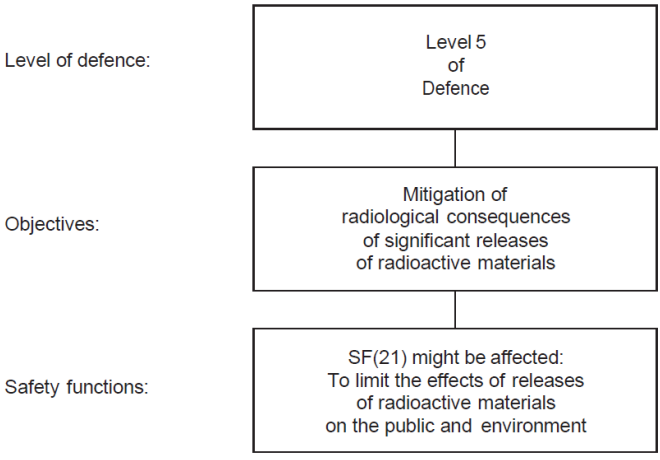


FIG. 10. Objectives to be achieved and barriers to be protected for Level 5 of defence in depth.

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.

This Appendix is structured to allow comparison of original OTs included in SRS-46 report with new (updated) OTs. Therefore, after each original OT copied from SRS-46, there is an updated OT, with the same number of the figure, just with the added label "Updated". In case when there is no updated version of the OT, for example due to merging together two previous OTs in a single updated OT, there is a blank page with the number of the figure and with an explanatory note, what happened with the original figure. Explanation/justification of the changes from the original OTs to updated OT is included in Annex III.

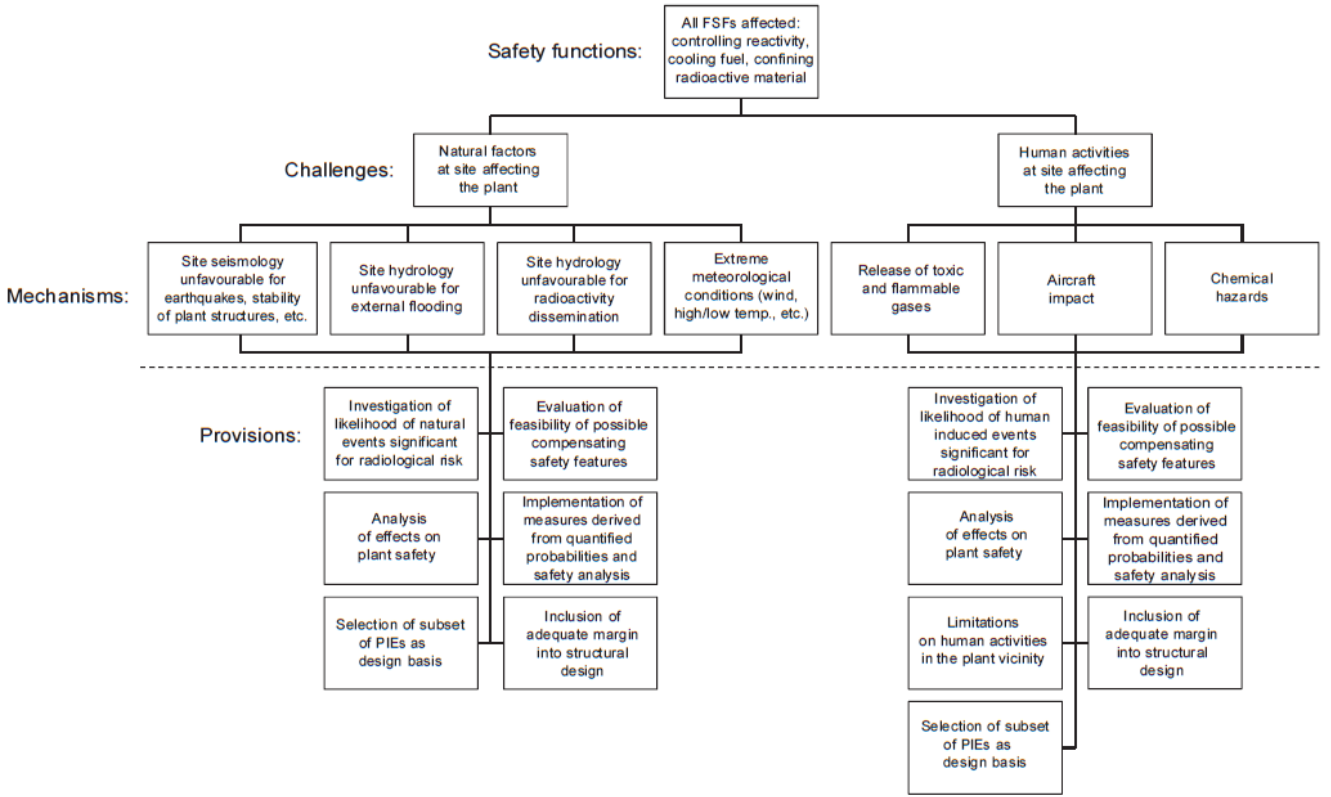


FIG. 11. Objective tree for Level 1 of defence in depth. Safety principle (136): external factors affecting the plant.

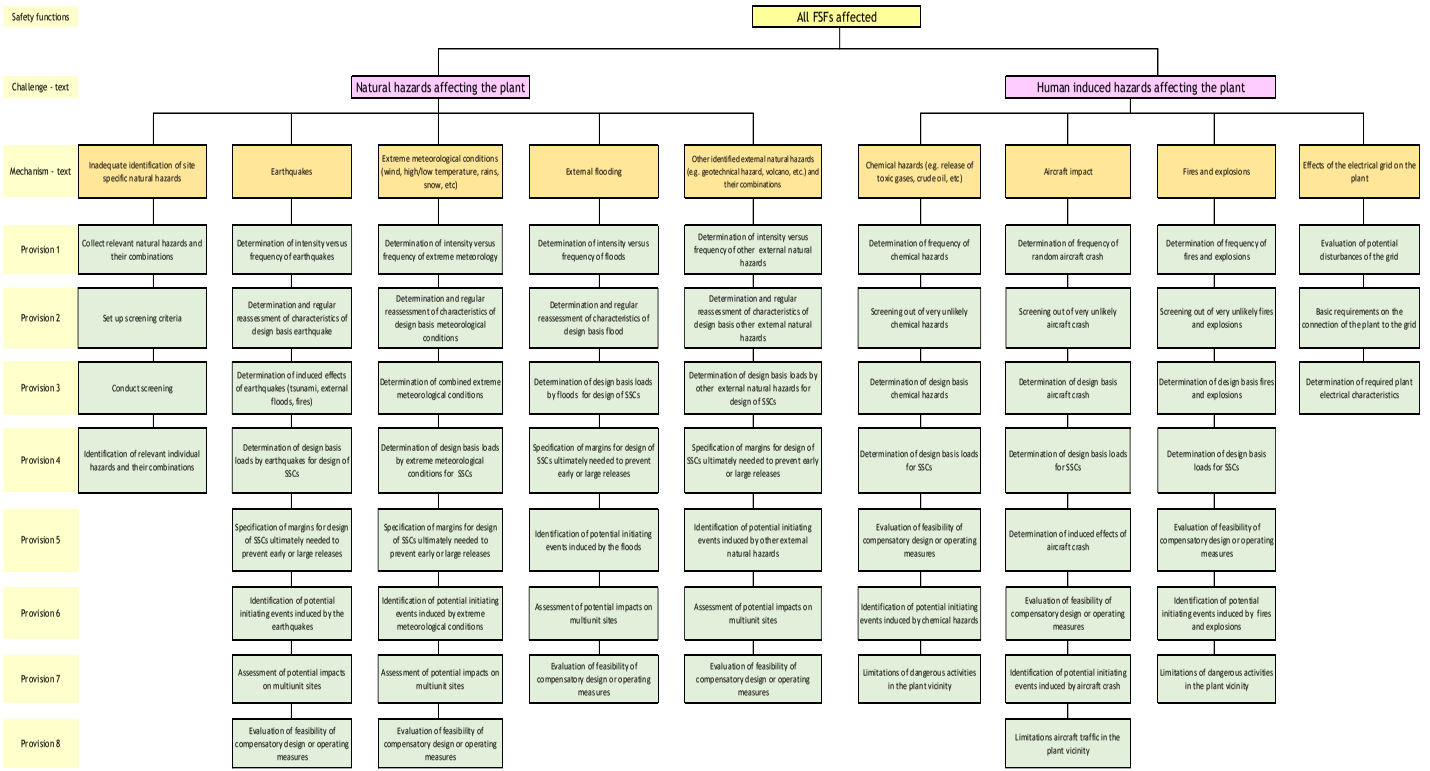


FIG. 11. Updated. Objective tree for Levels 1-4 of defence in depth. Safety principle (136): external factors affecting the plant.

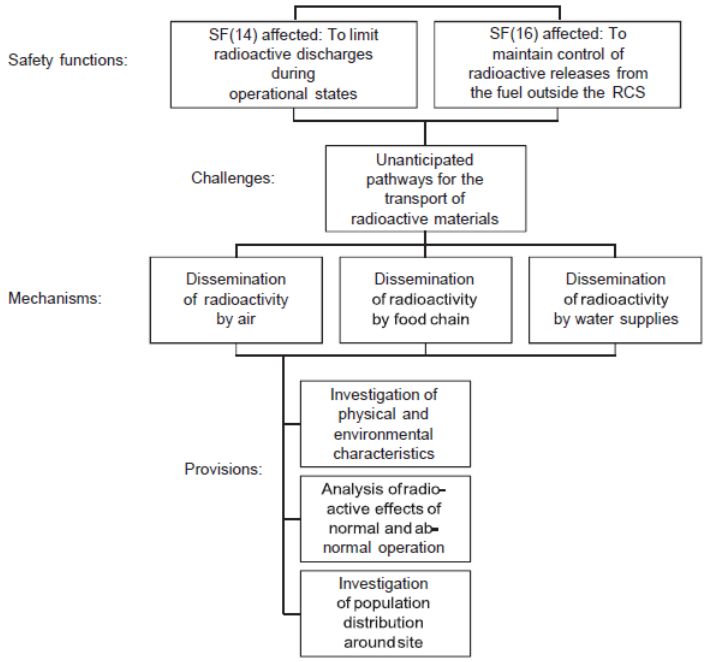


FIG. 12. Objective tree for Level 1 of defence in depth. Safety principle (138): radiological impact on the public and the local environment.

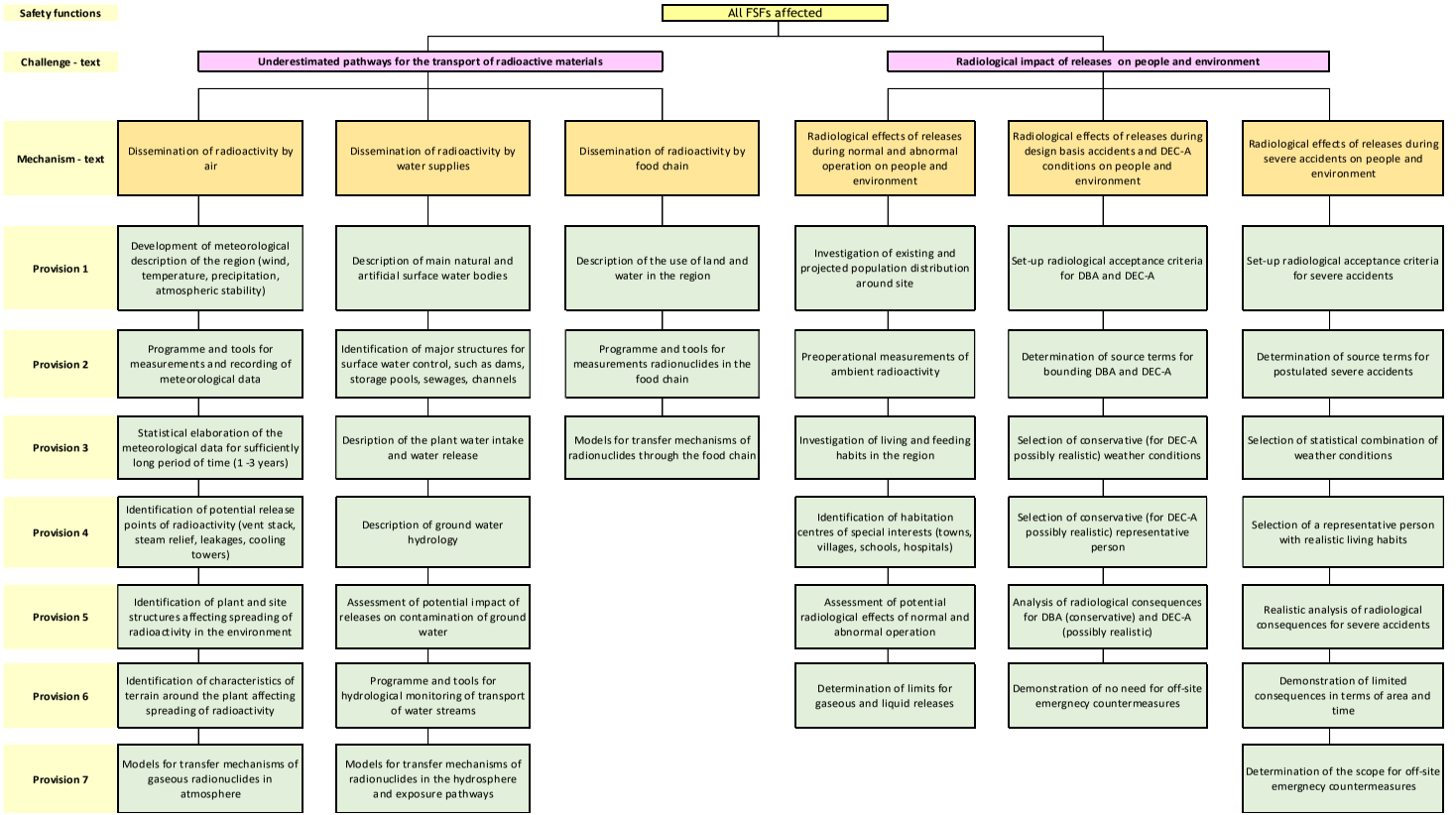


FIG. 12. Updated. Objective tree for Levels 1-5 of defence in depth. Safety principle (138): radiological impact on the public and the local environment.

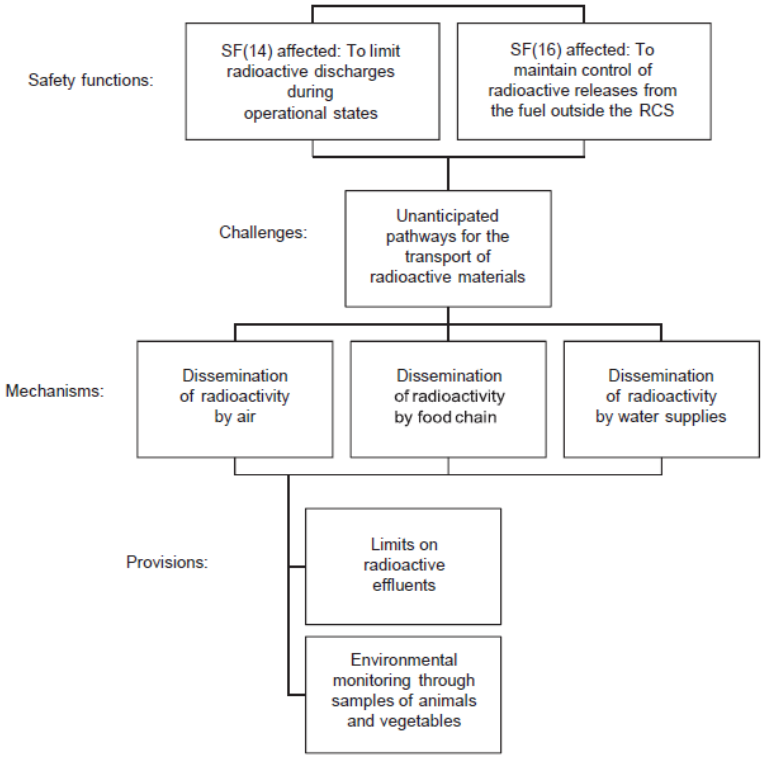


FIG. 13. Objective tree for Level 2 of defence in depth. Safety principle (138): radiological impact on the public and the local environment.

Fig. 13 was combined with fig. 12

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

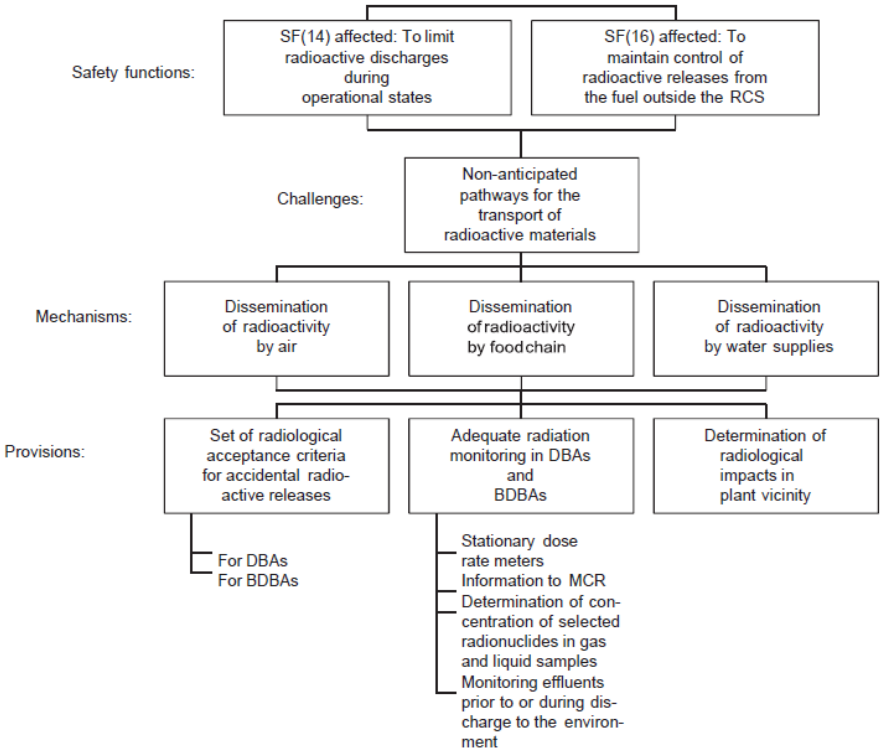


FIG. 14. Objective tree for Levels 3 and 4 of defence in depth. Safety principle (138): radiological impact on the public and the local environment.

Fig. 14 was combined with fig. 12

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

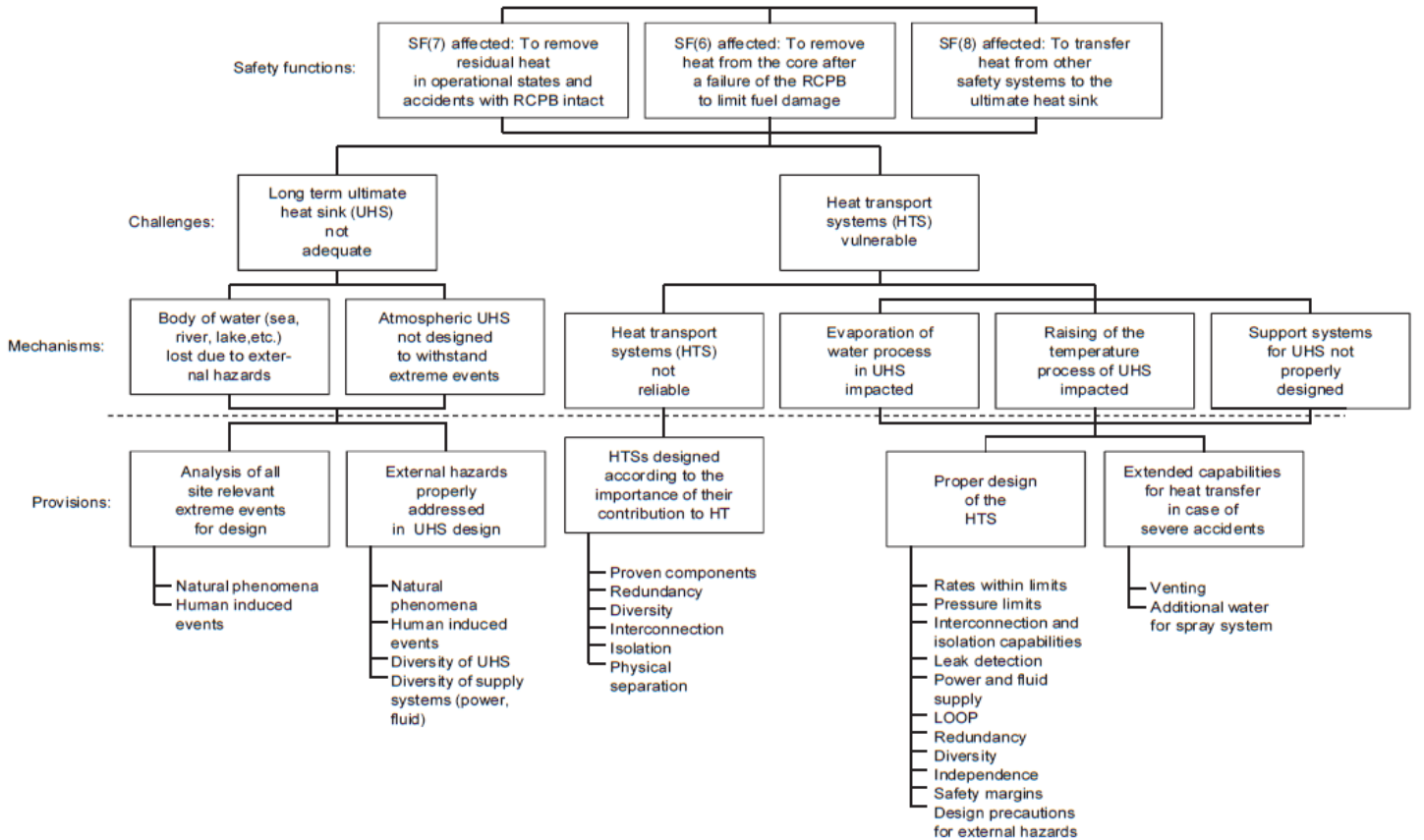


FIG. 15. Objective tree for Levels 1–4 of defence in depth.. Safety principle (142): ultimate heat sink provisions.

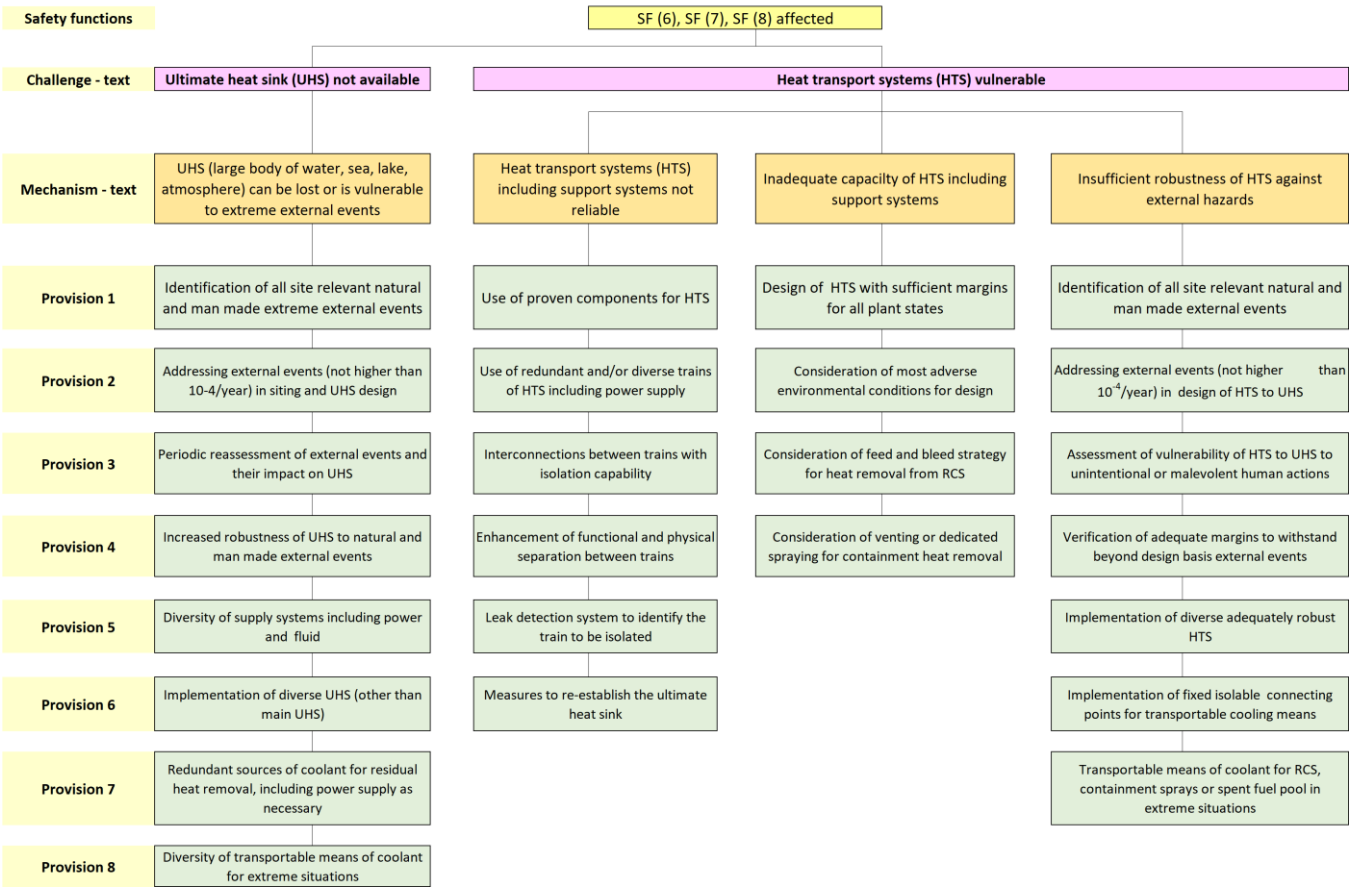


FIG. 15. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (142): ultimate heat sink provisions.

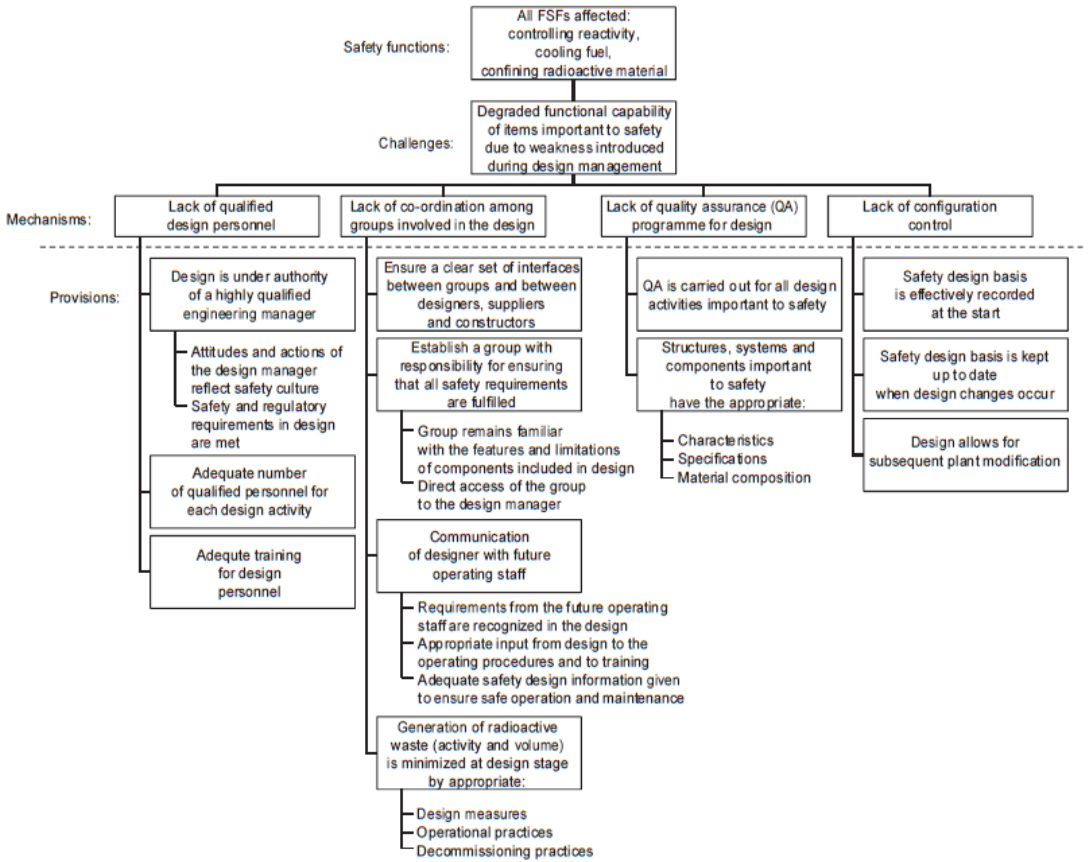


FIG. 16. Objective tree for Levels 1–4 of defence in depth. Safety principle (150): design management.

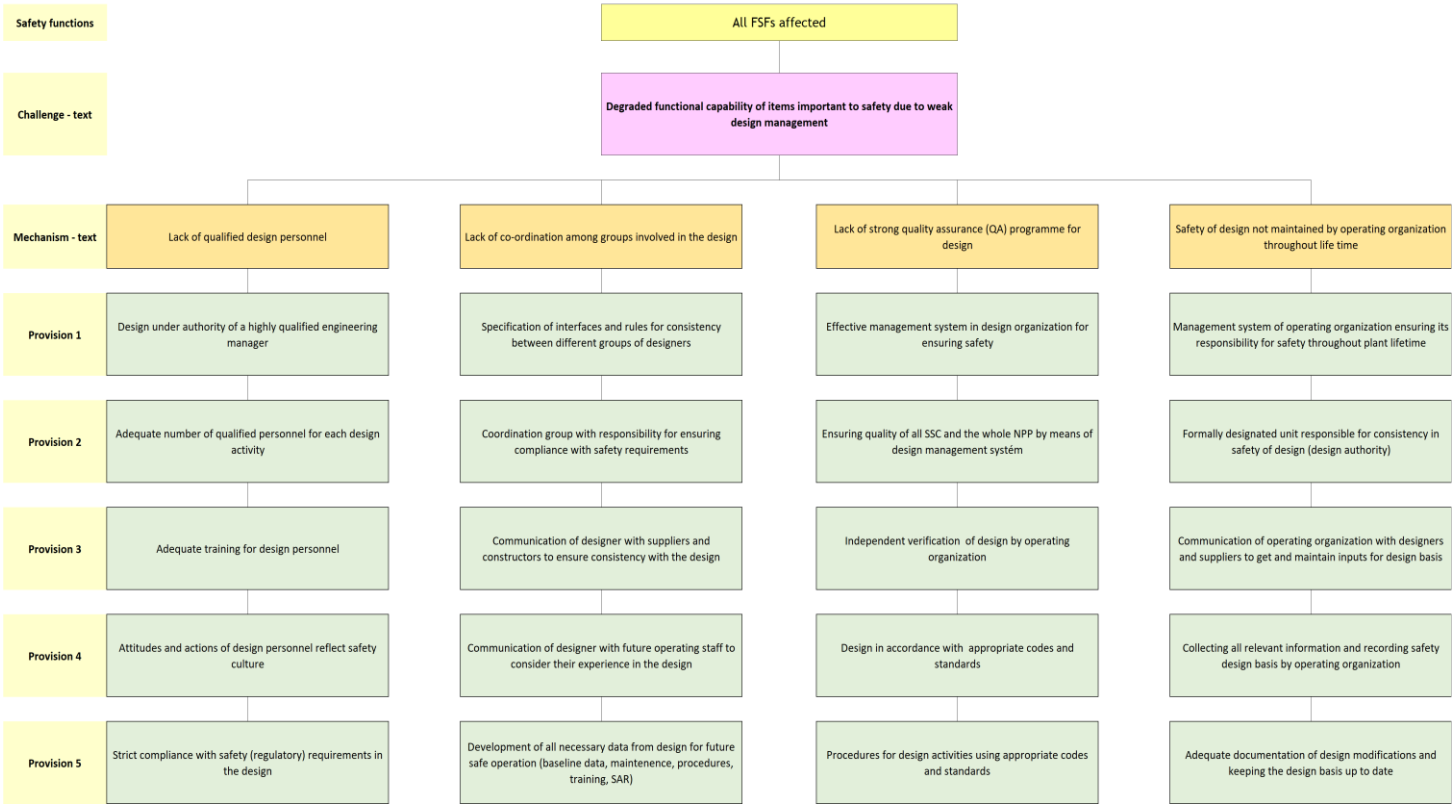


FIG. 16. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (150): design management.

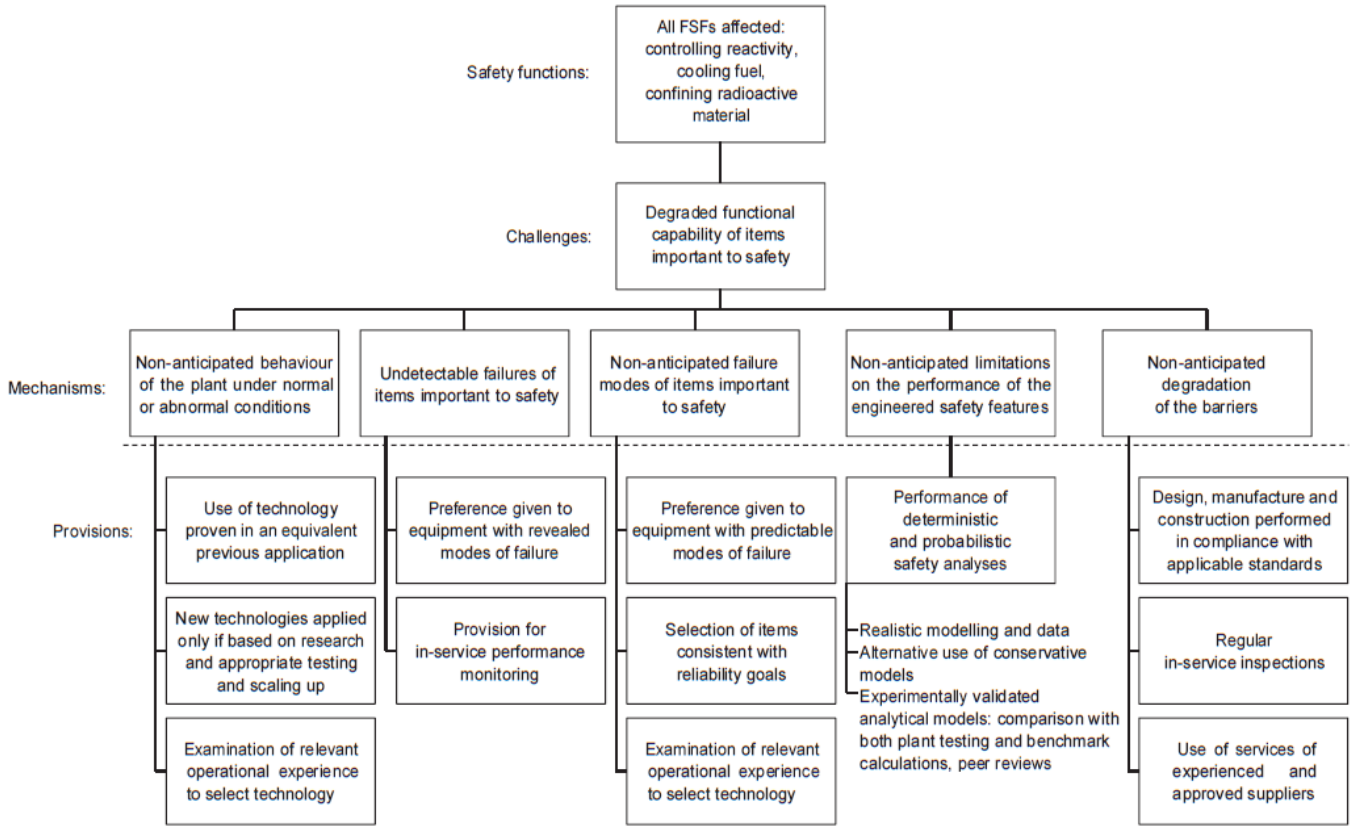


FIG. 17. Objective tree for Levels 1–4 of defence in depth. Safety principle (154): proven technology.

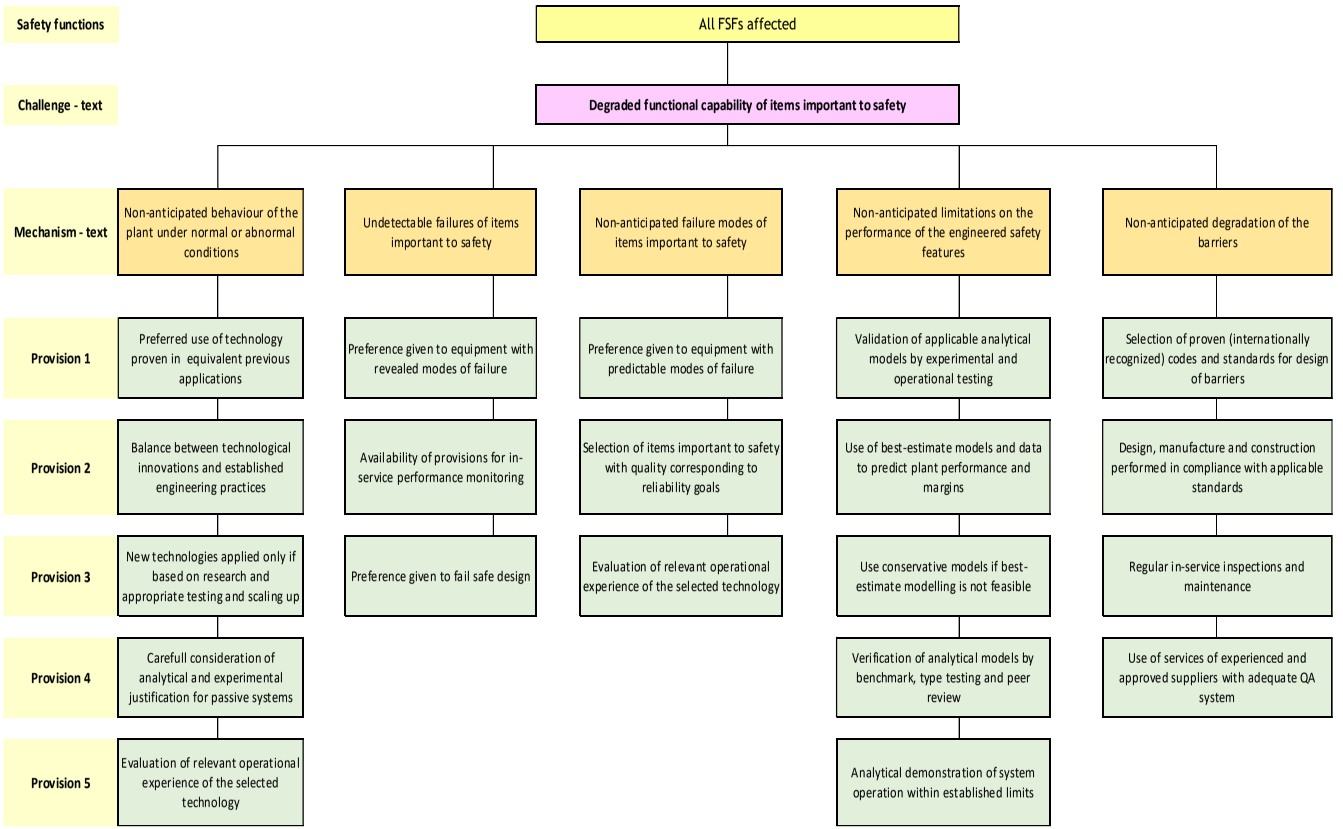


FIG. 17. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (154): proven technology.

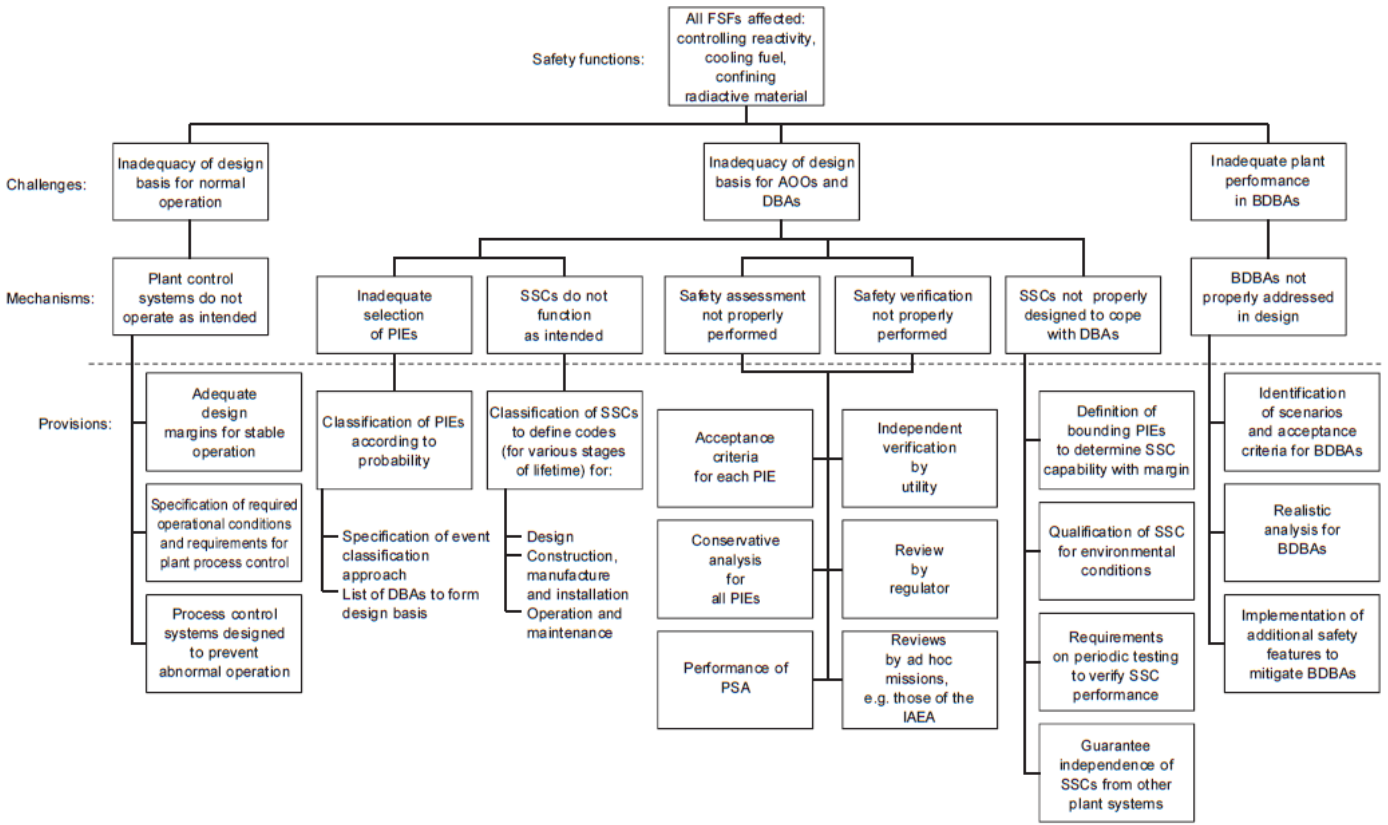


FIG. 18. Objective tree for Levels 1–4 of defence in depth. Safety principle (158): general basis for design.

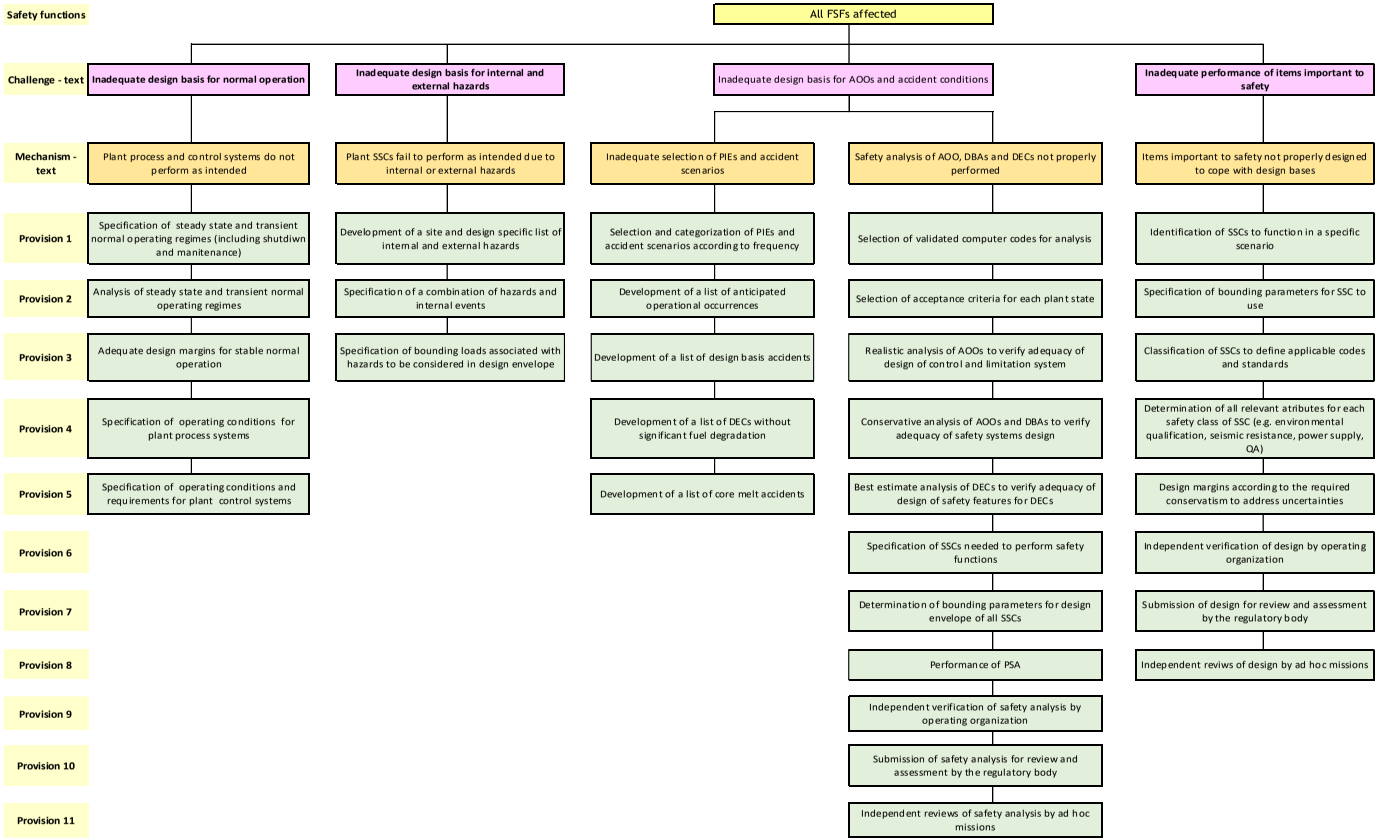


FIG. 18. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (158): general basis for design.

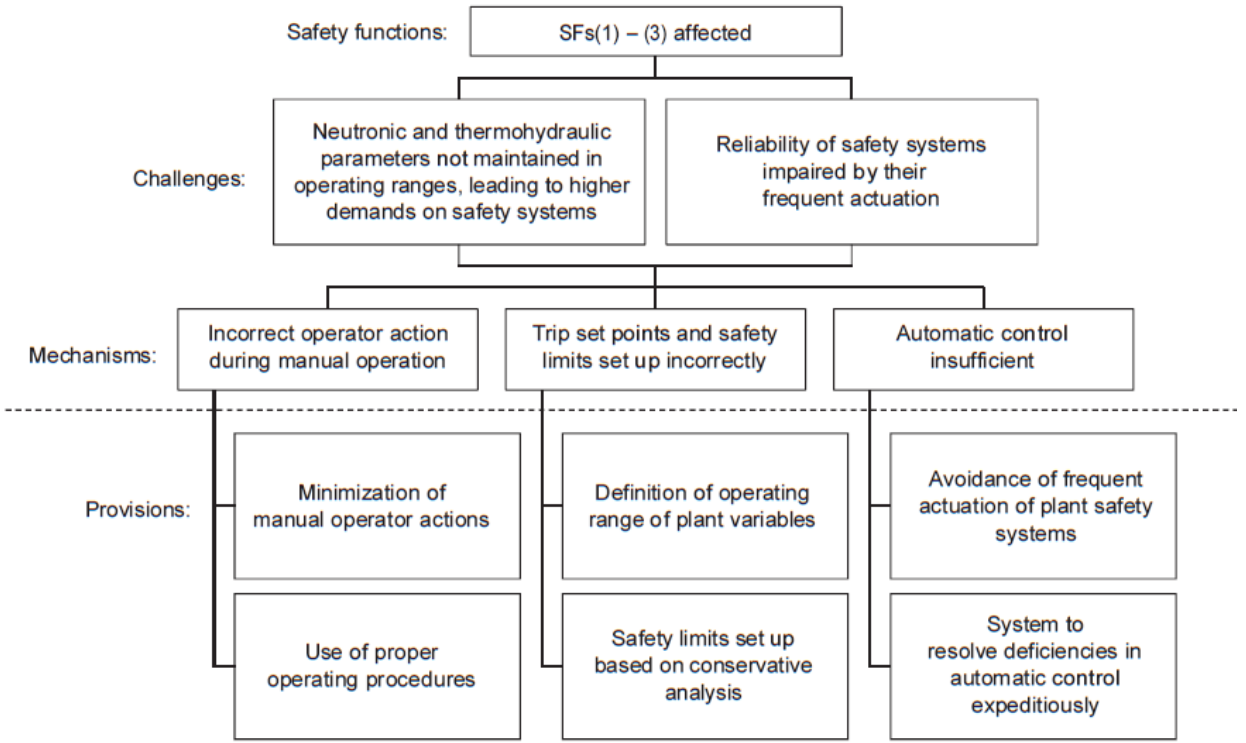


FIG. 19. Objective tree for Level 1 of defence in depth. Safety principle (164): plant process control systems.

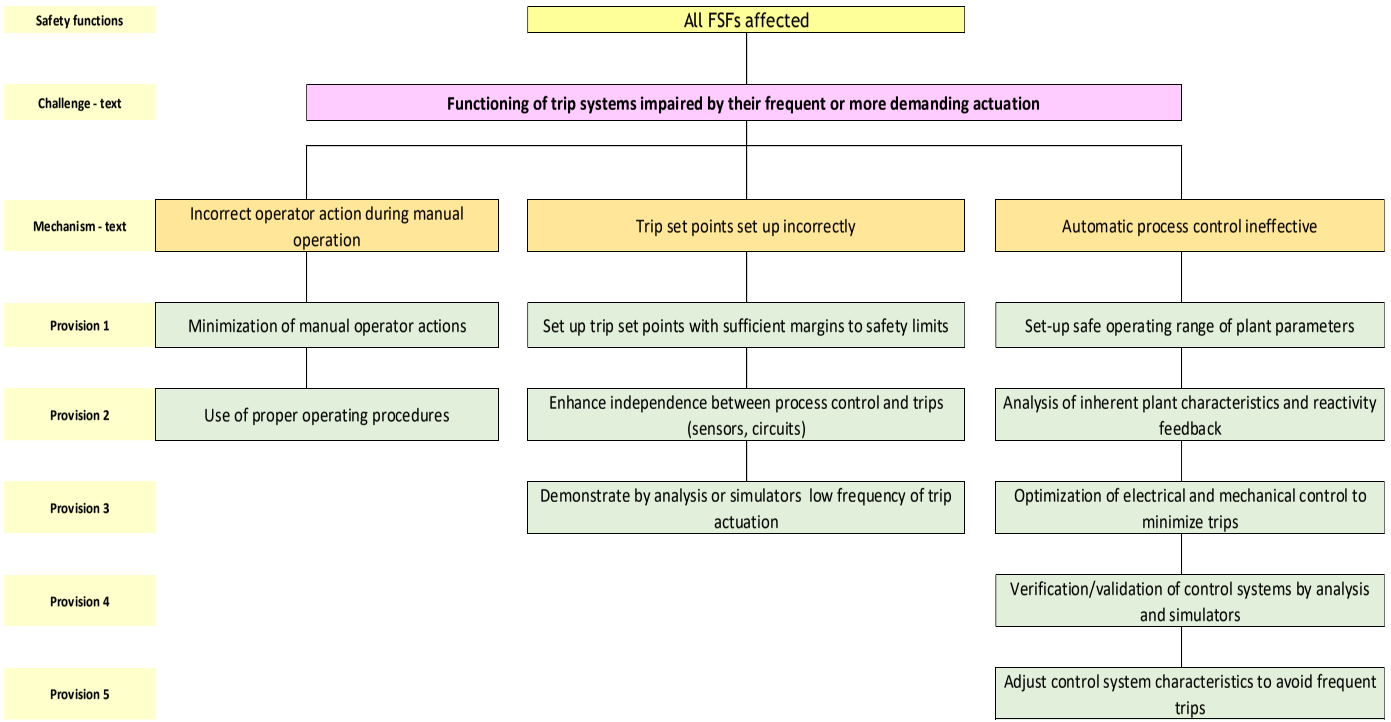


FIG. 19. Updated. Objective tree for Level 1 of defence in depth. Safety principle (164): plant process control systems.

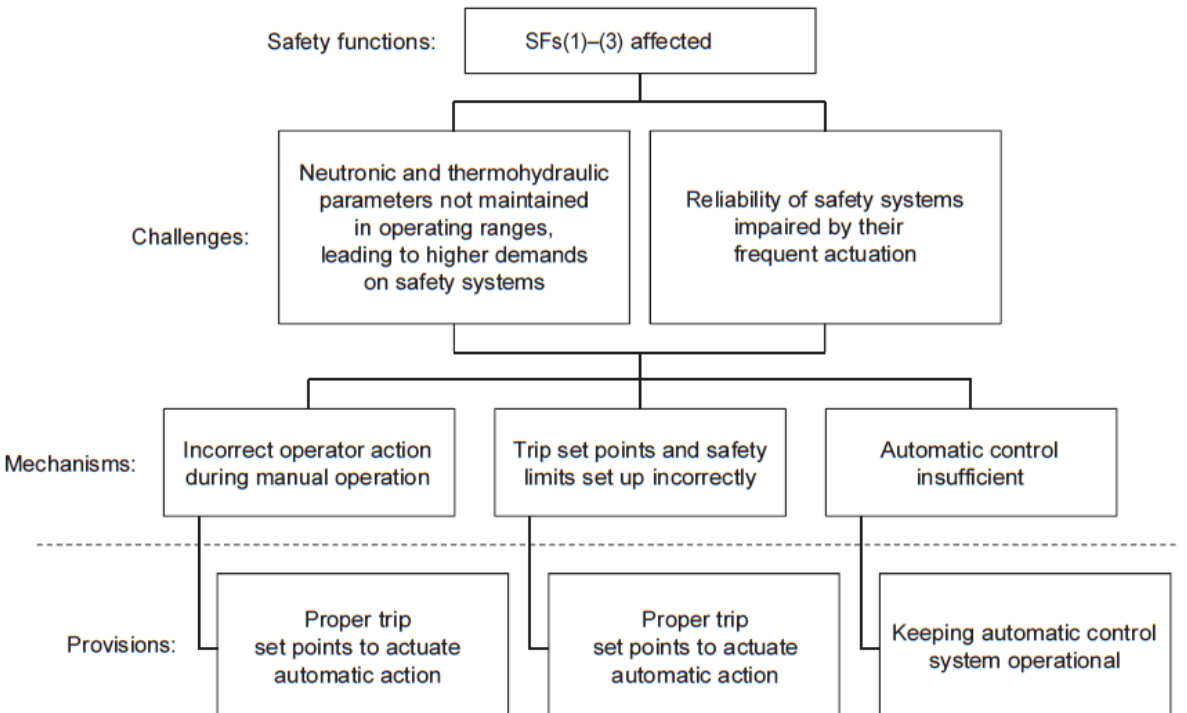


FIG. 20. Objective tree for Level 2 of defence in depth. Safety principle (164): plant process control systems.

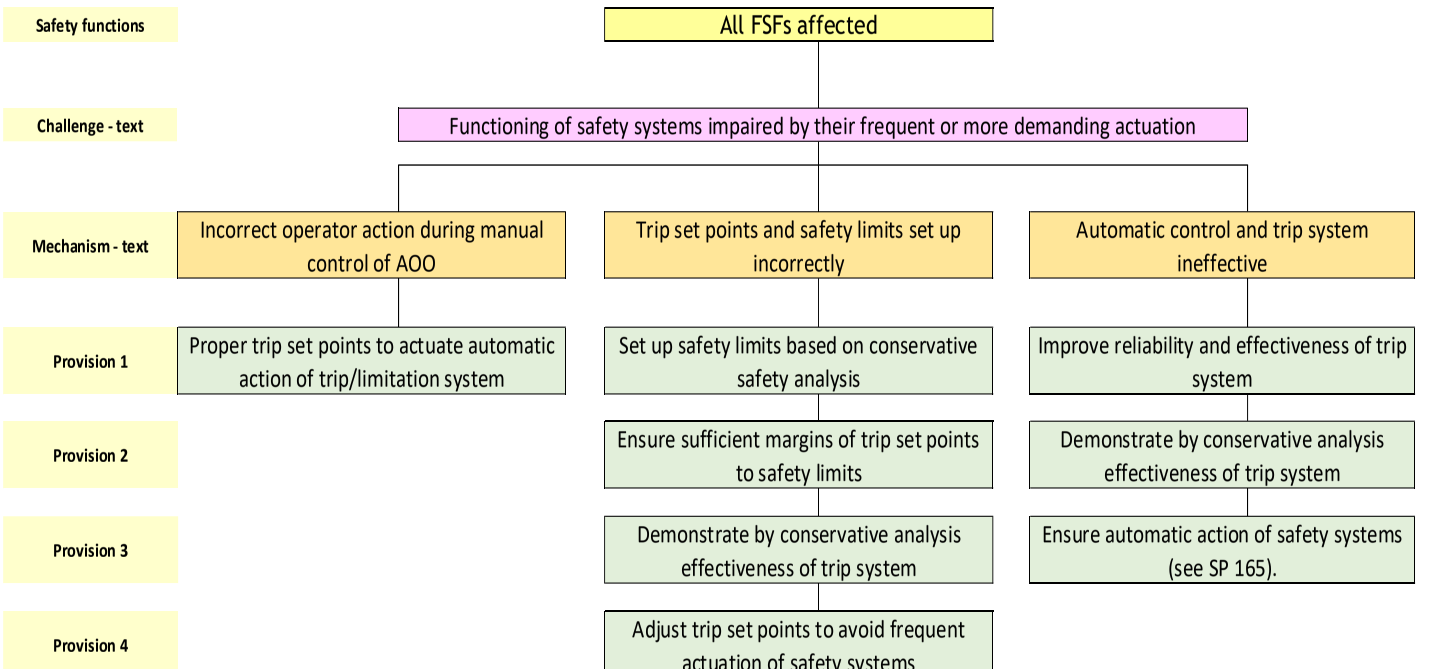


FIG. 20. Updated. Objective tree for Level 2 of defence in depth. Safety principle (164): plant process control systems.

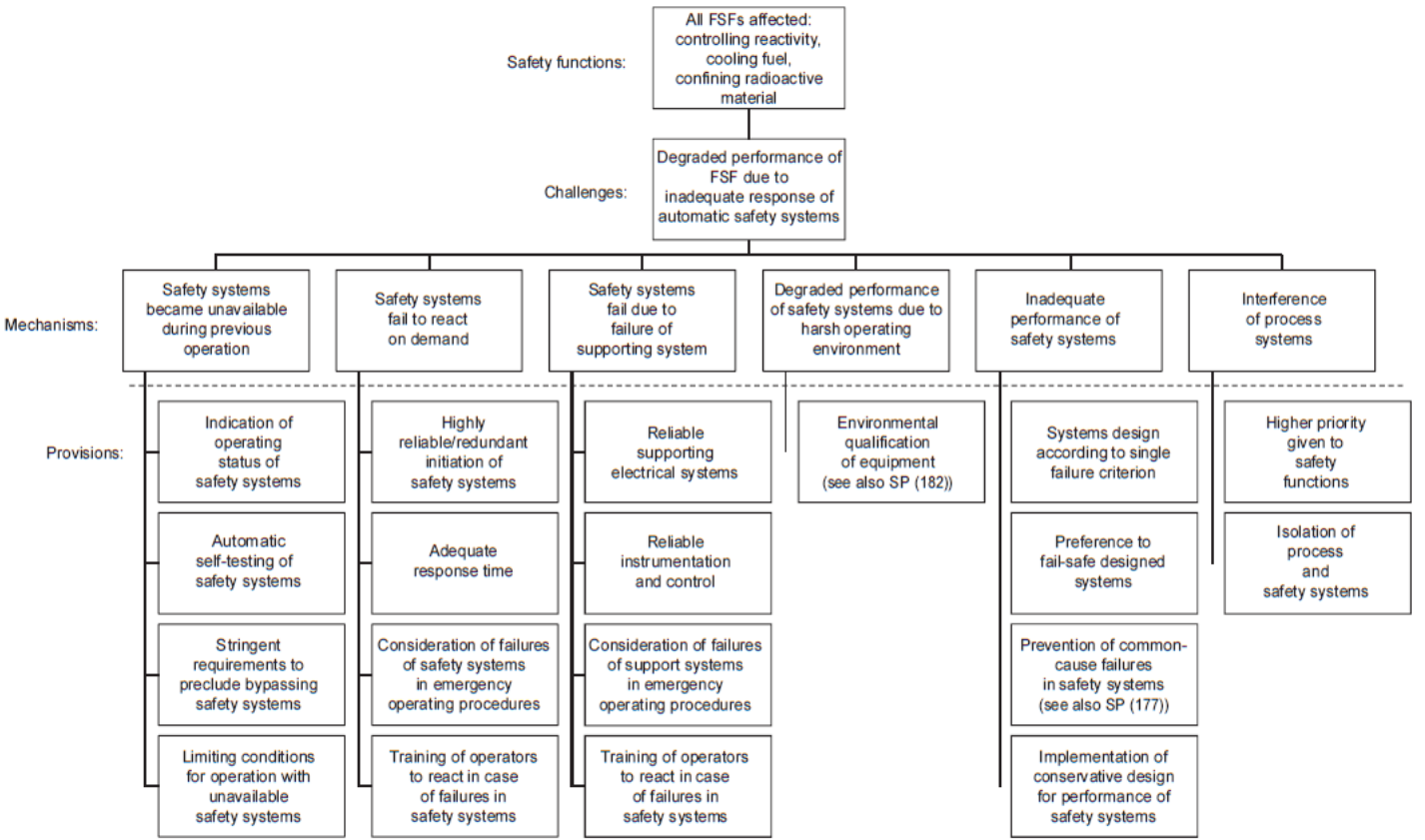


FIG. 21. Objective tree for Level 3 of defence in depth. Safety principle (168): automatic safety systems.

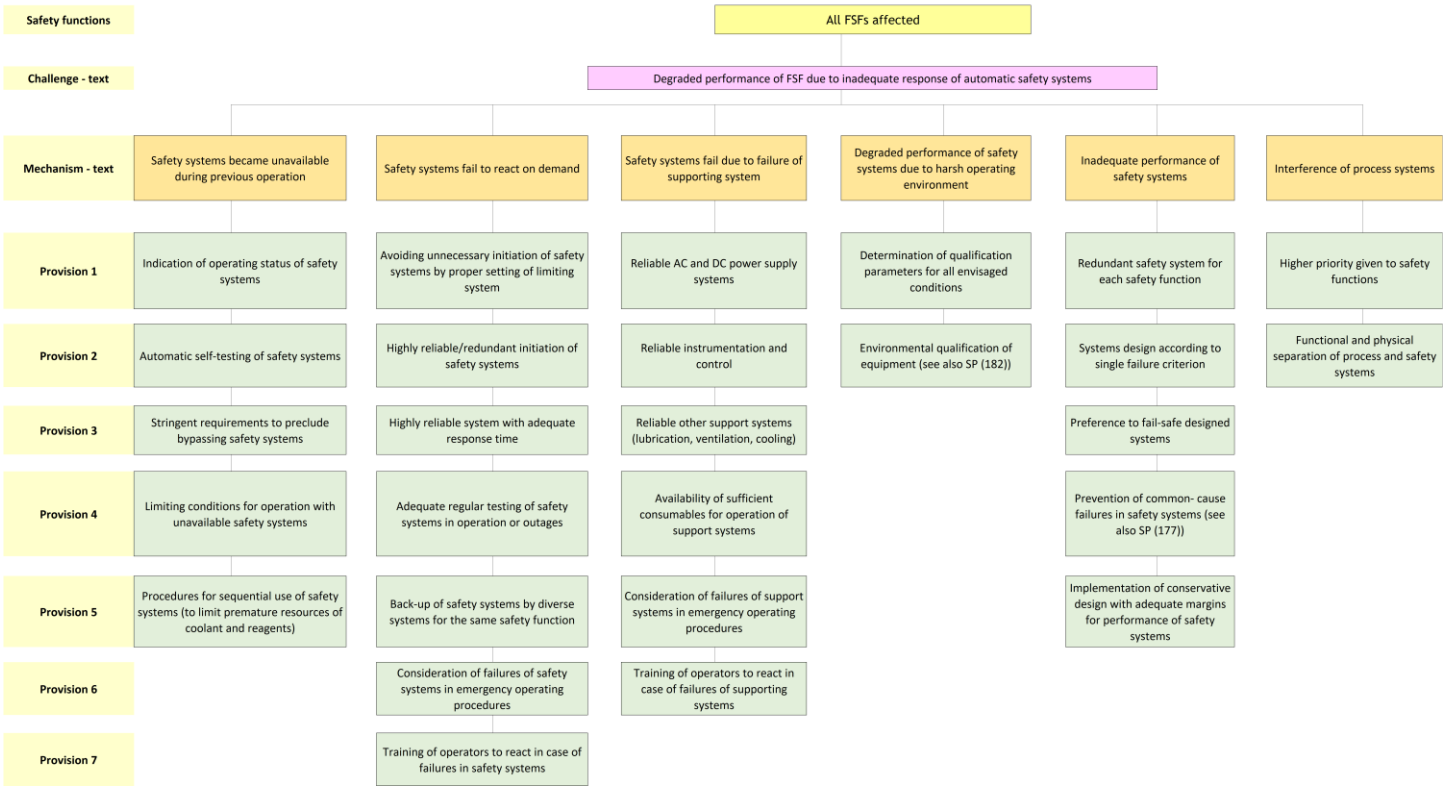


FIG. 21. Updated. Objective tree for Levels 3-4 (DEC-A) of defence in depth. Safety principle (168): automatic safety systems.

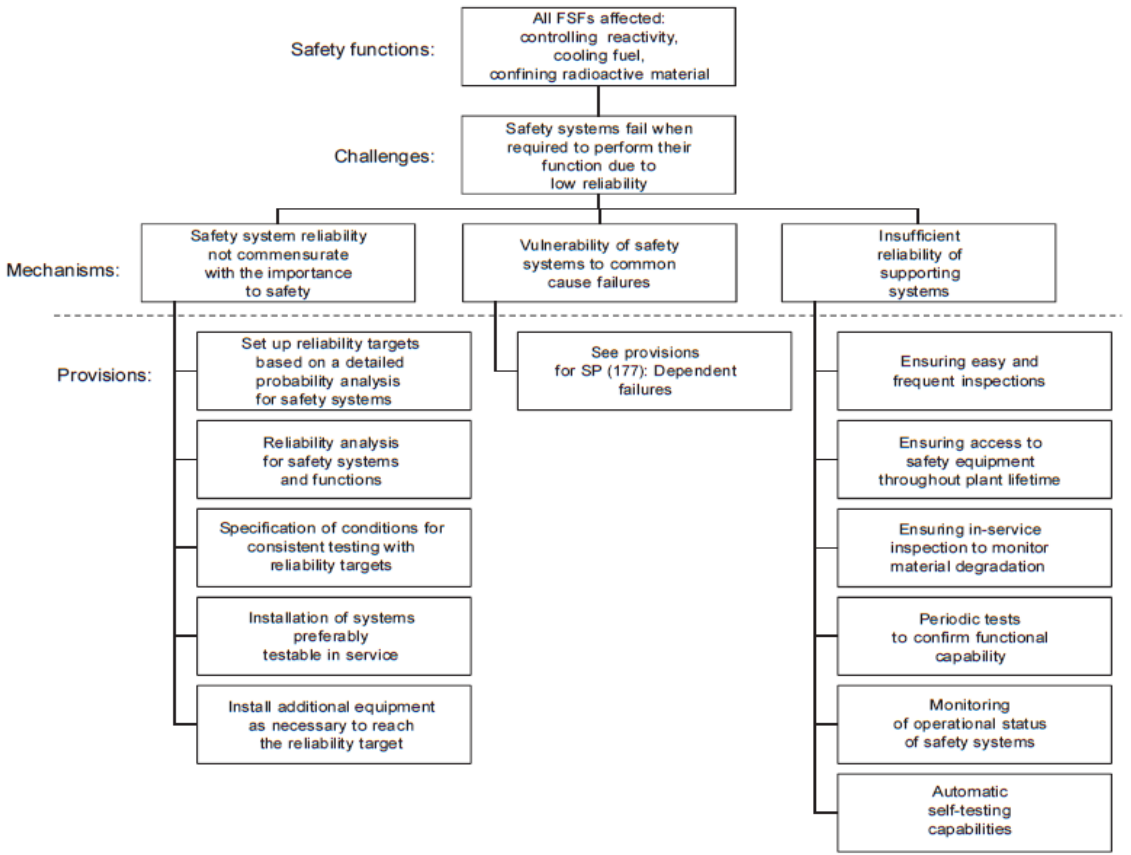


FIG. 22. Objective tree for Level 3 of defence in depth. Safety principle (174): reliability targets.

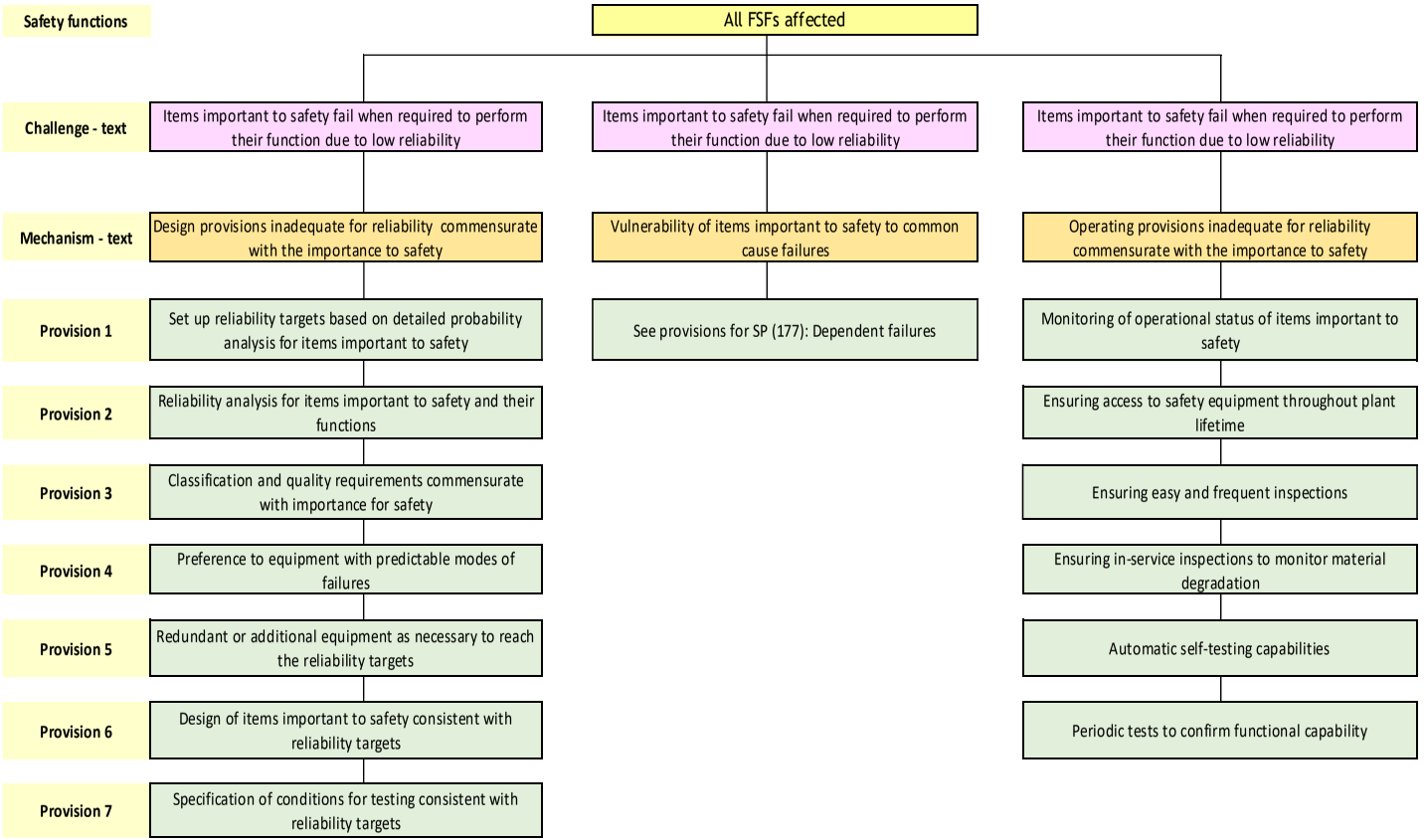


FIG. 22. Updated. Objective tree for Level 1-4 of defence in depth. Safety principle (174): reliability targets.

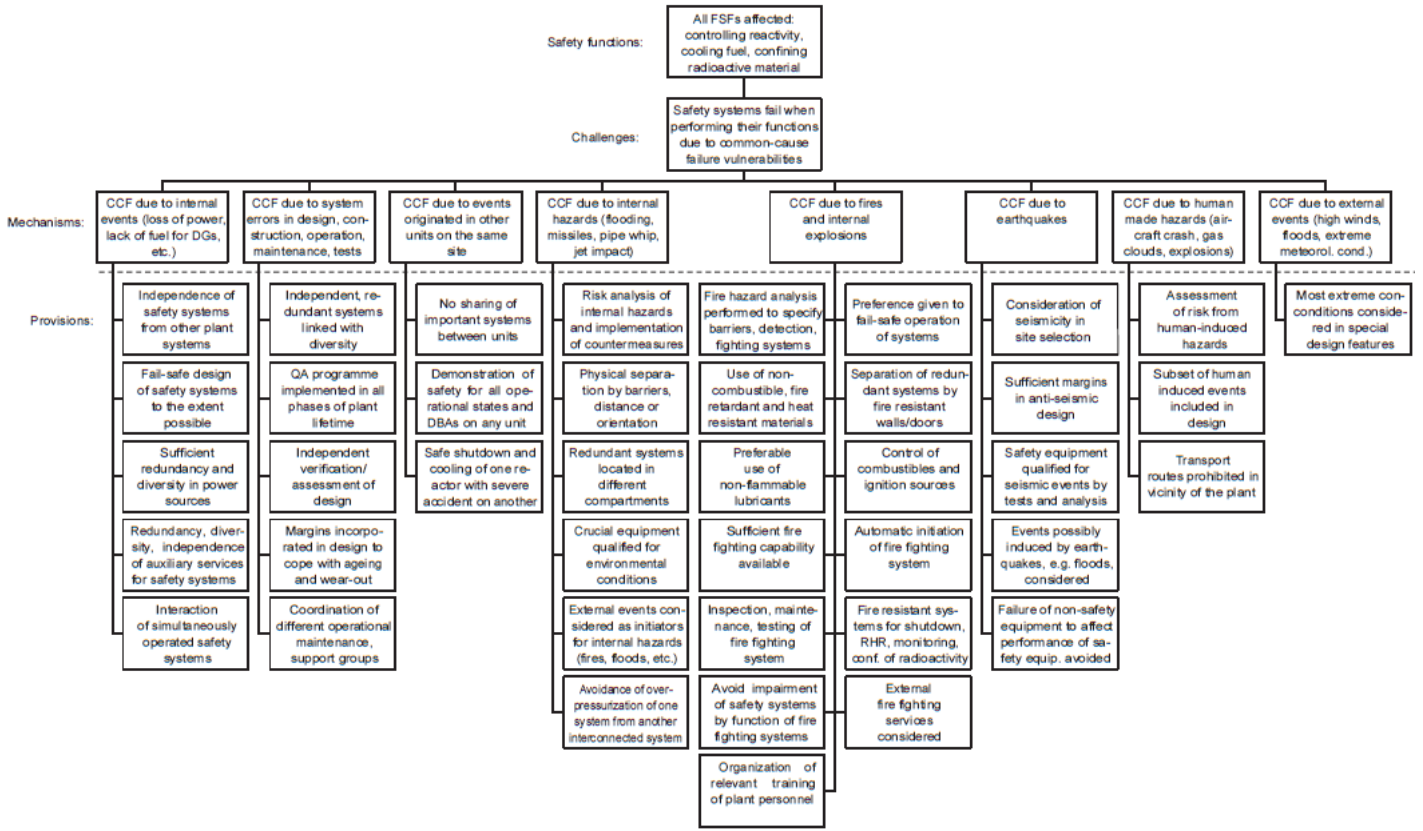


FIG. 23. Objective tree for Level 3 of defence in depth. Safety principle (177): dependent failures.

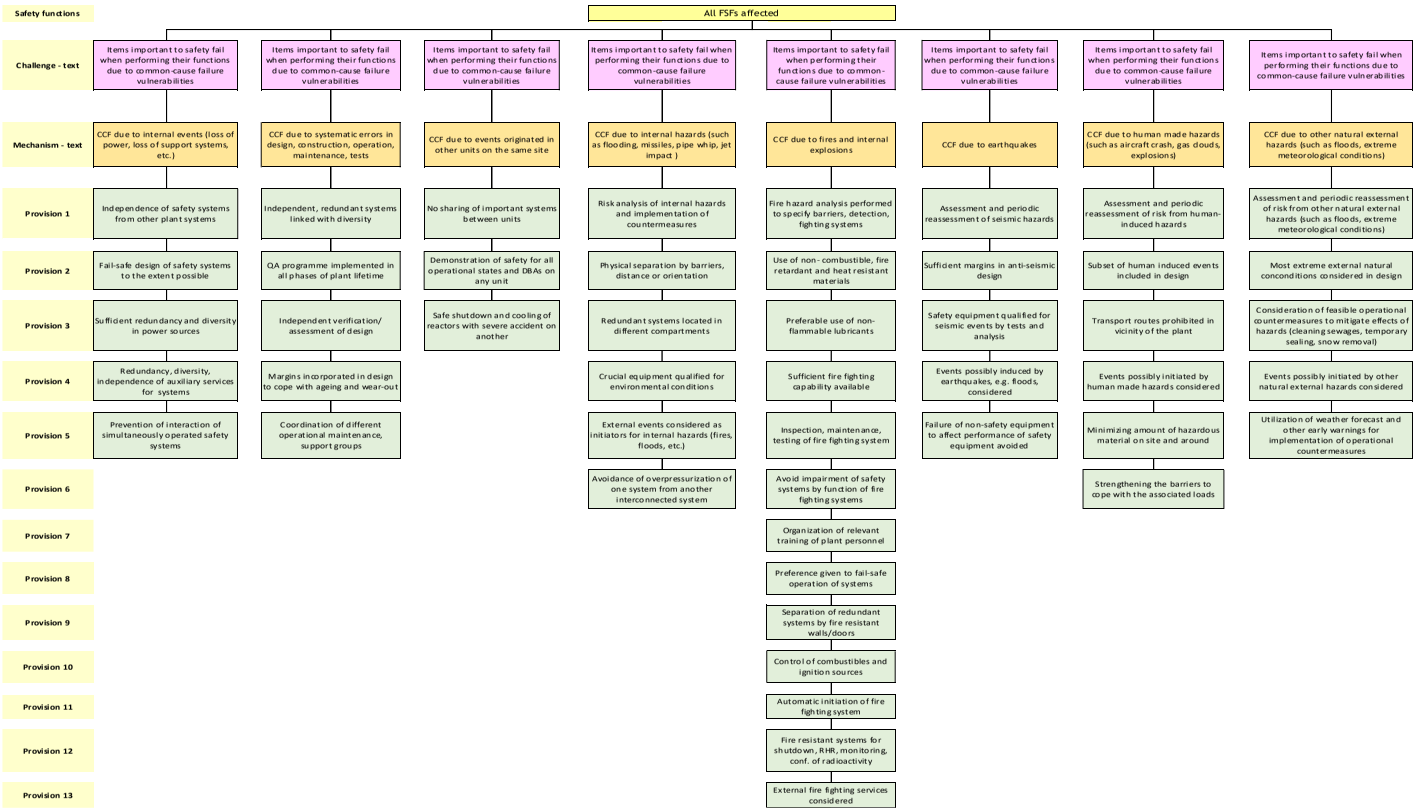


FIG 23 Updated. Objective tree for Levels 3 -4 of defence in depth. Safety principle (177): dependent failures.

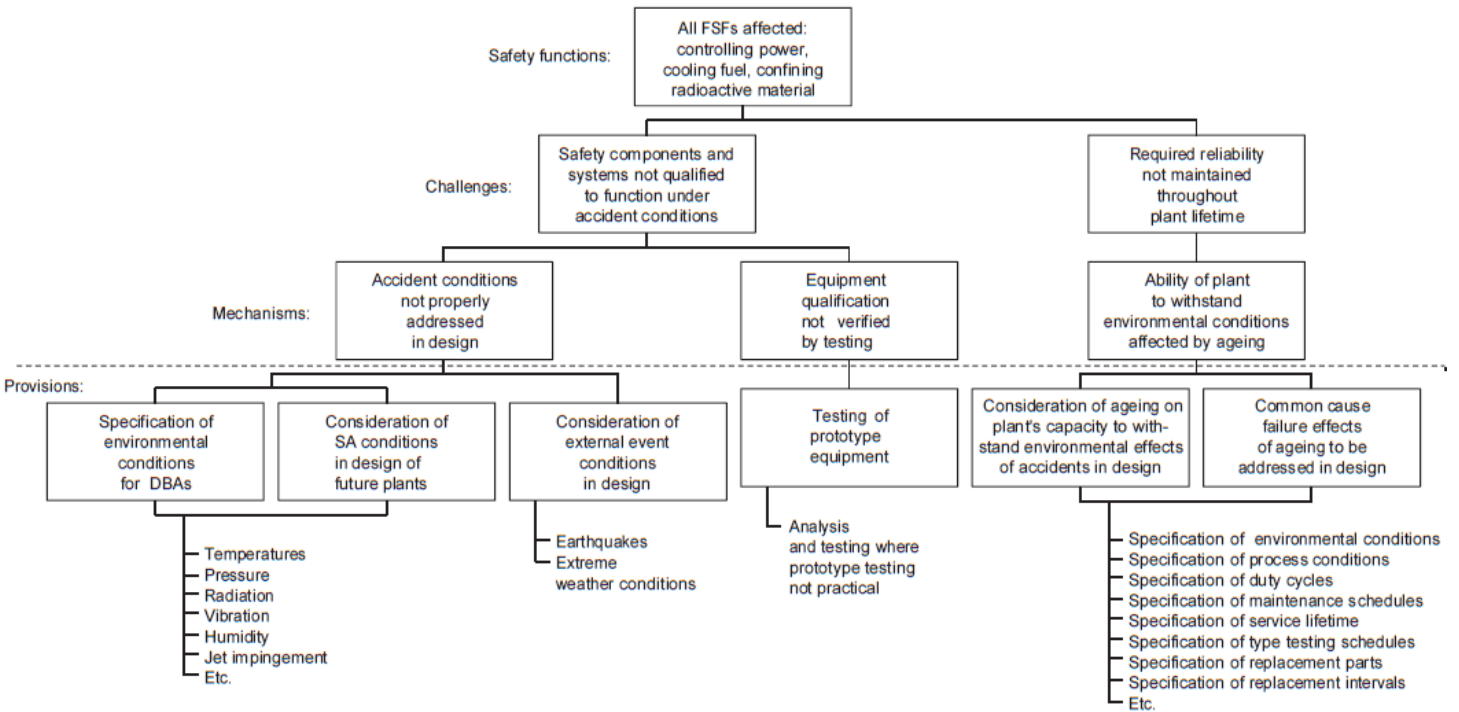


FIG. 24. Objective tree for Level 3 of defence in depth. Safety principle (182): equipment qualification.

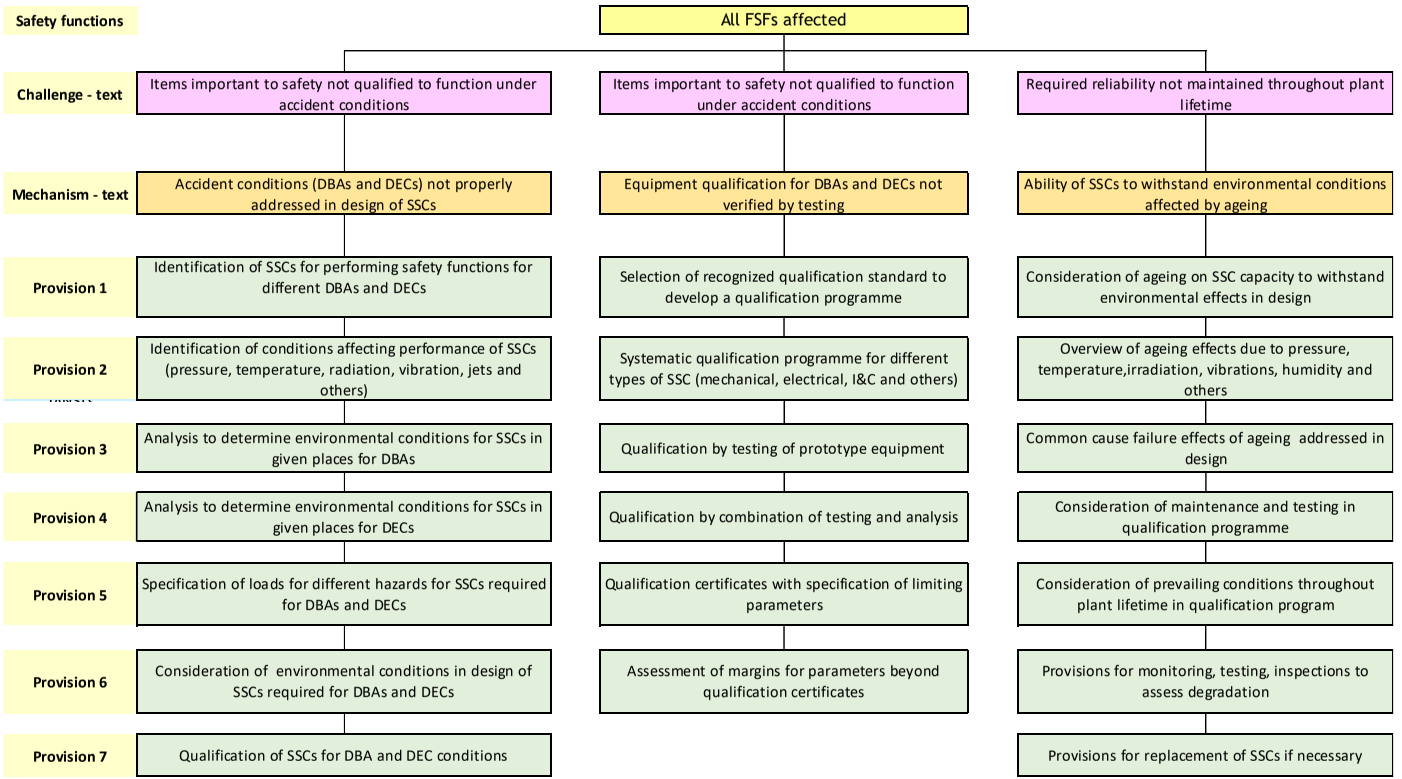


FIG. 24. Updated. Objective tree for Levels 3-4 of defence in depth. Safety principle (182): equipment qualification.

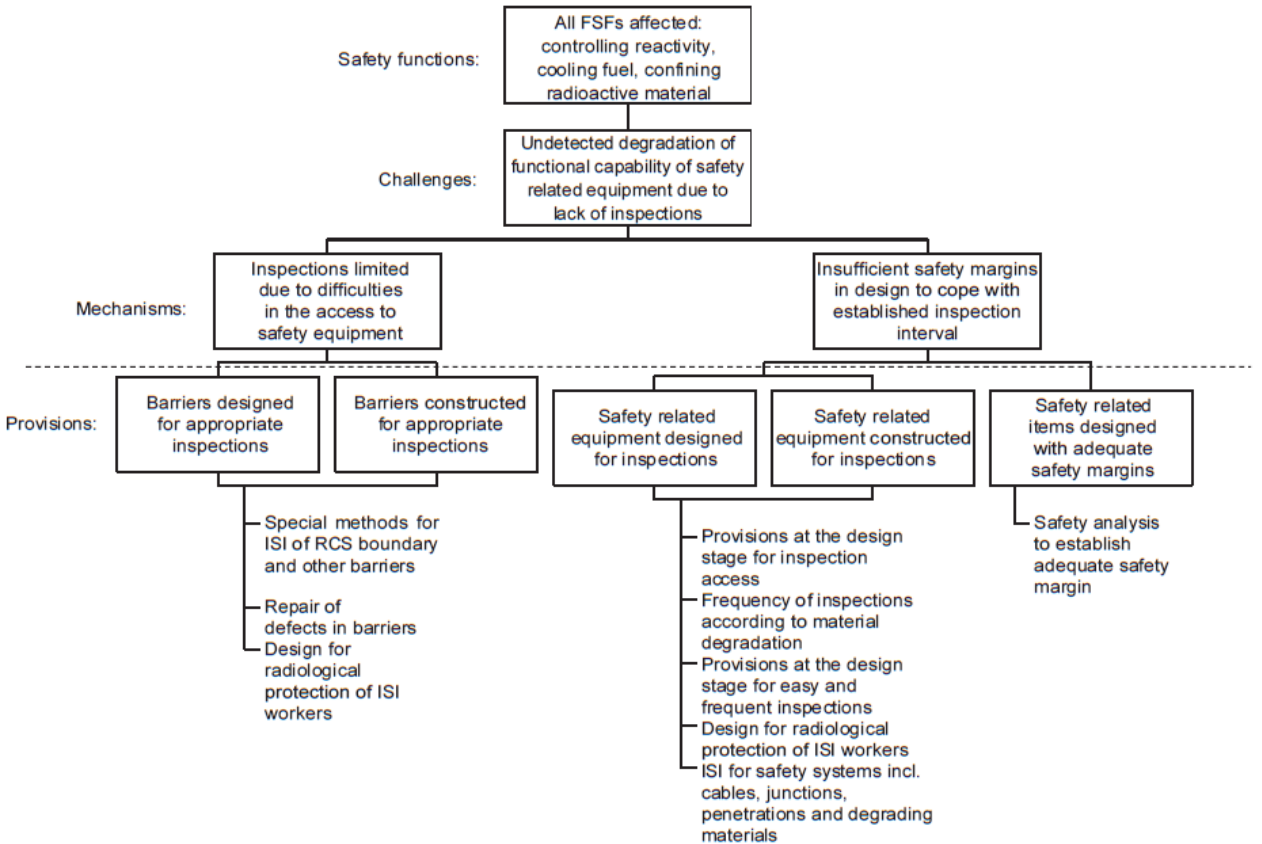


FIG. 25. Objective tree for Levels 1–4 of defence in depth. Safety principle (186): ease of access of safety equipment for inspection.

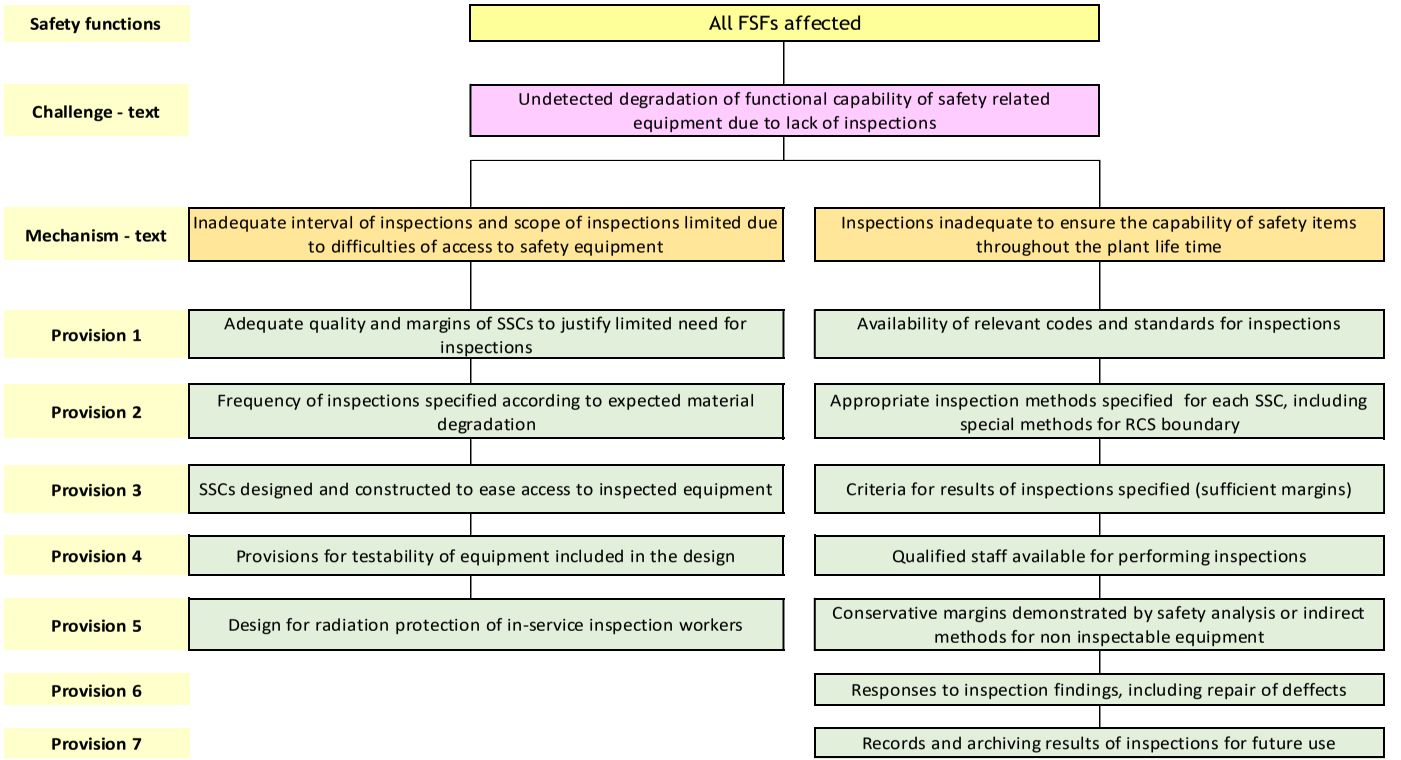


FIG. 25. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (186): ease of access of safety equipment for inspection.

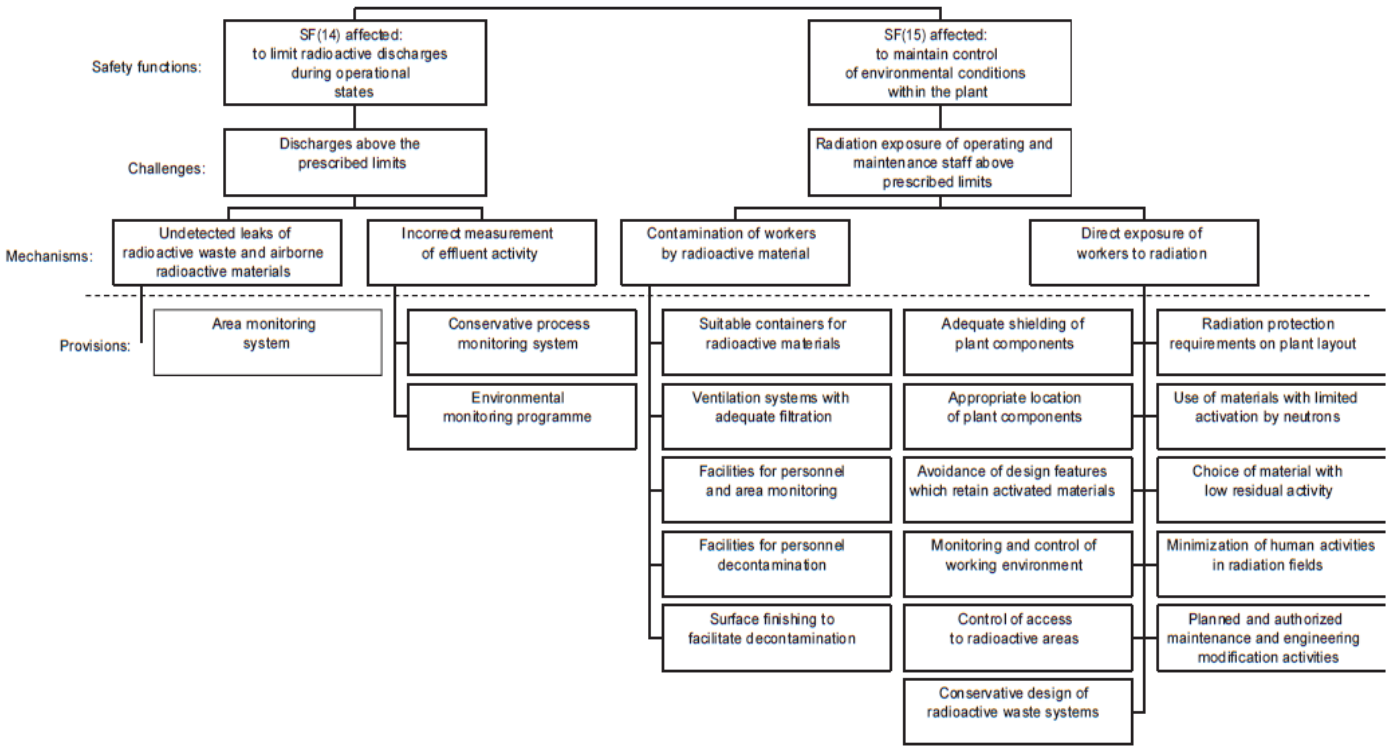


Fig. 26 Objective tree for Level 1 of defence in depth. Safety principle (188): radiation protection in design (see also SP (292)).

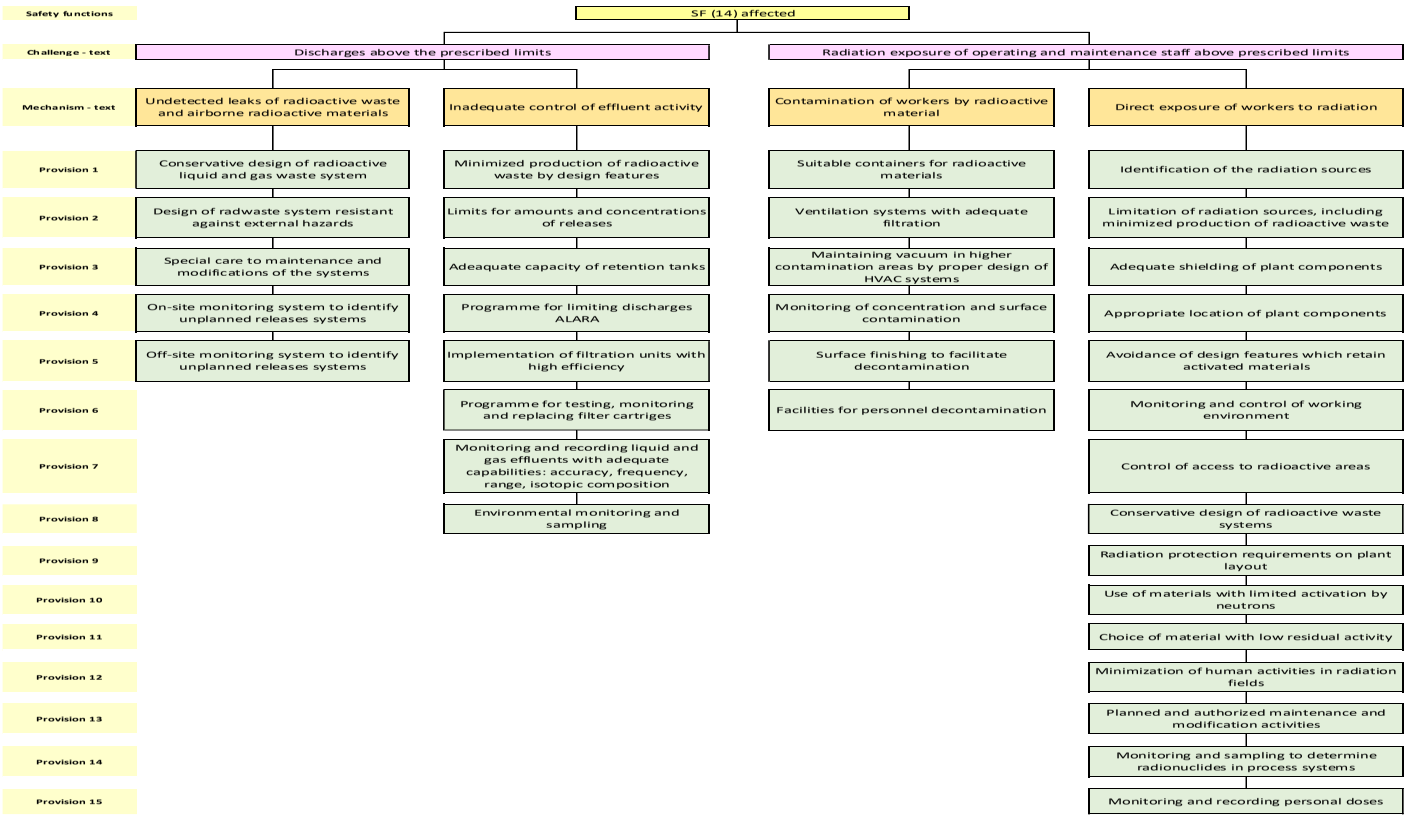


FIG. 26 Updated. Objective tree for Level 1 of defence in depth. Safety principle (188): radiation protection in design (see also SP (292)).

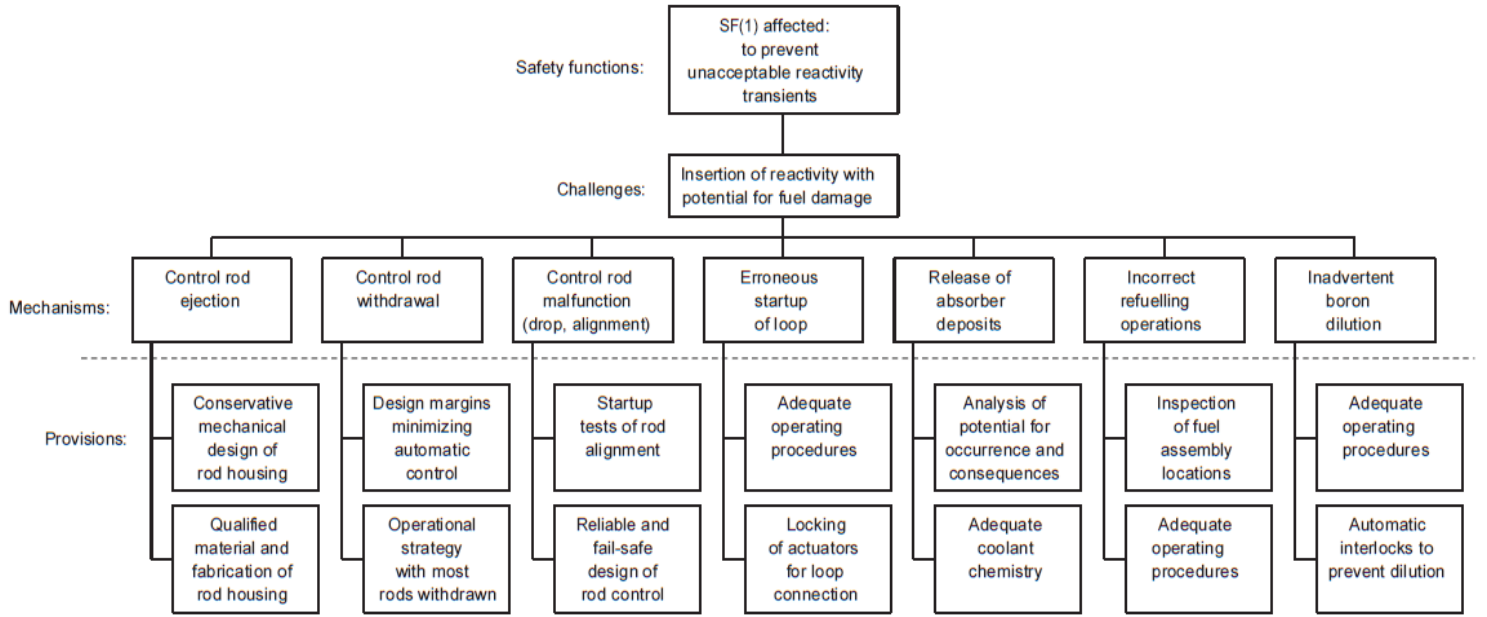


FIG. 27. Objective tree for Level 1 of defence in depth. Safety principle (192): protection against power transient accidents.

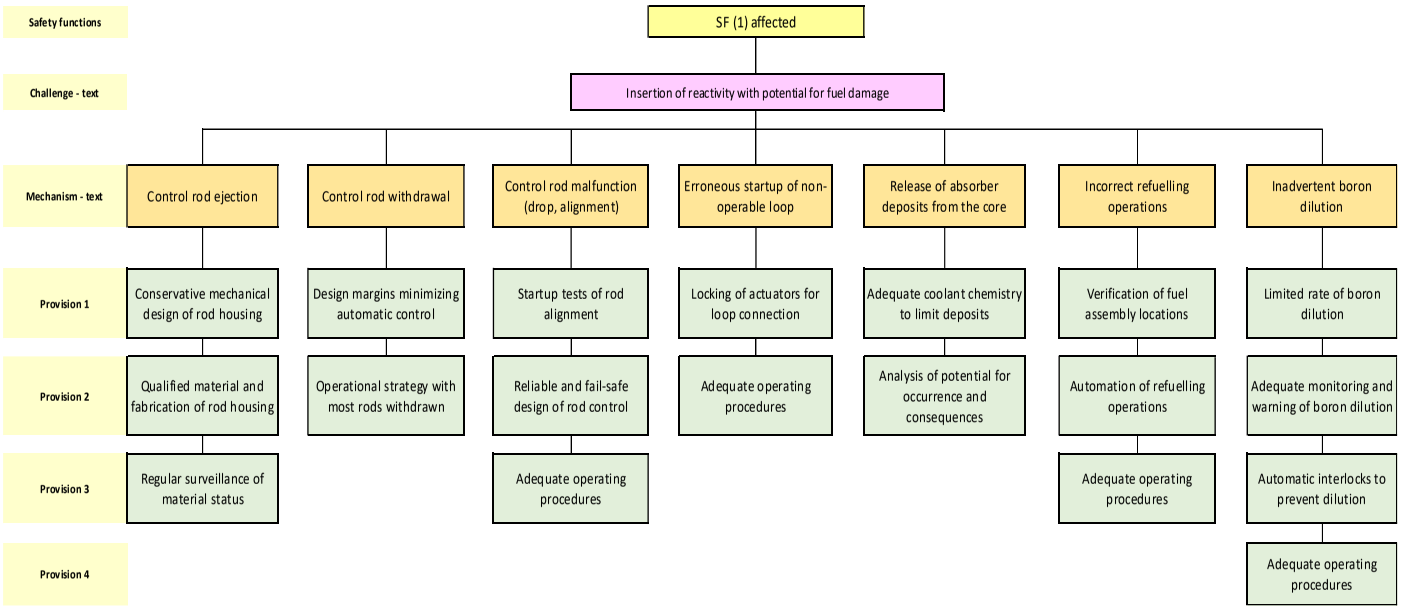


FIG. 27. Updated. Objective tree for Level 1 of defence in depth. Safety principle (192): protection against power transient accidents.

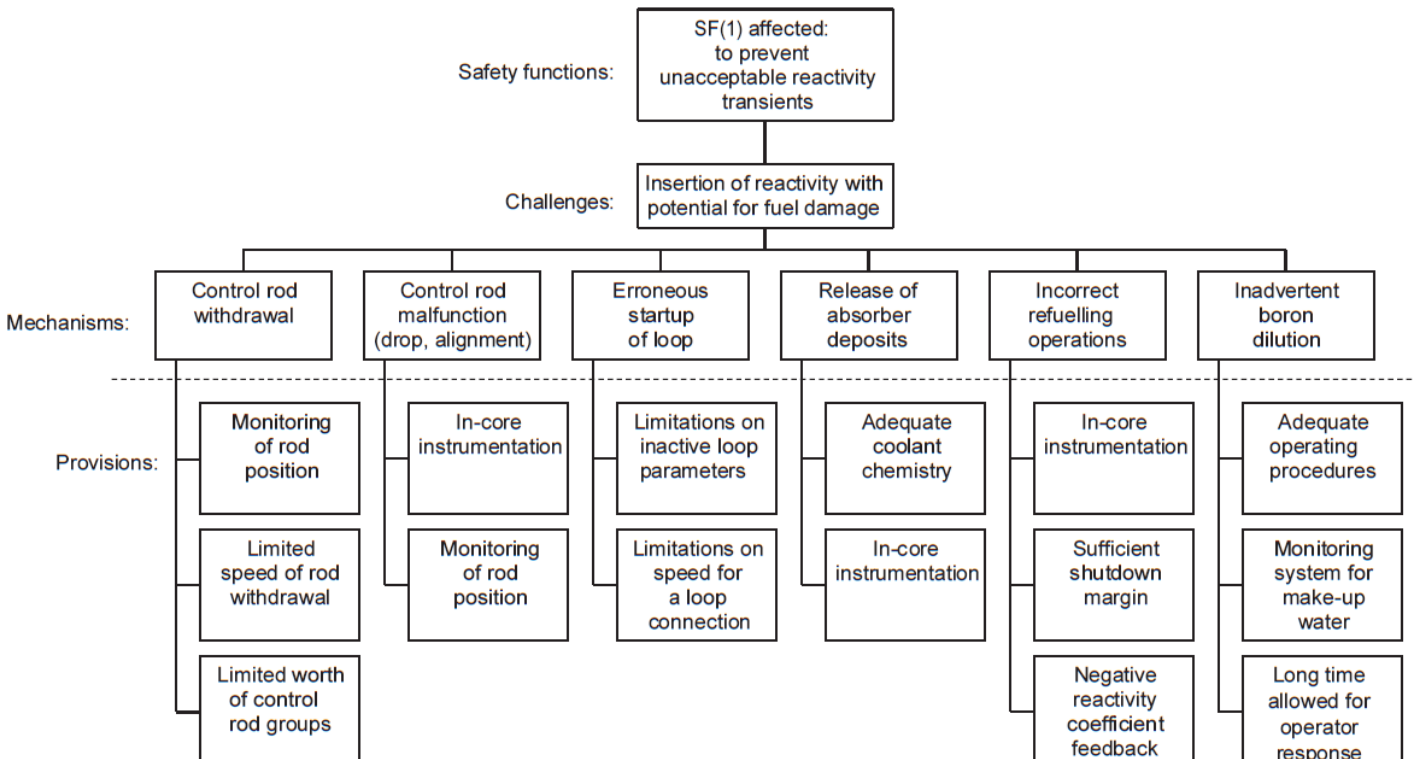


FIG. 28. Objective tree for Level 2 of defence in depth. Safety principle (192): protection against power transient accidents.

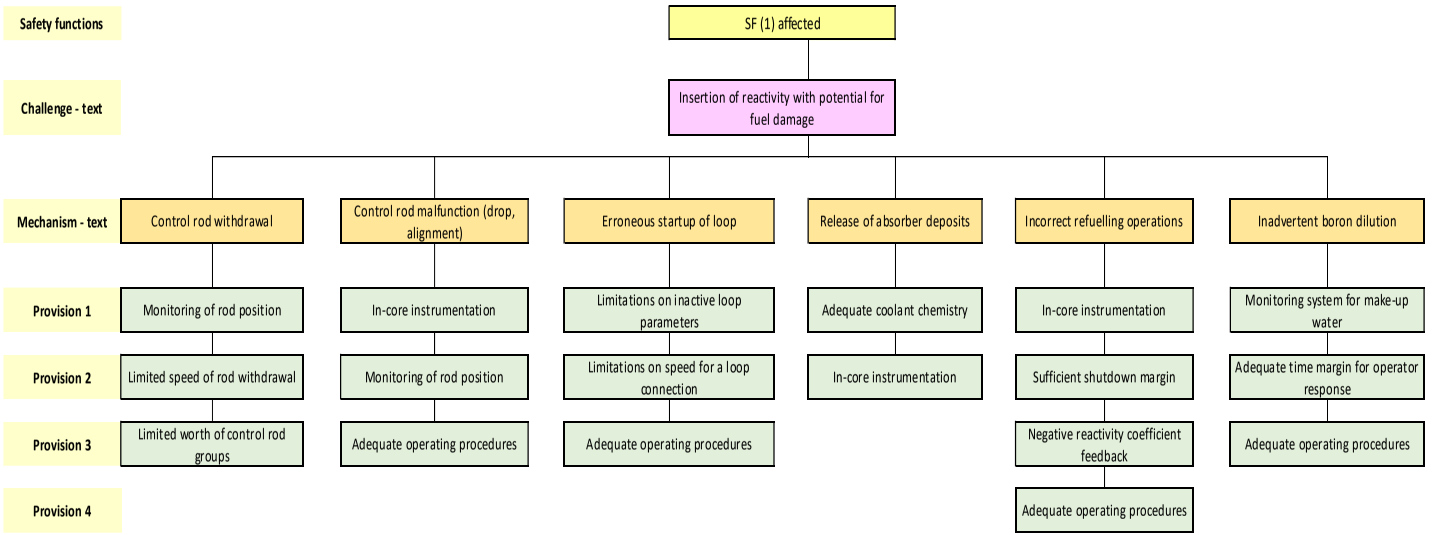


FIG. 28. Updated. Objective tree for Level 2 of defence in depth. Safety principle (192): protection against power transient accidents.

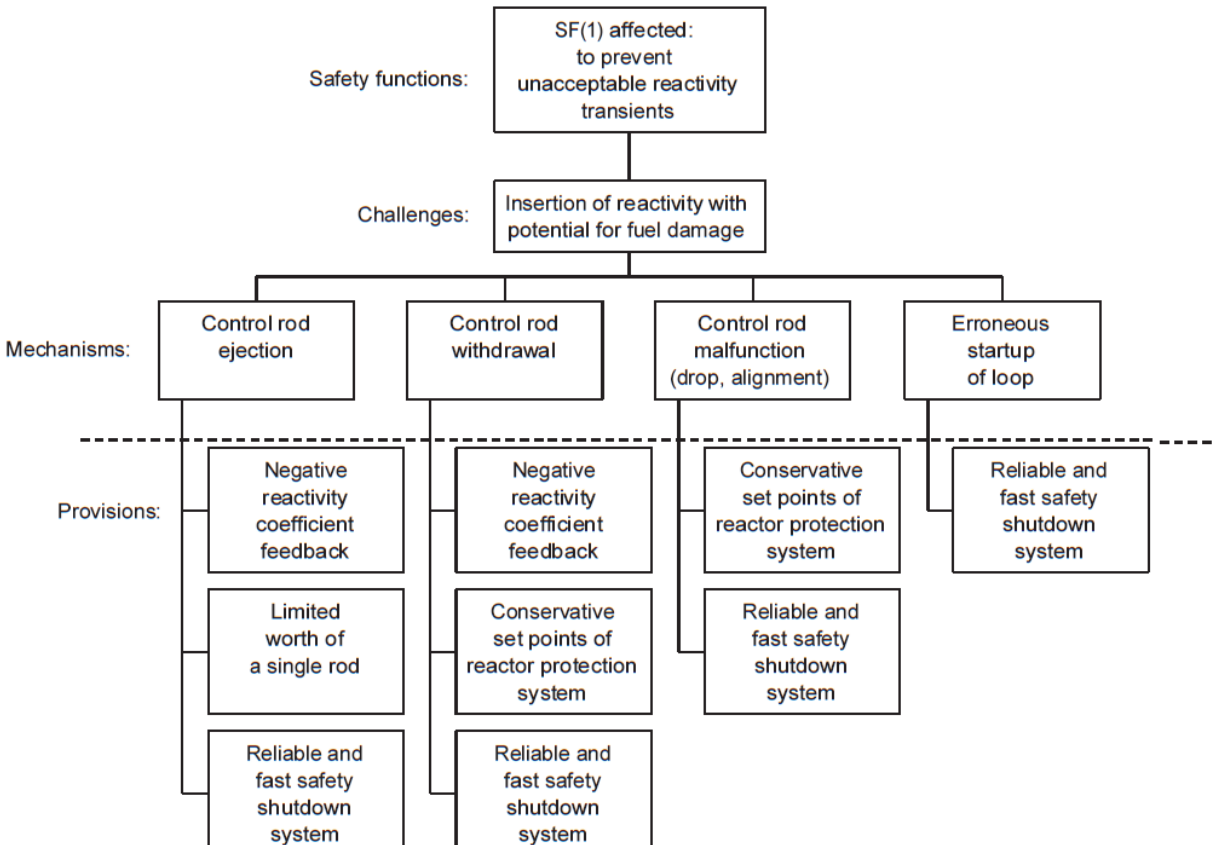


FIG. 29. Objective tree for Level 3 of defence in depth. Safety principle (192): protection against power transient accidents.

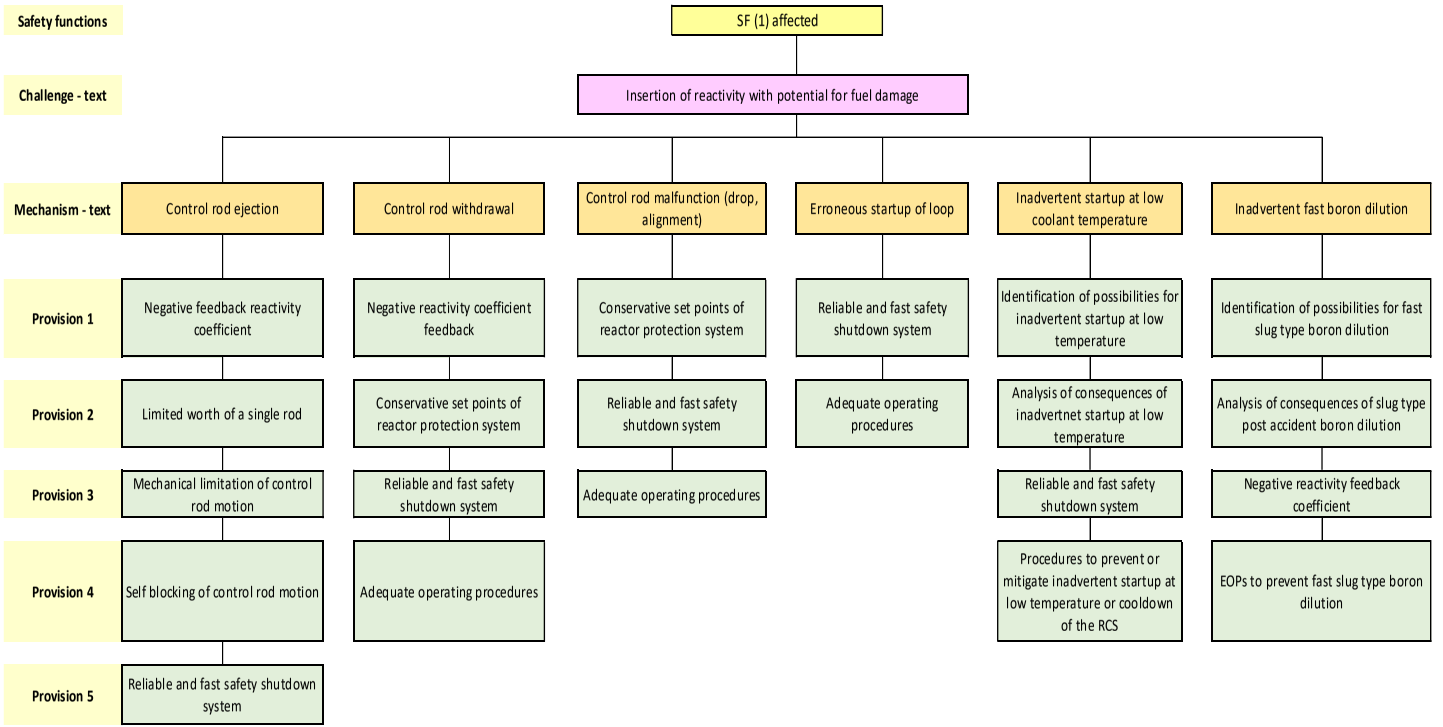


FIG. 29. Updated. Objective tree for Level 3 of defence in depth. Safety principle (192): protection against power transient accidents.

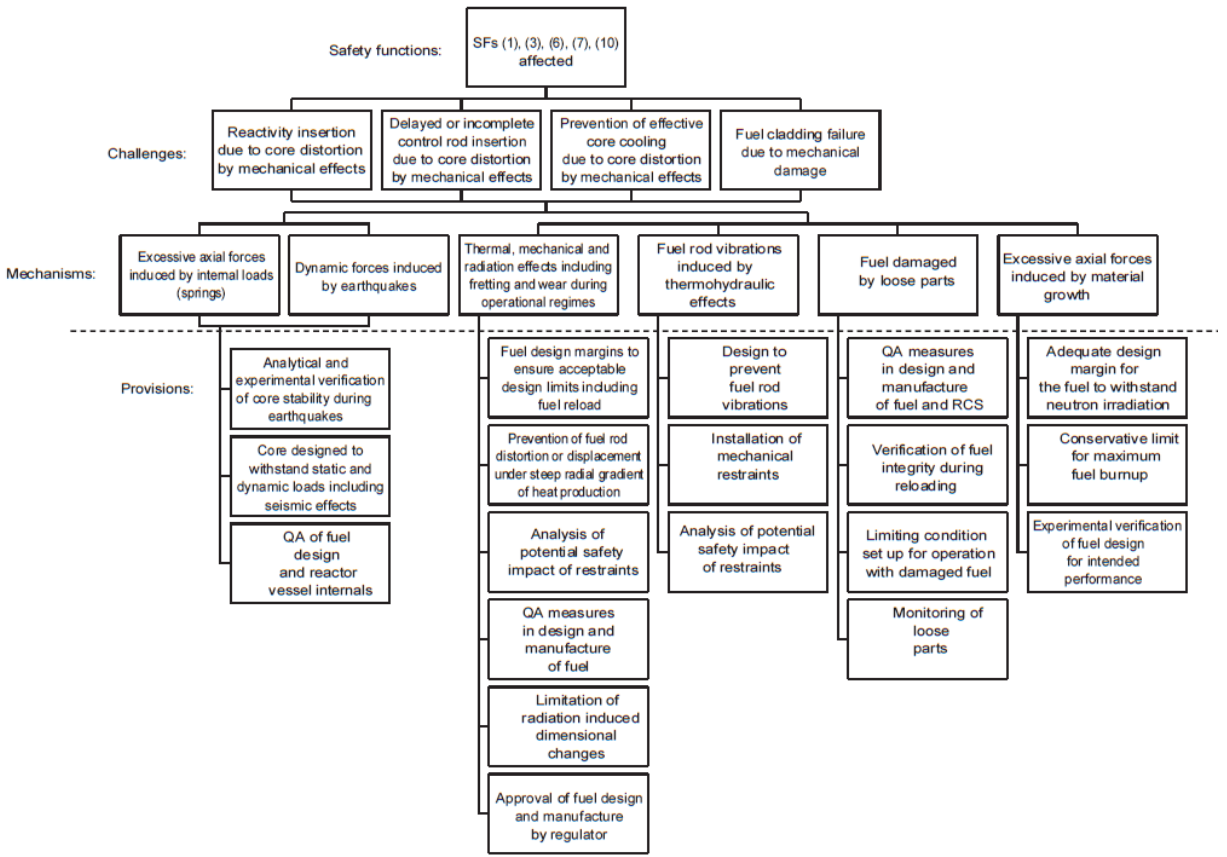


FIG. 30. Objective tree for Level 1 of defence in depth. Safety principle (195): reactor core integrity.

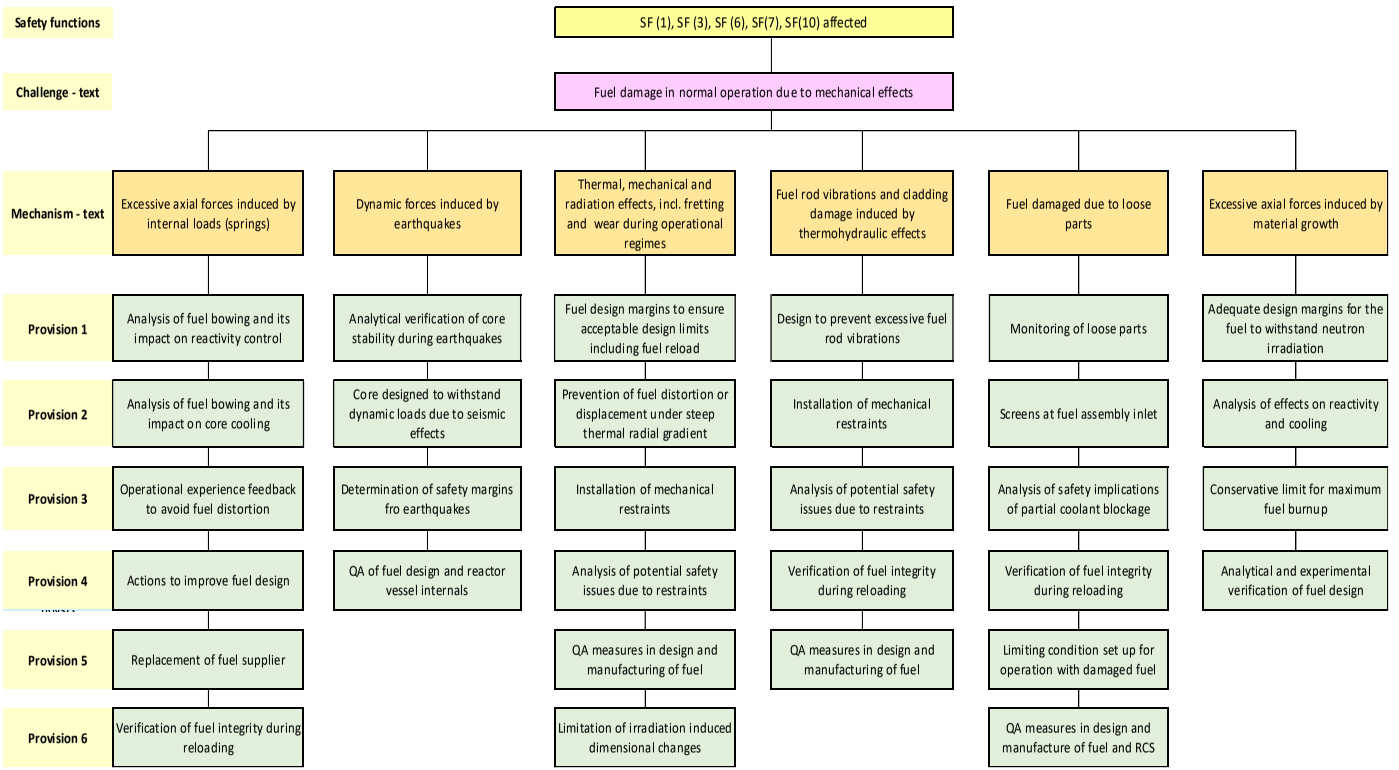


FIG. 30. Updated. Objective tree for Level 1 of defence in depth. Safety principle (195): reactor core integrity.

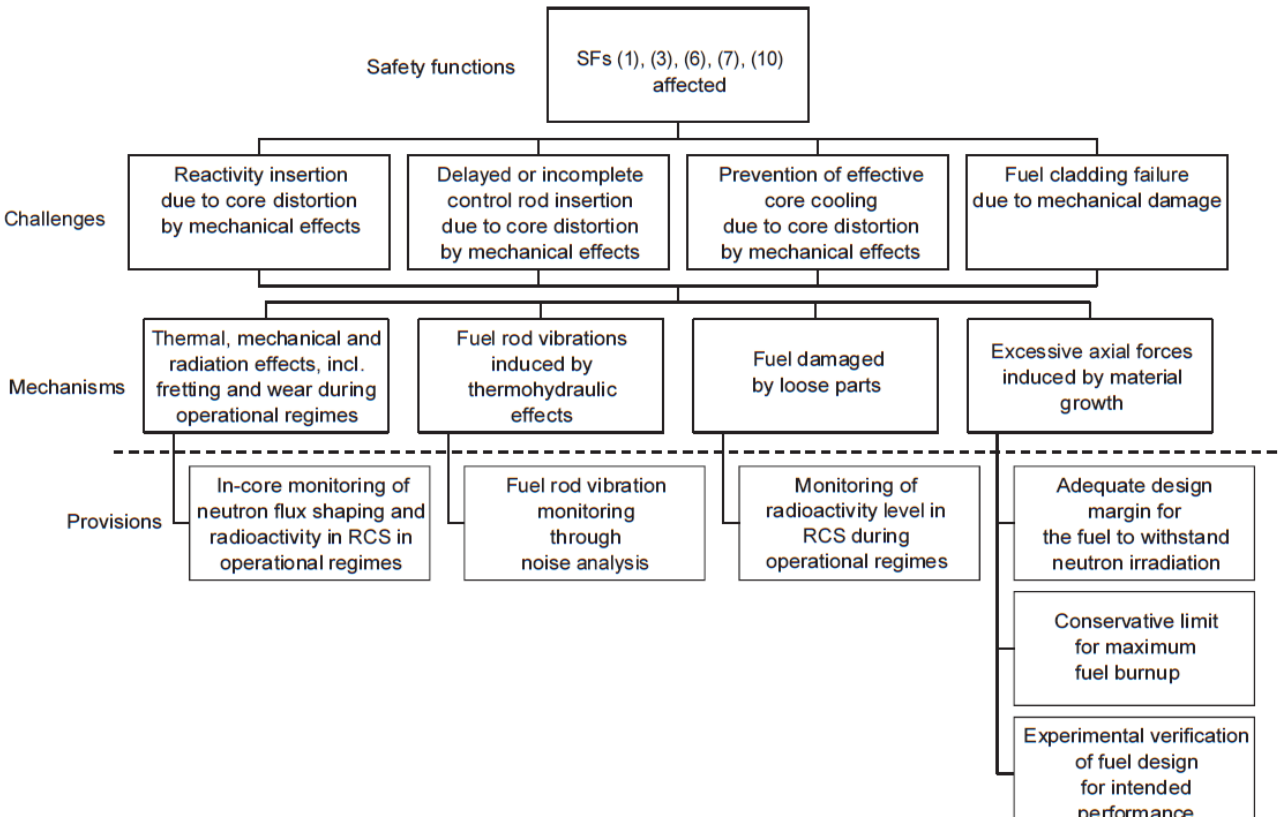


FIG. 31. Objective tree for Level 2 of defence in depth. Safety principle (195): reactor core integrity.

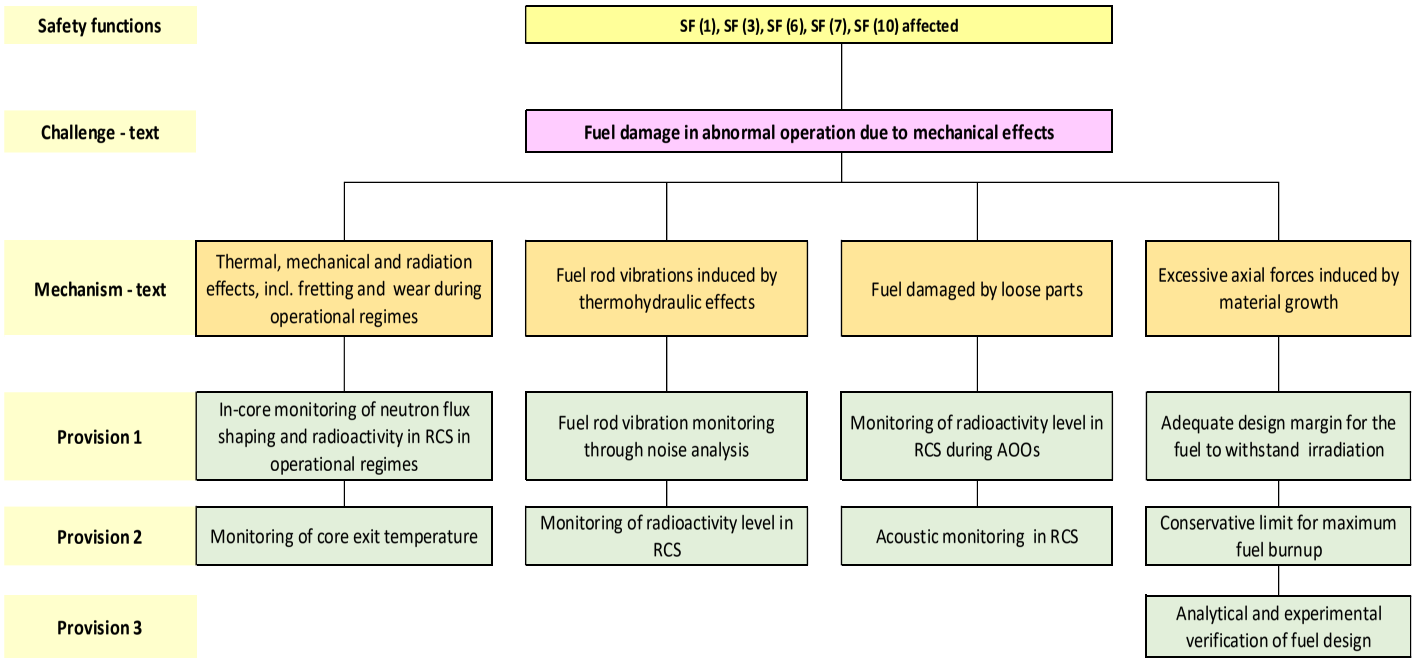


FIG. 31. Updated. Objective tree for Level 2 of defence in depth. Safety principle (195): reactor core integrity.

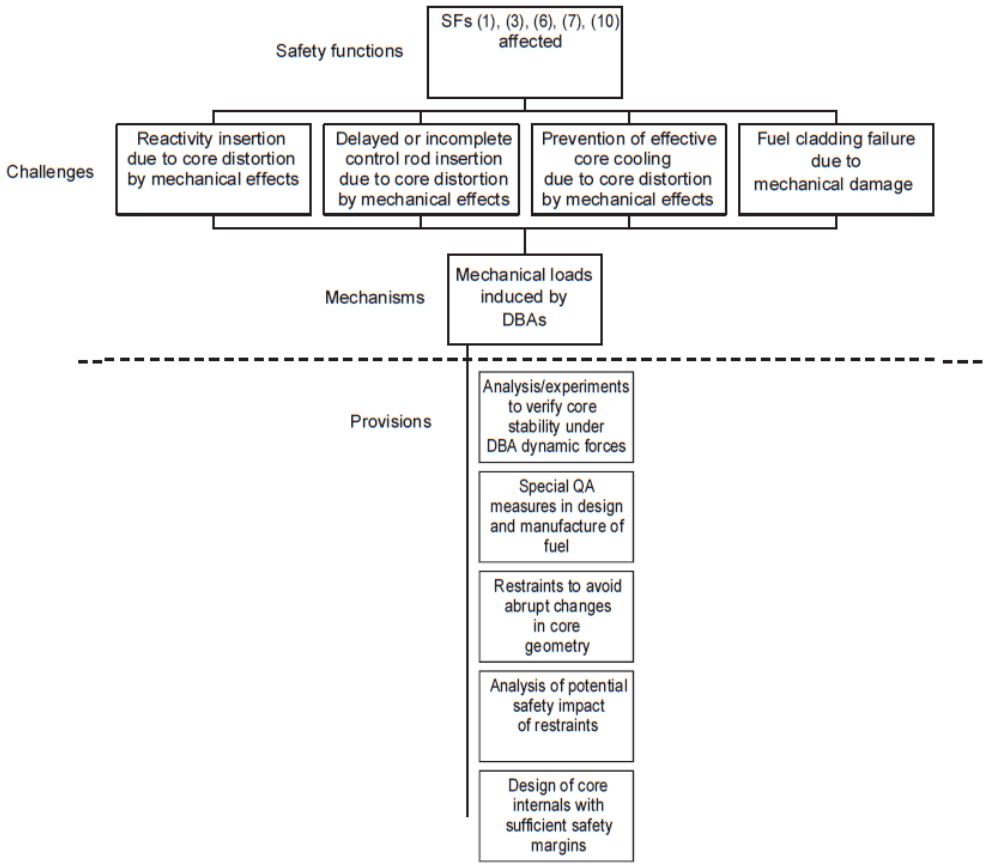


FIG. 32. Objective tree for Level 3 of defence in depth. Safety principle (195): reactor core integrity.

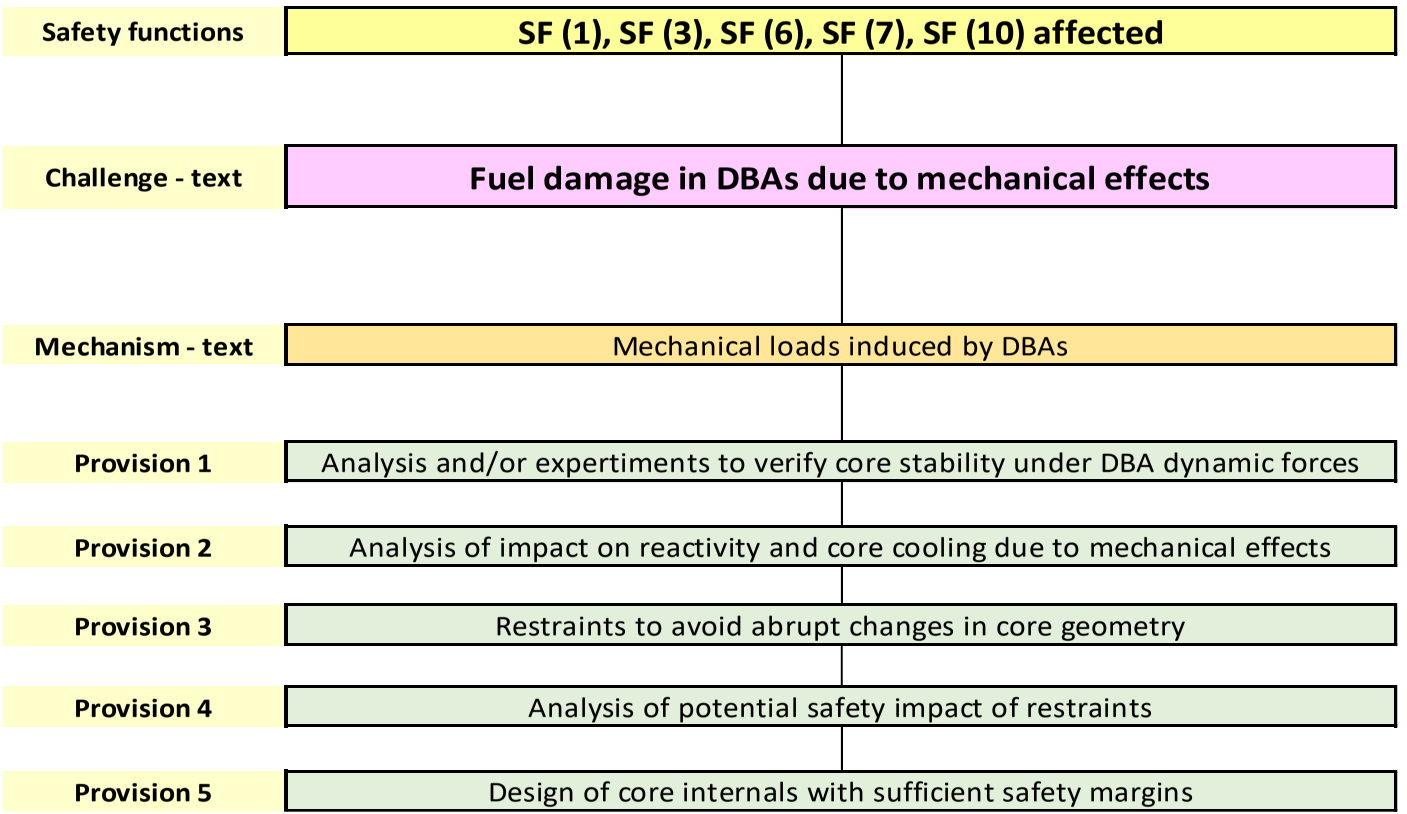


FIG. 32. Updated. Objective tree for Level 3 of defence in depth. Safety principle (195): reactor core integrity.

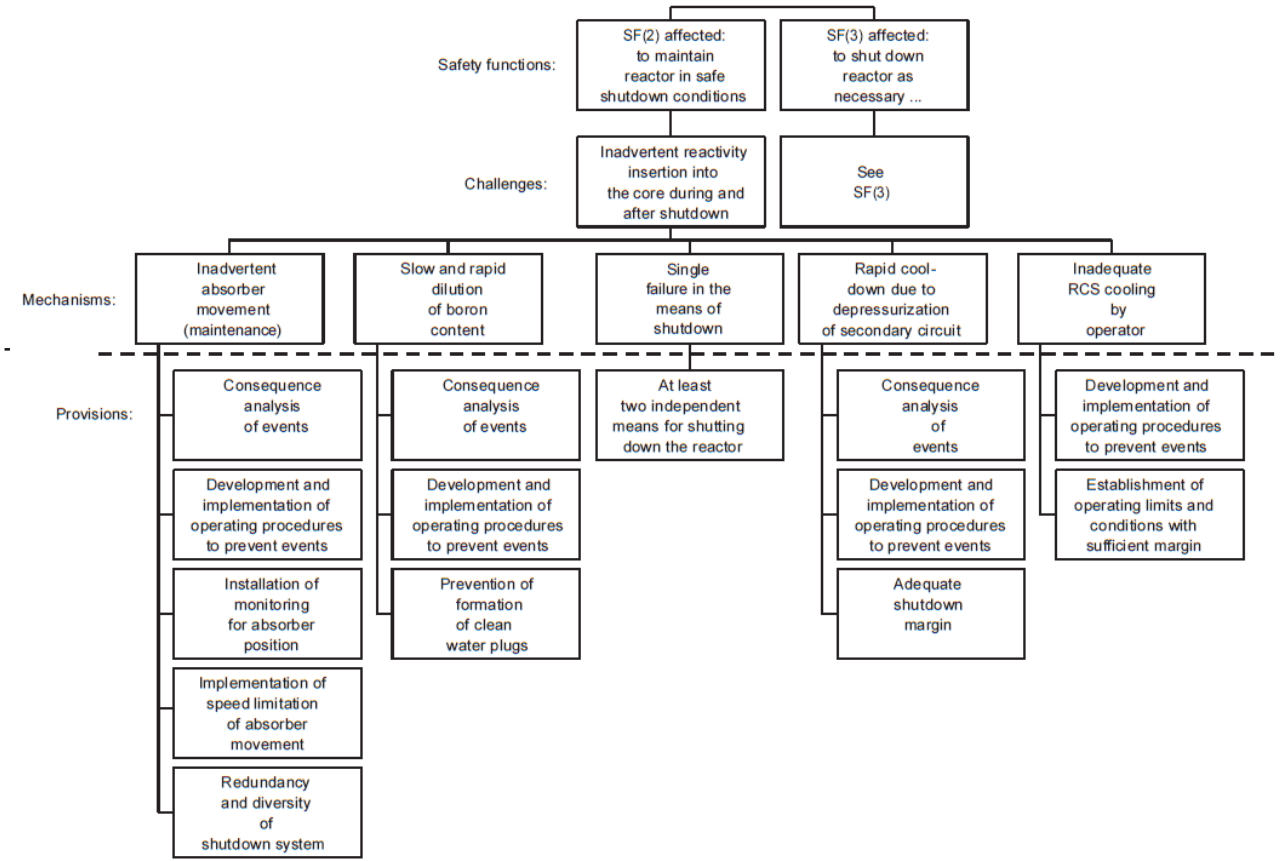


FIG. 33. Objective tree for Levels 3 and 4 of defence in depth. Safety principle (200): automatic shutdown systems, see also SF (2).

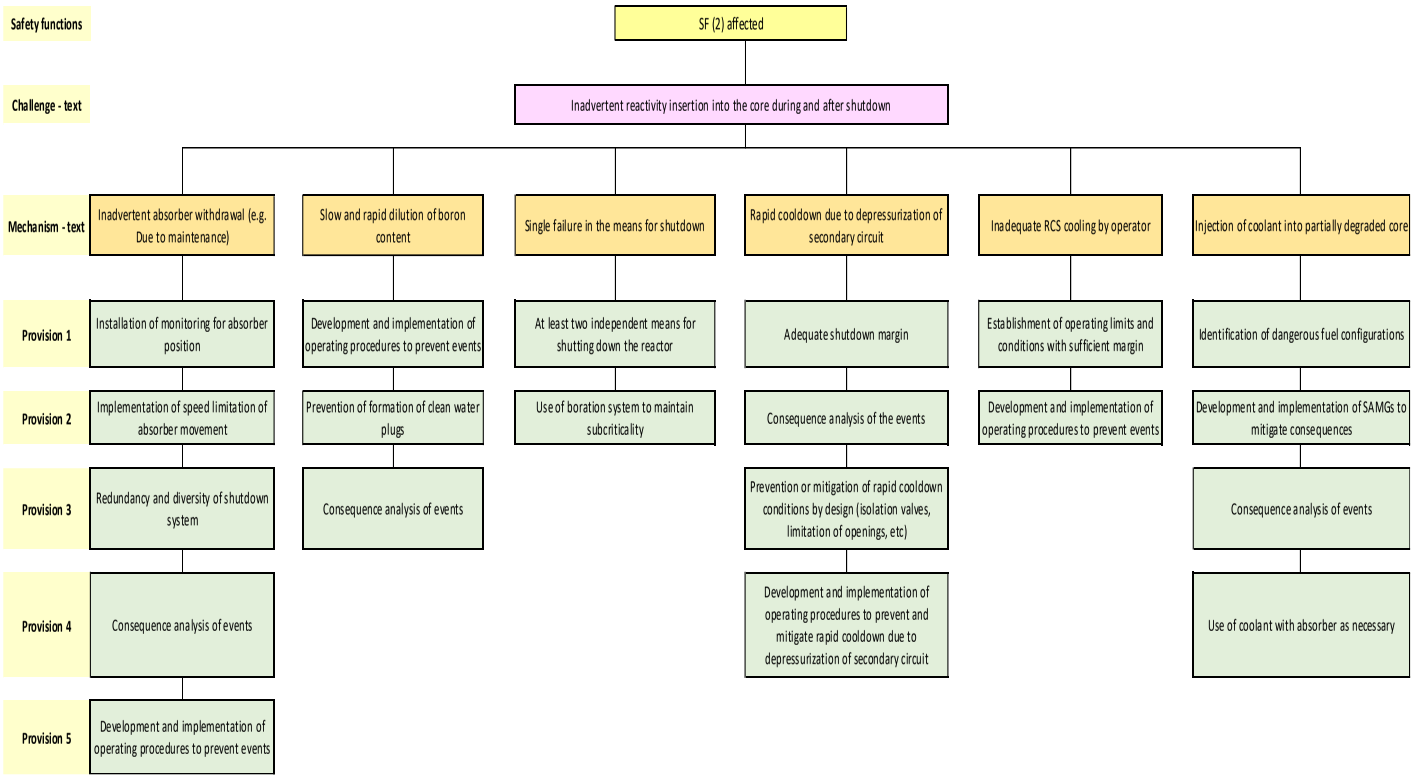


FIG 33 Updated. Objective tree for Levels 3 and 4 of defence in depth. Safety principle (200): automatic shutdown systems, see also SF (2).

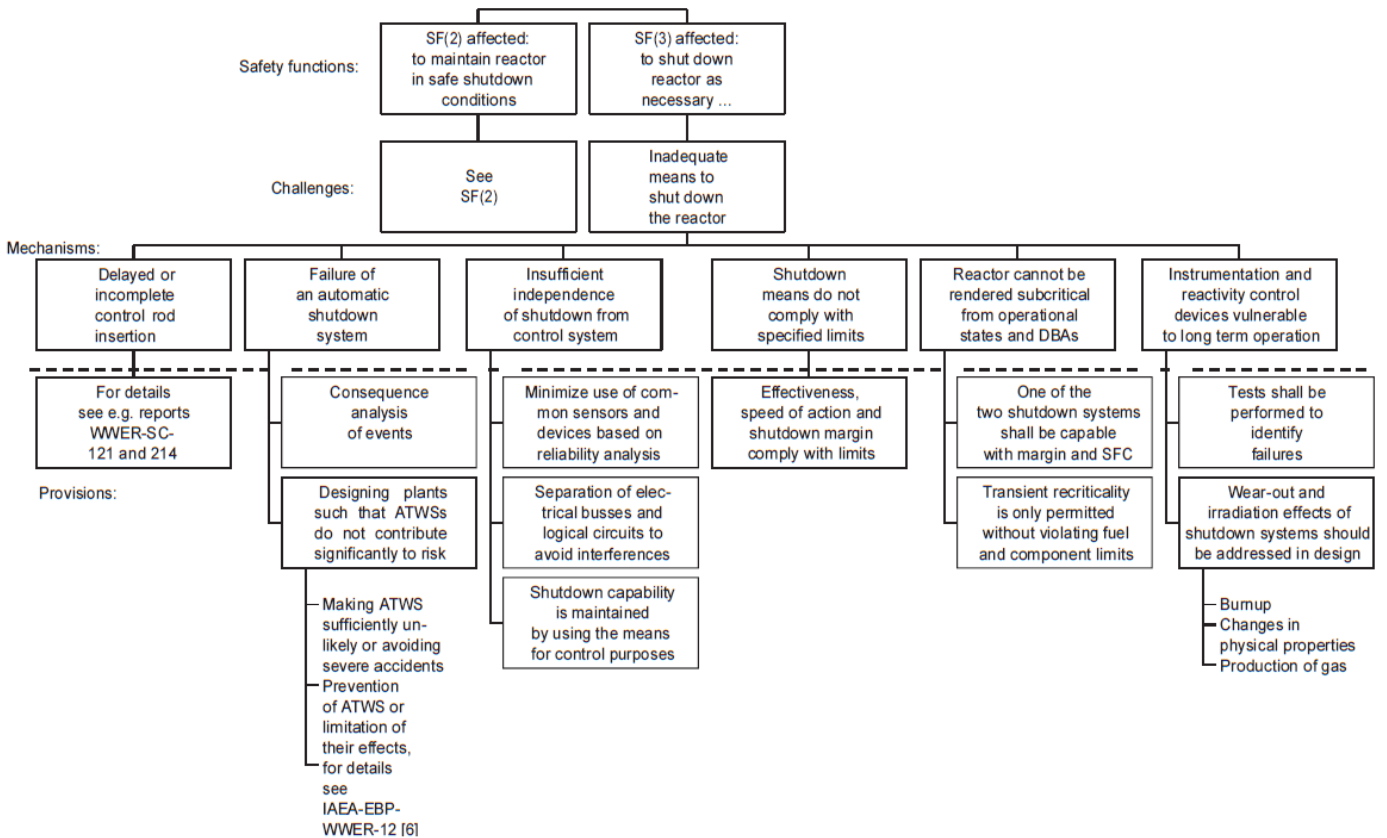


FIG. 34. Objective tree for Levels 3 and 4 of defence in depth. Safety principle (200): automatic shutdown systems, see also SF (3).

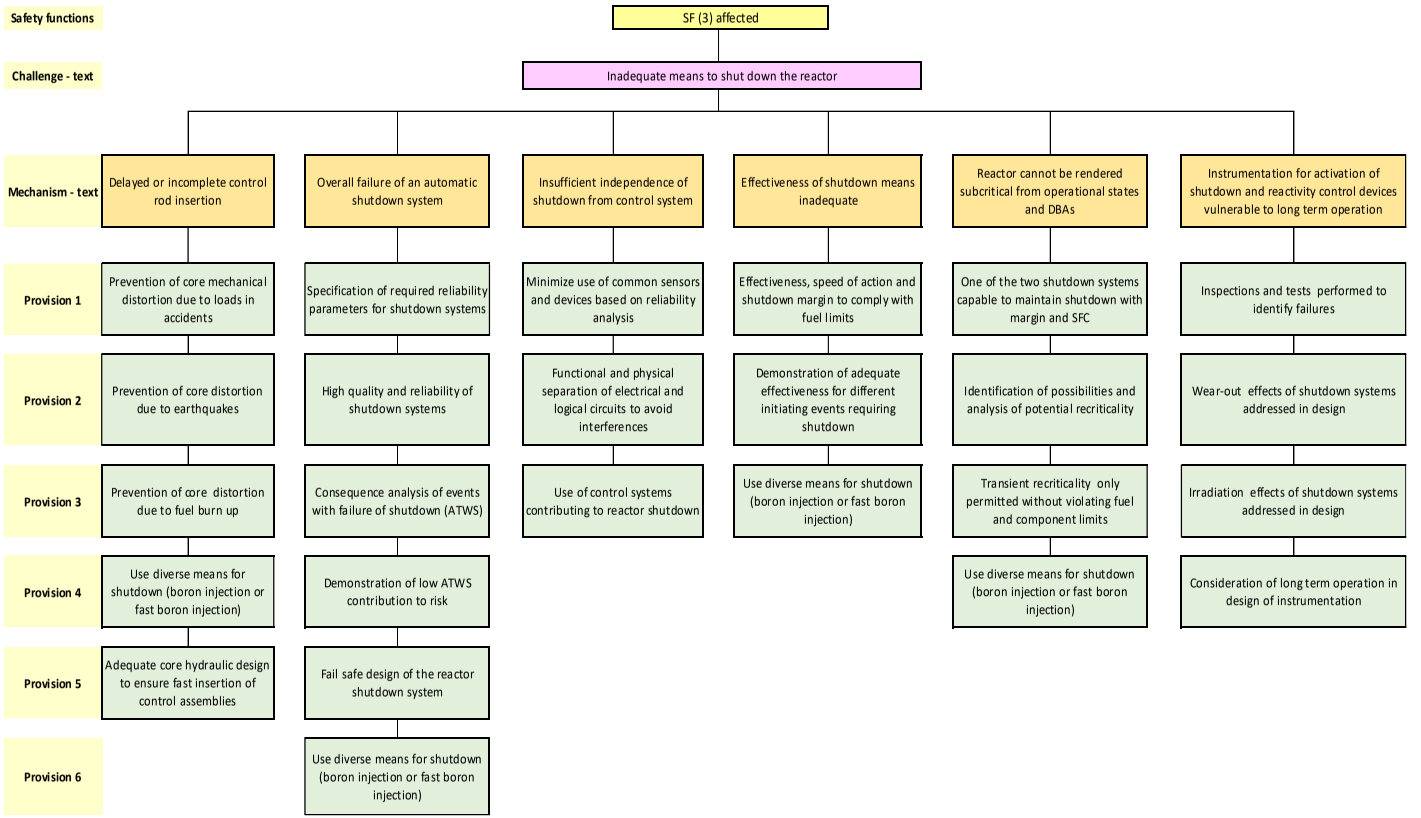


FIG. 34. Updated. Objective tree for Levels 3 and 4 of defence in depth. Safety principle (200): automatic shutdown systems, see also SF (3).

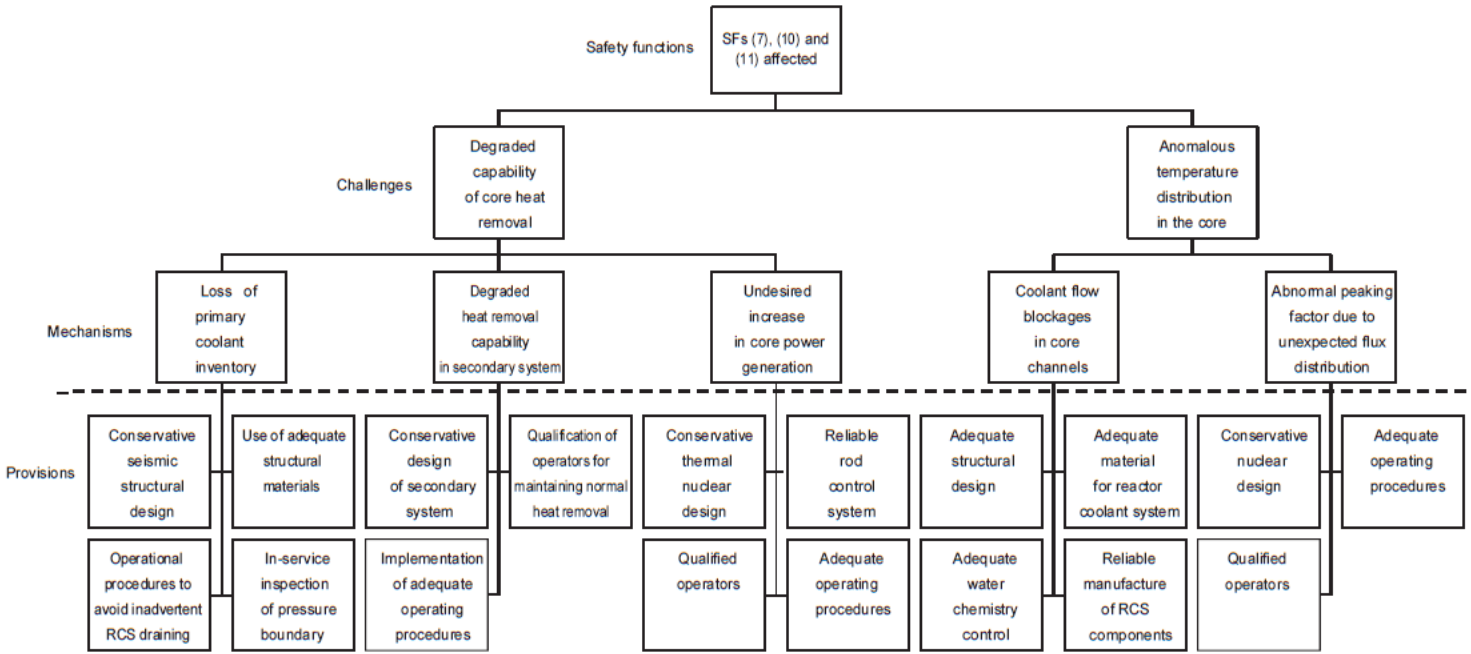


FIG. 35. Objective tree for Level 1 of defence in depth. Safety principle (203): normal heat removal.

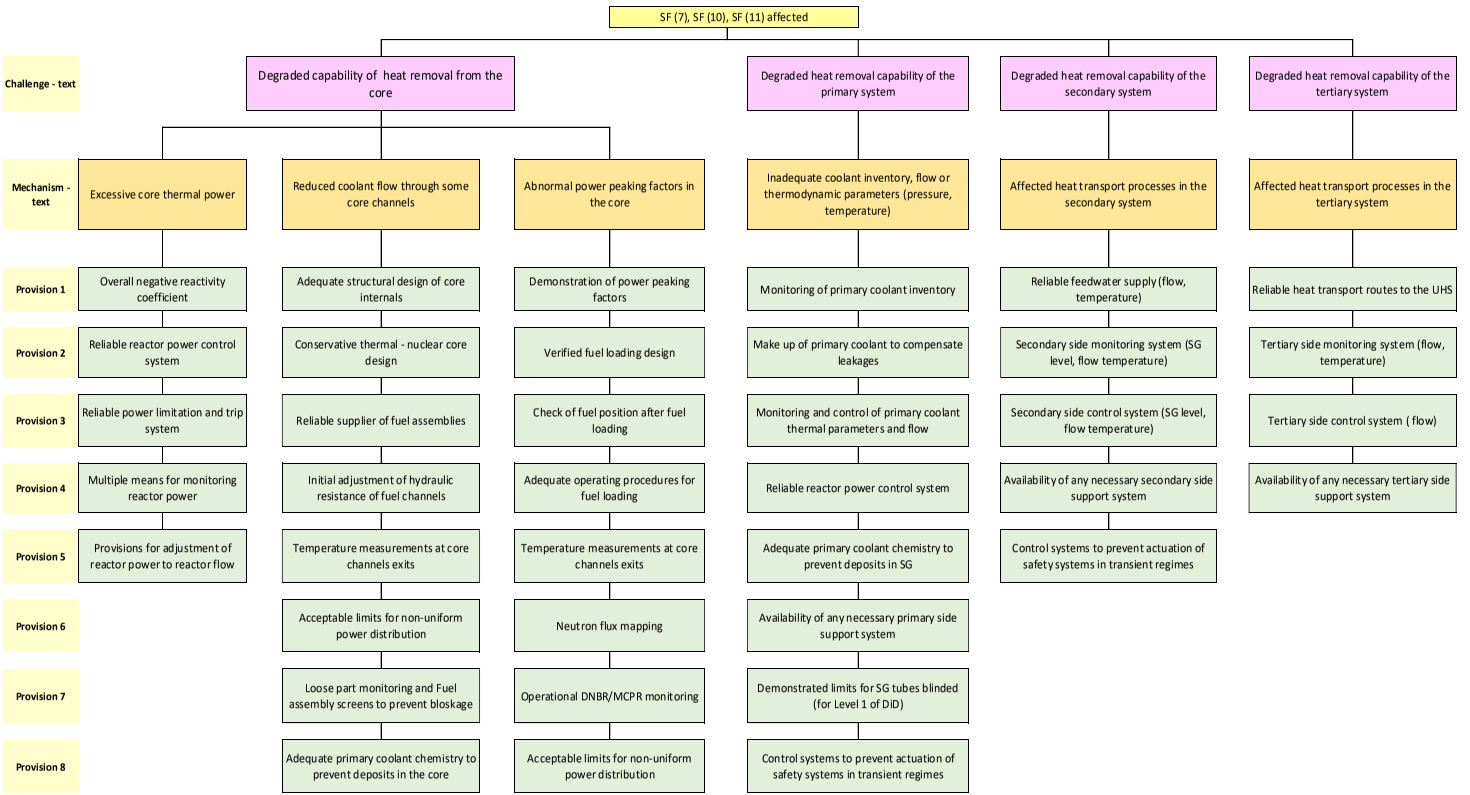


FIG. 35. Updated. Objective tree for Levels 1-2 of defence in depth. Safety principle (203): normal heat removal.

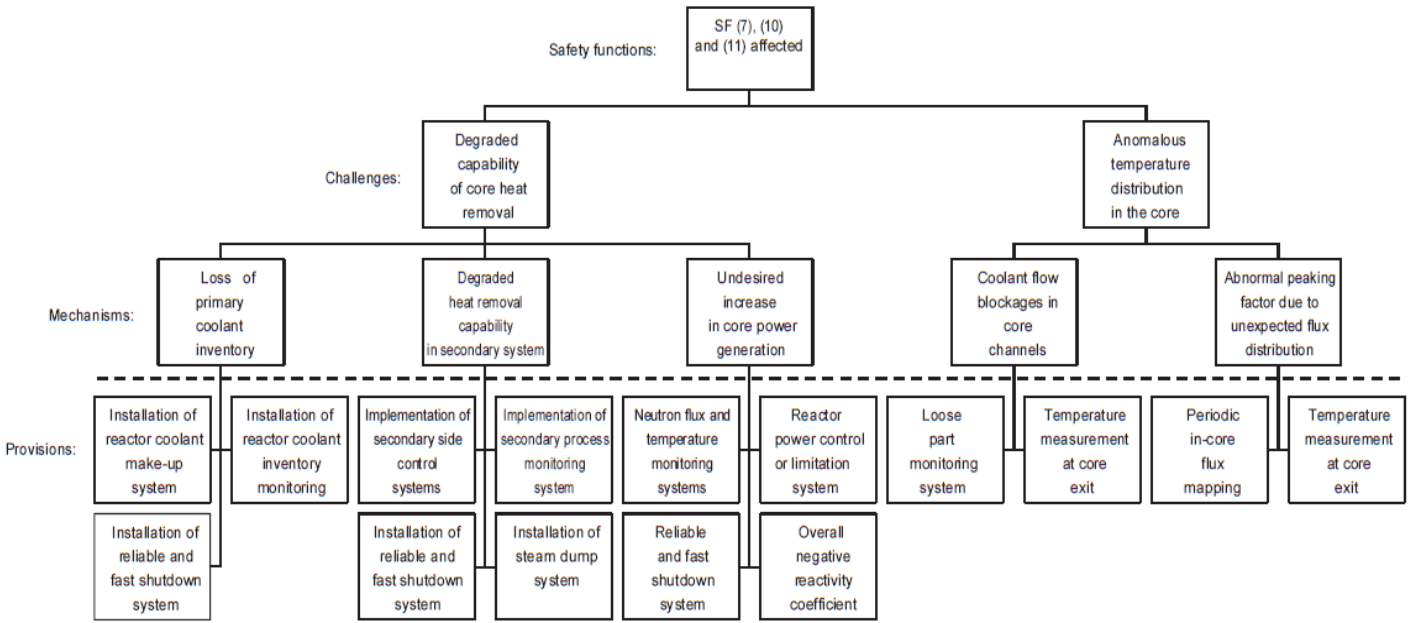


FIG. 36. Objective tree for Level 2 of defence in depth. Safety principle (203): normal heat removal.

Fig. 36 was combined with fig. 35

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

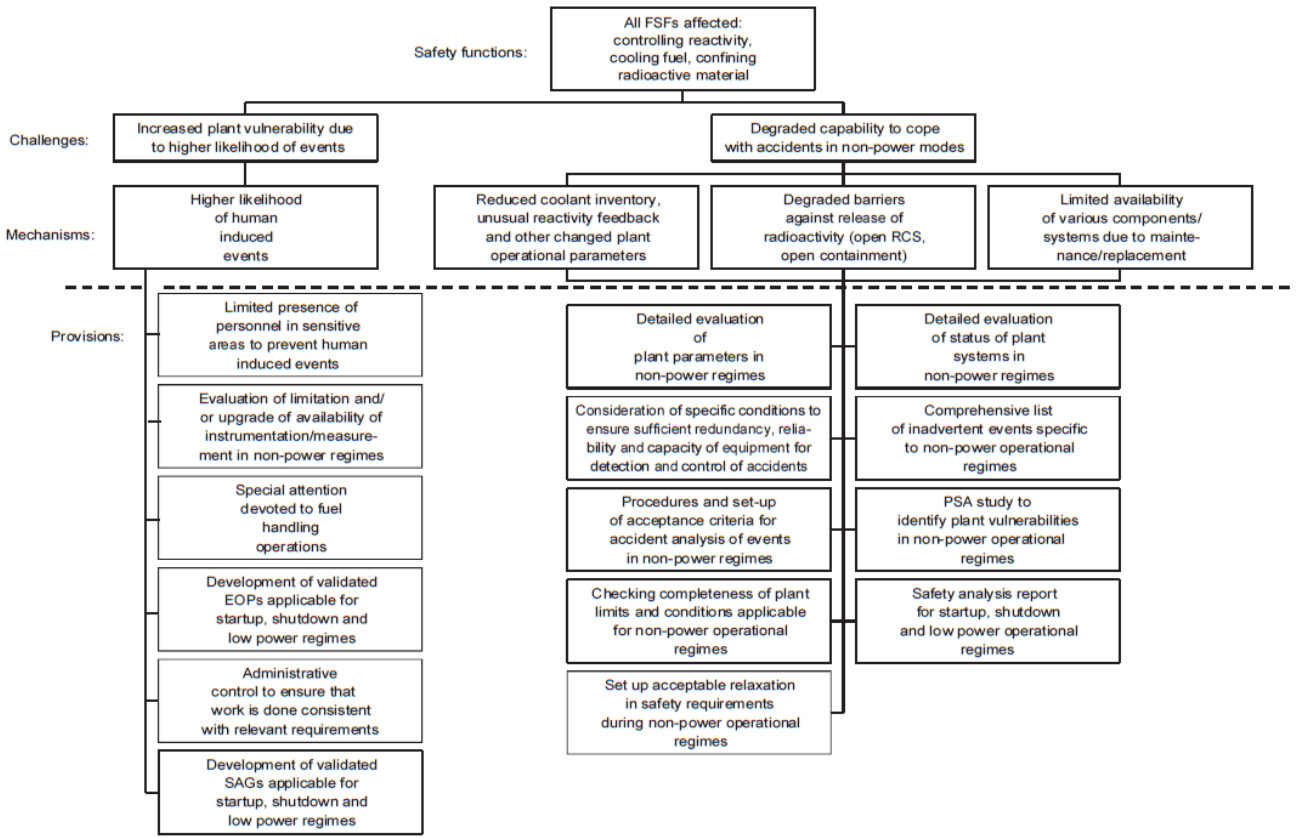


FIG. 37. Objective tree for Levels 1–4 of defence in depth. Safety principle (205): startup, shutdown and low power operation.

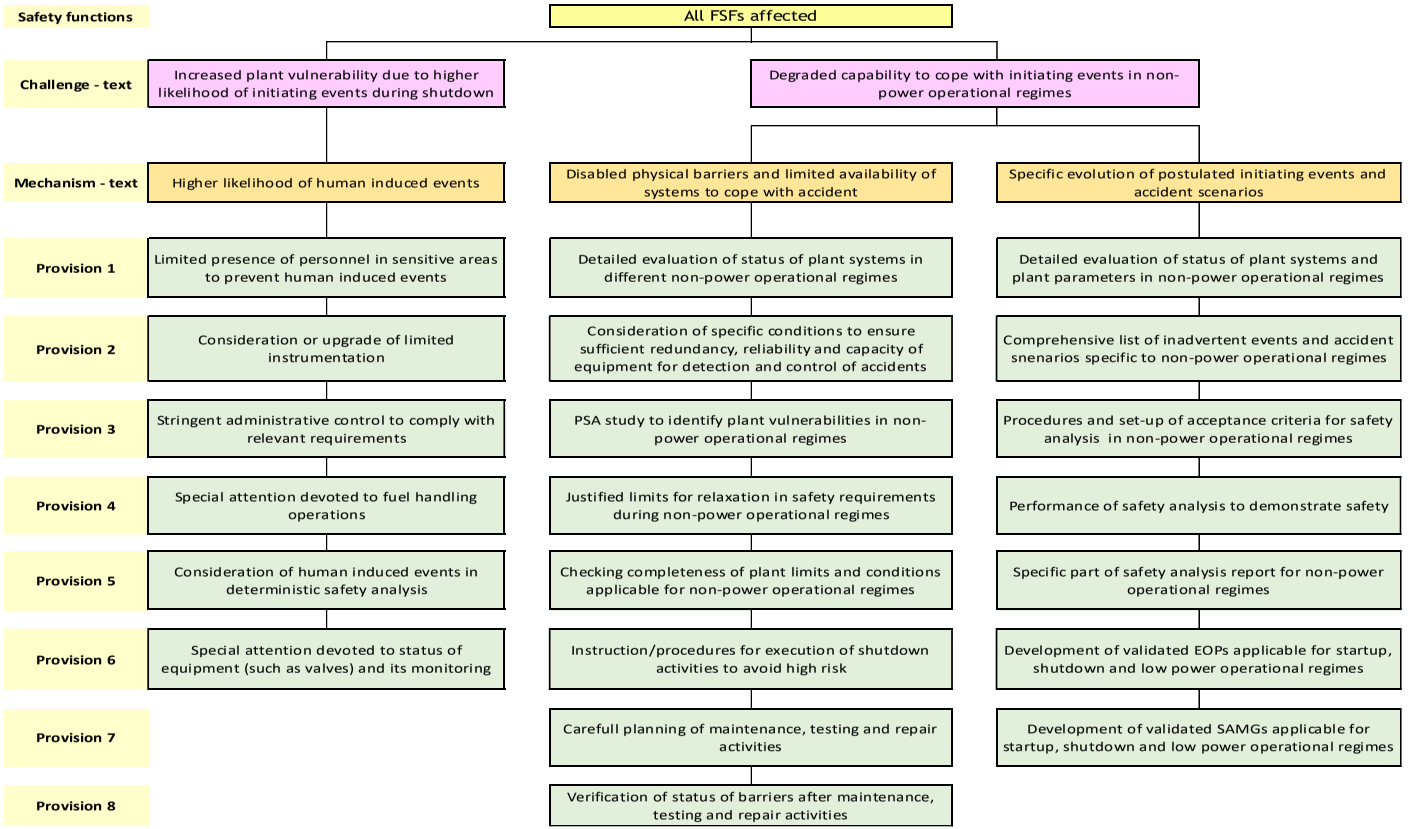


FIG 37 Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (205): startup, shutdown and low power operation.

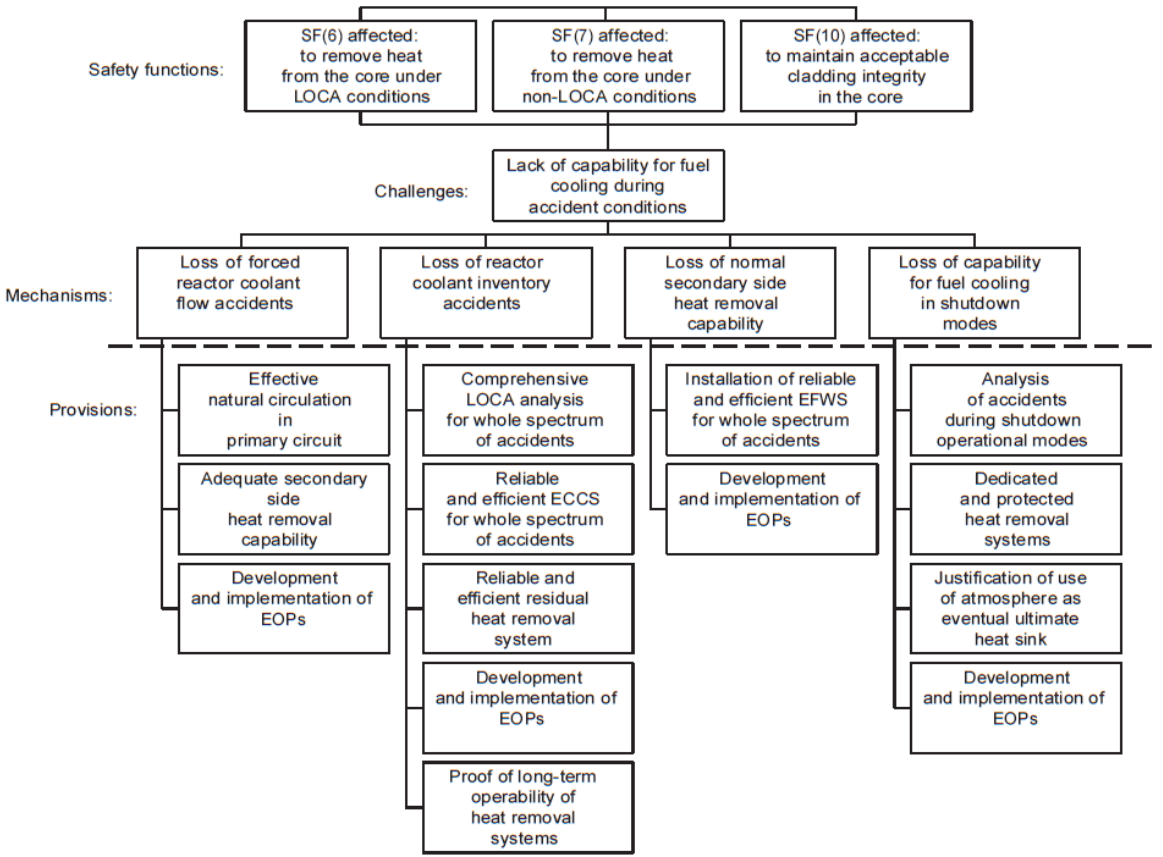


FIG. 38. Objective tree for Level 3 of defence in depth. Safety principle (207): emergency heat removal.

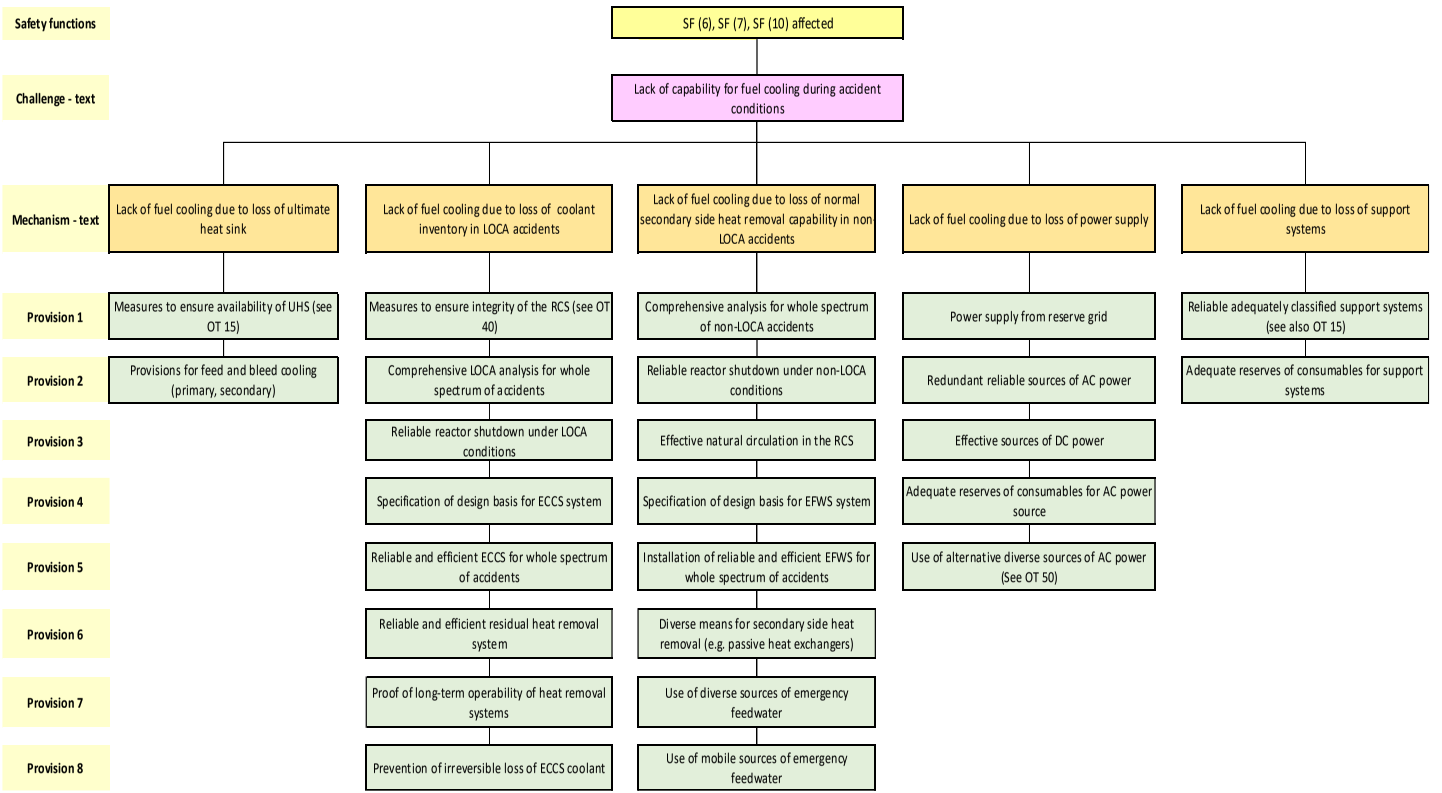


FIG. 38. Updated. Objective tree for Levels 3 -4 (DEC-A) of defence in depth. Safety principle (207): emergency heat removal.

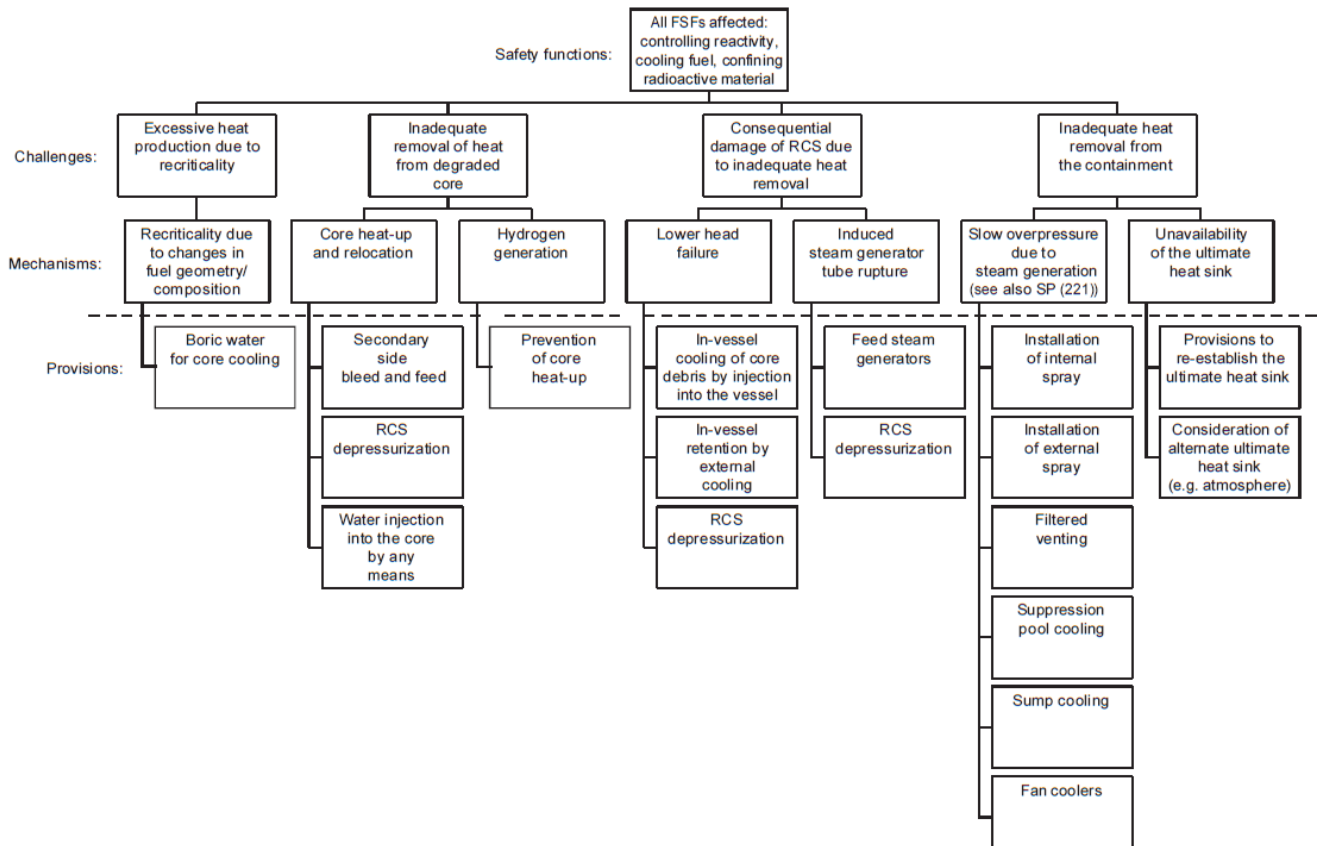


FIG. 39. Objective tree for Level 4 of defence in depth. Safety principle (207): emergency heat removal.

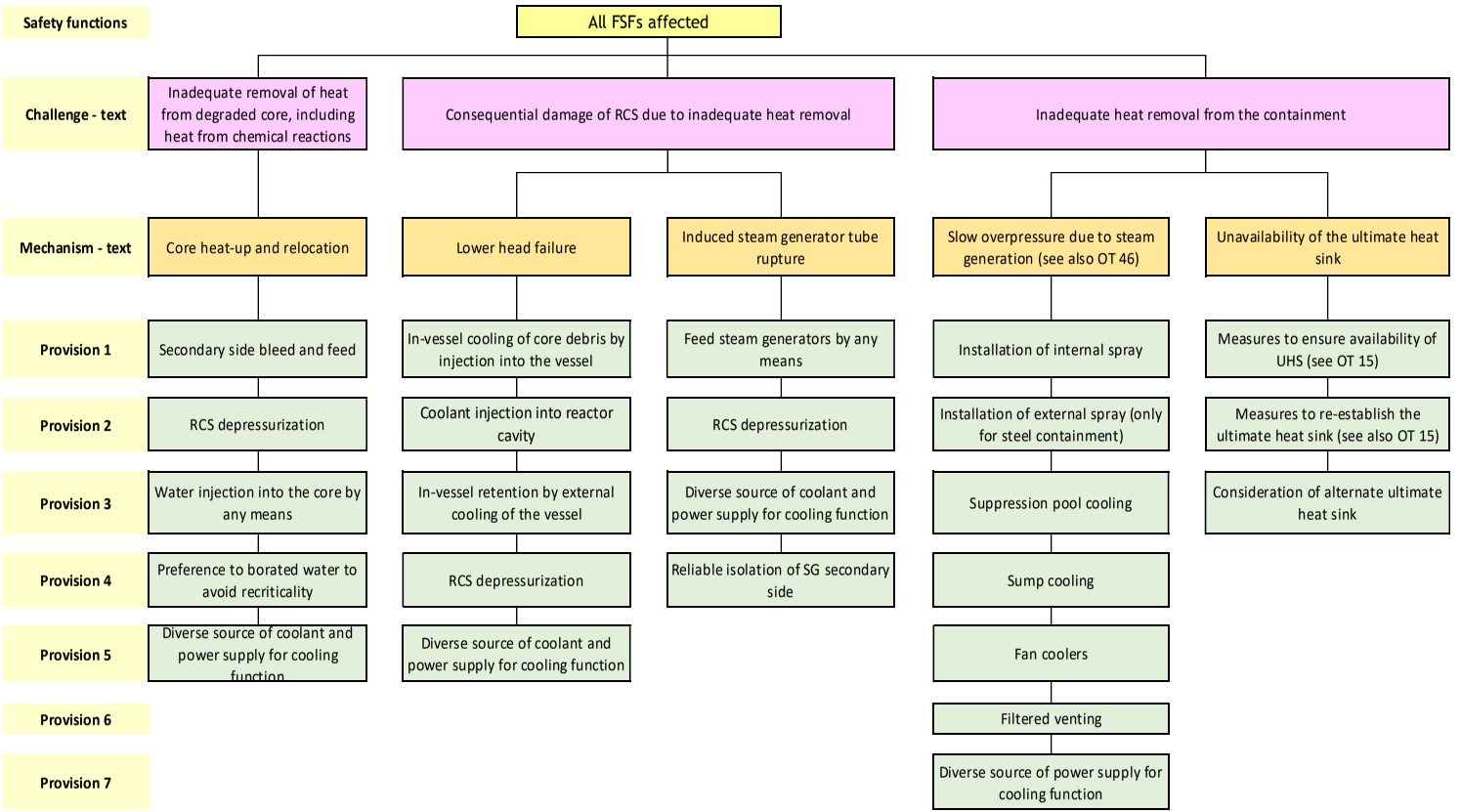


FIG. 39.Updated. Objective tree for Level 4 of defence in depth. Safety principle (207): emergency heat removal.

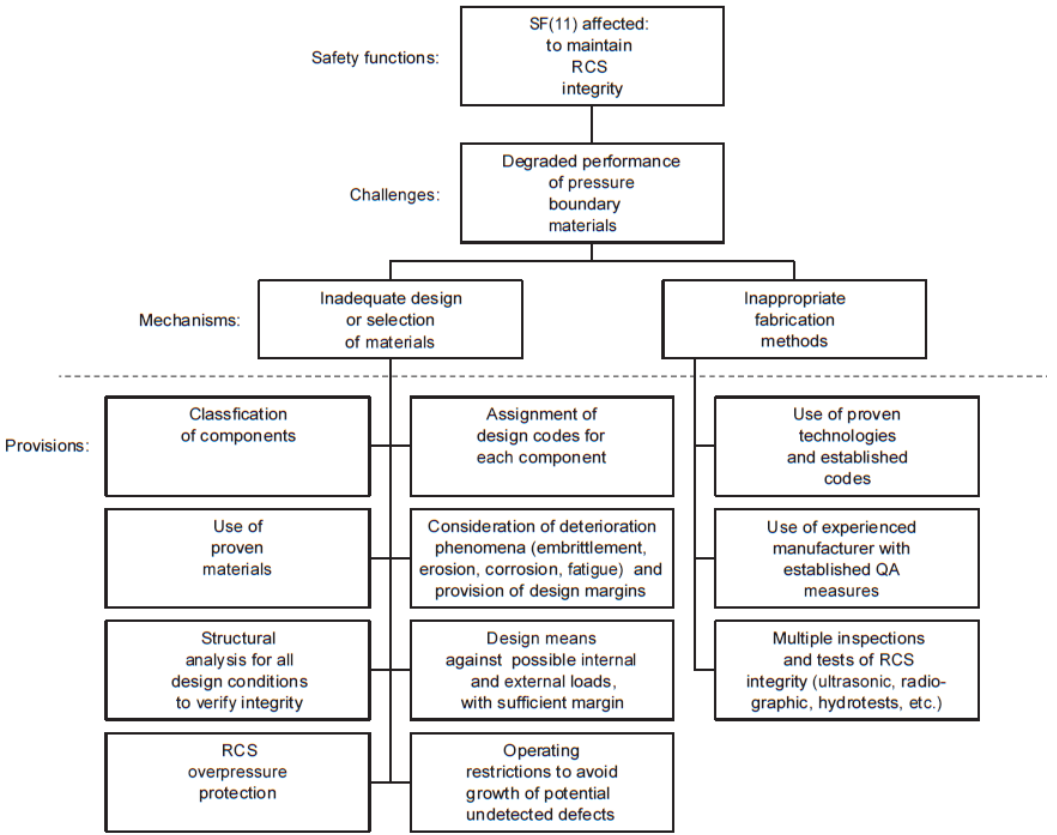


FIG. 40. Objective tree for Level 1 of defence in depth. Safety principle (209): reactor coolant system integrity.

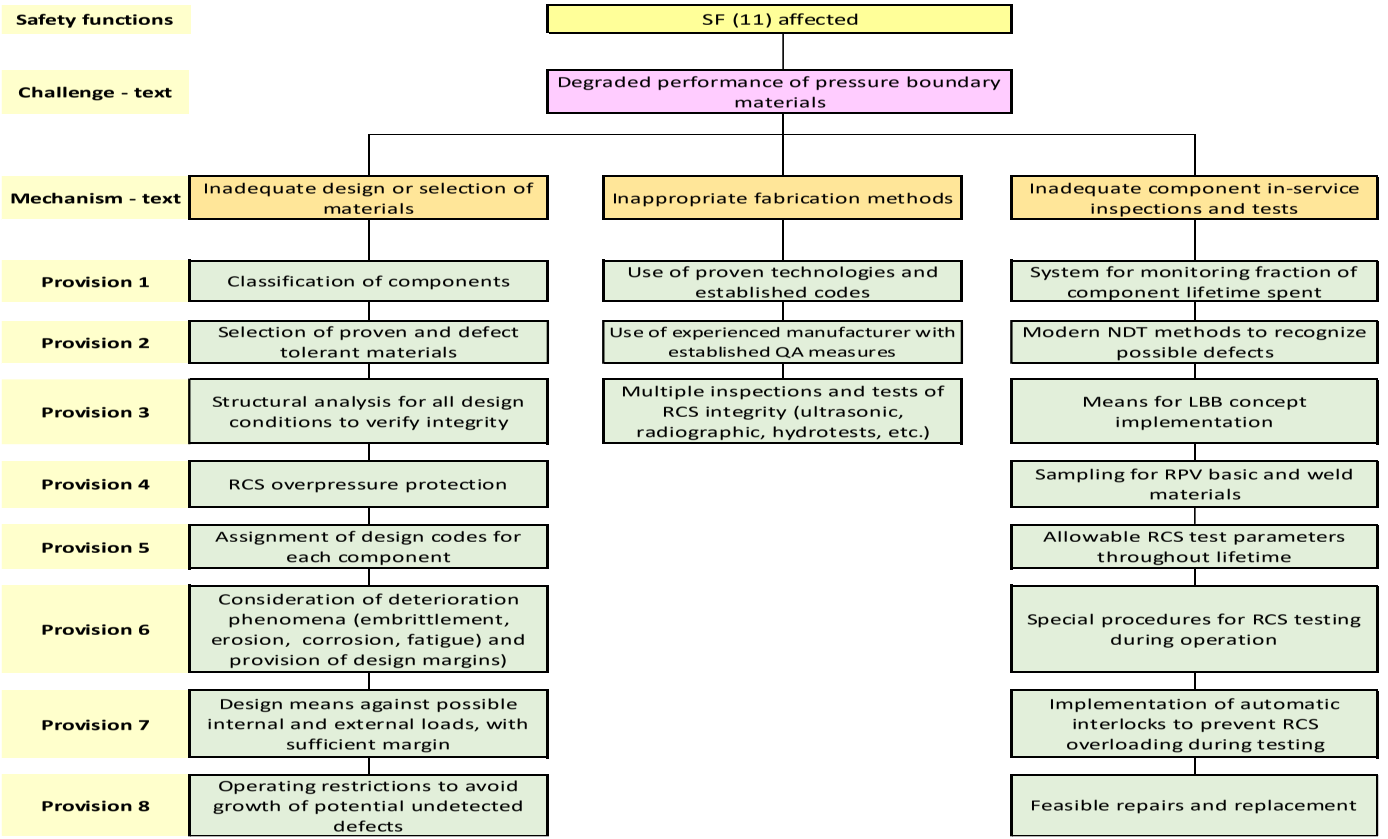


FIG. 40. Updated. Objective tree for Levels 1-2 of defence in depth. Safety principle (209): reactor coolant system integrity.

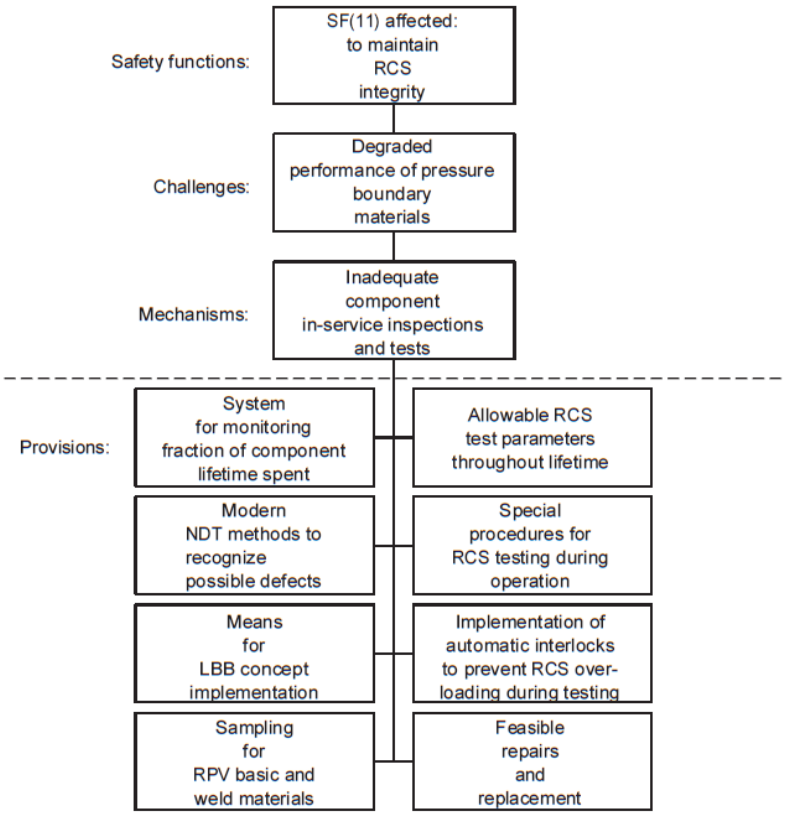


FIG. 41. Objective tree for Level 2 of defence in depth. Safety principle (209): reactor coolant system integrity.

Fig. 41 was combined with fig. 40

FIG. 41.Updated. Objective tree for Level 2 of defence in depth. Safety principle (209): reactor coolant system integrity.

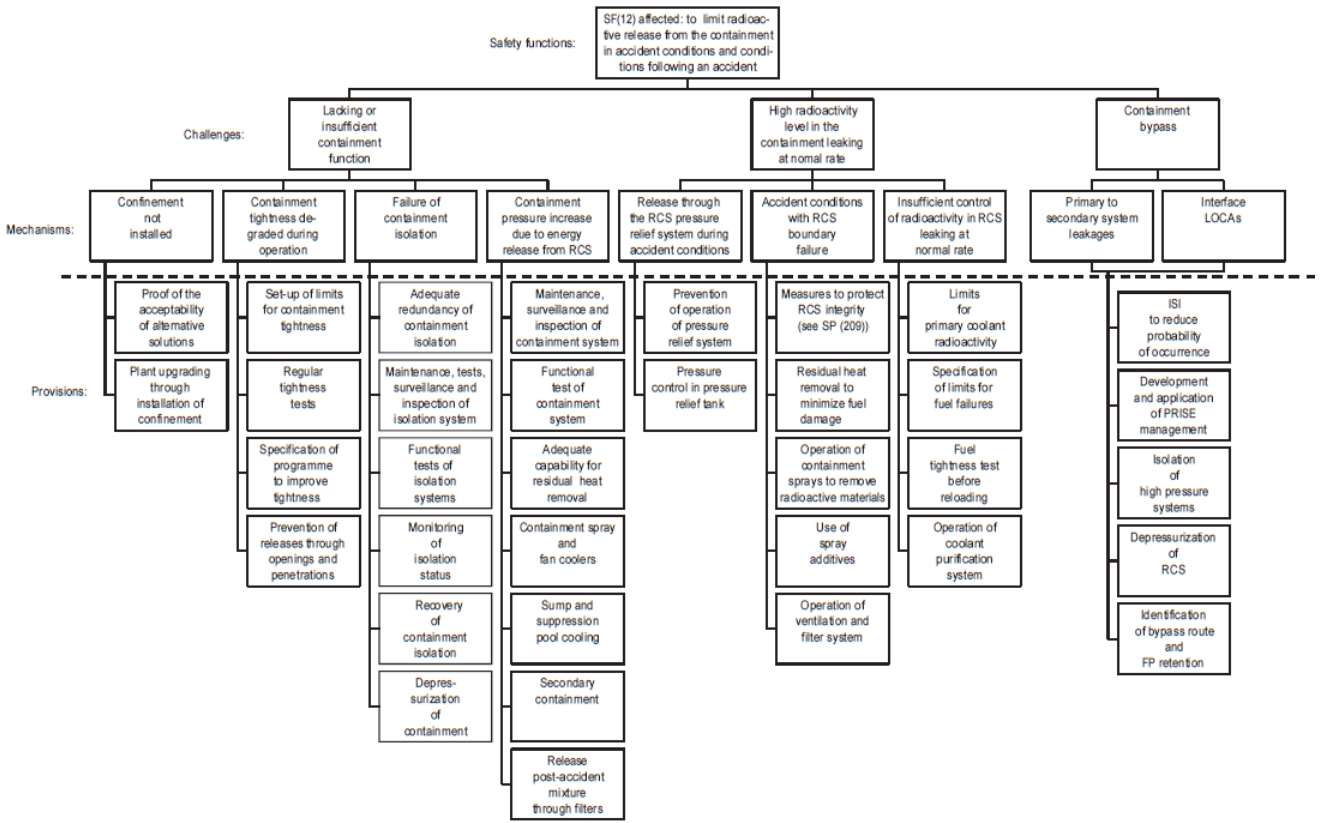


FIG. 42. Objective tree for Level 3 of defence in depth. Principle (205): startup, shutdown and low power operation. Safety principle (217): confinement of radioactive material (see also SF (12)).

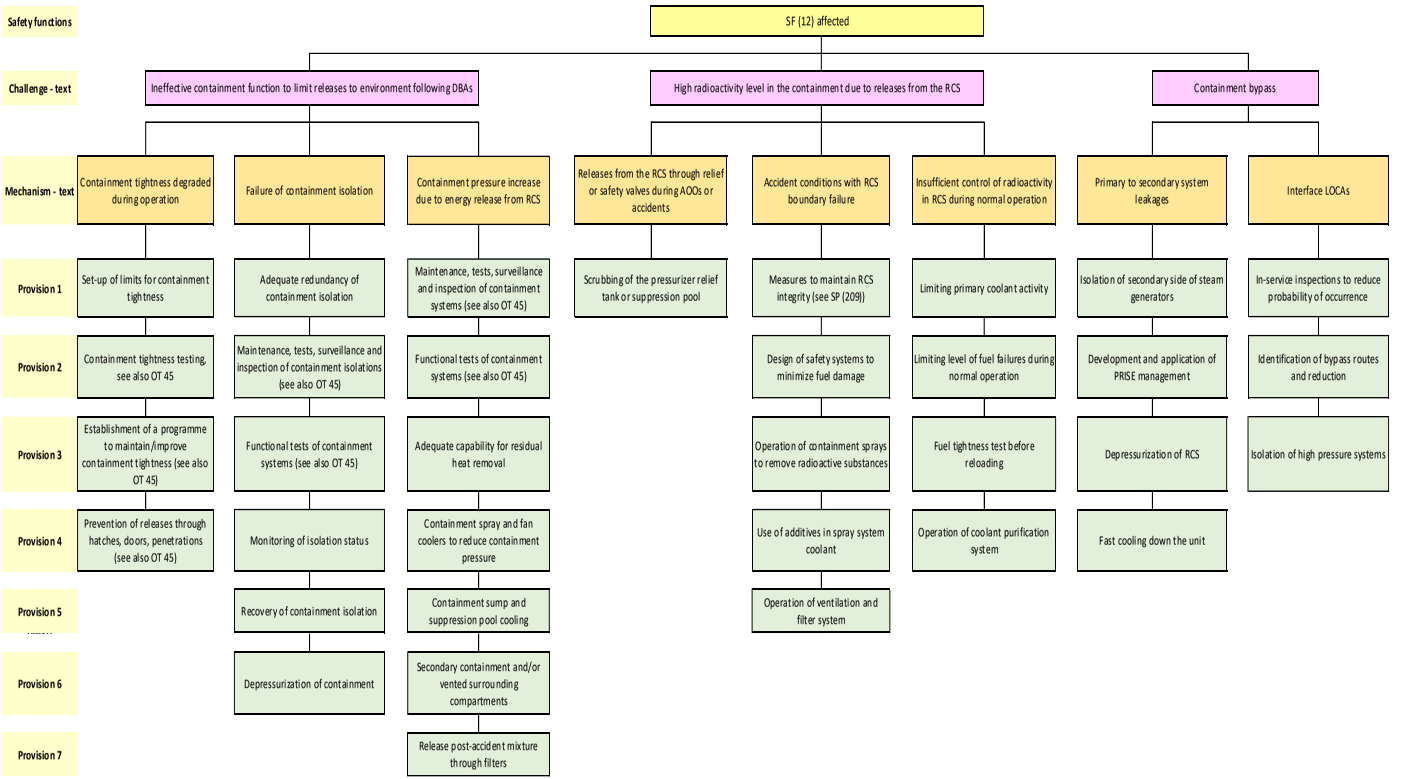


FIG. 42 Updated. Objective tree for Levels 2-3 of defence in depth. Principle (217): startup, shutdown and low power operation. Safety principle (217): confinement of radioactive material (see also SF (12)).

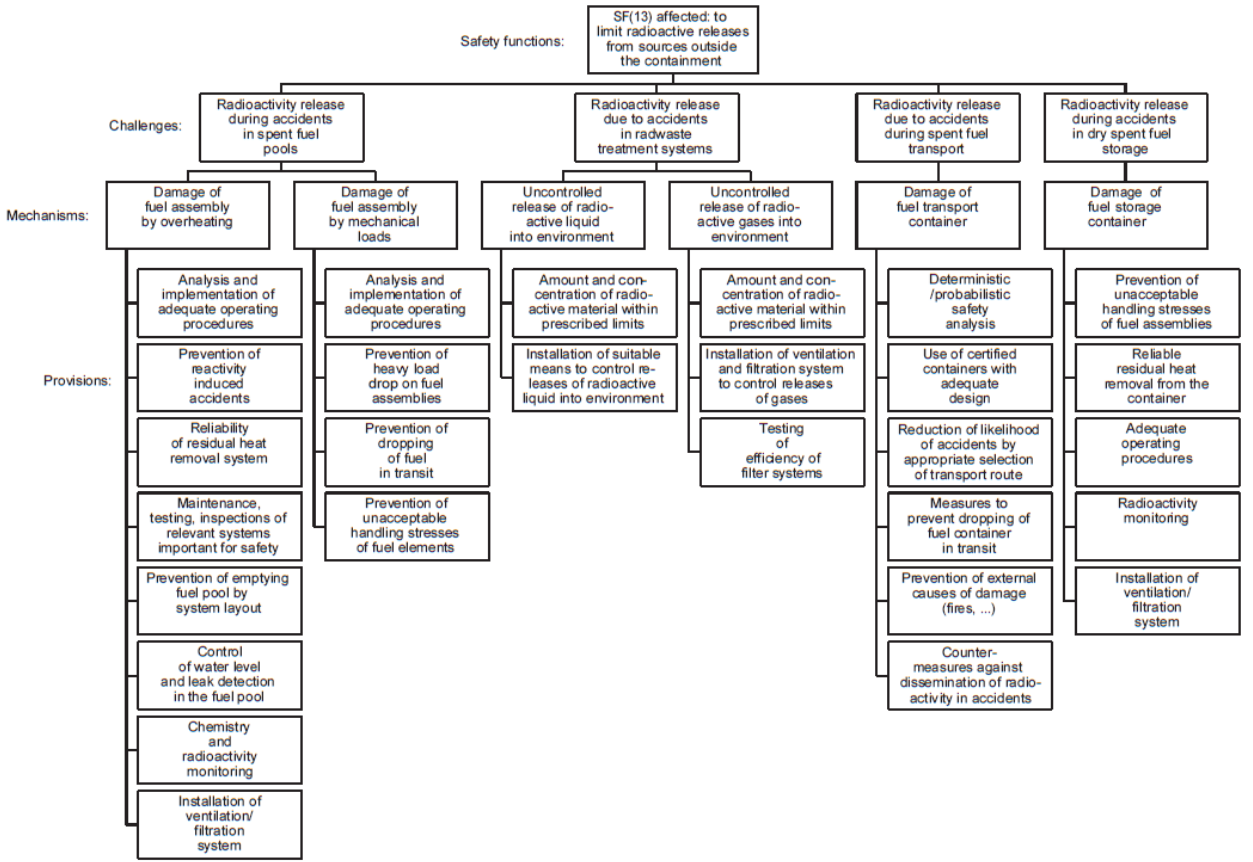


FIG. 43. Objective tree for Level 3 of defence in depth. Safety principle (217): confinement of radioactive material (see also SF (13)).

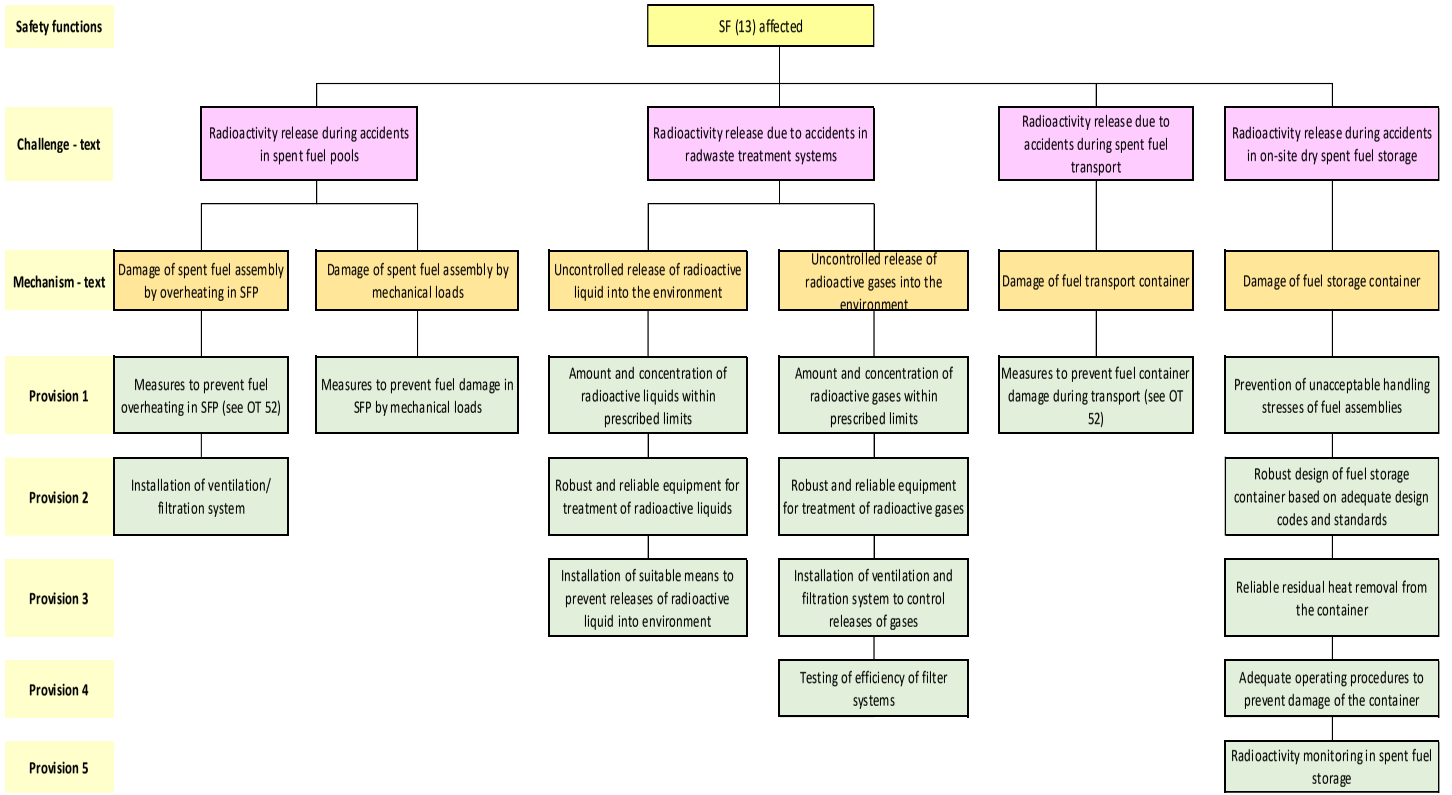


FIG. 43. Updated. Objective tree for Levels 2-3, 4 (DEC-A) of defence in depth. Safety principle (217): confinement of radioactive material (see also SF (13)).

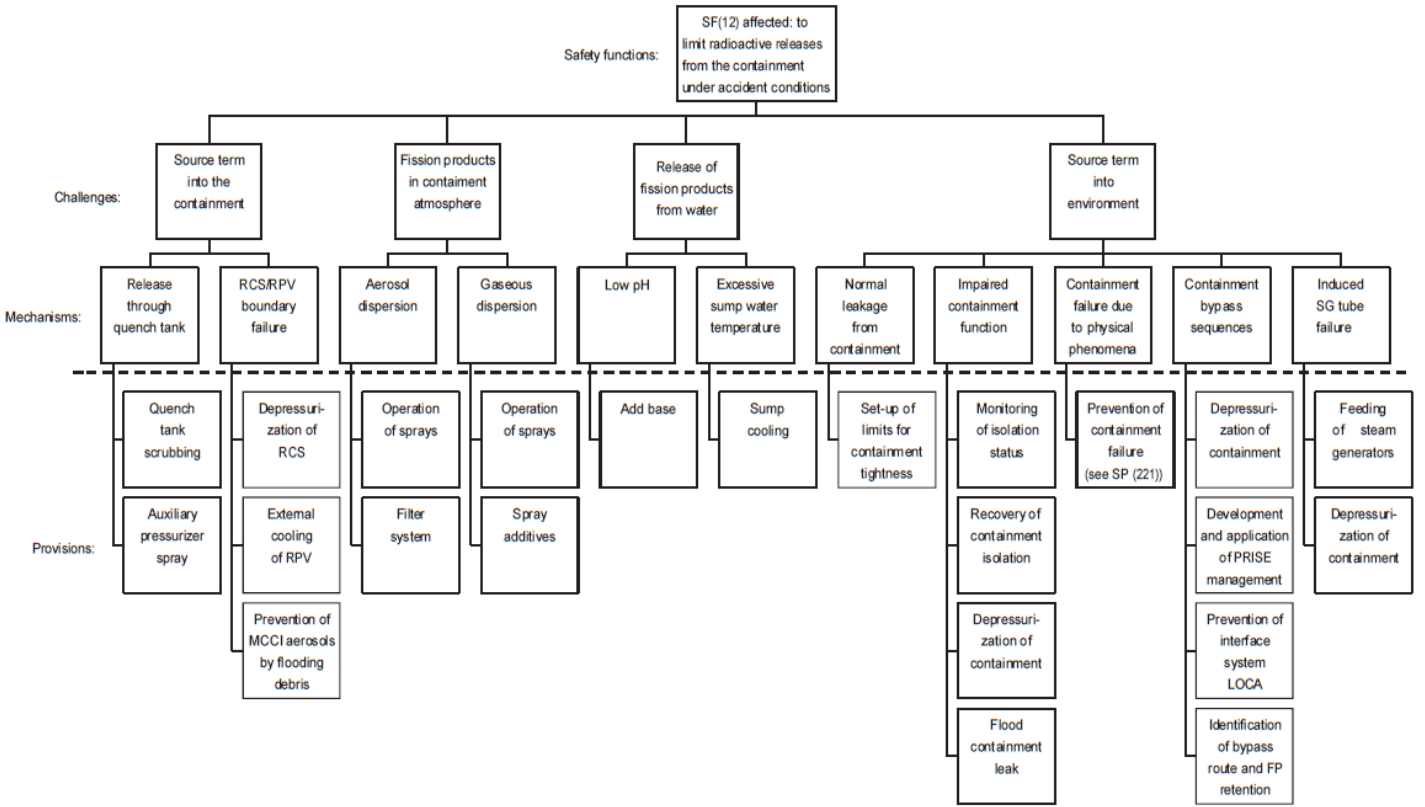


FIG. 44. Objective tree for Level 4 of defence in depth. Safety principle (217): confinement of radioactive material.

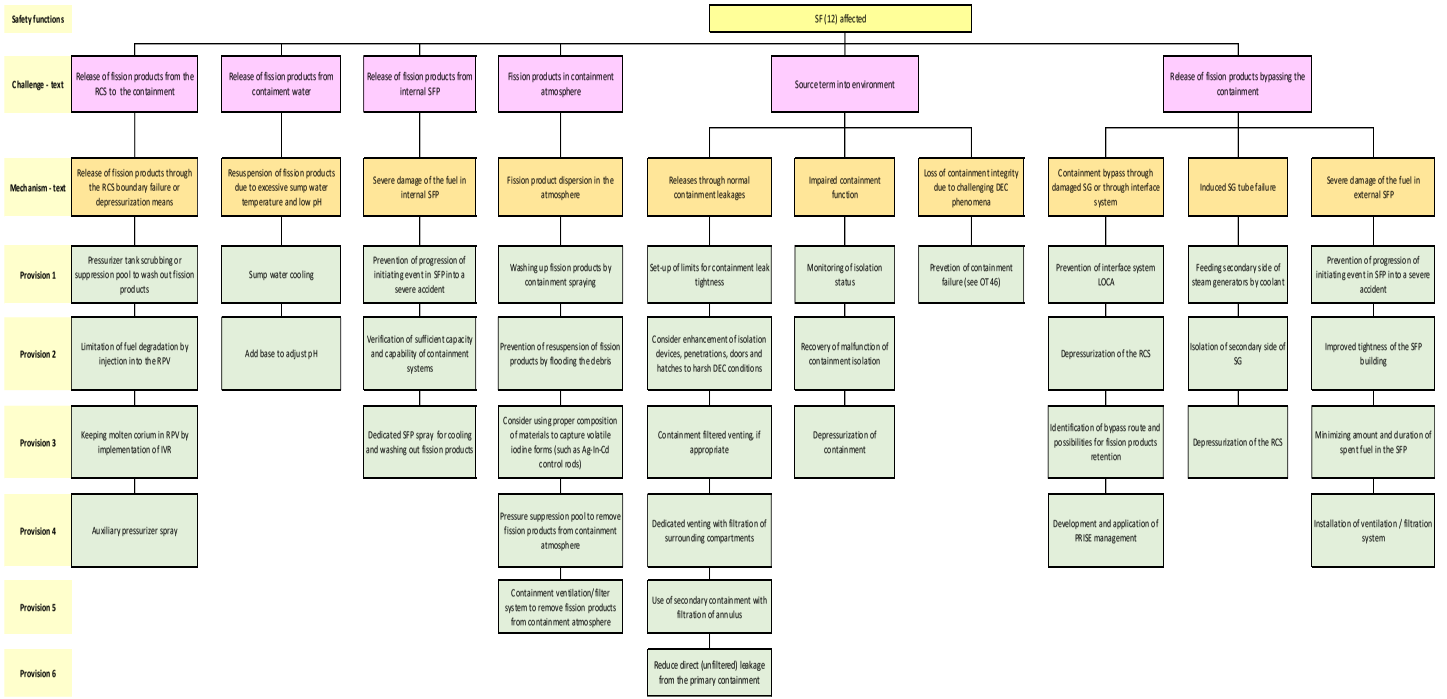


FIG. 44 Updated. Objective tree for Level 4 of defence in depth. Safety principle (217): confinement of radioactive material.

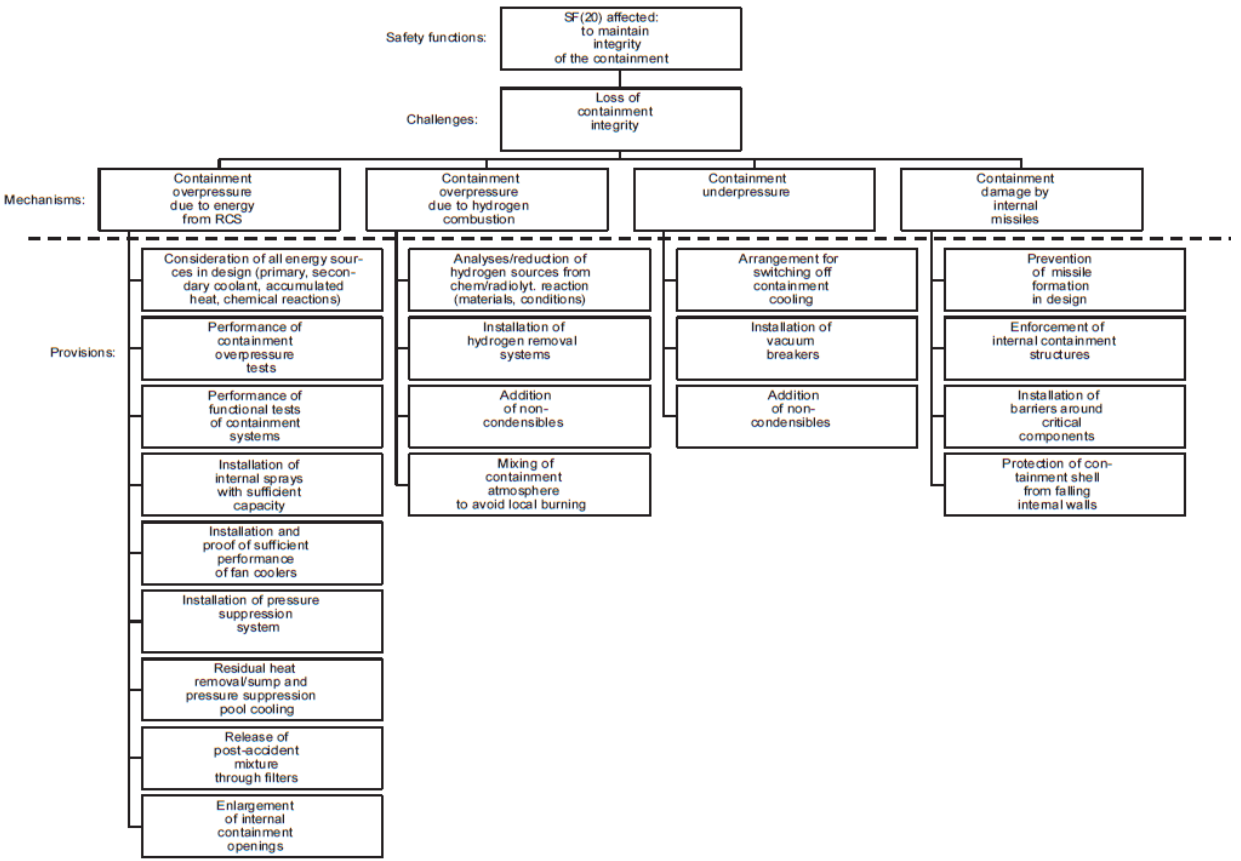


FIG. 45. Objective tree for Level 3 of defence in depth . Safety principle: protection of confinement structure (221).

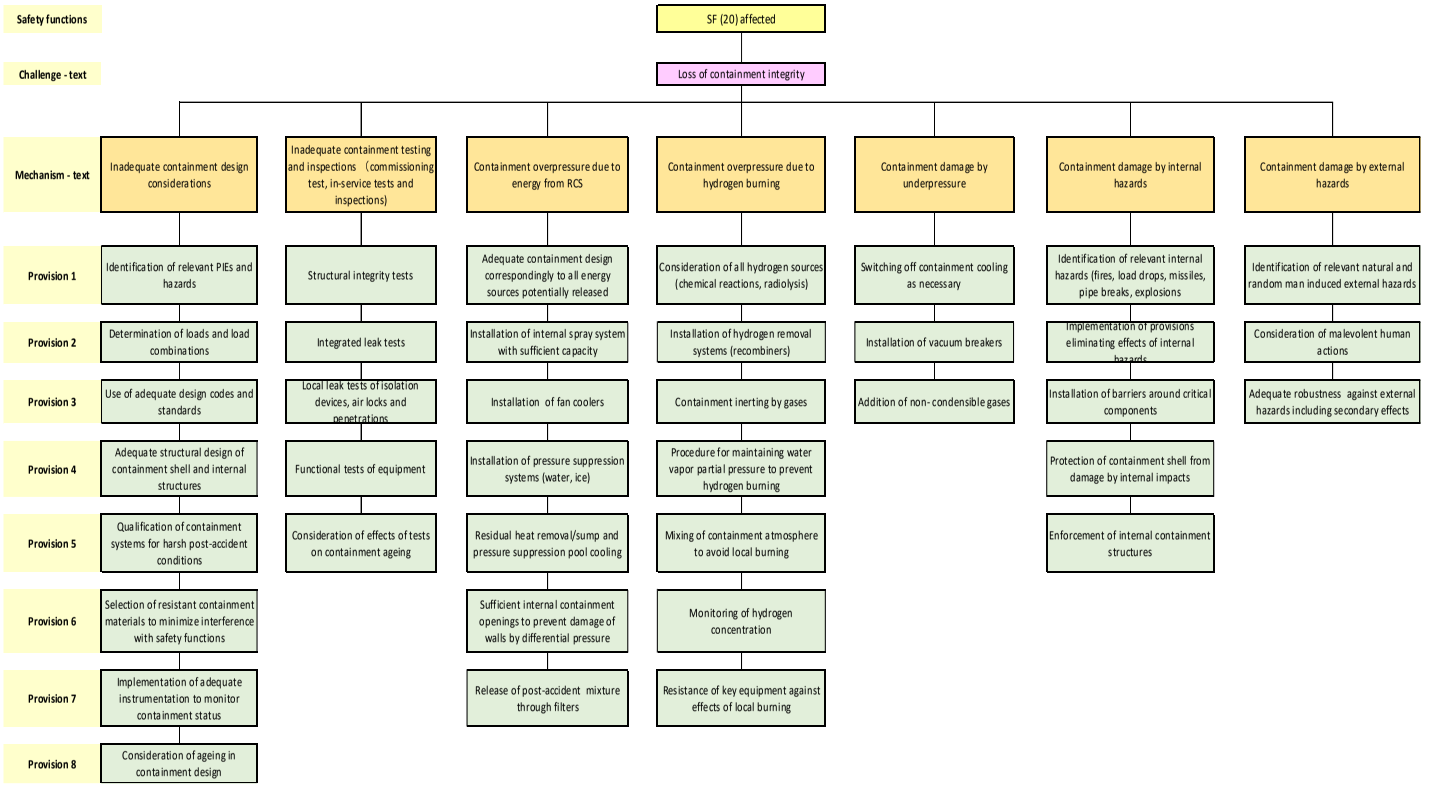


FIG 45 Updated. Objective tree for Level 3 of defence in depth. Safety principle: protection of confinement structure (221).

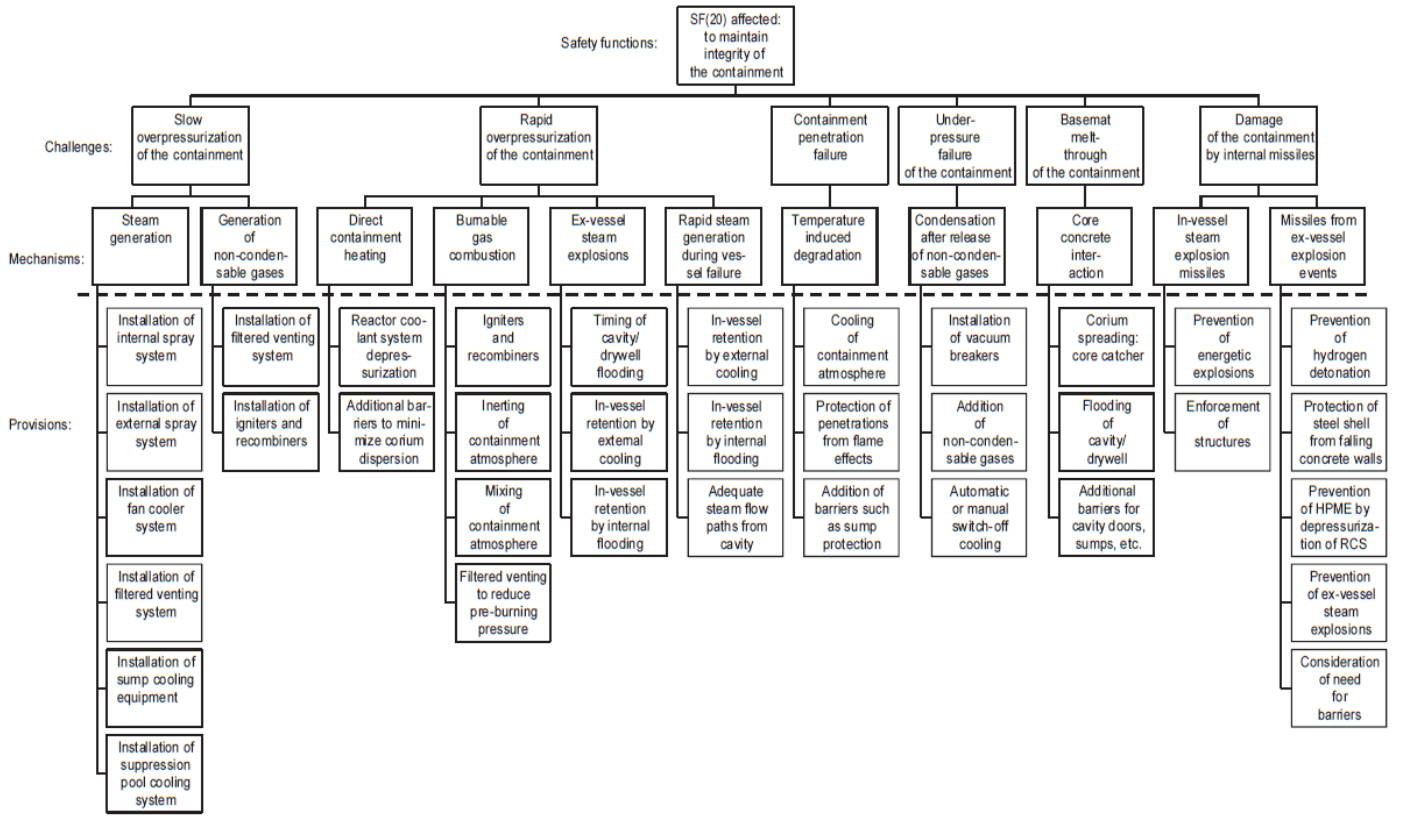


FIG. 46. Objective tree for Level 4 of defence in depth. Safety principle (221): protection of confinement structure.

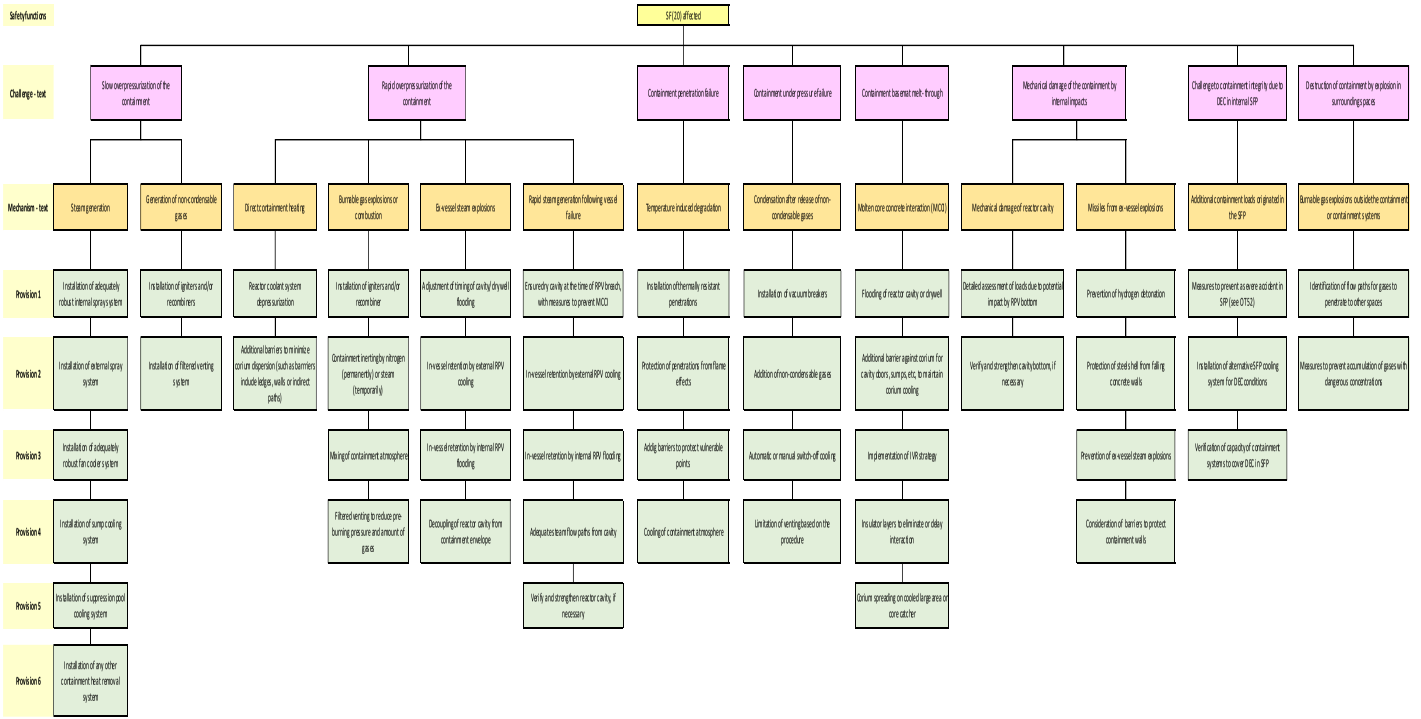


FIG 46 Updated. Objective tree for Level 4 of defence in depth. Safety principle (221): protection of confinement structure.

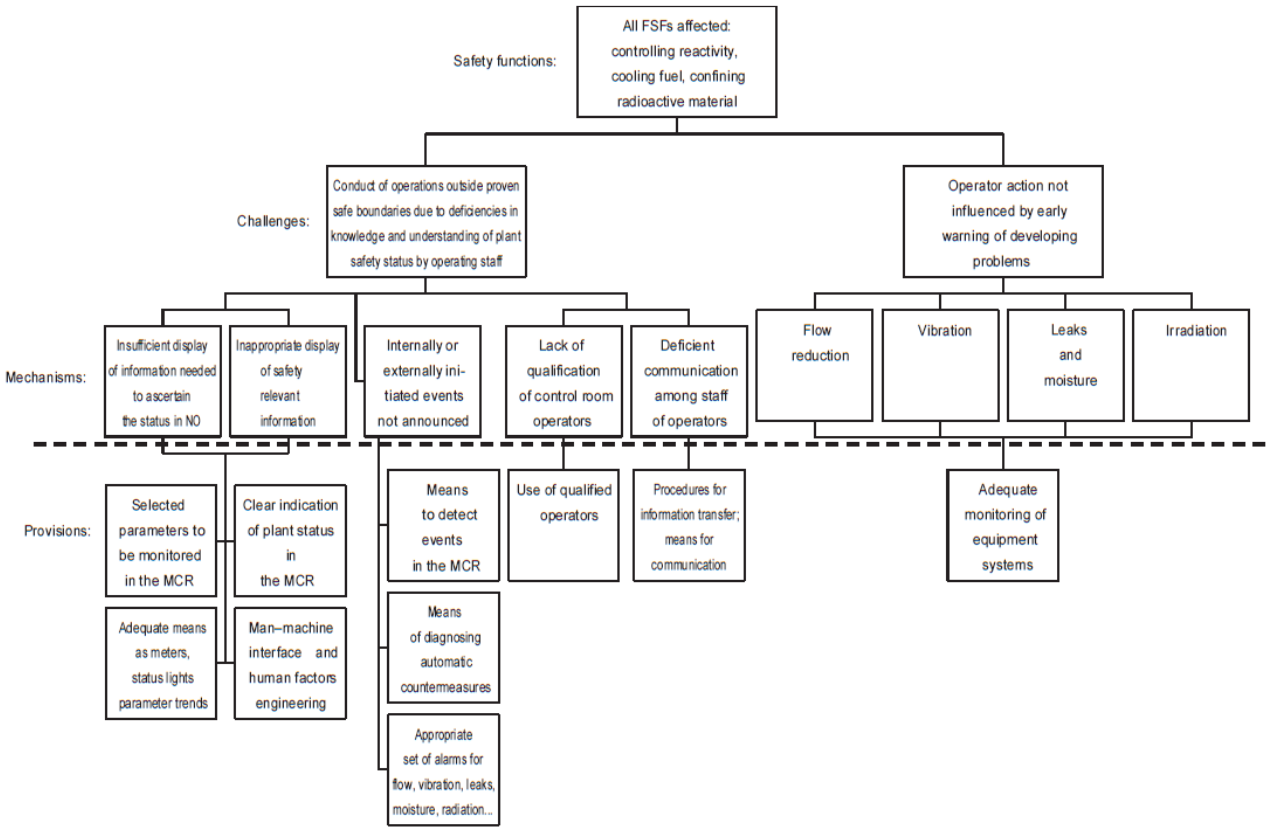


FIG. 47. Objective tree for Levels 1 - 2 of defence in depth. Safety principle (227): monitoring of plant safety status.

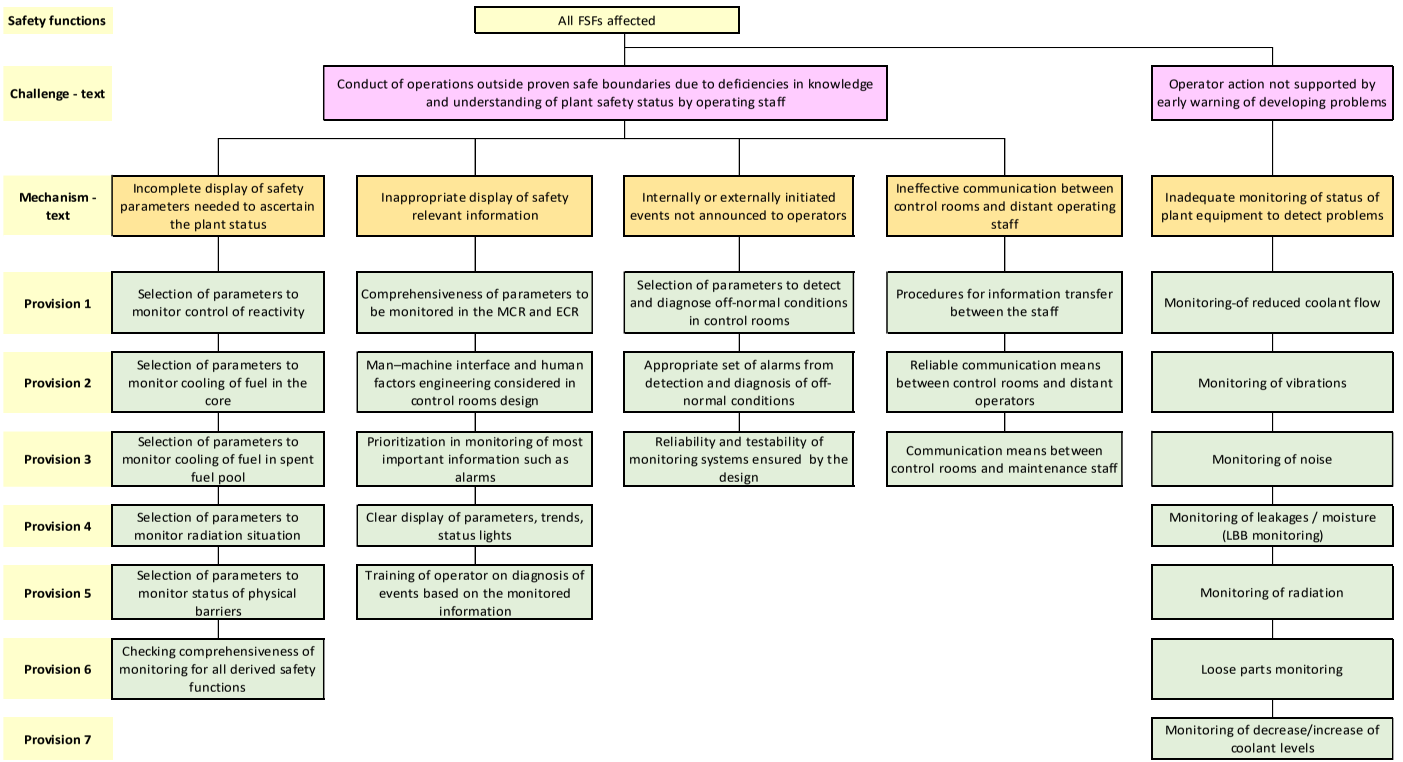


FIG. 47 Updated. Objective tree for Levels 1 - 2 of defence in depth. Safety principle (227): monitoring of plant safety status.

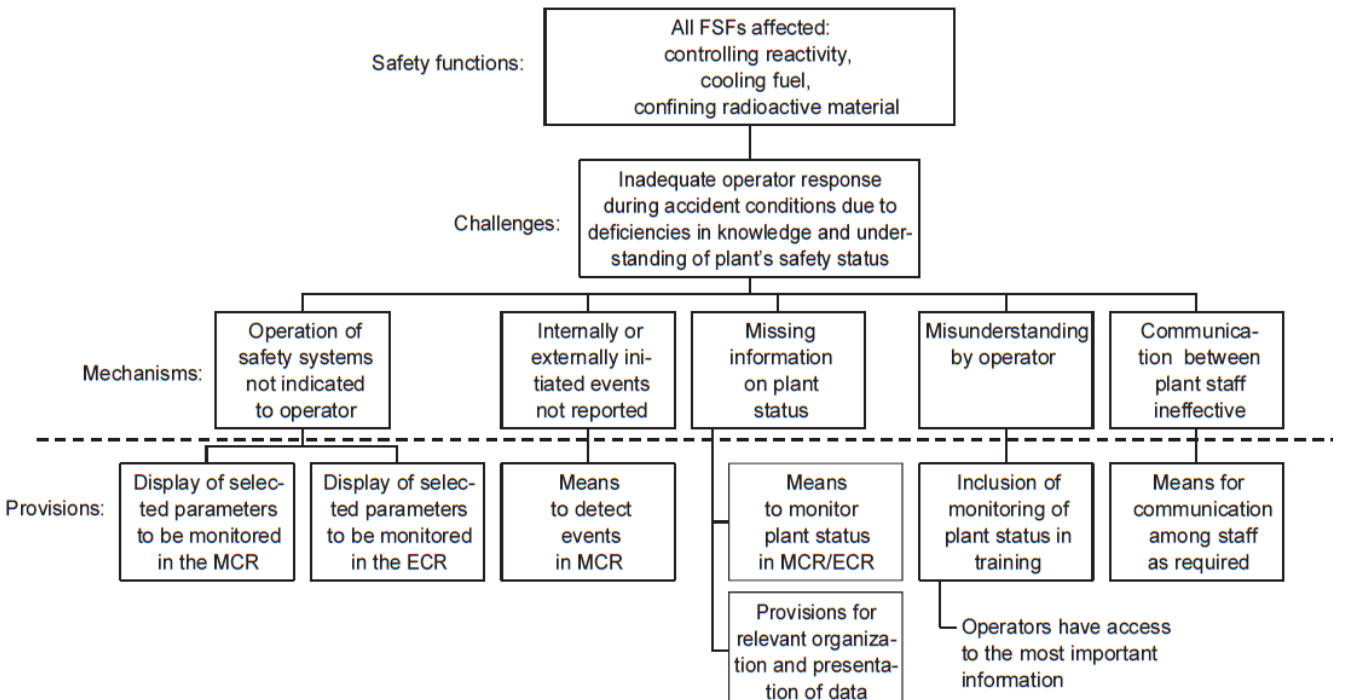


FIG. 48. Objective tree for Levels 3 and 4 of defence in depth. Safety principle (227): monitoring of plant safety status.

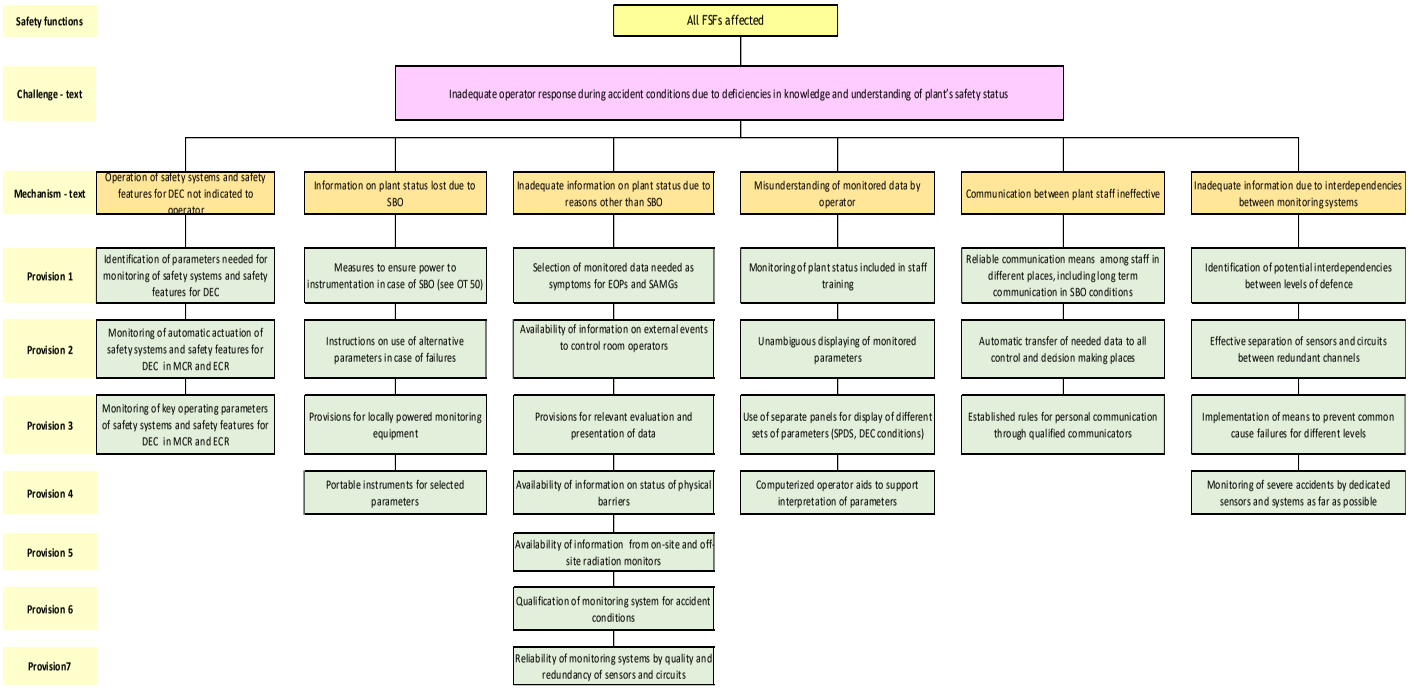


FIG. 48. Updated. Objective tree for Levels 3 and 4 of defence in depth. Safety principle (227): monitoring of plant safety status.

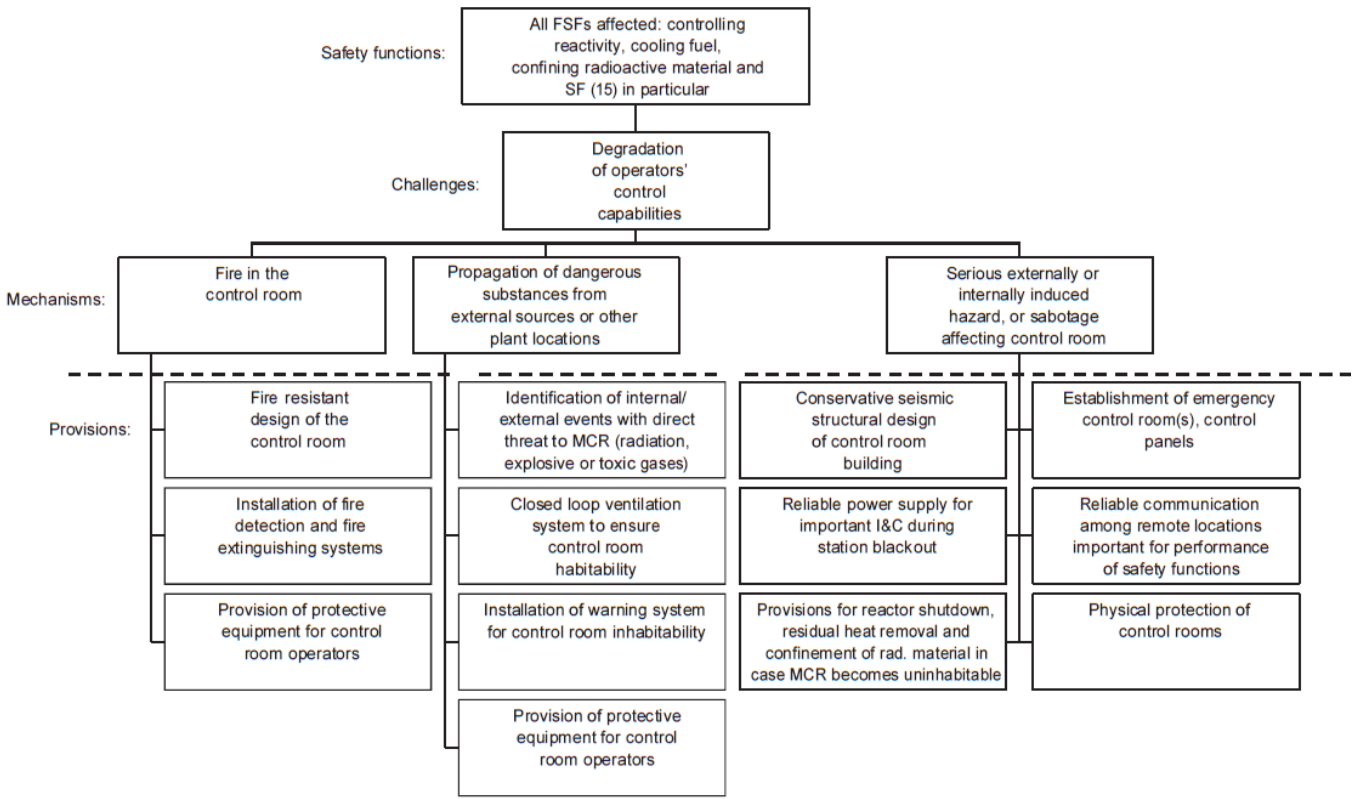


FIG. 49. Objective tree for Levels 1–4 of defence in depth. Safety principle: preservation of control capability (230).

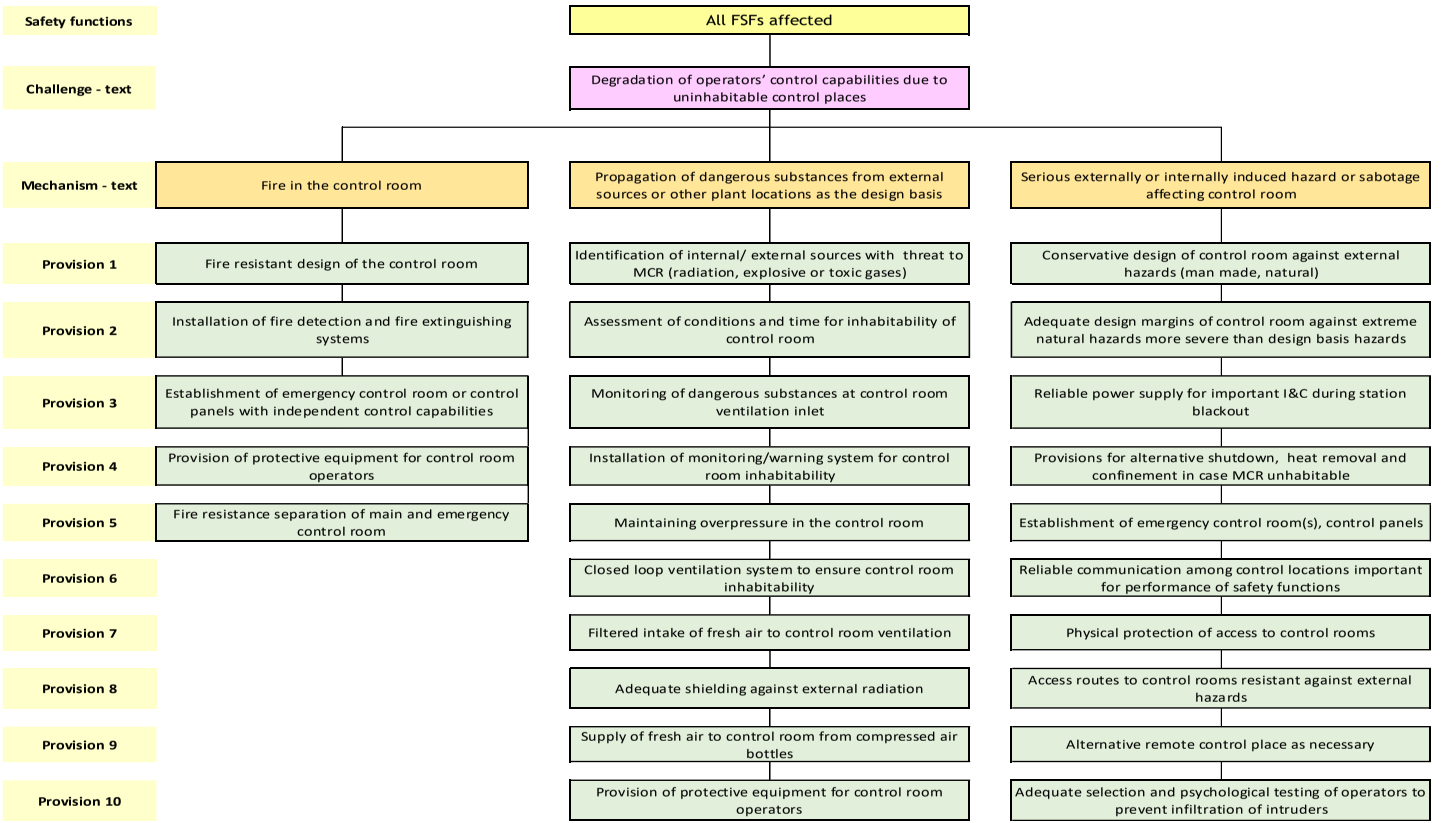


FIG. 49. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle: preservation of control capability (230).

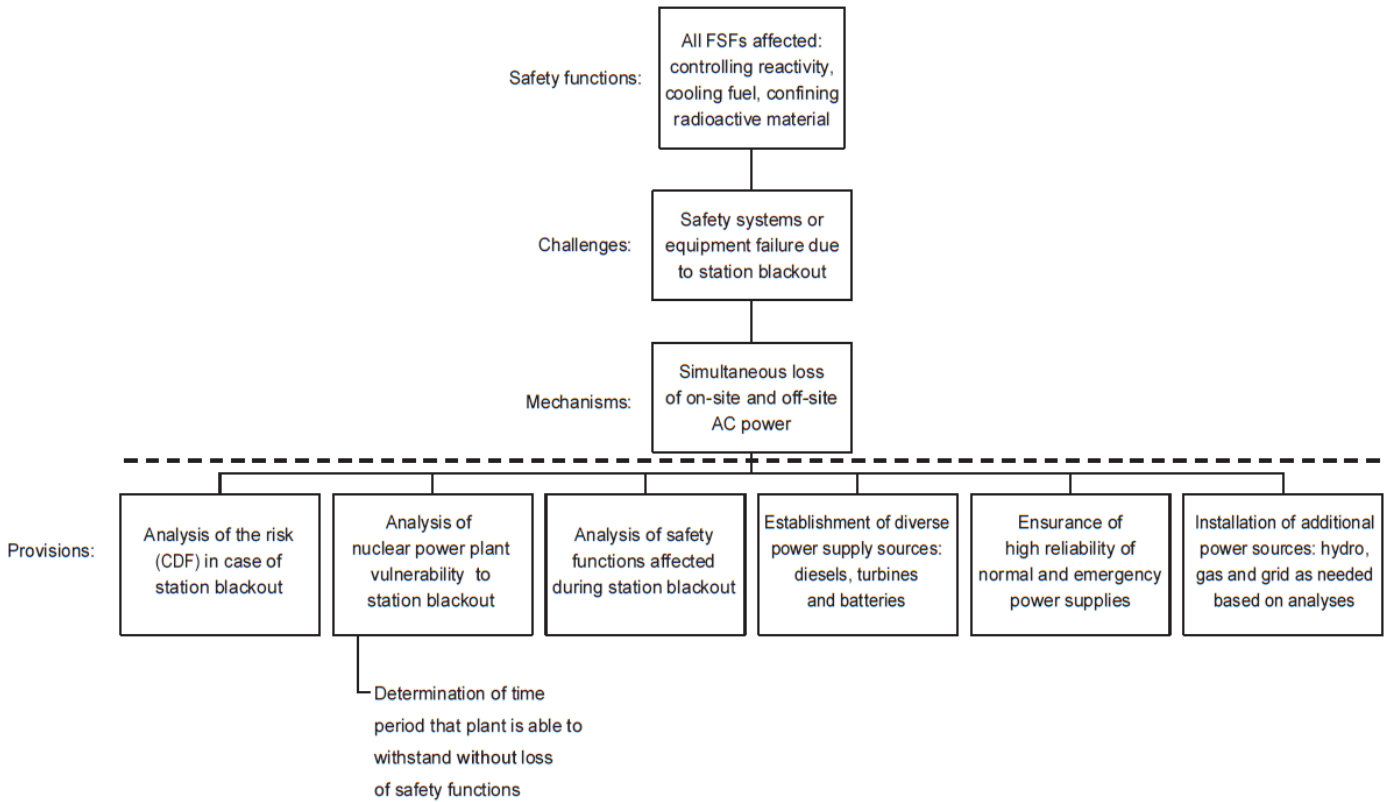


FIG. 50. Objective tree for Levels 3 and 4 of defence in depth. Safety principle: station blackout (233).

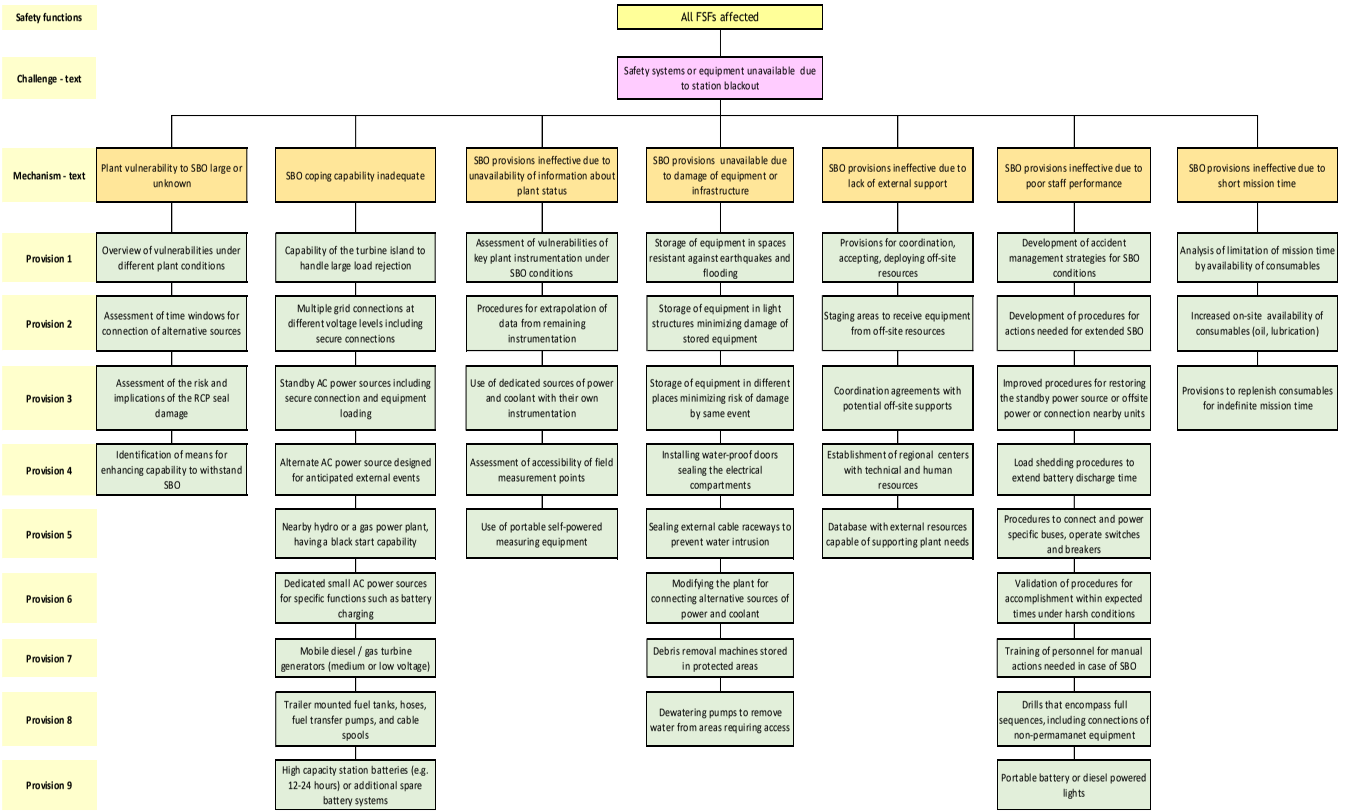


FIG. 50. Updated. Objective tree for Level 4 of defence in depth. Safety principle: station blackout (233).

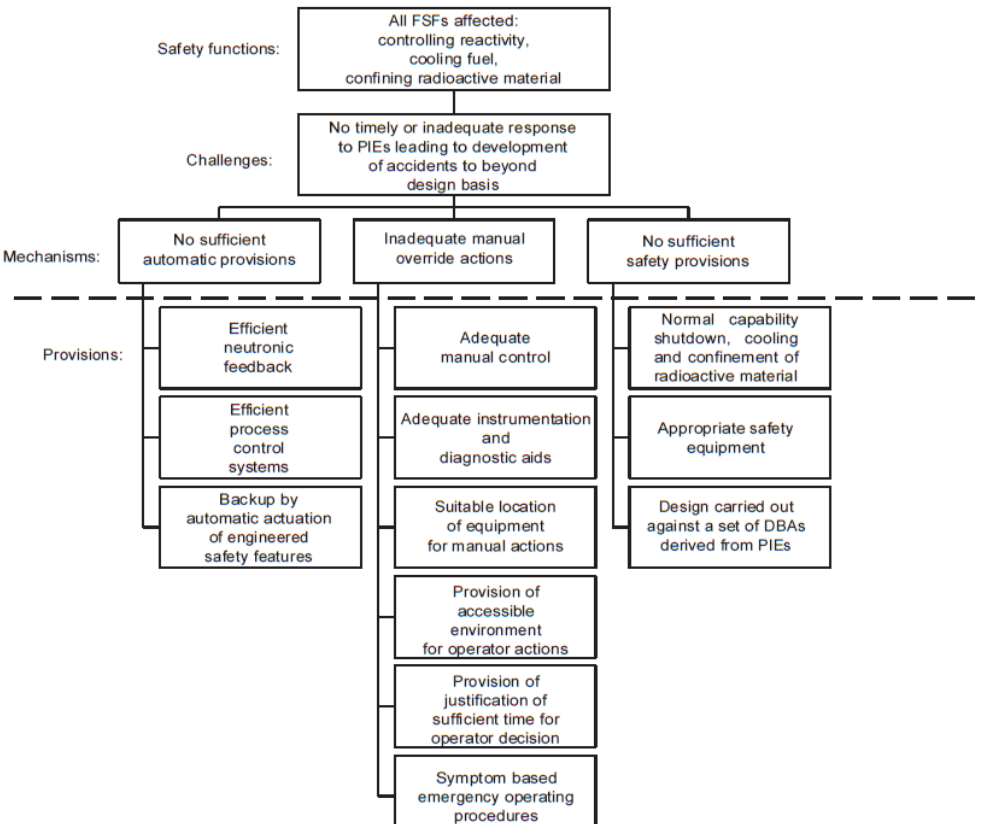


FIG. 51. Objective tree for Level 3 of defence in depth. Safety principle (237): control of accidents within the design basis.

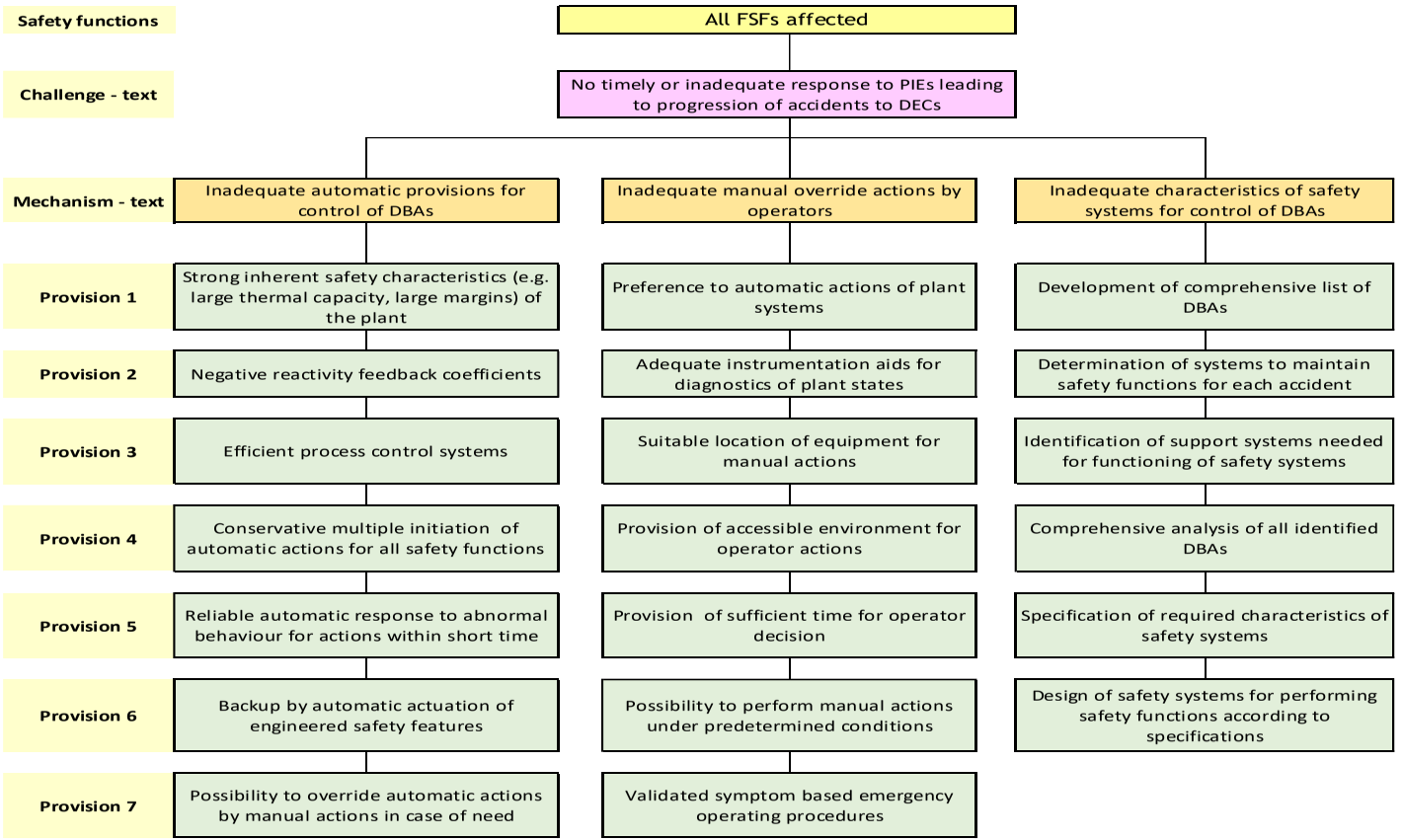


FIG. 51. Updated. Objective tree for Level 3 of defence in depth. Safety principle (237): control of accidents within the design basis.

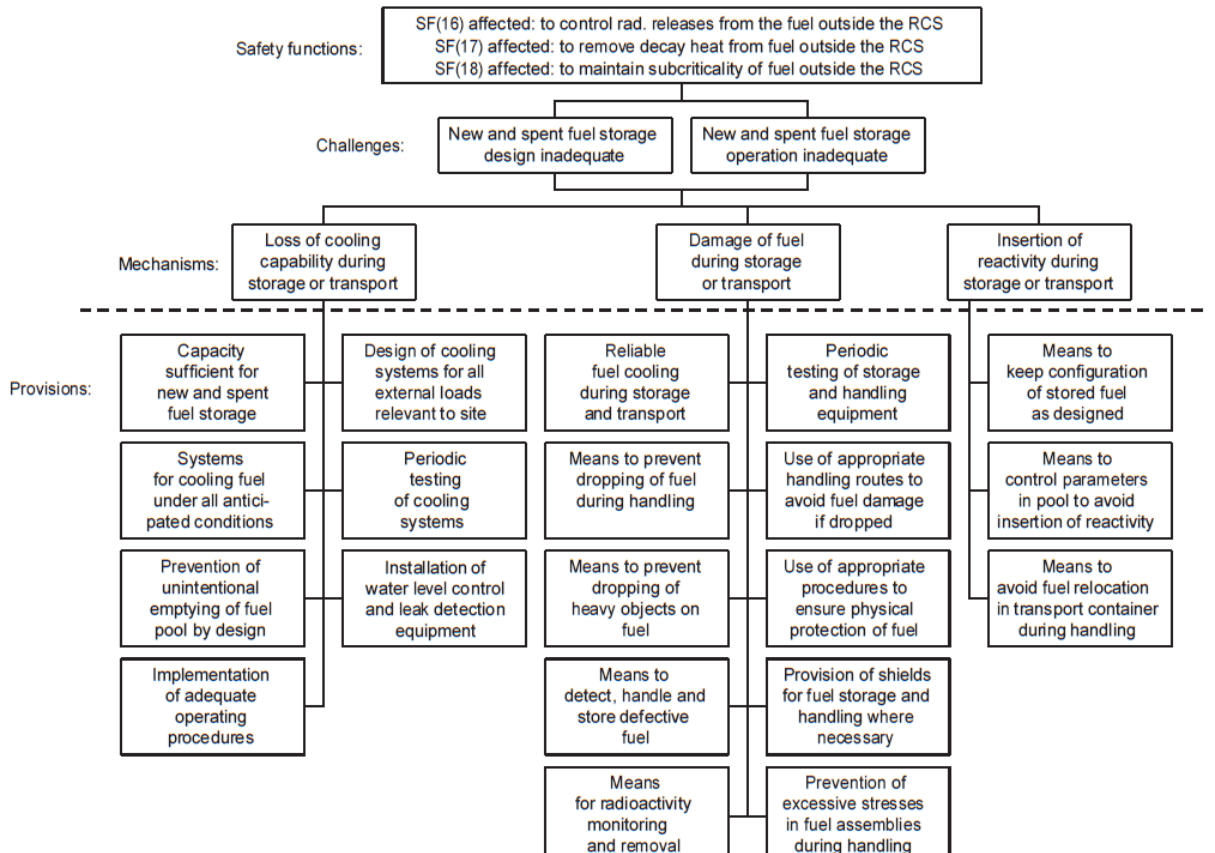


FIG. 52. Objective tree for Levels 1 and 2 of defence in depth. Safety principle (240): new and spent fuel storage.

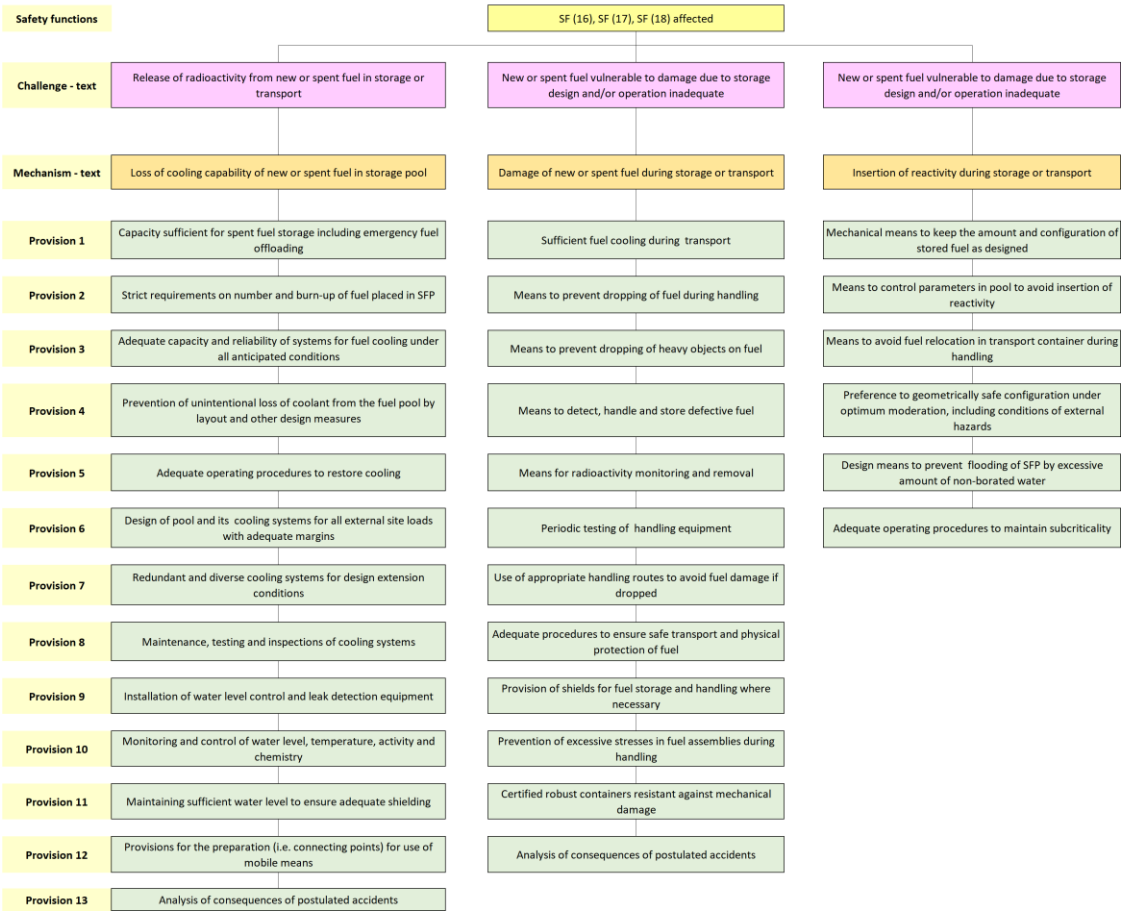


FIG. 52. Updated. Objective tree for Levels 1-4 of defence in depth. Safety principle (240): new and spent fuel storage.

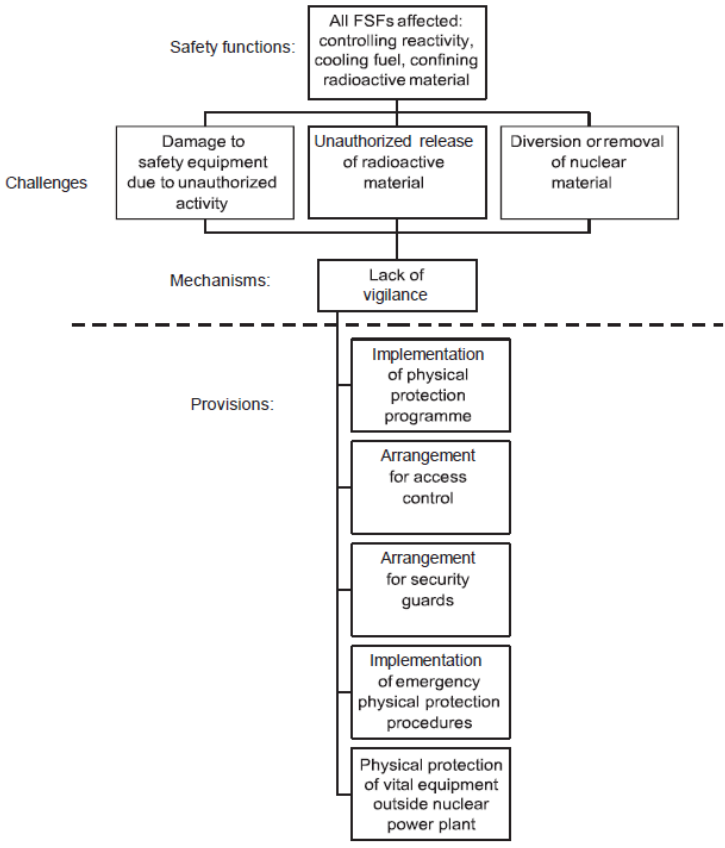


FIG. 53. Objective tree for Level 1 of defence in depth. Safety principle (242): physical protection of plant.

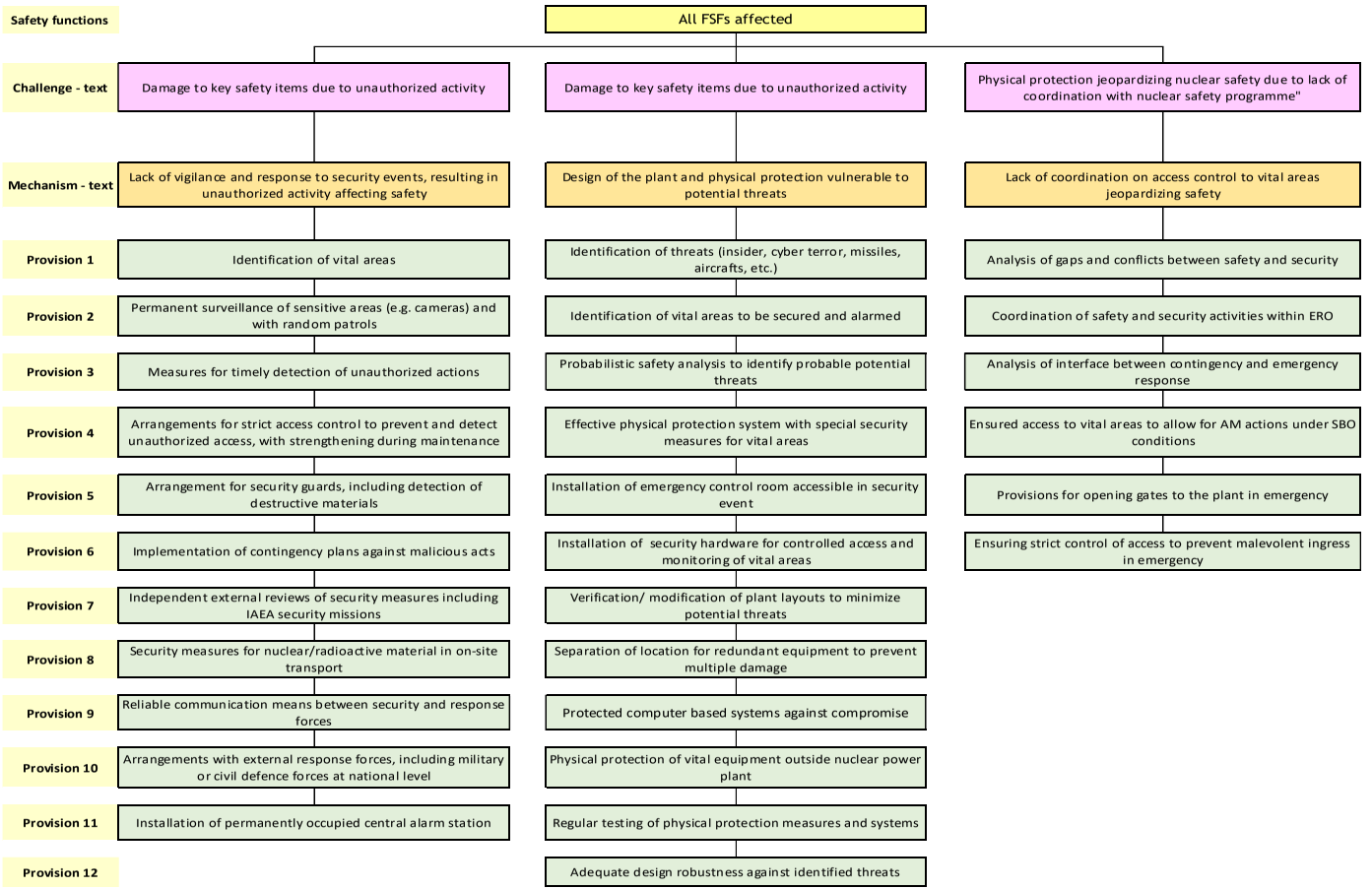


FIG 53. Updated. Objective tree for Levels 1-4 of defence in depth. Safety principle (242): physical protection of plant.

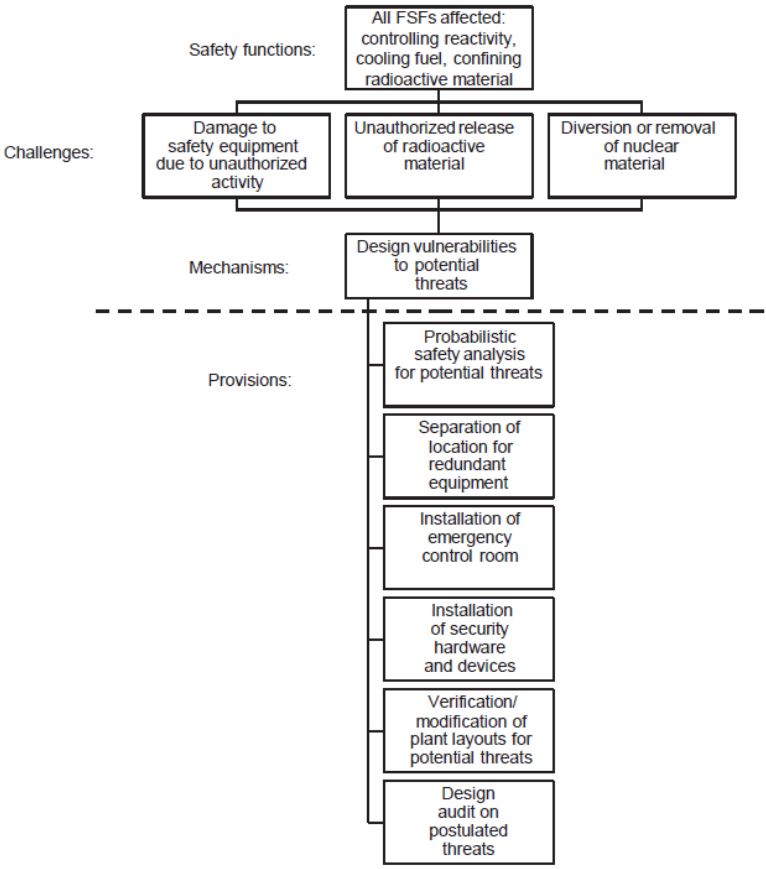


FIG. 54. Objective tree for Level 2 of defence in depth. Safety principle (242): physical protection of plant.

Fig. 54 was combined with fig. 53

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

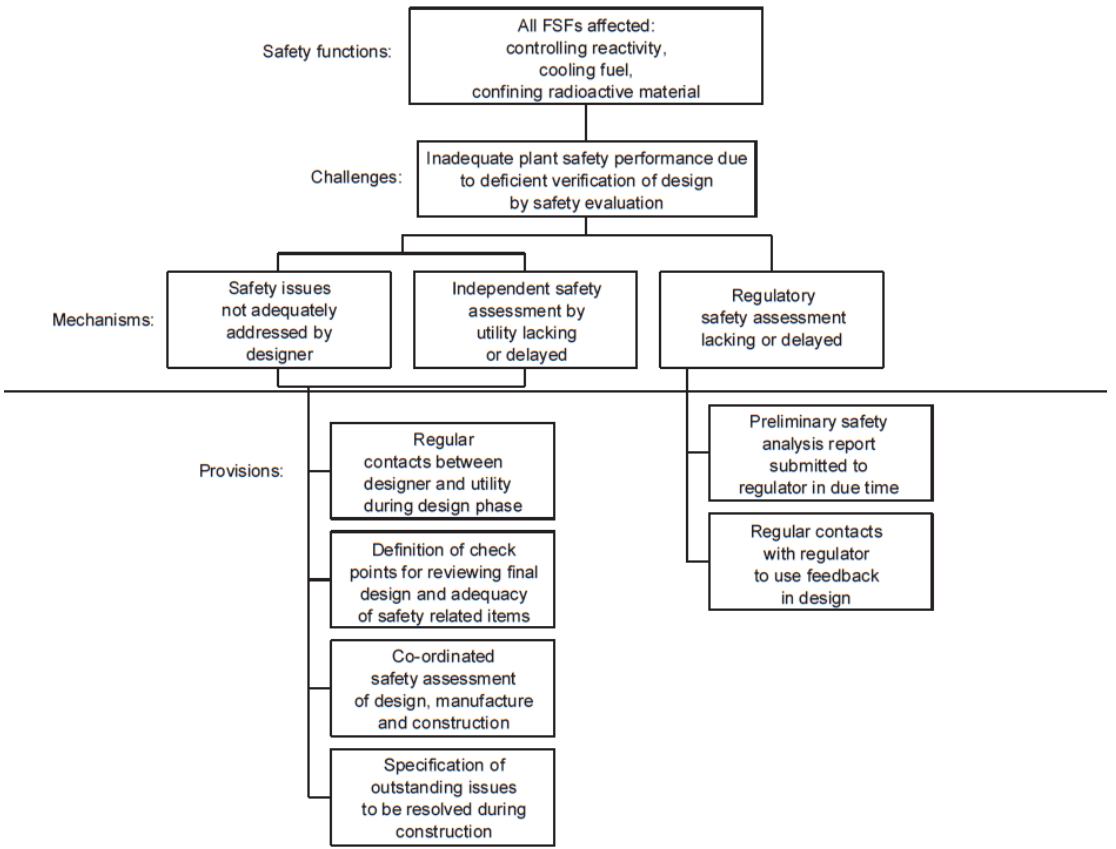


FIG. 55. Objective tree for Levels 1–4 of defence in depth. Safety principle (246): safety evaluation of design.

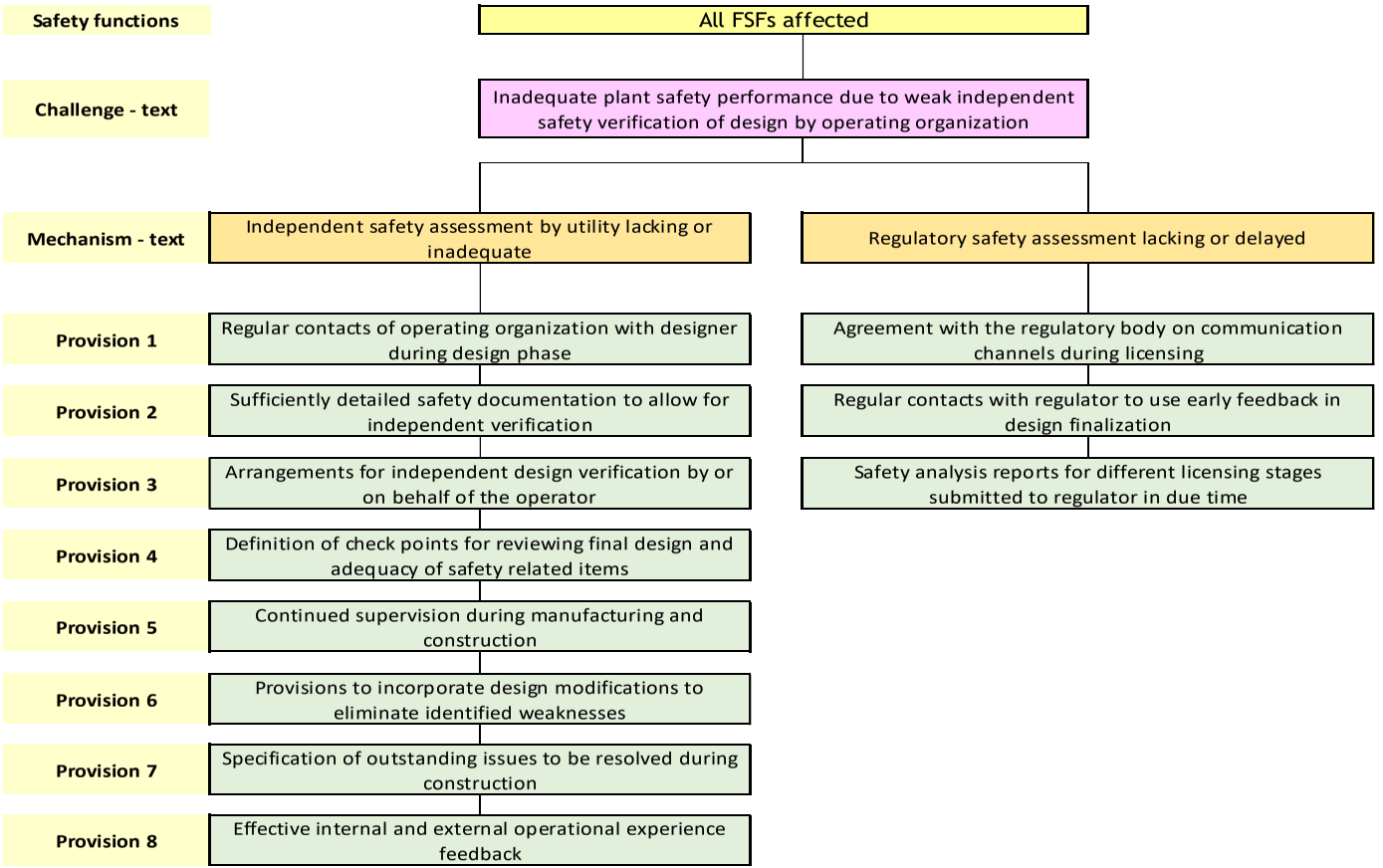


FIG. 55. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (246): safety evaluation of design.

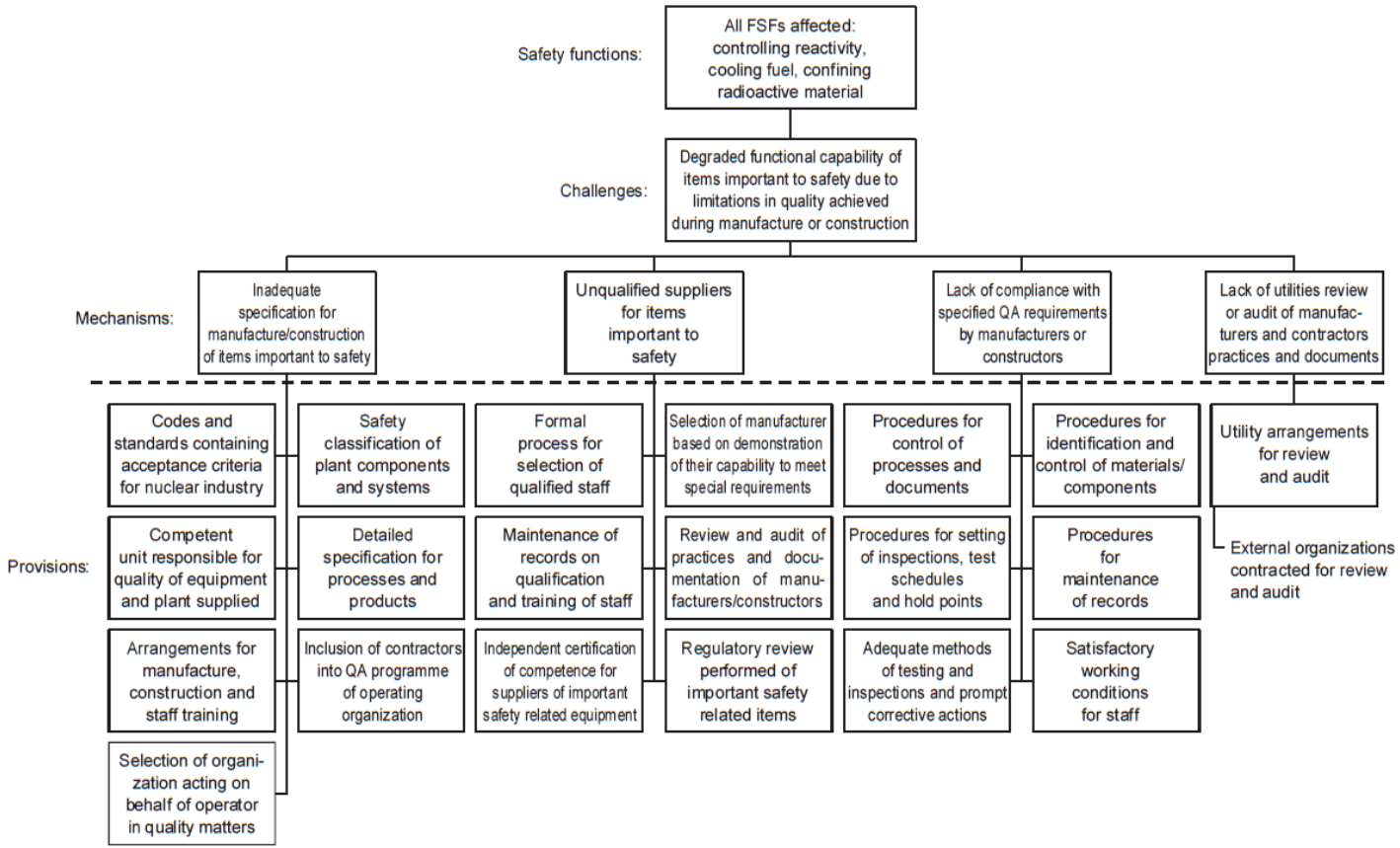


FIG. 56. Objective tree for Levels 1–4 of defence in depth. Safety principle (249): achievement of quality.

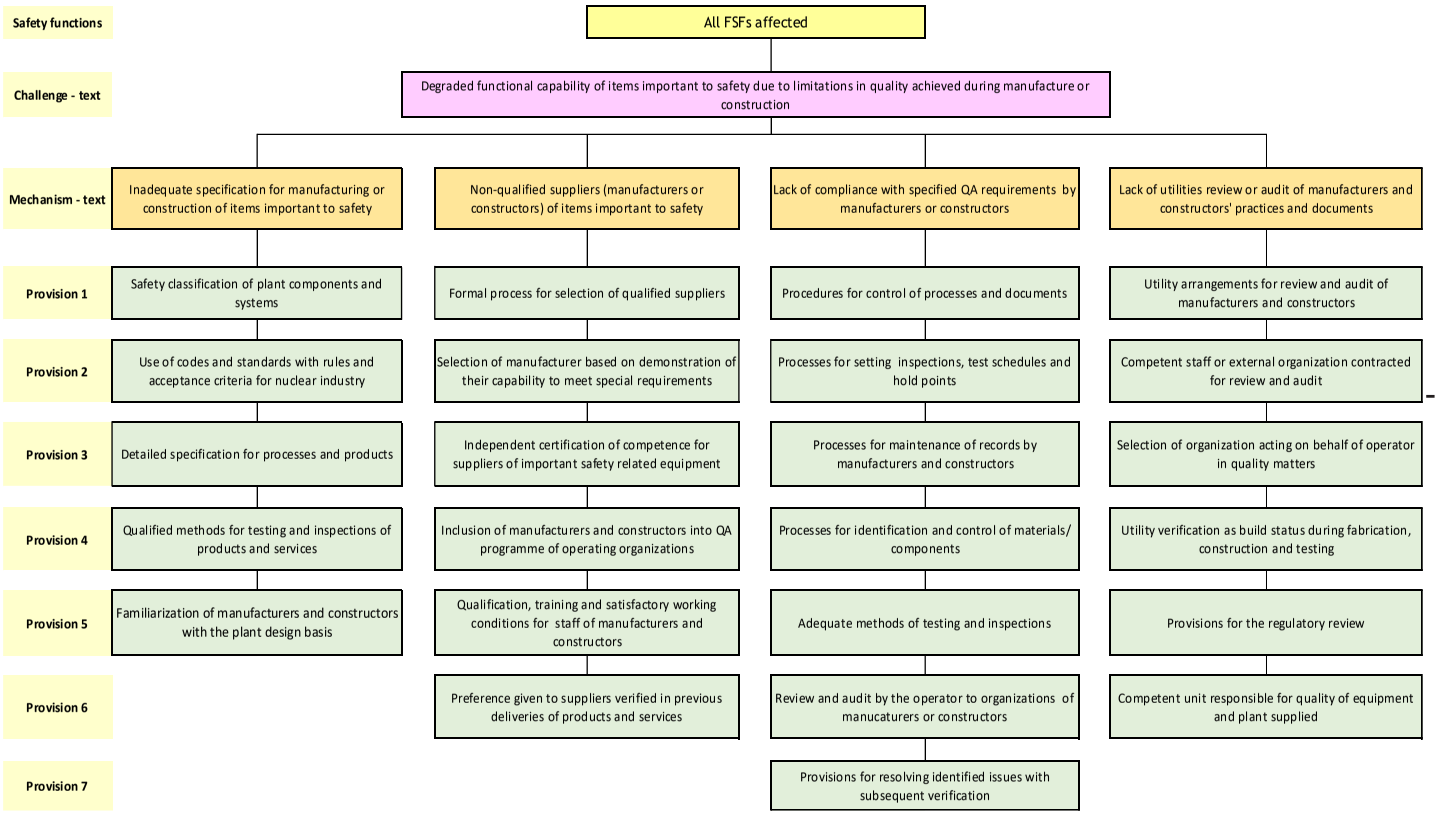


FIG. 56. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (249): achievement of quality.

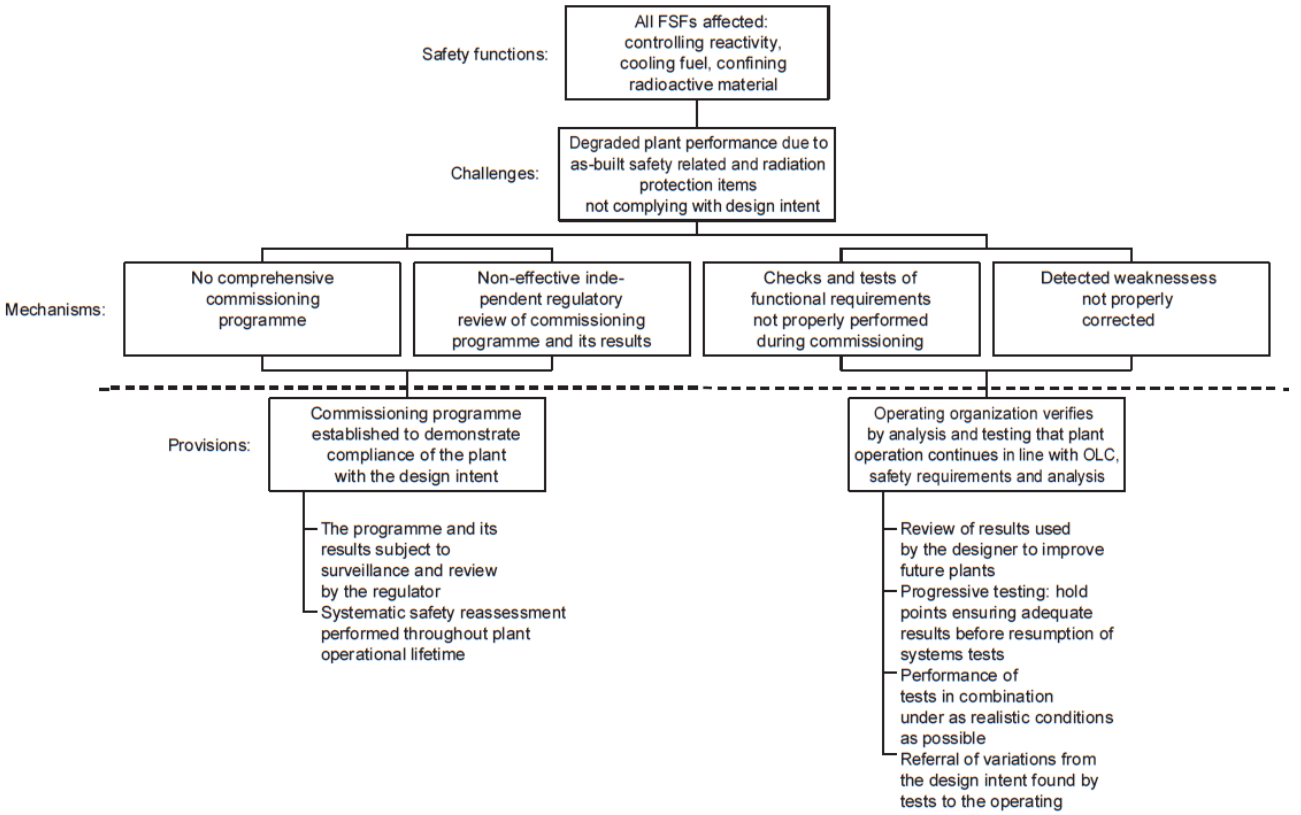


FIG. 57. Objective tree for Levels 1–3 of defence in depth. Safety principle (255): verification of design and construction.

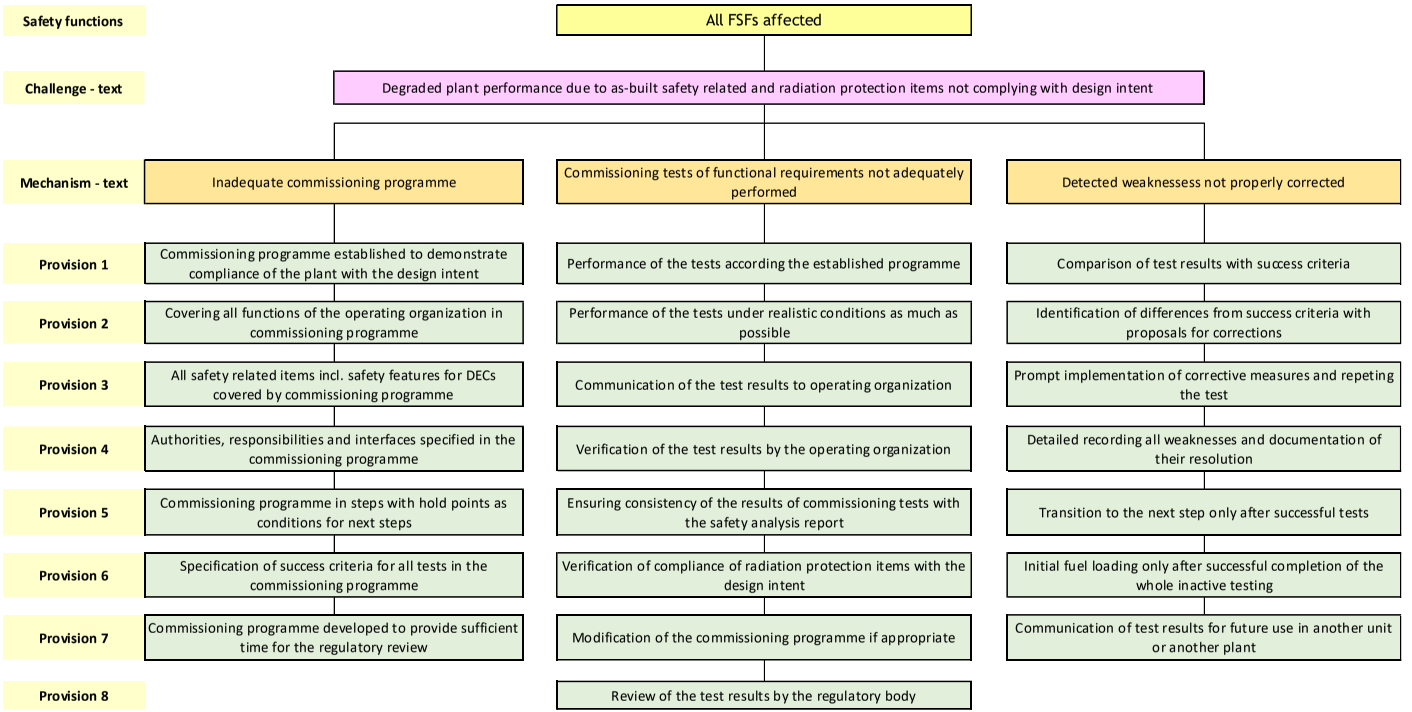


FIG. 57. Updated- Objective tree for Levels 1–4 of defence in depth. Safety principle (255): verification of design and construction.

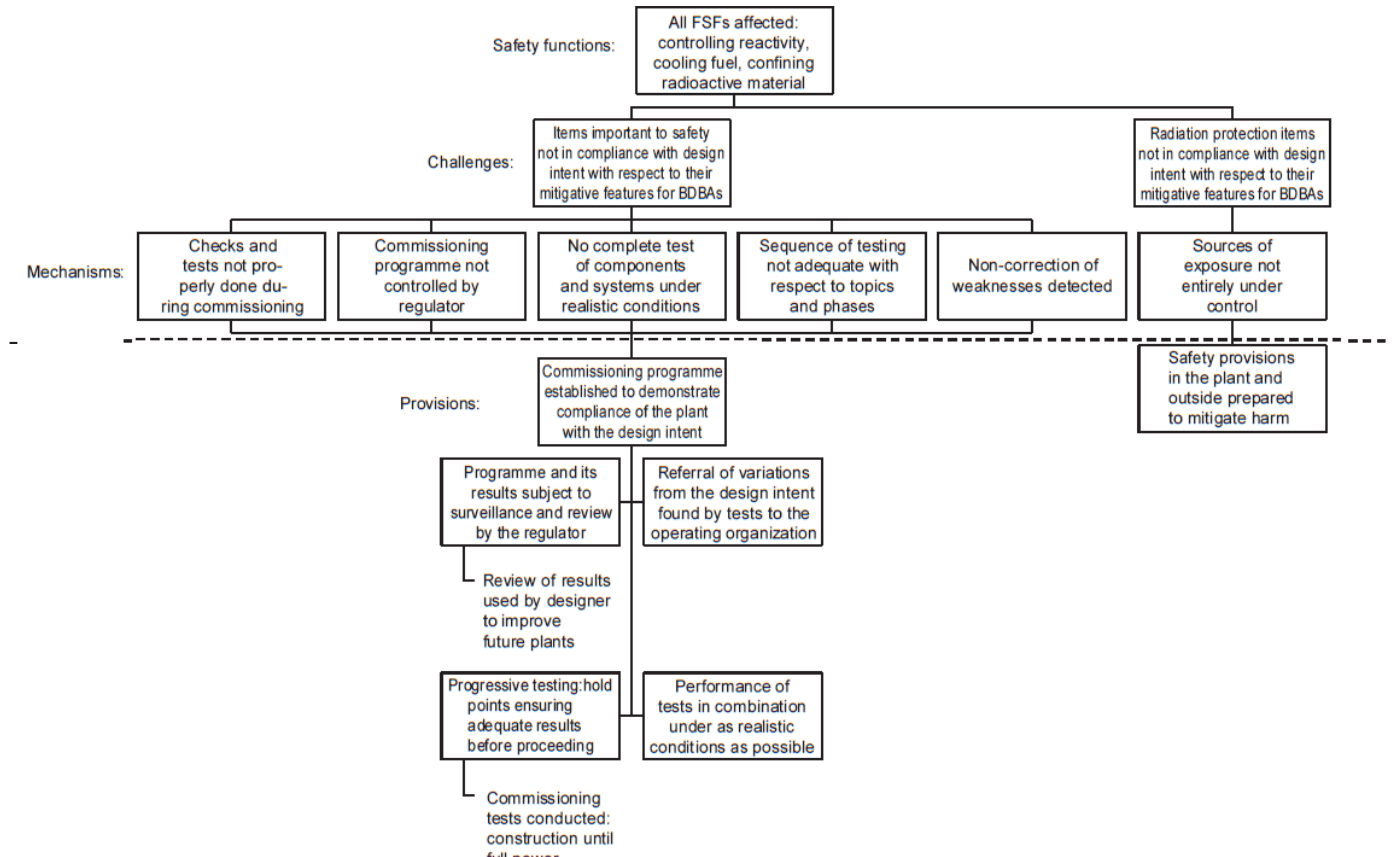


FIG. 58. Objective tree for Level 4 of defence in depth. Safety principle (255): verification of design and construction.

Fig. 58 was combined with fig. 57

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

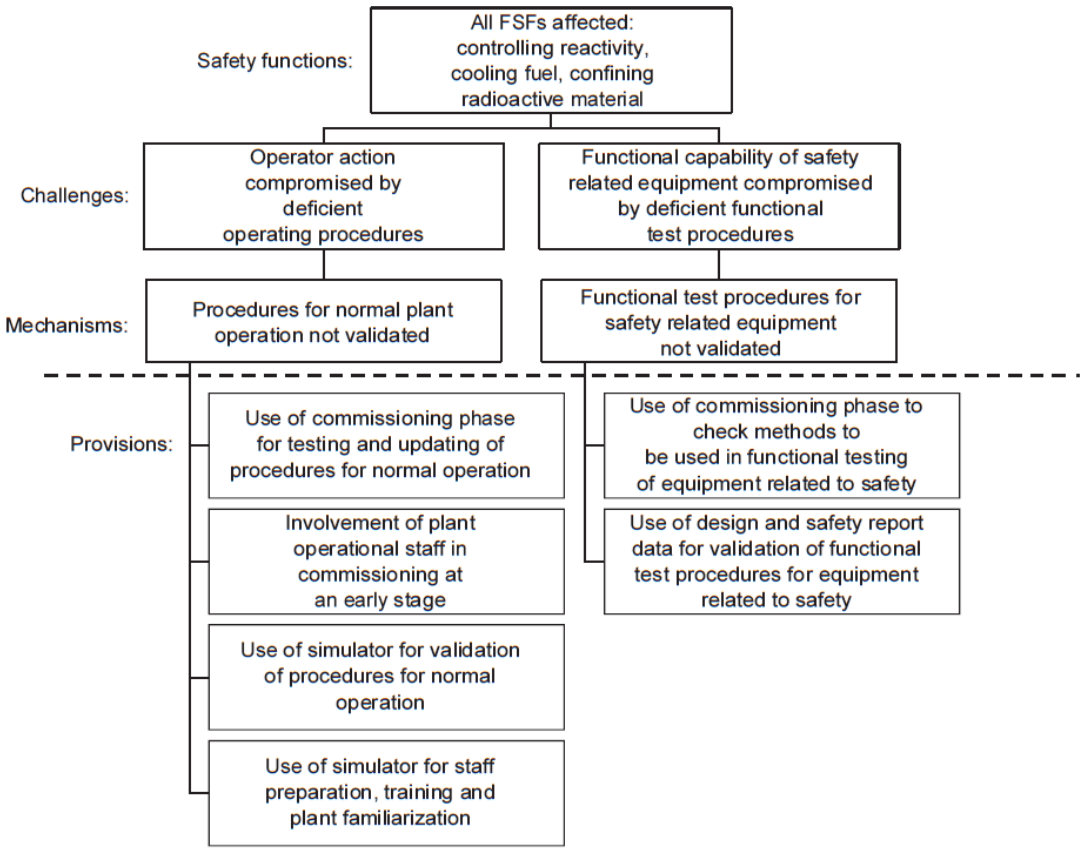


FIG. 59. Objective tree for Levels 1–4 of defence in depth. Safety principle (258): validation of operating and functional test procedures.

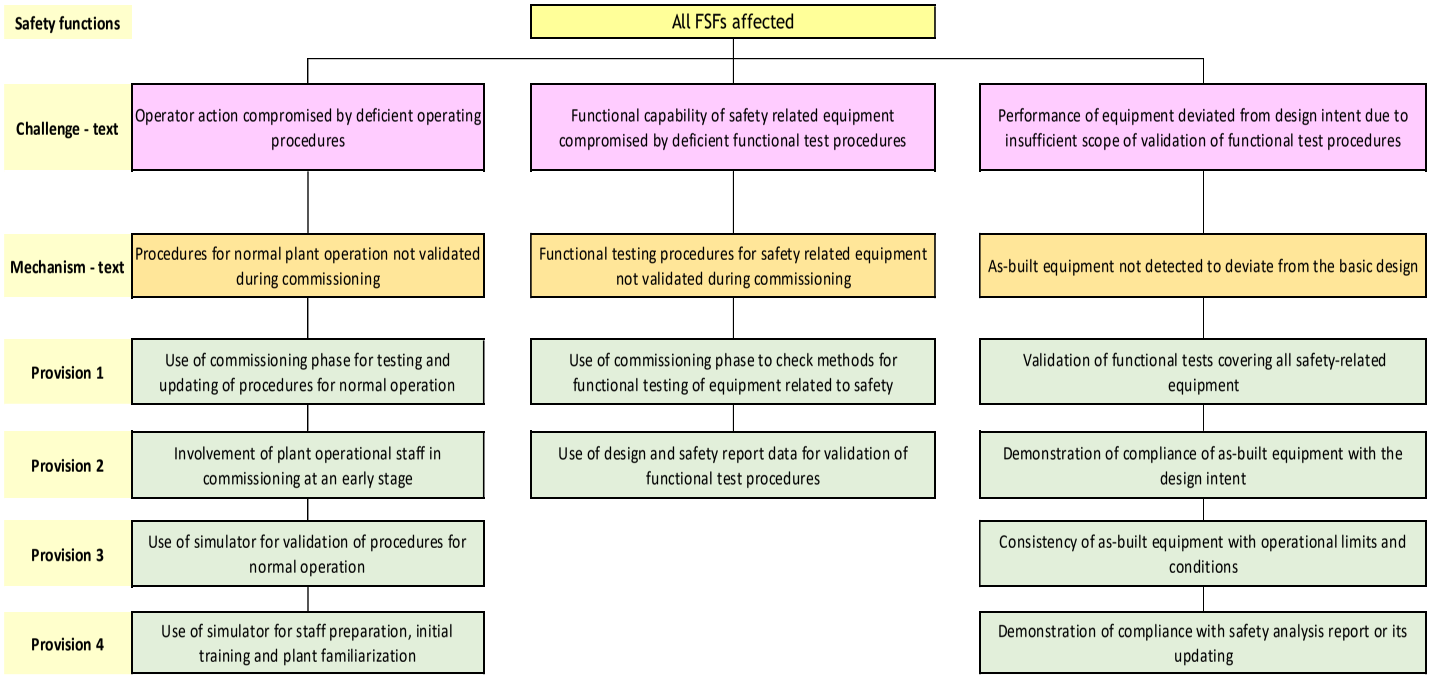


FIG. 59. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (258): validation of operating and functional test procedures.

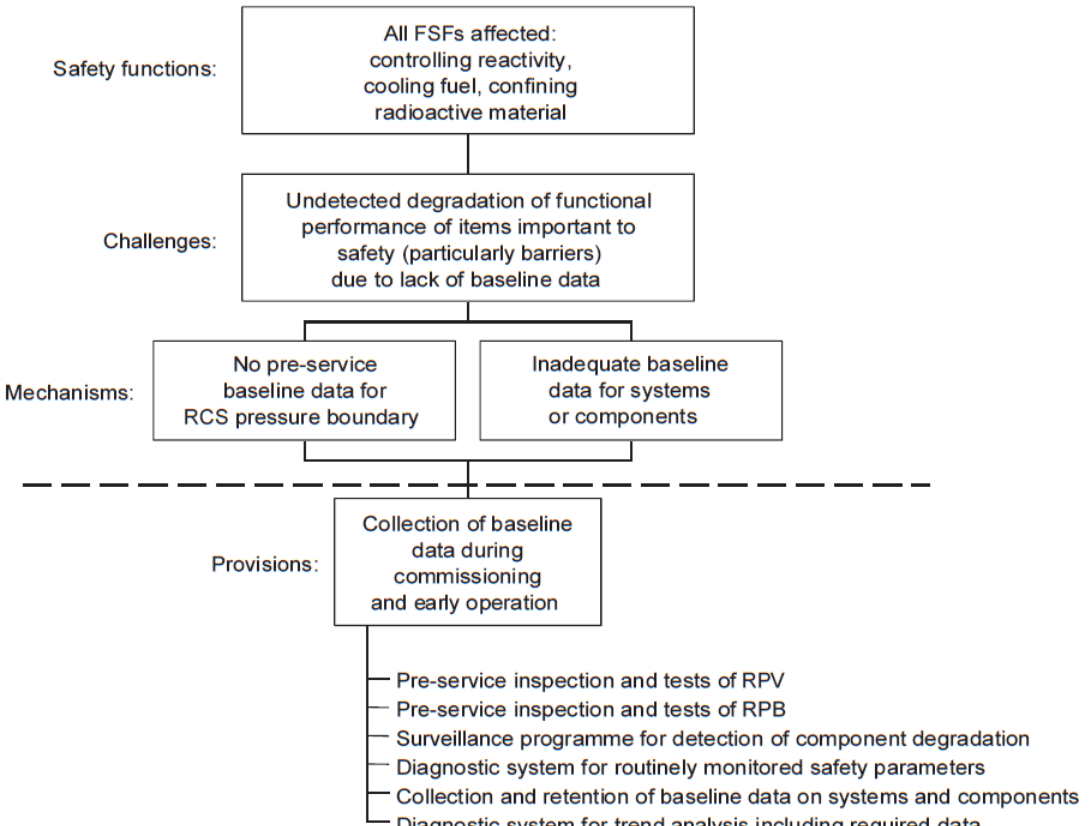


FIG. 60. Objective tree for Levels 1–4 of defence in depth. Safety principle (260): collection of baseline data.

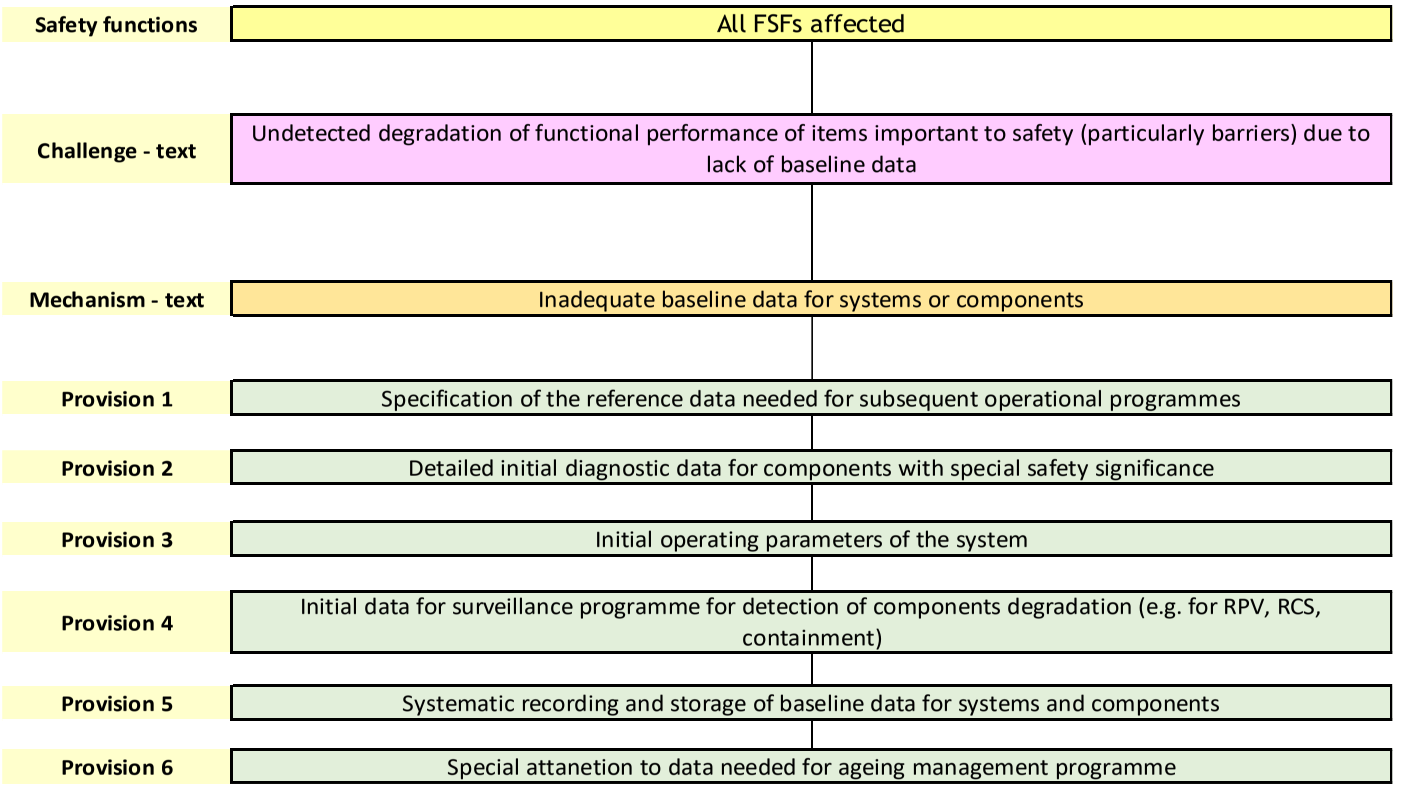


FIG. 60. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (260): collection of baseline data.

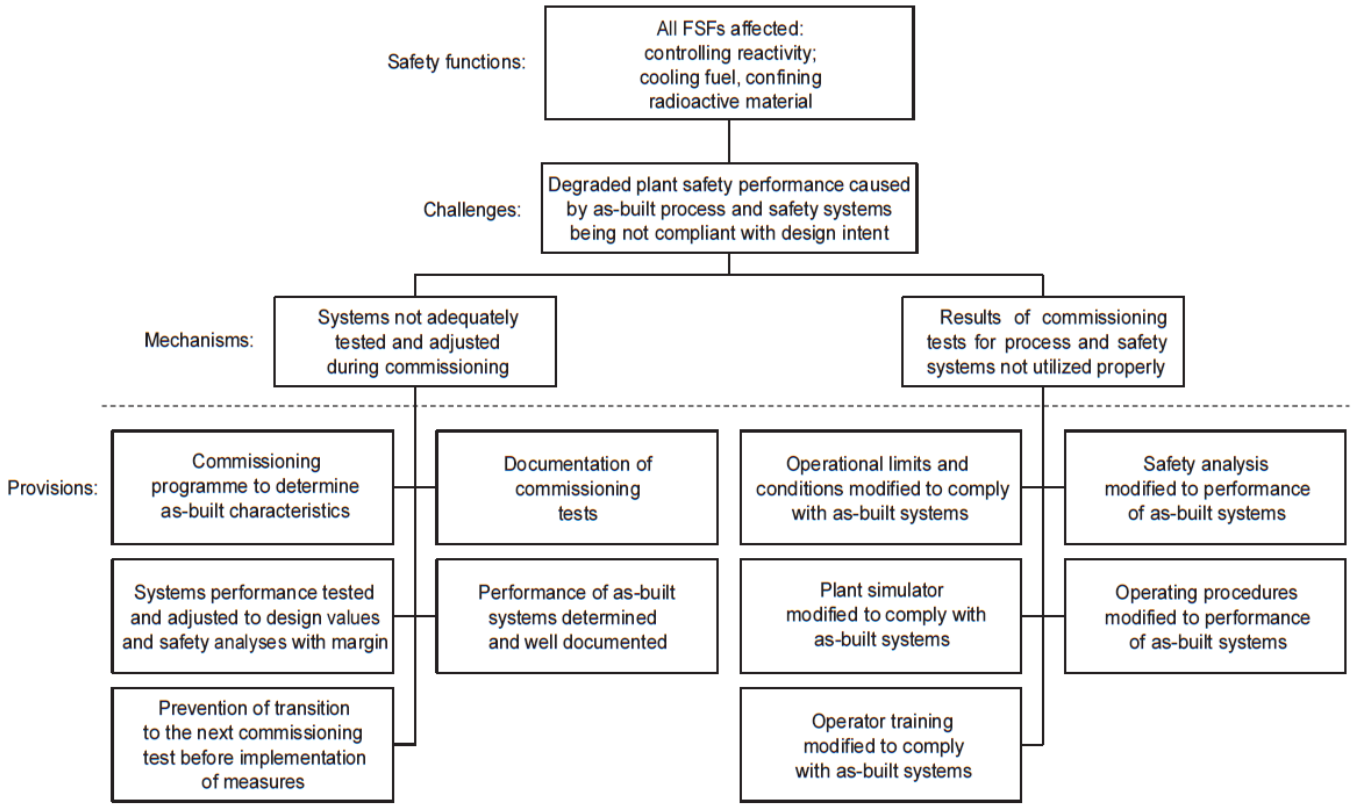


FIG. 61. Objective tree for Levels 1–4 of defence in depth. Safety principle (262): pre-operational adjustment of plant.

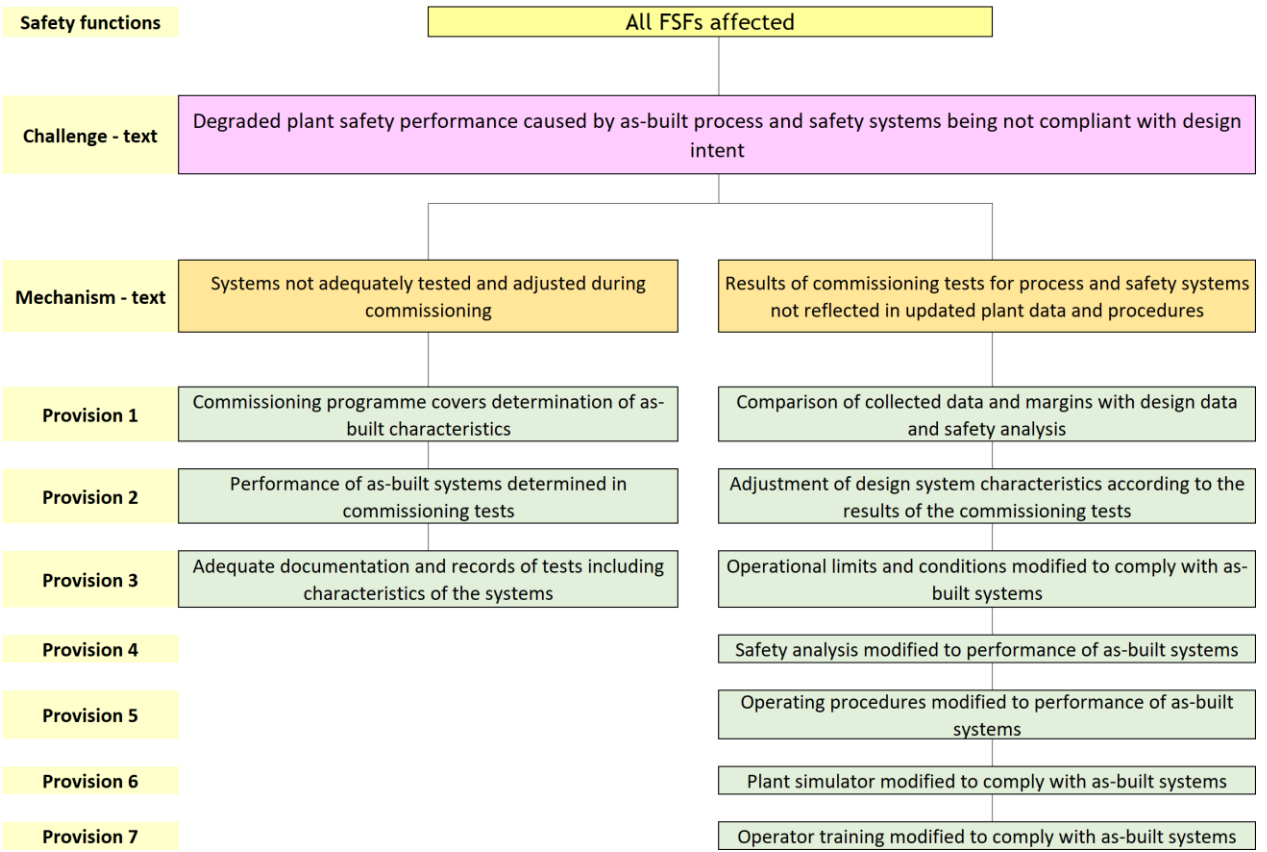


FIG. 61. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (262): pre-operational adjustment of plant.

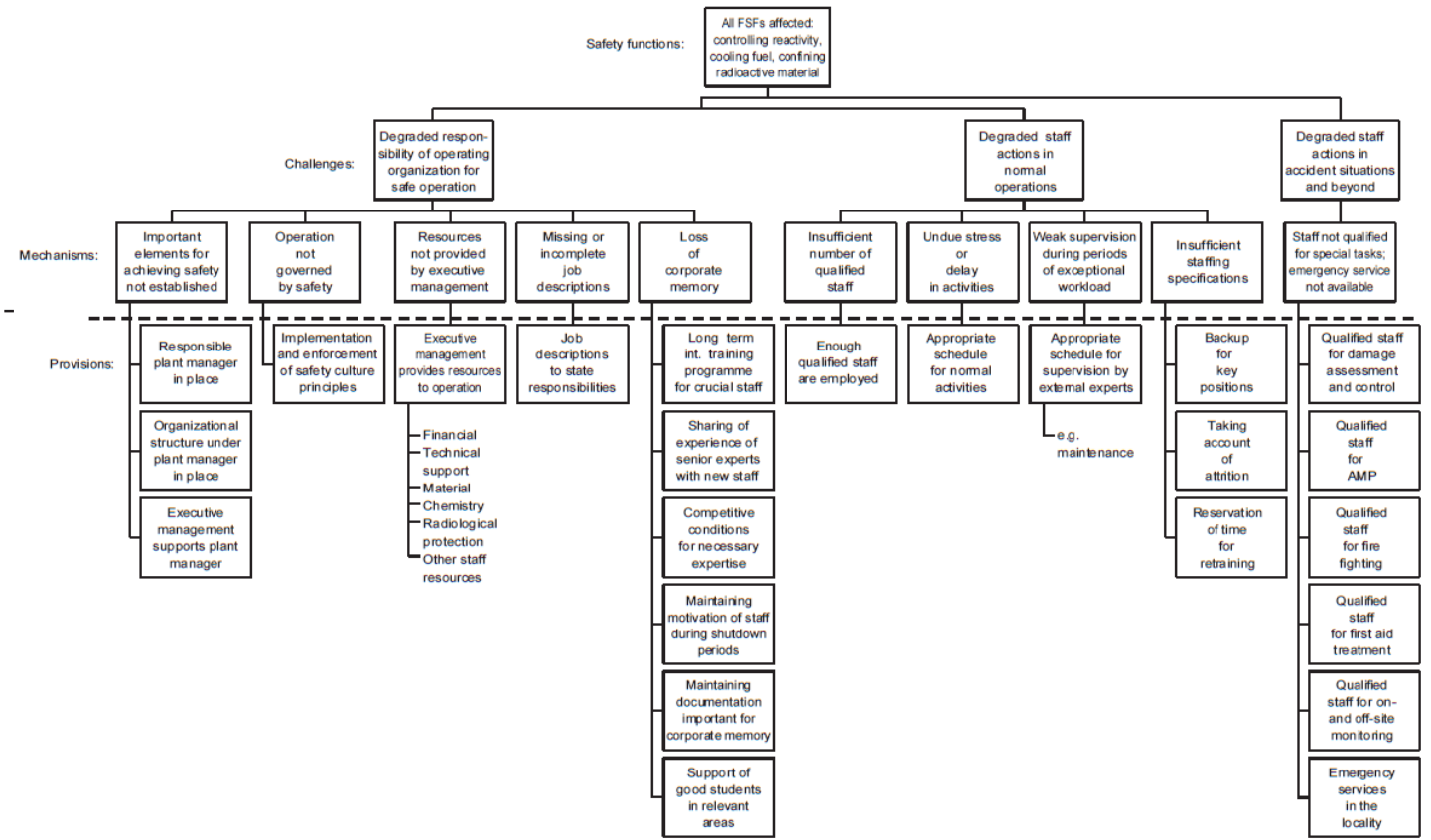


FIG. 62. Objective tree for Levels 1–4 of defence in depth. Safety principle (265): organization, responsibilities and staffing.

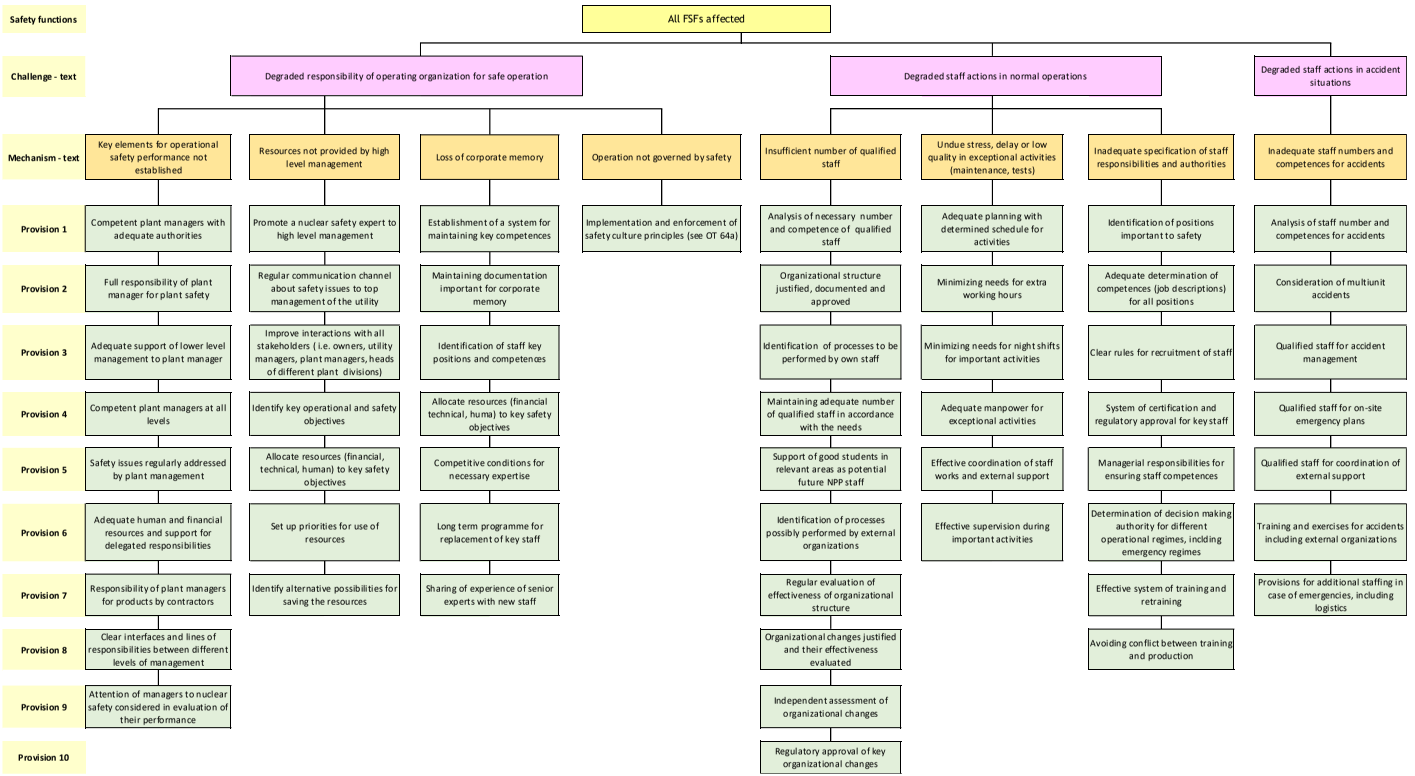


FIG 62 Upated. Objective tree for Levels 1–4 of defence in depth. Safety principle (265): organization, responsibilities and staffing.

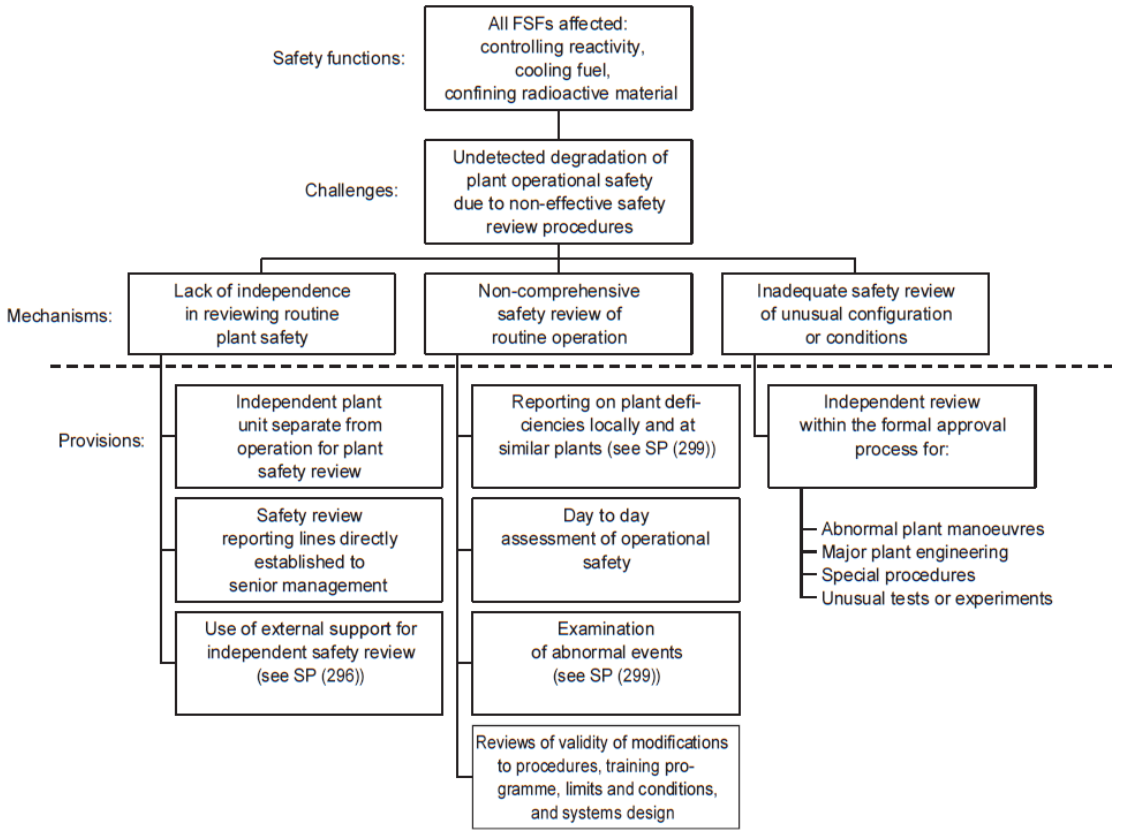


FIG. 63. Objective tree for Levels 1–4 of defence in depth. Safety principle (269): safety review procedures.

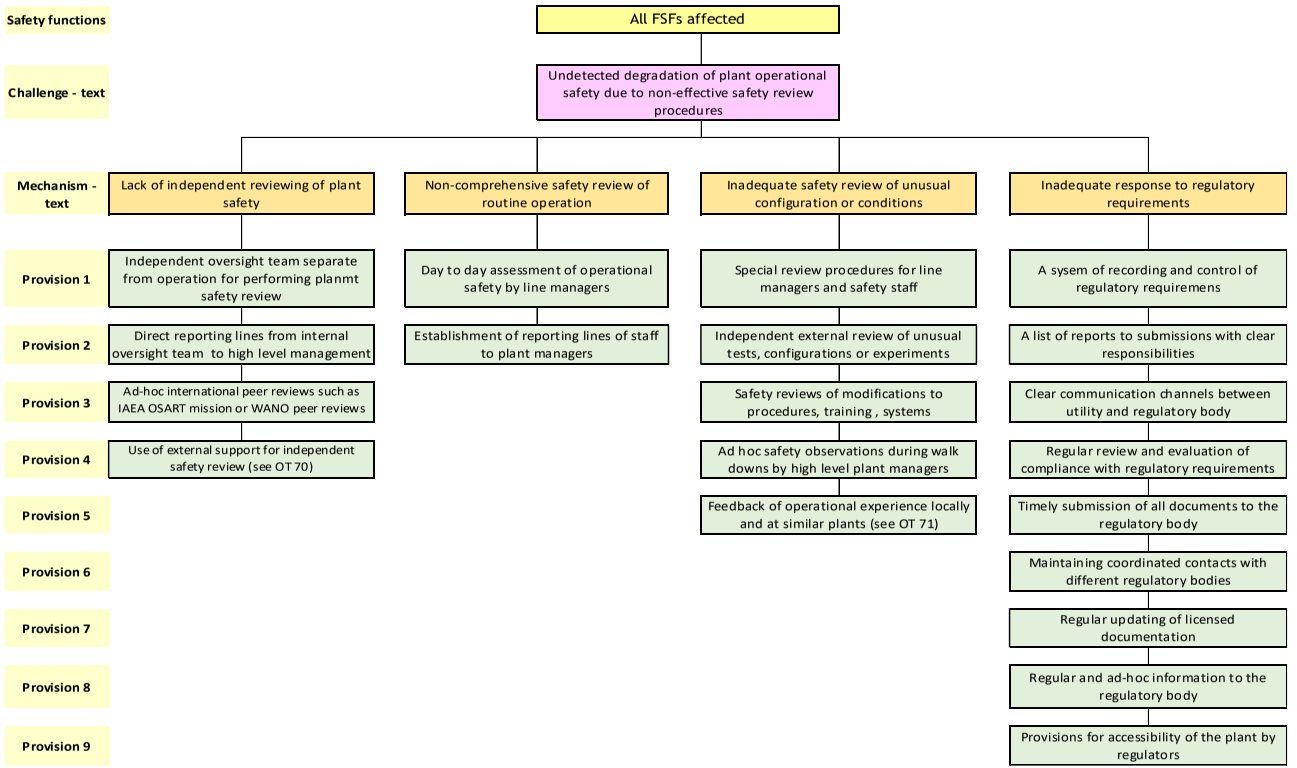


FIG. 63. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (269): safety review procedures.

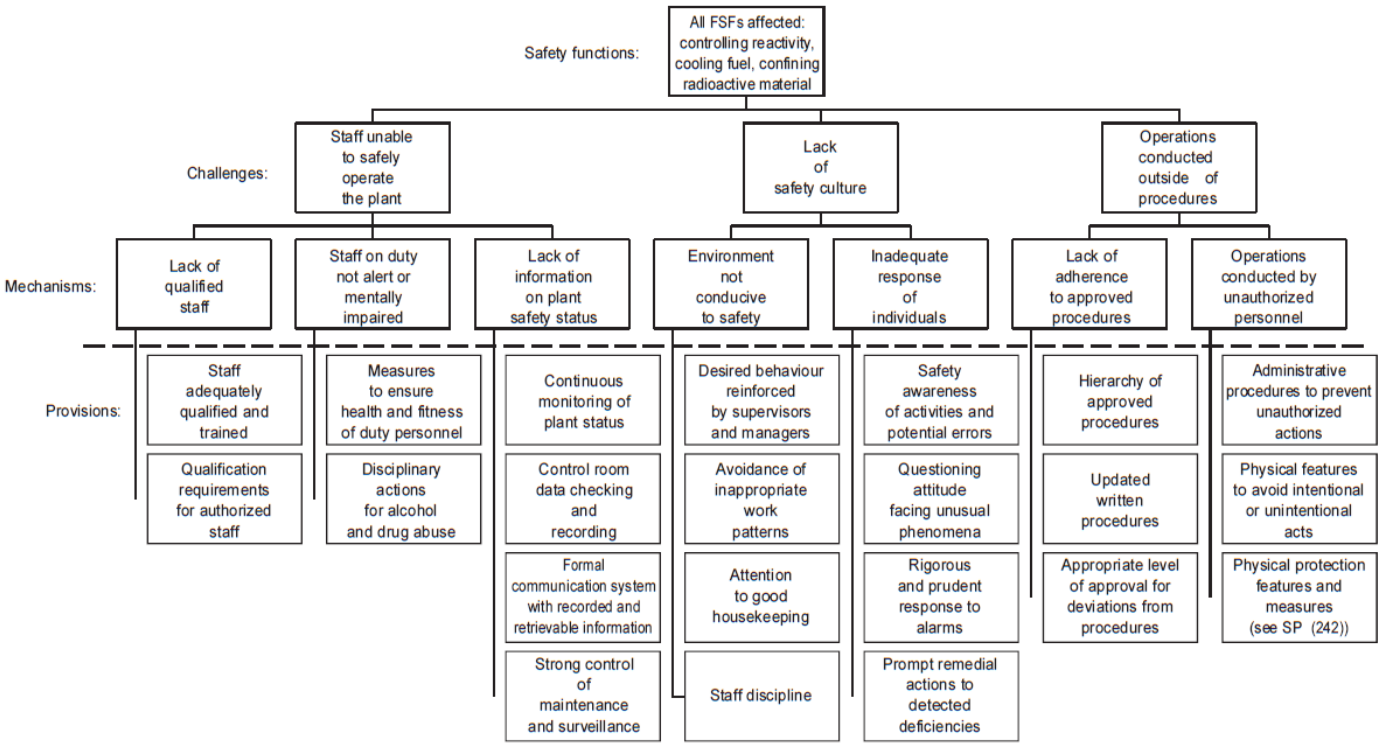


FIG. 64.Objective tree for Level 1 of defence in depth. Safety principle (272): conduct of operations.

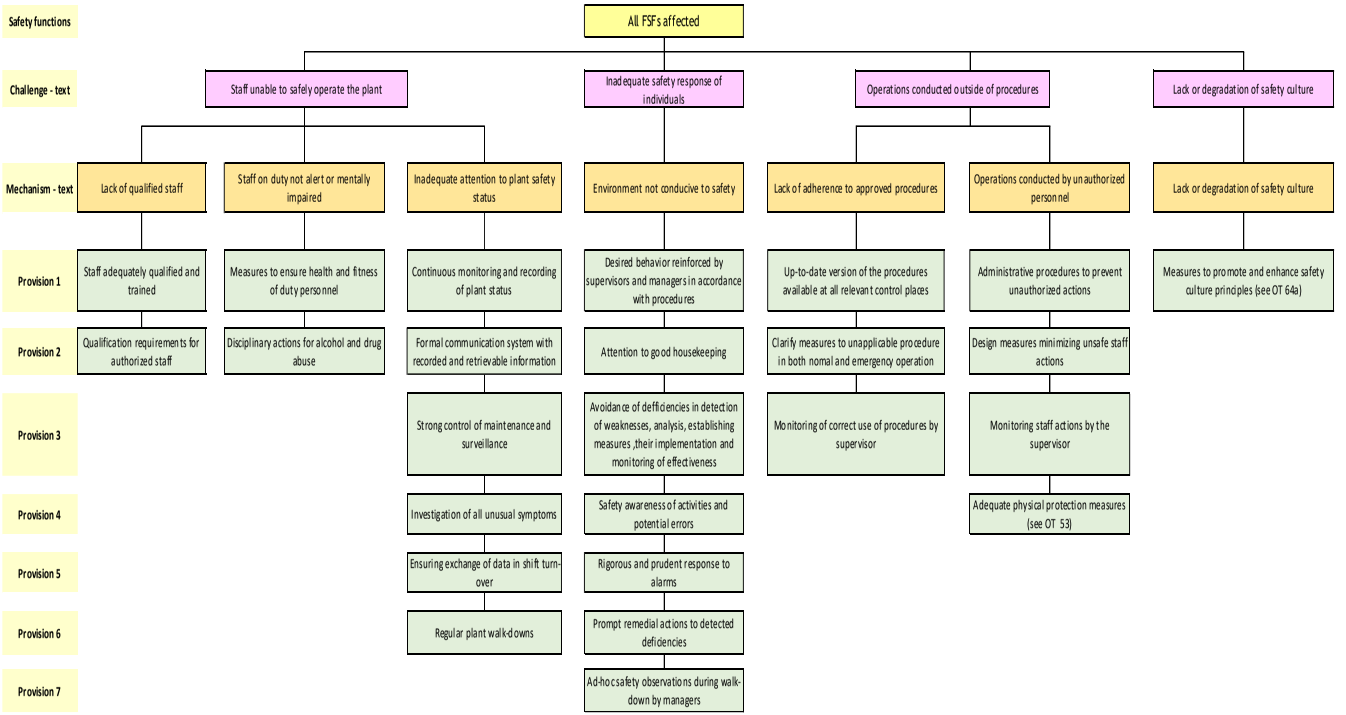


FIG. 64. Updated. Objective tree for Levels 1-4 of defence in depth. Safety principle (272): conduct of operations.

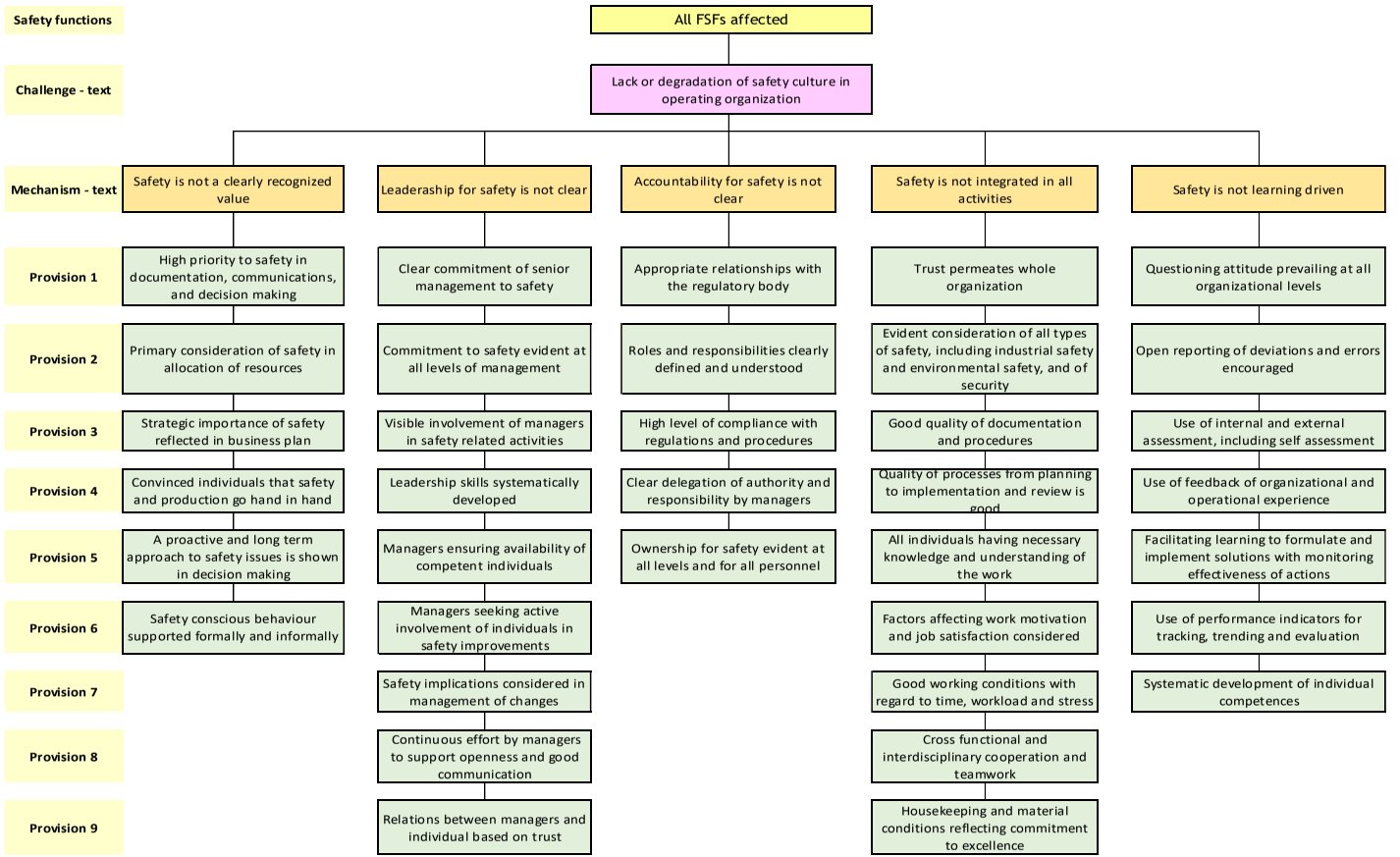


FIG. 64.a Updated. Objective tree for Levels 1-4 of defence in depth. Safety principle (272): conduct of

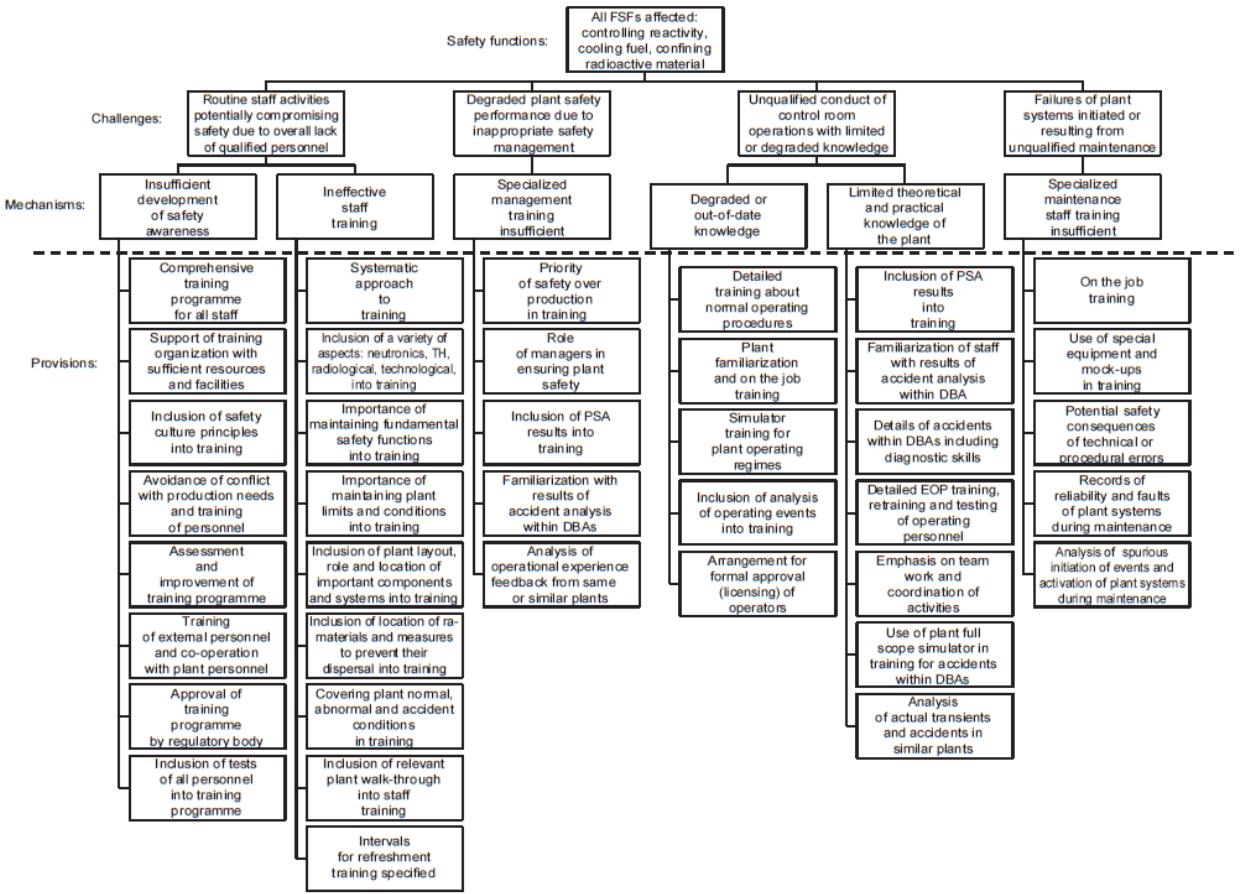


FIG. 65. Objective tree for Levels 1–3 of defence in depth. Safety principle (278): training (see also SP (323)).

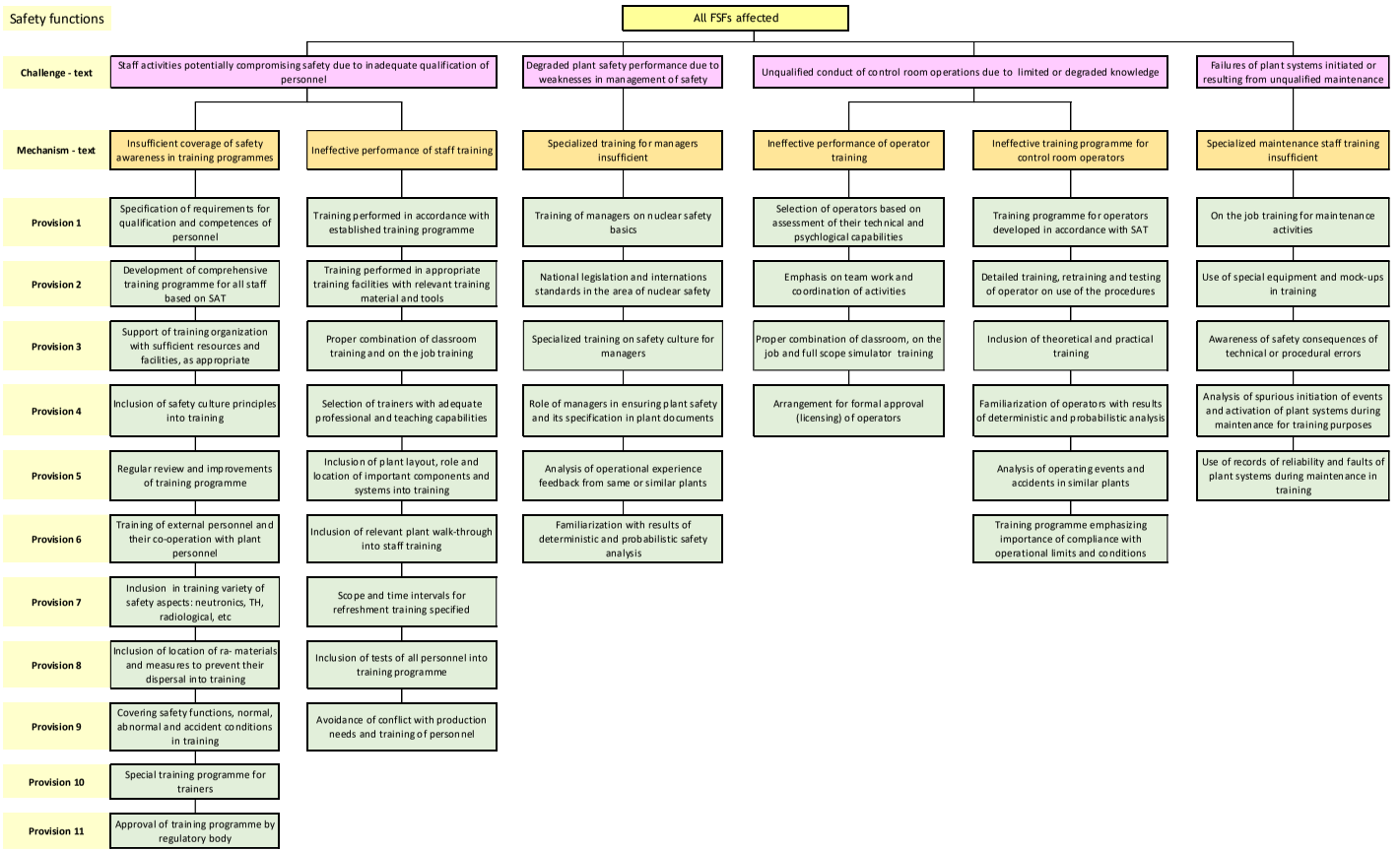


FIG. 65. Updated. Objective tree for Levels 1–3 of defence in depth. Safety principle (279): training (see also SP (323)).

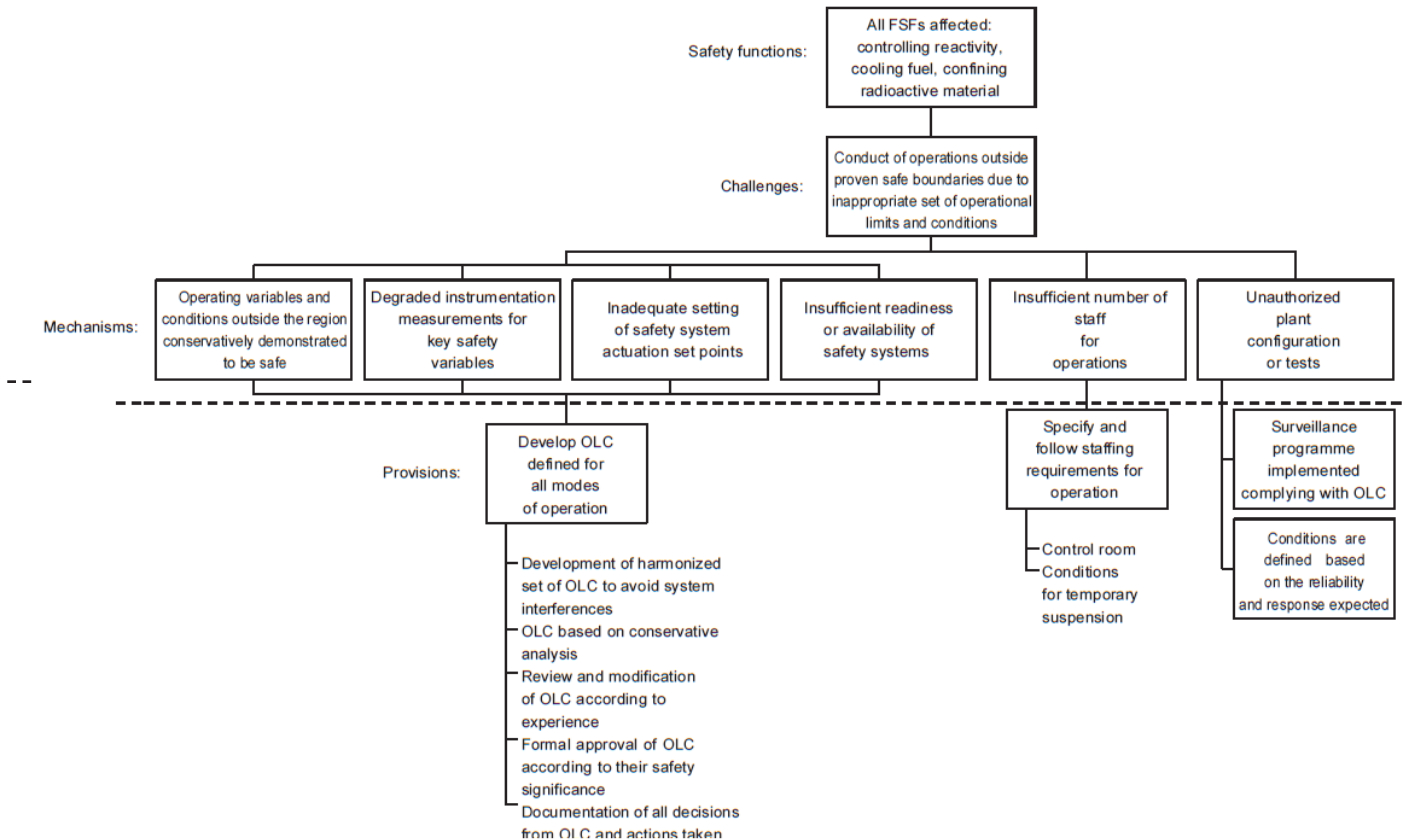


FIG. 66. Objective tree for Levels 1–3 of defence in depth. Safety principle (284): operational limits and conditions.

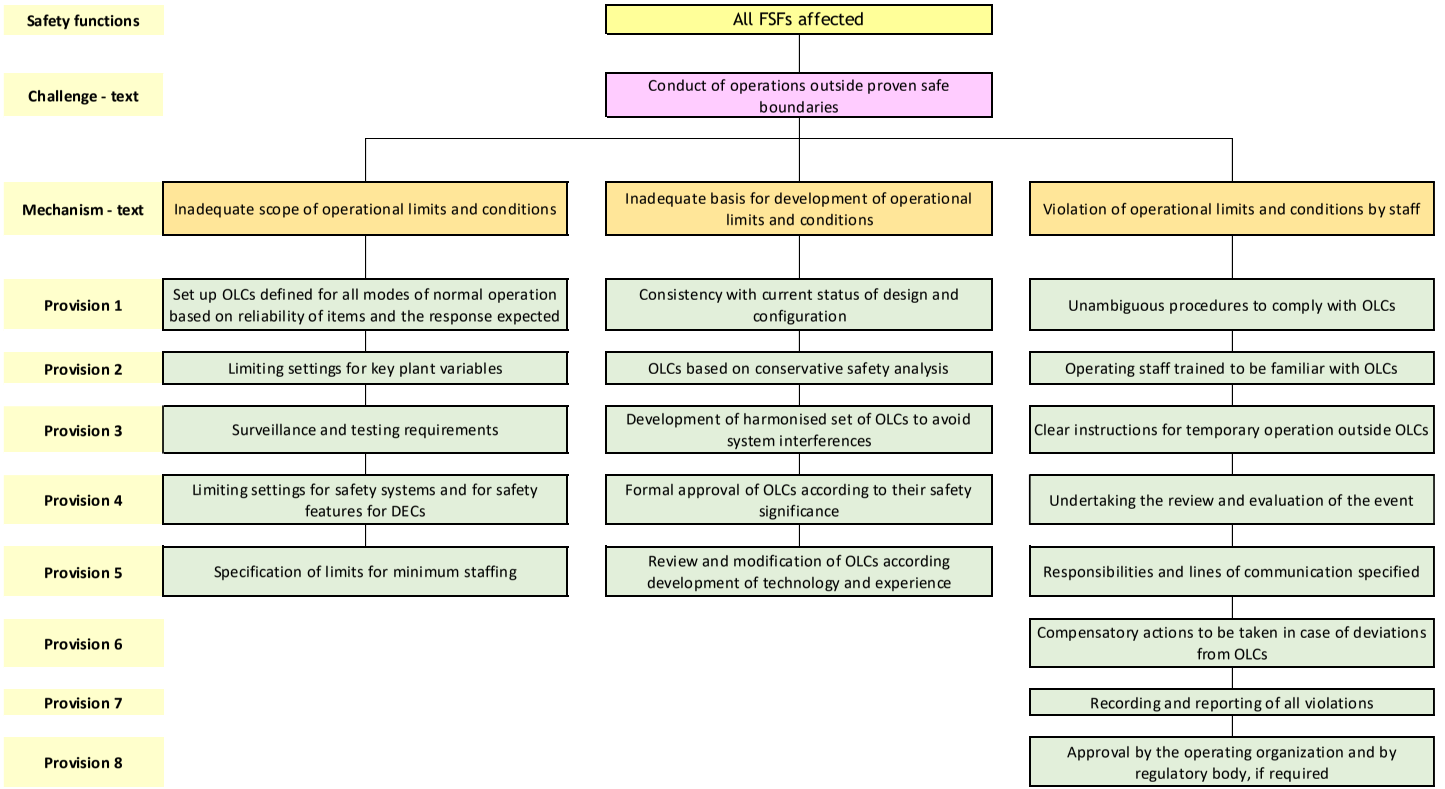


FIG. 66. Updated. Objective tree for Level 1 of defence in depth. Safety principle (284): operational limits and conditions.

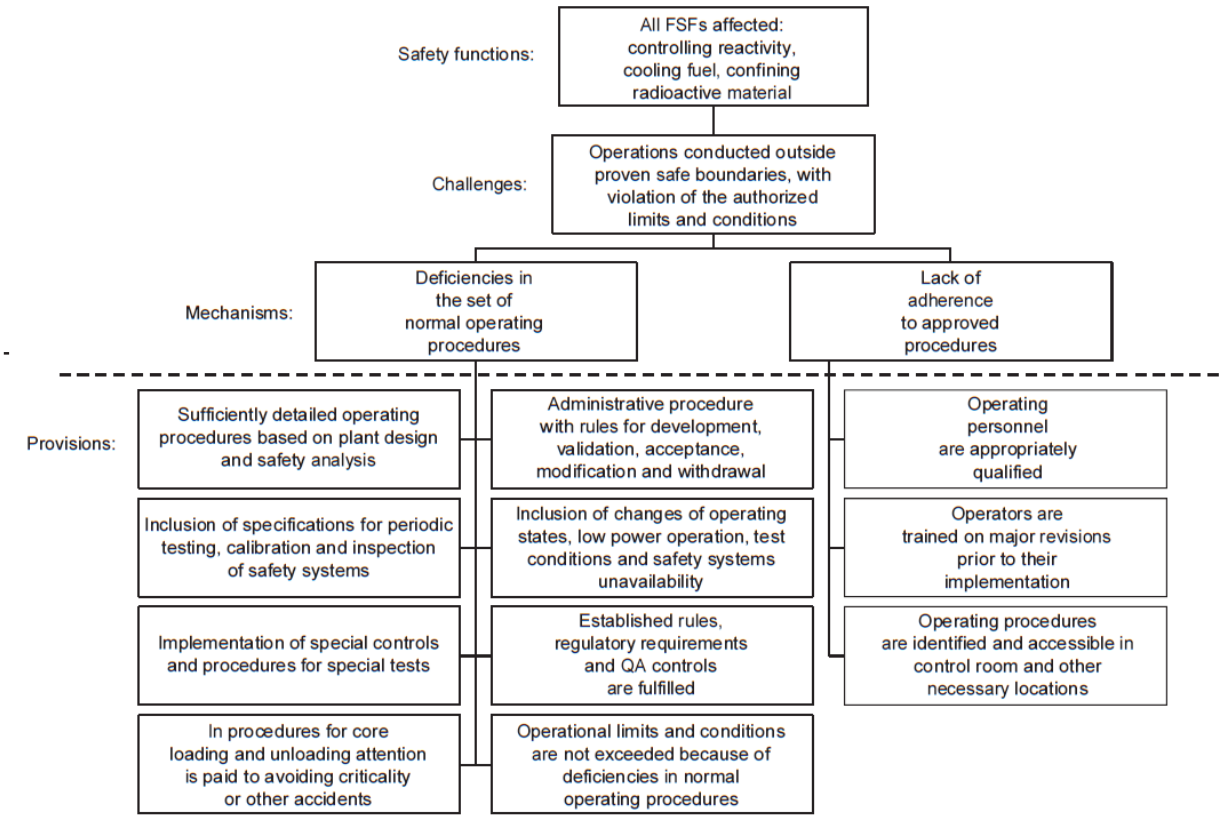


FIG. 67. Objective tree for Level 1 of defence in depth. Safety principle (288): normal operating procedures.

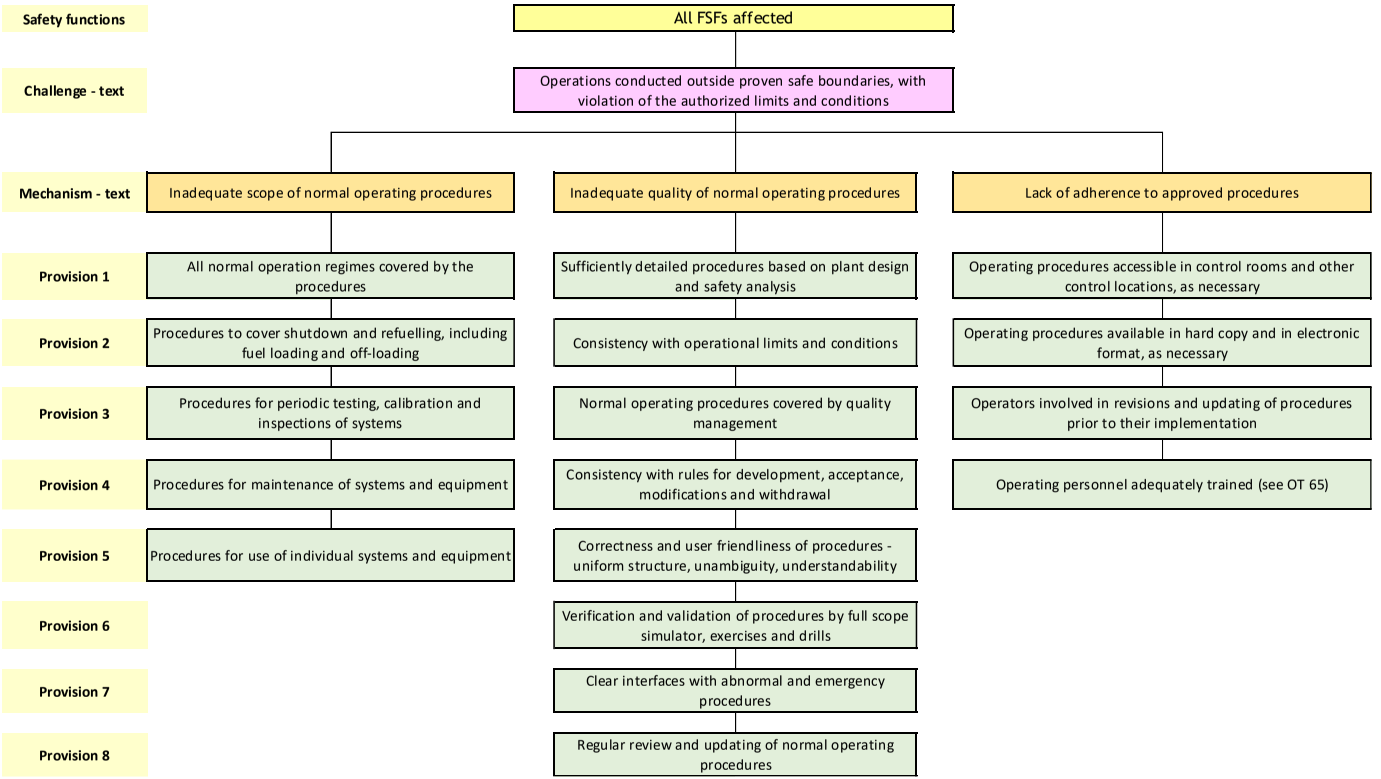


FIG. 67. Updated. Objective tree for Level 1 of defence in depth. Safety principle (288): normal operating procedures.

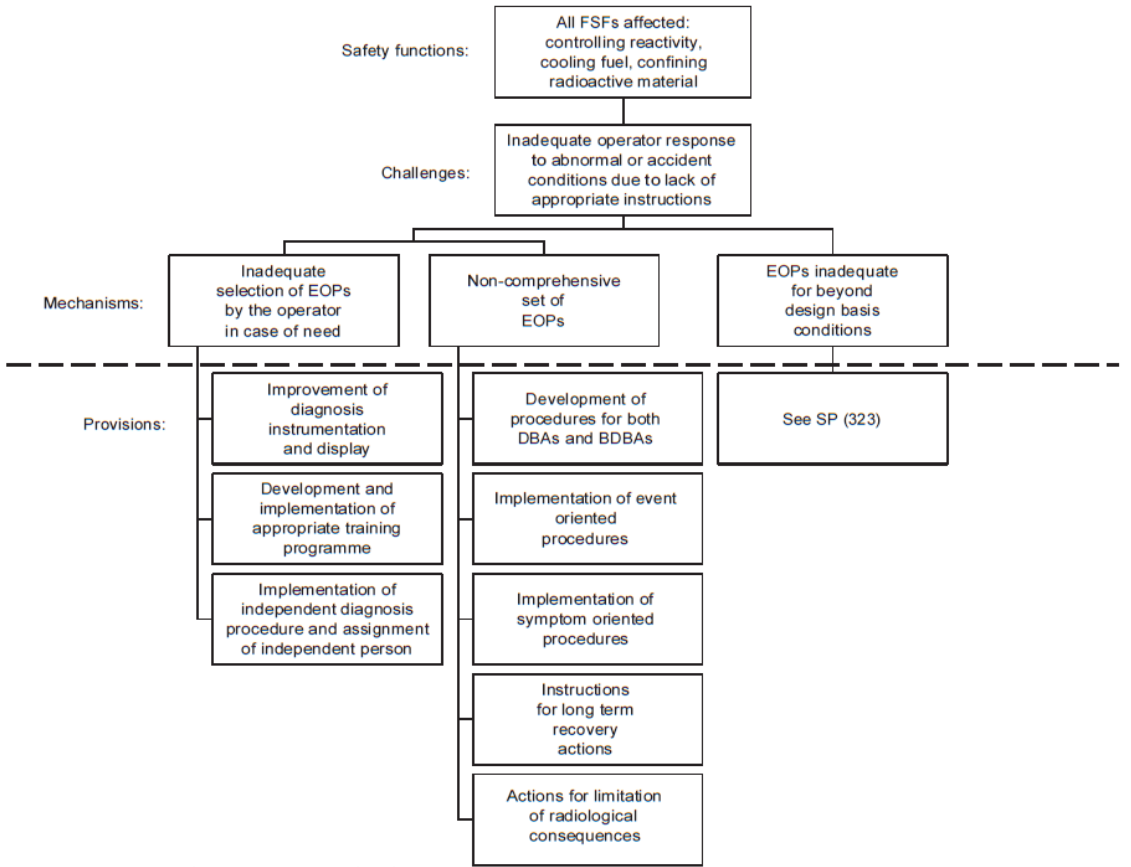


FIG. 68. Objective tree for Levels 2–4 of defence in depth. Safety principle (290): emergency operating procedures.

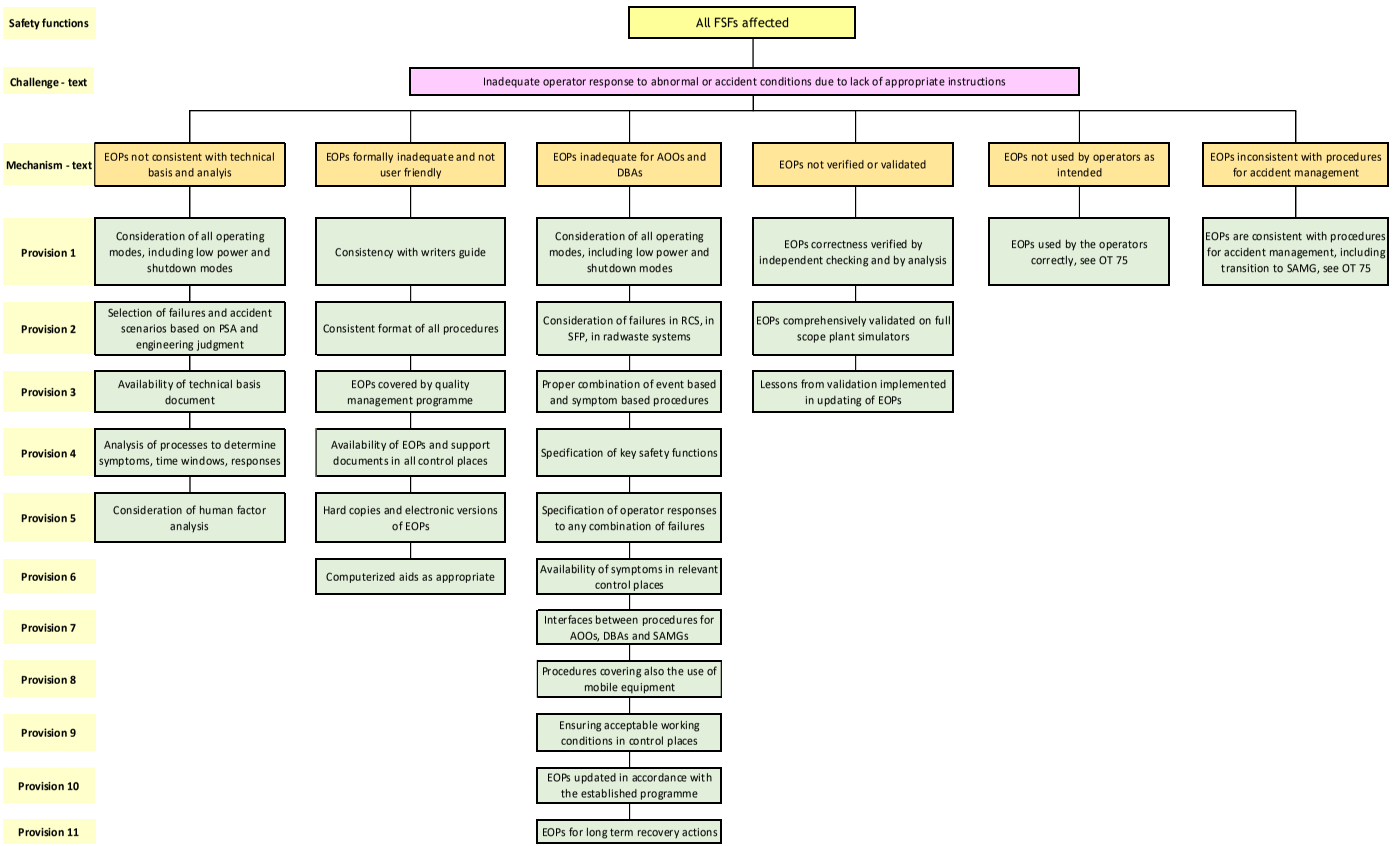


FIG. 68. Updated. Objective tree for Levels 2–4 of defence in depth. Safety principle (290): emergency operating procedures.

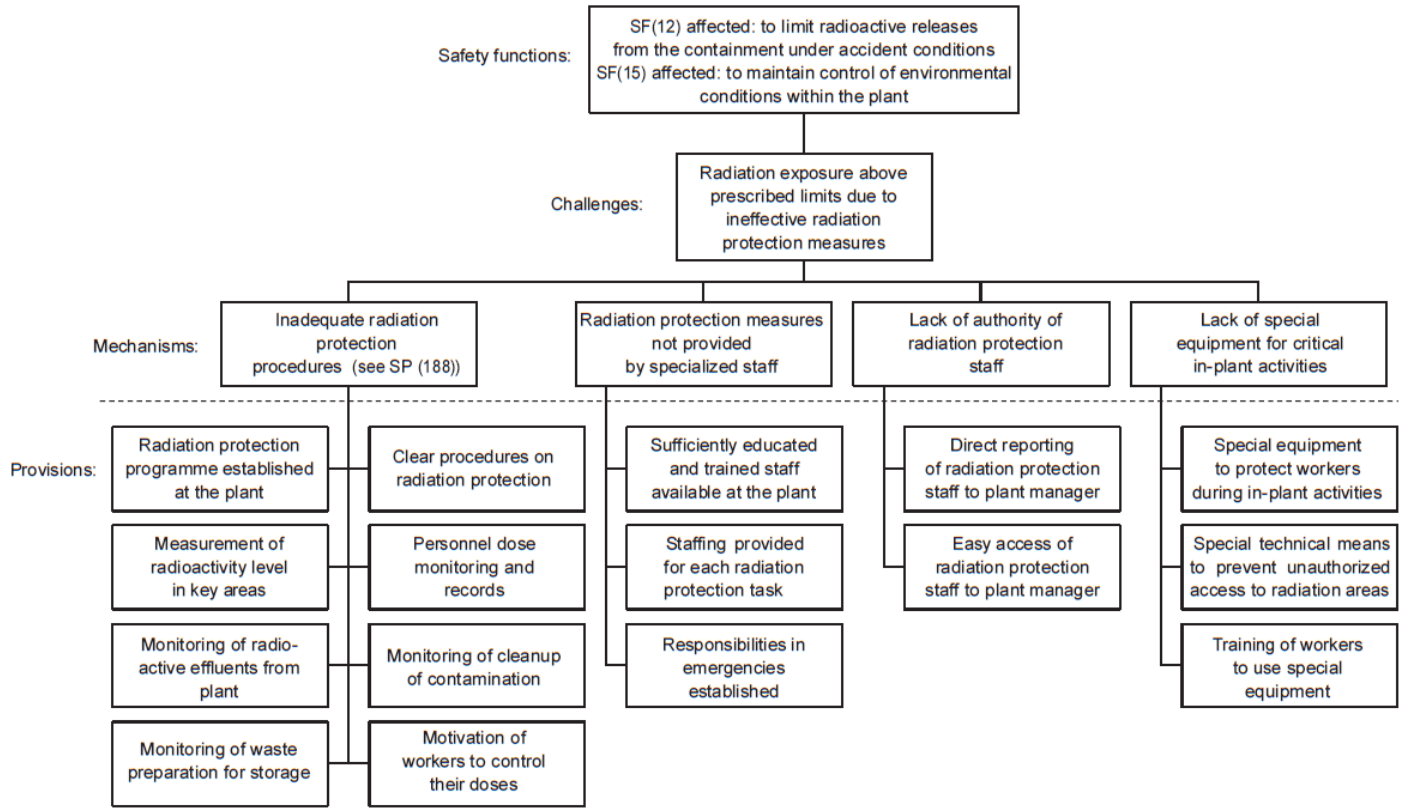


FIG. 69. Objective tree for Levels 1–4 of defence in depth. Safety principle (292): radiation protection procedures.

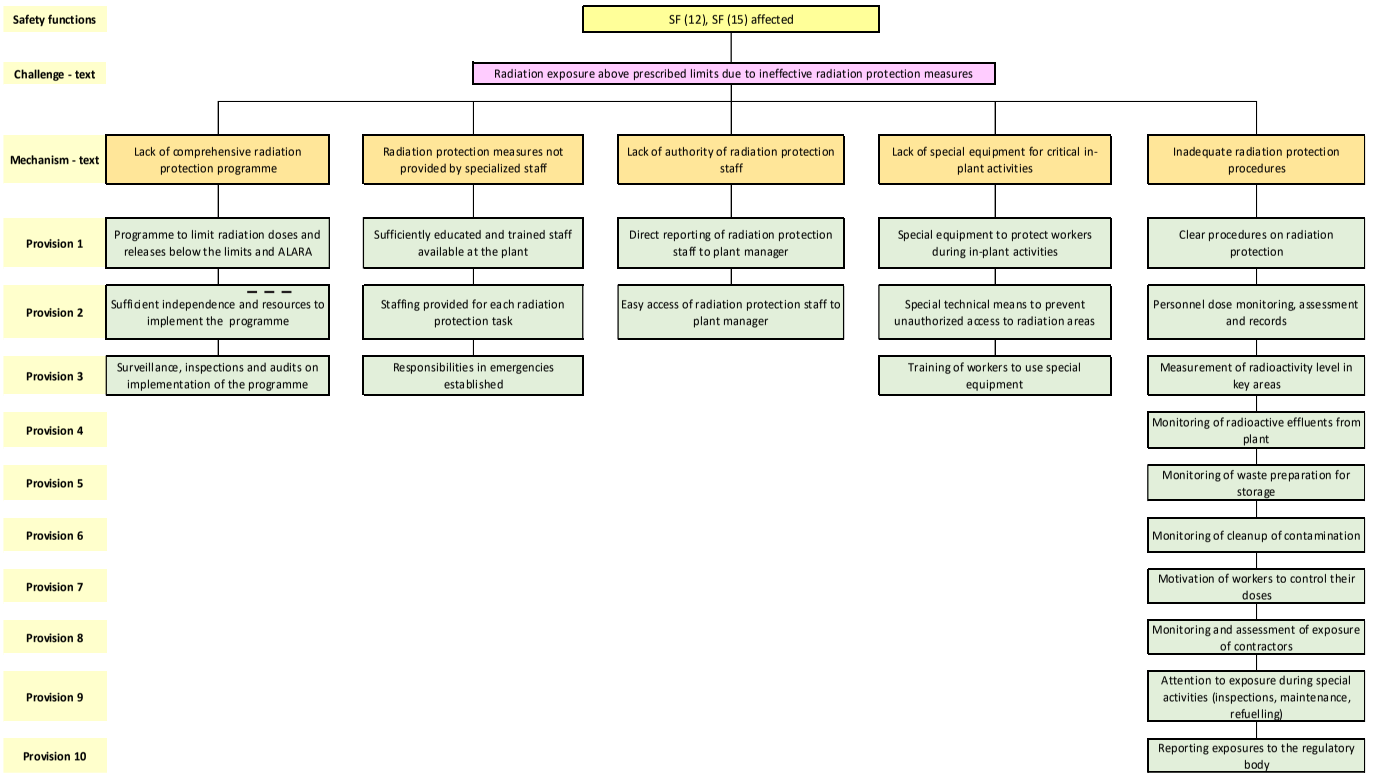


FIG. 69. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (292): radiation protection procedures.

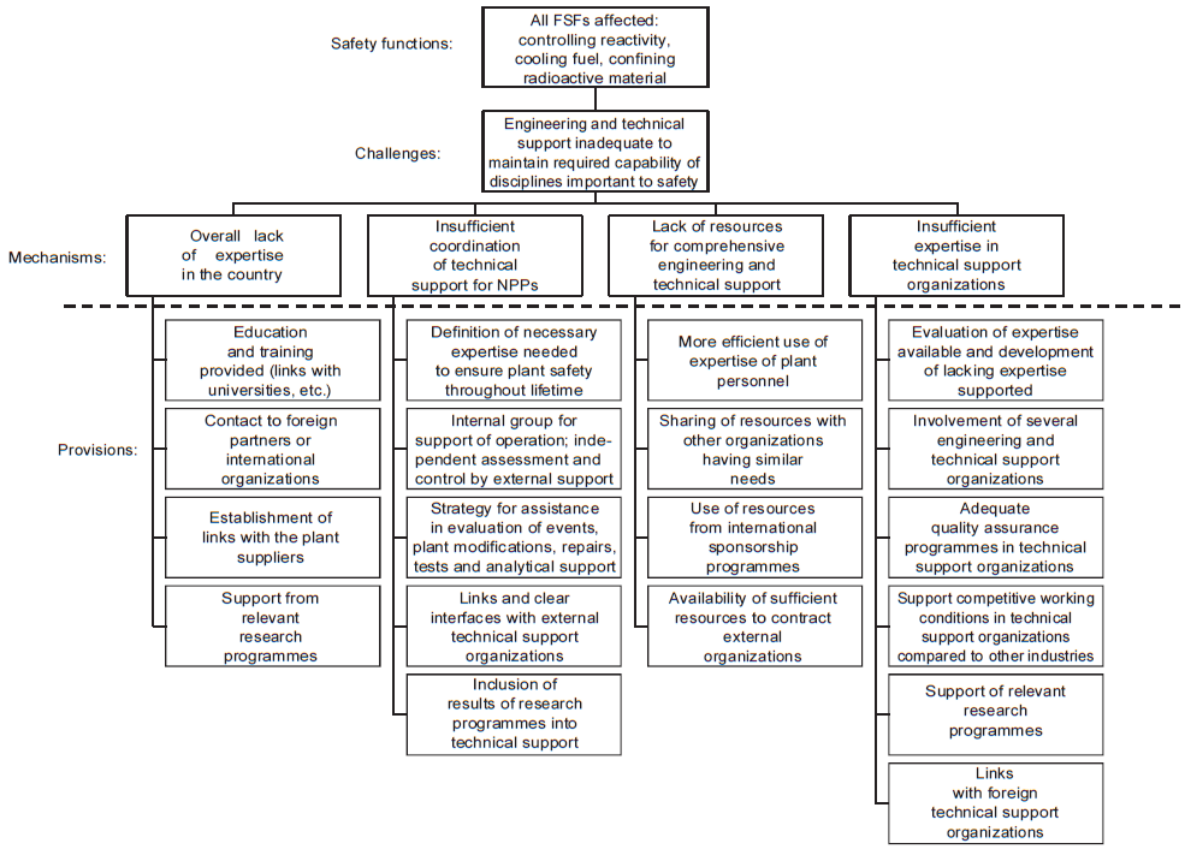


FIG. 70. Objective tree for Levels 1–4 of defence in depth. Safety principle (296): engineering and technical support of operations.

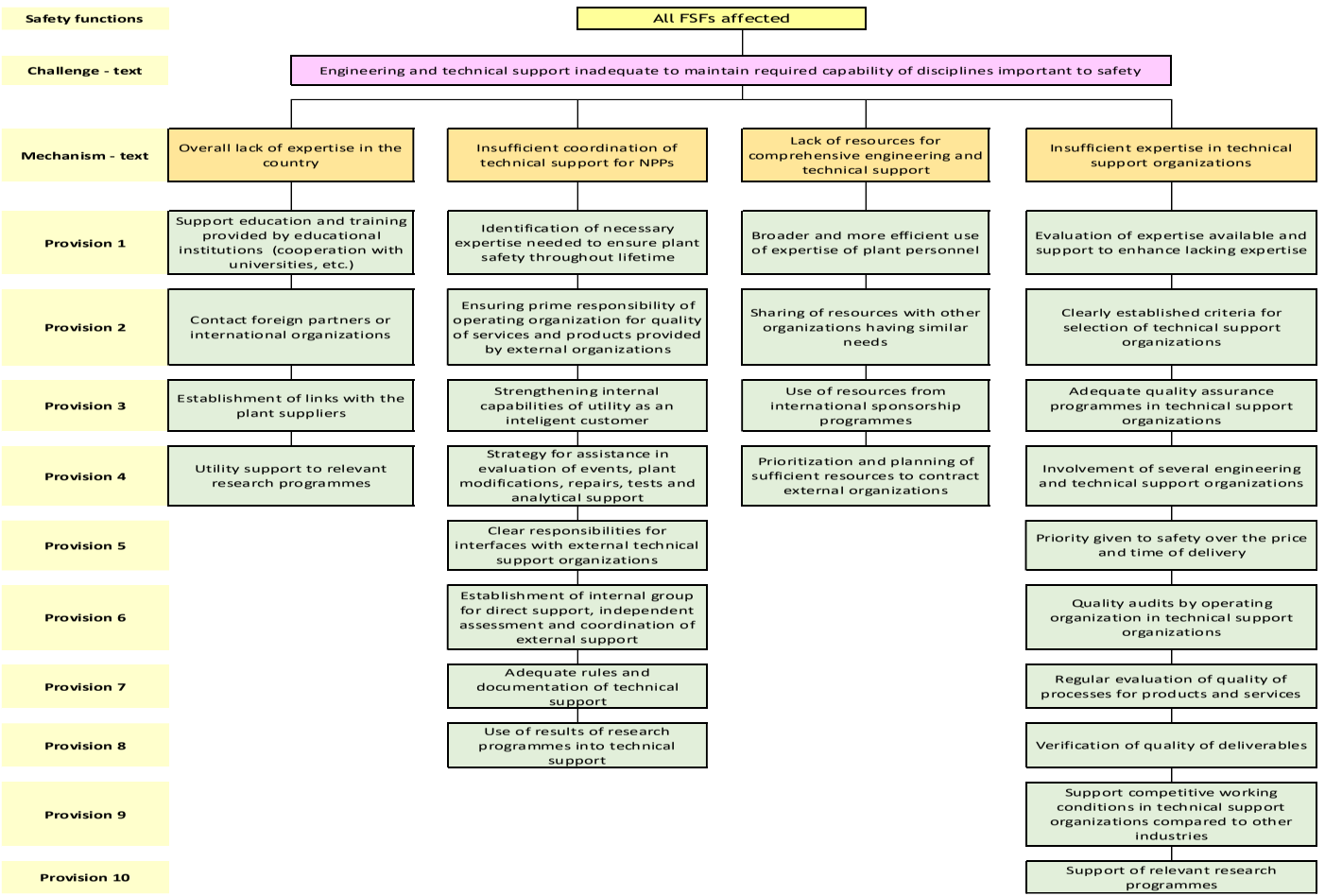


FIG. 70. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (296): engineering and technical support of operations.

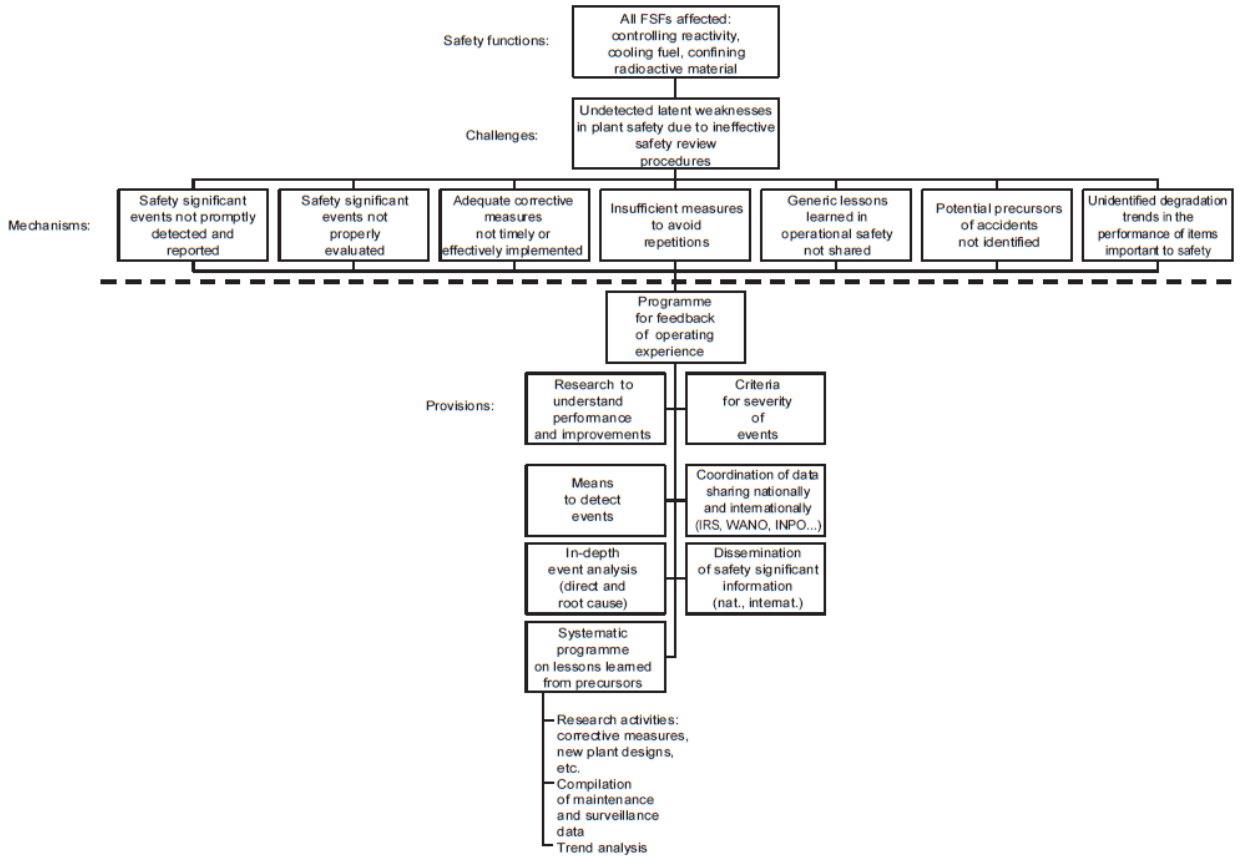


FIG. 71. Objective tree for Levels 1–4 of defence in depth. Safety principle (299): feedback of operating experience.

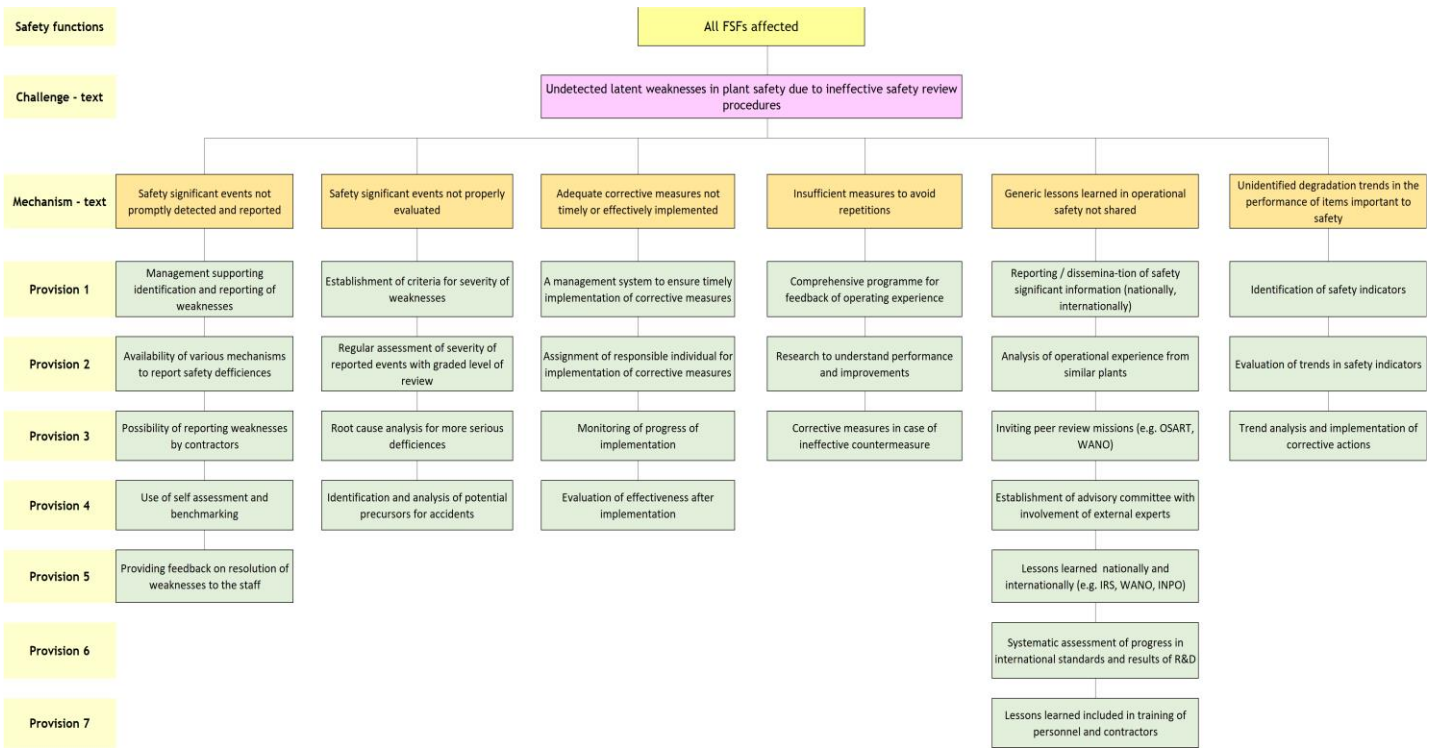


FIG. 71.Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (299): feedback of operating

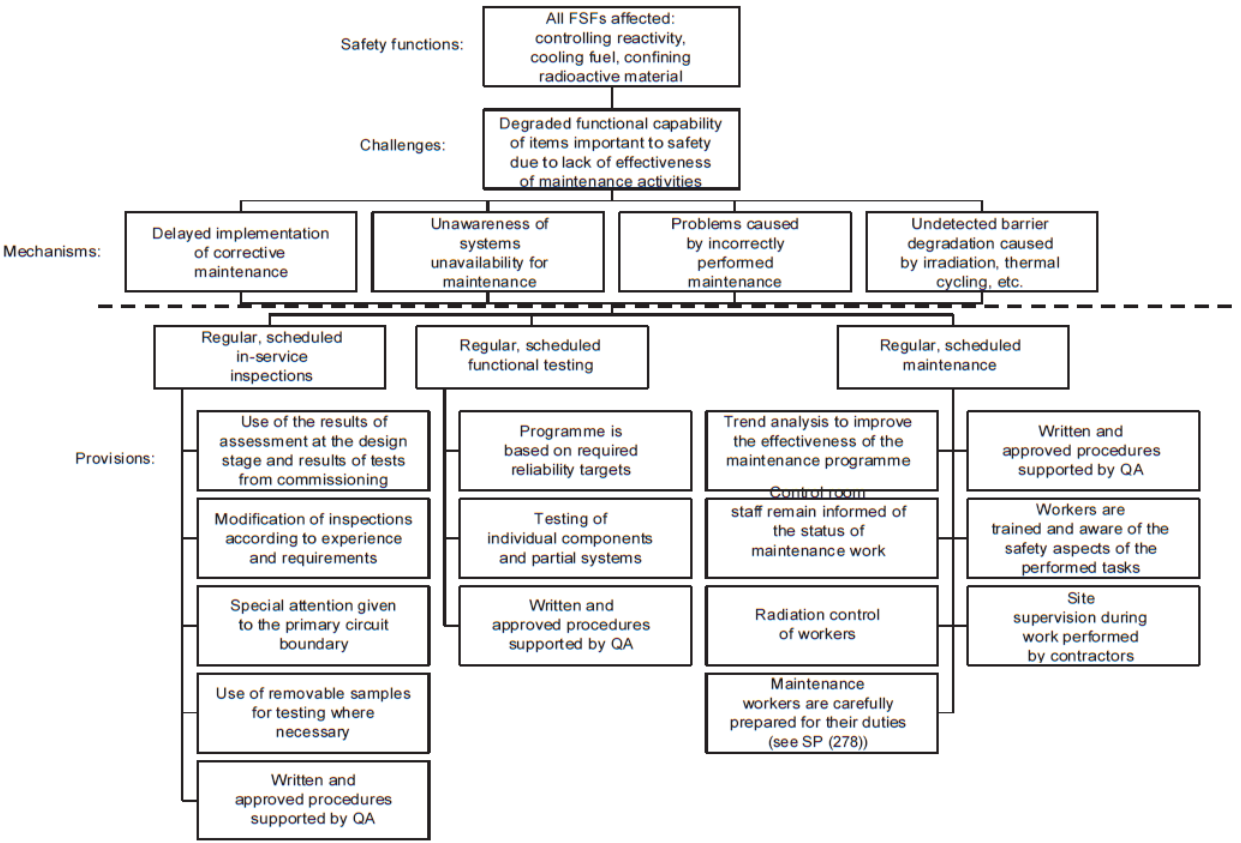


FIG. 72. Objective tree for Levels 1–4 of defence in depth. Safety principle (305): maintenance, testing and inspection.

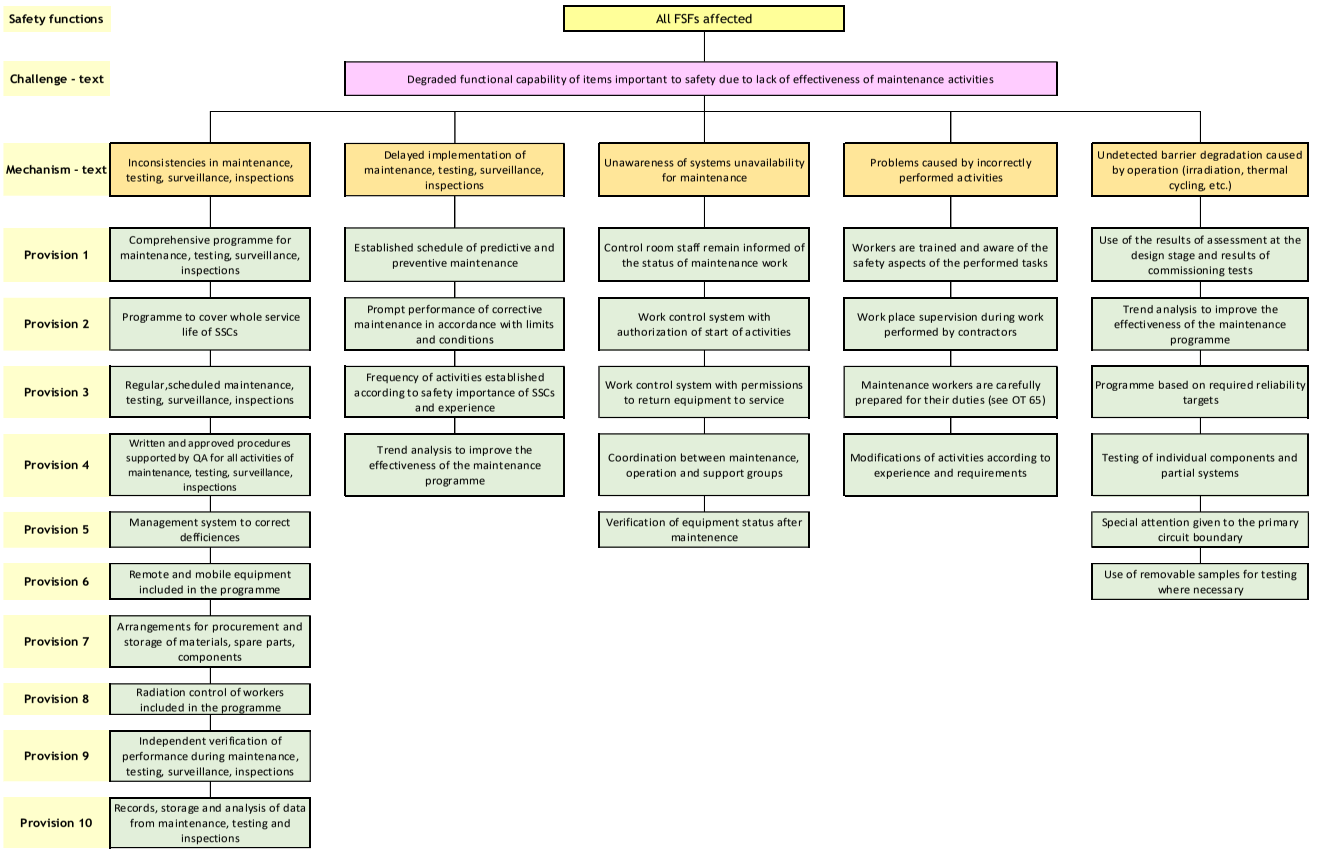


FIG. 72. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (305): maintenance, testing and inspection.

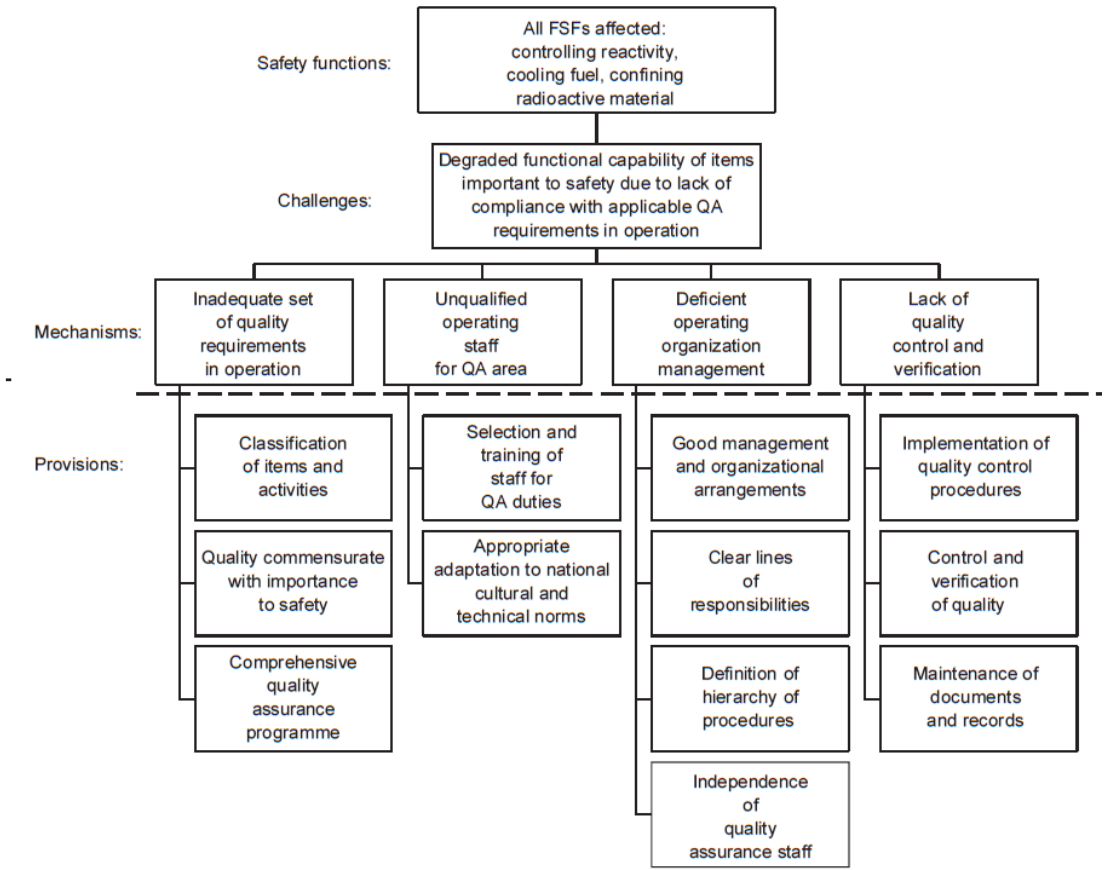


FIG. 73. Objective tree for Levels 1–4 of defence in depth. Safety principle (312): quality assurance in operation.

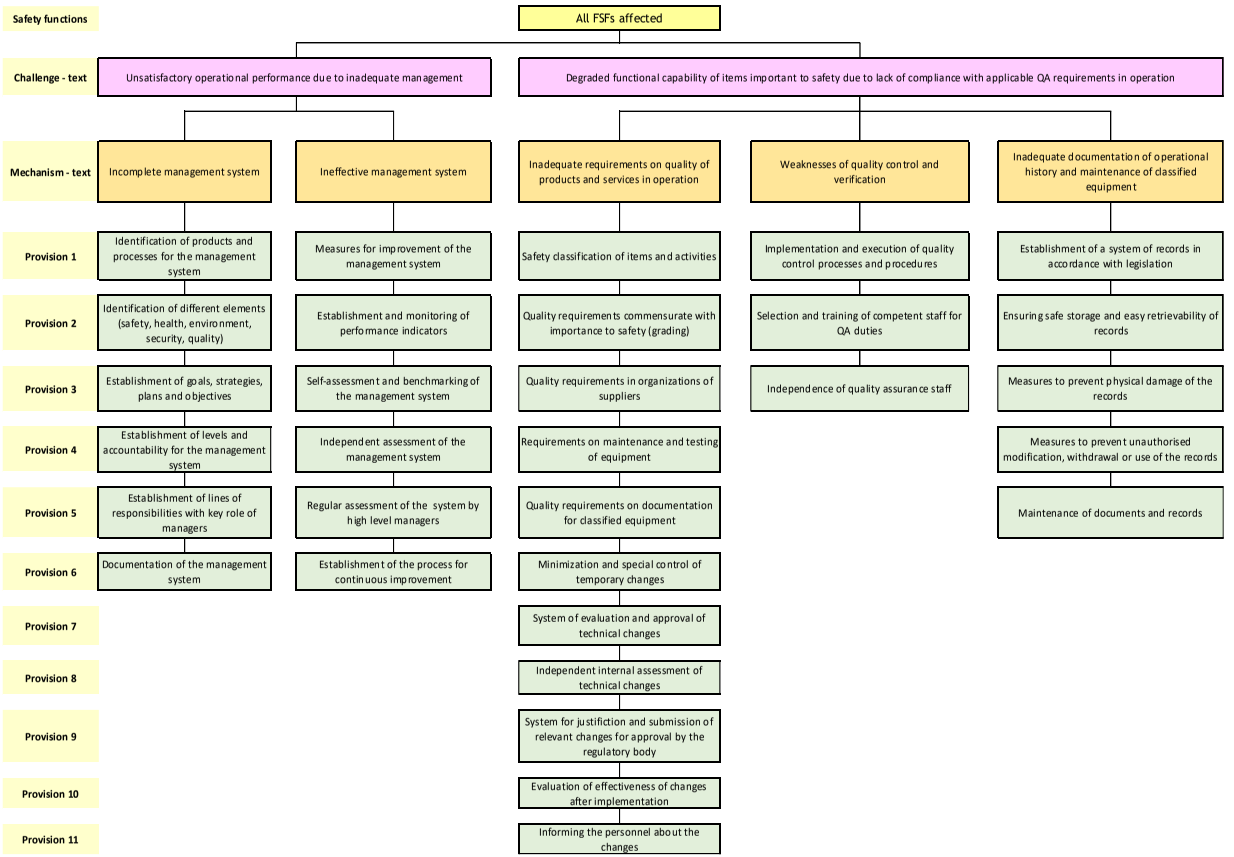


FIG. 73. Updated. Objective tree for Levels 1–4 of defence in depth. Safety principle (312): quality assurance in operation.

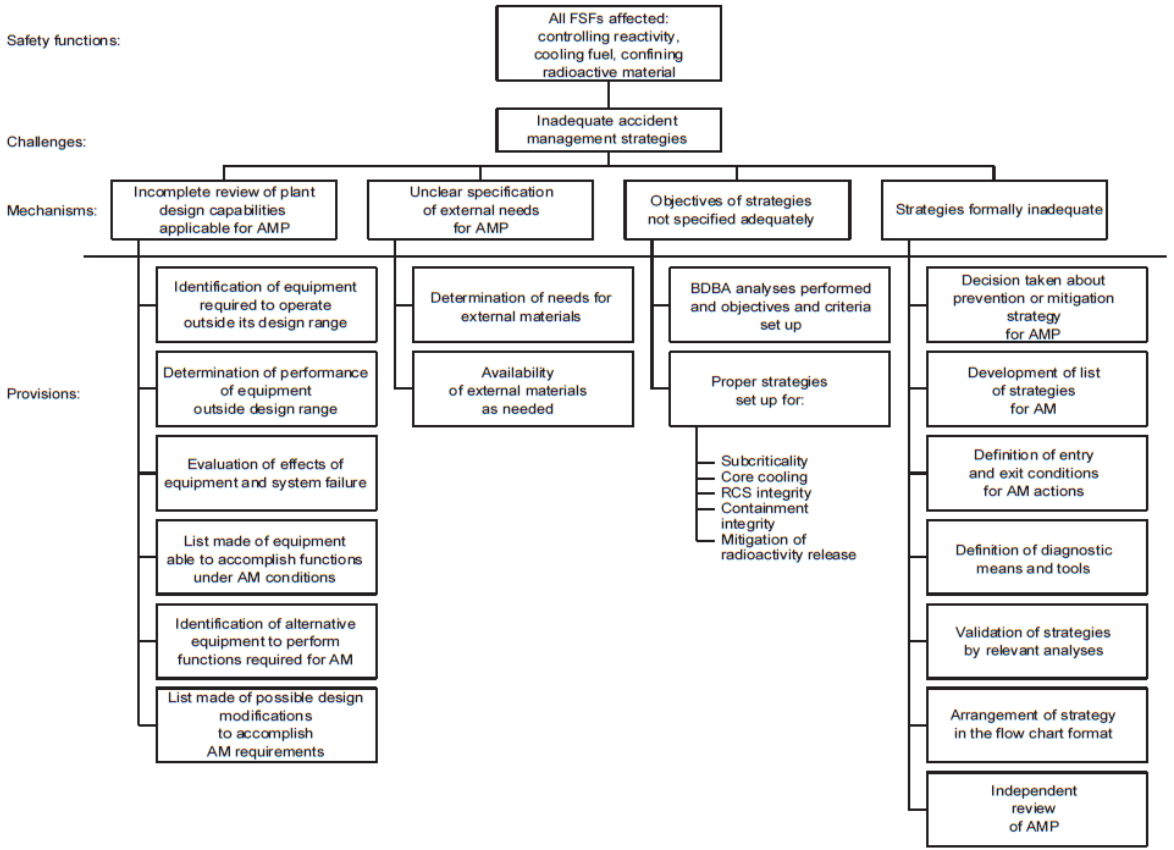


FIG. 74.Objective tree for Level 4 of defence in depth. Safety principle (318): strategy for accident

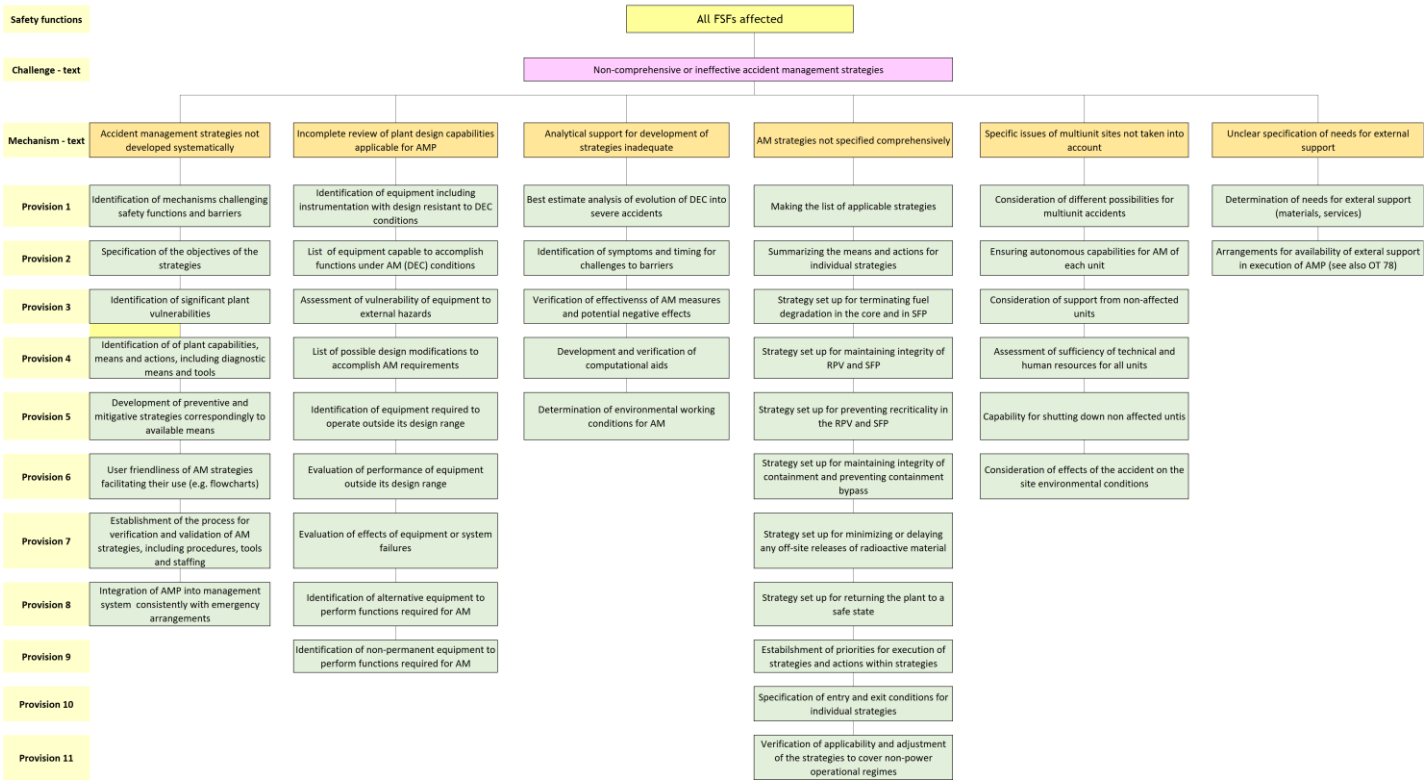
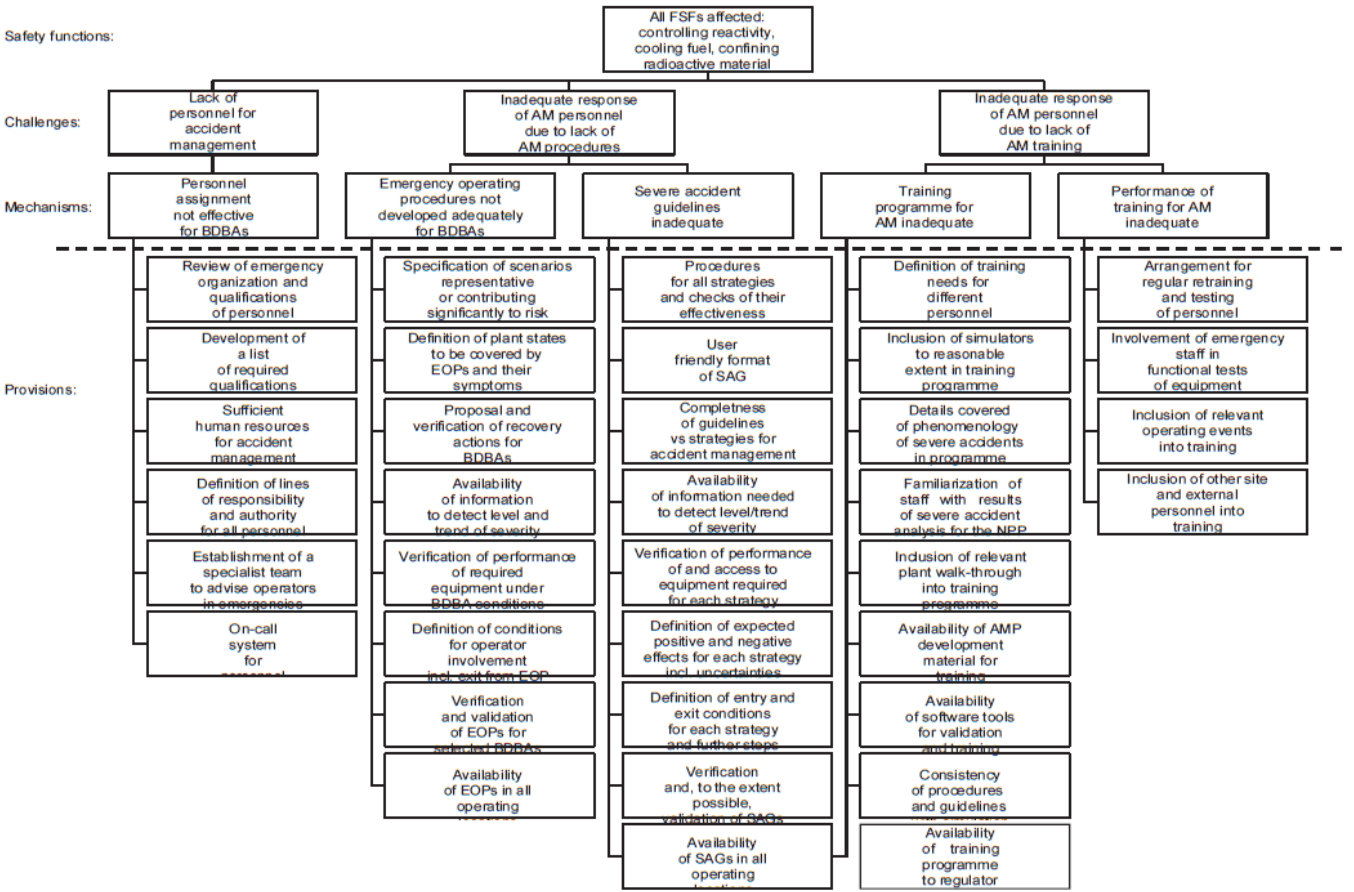


FIG. 74 Updated. Objective tree for Level 4 of defence in depth. Safety principle (318): strategy for accident



Objective tree for Level 4 of defence in depth. Safety principle (323): training and procedures for accident management.

FIG. 75.

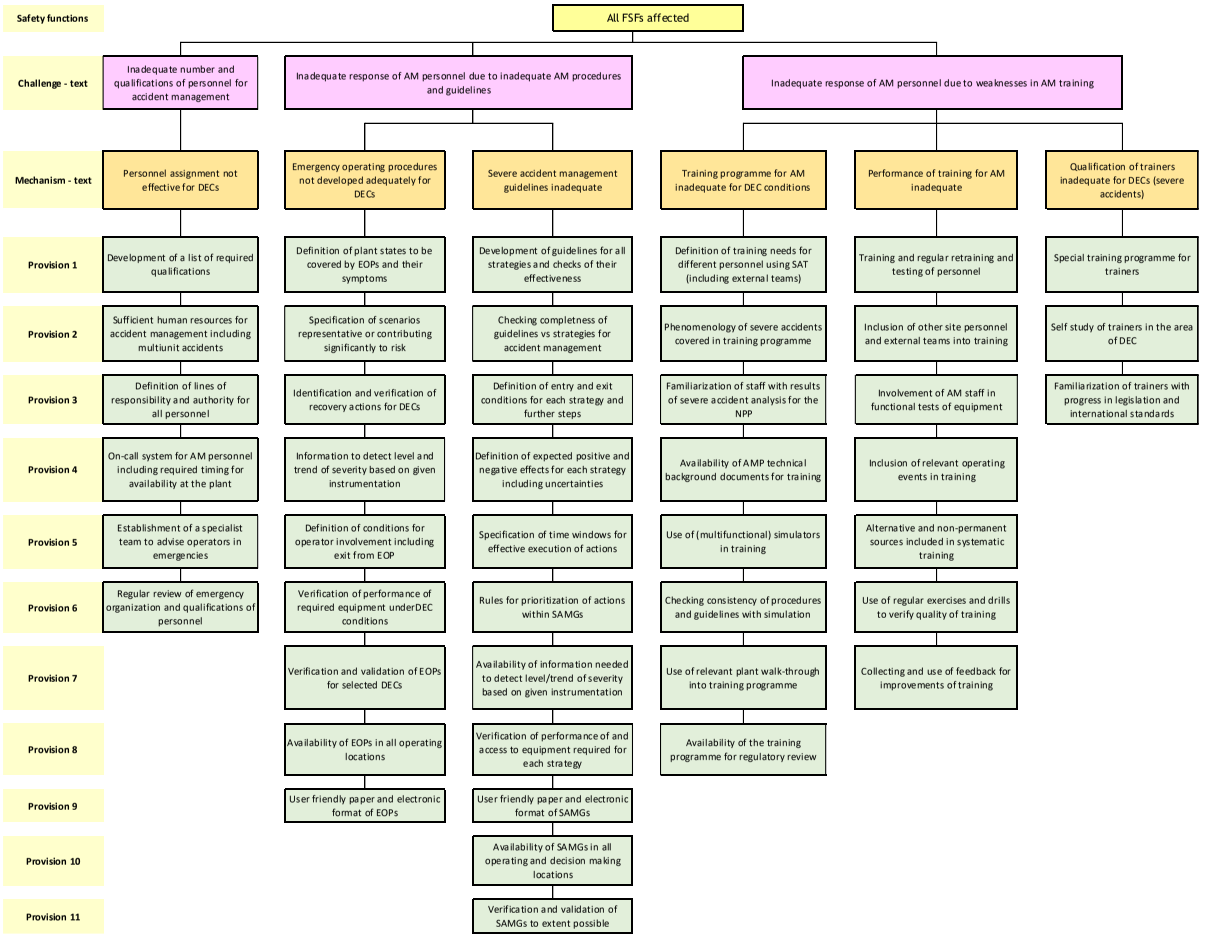


FIG. 75 Updated Objective tree for Level 4 of defence in depth. Safety principle (323): training and procedures for accident management.

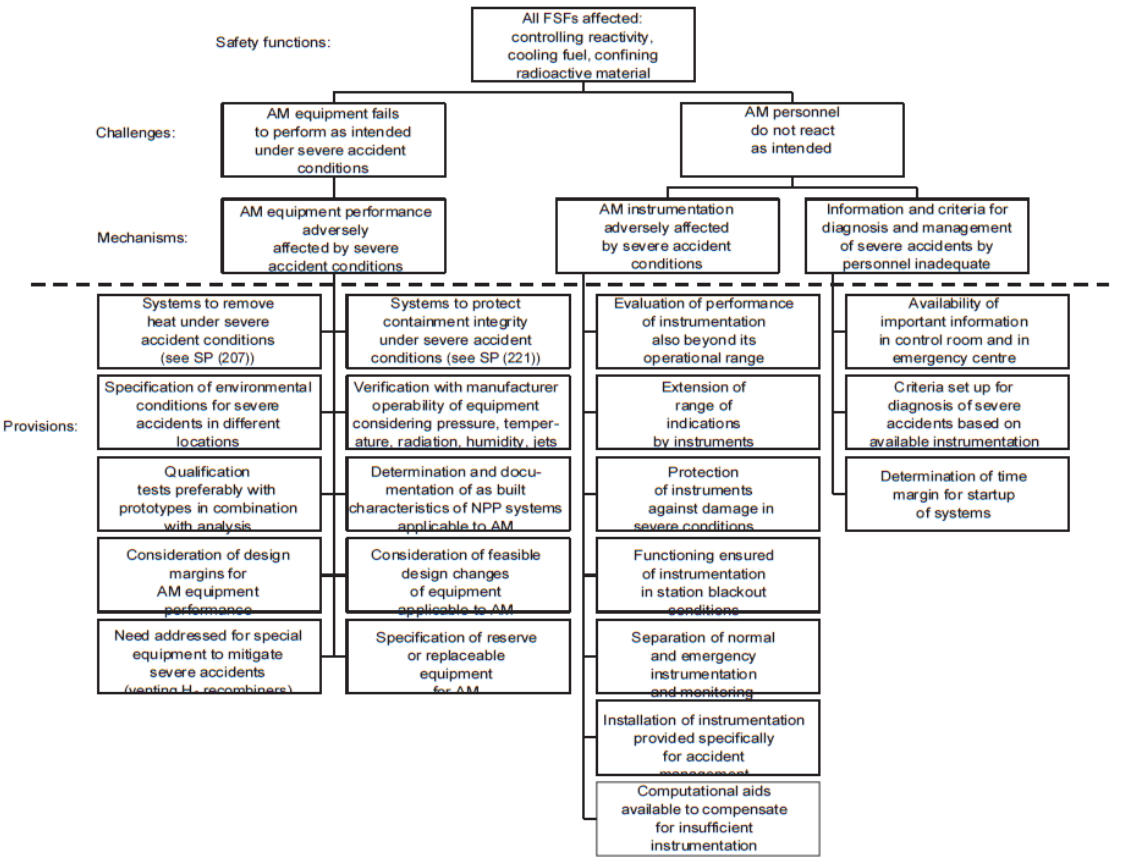


FIG. 76. Objective tree for Level 4 of defence in depth. Safety principle (326): engineered features for accident management.

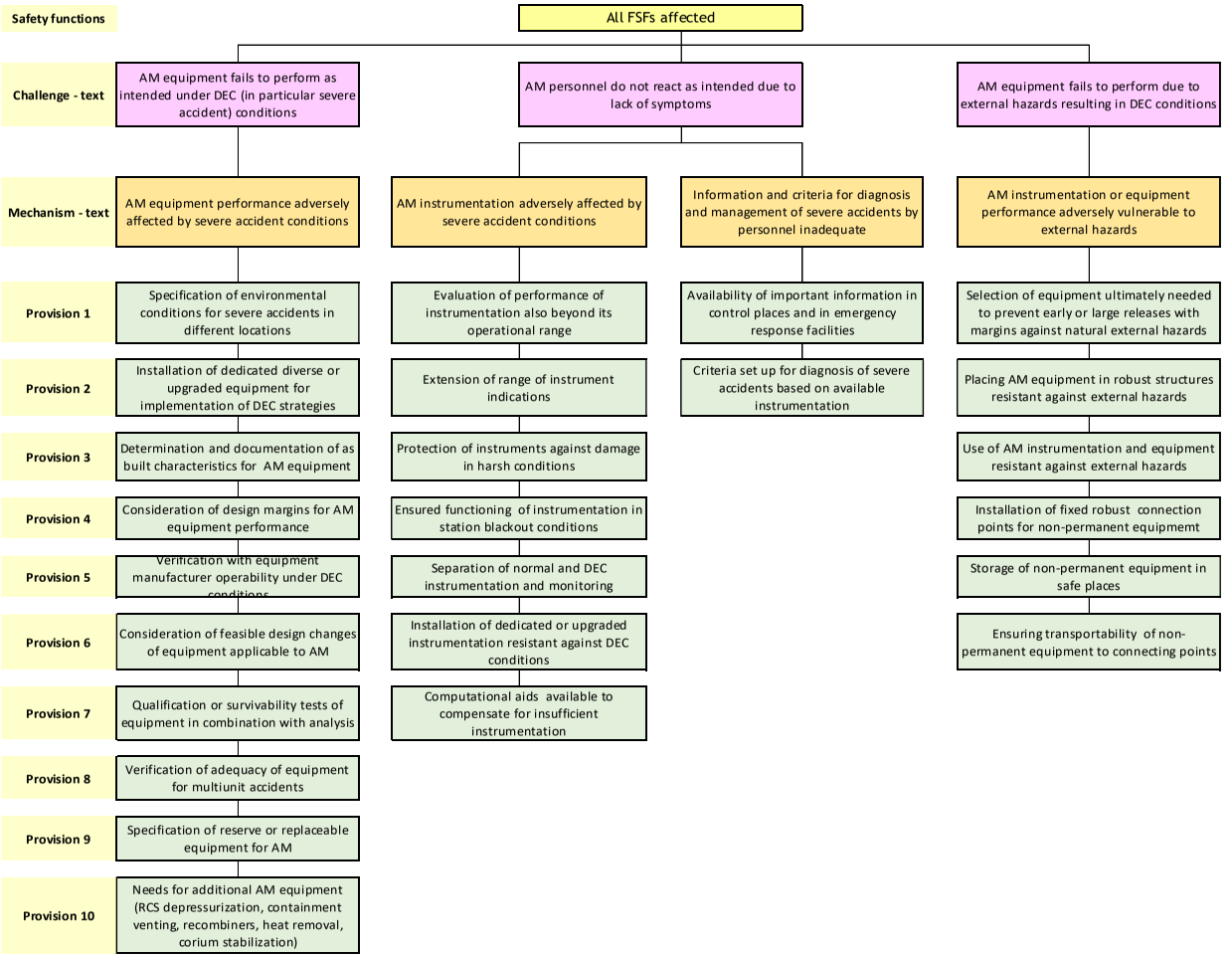


FIG. 76. Updated Objective tree for Level 4 of defence in depth. Safety principle (326): engineered features for accident management.

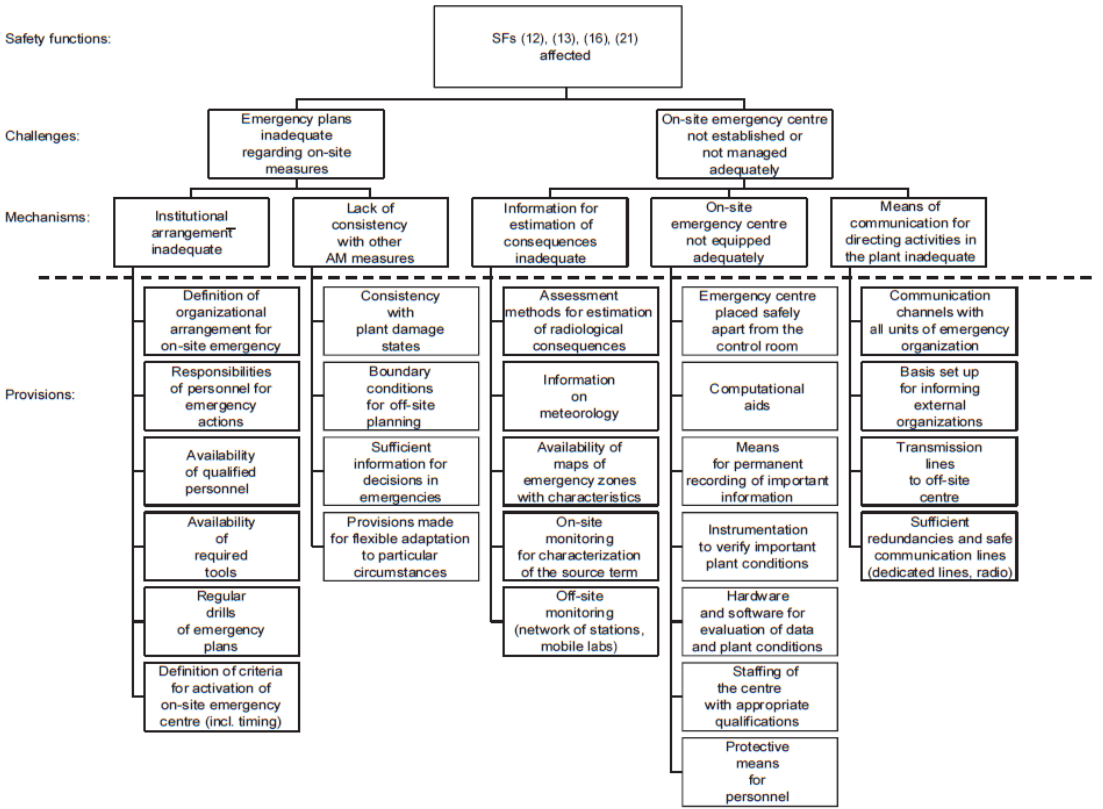


FIG. 77. Objective tree for Level 4 of defence in depth. Safety principles: emergency plans (333), emergency response facilities (336).

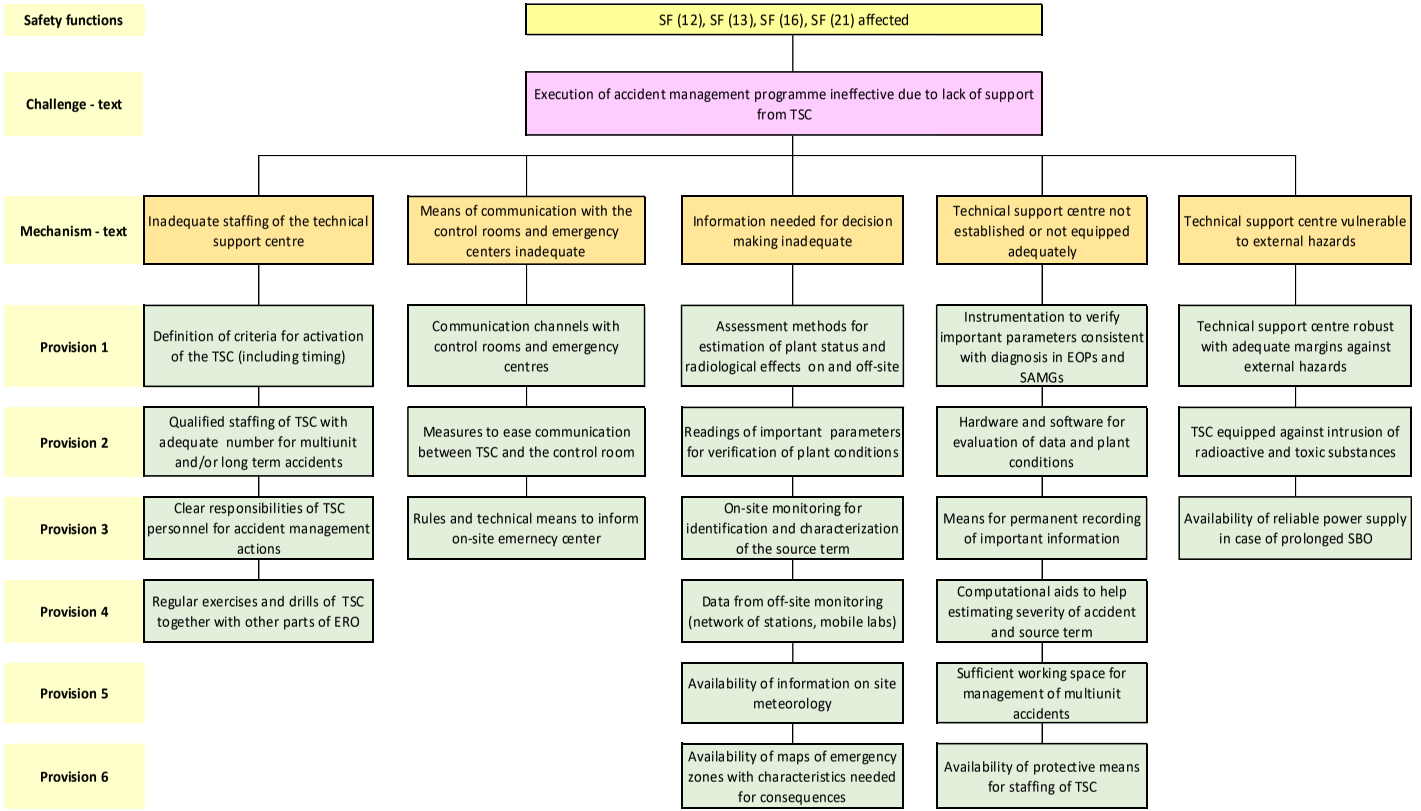


FIG. 77a Updated. Objective tree for Level 4 of defence in depth. Safety principles, emergency response facilities (336).

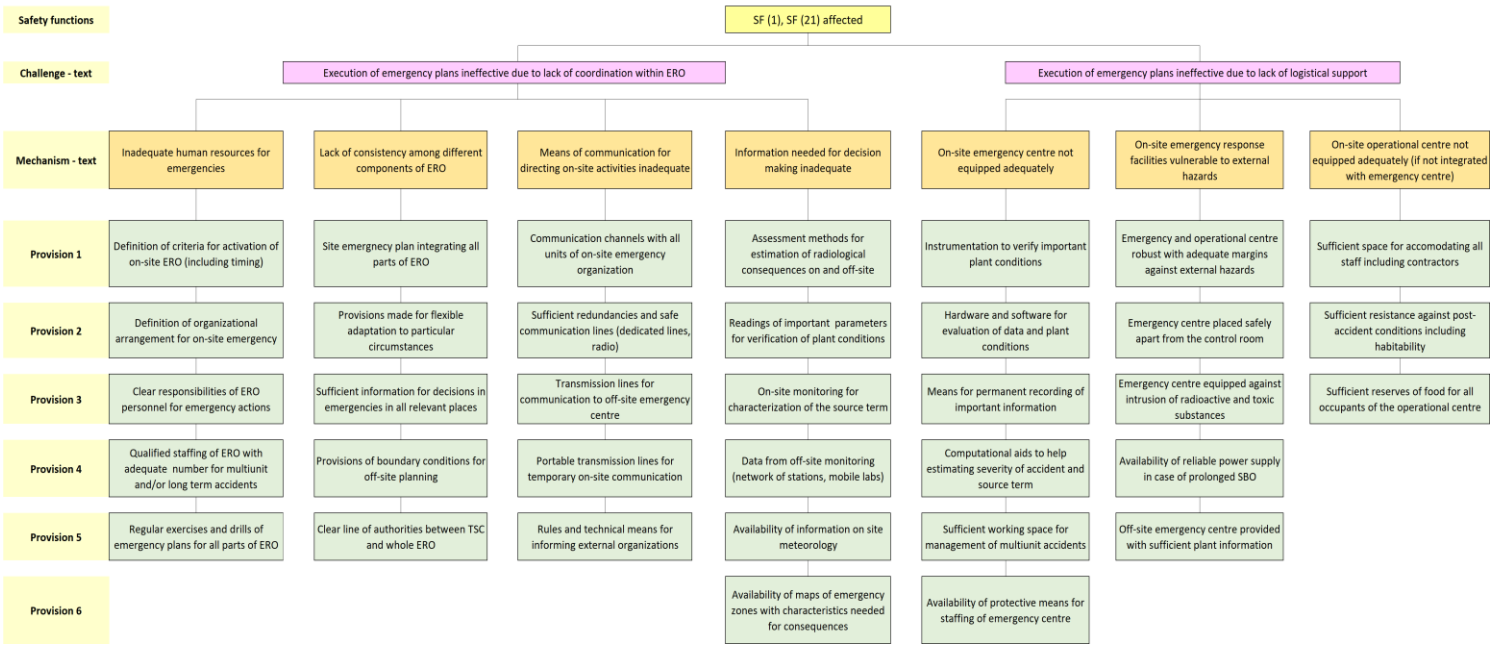


FIG. 77b Updated. Objective tree for Level 5 of defence in depth Safety principles: emergency plans (333), emergency response facilities (336).

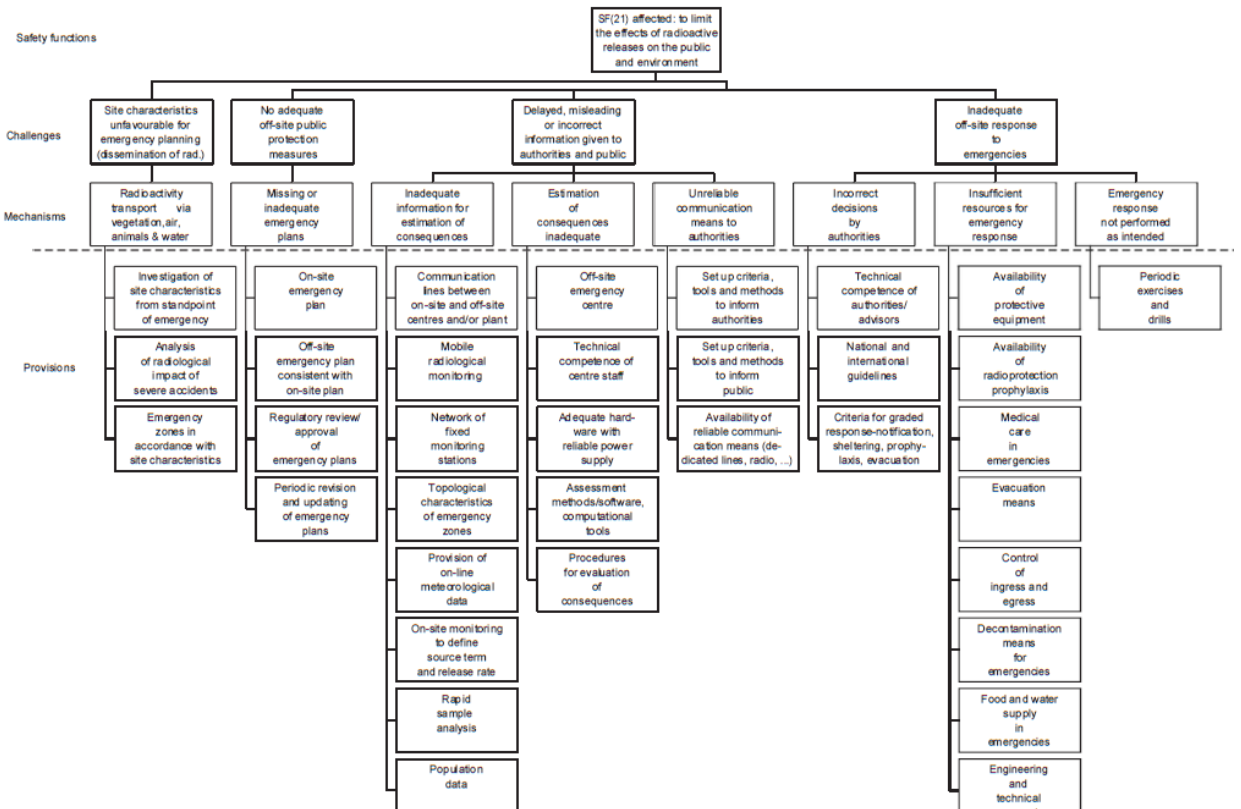


FIG. 78. Objective tree for Level 5 of defence in depth. Safety principles: radiological impact on the public and the local environment (138), feasibility of emergency plans (140), organization responsibilities and staffing (265), engineering and technical support of operations (296), emergency plans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

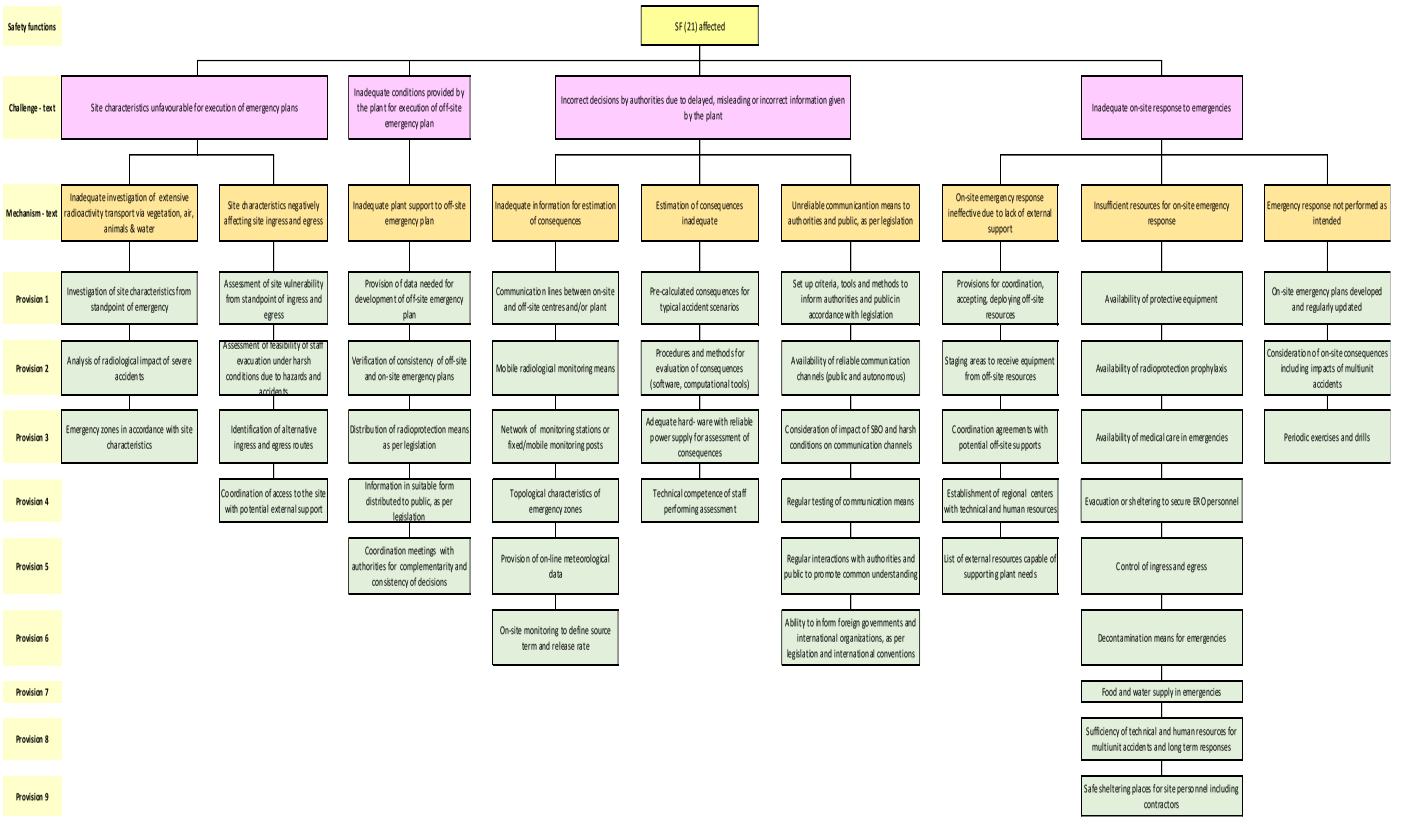


FIG. 78 Updated. Objective tree for Level 5 of defence in depth. Safety principles feasibility of emergency plans (140), emergency plans (333), assessment of accident consequences and radiological monitoring (339).

ANNEX I. SUMMARY OF KEY LESSONS LEARNED FROM THE MAIN REFERENCE DOCUMENTS USED FOR UPDATING THE METHOD

1. Modifications due to strengthening of IAEA Safety Requirements for siting

Main areas of strengthening in the IAEA Safety Requirements for siting [4]include the following items :

- The need to evaluate frequency and severity of external natural and human induced events, with consideration of potential combination of events;
- Establishing the design basis hazard level considering frequency and severity of events with associated uncertainties, considering long term historical data;
- Assessment of the feasibility of implementation of emergency plans, considering potential mutual effects among multiple nuclear and other facilities at one site;
- Periodic review of site specific hazards (every 10 years or shorter in case of significant changes in hazards) with evaluation of implications.

2. Modifications due to strengthening of IAEA Safety Requirements for design

Since Fukushima, the relevant IAEA Safety Requirements have been updated two times: once in 2012, second time in 2016 [5]. Main areas of strengthening in the updated Safety Requirements for design are as follows:

- Consideration in the plant design of all plant states up to DECs including severe accidents in the plant design envelope;
- Limitation of radiological consequences of accident conditions: no off-site measures needed for any DBAs, of-site measures limited in area and time for severe accidents, which are not practically eliminated;
- Strengthening the plant design basis by consideration of external hazards with implementation of sufficient margins;
- Practical elimination of unacceptable radiological consequences (elimination of early or large radioactive releases) to the public and the environment (elimination or minimization of site contamination) (see Annex II for description of a relevant possible approach);
- Reinforcement of the independence of defence in depth provisions, in particular between Levels 3 and 4 - dedicated safety provisions for DECs;
- Stressing the need for margins to avoid cliff edge effects;
- For items that ultimately prevent large or early releases more margins are required, also for external hazards more severe than those selected for the design basis;

- In a multiunit site, each plant unit to have its own safety systems and safety features for DECs, but considering interconnections between the units for enhancement of safety;
- Reinforced capabilities for heat transfer to the UHS; alternative heat sink or different heat transport route is required for conditions generated by beyond design basis external events;
- Strengthening design of the control room with margins against natural hazards exceeding the design basis;
- Implementation of features (design, procedures, etc.) to enable the use (e.g. hook-up) of non-permanent equipment;
- Reinforced capabilities for power supply in DECs; independent and separated alternate power sources for SBO accidents, with continuity of power for monitoring;
- Emergency response facilities on the site capable to withstand conditions generated by accidents and hazards;
- Additional measures for spent fuel pool (SFP) monitoring (temperature, water level, activity, water chemistry), cooling and maintaining inventory including use of non-permanent equipment (in order to practically eliminate severe accidents).

More detailed interpretation of the Safety Requirements on design has been provided in the IAEA TECDOC 1791 [15]. In the TECDOC plant control systems are considered differently from original consideration by INSAG at Level 1 of defence. The TECDOC also commented continued discussions (not yet finalized in IAEA, but introduced by WENRA) about subdivision of Level 3 of defence into two sub-levels: one sub-level would consist of DBAs, other sub-level would consist of DECs without significant fuel degradation.

3. Modifications due to strengthening of IAEA Safety Requirements for operation

Main areas of strengthening in the updated Safety Requirements for operation [6] are as follows:

- PSR to consider national and international experience, national and international standards and to cover site related aspects;
- Implementing corrective actions and reasonably practicable modifications to reduce likelihood and potential consequences of accidents;
- Strengthening means of communication, availability of information in emergency response facilities and locations with regular testing, validation and training on emergency preparedness;
- Strengthening accident management, degraded regional infrastructure and adverse working conditions, ensuring safe location and maintenance of non-permanent equipment;

- Periodical review and revisions of AMP;
- For multiunit sites considering concurrent accidents affecting all units with verification of availability of experienced personnel, equipment, supplies and external support;
- Considering contingency measures such as an alternative supply of cooling water and an alternative supply of electrical power to mitigate the consequences of accidents;
- Ensuring safe and accessible storage of temporary equipment;
- Appropriate competences, systems and technical support, with adequate validation, testing and exercises of accident management, including long-term actions;
- Feedback from operating experience to include emergency responses and lessons learned from other industries;
- Establishing maintenance programmes, training and exercises for no-permanent equipment.

4. Modifications due to post-Fukushima updating of WENRA reference levels for existing reactors

WENRA Reference Levels for existing NPPs were established in 2006, updated in 2007 and 2008 and finaly issued in 2008 [16]. All reference levels were subdivided into 5 safety areas, each for them further subdivided into issues, each of them consisting from 7 up to 44 recommendations, called reference levels (RLs).

During the period 2012 – 2014, WENRA updated the RLs taking into account all lessons learned from the Fukushima accident [9]. For about half of the issues, there have been either no or only very limited changes. The issues where there have been the most significant changes are the following:

- A - Safety Policy;
- C - Management System; RLs relevant to safety culture have been introduced;
- E - Design Basis Envelope for Existing Reactors;
- F - Design Extension of Existing Reactors; DECs have in particular been introduced for consistency with IAEA SSR-2/1 safety standard, as well as the need for independent and diverse heat removal means, one being effective for natural hazards exceeding the design basis;
- LM - Emergency Operating Procedures and Severe Accident Management Guidelines;
- N - Contents and Updating of Safety Analysis Report;
- O - Probabilistic Safety Analysis;
- P - Periodic Safety Review;

- R - On-site Emergency Preparedness.

In addition a new issue (Issue T), dedicated to natural hazards, has been established. This issue has a strong interface with issues E and F. The table 1 shows the change in number of RLs for each issue. The issues significantly influenced by the updating are marked in grey in table 1.

The key changes introduced in the RLs include broader consideration of natural hazards (new issue T), safety culture, safety of SFPs, sites with multiple reactors, conditions at the site after an accident, need for independent and diverse heat removal means and in general consideration of conditions more severe than the ones considered in the design basis of the plant.

The most significant changes were made in the issue F - Design Extension of Existing Reactors, which was practically completely rewritten.

The main differences for all indicated issues will be characterized in more detail in the following text. Only new or substantially changed reference levels will be summarized in the further text.

Table 1. Overview of the reference levels for existing NPPs with the changes between 2008 and 2014

Safety areas		Number of RLs 2008	Number RLs 2014
Safety Management	A – Safety Policy	8	9
	B – Operating organisation	15	15
	C – Management system	23	26
	D – Training and authorisation of NPP staff	15	15
Design	E - Design basis envelope for existing reactors	44	46
	F – Design extension of existing reactors	12	25
	G – Safety classification of structures, systems and components	7	7
	T – Natural hazards	Not included	19
Operation	H – Operational limits and conditions	19	19
	I – Ageing management	8	8
	J – System for investigation of events and operational experience feedback	16	16
	K – Maintenance, in-service inspection and functional tests	20	20
	LM – Emergency operating procedures and severe accident management guidelines	14	20
Safety verification	N – Contents and updating of safety analysis report	16	17

	O – Probabilistic safety analysis	16	16
	P – Periodic safety review	9	9
	Q – Plant modifications	15	15
Emergency preparedness	R – On-site emergency preparedness	18	20
	S – Protection against internal fire	20	20
Total		295	342

A - Safety Policy

- The safety policy shall require continuous improvement of nuclear safety using any new information, taking into account operating experience, safety research, advances in science and technology, with timely implementation of the reasonably practicable safety improvements;

C - Management System

Three new RLs have been introduced to underline the importance of compliance with the safety culture principles, in particular

- Role of managers at all levels to demonstrate, support and promote attitudes and behaviours of safety culture, discouraging complacency, encouraging reporting of issues, questioning and learning attitude;
- Implementation of all necessary attributes of safety culture and means supporting safety culture into the management system;
- Ensuring that all suppliers and contractors behave in accordance with principles of safety culture;

E - Design Basis Envelope for Existing Reactors

- Heat removal from the SFP in addition from the reactor core was specifically added to the SF;
- The list of design basis events shall take account of relevant experience and analysis also from other plants;
- More stringent requirements on justified method of safety analysis, which shall be auditable and reproducible and shall give the evidence that adequate margins are included in the design basis;
- For sites with multiple units ensuring appropriate independence between the units;
- Maintaining long-term subcriticality in the reactor and in fuel storages during and after normal operation, AOO and DBA;
- Specifically requiring at least one isolation valve even on any line penetrating containment not connected to the RCS boundary nor to the containment atmosphere;
- Requirement on availability of adequate instrumentation not only for the core, RCS and containment, but also for the SFP;

- Similarly, the need to control from the emergency control room (ECR) or equivalent control location the heat removal and monitoring the parameters associated with the spent fuel storages;
- Appendix containing the list of specific initiating events to be used for benchmarking has been removed from the RLs;

F - Design Extension of Existing Reactors

- Instead of beyond design basis accident, the term DEC is used, further subdivided into two categories of DEC:
    - DEC A for which prevention of severe fuel damage in the core or in the spent fuel storage can be achieved;
    - DEC B with postulated severe fuel damage;

  DEC shall be analysed with the objective to enhance plant capability to cope with the accident more severe than DBAs and minimise radioactive releases by means of reasonable practicable provisions;
- Additional efforts shall be implemented for spent fuel storage to ensure that a severe accident in such storage becomes extremely unlikely to occur with a high degree of confidence;
- For selection of DEC A events and combinations of events shall be considered, which cannot be considered with a high degree of confidence to be extremely unlikely to occur and which may lead to severe fuel damage in the core or in the spent fuel storage, covering:
    - Events occurring during the defined operational states of the plant;
    - Events resulting from internal or external hazards;
    - Common cause failures;
- All reactors and spent fuel storages on the site have to be taken into account, considering events potentially affecting all units on the site, potential interactions between units as well as interactions with other sites in the vicinity;
- Severe accidents (DEC B) shall be postulated for fuel in the core and, if not extremely unlikely to occur with a high degree of confidence, for spent fuel in storage, and by the analysis to identify reasonably practicable provisions to mitigate their consequences;
- The safety analysis of DEC, which should not be unduly conservative, shall adequately model relevant phenomena, shall consider equipment capabilities for foreseen accident management actions, shall demonstrate, where applicable, sufficient margins to avoid "cliff-edge effects" that would for DEC-A lead to severe fuel damage and for DEC-B to a large or early radioactive release, shall evaluate potential on-site and off-site radiological consequences resulting from the DEC (given successful accident management

measures) and shall define an end state and associated mission times for systems, structures and components;

- For DEC-A all main SFs shall be maintained, for DEC-B the capability to confine the radioactive material shall be maintained, which includes heat removal from the damaged fuel;
- SSCs including mobile equipment and their connecting points, shall have the capacity, capability and be adequately qualified to perform their relevant functions for the appropriate period of time;
- For mobile equipment to be used in accident management the accessible permanent connecting points shall be available; the mobile equipment, connecting points and lines shall be maintained, inspected and tested;
- Common resources of personnel, equipment shall be sufficient for each unit at all times and support between units shall not be detrimental to the safety of any unit;
- The NPP site shall be autonomous regarding supplies supporting SFs for a sufficient period of time;
- Sub-criticality of the reactor core and fuel storage shall be ensured in the long term at any time;
- There shall be sufficient independent and diverse means including necessary power supplies available to remove the residual heat from the core and the spent fuel, with at least one be effective after events involving external hazards more severe than design basis events;
- For the containment the requirements remained the same, but specific requirements regarding limitation of radioactive releases have been added, requiring that radioactive releases shall be limited as far as reasonably practicable to allow sufficient time for protective actions and avoid contamination of large areas in the long term;
- DEC instrumentation needed for accident management should be not only functional but also qualified for the conditions and should cover also spent fuel storage;
- There shall be an operational and habitable control room (or another suitably equipped location) available during DEC in order to manage such situations;
- Adequate power supplies during DEC shall be ensured considering the necessary actions and the timeframes defined in the DEC analysis, taking into account external hazards;
- Batteries shall have adequate capacity to provide the necessary DC power until re-charging can be established or other means are in place;
- The DECs shall be regularly reviewed, when relevant new safety information is available;

- Appendix containing the list of specific DECs to be used for benchmarking has been removed from the RLs;

LM - Emergency Operating Procedures (EOPs) and Severe Accident Management Guidelines (SAMGs)

- EOPs are required to prevent severe fuel damage not only in the reactor core, but also in the spent fuel storage;
- Procedures and guidelines shall be suitable to manage accident conditions that simultaneously affect the reactor and spent fuel storages, and shall take potential interactions between reactor and spent fuel storages into account;
- Possibilities for one unit supporting another unit on the site without compromising its safety shall be covered by the set of procedures and guidelines;
- The set of procedures and guidelines shall be such that they are able to be implemented even if all nuclear installations on a site are under accident conditions, taking into account the dependencies between the systems and common resources;
- EOPs for DBAs shall rely on adequately qualified equipment and instrumentation;
- EOPs for DEC and SAMGs shall primarily rely on adequately qualified equipment;
- The set of procedures and guidelines shall consider the anticipated on-site conditions, including radiological conditions, associated with the given accident conditions and the initiating event or hazard that might have caused it;
- Not only control room staff, but all licensee emergency response staff shall be regularly trained and exercised, for situations and conditions covered by the set of procedures and guidelines;
- Plans and exercise for interventions shall include those which may rely on mobile or off-site equipment; the potential unavailability of instruments, lighting and power and the use of protective equipment shall be considered;

N - Contents and Updating of Safety Analysis Report (SAR)

- The SAR shall describe the safety analyses not only AOO and DBAs, but also DECs against safety criteria and radiological release limits, with description of safety margins;
- The SAR shall consider the site as a whole, to take into account hazards which may challenge all installations within a short period of time and which arise from harmful interactions between installations;

O - Probabilistic Safety Analysis

- The PSA Level 1 and 2 shall be developed not only for the core, but also for the spent fuel storage, with adequate attention paid to external hazards;

P - Periodic Safety Review (PSR)

- More attention to be paid in PSR to operating experience, relevant research findings, and the current state of technology;
- This assessment shall highlight any issues that might limit the future safe operation of the plant and explain how they will be managed;
- In PSR, more attention to be paid to specific aspects, in particular to
    - Equipment qualification;
    - Ageing;
    - Deterministic safety analysis;
    - Probabilistic safety assessment;
    - Hazard analysis;
    - Safety performance;
    - Use of experience from other plants and research findings;
    - The management system and safety culture;
    - Procedures;
    - Human factors;
- The requirement to evaluate the safety significance of all findings and to consider the global assessment of all findings (positive and negative) and their cumulative effect on safety, with identification of safety improvements which are reasonably practicable;

R - On-site Emergency Preparedness

- The site emergency plan to address long-lasting situations and to clarify how site (and if applicable corporate) resources (human and material) common to several installations are used;
- Arrangements shall be established to ensure that sufficiently qualified personnel can staff appropriate emergency positions in long-lasting situations;
- The licensee emergency response shall be functional in cases where infrastructures at the site and around the site are severely disrupted;
- Arrangements to support on-site actions shall be in place with considerations for large-scale destruction of infrastructure in the vicinity of the site due to external hazards;
- Instruments, tools, equipment, documentation, and communication systems for use in emergencies (including necessary mobile equipment and consumables such as fuel, lubrication oil etc.), whether located on-site or off-site, shall be stored, maintained, tested and inspected sufficiently frequently so that they will be available and operational during DBA and DEC, with the

access to these storage locations possible even in case of extensive infrastructure damage;

- Arrangements to identify the knowledge, skills, and abilities needed to performed the assigned response functions as well as training shall include not only operating organization staff but also, if necessary, contractors;
- For sites with multiple nuclear installations, some exercises shall address situations affecting multiple facilities on the site;
- Exercises shall also include the use and connection of mobile equipment, if any;

T – Natural Hazards

- Natural hazards shall be considered an integral part of the safety demonstration, minimizing the threats (including threats on spent fuel storage) as far as reasonably practicable;
- All site specific natural hazards shall be identified with appropriate justification; the hazards shall include geological hazards, seismotectonic hazards, meteorological hazards, hydrological hazards, biological phenomena, forest fire as well as any mutually related hazards (e.g. earthquake and tsunami);
- The screening process of natural hazards shall be based on conservative assumptions; the hazards can be screened out on the basis of being incapable of posing a physical threat or being extremely unlikely with a high degree of confidence;
- Hazard assessments shall be performed using deterministic and, as far as practicable, probabilistic methods taking into account the current state of science and technology, including a relationship between the hazards severity (e.g. magnitude and duration) and exceedance frequency, where practicable;
- The following shall apply to hazard assessments:
    - The hazard assessment shall be based on all relevant site and regional data, with particular attention to include events beyond recorded and historical data;
    - Special consideration shall be given to hazards whose severity changes during the expected lifetime of the plant;
    - The methods used shall be justified and their uncertainties evaluated;
- For determination of design basis events a common target value of frequency, not higher than 10^{-4} per annum, shall be used for each design basis event;
- For the specific case of seismic loading, as a minimum, a horizontal peak ground acceleration value of 0.1g (where ‘g’ is the acceleration due to gravity) shall be applied;

- The design basis events shall be compared to relevant historical data to verify that historical extreme events are enveloped by the design basis with a sufficient margin;
- Design basis parameters shall be defined for each design basis event on a conservative basis;
- Protection shall be provided for all design basis events by means of suitable protection measures conservatively ensuring sufficient reliability of the fundamental safety functions with due consideration of any direct and credible indirect effects;
- The protection concept shall:
    - apply reasonable conservatism providing safety margins in the design;
    - rely primarily on passive measures as far as reasonable practicable;
    - ensure that measures to cope with a DBA remain effective during and following a design basis event;
    - take into account the predictability and development of the event over time;
    - ensure that procedures and means are available to verify the plant condition during and following design basis events;
    - consider that events could simultaneously challenge several redundant or diverse trains of a safety system, multiple SSCs or several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures;
    - ensure that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;
    - not adversely affect the protection against other design basis events (not originating from natural hazards);
- For design basis events, SSCs identified as part of the protection concept with respect to natural hazards shall be considered as important to safety;
- Monitoring and alert processes shall be available to support the protection concept, with thresholds (intervention values) defined to facilitate the timely initiation of protection measures;
- During long-lasting natural events, arrangements for the replacement of personnel and supplies shall be available;
- Events that are more severe than the design basis events shall be identified and justified; further detailed analysis of an event is not necessary, if its occurrence can be considered with a high degree of confidence to be extremely unlikely;

- When assessing the effects of natural hazards more severe than design basis events and identifying reasonably practicable improvements, analysis shall, as far as practicable, include:
    - demonstration of sufficient margins to avoid "cliff-edge effects" that would result in loss of a FSF;
    - identification and assessment of the most resilient means for ensuring the FSFs;
    - consideration that events could simultaneously challenge several redundant or diverse trains of a safety system, multiple SSCs or several units at multi-unit sites, site and regional infrastructure, external supplies and other countermeasures;
    - demonstration that sufficient resources remain available at multi-unit sites considering the use of common equipment or services;
    - on-site verification (typically by walk-down methods).

5. Modifications due to OECD/NEA lessons learned from Fukushima accident

The OECD/ NEA document No. 7248 published in 2016 [12] summarized lessons learnt from the Fukushima Daiichi accident on implementation of defence in depth at NPPs. The document reconfirmed that the use of the defence in depth concept remains valid after the Fukushima Daiichi accident and that lessons learnt from the accident and its impact on the use of defence in depth has reinforced its fundamental importance in ensuring adequate safety. Although the document is mainly of regulatory nature, it provides useful guidance also for operating organizations. Design principles available to promote defence in depth mentioned in the document include: redundancy, diversity, segregation, physical separation, train/channel independence, single-point failure protection and, as far as practical, independence between levels. It is essential to reflect defence in depth in developing the safety classification of systems and components. Large part of the document is devoted to strengthening of Level 5 of defence in depth – emergency arrangements and post-accident management.

In summary, the document stressed out the importance of the following aspects of the defence in depth implementation:

1. Reinforcing the need for independent effectiveness among the safety provisions for the various defence in depth levels (all five levels), to the extent practical, by means of:
    - Justification of the independent effectiveness of the design and operational provisions for each level;
    - The adequacy of the achieved independence demonstrated using probabilistic analyses;
    - Adequate application of functional isolation, the diversity principle and physical separation of the SSCs depending on the threats;

- Ensuring independence between the levels as far as is practicable understanding that complete independence of systems and components at the different levels is not possible;
- Safety systems functionally isolated and physically separated to the extent practical from systems at Level 1 and 2;
- The SSCs at Level 4 independent (functionally isolated and physically separate) to the extent practicable from the SSCs of other levels of defence in depth;
- Human and organisational factors playing a great role in the effectiveness of SSCs at all levels.

2. Emphasising the vital importance of ensuring that common cause and common mode failures, especially external events acting in combination, do not lead to breaches of safety provisions at several defence in depth levels by means of:
    - Special attention paid to common cause and common mode failures due to external hazards;
    - Enhancement of the diversity, separation and redundancy of safety provisions, and increased attention to the qualification of safety equipment, particularly instrumentation and control;
    - Adequate robustness, under all conditions, of safety services and controls (including control centres);
    - Particular attention to the impact of extreme external events on on-site and off-site electrical power, as well as on other services;
    - Where there are significant uncertainties in the derivation of design basis external events, additional margins or design provisions to be included to avoid cliff-edges;
    - Considering with particular interest extreme weather conditions due to the uncertainty of external events;
    - Consideration given to on-site induced flooding, due to possible failures of such equipment as the main cooling intake pipework;
    - Studies of the site-originated hazards (for example, fire, explosion or vehicle crashes) in relation to the impact on the effectiveness of independence between levels;
    - Attention to common cause and common mode failures caused by introducing new technological solutions;
    - High quality software, diversity and separation when using digital instrumentation and control;
    - Consideration of innovative design tools, such as those used in the design of the piping system, generating codes for I&C and plant modelling as a source of a common cause failure;

- Failures initiated by maintenance as a source of common cause failures, including failures in passive systems;
- Importance of failures or events related to the electrical supply system on and off the site as a source of a common cause and common mode failures;
- The manufacturing process and procedures or the supply of components, especially changes affecting them, as a source of common cause and common mode failures;
- Inappropriate storage or marking of safety related equipment resulting in common cause and common mode failures if used in SSCs across levels;

3. Greater attention needed to reinforce prevention and mitigation at the various levels, particularly at Level 4;
4. Using the concept of practical elimination of sequences leading to significant radioactive releases with consideration that:
    - For existing plants the significant radioactive releases should be prevented or mitigated by means of reasonable practicable modifications/backfitting measures and severe accident provisions as far as practicable.
    - The implementation of the practical elimination concept is most effective through design features, and thus it is easier to be implemented in new reactors. For operating reactors, there are likely to be fewer practical opportunities for enhancing safety. These opportunities have to be considered on a case-by-case basis.
    - The regulatory body should assess the licensee's evaluation and identification of, inter alia, phenomena that could challenge containment performance, event preclusion, accident progression, containment performance and potential radiological source terms.
    - The practical elimination concept is an approach that sets improved safety goals (or expectations) for nuclear installations by incorporating additional design features or, more rarely, operating provisions.
    - It is important that practical elimination is not used to justify a lack of severe accident management arrangements and capabilities, or the absence of fully effective emergency arrangements both on-site and off-site.
    - The practical elimination should specifically address challenges to containment performance as the last barrier to radioactive releases.
    - Challenges to the containment (e.g. severe accident performance and potential containment failure mechanisms, including bypassing the last barrier) should be identified through deterministic analyses, PSAs and engineering judgement. This process should include issues related to core melt concrete interaction, hydrogen combustion, over-pressurisation, direct containment heating, steam explosions.
    - Design and operational provisions should prevent or mitigate each severe accident phenomenon.

- Analysis (best estimate) should demonstrate the effectiveness of the design features established through practical elimination assessment.
- PSA should show the overall effectiveness of Level 1, 2, 3 and 4 activities in order to practically eliminate significant releases.
- In each case, the demonstration should include sufficient knowledge of the accident sequences analysed and of the phenomena involved, substantiated by relevant evidence, to conclude that the condition is physically impossible or extremely unlikely with a high degree of confidence.

5. Reinforcing the importance of assessments on the impact of human and organisational factors on defence in depth considering that:
    - Human and organisational elements of the safety provisions support can reduce or cut across the independent effectiveness of the SSCs at the various levels acting as a common cause failure.
    - Human and organisational aspects are of particular importance and include such matters as:
        - Safety culture as essential means for maintaining defence in depth
        - Design and operational management control, including quality assurance (QA), management of change and configuration control
        - Attention paid to the processes of construction and installation, maintenance, modification and operation due to their potential to degrade the independence of the levels
        - Greater attention to severe accident management, including leadership, emotional needs of staff (especially with external events that may have also affected their families and homes), decision-making responsibilities (the site director, or person acting in that role, should clearly be in charge of on-site activities) and staffing levels – particularly for the impact of external hazards on multi-unit sites
        - Importance of ensuring that the staff of the utility and their contractors and the regulator are aware of the need to preserve the safety provisions at the various defence in depth levels and their effective independence
        - Defence in depth as a part of the effective training programmes for operational and maintenance staff.
6. Implementation of defence in depth for operating reactors by due consideration of:
    - PSRs, plant-specific backfitting and feedback from operating experience to be used for implementation of upgrading;

- Fewer practical steps available to address event preclusion or containment failure mechanisms because fundamental design modifications are not usually practical;
- In some cases, the addition of hydrogen recombiners, containment flooding (usually through SAMGs), containment venting combined with other measures such as scrubbing, or filtered containment venting, can address specific severe accident sequences and contribute significantly to enhanced containment performance;
- Further studies which could be beneficial in identifying safety improvements including certain design modifications that would practically eliminate some severe accident sequences;
- Improvements for operating reactors are likely to be through mitigation strategies and measures rather than through prevention of the initiating event sequence;
- PSA is a useful tool to identify the most important sequences and opportunities for safety enhancements.

7. Consideration of defence in depth at multi-unit sites by means of:
    - Special attention given to interdependencies between the unit either enhancing or undermining safety;
    - Sufficient staffing levels for normal operation and for response to events, including multi-unit events;
    - Sufficient temporary or portable equipment to cope with DECs (e.g. diesel generators, water supply);
    - Development of emergency response procedures and SAMGs addressing multi-unit events;
    - Accommodating all staff in response to an incident affecting whole site;
    - Ensuring the ability of each unit to function on its own;
    - Considering what is credited as support from other units in accident conditions;
    - In exceptional cases when SSCs are shared between two or more reactors, ensuring that such sharing excludes safety systems and turbine generator buildings that contain high-pressure steam and feedwater systems, unless this contributes to enhanced safety;
    - Ensuring that in an accident involving one of the reactors, orderly shutdown, cool down, and removal of residual heat is achievable for the other reactor(s);
    - The adequacy of defence in depth provisions for each unit (facility, e.g. SFP, dry fuel storage) taking into account the impact of adjoining and nearby facilities;

- Site specific considerations noting that as far as practicable the safety provisions for each unit should be self-sufficient, although they may offer backup to other units;
- Implementing emergency preparedness measures taking into account multi-unit events.

8. Underlining importance of the issues associated with Level 5 defence in depth provisions (emergency arrangements) especially for long-term and multi-unit nuclear accidents, noting that the authorities and players involved are generally different, with consideration of the following points of view.

    - Basis for emergency planning
        - Planned emergency response may significantly differ from the real situation due to large uncertainty
        - There is a need of flexible emergency plans able to be extended beyond reasonably credible scenarios
        - Well trained system of response with timely and robust technical support is needed
        - Adequate procedures for radiation protection and countermeasures are needed
        - Smooth communication system for national and international use should be available
        - The potential long-term nature of some nuclear accident scenarios should be considered
        - Potential for escalating scenarios at multi-unit sites should be considered
        - General impact of an extreme external event off-site should be considered
        - Alternative arrangements are needed or hardened off-site centres should be provided
        - It should be taken into account that movement of assessment teams, emergency teams and evacuees may be severely affected
        - Considering a series of other emergencies in addition to the nuclear emergency.
    - Decision making
        - The roles and responsibilities of various decision makers should be clearly identified for making timely and appropriate decisions
        - The structure of the emergency response should be efficient and delegated appropriately down so as to enable rapid decisions
        - It should be considered that the decision structures can be complicated, multi-layered, and changing over time

    - Clear guidance and initial criteria should be developed in advance for the establishment and cessation of countermeasures
    - Reliable up-to-date plant information should be available as a basis for decisions

- Countermeasures
    - Impacts from radiation exposure can be difficult if not impossible to quantify
    - Accident-related stress impacts, and impacts due to evacuation, can be more tangible than radiation hazard
    - More consideration of the risks from implementing protective countermeasures, particular to vulnerable groups to be warranted
    - Decisions may be different for different groups and arrangements have to be in place to provide suitable care
    - The level of prudence involved, particularly in addressing protection in early, extremely uncertain conditions, should be considered
    - In some circumstances, cross-border co-ordination of protective actions during the early phase of a nuclear accident is necessary
- Communication
    - Timely and effective communication with the public and other stakeholders is important
    - Different channels understanding the possibilities and challenges of social media should be used
    - Communications should be built upon a prior, longer-term interaction with relevant stakeholders about the site and about radiological risk
    - Information needs of foreign governments, overseas nuclear regulators and international organisations should be considered
    - Ability to provide information in English, in real time and covering a wide range of topics concerning governmental decisions, including rationale and judgements is important
- Interactions with the recovery phase
    - Level 5 emergency management arrangements should be closely co-ordinated with recovery plans and implementation so as to ensure continuity and complementarity in decisions
    - Recovery approaches need to be established as a part of the pre-planning phase and must comprise considerable stakeholder input and involvement based on trusted relationships

- Considerable information in a suitable form should be provided to ensure the effective involvement of stakeholders, including local municipal officials and the public
- Given the rareness of significant off-site nuclear emergencies, pre-accident stakeholder involvement and communication has to be maintained over long periods
- Pre-accident efforts and post-accident focus on transparency are important aspects of nuclear emergency planning and recovery programmes.

- Interactions of authorities, response teams and other stakeholders
  - The needs of effective communication to promote common and appropriate understanding and balance among the various levels, noting that in some cases the terms are used differently.

6. Modifications due to recommendations from the post-Fukushima stress tests

Following the Fukushima accident, practically all countries operating NPPs have launched complementary safety reassessment of the safety margins of their NPPs under severe conditions usually called stress-tests. As a typical case stress tests have been launched in Europe under the European Commission (EC) coordination using WENRA and ENSREG as technically coordinating bodies. The assessment had 3 components:

- Assessment of the adequacy of selection of extreme natural events and capability of the plants to cope with such events
- Assessment of consequences and measures for prevention of loss of SFs from any initiating event conceivable at the plant site in case of loss of electric power, including (SBO, loss of UHS, or combination of both,
- Assessment of severe accident management (SAM) issues (design and operational provisions available to eliminate challenges to containment integrity after severe fuel damage).

Similar reassessment of safety level of existing NPPs in Europe was organized by all nuclear countries, although not necessarily in the same scope and using the same rules. One of the objectives of the assessment was to develop proposals for the increase of the robustness of the plant under conditions of extreme natural events. In the text below, an overview of such general proposals for improvements is provided, subdivided into the same categories as considered in the stress tests. The lists below are based not only on the compilation of the EU stress tests [10, 11], but also on information made available from the reassessment performed in all other countries through various IAEA meetings. Further on, the potential areas for studies and developments identified in the stress tests are listed.

Robustness of the NPP design against extreme external hazards

Proposed measures to increase resistance against extreme external hazards include:

- Selection of unlikely external hazards, in particular earthquakes and flooding as a part of the design basis: for plant reviews/back-fitting with respect to external hazards using the frequency 10^{-4} per annum and considering 0.1g as a minimum peak ground acceleration (PGA)
- Strengthening the PSR by a more consistent approach to the determination of margins for external events, including external event PSAs and regular reviews of the design and beyond design hazards
- Harmonization of natural hazards assessments, including earthquakes, flooding and extreme weather conditions, as well as the assessment of margins beyond the design basis
- Developing standards for plant walk downs with regards to earthquakes, flooding and extreme weather to provide a more systematic search for deficiencies
- Enhancement of monitoring and alert systems against extreme natural hazards
- Consideration of combination of external hazards and internal initiating events
- Harmonization of approaches for consideration of secondary effects of the earthquakes
- Protection against flooding: reinforcement or rising the dams and dykes, sealed perimeters of buildings against penetration of water
- Enhanced robustness of design against external hazards and security threats including malevolent actions; use of a hardened core of systems being one of the options
- Ensuring safe storage and availability of mobile equipment to perform necessary safety functions following a significant external event
- Enhancing external hazards robustness of on-site emergency centres.

Long-term loss of safety systems

Proposed measures for enhancement of capabilities to cope with loss of electric power supply and loss of UHS include:

- Enhancement of plant autonomy (independence from external support)
- Enhancement of on-site and off-site AC power supplies, robust grid connections, availability of additional diversified sources of AC power and cooling media on the site
- Increased on site stocks of fuel for emergency diesels
- Increasing capacity and reliability of DC power: enlarged battery discharge time, use of mobile battery chargers or mobile DC power sources to allow extended use of instrumentation and operation of controls
- Alternate means of cooling including alternate heat sinks, such as steam generator gravity feeding, or using other sources of water, supply from stored

condenser cooling water, alternate tanks or wells on the site, or water sources in the vicinity (reservoir, lakes, etc.) to enable core cooling and prevention of fuel degradation

- Enhanced robustness of plant systems by their separation and independence, enhanced capacities of ventilation systems, habitability of control rooms and robustness of the SFPs
- Implementation of alternate/additional heat transport routes to the UHS
- Use of special equipment with resistance against external hazards significantly beyond the design basis loads (bunkered systems or hardened core)
- Use of mobile sources of power and coolant, stored in safe and secured locations, with prepared quick connections, procedures on how to connect and use and staff training for use of such equipment
- Improvement of robustness and power independence of instrumentation and monitoring equipment
- Preparedness for the events that could affect multiple units by additional equipment and trained staff available to deal with events affecting all the units on one site
-
- Operational or preparatory actions such as improved inspections and training programmes, verification of access to essential equipment and ensuring the supply of fuel and lubrication oil.

Severe accident management

Proposed measures for enhancement of severe accident management and on-site emergency arrangements include:

- Implementation of the recognized measures to ensure containment integrity in severe accidents (hydrogen monitoring and mitigation, reliable depressurization of the RCS, containment overpressure protection, molten corium stabilization)
- Enhanced independence and diversity of provisions at different levels of defence, in particular at Level 4 aimed at prevention and mitigation of severe accidents
- Strengthened requirements on equipment for mitigation of severe accidents (redundancy, reliable power supply, resistance against external hazards)
- Availability of instrumentation and other hardware tools for management of severe accidents
- Finalizing SAMGs for multiunit accidents, damaged infrastructure, SFPs, shutdown operational regimes
- Improved training tools, methods and staff exercises for severe accidents

- Enhancement and validation of SAMGs for multi-unit accidents with long duration, under conditions of damaged infrastructure
- SAM exercises and drills for validation of procedures and organizational measures at extended level (including nation level)
- Improvement of both internal and external communication means in case of severe accidents
- Prevention/reduction of hydrogen risk in spaces with potential hydrogen migration beyond the place of its production, including hydrogen produced in SFPs
- Provisions for radiation protection of the staff involved in SAM and emergency arrangements
- Strengthening of on-site emergency centres against external hazards and harsh radiological conditions
- Establishment of rescue teams and equipment rapidly transportable to support local operators
- Confirmation of adequacy of SAM provisions by a comprehensive Level 2 PSA
-
- Development of conceptual solutions for post-accident fixing of contamination and the treatment of potentially large volumes of contaminated water.

Needs for future studies and development

Areas for such future studies and developments, identified in the stress tests include:

- Development of approaches to natural hazard determination, techniques and data, and development of a guidance on natural hazards assessments, including earthquake, flooding and extreme weather conditions
- Development of a guidance on the assessment of margins beyond the design basis and cliff-edge effects for extreme natural hazards
- Development of a systematic approach to extreme weather challenges and a more consistent understanding of the possible design mitigation measures
- Development of the approach for assessment of the secondary effects of natural hazards, such as flood or fires arising as a result of the seismic event
- Enhancement of PSA for natural hazards other than seismic (in particular extreme weather) and development of methods to determining margins and identifying potential plant improvements
- Overall enhancement of PSA analysis, covering all plant states, external events and prolonged processes, for PSA levels 1 and 2

- Development of advanced instrumentation based on simple physical principles (e. g. passive temperature, pressure readers) capable to be used in specific SBO and loss of DC power
- Systematic evaluation of the availability of safety functions required for SAM under different circumstances
- Detailed studies on progression of severe accident, allowing to determine timing of cliff edges such as core melt, reactor pressure vessel (RPV) failure, containment basemat melt through or other modes of containment failure, SFP fuel uncovery
- Analysis of severe accidents and demonstration of feasibility of AM actions for long processes with duration of several days, involving accidents occurring in parallel on several units, and taking into account potential interactions between the reactor and the SFP
- Investigation of cooling modes for partially relocated core prior to RPV failure
- Further assessment of the feasibility of various strategies for molten corium cooling, both in-vessel as well as ex-vessel, aimed at protecting containment integrity
- Further analysis of phenomena associated with reactor cavity flooding and related steam explosion risks following potential RPV penetration by molten corium
- Enhancement of the methods and tools for SAM training and exercises, (such as desk-top training, use of multi-function or full-scope simulators) including development of new training tools for NPP staff training
- Studies of long-term containment overpressurization due to excessive production of steam and non-condensable gases, and means for protection of containment integrity, including filtered venting
- Studies of potential re-criticality both in reactor cores as well as SFPs, taking into account potential geometry and material composition changes caused either by external hazards or by the progression of the severe accident
- Further analysis of hydrogen production, distribution, deflagration and detonation in complex containment geometries
- Analysis of potential for migration of hydrogen into spaces beyond where it is produced in the primary containment, as well as hydrogen production in SFPs and of measures to reduce the hydrogen risk
- Analysis of severe accidents involving molten fuel in the SFPs and measures for mitigation of the consequences, including venting of buildings in case of coolant boiling in the SFPs
- Determination of expected radiological conditions inside plant buildings and outside during severe accidents, as well as the limitation of radiological releases, including situations with the damaged containment

- Enhancement of methods for assessment of radiological situation on site including the case of multi-unit accidents, in connection with radiation monitoring, habitability and feasibility of SAM actions
- Development of conceptual solutions for post-accident fixing of contamination and the treatment of potentially large volumes of contaminated water
- Technical and organizational strengthening of on-site emergency arrangements, including on-site emergency centres protected against extreme natural hazards and contamination
- Studies of the logistics of the external support and related arrangements (storage of equipment, equipment and manpower resources, use of national defence resources, etc.)
- Studies of feasibility of operations in the event of widespread damage, for example, following an earthquake, including the needs for different equipment (e. g. bulldozers) and plans on how to clear the route to the most critical locations or equipment.

8. Modifications due to recommendations from the post-Fukushima IAEA Expert Meetings

There were several expert meeting organized by IAEA with the objective to formulate recommendations for improvements in relevant areas. The outcomes of the expert meetings were published in corresponding reports. Two most relevant expert meetings are summarized in the following text.

IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant [8]

In the report, several key technical areas important for strengthening reactor and spent fuel safety have been discussed. For each of the areas, the lessons learned were summarized and recommendations were formulated as follows:

Defence in depth

Lessons Learned: The application of the defence in depth concept should be improved to clarify how to focus safety measures on both the prevention of accidents and the mitigation of accident consequences should an accident occur. In particular, the mitigation measures to ensure containment integrity should be strengthened.

Areas for improvements

- Re-evaluate the hazards, robustness and vulnerabilities of the existing designs, and provide permanent and mobile equipment for identified vulnerabilities, especially for electrical power and cooling water capabilities;
- Use existing knowledge and continue research and development (R&D) of design improvements that would support accident mitigation, especially as regards confinement/ containment (e.g. filtered containment venting, hydrogen control, molten core control);

- Make design changes to improve protection of the core from severe damage and to increase the acceptable time for 'no action' on the part of the operators (e.g. SFP cooling, flood-proofing of structures, addition of permanent water and power sources).

Protection against extreme events and external hazards

Lessons Learned: Site and nuclear power plant specific external hazards and extreme events should be periodically re-examined and updated to ensure the adequacy of safety margins and protective measures.

Areas for improvements

- Hardening and improvement of the reliability of the external power system through:
    - Separation and diversification of the off-site electrical supply equipment;
    - Installation of fault locators to improve failure detection and diagnostic capabilities;
    - Implementation of modifications to achieve earthquake resistance and flood protection of essential substations and switchyard components;
    - Addition of measures to improve the capability to mitigate and quickly recover from a loss of off-site power.
- Hardening and improvement of the reliability of the on-site power supply systems through:
    - Better separation and diversification of the emergency AC power supply trains and of their essential buses and switchboards;
    - Enhancement of the DC power supply system and battery capacity;
    - Procurement of additional mobile battery sets and battery charging systems;
    - Installation of alternate backup power supplies (either mobile or fixed);
    - Implementation of a flood protection programme for buildings containing equipment essential to safety;
    - Provision of two or more outdoor, flood protected electrical tie-in points to facilitate connectivity of mobile equipment;
    - Deployment in safe storage of sufficient portable lighting systems, cabling and other electrical supplies.
- Improvement of the reactor cooling systems through:
    - R&D programmes to improve the tsunami prediction capability;

- Improvement of flood resistance and mitigation capability of cooling water systems and inventories;
- Enhancement of UHS defences and UHS failure mitigation capabilities, including the adoption of air cooled equipment;
- Improved operability of isolation valves;
- Installation of water injection ports outside the reactor building.

- Improvement of containment systems through:
  - Provision for adequate diversity of the primary containment vessel (PCV) cooling systems for boiling water reactors (BWRs), such as by adding an air cooled alternative or a gravity driven spray system that can also capture radioactive substances without having to rely on AC power or on the residual heat removal (RHR) systems;
  - Provision of cooling capability to the PCV top-head flange;
  - Improvement of the venting system operability, such as by adding an emergency battery and manual operation of the valves;
  - Installation of a valved bypass line to the rupture disk and increased filtering capability in the vent;
  - Preclusion of vent interconnectivity between units to avoid hydrogen and fire propagation;
  - Monitoring of hydrogen release rates and hydrogen concentration by controlling it.

Response to station black-out and loss of ultimate heat sink

Lessons Learned: The availability and operability of resources to cope with prolonged station blackout and loss of ultimate heat sink with or without concurrent extreme external events should be ensured.

Areas for improvements

- Improvements to the diversity and reliability of off-site power sources and associated systems, such as multiple power transmission lines from diverse routes and sources, and improved seismic resistance of the switchyard and substations;
- Additional high voltage and temporary cables along with backup electrical equipment;
- Provisions for additional equipment (installed, on-site and off-site) with permanent connections such as mobile power vehicles and necessary cables, diesel generators, power transformers, switchgear mobile batteries and battery charging systems, and additional diesel driven pumps;
- Portable alternative RHR systems and/or air cooling equipment along with enhanced water injection capabilities from pumps with high discharge pressures and water injection ports located outside the reactor building;

- Air driven pumps for flood response and supplies of fuel pumps, sump pumps, hose couplings and connections;
- Improved manoeuvrability of essential isolation valves by ensuring the availability of portable air compressors and DC power sources along with measures to manually operate essential isolation valves;
- Design changes such as installation of low leakage reactor coolant pump seals, permanent and qualified SFP cooling systems, additional steam driven and/or independently powered emergency feed pumps, and longer lasting DC power sources;
- Revision of SBO emergency procedures through the identification of optimal strategies and necessary equipment for use during an extended SBO;
- Revision of existing SBO regulations to include the implementation of corrective actions for identified vulnerabilities;
- Reconsideration of the current practice of assuming only a single unit station blackout at multi-unit sites by examining common cause failures affecting multiple units at the same time.

Hydrogen management

Lessons Learned: Implement measures for hydrogen removal and mitigation as well as measures for more efficient monitoring and control of hydrogen accumulation and propagation.

Areas for improvement

- Design and installation of hydrogen monitoring systems that would remain functional under severe accident conditions;
- Design and installation of emergency gas release systems for use under severe accident conditions that would be separate from existing operational or stand-by gas control systems;
- Ensured separation of neighbouring units on multi-unit sites by avoiding common release paths and cross-ties that would allow transfer of hydrogen from affected units to unaffected units;
- Review of hydrogen monitoring inside the containment and other buildings that would be susceptible to hydrogen propagation;
- Improvement of the understanding of hydrogen generation, accumulation and propagation, as well as of the effectiveness of hydrogen removal with respect to means and timing.

Containment systems and venting

Lessons Learned: Strengthen containment integrity by ensuring availability of monitoring, cooling and venting functions under severe accident conditions.

Areas for improvement

- Installation of containment vents with a filtering function designed for prevention of hydrogen explosion/combustion in filtering systems and for long term operation under BDBA conditions;
- Design considerations of structures, systems and components and instrumentation under accident conditions, for example, cooling of upper vessel flange seals to prevent failure under accident conditions;
- Isolation of gas vent systems from other operational and/or stand-by gas treatment systems;
- Avoidance of cross-ties and influence from other units on multi-unit sites.

Severe accident management and guidelines

Lessons Learned: Strengthen the severe accident management practices, guidelines and regulations to be used by the operating organizations and regulatory bodies.

Areas for improvement

- Re-evaluation and/or expansion of the SAM and emergency response, taking into consideration the availability/unavailability of on-site and off-site plant equipment and personnel, as well as the potential plant conditions that would bring the accident to the severe accident stage;
- Establishment of a clear scope and clear definitions, criteria and goals, as well as appropriate and continuous training for SAMGs, with better integration with abnormal and EOPs, and accident progression scenarios;
- Provision of qualified and reliable equipment for monitoring and control functions in order to manage the accident effectively;
- Design and installation of hardened emergency command centres that would not deteriorate during severe accident conditions, and improvements to ensure communication among centres where the responsible and accountable parties (at the plant, national, regional and international levels) operate by obtaining and maintaining robust communication equipment;
- Improved use of the latest R&D and technical knowledge concerning severe accident management, with a strong emphasis on accident mitigation through the prevention/minimization of the release of radioactive material;
- Possible development of tools to predict the physical phenomena leading to severe core damage and causing a consequent threat to the containment integrity, with the aim of improving SAMGs.
- Consideration of complicating factors such as destruction of support infrastructure, total site isolation and area devastation, common mode failures and failure propagation on a multi-unit site, the coincidence of radioactive releases, the unavailability of post-accident instrumentation, and severely damaged monitoring facilities

Instrumentation and control

Lessons Learned: Ensure robust capability to monitor essential plant safety parameters

and to facilitate actions that may become necessary during severe accidents.

Areas for improvement

- Increased robustness of I&C system to enable the necessary monitoring of safety parameters and plant conditions including DECs
- Ensuring appropriate operability time and the ability to continue instrument performance over the long term
- Expanding the range and specification of the instruments to cover extreme accident conditions and enhancing the emergency monitoring functions (e.g. by supplying power from emergency power sources, by adding dedicated power sources for monitoring equipment and by installing earthquake and flood resistance components)
- Providing hydrogen control and mitigation capabilities inside the containment or in other buildings, and emergency power enhancements for prolonged SBO and multi-unit events
- Considering engine driven generators and engine driven air compressors in powering critical I&C during a prolonged SBO.
- I&C improvements for damage mitigation monitoring strategies and environmental monitoring, in order to support decision making by local authorities.

Safety of spent fuel pools

Lessons Learned: Design and defence in depth evaluations of spent fuel pools and associated structures, systems and components should consider events that may lead to spent fuel damage in storage (e.g. loss of cooling, loss of pool inventory, re-criticality, hydrogen production, zirconium fire).

Areas for improvement

- Enhanced reliability of the water make-up injection systems for the SFP (e.g. ensuring diversity and redundancy and sufficient cooling water inventory).
- A more conservative spent fuel management policy favouring reduction of the spent fuel inventory in SFPs and in reactor buildings coupled with a more effective use of dry cask storage
- Ensuring that equipment and facilities are sufficient for dealing with multi-unit and prolonged SBO scenarios
- Enhanced reliability of SFP instrumentation available whenever there is irradiated fuel in the SFP, regardless of the external events or the operational mode of the reactor
- Resistance of critical instrumentation against seismic loads and protection from missiles.

at the Fukushima Daiichi Nuclear Power Plant [7]

As already indicated, many provisions for ensuring comprehensiveness of defence in depth belong to the category of human and organizational factors. While various hardware components are typically specific for different levels of defence and their failure affects just one level of defence, human and organizational factors have impact on several levels of defence, so that deficiencies in their implementation can negatively affect even all levels at the same time.

It is obvious, that specific features of the provisions in the category of human and organizational factors (such as affecting several levels of defence, large uncertainties and difficulties in predictability in human behaviour, sensitivity and vulnerability to psychological and societal influences, etc) require further attention and strengthening. The IAEA report [13] summarized a number of improvements in this area; some of them are listed below:

- Implementation of systemic approach to safety, taking into account interaction between individual, technical and organizational factors
- Strengthening mutual cooperation among all stakeholders (operators, vendors, regulators, contractors, TSOs, corporate organizations, international organizations) utilizing new communication interfaces and arrangements
- Strengthening interdisciplinary expertise by involvement of social and behavioural sciences
- Implementation of more practical ways for managers to strengthen safety culture supporting prioritization of nuclear safety (in particular, if a NPP is part of non-nuclear utility)
- Strengthening leadership and management for safety, mainly for top-level managers
- Objectively assessing efforts to strengthen safety and widely informing staff about safety initiatives
- Demonstrating high priority to safety culture by proactively introducing actions and ensuring resources for safety upgrading
- Continuously improving maintenance management and establishing closer cooperation with manufacturers and contractors
- Recognizing the efforts of personnel to protect and ensure the safety of the public, the workers and the plant
- Implementing improvements with regard to decision making and consideration of the use of tools to support decision making in emergency response
- Consideration of human and organizational factors in the planning, conduct and evaluation of emergency drills and exercises
- Identification of additional training, including understanding resilience, for operating personnel

- Enhancing the dialogue between the regulatory body and operating organization on topics beyond compliance and regulations, on safety practices and policies
- Enhanced efforts by the regulatory body to go out in the field and engage the licensee in conversations at the working level about safety practices and policies
- Establishing and maintaining the trust of local communities.

ANNEX II. APPROACH TO DEMONSTRATION OF PRACTICAL ELIMINATION OF EARLY OR LARGE RELEASES

IAEA Safety Requirements for design SSR-2/1 Rev. 1 [5] in para. 2.11 state that "plant event sequences that could result in high radiation doses or in a large radioactive release have to be 'practically eliminated". Practical elimination of early[11] or large[12] releases by design provisions is strictly required by Safety Requirements SSR-2/1 Rev. 1 (Req. 5, para 4.3, Req. 20, para 5.27 and 5.31). The same document states that "the possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise". Safety Requirements SSR-2/1 Rev. 1 do not quantify the values of early or large releases, they are described only qualitatively. The "certain conditions" to be addressed refer to hypothetical accident sequences that could lead to early or large radioactive releases due to containment failure or its by-pass that cannot (or hardly can) be mitigated with implementation of reasonable technical means[13]. It means that the NPP design has to be covered form 'normal operations' to 'design extension conditions', and also means that the conditions of 'beyond plant design envelope', more serious than design extension conditions, have to be practically eliminated.In this way the concept of practical elimination represents a complementary element to demonstration of compliance with comprehensiveness of defence in depth.

It is not yet clearly internationally established how to demonstrate practical elimination of conditions resulting in early or large radioactive releases and discussions are still ongoing. Nevertheless, the IAEA TECDOC-1791 [15] provides certain guidance on how to demonstrate practical elimination of early and large releases; this guidance was used as a basis for the approach described below.

According to the TECDOC-1791 the cases to be addressed for "practical elimination" could be grouped (for light water reactors) within the following five categories:

1. Events that could lead to prompt reactor core damage and consequent early containment failure:

   a. Failure of a large component in the reactor coolant system (RCS);

   b. Uncontrolled reactivity accidents.

2. Severe accident phenomena which could lead to early containment failure:

---

[11] Early radioactive release: A release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time.

[12] Large radioactivity release: A release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

[13] In some cases, in particular for operating reactors, prevention of certain conditions (such as steam explosions) can hardly be demonstrated; feasibility of mitigation of potential consequences should be then considered.

a. Direct containment heating;

b. Large steam explosion;

c. Hydrogen detonation.

3. Severe accident phenomena which could lead to late containment failure:

a. Molten core concrete interaction (MCCI);

b. Loss of containment heat removal.

4. Severe accident with containment bypass;

5. Significant fuel degradation in a storage pool.

TECDOC-1791 describes demonstration of practical elimination as follows: "The 'practical elimination' from consideration of accident situations that could lead to large or early releases has to be demonstrated by deterministic considerations supported by probabilistic considerations, taking into account the uncertainties due to the limited knowledge of some physical phenomena. It is a decision of the regulatory body to establish or not what are acceptable targets to support the demonstration of practical elimination."

Consistently with TECDOC-1791, the approach to the demonstration of practical elimination could consist of the following steps:

1st step: identification of the conditions (challenges) to be practically eliminated

2nd step: whenever possible, demonstration of practical elimination based on physical impossibility by the law of nature

3rd step: identification and implementation of design provisions for prevention of the challenges

4th step: identification and implementation of operational provisions (procedures) for prevention of the challenges

5th step: deterministic safety analysis and engineering judgment of effectiveness of the provisions

6th step: whenever appropriate and feasible, probabilistic safety analysis showing very low probability of failure of implemented design and operational provisions

Demonstration should not be based only by showing the compliance with a general probabilistic value; low probability solely should not be considered as a justification for not implementing reasonable design or operational measures. It is also noted that the concept of practical elimination applies to events of internal origin; in case of external hazards the concept of adequate margins is used.

Table 1 below presents examples of design and operations measures available to minimize the likelihood of conditions which could lead to early or large radioactive releases.

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

Challenge	Mechanism	Design and operational measures to prevent the mechanisms
Prompt reactor core damage and consequent early containment failure	Failure of a large component in the reactor coolant system;	• Most suitable composition of materials selected; • Metal component or structure as defect-free as possible; • Metal component or structure tolerant of defects • Mechanisms of growth of defects known • Design provisions and suitable operation practices in place to minimize thermal fatigue, stress corrosion, embrittlement, PTS, overpressurization, etc. • Effective in service inspection and surveillance programme in place during the manufacturing and the operation
	Uncontrolled reactivity accidents	• Identification of ways leading to fast insertion of reactivity • Analysis of challenges and consequences for fast reactivity insertions • Core design ensuring subcriticality under any plant conditions • Effective fast shutdown systems • Procedures to prevent potentially risky operating regimes
Severe accident phenomena which could lead to early containment failure	Core meltdown at high pressure (Direct Containment Heating)	• Reliable means to ensure opening of existing depressurization (relief, safety) valves of the reactor coolant system • Diverse system to depressurize the reactor coolant system • Additional barriers to minimize corium dispersion (such as barriers, include ledges, walls or indirect paths)
	Large steam explosion	• Using dry cavity • Adjustment of timing of cavity/ drywell

		flooding • In-vessel retention by external RPV cooling • In-vessel retention by internal RPV flooding • Decoupling of reactor cavity from containment envelope • Provisions for release steam from the cavity • Increased temperature of coolant for cavity flooding
	Hydrogen explosion;	• Large containment volume • Installation of igniters and/or recombiners • Containment inerting by nitrogen (permanently) or steam (temporarily) • Mixing of containment atmosphere • Filtered venting to reduce pre-burning pressure and amount of gases
	Containment boundary melt-through	• Flooding of reactor cavity or drywell • Additional barrier against corium for cavity doors, sumps, etc, to maintain corium cooling • In-vessel retention by external RPV cooling • In-vessel retention by internal RPV flooding • Insulator layers to eliminate or delay interaction • Corium spreading on cooled large area or core catcher
	Slow overpressurization of containment	• Large thermal capacity of the containment • Installation of adequately robust internal spray system • Installation of external spray system • Installation of adequately robust fan cooler system • Installation of sump cooling system • Installation of suppression pool cooling system • Installation of any other containment heat

		removal system • Installation of igniters and/or recombiners • Installation of filtered venting system
	Containment failure due to fast overpressurization or mechanical damage due to vessel failure	• Ensure dry cavity at the time of RPV breach, with measures to prevent MCCI • In-vessel retention by external RPV cooling • In-vessel retention by internal RPV flooding • Adequate steam flow path from the cavity • Verification and strengthening of cavity bottom, if necessary
Non confined severe fuel damage	Severe accident with containment by pass through damaged SG or through interface system	• Prevention of interface system LOCA • Depressurization of the RCS • Identification of bypass route and possibilities for fission products retention • Development and application of PRISE management • Ensuring SG tubes flooded by secondary coolant
	Significant fuel failure in a storage pool	• Pool structure designed against all conceivable internal and external hazards that could damage its integrity • Avoiding siphoning of water out of the pool • Redundant lines for pool cooling that eliminate possibility of long lasting loss of cooling function • Reliable instrumentation for pool level monitoring • Appropriate reliable means to compensate for any losses of water inventory' (e.g. SFP flooding from an external source)

ANNEX III. EXPLANATION AND JUSTIFICATION OF MODIFICATIONS OF OBJECTIVE TREES IN SR 46

The text below is intended to provide description and justification of changes made in original objective trees included in IAEA SR 46. Each of the original figures from SR 46 is commented separately, numbers are the same as numbers of the figures in SR 46. In the text, the content of the figures is named as the objective tree (OT).

1. **Fig. 11. External factors affecting the plant.** In this OT, there are as previously two kinds of mechanisms relevant for siting, potentially affecting the NPP: natural hazards and human hazards. Malevolent human actions are not to be considered as site specific mechanism. Such actions are implicitly covered by the updated OT 53, under two relevant mechanisms: "Lack of vigilance" and "Design vulnerabilities to potential threats" – malevolent action is considered as one of the threats. Provisions for individual mechanism are similar as previously, but they are formulated individually for each mechanism. Two additional mechanisms regarding natural hazards were added: one dealing with other) external hazards, like volcanos, other one is a general mechanism devoted to comprehensive identification of natural hazards relevant for the given site. Not only individual natural hazards, but also their meaningful combinations are considered in one of the mechanism and associated provisions. . Another new mechanism added to the OT is devoted to potential interactions between the grid and the plant. It is to be underlined that this OT is dealing with the site characteristics, not with the capabilities of the SSCs to cope with the site induced loads; assessment of the capabilities of SSCs should be part of the design. When it is required to specify margins for design of selected SSCs, it is meant to specify the increased site specific loads for which the SSCs are able to function in order to prevent early or large releases. Among the provisions associated with the siting there will be also "Evaluation of feasibility of compensatory design or operational measures". Examples of such compensatory measures are cleaning of sewage inlets, removal of snow layers, preventing water to enter electric cabinets by temporary sealing, etc. . Examples of compensatory measures for earthquakes can be dampers, strengthened structures, seismic monitoring, early shutdown of the reactor, etc. It was also recognized that it is needed to use carefully the words "adequate margin" and "sufficient margin". Adequate margin should be understood as more substantial, larger margin necessary in the case of large uncertainties, like those associated with external hazards.

2. **Fig. 12. Radiological impact on the public and the local environment.** Significant changes have been implemented in the modified OT. Differently from the original OT which had only one same set of provisions for 3 different mechanisms, in a new OT **s**pecific sets of provisions were developed for each of three transport mechanisms: air, water, food chain, with distinguishing of provisions for different mechanisms. In addition there are three new mechanisms added to the OT. These mechanisms are dealing with site characteristics affecting determination of the radiological effects of normal and abnormal plant operation, of design basis accidents together with DEC A (these

are design extension conditions without core melting), and of severe accidents on people and the environment. In addition it was realized that there is no reason to have separate OT for levels 1, 2, 3, 4, therefore OT originally placed on figures 12, 13 and 14 were merged together in fig. 12. It should be noted that the original OT 14 was quite vague. Now there is quite clear distinction between provisions related to site characteristics important for transport of radioactive materials via different exposure pathways (first three mechanisms, common to all levels of defence) and determination/limitation of radiological impact of different plant states, which is specified differently for levels 1-2, for level 3 and DEC-A, and for severe accidents. Three different levels were in this case put on one figure just because they were sufficiently simple to be placed in a single figure. It is the only OT where different mechanisms belonging to different levels of defense were put in a single OT. Otherwise the provisions for dissemination of radioactive materials differ for different levels of DiD due to the fact, that the acceptance (dose) criteria as well as methods for determination of radiological consequences (conservative versus best estimate) are different. In original OT 14, there was one of the mechanisms (with several more specific bullets) dealing with radiation monitoring. This was deleted from the combined OT 12 since it is not so much site specific. In addition, radioactive monitoring in operational states is more comprehensively covered in OT 26 (partly also in OT 69), for accidents the monitoring is covered in OT 77 and 78.

3. **Fig. 13. Radiological impact on the public and the local environment.** OT originally placed on fig. 12 and 13 were merged together as described in the text for fig. 12, there is no fig. 13.

4. **Fig. 14. Radiological impact on the public and the local environment.** OT originally placed on fig. 14 was merged together with fig. 12, as described in the text for fig. 12.

5. **Fig. 15. Availability of ultimate heat sink (UHS).** The problem with multiple mechanisms originally included in this OT was resolved by modification of the mechanisms and assigning just one string of provisions for each mechanism. By this change, instead of a list of not very specific bullets used in the previous OT, the standard “boxes” with provisions specific for each mechanism were implemented. It was verified that all relevant bullets are reflected in the boxes with provisions, without any omission. More attention was paid to consideration of the effects of external hazards on damaging mechanisms acting on both UHS themselves as well as on heat transport systems (HTS) to the UHS. It is understood that the boundary between the UHS and HTS is placed between the coolant of the UHS and the coolant of the Essential Service Water System (ESWS), it means that the HTS starts with ESWS. As an UHS, two different options (atmosphere or large body of water like the sea) were considered, although it was clear that only one of the options is normally used in many cases. Taking into account that only one of the options is normally applied it was decided to combine these two options of potential UHSs into one. For the heat transport system, three mechanisms were specified, related to: a) reliability of the system; b) capacity of the system for most adverse conditions and c) vulnerability of the system to external hazards, including those beyond the design basis events. Previously considered mechanisms dealing with heat

transfer phenomena (evaporation, raising the temperature) were deleted as they were not consistent with overall approach; the phenomena are addressed by the issues associated with capacity of the systems. Since a lot of discussion was devoted to correct consideration of various provisions, it is underlined that the provisions should be understood as options, not necessarily to be implemented in parallel. It also means that larger number of options is more convenient for the reviewer than the limited number, since it offers larger flexibility.

6. **Fig. 16. Design management.** With minor modifications, the mechanisms in this OT remained the same as before. Main changes in this OT were intended to be more specific in indicating responsibility of operating organization and at the same time partially suppressing the provisions devoted to activities in design organization (still the main provisions related to design organization are maintained). Changes for the first mechanism (lack of qualified design personnel) are aimed to avoid bullet points and to replace them by standard format of provisions, but none of the bullets was omitted. Provisions under second mechanism were slightly simplified (two bullet points suppressed) since they dealt with internal matters of the design organization (less relevant for the operator). In opposite, the provisions relevant for the operating organization were specified more clearly, so that none of the bullets remained neglected. Third and fourth mechanism were expanded in order to provide more details on responsibilities of the operating organization for establishment of design basis and maintaining continuity in safety of the design. Provisions for ensuring quality of design were also expanded and corresponding provisions presented as part of the management system. These changes are in accordance with the SSR-2/1 Rev 1, and also with GSR Part 2 on Leadership and Management for Safety. An attempt was made to ensure clearer determination what is the responsibility of the designer and what is the responsibility of the operating organization. Provisions related to minimization of radioactive waste were omitted from this OT as too specific for design management, and only one of many other similar provisions associated with the design management. Minimization of waste will be more explicitly articulated in OT 26.

7. **Fig. 17. Proven technology.** Changes in this OT are not large. All mechanisms remained the same. More significant differences were made only in the mechanism dealing with analytical demonstration of performance of the engineered safety features in order to define more specific steps for performing analytical demonstration of performance. Analytical demonstration is now put more logically as the last items of a chain of provisions, all items of provisions before the last one are preparatory steps for the analysis. In addition, those provisions were formulated so that it was possible to replace the set of bullets by standard boxes with the text of provisions. In addition to this more significant change, there are only small improvements in formulation of provisions.

8. **Fig. 18. General basis for design.** This OT is intended to summarize provisions aimed at specification of the plant design basis/design envelope. It is noted that in this OT the meaning of the term “design basis” is the same as “design envelope”. Both terms mean in accordance with IAEA TECDOC-1791 a set of initiating events, internal and external hazards and all other conditions

to be considered in the design of the NPP. In accordance with the same TECDOC the features to facilitate the use of non-permanent equipment are outside of the plant design envelope. In order to cover the issue of design basis/design envelope systematically and more comprehensively compared to SR 46, significant changes were made in this OT to more correctly reflect the formation of the design envelope. Similarly as in other OTs, the bullet items previously included in branches connected with some of the provisions were eliminated by putting relevant items into standard boxes with the text of provisions. The determination of the design envelope starts with identification of all plant states, from normal operation up to severe accidents. Loads originated from internal and external hazards can affect performance of any of the plant states and they form another, separate part of the design envelope. Next step in formation of design envelope is analysis of all plant states (in accordance with updated IAEA SSG-2 realistically and conservatively for AOOs, conservatively for DBAs, realistically for DECs) using validated computer codes to determine bounding parameters corresponding to different plant states. At the end for each relevant SSC the design envelope parameters are defined, SSC is safety classified as very important part of the general basis for the design and correspondingly to this classification the requirements on environmental qualification, reliability of power supply, seismic resistance and quality requirements are defined. At the end both safety analysis as well as the design are independently verified by the operating organization (or by any other qualified body on behalf of the operating organization), it is submitted for review and assessment to the regulatory body, or optionally can be partially verified by independent external review missions. Although different parts of this process (i.e. selection of plant states, performance of the analysis and designing of the items important to safety correspondingly to the design envelope) are described in separate sets of provisions, it is understood that in many cases there will be a need of several iterations between these two sets of provisions.

9. **Fig. 19. Plant process control systems.** There are significant changes in a number and formulations of provisions. In the updated OT there is more explicit separation between provisions for level 1 and 2 and provisions in comparison with SR 46 are formulated more specifically. An attempt was made to integrate OT 19 and 20, but it came out that it unnecessarily leads to mixing up the requirements on reactor trip systems, plant control systems and safety systems in the text of provisions. Therefore the OT 19 and OT 20 remained separated. One of the previous challenges associated with neutronic and thermal-hydraulic parameters outside their normal operation ranges was omitted due to its similar effect as another challenge, which is more frequent and more demanding (controlling wider range of parameters) functioning of the systems.

10. **Fig. 20. Plant process control systems.** The explanatory text made for OT 19 applies also for OT 20.

11. **Fig. 21. Automatic safety systems.** In addition to small improvements in formulation of some provisions, 8 new provisions were added to provide more specific options for applicable provisions, with more attention given to functioning of support systems to safety systems, including maintaining

reserves of consumables, higher reliability of systems, testing of systems and qualification of equipment. The most significant change is implementation of a new provision requiring a back-up diverse systems for given safety functions; this provision is important for coping with DEC-A conditions, which are newly covered by this updated OT.

12. **Fig. 22. Reliability targets.** Validity of this OT was extended from Level 3 to all other levels, it means to levels 1 to 4, since it is understood that the adequate reliability is required not only for safety systems, but for all items important to safety. Due to this change, the term "safety systems" in the text of some mechanisms and provisions has been changed to "items important to safety". Due to the same change, it was not logical to deal separately with the safety systems and separately with their supporting systems, since both of them belong to the items important to safety. Previous mechanisms, one dealing with safety systems, other with support systems, were not specified consistently with this new viewpoint and therefore have been changed in the updated OT. In the updated OT, the provisions are more logically subdivided into design and operational provisions affecting the reliability of items important to safety, understanding that the supporting systems are also essential components of the items important to safety. One of three mechanisms deals with design provisions for ensuring reliability, other with operational provisions for ensuring reliability. In addition, there is one mechanism dealing with common cause failures in the items important to safety, with a reference to a specific OT. The provisions themselves remained not very much changed and just 3 new provisions were added. As far as mobile equipment is concerned, in accordance with TECDOC-1791 this equipment does not belong to the design envelope and therefore provisions included under all mechanisms in OT 22 do not apply to mobile equipment. It is noted that mobile (non-permanent) equipment belongs to the equipment involved in accident management, i.e. to AM equipment.

13. **Fig. 23. Dependent failure.** Validity of this OT was extended from originally considered only Level 3 also to Level 4 in order to cover prevention of dependent failures not only in safety systems, but also in safety features for DECs. Due to this fact in the mechanisms the term "safety systems" has been replaced by "items important to safety", consistently with SSR-2/1 Rev 1. It should be also noted that the list of hazards given in the text of mechanisms is meant just as a list of examples, not as a comprehensive list of items. Besides this above commented change there are only insignificant changes in this OT.

14. **Fig. 24. Equipment qualification.** Validity of this OT was extended from originally considered only Level 3 also to Level 4. In response to this change, the term "safety systems" has been replaced by "items important to safety". The OT was improved by providing more specific provisions formulated in standard boxes instead of previously used branches with bulleted list. It is understood that items important to safety includes not only the safety systems and safety features for design extension conditions, but also their relevant support systems (without explicitly writing the term "support systems" in the text of provisions).

15. **Fig. 25. Inspectability of safety equipment.** The mechanisms in this OT remained the same as included previously in SR 46. Bulleted lists in the

branches connected to certain provisions were replaced by standard boxes with provisions, thus increasing number of provisions. The provisions are now written in more specific way so that they specify more broadly and more explicitly the provisions for performing inspections, selection of methods and evaluation of the results of inspections.

16. **Fig. 26. Radiation protection in design.** There is significant increase in number of provisions in the updated OT, in particular for first two mechanisms associated with uncontrolled releases to the environment. In the original OT there were only 3 provisions focused only on monitoring, there are now altogether 13 provisions covering also other features, including design of radwaste systems, filtration, ALARA measures, testing, etc. Less significant increase in number of provisions with partial modifications of the text of the provisions was also made under other two mechanisms associated with radiation exposure of the NPP staff.

17. **Fig. 27. Protection against power transient accidents.** There are **o**nly small modifications in formulation of some provisions, and 5 new provisions were added with the objective to provide more specific examples of available measures. Examples of surveillance methods of material status are non-destructive testing of the wall and the nozzles of reactor vessel head.

18. **Fig. 28. Protection against power transient accidents.** Original provisions included in SR 46 remained practically unchanged, and only 3 new provisions were added requiring availability of adequate operating procedures for those cases where possible mistakes in staff actions are relevant.

19. **Fig. 29. Protection against power transient accidents.** In addition to small improvements in formulation of provisions and adding 5 new provisions, there are also two new mechanisms with relevant 9 new provisions added. First of the mechanisms deals with inadvertent start-up of the reactor at low coolant temperature in the RCS, second of the new mechanism deals with prevention of fast slug type boron dilution. It should be noted that if such dilution would lead to very fast reactivity insertion (prompt criticality), such accident shall be practically eliminated. The issue of potential recriticality after injection of pure water into partially degraded core (control rods molten) is addressed under safety principle 200 (automatic shutdown system). Several of new added provisions deal with availability of adequate operating procedures in those cases where possible mistakes in staff actions are relevant. Optionally it would be possible (also in OT 28) in the text of the provision to specify the objective of the procedure, e.g. “Adequate operating procedures to prevent erroneous start-up of loop”.

20. **Fig. 30. Reactor core integrity.** This OT deals with potential damage of fuel due to various mechanical effects impacting the fuel during normal operation. First visible change in this OT compared to original one in SR 46 was made due to the fact, that a group of originally 4 challenges, either affecting the reactivity control, or core cooling, or direct damage of the fuel by mechanical effects were combined into one sufficiently general to achieve a standard shape of the objective tree. Second significant reason for the change was caused by the fact that for first two mechanisms specific sets of provisions was formulated

separately for each mechanism instead of previous one common string of provisions. This change was appropriate, since those two mechanisms were of quite different nature, first dealing with axial forces acting on fuel assemblies and second dealing with mechanical effect of earthquakes. Among the potential excessive forces there are also internal loads caused by springs, which are used in upper core plate preventing fuel assemblies to be pushed out from the core. In addition, there are some more specific provisions added and minor improvements made in wording of provisions.

21. **Fig. 31. Reactor core integrity.** This OT deals with potential damage of fuel due to various mechanical effects impacting the fuel during abnormal operation (anticipated operational occurrences). Since this OT corresponds to level 2 of DiD, provisions in this OT are those relevant for prevention of mechanical impact on fuel in case of anticipated operational occurrences. Similarly, as in the case of OT 30, original group of 4 challenges was combined into one more general to allow developing usual shape of the tree, i.e. group of boxes narrowing towards top of the tree. Besides that there were only minor changes in formulation of provisions.

22. **Fig. 32. Reactor core integrity. Similarly as in OT 30 and 31, a** group of 4 challenges was combined into one more general challenge. Besides that there are only minor changes in formulation of provisions.

23. **Fig. 33. Automatic shutdown systems, SF 2 (insertion of reactivity after shutdown).** In addition to small improvements in formulation of provisions and changed order of some provisions, one new mechanism was added – potential recriticality due to injection of non-borated coolant to partially degraded core, with 4 associated provisions aimed at prevention of this mechanism.

24. **Fig. 34. Automatic shutdown systems, SF 3 (capability to shutdown the reactor).** Although the mechanisms except small changes in wording remained the same, there are several changes in provisions in this OT. First, instead of making reference to hardly available IAEA VVER specific documents (VVER-SC-121 and 214) a specific relevant list of provisions is included. Second, instead of two branches with bulleted lists there are standard boxes with consistently formulated provisions. One of the issues addressed in this OT is potential recriticality, which is understood as any condition leading to excessive reactor cooldown either long-term or short-term (e.g. due to steam line break). In addition, there are some small improvements in formulation of the original provisions.

25. **Fig. 35. Normal heat removal.** This OT was significantly changed with much more specifically formulated provisions. It is to be noted that this OT deals only with normal heat removal from the reactor core, normal heat removal from the spent fuel pool is dealt with separately. This fact is also reflected in the modified formulation of the challenges. It was realized that it is not needed to have two OTs separately for level 1 and level 2 of defence, since the means for heat removal are the same for both levels 1 and 2. Therefore OT 35 and 36 were combined into one OT 35. It is also noted that the mechanisms and provisions associated with the reactor coolant system integrity (selection of materials, in-service inspections, structural design of the reactor coolant system) are not

included in this OT, since they are covered by a separate OT 40. Therefore, only structural design of the reactor internals is mentioned in this OT. Another important note is that the mechanisms and provisions in this OT are formulated assuming PWR design, which is more complex due to existence of both primary and secondary circuit; for BWR design appropriate integration of provisions applicable for the primary and secondary circuits should be made.

26. **Fig. 36. Normal heat removal.** The OT was combined with fig. 35 and thus was deleted from the set of OTs.

27. **Fig. 37. Startup, shutdown and low power operation.** Originally 3 mechanisms relevant for degraded capability of the plant to cope with accidents in non-power operational regimes were integrated into a single mechanism, with slightly modified common set of provisions. In addition, one new mechanism devoted to specific evolution of postulated initiating events and accident scenarios was added to this OT. This new mechanism is associated with a set of provisions, focused on identification of events and accident scenarios relevant for non-power operational regimes, selection of acceptance criteria, execution of deterministic safety analysis, development of specific EOPs and SAMGs. It is recognized, that although some relaxation of safety barriers during shutdown regimes is inevitable, it should be limited and used only if properly justified. Further on, there were improvements in formulation of some provisions.

28. **Fig. 38. Emergency heat removal.** The OT has been significantly changed, including its concept. The applicability of this OT has been extended from Level 3 of DiD also to DEC-A (part of Level 4, DEC conditions without core melting) conditions in order to reflect evolution of safety requirements since publication of INSAG-12, in particular after the Fukushima Daiichi accident. Therefore the applicability of the updated OT is for the heat removal from the fuel located in the reactor core (only) during DBAs as well as DEC-A conditions. Previously the mechanisms and provisions were formulated for 4 different types of accidents: loss of flow accidents, loss of inventory accidents (LOCA), loss of secondary side heat removal accidents and accident during shutdown operating regimes as a special group of accidents. At present the mechanisms and provisions are subdivided more generally but at the same time indicating more broadly potential reasons for failure in emergency heat removal: LOCA accidents, non-LOCA accidents, accidents with loss of heat removal due to loss of UHS, loss of power supply, and loss of support systems. As far as accidents due to loss of UHS are concerned, reference is made to OT 15. Accidents at non-power operational regimes are covered separately in OT 37. Previously considered in this OT38 development and implementation of EOPs is now covered by OT 68.

29. **Fig. 39. Emergency heat removal**. This OT deals with emergency hear removal from the fuel originally located in the core, but after core degradation and relocation possibly also in the reactor cavity or in the containment. Originally considered mechanism of unbalance between heat production and heat removal excessive heat production due to recriticality has been removed from the OT, since the issue of recriticality has been addressed in OT 33 and

the provision to address heat removal due to recriticality is addressed by one of the provisions dealing with inadequate removal of heat from the degraded core. It should be noted that among the sources of heat to be removed not only accumulated and decay heat should be considered, but all other sources in particular heat produced by chemical reactions between metallic materials and the coolant. Similarly as in the case of OT 38, as far as accidents due to loss of UHS are concerned, reference is made to OT 15. Slow over-pressurization due to steam generation is referred to OT 46.

30. **Fig. 40. Reactor coolant system integrity.** No change in mechanisms and provisions originally included in OT 40 was needed. However, originally the non-destructive testing of the RPV was by mistake under Level 2, which was covered in Fig. 41. It is more logical to merge both OT into 1 and assign them to both Levels 1 and 2 in modified OT 40. The OT includes provisions, necessary to ensure practical elimination of sudden rupture of large pressurized components (in particular reactor pressure vessel) as one of the challenges potentially leading to early or large releases.

31. **Fig. 41. Reactor coolant system integrity.** This OT was merged with fig. 40, see the text for fig. 40.

32. **Fig. 42. Confinement of radioactive material, for the releases of fission products from the RCS.** Important changes in this OT include: elimination of the option not existing containment as fully unacceptable for NPP thus not to be mentioned; and separation of provisions for two different mechanisms of accidents bypassing the containment (PRISE and interface LOCA), so that each mechanism has its own string of provisions. It is noted that the releases from sources other than RCS are dealt with separately, in OT 43. Further on, since the release pathways and the associated phenomena are quite different for DBAs and severe accidents, it is considered appropriate to have two different OTs, one for Level 3 and another for Level 4 of DiD.

33. **Fig. 43. Confinement of radioactive material, for the releases from the sources outside RCS.** This objective tree was significantly simplified using references between OT 43 and OT52, dealing with potential damage of the spent fuel in the storage or during the transport. Since it is clear that releases of radioactive materials (to be covered by OT 43) from the spent fuel can take place after the fuel damage (covered after updating more comprehensively by OT 52), such references are very convenient. Such references are used for both spent fuel pool as well as for transport containers. It is to be noted, that the spent fuel pool covered by OT 43 and wet spent fuel storage covered by OT 52 are the same facilities. OT 43 can to some extent deal also with the on-site dry spent fuel storage in the case of such storage is part of the same nuclear installation.

34. **Fig. 44. Confinement of radioactive material.** In addition to improvements of formulations more attention was paid to provisions reducing releases from the containment and releases bypassing the containment, mainly due to accidents in SFP and PRISE. One of the issues associated with potential releases from the containment is direct (unfiltered) leakage from the primary containment, which is often called “secondary containment by-pass”. This issue is relevant for double containments, in which major part of the releases from the primary

containment enters the containment annulus and afterwards is released to the environment through the filters. However, small part of the release (called secondary containment by-pass) can propagate through penetrations, isolation devices etc directly to the environment, thus by-passing the filters and determining radiological consequences. For all mechanism leading to containment by-pass the provisions contributing to practical elimination of early or large releases are listed.

35. **Fig. 45. Protection of confinement structure.** In addition to 3 previous mechanisms endangering the containment integrity due to containment overpressurization, low sub-atmospheric pressure and potential effect of internal missiles, 3 new mechanisms have been added to this OT. These new mechanisms address general design consideration, containment testing and inspections and potential damage by external hazards, both natural (e.g. earthquakes) as well as man induced (e.g. aircraft crashes, missiles, explosions). Random hazards should be identified based on their probability, malevolent human actions should be taken into account based on broader considerations. For both of them the design should be adequately robust. As far as malevolent actions are concerned, this mechanism is related to OT 53, dealing with security issues. OT 53 compared to OT 45 deals with broader consideration of hazards potentially affecting any vital areas of the plant, not just the containment. The mechanism of external hazards in OT 45 is particularly important due to the fact, that the containment belong to the SSCs ultimately needed for prevention of early or large releases, and therefore its adequate robustness is very important. In addition to the significant changes discussed above, there were some partial improvements in formulation of mechanisms and provisions in OT 45.

36. **Fig. 46. Protection of confinement structure.** In addition to improvements and more precise formulations, the OT is extended by challenges to containment integrity by SFP if located internally in the containment, and a challenge of destruction of the containment by explosions outside the containment (like it happened in Fukushima). In general it should be underlined, that equipment to be installed at Level 4 should preferably be independent from safety systems used at Level 3 (i.e. it should be dedicated). For existing plants such installation is often not feasible; in such case the systems at least should be adequately robust or enhanced to reliably survive DEC conditions. Previously as one of the mechanism also potential containment damage by internal missiles was considered. However, it was agreed in the discussion that the issue is worldwide considered as resolved and therefore the mechanism was eliminated from the OT. The column previously occupied by this mechanism was utilized for another mechanism, which is the potential mechanical damage either of the concrete reactor cavity bottom and-or other equipment located in the cavity by detached reactor vessel bottom impacting the cavity.

37. **Fig. 47. Monitoring of plant safety status.** The OT was modified in particular by providing more specific formulations of provisions. The problem of a group of mechanisms addressed by a single chain of provisions was eliminated by providing a set of specific provisions for each of the mechanisms.

38. **Fig. 48. Monitoring of plant safety status.** Similarly as in OT 47, the OT was modified in particular by providing more specific formulations of provisions and extending the list of provisions. In addition, two more mechanisms were added with their relevant provisions to address the issue of interdependencies between monitoring chains for different levels of defence and the issue of potential loss of plant information due to the loss of instrument power supply (with reference to OT 50 dealing with station blackout situation).

39. **Fig. 49. Preservation of control capability.** This OT deals with potential mechanisms leading to loss of control room inhabitability due to various reasons (fires, penetration of toxic gases or other dangerous substances, or damage of the control room by external hazards or other external actions. In addition to improvements and more precise formulations, the OT is extended by larger number and more specific provisions aimed at ensuring inhabitability of the control room and its larger robustness against natural external hazards. Possibility of a remote control place if found necessary is mentioned as well.

40. **Fig. 50. Station blackout.** The **o**bjective tree was significantly extended, it was practically re-done. Changes were done in accordance with a comprehensive IAEA TECDOC No. 1770 "Design Provisions for Withstanding Station Blackout at Nuclear Power Plants, published in 2015. Instead of original 1 mechanism, 7 mechanisms were identified in the updated OT 50, instead of original only 6 provisions 47 provisions were included in the updated OT. Significant updating reflects the importance of the issue of station blackout after Fukushima Daiichi accident.

41. **Fig. 51. Control of accidents within the design basis.** The **o**bjective tree was improved by providing more specific provisions. Three sets of provisions were developed: provisions to ensure performance of automatic actions, provisions to ensure performance of manual actions and provisions to ensure adequate characteristics of the safety systems. Equivalent provisions for Level 4 are covered by OT 74 -76.

42. **Fig. 52. New and spent fuel storage.** Applicability of this **o**bjective tree was extended from originally levels 1 and 2 to levels 1 to 4. The mechanisms remained nearly the same, but the list of provisions was extended to specify also the need of performing safety analysis, to take into account also DEC without fuel melting and to practically eliminate early or large releases. Among more important changes there are provisions on more complex monitoring of the SFP and on enhanced robustness of the SFP against external hazards. This OT is devoted to those provisions which are important to prevent fuel damage in storage systems for new as well as spent fuel, which are located inside the plant. Provisions of this OT are naturally frequently referred to in OT43, since prevention of radioactive releases (addressed in OT43) is closely interrelated to damage of the fuel, addressed in OT52. MOX (Mixed OXide) new fuel must be cooled in storage pool because its surface temperature and surface dose rate are much higher than those of UO2 new fuel.

43. **Fig. 53. Physical protection of the plant.** Previous separate two OTs (53 and 54) assigned only to Level 1 and Level 2 were combined together in a single OT, also understanding that deficiencies in physical protection of the plant can

affect all levels of defence. OTs 53 and 54 were thus merged together forming an updated OT 53, with its applicability extended to Levels 1 to 4. This OT does not cover whole area of physical protection, it deals only with interfaces between safety and security. Differently from the SR 46, previously covered unauthorized removal of nuclear or radioactive material is not explicitly covered by this OT. In this There are two challenges identified in this OT: either safety items damages by unauthorized activities (with two mechanisms, one dealing with lack of vigilance to prevent unauthorized access, another one dealing with deficiencies in design), another challenge is that the nuclear safety is potentially jeopardized by inadequate security measures. This OT thus deals with very important issue of existing interface between safety and security, which can be both positive and negative.

44. **Fig. 54. Physical protection of the plant.** OTs in fig. 53 and 54 were merged together in a single OT 53, and their applicability extended to Levels 1 to 4.

45. **Fig. 55. Safety evaluation of design.** This OT deals with the role of operating organization with independent verification of the design during manufacturing and construction of the plant. More specific provisions were added to this OT in order to underline the fact that the issue to be addressed by this OT should be independent verification of the design performed by or on behalf of future operating organization. One of the previous mechanisms (safety issues not addressed by the designer) was eliminated, since it does not belong to safety evaluation by the operating organization.

46. **Fig. 56. Achievement of quality.** Although not always explicitly stated it should be underlined that this OT formulates responsibility of the operating organization to ensure adequate quality of products and services delivered by external manufacturers or constructors. The terms manufacturers and constructors were more frequently used in this OT, but it should be clear that it is equivalent to the term suppliers (of products and services). Provisions in this OT were also partially reformulated with the attempt to improve formulations associated with some rearrangement of the provisions.

47. **Fig. 57. Verification of design and construction.** Mechanisms remained practically the same, just one of them (non-effective review by the regulatory body) was deleted since it is not the task by the operating organization. Nevertheless, this previous mechanism is reflected in the provisions to be performed by the operating organization. However, all provisions were developed practically from scratch to replace previous inconsistent bullets and to be more consistent with IAEA Safety Requirements for commissioning and operation (SSR-2/2). In SSR-2/2 it is also possible to find adequate details regarding the components of the commissioning programme.

48. **Fig. 58. Verification of design and construction.** This objective tree was previously developed for Level 4 only, but there was nothing specific for Level 4 in the provisions. In addition, for this general safety principle there is no reason to make strict difference between levels of defence. Due to these facts the fig. 58 was merged with the fig. 57, which is now formulated as OT 57 for Levels 1-4 of defence.

49. **Fig. 59. Validation of operating and functional test procedures.** Only minor changes were implemented in existing provisions for two originally formulated mechanisms. However, one new mechanism was added dealing with potential consequences impacting the equipment performance due to insufficient scope of validation of operating and functional test procedures. The main difference between the mechanism 59_2 and 59_3 should be that 59-2 deals with quality of validation, 59_3 with the scope of validation.

50. **Fig. 60. Collection of baseline data.** Compared to the previous version, there is only one mechanism left in this OT reflecting the potential impact of lacking baseline data. This mechanism also covers the previously considered in SR 46 second mechanism, specifically devoted to RPV, since it was realized that there is no strong reason to separate the RPV from the rest of the safety related equipment. In order to use the standard form of the objective trees, the previously used bulleted list was replaced by more consistent use of standard provisions in boxes.

51. **Fig. 61. Pre-operational adjustment of plant.** Relatively small changes were implemented in formulation of mechanisms and provisions. Two of previous provisions were shifted with small corrections from one mechanism to another.

52. **Fig. 62, Organization, responsibilities and staffing.** Significant changes in the level of details were implemented in this OT, with the use of experience of the author in PSRs of operating plants. This experience allowed identifying the relative significance of various provisions. It was realized that much more specific description of all provisions is needed to be formulated for the safety principle organization, responsibilities and staffing. This OT should be viewed in conjunction with other OT dealing with organizational matters, in particular OT 64, Conduct of operation, OT 64a, Conduct of operation - Lack or degradation of safety culture, OT 63, Safety review procedures, OT 73, Quality assurance in operation, OT 71, Feedback of operating experience.

53. **Fig. 63, Safety review procedures.** In addition to some improved formulations, main changes in this OT have been made to reflect all issues associated with communication between the operating organization and the regulatory body (one additional mechanism and 9 associated provisions for ensuring compliance with regulatory requirements were identified). Among means for independent safety review, the IAEA OSART missions and WANO peer review teams are specifically mentioned.

54. **Fig. 64, Conduct of operation.** Intentionally, there should be only minor changes in formulations of mechanisms and provisions. The OT is newly assigned to 4 levels of defence (originally it was only to level 1), since ineffective conduct of operation can affect all levels of defence at the same time. This OT also addresses the issue of operating procedures. However, it should be noted that the quality of procedures is addressed separately, in OT 67 -69 and 75, while the current OT deals just with approach to correct use of the procedures. From the provisions previously associated in the original OT with the mechanism “Lack of safety culture”, those associated with compliance with the rules and procedures were put separately under the mechanism “environment not conducive to safety”. The provisions associated with safety

culture are put separately and more comprehensively presented in a new page (OT 64a).

55. **Fig. 64a, Conduct of operation, Lack or degradation of safety culture.** This new OT is fully devoted to the challenge of lacking or degraded of safety culture. Five high level mechanisms were identified, with 36 associated provisions. The mechanism and provisions are based on the issues identified by IAEA in the document COMPENDIUM of IAEA Workshop for Senior Managers on Leadership and Culture for Safety, 28 September – 1 October 2015, EdF, Paris, France.

56. **Fig. 65, Training.** Mechanisms and provisions in the updated OT were better and more logically formulated and their order rearranged. The approach now is so that the OT 65 deals first with general provisions for training and afterword with special mechanisms and provisions for managers, for control room operators and for maintenance staff and. Separately another OT 75 is devoted to special features of training for accident management. General provisions for training are covered in a separate set of provisions, dealing separately with the scope (technical content) of training and with the execution (formal arrangements) of training.

57. **Fig. 66, Operational limits and conditions.** Applicability of this OT to levels of DiD has changed: originally OT was assigned to Levels 1-3, but correctly it should be assigned just to Level 1, since these are limits and conditions for normal operation. The original OT has been significantly modified. Number of mechanisms was reduced: instead of previous number of 6 mechanisms (which were however not related directly to OLCs, but rather to different problems in operation of a NPP, already covered by other OTs) there are now 3 mechanisms identified: inadequate scope, inadequate basis of OLCs, and violation of OLCs by the staff. The branches with a list of more specific provisions were connected to 2 previous more general provisions were replaced by standard provisions placed in boxes. Total number of provisions due to these modifications has been increased from previous 4 provisions to present 18 provisions.

58. **Fig. 67, Normal operating procedures.** The OT has been significantly modified. Three mechanisms were identified in this OT as compared to previous two mechanisms with the objective to cover more comprehensively all potential issues associated with normal operating procedures. These mechanisms are as follows: inadequate scope, inadequate quality and lack of adherence to approved normal operating procedures. Majority of provisions were newly written (added) with more specific formulation and some provisions were better formulated.

59. **Fig. 68, Emergency operating procedures.** This OT has been significantly rebuilt in order to cover more specifically the whole process of development and implementation of EOPs. In this OT under EOPs also abnormal operating procedures are considered. Individual mechanisms covered by this OT include the need to have sufficient basis for development of EOPs including relevant analytical support, to comply with adequate formal requirements applicable for the procedures, to have EOPs of adequate technical scope and quality and to have the EOPs verified and validated. A link is made in this OT to other safety

principle (and OTs) to cover the issue of adequate training on the use of EOPs. It is noted that EOPs cover also DEC-A of Level 4 conditions (prior to core melting) and they should be consistent with other set of procedures (guidelines) for accident management, i.e. with SAMG. It is also underlined that EOPs should cover not only accidents originated in the RCS, but also events in the SFP and in the systems for treatment of radioactive wastes. Since the EOPs cover also DEC-A Level 4 of defence, they should address also the use of mobile equipment.

60. **Fig. 69, Radiation protection procedures.** In this OT compared with its previous version a new set of provisions was added, associated with the need for availability of a comprehensive radiation protection programme. In addition, 3 new provisions were added to the radiation protection procedures, connected with potential exposure of contractors, with reporting of radiation doses to the regulatory body and with increased attention to exposures potentially received during special operational activities such as maintenance.

61. **Fig. 70, Engineering and technical support of operations.** In this OT, prime responsibility of operating organization for safety is further underlined in spite of the unavoidable external support. More attention is given to internal capability of the operating organization to organize and to ensure quality of the technical support provided by external organizations. Further on, the need for careful prioritization and planning of usually limited resources for technical support is addressed. More attention is also required for selection, auditing and verification of the quality of services and products in the area of nuclear safety, if delivered by external organizations.

62. **Fig. 71, Feedback of operating experience.** In the updated OT, differently from its previous version, for each of 6 individual mechanisms (one of the previous mechanisms was deleted as being unnecessarily too specific) its own string of provisions has been developed. Instead of previous 7 very generally formulated provisions, there are now about 25 provisions, specified separately for each individual mechanism.

63. **Fig. 72, Maintenance, testing and inspection.** In the updated OT, a new set of provisions was added regarding development of a comprehensive programme for maintenance, testing, surveillance and inspections. Other mechanisms remained basically unchanged and just few more specific provisions were added. The attention which needs to be devoted to the remote and mobile equipment is also addressed. The provisions in the updated OT are rearranged so that for each of the mechanisms there is a specific set of provisions.

64. **Fig. 73, Quality assurance in operation.** In the updated OT, instead of specific quality assurance provisions there are now more generally formulated provisions devoted to management systems, in accordance with the newly issued Safety Requirements on Leadership and Management for Safety, IAEA Safety Standards Series No. GSR Part 2. The mechanisms are subdivided into mechanisms associated with different general issues of the management system. Nevertheless there are still two mechanisms specifically addressing quality assurance of the classified equipment. In addition, new provisions are included in this OT, which are associated with keeping of key records important for r the

plant operational history and activities associated with maintenance of classified equipment.

65. **Fig. 74, Strategy for accident management.** The OT is significantly improved and extended, taking into account the latest version of updated IAEA Safety Requirements SSR-2/2 and Safety Guide NS-G-2.15 on severe accident management. In addition to the previous version of the OT, newly implemented in the OT are the requirements on systematic development of AM strategies, on comprehensive analytical support for the development of strategies and the most important strategies are explicitly listed. The issue of multiunit sites is also specifically addressed. Previously considered provisions related to formal adequacy of the strategies are partially covered by specific provisions placed under mechanisms 74_1 and 74_4. It should be however taken into account, that formal adequacy is not so important in development of strategies, it is very important for development of EOPs and SAMGs, as underlined by respective provisions in OT 75. Provisions of this OT apply also to mobile equipment used for execution of accident management actions under L4 condition.

66. **Fig. 75, Training and procedures for accident management.** Mechanisms and provisions in the updated OT were better and more logically formulated, and several more specific provisions were added to the existing mechanisms to provide more specific details. The provisions for training newly also include cases with accidents taking place in parallel on several units (multiunit accidents) and they also address the use of alterative and non-permanent (mobile) sources. As a new mechanism inadequate qualification of trainers with relevant provisions was added to this OT. The term multifunctional simulator is used to differentiate from full scope simulator. Multifunctional simulator is basically a PC with special means for presenting the results of calculations. Provisions of this OT apply also to mobile equipment used for execution of accident management actions under L4 condition.

67. **Fig. 76. Engineered features for accident management.** The updated OT is applicable for determination of provisions for management of accidents more severe than design basis accidents, i.e. for levels DEC-A and 4, including severe accidents. This OTs deal with general provisions to ensure availability of equipment and instrumentation under DEC conditions, without specifying the type of equipment or conditions; more detailed specifications of equipment and conditions is covered in previously discussed OTs, specific for residual heat removal and for protection of containment integrity. In addition to some better formulations, the most important changes in this OT is addressing the provisions regarding availability of sufficient equipment for management of multiunit accidents and availability of equipment resistant against natural external hazards more severe than design basis external hazards (beyond design basis events) with adequate margins. It should be underlined that the non-permanent equipment represents very important contribution to safety of the plants under DEC conditions, in particular of existing plants. Provisions of this OT partially apply also to non-permanent equipment used for execution of accident management actions under L4 condition.

68. **Fig. 77a. Emergency response facilities- Technical support centre.** TSC was

previously not included in the objective trees, while in accordance with GSR Part 7 and NS-G-2.15 it is a very important component of the emergency response facilities. Relevant provisions for TSC are similar to those of the emergency centre. However, there are some important differences. TSC is primarily providing support to the control rooms and therefore primarily belongs to Level 4 of defence, while other emergency response facilities belong to Level 5 of DiD. Of course, the TSC has an important role in emergency planning (i.e. also in Level 5), since TSC must communicate and provide important information to the emergency centre. Nevertheless, the coordination role in emergencies as reflected also in the objective trees is given to the emergency centres (see OT 77b), where the responsibility for overall coordination of the whole emergency response should be placed.

68. **Fig. 77b Emergency response facilities.** This OT deals with on-site emergency response facilities and arrangements. Compared to the original version in SR 46, the objective tree was significantly extended. In accordance with GSR Part 7, emergency response facilities include TSC, On-site Emergency Centre, Operational Centre, optionally also Off-site Emergency Centre. For TSC, which should belong to Level 4 a separate OT 77a was developed. Other previously listed components of the emergency response facilities should belong to Level 5. Two different functions of the emergency centre are covered by the OT: emergency centre as a place for providing logistical support to execution of emergency plans and emergency centre as a place for coordination of all activities of the on-site Emergency Response Organization (including coordination of the TSC). The issue of vulnerability of the emergency response facilities against post accident conditions and against external hazards is covered as an important factor to be verified.

69. **Fig. 78. Implementation of emergency plans.** The objective tree is focused on the duties of the operating organization to execute on-site emergency plans and to provide necessary inputs for execution of off-site emergency plans. It means that actions belonging to the off-site emergency plans which are usually under the responsibility of the local authorities or state authorities are not covered by this OT. As far as on-site emergency plans are concerned this OT is focused on the functions to be ensured, while the facilities needed for execution of emergency plans on the site (emergency response facilities) including adequate manpower and communication means are covered separately by OTs 77a and 77b.

REFERENCES

[1] IAEA Safety Glossary, Terminology Used in Nuclear Safety and Radiation Protection, 2016 Revision, IAEA, Vienna (2016).

[2] Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG-12, IAEA, Vienna (1999).

[3] Assessment of Defence in Depth for Nuclear Power Plants, Safety Report Series No. 46, IAEA, Vienna (2005).

[4] Site Evaluation for Nuclear Installations, Specific Safety Requirements, NS-R-3, Rev. 1, IAEA, Vienna (2016).

[5] Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1 Rev. 1, IAEA, Vienna (2016).

[6] Safety of Nuclear Power Plants: Commissioning and Operation, Specific Safety Requirements, SSR-2/2, Rev. 1, IAEA, Vienna (2016).

[7] IAEA Report on Human and Organizational Factors in Nuclear Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA, Vienna (2013).

[8] IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA, Vienna (2013).

[9] WENRA Safety Reference Levels for Existing Reactors – Update in Relation to Lessons Learned from TEPCO Fukushima Dai-ichi Accident, September 2014.

[10] Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Overview and Conclusions, ENSREG, April 2012.

[11] Stress Tests Performed on European Nuclear Power Plants as a Follow-up to the Fukushima Accident: Compilation of Recommendations and Suggestions from the Review of the European Stress Tests, ENSREG, July 2012.

[12] Implementation of Defence in Depth at Nuclear Power Plants - Lessons Learnt from the Fukushima Daiichi Accident, OECD/ NEA No. 7248, 2016.

[13] Fundamental Safety Principles, Safety Fundamentals No. SF-1, IAEA, Vienna (2006).

[14] Defence in Depth in Nuclear Safety, INSAG-10, IAEA, Vienna (1996).

[15] Considerations on the Application of the IAEA Safety Requirements for the Design of Nuclear Power Plants, IAEA-TECDOC-1791, IAEA, Vienna (2016).

[16] WENRA Reactor Safety Reference Levels, January 2008.

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 that are less frequent and more severe than anticipated operational occurrences .

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.

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.

cliff edge effect: in a nuclear power plant, is an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input.

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

design basis of a structure, system or component: The set of information that identifies conditions, needs and requirements necessary for the design of the structure, system or component including:

- the functions to be performed by a structure, system or component of a facility
- the conditions generated by operational states and accident conditions that the structure, system or component has to withstand
- the conditions generated by internal and external hazards that the structure, system or component has to withstand
- the acceptance criteria for the necessary capability, reliability, availability and functionality
- specific assumptions and design rules.

design extension conditions: Postulated accident conditions that are not considered for design basis accidents, but that are considered in the design process for the facility in accordance with best estimate methodology, and for which releases of radioactive

material are kept within acceptable limits.

early radioactive release: A release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time.

emergency operating procedures: plant specific procedures containing instructions to operating staff for implementing preventive accident management measures; EOPs typically contain all the preventive measures (for both DBAs and DECs).

emergency response facilities: For nuclear power plants, emergency response facilities (which are separate from the control room and the supplementary control room) include the technical support centre, the operational support centre and the emergency centre.

fundamental safety functions (or main safety functions) are: (a) Control of reactivity; (b) Removal of heat from the reactor and from the fuel store; (c) Confinement of radioactive material, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases.

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

large radioactivity release: A release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

margin, safety margin: The difference or ratio in physical units between the limiting value of an assigned parameter the surpassing of which leads to the failure of a structure, system or component, and the actual value of that parameter in the plant.

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

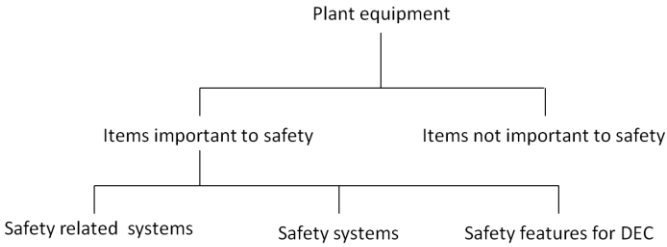
normal operation: Operation within specified operational limits and conditions. For a nuclear power plant, this includes starting, power operation, shutting down, shutdown, maintenance, testing and refuelling.

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.

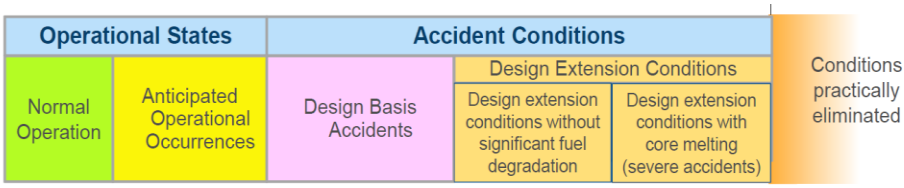
operational limits and conditions: A set of rules setting forth parameter limits, the functional capability and the performance levels of equipment and personnel approved by the regulatory body for safe operation of an authorized facility.

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

plant equipment:



plant states (considered in the design):



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.

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 completely or partially the mechanisms from occurring.

safe state: Plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable for a long time.

safety feature for design extension conditions: Item designed to perform a safety function or which has a safety function in design extension conditions.

single failure: A failure that results in the loss of capability of a system or component to perform its intended safety function(s) and any consequential failure(s) that result from it.

single failure criterion: A criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

safety function: A specific purpose that must be accomplished for safety for a facility or activity to prevent or to mitigate radiological consequences of normal operation, anticipated operational occurrences and accident conditions.

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

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. More specifically, validation of a computer code means assessment of the accuracy of values predicted by the code against relevant experimental data for the important phenomena expected to occur. Validation of EOPs or SAMGs means the proces of determining whether the actions specified in the EOPs or SAMGs can be executed by trained staff to manage emergency events.

verification: The process of determining whether the quality or performance of a product or service is as stated, as intended or as required. More specifically, verification of a computer code means review of source coding in relation to its description in the system code documentation. Validation of EOPs or SAMGs means the proces to confirm the correctness of a written procedure or guideline to ensure that technical and human factor concerns have been properly incorporated.