Draft Document on:

Assessment of Defence in Depth

for

Nuclear Power Plants considering Long Term Operation

Complement to IAEA Safety Reports Series No. 46

J. Hoehn

Consultant to the IAEA

FOREWORD

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

The historical development of the concept of defence in depth led to a general structure of multiple physical barriers and complementary means to protect the barriers themselves, the so-called levels of defence. Defence in depth is implemented through NPP lifetime to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the NPP and events initiated outside the NPP.

A comprehensive deterministic safety assessment approach was developed to consider the integrated contributions of overlapping provisions of different natures to the aim of defence in depth and published 2005 by the IAEA as Safety Reports Series No. 46: 'Assessment of defence in depth for NPPs'.

Currently, there is an increasing number of IAEA Member States giving high priority to continuing the operation of NPPs beyond the time frame of 30-40 years originally anticipated. To assist operators and regulators by appropriate guidance, the IAEA addressed the unique challenges associated with the long term operation and launched an Extrabudgetary Programme (EBP) on 'Safety Aspects of Long Term Operation of Water Moderated Reactors' in the period 2003-2006. The results of the EBP have been used by the IAEA to develop a Safety Reports Series on the technical aspects of 'Safe Long Term Operation of Nuclear Power Plants' based on the experience of MS that have successfully pursued long term operation to provide guidance to the needs expressed by MS who are preparing for long term operation as a reference when developing national programmes.

This report is to complement the IAEA Safety Reports Series No. 46 addressing the relevant aspects of defence in depth for plants considering long term operation.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

The IAEA Safety Reports Series on 'Safe Long Term Operation of Nuclear Power Plants' [1] developed and agreed upon by international experts fulfil the need expressed by MS for guidance, and is considered a precursor of an IAEA Safety Standard (Safety Guide) on long term operation (LTO) and therefore used as the technical basis for this report.

Long term operation of a nuclear power plant is operation beyond an established timeframe set forth by license term, design limits, standards, and/or regulations, etc. which has been justified by safety analyses considering life limiting processes and features for systems, structures, and components (SSCs).

Systematic assessment and verification of the implementation of defence in depth is performed throughout the lifetime of a NPP, being normally conducted by different organizations, within the frame of design development, licensing and regulatory purposes or operational safety management and needs to include LTO.

Therefore, it was desirable to complement IAEA Safety Reports Series No. 46 [2] developed for plants being currently operated by a technical report on plants' defence in depth to be operated beyond the original lifetime.

The information and references with respect to defence in depth assessment for plants being operated are applicable to this report and will be repeated here to the extent needed for LTO only; the details are provided in [2].

The evolution of safety according to recently published or being published Safety Standards related to LTO [10-14] is reflected in this report with the consequence that the relevant 'trees' as described in Section 3.2 have been modified in order to comply with, as the current requirements in design [8] and operation [10] don't have explicit references to LTO as well as to a common strategy. There has been also the need for some new trees like 'ageing management' because the corresponding safety principle is not addressed explicitly in [7].

This document is considered a self-standing document, i.e. the basic approach is repeated shortly with those 'trees' only indicating the levels of defence which might be affected by LTO

As the theoretical background of the approach is provided by [2] and this technical report complements the approach for plants considering LTO only, the presentation focuses on the practical aspects necessary to know on how to apply the approach.

This approach is considered a systematic way for reading the IAEA Safety Standards within the basic concept of defence in depth.

1.2. OBJECTIVE

The objective of this report is to provide practical guidance on how to assist MS considering application of LTO to their plants in reviewing defence in depth with respect to LTO and to consider necessary improvements on an engineering judgement basis.

The definition of defence in depth and the guidance on its implementation agreed upon and approved by international consensus has been laid down in a logical framework that can be used for self-assessments by NPP operators and for independent assessments by regulators or external reviewers. However, the assessment is not a replacement for the evaluations required by national or international standards. The assessment discussed here is considered to be a complement to regulatory evaluations and is intended to provide another perspective for deeper appreciation of the defence in depth capabilities of a NPP under LTO.

1.3. SCOPE

This report is considered a complement to [2] and therefore dealing with those defence in depth aspects influenced by LTO only.

According to the EBP [3] this report deals with technical aspects of LTO, i.e. aspects such as maintaining adequate competence, handling major organizational changes, economic feasibility, etc related to LTO as well as LTO feasibility at all [5] will not be addressed.

The assessment framework developed in this report is intended to be directly applicable to water moderated reactors.

While basically the assessment framework as published in [2] is applicable to all stages of NPP life from design to operation, the focus of this report is on the extension of the operational phase.

The report can also be used as a reference document containing comprehensive and balanced overview of provisions for all levels of defence and thus providing more clear understanding of the completeness of the concept of defence in depth with respect to LTO. The report, however, does not provide any guidance for evaluation of safety significance of omissions nor for prioritization of provisions.

1.4. STRUCTURE

The concept of defence in depth with underlining the importance of fulfillment of safety functions to achieve safety objectives for different levels of defence is presented in Section 2 in general and with focus on LTO.

The approach on how to assess defence in depth of NPPs is described shortly in Section 3 in general and with focus on LTO.

The specific aspects of defence in depth for plants considering LTO are discussed in Section 4.

Practical guidance is provided in Section 5 on how to apply the approach for plants considering LTO.

Conclusions are summarized in Section 6.

In the Annex there are the objective trees representing graphically on how the safety objectives of the different levels of defence for each relevant safety principle can be achieved by provisions in design and operation for plants considering LTO.

2. DEFENCE IN DEPTH CONSIDERING LONG TERM OPERATION

2.1. THE CONCEPT OF DEFENCE IN DEPTH

Safety Objectives [6,7] require that nuclear installations are designed and operated so as to keep all sources of radiation exposure under strict technical and administrative control.

The achievement of the Safety Objectives is driven by a comprehensive set of safety principles (SP) [7] resulting finally in measures to be taken to control 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. For NPPs the safety

objectives are ensured by fulfillment of the three fundamental safety functions (FSFs) [8]: *(1) Control of the reactivity, (2) Removal of heat from the fuel, and (3) Confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases* for all operational, accidental and post accidental conditions, within the design basis.

The extensive implementation of the strategy of defence in depth ensures that the FSFs are reliably achieved with sufficient margins to compensate for equipment failures and human errors. For the very unlikely accident situations beyond the design basis with significant degradation in the performance of the FSFs, additional measures are required to ensure that the consequences of significant releases of radioactive material are mitigated.

According to [9], defence in depth consists in 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, in normal operation, anticipated operational occurrences (AOO) and, for some barriers, in accidents at the NPP.

The concept of defence in depth, as applied to all safety activities, whether organizational, behavioural or design related, ensures that they are subject to overlapping provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the concept of defence in depth in a NPP provides a series of provisions at different levels of defence aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. Generally, several successive physical barriers for the confinement of radioactive material are put in place. 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.

Defence in depth is generally structured into five levels of defence [8,9]. Should one level fail, the subsequent level comes into play. The Table 1 summarizes the objectives of each one of the five levels and the correspondent essential means of achieving them. More details are provided in [8,9]. The levels are intended to be independent to the extent practicable. The general objective of defence in depth is to ensure that a single failure, whether equipment failure or human failure, at one level of defence, and even combinations of failures at more than one level of defence, would not propagate to jeopardize defence in depth at subsequent levels. The independence of different levels of defence is a key element in meeting this objective.

TABLE 1 - LEVELS OF DEFENCE IN DEPTH [9]

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

To ensure safety by avoiding failure of barriers against release of radioactive products and mitigate the consequences of their failure, the three FSFs shall be performed in operational states, during and following DBAs and to the extent practicable, in, during and following the considered NPP conditions beyond the DBA [8].

The FSFs can be considered a 'vital' equivalent of defence in depth and a measure of its appropriate implementation by provisions in design and operation as indicated by the underlying relevant safety principles. The aim of the provisions is to protect the barriers and to mitigate the consequences if the barriers are damaged. In general, the FSFs are ensured by means of control and safety systems and prepared staff actions [9].

In this way, the FSFs are defined to ensure proper response at the various times following any postulated initiating event (PIE), including those leading to BDBA. In terms of defence in depth, this means that provisions at Level 4 of defence may also reestablish the FSFs or at least strengthen their mitigative capabilities. Provisions at Level 5 of defence represent the mitigative features of the third FSF only.

Possible challenges to the FSFs are dealt with by the provisions established at a given level of defence which include such as inherent safety characteristics, safety margins, active and passive systems, procedures, operator actions, organizational measures, safety culture aspects. All mechanisms that can challenge the performance of the FSFs should be 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.

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, it will be the subsequent level that comes into play. As the objective of the first level of defence is the prevention of abnormal operation and system failures, if it fails, an initiating event comes into play. It can happen if either provisions at Level 1 were not efficient enough or a certain mechanism was not considered in establishing provisions at Level 1. Then the second level of defence will detect the failures to avoid or control the abnormal operation. Should the second level fail, the third level ensures that the FSFs are further performed by activating specific safety systems and other safety features, limiting the consequences for the design basis accidents. Should the third level fail, the fourth level limits accident progression by means of accident management measures, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last objective of the fifth level of defence is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

2.2. LONG TERM OPERATION AND DEFENCE IN DEPTH

The concepts of defence in depth and safety culture have served the nuclear power industry well as a basic philosophy for the safe design and operation of nuclear power plants currently operated as well as for future technologies.

An extension of operation beyond an established timeframe of 30-40 years originally anticipated requires maintaining or even strengthening plants' defence in depth for the period of LTO to ensure safe operation till the extended end of life; i.e. the intended safety functions will be maintained consistent with the current regulatory requirements for the period of LTO. Since NPPs were mostly designed and built to conservative standards with considerable remaining safety margins as we nowadays know and required that NPPs be operated in a foresight manner provide an profound basis for continuing operation beyond the initial established timeframe. However, NPPs experience time dependent changes which might result into gradual deterioration and degradation of the physical characteristics of SSCs so that their intended functioning may be endangered in case of demand. The resulting consequence can be a weakening of plants' defence in depth either by

impacting the physical barriers or the levels of defence or both. Further to that, during the initial period of operation there is a potential that plants can experience not anticipated changes in deterioration processes or new ones not expected at the time of design. That means, even in case of conservative operation of plants designed with significant margins there is a need to assess the effectiveness of plants' built in defence in depth for LTO. During the period of extended operation the design basis has to be continuously updated to be sure that no new PIEs arise or will be properly addressed by the design basis. Age related degradation of the physical characteristics of SSCs important to safety is one of the possible causes for events. Also the engineered safety systems and their support features must be functioning as intended to cope with DBAs and to mitigate events going beyond.

That means that all barriers and levels of protection of plants' defence in depth might be challenged during LTO either due to undetected changes of SSC characteristics before or within the LTO period. Therefore, maintaining defence in depth is properly achieved by strict performance of plant operation according to national standards and best international practice so that time dependent changes could early be detected and properly addressed to avoid any diminishing.

Section 4 will in general describe in more detail which of the elements of defence in depth might be affected by LTO so that strengthening through corresponding provisions is advisable.

3. APPROACH FOR INVENTORYING DEFENCE IN DEPTH FOR PLANTS CONSIDERING LONG TERM OPERATION

The approach for inventorying defence in depth for operating plants is described in detail in [2] and will here be repeated in short before the specifics for LTO are discussed.

3.1. THE APPROACH

Identification of all ways that can impact the performance of a FSF as well as the variety of possibilities how to avoid this impact for each level of defence is an essential task in the development of the logical framework for inventorying the defence in depth capabilities of a NPP. For the development, it is worthy to summarize the following reference concepts:

- To ensure safety, the three **FSFs** - and also their derived or subsidiary safety functions (SFs) - should be performed in all operational states, and accident conditions including normal operation, anticipated operational occurrences, design basis accidents and some beyond design basis conditions at any stage of the lifetime of the plant including LTO.
- The defence in depth concept involves **multiple physical barriers** against the release of radioactive material and **several levels of defence**, which include organizational, behavioural and design measures (provisions)**.** The focus of this report related to LTO is on technical means.
- Each level of defence has its specific **objectives** including protection of relevant barriers and its **essential means** of achieving it. To ensure the objective of each level of defence, all FSFs - and derived/subsidiary SFs - relevant for this level need to be performed.
- **Challenges** are generalized mechanims, processes or circumstances/conditions that may impact the intended performance of SFs. The nature of challenges is characterized by the safety principle which contributes to the achievement of the objective through performance of safety

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

- **Mechanisms** are more specific processes or situations whose consequences might create challenges to the performance of FSFs/SFs.
- To prevent any mechanisms to take place, **provisions** (means, measures) can be established such as inherent NPP safety characteristics, safety margins, system design features and operational as well as organizational measures, which can support the performance of FSFs/SFs.

A framework for inventorying the defence in depth capabilities should screen for each level of defence all the challenges and mechanisms, to identify possible safety provisions including essential means for achieving the correspondent objectives of each level (Table 1) as indicated by the relevant safety principles. It should also identify the contribution of the provisions to the performance of the FSFs/SFs.

The logical framework described above may be graphically depicted in terms of a '**objective tree**' such as shown in Figure 1. 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 barriers to be protected against release of radioactive materials. Below this, there is a list of Fundamental Safety Functions or derived Safety Functions (FSFs/SFs) which need to be maintained to achieve both the objectives and the protection of 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 (fuel matrix, cladding and pressure boundary of the RCS) through performance of FSFs/SFs. For Level 3, the objective is to control the accidents within the design basis. For these accidents it is required to limit damage of the first two barriers (fuel matrix and cladding), to avoid consequential damage of the reactor coolant system (RCS) pressure boundary and to avoid any damage of the reactor containment. The performance of FSFs/SFs might be impacted by challenges, which need to be determined as mentioned above. On the next lower level of the tree there are several mechanisms listed that can give rise to the challenges. Under each of the mechanism there is the listing of possible provisions that should be available to prevent the mechanisms to occur and avoid challenges to the subsidiary SF from arising.

The top down approach, i.e. from the safety objectives of each level of defence down through challenges and mechanisms and in the end down to the provisions is considered an appropriate way to develop the objective trees in the most comprehensive way.

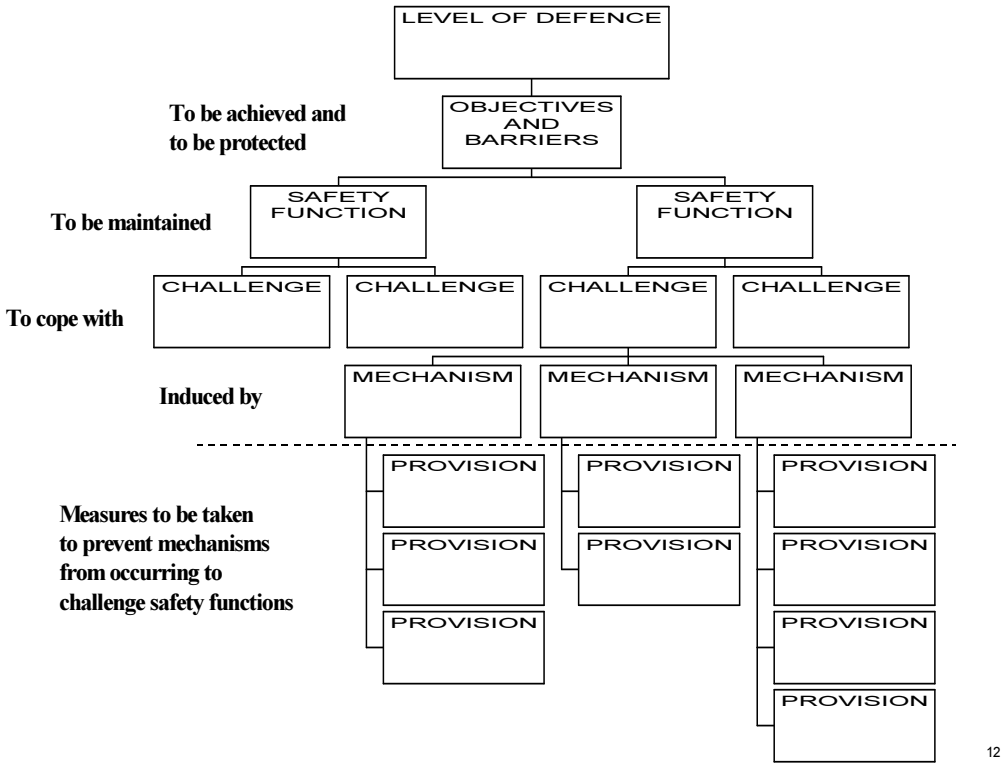


FIG. 1. Logic structure of objective trees [2]

The main objective of the method presented in this document is inventorying the defence in depth capabilities, i.e. provisions implemented during any stage of the lifetime of the plant including LTO. Its essential attribute therefore would be the completeness of the list of mechanisms grouped into generalized challenges endangering the fulfillment of FSFs/SFs and sufficient comprehensiveness of the list of safety provisions aimed at preventing those mechanisms to take place.

The defence in depth capabilities of a plant are established by means of the provisions that prevent mechanisms or combinations of them from occurring that might challenge the FSF/SF performance. It is intended that the list of provisions is provided as comprehensive as possible. A combination of expert judgement, the IAEA reference report INSAG-12 [7], the IAEA Safety Standards [8,10] and related ones has been used to provide guidance on the comprehensive selection of the main challenges, mechanisms and provisions for each of the safety functions to be performed.

INSAGs devised graphical depiction of the elements of defence in depth and safety culture was slightly modified by separating the safety principles for equipment qualification and ageing management over the life cycle including LTO of a NPP [7] and shown in Fig. 2.

Across the horizontal axis of the figure are listed the stages of life of a NPP beginning with design, progressing through construction and operation. NPP decommissioning is beyond the scope of the present report. 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 there are listed the major features (elements) that contribute to defence in depth during the NPP lifetime including LTO. The elements listed in the figure include features of NPP siting, design, manufacturing and construction, and commissioning as well as features of the organization and operation of the NPP. Each of the elements is representative of a specific safety principle discussed in detail in [7]. Lines connecting the safety principles in Fig. 2 are indicating interrelation among the safety principles.

Safety principles described in [7] are commonly shared safety concepts stating how to achieve safety objectives at different levels of defence in depth. The safety principles of course do not guarantee that NPPs will be absolutely free of risk, but, when the principles are adequately implemented, the NPPs should be very safe. The safety principles do not differentiate between new and existing NPPs considering naturally differences in level of implementation.

It can be seen from Figure 2, that many safety principles contributing to defence in depth have an influence on more than one level of defence. For example 'Maintenance, testing and inspection' at the stage of operation has an impact across Levels 1 to 4 since it ensures that the levels of reliability and availability of all SSCs that have a bearing on safety remain in accordance with the assumptions and intent of design and that plant safety is not adversely affected after the commencement of operation.

The concept of defence in depth relies on a high degree of independence between the defences, and ideally between the levels of defence. In practice, however, some sort of interdependencies exist as a result of the pervading nature of several of the principles. Of course, formal assignment of one safety principle to several levels of defence in depth does not necessarily mean lack of independence between the different levels. This is due to the fact that the same safety principle is typically applied to different systems, different manufacturers, different NPP staff and different NPP conditions and not necessarily the same weakness propagates through all of them. 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 such potential deficiencies.

Of course, certain amount of subjectivism in assignment of safety principles can not be avoided. However, this fact is not essential for comprehensiveness of the objective trees, since safety principles are one of various sources of information for development of the approach.

3.2. OBJECTIVE TREES

The objective trees developed for LTO are presented in the Annex for all relevant levels of defence based on the approach described in previous sections. The trees themselves intend to be self-explanatory, i.e. no additional text is provided to explain the challenges, mechanisms and provisions. Further guidance can be found in [7,8,10].

Following comments on the formulation of provisions in the objective trees can be provided:

- Impacts of mechanisms should be first analyzed by adequate tools, even this is not always explicitly expressed in the provisions. Selection and implementation of an appropriate measure should always be based on results of such analysis. Lack of analysis in particular for those safety principles, which are common to several levels of defence can easily represent a source for weakening of the defence in depth concept.
- The objective trees intend to provide a comprehensive list of possible options for provisions. Not necessarily all of them are to be implemented in parallel. The NPP operator based on insights from the approach is in a better position to decide upon implementation of the provisions, including any modified or additional provision.

- The provisions provided in the objective trees were mainly derived from the text of IAEA and INSAG safety principles, IAEA Safety Standards and complemented by relevant technical reports. Various types of provisions include: inherent plant safety features, systems, procedures, training of staff, safety management and safety culture measures.
- For safety principles common to several levels of defence, different ways of development of objective trees were used. If substantial difference in formulation of provisions for different levels were identified than a separate objective tree was developed for each of the respective levels. Otherwise, the same objective tree can simply be used for each of the relevant levels. However, it should be clear for such cases that the objectives and means at different levels are different and the same objective tree applies at least to different plant systems, i.e. NPP process systems, control systems, and safety systems as well as those established for accident mitigation.

4. STRENGTHENING DEFENCE IN DEPTH FOR PLANTS CONSIDERING LONG TERM OPERATION

The approach to strengthen defence in depth for plants considering LTO consists of two major steps:

1. To confirm that the plants considering LTO are currently operated with a 'healthy' defence in depth, i.e. current plants' operation is performed with conditions of both physical barriers and levels of defence that comply with national requirements and international good practice on how adequate defence in depth should be established. This could mean that some elements of defence in depth need to be qualified in case they have been identified as to be not adequate even for current operation.
   As example, the environmental qualification (EQ) of the mechanical and electrical equipment should be part of the design basis. Although the EQ has become part of regulatory requirements in many MS, the EQ programme are not always established and implemented.
2. To strengthen those aspects of defence in depth with respect to physical barriers and levels of defence which are in the centre of age related degradation for the time of continued operation beyond the design life. This could mean to reinforce existing defence in depth features already implemented to take into consideration LTO or to add additional provisions to address new challenges specific to LTO.
   In this sense, EQ programmes based on national/international standards are considered preconditions for LTO and the EQ status of SSCs is demonstrated to be valid for the LTO period while ageing effects will be managed effectively.

   The IAEA Safety Reports Series on 'Safe Long Term Operation of Nuclear Power Plants' [1] based on the Final Programme Report (FPR) of the corresponding EBP [3] provide general insights into strengthening defence in depth of plants considering LTO. The results of the FPR [3] formulated as recommendations indicate provisions for implementation in order to avoid mechanisms which could challenge the performance of SSCs' safety functions. That means, the relevant safety principles and derived objective trees have to be considered broader to cope also with the threat to safety affected by LTO. Therefore, relevant provisions should be implemented to strengthen and maintain 'healthy' defence in depth for plants considering LTO with respect to the main elements of defence in depth as follows:

   - The 3rd and 4th physical barrier (of water moderated reactors) among the components and structures important to safety deserve special attention for plants considering LTO. Reactor coolant boundary and confinement

are those barriers which can not easily or even not be replaced in case of inadmissible time dependent degradation. Therefore, existing or new provisions for Levels 1 to 3 are recommended to maintain the integrity of these barriers and to ensure their intended safety function even for the period of LTO. The objective trees for reactor coolant system integrity (Figs. 3 and 4) and protection of containment structure (Fig. 5) indicate provisions recommended for plants considering LTO; i.e. in particular for Level 2 such as supplementary RPV surveillance programme and revalidation of relevant plant specific safety analyses that involve time limited assumptions (TLAAs) and Level 3 such as regulatory requirements on maintenance, ISI and ageing management (AM) specific to structures, respectively.

- The focus on levels of defence for plants considering LTO is on the Levels 1 to 3 and even 4 mainly emphasizing existing provisions and complementing them for the period of beyond current plant operation. The majority of these provisions refer to safety principles applicable to Levels 1 to 4 addressing generic means/measures to ensure adequate defence in depth for plants considering LTO.

  The most prominent example is the safety principle on maintenance, testing and inspection (SP(305) according to [7]) belonging to the existing plant programmes for managing ageing during current plant operation and considered preconditions for LTO. Maintenance, testing, surveillance and inspection (MTS&I) of SSCs important to safety according to [8,10] require measures to ensure safe plant operation of process systems (Level 1), control systems (Level 2), safety systems (Level 3) and their use to mitigate accidents beyond DBA (Level 4). The corresponding provisions/means/measures of currently operated plants such as indicated in Fig. 18 are not only emphasized as important also for the period of LTO. In addition to that it is recommended - provided by examples, that:

  Maintenance programme for the structures in the scope of LTO should no longer be based on standard preventive maintenance (Level 1) but oriented to the monitoring of its effectiveness and therefore be of the 'condition based' type (Levels 3,4).

  Surveillance and monitoring programme established in currently operated plants to verify the integrity of all physical barriers and functioning of safety systems and availability of safety support features by means of mainly Levels 2 and 3. This is emphasized also for the period of LTO and complemented by special attention to electric cables and their mechanical, electrical, and physical/chemical properties through implementation of controlled ageing programme addressing Levels 1 to 4 too.

  ISI methods mostly defined by deterministic approaches should be complemented and increasingly adopted and developed for LTO by a risk informed (RI-SI) approach which use contribution to core damage frequency, consequence of failure and an assessment of degradation to define the scope and period of ISI. These and other provisions indicated in Fig. 19 strengthen all first four levels of defence but Levels 2 and 3 in particular.

For this report it is of second priority to indicate the application of SPs and their provisions caused by LTO during the main stages of a plant, i.e. siting, design, construction, …, operation, etc. Although the plants to be considered for LTO were designed for design life the necessary provisions for LTO have been realized during operation and assigned accordingly to the relevant levels of defence.

An outcome of the EBP [3] is that about one third of the recommendations refer to developments, they are taken as granted in the trees, such as the development of criteria.

5. PRACTICAL GUIDANCE FOR APPLYING THE APPROACH

In case, defence in depth for plants currently operated needs to be assessed then the full approach as provided by [2] has to be applied and the safety principles indicated in Fig. 2 to be impacted by LTO should be replaced by those addressed in this report.

This report and particularly this section is intended to provide practical guidance on how to apply the approach to evaluate plants' defence in depth for LTO, to judge the weaknesses of this universal concept for ensuring safety and to get suggestions and recommendations which provisions have to be implemented to strengthen defence in depth. It is provided, that defence in depth for the initial period of operation is well established and that an evaluation for the extended period of operation is requested.

The outcome of the EBP [1, 3] has been used to identify those areas/activities in plant design and operation which are expected to be impacted by LTO, i.e. mainly by time dependent changes of SSC characteristics and their potential impact on the demanded safety function performance. The relevant safety principles have been selected from [2] and reconsidered for LTO. Due to the evolution of safety during the last decade reflected by recently revised and new developed IAEA Safety Standards, mainly Safety Guides, the structure of trees was accordingly modified to reflect these trends in ensuring safety. There was one safety principle which was found to be so important that a separate treatment is indicated compared with [7] where ageing is still included in the safety principle on equipment qualification. The recent development of a Safety Guide on 'Ageing management for NPPs' [11] might justify this extension. Therefore, the objective trees and their provisions provided in the Appendix and depicted by boxes with single frame border lines are always applicable, those with double frame border lines and italic text addressing LTO related ones. Preconditions [1] are those plant programmes impacting all structures and components of plants in the initial period of operation and beyond and therefore called preconditions in a narrow sense such as maintenance, equipment qualification, etc.

In order to assess plants' defence in depth for LTO the objective trees provided in the Annex of this report are applied top-down. Starting the safety principle with the safety functions to be performed in order to achieve the corresponding safety objective. Next you will get an information on the challenges which might affect the safety function performance caused by the mechanisms below. To avoid the mechanisms to occur the provisions in design and operation below the broken line have to be in place to ensure proper defence in depth for the levels of defence indicated including the physical barriers to be protected for the corresponding levels of defence. For the plant under consideration this top-down application of the approach might indicate potential weaknesses in design and operation taking into consideration that the provisions indicated in the trees are recommended by the IAEA Safety Standards which must not fully comply with national Standards and therefore a judgement is necessary to decide on appropriate provisions concerning existing ones or those which need to be implemented.

Application of the approach from the bottom to the top indicates strengthening defence in depth through the implementation of appropriate provisions mechanisms might be avoided to occur and the challenge the safety function performance.

Each safety principle is assigned to one or more levels of defence. In case several levels of defence are represented by one tree, then no substantial difference in formulation of provisions for the different levels of defence were identified; otherwise separate objective trees were developed such as for ageing management. One should keep in mind that the objectives and means at different levels are different and that the same objective tree applies to different SSCs.

This application of the approach is a systematic reading of IAEA Safety Standards within the concept of defence in depth starting with safety principles stating on how safety objectives are to be achieved, derived requirements and recommendations on how the requirements should be fulfilled according to best international practice. The adoption of national standards is the responsibility of customers.

5. CONCLUSIONS

Defence in depth is expected to remain an essential strategy of nuclear safety for existing NPPs considering LTO.

The screening approach by means of objective trees offers a user friendly tool for determining strengths and weaknesses of defence in depth at a specific NPP. The approach is consistent with IAEA Safety Standards and INSAG documents. Safety is never absolute, but the approach defined here is intended to be comprehensive, in that INSAG have stated that when the safety principles [7] are adequately applied to a NPP it should be very safe. It has not been the aim in the development of this approach to discover any additional safety provisions that are not identified already in IAEA publications. Demonstration of defence in depth in a comprehensive and systematic way may provide reassurance for the NPP 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.

The approach is primarily intended to facilitate self-assessment of defence in depth by the NPP operators, although it can also be used by regulators or by independent reviewers. The approach has been developed to be as complete as possible, but it is sufficiently flexible to allow inclusion of other mechanisms and provisions related to specific NPP types or identified in national standards.

The approach is considered also as an appropriate tool for presentation of the progress made in strengthening defence in depth. In particular, NPP operators are encouraged to repeat in full the approach after completion of a major safety improvement programme, a substantial reorganization in the NPP or even in case LTO is considered.

Naturally, there are some limitations of the approach described in this report.

The approach does not include any quantification of the extent of defence in depth at a NPP or prioritization of provisions of defence. It is intended only for screening, i.e. for determination of both strengths and weaknesses for which provision should be considered.

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

There is no consideration in this approach on side effects of increased complexity and operational difficulties caused by 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. Therefore a regular iteration process is required; a PSA study is an appropriate tool for such process.

As soon as LTO is addressed by IAEA Safety Standards a revision of this document is recommended to cover in a comprehensive manner all relevant aspects of LTO going beyond the technical ones as addressed here.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Reports Series on Safe Long Term Operation of Nuclear Power Plants, Draft 250507, Vienna, 2007

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

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Final Report of the Programme on Safety Aspects of Long Term Operation of Water Moderated Reactors: Recommendations on the scope and content of programmes for safe long term operation, IAEA-EBP-SALTO, Vienna, submitted to publication, May 2007

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safe Management of the Operating Lifetimes of Nuclear Power Plants, INSAG-14, A report by the International Nuclear Safety Advisory Group, Vienna, 1999.

[5] OECD 2006 Nuclear Power Plant Life Management and Longer-term Operation, NEA No. 6105

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, IAEA Safety Series No. 110, Safety Fundamentals, Vienna, 1993.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev.1, INSAG-12, A report by the International Nuclear Safety Advisory Group, Vienna, 1999.

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

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, INSAG-10, A report by the International Nuclear Safety Advisory Group, Vienna, 1996.

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

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide DS382 Draft 2a, Vienna, as of April 17 2007

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. NS-G-2.6, Vienna, 2002

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Equipment Qualification in Operational Nuclear Power Plants: Upgrading, Preserving and Reviewing, Safety Reports Series No. 3, Vienna, 1998

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. NS-G-1.2, Vienna, 2001

GLOSSARY

Ageing
General physical, chemical and/or biological processes in which characteristics of systems, structures, or components are subject to time dependent changes (often degradation) arising from their service or storage conditions.

Ageing Management (AM)
Engineering, operations and maintenance actions to control within acceptable limits ageing degradation and wear out of systems, structures, or components (SSCs).

Ageing Management Programme (AMP)
Ageing management programme is broadly defined as any programme or activity that adequately manages the effects of ageing on SSCs. Maintenance programme, chemistry programme, ISI or surveillance activities, etc. are considered AMPs as well as those meeting the following generic attributes:

1. A defined programme scope
2. Identification of preventive actions or parameters to be monitored or inspected
3. Detection of ageing degradation/effects
4. Monitoring and trending including frequency and methodologies
5. Acceptance criteria
6. Corrective actions if a component fail to meet the acceptance criteria
7. Confirmation that required actions have been taken
8. Administrative controls that document the programme's implementation and actions taken
9. Operating experience feedback

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

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

Design life
The period of time during which a facility or component is expected to perform according to the technical specifications to which it was produced.

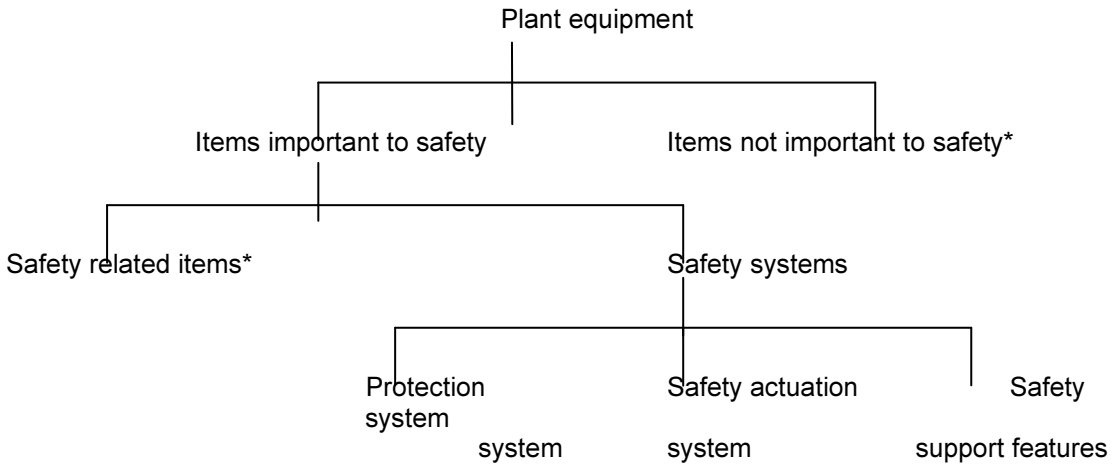
Items Important to Safety
See nuclear power plant equipment

Licensing Basis
The collection of documents or technical criteria that provides the basis upon which the regulatory body issues a license for the siting, design, construction, commissioning, operation or decommissioning of a nuclear installation.

Long Term Operation (LTO)
Nuclear power plant (NPP) operation beyond an established timeframe set forth by license term, design limits, standards, and/or regulations, etc., which has been justified by safety assessment considering life-limiting processes and features for systems, structures, and components(SSCs).

Plant programmes (existing plant programmes, NPP programmes)
Planned series of events or set of related long term measures or activities which are performed and conducted in certain order or manner to achieve the purpose for which a plant was constructed. For a nuclear power plant, this includes maintenance, refueling, in-service inspection and other associated activities.

Nuclear Power Plant Equipment
The diagram below demonstrates classification of equipments of a NPP according to IAEA Safety Standards.



* In this context, an "item' is a structure, system or component.

Items important to safety include:

- SSCs whose malfunction or failure could lead to undue radiation exposure of site personnel or members of the public;
- SSCs that prevent anticipated operational occurrences from leading to accident conditions; and
- Features that are provided to mitigate the consequences of malfunction or failure of SSCs.

Protection system: A system that monitors the operation of a reactor, and on sensing an abnormal condition, automatically initiates actions to prevent an unsafe or potentially unsafe condition. The "system" in this case encompasses all electrical and mechanical devices and circuitry, from sensors to actuation device input terminals.
Safety actuation system: The collection of equipment required to accomplish the necessary safety actions when initiated by the protection system.
Safety related item: An item important to safety that is not part of a safety system.
Safety system: A system important to safety, provided to ensure the safe shutdown of the reactor or the residual heat removal from the core, or to limit the consequences of anticipated operational occurrences and design basis accidents. Safety systems consist of the protection system, the safety actuation systems, and the safety system support features. Components of safety systems may be provided solely to perform safety functions or may perform safety functions in some nuclear power plant operational states and non-safety functions in other operational states.
Safety system support features: The collection of equipment that provides services such as cooling, lubrication, and energy supply required by the protection system and the safety actuation systems.

Periodic Safety Review (PSR)
A systematic reassessment of the safety of a nuclear power plant carried out at regular intervals to deal with the cumulative effects of ageing, modifications, operating experience, technical developments and site aspects that are aimed at ensuring a high level of safety throughout plant service life.

Qualified life
Period for which a SSC has been demonstrated, through testing, analysis or experience, to be capable of functioning within acceptance criteria during specified operating conditions while retaining the ability to perform its safety function in a design basis accident or earthquake.

Safety limit
The safety limit is a critical value of an assigned parameter associated with the failure of a system or a component (e.g., loss of coolable core geometry).

SCs
Structures or Components

SSCs
Systems, Structures or Components

Time Limited Ageing Analysis (TLAAs)/Residual Life Assessment (RLA)
NPP specific calculations and safety analyses that are based on an explicitly assumed time of plant operation or design life

Challenges

Generalized mechanisms, processes or circumstances (conditions) that may impact the intended performance of safety functions; a set of mechanisms having consequences which are similar in nature

Fundamental safety functions
1. control of the reactivity, 2. removal of heat from the fuel, 3. confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

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

Mechanism
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

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) list of provisions in design and operation preventing the mechanism to occur

Operational limits and conditions

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

Operational states

States defined under normal operation and anticipated operational occurrences.

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

ANNEX

The following safety principles according to [7] indicated by 'grey' boxes in Fig. 2 have been identified to be influenced by LTO. The corresponding 'objective trees' were slightly modified compared with those of [7] to reflect the current status of IAEA Safety Standards. In parenthesis the corresponding safety principles according to [7] are provided; the SPs of equipment qualification and maintenance, testing and inspection need two figures for presentation indicated by eg. (182/1) and (182/2).

The safety principles (SP) are represented by objective trees: provisions applicable during current operation are indicated by boxes with single frame border lines, those with double frame border lines and italic text are related to LTO. According to Section 4 the objective trees of safety principles affected by LTO can be grouped as follows:

Objective trees for levels of defence to protect the physical barriers:

Fig. 3 - SP: Reactor coolant system integrity (209) incl. LTO - Level 1 of Defence
Fig. 4 - SP: Reactor coolant system integrity (209) incl. LTO - Level 2 of Defence

Fig. 5 - SP: Protection of containment structure (221) incl. LTO - Level 3 of Defence
Fig. 6 - SP: Protection of containment structure (221) incl. LTO - Level 4 of Defence

Objective trees for levels of defence to achieve the corresponding objectives:

Fig. 7 - SP: Ageing management (184) incl. LTO - Level 1 of Defence
Fig. 8 - SP: Ageing management (184) incl. LTO - Level 2 of Defence
Fig. 9 - SP: Ageing management (184) incl. LTO - Level 3 of Defence

Fig.10 - SP: Equipment qualification (EQ) (182/1) incl. LTO - Level 3 of Defence
Fig.11 - SP: Equipment qualification (EQ) (182/2) incl. LTO - Level 3 of Defence

Fig.12 - SP: Reliability targets (174) incl. LTO - Level 3 of Defence

Fig.13 - SP: Monitoring of plant safety status (227) incl. LTO - Levels 1,2 of Defence

Fig.14 - SP: Training (278) incl. LTO - Levels 1,2,3 of Defence

Fig.15 - SP: Design management (150) incl. LTO - Levels 1,2,3,4 of Defence

Fig.16 - SP: General basis for design (158) incl. LTO - Levels 1,2,3,4 of Defence

Fig.17 - SP: Feedback of operating experience (299) incl. LTO - Levels 1,2,3,4 of Defence

Fig.18 - SP: Maintenance, testing and inspection (305/1) incl. LTO - Levels 1,2,3,4 of Defence
Fig.19 - SP: Maintenance, testing and inspection (305/2) incl. LTO - Levels 1,2,3,4 of Defence

Fig.20 - SP: Safety review procedures (269) incl. LTO - Levels 1,2,3,4 of Defence

Fig.21 - SP: Inspectability of safety equipment (186) incl. LTO - Levels 1,2,3,4 of Defence

Fig.22 - SP: Collecting baseline data (260) incl. LTO - Levels 1,2,3,4 of Defence

FIG. 3. Objective Tree for Level 1 of Defence
SAFETY PRINCIPLE: Reactor coolant system integrity (209) incl. LTO

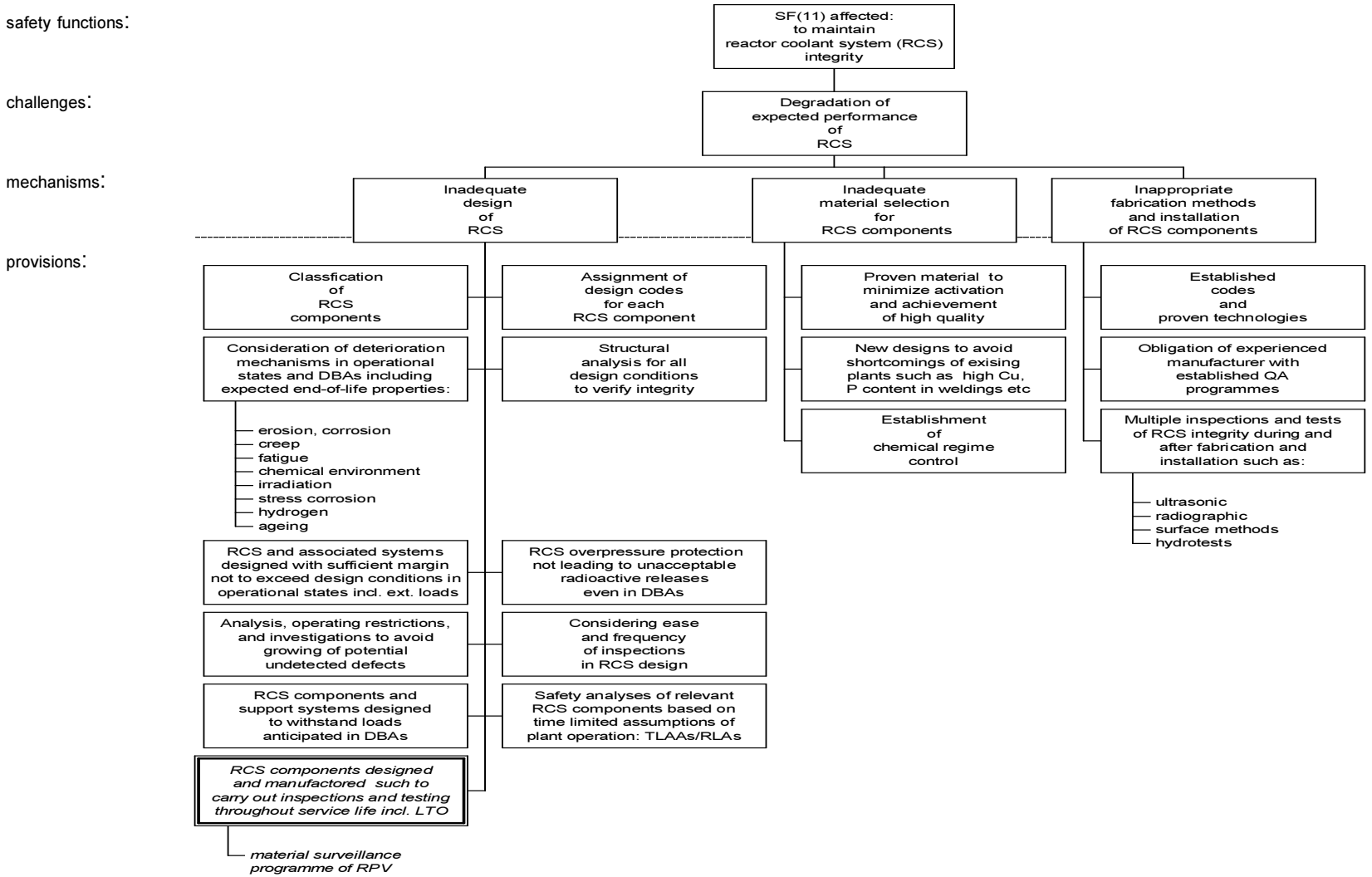


FIG. 4. Objective Tree for Level 1 of Defence
SAFETY PRINCIPLE: Reactor coolant system integrity (209) incl. LTO

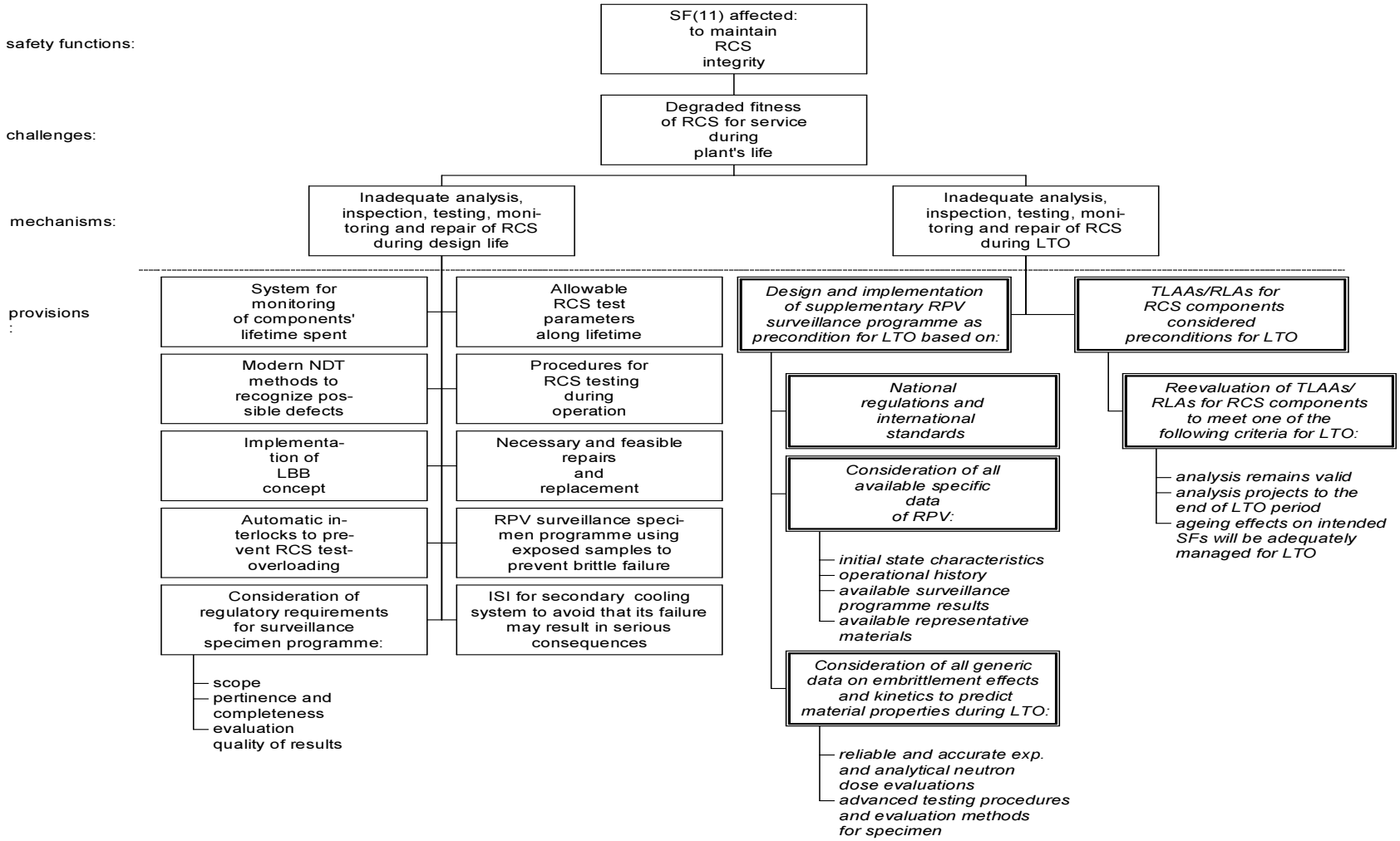


FIG. 5 Objective Tree for Level 3 of Defence
SAFETY PRINCIPLE: Protection of containment structure (221) incl. LTO

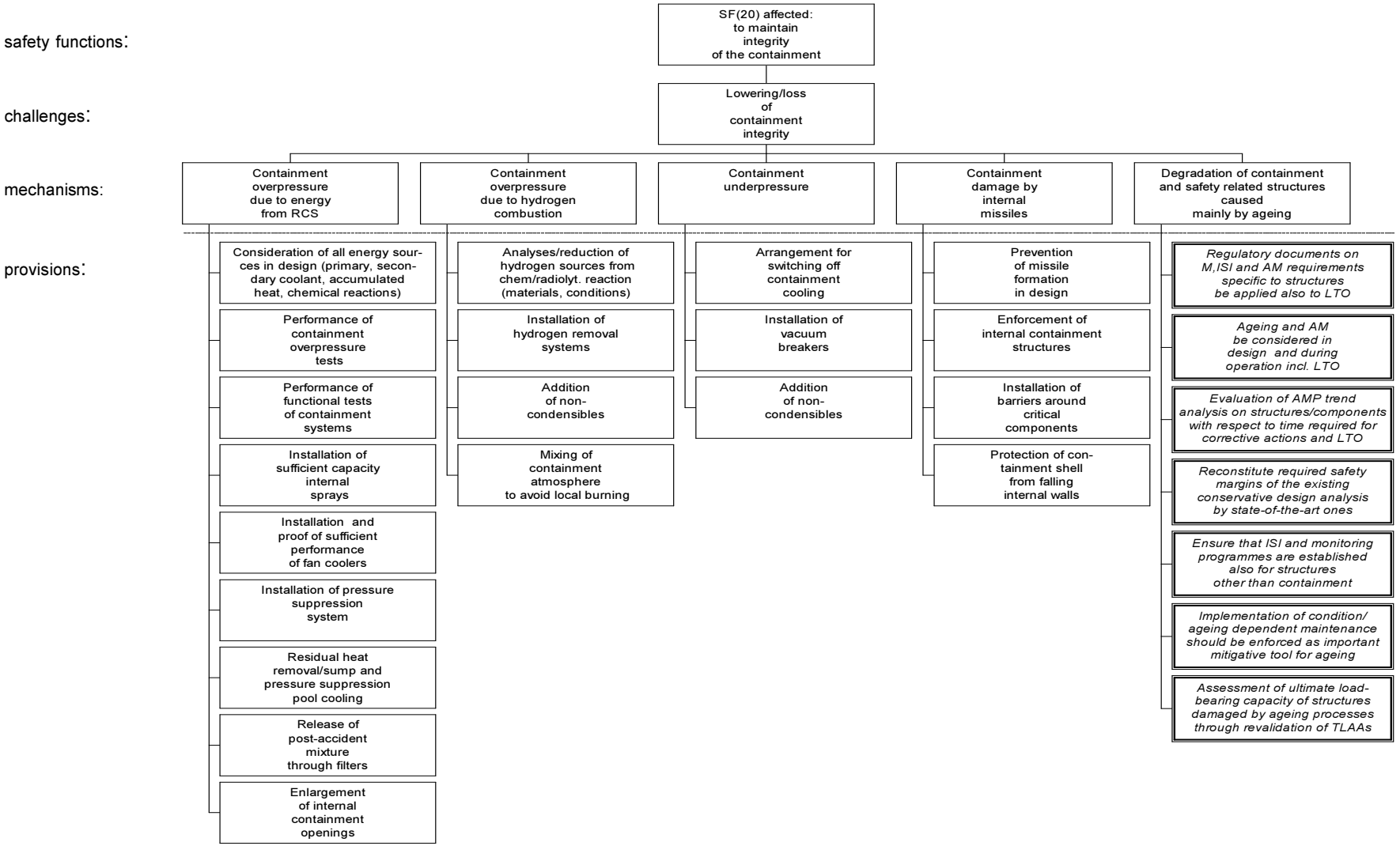


FIG. 6 Objective Tree for Level 4 of Defence
SAFETY PRINCIPLE: Protection of containment structure (221) incl. LTO

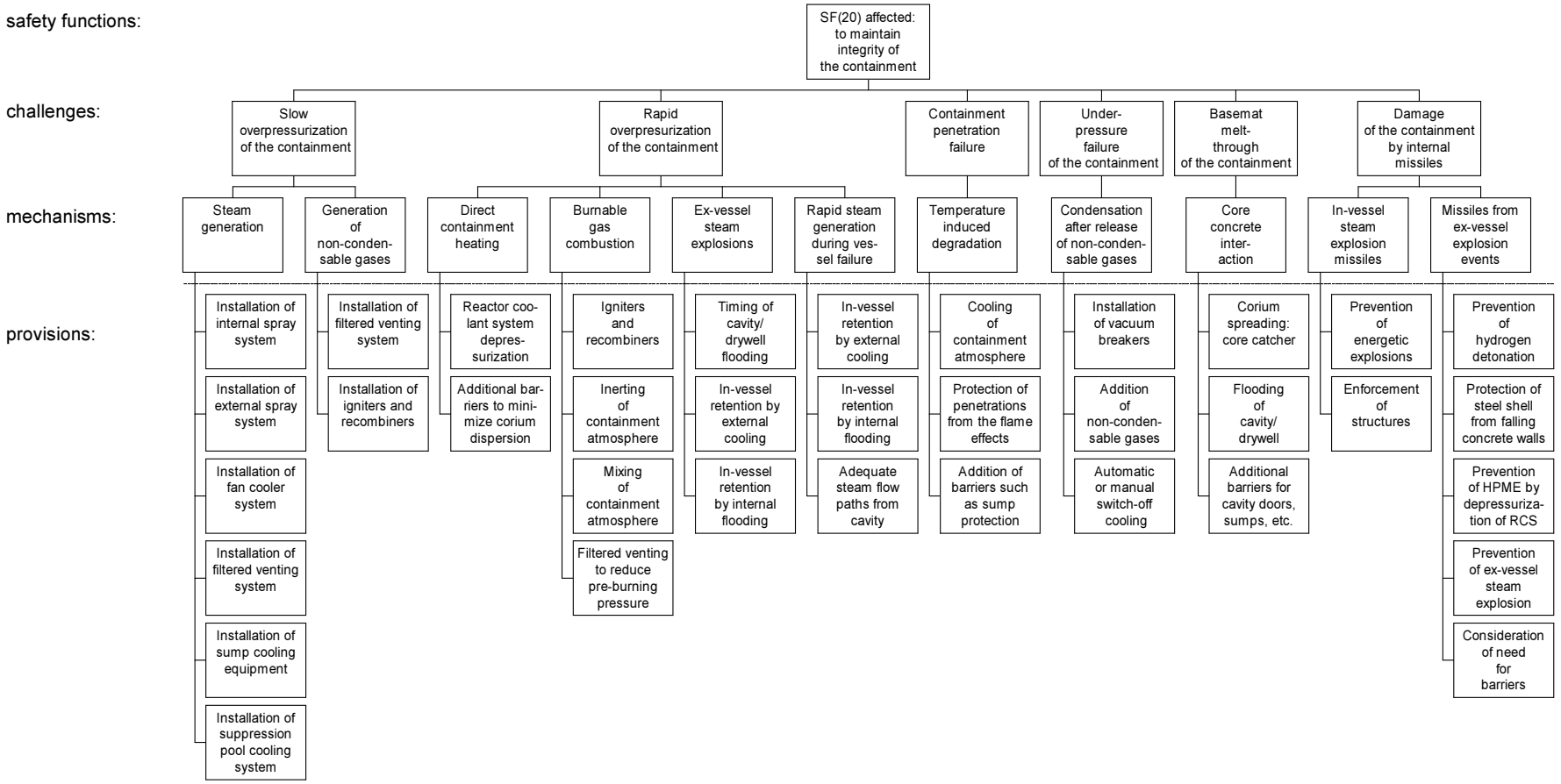


FIG. 7 Objective Tree for Level 1 of Defence
SAFETY PRINCIPLE: Ageing management (184) incl. LTO

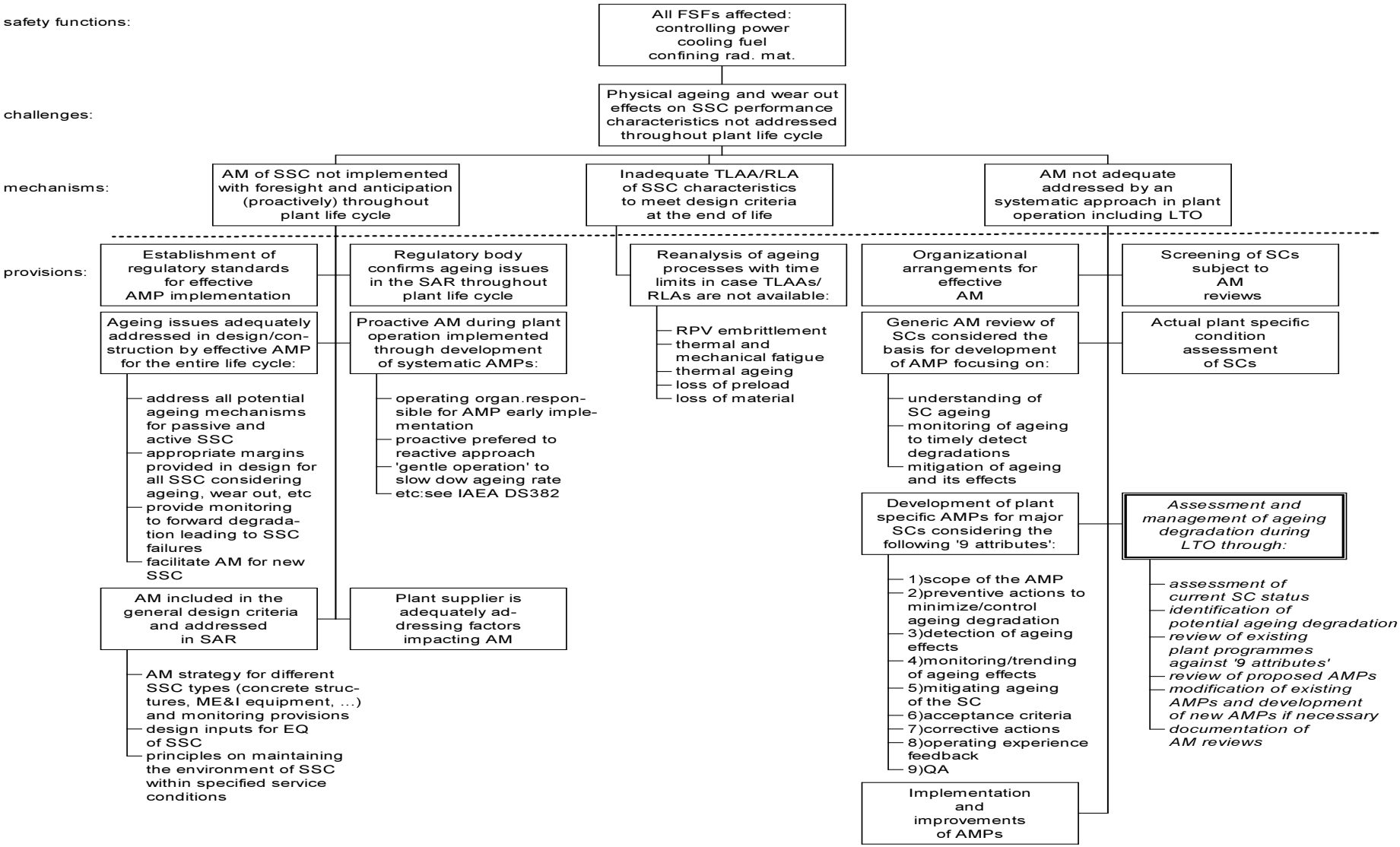


FIG. 8 Objective Tree for Level 2 of Defence
SAFETY PRINCIPLE: Ageing management (184) incl. LTO

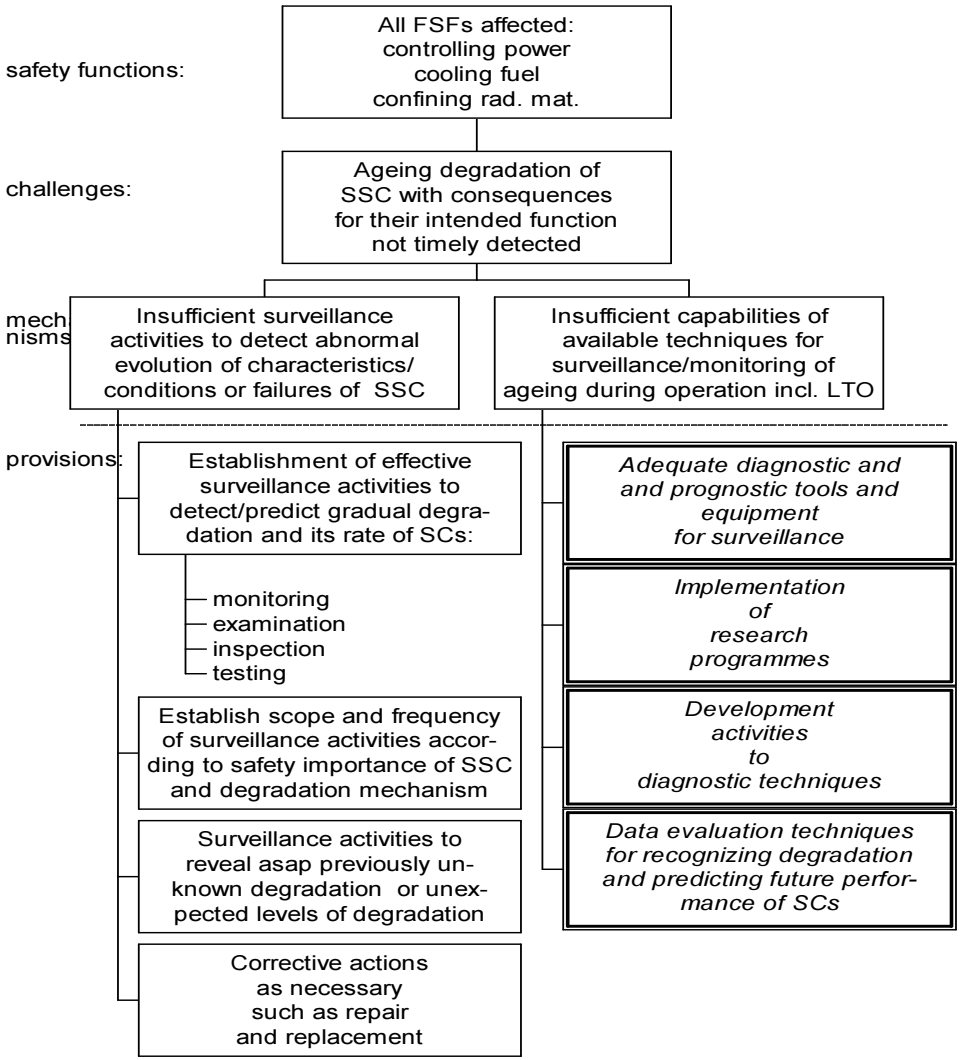


FIG. 9 Objective Tree for Level 3 of Defence
SAFETY PRINCIPLE: Ageing management (184) incl. LTO

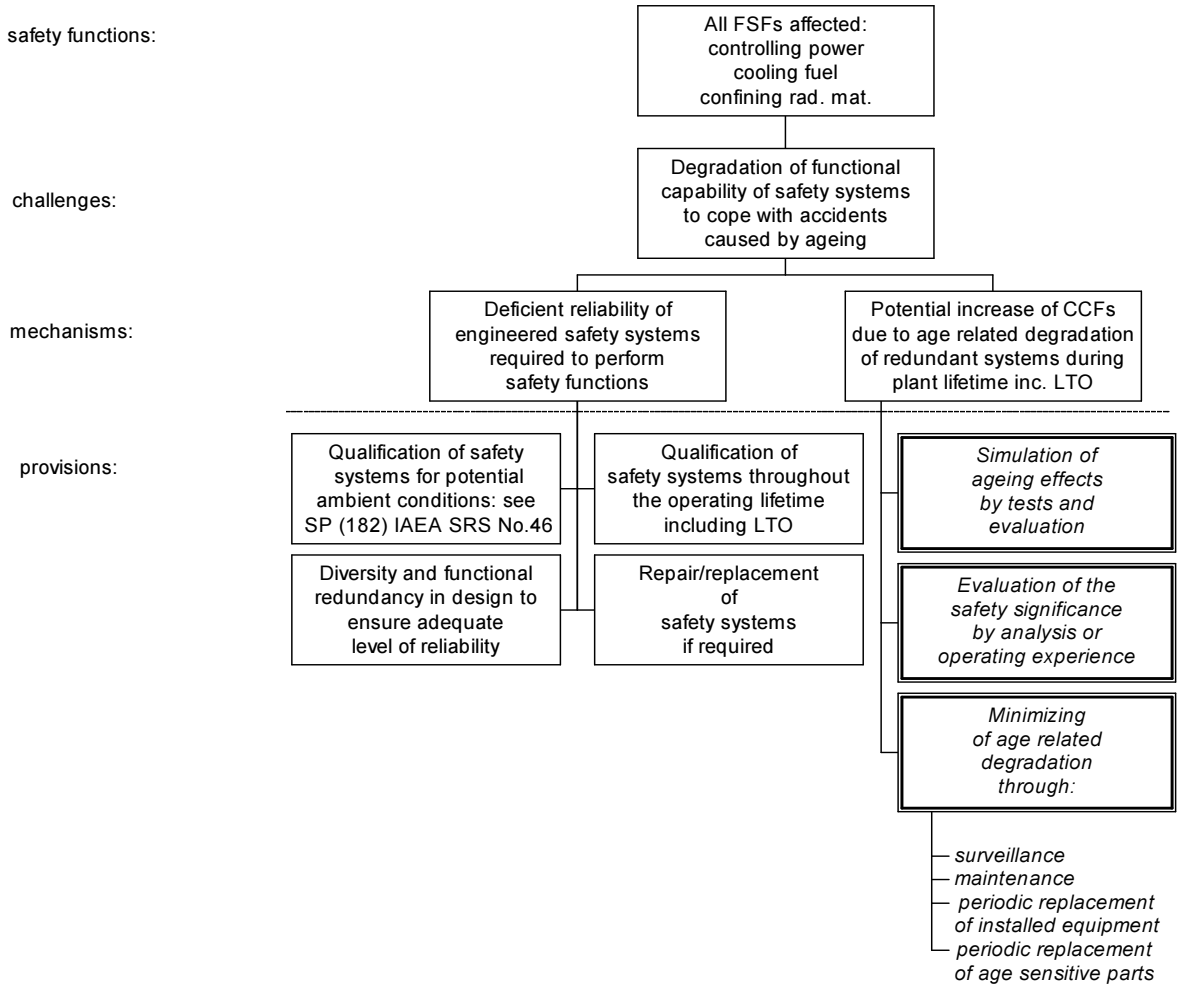


FIG. 10 Objective Tree for Level 3 of Defence
SAFETY PRINCIPLE: Equipment qualification (EQ) (182/1) incl. LTO

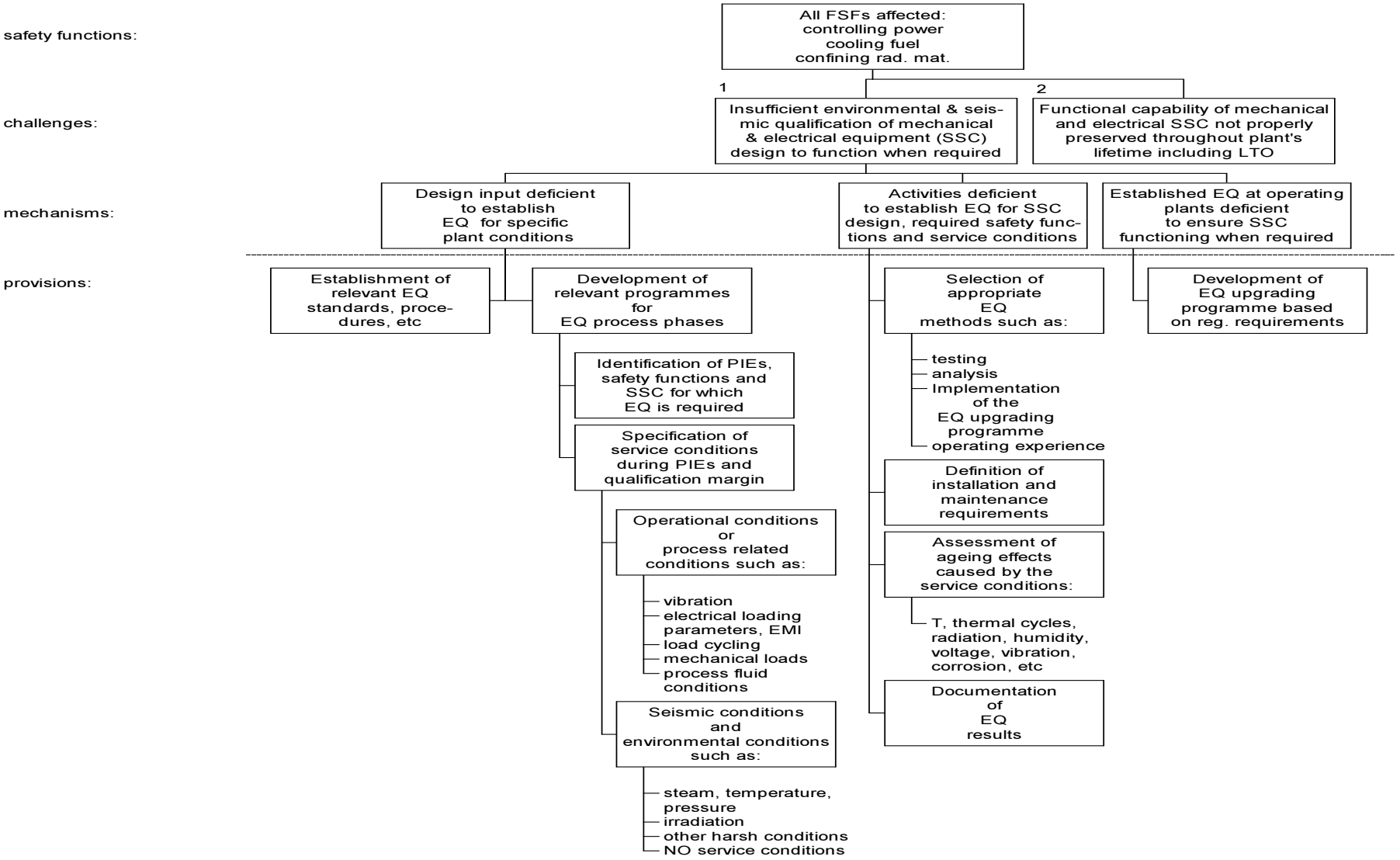


FIG. 11 Objective Tree for Level 3 of Defence
SAFETY PRINCIPLE: Equipment qualification (EQ) (182/2) incl. LTO

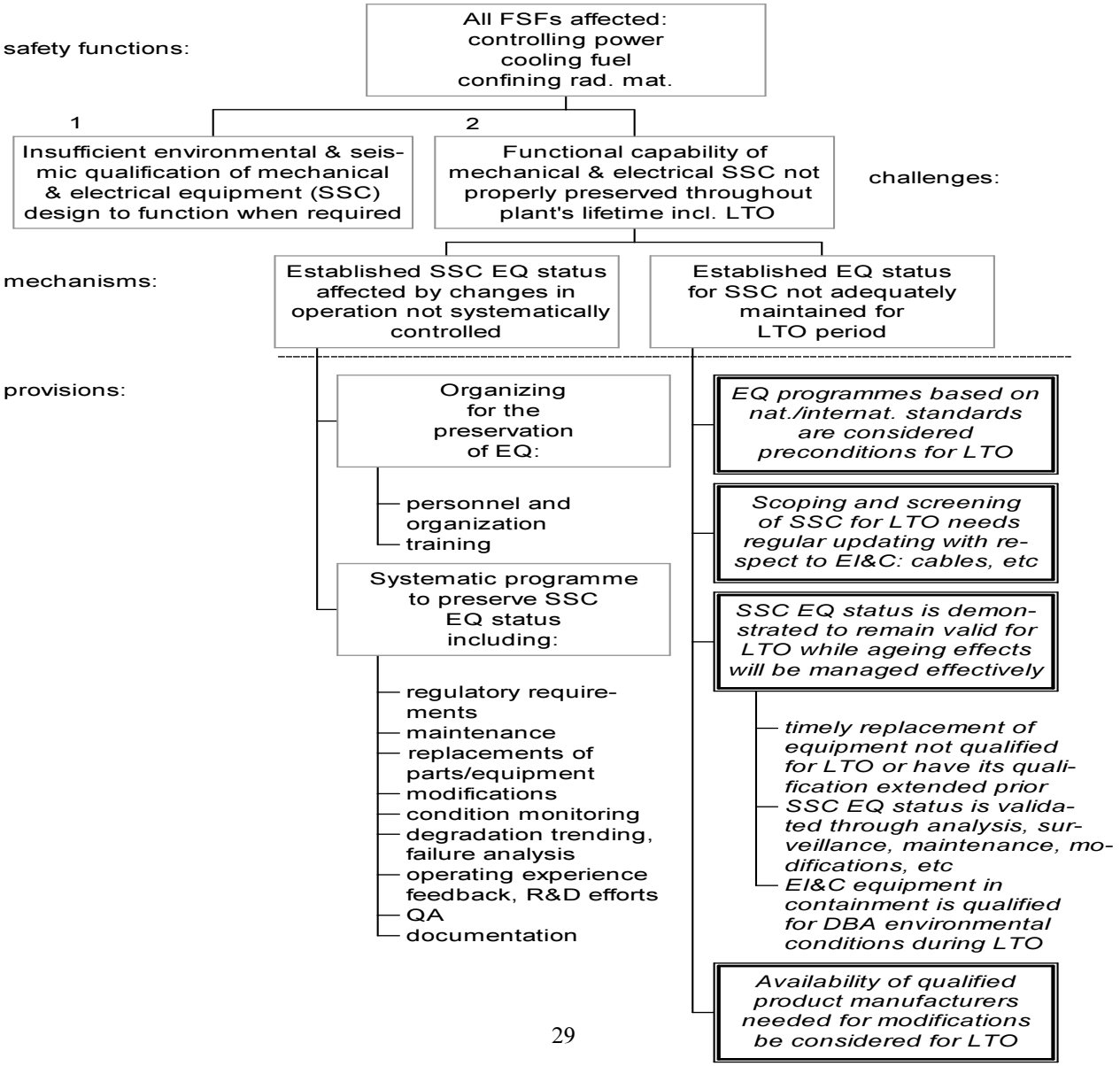


FIG. 12 Objective Tree for Level 3 of Defence
SAFETY PRINCIPLE: Reliability targets (174) incl. LTO

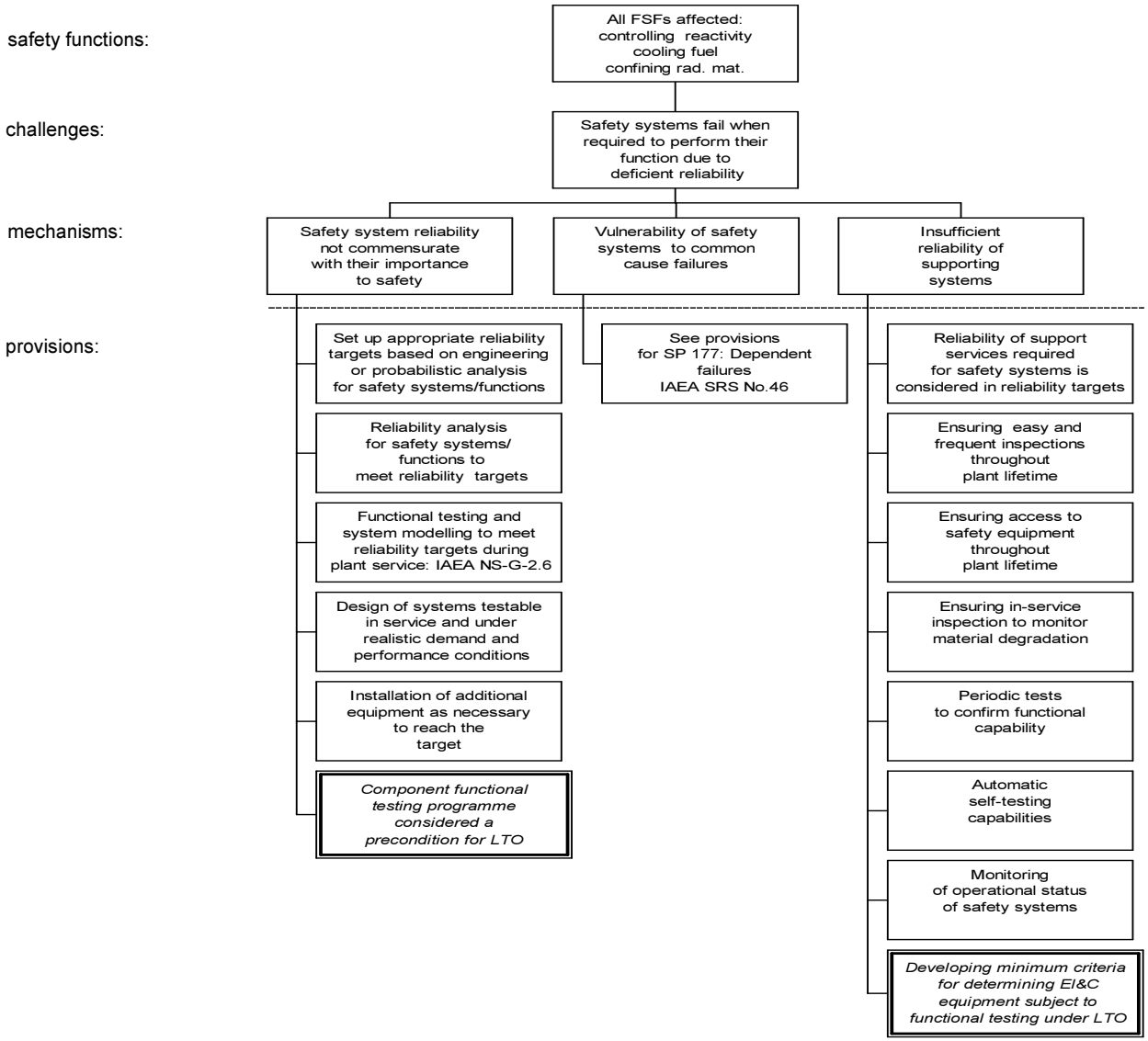


FIG. 13 Objective Tree for Levels 1,2 of Defence
SAFETY PRINCIPLE: Monitoring of plant safety status (227) incl. LTO

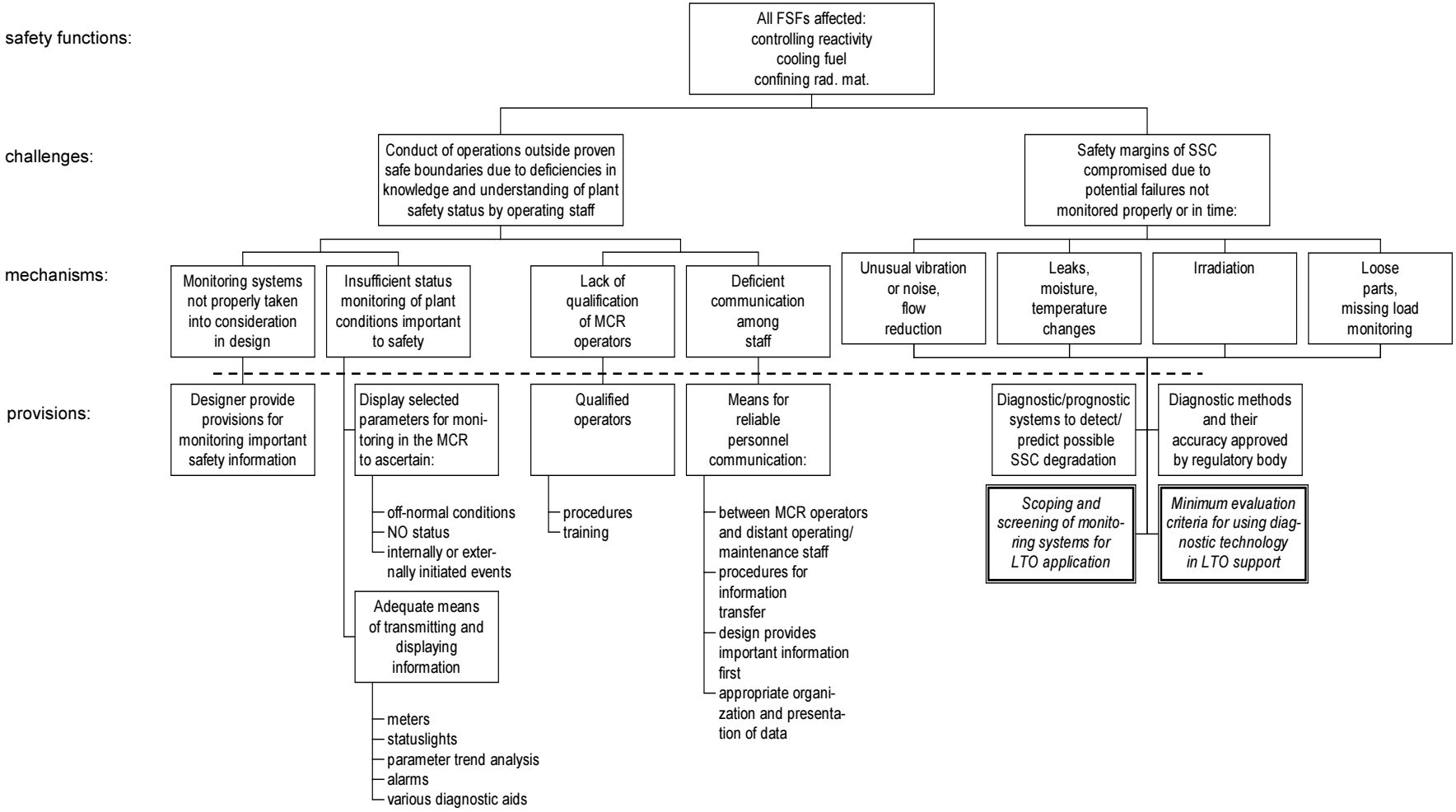


FIG. 14 Objective Tree for Levels 1,2,3 of Defence
SAFETY PRINCIPLE: Training (278) incl. LTO

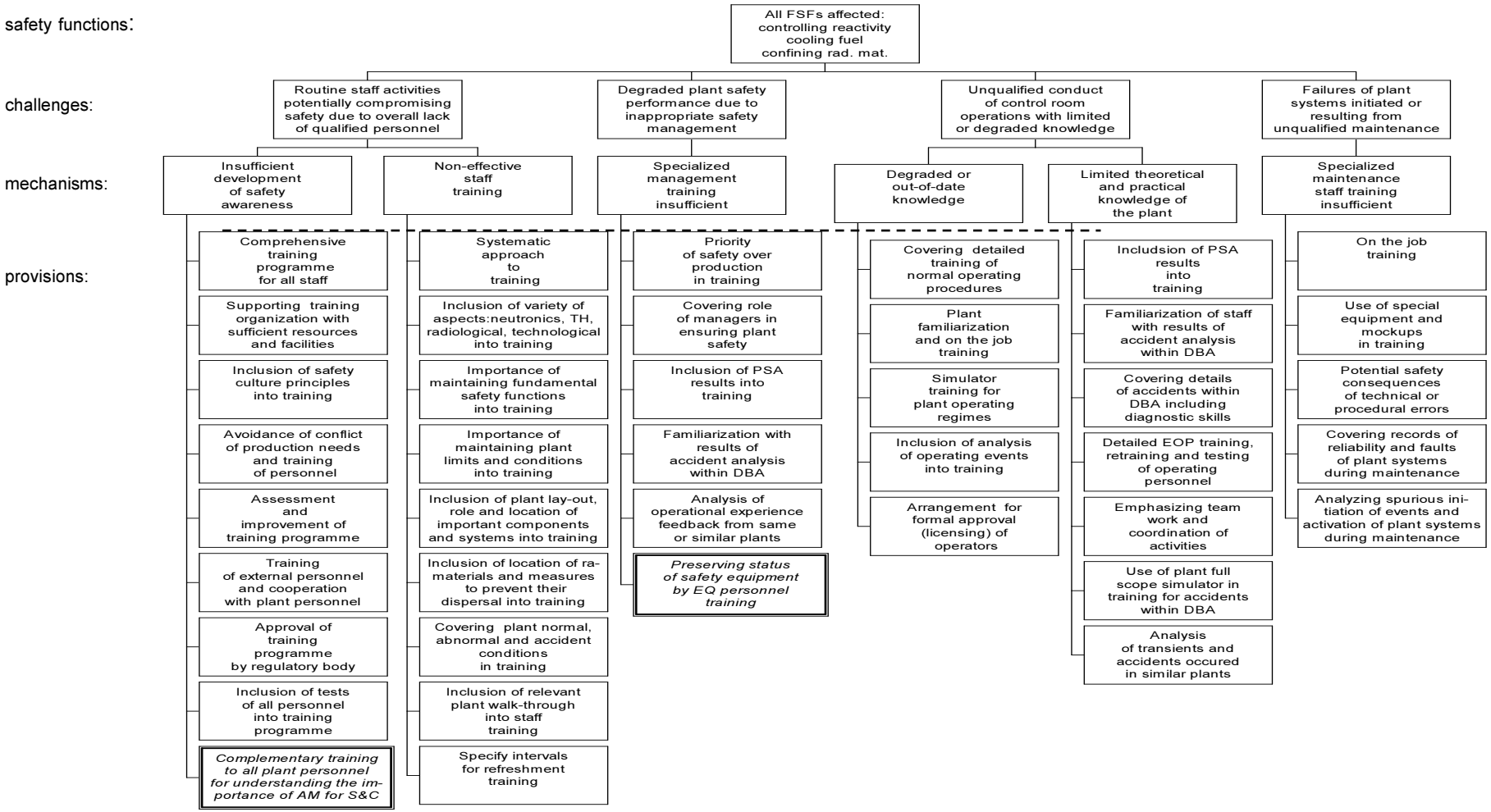


FIG. 15 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: Design management (150) incl. LTO

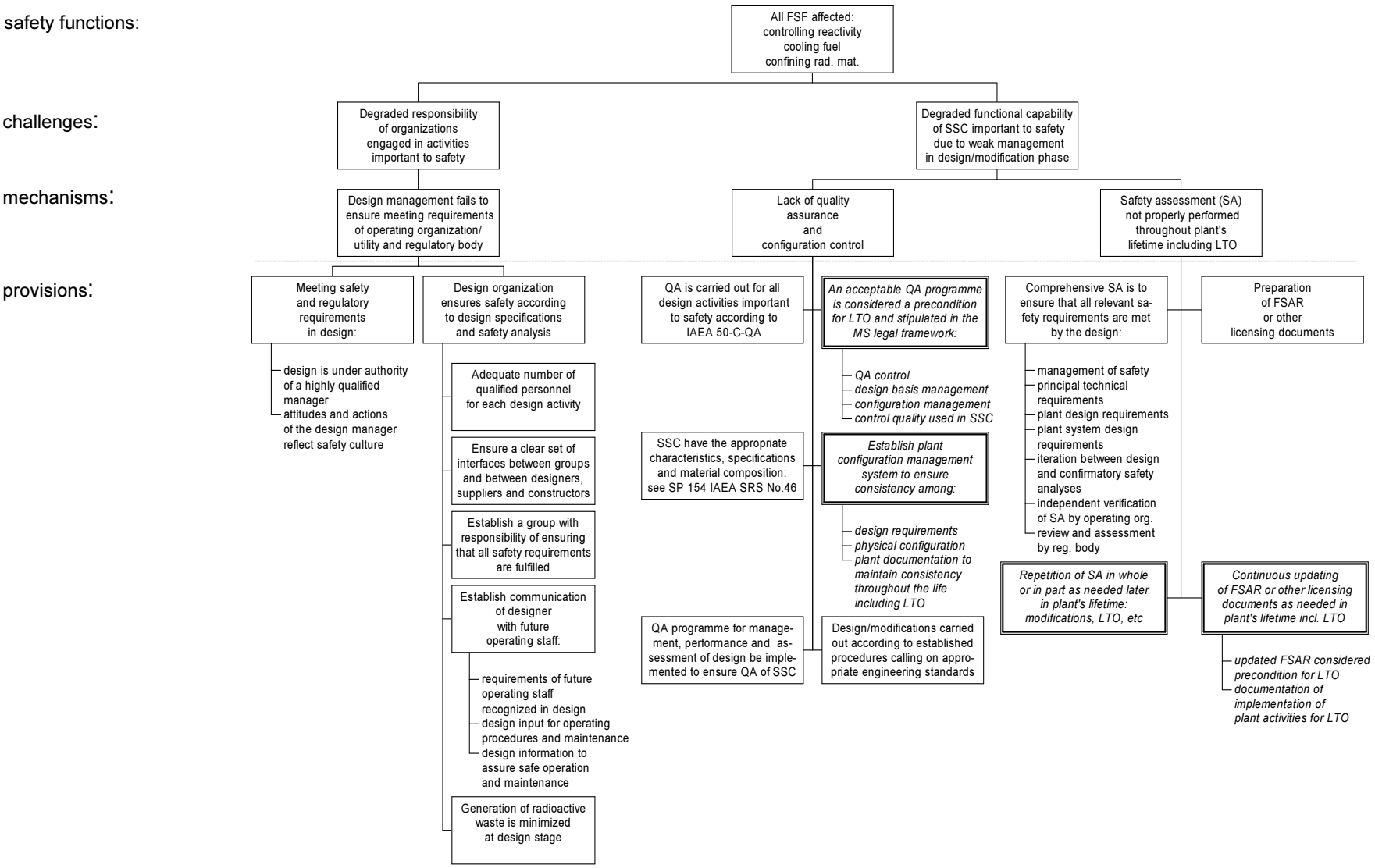


FIG. 16 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: General basis for design (158) incl. LTO

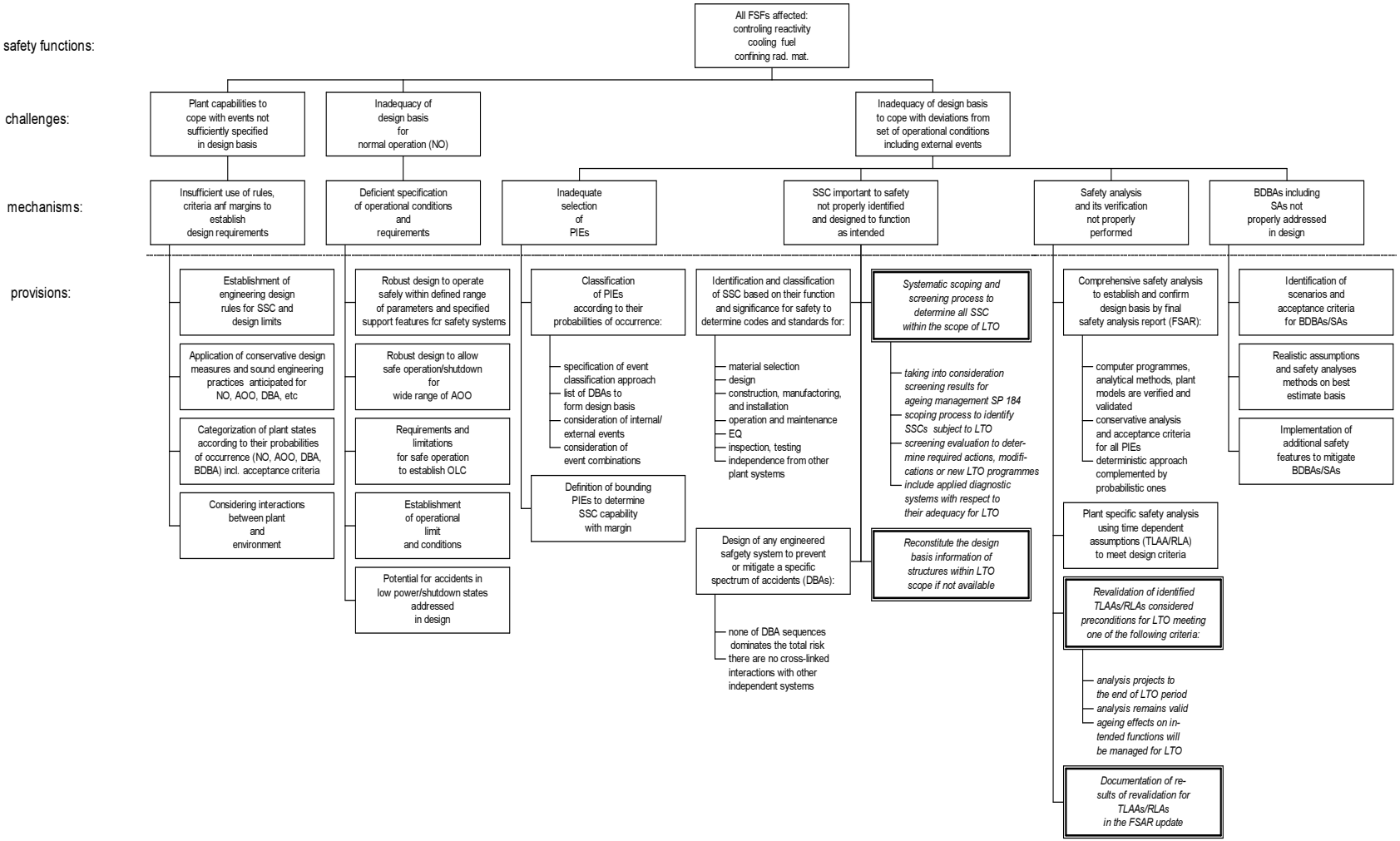


FIG. 17 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: Feedback of operating experience (299) incl. LTO

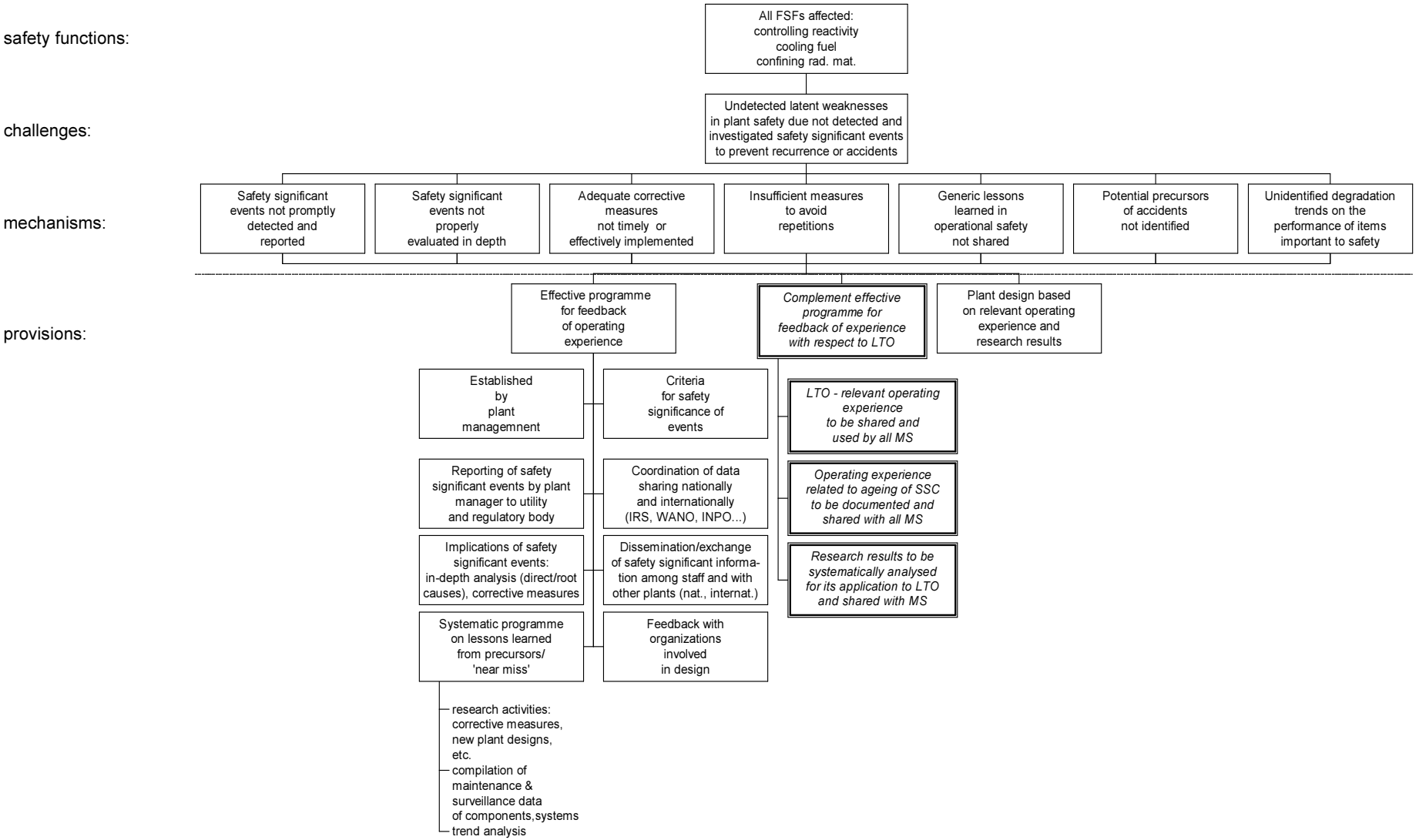


FIG. 18 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: Maintenance, testing and inspection (305/1) incl. LTO

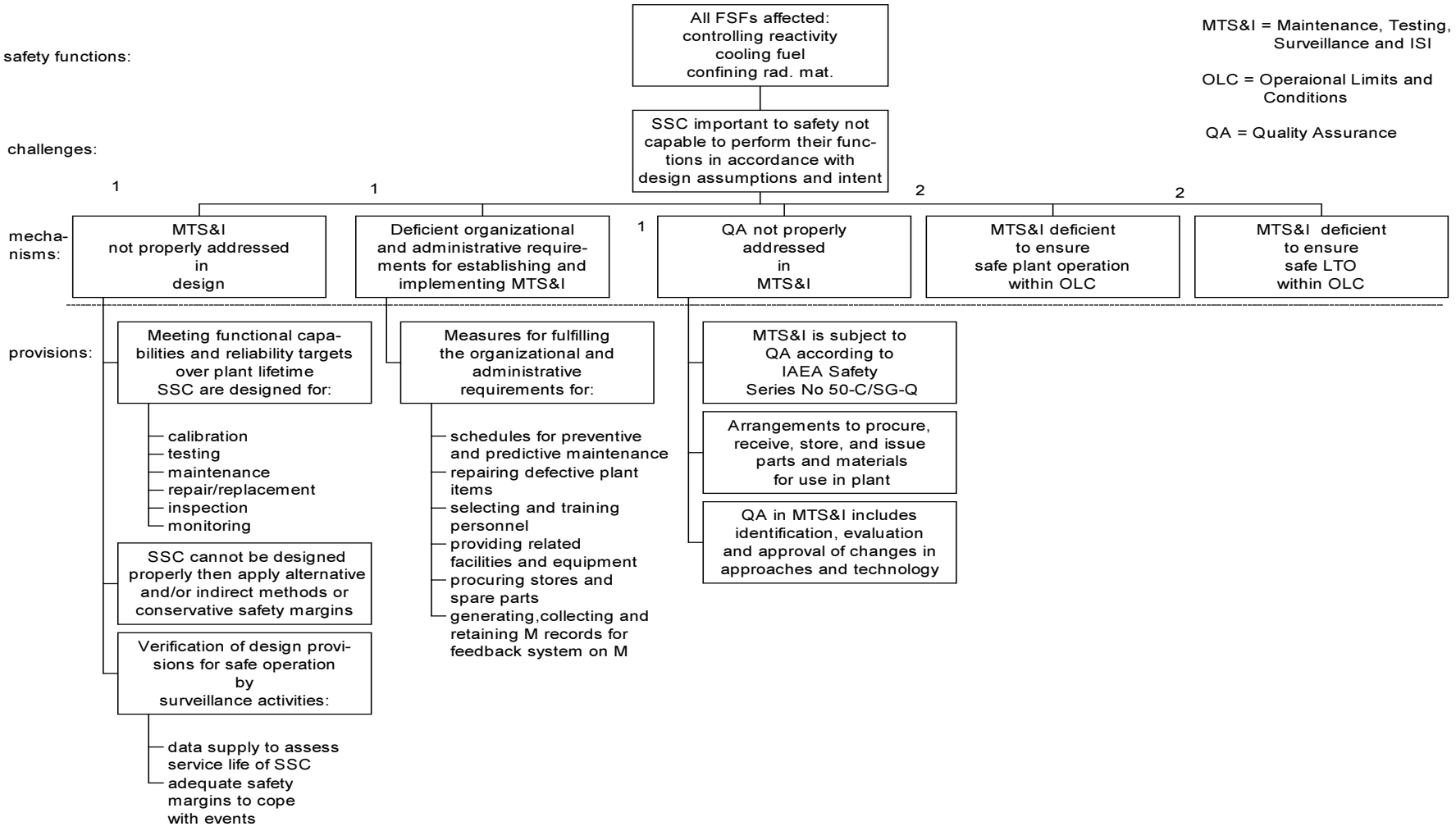


FIG. 19 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: Maintenance, testing and inspection (305/2) incl. LTO

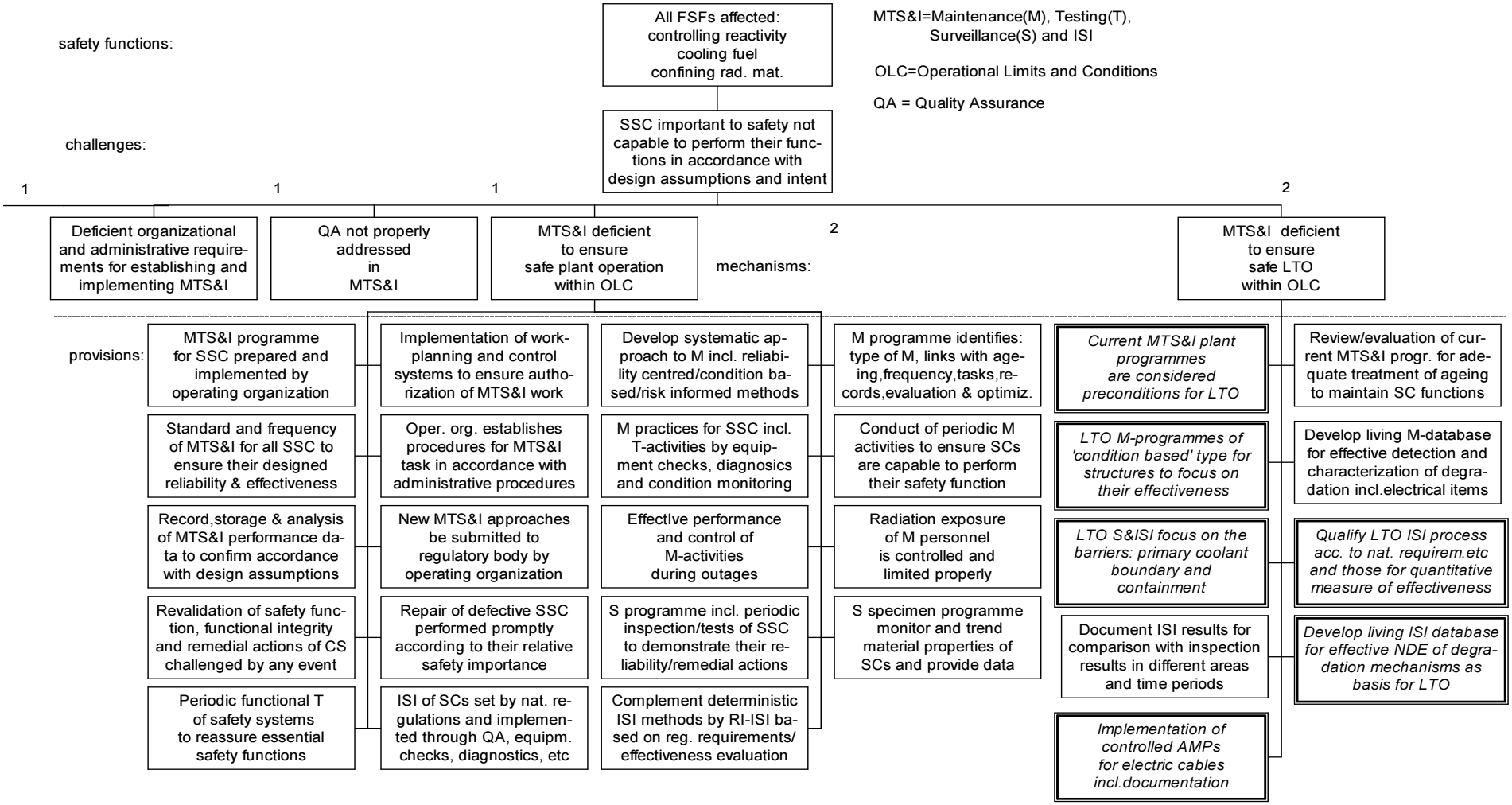


FIG. 20 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: Safety review procedures (269) incl. LTO

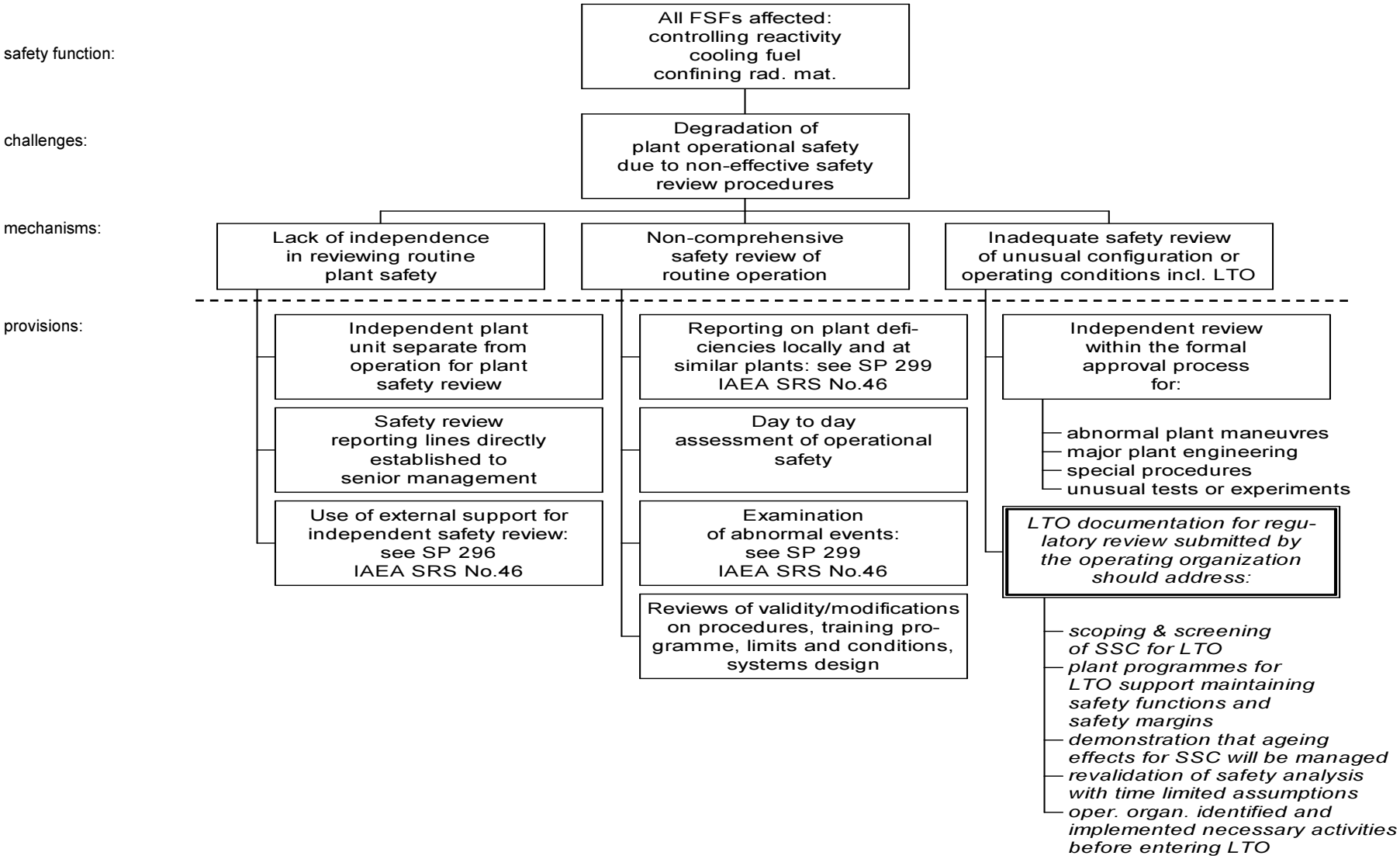


FIG. 21 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: Inspectability of safety equipment (186) incl. LTO

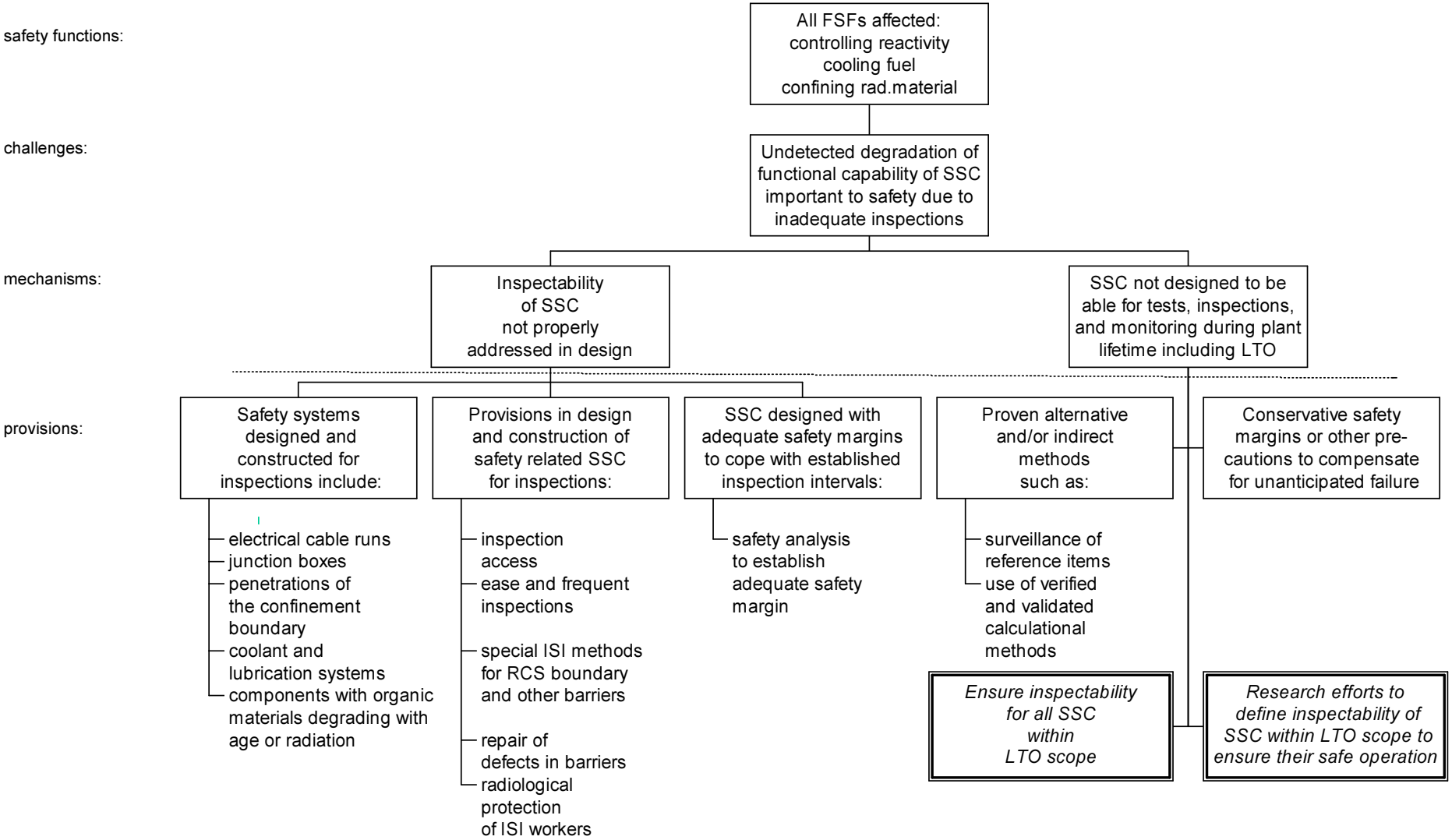


FIG. 22 Objective Tree for Levels 1,2,3,4 of Defence
SAFETY PRINCIPLE: Collecting baseline data (260)