

### 3. GENERAL SAFETY ASPECTS OF NUCLEAR POWER PLANTS

#### 3.1. SAFETY OBJECTIVES

The Safety of Nuclear Power Plants: Design [3], sets out basic objectives, concepts and principles for ensuring safety of nuclear installations in which the stored energy or the energy developed in certain situations could potentially result in the release of radioactive material from its designated location with the consequent risk of radiation exposure of people. The principles are derived from the following three fundamental safety objectives (the following five paragraphs are reproduced from reference [3]):

**General Nuclear Safety Objective:** *To protect individuals, society and the environment from harm by establishing and maintaining in nuclear installations effective defences against radiological hazards.*

This general nuclear safety objective is supported by two complementary safety objectives dealing with radiation protection and technical aspects. They are interdependent: the technical aspects in conjunction with administrative and procedural measures ensure defence against hazards due to ionizing radiation.

**Radiation Protection Objective:** *To ensure that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as reasonably achievable, and to ensure mitigation of the radiological consequences of any accidents.*

**Technical Safety Objective:** *To take all reasonably practicable measures to prevent accidents in nuclear installations and to mitigate their consequences should they occur; to ensure with a high level of confidence that, for all possible accidents taken into account in the design of the installation, including those of very low probability, any radiological consequences would be minor and below prescribed limits; and to ensure that the likelihood of accidents with serious radiological consequences is extremely low.*

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. However, the radiation protection objective does not preclude limited exposure of people or the release of legally authorized quantities of radioactive materials to the environment from installations in operational states. Such exposures and releases, however, must be strictly controlled and must be in compliance with operational limits and radiation protection standards.

In order to achieve these three safety objectives in the design of a nuclear power plant, comprehensive safety analyses are carried out to identify all sources of exposure and to evaluate radiation doses that could be received by the public and by workers at the installation, as well as potential effects of radiation on the environment. The safety analysis examines: (1) all planned normal operational modes of the plant; (2) plant performance in anticipated operational occurrences; (3) design basis accidents; and (4) selected severe accidents. The design for safety of a nuclear power plant applies the principle that plant states that could result in high radiation doses or radionuclide releases are of very low probability of occurrence, and plant states with significant probability of occurrence have only minor or no potential radiological consequences. An essential objective is that the need for external

intervention measures may be limited or even eliminated in technical terms, although such measures may still be required by national authorities.

### 3.2. THE DEFENCE IN DEPTH STRATEGY

The safety objectives will be achieved through the application of the defence in depth strategy. The strategy for defence in depth [4] is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority. The rationale for the priority is that provisions to prevent deviations of the plant state from well known operating conditions are generally more effective and more predictable than measures aimed at mitigation of such departure, because the plant's performance generally deteriorates when the status of the plant or a component departs from normal conditions. Thus preventing the degradation of plant status and performance generally will provide the most effective protection of the public and the environment as well as the protection of the investment. Should preventive measures fail, however, control, management and mitigatory measures, in particular the use of a well designed confinement function, can provide the necessary additional protection of the public and the environment.

The concept of defence in depth, as applied to all safety activities, whether organizational, behavioural or design related, ensures that they are subject to functionally redundant 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 the design of a plant provides a series of levels of defence (inherent features, equipment and procedures) aimed at preventing accidents and ensuring appropriate protection in the event that prevention fails. This strategy has been proven to be effective in compensating for human and equipment failures, both potential and actual.

There is no unique way to implement defence in depth (i.e. no unique technical solution to meet the safety objectives), since there are different designs, different safety requirements in different countries, different technical solutions and varying management or cultural approaches. Nevertheless, the strategy represents the best general framework to achieve safety for any type of nuclear power plants.

Generally, several successive physical barriers for the confinement of radioactive material are put in place. Their specific design may vary depending on the activity of the material and on the possible deviations from normal operation that could result in the failure of some barriers. So, the number and type of barriers confining the fission products is dependent on the adopted reactor technology.

Defence in depth is generally structured in five levels. Should one level fail, the subsequent level comes into play. Table I, summarizes the objectives of each one of the five levels and the correspondent primary means of achieving them. The general objective of defence in depth is to ensure that a 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 defeat defence in depth at subsequent levels. The independence of different levels of defence, i.e. the independence of the features implemented to fulfill the requested functions at different levels, is a key element in meeting this objective.

TABLE I. LEVELS OF DEFENCE IN DEPTH (FROM INSAG-10) [9]

Levels of defence	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 plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents (*)	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive materials	Off-site emergency response

\* For existing plants, the term ‘severe accidents’ is widely associated with significant melting of the core and large releases of radionuclides from the reactor vessel. Because of the characteristics and features of MHTGRs discussed in Section 2, and in particular the low core power density and high temperature capability of the coated fuel particles, no scenarios involving extensive melting of the core are apparent, even for very low probabilities/highly hypothetical events. Thus in the case of MHTGRs, the term ‘severe accident’ is taken to mean events which could challenge the structural integrity of the core and thus the ability to predict the course of the event, e.g. sustained (days) air ingress through large openings in the primary system and the confinement building. However, some action to manage these situations would be advisable to maintain the plant in a state that can be analysed. While such conditions could serve as a basis for considerations associated with Level 4 of defence in depth, it is important to point out that these extreme conditions will not necessarily involve large releases from the fuel, since existing data [7] show effective radionuclide retention at elevated temperatures when the fuel has burned back to the silicon carbide layer of the coated particles and remains in a high temperature air environment for days.

### 3.3. THE FUNDAMENTAL SAFETY FUNCTIONS

The objective of the safety approach is to provide adequate means:

- to maintain the plant in a normal operational state;
- to ensure the proper short term response immediately following a postulated initiating event (PIE);

- and to facilitate the management of the plant in and following any design basis accident, and following any plant states beyond the design basis that may occur (i.e. the “severe plant conditions”).

To ensure safety (i.e. to meet allowable radiological consequences during all foreseeable plant conditions), the following fundamental safety functions shall be performed in operational states, in and following a design basis accident and in and after the occurrence of severe plant conditions:

- control of the reactivity;
- removal of heat from the core; and
- confinement of radioactive materials and control of operational discharges, as well as limitation of accidental releases.

The possible challenges to the safety functions are dealt with by the provisions (inherent characteristics, safety margins, systems, procedures) of a given level of defence. Combinations of one or more provisions to cope with challenges to levels of defence are often called lines of defence (LOD) (see Section 3.4 for details). The way the fundamental safety functions are achieved and the specific LOD used, are obviously dependent on the specific design.

All mechanisms that can challenge the successful achievement of the safety functions are identified for each level of defence. These mechanisms are used to determine the set of initiating events that encompass the possible initiations of sequences. According to the philosophy of defence in depth, if the evolution of a sequence is not controlled by the provisions of a level of defence it will be by the subsequent level that comes into play (LOD functional redundancy).

Figure 2 shows the logic flow diagram of defence in depth and its correlation to the fundamental safety functions. The objective is always to maintain the plant in a state where the fundamental safety functions (confinement of radioactive products, control of reactivity and heat removal) are successfully fulfilled. Success criteria are defined for each level of defence in depth and for the moment they are expressed only in deterministic terms.

As the objective of the first level of protection is the prevention of abnormal operation and system failures, if it fails, an initiating event comes into play and a sequence of events is potentially initiated. Then the second level of protection will detect the failures or control the abnormal operation. Should the second level fail, the third level ensures that the safety functions are further performed by activating specific LODs (safety systems and other safety features). Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external releases of radioactive materials. The last level (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response.

Figure 2 shows that some challenges/mechanisms may compromise the effectiveness of the considered level of defence by affecting either the performance of the safety function directly or the reliability of a safety provision. The effectiveness of a level of defence is determined by the ability of the provisions to cope with mechanisms which challenge the performance of safety functions. The probability associated with challenges/mechanisms, the reliability of the demanded safety provisions and the associated potential radiological consequences will define the risk for the considered accident sequence.

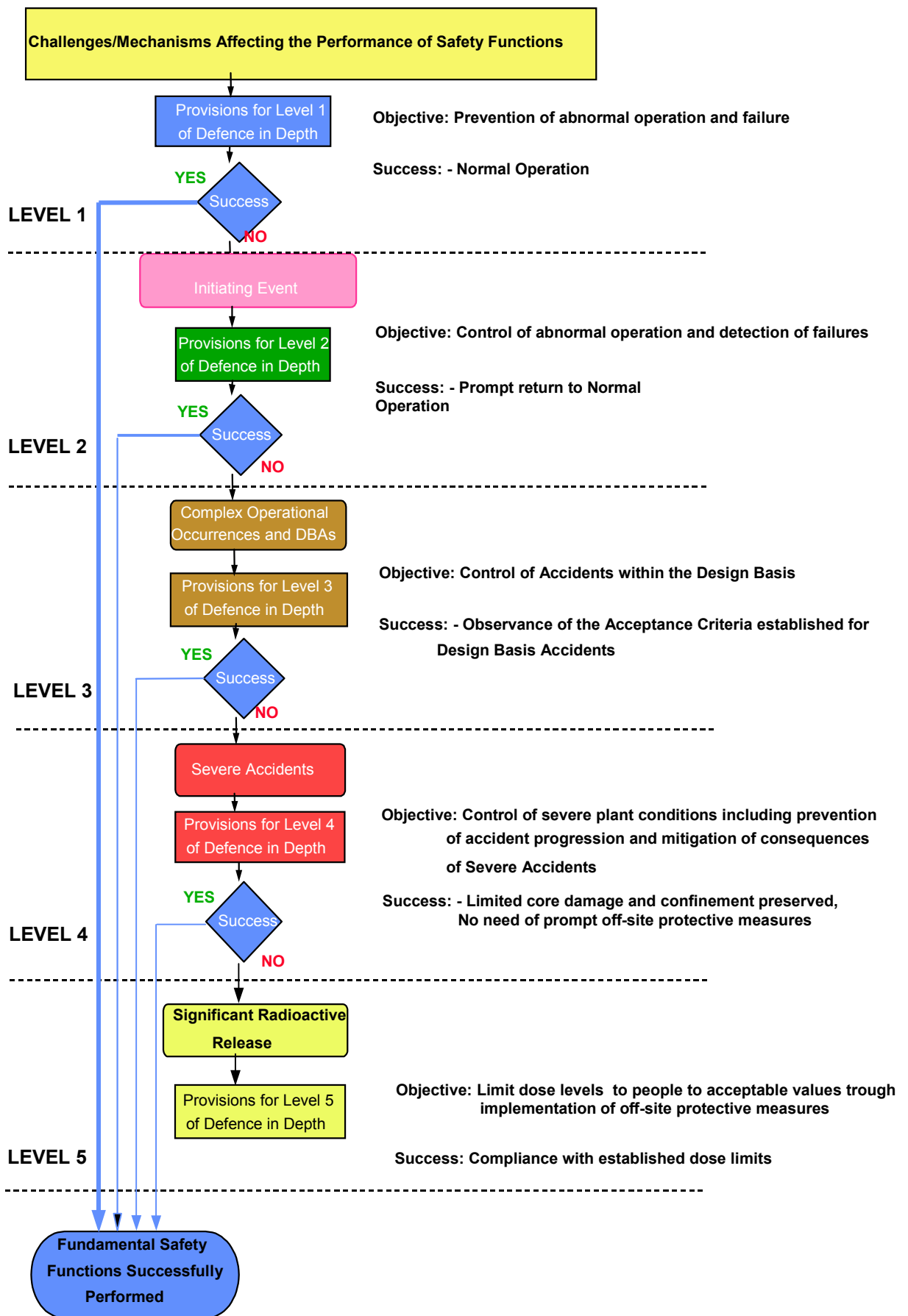


FIG. 2. Logic flow diagram of defence in depth.

### 3.4. THE CONCEPT OF LINES OF DEFENCE

To evaluate or compare the implementation of defence in depth by different reactor technologies, it is suggested to adopt a common approach that needs to have the following features:

- the safety objectives should be the same in terms of doses respectively to the operators, the public and the environment (i.e. radiological consequences) for all plant conditions at a given level of defence;
- the safety assessment method should use analogous and comparable approaches based on the integral adoption of defence in depth (all the levels should be considered);
- the approach should be able to integrate the unique characteristics of each type of reactor, with the number and the quality of the required “defences” being a function of the potential internal and external hazards and consequences of failures.

To implement this, it is useful to introduce the concept of lines of defence as any inherent characteristic, equipment or system implemented into the safety related plant architecture, as well as any safety relevant operational procedure, that are necessary to fulfil the safety functions.

The required number and strength of these lines of defence depend on the reactor type, i.e. the implemented LODs shall fulfil the missions requested to prevent abnormal situations or return the plant to a controlled or safe shutdown condition and maintain it in a safe state after a postulated initiating event (PIE). Their design shall take into account simultaneously the needs for performance (to meet the safety criteria), and the safety objectives as well as the recommendations concerning, for example, reliability, redundancy, diversity, in-service inspection requirements, etc.

In this logic, the physical barriers normally considered in LWRs (fuel, cladding, primary circuit and containment) are provisions to confine fission products. Their contribution to safety has to be assessed for each specific concept of reactor and considered in the general safety architecture of the plant.

As lines of defence can rely simultaneously on both active and passive systems as well as on inherent features, the safety assessment approach should consider their correspondent reliabilities to correctly take into account all the potential of the safety related architecture. The LODs can be classified into categories according to their reliability. The number and category of LODs can be used as a tool to assess the adequacy of the implementation of defence in depth.

### 3.5. CURRENT SAFETY APPROACH

Operating nuclear power plants are largely designed following a safety architecture dictated by the implementation of the strategy of defence in depth (physical barriers and levels of defence) as illustrated in Section 3.2. In the majority of the plants of the current generation the application of defence in depth is mainly based on deterministic considerations. This means that the plant is deterministically designed against a set of normal and postulated accident situations according to well established design criteria in order to meet the radiological targets. The adequacy of the defence in depth is established by the number of barriers and number and quality of systems in each level of defence.

The current design approach has been shown to be a sound foundation for the safety and protection of public health, in particular because of its broad scope of accident sequence considerations, and because of its many conservative assumptions which have the effect of introducing highly conservative margins into the design that, in reality, give the plant the capability of dealing with a large variety of sequences, in some cases well beyond those included in the design basis.

The deterministic approach is complemented by probabilistic evaluations with the main purpose of verifying that the design is well balanced and there are no weak areas or systems that could allow for the possibility of high risk sequences. Probabilistic safety assessment is recognized as a very efficient tool for identifying those sequences and plant vulnerabilities that require specific additional preventive or mitigative design features.

This safety approach is reflected in the current IAEA Safety Standards for the design.

### 3.6. THE IAEA SAFETY STANDARDS SERIES

Under the terms of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation. The regulatory related publications are issued in the IAEA Safety Standards Series, covering nuclear safety, radiation safety, transport safety and waste safety. There are three categories within the Safety Standards Series, schematically depicted in Fig. 3:

**Safety Fundamentals:** present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

**Safety Requirements:** establish the requirements that must be met to ensure safety. These requirements, which are expressed as ‘shall’ statements, are governed by the objectives and principles presented in the Safety Fundamentals.

**Safety Guides:** recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as ‘should’ statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

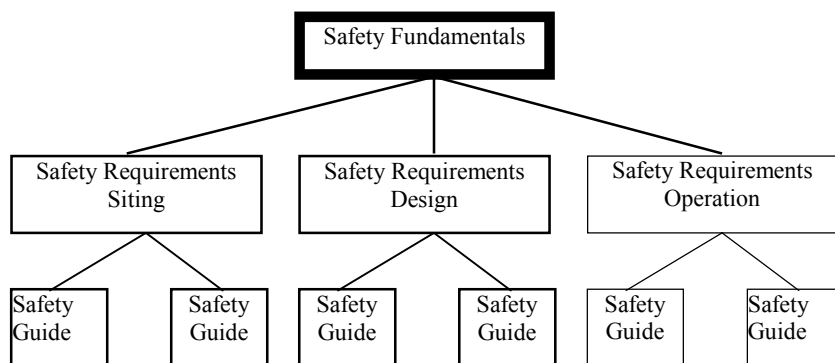


FIG. 3. The IAEA Safety Standards Series.

### 3.7. DEVELOPMENT OF GENERAL SAFETY DESIGN REQUIREMENTS

Design requirements play an important role in establishing the safety level<sup>1</sup> of the installation and also have great impact on its cost and operating procedures. The general logical process to generate the safety requirements for a reactor plant design is schematically represented in Fig. 4, and briefly described below.

The Safety requirements can be derived from a set of limited safety principles which directly descend from the three well established safety objectives. The safety objectives define the general targets that shall be achieved by a nuclear installation to protect the operators and the population. They are the same for all nuclear installations including nuclear reactors, and are independent of the kind or size of any given installation.

For nuclear reactors, the compliance with the safety objectives is achieved when the three fundamental safety functions *Confinement of radioactive material*, *control of the reactivity* and *removal of the heat from the core* are fulfilled for all the plant operational, accidental and post accidental conditions in accordance with radiological targets.

To ensure that the safety objectives are met with sufficient confidence and the fundamental safety functions are adequately fulfilled, an effective defence in depth should be implemented. For measuring and assessing the adequacy of the defence in depth, success criteria (expressed in deterministic and probabilistic terms) need to be defined for each level of defence.

Defence in depth has been proved to be generally applicable and very effective in assuring safety in NPPs. It can be used as primary guidance for the preparation of safety requirements. As a matter of fact, and as has been shown by INSAG [4], there is correspondence between the five levels of defence in depth and the safety requirements. It is reasonable to assume that this correspondence is maintained for all kind of reactors regardless of their size or specific safety features.

The safety requirements can be obtained by developing, for each fundamental safety function, the corresponding provisions necessary to meet the established success criteria for each level of defence. The correct implementation of the strategy of the defence in depth (i.e. the adoption of an adequate safety architecture) ensures that the fundamental safety functions are reliably achieved and with sufficient margins to compensate for equipment failure and human errors. More demanding success criteria will result in a more effective defence in depth and in more demanding requirements for the provisions for each level of defence.

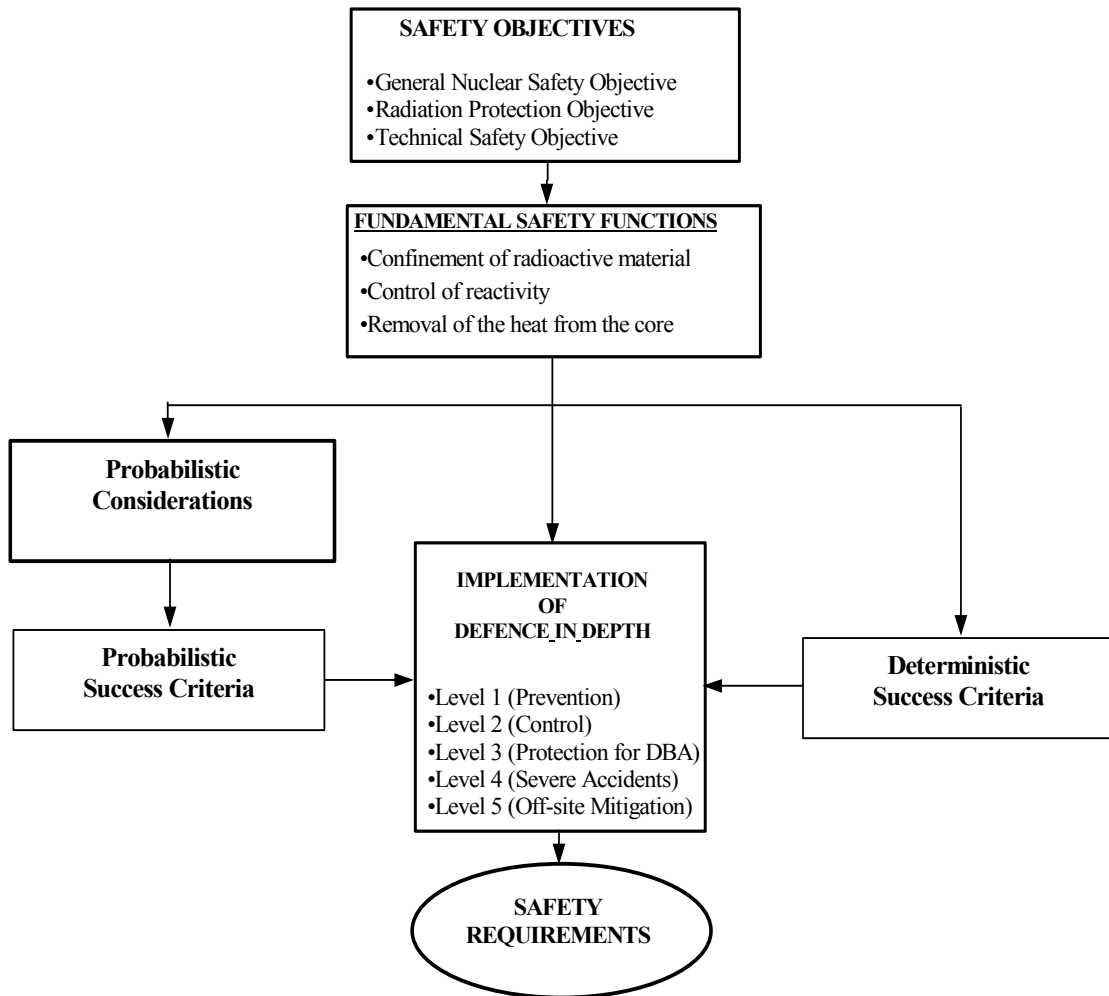
### 3.8. INTEGRATION OF DETERMINISTIC AND PROBABILISTIC CONSIDERATIONS IN THE SCHEME OF DEFENCE IN DEPTH

The generalized concept of defence in depth, as outlined in Section 3.2, needs to integrate both deterministic and probabilistic considerations (e.g. system reliability, probabilistic targets, etc.) to provide metrics for assessing the adequacy of the means of each level of defence. The integration of deterministic and probabilistic approaches also provides a basis for additional requirements and to ensure a well balanced design to identify and then

---

<sup>1</sup> The actual level of safety is determined by the full set of detailed criteria and requirements (deterministic and probabilistic) with which the design complies. In other words, the level of safety depends on the way defence in depth is implemented in the design taking into account the implications of the specific features and technology.

cope with all PIEs. The approach provides general guidance on what is understood to be key engineering judgements about the performance requirements of the plant systems. However, the levels of defence by themselves do not provide the metrics by which to judge adequacy of the implementation of defence in depth. Risk informed approaches which combine deterministic and probabilistic techniques, can be useful tools to assess the contribution of each line of defence to safety with a resulting integrated safety assessment relative to public health and safety.



*Fig. 4. Logical process for the generation of safety requirements.*

The approach that is recommended is the development of a probabilistic safety assessment model of all plant systems without any pre-conceived notion of what is safety related. This model can then be used to determine the importance to safety of systems, structures and components which can then lead to a determination of safety classification. This model can then also be used to assess the contribution of each level of defence to the ultimate safety of the plant as it relates to public health and safety. Should there be barriers or other provisions that need to be strengthened, the value of the improvement can be directly assessed.

A key factor in making safety adequacy assessments is the ability to tie the levels of defence concept to safety goals that are generally accepted for nuclear plants. This linkage provides the integration of safety with technology judgements of adequacy from a public health and safety point of view. The risk informed process can be used in plant design to optimize safety performance and to balance the lines of defence in an overall defence in depth strategy by the quantification possible through the use of probabilistic safety analysis.

One of the key issues in deterministic and probabilistic analysis is how to deal with uncertainties. Traditional deterministic approaches rely on a balance of prevention and mitigation with large design margins and the ultimate final barrier being the 'containment' to cover any unknown phenomenon or event that goes beyond what is generally expected or understood. With advanced reactors, the objective is to design the plant making extensive use of inherent safety features that do not rely on active systems to prevent plant conditions that could lead to fuel failure and fission products release. By employing the risk informed analysis, the contribution to safety of the design features and need for additional features can be assessed. To deal with uncertainties, especially in early deployment of the systems, sensitivity analysis the performance of key systems can be used to provide a measure of the impact of the uncertainty and appropriate design decisions can be made.

Figure 5 shows in a very schematic fashion the curve of the target risk that separates acceptable and unacceptable situations (frequency of the event  $\times$  consequences) and the integration of the level of defences with the probability associated to each event. The success criterion for each level of defence is represented by the area limited by the maximum acceptable consequence and probability for that level. (e.g. dotted area for Level 2).

An event sequence is initiated (see Fig. 2) if a challenge (internal or external to the plant) breaks the first level of defence (prevention of abnormal operation and failures).

The representation of Fig. 5, with adequate values of consequences and probabilities on the axes of the diagram gives a visual representation of the contribution of each level of defence to the general safety of the plant, provides a metric and allows for comparisons of the safety and implementation of defence in depth in different concepts.

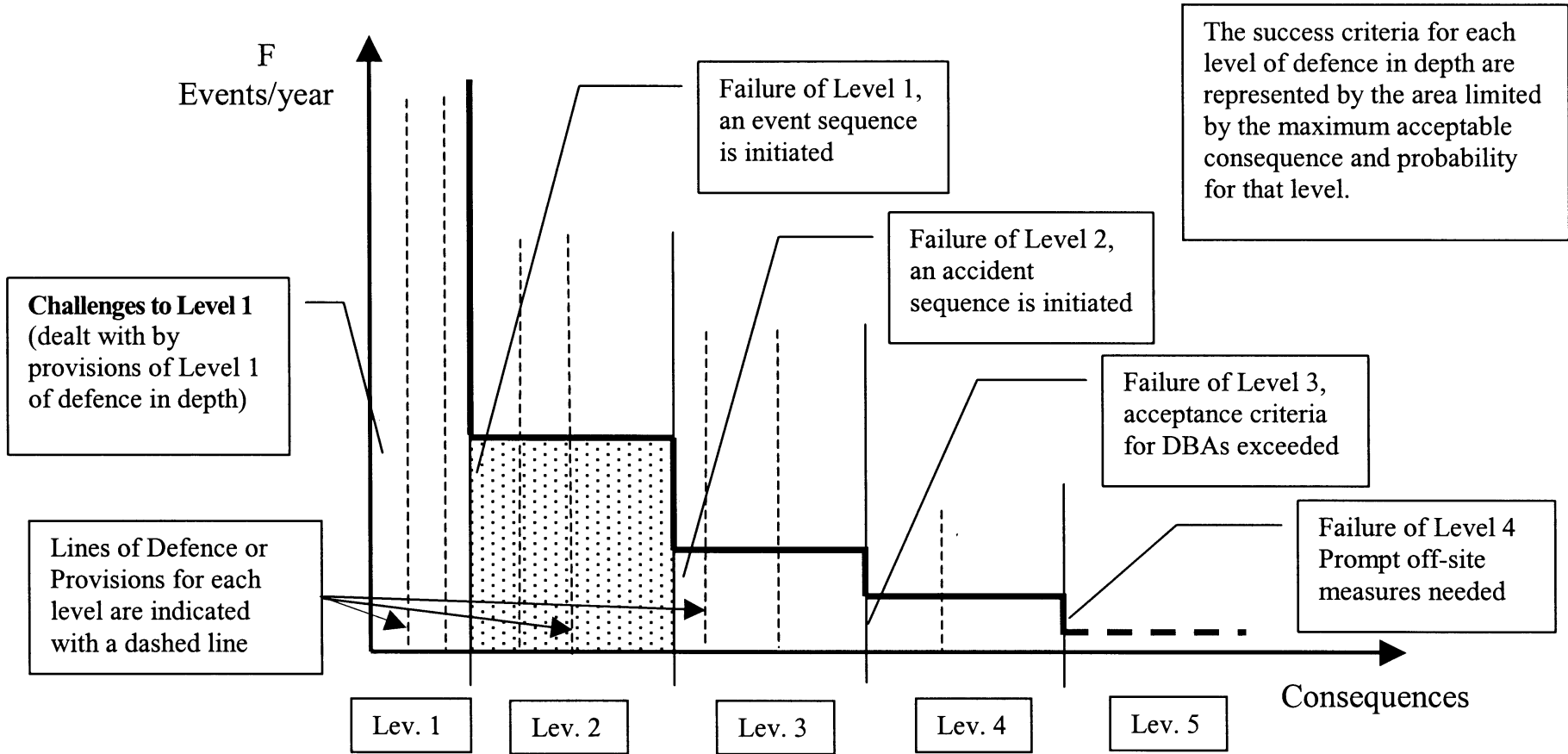


Fig. 5. Correlation of levels of defence and success criteria.