001
May 2017
Rev. 0

ALLEGRO

Safety Specifications and Objectives

B. Hatala - VUJE
J. Procháska - VUJE
T. Kliment - VUJE

V4G4 Centre of Excellence

CONTENT

CONTENT 3

LIST OF TABLE 4

LIST OF FIGURES 4

INTRODUCTION 5

1 SAFETY APROACH 6

1.1 GENERATION IV INTERNATIONAL FORUM SAFETY GOALS 6

1.2 GENERAL SAFETY APPROACH 6

1.3 FUNDAMENTALS SAFETY FUNCTIONS 6

2 CATEGORIES OF PLANT STATES 7

2.1 NORMAL OPERATION 7

2.2 ANTICIPATED OPERATIONAL OCCURRENCES 8

2.3 DESIGN BASIS ACCIDENTS (DBA) 8

2.4 DESIGN EXTENSION CONDITIONS (DEC) 9

2.4.1 Design extension conditions without significant fuel degradation 10

2.4.2 Design extension conditions with core melt 10

2.5 POSTULATED INITIATING EVENTS 12

2.5.1 Internal and external hazards 13

3 DEFENCE IN DEPTH 14

3.1 LEVELS OF DEFENCE IN DEPTH 14

3.1.1 First level 14

3.1.2 Second level 15

3.1.3 Third level 15

3.1.4 Fourth level 16

3.1.5 Fifth level 16

3.2 SUMMARY OF LEVELS OF DEFENCE IN DEPTH 17

3.3 INDEPENDENCE BETWEEN ALL LEVELS OF DEFENCE-IN-DEPTH 18

4 SYSTEMS, STRUCTURES AND COMPONENTS 20

4.1 SAFETY SYSTEMS 20

4.2 SAFETY RELATED SYSTEMS 21

4.3 SAFETY PRINCIPLES APPLICABLE TO THE DESIGN OF STRUCTURES, SYSTEMS AND COMPONENTS 21

4.4 SINGLE FAILURE 22

4.4.1 Definition of active and passive single failures 22

4.5 COMMON CAUSE FAILURES (CCFS) 23

5 DESIGN LIMITS 24

CONCLUSION 25

ABBREVIATIONS 26

REFERENCES **27**

ANNEX 1 INTEGRATED DESIGN APPROACH **28**

1 INTRODUCTION **29**

1.1 PRELIMINARY PLANT DESIGN CONCEPT (STEP 1) 30

1.2 DEFINITION OF THE HIGH-LEVEL (GENERAL) SAFETY OBJECTIVES AND OVERALL SAFETY REQUIREMENTS (STEP 2) 31

1.3 PROBABILISTIC SAFETY TARGETS AND CRITERIA (STEP 3) 31

1.4 PLANT DESIGN (STEP 4) 31

1.5 IMPLEMENTATION OF DEFENCE IN DEPTH (DID) LEVELS (STEP 5) 32

1.6 LIST OF INITIATING EVENTS (STEP 6) 36

1.7 DETERMINISTIC EVALUATION OF SAFETY (STEP 7) 37

1.8 PROBABILISTIC EVALUATION OF SAFETY (STEP 8) 37

1.9 FINAL DESIGN (STEP 9) 37

LIST OF TABLE

Table 2-1 Indicative expected frequencies of occurrence of different plant states [2] 7

Table 3-1 Structure of the levels of DiD 17

Table A1-1 Assumed plant operational states 30

Table A1-2 Description and objectives of Defence in Depth 32

LIST OF FIGURES

Figure 3-1 Defence in depth visualisation 18

Figure A1-1 IDA - master logic diagram 29

Figure A1-2 Adjusted Flow chart for DID 34

Figure A1-3 Structure for DID provisions at each level of defence 35

INTRODUCTION

The document deals with the requirements for nuclear safety proposed for the ALLEGRO Generation IV. reactor type.

Requirements for ALLEGRO nuclear safety are intended to ensure “the highest standards of safety that can reasonably be achieved” for the protection of workers, the public and the environment from harmful effects of ionizing radiation that could arise from nuclear power plants and other nuclear facilities.

This requirement is valid for all current nuclear installations and is also guiding the development of the Generation IV type of nuclear reactors.

1 Safety Aproach

1.1 Generation IV International Forum safety goals

The overall safety and reliability goals for Generation IV Nuclear Energy Systems are explained in the Generation IV International Forum (GIF) Roadmap as follows:

- Generation IV nuclear energy systems operations will excel in safety and reliability.

  Safety and reliability during normal operation, and likely kinds of operational events that set forced outage rate.
- Generation IV nuclear energy systems will have a very low likelihood and degree of reactor core damage.

  Minimizing frequency of initiating events, and design features for controlling and mitigating any initiating events causing core damage.
- Generation IV nuclear energy systems will eliminate the need for offsite emergency response.

  Safety architecture to manage and mitigate severe plant conditions, for making small the possibility of releases of radiation.

1.2 General Safety Approach

To achieve the highest level of safety that can reasonably be achieved in the design of a nuclear power plant, measures are required to be taken to do the following, consistent with national acceptance criteria and safety objectives [1]:

- To prevent accidents with harmful consequences resulting from a loss of control over the reactor core or over other sources of radiation, and to mitigate the consequences of any accidents that do occur;
- To ensure that for all accidents taken into account in the design of the installation, any radiological consequences would be below the relevant limits and would be kept as low as reasonably achievable;
- To ensure that the likelihood of occurrence of an accident with serious radiological consequences is extremely low and that the radiological consequences of such an accident would be mitigated to the fullest extent practicable.

The ALLEGRO design, have been enhanced to include additional measures to mitigate the consequences of complex accident sequences involving multiple failures and of severe accidents. The ALLEGRO design explicitly includes the consideration of severe accident scenarios and strategies for their management.

1.3 Fundamentals Safety Functions

Safety functions are functions that are necessary to be performed for the facility or activity to prevent or mitigate radiological consequences of normal operation and anticipated operational occurrences and accident conditions.In a nuclear power plant there exist the following three fundamental safety functions:

- Control of reactivity;
- Removal of heat from the reactor and from the fuel store
- Confinement of radioactive material, shielding against radiation, as well as limitation of accidental radioactive releases.

2 Categories of Plant States

Plant states shall be identified and shall be grouped into a limited number of categories primarily on the basis of their frequency of occurrence at the nuclear power plant.

Plant states considered in design:

1. Normal operation;
2. Anticipated operational occurrences (AOO),
   which are expected to occur over the operating lifetime of the plant;
3. Design basis accidents;
4. Design extension conditions, including accidents with core melting.

Criteria shall be assigned to each plant state, such that frequently occurring plant states shall have no, or only minor, radiological consequences and plant states that could give rise to serious consequences shall have a very low frequency of occurrence.

Table 2-1 Indicative expected frequencies of occurrence of different plant states [2]

Plant state		Indicative expected frequency of occurrence
Normal operation		-
Anticipated operational occurrences		$> 10^{-2}$ events per year
Design basis accidents		$10^{-2} – 10^{-6}$ events per year
Design extension conditions	without significant fuel degradation	$10^{-4} – 10^{-6}$ events per year
	with core melt	$< 10^{-6}$ events per year

2.1 Normal operation

The safety analysis for normal operation is required to address all the plant conditions under which systems and equipment are being operated. This includes all the phases of operation for which the plant was designed to operate in the course of normal operations and maintenance over the life of the plant, both at power and shut down.

The normal operation of an NPP includes the following conditions:

- Initial approach to reactor criticality;
- Normal reactor start-up from shutdown through criticality to power;
- Power operation including both full and low power;
- Changes in the reactor power level including house load operation and load follow modes if employed;
- Reactor shutdown from power operation.

2.2 Anticipated operational occurrences

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

Anticipated operational occurrences are events more complex than the manoeuvres carried out during normal operation that have the potential to challenge the safety of the reactor. These occurrences might be expected to occur at least once during the lifetime of the plant. Generally they have a frequency of occurrence greater than 10–2 per reactor-year.

The anticipated operational occurrence of ALLEGRO includes the following:

- Spurious automatic or manual control rod withdrawal;
- Spurious starting of a DHR loop;
- Excessive helium surge flow rate;
- Primary circulator over-speed;
- Excessive heat extraction by secondary circuit;
- Partial loss of primary flow rate;
- Spurious discharge of helium in helium supply system tank including temporary decrease of primary pressure;
- Loss of station service power of duration shorter than 2 hours;
- Reduction of secondary gas flow rate;
- Reduction of secondary gas inventory;
- Reduction of air cooler flow rate;
- DHR circulation malfunction;
- Partial closing of DHR loop check valve;
- Fuel handling cooling malfunction;
- Abnormal leakage in primary circuit;
- Vessel cooling malfunction;
- Random first barrier failure;
- Spurious opening of a valve of the cooling system of fuel handling system

2.3 Design Basis Accidents (DBA)

A set of accidents that are to be considered in the design shall be derived from postulated initiating events for the purpose of establishing the boundary conditions for the nuclear power plant to withstand, without acceptable limits for radiation protection being exceeded.

Design basis accidents are postulated for the purpose of establishing the design bases of the safety systems.

Design basis accidents shall be used to define the design bases, including performance criteria, for safety systems and for other items important to safety that are necessary to control design basis accident conditions, with the objective of returning the plant to a safe state and mitigating the consequences of any accidents.

The design shall be such that for design basis accident conditions, key plant parameters do not exceed the specified design limits. A primary objective shall be to manage all design basis accidents so that they have no, or only minor, radiological consequences, on or off the site, and do not necessitate any off-site protective actions.

The design basis accidents shall be analysed in a conservative manner. This approach involves postulating certain failures in safety systems, specifying design criteria and using conservative assumptions, models and input parameters in the analysis.

- Automatic or manual control rod withdrawal at full power;
- Rupture of one or several tubes of main IHX;
- Rupture of one or several tubes of IHX of DHR loop;
- Core loading error;
- Spurious opening of Helium Supply System surge valve;
- Spurious starting of DHR loops;
- Break on secondary circuit;
- Loss of primary flow rate;
- Loss of station service power of duration shorter than 72 hours;
- Break on hot duct of primary circuit;
- Break on primary circuit;
- Break on a DHR loop;
- Opening of safety valve of primary circuit;
- Loss of secondary flow;
- Break on secondary circuit of DHR;
- Spurious opening of a safety valve of secondary circuit;
- DHR hot duct break;
- DHR circulation failure;
- Total insulation or check valve closing on a DHR loop;
- Loss of flow on fuel handling system;
- Break on Helium Supply System;
- Loss of top vessel cooling;
- Break of cooling system of handling fuel system;
- Control rod ejection;
- Spurious and concomitant starting of all DHR loops;
- Circulator rotor instantaneous blockage;
- Fuel assembly partial blockage;
- Break on hot duct of main loop;
- Nitrogen ingress in the core;
- Fuel assembly drop in vessel during core loading;

2.4 Design Extension Conditions (DEC)

Design Extension Conditions are those conditions not included in the DBAs, and which have a frequency of occurrence that cannot be neglected and in some cases comparable with the frequency of some DBAs.

A deviation from normal operation can escalate into DECs either due to extraordinary severity of the event itself or more typically due to multiple failures of safety systems caused either by equipment malfunctions or human errors.

A set of design extension conditions shall be derived on the basis of engineering judgement, deterministic assessments and probabilistic assessments for the purpose of further improving the safety of the nuclear power plant by enhancing the plant's capabilities to withstand, without unacceptable radiological consequences, accidents that are either more severe than design basis accidents or that involve additional failures. These design extension conditions shall be used to identify the additional accident scenarios to be addressed in the design and to plan practicable provisions for the prevention of such accidents or mitigation of their consequences.

The most plausible reason for the failure of safety functions (such as reactivity control and core cooling) is the occurrence of dependent failures that may cause the failure of redundant trains simultaneously. Common cause failures (CCFs) are a predominant group that are given high attention and provisions are implemented in the design either to eliminate them or reduce their likelihood to the extent possible or to cope with their consequences. Systematic analysis of dependences between SSCs important to safety is a good practice to conclude whether CCFs have been adequately considered.

Design Extension Conditions is a postulated plant state that is determined by a postulated sequence of events, and for the same reasons that design basis hazards are not considered DBAs, more severe hazards are not considered DECs although they might result in a DBA or possibly in DEC.

The control of DECs is expected to be achieved primarily by features implemented in the design (safety features for DECs) and not only by accident management measures that are using equipment designed for other purposes. This means that in principle a DEC is such if its consideration in the design leads to the need of additional equipment or to an upgraded classification of lower class equipment to mitigate the DEC.

Requirement 20 of SSR-2/1 [1] specifies that a set of DECs be considered in the NPP design derived on the basis of engineering judgement as well as deterministic and probabilistic assessment. Operating experience and lessons learned from accidents as well as research results are also important bases for the engineering judgement that informs the set of DECs.

2.4.1 Design extension conditions without significant fuel degradation

In general, at least three types of DECs can be considered according to the postulated assumptions:

- Very unlikely events that could lead to situations beyond the capability of safety systems for DBAs. In general however, the inclusion of specific safety features for DEC is necessary.
- Multiple failures (e.g. Common Cause failures s in redundant trains) that prevent the safety systems from performing their intended function to control the PIE. An example is LOCA without actuation of a safety injection system. The failures of supporting systems are implicitly included among the causes of failure of safety systems.
- Multiple failures that cause the loss of a safety system while this system is used to fulfil the fundamental safety functions in normal operation. This applies to those designs that use, for example, the same system for the heat removal in accident conditions and during shutdown.

The use of both deterministic and probabilistic insights is essential in the identification and control of DECs is an important approach. This combination of insights is an effective design technique whether considering the entire NPP design or evaluating a specific safety function such as the containment function. Due to the extensive operating experience with the light water technology, research results and the numerous risk assessment studies performed over time in Member States, there are some typical DECs without fuel degradation that are not strongly design-dependent and commonly postulated. The list, that in some countries is also referred to as deterministically identified, may include:

- ATWS;
- SBO;
- Loss of core cooling in the residual heat removal mode;

2.4.2 Design extension conditions with core melt

SSR-2/1 [1] requires that the design is such to ensure the capability to mitigate the consequences of severe degradation of the reactor core. Therefore, it is necessary to select a representative group of severe accident conditions (DECs with core melt) to be used for defining the design basis of the mitigatory safety features for these conditions.

For postulating the DECs to be considered in the design, the accident sequences that lead to core melt and the plant conditions at the onset of the core melt are clearly identified.

For DECs with core melt, maintaining the integrity of the containment is the main objective. This also implies that the cooling and stabilization of the molten fuel and the removal of heat from the containment need to be achieved in the long term.

2.5 Postulated Initiating Events

The design for the nuclear power plant shall apply a systematic approach to identifying a comprehensive set of postulated initiating events such that all foreseeable events with the potential for serious consequences and all foreseeable events with a significant frequency of occurrence are anticipated and are considered in the design.

The postulated initiating events shall be identified on the basis of engineering judgement and a combination of deterministic assessment and probabilistic assessment. A justification of the extent of usage of deterministic safety analysis and probabilistic safety analysis shall be provided to show that all foreseeable events have been considered.

The postulated initiating events shall include all foreseeable failures of structures, systems and components of the plant, as well as operating errors and possible failures arising from internal and external hazards, whether in full power, low power or shutdown states.

An analysis of the postulated initiating events for the plant shall be made to establish the preventive measures and protective measures that are necessary to ensure that the required safety functions will be performed.

The expected behaviour of the plant in any postulated initiating event shall be such that the following conditions can be achieved, in order of priority:

1. A postulated initiating event would produce no safety significant effects or would produce only a change towards safe plant conditions by means of inherent characteristics of the plant.
2. Following a postulated initiating event, the plant would be rendered safe by means of passive safety features or by the action of systems that are operating continuously in the state necessary to control the postulated initiating event.
3. Following a postulated initiating event, the plant would be rendered safe by the actuation of safety systems that need to be brought into operation in response to the postulated initiating event.
4. Following a postulated initiating event, the plant would be rendered safe by following specified procedures

The postulated initiating events used for developing the performance requirements for the items important to safety in the overall safety assessment and the detailed analysis of the plant shall be grouped into a specified number of representative event sequences that identify bounding cases and that provide the basis for the design and the operational limits for items important to safety.

A technically supported justification shall be provided for exclusion from the design of any initiating event that is identified in accordance with the comprehensive set of postulated initiating events.

Where prompt and reliable action would be necessary in response to a postulated initiating event, provision shall be made in the design for automatic safety actions for the necessary actuation of safety systems, to prevent progression to more severe plant conditions.

Where prompt action in response to a postulated initiating event would not be necessary, it is permissible for reliance to be placed on the manual initiation of systems or on other operator actions. For such cases, the time interval between detection of the abnormal event or accident and the required action shall be sufficiently long, and adequate procedures (such as administrative, operational and emergency procedures) shall be specified to ensure the performance of such actions. An assessment shall be made of the potential for an operator to worsen an event sequence through erroneous operation of equipment or incorrect diagnosis of the necessary recovery process.

The operator actions that would be necessary to diagnose the state of the plant following a postulated initiating event and to put it into a stable long term shutdown condition in a timely manner shall be facilitated by the provision of adequate instrumentation to monitor the status of the plant, and adequate controls for the manual operation of equipment.

The design shall specify the necessary provision of equipment and the procedures necessary to provide the means for keeping control over the plant and for mitigating any harmful consequences of a loss of control.

Any equipment that is necessary for actions to be taken in manual response and recovery processes shall be placed at the most suitable location to ensure its availability at the time of need and to allow safe access to it under the environmental conditions anticipated.

2.5.1 Internal and external hazards

All foreseeable internal hazards and external hazards, including the potential for human induced events directly or indirectly to affect the safety of the nuclear power plant, shall be identified and their effects shall be evaluated. Hazards shall be considered in designing the layout of the plant and in determining the postulated initiating events and generated loadings for use in the design of relevant items important to safety for the plant.

Items important to safety shall be designed and located, with due consideration of other implications for safety, to withstand the effects of hazards or to be protected, in accordance with their importance to safety, against hazards and against common cause failure mechanisms generated by hazards.

For multiple unit plant sites, the design shall take due account of the potential for specific hazards to give rise to impacts on several or even all units on the site simultaneously.

Internal hazards

The design shall take due account of internal hazards such as fire, explosion, flooding, missile generation, collapse of structures and falling objects, pipe whip, jet impact and release of fluid from failed systems or from other installations on the site. Appropriate features for prevention and mitigation shall be provided to ensure that safety is not compromised.

External hazards

The design shall include due consideration of those natural and human induced external events (i.e. events of origin external to the plant) that have been identified in the site evaluation process. Causation and likelihood shall be considered in postulating potential hazards. In the short term, the safety of the plant shall not be permitted to be dependent on the availability of off-site services such as electricity supply and firefighting services. The design shall take due account of site specific conditions to determine the maximum delay time by which off-site services need to be available.

3 Defence in Depth

Defence in depth consists of recognizing that technical, human or organizational failures may occur in a demonstrator lifetime and to guard against them by introducing successive lines of defence.

The defence in depth concept is not to be understood as merely limited to the request for the implementation of a number of consecutive barriers and protection levels, but is to be understood as the main general principle that leads to the formulation of safety requirements including requirements necessary to achieve the quality and reliability expected for the barriers and for systems ensuring their integrity.

Prevention and mitigation are terms widely used in nuclear safety and they are mostly referred to accidents (prevention of accidents and mitigation of the consequences of accidents). With references to defence in depth, the essential means of each level prevent the need for activation of the essential means of the following level and, at the same time, they mitigate the consequences of the failure of the previous ones. Level 1, being the first level, has a predominant preventive function and level 5, being the last, has only a mitigatory function.

The concept of defence in depth as used in the IAEA Safety Standards is mainly based on INSAG-10 [3] and SSR-2/1 [1].

3.1 Levels of Defence in Depth

3.1.1 First level

The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices. To meet these objectives, careful attention is paid to the selection of appropriate design codes and materials, and to the quality control of the manufacture of components and construction of the plant, as well as to its commissioning. Design options that reduce the potential for internal hazards contribute to the prevention of accidents at this level of defence. Attention is also paid to the processes and procedures involved in design, manufacture, construction, and in-service inspection, maintenance and testing, to the ease of access for these activities, and to the way the plant is operated and to how operating experience is utilized. This process is supported by a detailed analysis that determines the requirements for operation and maintenance of the plant and the requirements for quality management for operational and maintenance practices.

The essential means required to meet the objective of the level 1 of defence in depth are, as indicated in Table 3-1, a conservative design and high quality in construction and operation. More generally this level includes all provisions implemented to avoid challenging the subsequent levels by preventing equipment failure, system malfunctioning and human errors. The need of an effective plant control system is not explicitly mentioned in the description of level 1 in SSR-2/1 [1]. The control system has the functions to maintain the values of the process parameters inside the normal operation range and to prevent abnormal operations. Malfunctioning of the control system are among the main causes of AOOs, therefore this system and the systems designed to control AOOs are not included in the same level of defence. The reliability of the equipment of level 1 of defence in depth is in general expected to be such that frequency of occurrence of an AOO is less than 1/reactor-year and the frequency of occurrence of accident caused by equipment failure less than 10-2 /reactor-year. Accidents not considered for the design of the plant are expected to have a likelihood that is very low. Although the level 1 of defence in depth is normally associated with normal operation, the essential means of this level such as conservative design and high quality in construction and operation are understood as applied also to SSCs that are designed for other plant states.

3.1.2 Second level

The purpose of the second level of defence is to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions.

This is in recognition of the fact that postulated initiating events are likely to occur over the operating lifetime of a nuclear power plant, despite the care taken to prevent them. This second level of defence necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or otherwise to minimize their consequences, and to return the plant to a safe state.

For level 2 the intervention of the limitation or protection system may be necessary for the shutdown of the reactor power to control some postulated abnormal conditions. Modern designs avail on a limitation system that reacts upon some perturbations of the normal operation regime that cannot be handled by the control systems, preventing or delaying a reactor trip by quickly reducing the power of the reactor and providing signals to key plant systems and components to stabilize the plant. For most reactor designs, the reactor trip system is a safety system that is also required for the control of accidents at the Level 3 of defence in depth.

Also a typical AOO like the loss of off-site power requires either the house-load operation or the intervention of the onsite emergency power that has also relevant functions on level 3. This shows specific cases of difficulty to implement independence between level 2 and level 3 of defence in depth.

Equipment of level 2 of defence in depth is aimed at reducing the number of challenges to the defence in depth level 3. Their reliability is at least expected to be such that level 3 of defence in depth is not necessary to intervene with a frequency higher than 10-2 per reactor-year. In practice, the frequency of an evolution from and AOO into an accident condition is expected to be lower.

3.1.3 Third level

For the third level of defence, it is assumed that, although very unlikely, the escalation of certain anticipated operational occurrences or postulated initiating events might not be controlled at a preceding level and that an accident could develop. In the design of the plant, such accidents are postulated to occur. This leads to the requirement that inherent and/or engineered safety features, safety systems and procedures be capable of preventing damage to the reactor core or preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state.

In this approach it is considered that level 3 deals with the mitigation of those postulated accident conditions the evolution of which can be controlled and the core melt prevented. This means that these accident conditions include DBAs and DECs without core melt. For practical purposes the Level 3 of defence in depth is considered as formed by two sub levels indicated as Design Basis Accident (DBA) and DEC-A without core melt. The distinction of DBAs and DEC-A without core melt serves to achieve a better alignment the design rules for safety systems and for safety features for DECs may be different as well as the acceptance criteria for DBAs and for DEC-A. If there were no differences, the safety features for DEC would be just additional safety systems.

The essential means of achieving the objective of level 3 (DBA) are the safety systems and the accident procedures for DBAs. The safety systems are designed with a set of conservative, prescriptive rules and criteria (e.g. application of the single failure criterion) which provide high confidence in their success to meet the relevant acceptance criteria and safety limits. The reliability of equipment of level 3 (DBA) of defence in depth is expected to be such that the probability of failure per demand of level 3 (DBA) is in the range of 10-3 - 10-4 [2]. DEC-A without core melt can typically be generated by multiple failures occurring in safety systems either in normal operation (e.g. loss of RHR during shutdown) or following an AOO or a DBA. It is important to note that in some cases the failure of level 2 can lead directly to level 3 (DEC-A) (e.g. ATWS, SBO) because some safety systems might be shared between level 2 and level 3 (DBA).

Level 3 (DEC-A) is mainly aimed at ensuring that for complex sequences based on internal events. Therefore level 3 (DEC-A) is further enhancing the prevention of core melt implemented by the previous level of defence in depth. Design rules for SSCs for level 3 (DEC-A) may be less conservative than those for level 3 (DBA).

It is understood that level 4 deals with the control of severe accidents and the major objective of level 4 is to mitigate the consequences of DEC-B (with core melt). The essential means of achieving the objective of level 4 include safety features for DECs and severe accident management procedures and guidelines.

DEC-B (with core melt), i.e. severe accidents, may be caused by the failure of level 3. A DEC-B (with core melt) is expected not to result directly from failures of level 2.

Additionally, since in SSR-2/1 [1], the single failure criterion is required to be applied to each safety group, the application of this criterion is not required for the safety features for DEC because they are not considered as part of the safety group. It holds, however, the requirement that the reliability of any item important to safety shall be commensurate to its significance to safety. Equipment belonging to defence in depth level 4 is implemented to limit the radiological releases in case of core melt and is aimed at maintaining the confinement functions.

Accident management encompasses both hardware and procedures necessary to maintain the radiological release as low as reasonably possible in any accident. In particular SSR-2/1 [1] requires (Requirement 67) the implementation of a Technical Support Centre (TSC) to provide technical support to the operation staff during accident conditions. Given its function, the Technical Support Centre is an important feature for the level 4 of the defence in depth.

3.1.4 Fourth level

The purpose of the fourth level of defence is to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident. The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release are required to be ‘practically eliminated.

3.1.5 Fifth level

The purpose of the fifth level of defence is to mitigate the radiological consequences of radioactive releases that could potentially result from accidents. This requires the provision of adequately equipped emergency response facilities and emergency plans and emergency procedures for on-site and off-site emergency response.

A relevant aspect of the implementation of defence in depth for a nuclear power plant is the provision in the design of a series of physical barriers, as well as a combination of active, passive and inherent safety features that contribute to the effectiveness of the physical barriers in confining radioactive material at specified locations. The number of barriers that will be necessary will depend upon the initial source term in terms of the amount and isotopic composition of radionuclides, the effectiveness of the individual barriers, the possible internal and external hazards, and the potential consequences of failures.

3.2 Summary of levels of Defence in Depth

Table 3-1 Structure of the levels of DiD

	Plan states considered in design					Conditions Beyond the Design Basis (Practically eliminated)
Plant State	Operational States		Accident Conditions			
	Normal operation (NO)	Anticipated operational occurrences (AOO)	Design basis accidents (DBA)	Design Extension Conditions: DEC-A Without significant fuel degradation	Design Extension Conditions: DEC-B With core melting	
Level of Defence in Depth	Level 1	Level 2	Level 3		Level 4	Level 5
Frequency of occurrence	-	> 10^{-2} events per year	10^{-2} – 10^{-6} events per year	10^{-4} – 10^{-6} events per year	< 10^{-6} events per year	-
Strategy	Accident prevention		Accident mitigation			
Objective	Prevention of abnormal operation	Control of abnormal operation	Control of accidents		Control of severe plant conditions	Mitigation of radiological consequences
Essential design means	Conservative design and high quality in construction of normal operation systems, including monitoring and control systems	Limitation and protection systems and other surveillance features	Engineered safety features	Safety features for design extension conditions without core melt	Safety features for design extension conditions with core melt. Technical Support Centre	On-site and off-site emergency response facilities
Procedures	Normal Operating Procedures	Procedures for Abnormal States	Emergency Operating Procedures		Severe Accident Management Guidelines	Off-site emergency response procedure
Response	Normal Operating Systems		Safety Systems		Engineering safety features for DEC-Bs	Off-site emergency preparations
Criteria for maintaining integrity of barriers	No failure of any of the physical barriers except minor operational leakages		No consequential damage of the reactor coolant system, maintaining containment integrity, limited damage of the fuel		Maintaining containment integrity	Containment integrity severely impacted, or containment disabled or bypassed

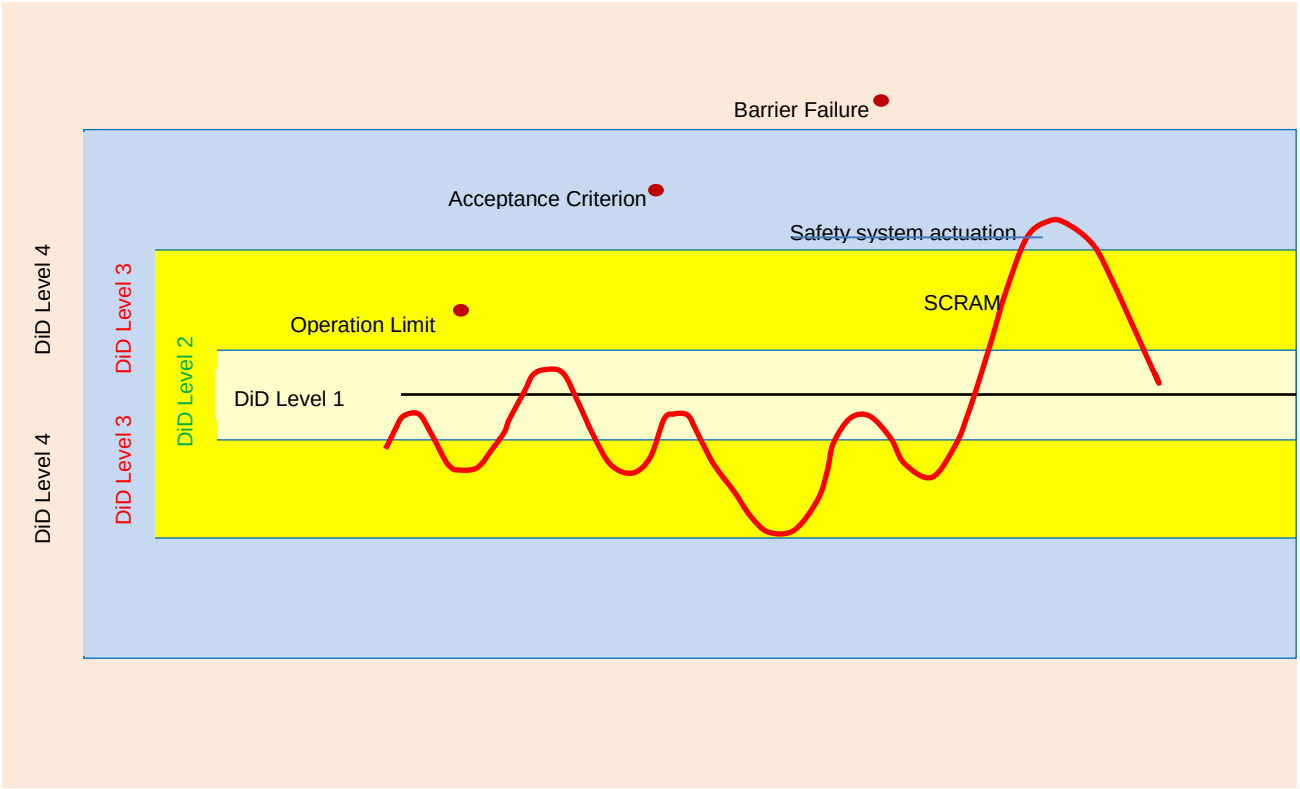


Figure 3-1 Defence in depth visualisation

3.3 Independence Between all Levels of Defence-in-Depth

Enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately as addressed in the previous three objectives) to provide, as far as reasonably achievable, an overall reinforcement of defence-in-depth.

The levels of defence in depth shall be independent as far as practicable to avoid the failure of one level reducing the effectiveness of other levels. In particular, safety features for design extension conditions (especially features for mitigating the consequences of accidents involving the melting of fuel) shall as far as is practicable be independent of safety systems Independence between systems, structures and components (SSCs)

It is considered that independent SSCs for safety functions on different DiD levels shall possess both of the following characteristics:

- the ability to perform the required safety functions is unaffected by the operation or failure of other SSCs needed on other DiD levels;
- the ability to perform the required safety functions is unaffected by the occurrence of the effects resulting from the postulated initiating event, including internal and external hazards, for which they are required to function;

As a consequence, the means to achieve independence between SSCs are adequate application of:

- diversity;
- physical separation, structural or by distance;
- functional isolation.

The following expectations on independence are related to the independence between SSCs as credited in the deterministic safety demonstration. If an accident was to occur, all available and effective equipment could obviously be used, including those not credited in the safety demonstration.

Basic safety expectations on the independence between different levels of DiD

- There shall be independence to the extent reasonably practicable between different levels of DiD so that failure of one level of DiD does not impair the defence in depth ensured by the other levels involved in the protection against or mitigation of the event.
- The adequacy of the achieved independence shall be justified by an appropriate combination of deterministic and probabilistic safety analysis and engineering judgement. For each postulated initiating event (starting with DiD level 2), the necessary SSCs should be identified and it shall be shown in the safety analysis that the SSCs credited in one level of DiD are adequately independent of SSCs credited in the other levels of DiD.
- Appropriate attention shall be paid to the design of I&C, the reactor auxiliary and support systems (e. g. electrical power supply, cooling systems) and other potential cross cutting systems. The design of these systems shall be such as not to unduly compromise the independence of the SSCs they actuate, support or interact with.

Implementation of the basic safety expectations

In applying the above basic expectations, the following considerations shall be taken into account:

- SSCs fulfilling safety functions in case of postulated single initiating events (DiD level 3 DBA) or in postulated multiple failure events (DiD level 3 DEC-B) should be independent to the extent reasonably practicable from SSCs used in normal operation (level 1) and/or in anticipated operational occurrences (level 2). This independence is so that the failure of SSCs used in normal operation and/or in anticipated operational occurrences does not impair a safety function required in the situation of a postulated single initiating event or of a multiple failure event resulting from the escalation of such failures during normal operation or a level 2 event.
- SSCs fulfilling safety functions used in case of postulated single initiating events (DiD level 3 DBA) should be independent to the extent reasonably practicable from additional safety features used in case of postulated multiple failure events (DiD level 3 DEC-B). For the safety analyses of postulated multiple failure events, credit may be taken from SSCs used in case of postulated single initiating events as far as these SSCs are not postulated as unavailable and are not affected by the multiple failure event in question; SSCs specifically designed for fulfilling safety functions used in postulated multiple failure events should not be credited for level 3 DBA event analyses for the same scenario.
- Complementary safety features specifically designed for fulfilling safety functions required in postulated core melt accidents (DiD level 4) should be independent to the extent reasonably practicable from the SSCs of the other levels of DiD.

4 Systems, Structures and Components

In compliance with IAEA Guides and relevant national regulations, for purpose of NPP systems, structures and components the proper selection is essential. The most important task is establishment their classification from the viewpoint of their importance for nuclear safety assurance.

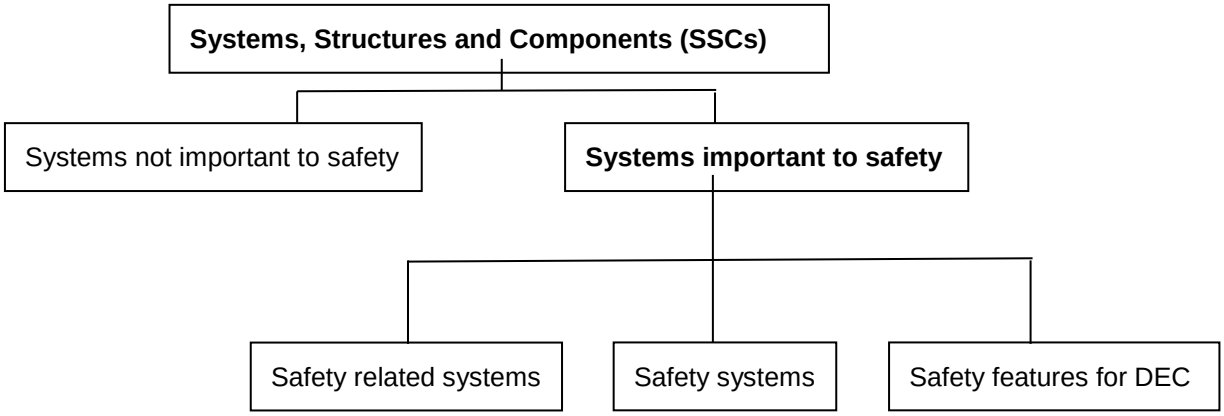
Such classification forms the basis for classification and qualification of the equipment either from the viewpoint of quality, seismicity or from that one of surrounding environment in which that equipment must perform required functions.

Establishment of a selected equipment list is required with respect to single equipment function to be ensured. That is why classification of technological systems shall be performed from the viewpoint of their functions. Furthermore, for each system must be selected such equipment, which is needed (necessary) for fulfilment of safety functions of given system.

In the sense of IAEA Guides and in agreement with common practice, division performed with respect to applied systems, structures and components includes both those ones meeting requirements on nuclear safety assurance and systems ensuring the electric energy production technological process as such.

From the nuclear safety assurance viewpoint, the systems (equipment) are divided as follows:

- Systems important in terms of nuclear safety (they fulfil at least one of safety functions)
- Systems non-important in terms of nuclear safety (they do not fulfil any safety function)



4.1 Safety Systems

Safety systems are systems providing safety functions in order to ensure safe shutdown of a reactor, remove residual heat from the core or limit the consequences of an abnormal operation and design basis accident during expected events (seismic event, fire, windstorm, flood, failure of important equipment and accident in NPP). Safety systems should be designed and operated in a such way that the fulfilment of safety functions will not be threatened for example by simple failure (redundancy) or common cause failure (diversity).

Safety systems represent a set of systems, which includes:

- Protective and control systems of active safety systems - systems monitoring the operation of the reactor unit and in case of abnormal conditions, these systems automatically initiate actions to avoid dangerous or potentially dangerous conditions (instrumentation for measurement and/or monitoring of safety important variables or nuclear installation states /nuclear safety/, as well as for automatic activation of relevant safety systems with the objective to ensure and keep nuclear system in safe state).

- Active (action) safety systems - the systems which after initiation from protective and control systems realize relevant safety functions. Nevertheless the active equipment of safety systems include only such equipment, which are necessary for fulfilment of given safety function.
- Supporting (auxiliary) systems - they provide functions of protective and active safety systems (such as power supply /feeding/, cooling, lubrication, etc.).

4.2 Safety Related Systems

Safety related systems are systems which create conditions for the fulfilment safety functions.

Safety related systems represent a set of systems, which includes:

- Protective and control systems - they control and switch-on both active safety related systems, as well as other safety non-important systems and equipment
- Active (action) safety related systems and structures
- Supporting (auxiliary) systems for safety related systems (such as power supply /feeding/, cooling, lubrication, etc.)

From the power supply source need viewpoint, all systems in NPP can be divided into active and passive. The principle is respected, that where the safety systems require for fulfilment of their safety functions functionality of another equipment (system), it is at the same time required also functionality of the equipment/systems ensuring supporting functions for safety systems (power and media supply, lubrication, etc.). However, it is not necessary to impose the same requirements on the supporting equipment/system as on the equipment/systems which is supported or ensured by it. It means, that the supporting systems from the range of electric feeding and control are classified in such a case as safety systems and requirements on them are identical with those ones, imposed on the system which they support by their.

4.3 Safety Principles applicable to the Design of Structures, Systems and Components

Safety systems designed to mitigate design basis conditions make use of redundancy or diversity and physical or geographical separation of redundant components. This principle is applied to ensure that safety actions are performed even in case of component failure.

Systems and components are inspected and regularly tested to reveal degradation that may lead to abnormal conditions or inadequate performance.

Systems and components are designed, constructed and tested according to quality standards commensurate with their importance to safety. The corresponding rules are based on the experience gained from previous generation plants.

The design criteria can be summarized as follows:

Simplicity and functional separation:

- The separation of functions is applied, as far as appropriate;
- Contradictory demands on valves in the short term are avoided as a basic principle.

Redundancy and diversity:

- Safety systems are designed to accomplish their safety functions even in case of a component failure or component unavailability (e.g. single failure or preventive maintenance);
- Diversity of systems and components is applied as much as possible to cope with the risk resulting from common cause failures. Priority is given to functional diversity over equipment diversity.

Divisional separation:

- Redundant trains of safety systems are arranged in separated divisions. The divisional separation is also extended to supporting systems such as helium storage & make-up system, power supply and I&C;
- The divisions are without interconnections up to the connection to the primary circuit, secondary circuit (or tertiary circuit).

Low sensitivity to failures, including human errors:

- Adequate design margins, automation and grace periods, high reliability of the devices in their working environment are implemented;
- Protection against common mode failures against load cases (e.g. earthquake) is provided by design;
- High autonomy allows large grace periods for operator actions;
- Man-machine interface is improved.

4.4 Single Failure

A single failure is a random failure and its consequent effects which are assumed to occur either during normal operation or in addition to an initiating event and its consequences. In assessing the consequences of an initiating event and a single failure, the possible interdependence of the system's redundant sub-systems shall be considered. In particular, cross-connections between the subsystems and connections to systems having no bearing on nuclear safety shall be considered. In the application of the failure criteria, two failure types shall be analysed, certain exceptions excluded. Both component functional failures i.e. active failures and passive failures, which may occur when a system or a component is in the process of carrying out its safety function, shall be considered.

A functional failure is a malfunction relating to the changed state of a component or its part. A component functional failure may occur e.g. when the component's functioning requires the mechanical movement of some part. The passive failure of a mechanical component or a fluid or gas system may be the loss of component or structural integrity or the clogging up of a flow path. A design basis passive failure shall be defined by analysing the possible failure and leak modes in such a way that a system's operational conditions are appropriately taken into account. For example, the failure of a pump or a valve sealing, or the rupture of a small-diameter pipe can be defined as the most design basis passive failure if, based on a system's operational conditions plus the design, manufacture and inspection of components and structures, it can be demonstrated that failures worse than these are highly unlikely.

4.4.1 Definition of active and passive single failures

A single failure may be an active or a passive failure. Active failures are considered for mechanical, electrical and I&C components performing safety functions while passive failures are considered for mechanical components only.

Active failure

Active failure is defined as a failure or a mispositioning sufficient to prevent equipment from performing its function.

Such a fault can be revealed in case of an initiating event and may consist of:

- Malfunction of a mechanical or electrical component which relies on mechanical movement to complete its intended function upon demand;
- Malfunction of a I&C component.

Spurious operation of a component is not taken into account in the frame of the single failure criterion but are considered in the design of the I&C system as an initiating event.

Human errors are not considered as a single failure, but are taken into account in the design of the I&C systems.

Passive failure

A passive failure is defined as a failure of equipment not demanding a mechanical movement to perform the required action. The passive failure is postulated in the long-term phase of an incident or accident. In other words a passive failure is postulated 24 hours after the initiating event.

The following are examples of passive failures:

- Failure of the pressure boundary of a fluid system resulting in certain flowrate up to its isolation. This failure, if not detected and isolated, develops to the flow corresponding to a full rupture,
- Other mechanical failures impairing the normal process flow of a fluid system. For electrical and I&C systems, any failure is considered as an active failure.

Exceptions to the single failure criterion

The single failure criterion is not applied in the following cases:

- For the containment isolation function in the demand mode.
- Other cases to be determined, if necessary.

4.5 Common Cause Failures (CCFs)

Requirement 24 of SSR-2/1 [1] states that “The design of equipment shall take due account of the potential for common cause failures of items important to safety, to determine how the concepts of diversity, redundancy, physical separation and functional independence have to be applied to achieve the necessary reliability.”

CCFs are used to designate failures of two or more redundant components of the same kind due to a number of different causes excluding those indicated before, that can take place simultaneously or close enough in time24 for the redundant components to fail to fulfil their required function following a PIE.

CCFs are relevant when they affect redundant equipment or provisions belonging to different levels of defence.

CCF is not used to designate for instance the failure of several components in a system due to the failure of a support system, e.g. power supply. This would be considered a functional dependence.

It addresses also the root causes of CCFs, the coupling mechanisms and defensive measures that could be adequate for each of them. Redundant equipment within a system is more exposed to commonalities in design, operational and maintenance practices. Other factors, such as internal or external hazards can affect several plant systems. Safety systems, in general, rely upon redundancy, functional independence, robust design and physical separation to ensure high reliability. Diversity is usually a measure applied to reduce the likelihood of CCFs between different levels of defence in depth.

Functional independence between different levels of defence in depth is an aspect that cannot be taken for granted as it has been a frequent practice to share systems between different levels of defence.

Functional independence, diversity, for instance on instrumentation, power supply or heat sink, as well as stronger safety margins and protection against external hazards, are among the measures to prevent CCFs from stretching through different levels of defence in depth.

5 Design Limits

A set of design limits consistent with the key physical parameters for each item important to safety for the nuclear power plant shall be specified for all operational states and for accident conditions.

The design limits shall be specified and shall be consistent with relevant national and international standards and codes, as well as with relevant regulatory requirements.

CONCLUSION

Adfffff

ABBREVIATIONS

AOO	Anticipated Operational Occurrences
CCF	Common Cause Failure
DBA	Design Basis Accident
DEC	Design Extension Conditions
DiD	Defence in Depth
DHR	Decay Heat Removal system
GIF	Generation IV International Forum
IHX	Internal Heat Exchanger
LOCA	loss of coolant accident
LOFA	loss of flow accident
NO	Normal operation
NPP	Nuclear Power Plant
PIE	Postulated Initiating Events

REFERENCES

[1] IAEA,: Safety of Nuclear Power Plants: Design. Specific Safety Requirements No. SSR-2/1 (Rev. 1) Vienna, 2016.

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

[3] IAEA, Defence in Depth in Nuclear Safety, INSAG Series No. INSAG-10, IAEA. Vienna 1996.

[4] Safety Objectives for New Power Reactors, WENRA, 2009

[5] IAEA, Fundamental Safety Principles No. SF-1, Vienna, 2006

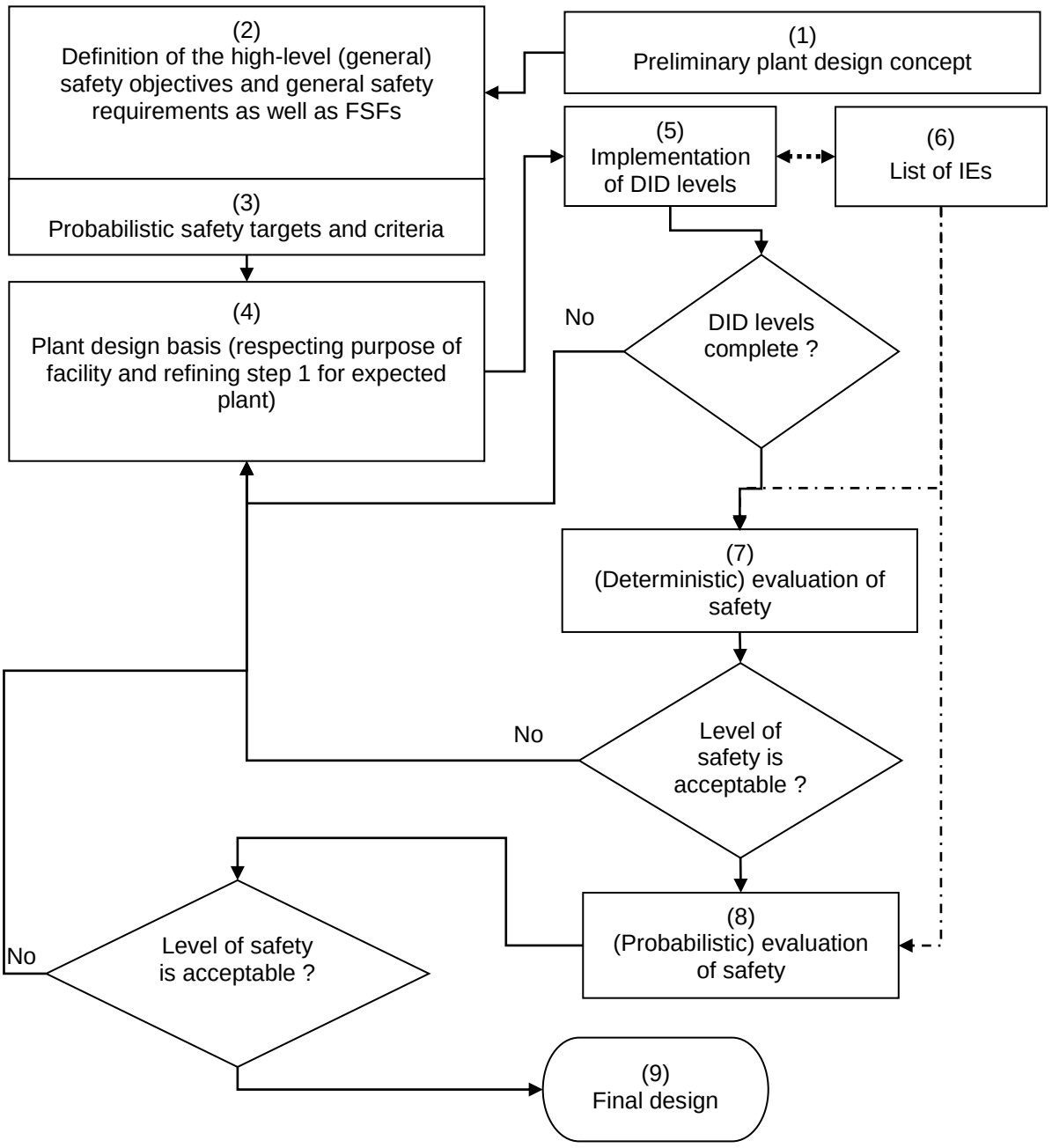
[6] x

ANNEX 1 INTEGRATED DESIGN APPROACH

1 Introduction

General outline of INTEGRATED DESIGN APPROACH is outlined in the next picture.

Figure A1-1 IDA - master logic diagram



Any design process in real life consists from many interacting simultaneous tasks that are deeply interconnected and create design that allows implementing DID levels having extra design requirements. So it is noted that even if Fig. 0 1 is presented like linear algorithm there can be many interactions (especially steps 5 and 6) and several iterations from steps 4 to 8.

1.1 Preliminary plant design concept (step 1)

Preliminary design concept forms realization of initial engineering idea, e.g. power reactor, research reactor cooled by gas etc.

In spite of fact that plant design shall contains appropriate safety features Preliminary plant design concept is focused mainly on physical phenomena (fast breaded reactor, gas colled) and the purpose of plant (e.g. energy production) and does not deal with safety provisions like DID etc.[1]

Aim and output of this step is to provide basic technical data (primary design basis data) describing principles of **robust** design of technological part of plant that is intended for nominal operational state with respect to [1], e.g. design basis of reactor including

- Reactor type and cooling media
- Number of loops
- Fuel and core properties
- I&C principles
- Further details regarding heat sink, i.e. concept of secondary circuit design
- Scope of expected working conditions including average and limit values of parameters describing overall nominal conditions, e.g. power, pressures, temperatures, flow rates etc.
- AC for foreseen operational states etc.
- If possible the preliminary design should also take into account anticipated plant operational states, see Table A1-1, as much as possible.

Table A1-1 Assumed plant operational states

Level	(Operational) state / mode / conditions	Criteria[2]	Note
1	Normal operation (Nominal (power or shutdown state)[3])	Criteria for normal state must be defined	§ 5.1
2	Abnormal operation / Anticipated operational occurrences	Criteria for normal state were violated and criteria for abnormal state are maintained. Such criteria must be defined in forward at preparation plant design concept.	
3	Design basis accidents	Criteria for abnormal operational state were violated and criteria for design basis accident are maintained. Such criteria must be defined in forward before DID levels are implemented, e.g. 1. Fuel is not substantially degraded, degradation of core is avoided and integrity of reactor and primary circuit is maintained 2. Occurred state is stable and can be controlled 3. There is a way to put plant into absolute safe state or return to normal state	Requirement 19
4	Design extension conditions	Criteria for design basis accident were violated and criteria for design extension conditions are maintained Such criteria must be defined in forward, e.g.	Requirement 20

[1] It is obvious that this one is idealization of reality. However; based on experience from nuclear field and requirements on nuclear safety preliminary concept should consider reactor shielded by containment(s), separation of plant technology between primary and secondary circuit, locations to install potential safety systems etc. in order to minimize to redone design work in step 4.

[2] [1] § 5.2

[3] It should be obvious that normal state can have several modes like full power operation, shutdown modes, refueling mode etc.

		4. Containment is available / functional 5. Occurred state is stable and can be controlled 6. There is a way to put plant into absolute safe state	
5	Sever accident conditions	Criteria for design for design extension conditions were violated	

1.2 Definition of the high-level (general) safety objectives and overall safety requirements (step 2)

In general this step; even if very important; is formal obligatory activity driven mainly by**.** In accordance with the aim of this step is to establish the fundamental safety objective, safety principles and concepts that will be followed during IDA to ensure fulfilment of principal technical requirements from [5]**,** i.e.

- Fundamental Safety Functions
- Radiation protection
- Design for a nuclear power plant
- Application of defence in depth
- Interfaces of safety with security and safeguards

1.3 Probabilistic safety targets and criteria (step 3)

Determination of probabilistic safety targets and criteria will be affected by legal and regulatory framework of particular country. Determination of targets and criteria should covers following areas:

- Criteria for CDF and LRF[4] including exact definition what is meaning of CDF and LRF[5].
- General criteria for availability of safety systems (reactor trip, activation and availability of safety functions)[6]

1.4 Plant design (step 4)

The aim of this step is refinement of overall plant design from step 1 in order to:

1. Propose overall robust self-contained design to meet safety objectives and general safety requirements from step 2 as well as probabilistic criteria from step 3.
2. Create favorable condition to implement DID levels, i.e. design basis should take into account general experience to avoid redone design basis as much as possible.

---

[4] This document does not treat topic early release. In compliance with fundamental safety principles release time point is irrelevant.

[5] Consistency between definition CDF (LERF) and acceptance criteria for success of DID3 (DID4) should be maintained, see 1.5

[6] It is essential clearly stated what is subject of safety assessment / analyses. It is also obvious that there will be interactions with several steps from approach in Table A1-1 It is also noted that criteria for availability (reliability) of SSCs shoud be based on realistic assumptions to be technically achievable.

Design basis is such complex activity, e.g. see § 1.4, § 2.8, § 2.15, Requirement 1: Responsibilities in the management of safety in plant design, Requirement 2: Management system for plant design in [5], that it is not possible to create a simple guide how to approach. That is the reason why [5] lists just set of requirements that shall be fulfilled and not links particular requirements to the certain parts of design process. So it is necessary to take following points:

1. Purpose of IDA is to provide plant design basis including DID implementation even if DID implementation is (formally) part of step 5.
2. Step 4 will be certainly repeated several time to refine design basis. The first design as well as several further designs will be just tentative designs that will be modified based on results of step 5 to 8.
3. According § 2.17. in [1]: *In practice, the design of a nuclear power plant is complete only when the full plant specification (including site details) is produced for its procurement and licensing. It implies:* **Each time when step 4 will be finished fulfilment of all (appropriate) requirements from [1] shall be checked.**

Output of step 4 are design basis data which specify primary data from step 1.

1.5 Implementation of Defence In Depth (DID) levels (step 5)

Aim of this step is, in accordance with [1], to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure occurs then it would be detected and compensated or corrected by appropriate measures on higher DID level. Eventually safety state will be maintained.

In general correct implementation of DID (i.e. the adoption of an adequate safety architecture) ensures that the FSFs are reliably achieved[7] with sufficient margins to mitigate impact of IEs.

In any case objective of particular DID levels shall be clearly stated limits (set of measurable parameters that allows to evaluate successful function or initiates transition into next DID level), see next table.

Table A1-2 Description and objectives of Defence in Depth

Level	Description of level	Objective / Purpose / function of DID level	Note
1	Prevention of abnormal operation and failures	Maintain Normal Operating Conditions[8]	*Success: Normal operation*
2	Control of abnormal operation and detection of failures	Return plant state to normal Operating Conditions	*Success: Return to normal operation after recovery from failure.* *Prevention of progress of AOOs*
3	Control of accidents within the design basis conditions	Mitigating a consequence of Abnormal Operation Conditions in order to avoid fuel damage and create controllable state which enables reaching Controllable Safe Long Term State (or return to normal state)	*Success: Accident consequences limited within the design basis.* Definition of Safe Long Term State conditions (ACs) for DID3 success state should be determined.

[7] If reliability, what is of course qualitative term, is defined as a probability that SSC will be able to fulfil its intended function at given conditions than deterministic analyses; even if they respect any principles are not capable of answering question whether FSFs are reliably achieved

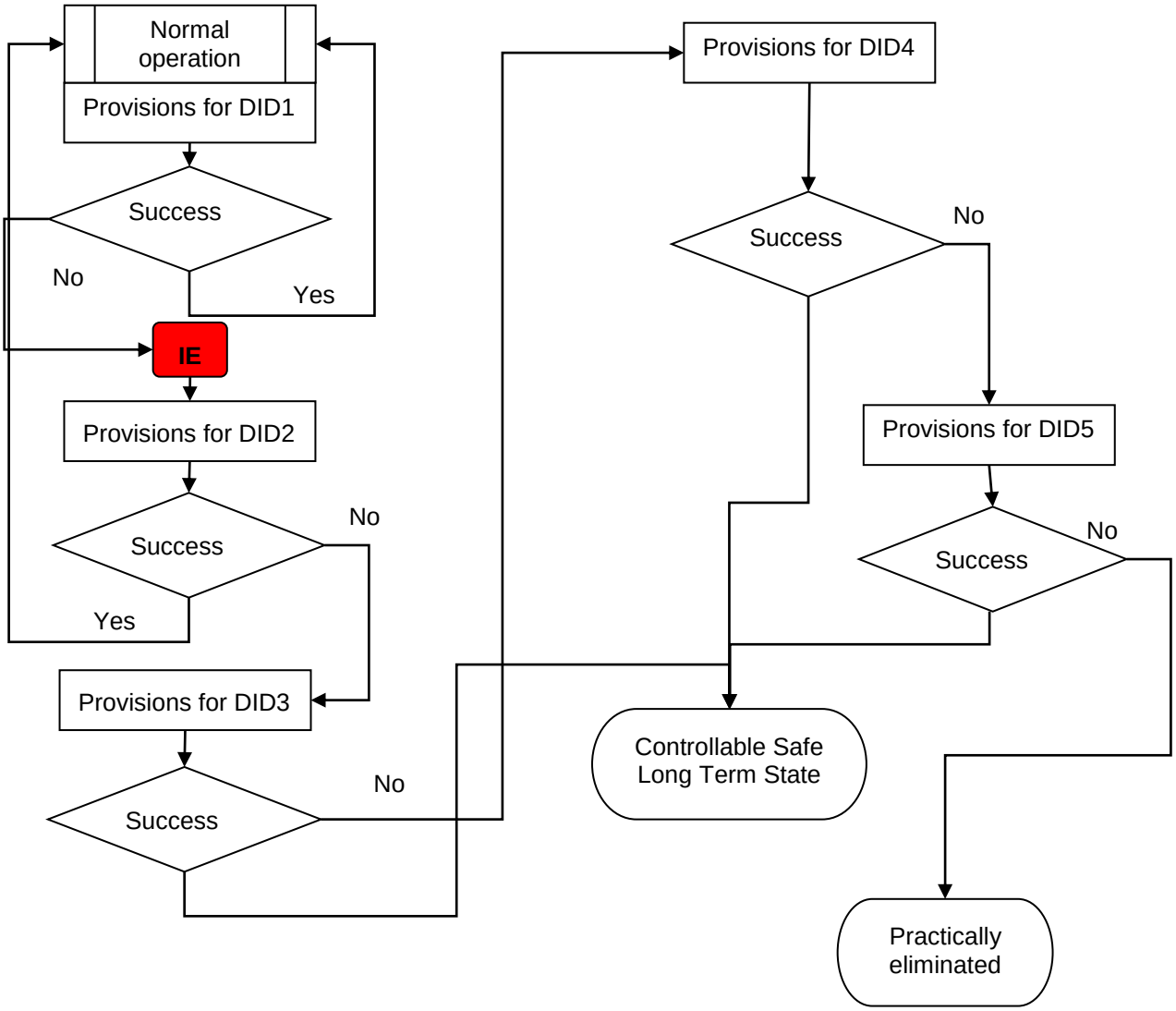
[8] See also Table A1-1

Level	Description of level	Objective / Purpose / function of DID level	Note
4	Control of severe plant conditions including prevention of accident progression and mitigation of the consequences of severe accidents	Mitigating a consequence of fuel damage to maintain controllable conditions of *in vessel stage* of severe accident (in vessel core retention) or at least to maintain controllable conditions of core retention in catcher after design basis accident (*out vessel core retention*) when DID3 fails as well as to avoid releasing of radioactive products into environment, i.e. containment integrity	*Success: Containment integrity preserved.* Definition of Safe Long Term State conditions (ACs) for DID4 success state should be determined.
5	Mitigation of radiological consequences of significant releases of radioactive materials	Protect people and environment against releases of radioactive materials	Definition of Safe Long Term State conditions (ACs) for DID5 success state should be determined.

Again is highlighted that fulfilment of any DID level objective shall be defined by mean of precise unambiguous measurable criteria, like values of physical quantities describing state of process, material properties etc.

Logical diagram for implementation of all DID levels is shown in Table A1-2. However implementation of DID levels is not straightforward task. None single method is available to determine challenges and select specific provisions that form DID levels as well as to assess importance of these provisions. In actually combination of qualitative analysis and quantitative methods is used. Computational analytical tools (quantitative methods) are typically used to evaluate the performance of the selected provisions (barriers, safety systems etc.). Quantitative methods, if appropriate, should demonstrate fulfilment of AC.

Figure A1-2 Adjusted Flow chart for DID

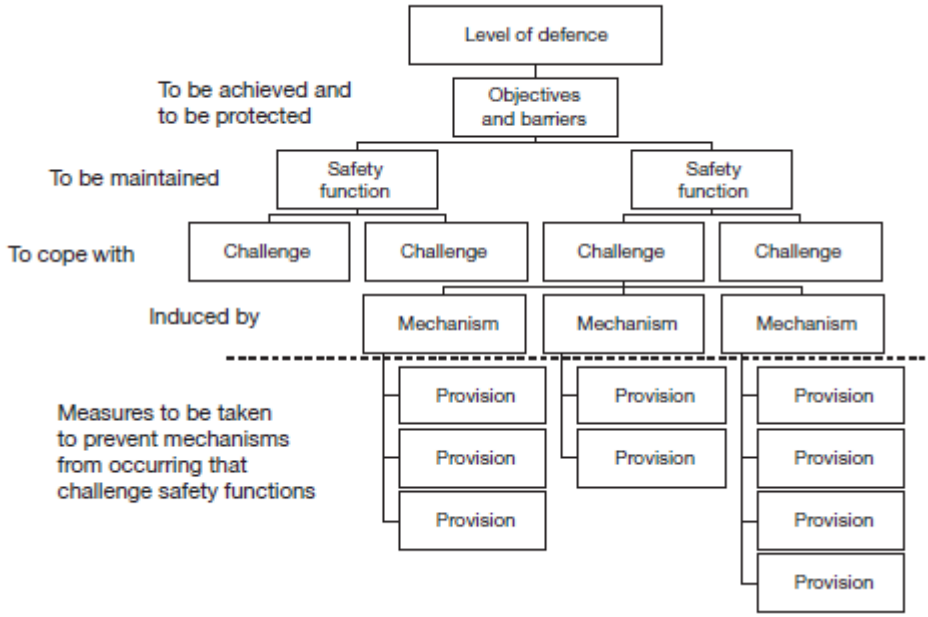


In addition, in the case of success DID3 and DID4 Achieving *Controllable Safe Long Term State* shall be demonstrated.

Objective of *Controllable Safe Long Term State* is such, that this an easy maintainable safe state establishes safe condition for a period of time which is necessary to concentrate sufficient resources to achieve absolutely safe state compliant with the fundamental safety objective - people and the environment shall be protected from harmful effects of ionizing radiation. **If absolutely safe state cannot be achieved then consequence of event that can lead to such unsafe condition shall be practically eliminated.**

Main basic qualitative tool which is used to determine of scope of particular DID level[9] is formed by objective trees.

Figure A1-3 Structure for DID provisions at each level of defence



Provisions are usually aggregated into safety groups or lines of protections. Consequently safety groups can form basis to design safety system. Any safety system shall respect basic design principles stated in [1], i.e. independence (of DID levels)[10] , single failure criterion, fail safe principle (if appropriate), diversity and resistance against common cause failures etc.

Any provision shall include reasoning to demonstrate its effectiveness to prevent / mitigate particular challenge including definition of working conditions, performance criteria etc.[11] .

This work interacts with task List of initiating events. Some challenges and mechanisms can be considered as IEs and vice versa.

Work as such is driven by as well as by related technical standards and scientific methods used to provide qualified reasoning regarding effectiveness of suggested provisions. Important aspects of step 5 are:

6 Step 5 has interrelations with steps 4, 6, 7 and 8.

7 Step 5 will be repeated several times by the same way as step 4. It is obvious that further and further iterations through step 5 will be formal and DID provisions implemented in previous iterations will be kept, i.e. only new issues will be analyzed

8 If reasoning and justification of DID provisions is based on analyses then requirement summarized in chapter shall be respected.

9 Performance of step 5 shall be ended examining fulfillment of requirements from presented in chapter

10 If any relevant requirement from chapter is not fulfilled or it is not possible to reach Absolute safe state by means of DID level 2 to 4 provisions then IE leading to such situation must be practically eliminated[12] .

---

[9] It means, even if designer provides clear evidences that current design contains adequate provisions the next level must be implemented. Such (rigorous and may be redundant) approach ensures compliance with basic philosophy of DID.

[10] It means that functional groups (safety systems) used in lower DID level shall not be considered to mitigate accident situation in higher DID level and higher DID level should be independent on lower level as much as possible, e.g. I&C, power supply, ultimate heat sink etc.

[11] [1] Requirement 14 and Requirement 15: Design limits

Output of this step is a list of provisions / safety groups / safety systems for particular DID levels. If all provisions / safety groups / safety systems are implemented into design basis, i.e. DID levels are complete, step 7 is entered, otherwise IDA return on step 4.

1.6 List of initiating events (step 6)

IEs (as basic input of safety analyses) are treated by many documents. However developing the list of IEs forms similar problem as implementation of DID levels, i.e. none universal way exists. Consequently several approaches (or they combinations) to build comprehensive list of IEs can be used:

- Engineering judgment
- Existing lists (generic or from reactors that are similar as reactor in interest)
- Results of objective trees (Fig. 0 3) where challenges and mechanisms form potential events
- Master logic diagrams and Failure Mode and Effect Analysis.

Aggregating of IEs into homogenous envelope groups is integral part of process to determine list of IEs, see paragraph 2.7 in **Chyba! Nenašiel sa žiaden zdroj odkazov.**[13] .

Specific aspect of IEs is combination of failures.

Combination of failures is frequent topic especially after Fukushima event . There are two aspect of combination of failures. Combination of failures can be caused by

1. Subsequent failures of equipment initiated by failure of one shared component, e.g. los of switchyard put out of order all devices connected to this switchyard.
2. Simultaneous failures of several items in short time due to spatial effects of internal or external hazards.
3. Simultaneous failures of several items in short time due to dependent failures, i.e. common cause failure.
4. Simultaneous failures of several items in short time due to independent failures.

---

[12] However there is none common understanding how practical elimination should be demonstrated. Following text just summarize some ideas how to do it. Two basic ways are available how to demonstrate that : deterministic and probabilistic.

Practically eliminated consequence of IE from deterministic point of view means:

- Occurrence of consequence is impossible from physical point of view (all phenomena leading to the consequence are suppressed)
- Occurrence of consequence is prohibited by physical features of design verified by experiments that are full-scale simulation of real conditions and real equipment will have considerable safety margins

Roughly say, practically eliminated consequence of IE from probabilistic point of view means that occurrence of consequence is negligible. Question is how to determine what is negligible because this definition is more political than logical task.

Anyway such probabilistic criterion should be based mainly on so called conditional probability. It means that we expect occurrence of IE with probability one and result of assessment is estimation of probability of unsuccessful mitigation of consequence of occurred IE. Based on experience from evaluation of nuclear safety such probability should be lower than 10-5 or 10-6. Further necessary condition for usage of probabilistic reasoning is independent evaluation by third party.

Concept of conditional probability eliminates uncertainty related to estimation of frequency of IEs. Further strengthening of probabilistic reasoning can be achieved by application of upper bound.

[13] In addition it should be noted that any division of IEs based on frequency of occurrence, operational conditions etc. is meaning less under consideration of definitions presented in previous table.

Case 1. Failures due to malfunction of key shared components are unavoidable. They should be prohibited (from deterministic point of view) by application of single failure criterion, i.e. usage of redundant provisions / safety groups / safety systems on each DID levels

Case 2. Spatial impact should be prohibited (from deterministic point of view) by plant design at least by appropriate implementation DID2 to DID4 foreseeing design level of postulated IEs.

Case 3. Common cause failures should be (partly) prohibited (from deterministic point of view) by diversification of equipment and safety groups. However; from deterministic point of view there is plenty of equipment that use the same principles, e.g. breakers, valves, sensors etc. and consequently from probabilistic point of view there is still some probability of common cause failure.

Case 4. Based on experience simultaneous failures of several items in short time due to independent failures are very rare events (if such event was observed). Moreover in real design there will be infinity number of such combinations that can put out of order particular DID level. It is unmanageable to develop some (deterministic) rules how to determine the most important combination of failures or to evaluate effect of all possible combinations. Particular answer can be obtained only by using probabilistic methods that provide list of minimal combination of equipment failures leading to the total failure having significant contribution to CDF or LRF.

1.7 Deterministic evaluation of safety (step 7)[14]

Aim of deterministic safety analyses is to demonstrate that challenges to safety in the various categories of plant states are addressed in appropriate manner and compliance with safety requirements (step2) is met[15]. One of the important inputs into safety analyses is formed by IEs (step 6).

1.8 Probabilistic evaluation of safety (step 8)

Aim of probabilistic safety analyses is to demonstrate that challenges to safety in the various categories of plant states are addressed in appropriate manner and compliance with safety targets (step3) is met. Basic input into safety analyses is formed by IEs. It is essential to use the same scope of IEs (step 6) everywhere where it is possible as well as the same AC (Probabilistic evaluation uses term success criteria).

Probabilistic evaluation of safety is considered as complement to deterministic analyses. It provides another insight and can also provide more comprehensive overview determining parts of design having low availability or chains of failures leading to the cliff edge effect.

1.9 Final design (step 9)

Step 9 is just formal to provide complete flow chart. Formal output of step 9 is plant design basis as output of IDA application.

Final design should be in compliance with requirement [1].

[14] It should be noted that steps 7 to 9 are incorporated just for sake of completeness in order to enable usage of IDA for full scope design process

[15] If thoroughgoing reasoning of provision is performed within step 5 almost of analyses from step 5 can be reused within this task.