

# Safety Improvement of Future Reactors by Enhancement of the Defence in Depth Principle

W. Frisch, G. Gros, IPSN  
GRS

M. Simon, F. Rollinger,  
GRS IPSN

---

## 1 Elements of the defence in depth principle

The defence-in-depth principle is one of the fundamental safety principles, which strongly influences safety philosophies, licensing requirements, plant design and plant operation. Basic elements have already been applied to the first nuclear power plants (e.g. the multi-barrier concept). It has been developed continuously, influenced by feedback of operating experience, design development, progress in research and technology and, last not least, by the systematic development of the safety strategies of responsible safety authorities.

The basic elements of defence-in-depth were fully developed in the early eighties and they were laid down in a comprehensive way in INSAG-3 in 1988. IAEA and INSAG have spent considerable effort in a further refinement and interpretation of the principle with respect to safety improvements of operating plants (e.g. accident management) and the application of the principle to future nuclear power plants /2, 3/.

For the purpose of this presentation only the most important objectives, principles and elements of defence-in-depth are presented here: The main objective as defined in INSAG-3 is:

*"To compensate for potential human and mechanical failures, a defence-in-depth concept is implemented, centred on several levels of protections including successive barriers preventing the release of radioactive material to the environment. The concept includes protection of the barriers by averting damage to the plant and to the barriers themselves. It includes further measures to protect the public and the environment from harm in case these barriers are not fully effective."*

The proper application of this principle ensures, that no single human or equipment failure would lead to harm to the public and even combinations of failures that are only remotely possible would lead to little or no harm.

Defence-in-depth helps to establish that the three basic safety functions (controlling the power, cooling the fuel and confining the radioactive material) are preserved.

The different levels of protection can be named by the objectives to be met or by the essential means to be provided to meet the objectives. Figure 1 gives the 5 levels of defence, based on INSAG 10. Level 4 has been divided into 4a (prevention of core damage accidents and 4b (mitigation of consequences) in this presentation for two reasons: the measures provided for 4a and 4b are completely different in future reactors and an important probabilistic target, the core damage frequency is related to level 4a,

not including 4b. Level 5 is not discussed further in this paper, because it is outside the plant design.

The strategy for the implementation of defence-in-depth is two-fold: first, within one level to prevent the occurrence of an event and secondly (if it occurs) to limit the consequences and to prevent its evolution to more serious conditions (= higher level condition).

An important principle is the independence of means provided on one level of protection from those of other levels in order to avoid that the failure of one system can jeopardize more than one level of protection. Special attention has to be given to events (hazards) which by themselves could potentially impair several levels of protection (e.g. fire or flooding).

There are prerequisites which are applicable to measures at all levels of protection in order to guarantee an effective implementation of the defence-in-depth principle: conservatism, quality assurance and safety culture.

Concerning the barrier concept, the principle is the provision of successive physical barriers for the confinement of radioactive material. For LWRs INSAG 10 lists four barriers:

- the fuel matrix
- the fuel cladding
- the boundary of the reactor coolant system
- the containment system.

The reliability of the barriers is affected by:

- a) features of the barriers themselves (e.g. quality)
- b) systems designed to protect a barrier

It is not possible (and not intended in the defence-in-depth concept) to define a 1:1 correspondence of levels of protection and barriers. This is because sometimes not all barriers are available (LOCA, shutdown conditions) and the events do not always proceed in such a way that they challenge the inner barrier first (e.g. an external hazard such as an explosion affects the containment first).

Situations in which one or more barriers are not effective (e.g. during shutdown) necessitate special attention. The same is true for events which have the potential of bypassing one or more barriers (e.g. steam generator tube rupture, containment bypass sequences).

The defence-in-depth principle in itself is a qualitative principle, and a judgement, whether the principle is applied in a proper way for a given concept, can be made in a qualitative way. Nevertheless, its proper application will show up in results of accident analyses, in results of PSAs and last not least in operational performance.

## **2 Implementation of defence in depth for future reactors**

For future reactors an enhancement of the well proven defence-in-depth principle is considered to be the proper strategy to further improve safety. This demand is expressed in several places, e.g. by IAEA in TECDOC 986 /3/ by INSAG in the report INSAG 10 /2/ and in numerous new national requirement documents for future reactors.

There are many specific recommendations concerning the implementation. It is important that all elements of the defence-in-depth principle are considered and that improvements are aimed at on each of the 4 levels. The main principle is that preventive measures have the highest priority, but mitigation measures also have to be foreseen, e.g. in INSAG 10 a further reduction of the probability of severe core damage is required as well as the strengthening of the confinement function to mitigate the consequences of severe core damage accidents. One rationale for the higher requirements on the containment function to cope with severe core degradation consequences is that improvement in the preventive area are difficult to proof for very low probabilities of occurrence (e.g.  $<10^{-6}$  per plant and year) due to uncertainties in the methods and data. Important elements to be considered are

- provision of the highest possible degree of independence of levels
- avoidance of accident situations jeopardising more than one level of protection
- avoidance of accident situations that bypass barriers
- provision of sufficient conservatism in the design with the higher degrees on the lower levels (more margin for events of higher frequency)
- hypothetical severe accident sequences that could lead to large radioactive releases due to early containment failure have to be eliminated with a high degree of confidence.
- design improvements on a higher level of protection should not be used to justify cutbacks or non-removal of deficiencies on lower levels

How the defence-in-depth principle is implemented in future reactor designs, will be presented in two steps, a first one which is very general and characterises only the general approach for the different types of reactors and a second one, in which detailed requirements and design solutions are presented for the French-German safety approach and the EPR (see chapter 3).

The defence-in-depth approach is briefly characterised for 3 types of future reactors:

- Evolutionary concepts (ABWR, APWR)
- Innovative concepts (PIUS, liquid metal cooled advanced reactors, high temperature reactors, "inherently safe" reactors)
- Evolutionary concepts with improved containment (EPR)

The aspect presented here is the extension of the 4 levels of protection compared to existing LWRs. Without any quantitative evaluation it is assumed that all future concepts have a higher degree of safety compared to existing plants. In Fig. 2 it is shown how the different levels of protection contribute to safety of the different types of future reactors. The safety improvement compared to existing plants is indicated by longer lines for future concepts, with no differentiation among the different future concepts.

The first line represents existing plant designs with a good balance between Levels 1, 2 and 3 and some effort on level 4 (more or less extended later on by the addition of accident management measures).

Evolutionary concepts are built very closely to an existing predecessor with improvements derived from operating experience and with no mayor conceptual changes. They are presented in the second line, indicating an overall safety improvement.

Innovative concepts generally rely on inherent safety features and passive components. If the inherent physical behaviour is such that unacceptable values are not exceeded, engineered safety features are not necessary or can be reduced to only a few measures. If it can be proven that core damage is "practically eliminated", no measures are necessary to cope with severe accidents. Therefore, nearly all effort to arrive at a high safety level shows up in the first two levels of protection. If - for such an innovative design - it can be demonstrated, that all conditions beyond protection level 2 are "practically eliminated", higher level protective measures are not necessary, and the defence-in-depth concept may not be applied in the same way as for evolutionary LWR concepts. However, it has to be emphasised, that the required proof is not easy to be achieved, because uncertainties have to be taken into account in the evaluation of the concept. Uncertainties are usually larger for new concepts when data from operating experience are missing or are not transferable from similar plant designs.

Evolutionary reactor concepts with special features to cope with core melt accidents are characterised by a safety improvement on all levels of protection, with special emphasis on level 4. The EPR belongs to this group, which is characterised in the last line of Fig 2. How the defence-in-depth principle is implemented in the French-German safety approach is demonstrated by some examples in the following chapter.

Evolutionary plants with passive features (e.g. AP 600 of Westinghouse BWR 1000 of Siemens) are not presented separately in this scheme. They are characterised by a high degree of system diversity due to the combination of active and passive systems, and thus by a good separation of levels of protection. However, the estimation of the contribution of these systems to the levels 2, 3 and 4a requires a careful analysis which was not possible within the frame of this paper.

### **3 The defence-in-depth concept in the French-German safety approach**

#### **3.1 Main Objectives of the French-German safety approach of 1993**

The safety approach for future PWRs jointly developed in France and Germany since 1993 is supposed to give guidance to the designer during the development of the European pressurised water reactor (EPR). The safety approach has been developed continuously since 1993 with increasing degree of detail in recent years.

The three main safety objectives of the approach of 1993 are:

1. A further reduction of the core melt frequency.
2. The "practical elimination" of accident situations which could lead to large early releases of radioactive material. If those situations cannot be considered as physically impossible, provisions have to be taken to "design them out".
3. For low pressure core melt situations the design has to be such that the associated maximum conceivable releases would necessitate only very limited protective measures in area and time (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long-term restrictions in the consumption of food).

Concerning safety principles to be applied, the defence-in-depth-principle is considered the most important one, this is expressed in chapter 2 of the approach of 1993.

*The defence-in-depth principle remains the fundamental principle of safety for the nuclear power plants of the next generation, with the implementation of several levels of protection including successive barriers against the release of radioactive substances to the environment. This principle has to be used to demonstrate that the three basic safety functions -reactivity control, cooling the fuel and confining radioactive substances- are correctly ensured. The aim is to ensure protection of the public and of the workers. This includes accident prevention as well as accident mitigation.*

*For the next generation of nuclear power plants, a general objective is to reinforce the defence-in-depth of the plants. To achieve this, the design should be made on deterministic bases, supplemented by the use of probabilistic methods. The objective should be reached considering the results of operating experience and of in-depth studies like probabilistic safety assessments conducted for pressurised water reactors (PWR), the progress in knowledge of the physical phenomena which may occur during the development of accidental situations, particularly core melt situations, has to be taken into account.*

*An important objective is to achieve a significant reduction of radioactive releases due to all conceivable accidents, including core melt accidents. The containment has to be designed in order to follow this objective.*

### **3.2 Refinement of the safety approach**

Since 1993 many safety relevant subjects have been treated and detailed GPR/RSK recommendations have been developed to give guidance to the designer during the design development of the EPR. In support of this development of recommendations nearly 50 IPSN/GRS reports have been produced on numerous subjects, such as system design, severe accident, internal and external hazards, containment design etc. These reports contain information on present practices in both countries, and on technical solutions of the designer. The subjects are analysed in detail and proposals for recommendations are given.

During this development of recommendations the main elements of defence-in-depth have always been considered such as:

- balance between levels of protection
- independence of the different levels of protection
- balance between prevention and mitigation
- conservatism in the design
- the protection of barriers
- special emphasis on shutdown states and on events which may affect more than one barrier at a time or may result in bypasses around barriers.

### **3.3 Examples for re-enforcement of the defence-in-depth**

Some examples are given in the following chapters to demonstrate how the re-enforcement of the defence-in-depth is expressed in terms of recommendations within the French-German safety approach. In some cases examples are also given for the technical realisation within the EPR design concept.

#### **3.3.1 Balance between levels of protection**

As can be seen from the main objectives of the approach (chapter 3.1) safety improvement is required on all levels of protection, and during the refinement of the approach attention has been given to the well-balancedness. Table 1 gives some examples for detailed requirements on each level of protection. However, the proper implementation of the defence-in-depth requires more than a number of arbitrary requirements. The key strategy is a proper classification of events, safety functions and systems and of rules and assumptions for analyses in order to implement all elements of the defence-in-depth principle.

This has been done by means of a classification concept for events and for systems to cope with these events. This strategy has already been discussed with respect to the implementation of the diversity principle /4/. Here only the concept of event classification is presented and linked with the different levels of protection of the defence-in-depth (fig. 3). The events are categorised into 2 groups. The plant condition categories (PCC) represent the conventional design basis as in previous plant designs. The Risk Reduction Categories (RRC) represent the extension of the defence-in-depth concept, especially the reinforcement of level 4.

A quantitative proof of proper and balanced implementation of defence-in-depth can only be obtained on the basis of a PSA. For this reason, the French-German safety approach asks for a PSA in the early phase of the design:

*The conduct of probabilistic safety assessments and the establishment of quantitative probabilistic targets are important tools at the design stage to gain an in-depth understanding of the relative weaknesses in the plants an to deal with complex situations involving several equipment and/or human errors.*

*A PSA at the design stages of the PWR shall be performed with the following objectives: supporting the choice of design options, including redundancy and diversity of the safety systems, well-balanced safety concept and valuation of expected deviations from present French and German safety practices appreciation of the improved safety level, compared to existing plants.*

#### **3.3.2 Independence of the levels of protection**

Several levels of protection are only useful when the measures and systems provided on each level are independent of each other. From figure 4 it can be seen that different systems are provided for each level of protection with the important requirement that a system of class F2 (level 4a) is different from the F1 system which has - due to its assumed complete failure - caused the transition of an event from level 3 or 4 to RRC-A. Systems to mitigate consequences of core melt accidents (level 4b) are by itself - due to the different basic safety function to be fulfilled - diverse to those of lower levels (systems to reduce hydrogen concentration, core melt cooling, containment heat removal).

The diversity of these systems alone is not yet sufficient as a design means against common cause failures affecting more than one level of protection. It must also be prevented that failures in support systems affect several levels of protection. This can be achieved by independent support systems for each level and / or highly reliable support functions with system diversity.

Concerning electrical power supply, the French-German approach of 1993 had already asked for diversity. After the proposal of the project (4 main diesel generators + 2 smaller diesels, backing up two of the main ones) more refined requirements were set up, especially with respect to the proof of sufficient independence and diversity among the two types of diesel generators.

Other relevant support systems are the component cooling water system (CCWS) and the essential service water system (ESWS). Already in 1997 GPR/RSK asked for a reduction of the impact of potential common cause failures in the two systems. In particular for the containment heat removal system the possibility of a common cause failure in this system and systems needed for core melt prevention (due to a loss of common auxiliary systems or the clogging of IRWST filters) was criticised.

Upon this, and based on preliminary PSA results, the designer has recently proposed a new design solution for the containment heat removal systems (CHRS) cooling chain. Each train of the CHRS has a dedicated cooling chain, independent of the CCWS/ESWS system consisting of:

- a dedicated essential cooling line connected to the ESWS piping just after the water intake of the pumping station, with a dedicated pump power supplied by the small (SBO) diesel generators and an intermediate heat exchanger,
- a dedicated intermediate cooling line between the intermediate heat exchanger and the CHRS heat exchanger, with a dedicated pump power supplied by the SBO-diesel generators too. (see fig.4).

Another potential degradation of different levels of protection can arise from effects of internal hazards (e.g. fire, flooding), if such an event jeopardises the operation of several systems on different protection levels. GPR/RSK clearly state *that the defence-in-depth principle has to be fully applied to the protection against internal hazards so as to limit the likelihood and the consequences of such hazards by the implementation of prevention, control and mitigation provisions.*

*Particular attention has to be devoted to those internal hazards having the potential to affect the three basic safety functions in more than one of the successive defence-in-depth levels.*

GPR/RSK also recommend to minimise common mode failures by installing components of different trains of safety systems in divisional areas designed such that an internal hazard affects only one train of the safety system (and thus does not affect the safety function to be performed by these systems).

### **3.3.3 Prevention and limitation (mitigation)**

As stated in chapter 1, an important element of defence-in-depth is the prevention of events and the limitation (or mitigation) of consequences, should they occur. This principle should be applied on each level of defence. The examples in table 1 give an indication that both aspects have been considered in the French-German safety approach up to the fourth level, where measures are foreseen to prevent core melt (e.g. primary side feed and bleed) and measures to cope with low pressure core melt

accidents (e.g. containment heat removal) in such a way that radiological consequences are limited to such values that objective 3 of chapter 3.1 is met.

For those event sequences, for which radiological limits according to objective 3 cannot be met (or where this cannot be proven with sufficient confidence), more effort is put into prevention. In those cases the requirement on prevention is much stronger, expressed by "practical elimination". The strategy is explained as follows:

*"single initiating events have to be "excluded" or "dealt with" (that is to say their consequences are examined in a deterministic way). Single initiating events can only be "excluded" if sufficient design and operation provisions are taken to that it can be clearly demonstrated that it is possible to "practically eliminate" this type of accident situations; for example, the vessel rupture can be examined in that way"*

*"As a design goal, accident situations which would lead to large early releases have to be "practically eliminated": when they cannot be considered as physically impossible, design provisions have to be taken to design them out"*. Examples of such event sequences specifically addressed in the safety approach are:

- Accident sequences involving core degradation and containment bypassing (via steam generators or circuits connected to the primary system which exit the containment)
- Reactivity accidents resulting from fast introduction of deborated water
- Core melt situations under high primary system pressure.
- Global hydrogen detonations

The practical elimination of high pressure core melt situations (primary system pressure < 20 bar at the time of vessel rupture) was an important issue from the beginning. GPR/RSK had asked to investigate specific valves to be actuated only in case of core melt sequences (in addition to the pressurizer safety valves, which also have a depressurisation function within the primary feed and bleed).

The designer has provided such a system (dedicated bleed valve with an isolation valve) with a high degree of diversity to the pressurizer safety valves in order to avoid common cause failures among the two depressurization systems. GPR/RSK put more refined requirements on this systems, e.g.: *It should be designed such that "... the opening of these specific valves can be guaranteed even for hot gas temperatures. Their discharge function must be available in case of loss of off-site power and unavailability of all diesel generators. Once open, the bleed path should stay fully open with high reliability through the progression of the accident.*

### **3.3.4 Conservatism in the design**

An important prerequisite to guarantee an effective implementation of the defence-in-depth principle is conservatism in the design and in the safety demonstration. This element is also an important one in the French-German safety approach, expressed in many places. Only a few examples can be given here .

Within the safety assessment, the radiological consequences are the relevant ones because they express the allowed impact on the public. The French-German safety approach defines: *"For accident situations without core melt, there shall be no necessity of protective measures for people living in the vicinity of the damaged plant no evacuation, no sheltering) and for low pressure core melt situations only very*

*limited protective measures would have to be implemented in area and time". (see objective 3 of chapter 3.1).*

In the safety demonstration an event classification concept is used as shown in fig. 3. Instead of using the radiological limits, technical criteria (= decoupling criteria) are specified, which have to be met. The strategy recommended by GPR/RSK is to define more stringent criteria for more frequent events. These criteria (e.g. DNBR, cladding temperature, system pressure) represent a considerable degree of conservatism, because their violation is by far not equivalent with the violation of radiological limits. Another means of introducing conservatism in the design is the set of conditions and assumptions to be followed in the safety demonstration (accident analyses), especially for the PCC events:

- Assumption of a single failure in a redundant safety system
- Assumption of one train of a safety system being in maintenance
- During PCC 3 and PCC 4 events operational systems are assumed to be not available (unless they worsen the situation)
- Operator interventions are assumed no earlier than 30 min.

In addition to these general accident analysis rules many specific requirements are set up to either provide additional margin or to check, whether an additional conservative assumption could lead to a significantly worse situation (cliff edge effect). Specific examples are:

- When the break preclusion concept is properly applied to the primary circuit, the largest break to be assumed in the primary circuit (PCC-4) is the complete guillotine rupture of the largest pipe connected to the main coolant line. GPR/RSK adds: *It is however recalled that the mass flow equivalent to a 2A-opening of the main coolant line has to be assumed for the design of the emergency core cooling function and of the containment pressure boundary, so as to implement safety margins concerning the cooling of the core to prevent core melt and concerning the containment function; the 2A-opening is also to be assumed for the supports of the components and for the qualification of equipment.*
- *"The adjunction of an internal liner would procure additional margins concerning the containment leak tightness to deal with phenomena such as fast local deflagrations".*
- Superposition of events for which a complete independence cannot be proven, e.g. loss AC power after a transient or loss of coolant accident of a design basis earthquake, is required.

The principle of conservative designer is kept and re-inforced within the French German safety approach. There is only one aspect where the wrong impression may arise that conservatism is reduced: It is the recommendation to replace conservative models by realistic models and consider the uncertainties in the results. This is recommended to support the use of more advanced and more accurate models (e.g. in thermalhydraulics), the accuracy of which is proven by an extended experimental program. Conservative assumptions are only changed, where it is proven that the model assumptions were too conservative.

The conservatism of the design has to be demonstrated by safety analyses following the conservative rules and assumptions mentioned above. It should be noted that there are

other types of accident analyses, where it is appropriate to use best estimate assumptions and conditions, e.g. in PSA-analyses, in the verification of emergency procedures and in simulators for operator training.

#### **4 Conclusion**

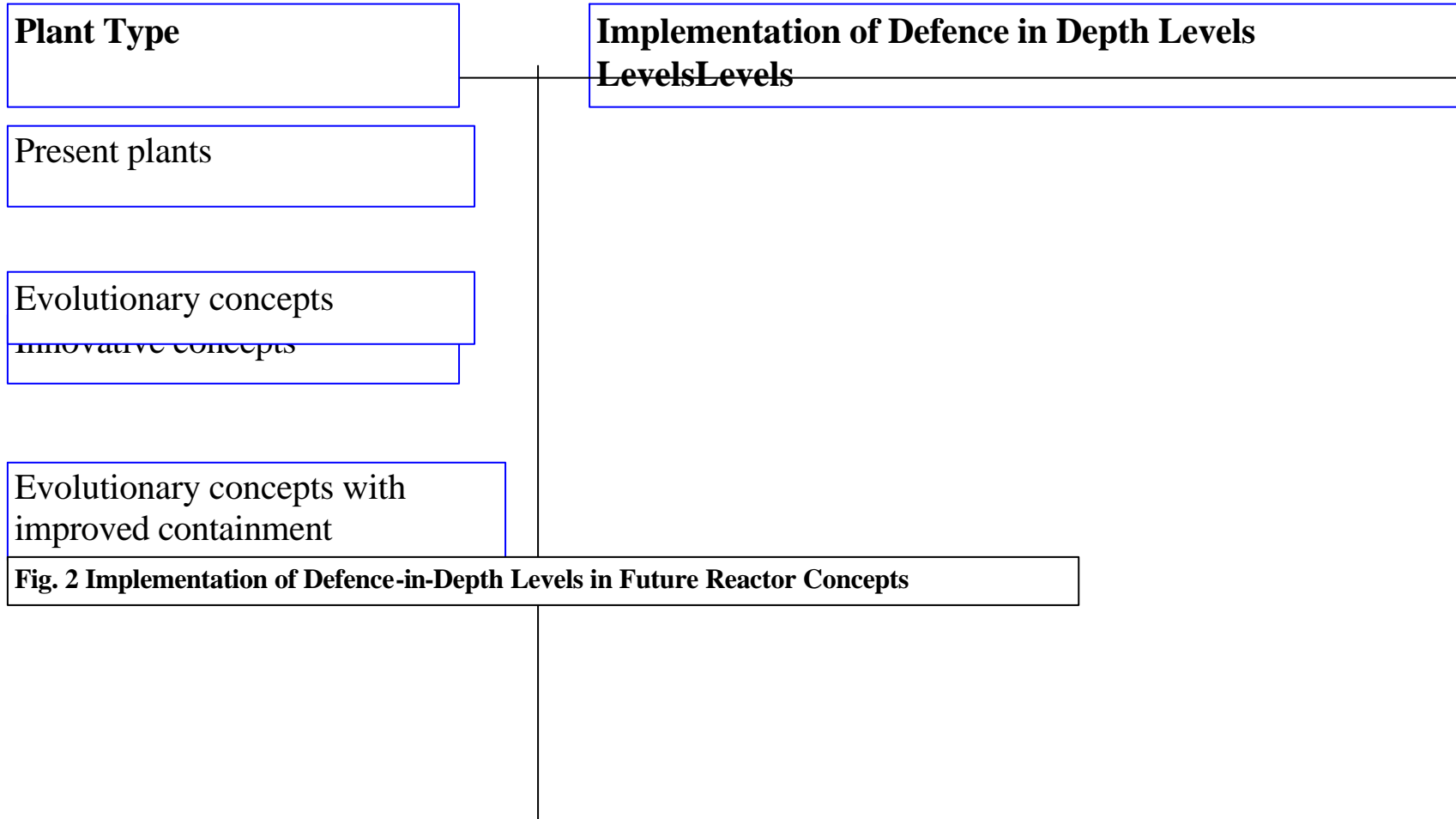
The French-German safety approach has incorporated the defence-in-depth principle with all its important elements. Compared to existing plants (and other advanced concepts) special emphasis has been put on preventive and mitigative measures on the fourth level (severe core damage accidents). The paper has given several examples how the elements were implemented. The demonstration was made in a qualitative way because the defence-in-depth concept is a qualitative one in itself. The effectiveness of its application can, however, be proven in a quantitative way based on results of a PSA (core melt frequency target, balanced design with no dominant event sequences and no dominant contributions of one particular system to core melt).

#### **5 References**

- /1/ Basic Safety Principles for Nuclear Power Plants  
A report by the International Nuclear Safety Advisory Group  
INSAG-3, Vienna 1988  
(Revision 1 to be published in 1999)
- /2/ Defence-in-Depth in Nuclear Safety  
A report by the International Nuclear Safety Advisory Group  
INSAG-10, Vienna 1996
- /3/ Implementation of Defence-in-depth for next generation light water reactors  
IAEA-TECDOC 986  
Vienna, December 1997
- /4/ Significance of the diversity principle in system technology of future PWRs  
W. Frisch (GRS), G. Gros (IPSN)  
GRS/IPSN Fachgespräch, Berlin, Nov 9-10, 1998

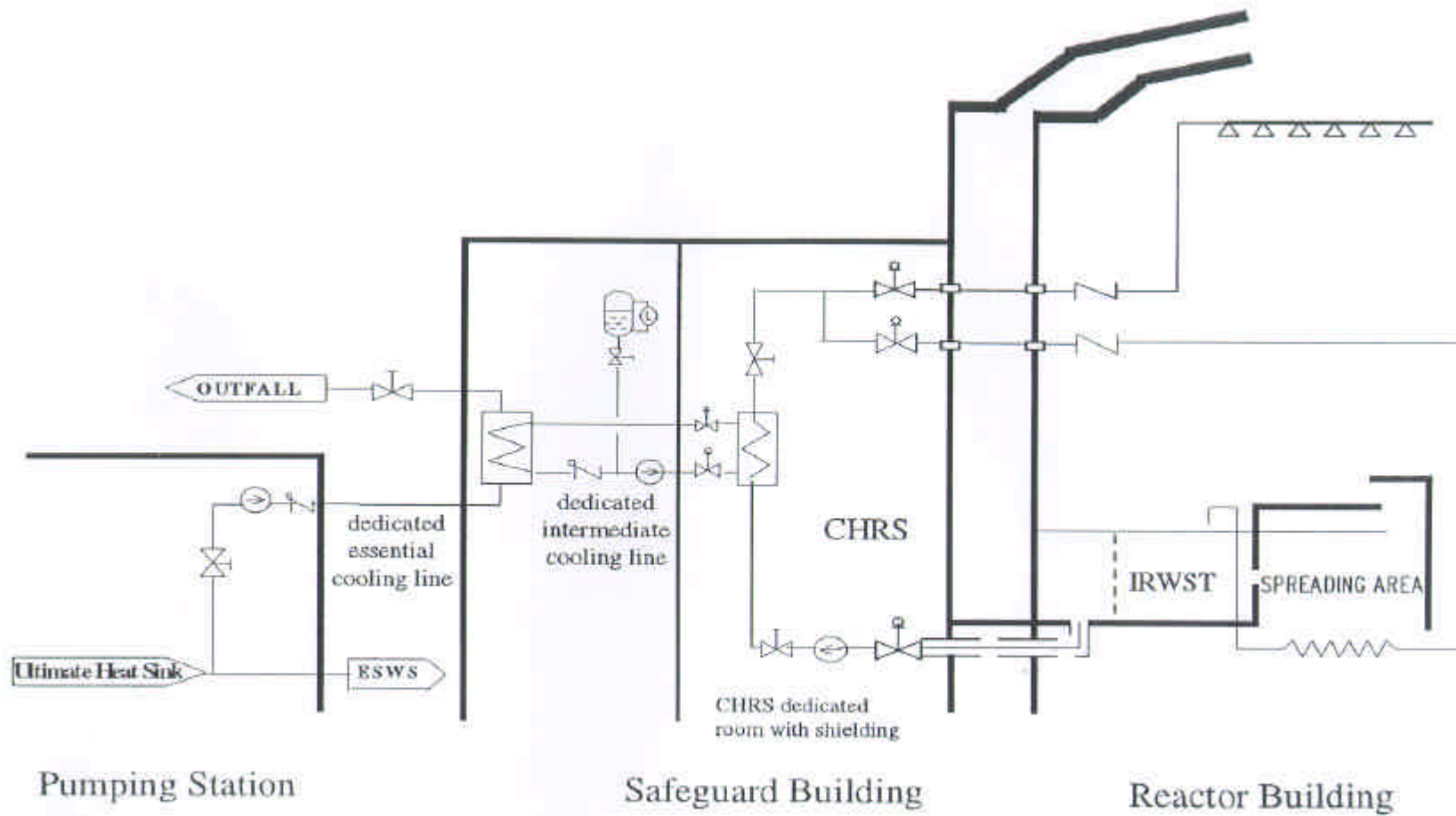
**Figure 1: Defence in depth**

<b>Levels of defence in depth</b>	<b>Objective</b>	<b>Essential means</b>
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 4a	Control of severe plant conditions, including prevention of accident progression	Complementary measures and accident management
Level 4b	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



Event Categorie	System and measures to cope with the events	Defence in depth levels
<b>Plant Ccondition Categories</b>		
PCC 1 Normal Operation	Inherently stable plant behaviour Operational Systems	1
PCC 2 Anticipated Operational Occurrences	Operational Systems Limitation Systems Safety Systems (F1) (partly)	2
PCC 3 Incidents	Safety Systems (F1)	3
PCC 4 Limiting Accidents	Safety Systems (F1)	3
<b>Risk Reduction Categories</b>		
RRC-A Prevention of core melt	Diverse Safety Systems (F2) to prevent core melt	4a
RRC-B Prevention of large releases after core melt (Mitigation)	Systems to mitigate consequences of core melt	4b

**Fig. 3 Event classification in French German Safety approach**



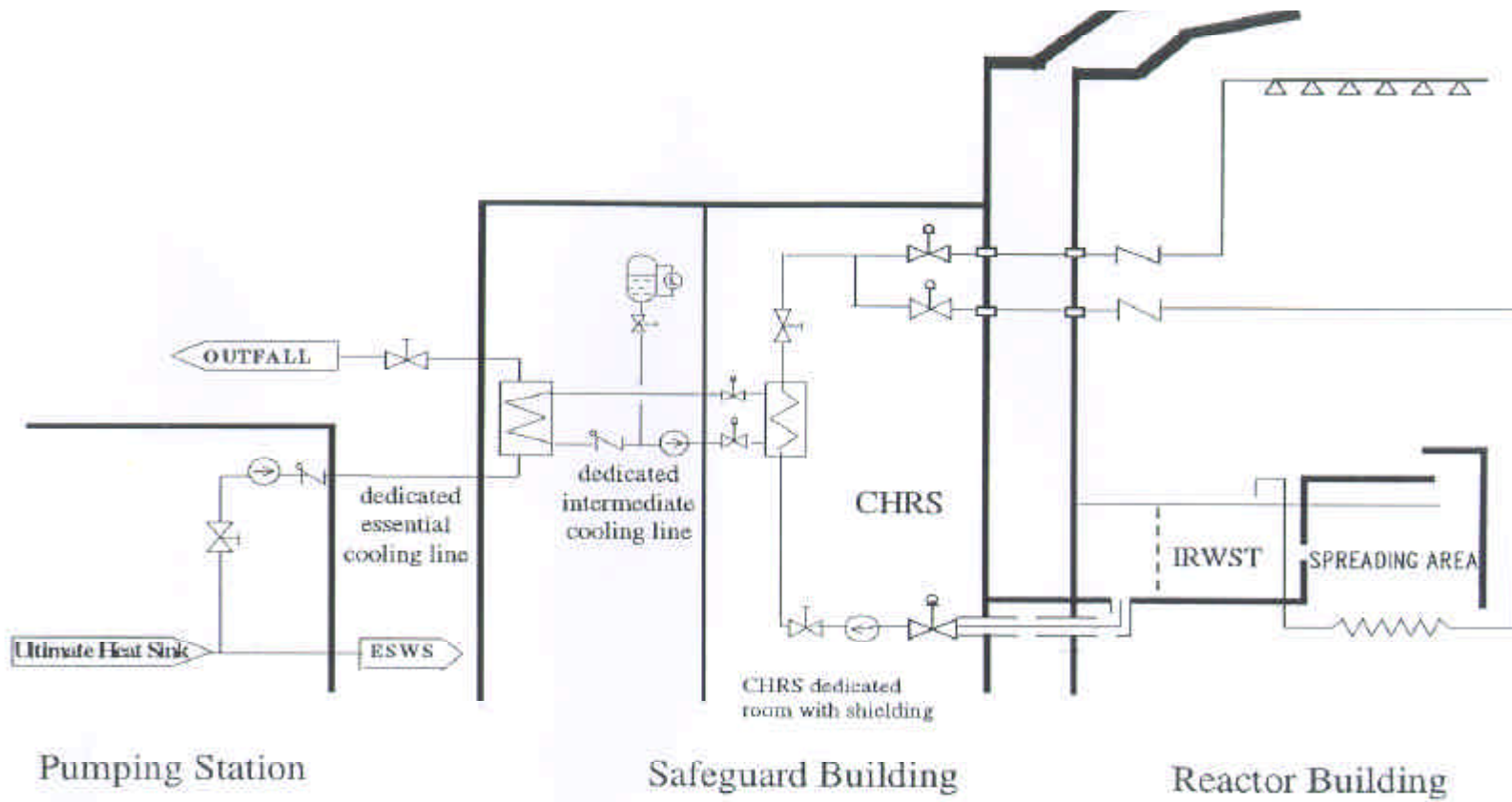


Figure 4: CHRS with dedicated cooling chain

**Table 1 Examples of defence in depth implementation in the French German safety approach**

Level of protection	Examples of requirements
1	<ul style="list-style-type: none"> <li>– Reduction of frequency of occurrence of initiating events (analysis of operating experience, improvement of reliability of operating system, avoidance of vibration, corrosion, cavitation etc)</li> <li>– Inherently stable plant behaviour (e.g. negative moderator feedback)</li> </ul>
2	<ul style="list-style-type: none"> <li>– Improvement of man-machine interface</li> <li>– Provision of limitation systems</li> </ul>
3	<ul style="list-style-type: none"> <li>– Provision of sufficient conservatism in the design by accident analysis rules (conservative technical criteria, single failure criterion etc) with special emphasise on shutdown states</li> <li>– High reliability of safety systems (class F1) by redundancy, physical separation and diversity (e.g. in the scram system components).</li> </ul>
4a	<ul style="list-style-type: none"> <li>– Provision of diverse systems (class F2) to cope with multiple failure situations: primary bleed and feed, extra boration system</li> <li>– Provision of support system with a high degree of diversity (e.g. two additional small diesels generators)</li> </ul>
4b	<ul style="list-style-type: none"> <li>– Highly reliable primary system depressurisation function (pressurizer safety valves + diverse depressurisation valves)</li> <li>– provisions to cope with low pressure core melt accidents: sufficiently tight containment and basemat, systems to reduce H<sub>2</sub> concentration, containment heat removal system.</li> </ul>