VIEWS ON DEFENCE IN DEPTH IMPLEMENTATION

T. VENEAU, A. FERRIER
SEPTEN, EDF/DIPNN 12-14 Avenue Dutriévoz, 69628 Villeurbanne – France

J. BARBAUD
DTI, EDF/DIPNN 1 Place Pleyel, 93282 Saint Denis - France

ABSTRACT

The Defence in Depth (DiD) concept was introduced to the field of nuclear safety in the sixties and early seventies. The concept has progressed over time and now there are five levels, including progressively situations issued from design extension conditions, to cope with severe accidents and dealing with accident management off-site. The 2011 Fukushima DaiIchi accidents, even if they raised many questions on nuclear safety issues, confirmed the merits of the DiD concept. Indeed, lessons learned from the accidents have reinforced the use of the DiD concept to ensure adequate safety. The paper presents first how the concept of DiD evolved over time, the link with the barriers notion, the current consensus on DiD definitions obtained despite some differences observed between standards (eg. IAEA and WENRA definitions), and discusses subjects like robustness and sufficient independence of the levels, before raising perspectives on how to achieve a sufficient independence of DiD levels.

1. Introduction

The DiD concept has been used for many years as a tool among others for the reactor safety design. Following the Fukushima accidents, numerous analyses were made by different organizations, and the lessons learned showed that the concept remains valid.

However, many questions arose from these analyses, highlighting the importance of the implementation of the DiD concept, and to understand how an external event can act as a common mode initiator for the failure of the safety provisions of DiD.

This paper discusses first the DiD concept (the link with the barriers method and its evolution over time to reach the current definition, and the differences observed between IAEA and WENRA definitions), before talking about their implementation, their robustness and the subsequent need of sufficient independence between the different DiD levels.

2. The DiD Concept

2.1 DiD and the barriers method

The first nuclear installations designed and constructed in France were based on an adapted safety approach, the so-called **barriers method**, described by Mr Bourgeois in 1973 as follows [1]: "*Protection of the public against the consequences of an accidental release of fission products rests on the interposition of a series of leaktight barriers. Safety analysis therefore consists firstly in ensuring the validity of each of these barriers and their correct operation under normal and accident reactor operating conditions. This kind of analysis emphasizes the progressive nature of safety by distinguishing three successive but interrelated stages: prevention …, monitoring…* [and] *mitigating action*."

As the first PWRs were constructed in France under an American license, which design is based on the DiD concept, French designers and engineers adapted the concept to take into account their own experience based on the barriers method. This experience served the nuclear safety discussions held by international organizations, which also adopted the notion of barriers, closely associating them to the DiD concept.

As a matter of fact, these barriers constitute an important feature when managing the 3rd fundamental function, i.e. the confinement of radioactive substances, shielding against radiation and control of planned radioactive releases, as well as limitation of accidental radioactive releases. It consists of putting in series barriers as independent and leaktight as possible. The method implies some notions close to those of DiD, concerning the prevention, monitoring and safety actions but it does not pretend to their independence (for example, the safety actions are put in place thanks to the monitoring). Each barrier is examined under these three aspects for the transients postulated during normal operation, incidents and accidents.

These three main barriers do not have the same perspectives:

- the 1st barrier present a maximum efficiency only for situations low disturbed (postulated initiating events – PIE – up to incident conditions); for accident conditions some damages are allowed;
- the 2nd barrier has another role than containment, an even more important role: it maintains the coolant inventory to core cooling (including some severe accidents) and neutrons poison (boric acid);
- the 3rd barrier has also a double role. It maintains the containment of radioactive substances for all accidental situations (severe accidents included), and the protection of primary circuit in case of external hazards. It shall be noted for this barrier, the importance of containment features (active and passive ones) that protect the containment and avoid severe consequences to the environment in case of high internal source term.

INSAG-10 [2] states that the application of the only method of barriers cannot ensure sufficient safety, since it does not include the means to provide the barriers themselves with successive layers or levels of protection. In fact, the barriers approach was intended to provide redundant means to ensure the fulfillment of the fundamental safety functions of controlling the power, cooling the fuel and confining radioactive material. The DiD concept was therefore gradually refined to constitute an increasingly effective approach combining both prevention of a wide range of postulated incidents and accidents and mitigation of their consequences, on the basis of single initiating events selected according to the order of magnitude of their frequency, estimated from general industry experience (see §2.2).

To each DiD level are therefore associated defence lines (features and documentation) and for instance, the barriers related to the situations to cope. These defence lines and their barriers allow to deal with disturbed situations by assuming the respect of deterministic criteria, and for example avoiding the situation to degradate, that could induce core melt for the more severe accidents.

Nevertheless, if they can intervene at all DiD levels, the main barriers are not associated to them. The barriers play their own role, they have their own efficiency and could not be totally independent from each other; a degradation of the first barrier can impact the second one and all failure of the 2nd barrier will impact the 1st and the 3rd ones. Indeed, if the 3rd barrier fails (as a protection against external hazards), it could affect the 2nd. Finally, common mode hazards such as earthquakes induce a charge simultaneously to all the barriers.

The barriers are therefore transverse to all DiD levels. The design of a reactor may use the barriers method and the DiD concept, but it’s not desirable to mix them to avoid a fractal vision of DiD, which could lead to difficulties in terms of independence. This link between the barriers notion and the DiD concept is absent in WENRA documents, but present in others (eg.: INSAG 10).

2.2 The DiD concept and its evolution

In the early stages the DiD concept included three levels. The concept was almost inexistent in 10 CFR (mentioned once, and without development) and some principles close to those currently used appeared in the sixties and early seventies.

Experience feedback and investigation of severe accidents resulted in extensions of the DiD concept, as additional measures to cope with significant multiple failures, or the implementation of accident management in order to prevent accidents or to mitigate their consequences.

In summary, the historical development of the concept of DiD led to a general structure of physical barriers and five successive levels, which were described in INSAG- 3 & 12 ([3] and [4]) and INSAG-10 [2]. Therefore, DiD consists in a deployment of different levels of equipment and procedures in order to maintain the effectiveness of physical barriers placed between radioactive material and workers, the public or the environment, to cope with different situations, from normal operation to severe accidents, and to manage emergency situations if they should appear. It is implemented through design and operation to provide a graded protection against a wide variety of transients, incidents and accidents, including equipment failures and human errors within the plant and events initiated outside the plant. The objectives include the compensation for potential human and component failures, maintaining the effectiveness of barriers by averting damage to the plant and to the barriers themselves, and the protection of the public and the environment from harm in the event that these barriers are not fully effective.

DiD is currently structured in five levels (cf. Table 1). Should one level fail, the subsequent level comes into play. The general strategy is composed of two principles: first, to prevent and monitor accidents, and second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. Taking account severe accident as a part of the concept, it included progressively situations issued from the design extension conditions (DECs), to cope with severe accidents and deal with accident management off-site.

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

Tab 1: Levels of DiD - INSAG-10 [2]

The general objective of DiD is therefore to ensure that a single failure at one level of defence, and even combinations of failures at more than one level of defence, would not propagate to jeopardize DiD at subsequent levels. A sufficient independence of different levels of defence is a key element in meeting this objective (see §3.3).

Finally, DiD as a concept is not just related to reactor design and its assessment but also covers all other aspects that may affect the safety of the NPP. In particular, human and organisational elements must be seen as part of the safety provisions at all levels in an integrated approach of DiD.

Then, the concept of DiD for the current operating reactors was further developed to take into account severe plant conditions that were not explicitly addressed in the original design (hence called “beyond design conditions”), in particular lessons learned from the development of probabilistic safety assessment and from known accidents (Three Mile Island accident in 1979 and Chernobyl accident in 1986).

The need for safety provisions beyond those provided at DiD level 3 for coping with design basis accidents has been enhanced in IAEA safety standards through the use of the concept

of DECs (i.e. conditions beyond the design basis accident that are nevertheless considered on the basis of best estimate methodology).
However, over the last few years, DECs have been refined to more comprehensively address credible multiple failures (common cause and common mode failures), complex sequences, rare internal and external events and severe accidents. The requirements entailed in this concept mainly concern new NPPs, but they can also be applied to existing plants to define reasonably practicable improvements.
Consequently, DECs now include:

- Combinations of failures selected on the basis of deterministic analysis, probabilistic risk assessment or engineering judgement;
- Internal and external events more severe than those considered in the design basis, caused by rare events that are very unlikely to occur but nevertheless considered credible events;
- Severe reactor accidents (that is, accidents involving core damage/fuel melt).

2.3 3rd and 4th DiD levels definition

In the DiD approach, the objectives of the different levels of defence are mainly defined as successive steps in the protection against the escalation of accident situations.
If the definition of levels 1, 2 and 5 are almost homogeneous, there is a notable difference in the limit between levels 3 and 4, which can be interpreted in 2 ways:

- Limit between design basis and DEC, i.e. complex situations resulting from multiple failures that could lead to core melt;
- Or putting the prevention of accident with core melt in level 3, and management of core melt accidents in level 4.

As a matter of fact, the phenomena involved in accidents with core/fuel melt (severe accidents) differ from those which do not involve a core melt.
Thus, the definition of DiD has been refined in different ways to include design basis events and design extension conditions (DECs), with and without core melt. For IAEA [5], DEC without core melt are covered in DiD level 4, as they are considered to be similar to severe accidents and thus the same approach to their assessment is used. For WENRA, they are covered in DiD level 3 as a sublevel, since they are considered to be closer to design basis events in terms of the radiological objectives and physical phenomena involved (see Table 2).

Levels of Defence		**Objective**	**Essential Means**	**Radiological consequences**
Level 1		Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation, control of main plant parameters inside defined limits	No off-site radiological impact (bounded by regulatory operating limits for discharge)
Level 2		Control of abnormal operation and failures	Control and limiting systems and other surveillance features	
Level 3	3a	Control of accident to limit radiological releases and prevent escalation to core melt conditions	Reactor protection system, safety systems, accident procedures	No off-site radiological impact or only minor radiological impact
	3b		Additional safety features, accident procedures	
Level 4		Control of accidents with core melt to limit off-site releases	Complementary safety features to mitigate core melt, Management of accidents with core melt (severe accidents)	Off-site radiological impact may imply limited protective measures in area and time
Level 5		Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response Intervention levels	Off site radiological impact necessitating protective measures

Tab 2: Levels of Defence in Depth - WENRA [6]

For new reactor designs, there is a clear expectation to address in the original design what was often “beyond design” for the previous generation of reactors, such as multiple failure events and core melt accidents, called DEC in IAEA SSR-2/1. This is a major evolution in the

range of situations considered in the initial design to prevent accidents, control them and mitigate their consequences, and in the corresponding design features of the plant. It implies that the meaning of “beyond design basis accident” is not the same for existing reactors and for new reactors. Several scenarios that are considered beyond design basis for most existing reactors are now included from the beginning in the design for new reactors (postulated multiple failure events and core melt accidents).
In addition, for new reactors, design features that aim to prevent a core melt condition and that are credited in the safety demonstration should not belong to the same level of defence as the design features that aim to control a core melt accident that was not prevented. However, should a core melt accident occur, all plant equipment still available may be used, when their use do not aggravate the situation. Indeed, in real situations, if features devoted to mitigation are available to prevent core melt, they will be used (avoiding core melt is always preferable, and a priority in accident management).
The question has been discussed by WENRA whether for multiple failure events, a new level of defence should be defined, because safety systems which are needed to control postulated single initiating events are postulated to fail and thus another level of defence should take over. However, the single initiating events and multiple failure events are two complementary approaches that share the same objective: controlling accidents to prevent their escalation to core melt conditions.
Hence, WENRA has proposed to treat the multiple failure events as part of the 3rd level of DiD, but with a clear distinction between means and conditions (sub-levels 3a and 3b, see Table 2).
The scope of the related safety demonstration has to cover all risks induced by the nuclear fuel, including all fuel storage locations, as well as the risks induced by other relevant radioactive materials.
Even though no new safety level of defence is suggested, a clear distinction between means and conditions for sub-levels 3a and 3b is lined out. The postulated multiple failure events are considered as a part of DEC in IAEA SSR-2/1. These proposals are both built on the original INSAG concept and strengthen its implementation, but [7] recognizes that two interpretations are possible (see Table 3).

<table>
<tr><th colspan="2">Levels of Defence Approach 1</th><th>Objective</th><th>Essential Design Means</th><th>Essential Operational Means</th><th colspan="2">Levels of Defence Approach 2</th></tr>
<tr><td colspan="2">Level 1</td><td>Prevention of abnormal operation and failures</td><td>Conservative design and high quality in construction of normal operation systems, including monitoring and control systems</td><td>Operational rules and normal operating procedures</td><td colspan="2">Level 1</td></tr>
<tr><td colspan="2">Level 2</td><td>Control of abnormal operation and detection of failures</td><td>Limitation and protection systems and other surveillance features</td><td>Abnormal operating procedures/emergency operating procedures</td><td colspan="2">Level 2</td></tr>
<tr><td rowspan="2">Level 3</td><td>3a</td><td>Control of DBA (postulated single initiating events)</td><td>Engineered safety features (safety systems)</td><td rowspan="2">Emergency operating procedures</td><td colspan="2">Level 3</td></tr>
<tr><td>3b</td><td>Control of DEC to prevent core melt</td><td>Safety features for DEC without core melt</td><td>4a</td><td rowspan="2">Level 4</td></tr>
<tr><td colspan="2">Level 4</td><td>Control of DEC to mitigate the consequences of severe accidents</td><td>Safety features for DEC with core melt. Technical Support Centre.</td><td>Complementary emergency operating procedures/severe accident management guidelines</td><td>4b</td></tr>
<tr><td colspan="2">Level 5</td><td>Mitigation of radiological consequences of significant releases of radioactive material</td><td>On-site and off-site response facilities</td><td>On-site and off-site emergency plans</td><td colspan="2">Level 5</td></tr>
</table>

Tab 3: IAEA-TECDOC Levels of DiD for the design of new NPPs [7]

As a matter of fact, a NPP can be designed based on both approaches, but compliance to both would induce an increase on independence requirements, even though they are already

difficult to satisfy. Otherwise speaking, there is no matter on which approach (IAEA or WENRA) is used, unless the independence requirements are not absolute. In the following, the WENRA approach is analysed.

3. Analysis

Following the Fukushima accidents, attention was paid to different areas during international discussions:

- The notion of levels robustness, generally addressed separately from their definition, but that could play an important role in their effectiveness,
- The notion of levels independence, that WENRA wants to reinforce,
- The role of diversity when obtaining independence, a notion presented at this form only in the WENRA document,
- The importance of ensuring that common cause and common mode failures, especially external events acting in combination, do not lead to breaches of safety provisions at several DiD levels, taking note of the particular attention that human and organizational factors demand,
- The concept of “practical elimination” of sequences leading to significant radioactive releases.

They are discussed in the following sections.

3.1 DiD implementation

3.1.1 Implementing safety provisions

Although DiD is largely used, it does not establish specific acceptance criteria for the adequacy of safety provisions. Other inputs are also taken into account when designing nuclear facilities and assessing their safety. They include deterministic analyses of normal operating conditions, design basis conditions and DEC as complemented by PSA (Probabilistic Safety Assessment).

In practice, the safety provisions for DiD are implemented in the design using:

- A deterministic engineering approach and analyses, which mainly relate to levels 1 through 3, plus specific features to address DEC, in particular containment performance during severe accidents (level 4); supplemented where necessary by PSA to identify cross-linkages, vulnerabilities and interdependences.
- Probabilistic studies to identify plant vulnerabilities, including complex situations due to several equipment and/or human failures, with a deterministic analysis used to establish scenarios that must be addressed, such as loss of electrical power or heat removal capability.

3.1.2 Practical elimination (as WENRA perspective)

In each level of DiD, some situations need to be practically eliminated as it cannot be demonstrated that, should they occur, their radiological consequences would be tolerable. Situations that could lead to early or large releases of radioactive materials have to be practically eliminated. Practical elimination, however, does not mean complete elimination or that events of significant releases are physically impossible, but rather that, with a high degree of confidence, such events have been demonstrated to be extremely unlikely.

Practical elimination can be applied using both prevention and mitigation safety measures. For existing plants, significant radioactive releases should be prevented or mitigated by means of reasonable practicable modifications/backfitting measures and severe accident provisions as far as practicable.

As noted above, DiD levels 1, 2 and 3 address the prevention and mitigation of anticipated events and unlikely but credible accidents. DiD level 4 addresses the mitigation of a severe accident. The goal of level 4 is to prevent or mitigate any significant radioactive releases from such accidents. In some cases, prevention and mitigation through the implementation of DiD should be reinforced, and those sequences leading to significant radioactive releases have to be “practically eliminated”.

Level 4 deals with scenarios that are already very rare, given the effective implementation of safety provisions at levels 1 to 3. It is included in both the IAEA safety requirements for new reactor designs (IAEA, 2016 [5]) and in WENRA objective O3 for accidents with core melt ([6] §03.4). The goal of WENRA objective O3 is that new NPPs have to be designed in such a way that even in case of an accident with core melt *“only limited*

protective measures in area and time are needed for the public […] and that sufficient time is available to implement these measures".

The implementation of the practical elimination concept is most effective through design features, and thus it is easier to implement in new reactors. For operating reactors, there are likely to be fewer practical opportunities for enhancing safety. These have to be considered on a case-by-case basis. It is important to highlight that a priority shall be given to practically eliminating "large and early releases" (LERs), as they are not consistent with public protection and may induce public contamination, compared to "large releases" that shall be prevented to avoid environment contamination (but with no direct human contamination).

The practical elimination concept is linked with DiD approach. As a matter of fact, it consists of an approach that put in the residual risk some initiating events or sequences or situations. As a matter of fact, the initiators leading possibly to a severe accident do not go through each DiD level until level 4.

3.1.3 From a DiD Level to another

DiD is implemented primarily through the combination of a number of consecutive levels of protection with independent effectiveness that would have to fail before harmful effects could be caused to people or to the environment. Design principles available to promote DiD include: redundancy, diversity, physical separation, train/channel independence, single-point failure protection and, as far as reasonably practicable, independence between levels. It should be implemented in a manner that ensures that each level is effective in meeting its specific objective.

In order to better understand this point of view, the following section will discuss some possible situations aggravation from different initiators.

This difference on the definitions mainly concern accidents with multiple failures. It mainly impacts the discussions relative to the independence between DiD levels:

- Is that required to search for independence between levels 3a and 3b?
- If diversity requirement is strengthen between DiD levels (as recommended by WENRA), this could lead to require beyond the necessary and feasible the requirements of diversification, as 3b corresponds to multiple failures, and that prevention to this is already based on diversity.

Nevertheless, in practice, level 3b is reached in the majority of the situations of failure of level 2 via multiple failures. Situations of degradation from level 3a to 3b (i.e. Design basis accident + common cause failure) that have a significant frequency are not numerous, so that WENRA expectations could not lead to impossibilities.

3.2 Levels robustness

It would not be sufficient to display different DiD levels if each one does not present an intrinsic robustness allowing to limit the risk of degradation of the situation and to reach the subsequent level. Concerning the inacceptable situation corresponding to the default of all levels, it would be theoretically possible to share a level of robustness to each one, in order to reach a global robustness envisaged. This does not correspond to the practice for multiple reasons.

First, as seen in §3.1.3, there are not systematically 5 levels of DiD for each postulated initiating event. Defaults leading to the 2nd level of DiD are quite frequent: typically a loss of an active function (for instance, loss of void at the condenser) or its intempestive action (inadvertent control rod withdrawal). Defaults of passive features like piping ruptures lead directly to the 3rd level, and there are defaults not taken into account in design, like the rupture of big primary components (e.g. the vessel). For these important defaults, the 2nd, the 3rd, or the 4th level could not exist. Other situations could be found for which at least one DiD level does not exist (see Table 4).

In those cases, the remaining levels are reinforced / strengthened, and in the case where only the 1st level exists, its robustness is obviously extremely strengthened. In the United Kingdom, the associated concept is called "Incredibility Of Failure" (IOF), applied mainly to the rupture of the big primary components (which can be assimilated to the practical elimination approach, but consists more on an initiator preclusion).

Generally speaking, as well as this single initiating events, one search to put in the “residual risk” some situations for which the consequences would not be manageable by the lasting DiD levels. Once these situations are put in the residual risk, DiD approach is in general no more applied.

Typical evolution of an event across DiD levels	AOO	Frequent Accident	Unfrequent Accident	Unexpected event	
Normal Operation	0	0	0	0	0
Incident	0				
Single Accident		0	0		
Event + multiple failure	0	0		0	
Severe accident	0	0	0	0	
Practical elimination	Possible at each step				Incredibility Of Failure (IOF)

Tab 4: Illustration of the difficulties when going across all DiD for implementation

Robustness of each level may vary considerably. The following are typical values associated for DiD levels:

- 1st DiD level covers a very large domain (the default frequencies may vary from 10^{-1} to very low frequencies (IOF), depending on the causes and consequences related to).
- The robustness covering area for the following levels are generally less wide. Typically, for levels 2 and 3, the single failure criterion is taken into account, which will lead to a probability of default in general less than 10^{-3}.
- Concerning level 4, it is not usual to take into account the occurrence of a single failure, and INSAG-12 [4] has as objective of 10^{-1} between the risk of core melt and the risk of large releases, which corresponds to the minimum robustness of this level.

Therefore, levels 2 and 3 are privileged in comparison to level 4, as regard of global safety objectives (preventing is always better than mitigating core melt).
Regarding these typical values, reinforcements may be necessary to strengthen certain features in order to reach the global safety objectives assigned to the plant.

3.3 DiD levels sufficient independence

The use of the DiD concept has been promoted through the IAEA Safety Fundamental Principles [8] and Standards [5]. The need for independence between DiD levels is not a new subject (see INSAG 10; [2] §25), but it is not systematically mentioned in the reference documents, and its scope is generally not developed. Even though the independence is not systematically mentioned, it can be considered that it is a part of the DiD concept as, if a level of defence fails inducting to a failure of the subsequent levels, thus there is not really defence in depth.
The corresponding requirements are generally not really developed:

- The IAEA safety fundamental principle 8 [8], in particular, states “*The primary means of preventing and mitigating the consequences of accidents is ‘defence in depth’… The independence effectiveness of the different levels of defence is a necessary element of defence in depth*”.
- IAEA SSR-2/1 [5] states in 2.12 “*This is to ensure that all safety related activities are subject to independent layers of provisions so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures*” and sets a specific requirement for the design “*Requirement 7: Application of defence in depth. The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable*”.
- SAPs [9]: “*The methodology ensures that if one level fails, it will be compensated for, or corrected by, the subsequent level*” (independence is nevertheless not mentioned here).

3.3.1 The principle of independence

Let’s recall that to each DiD level are associated initiating events, chosen and studied to ensure that the safety criteria attached will be respected and that the DiD level will not ‘fail’. Therefore there is, from a deterministic point of view, independence of levels.

Nevertheless, it is important to complete this analysis to ensure their independence, by a probabilistic method.
It is important to identify which features are used in a DiD level to resist the initiating event, and only the strictly necessary to manage the situation (as used in the deterministic approach). These features are concerned by the need for independence. All other systems (that were in function when the event starts, or those that are not necessary) are not concerned.
All features that are not called by DiD levels 2, 3 and 4 are associated to the normal operation (which also need different requirements and adequate safety classification for monitoring and protecting the operation under normal conditions).
In practice, the way to reach the independence *"as far as it is practicable"* is not specified. The whole classical means and features used to obtain "independence" may therefore be used, like redundancy, physical separation and diversity, and the reinforcement of independence may be obtained by reinforcing one of these means. Each way presents intrinsic limits, and in particular, a high level of redundancy is generally more efficient from a probabilistic point of view if it is associated to adequate diversification. WENRA promotes diversity, which plays an important role, but it is not an exclusive one.
An adequate independence is important for all levels, including the systems, structures and components (SSC) that are at the second level of DiD, to control anticipated operational occurrences (AOO) when using different types of controllers, limitations and protection systems for example. These SSCs are intended to detect and control deviations from normal operation states in order to prevent AOOs at the plant from escalating to accident conditions.
However, for some AOOs, these measures are not sufficient to prevent an accident condition from occurring, thereby activating the safety systems. Safety systems such as the reactor scram system and, depending on the type of the plant type, the overpressure protection system of the primary and secondary side, the emergency feedwater system and diesel generators, are needed as part of the design basis of the plant to prevent an event from escalating to a severe accident.

3.3.2 Prevention, monitoring and mitigation

At the beginning, the DiD concept was very simple and stated that all measures shall be taken to **prevent** an accident, but despite that, the potential occurrence of this accident shall be considered and therefore **monitoring** of the accident course shall be provided as well as **mitigating** features. The 3 key words are **prevention**, **monitoring** and **mitigation**. This concept was first applied in the design and especially in the definition of safety systems and features to prevent, monitor and mitigate accidents.
It was later extended to operational aspects for the prevention and mitigation of human errors.
With that definition, the need of independence between preventive and mitigative features was quite obvious. A failure of a preventive measure shall not affect the mitigating feature for the same accident.
A first drift of interpreting DiD and independence occurred when it was applied to the barriers approach. Of course the DiD concept should be applied to each individual barriers (cladding, primary system and containment on PWRs), but the barriers should have been independent, the failure of any of them should not affect the others. Clearly this suffered several important exceptions, since LOCA (primary system failure) could affect the cladding (first barrier) and on steam generators the second and third barriers were combined. But the independence can be considered sufficient if no credible PIE may induce the failure of all the barriers.
As showed in II.C, IAEA introduced significant changes in the DiD concept. It was not applied to individual accident or failure but was linked to plant conditions. 4^{th} and 5^{th} levels were introduced, with level 1 associated with normal operation, level 2 with AOOs, level 3 with design basis accidents (DBA), level 4 with multiple failures and severe accidents and level 5 with emergency arrangements.

With this new definition of the DiD concept, independence of DiD levels are much less clear and should be reinterpreted. Clearly it cannot mean that the various safety provisions should be different at each level. Otherwise it would mean the multiplication of dedicated systems specific to each level. That would introduce a lot of complexity in the design without obvious safety benefit. That is particularly true for support systems that serve both normal operation and accident conditions. For instance, is it reasonable to provide individual cooling and heat sink and HVAC for each level of DiD? It is well recognized that systems that are continuously in operation are more reliable than systems that operate only on demand. But of course, adequate provisions should be provided to cope with common cause failure of these systems.

Therefore a new definition of the independence of DiD levels should be produced.

Complete independence of systems and components at the different levels may not be possible; however, the aim should be to ensure as far as is practicable that the SSCs provided at different levels are independent of one another for the event they are intended to prevent or mitigate.

3.3.3 The role of diversity in obtaining independence

Thus, even if the application of the DiD principle across safety levels is a good and recognized international practice, a prescription of additional diversity and independence across all safety levels could result in inappropriately complex technical solutions. Moreover, this would be a significant departure from the international practice in designing Generation 3 reactors that may hinder design standardization. In addition, some designs may prefer to introduce diversity inside the same level of defence.

The DiD concept stipulates that independent protection against failure of safety functions should be provided, as far as practical, for different accidental situations. The effectiveness of this protection is established using the principles of, inter alia, redundancy, diversity, segregation, physical separation and single-point failure protection.

In practice, diversity is largely used in levels 2 and 3b, as features to cope with defaults of multiple common faults like mitigating an incident. It is also used inside level 3a, like protection concerning the long term situations. Concerning level 4, diversity is effectively used, including the updating strategies for existing generation II reactors (for example, confinement venting, hydrogen recombiners…). But it is not systematic. For EPR, the voluntary depressurization of the primary circuit is made by two identical lines, one dedicated to level 3b (feed and bleed), another for level 4 (prevention to core melt at high pressure and to induced steam generators tube ruptures). Even though it is not diversified, this redundancy allows a better independence between levels of DiD, in strict compliance with WENRA statement "*Use of dedicated systems to deal with core melt accidents, so that independence of the 4th level of the DiD is better ensured*".

More generally speaking, diversity allows a better visibility relative to the independence between defence lines. In practice, it is restricted by certain limits, for example:

- The possibilities of diversification, concerning, among others, support systems. Thus, each level of defence needs Instrumentation and Control (I&C) and diversity shall also be required inside the same level. Even if for 5th level the I&C is marginal, the current GEN 3 projects have 2, or at the most, 3 types of I&C platform, which could not be sufficient to apply diversity wherever we would want.
- For certain functions like confinement, it does not seem realistic to double or diversify them. It is better to design the containment to resist all postulated solicitations at each of the levels where it is acting.
- Even though diversity is technically feasible, it could induce important overcosts, which could not be justified according to the safety benefit it provides. Diversification shall remain reasonable.

Thus, an alternative to systematic diversity consists of ensuring, for each of the causes leading to the 3rd level failure, that these causes do not lead to the failure of the 4th level, and

to optimize the design to reduce these dependences. As a consequence, a particular attention should be paid to obtain a sufficient independence between levels 3 and 4.

Diversity is a good way to reinforce the robustness of prevention or mitigating an accident situation. Having two diverse provisions (both different hardware or hardware and human action) to prevent an event or to mitigate it would certainly bring safety benefits. But again this principle should not be applied across the 5 DiD levels. The need depends on the frequency of events. It is likely to be useful for frequent events but not for infrequent ones. The implementation of diversity should be looked at in an overall assessment of risk.

The independence between DiD levels should not be an absolute design principle but risk analysis should be used to identify areas where this would be necessary. For instance, the use of safety related cooling water systems for operation purposes ensure their availability in case of accident conditions, for accidents that are not initiated by loss of cooling water.

4. Conclusions

DiD as a concept has been used for many years, along with other tools (as barriers method), to optimize nuclear safety in reactor design, operation and assessment.

The use of the DiD concept remains valid after the Fukushima Daiichi accident. Indeed, lessons learned from the accident and its impact on the use of DiD have reinforced its fundamental importance in ensuring adequate safety.

Consideration of the accident has led to further work on DiD implementation, in particular on discussing the need for reinforcement of independent effectiveness among the safety provisions for the various DiD levels, to the extent practical.

Additionally, it shows that the concept of practical elimination of sequences leading to significant radioactive releases is crucial. Fukushima accidents do not mean that a “practical eliminated situation” occurred, but it showed that the design basis level of the flooding induced by a credible tsunami was underestimated. This accident reinforces the need for a regular reassessment of the design basis through periodic safety review, as a cornerstone for nuclear safety. Attention should be paid to reassessing design basis levels of natural hazards considered, taking into account the recent feedback available. Thus, sufficient independence of DiD levels should consider the sufficient robustness of each level, and adequate use of diversity.

5. References

[1] J. Libmann, *“Elements of nuclear safety”*, p.35, Les Editions de la Physique, IPSN, Les Ulis (1996)

[2] IAEA - INSAG 10 *“Defence in Depth in nuclear safety”* (June 1996)

[3] IAEA – 75-INSAG 3 *“Basic safety principles for nuclear power plants”* (1988)

[4] IAEA - INSAG 12 *“Basic safety principles for nuclear power plants – 75-INSAG-3 Rev.1”* (October 1999)

[5] IAEA - SSR-2/1 Rev 1 *“Safety of Nuclear Power Plants: Design”* (February 2016)

[6] WENRA (RHWG) Report *“Safety of new NPP designs”* (March 2013)

[7] IAEA-TECDOC-1791 *“Considerations on the application of the IAEA Safety Requirements for the Design of Nuclear Power Plants”* (May 2016)

[8] IAEA – SF-1 *“Fundamental Safety Principles”* (November 2006)

[9] Safety Assessment Principles for Nuclear Facilities (November 2014)