ENISS
European Nuclear Installation Safety Standards

POSITION PAPER

Defence-in-Depth (DiD) Implementation

October 2019

Table of Contents

Summary

ENISS Licensees support the need to create common principles and guidance that would be widely accepted by the European Regulators. ENISS members share information about their practices and discuss their regulatory and technical rationales to agree on common positions.

This document provides an overview of the ENISS common licensee understanding and position on Defence in Depth (DiD), from the concept to its implementation with its associated requirements and practices.

DiD is a powerful concept to ensure safe designs, safe operations, and support nuclear safety improvements. It has been used for decades and has evolved over time. Applying the DiD concept is a recognised international practice with general safety principles being common to regulators, licensees and designers. However the details of its implementation may differ from country to country and may be plant-specific. ENISS members share the view that the implementation should account for reasonable practicability and that there are some limits to be appropriately taken into account concerning the requirements of independence across the DiD levels.

Based on observations and key elements drawn from experience in European countries, ENISS members endorse the following principles for a successful DiD implementation:

- Principle 1: ***DiD concept is, in practice, adequately implemented via a comprehensive set of safety-related considerations, requirements and rules*** *(e.g. deterministic analysis)*

- Principle 2: ***A holistic approach should be adopted to ensure DiD robustness, while addressing prevention and mitigation***

- Principle 3: ***Independence requirements should be applied in a broad perspective***

- Principle 4: *In order to confirm that the DiD concept and the associated requirements are appropriately implemented,* ***importance should be duly given to probabilistic safety analyses as a complementary approach***

1. Definitions, existing framework and documents

Defence in depth (DiD) is a design concept first applied to the nuclear industry in the sixties and early seventies. The historical development of the concept is outlined in INSAG-10 (1996) [1]. The March 2011 Fukushima Daiichi Nuclear Power Plant accidents raised a number of questions on the implementation of DiD, particularly for external hazards, but confirmed the merits of the DiD concept.

In setting down the Basic Safety Principles for NPPs, INSAG-3 [2] (revised by INSAG-12 [3]) defined the DiD Principle as:

> *« To compensate for potential human and mechanical failures, a defence in depth concept is implemented, centred on several levels of protection 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 the harm in case these barriers are not fully effective. »*

This is captured in the IAEA « Safety Fundamentals » (SF-1 [4]), « Principle 8: Prevention of accidents » states in 3.31:

> *« 3.31 The primary means of preventing and mitigating the consequences of accidents is 'defence in depth'. Defence in depth is implemented primarily through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defence in depth ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability. The independent effectiveness of the different levels of defence is a necessary element of defence in depth. »*

Even though implementation of the DiD concept may differ from one country to another (see §2.2) and may, to a certain degree, be design dependent, the main principles are common and, as presented in [1], the *"objectives are as follows:*

- *to compensate for potential human and component failures;*
- *to maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves; and*
- *to protect the public and the environment from harm in the event that these barriers are not fully effective."*

DiD is currently structured in **five levels** (described by 2.13 of SSR-2/1 Rev 1 [5] and summarised in Table 1). Should one level fail, the subsequent level would come into play to compensate for or take control of the situation. The idea of multiple levels of protection is the heart of DiD strength. Practically, DiD implementation via provision of means is based upon two corollary principles: **prevention and mitigation**.

As stated in INSAG-3 [2], the DiD concept is associated with the interposition of successive physical barriers between a radioactive source and the people or environment to protect. The

reliability of these barriers is enhanced by applying the DiD concept, thereby protecting each of them by a series of measures. It is necessary to ensure, to the extent practicable, that the different safety systems protecting the physical barriers are functionally independent under accident conditions.

The general objective is therefore to ensure, to the extent practicable, that a single failure at one level of defence, and even multiple failures at more than one level of defence (such as the scram system, the electrical power supply, the steam generator feedwater systems, or the ultimate heat sink), would not hinder the effectiveness of subsequent levels. A frequently mentioned way to implement DiD is to ensure, as far as reasonably practicable, independence between the different levels of defence, taking into account all plant provisions and operating procedures [6], as stated in SSR-2/1 Rev1 [5] (Requirement 7 - Application of DiD):

> *"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."***

A sufficient independence between the different levels of defence becomes therefore a key element in meeting this objective (see §3.2).

TABLE 1. Levels of DiD (INSAG-10 [1])

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

These five levels of DiD are also referred to in other texts including WENRA documents in Europe and in the national requirements from different countries (see §2.1). However, some situations are considered as « beyond design » for existing plants (such as multiple failures events and core melt accidents) and the same situations are considered in the design envelope of new plants. As a consequence, WENRA [7] has refined the DiD approach to introduce the concept of Design Extension Conditions (DECs), while remaining consistent with the IAEA SF-1 document [4]. The introduction of DECs without core melt within the level 3

(identified by WENRA as level 3.b, also called DEC-A) is consistent with the objective of that level, which is to control accidents (i.e. to prevent core melt) and stay within the plant design envelope.

These refinements of DiD levels (level 3 for WENRA [7], level 4 for IAEA [8]) were introduced in international standards to provide guidance on DiD implementation. In practice, implementation of DiD consists of design [5] and operational [6] means, including for example:

- a prudent design interposing barriers, based on a deterministic approach complemented by a probabilistic approach, to ensure the fundamental safety functions,
- the organisation of operational safety (through technical specifications and operating procedures, taking into account the management of safety culture, the human factor and training of plant staff, maintenance, testing, surveillance and inspection),
- management of accidents and emergency preparedness and response,
- design of safety improvements (taking into account operating experience, analysis of the safety impact of plant modifications …).

The DiD concept has been used for decades and its implementation is a recognised international practice.

2. Observations and examples of application

2.1 Mandatory national regulatory frameworks

Application of DiD principles may result in different national regulatory requirements, due to (for instance):

- **specific natural/geographical conditions**, in particular with regard to potentially extreme natural events: assumptions on event severity such as extreme meteorological conditions can largely differ (e.g. Sweden versus Spain: snow, frost, heat-wave, etc.);

- the different **nature of specifications**, for example:
  - guidance for safety analysis potentially leading to different assumptions (depending on the type of event, more or less conservative / realistic) or different acceptance criteria, etc.
    For example, in Finland (YVL Guide B.1 §4.3), WENRA DiD level 3.b (4.a for IAEA or DEC-A) is subdivided in:
    - « DEC-A » (AOO and accidents until DBC-3 involving an additional common cause failure in a system required to execute a safety function),
    - « DEC-B » (Combination of multiple failure events selected as significant on the basis of a PRA) and,
    - « DEC-C » (relative to rare external events, which the facility is required to withstand without severe fuel failure);
  - prescriptions from the regulators: in France, based on ASN prescriptions issued at the beginning of 2000's and since the end of 2007, all reactors in operation are equipped with hydrogen passive autocatalytic recombiners (PAR) to manage the risk of high hydrogen concentration inside the containment in core melt accident situations.

- various approaches to **periodic safety reviews** and their applications;

- **lessons learnt from national operating experience** leading to an over-sensitivity on some topics, for example:
  - in France, following the flooding event at Blayais site in December 1999, EDF initiated a reassessment of every single site protection against external flooding events (revision of the flood safety level, …),
  - in Sweden, the electric power system event at Forsmark site in July 2006 (resulting in voltage fluctuations spreading across several electrical systems of the plant) had a major influence on the measures taken as part of backfitting and modernisation programs related to electrical systems, including grid disturbances;

- a **large range of types** (PWR, VVER, gas-graphite, PHWR …) **and generations of NPPs** in operation, from country to country;

- **different interpretations** of higher level requirements or principles;
- other factors influencing the regulatory decisions (**timely implementation of improvements**, **specific risk related decision-making** and associated **time pressure**, sometimes under political and/or societal influence).

Even though in all countries the regulatory framework is regularly updated, these evolutions are not submitted to a harmonised European schedule but rather to national consideration and availability of resources (e.g. the implementation of the 2014 WENRA Safety Reference Levels [9] in the national regulatory frameworks [10]).

Indeed, some countries have already reviewed and modified their regulatory framework, whereas others are still in a review process to identify, if any, appropriate changes required to reflect recently revised international standards.

Here follows some examples of requirements or guidance applying to DiD in European countries:

Belgium: FANC is revising a Royal Decree in order to transpose the WENRA Safety Reference Levels updated in 2014 [9]. A set of DEC sequences is defined, based on a dedicated methodology. DEC-A and DEC-B objectives and criteria are being developed by the licensee.

Czech Republic: DiD is applied through a functional analysis based mainly on IAEA SSG-30 [11], TECDOC-1791 [8] and SRS46 [12], and considered from two points of view, the standpoint of the Unit which defines the DiD levels, and the standpoint of the Structures, Systems and Components (SSCs) which provides functions into a set of DiD lines. The aim of the functional analysis performed in connection with design basis reconstruction is to provide an evaluation of the independence of the DiD levels and their individual strength upon various challenges (hazards, events). It allows SSCs of different types (mechanical equipment, electrical systems, civil, I&C, HVAC, firefighting…) to fit in various DiD lines. For instance, for a Loss Of Coolant Accident (unit state is DiD-3), power supply sources and power distribution will be in a DiD line that almost corresponds to normal operation (DiD-1).

Finland: YVL Guide B.1 gives detailed guidance in chapter 4.3 « Application of defence in depth principle in the design », including independence of levels and their individual strength. The text allows a certain dependency for specific systems: §429 states that « *Due consideration shall be given to the dependence on the auxiliary systems supporting safety functions at different levels of defence-in-depth concept…* » and §439 states « *If the redundant parts of a safety system are interconnected for the distribution of electricity or control signals, the safety advantage as compared to a solution without such interconnections shall be justified* ».

France: DiD concept was applied for the design of existing plants. Since 2012, as formally stated by Ministerial Order, the requirement evolved. An explicit demonstration of compliance with the DiD concept and with a « sufficient independence of levels of DiD » is required. More details are given in ASN (French regulator) decision No.2015-DC-0532 (requirements related to the safety analysis report: objectives, content and update) and, for new reactors, in the ASN guide No.22 (safety when designing PWRs). This guide states, for instance, that the SSCs required to ensure safety functions during severe accident situations should be, as far as reasonably possible, independent from those used during normal operation or under AOOs, DBA and DEC-A situations.

Sweden: National publications regarding DiD are mainly based on INSAG-10 [1] and INSAG-12 [3]. SSM, the Swedish regulator, sets the national requirements in SSMFS 2008:1, which is a cornerstone for achieving and maintaining sufficient radiation protection. *"The defence in depth system should be applied on five levels in accordance with the table below. If one level of defence should fail, the next level will take over. A failure in a component or in a manoeuvre on one level, or combinations of failures which occur simultaneously on different levels, must not jeopardise the function on the next level. Thus, independence between the different levels in the defence in depth system is essential to achieve this."*

UK: The UK can be seen as specific, as the licensee is responsible for providing its own standards and guidance (e.g. the « Rationale for the Nuclear Safety Principles » and detailed guidance documents and specifications) while meeting the requirements of the Nuclear Site Licence which is approved by the regulator (ONR). The regulator also provides guidance to its inspectors and makes available these guidance documents for information. The main document is the « Safety Assessment Principles for Nuclear Facilities » (SAPs [13]), supported by various Technical Assessment Guides (TAGs) which provide detailed guidance to the inspectors in their assessment of various technical areas. One of the Key Engineering Principles in the SAPs is EKP.3 Defence in Depth. "*Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression*". DiD is referred to in a number of other SAPs requirements but generally as an underpinning principle to be taken into account.

Since national regulations or safety requirements, as well as the actually implemented safety measures, are country-specific and reflect particular operating experience or practice within the country, there are differences in priorities and schedules among ENISS members when implementing safety improvements.

Even though implementation of the concept of DiD may differ from country to country and may to a certain degree depend on plant design, the general principles are common to all the regulators, licensees and designers.

2.2 Application by licensees

The ENISS licensees comply with their national regulations and generally follow closely their national regulatory guidance, among which many requirements and guidelines stem from the DiD concept. However the detailed rationale on how the DiD international guidance and recommendations are derived can be fairly implicit.

The use of the DiD concept, along with deterministic and probabilistic safety analyses, has been key in enhancing nuclear safety over the last decades, both for the re-assessment of the requirements for new reactors and for the identification of reasonably practicable and achievable safety improvements to existing reactors. As an answer to SSR-2/1 Rev 1 ([5]; e.g. §2.13 on severe accidents mitigation and §4.13A on levels sufficient independence), the requirements/expectations for DiD have been enhanced in many countries, in particular in relation to accident situations (levels 3, 4) and emergency preparedness and response (level 5).

ENISS members note that, even though Fukushima Daiichi lessons learned led to enhancing water & power supplies as well as emergency preparedness and thus strengthening DiD levels, it is not a result from a change to the DiD concept.

Furthermore, the choice of plant-specific back-fitting depends on the regulatory-specific prescriptions. National requirements greatly differ from one country to another or evolve significantly between two Periodic Safety Reviews (PSRs) that even « sister plant » designs may diverge and the designs may become plant-specific. For example, Forsmark I & II (Sweden) were essentially identical to Olkiluoto I & II (Finland) at commissioning stage, but their retrofits have followed different routes, often for regulatory reasons, resulting in plant designs that are clearly different now. This is also the case for new designs that had to be customised to fit the site-specific conditions but also local regulatory requirements and expectations, making it hardly achievable to define a single « reference plant ».

The previous examples illustrate that reaching a satisfactory nuclear safety level, or a full application of the DiD concept may take different routes.

For a nuclear facility on a dedicated site, the licensee applies a list of requirements approved by its national regulator. In practice, despite being derived from a common DiD concept, those selected requirements may be very plant- or country-specific.

3. Key elements drawn from experience in implementing the DiD concept

3.1 A concept rather than a piece of demonstration

The DiD concept is defined by high level standards (mainly by IAEA and WENRA) which are considered as high level recommendations without being explicit design requirement by themselves. For ENISS members, it remains a general concept rather than an engineering tool. This concept is applied through design approaches and methods contributing to the robustness of the design which are to be considered concurrently.

New analysis applying DiD concept can be triggered under different situations: DiD is considered as monitored, explicitly or not (for example as part of a modification assessment), as a part of PSRs or after particular events (feedback from accidents, internal or external events), as well as based on operating experience or PSA results. All these situations can trigger new analyses.

Safety demonstration intrinsically implements the DiD concept: although DiD is used in almost all regulatory systems, it is not seen as establishing specific acceptance criteria for the adequacy of safety provisions. The implementation of DiD when assessing nuclear plant safety includes deterministic analyses (normal operating conditions, design basis accidents and design extension conditions), probabilistic analyses and engineering judgement. The DiD concept can also provide a logical structure for formulating and assessing safety design measures as well as assessing operational provisions.

Application of the DiD concept is more effective when addressed early during a project: to maximise the effectiveness of the use of DiD, it can be part of the early design process and addressed in a consistent way. It can be illustrated for a new project, when a particular attention to sufficient independence of the safety provisions at different levels of DiD can avoid common cause failures into the design.

3.2 Sufficiently independent levels of protection

Following the Fukushima Daiichi accidents, numerous analyses have been made by different organisations, and the lessons learned show that the concept remains valid [14]. However, many questions arose from these analyses, highlighting the importance of the implementation of the DiD concept (how it has been or can be used in practice), and in particular on the following subjects:

- the notion of robustness of a DiD level, generally addressed separately from the level definition, but playing an important role for the efficiency of the concept,
- the notion of independence between levels and the need for strengthening them,
- the role of diversity to achieve independence between levels (a notion presented by WENRA [7] O3.2 Position 2).

It should be noted that the reasonable practicability limits the requirement of independence:

- The events/situations considered as part of one level do not systematically result from a failure of system/features associated with the previous level of defence, and thus to face the occurrence of an event, there are not systematically means from each of the five levels of DiD to protect the plant. **Therefore, it is not practicable to design a NPP with independent systems performing the safety functions for all Postulated Initiating Events (PIEs) at each relevant level of DiD**.
- There are several SSCs in a NPP that are credited in more than one level of DiD (e.g.: pressure vessel, containment and its associated features, main control room (MCR, and ultimately the operating crew), protection system, electrical supply, cooling chain, heat sink, the HVAC, …), **and it is not feasible nor beneficial for safety, due to the potential induced complexity, to allocate each SSC to one particular level of DiD**.
- With an objective not to increase the complexity of the I&C system and Man-Machine Interface, actuation of equipment needed to handle anticipated operational occurrences may be combined with I&C for normal operation if sufficient compensatory requirements are satisfied.
- The grid connection may belong to DiD level 1 but may be also used, if available, in DiD levels 2, 3, 4. This is beneficial for nuclear safety to be able to rely on such an electric power supply, when available.
- The emergency AC power supply (which may be seen as belonging to DiD level 3) may be used also in DiD level 2 (e.g. short Loss Of Offsite Power). An additional diverse AC power supply may be designed for DiD level 3.b (DEC-A) as a response to a common-cause failure of the (not-diversified) emergency power supply. This alternate power source for DiD level 3.b (DEC-A), if available, may also be used for DiD level 4 (accidents with core melt, or severe accidents). The rationale for this is that an additional and diversified power supply is not significantly reducing the risks, while the ability to achieve diversification from the emergency and alternate supply is a huge challenge.
- Since the principles of equipment and cable separation already exist between redundant systems and between safety classified and non-safety classified systems, it may not be reasonably practicable to introduce additional separation on the basis of levels of defence.

Thus, a prescription of additional diversity and independence across all safety levels could result in requiring complex technical solutions, the implementation of which may have adverse effects on nuclear safety. The independence between DiD levels should not be an absolute design principle but risk analysis should be used to assess relevant common cause failures and then identify the areas where this would be necessary. For instance, devoting all equipment/systems to a single level (without possibility of sharing them with other levels) could negatively impact the overall plant nuclear safety as it might increase the plant and operations complexity.

As discussed above and stated in §28 of INSAG-10 [1], complete independence of systems and components at the different levels may not be feasible. In that case, other means may be implemented:

> "***If it is not feasible to have independent levels of defence against some events (such as sudden reactor pressure vessel failure), several levels of precautions are introduced into the design and operation****. Such precautions may be taken, for instance, in the selection of materials, in periodic inspection or in siting, or in design by incorporating additional margins of safety."*

However, the aim should be to ensure as far as is practicable that the SSCs provided at different levels are not claimed at a level, having already failed at the previous level. This can be verified for accident sequences using PSA, where dependencies are modelled. Complete independence at each level would, in principle, provide some defence against unknown initiators but may not be practicable.

For ENISS members, sufficient independence of DiD levels should be based on a minimum level of redundancy, on physical separation and on diversity (even though this is not systematically necessary). Achieving sufficient independence of DiD levels does not mean that different systems for each level should be used but that the risk from common cause failures should be sufficiently reduced. As an illustration, if a system is not affected by an initiating event, it can be used for instance for level 2 and, if the situation escalates to the next DiD level it can also be used for level 3 mitigation.

For existing plants, some ENISS members noticed possible issues with the independence of DiD levels and/or the demonstration of sufficient margins (e.g. cliff-edge effect) or robustness of levels. A typical example for existing plants lies with geographical separation, that can limit improvements possibilities even when applying diversity (for example if different safety divisions hosting redundant parts of safety systems are located in the same building or housed in the same compartment with limited separation; in certain cases, any improvement may rely on modification that would not be reasonably practicable, such as creating a new separated building).

This confirms that implementation of safety measures should also account for reasonable practicability. The acceptability of the degree of independence between DiD levels should be evaluated by deterministic and probabilistic risk analyses along with engineering judgement in terms of real contribution to nuclear safety improvement.

4. Principles for a successful approach

Based on the observations and key elements drawn from experience in European countries, the following principles are suggested for a successful approach when implementing DiD:

1. **DiD concept is, in practice, adequately implemented via a comprehensive set of safety-related considerations, requirements and rules** (e.g. deterministic analysis);
2. **A holistic approach should be adopted to ensure DiD robustness,** while addressing prevention and mitigation;
3. **Independence requirements should be applied in a broad perspective;**
4. In order to confirm that the DiD concept and the associated requirements are appropriately implemented, **importance should be duly given to Probabilistic Safety Analysis as a complementary approach**.

4.1 DiD is adequately implemented via a comprehensive set of safety-related considerations, requirements and rules

Much has been done by European countries in benchmarking and continuously improving their nuclear safety frameworks and regulations, in great part through the application of the DiD concept.

This application is based chiefly on:

- the choice of an appropriate site, with particular consideration for the potential natural or human-induced risks that could affect the nuclear installation;
- the identification of the whole set of safety functions contributing to the demonstration of nuclear safety;
- a proportionate approach according to risk;
- a cautious design approach, integrating design margins and wherever necessary introducing adequate redundancy, diversification and physical separation of the items important for safety that fulfil safety functions necessary to achieve a high safety level;
- the quality of equipment and activities important for safety, to reach a high reliability level;
- a good preparation (training, regular exercise…) for the management of incident and accident situations.

The high level of nuclear safety of ENISS members' nuclear power plants is demonstrated by a prudent deterministic approach (including conservative assumptions and bounding analyses) which reflects the sound application of the DiD concept. This approach integrates the technical, organisational and human dimensions. Safety analyses are performed to demonstrate that barriers to the release of radioactive material prevent an uncontrolled release to the environment. This demonstration includes the control of the fission process within the acceptable design limits, the cooling of the reactor core with the heat transferred to ultimate heat sinks, the confinement of radioactive material, shielding against radiation, along with

ensuring various other acceptance criteria. Moreover the deterministic safety analysis is complemented by probabilistic safety analysis of accidents and their consequences.

The above set of considerations, appropriately applied, give confidence that the DiD concept is adequately implemented.

4.2 A holistic approach should be adopted to ensure DiD robustness, while addressing prevention and mitigation

As Fukushima Daiichi accidents lessons showed [14], it can be tempting to focus on a specific line of defence, in this example, specially addressing Severe Accident mitigation issues or very rare events, rather than having a balanced selection process of reasonably practical measures (e.g. risk informed decision making process). The goal should be to ensure a relevant balance between prevention and mitigation.

It should be remembered that, even though a number of resilience enhancements were identified as a result of reviews of lessons learned from the Fukushima Daiichi Nuclear Power Station accidents, in most cases these were to provide additional protection against undefined postulated failures rather than being driven by weaknesses in the current DiD provisions (i.e. defence against “unknown, unknowns”, which is one of the roles of DiD). As a result, these modifications mobilised the whole available resources for safety improvements, while their impact in terms of overall risk reduction can be relatively small.

The design should be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation to accident conditions for all failures or deviations from normal operation that are likely to occur over the operating lifetime of the NPP (SSR-2/1 Rev 1 § 4.13).

ENISS members’ perspectives for safety improvements to enhance DiD levels robustness include a holistic approach that considers both prevention and mitigation features.

4.3 Independence requirements should be applied in a broad perspective

As stated by IAEA SSR-2/1 Rev.1 [5], independence between DiD levels shall be applied “as far as reasonably practicable”. The need for harmonisation / additional guidance on DiD may depend on national specificities.

In the future discussions or developments of additional requirements/guidance in this area, it is important to keep in mind that “*total* independence” (i.e. implying that only different/dedicated systems are able to form independent DiD levels) could be unachievable and not desirable for the sake of nuclear safety. It should be possible to keep some SSCs shared between more than one DiD level, even for new designs (e.g. control rooms, essential power supply or support systems, possible advantages of cross-connections).

If future additional guidance is provided from international standards, the independence requirements should remain in a broad perspective, the primary goal being the overall safety effectiveness of the Defence-in-Depth implementation.

4.4 Importance should be duly given to Probabilistic Safety Analysis (PSA) as a complementary approach

Probabilistic safety assessment (PSA) is an effective means of enhancing the understanding of plant vulnerabilities, including possible dependencies or complex situations due to several equipment and/or human failures. The results can be used to improve DiD in order to inform detailed risk management and decision-making.

PSA is also a useful tool for optimising efforts in implementing DiD. In association with deterministic analyses, PSA may support where relevant the verification that DiD has been given appropriate and prudent attention. PSA support logical thinking in terms of structuring the safety assessment and assessing the risk. It also helps to structure the demonstration of risk reduction to an ALARP (As Low As Reasonably Possible) level i.e. breaking down reasoning through different levels and thinking about whether adequate means are available for prevention and mitigation.

INSAG-10 [1] encourages the use of PSA, whilst recognising, and allowing for, its limitations. NRC (USA regulator) have embraced this approach and issued a "PRA Policy Statement" [15] which formalised the US Nuclear Regulatory Commission's commitment to risk-informed regulation through the expanded use of PRA. The PRA Policy Statement states:

- The use of PRA technology should be increased in all regulatory matters to the extent supported by the state of the art in PRA methods and data, and in a manner that complements the NRC's deterministic approach and supports the NRC's traditional defence-in-depth philosophy;
- PRA should be used to reduce unnecessary conservatisms associated with current regulatory requirements.

For existing reactors, Defence in Depth can be enhanced through processes such as Periodic Safety Reviews (PSRs), plant-specific back-fitting and feedback from operating experiences. However applying only deterministic approaches may lead to unbalanced improvement choices, for example and especially for existing plants putting too much emphasis upon accident mitigation whereas prevention of initiating or consequential events might bring more benefits. For ENISS members PSA insights are also necessary to identify the most significant sequences and opportunities for safety enhancements for both new and existing reactors.

A major outcome of a design assessment is to ensure that the DiD concept has been properly applied and that the residual risk is acceptable, which reflects that all relevant efforts have been made to reach an adequate degree of defence in depth. To this end the use of PSA as a complementary means is needed and its use should be encouraged to direct the efforts where fruitful for the overall level of nuclear safety.

5. Abbreviations

Abbreviation	Definition
AOO	Anticipated Operational Occurrences
ALARP	As Low As Reasonably Practicable
ASN	Autorité de Sûreté Nucléaire (France) – The French Regulator - Safety Nuclear Authority
ATWS	Anticipated Transient Without Scram
DBA	Design Basis Accidents
DBC	Design Basis Conditions
DEC	Design Extension Conditions
DiD	Defence in Depth
ENISS	European Nuclear Installations Safety Standards
EURATOM	European Atomic Energy Community
FANC	Federal Agency for Nuclear Control (Belgium)
HVAC	Heating, Ventilation, and Air Conditioning system
IAEA	International Atomic Energy Agency
I&C	Instrumentation & Control system
LOCA	Loss Of Coolant Accident
MCA	Maximum Credible Accident
MCR	Main Control Room
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission (United States of America)
NSD	Nuclear Safety Directive 2014/87/EURATOM 2014
ONR	Office for Nuclear Regulation (UK)
PAR	Hydrogen Passive Autocatalytic Recombiners
PE	Practical Elimination
PHWR	Pressurized Heavy Water Reactor
PIE	Postulated Initiating Event
PRA	Probabilistic Risk Assessment
PSA	Probabilistic Safety Assessment
PSR	Periodic Safety Review
PWR	Pressurized Water Reactor
RHWG	WENRA Reactor Harmonisation Working Group
SAPs	ONR Safety Assessment Principles for the UK
SBO	Station Black-Out
SSCs	Structures, Systems and Components
SSM	Swedish Radiation Safety Authority (Sweden)
STUK	Radiation and Nuclear Safety Authority (Finland)

TAG	ONR Technical Assessment Guide
UK	United Kingdom
VVER *or* WWER	Water-Water Energetic Reactor (Russian Design of Pressurized Water Reactors)
WENRA	Western European Nuclear Regulators Association
YVL	Ydinturvallisuusohjeet - Finnish Regulatory guides on nuclear safety, issued by STUK

6. References

[1]. IAEA - INSAG 10 *"Defence in Depth in Nuclear Safety"* (June 1996)

[2]. IAEA – 75-INSAG 3 *"Basic Safety Principles for Nuclear Power Plants"* (1988)

[3]. IAEA - INSAG 12 *"Basic Safety Principles for Nuclear Power Plants – 75-INSAG-3 Rev.1"* (October 1999)

[4]. IAEA – SF-1 *"Fundamental Safety Principles"* (November 2006)

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

[6]. IAEA – SSR-2/2 (Rev. 1) « *Safety of Nuclear Power Plants: Commissioning and Operation* » (2016)

[7]. WENRA (RHWG) Report *"Safety of new NPP designs"* (March 2013)

[8]. IAEA -TECDOC-1791 *"Considerations on the application of the IAEA Safety Requirements for the Design of Nuclear Power Plants"* (May 2016)

[9]. WENRA (RHWG) Report *"Safety Reference Levels for Existing Reactors – Update in relation to lessons learned from TEPCO Fukushima Dai-Ichi accident"* (September 2014)

[10]. WENRA (RHWG) Report « *Status of the Implementation of the 2014 Safety Reference Levels in National Regulatory Frameworks as of 1 January 2018* » (March 2018)

[11]. IAEA - SSG-30 « *Safety Classification of Structures, Systems and Components in Nuclear Power Plants* » (May 2014)

[12]. IAEA – Safety Reports Series N°. 46 *« Assessment of Defence in Depth for Nuclear Power Plants »* (February 2005)

[13]. ONR « *Safety Assessment Principles for Nuclear Facilities* » 2014 Edition, Revision 0 (November 2014)

[14]. OECD/NEA Report n° 7248 « *Implementation of Defence in Depth at Nuclear Power Plants : Lessons Learnt from the Fukushima Daiichi Accident* » (2016)

[15]. NRC 60 FR 42622 « *PRA Policy Statement* » (August 1995)