Scientific Research Publishing

Open Journal of Safety Science and Technology, 2016, 6, 35-54
http://www.scirp.org/journal/ojsst
ISSN Online: 2162-6006
ISSN Print: 2162-5999

The Evolution of Defense in Depth Approach: A Cross Sectorial Analysis

Lorenzo Chierici[1], Gian Luigi Fiorini[2], Stefano La Rovere[3*], Paolo Vestrucci[3]

[1]Via Toffano 4, Bologna, Italy
[2]Le Clos des Lierres, Ville Laure, France
[3]NIER Ingegneria S.p.A., Via Bonazzi 2, Castel Maggiore, Bologna, Italy
Email: *s.larovere@niering.it

How to cite this paper: Chierici, L., Fiorini, G.L., La Rovere, S. and Vestrucci, P. (2016) The Evolution of Defense in Depth Approach: A Cross Sectorial Analysis. *Open Journal of Safety Science and Technology*, **6**, 35-54.
http://dx.doi.org/10.4236/ojsst.2016.62004

Received: July 14, 2016
Accepted: September 4, 2016
Published: September 8, 2016

Abstract

The Defense in Depth (DiD) is a classical defensive concept currently applied to a variety of technical fields, including nuclear (where this concept is widely applied) and chemical industry, Information and Communication Technology (ICT), transport, and many others. It deals with slowdown of the progression of an "attack" against a "target" by using multiple and independent levels of protection (or lines of defense), designed to compensate for the failure of one or more defenses, ensuring that the risks are kept acceptable. Concerning the current practices for the DiD implementation and the rationale for its evolution, there is a shared recognition that the reinforcement of DiD is the key to improve the safety of future installations for all types of technologies and industries. Within this context, the results of Probabilistic Safety Assessment (PSA) play a key role in the demonstration of both the robustness of the design and safety, supporting the verification that the DiD principles are correctly implemented. A key issue, still open, is related to the link that must be put in place to provide the DiD probabilistic success criteria through PSA insights. After an analysis of DiD evolution in time and DiD application to different industrial fields, this paper deals with the key issue, still open, relevant to the link that must be put in place to provide the DiD probabilistic success criteria through PSA insights. Practical proposals outlined point out the open questions.

Keywords

Defence in Depth, PSA, Risk Informed DiD

1. Introduction

The Defense in Depth (DiD) originated in military arena as a defensive strategy aimed

to protect the population while preserving the effectiveness of defense installations[1]. It deals with slowdown of the progression of an attack by using different successive layers, such as fortifications, troops, and field works, instead of concentrating all resources onto a single defensive line. The concept is currently applied to nuclear, chemical, ICT, transport, and others fields. The central idea of DiD is the implementation of multiple and independent levels of protection (or lines of defense) [1], to reduce the risk related to an accidental scenario so that, if one line were to fail, the subsequent would come into play in guaranteeing the required safety functions [2]. In other terms, the DiD main objective is to compensate for the failure of one or more defenses, ensuring that the risks[2] are kept acceptable.

2. DiD in Nuclear Fission

2.1. "Classical" DiD

Nuclear Power Plants (NPPs) present high energy density, ionizing radiations and the presence of a source term which can be mobilized in case of accident. Consequently, DiDhas fulfilled a primary role in promoting and implementing safety and security measures. The term was first introduced in the 1970s [3], although the concept was effective since the design of the first reactor realized by the Enrico Fermi's group in 1942 [4] [5].

Initially, the DiD was seen as a set of independent physical barriers (cladding, vessel, containment, …). To address the lack of data on barrier's performances and effectiveness, *i.e.* the uncertainties about the safety features, these barriers were conservatively designed (introducing safety margins) and implemented guaranteeing, as far as feasible, independency, diversity and functional redundancy, characterizing the DiD with a deterministic connotation. Although this deterministic connotation is not a peculiarity of DiD, for long time it has been the unique DiD interpretation key. With INSAG-10 [2], the physical barriers have been enveloped into the concept of "lines of defense", referred to all systems, structures and components, aimed at ensuring the safety functions and to prevent and/or mitigate radioactive releases. Progressively, the improvements of safety measures, the experiences from operations and the experience feedbacks, have led to a more comprehensive vision of the DiD; the latter started to constitute a holistic approach to address a set of deterministically selected accidents scenarios—or "plant conditions[3]"—named Design Basis Accidents (DBAs), chosen for the design and the implementation of the safety architecture. DBAs were considered as the representative accidents that could generate the most significant consequences. Nevertheless, the evo-

[1]Historians tell stories of a technique of "defense in depth" that was used in 2900 BCE to Hierakonpolis in Egypt, based on a defense involving parallel and independent walls to strengthen the protection of the city.

[2]In the field of industrial safety, "risk" is defined as the likelihood to see a hazard to be materialized in one or more scenarios associated with adverse consequences. The "level of risk" is then quantified by evaluating the probability of each scenario and the amplitude of the gravity of the corresponding consequences: Risk = Probability x Severity.

[3]The "plant condition" is defined as a specific Initiating Event associated to a given state of the installation (nominal operation, shutdown, maintenance, etc.). The possible abnormal behavior of the provisions which are implemented to manage the plant condition generates the incidental and accidental scenarios.

lution of the DiD concept kept the deterministic character. At the end of 1970s and following Three Mile Island accident [5], due to the consolidation of Probabilistic Risk/Safety Assessment (PSA) techniques, the attention was enlarged to those accidents, highly hypothetical but potentially catastrophic (severe), that could simultaneously jeopardize several levels of the DiD, leading the plant to plausible core melting scenarios. These accidents, defined "Beyond Design Basis Accidents" (BDBAs) or, recently, "Design Extension Conditions" (DEC), were not considered among the DBAs and, despite the possible contribution of the PSAs, were still selected deterministically[4] and primarily to prove the capability of the containment to withstand highly degraded plant conditions. Finally, DiD is today accepted worldwide by nuclear institutions and has evolved to a wide concept of an overall safety strategy[5]; nevertheless, there is still no full and harmonized understanding of the concept and its implementation. We can define "*Classical*" the DiD declined according to a deterministic approach, as far as the PSA was not completely developed and accepted. A NPP is considered safe if it can prevent, manage and mitigate a given set of DBAs [4] and DECs and the uncertainties correctly addressed. Concerning the uncertainties (*i.e.* those that exist and have been identified, the known unknowns-k_unks-, and those that exist and have not been identified, the unknown unknowns-unk_unks-), the approach used to include safety margins, redundancies, diversities, and ad-hoc[6] conservative assumptions [6]. It should be noted that the DiD is intimately based on evidence that barriers can fail (e.g. due to the presence of possible default or loadings larger than those considered). In order to implement the notion of "proportionate approach" [7], different categories are assigned to incidental (DBAs) and accidental (DBAs and DECs) events and related plant conditions, according to different values for their frequency of occurrence[7]. Simultaneously, acceptability criteria are defined as a function of these frequencies (*i.e.* the Farmer curve approach). For these reasons, this "*Classical*" DiD could be seen as a "*zero revision*" of the (non-null) probabilistic contribution: probabilistic aspects and uncertainties are taken into account, but through a conservative approach.

2.2. DiD According to Some Institutions

The state of the art of the DiD in the nuclear field can be fixed through works carried out by three of the main nuclear institutions/regulatory bodies: the International Atomic Energy Agency (IAEA), the U.S. Nuclear Regulatory Commission (NRC), and the Western European Nuclear Regulators Association (WENRA). Despite the fact that no univocal definitions are available, interpretations and insights from these bodies can help to fix the concept.

[4]*i.e.* not necessarily with reference to their plausible character.

[5]Cf. Liebmann (1996): "*The concept of defense in depth is not only a guide for the review of a particular technical solution as, for example, a set of singular barriers, but a method of reasoning and a general framework to examine more fully the entire facility, both for its design and for its analysis*"; Libmann J. Eléments de sûreténucléaire. 1 janvier 1996.

[6]Conservative approach for the DBA and Best estimated approach, coupled with the assessment of uncertainties, for the DEC.

[7]It also recognizes the possibility to relax some design constraints for "rare" events, accepting the loss of the system operability but guarantying the required safety function(s).

2.2.1. IAEA

One of the IAEA main missions is to promote safety in nuclear industry, by providing objectives and high standard requirements. The current definition of the DiD, stated within the IAEA Safety Fundamentals—N˚ SF-1 [8] is: "The primary means of preventing and mitigating the consequences of accidents is "Defense in Depth". DiD 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 environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, DiD ensures that no single technical, human or organizational failure could lead to harmful effects, and that combinations of failures that could give rise to significant harmful effects are very low probabilities. The independence effectiveness of the different levels of defense is a necessary element of defense in depth". INSAG, a group supported by IAEA, clarifies some relevant issues of the DiD (see INSAG-3 and INSAG-12 [1]), introducing the concept of lines of defense: "All safety activities, whether organizational, behavioural equipment related, are subject to layers of overlapping provisions, so that if a failure should occur it would be compensated for or corrected without causing harm to individuals or the public at large". INSAG-10 [2] structures the DiD main goals (prevention, protection, and mitigation) in five levels with the scope of reducing the risk of radioactive release. The strategy is the following: "should one level fail, the subsequent comes into play. The objective of the first level of protection is the prevention of abnormal operation and system failures. If the first level fails, abnormal operation is controlled or failures are detected by the second level of protection. Should the second level fail, the third ensures that safety functions are further performed by activating specific safety systems and other safety features. Should the third level fail, the fourth level limits accident progression through accident management, so as to prevent or mitigate severe accident conditions with external release of radioactive materials. The last objective (fifth level of protection) is the mitigation of the radiological consequences of significant external releases through the off-site emergency response". The DiD strategy objectives are: "to compensate for potential human and components failures, to maintain the effectiveness of the barriers by adverting 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" [2].

2.2.2. NRC

The NRC is responsible for licensing U.S. NPPs and supervising their safety. Nuclear safety regulations are grouped into the number 10 of the American Code of Federal Regulations (CFR). The implementation and maintaining of the DiD is one of the focal points of these regulations. A current definition for DiD states: "Defense-in-depth is an element of the NRC's Safety Philosophy that employs successive compensatory measures to prevent accidents or lessen the effects of damage if a malfunction or accident occurs at a nuclear facility. The NRC's Safety Philosophy ensures that the public is adequately protected and that emergency plans surrounding a nuclear facility are well

conceived and will work. Moreover, the philosophy ensures that safety will not be wholly dependent on any single element of the design, construction, maintenance, or operation of a nuclear facility" [9]. Recently, NRC implicitly recognized the need for further improvements: "Whether used explicitly, as for power reactors, or implicitly, as for materials programs, the concept of defense in depth has served the NRC and the regulated industries well and continues to be valuable today. However, it is not used consistently, and there is no guidance on how much defense-in-depth is sufficient" [10].

2.2.3. WENRA

WENRA promotes nuclear safety harmonization between Western European Regulators [11]. WENRA has recognized the fundamental role of the DiD, underling the necessity of continuously adapt it to new generations of NPPs. Reference [3] states that: "the DiD concept should be strengthened in all its relevant principles" and, discussing the objective " Independence between all levels of defence-in-depth", details the concept: "Enhancing the effectiveness of the independence between all levels of defense-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately as addressed in the previous three objectives), to provide as far as reasonably achievable an overall reinforcement of defense-in-depth". In 2013 WENRA [3] proposed to reformulate the DiD interpretation by correlating, in a bi-univocal manner, the considered plant conditions (DBA & DEC) and the different DiD levels. Moreover, WENRA extended the DiD application to a holistic safety strategy, stating that: "It also shall be ensured that the DiD capabilities intended in the design are reflected in the as-built and as-operated plant and are maintained throughout the plant life time" [3]. One can point out that this approach is implicitly endorsed by the Generation IV International Forum (GIF) principle which, while considering the DiD as the foundations for the safety architecture, preconizes that safety must "built-in" rather than "added-on" [12].

2.3. Risk Informed DiD

After the publication of NUREG-75/014 (WASH-1400) in 1975, a "Risk informed" approach for the design and the assessment took the place of the "*Classical*" DiD, with the objective of integrating insights from the former (**Figure 1**).

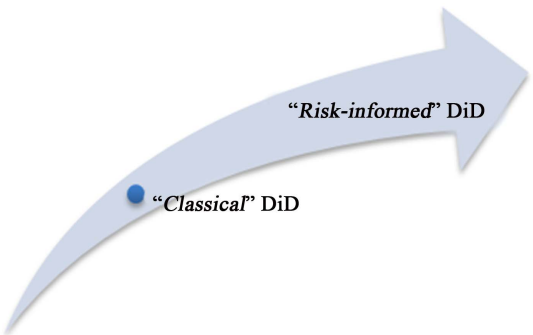

Figure 1. "Classical" and "evolutionary" DiD.

The "Classical" (elsewhere "structuralist [13]") DiD asserts that DiD principles shall be embodied in the structure of regulations and consequently in the design of facilities. The design requirements come from the repetitive question: "what if this barrier or safety feature fails?". In some instances, it has led to excessive regulatory burden. Furthermore, the lack of an integrated view of the systems has resulted in some significant accident sequences not identified until PSA development. The "Risk-informed" (elsewhere "rationalist [13]") DiD asserts that DiD is the aggregate of provisions made to compensate for uncertainty and incompleteness in our knowledge of accident initiation and progression. It requires to quantify risk and estimate uncertainty through PSA. Following this logic, attempts have been made to go until the fully quantitative probabilistic approach (*i.e.* risk based), which, nevertheless, due to the intrinsic PSA limits (*i.e.* the existence of uncertainties), has not been adopted. The actual conclusion is that, because of the uncertainties and the awareness of possible lack of exhaustiveness, the deterministic approach, with safety margins and other conservative assumptions, shall be kept as foundation, even though at a higher level, to allow covering the various sets of residual *k_unks* and *unk_unks*. The necessity of integrating the "*Classical*" DiD with the PSA is recognized in NUREG-2150 [10] as follows: "Risk assessments provide valuable and realistic insights into potential exposure scenarios. In combination with other technical analyses, risk assessment caninform decisions about appropriate defense-in-depth measures", and "the characterization of DiD could be extended for power reactors to be more specific and to reflect the availability of quantitative methods (probabilistic risk assessment)".Coherently with the indication of INSAG-25 [14], deterministic and probabilistic approaches start to support each other in an iterative process, known as Integrated Risk-Informed Decision-Making (IRIDM), with the final aim of best implementing the DiD into the NPPs and decide how much DiD is sufficient. They became inputs to be firstly weighted and then, iteratively, to be elaborated to reach the most reliable and balanced decision, in terms of safety. In this logic, with regard to IRIDM, INSAG-25 [14], citing the IAEA GSR Part 4 [15], states as follows: "The result of the safety assessment have to be used to make decisions in an integrated, risk informed approach, by means of which the results and insights from the deterministic and probabilistic assessment and any other requirements are combined in making decisions on safety matters in relation to the facility or activity". The objective is fair, but the implementation of pertinent solutions is difficult for the designer and needs technical guidance. This has been one of the challenges tackled by GIF, through the definition of the safety philosophy and the development of specific design methodologies for future NPPs.

2.4. Generation IV and DiD

The design of GIF system shall comply with the DiD and its principles in order to achieve safety robustness, thereby helping to ensure that nuclear systems do not exhibit any particularly dominant risky [16]. To help designers to correctly implement the DiD, the GIF developed the Integrated Safety Assessment Methodology (ISAM).

Through a set of complementary tools, ISAM allows implementing deterministic and probabilistic approaches [16]. The methodology consists of five distinct analytical tools, each of which can be used to answer specific kinds of safety-related questions, with different degrees of detail, and at different stages of design (**Figure 2**). ISAM is integrated, as evidenced by the fact that the results of each tool support or relate to inputs or outputs of other tools. **Figure 2** [16] details the overall task flow of the ISAM and indicates which tools are intended for use in each phase of GIF system development.

A pillar of the ISAM methodology is the notion of safety architecture, based on that of Line of Protection (LOP)[8]: for each initiating event and plant condition, and for each safety function, the representation of the safety architecture shall allow the designer to clearly identify, for each of the DiD levels, the set of provisions which, together, will achieve the requested mission, *i.e.* to meet the corresponding safety objectives. For a given level of the DiD, the LOP assembles the set of provisions and, for the initiator and safety function under consideration, materializes the content of the DiD level. Two ISAM tools are more specifically related to safety architecture and DiD [16]:

- *The Qualitative Safety Features Review (QSR)*: it is structured following the DiD levels, provides a systematic mean of ensuring and documenting that the evolving GIF concept of design, incorporates the desirable safety attributes and characteristics.

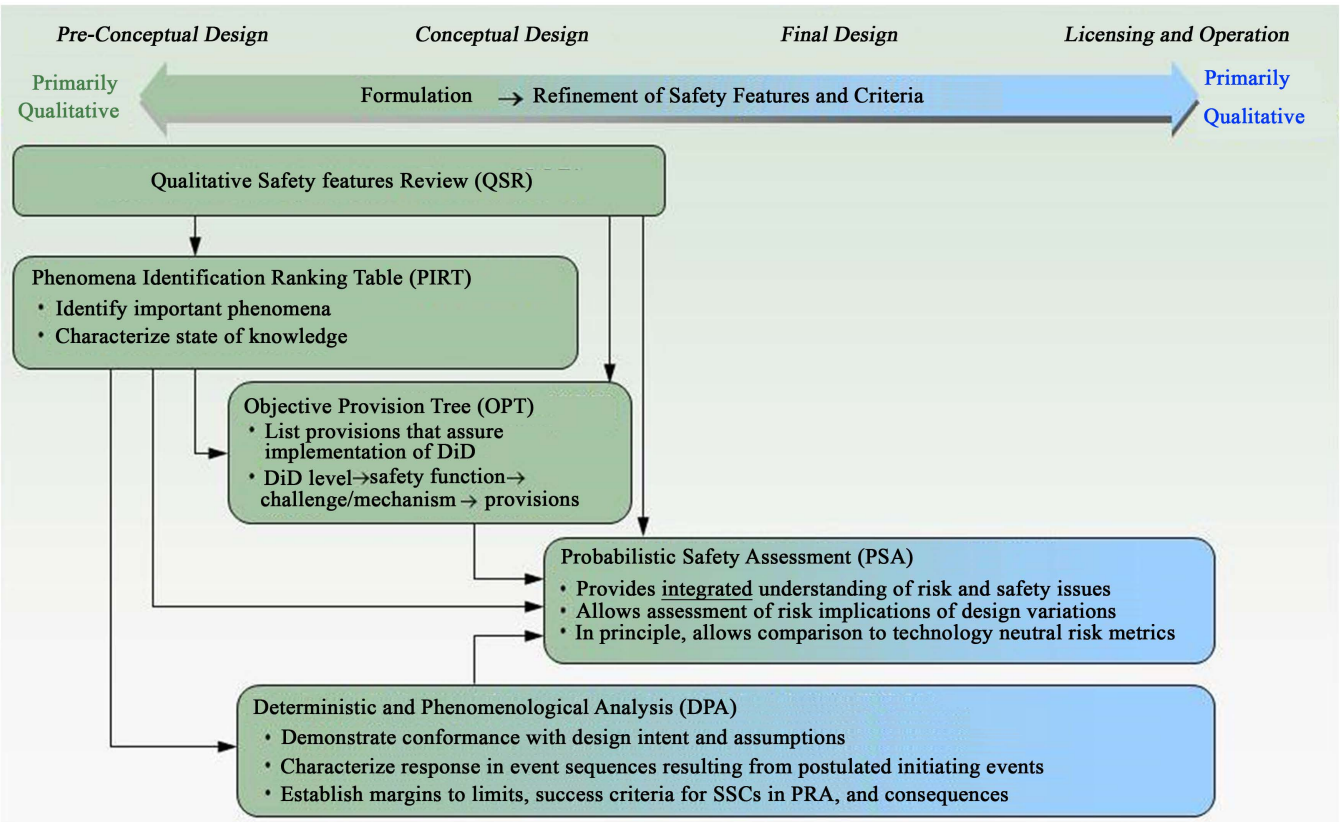

Figure 2. Proposed GIF Integrated Safety assessment Methodology (ISAM) task flow.

[8]The notion is consistent with that of "layers of provisions" discussed by the IAEA safety standards (e.g. IAEA-Safety of Nuclear Power Plants: Design; No. SSR-2/1 Specific Safety Requirements; Vienna 2012) when addressing the concept of DiD and the content of DiD levels.

The Objective Provision Tree (OPT, **Figure 3**, [17]): it can be extremely useful in focusing and structure the analyst's identification and understanding of initiators and abnormal conditions, accident phenomenology, success criteria, and related issues. The final OPT purpose is to identify, motivate and document the LOP provisions; as such, the OPT can be considered as an innovative mean to represent the whole safety architecture and an essential support to help proving the correct implementation of the DiD.

The matching of the objective formulated by INSAG 25 for making a decision through an integrated risk informed approach needs the harmonization in understanding the content of the DiD and its implementation. As such, the use of risk space, as a means to merge the deterministic and probabilistic approaches, appears as a key step, especially concerning the DiD evolution for GIF systems. ISAM provides the tools which will help the designer to construct a DiD architectures, and the analyst to assess the pertinence of the solutions.

3. Did in Nuclear Fusion

Two fusion machines-TFTR and JET, both based on Tokamak design[9]-have been involved licensing procedures. Currently, the Deuterium-Tritium machine, ITER, is under construction in France. Even if the ITER licensing represents the first procedure for a fusion facility managing a significant Tritium inventory, the demonstration of safety

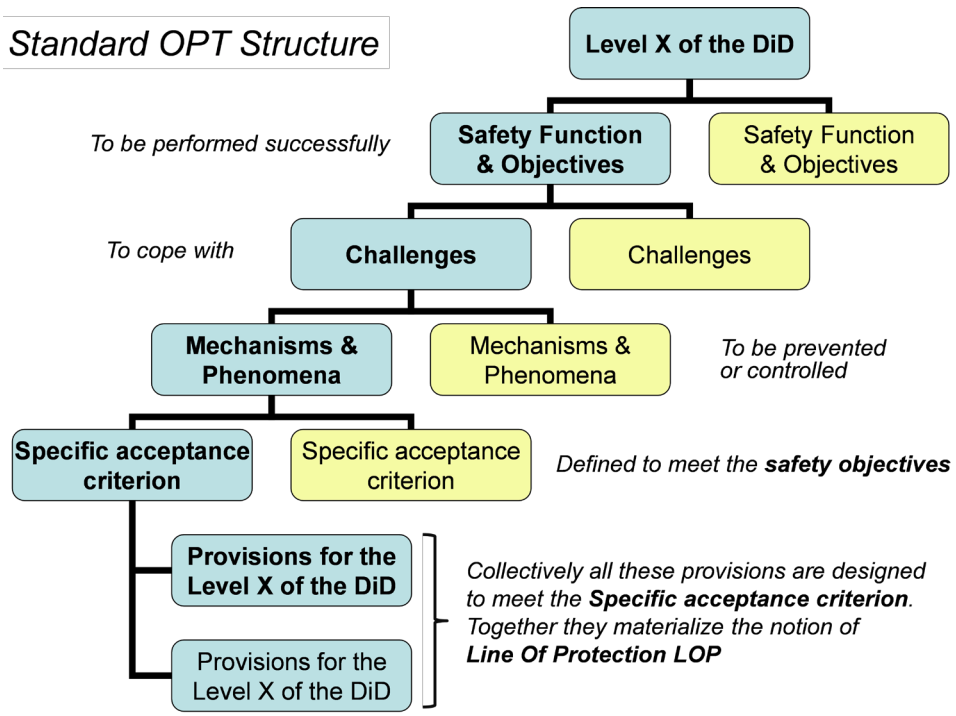

Figure 3. Objective Provision Tree (OPT): Standard structure.

[9]The leading designs of facilities for controlled-fusion research use magnetic or inertial confinement. Magnetic confinement attempts to create the conditions needed for fusion energy production by using the electrical conductivity of plasma to contain it by magnetic fields.

of fusion facilities is supported by experiences made in nuclear fission. Compared to fission, fusion is believed to have favorable safety and environmental characteristics [18]. The three basic safety functions of fission plants can be applied: the first two—control of the nuclear process and core heat removal—have minor significance because of limited potential increase of power and lower power density; the third basic safety function-confinement of the radioactive materials-is the most important one, and asks for a reliable confinement system. ITER shall be licensed as a Basic Nuclear Installation. Licensing submissions to the French nuclear safety authorities shall respect in particular the *Arrêté du* 7 *février* 2012 *fixant les règlesgénérales relatives aux installations nucléaires de base* [7]. According to the *Arrêté* 2012, DiD is among the key principles to guide both the design and the independent review and assessment. ITER aims at incorporating the DiD approach since the very beginning of its conceptual design. The safety architecture is based on overlapping levels of safety provisions so that a failure at one level would be compensated by another level with other provisions. Successive lines of defense, functionally redundant, are available to achieve the required safety functions: for the confinement function, they consist of multiple static barriers (e.g. Vacuum Vessel) and dynamic confinement system (e.g. for Vacuum vessel penetrations); for the heat removal functions, they consist of multiple paths and systems provided for normal operation, independent redundant cooling loops having a natural circulation capability, thermal radiation to the magnet structures and cryostat and ultimately to the environment, and possibility of assisting ultimate decay heat transfer by gas introduction. Coherently with the DiD principles, the independent layers comprise [19]:

- the use of conservative design practices, the application of quality assurance and the promotion of a positive safety culture;
- provisions for the control of abnormal operation and the detection of failures that could lead to damage to confinement barriers;
- safety systems and protective systems;
- accident management provisions.

Safety analyses aim at demonstrating that the foreseen provisions for implementing the DID levels allow keeping the facility below the safety limits during normal and incidental conditions; in this framework, they provide evidence of the capability of the adopted confinements to avoid dispersion of dangerous materials[10] [20]. The international fusion safety practice, adopted in ITER, is to discriminate between DBA and BDBA[11]; safety requirements include the prevention of accidents and the mitigation of their consequences, the need to avoid public evacuation in any accident, the protection of the public and the environment against radiological hazards, the protection of the site workers against radiation exposure [21]. Parametric studies are used to investigate the ultimate safety

[10]Environmental hazards come from different sources: neutronic fluxes during plasma operation; radioactive products, including tritium, activated materials and dusts, activated corrosion products and gas; chemical materials, toxic and cryogenic ones, such as beryllium, hydrogen, ozone, inert gas, insulator gas, ….

[11]A sequence of events is a "beyond-design- basis" accidents either if the expected frequency of the initiating event is below a threshold (10-6 /yr) or if an event considered within design basis is further degraded by assuming a further independent aggravating failure of a component or system needed in the response to the event.

margins in BDBA situations and to demonstrate the absence of cliff-edge effects [19].

The safety assessment of ITER is based on a set of accidental sequences, conservatively selected on a deterministic basis. Techniques for deterministic safety analysis have been used to determine a fully representative set of reference events, just supplemented by techniques of probabilistic assessment to check its comprehensiveness. Each sequence starts with a postulated initiating event, adds all consequential failures, up to the release into the environment. Consistently with DiD, the rationale for the selection of reference events consists firstly of the identification of every radiological source and its confinement barriers; failure of one or several of these barriers may then be presumed and a scenario defined; consequences are evaluated and compared with safety objectives [20]. The postulated events and sequences are categorized according to expectation of occurrence. Loading conditions on ITER (mechanical) components are categorized through the same categories. Acceptable damages under incidental conditions are specified according to the "safety importance" of components. Up to now, the methodological approach adopted for the ITER safety demonstration has been substantially a "Classical" DiD, although probabilistic risk assessment could be required by regulators, and for future fusion reactors.

4. DiD in Other Sectors

4.1. Chemical Industry

The safety approach for chemical industry is characterized by the scope of interrupting the escalation of initiating events into hazardous conditions, largely in accordance with the nuclear one. In the USA, the Occupational Safety and Health Administration and the Environment Protection Agency have established the Process Safety Management (Title 29 of CFR Section 1910.119), and the Risk Management Program (RMP) (Title 40 CFR Part 68) regulations, respectively, which provide the requirements to insure compliance and acceptability of highly hazardous chemical processes. DiD is not mentioned explicitly, but DiD philosophy is clearly observed throughout the implementation of *lines of defense* (or *layers of defense*) that are aimed to reduce the risk associated with major accidents and, therefore, prevent their likelihoods of occurrences and/or mitigate their consequences. The concept of *lines of defense* was introduced in 1993 by the American Institute of Chemical Engineers (AIChe) [21]. According to AIChe, three lines of defense should be implemented[12] with the main functions of: *Prevention, Protection, Mitigation.* Each line is made of specifics *protection layers* (or *safeguards*), intended as [21]: "any device, system or action that would likely interrupt the chain of events following an initiating event". The nature of the lines covers physical, human, operational, and organizational elements. An important remark concerns the notion of *IPL*: "a device, system, or action that is capable of preventing a scenario from proceeding to the undesired consequences regardless of the initiating event or the action of any other protection layer associated with the scenario" [21]. To be considered an IPL, a protection layer must meet certain requirements, *i.e.* specificity, independence, depen-

[12]Despite the difference in number-three lines for the chemical plants versus the five lines requested for the NPP-, one can consider that the basic DiD principle are exactly the same.

dability, and auditability [21]. These requirements are embodied in the Layers of Protection Analysis (LOPA)[13].

The LOPA methodology is in compliance with the PSM (and the RMP), and promoted with the DiD principle. It has been developed from the concept of lines of defense, with the aim of:

- Determine if a protection layer meets the IPL requirements,
- Estimate the risk of severe accidents,
- Assess the adequacy in terms of physical performances and reliability of the IPLs to adequately reduce the risk of an accident [22].

The LOPA comes systematically in conjunction with an initial qualitative analysis—the Preliminary Hazard Analysis—and can be followed by a Quantitative Risk Analysis (QRA). For that reason, it is considered a semi-quantitative method, obtaining risk values that—nevertheless—may be orders of magnitude larger than the QRA ones[14]. The way the LOPA addresses the IPLs represents an implicit estimation of the DiD effectiveness. A Probability Failure on Demand (PFD) is allocated to each IPL, accounting for its reliability to perform a specific function on demand. The PFD is a pure number varying from 0 to 1, with the smaller the number the larger the Risk Reduction Factor of the undesired consequence [23]. Thereby, the international standard of rules IEC 61508 [24] has established a link between the PFD and the Safety Integrity Level (SIL[15]).

4.2. ICT

Due to the recent development of the Information and Communication Technology (ICT), information security has become extremely important. Security measures, criteria, and strategies have been established with the aim of keeping the system assets (information and data): Confidential, Intact, and Available (*i.e.* the CIA Triad), and to reduce the risk of being exposed to threats[16]. ICT security has given a major attention to those threats that can affect the system from inside, *i.e.* the technical threats, such as malware, improper system operations, etc. This is due to the fact that the internal threats represent the most rapid and easiest way of causing harms and that they are characterized by a high degree of uncertainty (or "*element of surprise*" [25]), since more sophisticated forms are in evolution. This reason has highlighted the need to develop a security architecture, with several DiD levels, focused on:

[13]The analogies between the LOP notion, as introduced by the GIF/RSWG, and the LOPA methodology, as discussed here, deserve deep analysis.

[14]The LOPA analysis generates results that are "orders of magnitude" more important than those that are expected from the quantitative analysis, *i.e.* with a conservatism that might seem excessive. Nevertheless, the LOPA is very simple and easy to apply and this is why it generates considerable interest, because the quantitative risk analysis, except in rare cases, can be excessively expensive.

[15]The SIL is an integer (varying from a minimum of 1 to a maximum of 4) which expresses the level of RRF provided by an IPL.

[16]In the ICT, a threat is considered as an attack that has the potential to cause harms to a system asset, jeopardizing its productivity. Generally, four types of threats exist: physical, environmental, site-related, and technical.

[17]Vulnerability is a system weakness that can be exploited by threats to cause harms to the asset [26].

- Exploring systematically the system vulnerabilities[17],
- Gathering the major number of information regarding threats and potential attackers, reducing the element of surprise,
- Identifying protection and response measures.

The implementation of multiple levels of defense blends in well with the original DiD approach, as conceptualized in the military arena, provided that the notions of threats, system vulnerabilities, and assets to protect are thoroughly understood. The ICT security relies upon the whole security architecture system. According to the DiD concept in the nuclear and chemical industries, at least three main levels or functions are required to successfully implement a security architecture within the ICT [25]: *Prevention*[18]*-Detection, Protection, Response.* It should be noted that the final mitigation level of the DiD, as intended in the nuclear and chemical industries, is now characterized more with a function of "response", which should provide the adequate countermeasures in the less time possible, following a sort of dynamism principle [25]. Each level of the DiD shall be provided with specific *security controls*, dealing at the same time with all the types of threats, and addressing, in a balanced way, the following principal elements [26] considered as possible sources for threats: *People, Technology, Process.* A security control should be independent from any type of considered threats, and simultaneously should provide—as far as feasible[19]—protection against threats that are unknown. Furthermore, a greater emphasis is given to their dynamic nature and the need of cooperating [25]. One of the first insights the ICT has assimilated from nuclear safety, is DiD as a link between the deterministic approach and the PSA.

Implementing the DiD means firstly carry out a risk analysis, with the aim of:

- Classifying the system assets (data and information) according to their importance,
- Identifying and understanding the threats and evaluating their severities,
- Establishing a degree of system vulnerability, as a function of the associated risk, calculated for each threat-asset pair.

The number, the quality and the reliability of the levels implemented will be in compliance with the value of risk calculated and the allowable degree of uncertainty. It should be noticed that, if the threats identification is too imprecise (and the element of surprise prevalent), a greater worth will be given to the deterministic approach, respect to PSA.

4.3. Transport

As a result of the recent rise of constraints and potential consequences influencing a transport system, the French public transport operator, *Régie Autonomes des Transports Parisiens (RATP)*, which has always been reliable in managing safety and security activities, has decided to improve its operations by implementing a DiD approach. RATP considers the DiD as: "the set of provisions and means organized, contributing to the control of the potential final effects susceptible to be created by all forms of ag-

[18]The notion of "prevention", while non-explicit within the Ref. [25] is likely implicitly considered under the term "detection".

[19]*i.e.* looking for exhaustiveness.

gressions on sensitive elements", and the: "global and dynamic defense, implementing several coordinates lines of defense, against internal and external aggressions, potential or proven—and that on all the cycle of life of the transport system" [27]. The DiD shall be accomplished by implementing successive and autonomous lines of defense. According to the previous sectors, three main functions are required: *Prevention, Protection, Safeguard-Mitigation.* Each line gathers several elements of defense (or barriers) and addresses the following elements, with the aim of reduce the risk, ensuring it is kept acceptable or, in the worst cases, tolerated (Figure 4)[20]:

- The attacker (or the threat),
- The aggressive flow (generated by the attack),
- The sensitive element (or the system vulnerability).

5. Discussion: What Is Possible to Learn

5.1. DiD and PSA Integration

5.1.1. From DiD Perspective

Figure 5 shows a qualitative depiction of the DiD trajectory evolution along the nuclear history, taking account for the different contributions coming from the deterministic and probabilistic approaches. The upper-left corner of the picture represents a pure-

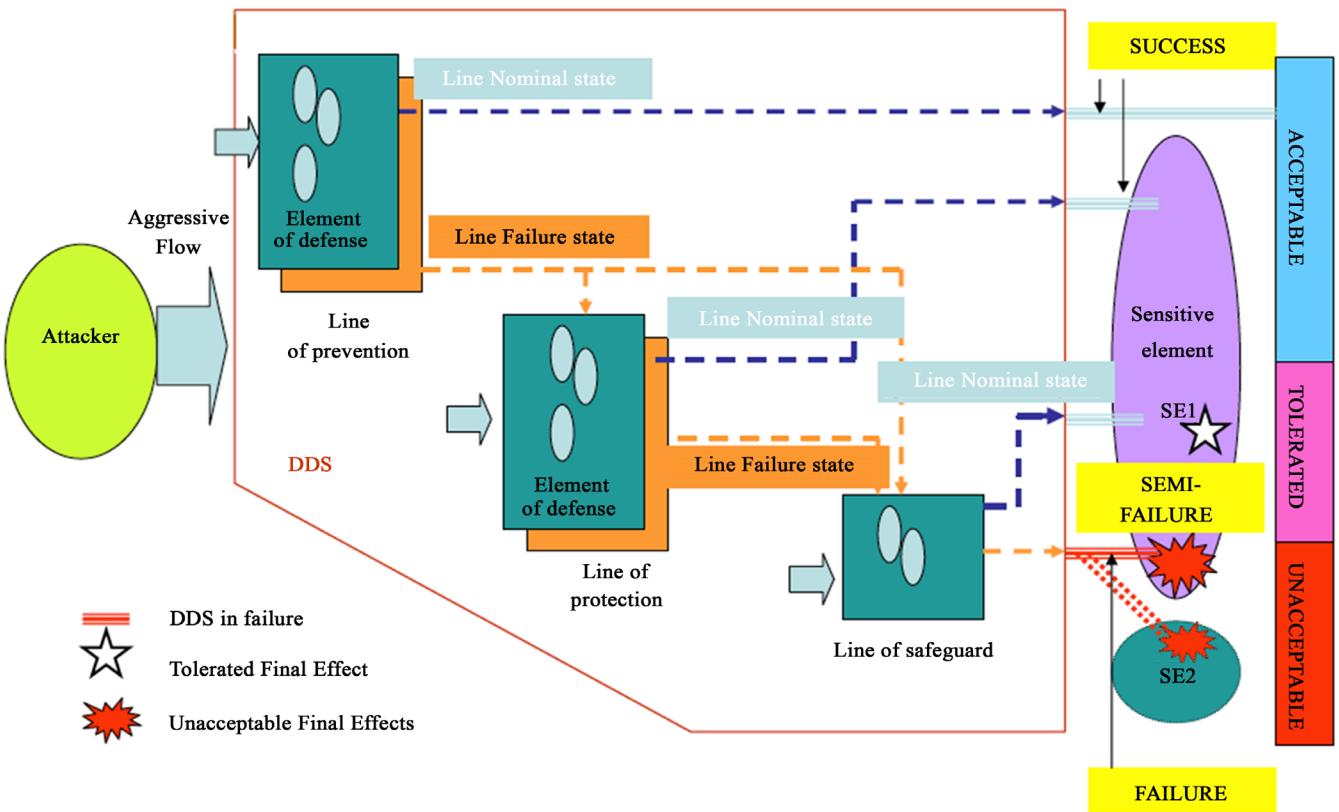

Figure 4. Defense in Depth System (DDS), RATP.

[20]In this figure the possible bypass of an "element of defense" (e.g. the "line failure state" (the dotted orange line) that goes through the "line of protection") should be clarified.

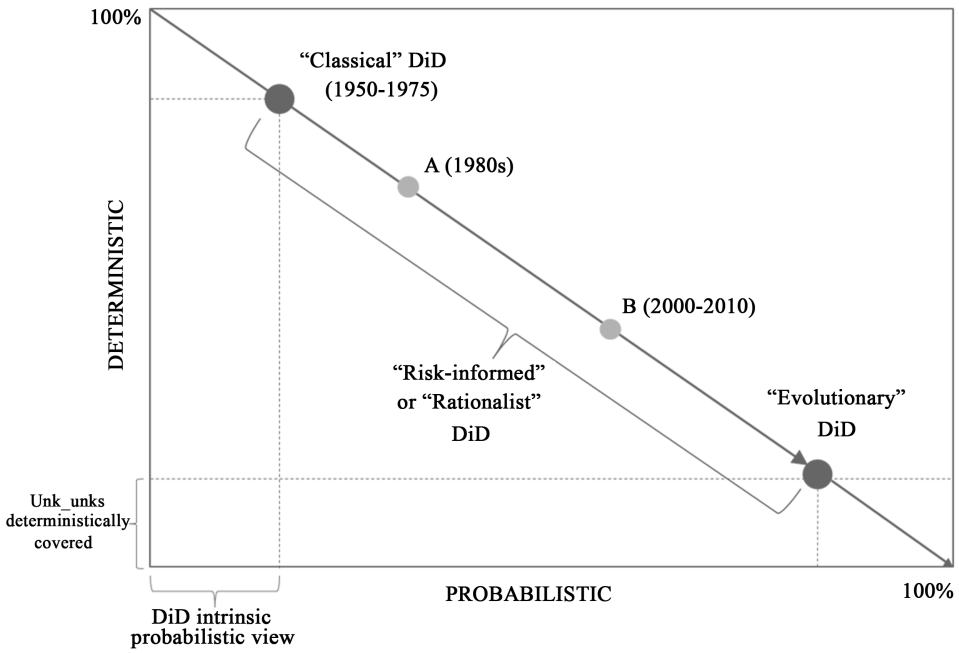

Figure 5. Trajectory of DiD evolution.

deterministic approach (0% probabilistic, 100% deterministic), which is substantially overcome from the adoption of DiD principles; "Classical" DiD does not coincide with the upper-left corner because of a non-null intrinsic contribution of the probabilistic approach. Point A represents a first "improvement" of the "Classical" DiD with further probabilistic insights (approximately in 1980s). Point B shows a further development of probabilistic approach (2000-2010), aimed at assessing uncertainty on the estimations, recognizing the existence of k-unks and unk-unks. Assuming that the increasing contribution of probabilistic insights will allow reducing the influence of the *k_unks* uncertainties, the asymptotic limit beyond which the deterministic approach "only" covers the residual *unk_unks* uncertainties (e.g. the awareness of possible lack of exhaustiveness) is identified as "Evolutionary" DiD. The lower-right corner of the picture represents the risk-based approach (100% probabilistic, 0% deterministic), and cannot be reached in any way.

It is apparent that the two points of view—deterministic and probabilistic—are complementary and not alternative.

5.1.2. From PSA Perspective

The role of probabilistic studies in Risk informed DiD is twofold: on one hand there is the possibility to take into account the reliability of the safety architecture's components; on the other hand, there is the use of a probabilistic approach to better manage the uncertainties. Starting from the frequency of occurrence of initiating events, the taking into account of the component reliability allows a better assessment of the probability associated with the sequences that, in turn, ensures proportionate approach to the associated risk's treatment. With regard to uncertainties, probability distribu-

tions are used to characterize them on each input variable; sampling techniques are used to propagate these uncertainties. The estimation of the uncertainties provides information to rank components according to the model output sensitivity and then to optimize the safety performances, avoiding excesses in the sizing of the safety provisions. Looking for a "risk informed" approach, the concept of risk[21] can be used to make the link between deterministic and probabilistic analyses. Several elements contribute to the integration of the deterministic approach with the notion of risk [28]-[31]. First of all the Farmer's curve which provides a tool to identify what is allowable and what is not. The consideration of this curve allows addressing the full set of possible plant conditions duly categorized as a function of their risk[22].

Secondly, for a given plant condition there is the need to:

- Define the safety objectives, i.e. to establish quantitative criteria concerning risk acceptability (achieved positioning the Farmer curve within the risk space).
- Quantify the requested efficiency of the different DiD levels versus the potential risk generated by the plant condition. It has to be stressed that this step is directly related to the rules for the component classifications.
- Define and assess how much DiD is enough.
- Deal with uncertainties.
- The correct implementation of these elements can also help guaranteeing two complementary criteria:

The exhaustiveness of the analysis, which mainly deals with the need to correctly address the rare sequences events identification;

- The balance between the level of risk and the efforts deployed to guarantee the requested safety through a cost benefit analysis[23].

Coherently with ISAM methodology, the requirements singularly applicable to each provision and collectively to the entire LOP, can be deduced with the use of the Farmer Curve (**Figure 6**) by placing different levels of DiD on the figure. It can be pointed out that, while leaving open some details concerning the exact positioning[24], the principle is perfectly consistent with the guidance available from WENRA [3] and NRC [10].

As qualitatively indicated in **Figure 7**, success criteria can be derived both in terms of physical performances ($A_{failure} \Rightarrow B_{success}$) and reliability ($A_{failure} \Rightarrow C_{success}$); these success criteria are essential to size the LOP's provisions which are associated with the corresponding level of DiD.

5.2. DiD and Probabilistic Studies: A Challenge for the Designer and the Analyst

Within the previous sections the evolution of the DiD and the shifting from a deterministic toward a risk informed approach, are discussed for different fields. For all these

[21]cf. Foot note N˚2.

[22]The set include both the DBA (i.e. the anticipated operational occurrences (AOO), the incidents and accidents), as well as the hypothetical Design Extension Conditions (DEC).

[23]The implementation of the ALARA principle remains mandatory.

[24]E.g. the place for the 1st level of the DiD which differs from the proposal made by WENRA and NRC and that should be discussed.

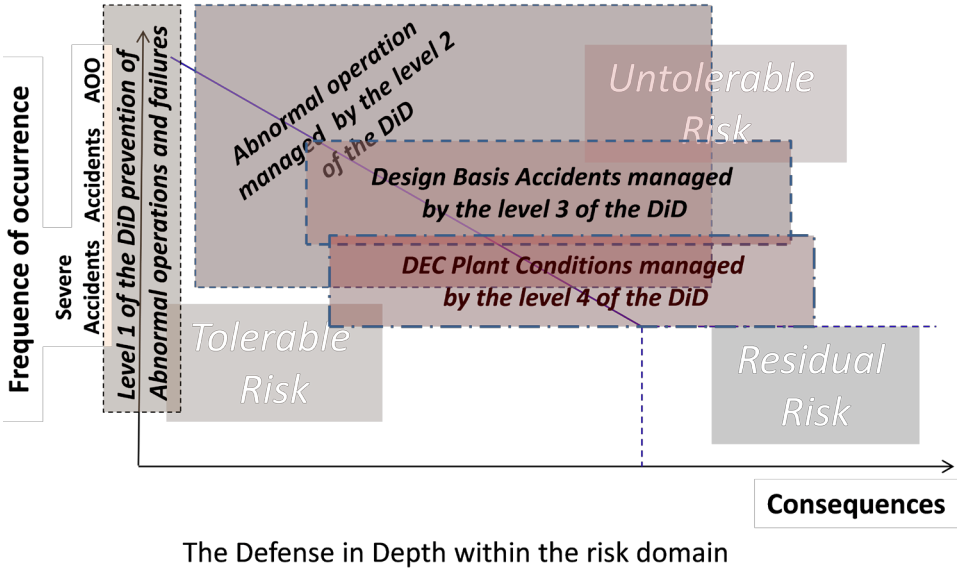

Figure 6. The DiD levels within the risk space (farmer curve).

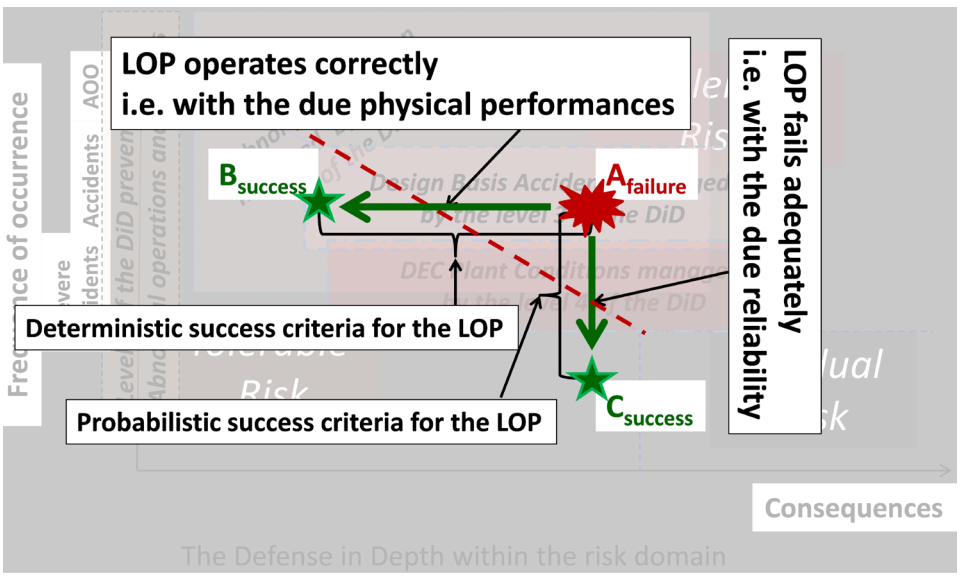

Figure 7. LOP behavior: deterministic and probabilistic success criteria.

fields, a common goal is to achieve a robust design with respect to possible threats and hazards, coupled with a robust safety demonstration. As already discussed, DiD and PSA are essential elements of this effort; below are summarized indications and guidelines to improve their contribution and to identify the needed research and development effort.

5.2.1. Design and Demonstration Robustness: The Role of DiD and PSA

In terms of DiD, the guidelines that can be adopted for a robust design approach, address the elements that contribute significantly to the strength of the safety architecture, *i.e.*: the consideration, as comprehensive as practicable, of accidental situations; the

routine coverage of physical phenomena that may occur; the demonstration of the envelope character of situations selected for the design; the control of uncertainties; the research of potential threshold effects and identification of margins versus these thresholds. On the other side, to ensure the robustness of the demonstration, the designer must be able to show that the specific risks of the technology are controlled by an adequate level of knowledge, be able to identify and justify the positioning of the provisions implemented for each level of the DiD, to justify their performance and reliability, and ensure that the principles of independence, progressiveness, and balance between the different levels are met. In particular the level of coverage and the quality of modeling for the degraded situations, participate to the robustness of the demonstration. In the above context, the use of PSA allows modeling and allocating a probability to all plausible sequences to which the facility could face. The completion of these studies allows to check the list of initiators and their categorization, to broaden the base of deterministic design for the implemented provisions, to verify the progressive and balanced design of the safety of the facility, to review the list of complex operation conditions, to bring a judgment on the probabilistic evaluation of hazards, to quantify where appropriate the probability for consequences, to justify the program of preventive maintenance and finally, to assess the overall system safety level. That said, the PSA, like any modeling, involve uncertainties, particularly on degraded operating modes, and the estimated reliability rates that are integrated into calculations. This leads to temper the decisions taken on the basis of their results.

5.2.2. Role of PSA in the Design and Evaluation of New Facilities

In the specific case of new facilities, probabilistic studies will be conducted and enriched by successive stages, as the development of these facilities. In the course of this development process, "on-line" PSA bring in an aid in the design of safety provisions (comparison of technical solutions, impacts of redundancy, diversification and separation), in the evaluation of the gain provided by specific provisions (e.g. for the prevention of severe accidents), for the demonstration that sequences that may lead to intolerable consequences are "practically eliminated", and finally for the comparison of the level of safety compared to that of operating facilities or other facilities under development. These studies must be improved as the data acquisition progresses in the following areas: the list of plausible initiating events; the uncertainty about the reliability data on the common cause failures, the human reliability and the contribution of support systems; the list of internal and external hazards that must be considered with the development of appropriate methods.

5.2.3. R & D Needs for the Analytical Methods

In support of the issues mentioned above, methods and tools to be developed or under development include:

- Method of identification and classification of the operating conditions,
- Method of identifying and analyzing threats and hazards and their consequences,
- Method for the description of the safety architecture to address all the components

of the safety architecture,
- Method of identification and classification of lines of protection,
- Method to quantify the provisions reliability, incorporating the management of attached uncertainties,
- Methods of analysis and quantification of the human factor and hardware and software reliability,
- Methods of assessing radiological consequences (for nuclear installations).

6. Conclusion

Concerning the current practices for the DiD implementation and the rationale for its evolution, there is a shared recognition that the reinforcement of DiD is the key to improve the safety of future installations for all types of technologies and industries. Specific R&D needs are identified. They essentially address methods to represent and assess the actual practical DiD implementation, contributing to the requested reinforcement. Within this context, the PSA results play a key role in supporting both the robustness of the design and of the safety through a thorough support for the verification that the DiD principles, such as the efficiency, independence, the progressiveness of the different DiD levels, are correctly implemented and that the balance of the installation's safety is adequate. Nevertheless, one should point out that, if the principles for the interpretation of the role of DiD and PSA are well defined, discrepancies exist concerning the details for their practical implementation. A key open issue is the link that must be put in place to provide the DiD probabilistic success criteria through PSA insights. Practical proposals come, for example, from the GIF safety activities; starting from insights collected within some IAEA standards and WENRA or NRC documents, they are founded on the use of the risk space as integrator between DiD and PSA. Nevertheless, while widely discussed and accepted, they have not yet been formally agreed by the different communities.

References

[1] International Nuclear Safety Advisory Group (1999) Basic Safety Principles for Nuclear Power Plants. Safety Series No. 75-INSAG-3, Rev. 1 INSAG-12, International Nuclear Safety Advisory Group, Vienna.

[2] International Nuclear Safety Advisory Group (1996) Defense in Depth in Nuclear Safety. INSAG-10, International Nuclear Safety Advisory Group, Vienna.

[3] Western European Nuclear Regulators Association (2013) Safety of New NPP Designs.

[4] Modarres, M. and Kim, I.S. (2010) Deterministic and Probabilistic Safety Analysis. In: Cacuci, D.G., Eds., *Handbook of Nuclear Engineering*, Springer, Berlin, 1739-1812. http://dx.doi.org/10.1007/978-0-387-98149-9_15

[5] Keller, W. and Modarres, M. (2004) A Historical Overview of Probabilistic Risk Assessment Development and Its Use in Nuclear Power Industry: A Tribute to the Late Professor Norman Carl Rasmussen. *Reliability Engineering & System Safety*, **89**, 271-285. http://dx.doi.org/10.1016/j.ress.2004.08.022

[6] Reinert, J.M. and Apostolakis, G.E. (2005) Including Model Uncertainty in Risk-Informed

Decision Making. *Annals of Nuclear Energy* **33**, 354-369. http://dx.doi.org/10.1016/j.anucene.2005.11.010

[7] Arrêté du 7 février 2012 fixant les règlesgénéralesrelatives aux installations nucléaires de base.

[8] International Atomic Energy Agency (2006) Fundamental Safety Principles. IAEA Safety Standards Series No. SF-1, International Atomic Energy Agency, Vienna.

[9] US Nuclear Regulatry Commission (2008) Strategic Plan: Fiscal Years 2008-2013. Vol. 4, NUREG-1614, US Nuclear Regulatry Commission.

[10] US Nuclear Regulatry Commission (2012) A Proposed Risk Management Regulatory Framework. NUREG-2150, US Nuclear Regulatry Commission.

[11] Western European Nuclear Regulators Association (2005) WENRA Policy Statement. Stockholm.

[12] Risk and Safety Working Group of the Generation IV International Forum (2010) Basis for the Safety Approach for Design & Assessment of Generation IV Nuclear Systems. Gen IV International Forum, 4.

[13] Sorensen, J.N., Apostolakis, G.E., Kress, T.S. and Powers, D.A. (1999) On the Role of Defense-in-Depth in Risk Informed Regulation. *International Topical Meeting on Probabilistic Safety Assessment* (*PSA*'99), Washington DC, 22-25 August 1999, 3-5.

[14] International Nuclear Safety Advisory Group (2011) A Framework for an Integrated Risk Informed Decision Making Process. INSAG-25, International Nuclear Safety Advisory Group, Vienna.

[15] IAEA Safety Assessment for Facilities and Activities (2009) General Safety Requirements. Part 4, No. GSR Part 4, Vienna.

[16] RSWG (2011) An Integrated Safety Assessment Methodology (ISAM) for Generation IV Nuclear Systems. RSWG Report, Version 1.1.

[17] Fiorini, G.L., Ammirabile, L. and Ranguelova, V. (2013) The ISAM Tool "Objective Provision Tree (OPT)" for the Identification of the Design Basis and the Construction of the Safety Architecture.

[18] Rodríguez-Rodrigo, L. and Elbez-Uzan, J. (2006) Safety Methodology Implementation in the Conceptual Design Phase of a Fusion Reactor. 8*th IAEA Technical Meeting on Fusion Power Plant Safety*, Vienna, 10-13 July 2006, 4.

[19] ITER-Generic Site Safety Report (GSSR) Volume I—Safety Approach. G84RI101-07-09 R 1.0.

[20] Pinna, T., Raboin, S., Uzan-Elbez, J., Taylor, N. and Semeraro, L. (2005) Methodology for Reference Accidents Definition for ITER. *Fusion Engineering and Design*, **75-79**, 1103-1107. http://dx.doi.org/10.1016/j.fusengdes.2005.06.030

[21] Gesellschaftfür Anlagen-und Reaktorsicherheit (GRS) gGmbH (2016) Review of the Safety Concept for Fusion Reactor Concepts and Transferability of the Nuclear Fission Regulation to Potential Fusion Power Plants. GRS-389.

[22] Center for Chemical Process Safety (CCPS) (1993) Guidelines for Safe Automation of Chemical Process. American Institute of Chemical Engineers, 7-16

[23] Center for Chemical Process Safety (CCPS) (2001) Layer of Protection Analysis, Simplified Risk Assessment. American Institute of Chemical Engineers, New York.

[24] Tolmare, G.B. (2007) Holistic Approach to Process Safety. Occupational Safety, Heath and Sustainable Economic Development, New Delhi, 113-122.

[25] International Electrotechnical Commission (2010) Functional Safety of Electrical/ Electronic /Programmable Electronic Safety-Related Systems (IEC 61508).

[26] Central Information Systems Security Division (DCSSI) (2004) In Depth Defence Applied to Information Systems. Version 1.1, DCSSI Advisory Office, Paris.

[27] IT Security Expert Advisory Group (ITSAEG) (2008) Trusted Information Sharing Network for Critical Infrastructures Protection: Defense in Depth. ITSAEG.

[28] Cointet, A. (2005) Defense in Depth: Modeling Defense Elements for a Transport System. RATP, Paris.

[29] International Atomic Energy Agency (2003) Consideration in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors. IAEA-TECDOC-1366.

[30] International Atomic Energy Agency (2005) Risk Informed Regulation of Nuclear Facilities: Overview of the Current Status. IAEA-TECDOC-1436.

[31] International Atomic Energy Agency (2007) Proposal for Technology-Neutral Safety Approach for New Reactor Design. IAEA-TECDOC-1570.