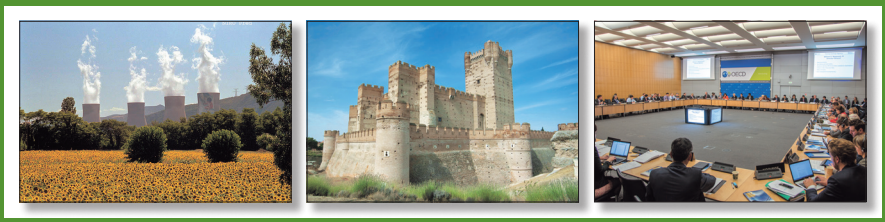
Nuclear Regulation
2016

Implementation of Defence in Depth at Nuclear Power Plants

Lessons Learnt from the Fukushima Daiichi Accident



OECD
BETTER POLICIES FOR BETTER LIVES

NEA
NUCLEAR ENERGY AGENCY

Implementation of Defence in Depth at Nuclear Power Plants

Lessons Learnt from the Fukushima Daiichi Accident

NEA No. 7248

NUCLEAR ENERGY AGENCY
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 34 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the OECD Secretary-General.

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1 February 1958. Current NEA membership consists of 31 countries: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Norway, Poland, Portugal, Russia, the Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The European Commission also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes;
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include the safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information.

The NEA Data Bank provides nuclear data and computer program services for participating countries. In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

Cover photos: Cruas nuclear power plant, France (Fred Niro, 2008); Castillo de la Mota, Medina del Campo, Spain (Garijo, 2011); NEA Steering Committee meeting (October, 2015).

Foreword

The Nuclear Energy Agency (NEA) Committee on Nuclear Regulatory Activities (CNRA) is an international body made up of senior representatives from nuclear regulatory authorities. The CNRA guides the NEA programme concerning the regulation, licensing and inspection of nuclear installations with respect to safety. It acts as a forum for exchange of information and experience, and for the review of developments that could affect regulatory requirements.

The NEA has produced a series of regulatory guidance documents, known as "green booklets", which are prepared and reviewed by senior regulators, and provide a unique resource on key contemporary nuclear regulatory issues. The booklets examine various regulatory challenges and address the major elements and contemporary issues of a nuclear safety regime. (See Appendix 2 for a complete list of published reports.)

Although the audience for this report on defence in depth is primarily nuclear regulatory bodies, the information and ideas herein are also expected to be of interest to licensees, nuclear industry organisations and the general public. The NEA believes this booklet could be of special interest and use to countries looking to begin a nuclear energy programme, but which have yet to develop well-established regulatory regimes. The NEA also encourages and challenges all established regulatory bodies to use the report as a benchmark for improvement and training, continually striving to enhance their effectiveness as they fulfil their mission to protect public health and promote safety.

This report on defence-in-depth (DiD) lessons from the Fukushima Daiichi nuclear power plant accident was prepared by the CNRA Senior-level Task Group on Defence in Depth (STG-DiD) on the basis of discussions and input from members of the group, as well as information from a wide array of documents produced by the NEA, its member countries and other international organisations.

Jean-Luc Lachaume (France) chaired the meetings and work of the group. The members of the STG were Douglass Miller (Canada), Greg Rzentkowski (Canada), Nina Lahtinen (Finland), Keijo Valtonen (Finland), Laurent Foucher (France), Shri S. Harikumar (India), Tomoho Yamada (Japan), Rashet Sharafutdinov (Russia), Mark Kuznetsov (Russia), Lennart Carlsson (Sweden), Jan Hanberg (Sweden), Klaus Theiss (Switzerland), Gary Holahan (United States), Donna Williams (United States), Kay Nünighoff (WENRA), Emmanuel Wattelle (WENRA), Edward Lazo (NEA CRPPH Secretariat), Andrew White (NEA CSNI Secretariat), Javier Reig (NEA), Nancy Salgado (NEA) and Mike Weightman (NEA Consultant).

Table of contents

Executive summary

Defence in depth (DiD) is a concept that has been used for many years alongside tools to optimise nuclear safety in reactor design, assessment and regulation. The 2011 Fukushima Daiichi nuclear power plant accident raised many questions and gave unique insight into nuclear safety issues, including DiD.

In June 2013, the NEA held a Joint Workshop on Challenges and Enhancements to DiD in Light of the Fukushima Daiichi Accident (NEA, 2014), organised by the NEA Committee on the Safety of Nuclear Installations (CSNI) and the NEA Committee on Nuclear Regulatory Activities (CNRA). It was noted at the time that further work would be beneficial to enhance nuclear safety worldwide, especially with regard to the implementation of DiD. Accordingly, a senior-level task group (STG) was set up to produce a regulatory guidance booklet that would assist member countries in the use of DiD, taking into account lessons learnt from the 2011 accident.

This regulatory guidance booklet builds on the work of this NEA workshop, of the International Atomic Energy Agency (IAEA), the Western European Nuclear Regulators Association (WENRA) and of other members of the STG. It uses as its basis the International Nuclear Safety Advisory Group's *Defence in Depth in Nuclear Safety* study (INSAG-10) (IAEA, 1996).

The booklet provides insights into the implementation of DiD by regulators and emergency management authorities after the Fukushima Daiichi accident, aiming to enhance global harmonisation by providing guidance on:

- the background to the DiD concept;
- the need for independent effectiveness among the safety provisions for the various DiD levels, to the extent practicable;
- the need for greater attention to reinforce prevention and mitigation at the various levels;
- the vital importance of ensuring that common cause and common mode failures, especially external events acting in combination, do not lead to breaches of safety provisions at several DiD levels, taking note of the particular attention that human and organisational factors demand;
- the concept of "practical elimination" of sequences leading to significant radioactive releases;
- the implementation of DiD for new and existing reactors, multi-unit sites and other nuclear facilities;

- the implementation of DiD through regulatory activities (based on a survey among CNRA members);
- the protection measures in the DiD concept of level 5 – off-site emergency arrangements.

The use of the DiD concept remains valid after the Fukushima Daiichi accident. Indeed, lessons learnt from the accident and its impact on the use of DiD has reinforced its fundamental importance in ensuring adequate safety. This is illustrated by the recent Vienna Declaration on Nuclear Safety adopted by the contracting parties of the Convention on Nuclear Safety.

This regulatory guidance booklet also identifies areas where further work may be beneficial, including:

- the impact of human and organisational factors on DiD;
- improvements on the use of the DiD concept for new reactor designs, multi-unit sites, fuel cycle facilities and research reactors;
- the implementation of countermeasures for level 5 of DiD;
- benchmarking and further harmonisation of regulatory use of DiD through training, workshops and other means;
- the impact of new technologies.

1. Introduction

Background

Defence in depth (DiD) is a concept used for many years alongside other design principles and tools to optimise nuclear safety. It is based on an ancient military philosophy of providing multiple barriers of defence and is used in the design of nuclear facilities, the assessment of such designs and all aspects of their regulation.

The 2011 accident in Fukushima gave unique insight into nuclear safety issues, and raised many questions about the tools used at nuclear power plants, including the effectiveness of the DiD concept, but it also provided opportunities to review whether DiD can be enhanced and its implementation improved. It illustrated, in particular, how an external event can act as a common mode initiator for the failure of the safety provisions in several levels of DiD.

In June 2013, the NEA held a Joint Workshop on Challenges and Enhancements to DiD in Light of the Fukushima Daiichi Accident, organised by the NEA Committee on the Safety of Nuclear Installations (CSNI) and the NEA Committee on Nuclear Regulatory Activities (CNRA) (NEA, 2014). The outcome was discussed at the December 2013 meeting of the CNRA and it was decided that further work would be beneficial, especially in relation to the implementation of DiD in order to further enhance nuclear safety worldwide. Accordingly, a CNRA senior-level task group (STG) was set up to produce a regulatory guidance booklet that would assist member countries in reconsidering and clarifying DiD and its implementation using lessons from the accident.

This regulatory guidance booklet builds on the work of this NEA workshop, on the IAEA DiD conference in October 2013 (IAEA, 2013) and its recent work on revising standards and creating additional guidance on design (IAEA, 2012), as well as on recent developments on the use of DiD by the Western European Nuclear Regulators Association (WENRA, 2013). It is based on the solid foundation of the approach described by the International Nuclear Safety Advisory Group (INSAG) (IAEA, 1996).

Scope

The NEA workshop concluded that:

- DiD remains valid but strengthening may be needed;

- implementation of DiD needs further work, in particular regarding external hazards;
- additional guidance is needed to enhance harmonisation;
- improvements should focus not only on preventing accidents but also on mitigating consequences.

This booklet seeks to address these points and enhance the usefulness of the DiD concept, learning from the lessons of the Fukushima accident. To do so, the booklet:

- describes the basis of the DiD concept and how it has been further developed in response to lessons derived from the accident (Chapter 2);
- addresses the main generic issues identified by the NEA workshop and CNRA as being of prime interest for further study and clarification in a regulatory context, for example:
  - The structure of the levels of DiD (Chapter 2);
  - DiD implementation (Chapter 3) including:
    - independence;
    - impact of common cause and common mode threats (including external events);
    - human and organisational factors;
    - practical elimination of significant releases;
    - new and operating reactor considerations;
    - multi-plant sites;
    - DiD for other nuclear facilities;
    - regulatory implementation of DiD including survey results.
  - Emergency arrangements off-site (Chapter 4).
- provides an overall discussion of the use of DiD post-accident for regulators, and concludes that further studies by the NEA would be beneficial to enhance implementation.

Other international work is in progress on the use of the DiD concept to enhance implementation, notably by INSAG on institutional DiD. This booklet is primarily aimed at senior regulators to provide clarity and assistance when considering the impact on the use of DiD after the accident.

2. The concept of defence in depth

The basis

For the purposes of this booklet the original description of the DiD concept for operating plants and its principles from INSAG-10 (IAEA, 1996) are used as a basis for this booklet (see Table 1). INSAG presents in fact two DiD approaches. One for the operating nuclear power plants (NPPs) and the other for the new plants. Some countries have expanded this definition to facilitate implementation, but it does not affect the usefulness of the basic concept as established by INSAG.

Table 1. INSAG-10 DiD levels

Level of defence in depth	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

The DiD concept stipulates that independent protection against the failure of safety functions should be provided, as far as practical, for different plant states.

The effectiveness of the protection is established using the principles of, *inter alia*, redundancy, diversity, segregation, physical separation and single-point failure protection.

The use of the DiD concept has been promulgated through the IAEA Safety Fundamental Principles and Standards (see IAEA SSR 2/1 [IAEA, 2012]). The IAEA safety fundamental principle 8, in particular, states:

> *"The primary means of preventing and mitigating the consequences of accidents is 'defence in depth' ..... The independent effectiveness of the different levels of defence is a necessary element of defence in depth."*

And, the IAEA SSR 2/1 sets a specific requirement for the design:

> *"Requirement 7: Application of defence in depth. The design of a nuclear power plant shall incorporate defence in depth. The levels of defence in depth shall be independent as far as is practicable."*

Implementation of the original INSAG DiD concept has developed over the years, and this has been reinforced after the Fukushima accident. As explained below, this has included a modified description of the five levels of defence.

Regulatory considerations for DiD: Lessons learnt from the Fukushima Daiichi accident

The original DiD concept, as described in INSAG-10, has been implemented in some currently operating and new NPPs. However, lessons learnt from the accident have given cause for the nuclear industry to enhance elements of DiD, and to seek to strengthen implementation of the DiD concept.

There has been no significant change to the concept but a strong emphasis on ensuring that an appropriate design basis is established for all relevant hazards (natural and man-made), events and combinations. To facilitate implementation, some organisations, such as WENRA (2013), have found benefit in subdividing level 3, others have proposed including beyond design basis accidents, with or without core damage in level 4, or using 6 rather than 5 levels of DiD. These proposals all build on the original INSAG concept and strengthen its implementation, but none have been universally adopted.

The Fukushima accident reinforced the need to gain assurance that there was an adequate, fundamental basis for the design and operation of a plant such that it has the ability to safely withstand the full range of external and internal events to which it may be exposed. While the Fukushima Daiichi site substantially withstood the direct effects of the earthquake, with the operating reactors shutting down and cooling established, the earthquake caused all six off-site power lines to be lost and the associated tsunami took out all but one on-site emergency alternating current (AC) power supply. Additionally, the tsunami effectively eliminated access to the heat sink and nearly all of the electrical systems, both AC and (in some cases) direct current (DC), and eventually caused instrumentation failure. Some of this was related to the layout of the plant, as well as to the absence of reliable defences against flooding.

In effect, there was an inadequate basis for the safe operation of the plant and no independent effectiveness of the protective and mitigating systems for the first four levels of DiD, both in terms of the original basis used for the design of the plant and of the outcome of any periodic reviews or other safety reviews. There is therefore a clear message for regulators, reinforcing the need for close attention to the basis for the design and operation of a plant or site, and the need to review this basis – especially for external hazards and events – to ensure that safety functions at the various DiD levels have adequate, independent effectiveness.

This adequate independence is important for all levels, including the systems, structures and components (SSC) that are at the second level of DiD, to control anticipated operational occurrences (AOO) when using different types of controllers, limitations and protection systems for example. These SSCs are intended to detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions.

However, for some AOOs, these measures are not sufficient to prevent an accident condition from occurring, thereby activating the safety systems. Safety systems such as the reactor scram system and, depending on the plant type, the overpressure protection system of the primary and secondary side, the emergency feedwater system and diesel generators, are needed as part of the design basis of the plant to prevent an event from escalating to a severe accident.

Similarly, the Fukushima Daiichi accident emphasised for regulators the need to gain assurance that the design basis accident and design extension requirements used by designers and safety assessors covers those needed to ensure the independent effectiveness of the safety provisions for INSAG levels 3 and 4.

The need for safety provisions beyond those provided at INSAG level 3 for coping with design basis accidents has been enhanced in a number of countries and in IAEA safety standards through the use of the concept of design extension conditions (DECs). DECs are conditions beyond the design basis accident that are nevertheless considered on the basis of best estimate methodology. The analysis of design basis accidents, and the design of safety provisions for such accidents, uses established design criteria and conservative methodology, and seeks to demonstrate that any release of radioactive material is kept as low as reasonably achievable and within acceptable limits. For design basis accidents, the first goal is to limit or ensure only minor radiological off-site consequences that do not necessitate protective action off-site. In some countries, specific acceptance criteria are set for DECs without core melt.

The concept of design extension conditions was introduced in a number of countries, as well as in IAEA safety standards, prior to the occurrence of the accident. However, over the last few years, design extension conditions have been refined to more comprehensively address multiple failures (common cause and common mode failures), some complex sequences, rare internal and external events and severe accidents. The requirements entailed in this concept mainly concern new NPPs, but they can also be applied to existing plants as far as is reasonably practical.

Consequently, design extension conditions now include:

- postulated initiating events that involve a common cause and common mode failure resulting in multiple failures in the safety system designed for coping with the event concerned;
- combinations of failures selected on the basis of deterministic analysis, probabilistic risk assessment or engineering judgement;
- internal and external events more severe than those considered in the design basis, caused by rare events that are very unlikely to occur but nevertheless considered credible events;
- severe reactor accidents (that is, accidents involving core damage/fuel melt) and severe spent fuel storage accidents.

For such credible multiple failure events, combinations of failures or rare internal and external hazards and events, the regulator needs a demonstration that it is possible to fulfil the fundamental safety functions of reactivity control, core (fuel) cooling, confinement of radioactive material and hence minimisation of significant releases. Based on the design and safety analysis, the regulator would need to be shown that following an accident, to the extent practical:

- the reactor core (fuel) can be brought and maintained subcritical;
- the deformations in reactor internals and fuel rods do not endanger the cooling of the reactor core (only limited fuel damage is acceptable);
- the pressure in the reactor coolant pressure boundary does not exceed an acceptable value, for non-core damage accidents;
- containment integrity remains functional (with or without the need for venting);
- the fuel in the spent fuel pool can be sufficiently cooled, including an appropriate margin.

The demonstration should show that once the controlled state[1] is reached the plant can be brought to a safe state[2] and maintained there over the long term in such a way as to meet the radiological criteria.

Overall, the safety objective for INSAG level 4 provisions is that significant releases would be avoided or minimised. To this end, the regulator may seek to be ensured that accident sequences that lead to significant radioactive releases are

1. IAEA SSR-2/1: A controlled state is when, following an anticipated operational occurrence or accident conditions, the fundamental safety functions can be ensured and can be maintained for a time sufficient to implement provisions to reach a safe state.
2. IAEA SSR-2/1: A safe state is when, following an anticipated operational occurrence or accident conditions, the reactor is subcritical and the fundamental safety functions can be ensured and maintained stable over the long term.

"practically eliminated". There has been some debate about what this means in practice. Chapter 4 provides regulators with further guidance in this regard.

For INSAG level 4, regulators can expect that analysis methods and boundary conditions, or design and safety assessment rules, are developed according to a graded approach, based on probabilistic insights, and using best estimate methodology. Less stringent analysis rules and equipment performance requirements than those for INSAG level 3 may be applied if appropriately justified.

The accident in Fukushima provided several important lessons for the implementation of INSAG level 5. In particular, it illustrated that no matter how much other levels are strengthened, and very rare severe event scenarios are practically eliminated, effective emergency arrangements and other responses are essential parts of the DiD concept. To be effective, they have to be functional in the particular circumstances of the accident.

It also served to illustrate the need to consider the implications of long-term releases and escalating events that can be associated with a multi-unit site, particularly as regards resourcing. The resourcing of the response over long periods was a challenge for response teams but also for regulator resources, as well as others. In a country affected by a significant nuclear accident, the regulator's resources have not only to be robust to deal with the national response but they also have to be sufficient for supporting the information needs of the international community.

In addition, there was a considerable direct impact of the earthquake and tsunami on the infrastructure, equipment and facilities provided for an off-site emergency response. The normal flow of information between the site and off-site organisations involved in the emergency response can be severely hampered in terms of quality, quantity and timeliness. This in part can be a consequence of damage to the normal channels of communication. Other capabilities, such as off-site help to the affected site, can also be hindered. Such difficulties are more complicated and extensive with accidents at multi-unit sites, especially with regard to site status analysis and source-term estimates.

Integrated DiD

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

3. Implementation of defence in depth

Introduction

This chapter addresses two areas of interest for regulators: how the DiD concept has been or can be used in practice, demonstrating what is good practice or reasonably practicable; and how regulatory bodies can secure such implementation through their regulatory activities.

It begins with an overview of the implementing elements (programmes, measures and features) of DiD, including a table to show how they are used at the various levels. It then discusses three topics that require further guidance, particularly following the Fukushima accident. These are independence, common cause failures and the practical elimination of significant radiological releases.

Subsequent sections discuss examples of implementation of the DiD concept in new and operating reactors, multi-plant sites and non-nuclear facilities, as well as its implementation by regulators.

The implementation of DiD has been refined in different ways by various organisations to include design basis events and design extension conditions, with and without core melt. In some regulatory systems, design extension conditions (DECs) without core melt are covered in INSAG level 4 of DiD, as they are considered to be similar to severe accidents and thus the same approach to their assessment is used. In other systems, they are covered in INSAG level 3 as a sublevel, since they are considered to be closer to design basis events in terms of the radiological objectives and physical phenomena involved. Elsewhere, a new level has been used to cover DEC without core melt. As noted earlier, such adjustments do not invalidate the original INSAG concept and its original description (Table 1) as used for the purposes of this document.

General elements of implementation

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

Figure 1 summarises a practical example from Canada of implementation measures and features for each of the INSAG levels of DiD.

Figure 1. Canadian example of DiD implementation based on INSAG levels: Accident prevention and mitigation

Level	Implementation
1. Normal operation: To prevent deviations from normal operation, and to prevent failures of structures, systems and components (SSCs) important to safety.	Conservative design. High-quality materials, manufacturing and construction (e.g. appropriate design codes and materials, design procedures, equipment qualification, control of component fabrication and plant construction, operational experience). A suitable site was chosen for the plant with consideration of all external hazards (e.g. earthquakes, aircraft crashes, blast waves, fire, flooding) in the design. Qualification of personnel and training to increase competence. Strong safety culture. Operation and maintenance of SSC in accordance with the safety case.
2. Operational occurrences: To detect and intercept deviations from normal operation, to prevent AOOs from escalating to accident conditions and to return the plant to a state of normal operation.	Inherent and engineered design features to minimise or exclude uncontrolled transients to the extent possible. Monitoring systems to identify deviations from normal operation. Operator training to respond to reactor transients.
3. Design basis accidents: To minimise the consequences of accidents and prevent escalation to beyond design basis accidents	Inherent safety features. Fail-safe design. Engineered design features, procedures that minimise design basis accident (DBA) consequences. Redundancy, diversity, segregation, physical separation, safety system train/channel independence, single-point failure protection. Instrumentation suitable for accident conditions. Operator training for postulated accident response.
4. Beyond design basis accidents: To ensure that radioactive releases caused by beyond design basis accidents, including severe accidents, are kept as low as practicable.	Beyond design basis accidents guidance to manage accidents and mitigate their consequences as far as practicable. Robust containment design with features to address containment challenges (e.g. hydrogen combustion, overpressure protection, core concrete interactions, molten core spreading and cooling). Complementary design features to prevent accident progression and to mitigate the consequences. Features to mitigate radiological releases (e.g. filtered vents).
5. Mitigation of radiological consequences: To mitigate the radiological consequences of potential releases of radioactive materials that may result from accident conditions.	Emergency support facilities. On-site and off-site emergency response plans and provisions. Plant staff training on emergency preparedness and response.

In practice, the implementation of safety provisions for DiD is implemented in the design using:

- A deterministic engineering approach and analyses, which mainly relate to levels 1 through 3, plus specific features to address design extension conditions, in particular containment performance during severe accidents (level 4); supplemented where necessary by probabilistic safety assessment (PSA) to identify cross-linkages, vulnerabilities and interdependences.
- Probabilistic studies to identify plant vulnerabilities, including complex situations due to several equipment and/or human failures (IAEA, 1992), with a deterministic analysis used to establish scenarios that must be addressed, such as loss of electrical power (no power) or heat removal capability (no services).
- An assessment of release monitoring processes and instrumentation to support off-site emergency management (level 5).

Although DiD is used in almost all regulatory systems, it is not seen as establishing specific acceptance criteria for the adequacy of safety provisions, but simply provides one input into such a decision. Other inputs are also taken into account when designing nuclear facilities and assessing their safety. These include deterministic analyses of normal operating conditions, design basis accidents and design extension conditions as complemented by PSA. As such, DiD should be considered as complementary, but nonetheless overarching these other inputs into design and the safety assessment of design. As shown in Figure 1, DiD also provides a logical structure for both formulating and assessing the safety measures of a reactor design and in assessing the provisions for reactor operation.

To maximise the effectiveness of the use of DiD, it must be part of the early design process and addressed in a consistent and effective way. Thus, the regulator should ensure that it has been incorporated into the design management arrangements.

An illustration of the importance of this early use is that it is essential in developing the safety classification of systems and components. If classification and categorisation have developed without reference to DiD, rather than DiD being one of the drivers for classification and categorisation, later analysis can reveal that the independence of the safety provisions at the various layers of DiD has been undermined, with the possible introduction of a common cause failure into the design.

Independence of the levels of DiD

The concept of the independence of the levels of DiD applies to all five levels. As indicated above, the independent effectiveness of each of the safety provisions at the various levels is an essential basis for the safety of the plant. The regulator would wish to be ensured that failure at one level (or barrier) of defence does not, as far as practical, cause the failure of others.

Regulators use their normal approach to assess how the licensee has justified in the safety case the independent effectiveness of the design and operational provisions for each level. This is done to gain assurance that the ability to perform the required safety function at a particular DiD level is unaffected by the operation or failure of the other systems, structures and components (SSCs) needed for other DiD levels, or by the effects resulting from the postulated initiating event.

The systems, structures and components required for each postulated initiating event are identified, and it is shown by means of deterministic analyses that the systems, structures and components required for implementing safety functions at any one level of DiD are sufficiently independent from those at other levels, taking into account the threats that can affect them. The adequacy of the achieved independence is also analysed using probabilistic analyses.

Independent effectiveness is based on the adequate application of functional isolation,[1] the diversity principle and physical separation[2] of the SSCs depending on the threats.

Optimally, systems and components assigned to different levels are functionally isolated from one another to ensure that the mode of operation or the failure of a system or component of a lower level does not result in the malfunction or loss of function of a system of a higher level, and similarly that the failure of higher level SSCs do not impair the function of lower level systems. In addition, the redundant parts of a system performing safety functions have to be physically separated from each other. Interference between safety systems or between redundant or diverse elements of a system is prevented by various means, including electrical isolation and independent data transfer. The impact and capacity of common services, such as ventilation and cooling water systems has to be taken into account as well.

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

Safety systems such as the reactor scram system and, depending on the plant type, the overpressure protection system of the primary and secondary side, emergency feedwater system and diesel generators, which are used at level 3, are to be functionally isolated and physically separated to the extent practical from those systems which are used for normal operation at level 1 and those which are intended to detect and control deviations from normal and abnormal operational occurrences at level 2 (IAEA, 1996).

The SSCs at INSAG level 4 are independent to the extent practicable from the SSCs of other levels of DiD. The additional systems supporting implementation of

1. Functional isolation refers to the isolation of systems from one another so that the operation or failure of one system does not adversely affect another system.

2. Physical separation refers to the separation of systems or components from one another by means of adequate barriers, distance or placement or combinations thereof.

INSAG level 4 DiD, intended for controlling reactor accidents, are functionally isolated and physically separate from the systems intended for normal operation, anticipated operational occurrences and for controlling design basis accidents (levels 1, 2 and 3, respectively). Those SSCs which are ensuring safety functionality for multiple failure events, for rare external events and for severe accidents are to be independent from each other to the extent practicable.

In addition to assurance about the provision of hardware SSCs, the regulator should also be interested in the human factor and performance aspects provided at each level of DiD, including the ability of NPP operation staff (and contractors where relevant) to implement effective emergency actions, especially for multi-unit sites. It has been noted that human and organisational factors play a great part in the effectiveness of SSCs at all levels. Indeed, at level 4, the importance of severe accident management provisions in existing plants including hardware provisions, emergency operating procedures and severe accident management guidelines has increased as a result of the lessons learnt from the Fukushima accident, particularly for operating reactors. In new reactor design such provisions should already be included in the design phase of the plants.

Common cause and common mode failures (including external hazards)

The accident in Fukushima demonstrated that it is vital to consider the impact of common cause and common mode failures when implementing the concept of DiD, particularly from external hazards, as they can lead to a loss of several levels of DiD safety provisions or significantly reduce independent effectiveness.

Applying the concept of DiD and the need for independence of the various levels is an effective way of identifying and addressing common cause and common mode failures.

The regulator is likely to expect a detailed analysis of the various hazards, initiating events and faults against the concept of independent effectiveness of safety provisions at the various levels of DiD. This can provide a very valuable assessment of the plant's robustness. Such analyses can lead to an enhancement of the diversity, separation and redundancy of safety provisions, and to increased attention to the qualification of safety equipment, particularly instrumentation and control (I&C). Of special importance is the need to ensure adequate robustness, under all conditions, of safety services and controls (including control centres).

External hazards and events

It is a basic requirement for any nuclear reactor that relevant external hazards/events, including credible combinations of them, are adequately identified, assessed and taken account of in the design. As an external event can impact several levels of DiD simultaneously, the regulator will want to be ensured that special attention has been paid to the plant design so as to ensure the robustness of the remaining levels of DiD. Of particular note is the impact of extreme external events on on-site and off-site electrical power, as well as on other services.

The importance of adequate consideration for extreme external hazards and events cannot be overstated given the impact that they can have on the

independent effectiveness of the SSCs provided at the various levels of defence, on the creation of a common cause fault, and on the capability of response on and off the site. This is well illustrated by the 2011 accident. When considering extreme external events, particular attention should be given to cliff edge effects. Additionally, where there are significant uncertainties in the derivation of design basis external events, additional margins or design provisions are expected to be included.

Of particular interest with regard to the uncertainty of external events are extreme weather conditions. These can impact both on-site and off-site DiD safety provisions. Given the enhanced variability associated with climate change, particular regulatory attention has to be accorded to ensuring not only an adequate consideration of its impact but also on reviewing any changes in information, knowledge or understanding.

Internal hazards and events

Some example of these types of common cause and common mode failures are provided below. It is not an exhaustive list.

Flooding on the site from internal events

As observed from the 2011 accident and other events worldwide, flooding can have devastating effects at a nuclear facility site. It can be induced from outside the site as was the case in 2011. However, consideration must also be given to on-site induced flooding, through failures of such equipment as the main cooling intake pipework. Among other impacts, such an event can undermine the foundations of buildings. Internal flooding within buildings housing equipment important to safety can potentially damage the safety systems designed to protect against flooding.

Site impact events

As part of ensuring that potential common cause site hazards or events will have minimal impact on DiD safety provisions, the regulator may expect that an impact study is undertaken for site-originated hazards (for example, fire, explosion or vehicle crashes) in relation to the impact on the independence effectiveness of the safety provision at various levels. Such a study is expected to include the combination of fire with other events, especially external hazards, and the capability of fixed and mobile firefighting responses in such circumstances.

Design and supply related factors

New technology

If widely employed across a plant, new technology may introduce common cause and common mode failures that cut across the concept of independence of levels – for example, embedded chips in individual safety components. Similarly, the widespread use of digital I&C may cut across several levels of DiD if sufficient attention is not paid to the need for high quality software, diversity and separation.

Innovative design tools, such as those used in the design of the piping system, generating codes for I&C and plant modelling, may also be a source of failure of the DiD concept. Failures in maintenance can introduce common cause failures in passive systems as well, and this may be an important unrevealed fault. Regulator attention should thus focus on such initiatives, recognising that further work is required in this area.

Electrical, I&C and other auxiliary systems

Failures or events related to the electrical supply system on and off the site can clearly be a source of a common cause and common mode failure. The Fukushima accident illustrated that such failures can result from the layout of the equipment (susceptible to flooding) across the site and plant. Other incidents have illustrated the need to consider the impact of hazards such as lightening, electrical storms, grid instabilities and failures or maintenance, all of which can invoke a common cause failure of the site's electrical systems. The regulator will want to see how the designer/licensee has dealt with the impact of external hazards/events on the grid system, especially as it is not anticipated to be as robust as the site systems under extreme external conditions.

The regulator will also look for assurance that consideration has been given to common cause failures of I&C and other auxiliary systems, given their importance to ensure effective safety across a number of DiD levels.

Procurement, storage and installation of SSCs

The manufacturing process and procedures or the supply of components, especially changes affecting them, can lead to common cause and common mode failures. Similarly, inappropriate storage or marking of safety related equipment can have an impact on safety performance and thereby result in common cause and common mode failures if used in SSCs across levels. Regulatory interest in this area has expanded recently, particularly as regards the potential supply of non-conformance and counterfeit components into safety systems. Replacement of SSCs across the plant may also be a source of failures.

Human and organisational factors

Of particular note to the regulator will be whether the human and organisational elements of the safety provisions support, reduce or cut across the independent effectiveness of the SSCs at the various levels – acting as a common cause failure. Hence, human and organisational aspects are of particular importance and include such matters as:

- Safety culture in the industry and the regulatory body.
- Design and operational management control, including quality assurance (QA), management of change and configuration control.
- Construction and installation, maintenance, modification and operation that could degrade the independence of the levels.
- The need for greater attention to severe accident management, including leadership, emotional needs of staff (especially with external events that

may have also affected their families and homes), decision-making responsibilities (the site director, or person acting in that role, should clearly be in charge of on-site activities) and staffing levels – particularly for the impact of external hazards on multi-unit sites. The regulator should be convinced that in the case of a severe accident and a damaged plant (and possibly the rest of the site or other plants) operator actions will be performed in a timely and feasible manner.

It is important to ensure that the staff of the utility, their contractors and the regulator are aware of the need to preserve the safety provisions at the various DiD levels and their effective independence.

Information about the systems that contribute to DiD, and the importance of maintaining effective DiD, contributes greatly to developing and enhancing a vibrant safety culture.

This guidance indicates that DiD should be part of the foundations for effective training programmes for operational and maintenance staff, especially as it can be broken down into simple concepts, and indeed it could be part of site induction programmes for all personnel. It can also be used on a routine basis to display to staff and others at the work place the status of the various protection systems, enhancing understanding and attention to items important for safety.

Practical elimination of significant radioactive releases through DiD

Practical elimination of significant radioactive releases should be addressed in the design of new plants and can be applied to both prevention and mitigation safety measures. This does not imply that other safety goals, such as individual and societal risk criteria, should not be addressed, but it adds a further dimension to the assessment and demonstration of safety by providing a final check that all required measures of protection have been established. For existing plants significant radioactive releases should be prevented or mitigated by means of reasonable practicable modifications/backfitting measures and severe accident provisions as far as practicable.

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

The concept of the “practical elimination” of significant releases has been introduced for new reactor designs. It deals with very rare phenomena, given the effective implementation of safety provisions at levels 1 to 3. It is included in both the IAEA safety requirements for new reactor designs (IAEA, 2012) and in WENRA documentation (WENRA, 2013). The re-examination of high consequence events after the 2011 accident has led to enhanced consideration of the practical elimination concept and further plant improvements. Practical elimination,

however, does not mean complete elimination or that events of significant releases are physically impossible, but rather that, with a high degree of confidence, such events have been demonstrated to be extremely unlikely. To date, there does not seem to be a common understanding of what that implies for reactor safety systems. This section explores this concept and puts forward an approach.

The implementation of the practical elimination concept is most effective through design features, and thus it is easier to implement in new reactors. For operating reactors, there are likely to be fewer practical opportunities for enhancing safety. These have to be considered on a case-by-case basis.

In determining whether a design adequately addresses the practical elimination of significant radioactive releases, the regulator is expected to assess the licensee's evaluation and identification of, *inter alia*, phenomena that could challenge containment performance, event preclusion, accident progression, containment performance and potential radiological source terms.

The practical elimination concept is an approach that sets improved safety goals (or expectations) for nuclear installations by incorporating additional design features or, more rarely, operating provisions. These features or provisions can be associated with level 1, 2, 3 or 4, or any combination of these.

It is important that practical elimination is not used to justify a lack of severe accident management arrangements and capabilities, or the absence of fully effective emergency arrangements both on-site and off-site. Such an approach would go against the concept of DiD and the independent effectiveness of the various levels of DiD.

In the implementation of the practical elimination concept through event preclusion, the regulator is likely to expect a safety demonstration:

- to clearly state the improved safety goal;
- to express this goal in terms of impacts and requirements on the construction of the safety demonstration (e.g. elimination of incidental or accidental sequences, exclusion of some accidental scenarios);
- to describe the technical requirements to exclude these accident scenarios (e.g. exclusion of high pressure core melt, a particular pipe break preclusion);
- to describe the design provisions, criteria and operative measures which demonstrate that these requirements can be excluded because of physical reasons or because a high degree of confidence makes them extremely unlikely;
- to justify why these design and operative provisions will remain available through the whole life of the installation.

In addition, the practical elimination concept should specifically address challenges to containment performance; the last barrier to radioactive releases,

i.e. safety provisions of DiD level 4. In addressing containment performance, the regulator may expect the following to be considered:

- Identification, through deterministic analyses, PSAs and engineering judgement, of the challenges to containment (e.g. severe accident performance and potential containment failure mechanisms, including bypassing the last barrier). This could include issues related to: core melt concrete interaction, hydrogen combustion, over-pressurisation, direct containment heating, steam explosions.
- Design and operational provisions to prevent or mitigate each severe accident phenomena.
- Analysis (best estimate) to demonstrate the effectiveness of the design features established through practical elimination assessment.
- PSA to show the overall effectiveness of level 1, 2, 3 and 4 activities to practically eliminate significant releases.

The regulator may note that the PSA is not a substitute for providing practical design features; it is part of the process to identify potential safety enhancements and to judge their effectiveness. Improved design methods and criteria should be implemented to demonstrate the achievement of improved requirements.

According to IAEA safety standards (IAEA, 2012), accident conditions with significant radioactive releases are considered to have been practically eliminated:

- if it is physically impossible for the condition to occur; or
- if the condition can be considered with a high degree of confidence to be extremely unlikely to arise.

Physical impossibility can be demonstrated by a design feature that would preclude initiation or further progress of an accident scenario. Assumptions used to support the demonstration should be adequately acknowledged and addressed. In some cases, the additional design features are considered sufficient to justify that the occurrence of a particular type of accident scenario does not need to be accounted for in the safety demonstration.

When the concept of practical elimination is applied to initiating events, these additional provisions are considered sufficient to justify that the safety demonstration does not need to account for some types of accidents. For example, the elimination of piping welds and the use of high pressure piping can remove known pipe failure mechanisms sufficiently to exclude such events from a plant's design basis. This approach is sometimes called "event preclusion". Whether through event preclusion or severe accident provisions, real physical features are expected to be included in new designs to prevent a possible event initiator or an accident sequence that would lead to a known containment failure mechanism. In both cases, the phenomena must be well understood and the actions proposed must be adequately supported by experiments, testing, theory and analysis. Similarly, the development of the design must be adequately based on appropriate design codes, choice of materials, etc.

To demonstrate practical elimination of a condition as extremely unlikely with a high degree of confidence, the regulator will expect the following to be considered:

- The degree of substantiation provided for the demonstration of practical elimination, and the degree of confidence.
- Practical elimination of an accident scenario or more than one scenario is not claimed solely based on compliance with a probabilistic cut-off value. Even if the probability of an accident sequence is very low, any additional design features, operational measures or accident management procedures to further lower the risk should be implemented (or have been implemented) to the extent practicable.
- That the necessary high confidence in low likelihood is, wherever possible, supported by means such as:
  - multiple layers of protection;
  - application of the safety principles of independence, diversity, separation and redundancy;
  - enhanced margins in the design;
  - use of passive safety features;
  - use of multiple independent controls.

In each case, the demonstration should include sufficient knowledge of the accident sequence analysed and of the phenomena involved, substantiated by relevant evidence, to conclude that the condition is physically impossible or extremely unlikely with a high degree of confidence.

To minimise uncertainties and to increase the robustness of a plant's safety case, demonstration of practical elimination should preferably rely on prevention through the criterion of physical impossibility (i.e. event preclusion), rather than the second criterion (extreme unlikelihood with high confidence). It has been noted that in practice, new reactor designs have been using provisions at several levels of DiD; eliminating some event challenges and providing mitigation features to enhance containment performance.

The regulator will want to ensure that the safety measures supporting practical elimination are guaranteed to be available throughout the life of the plant and for all fault sequences or circumstances that may affect them. This may be difficult where the form of the additional safety measure does not lend itself to inspection, testing or maintenance, which can ultimately affect the choice of the design provision or the degree of substantiation necessary.

The Fukushima accident revealed weaknesses in the current implementation of DiD in some plants primarily by exposing the sensitivity of different levels of defence to the same hazard (the lack of independence, the inadequate design basis and the insufficient safety margins, which can result in a common mode failure. It is therefore important that features to deal with DECs, including severe accidents,

are not dependent on design elements which could have failed in the first three levels of DiD.

Implementation of DiD in new and operating reactors

For new reactors, it is expected that DiD will be fully implemented as described in the IAEA's design requirements document SSR 2/1 or in the equivalent national standard.

For operating reactors, DiD is enhanced through ongoing regulatory oversight and through mechanisms such as periodic safety reviews (PSRs), plant-specific backfitting and feedback from operating experience.

Licensees, in PSRs, are normally expected to demonstrate the extent to which the safety requirements of the DiD concept are fulfilled in their global assessment of plant safety. Typically, they are also expected to identify strengths and weaknesses when fulfilling the safety requirements of the DiD concept through their integrated implementation plan, or otherwise demonstrate that they have done all that is reasonably practical.

For operating reactors, the regulator may expect that fewer practical steps can be taken to address event preclusion or containment failure mechanisms because fundamental design modifications are not usually practical for operating reactors. However, in some cases, the addition of hydrogen recombiners, containment flooding (usually through severe accident management guidelines), containment venting combined with other measures such as scrubbing, or filtered containment venting, can address specific severe accident sequences and contribute significantly to enhanced containment performance. Further study could therefore be beneficial in identifying safety improvements including, in some cases, for existing reactors design modifications that would practically eliminate some severe accident sequences. Such improvements for existing operating reactors are likely to be through mitigation strategies and measures rather than through prevention of the initiating event sequence as is the case for new reactors. PSA is a useful tool to identify the most important sequences and opportunities for safety enhancements for both new and operating reactors.

Consideration of DiD at multi-unit sites

Many countries have more than one nuclear power plant on a particular site. Present arrangements include sites with two separate plants at one location; four plants with a common control room and other shared systems, structures and components; or six or more plants with combined control rooms. (It should be noted that the requirements in SSR 2/1 would restrict some of these existing configurations.)

In almost all cases there are some interconnections (e.g. connection of electrical power from one plant, sharing of mobile diesel generators) and in some cases, there are greater interdependencies between units on the site. Special attention should be given to whether such interdependencies enhance or undermine facility safety.

Other issues should be considered, such as:

- staffing levels for normal operation and for response to events, including multi-unit events;
- sufficient temporary or portable equipment to cope with design extension conditions (e.g. diesel generators, water supply);
- emergency response procedures and severe accident management guidelines that address multi-unit events;
- accommodating staff in response to an incident affecting all of the site.

There are concerns regarding multi-unit sites that are related to independence of the units. As such, DiD assessments should be carried out to determine the ability of each unit to function on its own.

However, it is also important to consider what is credited as support from other units in the safety case, mainly in accident conditions. For example:

- Are the provisions feasible in terms of the need for power from an adjacent unit?
- Are actions from other unit operators credited, where operators from other units have to come in and perform certain actions on the unit affected?

There are some key questions to be addressed as well regarding DiD implementation for multi-unit sites:

- To what extent should each unit be autonomous?
- What degree of sharing of SSCs, if any, should be permitted at multi-unit sites?

SSCs important to safety shall typically not be shared between two or more reactors. In exceptional cases when SSCs are shared between two or more reactors, such sharing shall exclude safety systems and turbine generator buildings that contain high-pressure steam and feedwater systems, unless this contributes to enhanced safety. If sharing of SSCs between reactors is arranged, then the following requirements shall apply:

- safety requirements shall be met for all reactors during operational states, DBAs and DECs;
- in the event of an accident involving one of the reactors, orderly shutdown, cool down, and removal of residual heat shall be achievable for the other reactor(s).

When an NPP is under construction adjacent to an operating plant, and the sharing of SSCs between reactors has been justified, the availability of the SSCs and their capacity to meet all safety requirements for the operating units shall be assessed during the construction phase.

The adequacy of DiD provisions for each unit (facility, e.g. spent fuel pool, dry fuel storage) need to take into account the impact of adjoining and nearby facilities, and what they are relying on from other facilities.

It may be difficult to establish specific requirements regarding multi-unit facilities. A judgement would likely have to be made in the particular circumstances on the overall adequacy of DiD provisions for all units on the site, and the site as a whole, noting that as far as practicable safety provisions for each unit should be self-sufficient, although they may offer backup to other units for some events.

Lastly, emergency preparedness measures, level 5 of DiD, need to take into account multi-unit events. This level of DiD is discussed further in Chapter 4.

Other nuclear facilities

The DiD concept can be useful for the nuclear fuel cycle facilities, research reactors and other nuclear facilities. In principle, current IAEA safety standards cover the application of DiD to these facilities. However, some of these sites may have been designed without the advantage of such a formal application of DiD. The practice varies from country to country, but some elements of DiD may have already been addressed (e.g. physical barriers and technical measures). Nevertheless, this is an area that may warrant further consideration and guidance.

Regulatory implementation of DiD

The use of the DiD concept, along with other techniques such as PSA and structured deterministic analysis, has done much to enhance safety over the last 20 years. The learning opportunities afforded by the 2011 accident has given increased drive to this use of DiD, both for the re-assessment of the requirements for new reactors and the identification of reasonably practical and achievable continuous improvements to existing reactors. Similarly, regulators have an opportunity to review their use of DiD concepts in their regulatory activities, seeking to learn from other nuclear regulators in a spirit of continuous improvement and harmonisation.

To assist in the development of such an approach, a survey has been completed of the use of defence in depth among the regulatory bodies represented at the CNRA. It covers the main regulatory activities. These are: making regulations; producing guidance, codes of practice and regulatory assessment principles; assessment of designs, safety cases and events; inspections; and enforcement. The survey sought to identify how regulatory bodies promulgated the use of the DiD concept through training of their staff. It looked at whether DiD was used explicitly in a regulatory activity, and if so what relevant documents were used; whether there were any changes in its use after taking account of the lessons from the accident; and whether there was implicit use or explanation of its use. This latter aspect is of particular importance given the range of different regulatory systems for nuclear safety, from a prescriptive, detailed setting of regulations to goal setting around minimising risks. All such approaches are valid in their own

context when harmonised. While recognising their diverse nature, together they can provide a means of ensuring high levels of nuclear safety worldwide.

The results provide a useful basis for fostering increased attention by regulators to secure the use of DiD in ensuring high levels of safety. They illustrate the need to have a more universal understanding of the concept and principles of DiD, and a need for a greater harmonisation of approaches, if the best practices of securing DiD through regulation are to be achieved worldwide.

Additionally, in response to the Fukushima accident, regulators in many countries have enhanced their requirements for DiD, in particular in relation to levels 3, 4 and 5 of DiD.

4. Emergency arrangements and post-accident management off-site (DiD level 5)

This chapter provides specific guidance on DiD provisions at level 5 resulting from considerations following the accident in Fukushima.

Basis for emergency planning

Emergency planning and resource allocation are based on reasonably credible scenarios, while the actual emergency response has to respond to the real situation, which in general is extremely uncertain initially. Nuclear emergency plans must therefore be flexible, and able to be extended to beyond reasonably credible scenarios (i.e. there should be no cliff edge aspects to the emergency plans). Emergency preparedness should be based on a well trained system of response with timely and robust technical support, adequate procedures for radiation protection and countermeasures, and a smooth communication system for national and international use. Training has to take account of such extendibility, especially the potential long-term nature of some nuclear accident scenarios, the particular potential for escalating scenarios at multi-unit sites and the general impact of an extreme external event off-site.

The off-site circumstances, such as those of the 2011 accident, illustrated how wide ranging external events (such as earthquakes, flooding or extreme weather), and the resulting infrastructure damage, can cause major complications to the off-site management of nuclear emergencies. Indeed, off-site centres may be inoperable. Alternative arrangements have to be pre-planned or hardened off-site centres provided. The movement of assessment teams, emergency teams and evacuees may be severely affected. Additionally, emergency management may have to deal with a series of other emergencies in addition to the nuclear emergency.

Decision making

One vital aspect of an effective emergency response is making timely and appropriate decisions. The roles and responsibilities of various decision makers should be clearly identified, and the structural aspects must be efficient and delegated appropriately down so as to enable rapid decisions. However, it has to be noted that, unlike other DiD levels, decision structures can be complicated and multi-layered, and will change over time (e.g. early: operator, nuclear safety authority, emergency management authority; medium term: safety authority, emergency management authority, stakeholders; long term: recovery authority,

stakeholders). Additionally, the nuclear safety regulators, their involvement and their responsibilities are likely to be different than those for other levels of DiD.

To aid decision making, emergency arrangements should include clear guidance and initial criteria developed in advance for the establishment and cessation of countermeasures, ensuring processes to take full account of stakeholder concerns. Moreover, reliable up-to-date plant information should also be established – to the extent possible under the circumstances – as a basis for decisions, although not to an extent that would delay timely decisions.

Countermeasures

Analyses of the health impacts of the 2011 accident demonstrate that discernible impacts from radiation exposure can be difficult if not impossible to quantify or even identify, given the low predicted impact against the background level of cancers. While such a conclusion is very accident-specific, accident-related stress impacts, and impacts due to evacuation, are more tangible. For example, there have been reports of considerable health impacts from the 2011 accident evacuation caused by such things as the forced movement of hospital patients with insufficient follow-up care. In addition, long-term stress health issues (e.g. increased childhood obesity, stress-driven illnesses) have been associated with such accidents. This illustrates that pre-accident planning and post-accident decision making for off-site responses may be more complicated than previously considered in emergency arrangements. More consideration of the risks from implementing protective countermeasures, particular to vulnerable groups, may thus be warranted.

Decisions may be different for different groups and arrangements have to be in place to provide suitable care if such groups are not evacuated, or if they are. The level of prudence involved, particularly in addressing protection in early, extremely uncertain conditions, should be carefully considered. This has to be balanced against the need at the time to make decisions against a background of uncertainty, particularly with regard to the level of radioactive release over a given area and over a given time. In some circumstances, cross-border co-ordination of protective actions during the early phase of a nuclear accident is necessary.

Communication

Of prime importance is the ability to ensure timely and effective communication with the public and other stakeholders, especially those who may be affected by countermeasures or who may perceive that they could be risk. Such communications must be understandable, clear, as up to date as possible, open and honest, and communicated using different channels understanding the possibilities and challenges of social media. It is most effective if such communications are built upon a prior, longer-term interaction with relevant stakeholders about the site and radiological risks.

The global interest and response to large-scale accidents, such as the Chernobyl and the Fukushima Daiichi accidents, illustrates that emergency arrangements have to take into account the information needs of foreign governments, overseas nuclear regulators and international organisations. Once radioactive releases occur, international communications and consultations become even more significant.

Foreign governments will have to make many decisions such as on whether radioactive plumes will significantly contaminate their country; on whether to take protective action for their citizens in the affected area to arrange transport for people who wish to return home, for example; on imports from the affected area; on trade issues. Thus, emergency arrangements normally have to include the ability to provide information:

- in English language;
- in real time;
- covering a wide range of topics concerning governmental decisions, including rationale and judgements.

Interactions with the recovery phase

It has been noted that although there have thus far been no discernible health impacts from the Fukushima Daiichi NPP radiological releases – in view of effective countermeasures implemented in Japan – a nuclear accident could have significant radiological impacts on health, and even without can have extensive far-reaching social and economic impacts, particularly on the environment. The recovery phase is intimately connected to level 5 emergency arrangements, although not formally a part of them, as it involves a shift of roles and responsibilities. Level 5 emergency management arrangements have to be closely co-ordinated with recovery plans and implementation so as to ensure continuity and complementarity in decisions.

Recovery approaches need to be established as part of the pre-planning phase and must comprise considerable stakeholder input and involvement based on trusted relationships. This will require considerable effort and structured processes that may be established in regulations for consultation. In order to ensure the effective involvement of stakeholders, including local municipal officials and the public, considerable information in a suitable form must be provided. Given the fortunate rareness of significant off-site nuclear emergencies, pre-accident stakeholder involvement and communication has to be maintained over long periods.

The basis of effective off-site emergency arrangements and recovery will be the trust of the public and other stakeholders. Post-accident trust in nuclear safety and recovery authorities is fragile after an accident. Pre-accident efforts and post-accident focus on transparency are important aspects of nuclear emergency planning and recovery programmes.

Interactions of authorities, response teams and other stakeholders

The individuals and authorities involved in establishing protective measures on the site in relation to DiD levels 1 to 4 may be different from those involved in establishing and implementing level 5 off-site countermeasures. There needs to be effective communication to promote common and appropriate understanding and balance among the various levels, noting that in some cases terms are used differently. There should at least be a recognition of legitimate differences and, if possible, some broad agreement on a common view.

5. Conclusions

DiD as a concept has been used for many years, along with other tools, to optimise nuclear safety in reactor design, assessment and regulation.

The use of the DiD concept remains valid after the Fukushima Daiichi accident. Indeed, lessons learnt from the accident and its impact on the use of DiD has reinforced its fundamental importance in ensuring adequate safety. This is illustrated by the recent Vienna Declaration on Nuclear Safety adopted by the contracting parties of the Convention on Nuclear Safety on 9 February 2015 (IAEA, 2015).

Consideration of the accident has led to further work on DiD implementation, in particular on:

- reinforcing the need for independent effectiveness among the safety provisions for the various DiD levels, to the extent practical;
- emphasising the vital importance of ensuring that common cause and common mode failures, especially external events acting in combination, do not lead to breaches of safety provisions at several DiD levels;
- illustrating that greater attention is needed to reinforce prevention and mitigation at the various levels, particularly level 4;
- using the concept of practical elimination of sequences leading to significant radioactive releases;
- reinforcing the importance of assessments on the impact of human and organisational factors on DiD;
- providing useful insights into the issues associated with level 5 provisions (emergency arrangements) especially for long-term and multi-unit nuclear accidents, noting that the authorities and players involved are generally different.

This regulatory guidance booklet provides advice for regulators in all these areas of DiD implementation.

The results of the survey on the regulatory use of DiD emphasises that greater harmonisation is needed in the understanding and implementation of DiD in its present form. This booklet is intended to assist in achieving this aim, including through benchmarking and training.

Finally, this regulatory guidance booklet identifies areas where further work may be beneficial, such as on:

- the impact of human and organisational factors on DiD;
- improvements in the use of the DiD concept for new reactor designs, multi-unit sites, fuel cycle facilities and research reactors;
- the implementation of arrangements for level 5 of DiD;
- benchmarking and further harmonisation of the regulatory use of DiD through training, workshops and other means;
- the impact of new technologies.

6. References

IAEA (2015), "Vienna Declaration on Nuclear Safety", INFCIRC/872, IAEA, Vienna, www.iaea.org/sites/default/files/infcirc872.pdf.

IAEA (2013), "International Conference on Topical Issues in Nuclear Installation Safety: Defence in Depth – Advances and Challenges for Nuclear Installation Safety", 21-24 October 2013, Vienna.

IAEA (2012), *Safety of Nuclear Power Plants: Design,* Safety Standard SSR 2/1, IAEA, Vienna.

IAEA (2006), *Fundamental Safety Principles*, Safety Fundamentals No. SF-1, IAEA, Vienna.

IAEA (1996), *Defence in Depth in Nuclear Safety*, INSAG-10, IAEA, Vienna.

IAEA (1992), *Probabilistic Safety Assessment*, Safety Series No. 75-INSAG-6, IAEA, Vienna.

NEA (2014), "NEA/CNRA/CSNI Joint Workshop on Challenges and Enhancements to Defence in Depth (DiD) in Light of the Fukushima Daiichi NPP Accident: Workshop Proceedings", NEA/CNRA/R(2014)4.

WENRA (2013), "Report: Safety of New NPP Design", study by WENRA RHWG, www.wenra.org/media/filer_public/2013/04/30/rhwg_safety_of_new_npp_designs.pdf.

Appendix 1
List of abbreviations and acronyms

AOO	Anticipated operational occurrences
CNRA	Committee on Nuclear Regulatory Activities
CSNI	Committee on the Safety of Nuclear Installations
CRPPH	Committee on Radiation Protection and Public Health
DEC	Design extension conditions
DiD	Defence in depth
I&C	Instrumentation and control
IAEA	International Atomic Energy Agency
INSAG	International Nuclear Safety Advisory Group
NEA	Nuclear Energy Agency
NPP	Nuclear power plant
PSA	Probabilistic safety assessment
SSC	Systems, structures and components
STG	Senior-level task group
WENRA	Western European Nuclear Regulators Association

Appendix 2

Complete list of the NEA series of regulatory guidance reports ("Green Booklets")

1	1999	*The Role of the Regulator in Promoting and Evaluating Safety Culture*
2	2000	*Regulatory Response Strategies for Safety Culture Problems*
3	2001	*Nuclear Regulatory Challenges Arising from Competition in Electricity Markets*
4	2001	*Improving Nuclear Regulatory Effectiveness*
5	2002	*The Nuclear Regulatory Challenges in Judging Safety Backfits*
6	2002	*Improving versus Maintaining Nuclear Safety*
7	2003	*The Regulatory Challenges of Decommissioning Nuclear Reactors*
8	2003	*Nuclear Regulatory Review of Licensee Self-assessment (LSA)*
9	2004	*Nuclear Regulatory Challenges Related to Human Performance*
10	2004	*Direct Indicators of Nuclear Regulatory Efficiency and Effectiveness: Pilot Project Results*
11	2005	*Nuclear Regulatory Decision Making*
12	2006	*Regulatory Challenges in Using Nuclear Operating Experience*
13	2008	*The Regulatory Goal of Assuring Nuclear Safety*
14	2011	*The Nuclear Regulator's Role in Assessing the Licensee Oversight of Vendor and Other Contracted Services*
15	2012	*Challenges in Long-term Operation of Nuclear Power Plants: Implications for Regulatory Bodies*
16	2014	*The Characteristics of an Effective Nuclear Regulator*
17	2016	*Implementation of Defence in Depth at Nuclear Power Plants: Lessons Learnt from the Fukushima Daiichi Accident*
18	2016	*The Safety Culture of an Effective Nuclear Regulatory Body*

NEA PUBLICATIONS AND INFORMATION

The full **catalogue of publications** is available online at www.oecd-nea.org/pub.

In addition to basic information on the Agency and its work programme, the **NEA website** offers free downloads of hundreds of technical and policy-oriented reports.

An **NEA monthly electronic** bulletin is distributed free of charge to subscribers, providing updates of new results, events and publications. Sign up at www.oecd-nea.org/bulletin/.

Visit us on Facebook at www.facebook.com/OECDNuclearEnergyAgency or follow us on **Twitter** @OECD_NEA.

OECD/NEA PUBLISHING, 2 rue André-Pascal, 75775 PARIS CEDEX 16

Implementation of Defence in Depth at Nuclear Power Plants

Defence in depth (DiD) is a concept that has been used for many years alongside tools to optimise nuclear safety in reactor design, assessment and regulation. The 2011 Fukushima Daiichi nuclear power plant accident provided unique insight into nuclear safety issues and raised questions about the tools used at nuclear power plants, including the effectiveness of the DiD concept, and whether DiD can be enhanced and its implementation improved.

This regulatory guidance booklet examines and provides advice on the implementation of DiD. A key observation is that the use of the DiD concept remains valid after the Fukushima Daiichi accident. Indeed, lessons learnt from the accident, and the accident's impact on the use of DiD, have reinforced the fundamental importance of DiD in ensuring adequate safety.

This report is intended primarily for nuclear regulatory bodies, although information included herein is expected to be of interest to licensees, nuclear industry organisations and the general public.

Nuclear Energy Agency (NEA)
46, quai Alphonse Le Gallo
92100 Boulogne-Billancourt, France
Tel.: +33 (0)1 45 24 10 15
nea@oecd-nea.org www.oecd-nea.org

NEA No. 7248