IAEA-TECDOC-986

Implementation of defence in depth for next generation light water reactors

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

December 1997

The IAEA does not normally maintain stocks of reports in this series. However, microfiche copies of these reports can be obtained from

INIS Clearinghouse
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

Orders should be accompanied by prepayment of Austrian Schillings 100,— in the form of a cheque or in the form of IAEA microfiche service coupons which may be ordered separately from the INIS Clearinghouse.

IAEA-TECDOC-986

Implementation of defence in depth for next generation light water reactors

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

The originating Section of this publication in the IAEA was:

Engineering Safety Section
International Atomic Energy Agency
Wagramerstrasse 5
P.O. Box 100
A-1400 Vienna, Austria

IMPLEMENTATION OF DEFENCE IN DEPTH FOR
NEXT GENERATION LIGHT WATER REACTORS
IAEA, VIENNA, 1997
IAEA-TECDOC-986
ISSN 1011–4289

Printed by the IAEA in Austria
December 1997

FOREWORD

The publication of this IAEA technical document represents the conclusion of a task, initiated in 1995, devoted to defence in depth in future reactors. It focuses mainly on the next generation of LWRs, although many general considerations may also apply to other types of reactors.

The IAEA is grateful to the experts who contributed to this publication. The officer of the IAEA responsible for the TECDOC was M. Gasparini of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

In preparing this publication for press, staff of the IAEA have made up the pages from the original manuscript(s). The views expressed do not necessarily reflect those of the IAEA, the governments of the nominating Member States or the nominating organizations.

Throughout the text names of Member States are retained as they were when the text was compiled.

The use of particular designations of countries or territories does not imply any judgement by the publisher, the IAEA, as to the legal status of such countries or territories, of their authorities and institutions or of the delimitation of their boundaries.

The mention of names of specific companies or products (whether or not indicated as registered) does not imply any intention to infringe proprietary rights, nor should it be construed as an endorsement or recommendation on the part of the IAEA.

CONTENTS

1. INTRODUCTION

1.1. BACKGROUND

An extensive programme on the safety of future reactors has been conducted at the IAEA since 1991, following recommendations of the General Conference. A first task, aimed at preparing safety objectives and principles for future reactors, has been completed, and the results of the work have been published in the IAEA-TECDOC-801, Development of Safety Principles for the Design of Future Nuclear Power Plants [1]. This report has been received by the nuclear community with great interest and has provoked considerable discussion. As recommended by the General Conference, the preparation of TECDOC-801 was based on the prior work of the International Nuclear Safety Advisory Group (INSAG). The report INSAG-3, Basic Safety Principles for Nuclear Power Plants [2], was used as the basis for developing safety principles for nuclear plants of the next generation. TECDOC-801 is now being considered as a reference for the revision of the IAEA's Nuclear Safety Standards (NUSS) for Nuclear Power Plants (NPPs).

The substantial innovation proposed in TECDOC-801 includes the explicit consideration of severe accidents in the design of future NPPs, together with the minimization of off-site effects in the event of a severe accident. This report, together with other factors discussed in the following, suggested the need for continuing discussion of several aspects of the safety approach to future NPPs, including further work on the concept of defence in depth.

The importance of defence in depth as a fundamental strategy to achieving safety has been reaffirmed several times and is not under discussion. INSAG has recently prepared a report, INSAG-10, Defence in Depth in Nuclear Safety [3], which suggested a more structured interpretation of the concept of defence in depth, compared with the traditional meaning as outlined in INSAG-3. INSAG-10 presents defence in depth in general terms, with only a small part (Section 5) devoted to future reactors. The present report, specifically focused on future reactors, builds on and is consistent with INSAG-10, which was available in draft form during the preparation of this report.

For future reactors, the new safety principles, the emergence of new technologies, the indications from operating experience and variations in safety trends and expectations for future plants from country to country all indicate the importance of improving the current guidance on how the defence in depth concept will be implemented. This report therefore includes a discussion of the balance between prevention and mitigation, and how efforts to achieve a higher standard of safety for future plants will be distributed among the five levels of defence in depth.

Both INSAG-10 and TECDOC-801 have been used extensively in preparing this report. Definitions of terms used in this report are based on those provided in TECDOC-801.

1.2. PURPOSE AND SCOPE

There is general agreement that severe accidents should be considered in the design of future NPPs. Great effort has been devoted at the IAEA in this area, with the aim of providing a basis or framework for identifying those accidents beyond the design basis that are expected to be explicitly addressed in the design of future NPPs, and which should serve as a basis for preventive or mitigatory features in the plant to meet those safety and radiological objectives generally agreed upon for future NPPs.

The need to present these innovative elements from TECDOC-801, in the context of INSAG-10, represents one of the most important reasons for preparing a specific document on defence in depth for future NPPs. The information coming from the continuously growing base of operating experience also contributes to new considerations for implementing defence in depth in future NPPs.

It was recognized by the authors that the implementation of defence in depth is design-specific, and is also influenced by individual Member States' safety policies and regulations. This report has mainly focused its attention on the next generation of LWRs.

Section 2 of this report presents a general description of the application of the principle of defence in depth which is taken directly from INSAG-10 with some changes of text, on the basis that most of the safety considerations for existing nuclear plants remain valid for future plants.

The objective of this work was to bring together the relevant aspects of the existing publications on both defence in depth and future reactor designs, and then to apply recent defence in depth formulations specifically to ongoing developments in future plant designs.

Section 3 of this report therefore provides a review of the five levels of defence in depth listed in INSAG-10, in the context of TECDOC-801, identifying areas of particular interest and importance for future reactor designs. For completeness, some examples taken from well known advanced designs which are now under development or construction are included in this report.

1.3. FUTURE REACTORS (DEFINITIONS)

On a worldwide scale, several concepts for future reactors are being considered or implemented. The various proposed and completed advanced designs differ considerably with regard to technical details, plant size, and time scale for commercial application. With respect to the term 'future reactors', there is no overall consensus on which of the advanced designs currently under development or in construction are considered 'future reactors' for purposes of applying new guidance, such as in TECDOC-801 and this report. In IAEA-TECDOC-936, Terms for Describing New, Advanced Nuclear Power Plants [4], 'future reactor' is defined as a primarily time related term that generally refers to reactors that have not yet been built. For the purpose of this report, the terms 'future reactors' and 'new generation reactors' are used interchangeably.

A more complete description of this evolution of designs leading to reactors with enhanced safety characteristics is presented in TECDOC-801. The advanced reactor designs of TECDOC-801 are those that have benefited from the lessons of recent operational experience, research and development (R&D), design, testing and analysis which has been performed over the last decade or so. Advanced plants are expected to conform to the enhanced safety targets of INSAG-3 and TECDOC-801. Practically speaking, most of the advanced designs that have been developed in this decade have embraced most of the emerging guidance on future reactors.

Although there is in reality a continuum in the evolution of advanced reactors that makes a clear classification of current and future plants difficult, INSAG-10 [3] distinguishes two basic approaches to future reactor designs, evolutionary and innovative:

- The first approach basically aims at design improvement through an evolution of currently operating plants, taking into account the results from safety research and plant operation. This approach makes maximum use of proven technology and operating experience, but may nevertheless include new safety features, some of which can be passive. Within this category are "large evolutionary" plants, typically water cooled, which require no prototype for proof of performance, and which are expected to be available for commercial application within the next few years. This category also includes mid-size LWR designs, based primarily on proven technology but incorporating to a greater extent new passive safety features that can be separately tested (and therefore do not require prototype testing).

- The second approach implies more fundamental changes compared with present designs, often with strong emphasis on specific passive features protecting the fuel integrity and thereby preventing potential core damage. Owing to the nature and capability of those passive features, such innovative designs are mostly of smaller power output. For these plants, substantial R&D, feasibility tests and a prototype or demonstration plant are probably required.

These categories are regarded as helpful to understanding. It is important to recognize that new generation designs which might be realized in the near future are more likely to be well developed large or mid-size evolutionary plants that do not require prototype demonstration. Hence, they deserve more immediate attention. Long term designs are less well developed and are typically based on less proven concepts. This report is not directly applicable to these less proven design concepts because it is focused on next generation technology. It should be noted that substantial effort and consensus will be needed to adapt defence in depth to some of these advanced concepts, since many of them are based on design approaches that attempt to achieve higher confidence in the lower levels of defence (e.g. fuel integrity), so as to relax or eliminate requirements for higher levels (e.g. no pressure-tight containment).

1.4. GENERAL APPROACH TO DEFENCE IN DEPTH FOR FUTURE REACTORS

An important consensus on how defence in depth should be achieved for future reactors has already emerged from TECDOC-801 and the work of INSAG. TECDOC-801 and INSAG-10 both emphasize improvements in future designs that would result in a much higher assurance of accident prevention, a better mitigation of accidents (particularly those that could lead to early containment failure), and a more explicit consideration throughout of accident sequences beyond the standard design basis.

An important implication of these safety improvements for future plants, as presented in TECDOC-801, INSAG-10 and the work to date on a potential revision to INSAG-3, is that safety will be improved at each of the defence in depth Levels 1–4, resulting in much lower off-site consequences from an accident — much lower in likelihood, in severity, in need for rapid response and in the size of the area around the plant that could be affected by an accident. As a result, both TECDOC-801 and INSAG recognize that the strengthening of the earlier barriers and levels of defence in depth may be used to reduce or even eliminate the need for most of the off-site features that relate to emergency planning. Nevertheless, both documents recognize the need to retain an off-site emergency response capability as a prudent final level of defence in depth. They agree that this final level must include proper planning, but may involve simplification of the features and actions to be taken.

2. THE DEFENCE IN DEPTH APPROACH

2.1. OBJECTIVES OF DEFENCE IN DEPTH

INSAG's Nuclear Safety Objective, to which defence in depth contributes, is to ensure the protection of workers and the public from risks arising from the operation of nuclear power plants. The term defence in depth refers to the creation of multiple successive levels of overlapping provisions, each of which has the independent objective of stopping the progression of a fault which has already evolved because of the failure of a lower (or earlier) level.

Defence in depth is implemented through design and operation to provide a graded protection against a wide variety of transients, abnormal occurrences and accidents, including equipment failures and human error within the plant, and events initiated outside the plant.

INSAG-3 provides for implementation of defence in depth with the following objectives:

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

INSAG-10 provides a more structured interpretation of the concept, suggesting four specific barriers against the release of fission products and five specific levels of defence in depth to fully exploit these redundant barriers.

The fundamental approach for defence in depth is similar for existing and for future plants. However, for future plants it is achieved in a more systematic and comprehensive manner, with greater emphasis on the earlier barriers and lower levels.

2.2. THE BARRIERS

The protection of the public and of the environment is primarily accomplished by means of barriers, the effectiveness of which should in principle never be jeopardized. These physical barriers are generally set to provide confinement of radioactive material at different locations, depending on their activity, and on the possible deviations from normal operation that could imply the failure of some barriers. Typically, at power operation, the barriers enclosing the fission products in water reactors are:

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

The defence in depth concept applies to both the provision of and protection of these barriers. The barriers may serve operational and investment protection purposes, as well as safety purposes, or safety purposes exclusively. The proper integrity of barriers should be maintained and ensured at all times. Situations in which barriers are taken out completely for a particular activity (e.g. during refuelling shutdown) require special attention. Situations in which the redundancy or diversity of protection provided by a barrier is temporarily reduced (e.g. on-line maintenance of a redundant train) also require special attention.

2.3. GENERAL STRATEGY FOR DEFENCE IN DEPTH: THE LEVELS

The general strategy of defence in depth is twofold: to prevent abnormal events and incidents, and if this fails, to mitigate their potential consequences and to prevent progression to a more severe condition. Prevention is the first priority. The basic rationale for this priority is that provisions to prevent deviations of the plant state from well known operating conditions are generally more effective and more predictable than measures aimed at mitigation of the consequences of such a departure. This is because plant performance often deteriorates when the status of a system or a component departs from normal conditions, and therefore becomes more difficult to predict. Moreover, emphasis on this first priority is fully consistent with optimum protection of public health and safety, optimum protection of the plant investment and earliest return of the plant to service.

Thus, preventing degradation of plant status and performance will provide the most effective protection of the public and the environment, as well as of the productive capability of the plant. On the other hand, mitigatory measures, in particular a well designed containment function, provide additional protection for the public and the environment, and would be called for should preventive measures fail.

The defence in depth concept is generally structured in five levels, as outlined in Table I of INSAG-10, which is reproduced below.

TABLE I. LEVELS OF DEFENCE IN DEPTH (from INSAG-10)

Levels 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 fundamental principle of defence in depth is that should one level fail, the subsequent level is necessarily invoked. The objective of the first level of defence is prevention of abnormal operation and system failures. If this level fails, failures are detected

and abnormal operation is controlled at the second level of defence. Should the second level fail, the third one ensures that safety functions are performed to prevent core damage by activating specific engineered safety systems. Should the third level fail, the fourth level limits further accident progression through design features and accident management procedures developed to prevent or mitigate severe accident conditions. The last objective (fifth level of defence) is mitigation of radiological consequences of significant off-site releases through off-site emergency response.

Table I was reviewed carefully, in the light of TECDOC-801 and Section 5 of INSAG-10. Certain extensions of the above objectives and essential means particularly for Levels 1 to 4, were identified that are being considered for future NPPs. These extensions and clarifications are presented later in the specific discussions of each level, and in a new proposed table which summarizes the means of implementing defence in depth and evaluating its achievement.

An effective implementation of defence in depth needs support from certain prerequisites which apply to all measures considered at Levels 1 to 5. The IAEA Safety Fundamentals, Safety Series No. 110 [5], and INSAG-3 both note the importance of a number of general technical principles and related measures which assure the reliability or fidelity of the means of achieving the objectives. These measures include:

- reliance on proven engineering practices;
- conservative design margins (e.g. to address uncertainty);
- classification and qualification of structures, systems and components;
- appropriate quality assurance (QA) commensurate with the safety classification of structures, systems and components;
- general engineering quality for all aspects of the design, through construction and operation;
- safety assessment, including verification;
- hazard provisions such as diversity, segregation and barriers for external events and other common-cause threats;
- operational and maintenance practices, including provision for lessons from operating experience;
- safety culture and human factors;
- provisions for ensuring the accountability of the operating organization and the independent role of regulatory bodies.

These measures are generally applicable to all of the levels and they act together with specific design provisions to ensure the integrity of the physical barriers.

INSAG-10 considered three of the above measures to be sufficiently important to be highlighted as "basic prerequisites" due to their applicability and impact at all levels. These are: appropriate conservatism, quality assurance, and safety culture.

Appropriate conservatism

Conservatism is broadly applied in the design at the first three levels of defence. Conservative assumptions are made for site selection, design and construction, commissioning and operation. Appropriate conservative assumptions and safety margins are also considered in the review of modifications, the assessment of ageing effects, periodic safety reassessment and the development of emergency plans, as well as in regulatory review and subsequent licensing decisions. At Levels 4 and 5, best estimate considerations are increasingly important.

The degree, rigour and formality of conservatism are most evident at Level 3. Although conservatism is broadly applied to the design process at Levels 1 and 2, assessments of that conservatism are performed where possible with realistic assumptions, data and models.

Future plants are likely to adhere quite rigorously to the principle of using best estimate analysis for Levels 4 and 5, while maintaining appropriate conservatism in the safety analysis at lower levels, particularly Level 3. This is because in future plants, an important distinction is made between conservatism in plant design margins and in subsequent assessments of those margins. In general, conservative design margins are used throughout, in order to achieve the goals of improved safety, simplicity, longer design life, etc. However, with the advances in knowledge provided by research, testing, improved computer models, operating experience data, etc., many uncertainties in plant behaviour, ageing effects, and the like, are being removed. This enables a reduction in the use of intentionally conservative or bounding assumptions in the safety analysis of the design, where justifiable and where allowed by the relevant codes, standards, and regulations.

Quality assurance

Each level of defence can be effective only if it can rely upon quality of design and materials, quality of structures, systems and components, and quality of operations and maintenance. Quality assurance programmes are used first to ensure development of a safe design (including site evaluation, design of process and safety systems, design of barriers, design of modifications and safety analysis), secondly to ensure that the plant as built achieves the intent of such design, and thirdly to ensure that the plant is operated as intended and maintained as designed.

Safety culture

Organizations and individuals involved in activities which may have an impact on each level of defence need to be committed to a strong safety culture (see INSAG-4, Safety Culture). The operating organization and the governmental organization, as well as organizations involved in design, manufacturing, construction, maintenance, testing and in-service inspection must ensure that appropriate methods are used. This also applies to assistance from other outside organizations (e.g. as in emergency interventions).

2.4. DESCRIPTION OF THE LEVELS OF DEFENCE IN DEPTH

As already outlined in Table I from INSAG-10, the measures relative to defence in depth are generally organized in five levels. This section expands on the table and the descriptions of each level in INSAG-10 to explicitly address the implementation of defence in depth for future plants.

According to INSAG-10, the first four levels of defence are directed towards the protection of barriers and mitigation of releases; the last level relates to off-site emergency measures that protect the public in the event of a significant release. Even though implementation of the concept of defence in depth may differ from country to country and may to a certain degree depend on plant design, the main principles are commonly accepted.

2.4.1. Level 1: Prevention of abnormal operation and failures

Measures at Level 1 include a broad range of conservative provisions in design, from siting through to the end of plant life, aimed at confining radioactive material and minimizing deviations from normal operating conditions (including transient conditions and plant

shutdown states). The safety provisions at Level 1 are made through the choice of site, and through requirements for design, manufacturing, construction, commissioning, operations and maintenance, such as:

- the clear definition of normal and abnormal operating conditions;
- adequate margins in the design of systems and plant components, including robustness and resistance to accident conditions, in particular aimed at minimizing the need to take measures at Level 2 and Level 3;
- inherent plant features such as neutronic and thermohydraulic core stability, and thermal inertia;
- provision in the design for adequate time for operators to respond to events; and appropriate human–machine interface design, including operator aids, to reduce the burden on the operators;
- careful selection of materials and use of qualified fabrication processes and proven technology, together with extensive testing;
- comprehensive training of appropriately selected operating, maintenance, engineering, and management personnel whose behaviour is consistent with a sound safety culture;
- adequate operating instructions and reliable monitoring of plant status and operating conditions;
- recording, evaluation and utilization of operating experience;
- comprehensive preventive maintenance, prioritized in accordance with the safety significance and reliability requirements of systems.

Furthermore, Level 1 provides the initial basis for protection against those external and internal hazards relevant to the design or site (e.g. earthquakes, fire, flooding), even though some additional protection may be needed at higher levels of defence.

2.4.2. Level 2: Control of abnormal operation and detection of failures

Level 2 incorporates systems to control abnormal operation (anticipated operational occurrences), with account taken of phenomena capable of causing further deterioration in plant status. The systems to mitigate the consequences of such operating occurrences are designed according to specific criteria (such as redundancy, layout and qualification). The objective is to bring the plant back to normal operating conditions as soon as possible.

Diagnostic tools and equipment such as automatic control systems can be provided to actuate corrective actions before reactor protection limits are reached; examples are power operated relief valves, automatic limitations on reactor power and on coolant pressure, temperature or level, and process control systems which record and announce faults in the control room. Ongoing surveillance of quality and compliance with the design assumptions, by means of in-service inspection and periodic testing of systems and plant components, is also provided to detect any degradation of equipment or systems before it can affect the safety of the plant.

2.4.3. Level 3: Control of accidents within the design basis

In spite of early provisions for prevention, accident conditions may develop. Engineered safety features and reactor protection systems are provided to prevent evolution towards severe accidents and also to confine radioactive materials within the containment system. The measures taken at this level are aimed in particular at preventing core damage.

Engineered safety features are designed on the basis of postulated accidents representing the limiting loads of sets of similar events. Typical postulated accidents are those originating in the plant, such as the breach of a reactor coolant pipe (a loss of coolant accident) or breach in a main steam line or feedwater line, or loss of control of criticality, such as in a slow uncontrolled boron dilution or control rod withdrawal.

Design and operating procedures are aimed at maintaining the effectiveness of the barriers, especially the containment, in the event of such postulated accidents. Active and passive engineered safety systems are used. Safety systems are actuated immediately by the reactor protection system when needed.

To ensure high reliability of the engineered safety systems, the following design principles are adhered to:

- redundancy;
- prevention of common mode failure due to internal or external hazards, by physical or spatial separation and structural protection;
- prevention of common mode failure due to design, manufacturing, construction, commissioning, maintenance or other human intervention, by diversity or functional redundancy;
- automation to reduce vulnerability to human failure, at least in the initial phase of an abnormal occurrence or an accident;
- test-friendly overall architecture to provide clear evidence of system availability and performance;
- qualification of systems, components and structures for specific environmental conditions that may result from an accident or an external hazard;
- reliability — essential ancillary and support systems are designed, manufactured, constructed, commissioned and operated consistent with the required reliability of engineered safety systems.

2.4.4. Level 4: Control of severe conditions including prevention of accident progression and mitigation of the consequences of a severe accident

For the concept of defence in depth as applied to currently operating plants, it is assumed that the measures considered at the first three levels will ensure maintenance of the structural integrity of the core and limit potential radiation hazards to members of the public. For future plants, additional specific provisions are made in both design and operations in order to further reduce residual risk. The broad aim of the fourth level of defence is to ensure that the likelihood of an accident entailing severe core damage, and the magnitude of radioactive releases in the unlikely event that a severe plant condition occurs, are both kept as low as reasonably achievable, economic and social factors being taken into account. Accident management is not used to excuse design deficiencies at prior levels.

Consideration is given to severe plant conditions that are not explicitly addressed in the deterministic design basis owing to their very low probabilities. Such plant conditions may be caused by multiple failures, such as the complete loss of all trains of a safety system, or by an extremely unlikely event such as a severe flood. Some of these conditions bear a potential that radioactive materials could be released to the environment. The increased margins and thermal inertia of future plants provide additional time to deal with some of these conditions by means of additional measures and procedures.

Measures for accident management[1] are aimed at preventing accidents, controlling the course of severe accidents and mitigating their consequences. In terms of core damage, accident management comprises both preventive and mitigatory measures. Essential objectives of accident management are:

- to monitor the main characteristics of plant status;
- to control core subcriticality;
- to restore heat removal from the core and maintain long term core cooling;
- to protect the integrity of the containment by ensuring heat removal, and by preventing dangerous loads on the containment in the event of severe core damage or further accident progression;
- to regain control of the plant, in order to prevent further plant deterioration.

The most important objective for mitigation of the consequences of an accident in Level 4 is the protection of the confinement. For most reactor designs there exists a containment structure which withstands pressure, with strict deterministic design basis limits on permissible leakage under a specified pressure. Functions that protect the containment, such as containment cooling and penetration control, are typically designed and analyzed to the same conservative standards as engineered safety features. Such design philosophy, established at Level 3, provides reasonable assurance of maintaining effective functioning of the containment under most severe plant conditions. Specific measures for accident management are established on the basis of safety studies and research results. These measures fully utilize existing plant capabilities, including available non-safety-related equipment. For example, any source of fresh water could be used in the event of loss of the ultimate heat sink in order to feed the secondary side of the steam generators. Measures for accident management can also include permanent features or temporary hardware connections. Examples are filtered containment venting systems and the inerting of the containment in boiling water reactors in order to prevent hydrogen burning in severe accident conditions. For such additional measures, specific design rules can be applied in a pragmatic way.

The role of the operators is vital in actuating hardware features for accident management and in taking actions beyond the originally intended functions of systems or in using temporary or ad hoc systems. Adequate staff preparation and training for such conditions is a prerequisite for effective accident management.

2.4.5. Level 5: Mitigation of the radiological consequences of significant external releases of radioactive materials

Even if the efforts described in the foregoing are expected to be highly effective in limiting the consequences of severe accidents (particularly so for future plants), it would still be inconsistent with defence in depth to dismiss off-site emergency plans. These plans cover the functions of collecting and assessing information about the levels of exposures expected to occur in such extremely unlikely conditions. They may also address possible short term and long term protective actions that might be judged to be prudent contingency plans, even though these actions are expected to be limited in time and area for future reactors.

---

[1]The term used depends on the country and the plant design: typical expressions are 'complementary measures', 'emergency procedures' and 'on-site accident management'. In the present text, the term 'accident management' is used.

Off-site emergency procedures are prepared in consultation with the operating organization and the authorities in charge, and must comply with international agreements. The responsible authorities take the corresponding actions on the advice of the operating organization and the regulatory body. Both on-site and off-site emergency plans are exercised periodically to the extent necessary to ensure the readiness of the organizations involved.

3. IMPLEMENTATION OF DEFENCE IN DEPTH

Section 3 describes the way the defence in depth principles presented in Section 2 are implemented in future designs. With respect to current plants, this implementation will continue to be accomplished primarily through deterministic analysis, probabilistic studies, and consideration of operational experience. As for future plants, explicit consideration of severe accidents is leading to additional design features and procedures.

3.1. DESIGN AND SAFETY ASSESSMENT

The process of design and safety assessment for future plants, from a defence in depth perspective, is depicted in Table II. This table is not intended to provide a complete picture of all aspects of implementation of defence in depth but only a general overview and an example to show how different factors affect each level.

3.1.1. Design process for Levels 1, 2 and 3

Future plants will be designed in accordance with a dual process that starts with the classical deterministic approach which accommodates a set of postulated events grouped into categories (e.g. anticipated operational occurrences, design basis accidents, or DBAs). This approach is complemented by a probabilistic safety analysis contribution to the design process. The deterministic analysis of these event groups and the design of the related Level 3 safety equipment is done using a combination of conservative assumptions, conservative design rules and conservative acceptance criteria.

Conservatism including safety margins is part of all these steps. It applies to the process of site selection, systems design, material specifications, quality requirements, qualification tests, acceptance criteria, commissioning tests, in-service surveillance and inspection requirements, technical specifications and safety assessment. Design considerations such as segregation, redundancy and single failure assumptions, and diversification where needed (e.g. for reactor trip initiation and actuation), provide a high degree of protection against potential functional failures.

The potential for common mode failures is reduced mainly through deterministic consideration of possible common mode failure sources such as internal or external hazards, through the implementation of an in-service test programme, and through functional diversification (see above) where appropriate. Probabilistic safety assessment (PSA) is also used to identify potential common mode failures and to assess their safety significance.

Other contributions to reducing common mode failures include:

- high quality and reliability by use of proven technology, high quality standards, appropriate safety margins, and an appropriate consideration of site characteristics (Level 1 of defence);

TABLE II. IMPLEMENTATION OF DEFENCE IN DEPTH FOR FUTURE NPP DESIGN AND SAFETY ASSESSMENT

Levels of defence in depth	Objective	Essential means	Category of representative events	Design response		Plant safety assessment	
				Systems/features	Design criteria	Assumptions and methods	Main acceptance criteria/ targets
1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation	Normal operation	Operational features incl. control, surveillance features	• Operational conditions • Robustness, design margins to meet all standards • High reliability	• Best estimate methods and data wherever possible • Conservative assumptions as necessary to address uncertainties	• Operational radiological limits • Safety Operating Limits
2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features	Anticipated operational occurrences (expected in the lifetime of the plant)	• Reactor protection system • Engineered safety features • Containment	• Redundancy (single failure) • Protection against specified internal/ external hazards • Test-friendly • Qualification • Design margins	• Bounding assumptions • Single failure criteria • Credit for safety-related equipment only	• Effectiveness/integrity of all barriers for confinement of radioactive material
3	Control of accidents within the design basis	Engineered safety features and accident procedures	Design basis accidents (not expected in the lifetime of the plant)				• Minor radiological consequences • Effectiveness of at least one barrier for confinement of radioactive material
4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management	Severe accidents without severe core damage	Additional or diverse features for core damage prevention	• Functional independence	• Best estimate (e.g. in-vessel and ex-vessel analysis, source terms, containment response, meteorology)	• Core damage frequency < $10^{-5}a^{-1}$ (target**)
			Severe accidents with severe core damage	Containment, core damage mitigation features	• Survivability		• Frequency of large offsite release < $10^{-6}a^{-1}$ (target**) • Other national criteria
5	Mitigation of radiological consequences of significant releases of radioactive materials	Offsite emergency response	NA	NA	NA	NA	NA

** Targets according to INSAG 3 and TECDOC 801.

- systems to prevent departure from normal operating conditions or to monitor any deviation and to restore the normal operating conditions (Level 2 of defence);
- safety systems to cope with postulated accidents and to prevent further degradation (Level 3 of defence).

3.1.2. Consideration of severe accidents in the design (Level 4)

PSA constitutes an effective design tool to gain an in-depth understanding of plant vulnerabilities, including complex situations involving several equipment and/or human failures. The results can be used in order to improve defence in depth. It is also a useful tool for optimizing the efforts and prioritizing the relative importance of various actions in defence in depth implementation.

For future plants, probabilistic studies are conducted from the beginning of the design process, in order to optimize the systems and later on to identify potential weaknesses and to check the overall design against probabilistic safety targets. This process is iterative and applied frequently until the end of the design process, in order to identify design weaknesses and vulnerabilities, often from common causes and interdependencies, and to enlighten the deterministic design process.

Based on these mainly probabilistic considerations, the design of future plants will also take into consideration a particular set of events (identified as beyond design basis events), for which the design should address both the prevention of core damage and also the mitigation of selected severe accident sequences involving core damage.

However, the expansion of the scope of events considered in the design to ensure a more comprehensive consideration of severe accident prevention and mitigation is not meant to imply that the same conservative design basis rules (such as those for DBAs) should apply to severe accident analyses or equipment. For those accidents beyond the design basis which need to be addressed, it is more appropriate to use engineering judgement, as well as best estimate analyses and acceptance criteria, in implementing these additional margins in the design. Likewise, redundancy, diversity and the quality of equipment can be different from that applied to design basis equipment. These different design criteria for events beyond the established deterministic design basis are appropriate because of the very low likelihood of such events, and because design basis accidents are considered with such large margins that they often overlap into accident sequences beyond design basis. Experience has demonstrated that it is important to use best estimate assumptions and analysis to reasonably characterize these low probability and sometimes uncertain event sequences.

A Technical Committee meeting (TCM) met in October 1995 to identify the severe accidents to be considered in the design of future NPPs. The draft conclusions of that meeting stated that low pressure core melt sequences should be addressed explicitly in the design, and that phenomena which could lead to early containment failure (such as steam explosion, H_2 detonation or high pressure core melt sequences) should be "practically eliminated" by design.

Severe accident sequences can be grouped for purposes of design in two categories: those that need to be explicitly addressed in the design (typically through both prevention and mitigation features); and those that, either because of their extremely low likelihood, or because they are based on unrealistic assumptions, are either discounted or are primarily addressed in the design through assurance of prevention (i.e. "practically eliminated"). The consideration and assignment of accident sequences in these categories is based on a

combination of best estimate deterministic analyses, probabilistic considerations and engineering judgement.

Both deterministic and probabilistic analysis methods and criteria are employed to aid in the selection of those accidents, including severe accidents, which are to be addressed in the design, and in decisions on the need for preventive and/or mitigative design features. Initial determinations in this selection process are made by the designers, taking into account the requirements of the users wishing to purchase the design, and the expectations of the national authorities. National authorities will then make final decisions based on various national procedures for assuring adequate protection of public health and safety and the environment. These national processes variously address these severe accident considerations.

Further, still according to the draft conclusions of the October 1995 TCM, it should be demonstrated that hypothetical severe accident sequences which could lead to large releases through early containment failure are essentially eliminated in the design with a high degree of confidence. This demonstration should be provided through deterministic and/or probabilistic means.

Also, credible severe accidents that could lead to late containment failure should be considered explicitly in the design process. This should include consideration of both prevention and mitigation, and should include a careful, realistic (i.e. best estimate) review of the confinement function and opportunities for improvement under such scenarios.

There are some aspects of plant safety which are difficult to assess either quantitatively or on a deterministic design basis. Examples include the influence of the operating organization and safety culture, as well as some aspects of common cause effects, software reliability, and some types of human error not well quantified by operating experience data. It is important for both plant designers and management to limit the influence of such aspects. Other examples include new technologies that have not been proven in reactor or other industrial usage, or otherwise lack operation experience feedback or test data.

3.1.3. Emergency response (Level 5)

Emergency planning also includes consideration of intervention measures such as addressed by ICRP 63 and IAEA-BSS. As discussed at the beginning of this report, special consideration should be given, for future reactors, to reducing the reliance on Level 5, which deals with mitigation of radiological consequences of significant off-site releases. Some of the historic provisions here could be reduced, due to improvement at all previous levels of defence; and because of improved testing, data and analysis of anticipated source terms, improved and more credible release and transport models, improved understanding of event timing, natural filtration phenomena, etc. TECDOC-801 discusses the rationale for improvements in this level of defence in greater detail. It reflects an international consensus that some basic level of planning and preparation for emergencies should be maintained, but that the size of evacuation zones and the specific actions required within these zones can be simplified. Each nation that builds a new generation reactor should review this question in the light of its particular situation.

3.1.4. Safety assessment and verification of defence in depth implementation

Basically, the verification process takes advantage of two complementary approaches, the deterministic and probabilistic methods. These methods have inherent and complementary

strengths and limitations. Demonstration of an efficient implementation of defence in depth requires their careful application, accounting for these strengths and limitations.

For Levels 1 to 3, the safety assessment is primarily deterministic and serves the purpose of proving that for the specified representative events, the radiological limits and the specified design criteria are met, considering dedicated systems, and — in general — conservative assumptions including the deterministic failure assumptions. For the analysis of operational features, it is appropriate to consider the application and use of best estimate methods and data, and to take conservative assumptions mainly where necessary to address uncertainties and where required by various codes, standards or regulations.

For accident situations without core damage, it should be possible to demonstrate that designs can obviate the necessity for protective measures for people living in the vicinity of a damaged plant (no evacuation, no sheltering). For those accident sequences involving potential core damage which have not been practically eliminated in the design, best estimate analysis should be used to demonstrate that only very limited protective measures in area and time would be needed.

A general consensus exists regarding the safety targets of INSAG-3 and TECDOC-801 for future plants, which for a probability of a severe core damage of below about 10^{-5} events per reactor operating year, and a probability of large off-site releases requiring short term off-site response, of about 10^{-6} events per reactor operating year.

3.1.5. Correlation of defence in depth and safety classification

As outlined in Table II, there is a certain correlation between the defence in depth levels and the classification of plant systems and features.

Safety systems according to the Code on the Safety of Nuclear Power Plants: Design (IAEA Safety Series No. 50-C-D, Rev. 1) contribute mainly to the control of anticipated operational occurrences and design basis accidents (defence in depth Levels 2 and 3). The safety assessment of representative events of these event categories should rely specifically on these safety systems, which are therefore subject to strong design requirements.

Operational systems are those systems which are mainly used during normal operation (defence in depth Level 1). They may also be helpful in defence in depth Level 2 as far as they contribute to control, surveillance and testing functions. Their classification depends on the various functions to be performed.

Design features that are provided to address severe accidents are not expected to meet the stringent design criteria and requirements applied to the engineered safety features to cope with design basis accidents, such as redundancy, diversity and conservative analysis and acceptance criteria. However, design features meant to address severe accidents are still engineered in a way which would give reasonable confidence that they are capable of achieving their design intent.

3.2. POTENTIAL COMMON FAILURES TO MULTIPLE LEVELS OF DEFENCE IN DEPTH

An important objective of the design process is to assure that a single equipment or human failure at one level of defence, or even combinations of failures at more than one

level, would not propagate to jeopardize subsequent levels of defence in depth. The independence of different levels of defence is a key element of this objective. If independent levels of defence are not feasible for the control of some events (e.g. sudden reactor vessel failure), specific stringent requirements are introduced in the design, construction, installation, commissioning and operation in order to practically eliminate that event. These measures may include for example: the use of sound design concepts and proven design features, the use of proven materials, the application of high standards of manufacture and construction including in-process inspection, high standards of quality assurance at all stages, pre-service and in-service inspection, provision of appropriate plant and materials monitoring, etc.

For future designs, efforts to identify and address factors which have the potential to affect multiple levels of defence in depth will continue This should provide high confidence that appropriate actions will be taken to ensure the effectiveness of defence in depth concept against failures that have the potential to impinge upon multiple levels of defence in depth.

3.2.1. Human failure

INSAG-3 states that the human error contribution to events has been too great in the past. Human errors are a potential source of impairment of defence in depth because human activity is involved at all levels of defence. Therefore, it is an objective that future designs are made more simple and straightforward to operate, and specific design provisions are being made in order to render these plants more tolerant to human failure, as well as to reduce the potential for human interference initiating abnormal plant conditions.

The following design improvements can contribute to reducing the potential of human failures:

- major system simplification through smarter design and greater inherent design margins that reduce the need for overly complex control systems and procedures;
- greatly improved human–machine interface with a priority on straightforward and unambiguous indications of plant parameters, simpler and more forgiving controls with direct feedback on results of actions taken;
- use of symptom based procedures to complement event based procedures;
- prolonged grace periods by provision of increased time constants for the reactor system or by a higher degree of automation.

Improvements currently being applied in future reactor designs should make these plants more operator friendly and reduce the potential for deterioration of defence in depth through human failure.

3.2.2. Internal and external hazards

Hazards of internal or external origin such as fires, flooding or earthquakes have the potential to initiate abnormal events, to adversely affect more than one barrier against release of radioactive material and — at the same time — to adversely affect design features provided for mitigating the consequences of such events. Measures against these hazards include the design and qualification of structures and components against the associated loads, as well as the introduction of barriers or spatial separation for protection purposes.

Future designs should ensure that potential hazard sources are identified and dealt with in a rigorous and systematic way in order to minimize the potential for deterioration of defence in depth. PSA has been particularly useful in providing a more systematic and risk-based approach to assessing these hazards and their importance, while they nevertheless remain primarily within the deterministic part of the design process.

3.2.3. Containment bypasses

Defence in depth requires that radiological barriers fulfil their barrier function independent of each other. Recently, the potential for residual weaknesses in the containment barrier has received renewed attention because of the desire to further reduce the potential for early failures or bypasses of this barrier. Efforts have focused mainly on containment penetrations. For future designs, it is important to minimize the potential for containment bypasses. Areas of focus are:

- optimization of equipment placement (i.e. inside/outside the containment), specifically the location of refuelling and safety injection water storage, residual heat removal (RHR) systems, pressure transmission lines connected to the primary system, etc.;
- improvement of the steam generator tube reliability and rupture prevention for PWRs, along with consideration for mitigation strategies for steam generator tube rupture;
- improvement in the prevention of V-LOCA (LOCA outside the containment) conditions.

3.3. OPERATIONAL SAFETY

3.3.1. Operating experience

Feedback of operating experience provides an important tool to ensure proper consideration of risk initiators and design response and assists in achieving a consistent defence in depth for the design of future plants.

3.3.2. Operating procedures

The normal operating procedures address limits and conditions set by the design. These procedures cover Levels 1 (and 2) of defence in depth, and also shutdown conditions. Emergency operating procedures are set up to cope with abnormal operating conditions and accident conditions, and are part of both Level 2 and Level 3 defence.

Beyond the emergency operating procedures, accident management guidelines provide special emergency procedures aimed at the prevention and mitigation of core damage. If the engineered safeguards explicitly provided for design basis accident situations have failed, or have been confronted with situations beyond their design basis capability (multiple failures, etc.), these accident management procedures provide extended protection at Level 4 of defence in depth.

The use of so-called symptom based procedures (or physical state oriented procedures), which complement event based procedures applicable to normal and abnormal operation, is a well established course of action in the area of accident management.

Event based procedures are based on a preventive strategy for specific abnormal occurrences and single design basis accidents. Their limitation lies in the fact that the real accident does not necessarily match with the assumed sequence of events and analysis made

in advance. A potential consequence of event based procedures is operator confusion and mistakes as, for example, in the Three Mile Island event in the USA in 1979.

The state or symptom oriented procedures are, in contrast, based on various anticipated situations that might develop during the course of the accident, guided by indications such as thermohydraulic parameters and other instrument readings on the state of the system. Decisions do not require examination of the initial causes of events leading to this state. Symptom based procedures are understandable and applicable to a much larger combination of situations and events. Operating experience has provided the basis and motivation for this important change in procedure writing. It has been applied to many existing plants, and is an integral part of the design and procedure development of future reactors.

3.3.3. Maintenance and plant ageing

The prevention of safety significant degradation of equipment is a basic objective of a maintenance policy. In order to achieve the overall goals of future plants policy, maintenance and ease of maintenance should be taken into account from the beginning of the design process.

It is essential that potential ageing mechanisms are considered at the design stage in order to guide the establishment of conservative safety margins necessary to allow for the effects of time dependent degradation. Particular consideration should be given to those safety related components or systems which may be difficult or impracticable to replace. In-service monitoring programmes should also be provided, with the objective of verifying that the design assumptions remain valid throughout the working life of the plant.

Selection of materials which have known ageing tolerant characteristics is another well established means by which confidence in lifetime plant reliability can be improved.

Other measures to be taken into account in dealing with ageing include improved reliability centred maintenance practices, ease of system or component replacement, enhanced equipment diagnostic techniques, and improved maintenance methods.

3.4. NON-POWER STATES

Recently, there has been increased emphasis on consideration of non-power states. INSAG-3 and INSAG-10 state that during normal power operation, all levels of defence should be available at all times. During other plant conditions an appropriate number of levels must be available in order to maintain an adequate level of safety. This is because, during certain shutdown conditions, radiological barriers may be made ineffective (e.g. reactor coolant pressure boundary, containment) for operational or maintenance reasons. Future plants will ensure that the principle of defence in depth can be implemented appropriately during those specific shutdown conditions. Specifically, future designs have explicitly addressed safety in non-power states, primarily through improved defences at Level 1, that reduce the probability and safety significance of loss of decay heat removal events. This is often a design specific determination.

3.5. PROPOSED TECHNICAL IMPROVEMENTS

Some of the possible improvements now under consideration by designers of future plants are described and discussed below, by way of example, for each one of the five levels of defence in depth.

3.5.1. Some possible enhancements to Level 1 of defence in depth

The means adopted in order to meet the objective of the first level of defence in depth include excellent and conservative design, together with high quality in construction and operation. Specific areas of future plant enhancements include:

1. Design margins and robustness; response time to faults

Typical improvements that enhance overall design robustness include an increase in certain design margins and response time constants for the overall reactor system, to reduce perturbations and abnormal events. For example, for a PWR, an increase in the size of the pressurizer, an increase in the secondary system water content per unit thermal power and a decrease in average fuel rod heat rate are among the provisions which are under consideration to increase the thermal inertia of the system and to slow down the transient response of the system.

These measures allow more time for automatic control action and operator action, they simplify the design of control systems and simplify the actions required of operators, and they decrease the number and severity of challenges to structures and safety systems.

2. Simplification

The simplification of plant systems is another well established trend for future reactors, especially with regard to safety systems. This goal of greater design simplification goes hand-in-hand with the goals of increased design margins, robustness and response times.

During recent years a number of previously unconsidered accident conditions have been postulated on the basis of research or operating experience, including precursor studies. For current plants, this has often led to event specific or issue specific backfits that have had a cumulative effect of adding significant complexity to the basic design.

As a consequence, current plant reactor systems have become more capable of addressing a wider range of postulated accident situations, but at a cost of becoming significantly more complex. The need for system simplification has been felt for a number of years. The opportunity to address each of these historic issues that have driven piecemeal or unco-ordinated design changes in the past is obvious at the point of designing an entirely new plant, where these same issues can be addressed in a more integrated, coherent process. A simplified system is one that is more easily operated and maintained, which has reduced the number of components to the minimum necessary to provide all safety and performance functions (thereby reducing the number of failure points and modes), and which will be resilient to human errors in operation.

3. Irradiation embrittlement

An important improvement for future plants includes a decrease of the design neutron fluence to the reactor pressure vessel (RPV) wall, particularly for PWRs; and related design changes that minimize welds in the beltline region of the vessel during fabrication.

An added benefit of these improvements is to increase the confidence in the evaluated amount of the reduced level of end-of-life vessel wall embrittlement. There are still uncertainties in the exact interplay of all of the involved physical parameters (chemical,

metallurgical, environmental), so RPV embrittlement is still subject to continuing research and discussion among experts. Decreases in design fluence below the customary 3×10^{19} nvt (energy >1 MeV) tend to diminish the extent of possible disagreement. For BWRs the problem is much less significant, due to the relatively larger diameter of the BWR RPV, which in combination with internal structures between the core and RPV wall, greatly reduces fluence levels. Also, BWRs operate at substantially lower pressures than PWRs.

3.5.2. Some possible enhancements to Level 2 of defence in depth

The general way in which the objectives of this level are implemented is through the use of control systems, including analogue and limitation functions, and other surveillance features. In general, Level 2 defence is being improved significantly through the increased application of modern, highly reliable digital instrumentation and control (I&C).

For future reactors, greater care is being taken to ensure strict separation of control systems (Level 2) from protection systems (Level 3). This approach not only enhances safety through rigorous adherence to defence in depth and thus increased reliability of the specific function in question, but also enhances safety by reducing the number and severity of challenges to reactor protection systems. This, in turn, improves overall plant performance and plant availability.

Further, within the control systems, in instances where a limitation function is used to decrease the challenges to protection systems, the limitation actuation is typically functionally independent of normal control logic (e.g. automatic limitations on reactor power are independent of manual or load following rod controls).

3.5.3. Some possible enhancements to Level 3 of defence in depth

The primary tools of defence in depth at this level are engineered safety systems and features, including reactor protection systems and emergency operating procedures. The three fundamental tasks of the engineered safety systems are: reactor shutdown, decay heat removal, and containment of radioactive releases from the core.

Recent trends in the design of engineered safety features for water reactors are: application of digital technology, priority on system simplification, increased focus on assurance of system isolation and containment integrity, and capability for primary system depressurization for passive plants. Some of these enhancements contribute to safety at both Levels 3 and 4.

1. Digital instrumentation and control for protection systems

A major technological development that is being applied to nuclear safety is the use of microprocessor based instrumentation, control and protection systems (digital technology). These systems have demonstrated very high reliability in many industrial applications, including NPPs. New generation designs offer the opportunity to fully implement this technology. Digital systems allow for a more logical treatment of input signals and a more reliable and accurate set of automatic actions, as well as improved display of information to operators, than that derived from hard wired or analog systems.

Challenges to implementation of digital technologies include a potential sensitivity to electrical disturbances, and the cost and time requirements of software (firmware) qualification

and reliability demonstration. Extensive operating experience is accumulating that will contribute to higher confidence in this reliability demonstration process.

In the interim, some hard wired backup systems may be retained for the most critical protective actions and the most critical safety functions.

2. Grace period

Various design enhancements, including increased design margins, improvements in instrumentation, control and protection systems, etc., lead to the possibility of prolonging the grace period for the necessary intervention of operators. For future reactors a grace period of 30 minutes is now considered feasible and appropriate, a significant improvement over many previous designs.

The concept of grace period is itself an application of defence in depth philosophy, because it relies on the designer to take into account potential shortcomings in operations and procedures, while at the same time relying on the operator, in a more relaxed mode and with more time to evaluate actions, to take into account potential malfunctions in the design (e.g. in automatic responses), should they occur. This positive outcome is ensured by applying grace periods to the design of automatic control systems such that no human action should be *necessary* for that period, as opposed to no human action being *allowed* for that period. Designs should be such that plant personnel can initiate safety functions and initiate necessary actions to deal with circumstances that could prejudice safety, but should not be able to negate correct safety system action.

3. Passive safety systems — general

The attention of utilities, and thus of many designers, has been attracted by passive systems, because they represent an opportunity to implement simplifications while retaining or improving safety.

Especially, they offer the opportunity to eliminate complex active components that rely on a large number of safety grade support systems, by applying the advantages of simple gravity driven or thermal gradient driven safety systems. The challenge to passive safety system designers is to demonstrate the capability and high reliability of these passive systems, and to deal with their longer time responses.

4. Primary system depressurization for passive plants

In some passive plant safety concepts, depressurization valves are used to accomplish the safety function of long term decay heat removal, automatically acting in three or more successive stages, if all normal and backup heat removal systems fail. These systems incorporate redundancy and diversity of components as necessary to achieve system reliability goals, and allow for a very large total flow capacity. In this way, active safety systems can be eliminated, and full reliance can be placed on complete primary system depressurization, down to the level where gravity driven injection is possible, for the plant's critical safety function of heat removal.

Passive plant automatic depressurization systems are designed to minimize the possibility of a potential spurious actuation and the disturbance it would create to the plant. Maximum care is being exercised by designers to prevent this.

3.5.4. Some possible enhancements to Level 4 of defence in depth

1. Primary system depressurization

Primary system depressurization is a manually-initiated accident management strategy that has the advantage of allowing the intervention of safety injection systems, as well as other non-safety coolant charging systems, in the case that the cooling function is lost at high primary pressure conditions.

Depressurization is also a powerful means of avoiding high-pressure severe accident sequences. The objective, here, is to avoid excessive challenges to the containment and overcome the many uncertainties in safety assessment. This depressurization function is effected by the operation of relief valves (e.g. by separate design features, or use of installed safety relief valves in a manner that is functionally independent of reactor coolant system over-pressure protection).

2. Core damage prevention and consequence mitigation

There is a consensus that future reactors will explicitly address severe accidents in the design, allowing for optimum use of all installed equipment, provision for portable equipment, and some improvements in mitigation features for credible scenarios.

Some uncertainty still exists in knowledge of phenomena associated with a severe accident (typically after core damage). Experience with tests and analyses to date suggests the need to deal with these phenomena with best estimate assumptions and methods.

The main technical objectives of mitigation are the cooling of the damaged core and the defence of the containment's integrity and leaktightness. There are significant areas of consensus on some of the issues among experts. Four of the issues are dealt with and discussed below:

(a) First, there is a consensus that for LWR accident conditions, water is good. Water will be fed in all cases to a damaged core. This technical conclusion stands despite certain temporary negative effects of adding water to an overheated core, such as: steam pressure spikes, core fragmentation and sudden hydrogen production. The possibility that these phenomena would occur with any destructive strength is considered quite low, or at least so low as to not counterbalance the benefit of water addition.

(b) The second area of consensus relates to the generally recognized need to avoid high-pressure core damage sequences. Indeed, core damage in the vessel at high pressure could entail local or general failure of the RPV lower head, with energetic injection of molten core materials into the reactor cavity. Steam explosions in the cavity or direct containment heating are phenomena that have been hypothesized that might follow in this situation. In addition, there is a remote potential for some upward displacement of the vessel. All of these possible but largely theoretical consequences are affected by uncertainties which make the design of protective measures rather difficult. The prevention of high pressure sequences is clearly preferred. Strong preventive measures at the first three levels of defence, plus primary system depressurisation at Level 4, are considered to be sufficiently adequate measures for these high pressure scenarios to allow them to be considered practically eliminated in the design.

Similarly, a consensus exists on preventive actions for the issue of potential hydrogen explosion. Here, while it is generally agreed for PWRs that the containment building should be designed to resist a substantial hydrogen burn, a prevention strategy is preferred for possible deflagration-detonation transition (DDT), by timely control of hydrogen concentration. Catalytic recombiners and hydrogen igniters of various kinds are considered adequate for preventing this phenomenon.

(c) Regarding defence against the consequences of low pressure core damage sequences, various proposed solutions exist. Here, the potential effects to be avoided are destructive steam explosions in the reactor cavity and perforation of the containment floor by a postulated molten core.

The first problem is resolved in the view of experts either by reduction (by geometry) of the water inventory in the reactor cavity, or by flooding the reactor cavity with water before vessel failure and cooling of the core within the vessel by the same means.

The choice between the two solutions is influenced by such design specific factors as vessel size and decay heat power-vessel surface ratio. These factors tend to favour the in-vessel cooling solution, especially for the smaller power reactors.

For larger reactors, reliance is also placed on introducing a large spreading area on the containment floor, along with provision for removing heat from this region. Some experimental confirmation of this approach to core cooling for a core-on-the-floor situation already exists today, but some experts still believe more research is desirable. Engineering experience suggests the prospect of a viable resolution of this issue by the above means.

d) Finally, defence against significant containment leakage in severe accident situations has received significant attention, especially in view of the trend of adopting lower targets for radioactivity releases to the environment.

Threats to leaktightness may come from random malfunction of isolation devices, and high pressure and temperature in the containment. The generally agreed upon defences against these threats are: reducing the number of penetration lines; redundancy and survivability of isolation devices and required systems; collection and control of leaks, at least for the most likely sources of leaks; and procedures for post-accident leak detection and repair.

3.5.5. Some possible enhancements to Level 5 of defence in depth

This level of defence is implemented by off-site emergency provisions. For presently operating reactors, this typically includes on-site and off-site monitoring, population sheltering and evacuation, food and water usage control.

A perceived public demand for reduced risk from nuclear power, and/or augmented population protection against possible reactor accidents, appeared in some countries after the Chernobyl accident, despite the fact that neither the Chernobyl accident sequence nor its consequences are possible in western reactors. This led many technical decision makers in the nuclear safety field to seek further improvements for future nuclear plants against certain severe accident conditions, even though such conditions would only lead to the off-site release of a small amount of radioactive products. This purpose and objective was strongly stated by several national representatives in the 1991 IAEA Conference on the Safety of Nuclear

Power [6]. In particular, prompt population evacuation could be substantially reduced or eliminated, if future plants were made even safer and even less likely to release significant radionuclides if a severe accident were to occur. Other prompt actions such as immediate notification over large areas (e.g. sirens) could be curtailed. Some other emergency provisions might, however, remain largely unchanged (e.g. environmental monitoring and prudent planning for contingencies).

One of the main aims in the development of future reactor designs is therefore to satisfy this demand for the simplification of emergency planning provisions. It should be recognized that the implementation of demonstrable improvements at Levels 1 to 4 of defence in depth (as discussed in this report), when applied to current national policies and methods of establishing emergency planning parameters, are likely to achieve the primary objective of reducing the need for detailed emergency planning. Nevertheless, in practice, national governments, local authorities and the general public may still expect some aspects of emergency planning to be retained.

4. CONCLUSIONS

- The document Defence in Depth in Nuclear Safety (INSAG-10) is to a very large extent applicable to future reactors, and was used as a primary source for this work.

- The considerations and examples included in this report refer mainly to LWRs. Even if many of them can be applicable to other kinds of more advanced reactors (e.g. gas cooled reactors, liquid metal cooled reactors), a more specific analysis of the peculiar aspects of defence in depth for these reactors is necessary. This is especially true for those advanced reactors that have advocated reduction or elimination of Level 3 or 4 provisions in recognition of improvements in design (i.e. fuel design).

- This report reaffirmed the distinction between the levels of defence in depth and the safety classification used to define the design specifications, and produced a table (Table II) which displays these relationships for future plants.

- Level 3 of defence in depth dealing with control of accidents within the design basis should consider the traditional set of accident conditions and methods. Level 4 should consider severe accidents, and, as appropriate, some conditions initiated by multiple failures, through use of best estimate assumptions, methods and data.

- Specific attention should be paid to sources of potential common failures to multiple levels of defence in depth, such as human failure and internal and external hazards.

- Possible enhancements to different levels of defence in depth were proposed for future plants, such as improved robustness and response times to faults, simplification of systems, improvements to reduce or control irradiation embrittlement, primary system depressurization and other features to improve core damage prevention and core damage mitigation.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Development of Safety Principles for the Design of Future Nuclear Power Plants, IAEA-TECDOC-801, Vienna (1995).

[2] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants. Report by the International Nuclear Safety Advisory Group, Safety Series No. 75-INSAG-3, IAEA, Vienna (1988).

[3] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, Safety Series No. 75-INSAG-10, IAEA, Vienna (1996).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Terms for Describing New, Advanced Nuclear Power Plants, IAEA-TECDOC-936, Vienna (1997).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Fundamentals: The Safety of Nuclear Installations, Safety Series No. 110, IAEA, Vienna (1993).

[6] The Safety of Nuclear Power: Strategy for the Future (Proc. Conf. Vienna, 1991), IAEA, Vienna (1991).

CONTRIBUTORS TO DRAFTING AND REVIEW

Antoshko, Y.	State Center on Nuclear and Radiation Safety, Ukraine
Berger, J.P.	Electricité de France, France
Bhardwaj, S.A.	Nuclear Power Corporation India Ltd, India
Caron, J.L.	Nuclear Power International
Cowley, J.S.	Nuclear Installations Inspectorate, United Kingdom
Del Nero, G.	Agenzia Nazionale Protezione Ambiente, Italy
Foskolos, K.	Paul Scherrer Institute, Switzerland
Gasparini, M.	International Atomic Energy Agency
Gomez, J.A.	Directorate General XI-CII, European Commission
Jurkowski, M.	National Inspectorate for Radiation and Nuclear Safety, Poland
Kabanov, L.	International Atomic Energy Agency
Keinhorst, G.	EC Directorate General XII, Eureopean Commission
Krugmann, U.	Siemens, Germany
Kurachenko A.W.	Ministry of the Russian Federation for Atomic Energy, Russian Federation
Kusnowo, A.	Reactor Technology Research Center, Indonesia
Kymäläinen, O.J.	IVO International Ltd, Finland
Pearce, K.I.	Magnox Electric, United Kingdom
Pedersen, T.	International Atomic Energy Agency
Petrangeli, G.	Agenzia Nazionale Protezione Ambiente, Italy
Summers, J.L.	Nuclear Installations Inspectorate, United Kingdom
Teimouri, M.	Atomic Energy Organization, Islamic Republic of Iran
Vine, G.L.	Electric Power Research Institute, United States of America
Wider, H.	Joint Research Centre, Ispra
Yoon, W.H.	Korea Institute of Nuclear Safety, Republic of Korea

97-04781