IAEA-TECDOC-1341

Extreme external events in the design and assessment of nuclear power plants

INTERNATIONAL ATOMIC ENERGY AGENCY IAEA

March 2003

The originating Section of this publication in the IAEA was:

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

EXTREME EXTERNAL EVENTS IN THE DESIGN OR ASSESSMENT OF NUCLEAR POWER PLANTS

IAEA, VIENNA, 2003
IAEA-TECDOC-1341
ISBN 92–0–102003–1
ISSN 1011–4289

Printed by the IAEA in Austria
March 2003

FOREWORD

The analysis of feedback experience from the operation of nuclear power plants (NPPs) in the past 20 years shows few cases of degradation of the plant safety initiated by external events. However, when these have occurred, the consequences have been serious, involving challenges to the defence in depth of the plant.

Part of the problem involves the definition of the design basis parameters for some scenarios and differences among regulators on the methods for the protection of operational NPPs in relation to external events. This results in different engineering practices in Member States for the siting and design of NPPs.

In the framework of the present revision of the IAEA safety standards on siting and design of NPPs, many initiatives have been implemented by the IAEA in recent years aimed at a systematic analysis of engineering practices in Member States. The most recent event in this connection was a Technical Committee Meeting (TCM) on Structural Safety of NPPs in Relation to Extreme External Loads, organized with the specific objective of evaluating the state of the art of NPP design in relation to external events. Such an analysis provided a technical background for the development of a common technical basis for an integrated approach in site evaluation, design and operation in relation to extreme external events. The scope included new and existing plants, as they are required to meet the same general safety principles, in spite of their peculiarities. This meeting was held in 2000 and was attended by 28 national experts from 21 countries, representing a significant portion of the nuclear community.

This TECDOC aims at providing a comprehensive summary of the experience in Member States and of the results of discussion collected at the TCM, with special emphasis on the development of a unified approach. When a unified approach was not possible, the issue was well defined and the different proposals for a solution were described in detail for future consideration.

The work of all the contributors to the drafting and review of this TECDOC is greatly appreciated. In particular, the contributions of G. Augusti (Italy), J. Donald (United Kingdom), A. Godoy (Argentina), S. Nefedov (Russian Federation), M. Petrescu (Romania), J. Riera (Brazil), J. Johnson (USA), J. Stevenson (USA) are acknowledged. The IAEA officer responsible for this publication was P. Contri of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

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

According to the databases on operational experience worldwide in nuclear power plants (NPPs) [1–3], extreme (and rare) external events have proven to be some of the most serious initiators of degradation of defence in depth. Among them, the most serious consequences were recorded for low temperatures, high winds, flooding, lightning, biological fouling, electromagnetic interference and earthquakes. These either directly affected the plant or caused the degradation of safety features through the unavailability of off-site power, of the ultimate heat sink (UHS) and of evacuation and/or access routes.

Moreover, a systematic review of practices in Member States, carried out by the IAEA through many initiatives, highlighted some intrinsic difficulties in the definition of appropriate design parameters for such scenarios (and sometimes for their combination) owing to their very low probability of occurrence. Some discrepancies in engineering practices in Member States were also identified for different scenarios (e.g. some orders of magnitude between the probability targets assigned to precipitation and earthquakes) and for different States (e.g. different reference aircraft are considered in the Member States).

In 1998 the IAEA commenced a review of its safety standards so as to reflect new evidence, new data and new practices. Many Safety Guides on site evaluation and design deal with external events in general, and in particular with the hazard from earthquakes, floods, extreme events (wind, temperatures) and design of the relevant protection systems [4–12]. All are under review to be completed by 2004.

To support such a review, in 2000 the IAEA organized a Technical Committee Meeting (TCM) on Structural Safety of NPPs in Relation to Extreme Loads focused on the main technical issues which prevent a unified engineering approach to these disciplines. The TCM addressed only very specific topics trying to solve the conceptual and the engineering differences that still affect this discipline, preventing a unified approach in Member States.

One of the main topics for discussion concerned the generally accepted ‘risk based’ context, where the probability of event occurrence is analysed together with the probability of an induced radiological consequence. This is conceptually accepted by the engineering community, but its real application still proves to be unreliable and difficult. In fact the evaluation of the risk usually adds large uncertainties to the whole siting and design process; therefore the final plant safety level associated to a specific external event is sometimes difficult to be demonstrated within a rigorous risk based approach.

The design provisions relevant to the extreme scenarios were also discussed. It shows many relevant differences among the practices in Member States: different classification criteria, different monitoring procedures and different operating procedures for pre- and post-event, leaving the impression that every Member States gives different priority to the relevant safety issues.

At last, the evaluation of existing plants still shows controversial approaches among Member States and deserved a specific analysis at the TCM. In many cases deep modifications of the ‘boundary conditions’ which were assumed at the siting and design

phases (modification of population density, of industrial installations, of hazards, of legislation, etc.) were observed, demanding for a systematic re-evaluation approach.

One basic tool used at the TCM for the understanding and comparison of Member States' practice on external event siting and design was the processing of the result of a questionnaire sent by the IAEA before the meeting.

The questionnaire intended to feed the discussion with real and recent data from Member States' practice and to have a global updated picture of it, as a basis for a consensus on possible improvements in methods of safe design for NPPs.

The analysis experience was then completed at the meeting with other data from IAEA databases and from recent case studies offered by Blayais NPP (France), Humboldt Bay NPP (USA), Turkey Point NPP (USA), David Besse (USA), Chinon (France), Maanshan (China).

It was decided to collect in the main text of this publication only the results of the discussion where a consensus was reached; leaving to the appendices some proposals for unified approaches that can be useful for future attempts of a more systematic approach to the matter.

1.2. OBJECTIVES

The objective of this publication is to provide a technical background to drive regulators, plant owners and designers in the definition of a consistent strategy in selected safety issues on site evaluation, design and operation in relation to extreme external events.

This publication is also of support to the IAEA in the development of safety standards since many Safety Guides dealing with related topics are under periodic review.

Four major tasks were identified to comply with these general objectives:

- identification of major unresolved safety issues and of areas of potential future improvement/clarification,
- overview of adopted approaches in Member States for site evaluation and design of new and existing plants,
- presentation and discussion of few case studies and examples from regulatory and engineering practice,
- preparation of a technical report, synthesis among the contents of current IAEA Safety Guides and the most updated engineering practice in Member States, for a common understanding of major safety issues connected with extreme events.

1.3. SCOPE

This publication refers to nuclear power plants. However most of its content is still valid for other nuclear facilities provided the necessary 'grading' is applied.

External events in this publication include also events originated at the site, of such nature that they can be assimilated, in terms of source and effect characterization, to events originated off the site.

1.4. STRUCTURE

The material presented here is derived from the following major sources:

- Analysis of the 'meeting oriented' questionnaire on current practice of regulators and designers (16 States answered to the questionnaire over 21 attending the TCM).
- Secretariat experience from the review of IAEA Safety Guides and recent IAEA review missions.
- Analysis of the feedback experience in available databases (IRS [1], INES [2], NPE [3], etc.).
- Discussion at the TCM.
- Contribution by Member States' representatives on specific issues, as experience in their State.
- Contributions by experts, at individual level, in the form of proposals.

This material has been ordered and rearranged by the technical officer as described in the following.

- Section 2 provides the description of the main issues related to external event siting and design, providing also definitions and details related to the general IAEA approach.
- Section 3 collects the results of the feedback experience, in IAEA databases and Member States.
- Section 4 is the synthesis of the discussion at the TCM when an attempt of rational answer to the key issues was carried out.
- Section 5 represents contributions from Member States on selected topics, where a reasonable agreement was reached.
- Annexes collect two proposals for unified approaches to specific issues, as a contribution for further discussions and actions.

2. GENERAL MATTERS

2.1. GENERAL CONCEPTS AND DEFINITIONS

The revision process for IAEA safety standards has clarified some basic concepts concerning the design of NPPs in relation to external events. Such improved background was also taken as starting point for the TCM discussion and therefore it is shortly summarized in this section, for an easy reference, as such material is published in many different Safety Guides.

In particular the hazard evaluation associated to extreme events has been extended from the siting of the plants (as it was mainly in the past) to the whole lifetime of the plant, including decommissioning. Therefore a new term will be used for this process in the IAEA Safety Guides as 'site evaluation', defined as in the following [6]:

The analysis of the sources of external events for a site that could give rise to hazards with potential consequences for the safety of a nuclear power plant constructed on that site. This includes: site characterization; consideration of external events that could lead to a degradation of the safety features of the plant and cause a release of radioactive material from the plant and/or affect the dispersion of such material in the environment; and consideration of population issues and access issues significant to safety (such as the

feasibility of evacuation, the population distribution and the location of resources). The process of site evaluation continues throughout the lifetime of the facility, from the siting phase to design, construction, operation and decommissioning.

Also the boundary between 'hazard evaluation' and 'design basis' has been better defined with respect to the former Safety Guides, leaving to the design basis only the final, deterministic selection of a single design basis value on the probabilistic hazard curve (if any), for any event. Therefore the definition of the exceedance curve is part of the hazard evaluation. Such sharp distinction is broadly used also in this report.

Another useful concept was clarified as a basis for discussion: the different statistics and hazard evaluation procedure requested for 'frequent' events and for 'rare' events.

In the former case (e.g. extreme winds, extreme precipitation, extreme snow pack, extreme temperatures), a statistics on the extreme values is possible and mainly relies on measurements at the site and in the region.

In the latter case (e.g. earthquakes, tornadoes, tropical cyclones lightning), a statistics cannot be carried out on the events at the site as they are rare and therefore in many cases never observed. The rare events require special procedures for hazard assessment, more based on simulation and integration of different indicators of their likelihood.

A more refined analysis of initiating events [1, 2] clarified also that the common classification of events into 'external' and 'internal' should not be referred to the site fence. Very often in fact the hazard for safety related components came from equipment installed at the site, but external to the buildings (like in the case of explosion of big transformers or fuel storage at the site) or in general from different units sharing the same site. It is a common scenario to have units at different levels of construction or in different status (construction, operation, maintenance, decommissioning), representing a potential source of hazard to each other.

Therefore the reference to the source itself is a preferred approach that does not need further classifications.

In the practice of many Member States it was also recorded a general tendency to site reuse either for the same kind of power production plant or for different plants, technology related (such as fuel reprocessing plant). In these cases the design basis had to be re-evaluated, but also the hazard for the new plants had to be reconsidered as some scenarios were screened out for the design of the first facility. The conclusion is that also the site hazard should be regarded as 'plant' or 'layout' dependent to some extent.

2.2. EXTERNAL EVENT CLASSIFICATION

The safety analysis of a plant should assess number and characteristics of the safety systems (including the barriers to prevent radiological accidents) through analysis of the consequences of any postulated initiating event (including external events) with application of the 'single failure' criterion to any safety group (see Ref. [10] for definitions). Special limitations to redundancy and diversity may be considered for passive systems, as specified in [10].

The safety analysis should be mainly based on the application of the defence in depth concept, aimed at maintaining the effectiveness of the physical barriers placed between radioactive materials and workers, the public and the environment.

Special care has to be used in the application of the 'common cause failure' concept in the safety analysis as many external events affect many items at the same time (the case of the earthquake is typical). Detailed provisions for such an assessment are provided in [13].

In order to meet the general safety requirements for the external events selected in the site evaluation phase, a classification of the plant items can be developed to provide a rational basis for design. The IAEA Safety Guides present an external event classification (EEC) of items with reference to external events which aims at identifying the specific system requirements in case of a design basis external event (DBEE) (for design and maintenance), the risk associated with their failure and at driving very focused post-event operator action.

Depending on their external event classification (EEC), different acceptance criteria (according to the required function), different safety margins (according to the associated risk) and specific operation, inspection and maintenance procedures are associated to the items according to their importance or vulnerability in case of a DBEE.

The external event classification can be developed according to the general safety classification of the plant, which identifies those structures, systems and components important to safety [10], defined as in the following:

(1) Items whose failure could directly or indirectly cause accident conditions.
(2) Items required for shutting down the reactor, monitoring critical parameters, maintaining the reactor in a shutdown condition and removing residual heat over a long period.
(3) Items that are required to prevent radioactive releases or to maintain releases below limits established by the regulatory body for accident conditions (e.g. all the defence in depth levels, robustness and barriers).

The external event classification (EEC) may include and possibly reclassify other items, such as:

- the items which in case of a DBEE can affect the functionality of a safety classified item (these items are non important to safety according to [10]);
- the items required to prevent or mitigate accident conditions for such a long period that there is a reasonable likelihood that a DBEE may occur during that period.

and can exclude items not affected by any DBEE (e.g.: items located at elevation higher than flood level and not affected by any other DBEE).

In principle the EEC could differentiate according to the external events. However, the engineering practice shows that most of these EEC items are designed with the same philosophy and with the same safety margins, suggesting therefore a unified approach.

For a rational basis in the design, such information can be organized through the external event classification process of all plant items in order to identify the items who need to be considered in case of any EE and the relevant requirements.

To this aim, three classes can be identified:

- **External Event Class 1**: safety systems pertaining to EE safety groups or safety systems which, during and after an EE, interact with items in the safety group of the EEs
- **External Event Class 2**: safety systems which are not in the EE safety groups and which, during and after an EE, don't interact with EEC1 items.
- **External Event Class 3**: items not important to safety which could impair proper functions of EEC1 and EEC2 items or the operator action.

A scheme of such classification is shown in Fig. 1.

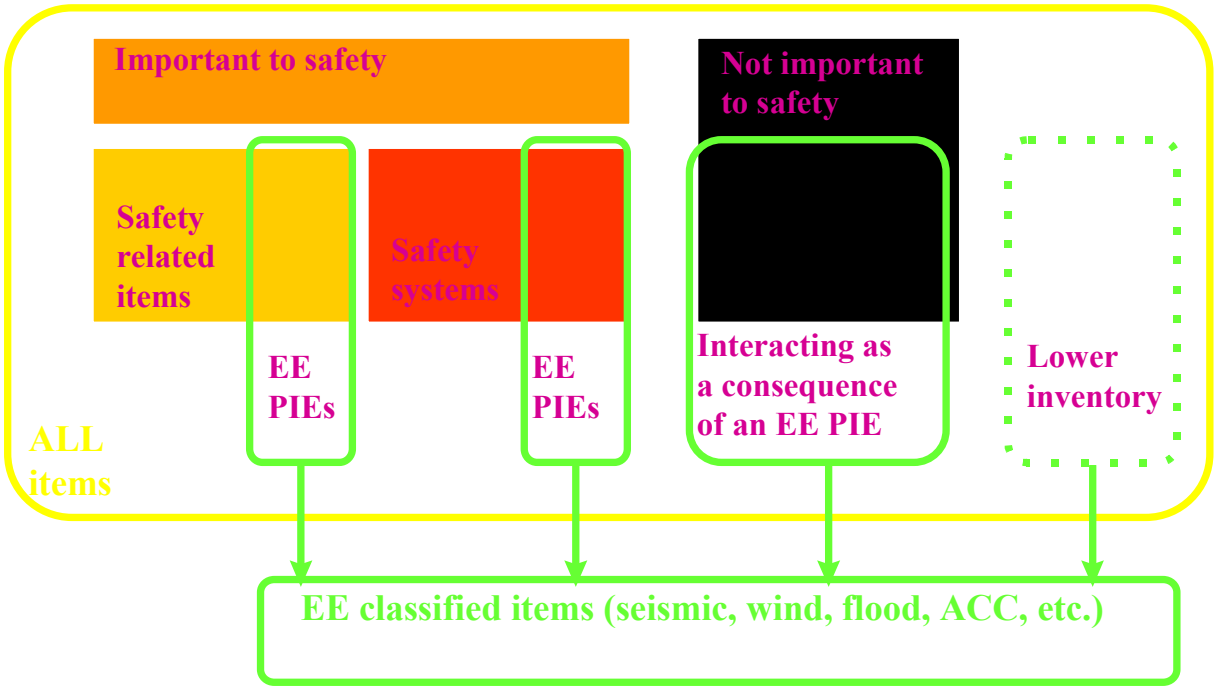

FIG. 1. Scheme of the proposed EE classification.

Acceptance criteria should then be stated for both the operational state of the facilities and the accident conditions considered in the design of the facility. Such criteria vary among Member States: they may include considerations such as those listed below.

(a) Radiological criteria, such as:
- ALARA levels
- Dose limits (or targets) for facility staff and workers at the facility site and the general public;
- Release limits to the environment; and
- Risk criteria (where applicable)

(b) Performance criteria, including
- Limits to damage of the first physical barrier
- Limits to damage of safety significant structures, systems and components
- Frequency limits for certain anticipated operational occurrences and for particular accident conditions, including frequency limits for significant damage of physical barrier (where applicable).

These criteria should define relevant behaviour limits for any component and structure in any EEC class above according to the safety function which is associated to them in case of a sequence where an external event is the PIE.

It turns out that the EE classification is not related to the kind of behaviour limit (acceptance criteria) associated with the component/structure, but it is related only to the amount of safety margin required (Fig. 2). The more relevant a component is for safety, the highest safety margin has to be considered in its design. Therefore, the classification aims at the identification of the safety margin to be applied to any safety function (horizontal arrow in Fig. 2), with grading from the highest associated radiological risk to the lowest. In this framework, the classification does not mix the behaviour limit (elasticity, integrity, etc.) with the required amount of safety margin (vertical arrow in Fig. 2).

In probabilistic terminology, the deterministic concept of 'safety margin' is in relation to the probability of exceedance of the design limit. This safety margin has to be intended in a general sense as it might include design safety margins, but also qualification requirements, requirements for redundancy and diversity, reliability evaluations, number of safety features, QA prescriptions etc., as described above.

2.3. THE REFERENCE PROCESS

According to the general definitions discussed above, external events are involved in the whole process of siting, design and operation of a plant. A short description of different phases of such process is in the following with specific reference to external events.

It has to be reminded that such steps are not necessarily sequential as, for example, design can start earlier than site confirmation (particularly in case of 'unified' design). Therefore such sequence represents only a logical flow for future reference in this publication.

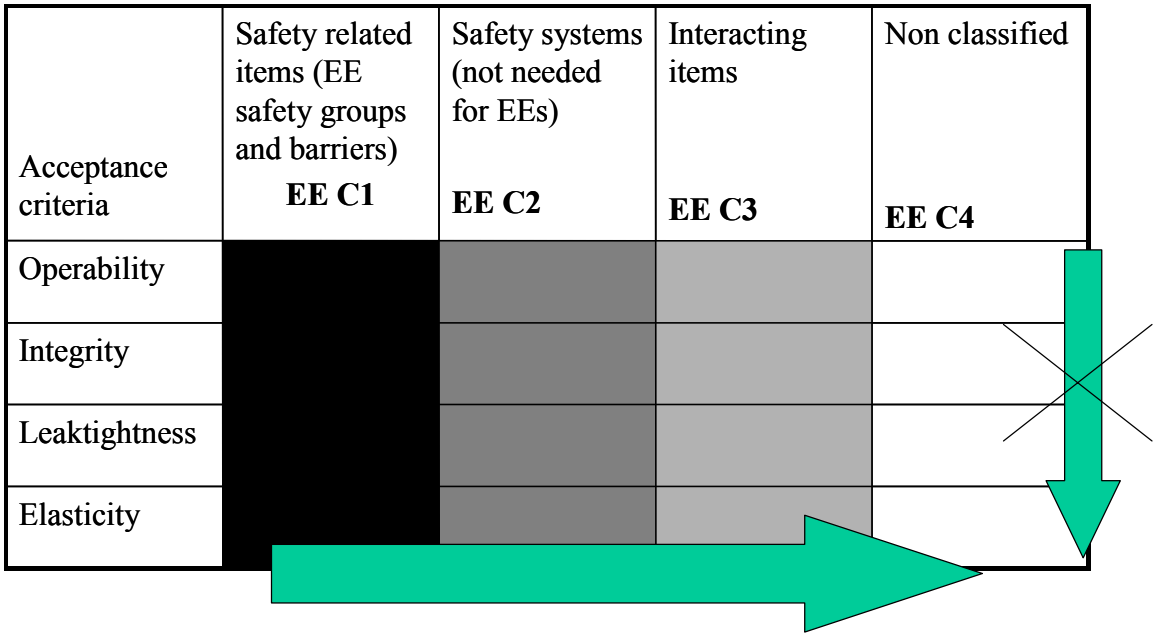

FIG. 2. Interaction between item classification and acceptability limits.

- *Site selection stage.* One or more preferred candidate sites are selected after study and investigation of a large region, rejection of unacceptable sites and screening and comparison of the remaining ones.
  At this level, a selection of external events is carried out preliminary to the hazard evaluation for the preferred sites.
- *Characterization stage.* This stage is further subdivided into:
- *Verification.* The suitability of the site to host a nuclear power plant is verified.
  In this stage the so called 'site exclusion criteria' are applied. They are the result of a combination of external event scenarios with rational approaches in the design of engineering features to cope with them. Typical criteria for NPPs are related to surface faulting at the site, high soil liquefaction hazard, etc.
- *Confirmation*. The characteristics of the site needed for analysis and detailed design are determined.
- *Design stage.* A suitable installation design has to protect the plant in case of external events. In this stage the design basis is finalized and the plant items designed according to their classification criteria (such as 'safety', 'external events', etc.). A screening phase for external events defines the events to be considered in the design and for them defines their loading schemes.
- *Design assessment.* The design is systematically reviewed to ensure that all the relevant safety requirements are met. In this stage the classification of items in relation to external events is the basis for the assessment.
- *Pre-operational stage*. Studies and investigations on hazard and site parameters begun in the previous stages are continued after the start of construction and before the start of the operation of the plant to complete and refine the assessment of site characteristics. The obtained site data allow a final assessment of simulation models used in final design.
- *Operational stage.* Appropriate safety related site evaluation activities are carried out throughout the life of the facility, mainly by monitoring and periodic safety review. In this stage external event hazard is periodically evaluated, with reference also to new, if any, methodology for its assessment and to new standards.

The screening process mentioned in the design stage above is mainly based upon the following criteria:

- 'Extremely low' probability of occurrence: the screening probability level (SPL)
- 'Very large' distance from the site (for fixed sources): the screening distance value (SDV)
- 'Extremely low' probability to cause a radiological accident at the site: the conditional probability value (CPV)

Of course such criteria has to be assessed at the end of the design when the conditional probability to cause a radiological accident is measurable and not assumed.

2.4. REFERENCE EVENTS

The following scenarios, related to external events, are usually considered in NPP design and were discussed at the TCM.

(a) Human induced

- Aircraft crashes.
- Explosions (deflagrations and detonations) with or without fire, originated from off-site sources and on-site (but external to safety related buildings), like storage of hazardous materials, transformers, high energy rotating equipment.
- Release of hazardous gas (asphyxiant, toxic) from off-site and on-site storage.
- Release of corrosive gas and liquids from off-site and on-site storage.
- Fire generated from off-site sources (mainly for its potential for smoke and toxic gas production).
- Collision of ships and floating debris (ice, logs, etc.) with the water intakes.
- Electromagnetic interference from off-site (e.g. from communication centres, portable phone antennas) and on-site (e.g. from the activation of high voltage electric switch gears).
- Any combination of the above as a result of a common initiating event (e.g. explosion with release of hazardous gases, smoke and fire).

(b) Natural

- Earthquakes
- Extreme meteorological conditions (temperature, snow, hail, frost, subsurface freezing, drought).
- Floods (from tides, tsunamis, seiches, storm surges, precipitation, waterspouts, dam forming and dam failures, snow melt, landslides into water bodies, channel changes, work in the channel).
- Landslides and avalanches.
- Cyclones (hurricanes, tornadoes and tropical typhoons).
- Abrasive dust and sand storms.
- Lightning.
- Volcanism.

This list is not exhaustive and other external events, not included in the list, may be identified and selected as design basis external events at the site.

It has to be reminded that some scenarios are tackled preferably trough site protection features (e.g. site drainage, protecting dams and levees, etc.) than with plant design measures.

Furthermore, considered external human induced events are of accidental origin. Considerations related to physical protection of the plant from wilful action by third parties are not in the main scope of this publication, following the generic policy of IAEA Safety Guides, and therefore they are mentioned only in Section 5 of this report.

2.5. IAEA BASIC REFERENCE PUBLICATIONS

Table I shows safety standards in which external and internal events are considered.

Other IAEA publications are dealing with seismic hazard [14, 15], QA [16, 17], PSA [18] and re-evaluation of existing plants [19].

TABLE I. IAEA SAFETY GUIDES AND SAFETY REQUIREMENTS IN WHICH EES ARE DISCUSSED

Scenario	**Site Req. (para. no.)**	**Specific Hazard (ref. no.)**	**Design Req.**	**Event based design**	**RCS UHS**	**Fuel storage**	**Contain-ment**	**EPS**	**I&C**
SITE EXTERNAL									
Ext. explosion (Pressure, fire, projectiles, smoke, vibrations, etc.) from fix and/or mobile sources, solid, liquid or gaseous	445	[6]		[11]	[20]		[21]		
Ext. fire (Pressure, fire, projectiles, smoke, etc.) from fix and/or mobile sources, including fire on the sea after oil spill from a vessel		[6]		[11, 22]					
Release of asphyxiant and toxic gases	451	[6]		[11]					
Release of corrosive gases and liquids, including atmospheric attack (salt) and aerosols	451	[6]		[11]					
Aircraft crash and ext. missiles in general (from tornadoes, high energy rotating machinery, etc.), incl. skidding from out-of-site impacts and vibration	441	[6]		[11]	[20, 23]		[21]		
Ground collapse (subsidence, uplift, mining, quarrying)	421	[5, 6, 7]		excluded					
Slope instability, avalanches and earth movements	418			excluded	[20]				
Settlements, liquefaction, soil stability		[7]		[7]					
Groundwater related effects		[24]		[7]					
Blockage/damage of water intake (ice, debris, logs)	449	[8]		[11]					
Blockage/damage of water intake (ships) and water contamination by oil	449	[8]		[11]	[20]				

spills									
Biological phenomena in water (plants, marine growth) and air (insects, leaves), including biological contamination		[6]		[11]	[20]				
Electromagnetic interference		[6]		[11]					[25]
Extreme meteorological conditions (temperature, hail, frost, fog, subsurface freezing, etc.)	440	[9]	517	[11]	[20]				[25]
Floods (tides, seiches, waves, storm surges, on-site and runoff precipitation, waterspouts, dam failures, channel changes, landslides into water bodies, snow melt, works in the channel) and related dynamic actions	401, 410	[8]	517	[11]	[20]	[26]			
Drought (unavailability of UHS)	449	[8]		[11]	[20]				
Tornadoes and tropical cyclones (only wind and secondary missiles)	432, 440	[9]	517	[11]					
Dust and sand storms, abrasive effects	440	[9]		[11]					
Site instability (erosion from sea and rivers, groundwater table excursion, etc.)		[8]		[11]					
Lightning (grounding)		[9]		[11]				[27]	
Tsunami (from earthquake, landslides and ice falling)	405	[8]		[11]					
Snow, ice pack and blizzard	440	[9]		[11]					
Earthquake	424	[5]	517	[28]	[20]		[21]		
Volcanism and related effects (lava, ash, gases, missiles, lightning, lahars, flood, earthquake, tsunami, ground water)	440	/		[11]	[20]				
Loss of off-site power					[20, 23]			[27]	
ON-SITE, EXTERNAL									

Fire, floods, explosions, release of asphyxiant, toxic and corrosive liquids and gases from the site, but external to the safety related buildings		[6]		[11]					
INTERNAL									
Internal missiles (from explosions, ruptures, collapses, dropping, high energy rotating machinery)			514	[11]	[20]		[21]		
Pipe whip			514	[29]			[21]		
Jet impact			514	[29]			[21]		
Internal flood			514	[30]	[20, 23]	[26]			
Internal explosions			509	[29]					
Internal release of hazardous gases and liquids				[11]					
Internal fire			509	[22]	[20]	[26]			
Vibrations				[28]					
NOT CONSIDERED									
Malevolent attack, war	no	no	(Phys. Prot.)						
Meteorites									

Note: RCS: reactor coolant system, UHS: ultimate heat sink, EPS: emergency power supply, I&C: instumentation & control.

3. STATE OF THE ART IN MEMBER STATES

3.1. QUESTIONNAIRE

3.1.1. Questionnaire targets and arrangement

In order to facilitate the comparison of current practice in siting design and operation of NPPs in relation to extreme external events, a survey on '**Current practice for siting, design and operation in NPP in relation to extreme external events**' was carried out through a questionnaire sent to NPP operators and regulatory bodies in Member States prior to the TCM. The results formed the background for discussion at the TCM.

The questionnaire requested information in two main areas:

- Part 1 dealt with the regulatory requirements in the State (to be filled by the Regulatory Body representatives). It contained the following sections:
  (1) Dates and content of major steps in the evolution of requirements for external events siting, design and monitoring
  (2) Hazards definition
  (3) Accidental external events to be considered in NPP siting in the State and relevant probability level

(4) Differences between extreme (rare) and other normal (i.e. deadweight, live and impact loads) and anticipated loads (i.e. building code required earthquake, wind, precipitation, etc.) with 50 to 100 year return period in terms of associated probability, design limits or other
(5) Site exclusion criteria
(6) Event combination criteria
(7) Modified criteria for site evaluation and design of existing plants (related to external events), if any
(8) Frequency of periodical safety assessments and their target: mechanisms for safety upgrading
(9) Major events associated to external root cause recorded in the State
(10) Any requirements in the accuracy of load definition and on its compatibility with the accuracy of design procedures?

- Part 2 dealt with the design basis of specific plants and relevant operational procedures (to be filled by operator representatives or by regulator representatives with knowledge of the plant, mainly taking data from the SAR, from the operation and QA manual of the plant). It contained the following sections:

(1) General site conditions.
(2) General plant configuration (containment, embedment, etc.).
(3) In service date.
(4) Events considered in the design: their reference values and associated probability.
(5) Date of the oldest historical data used in hazard estimation (for flood, earthquakes, precipitation, etc.).
(6) Methodology of hazard extrapolation from historical data to the probability level used in the design.
(7) Major events which affected the plant, associated to external causes in the State.
(8) Their root cause and their effects on the plants.
(9) Corrective actions taken.
(10) Site protection measures (type and safety relevance, etc.).
(11) Safety classification of items according to the extreme external loads and associated design limits.
(12) Combination rules applied in the design (also with internal events).
(13) Design limits according to different events and their combination.
(14) Monitoring systems.
(15) Periodical safety reviews: dates, frequency, and major outcomes (relevant to the extreme external events).
(16) Modifications of site related parameters respect to the design phase, if any.

An addendum of the questionnaire was agreed at the TCM and sent to Member States. It contained a request for more details in the different phases of plant design and assessment, as shown in Annex III.

The results were provided in a standard format in which individual plants and utilities were not identified in order to preserve the confidentiality of the information.

TABLE II. RESULTS FROM THE QUESTIONNAIRE — DESIGN TARGET LEVELS FOR DIFFERENT EES

EVENT/STATE	A	B	c	D	e	f	g	h	I	l	m	n	o	p	q	s	t
Explosion		1E-5 – 1E-7	1.E-07	1.E-07	**1.E-06**	hist		NA	det.	standard		**1.E-07**		**1.E-07**	1.E-04	NA	1.E-07
Fire	2.7E-3 in10 km		1.E-07	1.E-07	**1.E-06**	hist		NA	site dep.	site dep.		NA		**1.E-07**	1.E-04	NA	1.E-07
Asphyxiant gases			1.E-07	1.E-07	det	hist		NA	site dep.	site dep.		NA		**1.E-07**	1.E-04	NA	1.E-07
corrosive substances			1.E-07	1.E-07	det	hist		NA	site dep.	site dep.		NA		**1.E-07**	1.E-04	NA	1.E-07
ACC	1E-6 in0.2 km	1E-6 – 1E-7	1.E-07	6.E-08	**1.E-06**	hist		1.E-08	site dep.	**1.0E7** or det.		**1.E-06**	**1.E-07**	**1.E-07**	1.E-04	det.	det.
ground collapse			NA	NA	excl	hist		NA	site dep.	site dep.					1.E-04	det.	site dep.
slope instability	NA		NA	NA	excl	hist		NA	site dep.	site dep.					1.E-04	NA	site dep.
settlements			1.E-04	NA	excl	hist		**2.E-05**	site dep.	site dep.					1.E-04		site dep.
groundwater			1.E-04	NA	excl	hist		NA	site dep.	site dep.					1.E-04	NA	site dep.
water intake	NA		1.E-07	NA		hist		NA	NA			NA			1.E-04	NA	site dep.
damage by ships	NA		1.E-07	NA	NA	hist		NA	NA		NA	NA			1.E-04	NA	site dep.
biological phenomena	NA		1.E-07	NA	NA	hist		NA	NA		NA	NA			1.E-04	NA	site dep.
Electromagnetic		NA	NA	NA		hist	NA	NA	NA	site dep.	NA			NA	1.E-04	NA	site dep.
extreme temp	NA	Conv. standard	1.E-07	NA	hist	hist		NA	**1.E-04**	**1.E-04**	**1.E-02**	NA		**1.E-05**	1.E-04	hist.	hist.
floods	1.E-08	**1.E-04**	1.E-07	7.E-06	1.E-3, 1E-2	1.E-02	1.E-03	NA	site dep.	**1.E-04**	**1.E-03**	**1.E-06**	**1E-2, 1E-3**	**1.E-05**	1.E-04	hist.	hist.
drought	NA		1.E-07	NA	hist	hist		NA	site dep.	**1.E-04**	excl	NA		**1.E-07**	1.E-04	hist.	
wind	5.E-06		1.E-07	3.E+06	conv. standard		1.E-02	**1E-4, 1E-2**	**1.E-04**	**1.E-04**	**1E-4,1E-3**	**1.E-07**	**1.E-07**	**1.E-06**	1.E-04	hist.	
tornadoes	4.E-06		NA	5.E-06	conv. standard	2.E-07		**1E-7, 1E-4**	**1.E-04**	**1.E-04**	**1E-4,1E-3**	**1.E-07**	**1.E-07**	**1.E-06**	1.E-04	hist.	NA
dust	NA	NA	NA	NA	NA	hist		NA	site dep.		excl	NA		NA	1.E-04		NA
site instability	NA		1.E-07	NA	excl	hist	NA	NA	site dep.			NA			1.E-04	NA	site dep.
lightning			1.E-07	NA		hist		NA	site dep.			NA			1.E-04		site dep.
tsunami	NA	NA	NA	NA	NA	hist		NA	NA			1E-3-1E-4		**1.E-04**	1.E-04	NA	NA
snow	NA		1.E-07	NA	1.E-02	hist		**1.E-02**	**1.E-04**	**1.E-04**	NA	NA		**1.E-04**	1.E-04	NA	site dep.
earthquake	yes	1E-4 - 1E-6	1.E-04	6.E-05	hist	1.E-04	1.E-04	**1E-4, 1E-2**	**1.E-04**	**1E-4 or 5E-3 in 50 Years**	**1E-4, 1E-2**	1E-3, 1E-4	**1.E-04**	1.E-04	1.E-04	site dep.	prob.
volcanism	NA	NA	NA	NA	excl	hist		NA	NA		NA			NA	1.E-04	NA	

Legend:

NA = not considered
blank = no info provided
figure in bold = regulatory requirement
figure not in bold = design according either to deterministic values or to historical values; the figure comes from a posteriori PSA
hist = based on historical data, but neither a probability nor a deterministic value are defined
excl = exclusion criteria
conv. standard = det. values selected according to standards for conventional buildings
site dep. = analysis is required, no unified criteria available
det. = a deterministic value is defined for the whole State

TABLE III. RESULTS FROM THE QUESTIONNAIRE: APPROACH TO SITE EVALUATION FOR DIFFERENT SITES

State	**a**	**b**	**c**	**d**	**e**	**f**	**g**	**l**	**p2**	**p3**
Site	land	all	canal	river	land	sea	sea	river	sea	sea
Soil	soft		hard	hard	hard	soft	hard	soft	hard	hard
temp (degrees C)	-35+40	-40+40	-28+42	-28+37	-25+35	-1+50	0–40	-45+45	0+37	-18+40
pop density	scarce	medium	medium	high	high	medium	medium	scarce	low	low
Industry						41 in 30 km	no	no	no	medium
embedment (m)		5-15	11.3	20	9	10	10	8	11	4
SL-2	mag 6	0.1-0.3g	0.2, 0.1g	0.3, 0.15	0.1g		mag 6	0.05g	0.2g	0.2g
Wind				140km/h, 2E-4	30KPa	30m/s	63m/s	0.3KPa	63m/s (3sec)	47m/s (3 sec)
Flood	2.5m		7.8	30mm/h, 6500mc/s (1E-4)			6.22		6.5 (30cm higher)	8 (1 m higher)
chemicals				230 t fluorine						
ACC			6E-6							
SI-2data (years)	100	1000	200	120	300	25	33	900		
wind data (years)	34			39	100	49	89			
flood data (years)	34	100	104	74	100	49	64			
prec. data (years)				30		49	116			
fire data (years)	4									
ACC data (years)	2		21		20					
extrapolation method	extr. value		SSE: max. recorded +1 MSK		Exp. Judgement				Gumbel, Pierson	
site protection strategy	ventilation against smoke, heated water intake, dam operation for the level in UHS	flight forbidden	dry site	dyke	light forbidden with monitoring	light forbidden			dyke, break water	break water are not designed for safety class
classification			pressure containment, functionality					damage of fuel elements, failure of safety systems, seismic		

monitoring at the site	seismic	seismic, flood, chemical gases	containment deformation, prestressing system, settlement, seismic	seismic	ACC, road transportation	meteo, seismic	meteo	meteo seismic, population, transportation	dyke settlement, seismic	
post event action		flood, seismic			emergency planning					
modification after PSR					emergency proc for external events., acc, chemicals	SSE: 0.5-0.4				

State	**n1**	**n2**	**n3**	**n4**	**n5**	**n6**	**n7**	**n8**	**o**	**p1**
Site	sea	sea	sea	sea	sea	sea	sea	sea		sea
Soil	rock	hard	hard	hard	hard	hard	hard	hard		hard
temp (degrees C)	-19+38	-19+39	-13+37	-13+37	-13+37	-13+37	-13+37	-13+37		-7+38
Pop density	high	high	high	high	high	high	high	high		low
Industry	no	no	small	small	small	small	small	small		no
embedment (m)	15	7	15	10	7	10	10	15		11
SL-2	0.2g	0.2g	0.2g	0.2g	0.2g	0.2g	0.2g	0.2g	0.2g	0.11g
Wind	40m/s	40m/s	45m/s	45m/s	45m/s	45m/s	45m/s	40m/s	100mph	42m/s (3 sec), 27 m/s (10 min)
Flood	10m	10m	10m	10m	10m	10m	10m	7m		9.57 (50cm more)
chemicals										
ACC				yes, on the same site						
SI-2data (years)	101	101	101	101	101	101	101	101		
wind data (years)	94	94	94,259	94,259	94	94	94	94		28
flood data (years)	94	94	94	94	69	69, 57 same site!	69, 1300 same site!			
prec. data (years)										
Fire data (years)										
ACC data (years)										

State	n1	n2	n3	n4	n5	n6	n7	n8	o	p1
extrapolation method	Gumbel	Gumbel	Gumbel	Gumbel						Gumbel, Pierson
site protection strategy	dewatering system against internal floods, cathodic of underground structures		dry site, dewatering system against internal floods, cathodic of underground structures					dry site, dewatering system against internal floods, cathodic of underground structures, coastal protection		dyke, break water
classification	seismic class is applied to all extreme events									
monitoring	meteo seismic									dyke settlement, seismic
Post event action	scram at OBE, at 33m/s wind									
modification after PSR										

3.1.2. Summary of the answers from Member States

Number of received questionnaires

Part I:	18 States
Part II:	16 States
Addendum:	5 States

The following States participated to the survey: Argentina, Bulgaria, Brazil, China, Czech Republic, France, Germany, India, Islamic Republic of Iran, Republic of Korea, Lithuania, Pakistan, Romania, Russian Federation, Slovenia, United Kingdom, Ukraine, United States of America.

Questionnaire results were processed at IAEA in order to get a picture of the experience in Member States in design requirements and design data in relation to external events: the results are shown in Tables II and III, respectively.

The analysis of the addendum was not successful: in Member States regulatory requirements and engineering practice there is a general lack of clarity in the difference between procedures to be used in the screening phase of the siting, in the hazard evaluation, in the design phase and in the safety assessment phase. A full comparison was therefore impossible on this last part.

The following events were recorded in the questionnaire from operational experience in Member States, as a general confirmation of the statistics carried out on IAEA databases (see below):

- Forest fires (2 events): scram and turbine trips
- Lightning (5 events): scram
- Earthquakes (5 events): turbine trip
- Wind and snow (2 events): loss of off-site power
- Flooding in river and estuaries (4 events): challenge to defence in depth
- Salt sprays (2 events): grounding and corrosion
- Biological fouling and mud in the intakes (3 events)
- Electromagnetic interference (1 event)
- Cathodic corrosion of underground metallic components and piping (4 events)
- Gas cloud explosions (not affecting NPPs) (1 event)
- ACC (not affecting NPPs) (2 events)

All other information collected from the questionnaire is discussed in the next section, topic by topic. In the ‘lesson learnt’ sections, many recommendations are provided as agreed and issued by the TCM participants. They should not be interpreted as IAEA recommendations, but rather as suggestions of the engineering community to the IAEA for consideration in the management of the next technical activities.

3.2. OTHER DATABASES

3.2.1. IAEA databases

A detailed analysis of the events in two major IAEA databases, INES [2] and IRS [1], allowed a statistic evaluation of the importance of external events in a safe design for NPPs. The statistic was carried out over 3000 events since 1980.

Results are summarized in Figs 3–5.

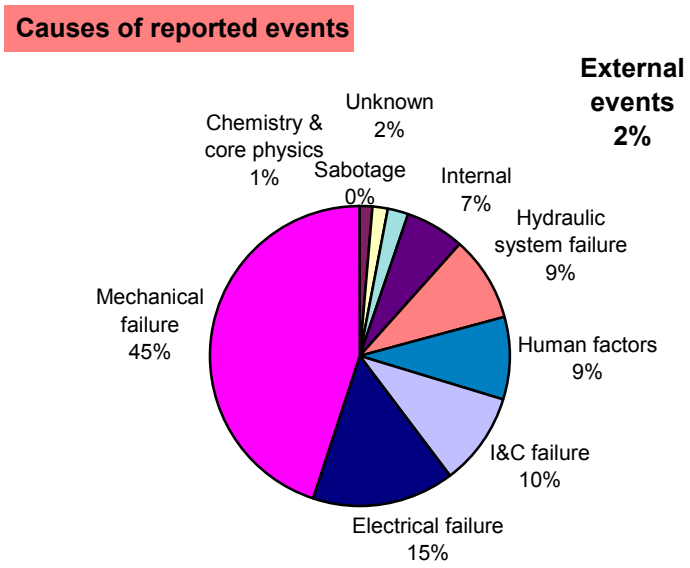

FIG. 3. Analysis of causes of recorded events in INES [2] and IRS [1].

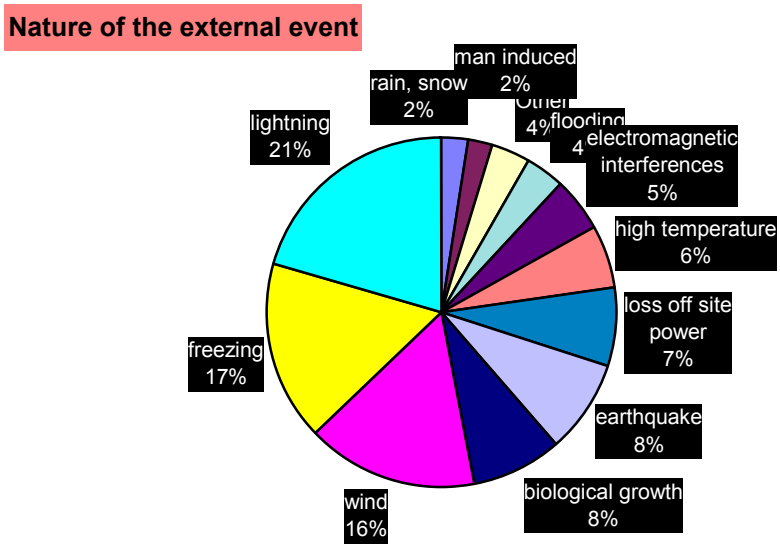

FIG. 4. Analysis of the nature of external events affecting NPPs according to [1].

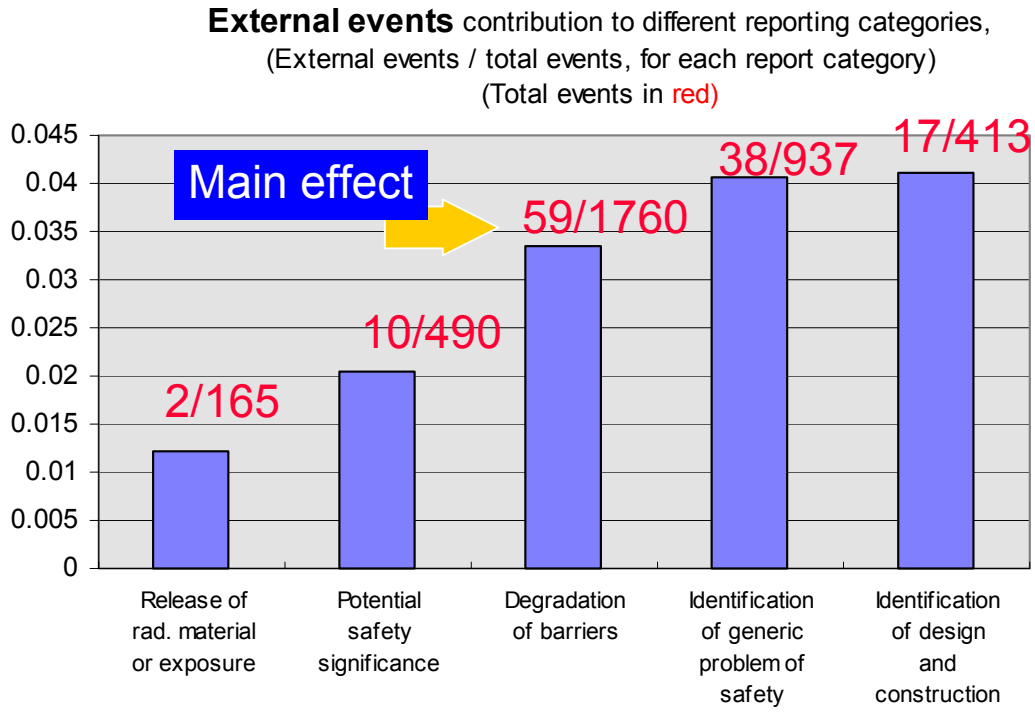

FIG. 5. Contribution of external events to different reporting categories [1]. The figures represent the ratio external events/total events in that reporting category.

A more detailed analysis on mentioned events clarified the event evolution and the major consequences on the plants. They are summarized in the following:

(a) Floods from rivers

- 14/11/80 Garigliano Italy — Increase in water table level, leakage — Contamination of ground water from spent resins storage tanks
- 3/12/82 Dresden USA — 60 cm above the historical max at the site — Damage to meteorological stations, telephone and plant
- '93+31/3/94 Cooper USA — River overpassing the predicted 10.000 years flood level — In-leakage from groundwater, damage to electrical, cable tunnels as pathways, contamination. Interruption of the planned emergency evacuation route

(b) Floods (droughts) from sea

- 13/12/80 Hinkley UK — Combination of waves from storm and high tide — Destruction of pump house, loss of SW
- 22/1/84 Borssele Netherlands — Low tide (less the historical) and strong wind+shoal in service water channel — Loss of service water
- 12/1999 Blayais France — Site flooded and emergency systems impaired
- (Since 1985 US NPPs — 17 occurrences of inadequate protection against external floods (source: NRC generic reports in IRS))

(c) Floods from precipitation

- 11/7/2000 Chernobyl 3 RF — Flooding of diesel building due to poor drainage on site, unavailability of three emergency power supply systems, reactor shut down

(d) Leakage from groundwater (suspected elevation of groundwater table)

- 17/10/80 Indian Point USA — Leakage — Damage to electrical and pumps
- '87+11/12/89 Clinton USA — Leakage in unsealed openings

(e) Water related accidents

- 12/1/87 St. Laurent France — Ice in water intake plus loss of off-site power because of storm on other plants — Loss of SW
- 1980–1990 Six NPPs in the USA, two NPPs in the Republic of Korea, one Indian and one NPP in the Netherlands suffered loss of SW because of biological fouling (mussels, fish, clams, shrimps, jellyfish, etc.), often coincident with increase of sea level
- 1985 USA — Salt contaminations to switchyards

(f) Combined effects

- loss of off site power (33 events due to external floods)
- grid unavailability
- unavailability of evacuation routes
- unavailability of the ultimate heat sink (UHS)

(g) External missiles

- 1982 France — Sabotage attack with weapons. Perforation of concrete shell.
- 1999 UK — Crash of a Tornado aircraft 800 m from the NPP fence.

(h) Internal missiles

- 30 events — Turbine overspeed, turbine disk cracks, failure of steam generator plugs, dropped fuel assembly, dropped transport cask

(i) Explosions with fire, off site

- 1988 USA — Explosion in a chemical plant, 5 km far from an NPP, with toxic smoke. NPP unaffected.

(j) Explosions with fire, on site

- 32 events — Explosion of transformers — Explosion of hydrogen storage or released by plant operation.

(k) Fire, on site

- 134 events — Transformers. Waste ignition. Fuel in diesel bldg. Maintenance operation. Turbine and generators. Chemistry lab.

(l) Release of Toxic gas

- 6 events — All from internal sources

(m) Electromagnetic interferences, on-site and off-site

- 6 events on site — Interferences from high voltage switches
- 2 events off site — Proximity of communication centre, but mainly unknown

(n) Damage to water intake

- 3 events — Damage from ice and debris

Some conclusions can be drawn from the analysis of the above pictures and data, even if the sample is not very broad and the time interval relatively small:

- there is a confirmation on the importance of events usually not considered in the design basis, such as biological fouling, electromagnetic interference, freezing, etc.
- the percentage of external events as initiator of incident reporting is rather small (3%), but they have their highest percentage in serious consequences such as 'degradation of barriers'. Therefore external events usually challenge the safety barriers, showing their potential for safety significant incidents
- a big improvement in safety can be obtained with relatively small investment to provide protection against such major causes of incidents. In fact protection to earthquake proved to be rather expensive, being usually 10–15% of overall construction costs for the plant (the general estimate is that for any 0.1 g of design basis, an additional cost of 8–10% on plant cost is required, including structure, piping and component qualification), while protection against other events such as wind demand for 1–2% of plant cost (however, often it is enveloped by earthquake). Globally, external events contribute to the total plant costs for 12–22% [31]. Therefore, even from the economic perspective, a higher protection to events other than earthquake proves to be convenient and providing a major advantage in terms of safety.

3.2.2. US IPEEE programme

On June 1991, the US Regulatory Body (NRC) issued a request that each licensee perform an individual plant examination of external events (IPEEE) to identify vulnerabilities, if any, to severe accidents and report the results together with any proposals for improvement and corrective actions. The events considered in the IPEEE include earthquake, internal fire, high wind, flood and human induced events. Guidelines were also issued by NRC for conducting IPEEE as a guarantee of the homogeneity of the tasks carried out by plant owners.

The NRC received 70 IPEEE submittals covering all operating US reactors/sites; both PWR and BWR type reactors.

A draft report [32] is under preparation at NRC with the synthesis of the collected data, which are already available and which represent an invaluable source of information for the following reasons:

- they represent data from a large population of reactors with rather homogeneous design, operated and maintained with identical regulations;
- they provide a detailed analysis of the plant improvements proposed by the plant owners (grouped into hardware, maintenance/housekeeping, procedure/training improvement respectively) which provide a useful collection of experience potentially applicable to other sites;
- they provide an analysis of the dominant contributors to the core damage frequency (CDF) from probabilistic risk assessments and seismic margin assessment, useful for the prioritization of the upgrading measures;
- they highlight some other issues for future consideration such as seismic induced fire and flood, soil liquefaction, soil settlement, flood hazard modification, etc.

Some data processing was carried out on the draft report [32]. The result is summarized in three main graphs:

- the contribution to the CDF for the different EEs (Fig. 6). The comparison is carried out only at the 'population' level and not plant by plant as CDF for internal and external events were not evaluated in full consistency. However, in some cases earthquake (and fire, for comparison) shows a CDF higher than internal events, comparable with CDF for wind and flood. Other events seems to have lower importance and often they are screened out from consideration at the annual probability value of 1.E-6/ry.
- the number of improvement typologies (Fig. 7) for the different EEs. Improvement typologies might represent very extended upgrading measures; what is shown in Fig. 7 provides an idea of the variety of solutions put in place by plant owners to cope with safety requirements.
- the dominant contributors to the seismic failures (Fig. 8). Electrical equipment and buildings play the major role as contributors to the seismic CDF, showing the unequal distribution of the safety margin in design/qualification of structures, systems and components.

3.3. DETAILED ANALYSIS OF RELEVANT ACCIDENTS

3.3.1. Perry NPP — Earthquake, 1986

(a) Event description

A US plant close to Cleveland was affected by Leroy earthquake (Magnitude 5) in 1986 [33].

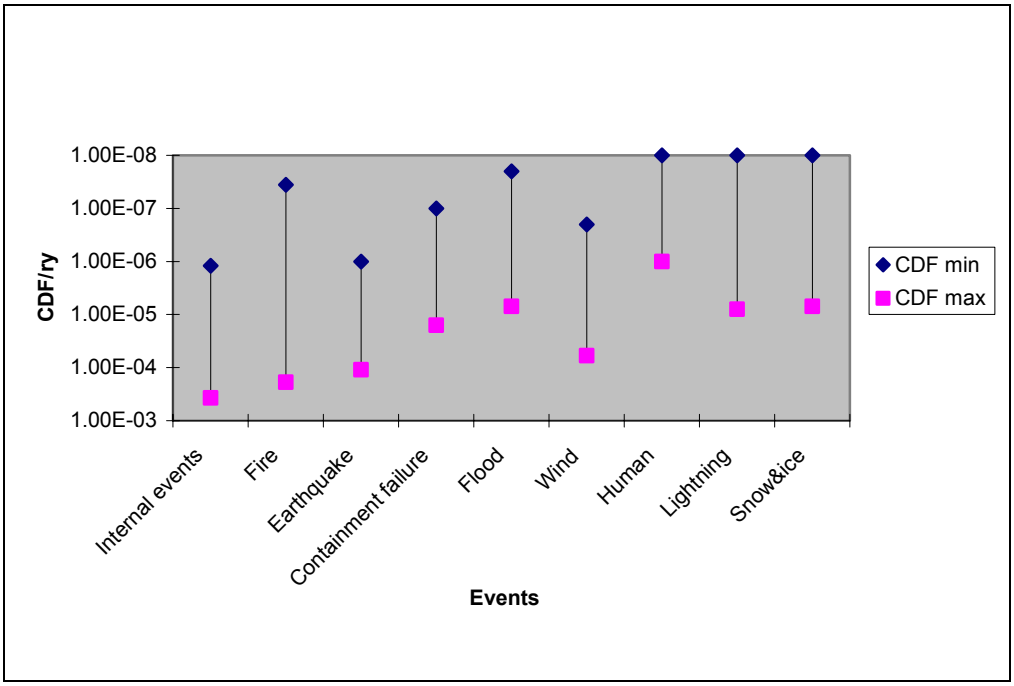

FIG. 6. Contribution to CDF from different EE (Internal events, fire and containment failure for comparison).

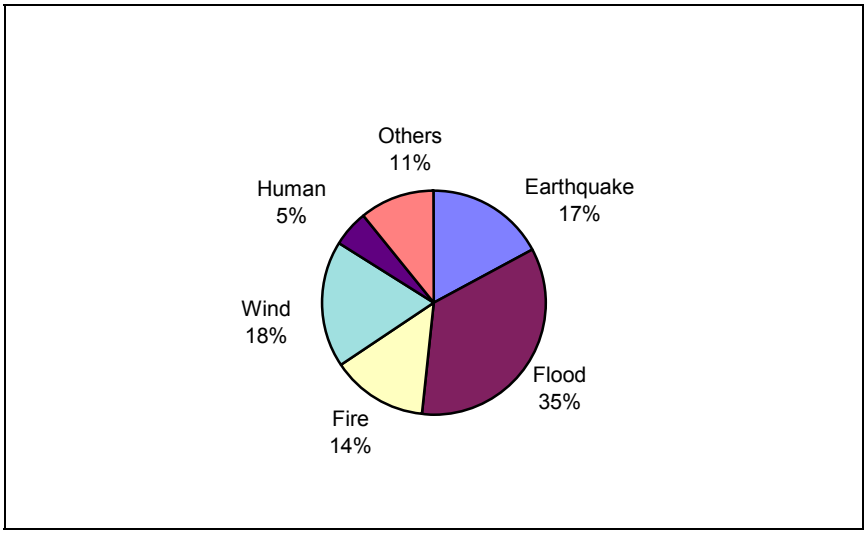

FIG. 7. Number of improvement typologies put in place for different EE.

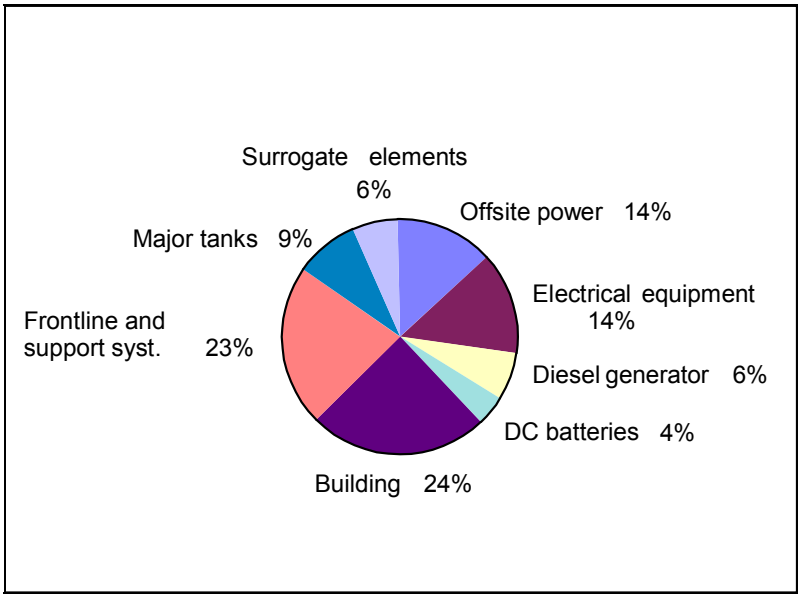

FIG. 8. Dominant contributors to CDF from seismic probabilistic assessments of 27 plants.

The interesting aspect is related to the vicinity of the epicentre to the NPP: only 18 km between epicentre and NPP. The strong motion duration of the earthquake was 1 second with a total earthquake duration of 2.7 seconds. The Pga at the site was 0.19 g, higher than the design value at 0.15 g. CAV parameter registered a value of 0.08 g sec (a potential damage is usually associated to values of 0.3 g or more). Relative displacement between basemat and containment shell was 0.1 cm while the design value was 0.36 cm.

Plant operating personnel were dispatched into the plant, just after the earthquake, to survey for any major damage. Subsequently, a team of 65 engineers and technicians was organized to perform a detailed walkdown.

These walkdown inspections found no damage to any structure, system or component: the plant systems, both safety and non safety related, operated properly during and following the seismic event.

(b) Lessons learnt

- Pga as damage indicator is not a suitable choice, while CAV or relative displacement confirmed their validity
- Low energy earthquakes, even if very close to the site, induce low damage because of their short duration and high frequency content
- 65 people for a walkdown is too large a number and technical outcomes could be confused and contradictory

3.3.2. Humboldt Bay NPP — Earthquake, 1980

(a) Event description

A plant in California, USA, withstood an earthquake in 1980 (Eureka) [33]. Epicentre was off coast, magnitude 7.0 at 120 km. Free field Pga at the site was 0.2–0.25 g (horizontal).

Plant design original value was 0.25 g, upgraded in 1975 to 0.5 g. Significant modifications were implemented to structural steel and lateral restraint to piping.

No visible damage was recorded at structures, systems and components.

(b) Lesson learnt

Upgraded structures can withstand events higher than the original design basis.

3.3.3. David Besse NPP — Tornado, 1998

(a) Event description

A US plant close to Lake Erie was affected by a tornado in 1989 [33]. The tornado was classified as Fujita-2 (F-2), with wind in the range 54–75 m/s, within the design basis of the plant.

Significant damage was recorded at the switchyard and to non-safety-related outbuildings and roofs. Lightning strikes opened and closed several times the circuit breakers. Emergency diesel were manually started from control room. The emergency response communication system was highly challenged by the damage of two of the three available telephone systems (only the microwave remained operational). Total loss of off-site power was recorded and the reactor protection system had to trip the reactor. Plant computer system failed because of loss of power.

Rain entered the turbine hall through the damaged roof (large holes). Heat removal (hot shutdown) was completed after 7 hours of natural circulation.

(b) Lesson learnt

- Even within design basis, the F-2 tornado created major troubles to the plant requiring a better, more detailed analysis of the items needed during such events.
- The emergency plan needs to be tested during a major event as most of the needed features might not be available.

- Timing is important in accident prevention: shutdown requires 7–8 hours and the meteorological forecast has to be part of the operational procedures to allow enough time to the operator for protecting actions.

3.3.4. Turkey Point NPP — Hurricane, 1992

(a) Event description

A US plant in Florida experienced hurricane Andrew in 1992 [33] with winds at 233 km/h and gusts at 282 km/h (level 4 of intensity of a scale ranging from 1 to 5) below design basis for seismic class 1 structures.

On the basis of the weather forecast, equipment was removed from outside areas or tied down, drains plugged to prevent water into buildings, removable goods were secured and operators requested to stay into diesel building as transfer between buildings was expected to be impaired by the storm. Unit 1 and 2 started shutdown 10 and 9 hours before expected impact.

Seismic class 1 structures did not suffer any damage. A total loss of off-site power was recorded for 5 days, but emergency diesel maintained the plant during recovery. One diesel unit had to be stopped because of high temperature, incompatible with operating procedures.

ECCS was activated and performed well.

Many false alarms in the spent fuel created concerns because it was not accessible during the storm.

Off-site communications were lost and access roads blocked: helicopters had to be used for fuel and consumable. Families had to be taken and hosted at the plant and fed, to allow operators to work in a non-emotional environment.

A water tower collapsed with major damage to fire protection system piping, water supply system, electrical services and instrumentation. Some non-safety-related buildings (warehouse, administrative) were destroyed.

(b) Lesson learnt

- Diesel units should be designed for long operation: also enough fuel should be stored at the site or provisions should be taken for a prompt supply at the site, even during and after accidents.
- Transfer of personnel between buildings during the external event could be necessary
- Access roads should be maintained operable during and after an extreme event
- Operator families created a major concern mainly because of the break off of the communication channels.
- Interaction problems (fall of the water tower) can create major damage to safety related systems and can impair operator manoeuvres at the site.

3.3.5. Blayais NPP — Flood, 1999

(a) Event description

The site of Le Blayais nuclear power plant, which comprises four 900 MW(e) pressurized water reactors, is 50 km northwest of Bordeaux and 30 km southeast of the Atlantic ocean, on the banks of the Gironde estuary, in a swampy area. The Design Basis Flood (DBF) used to design the site protection system (dykes) is 5.02 m NGF (French national datum level). The DBF was calculated as the level of water resulting from the maximum astronomical tide and the 1000 years storm surge (setup).

The site is surrounded by a dyke. The dyke is made of earth and is protected on the River Gironde side by a pile of stone blocks. Alongside the River Gironde, its height is 5.2 m above the national datum, and its height is 4.75 m at the sides.

The hydraulic event observed on the 27 of December 1999 resulted from the following phenomena:

- Tide level: high but not an extreme tide amplitude,
- Storm surge: observed extreme value which is equal to the calculated 1000 years set-up (2.01 m), the maximum level measured prior to 27 December 1999 was 1.20 m for a 40 years historical series of data,
- Wind speed: observed extreme value (maximum ten minutes average wind speed of about 100 km/h at 10 m height)
- Wind waves: observed extreme value (significant wave height estimated to 2.00 m, no measurement of this parameter in the estuary)

Investigations carried out on the site after the storm showed that the water had jumped over obstacles from 5 to 5.30 m.

Loss of the 225 kV auxiliary power supplies and loss of the 400 kV grid for Units 2 and 4 occurred during the storm [34]. Attempts to switch the units to house load operation to enable them to continue powering their auxiliaries following disconnection of the grid failed, causing these two units to shut down; the diesel generators of both units started up and operated correctly pending reconnection of the 400 kV grid, which occurred later. The 400 kV line powering Units 1 and 3 continued to be unavailable. This led to the shut down of all the 3 operating units.

Meanwhile, strong waves submerged the plant platform, with water entering mainly on the northwest side of the dyke. The waves moved the rocks, protecting the dyke, and part of it was washed away alongside the River Gironde. The water reached a depth of around 30 cm in the northwest corner of the site.

Units 1 and 2 were severely affected by incoming water: one of the essential service water pumps was lost as a result of immersion of the motors, some utility galleries were flooded, some rooms containing outgoing electrical feeders were flooded and electrical switchboards made unavailable, the bottom of the fuel building of Units 1 and 2 containing the cells of the two LHSI pumps and the two containment spray system pumps was flooded. The volume of water which came into the facilities has been estimated as about 90,000 m^3.

(b) Lesson learnt

- Dyke level and shape: it was designed without taking into account the wave effects (overtopping)
- Warning system: it was based on the water level monitoring in the entrance of the estuary and provided insufficient delay. It was also affected by communication failures due to the storm.
- Site isolation: the regional storm effect (roads obstruction by water and debris as trees), resulted in difficulties in getting emergency response personnel to the site. Access of personnel is a major issue for the emergency planning.
- Dedicated operating procedures are needed to bring all the units at the site into a safe state and maintaining them there after a flood.
- Flood confirmed to be a potential mode for common cause failures (also for all the unit at the site). In case of required shutdown, the evaluation of the time needed should account for all the units at the site.

3.3.6. Saint Laurent des Eaux NPP — Low temperature, 1987

(a) Event description

An incident occurred at the Saint-Laurent-des-eaux, a natural uranium gas cooled power station, on 12 January 1987, with two main consequences [35]:

- a partial blockage of unit 1 water intake caused a reactor trip and one hour unavailability of all the auxiliary turbo generators of the unit
- two hours later a voltage reduction on the transmission grid, caused by a trip of a neighbour power station, led to the trip of the unit 2 main generators, two line breakers and reactor.

The root cause of this twofold incident was the cold weather which prevailed over the west of France: ice floes transported by the river Loire caused the unit 1 water intake blockage; the cold weather was also responsible for the trip of the neighbour thermal power station.

(b) Lesson learnt

This incident highlighted the risks associated with cold weather conditions and confirmed the importance of the decision to install independent diesels generators at that station and the importance of developing procedures to address a general loss of electrical supplies or a loss of fresh cooling water.

Furthermore, this incident highlighted an inadequate configuration of the pumping station for these units and errors in the general station operating instructions.

3.3.7. Chinon NPP — Low temperature, 1987

(a) Event description

During winter, several level sensors of safety related tanks were locked by freezing, causing problems to reactor operation. A loss of off-site power was recorded at the same time [35].

(b) Lesson learnt

This event triggered a review of the effects of low temperature on NPPs in France. Particularly, the effects of a loss of external power occurring during the period of extreme cold weather was highlighted. This scenario is very likely, as a consequence of an increase in power supply demand during severe weather conditions.

The main safety related equipment availability should be assessed for very low temperature (for France the reference temperature was around –40°C). Moreover, the following actions could be taken as additional protection measures:

- definition of new operational procedures specifically for extreme weather scenarios
- qualification of equipment and components more exposed to low temperature, namely the pumping station and outdoor level sensors
- addition of bypass for water inlet warmed by condenser output
- addition of trace heating systems to piping.

3.3.8. Cadarache Laboratories — Forest fire, 1989

(a) Event description

A large forest fire was ignited 3 km from the site of Cadarache in France where many nuclear experimental facilities are located [36]. Fire spread fast towards the site fence, owing to the strong wind. Heavy smoke invaded the site and fire approached the site fence. Personnel were not evacuated and could co-operate to the emergency operations. The access to the site was extremely difficult. Fire extinguishing planes were used, flying continuously over the site, often in dangerous routes, as close as possible to the main fire sources.

(b) Lesson learnt

- The external fire hazard requires a suitable design of the ventilation systems (against smoke) and against burning projectiles transported at the site by wind.
- The possibility of a safe access to the site during emergencies plays a major role in the availability of specialized personnel and fireguards.
- During fire emergencies, an aircraft crash hazard may be evaluated, in consideration of the difficult environment where the planes have to operate. This hazard should be evaluated even if it has not been considered in the design basis of the plant. Administrative measures may be implemented to constraint the flying routes.

3.3.9. Maanshan NPP — Salt sprays, 2001

(a) Event description

A loss of off-site power affected the Maanshan NPP in China (Taiwan), a two unit PWR 900 MW, during a heavy tropical storm with salty wind [37, 38] A buildup of salt crystals transported by heavy sea winds on the insulators on trunk power lines leading to the plant was the root cause of the event, which triggered a breaker fire.

Several trips on grounding caused by heavily ionized air and smoke through several electrical arches and shorts prevented an effective breakers operation. Activation of two separate emergency diesel generators failed (one because the fire in the breakers prevented the generator from picking up the load, the other one because of a wrong manual activation) and

the plant was left without power for about two full hours. One unit scrammed and the other was kept in hot standby.

(b) Lesson learnt

- Maintenance and special design provisions should be required to prevent electrical equipment and transmission lines from attack by salty winds.
- Start up of emergency diesel generators should be guaranteed by a reliable combination of automatic systems and operator actions, assessed for emergency conditions (human errors should be minimized, particularly in case of emergency scenarios).

4. SELECTED ISSUES

4.1. GENERAL

The TCM discussed a number of selected issues, that cover the topics where most of the differences in Member States practice was detected by the questionnaire.

The major conclusions from the discussion are presented in the following, organized in a grid such as:

(1) Explanation of the issue: the issue is summarized and its problematic aspects highlighted
(2) Results from the questionnaire: the results are summarized with reference to the data described in Section 2
(3) Current IAEA position, reference to IAEA publications: reference is made to Section 3, but more detailed information is provided
(4) Discussion at the TCM and elements for an evaluation: additional elements provided at the discussion and attempt for a unified approach in Member States, final recommendations from the TCM

4.2. EVENT SELECTION AND SCREENING APPROACHES

(a) Explanation of the issue

Recent events and the detailed analysis of event databases show that a relevant amount of events was initiated by scenarios not considered in the design basis. The responsibility for such inclusion–exclusion of events is in the screening phase (see Section 3) that has to be improved to avoid unexpected events affecting the plants.

(b) Results from the questionnaire, databases and practice in Member States

- The majority of small fatality events recorded by Member States in the questionnaire is related to flood and tornadoes; larger fatality events are less frequent and dominated by hurricane and earthquakes
- The surveys described in previous Section shows the importance for a continuous upgrading of design basis events to avoid incidents from ‘unexpected’ events (such as damage or fouling of the intakes, electromagnetic interference, lack of cathodic protection) and therefore to drive regulatory action in a proper way. In many Member States, the design recommendations had to be recently upgraded to include toxic gases, biological fouling, hazard from industries, transport roads, military facilities and airports.

- A general tendency of merging requirements for nuclear and other industrial facilities (mainly chemicals) according to their risk for the environment was recorded in some Member States, even if there is no consensus yet on the evaluation methodology for such risks.
- Exclusion criteria in Member States are based either upon distance (SDV) (for fixed sources), or probability of occurrence (SPL), or deterministic criteria, such as:
  - active faults (but no agreement on the distance (0.5–8 km)
  - ground related hazards (settlements, karsting, landslides)
  - volcanism or high seismic activity (8–9 MSK)
  - reservoir upstream
  - impossibility of emergency planning and evacuation
- Usually SPL is assumed at 1E-7

(c) Current IAEA position, reference to IAEA publications

IAEA has long term programmes for updating of the databases and the content of Safety Guides according to Member States' experience. IAEA settled criteria are described in Section 2.

(d) Discussion at the TCM, elements for an evaluation

- While the threshold for exclusion criteria is a matter of discussion, being subjected to convenience and available engineering features, it is extremely important to keep emphasis on the feasibility of evacuation plans and the guarantee of access to the site in case of design basis scenarios. This approach is in line with IAEA *requirements for emergency plans which requires the possibility of their implementation during and after a design basis event, including the EE.*
- TCM discussion expressed his major concern for a correct use of the screening criteria such as SDV and SPL: *they should be used only as initial screening criteria* in the first phases of the project, but their conclusions should be assessed during the safety assessment stage (see Section 2) and during periodic safety reviews.
- It was noted that in many cases some effects from complex scenarios can be enveloped by other scenarios: it is the case, for example, of the fuel spilled from aircraft crash that in some Member States is enveloped by external fire scenario. But there is a concern on different probabilities and also on different provisions for prevention; in the case of sabotage, for example, *it is preferred to have it as a separate scenario*, not connected with explosions or with tornado missiles. The engineering treatment of the scenario is much more consistent.
- The combination of scenarios should be addressed carefully. For example earthquake is responsible of 60% of fire occurrences in North US in conventional buildings. In nuclear plants this percentage is much lower but the interaction effects in general have a high probability of occurrence. *It is recommended to give adequate emphasis to the study of simultaneous or cascading effects in the definition of hazard scenarios from the screening stage*.

4.3. APPROACH TO SITE EVALUATION

(a) Explanation of the issues

- Probabilistic approach in hazard evaluation is more and more used in Member States, but the request of evaluation of the exceedance curve for very low probability values

(of the order of 10E-6 or even lower for PSA) compels engineers to assume mathematical trends for the hazard curve extrapolated from the range where data are available. This process sometimes add high uncertainties to the result, which are not considered any more in the later stages of the design process, and relies on strong mathematical hypotheses, such as a steady state hypothesis, that should be assessed for their compatibility.Moreover, a certain confusion is shown in the engineering community among mean and median values for the statistics.A selection of a suitable statistics and the understanding of their intrinsic applicability limitations was discussed at the TCM.

- For many events a statistic of event at the site is neither possible, because of lack of data, nor meaningful, because of their nature of 'rare' events. In these cases (such as tornadoes, earthquakes, extreme winds, etc.) a different statistics has to be applied on the events of the whole region, integrated with other considerations and numerical modeling to come to a realistic design basis. In the case of tornadoes, for example, a simulation of meteorological events in the region is required; in the case of earthquakes, a strong integration with seismotectonics is needed. Moreover a similar problem is experienced in case there is no monitoring available at the site and therefore the engineers have to look for data in States with similar 'boundary conditions' to define a reasonable hazard.
  A selection of suitable statistics for 'rare' events and procedures for 'similarity' to different States were discussed at the TCM.
- Load combinations are affected by the probabilistic hazard evaluation through two different mechanisms: the combination of events could be screened out because of its very low probability (as often in the case of earthquakes and extreme wind) or the combination might include events which are not extreme but more likely to occur ('grading' in load definition, as in the case of wind or flood). A selection of suitable load combinations was discussed at the TCM.
- In the site hazard definition and in the collection of site related data (investigation campaigns), the accuracy level has to be consistent with the accuracy requested in the overall design. The TCM was requested to discuss relevant topics: methodologies for evaluation of data reliability, definition of the need for further investigation campaigns, procedures in case of data unavailability, compatibility between site evaluation accuracy and design accuracy, consistency of accuracy levels among the different site evaluation phases (i.e.: site survey, site characterization, pre-operational and operational phases).

(b) Results from the questionnaire, databases and practice in Member States

- There is a low correlation in general between site evaluation procedures and nature of data record (e.g.: 'temperature' sometimes is evaluated on probabilistic basis and 'tsunami' sometimes is evaluated on historical basis). Difference between 'rare' and 'frequent' phenomena is generally accepted, but its effect on processing of historical data is not always clear
- Hazard definition is very different between general design and PSA and it had to be re-evaluated very often for PSA studies
- It was noted that the extrapolation to low probability values is often carried out on records of very different length. A detailed analysis on the questionnaire data showed high discrepancies among Member States practice, as can be noted in Fig. 9.
- Graded hazard levels for wind, earthquake, temperature, snow, and particularly for load combination are common in Member States.

- In case of mixed deterministic–probabilistic approach for the hazard evaluation, very different safety margin values are added deterministically on top of the maximum historical data (e.g. for floods the range is 0.3–2 m, for earthquake the range is +0+1 MSK).
- Very often some minimum values (for example for earthquake, aircraft crash, wind) are deterministically defined even in a probabilistic context, meaning the envelope of secondary, minor effects
- The accuracy level in the overall design is affected in the Member States practice by different issues:
  - site parameters (typically: soil structure interaction parameters)
  - design parameters (structural parameters: typically material properties)
  - design procedures (typically: analytical methods versus finite element method)
  - QA requirements (in engineering, procurement, installation) which yield different fragility curves for materials and components. In some Member States, the 'nuclear grading' for materials implies a factor of 4 in costs, but the relevant improvement in global accuracy of the overall design is not easy to be demonstrated
  - There are no requirements in Member States dealing with the correlation in data accuracy between site evaluation and design phase

(c) Current IAEA position, reference to IAEA publications

See Section 2.

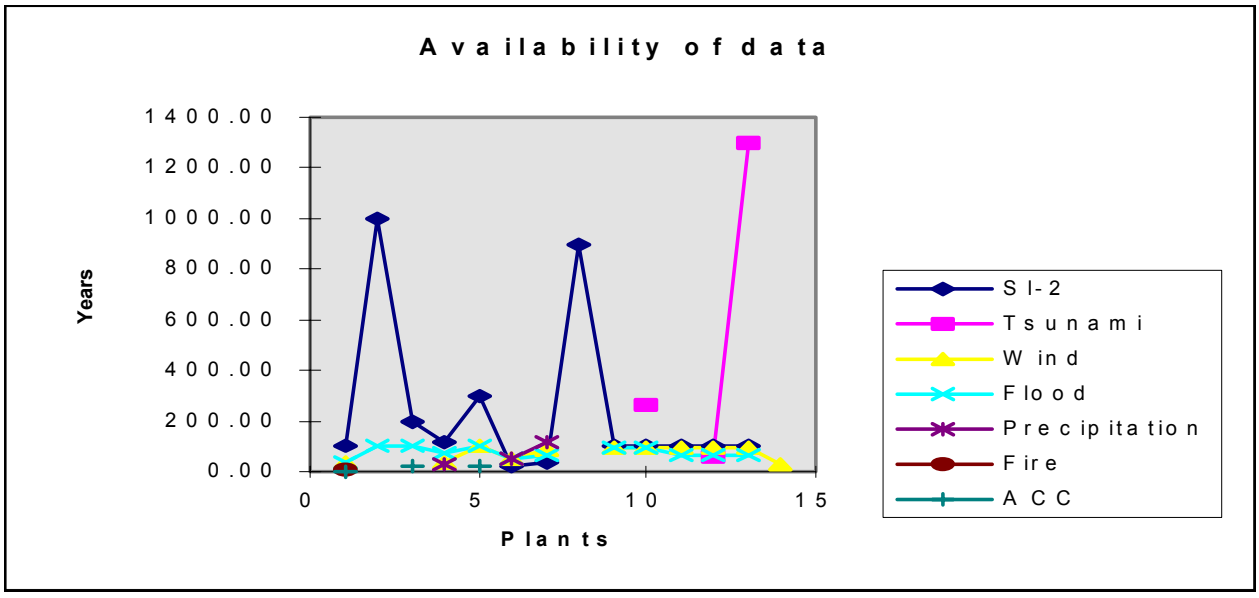

FIG. 9. Record length used in different Member States for data extrapolation for different external event scenarios.

(d) Discussion at the TCM, elements for an evaluation

- The comparison among different Member States should account for the different data acquisition and processing procedures. In fact in some cases data records might show different data and the engineering conclusions could be misled.In the case of wind, for example, an acquisition system of wind speed every 3 seconds is aimed at capturing the gust effect, to be considered for design of local and small items only. A longer sampling, for example at 20 sec, aims at capturing global effects and therefore to support the evaluation of global pressure on buildings and structures. *It is recommended that appropriate technical specifications in the site evaluation phase (and QA) are consistent with design assumptions and methodologies*.
- The derivation of the site hazard is very much dependent on the quality of the database used for data analysis. The lack of local data is chronic and the use of regional or even international data for site analysis might arise some compatibility problems. The only solution seems to be the *heavy use of **local** numerical models with suitable boundary conditions taken from a larger areas*. This is currently done for meteorological events also with interface with marine models for wave and storm surge effects. Recent events enforced the need for such approach (Blayais NPP, see Section 3).
- From the statistical point of view, as a rule of thumb, the data extrapolation should be carried out at a maximum of 4 times the record length, to provide with a sufficient reliability in the result. This statement implies that the request of very low probability of exceedance compels also the designers *to integrate different consideration sources in the final evaluation of the site hazard*. If this is practice in some cases for earthquake hazard, it should be extended also to other scenarios in a similar way, integrating experimental data and numerical models, local and worldwide data, different related disciplines for evidence in past time, etc.
- In some Member States the concern for a reliable extrapolation methods (saw as a responsible for additional uncertainties instead of as a more rigorous approach) suggested the application of deterministic margin over statistical data, referred to a reasonably 'short' length. The discussion was not able to solve the trade off between the two approaches and left to the Member States the evaluation of the most suitable one according also to national experience. It should be reminded that the application of a 'simplified' approach was one of the causes for a recent event, where such additional margin was underestimated
- It should be noted also that the statistical processing on raw data should be carried out only on homogeneous series. *A test for such applicability should be requested* and in general it should help separating different sources that developed into similar effects on plants. The statistics should be carried out only on homogeneous sources, irrespective of their consequences.
- In the analysis of data for the evaluation of the exceedance curves, attention should be paid to the best selection of the most representative parameter for the description of the scenario (and therefore of its effects on structures, systems and components). In many cases the intensity could be misleading, while duration might be a critical indicator of the induced damage. *A two parameter law should be developed in these cases*.
- Availability of data might be influenced also by a sort of 'notification effect': for example in USA the number of occurrences for tornadoes has increased also due to the recent availability of insurance coverage for tornado induced damages. This effect was also observed in relation to events with potential effects on plants, but

developing in the region and not affecting any plant. The example was taken from many aircraft crashes not recorded in nuclear databases because of no interaction with existing plants, but important from the hazard evaluation perspective. *The databases for events should include all these kinds of potential hazard and the relevant statistics include them in their time series*.

- The TCM agreed that, according to the engineering experience, most of the design uncertainty is related to site evaluation issues. Therefore it was recommended to reduce uncertainty in such phase and, when this is not possible at the maximum extent, at least *provide a range to the structural designer for sensitivity analysis*.
- The selection of the statistics to be used in site hazard evaluation is more and more influenced by the perception of the risk that the public opinion has. *This effect cannot be disregarded, but a scientific consistency should be maintained among different sources of hazard*.
- The import of nuclear technology (unified projects) from States where EE hazard levels are significantly different is a very frequent scenario. *A preliminary assessment of the compatibility of the hazard levels among the two States (origin and destination) is therefore recommended*.

4.4. APPROACH TO DESIGN BASIS SELECTION

(a) Explanation of the issue

- In the design phase, the design basis has to be derived from the site hazard. If the hazard is defined in a probabilistic way, some criteria have to be defined (so called design probabilistic targets) to select the reference parameter for the design basis on the exceedance curve. In case a deterministic procedure is followed since the beginning, a probabilistic evaluation has to be carried out a posteriori, at least for comparison purposes.Definition of probabilistic targets is a major issue in this process as they imply connections with the radiation protection targets, with the targets used in design of conventional industrial facilities, with their different potential impact on plant site population, with the targets assigned to internal events (usually less stringent) and with the targets assigned to all external events. The TCM discussed such issues to support a common approach.
- A risk based approach implies a detailed comparison among other sources and among different events. As examples:
  - the explosion of a small LNG tank in the USA in late 1980s has dug a hole 0.5 km radius, 100m deep and killed 1000 people
  - flood and tornado have usually an associated risk lower (10^{-7}) than earthquake (10^{-4}) and both they should be lower than internal events.

In particular, a risk based formulation is rather different for different events. In general terms, the probability of a radiological dispersion can be evaluated as

P(radiological accident) = P(event) * P(overstress) * P(release) (if independent)

In the cases of earthquake, aircraft crash and explosion, this statement can be modified as in the following (figures are taken from the experience in some Member States):

- 10^{-7}/year = X * 10E-2/y * 10E-1/y (for earthquake)

- 10^{-7}/year = X * target exposure * target capacity (for aircraft crash)
- 10^{-7}/year = X * NPP exposure * target features (for explosions)

According to these examples its is also clear why in some Member States P(event) is reduced around 10^{-5}/year (also used as SPL value) and it is coupled with analysis of engineering provisions.

Therefore the TCM was requested to evaluate the appropriateness of old ('min–max' approach, when the maximum event recorded in the region is located at the site) and new (probabilistic, risk based) approach, with attention to the targets for single events and for combined events.

- The probabilistic definition of design targets implicitly requires the development of probabilistic safety assessment for the plant. The IAEA Safety Guides recommend the development of such a tool, but it is not yet common practice in Member States. Particularly its reliability in decision making processes is still a matter of debate in safety authorities. The TCM discussed the topic trying to suggest alternative methodologies to guarantee the design targets even in case a full PSA is not available.
- The explicit evaluation of the safety margin of the overall design is usually not requested as it is implicitly guaranteed by the design standards. However, the complicated interaction with site related data, the adoption of different standards for the same project, the potential existence of 'cliff edge' effects and the common implementation of re-evaluation programmes with different requirements than the original design sometimes makes the evaluation of the safety margin (or probability of exceedance of design targets) very difficult. The TCM discussed the need to carry out such assessment and the most suitable methodologies.
- The evaluation of the overall safety margin of a design is not usually a straightforward task. Conservatism and margin are typically stored in many steps of the project, as shown in Fig. 10.

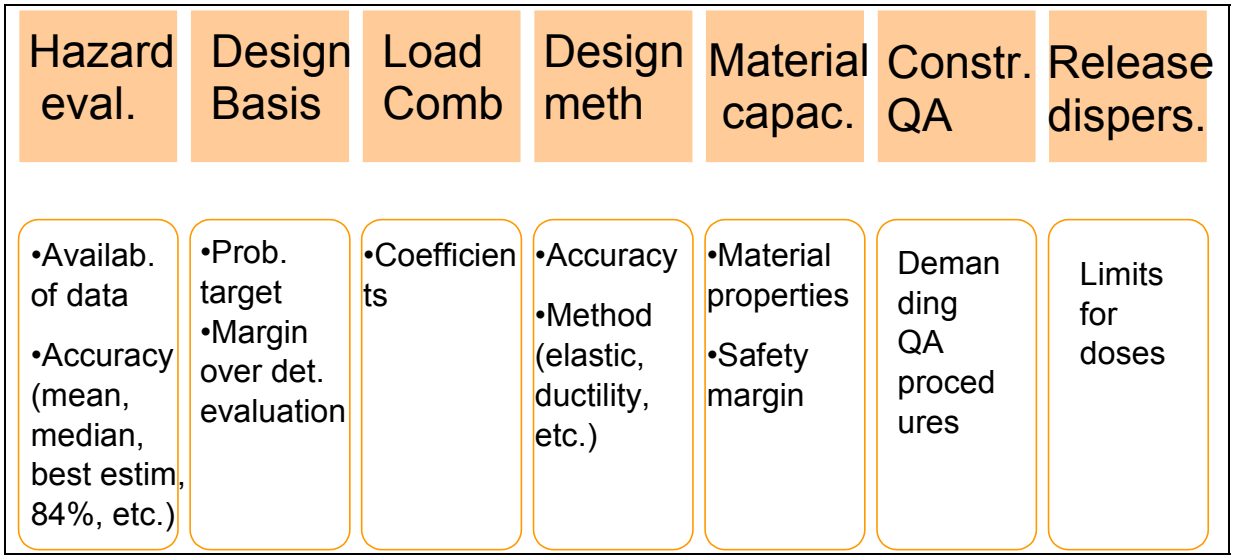

FIG. 10. Location of margins in the whole design process.

The TCM discussed the most reasonable approaches for a safe design and the effective methodologies for the evaluation of a safety margin.

(a) Results from the questionnaire, databases and practice in Member States

- Few States show a regulatory limit anchored to the **risk** of radiological hazard, usually selected at 1E-6 (it corresponds to a limit on the result of PSA level 3) or even represented as a curve probability–dose, while most of the States have a mixed approach deterministic and probabilistic on hazard definition, but not risk based. In some cases both are required and priority is given to the probabilistic one. Many PSAs have confirmed 'reasonable' and consistent targets, however, in most States, PSAs are not available yet.
- In some Member States, there is a limit to the contribution of any external event to the core damage frequency (CDFM): it has to be lower than 10% of the total value.
- There is a total disagreement among Member States on the selection of the probabilistic targets (flood, temperature, wind, snow could reach 1E-2) which looks also totally uncorrelated with population density and industrial installations close to the site. In some cases, natural hazard have different design targets even in case of States upwind and upstream: the design approaches look too much State dependent and there are few attempts to homogenize the requirements, at least for neighbouring States.
- In some Member States the design basis for most scenarios is evaluated with reference only to the probability of exceedance for the hazard, while in most of them it is based on the evaluation of the combined probability of exceedance in the radiological release where major contributions are coming from the hazard, the fragility and the release mechanism (maybe converted into conservative and deterministic estimates at the end). This difference leads in the former cases to a factor of 2–3 to be applied to the design loads considered for conventional installation, while in the latter ones this factor is in general much higher.
- In some cases different units at the same site have different hazard (there is a sort of 'contractor' dependency)
- There is a general confused practice in the selection of standards for site hazard evaluation and therefore for the design target selection: in many Member States nuclear and non nuclear requirements are mixed without a clear understanding of the different involved risks.
- In many Member States a design target is defined for the combination between external event (usually set at 1E-6,7) and between external and internal events (80% of Member States combine LOCA and SL-2 earthquake)
- The most common approach for safety margin in Member States considers the safety margin mainly in the hazard evaluation phase and in material capacity evaluation, but a global policy is seldom explicit and not correlated with other facilities at different risk.

(b) Current IAEA position, reference to IAEA publications

In the Safety Guides review process, the following items have been added to the Safety Guides:

- Decommissioning implications
- Multi-unit sites
- Different hazard at different construction stages of the plant

- Plant dependence for site hazard evaluation: site destination, site reuse, life extension and beyond design basis considerations

In general the Safety Guides do not recommend numerical targets, leaving the Member States the maximum freedom, and do not suggest exclusion criteria, as they are affected in general also by non-safety aspects. A strong emphasis is on the feasibility of emergency planning and availability of reliable siting data.

However, some criteria are suggested in Safety Guides for design target homogenization among different States, from the conceptual perspective:

- Installed thermal power in the facility
- Need for active safety systems to cope with mitigation of postulated accidents; amount of engineering features implemented for preventing and mitigating serious consequences from accidents
- Characteristics of the process or of the engineering features which might show a sort of 'cliff edge effect' in case of an accident, without possibility to prevent the degeneration into radiological consequences
- Characteristics of the event (e.g. wind and explosion have a high potential for dispersion, while earthquake and aircraft crash have a minor contribution on the dispersion)
- Environmental characteristics of the site relevant to dispersion (e.g.: windy area, sea site, etc.)
- Feasibility of an efficient evacuation and emergency plan
- Potential for long term effect in case of contamination (long lived radionuclides, persistent effect in the environment)
- Number of people potentially affected by an accident at the facility.

In general the identification of the design probability target should be carried out consistently with the comparison with other risks and standard for design of relevant facilities. Some useful references could be found in [39, 40] where a broader review of probabilistic risk evaluation is described, with reference to sources of hazard for public and environment other than nuclear.

- All possible operational states should be considered in the design against EE, particularly: operation, maintenance, effect of external events on evacuation plan and emergency procedures
- Safety Guides now recommend a PSA in the design as confirmation of site evaluation analysis [10]
- Safety Guides recommend a strong emphasis on consistency in the accuracy level between siting and design phases, for a global safety assessment of the plant.

(c) Discussion at the TCM, elements for an evaluation

- Design targets defined in terms of risk are difficult to be applied in practical design, mainly based on deterministic procedures, and in some cases the uncertainty they implicitly carry, related to the PSA level 3, suggest simplified but *more realistic approaches based on the probability of the event and on engineering experience*. For example the following set of thresholds is usually considered reasonable:

- SPL: 1E-7
- Conditional probability for rad dispersion: 1E-6, 1E-5
- Design target: 1E-4, 1E-5 (mean)
- Threshold for operator action (see below): 1E-2

Of course it is recommended to assess such values in a safety assessment context, also to evaluate a reasonable balance among different scenarios (radiological risk should not be dominated by a specific event, either internal or external). *A risk comparison* with other installations in the State, even not nuclear, is also extremely useful for a proper grading between conventional buildings and NPPs.

- *Definition of design targets should account for the combined effect of uncertainties in hazard evaluation, fragility and release mechanism*. Particularly, the contribution of the fragility is very much dependent on the construction technology and design assumptions; for example the earthquake scenario can rely on a structural ductility contribution always available (at different levels) in usual nuclear installations, while flood cannot benefit from such gradual mechanism and reserve of capacity.
- The probability associated to combinations of events should account for the characteristics of the effects. For example, the duration of the effects from a certain event combination can be much longer than the duration of the events themselves and therefore *the former duration (and not the latter one) should be considered in the probability to be associated to the combination*.
- Life extension in a plant might change the selection of its design basis. *This item should be addressed* in the licence extension process.
- *PSA should be used in design* to carry out the following tasks:
  - to check compliance with probabilistic safety targets, to check the consistency between design targets for internal and external events
  - to drive maintenance and operation providing priorities
  - to support plant modification strategy, both in the decision of the priority items to be modified and in the evaluation of the compliance with the safety goals
  - as a 'learning tool': the evaluation of the most convenient mitigation strategy for selected EEs should have useful outcomes for the deterministic design.

IAEA safety standards require [10] the completion of PSAs for NPPs as a standard practice in the design.

- *Some issues should be considered* to guarantee an effective implementation of a safety margin policy in the design against EE, such as:
  - 'design robustness', to be understood as: high quality design, low sensitivity to variation in parameters, consideration of BDBE, high conservatism and demonstrably conservative
  - clear accident management programme
  - consistency with SPL screening approach in site evaluation
  - provisions for maintenance of safety levels in time

Moreover, the selected policy should be consistent in all site evaluation and design phases, with an efficient management of the uncertainties induced by any design process in the evaluation of overall design reliability.

- Many procedures are available for the evaluation of the safety margin of the overall design. Mainly two are in use in Member States:
  - SMA approach [41]: it aims at the quantification of the margin without increasing the design basis. It assumes the margin lies in hazard and in material capacities, leaving a median value to the calculation methodology (fragility). The selection of the RLE compared with the DBE in case of the earthquake should be consistent with this approach.
  - CDFM approach [42]: it aims at carrying out in a deterministic way a simplified probabilistic analysis of the combination of demand and capacity uncertainties

  Recommendations on their best application are provided in the dedicated references.

- Design basis is in some Member States very much layout dependent. Typical case is the load function for aircraft crash defined in some European States where a different function is suggested for 'corners' and for 'large slabs'. This approach was not encouraged at the discussion as it requires many engineering assumptions and the final safety assessment is not easy and convincing in some cases.

4.5. EXTERNAL EVENT CLASSIFICATION AND SITE PROTECTION FEATURES

(a) Explanation of the issue

- The application of defence in depth principle and single failure criteria to NPP protection against external events is not straightforward from the general design requirements: many passive systems are involved, site protecting measures are part of the defence (but often not regarded as safety related) and the redundancy provision is not always very clear. The TCM discussed the details of the application of general safety concepts to the protection from external events.
- The safety classification criteria for systems and components could be complemented by a classification in relation to external events consistently with the safety classification, seismic, QA, etc. The IAEA approach is described in Section 2, but essential details are still to be clarified, such as: the safe shutdown equipment list for external events, the safety criteria and the performance criteria.
- Design of site protection measures: recent events highlighted the need for a consistent design basis among the protection structures and the plant itself to avoid discrepancies.

(b) Results from the questionnaire, databases and practice in Member States

- Protection form external flood has some redundancy in some Member States practice, but this is not the case for wind and other external events (EE)
- Seismic and safety classification are always requested in Member States practice, but the connection between the two is not always very clear
- In some cases EE classification is assumed coincident with the seismic one
- Passive barriers do not have redundancy and often the design of the plant relies on their effectiveness and therefore some events originated outside the site are excluded from plant design basis
- Site protection measures in Member States have different arrangement:

- flood: dry site, dykes, drainage systems, breakwaters
- temperature: heating of water intake
- in-leakage and corrosion: cathodic protection

Many site protection structures have been designed with conventional standards and not regarded as safety related for maintenance, monitoring, review, etc.

(c) Current IAEA position, reference to IAEA publications

In the Safety Guides review process, the following items have been clarified.

- Site protection measures should be safety classified
- Adequate design provisions should be considered so that the general safety requirements can be met. To perform the safety functions required for DBEEs the designer can use either systems specific to external events or the safety systems already present in the plant for internal events. In both cases, the design of the plant for safety should have due regard for the single failure criteria; this may be achieved by redundancy of safety systems.Common cause failure should also be considered for external event PIEs together with the requirements for redundancy of passive systems [10]. Defence against common cause failures includes quality, segregation and diversity [13]: the safety analysis should evaluate their effectiveness in case of external events.To this concern, there are two basic forms of plant protection against EE:

  (a) either the influence from an external event is reduced by means of a 'passive barrier' (e.g. 'dry site' for flood, site protection dam for flood, external shield for ACC, barriers for explosions, building base isolation for earthquake), (see Fig. 11)
  (b) or the ability of the safety systems to resist those influences can be increased

The solution should represent the best balance among safety, operational aspects and other important factors. For example, an inherent capability to withstand localized events (e.g. aircraft crash) can be provided by physical separation of redundant systems, such that the simultaneous failure of the redundant systems due to the effects of building vibration, debris or fire from aircraft fuel is precluded. Otherwise, it will be necessary to provide additional protection in the form of barriers or to increase the spatial separation by the modification of plant layout.

In general, external events may challenge many levels of the defence in depth. The basic plant protection should be addressed in the first level of defence, according to [10], either through an adequate design of all the physical barriers or by component qualification. However, all the levels should be designed against the external events to guarantee that in case of an internal DBA all levels of defence are in place. Probabilistic evaluations should be carried out for the definition of suitable design combinations between external events and internal accidents, addressing both their potential correlation and their joint probability.

However, some external events included in the design basis may be associated with very low probability and catastrophic scenarios: examples could include large aircraft impacts, devastating explosions in the plant vicinity and extreme floods. The evaluation of their effects on the plant can be affected by high uncertainties, for the following reasons:

- extreme external events with very low probability of occurrence could have effects not properly foreseen in terms of their action on the plant and/or their magnitude;

- the estimation of the effects from extreme external events is affected by gross uncertainties, discussed in Safety Guides [5–9] for the hazard, but not explicitly considered in a deterministic design;
- there is an intrinsic lack of operating experience concerning the effects that such extreme events could have on plant safety, due to their low probability of occurrence.

For these reasons, the design of a full scope protecting barrier may be unreliable and in some cases even unfeasible[1] and a challenge to one level of defence may be envisaged.

In these cases some special engineering approaches may be put in place, including all or a selection of the following measures:

- the selection of systems required for plant protection against such events may be less stringent than for other DBEE, including only a subset of safety classified items, usually only the items in the safety group of the extreme events
- only load combinations with the most probable plant statuses and operational modes are considered (i.e. no accident states and no refuelling or maintenance conditions with the containment open)
- lower safety margins or reduced acceptance criteria compared with other DBEE may be specified for items pertaining to the third of fourth level of defence in depth (mitigation of design basis accidents and of severe accidents)
- best estimate rather than conservative material properties, design and analysis methods may be used.

However, if such a challenge to a level of defence in depth is envisaged, dedicated operational procedures should be put in place with reference to limits and conditions for normal operation (NOL), supported by adequate warning systems (when possible) and monitoring (see sections below). Moreover, a dedicated probabilistic evaluation should be carried out on the consequences of these special assumptions.

In addition to that and particularly in the case a) described above, it is reasonable relying on passive barriers according to [10], but due attention should be paid to provide adequate capacity for events beyond design basis, avoiding ‘cliff edge’ effects as far as possible (e.g. in the case of a site protection dam, as soon as the dam is overtopped with a small additional water level, the site might be suddenly flooded at the maximum level of the flood. See Fig. 12). Additional engineering provisions should be implemented on safety systems at least for a safe shutdown mode.

In synthesis, the protection strategy for EE can be summarized as in the following [13]:

- For *frequent* events (typically wind and snow): only qualification and/or segregation is required
- For *extreme* events (typically earthquake, aircraft crash, etc.): qualification and segregation or barriers + operational and safety limits (for earthquake, ACC, etc.). Design basis for the site will be only related to the effect ‘filtered’ by the barrier (e.g. in the case of an acc, only the vibration filtered by the external shield will be considered in the design of the internal equipment)

[1] This is the case, for example, of a containment building subjected to a large aircraft crash: its leaktightness is usually not required.

- However, when *cliff edge effects* (e.g. floods) are present, protection of the safety group (safe shutdown path), with redundancy, is required. The design basis of the safety group is 'reasonably' lower than the design basis of the barrier. In this case, the *safety group* (safe shutdown path) for the event will be designed against flood either
  - with additional internal barriers
  - by direct qualification of exposed items
  - by use of warning, monitoring systems and operational procedures

Operational and safety limits will be implemented (see below) for a proper and timely operator action.

- Special operational procedures should be defined, based on the real time monitoring data of the identified flooding causes, when events have a 'slow' rising time.
  This approach is considered acceptable provided a warning system is available able to detect a potential site challenge with sufficient time to complete the safe shut down of the plant, accompanied by the implementation of the adequate emergency procedures.

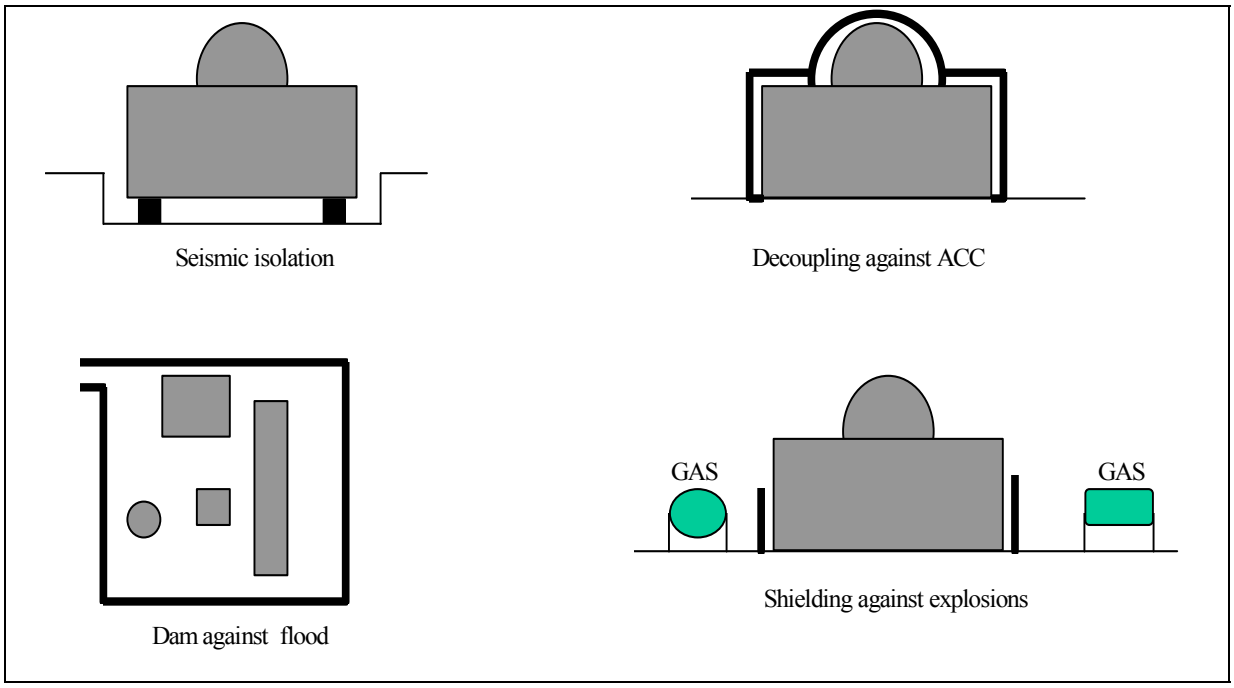

FIG. 11. Protection of the plant by a barrier against external events.

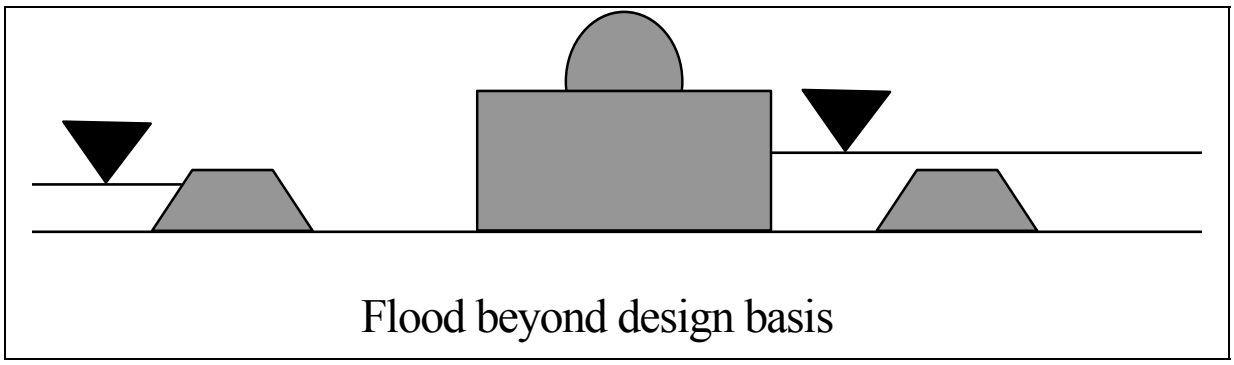

FIG. 12. Example of a 'cliff edge effect' in case of flood.

- All warning systems, powered with protected off-site power supply, should be designed to withstand the event producing conditions (e.g. in case of a site flooding, they might be represented by wind, landslides, etc.) that are considered characteristic of the geographical region where the site is located (excluding extremely rare combinations).
- An EE classification (including the seismic one) is developed in Ref. [11], compatible with the safety and the seismic ones, for a more consistent and rational design process.

(d) Discussion at the TCM, elements for an evaluation

- *Fire protection features should be classified* for external events and their inadvertent activation excluded in case of extreme events to avoid impairing of operator actions or interaction effects on safety related items
- Classification aspects concerning operator access and physical interaction scenarios during an event should have more emphasis and dedicated requirements

4.6. SITE MONITORING AND OPERATOR ACTIONS DURING EXTERNAL EVENTS

(a) Explanation of the issues

- Monitoring issues: the main goals for monitoring systems at the site are not always very clear as they can support different tasks: 1) support operator actions during an event, 2) confirm design assumptions, 3) support long term periodical safety review. In some cases they are safety related and according to such classification, responsibilities for data acquisition, processing and reporting should be defined. The TCM discussed the proper framework for each system.
- In case of monitoring systems designed to support operator actions or to activate emergency planning, methodologies for forecasting event evolution should be defined and operator actions clarified in case of extreme events, in particular: the logic of the alarm system, the threshold for the forecasting, the compatibility with time needed for reactor shut down, the items to be inspected after a significant event, the procedures for inspection.

(b) Results from the questionnaire, databases and practice in Member States

- The most common monitoring system (or procedures) in operation in Member States for EE are: meteorological, seismic, flood, chemical gases, settlements, radiological, population density. Only in few cases there are clear responsibilities and operating procedures
- Operating procedures rely upon monitoring systems only in case of flood, wind (33 m/s), and earthquake (OBE)
- Forecasting is never mentioned in the questionnaire, but it is a new practice in few Member States
- Procedures for post event inspections are not mentioned in the questionnaire: only very few States defined the responsibilities, the extent, the procedures.
- Administrative measures in Member States in relation to EE are often limited to: limitation to air and ground traffic, definition of ‘exclusion zones’

(c) Current IAEA position, reference to IAEA publications

Site monitoring may have different targets [11]:

- For design confirmation
- For operator actions (OLC)
- To support periodic safety reviews (PSR)

A site monitoring is requested when the EE is 'sizing' for the plant.

Particular Operating Limits and Conditions (OLC) should be defined for any EE that proves to be important for plant design, in terms of relevance of the hazard, contribution to sizing of safety related items and contribution to the results of PSA. They should be associated to dedicated surveillance procedures (pre- and/or post-event), a plant safe state (possibly a reactor shutdown) to be reached in case of 'abnormal' events and a post-event revalidation procedure for any item important to safety which may have been challenged.

A set of operational limits should be defined for items classified for external events, derived from Ref. [20]:

- safety limits (SOL): they are specified in the safety classification (and also in the EEC) and represent the design basis conditions for the items. Their exceedance represents a challenge for the plant safety and therefore a plant shutdown is required with precise post-event revalidation.
- limits and conditions for normal operation (NOL): they represent the limits for a safe operation with due consideration to the uncertainties of the design process described above. They do not affect the design being intrinsically related to the uncertainty of the hazard for very low probability of exceedance. Their exceedance is preliminary to the activation of the safety systems in the safety group able to bring the plant into a safer state, such as power reduction or reactor shutdown. Resuming operation is conditioned to appropriate investigations on causes and effects.

In any case in relation with an external event development, the plant should start shutdown if any of the following conditions is met:

- when the operating personnel cannot ascertain that the power plant is being operated within OLC;
- there is any evidence of damage to classified items;
- there is reasonable confidence that the OLC will be exceeded in a shorter time than that needed for a shutdown, according to reliable forecasting procedures on the event development (e.g. for flood or cyclones)

NOL should be specified for any EE that proves to be critical for plant design, in terms of relevance of the hazard, contribution to sizing of safety related items and contribution to the results of PSA. They should be specified in the hazard evaluation phase and adequate procedures should be implemented for their monitoring and for the prompt evaluation of their exceedance, to be specified in terms of all the parameters affecting the hazard definition.

If design provisions to protect the plant against the EE has followed the strategy a) above (i.e. a passive barrier to reduce the EE effects on the plant), NOL should be referred to the barrier safety function and therefore plant operation can be extended up to SOL, assuming a high degree of conservatism in the design of the barrier, provided no 'cliff edge' effects are foreseen.

Concerning the post event operator actions, most of the experience in Member States in monitoring and related operator actions concerns the earthquake protection. According to that, IAEA set up some recommendations to drive the decision either for an automatic scram system or for a seismic monitoring supporting operator action. Such criteria are listed here below:

- Level, frequency and duration of earthquake activity at the NPP site: in case of low seismic activity an automatic system is rarely justifiable.
- Seismic capacity of NPP structures, equipment and distribution systems: particularly in case of seismic hazard re-evaluation, automatic systems could be useful.
- Safety considerations related to spurious scrams: in case of high ambient noise, also induced by other plant equipment, it could be advisable to avoid any automatic system.
- Expected time of seismic scram and comparison of this time to the expected time to reach the strong motion part of the earthquake time history: the automatic scram is efficient only if it enables a trip of the reactor before the maximum shaking of the earthquake. If not, the transient which will result from the trip will be superimposed on the seismic transient and may further challenge the plant equipment.
- Broad ranging safety issues related to the consequences in the State from a shutdown of the plant immediately following an earthquake.
- Level of operator confidence and reliability: in case of a non automatic system, the operator plays a major role in the decision of post earthquake actions.

In any case the lower trigger level (alert) should be close to SL-1 (usually associated to operational limits), where significant damage to safety related equipment is not expected. In case of seismic capacity lower than SL-1 (for example during the process of hazard re-evaluation), such level should be referred to the real plant capacity.

In case of an automatic scram system, the highest trigger level (reactor scram) should be close to SL-2, but consideration should also be given to the fact that usually at such levels of earthquakes, major destruction in the site vicinity is expected, including loss of off site power and alteration of water supply needed for residual heat removal. The whole emergency procedures and operator actions should be consistent with such scenario.

The sensors should be located preferably at the free field and at the location of safety related equipment in the plant[2]. The trigger levels should be adapted to the location of the sensors in the plant, according to the seismic design results.

In case of multiunit sites, the scram logic should be co-ordinated among the different units.

The control panel of the system should be located in the control room for an easy access by the operator.

[2] A minimum amount of sensors is usually installed at nuclear power plant sites as follows:
(1) One triaxial strong motion recorder installed to register the free field motion time history.
(2) One triaxial strong motion recorder installed to register the motion of the base mat of the reactor building.
(3) One triaxial strong motion recorder installed on the most representative floor of the reactor building.

Both post earthquake operator actions and automatic scram should be based upon a proper set of parameters derived from the recorded data, but suitably processed with two main goals:

- to avoid spurious signals;
- to develop an indicator of damage, representative of the exceedance of the design spectrum

Such goals could be delivered with appropriate software based on the combination of the signals from different locations and directions (spurious signals could be filtered out), appropriate filtering of the frequencies in the signal (in order to remove the contribution of the non-damaging part of signal) and evaluation of cumulative damage parameters, substantiated by walkdowns.

Cumulative damage parameters should be mainly based on the integration of the acceleration record, thus providing a more representative parameter of an earthquake induced damage in the safety related equipment. Such values should be compared with the same quantities derived from the free field design basis earthquake, but analogous comparison in other locations of the plant is recommended as it could provide a good support for the post earthquake walkdown and therefore for the decision of the plant restart.

Post earthquake actions should be organized even when an automatic scram system is installed.

The control room operator should be informed of the occurrence of an earthquake by the installed seismic instrumentation. Subsequent responses should include an evaluation of recorded earthquake motion as compared to the specific design of structures, systems and components, a walkdown evaluation of the damage experienced at the NPP and an evaluation to determine the readiness of the plant to resume (or to maintain) operation following the earthquake occurrence.

The item list to be inspected in such walkdown should be consistent with the safety and seismic classification of plant items. Type, extension and location of tests to be carried out after an earthquake should be clearly defined and directly related to the expected damage from earthquakes.

For practical reasons they might be limited to visual inspection of accessible items and to validated comparison with the seismic behaviour of all other safety related items.

Different levels of such inspections could be defined according to the experienced earthquake level damage (measured through appropriate analytical parameters): different responsibilities should be identified accordingly among the operators, the technical support in the plant and external specialized teams.

Also the notification to the Safety Authority and its involvement in the plant restart should be defined in appropriate regulatory procedures, according to the main assumptions in design and classification.

(d) Discussion at the TCM, elements for an evaluation

- Site accessibility (for example by operator shifts and/or fire guards) and possibility for operators to move at the site from building to building during an extreme event was highlighted, also with reference to many recent incidents.

Moreover, many emergency generators and sprinkler systems deemed their weakness in recent earthquakes, also impairing the operator access to critical areas. *Operator accessibility should be requested during and after EEs.*

- It was noted that the shut down of nuclear units requires 6–8 hours as an average: this time should be accounted for in the logic of operator actions supported by monitoring systems. Moreover, for multiunit sites in case of events able to induce common cause failures, *this time has to be multiplied for the number of units.*
- In case of events without warning, such as earthquakes and tornadoes, operator procedures should be different. Operator procedures should be differentiated according to the *warning time and a proper interface with monitoring systems should be defined with thresholds for the operator actions.* In case of short time alert, only measures on lifelines, personnel, temporary barriers, fuel supply etc., can be put in place as **additional** measures to the design engineering provisions (i.e. no credit is given to short term actions in a design and safety assessment framework).
- The availability of a suitable forecast for 'slow developing' events demands for *reliable communication channels* with the operators (safety related) and for a sort of involvement in the responsibility for accident management. Experience of France (for floods) and the USA (for tornadoes) can be used as a reference for other Member States.
- The selection of thresholds to drive operator action in the interpretation of forecasting should address different hazard levels (e.g. operational limits, safety limits, etc.) and should consider at least two basic parameters: the rate of development and the maximum expected values for the phenomena. An uncertainty value for the forecasting should also be added to the evaluation. Some *level of freedom for operator judgement should be inserted in the procedures* and therefore an automatic decision taken only on the base of the forecasting models should be avoided, due to their intrinsic high level of uncertainty of meteorological models.
- It was noted that operator action could be strongly influenced by the emotional environment. Therefore, the communication channel with the areas surrounding the site is important also for a reliable operator action, particularly in case of events with very short warning time.
- Procedures for post-event inspections should be developed with reference either to probabilistic methodologies or deterministic procedures for the evaluation of the safety margin in order to priorities item contribution to safety in case of a selected PIE. The SMA [41] approach was identified as one of the most suitable technique to be used in this framework.
- An evaluation of degradation effects induced by an extreme external event affecting a plant should be carried out in most cases and relevant upgrading of expected service life for SSC completed. There is no evidence of major degradation (for example after earthquakes) according to available operational experience, but the mechanism is possible in principle. The issue is even more critical in cases where plant construction is suspended for a period of duration comparable with its expected operating life. In this case, the degradation of installed SSC may show mechanisms very different from those considered at the design stage, as the plant withstood the events in a non foreseen status. *A detailed evaluation should be carried out with large use of available techniques for ageing and degradation evaluation, with reference to the real history of the plant*.

4.7. ADMINISTRATIVE ACTIONS

(a) Explanation of the issue

The modification of potential sources (e.g.: rerouting of air flights) and the impact of external events on the neighbourhoods of the plant but affecting the plant (e.g.: availability of access routes for emergency teams and or operator shifts, etc.) are typical example of administrative measures that should be connected and controlled by the plant management. *The TCM discussed the topic with reference also to the different responsibilities involved and to their effectiveness throughout the plant life.*

(b) Results from the questionnaire, databases and practice in Member States

- Administrative measures in Member States in relation to EE are often limited to: limitation to air, water and ground traffic, definition of 'exclusion zones'

(c) Current IAEA position, reference to IAEA publications

- Administrative actions are needed to protect evacuation routes and access to the plant, as guarantee of the effectiveness of emergency planning

(d) Discussion at the TCM, elements for an evaluation

- The major problem for the application of administrative measures seems to be their enforcement in the long time and the number of different authorities involved. Therefore it was recommended that *major design assumptions rely on engineering features instead of administrative measures*, to guarantee a better control of design assumptions in time.

4.8. PERIODIC SAFETY REVIEW AND RE-EVALUATION OF EXISTING PLANTS

(a) Explanation of the issue

There is a rising concern for a periodic review of site hazard evaluation requested by evidence such as: climate change issues, modification of land use, of population distribution of industrial exploitation. Forecasting techniques are then considered and periodic safety review are more and more required to be a systematic process that is carried out to ensure that all relevant safety requirements are met by the site during the whole lifetime of the plant.

Particularly, concerning the climate change issue, the following data are commonly referred to by scientific community under the label 'global warming':

Current evidence

- +0.3–0.6 ºC in air temperature over the past century
- +10–25 cm sea level rise over the past century
- larger anomalies since 1976 (El Nino)

Expectations

- +1–3 ºC in air temperature in the next century (greater than in the past 10,000 years)
- +15–95 cm sea level rise in the next century
- a great portion of warm season precipitation will come in heavy showers instead with long lasting gentle rains

- persistence of CO_2 for centuries, with delayed effects: the extrapolation on current data could be misleading

The TCM discussed the issue and provided recommendations for relevant modifications in PSR procedures.

- Re-evaluation of existing plants: the re is a rising demand for such task but specific requirements are generally lacking and upgrading measures are implemented in very different ways among Member States.

(b) Results from the questionnaire, databases and practice in Member States

- In Member States practice, there are no 'discounts' on hazard evaluation for existing plants compared to new design
- Ductility in seismic structural evaluation is common practice in re-evaluation of existing structures
- In few cases a full 'risk based' approach is allowed in plant re-evaluation phase with considerations to cost, risk and remaining life of the plant (as low as reasonably achievable (ALARA) approach)
- In most cases formal PSR are requested every 10 years (few exceptions at 5 years). In some cases PSR are not required, and regulatory action is limited to ISI and periodic testing

(c) Current IAEA position, reference to IAEA publications

- Re-evaluation of existing plants is not addressed in Safety Guides
- PSR is required as guarantee of the safety of the plant and it is mainly dedicated to the review of the hazard evaluation and of the design basis, based upon [43]:
  - new evidence (global warming, accidents, etc)
  - construction of additional units at the site
  - modifications in communications, evacuation routes, grid characteristics and protection
  - new industrial installations, population growth, change in land and -water use, aircraft routes, deforestation
  - results from monitoring
  - new legislative framework
  - operational experience (IRS, etc.)
  - availability of scientific studies and extensive data collection

(d) Discussion at the TCM, elements for an evaluation

- In case of 'small' deviations from original design basis, as a result of the periodic safety review, there is a general confidence in Member States that the deviation can be accommodated in the 'design robustness' and improved surveillance procedures.
- It was considered that methodologies like SMA [41], originally developed for seismic re-evaluation of existing plants, *could be well applied to all the following tasks*, mainly activated during a PSR:
  (1) seismic re-evaluation of an existing facility: in that case RLE can be assumed as SL-2 and the SSEL should include the 'safe shutdown equipment list'

(2) evaluation of the new safety margin of the plant after the design modifications that usually are implemented. All safety classified items should be involved in the safe shutdown equipment list in this case
(3) elimination of some useless conservatism, if any, applied at the design phase as a consequence of unavailability of appropriate investigation or design methodologies
(4) qualification of isolated items (equipments and components)

- It was noted that both design and siting *feedback experience from conventional installations could be very useful for the nuclear industry*. In case of recent earthquakes, for example, the importance of operator access, of availability of emergency generators and of fire protection systems, and some provisions in the design (typically the detailing of the reinforcement at the structural joints) suggested an adequate consideration also by the nuclear community, to avoid similar scenarios.
- In some Member States the plant protection strategy could be different between new and existing plants: for floods, for example, removable protections are allowed only for existing plants.

5. COMMENTARY FROM MEMBER STATES

In this section, contributions from Member States on selected topics are collected. Each section was originally prepared by a different author and revised by the technical officer, therefore in principle they bring the experience of specific States. However, the authors tried to provide a detailed overview of the selected topics, preliminary to further discussions, more than a solution to the pending open questions. Therefore the whole section could be seen as a more detailed explanation of the issues identified in the previous sections, with some attempts for a unified solution.

The issues discussed in this section are:

- Definition of design basis: probabilistic versus deterministic
- Margin methodologies versus probabilistic safety assessment: load definition, load combinations and basic references
- Beyond design basis external events: basic philosophy
- Limit states and acceptance criteria in relation to EE
- Effectiveness of administrative measures
- Sabotage and war related scenarios: enveloped by EE?
- Sites with low hazard from EE
- Basic statistics for probabilistic treatment of EE hazard

5.1. DEFINITION OF DESIGN BASIS PROBABILISTIC VERSUS DETERMINISTIC

External events applicable to NPPs can be characterized as human induced events or natural events. For either type of event, the magnitude can be highly variable, for example seismic events or vapour clouds from nearby industrial facilities, or they can be more tightly bounded, for example air temperatures or ground borne vibration.

In the definition of a design basis or of a basis against which existing NPPs can be assessed, two fundamental approaches can be defined, probabilistic or deterministic. In practice, there is frequently overlap between the probabilistic and deterministic approaches.

5.1.1. Experience in Member States

The experience in Member States of the choice between deterministic and probabilistic selection of design basis is variable.

For some types of external events, the majority or all of the Member States use probabilistic methods to determine that no design basis is required (screening). For such external events, the initial selection of the site and/or topography ensures that the event could be defined as incredible with the probability of occurrence below 10^{-7} per annum. Examples of such events could include volcanic activity.

For other design basis parameters such as ground water levels (giving rise to buoyancy effects) or settlements, the majority of the Member States adopt deterministic methods to define a design basis. Generally in such cases, the causative effect can be constrained within specific limits and the difference between a probabilistically and deterministically defined design basis would be small.

For most of the major design basis parameters, which have potentially significant effects on the overall safety and cost of NPPs, the Member States approaches are more variable, with some states selecting a design basis using deterministic methods and others using probabilistic methods. In addition many Member States use a combination of both methods.

5.1.2. Benefits of deterministic definition of design basis

For a number of external events, such as slope stability or ground collapse, the parameter is entirely site specific and no or limited historical data exists from which a design basis can be assigned. In such cases, where the physical conditions at site limit the extent of the design basis, then a deterministic approach is essentially the only possible route.

For a further group of external events, the historical archive is very unreliable or the statistical methods by which historical data can be interpreted are unreliable. For such events, a deterministic definition of a design basis is no more or less valid than a probabilistic method and can require less justification.

In the initial design phases of an NPP, or when an existing facility is being reassessed, a deterministic definition of a design basis can provide a simple route to allow the design to proceed prior to a rigorous justification of the various design parameters. In addition, this method of determining the magnitude or extent of an event can be used to define siting and segregation parameters, which are also required early in a major project.

Minimum ‘national’ standards can be used to define characteristic design basis events. These typically correspond to 1:50 year or 1:100 year targets, and can provide a useful design basis for combination events. These standards can also be selected in the early stages of a project and by enhancement used to define extreme events until a more rigorous justification becomes available.

5.1.3. Benefits of probabilistic definition of design basis

Most notionally deterministic design basis events are in fact underpinned by some degree of probabilistic definition. National standards for external events such as

meteorological conditions are generally based on observed evidence, historical data and statistical manipulation.

Probabilistically defined design basis events can be used to justify that the NPP meets risk based criteria. They can also be used to show that the design is balanced with no single event or range of events generating a significant proportion of the overall risk. However, in many cases, this is not straightforward: for probabilistic safety assessment most techniques would look to best estimate data; for the selection and justification of design basis events, the parameters selected are frequently more onerous than best estimate to account for the, often significant, levels of uncertainty.

The risk from a single reactor site can vary depending upon the power state or shutdown mode of the reactor. For multiple reactor sites, the risk from the site will increase as units are added. Probabilistically defined design bases can be used in these contexts to allow the design basis to vary whilst keeping the overall risk within tolerable or acceptable limits.

For existing facilities, the probabilistic approach can also be used to determine the potential benefit to be accrued from the use of exclusion rules.

In some cases, the use of a probabilistic approach can completely remove the external event from the design basis because it becomes 'incredible'.

5.1.4. Conclusions

In most cases, deterministic and probabilistic approaches to design basis events should be complementary.

For a limited number of external events a design basis defined using only deterministic or only probabilistic methods can be appropriate. This is generally because of either very low frequencies of occurrence or because the external event is narrowly bounded and deterministic criteria are easier to define and justify.

For most other external events, either approach (deterministic or probabilistic) can be used to define the design basis event. In either case, the resulting design should be confirmed to achieve risk criteria using a probabilistic safety analysis.

No single external event or group of events should dominate the risk calculated for a NPP.

5.2. LOAD COMBINATIONS FOR SEISMIC MARGIN METHODOLOGIES

Seismic margin methodologies are more and more applied in the re-evaluation of existing plants, as a consequence of a modified hazard evaluation at a site. Their application relies on a set of special assumptions in terms of loading, load combinations, identification of the safety group, material capacity, etc., different from those used for the design of new plants.

This section presents a proposal for load combination arrangement elaborated from [41], for further discussion and evaluation by the engineering community.

Loads combination for safety margin assessment methods (SMA) is fundamentally based on the combination of normal operating loads and seismic margin earthquake (SME) loads.

- Seismic margin earthquake (SME) is the selected seismic loading at which the capacity of the NPP has to be evaluated. It is defined in terms of a ground motion spectrum.
- Normal operating loadings are those applicable to the SMA purpose, having a reasonably probability of occurrence with an external seismic event and resulting in the failure of the structure, systems and components (SSC). In the load combination those loading that are self-limiting prior to a failure are not included (e.g. most temperature loads). Only the normal operating loads expected to occur concurrently with SME should be combined.

Since SMA addresses the ultimate code stress (taking into account the material strength and the inelastic energy absorption capacity), no additional conservatism has to be added to the load combinations. Furthermore, for the containment evaluation, the SME should be added to the normal operating loads, as per accident pressure account. This accident pressure should be based on a postulated small LOCA following to a SME.

The occurrence of the safety relief valves (SRV) discharge loading is considered as being probable during a SME event. Structural response motions from an SRV discharge loading only need to be included in the SMA for equipment load combinations for acceleration sensitive failure modes.

The SRV resulted form automatic depressurization releases are not to be considered in the SMA load combinations. If test data exist, the plus one standard deviation SRV loading should be used. If test data are not available, the design basis SRV loading should be used.

Only the significant SRV induced displacements are to be considered in the load combinations with other loading events. When SRV responses are to be included they should be combined with SME responses by the SRSS (square root of the sum of the squares) method. The resulting response is then added by ABSOL (absolute sum) method to the normal loading event responses.

5.2.1. Load combinations for structures

5.2.1.1. Load combination for concrete and steel structures

The load combination for concrete and steel structures is given by Eq. (1)

$$D + L + T_o + K_\mu E_{SME} < \text{Code Ultimate Strength} \qquad \text{Eq. (1)}$$

where:

D = Dead load (including equipment)
L = Operating live load during normal operation plus any live load occurring as a direct result of earthquake or fluid transient loading. Operating live load is not the same as the design live load.
T_o = Operating temperature

E_{SME} = Seismic margin earthquake load

K_μ = Ductility reduction factor (K_μ is same as $1/F_\mu$).

$F\mu$ = Inelastic energy absorption factor determined from non-linear analyses.

Since thermal loads are self-limiting, they are not included in load combinations for the seismic margin evaluation of structures.

The influence of the settlement loads (that are also self-limiting) should be assessed, but usually they may be omitted from Eq. (1).

5.2.1.2. Load combination for concrete reactor containment

The possible effects of pressure should be taken into account. Temperature effects due to a small LOCA are not coincident with the SME event and are not included in the load combination.

$$D + F + L + P_a + K_\mu E_{SME} < \text{Code Ultimate Strength} \qquad \text{Eq. (2)}$$

where:

F = Prestress load

P_a = Maximum pressure during the time of the SME associated with a small LOCA

Live or settlement loads should not be considered if they are found to reduce the effects of dead and seismic loads. The effects of inelastic energy dissipation should be accounted for, as a result of SME, by means of a ductility reduction factor, K_μ ($K_\mu < 1$, for post-yield behaviour).

5.2.2. Load combinations for components and subsystems

5.2.2.1. Load combination for pressure boundaries of components and piping

Only primary stresses for Level D Service (Faulted) conditions should be considered, as per BPVC ASME code requirements [44].

Thermal anchor movements (TAM) and seismic anchor movements (SAM) should not be combined with SME, except when SAM values are considered significant.

$$D + L + P_N + OML + K_\mu (E^2_{SME} + SAM^2)^{1/2} < \text{Code Stress Limit} \qquad \text{Eq. (3)}$$

where:

D = Dead load (including equipment)

L = Operating live load during normal operation plus any live load occurring as a direct result of earthquake or fluid transient loading. Operating live load is not the same as the design live load.

P_N = Normal operating pressure,

OML = Non-seismic operating mechanical load from connecting piping including weight, restraint of free end thermal displacements and thrust loads,

E_{SME} = includes seismic inertial loading of the component and connecting piping,

SAM = includes SAM of component supports and the SAM effects of connecting piping.

TAM and SAM effects may be excluded from the load combination if are self-relieving.

5.2.2.2. Load combination for component supports for piping and pressure components

The effects of restraint of thermal expansion of attached piping and differential support displacements of piping and component supports should be taken into account, except the case when they tend to be self-relieving, due to the yield occurrence in the component.

For ductile failure modes, the loading combination equation is given by:

$$D + L + OML + K_{\mu} [E^2_{SME} + SAM^2]^{1/2} < \text{Code Ultimate Strength} \qquad \text{Eq. (4)}$$

For brittle failure modes, the loading combination equation is given by:

$$D + L + OML + [E^2_{SME} + SAM^2]^{1/2} < \text{Code Ultimate Strength} \qquad \text{Eq. (5)}$$

OML loading due to restraint of free thermal expansion should not be included in the Eq. (4) because the failure mode is ductile and the thermal stresses will tend to be relieved. In contrast, free thermal expansion should be included in Eq. (5), since the failure mode is assumed to be brittle.

5.2.2.3. Component supports for non-pressure components and supports

Electrical and control cabinets, electrical components supports, cable tray and conduit supports, HVAC ducting supports and supports of motors and engine generators, etc., should be evaluated according to Eq. (6), when they are not acceleration sensitive:

$$D + L + K_{\mu} [E^2_{SME} + SAM^2]^{1/2} < \text{Code Ultimate Strength} \qquad \text{Eq. (6)}$$

SAM may not be taken into account in the Eq. (6) for those components supported at the same elevation. For components that are acceleration sensitive (i.e. relays):

$$D + L + [SR\, V_a^2 + E^2_{SME}]^{1/2} < \text{Code Ultimate Strength} \qquad \text{Eq. (7)}$$

where SRV is the acceleration loading from SRV discharge.

5.2.2.4. Loads combination for electrical and HVAC distribution systems

These systems are considered to be ductile, therefore the loading combination equation should be:

$$D + L + K_{\mu}\, E_{SME} < \text{Code Ultimate Strength} \qquad \text{Eq. (8)}$$

5.3. BEYOND DESIGN BASIS EVENTS

Beyond design basis events should be considered for existing and new nuclear power plants. In all cases, the definition of design events (operating, environmental, and accidental) is probabilistically based. That is, the design parameters are defined based on the likeliness of occurrence. Normal operating conditions have a likelihood of one, they will occur. Abnormal conditions are assumed to occur on a less frequent basis and the design parameters (loading and capacity) are selected to correspond to the probability of occurrence of the event, sometimes interpreted as a return period, and the consequences of the event. For example, the design wind loading on the buildings on site may have a probability of occurrence of 0.025 events per year (or a return period of 40 years). Hence, the design wind speed and ancillary conditions, if any, will typically be defined from statistical data recorded over a long period of time and interpreted over the desired return period.

Given the nature of the definition of accident events and the corresponding design parameters, there is a small likelihood that the accident event itself or the parameters defining this design event will be exceeded in any given year or over the life of the plant. However, it is this small likelihood of exceedance that leads to the interest in evaluating beyond design basis events. In addition, it is necessary to demonstrate that the occurrence of an event slightly greater than the design basis will not produce a catastrophic consequence, i.e. that there does not exist a 'cliff edge effect.' The nuclear power plant has reserve capacity ('robustness') in its structures, systems, and components to prevent a catastrophic consequence if the design basis event is exceeded. A question to be addressed in regulation and technical spaces is: what is an acceptable exceedance of the design basis event for which it can be demonstrated that there is high confidence that the plant will be safely shut down, if necessary?

There is an additional benefit to considering beyond design basis events. Approaches to evaluating the effects of beyond design basis events focus on what might go wrong which differs from the design process of assuring what will go right. This difference in approach can lead to insights not readily obvious from the design process.

These observations apply equally to existing designs for operating plants and new designs for plants not yet built and operated. For operating plants, there are a number of situations that provide additional motivation for the need to consider beyond design basis events:

- The perception of the hazard defining the event has changed from its establishment during the licensing and design process. Examples relating to seismic design criteria include: a previously unidentified fault or fault system has been discovered within the range of effect of the plant site; a previously identified fault system or area of seismic activity has been re-evaluated, based on new information, and judged to be capable of larger events than originally thought during the design process; an earthquake has occurred which produced parameters greater than the design values, e.g. the LeRoy earthquake's occurrence and effect on the Perry nuclear power plant; ground motion recordings have validated the existence of high frequency motions in earthquakes, etc.
- Methods and approaches to design have evolved since the original design process was performed. Examples relating to seismic design criteria include: seismic qualification of equipment and components has changed due to the evolution of

shake table technology; analysis techniques for soil–structure interaction, dynamic behaviour of structures, systems, and components; etc.

- The capacity of structures, systems, and components has been shown to be less than originally assumed in the design process. This could be due to unexpected material deterioration due to environmental conditions.

For new and operating plants, the consideration of beyond design basis events is a component of the severe accident management policy, i.e. to ensure that the plant operators are knowledgeable of potential severe accidents and the behaviour of their plants under these conditions.

There are several methods or approaches to be used to investigate beyond design basis events. In the area of external events, screening techniques, deterministic methods, and probabilistic approaches are available:

- Screening techniques, typically, involve screening out the event at the event occurrence phase.
- Deterministic methods often involve a systematic deterministic approach which leads to high confidence that the structures, systems, and components necessary to achieve safe shutdown of the facility are available and have very low likelihood of failure if a beyond design basis event occurs. An example is the seismic margin assessment (SMA) methodology for beyond design basis earthquakes. The EPRI approach to an SMA is to address the question: At what excitation level, does one have high confidence of a low probability of failure of the system? The steps in this approach involve: 1) Specifying a review level earthquake for which the assessment is performed. 2) Identifying redundant success paths to attain safe shutdown. 3) Identifying equipment and components which comprise these system success paths. 4) Determining seismic demand and seismic capacity of the individual components and the resulting safe shutdown success paths. 5) Documenting and reporting the results. Another example is the EPRI methodology for evaluating internally generated fire risks [41].
- Probabilistic approaches focus on probabilistic safety assessment (PSA) techniques. The PSA approach is complete in that it provides a complete perspective of plant risk. For beyond design basis seismic events, a seismic PSA is comprised of the following steps: define the seismic hazard probabilistically; calculate the plant seismic response when subjected to earthquakes defined by the range of earthquakes of the seismic hazard analysis; model the plant structures, systems, and components through the use of event and fault trees; evaluate the seismic capacity of structures and components identified in the previous step; and quantify plant seismic capacity and other quantities of interest for decision making. All beyond design basis events may be evaluated by PSA techniques.

There is important value to be gained for existing and new plants to consider beyond design basis events. It is this value that has led the international nuclear industry to adopt a philosophy of considering such conditions.

5.4. EFFECTIVENESS OF ADMINISTRATIVE MEASURES

Both the previous and the revised versions of the IAEA Safety Guide dealing with external human induced events in relation to site evaluation [6], indicate the need for

administrative measures aiming to controlling the development of activities likely to cause external induced events and to their continuing development in the region, taking into account the required degree of protection of the nuclear power plant.

The key in this point is that, in order to be effective, the administrative control is to be exercised permanently from the time a site is selected and — from then — throughout the lifetime of the plant with periodic reassessment of the situation.

The issue is more critical in case that the source of an induced external event is found to be within the screening distance value (SDV) or that it has a higher probability of occurrence than the screening probability level (SPL) or in cases when it is not practicable to have the event as a design basis for the nuclear power plant. Therefore, due consideration should be given to control the distance and/or the size of the source in such a way that it will always be outside the SDV or have a probability of occurrence lower than the SPL. In this case is just not only the need for controlling the development of the activity, which may be the source of the event, but the need of controlling the occurrence of the event itself.

A typical example is the administrative restriction to aircraft flights when the competent authority decides administrative measures for moving the established air corridor outside the screening distance values. The experience of the site evaluations performed by IAEA teams in a number of nuclear power plant sites in the last decade showed flagrant flaws when pilots of commercial planes, using valid charts, passed over nuclear plant sites which are used as turning points. This was directly verified by IAEA staff on spot basis in European flights of western airlines as well as in Latin America ones.

The required administrative control is to be performed by a competent authority that is changing from time to time. Keeping its effectiveness in the long term is difficult to assure if these restrictions, requirements or reassessments are not enforced in operating procedures under the responsibility of the plant management itself. But even then, how can they control the air traffic in order to enforce a rule that no flight should be undertaken over the plant site?

The conclusion is that the application of administrative measures for controlling the development of activities for controlling the occurrence of a certain external event should be accompanied by an evaluation of its effectiveness. The means of implementing such controls and the extent to which they are exercised are still under discussion in the Member States, and the experience shows the need of verifying their effectiveness periodically. If this cannot be assured the corresponding event should be reassessed.

It has to be reminded that administrative measures are not related to the monitoring systems that are designed and operated at the site, under the plant management responsibility, to confirm the siting and design assumptions and to prevent the evolution of the initiating events into nuclear accidents.

Usually, monitoring systems are operated in relation to natural phenomena, like floods, earthquakes, volcanic activity, winds, etc. Specialized governmental agencies are usually involved in this task with different views and priorities than the management plant ones, especially in the emergency created by unlikely events. Therefore, administrative measures should be clearly distinguished from monitoring systems because the subject and the liability involved are usually different.

In conclusion, it may be considered that the accomplishment or fulfilment of administrative measures should be monitored throughout the lifetime of the plant.

5.5. SABOTAGE AND WAR RELATED SCENARIOS: ENVELOPED BY EXTERNAL EVENTS?

5.5.1. Definition

The definition of sabotage and war related scenarios and their classification as external events acting against nuclear facilities is treated in the IAEA INF CIRC/225 Rev. 2 (Dec. 1989). Sabotage is *"any deliberate act directed against a plant, facility, nuclear material transport vehicle or nuclear material which could directly or indirectly endanger the public health and safety by exposure to radiation"*. The definition of war related scenarios — although it may come from a more general and global confrontation between parties — may also be included in the one given above.

What is essential and common to both definitions is that sabotage or a war related scenario is an act generated by human beings and not by the nature. Such act can generate an event at a given site/plant, which in term could jeopardize the plant safety, and which is not of accidental origin but — on the contrary — is the result of a wilful, intentional action produced by third parties, either individuals or groups.

Therefore, and regarding the different origins of external events against which the nuclear power plants are designed, and complementary to the well known and more classical classification about natural and human induced events, two different types of events should be differentiated:

- External events from accidental origin, and
- External events from intentional, wilful, deliberate origin

Both types of events should be carefully separated for analysis during siting, design, construction and operation of nuclear power plant facilities. They also deserve a different terminology and specific requirements. Thus, those from the accidental origin field are extensively treated and considered in the current practice and subjected to the well known public normative environment. On the contrary, those from the wilful/intentional origin field are usually confined within the so-called physical protection or security field.

As a summary, the external events may be classified as:

- Accidental origin:
  - natural origin
  - human induced origin
- Intentional, wilful, deliberate origin: (physical protection or security field)
  - Sabotage: a 'punctual' scenario of aggression
  - War related acts: a 'global' scenario of aggression

According to the short and limited operating experience in worldwide NPPs and to the best engineering evaluation in many Member States, some intentional acts are either explicitly or implicitly considered in NPP design, such as:

- explosions from a source external to the site, and induced missiles

- projectiles or portable missiles shot by a location outside the fence, as it happened in Creys Malville in France
- vehicles launched malevolently against the site entrance, as considered in recent US standards
- explosion at the site of some sources launched inside
- projectiles launched by a small aircraft: this was the case at Bushehr site in the Islamic Republic of Iran during a wartime attack by helicopters.

5.5.2. Safety requirements

The IAEA Safety Standards Series establishes the requirements for designing the structures, systems and components important to safety that should be met for preventing the occurrence of accidents (i.e. the safe operation of the facility) and for mitigating the consequences of events that could jeopardize safety.

At national level many States have also established their own requirements and norms according to the degree of development reached by the industry.

Regarding the IAEA safety standards, it is required that a …*"comprehensive safety assessment is to be carried out in order to identify the potential hazards that may arise from the operation of the plant under the various plant states (i.e. operational states and accident conditions). The safety assessment process includes the complementary techniques of deterministic and probabilistic safety analysis, for which Postulated Initiating Events (PIE) need to be considered*" [4].

These PIEs may include many factors that, alone or in combination, may affect safety and which may:

- originate in the operation of the plant itself;
- be caused by human action;
- be directly related to the plant and its environment.

This means that the safety assessment should identify all types of PIEs. Therefore, in the case of those caused by human actions, the identification should include those from either accidental or intentional origins.

The assessment of the potential magnitude of the aggression is usually difficult, when this magnitude does not respond to certain kind of 'law' and it is possible to overpass the known or estimated level, just as a question of power, or intention, or technological/economic availability. In other words, to prescribe today a certain magnitude of the 'aggression load' it may be totally superseded tomorrow, once a potential aggressor knows the adopted value. It is also true that criteria for security or physical protection of a facility are more related to a methodology based on dissuasion, prevention and mitigation than on design, in a matter more close to social and political sciences than to the engineering one.

Concerning national practice in this subject, some Member States have developed criteria and procedures for specific threats. In this regard, an example is the design basis for a 'malevolent vehicle' adopted by [45] in which guidance is provided for a vehicle barrier system selection for preventing intrusion to a protected area. The information regarding the

maximum parameters of the vehicle threat is Safeguards related information and it should be handled accordingly, taking into account what is mentioned in the previous paragraph.

5.5.3. Description of the problem

As described above, sabotage and war related scenarios are not explicitly considered for design bases in most NPPs. However, in some cases the definition of some design basis external events was done with an implicit consideration of some kinds of sabotage or intentional actions.

This was often done through hiding or covering up this wilful origin within the envelope provided by a certain natural or accidental human induced external event. If the specific hazard of this accidental external event be analysed, (which was selected as design basis) it could have had other magnitude level, or even its potential occurrence may have been neglected. However, it was selected for design basis because the necessity to cover, through it, some other intentional event.

A good example of the above mentioned problem is the definition of the loads generated by tornado, which were a loading 'used' for such purposes. According to the practice of some Member States, the tornado design basis was selected with the criteria of being those loads that corresponded to a relatively low level of occurrence probability (mean annual probability of 10^{-7}). This level is several orders of magnitude lower than other natural phenomena (e.g. as earthquake with a typical mean annual probability of 10^{-4} for the most severe condition).

The guideline for selecting the design level as indicated above, (with such low level of occurrence frequency), is explicitly indicated for the evaluation of design basis tornado in the IAEA Safety Guide [9]. This concrete reference and guide was used by a number of Member States for defining the tornado design basis in a number of plant sites.

The rationale, behind the recommendation for using such low occurrence frequency level, would have been to select the one (i.e. 10^{-7}) for which a high value of static overpressure would be obtained from the tornado load hazard assessment and which, therefore, may be equivalent (i.e. producing a similar or equivalent effect) than the one generated by some assumed level of sabotage or war action (for example, an explosion or a missile action).

In other words, in a first step and as result of the assessment of a sabotage action (assessment or a deterministic security decision), a static overpressure value was obtained for protecting the facility. From this value of the 'magnitude', in a second step, and given the hazard curve of certain external accidental natural phenomena (as tornado for example), the occurrence probability level which corresponds to such pressure value would be obtained. This value resulted in a very low probability level and thus was recommended or required in the standard or guideline.

Another example has been the use of criteria about aircraft crash or explosions, in some specific applications, to envelope effects from projectiles and terrorism. Was that wrong or right? What is important here is that if the designer knows the rationale behind the criteria as explained he can accept it or not. But if it is not known, different concepts can be mixed,

non-appropriate criteria may be used and an unbalanced situation in the plant safety can be created.

When deterministic approaches are followed for selecting design basis for external events, what is mentioned above may be accepted. However, if a probabilistic approach is used for selecting the design basis external events in line with a given safety goal, it does not seem reasonable to define hazard curves for all events and, afterwards, to select their magnitude levels 'mixing' different probability levels without a proper justification, based on a predefined criteria (as example, 10^{-4} for earthquakes and 10^{-7} for tornadoes).

In fact the risk posed by different PIEs, expressed in terms of core damage frequency, or offsite population dose, should be balanced among different types of PIEs. That does not mean that the annual probability levels of the design basis for different hazards need to be equalized in the design. What should be balanced is the risk as expression of a concretely defined safety goal, i.e. the product of the hazard times the conditional probability of core damage (or offsite population dose) given the hazard. This is the way recommended by the current recognized practice nowadays and, because of that, it should be avoided the selection of probability levels for different hazards according to a 'hidden objective' which does not respond to the rigour of a logical methodology.

5.5.4. Conclusions

In a framework of selecting the design basis for external events in line with global and comprehensive safety goals, expressed in probabilistic terms, it is recommended to use specific and appropriate criteria for each type (from accidental or intentional origin) of events. The treatment (identification, selection, assessment) for accidental origin events should be separated from the treatment corresponding for those of intentional origin.

Criteria for establishing design measures to prevent or mitigate intentional actions may be necessary and those criteria should be established independently from those corresponding to accidental events.

In line with that, the following should be included in the discussion, to be held between the nuclear safety community and the safeguards community:

- Characterization of the threat
  - From a localized or global conflict.
  - Sabotage or act of war. There has been a concrete example of the latter in the case of the air attack against a nuclear facility under construction (Bushehr NPP Iran).
- Hazard evaluation
  - Deterministic/probabilistic
  - Explosion, projectiles, poisoning, malfunctioning.
- Design criteria
  - Enveloping with other external events for which design bases are defined.
  - Load combination
  - Structural behaviour criteria
  - Physical protection measures. Barriers.
- Damage limitation

However there is a number of issues where most Member States share the same feeling:

- It is a general feeling that war cannot be excluded in any State, but in that case the whole State would be affected, and therefore there is no reason to discuss a warlike attack on a nuclear power plant. Against weapons there is no defence: in case of a war risk the plant should be shut down.
- Concerning the wilful actions, the impression is that there is no final protection as there is no clear hazard in general. However, when a global analysis is needed, it should consider the essential role played by physical protection which could be assumed 'adaptive' to the risk: if the risk increases, the plant administration will ask for more guards and measures. In this framework, also the hazard evaluation can be more realistic: the maximum amount of explosive that can be moved close to the site or the maximum amount that can be brought by a commando up to the site fence should be limited by physical protection measures.
- The risk evaluation should be coherent with other risks in the State: for example an oil tank of a refinery is pretty much exposed to an external attack.
- The plant design may include some generic protection measures against wilful actions. Some of these measures may be enveloped by the protection against accidental events. Therefore in general, the envelope is acceptable on the protection, but not in the hazard evaluation, where a detailed analysis is recommended to avoid useless conservatism and to allow a proper safety assessment of the plant.

5.6. SITE WITH LOW HAZARD FROM EXTERNAL EVENTS

Many nuclear sites in the world show a very low seismicity or, in general, very low hazard from all external events. In several geographical areas in the world, which include northern Europe, eastern South America and the Southeastern United States, nuclear power plants are located in low seismicity sites (pga < 0.12g). However, a minimum deterministic value for some external events is recommended by many regulatory bodies and also by the IAEA (see for example the recommendation for a minimum earthquake at 0.1 g Pga in [5]).

This deterministic assumption requires a minimum site specific hazard evaluation to attach realistic physical properties to the deterministic requirement and the implementation of simplified design/re-evaluation methodologies to avoid disproportionate analysis efforts and protection measures. The issue is particularly important for existing plants where the need for low additional investments is high and can be compensated by some conservatism.

In general many plants implemented first an 'easy fixes' programme supported by a deterministic study based on the minimum earthquake (0.1 g). Later, most of them developed a probabilistic safety analysis (PSA) to support a risk informed decision process.

In case of low values for the extreme events at the site, some minimum actions are recommended to prove a generic ruggedness of key items against external events, namely:

- a structural capacity evaluation for main buildings
- a structural response calculation for main buildings
- a structural assessment of fundamental equipment which requires high reliability, including the core assembly, control rods, primary circuit, etc.

- a detailed identification of the systems needed for plant protection against external events
- a definition of the plant strategy for defence against external events (n. of lines of defence, etc.)
- a walkdown on seismic and flood (from rain and sea, rivers or lakes) easy fixes
- a seismic specific relay evaluation
- an evaluation of monitoring systems and of their interaction with operator actions
- an evaluation of emergency planning in case of extreme events

For seismic appraisal using a seismic margin (SMA) or PSA approach, most of these minimum actions are required as precursors to either. The first task is to complete all of these precursor activities to a consistent standard in order to: 1) gain confidence that an interim justification is secure, 2) provide an indication of where improvements can be introduced and 3) guide selection of SMA or PSA.

In the case of the seismic hazard, the evaluation of the hazard from a deterministic pga is a process full of uncertainties: the duration of the input motion, its spectrum shape and the associated probability of occurrence may require a large use of engineering judgement. It is recommended that this process is based on site specific investigations to avoid inconsistencies and non realistic assumptions.

Unless a site specific probabilistic hazard study is conducted and the earthquake propagated to the surface, a seismic PSA can only be done using some generic hazard estimated for the site. Likewise, a seismic margin assessment could only be performed using a default pga such as the IAEA recommended minimum of 0.1g and a standard spectral shape. This later choice may lead to excessive upgrades but with the lack of a detailed site specific hazard study, this is speculation based on recommendations of others regarding the low hazard of the site.

The experience of seismic re-evaluation in some low seismicity States is shortly summarized in the following.

In Finland, the Loviisa and Okiluoto plants elected to conduct seismic PSA to demonstrate their seismic safety. Detailed hazard studies were conducted and the resulting hazard was very low. The 1×10^{-4} pga was less that 0.1g. As a result, very few upgrades were required to demonstrate very low probability of core damage due to earthquakes.

In Sweden, two plants, Oskarsham 2 and Forsmark, have completed a Seismic Margin assessment for a Swedish Envelope Uniform Hazard spectrum. The actual pga used for the margin assessments was modified for site specific conditions and was slightly less than 0.1g. In the case of the Swedish plants, the seismic margin approach was used to effectively establish a seismic design basis. As a consequence, the documentation and seismic upgrades were more extensive than in the case of the seismic probabilistic risk analyses conducted in Finland. In both cases, the risk afforded by the low seismicity was very low.

As a conclusion, an application of SMA for low seismicity areas represents the most common approach in Member States.

In most cases for existing plants the review level earthquake (RLE) was selected equal to the SL-2 (according to IAEA Safety Guide [5]). In this way the margin evaluation provides an assessment of the capacity of the plant against external events, but it does not represent a real margin evaluation beyond the design basis.

In general, concerning the re-evaluation methodologies, when mean probabilities of exceedance at the 10^{-4}/a level are less than 0.1g peak ground acceleration, considerations should be given to developing reduced scope Seismic Margin Assessment procedures. The existing procedures which were developed on a site specific basis for moderate — 0.12–0.33g peak ground acceleration sites may not be appropriate or cost benefit effective for such low seismicity sites and new approaches should be developed for a realistic, but safe, analysis of the protection against external events.

5.7. BASIC STATISTICS FOR PROBABILISTIC TREATMENT OF EXTREME EVENTS

5.7.1. Introduction

This contribution aims at providing some basic references for a statistical analysis of data preliminary to hazard evaluation. It is based on academic research and engineering practice, particularly from the most updated approaches for design of conventional buildings.

In fact, the experience accumulated in the development of the Eurocodes for design of conventional buildings in European States could be of interest both for consistency between NPP and the most advanced conventional building design and for the solid technical background accepted by all European Member States.

A useful set of definitions may be taken from Eurocode EN 1990 'Basis of Structural Design' (2001) [46, 47], where an extreme event can be classified as an *accidental action*, i.e. an "action, usually of short duration, that is unlikely to occur with a significant magnitude on a given structure during the design working life". It has to also be noted that "An accidental action can be expected in many cases to cause severe consequences unless appropriate measures are taken". The treatment of accidental actions and accidental design situations is the specific object of Eurocode ENV 1991-2-7, now under revision as EN 1991-1-7.[3]

According to the Eurocode, an action is usually introduced by means of its *characteristic value,* that [46] defines *principal representative value of an action*, and goes on stating that "In so far as a characteristic value can be fixed on statistical bases, it is chosen so as to correspond to a prescribed probability of not being exceeded on the unfavourable side during a 'reference period' taking into account the design working life of the structure and the duration of the design situation".

With reference to extreme events and related *accidental actions* a distinction is made in [46] between cases in which statistics are possible and allow to establish the characteristic value according to the definition above, and cases in which this is not possible because the event is truly exceptional. In this second case, a 'characteristic value' L_k is used that is merely a 'scenario value' to which no 'probability of occurrence' can be attached.

[3] For the readers' convenience, references are made to the latest version of Eurocodes EN 1990 and 1991-1-7, that are in substantial agreement with the corresponding ISO and other current International Standards.

While the following treatment assumes that the actions can be statistically modelled (i.e. is related to the first case), in practice, even in this case, the characteristic value L_k is often specified without due consideration of the rate at which the load changes its intensity nor of the design life of the system, and is merely based on the expected (*average*) value of the action under consideration, increased by its *standard deviation* multiplied by a factor of the order 2–4: in principle, this should lead to a *fractile*, i.e. a load level that presumably has a specified probability (say, 90 to 99%) of not being exceeded.

In most codes, the *design value* L_d of the action is obtained by multiplying L_k by a *safety factor* γ, which takes account of the possibility of unfavourable deviations of the action values from the representative values and also of model uncertainties and dimensional variations (since analogous factors are applied to the other relevant variables, like material resistances, geometrical dimensions, etc., γ's are usually indicated as *partial factors*)

Likewise, the *design load combination* S_d is usually obtained by means of expressions of the form:

$$S_d = \quad _{i=1} \gamma_i \psi_i c_i L_{k,i} \tag{9}$$

in which $L_{k,i}$ represents the characteristic value of the i-th load, γ_i the partial (safety) factor, $\psi_i < 1$ a load combination factor and c_i the influence coefficient for the i-th load. The load combination factors were first introduced in the ACI 359/1975 and ACI 359/86 codes, finding later wide acceptance in structural codes around the world, including Eurocodes.

Usually, none of the factors appearing in the summation in eq. (9) is considered dependent on the frequency of load application nor on the design life of the structure.

In this context, it may be recalled that in 1965 R.E. Ginna NPP containment was the first such structure in the world to be designed using factored loads [48]: this represented an important and pioneering development in the field. In fact, the American Concrete Institute (ACI) had already published a number of papers proposing the use of load factors in the design of concrete structures in the 1950s and codified the method in ACI Building Code, ACI 318-63. However, as pointed out by [49], although some attempts were made to formally incorporate probability theory in this development, *the basis of load factors in ACI 318 seems to remain heuristic.*

On the other hand, ASCE 7 load factors are based on extensive later research, such as [50, 51], but the final format still seems inadequate. In his review of the partial load factors method, it was shown that ACI and ASCE dead and live load combination equations result in reliability different by at least one order of magnitude. Similar contradictions have been found with regard to the Eurocodes.

Now, a couple of decades after the first introduction of the 'load factor' approach, it should be clear that an alternative, more rigorous, format is necessary, in which all actions should be defined as random processes with given space and time distributions. Note that in this discussion only the evolution of actions with time is being addressed. Hence, the first problem consists of the determination of the probability density of the peak value of a random process within a specified time period. This serves then as the basis for the solution of the load combination problem, which requires, as a starting point, the evaluation of the probability density of the combined effect.

Both topics have been extensively dealt with in the last thirty years, at least for stationary, simple models of the individual loads [52, 53, 54, 55]. These include the following basic types of stationary random processes:

(a) Poisson square wave process
(b) Poisson pulse process (also designated *pike process*)
(c) Filtered Poisson process (also *renewal rectangular pulse process*)

which are shown in Fig. 13. The first two processes are completely defined by the rate of occurrence of changes in the intensity level or occurrence of pulses, λ, and by the probability density of the load amplitude, known as *point in time value.* The third model requires also the specification of the distribution of t_d, the duration of the rectangular pulses. Note that when the probability density of t_d is a Dirac impulse at the origin, the process type (c) reduces to type (b).

More elaborate models have been proposed, which nevertheless retain most properties of the three basic cases. For instance [56, 57] and others consider renewal pulses with triangular and other shapes. An earlier, simpler model consisting of arbitrarily distributed equal duration pulses, which admits intervals with no load, is known as the Borges–Castanheta model [52]. Another potentially useful model for the distribution of events is the Polya process, which reflects the tendency of certain physical phenomena, for example, tornadoes or seismic events, to cluster [57].

The characterization of the peak value of a random process is briefly discussed below, by way of introduction to the so-called method of the first two moments, described later. In fact, the linear combination of various random processes may be handled using four different approaches, namely:

(1) the method of load coincidence [53, 54]
(2) the method of upcrossing rate and bounding technique [56, 58]
(3) the method of renewal equation [59]
(4) the method of first two moments [55, 60]

In most applications, the four approaches yield substantially equivalent results. However, the last method seems to be easier to grasp and appears therefore better suited for use in structural codes, for which reason it will be discussed in more detail in para 5.2.4.

Application of the methods described in para 5.7.3 and 5.7.4 requires the description of loads as random processes of types (a) to (c). In fact, regardless of the approach followed to evaluate the basic statistics of the peak combined value of the load effect, that is, *of the design load effect*, such information is essential *for rational structural design*, as well as in structural reliability studies. Within this context, some available data are summarized in the following, where models to quantify wind loads produced by various meteorological phenomena are also discussed, illustrating the kind of information presently missing in most codes.

Finally, in para 5.7.6, a proposal is advanced, based on the method of the first two moments, to combine any number of loads in an easily applicable code procedure.

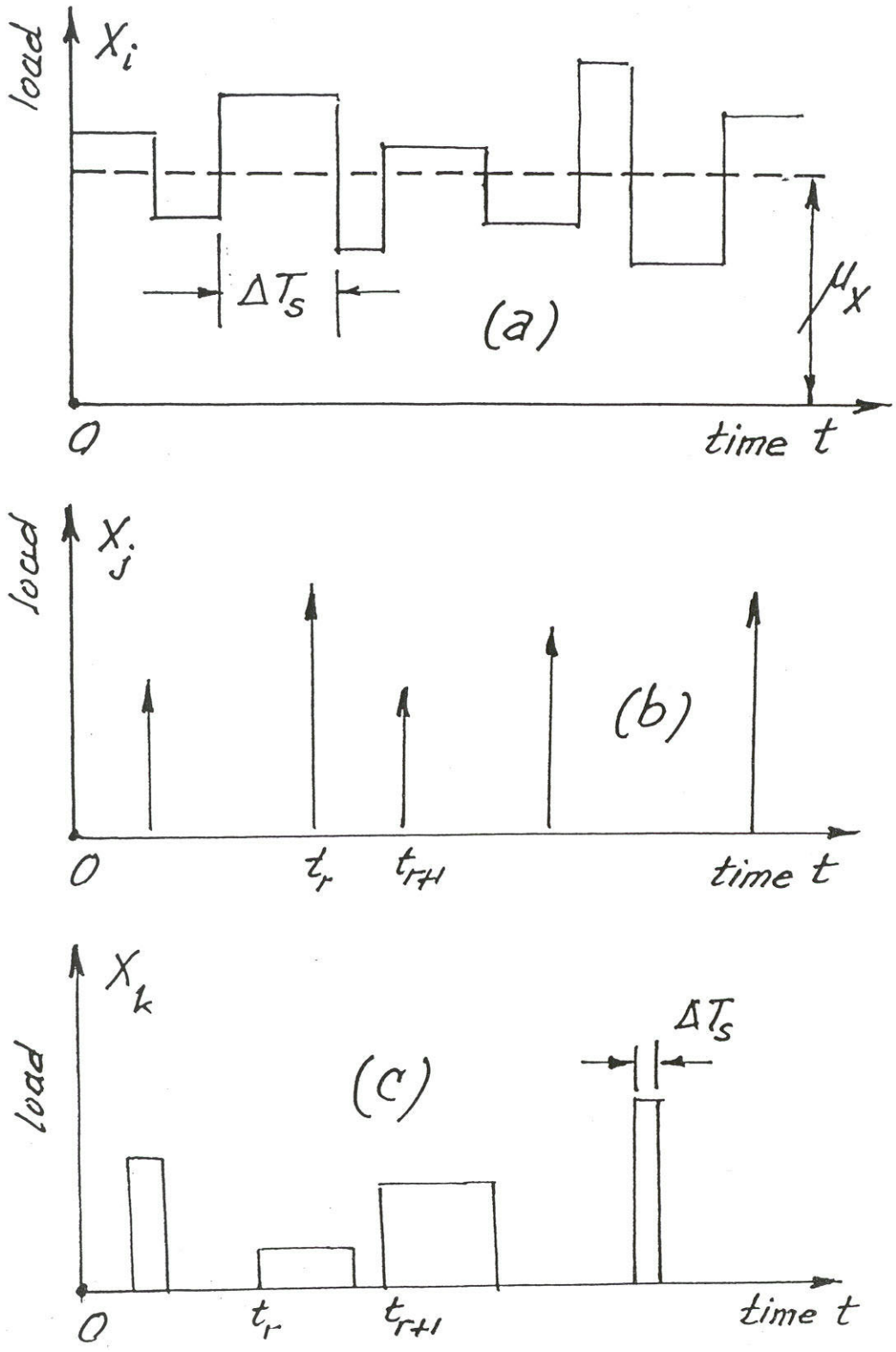

FIG. 13. Basic Models of random processes, types (a), (b), (c).

5.7.2. Peak value of a stationary random process

Given n independent observations of a variate X, characterized by its first two moments μ_x and σ_x^2, the expected value and the standard deviation of its maximum value can be put in the form:

$$\mu_{max} = \mu_x + \xi(n)\, \sigma_x \tag{10}$$

$$\sigma_{max} = \zeta(n)\, \sigma_x \tag{11}$$

For two parameter distributions that do not change shape when shifted, like the normal, shifted exponential and Fisher–Tippett Type I distributions, the coefficients ξ and ζ in eqs (10)–(11) depend only on the sample size n. In a general situation, these coefficients may be expressed in terms of n and the coefficient of variation of the original variate X.

For a normal variate, the following expressions were fitted to numerically determined values of the expected value and the standard deviation of the extremes of n realizations [60]:

$$\xi(n) = [\, \ln (n - 0.918 \ln n)]^{\,0.604\,(1\,-\,0.866/n2)} \tag{12}$$

$$\zeta(n) = (1 + 0.0267 \ln n) / (1 + 0.3486 \ln n) \tag{13}$$

For n smaller than 10000, eqs (12)–(13) are accurate up to the third digit, which far exceeds practical needs. It may be easily verified that for a Type I parent distribution, the following coefficients hold:

$$\xi(n) = 0.780 \ln n \tag{14}$$

$$\zeta(n) = 1 \tag{15}$$

Figs 14 and 15 show plots of the ξ and ζ functions for a Gaussian parent distribution, as well as for the Fisher–Tippett I distribution; the expected values and standard deviations of the first order statistics for a Gaussian parent distribution are also presented.

It may be anticipated at this stage that if the normal and the Type I distributions are regarded as representative of distributions of variates with a light and heavy tail, respectively, *then the curves for the normal and the type I distributions may be viewed as bounds of the range of variation of the ξ and ζ factors* in practical situations involving load processes.

In order to apply the preceding results from extreme value theory to load processes, the number of *effective* realizations n in the lifetime T should be evaluated. In case of a process of type (a), (b) or (c), the number of occurrences n in an interval T follows a Poisson distribution:

$$F(n) = (\lambda T)^{n} \exp (-\lambda T) / n! \tag{16}$$

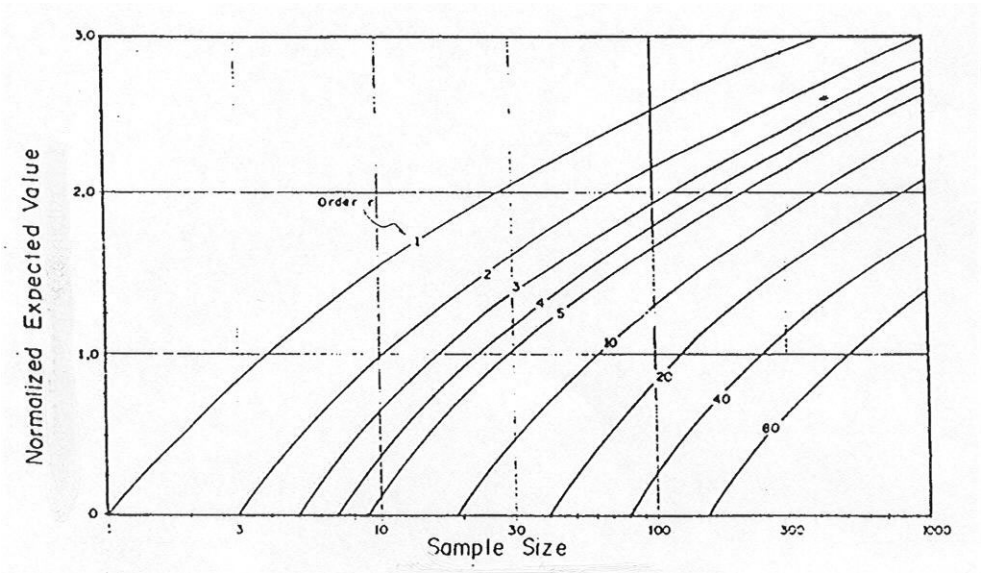

FIG. 14. Mean value of order statistics for i<80 and n<100. (Zero mean and unit variance Gaussian parent distribution).

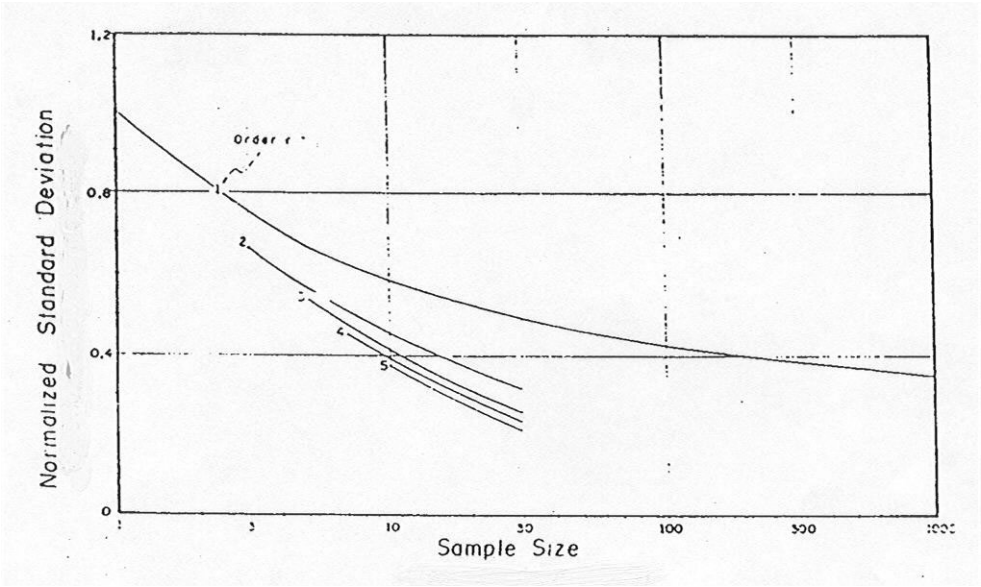

FIG. 15. Normalized standard deviation of order statistics. (Zero mean and unit Gaussian parent distribution)

Neglecting higher order terms, which has negligible influence on the results for n larger than about 5, expressions adequate for design purposes result from setting n in eqs (12)–(15) equal to its expected value λT. For values of n, i.e. λT, approaching unity, more terms should be retained in the expansions, or alternative approaches used to evaluate the appropriate coefficients. These are then continuous and yet unknown functions of λT that coincide with the well known ξ and ζ coefficients for large arguments but depend, for low

values of λT, as indicated above less than about 5, on the type of load process. Hence, for *random processes*, the expected value and the mean of the peak in a time interval T are expressed by:

$$\mu_{peak} = \mu_i + p(\lambda T)\, \sigma_i \tag{17}$$

$$\sigma_{peak} = q(\lambda T)\, \sigma_i \tag{18}$$

The variance of the Poisson distribution is also λT. Since the expected value of the number of events for another relevant model, the Polya process, is likewise λT, for large arguments there is no difference in the evaluation of the mean peak value between these two processes. It should be borne in mind, however, that the variance in case of the Polya process is given by

$$\mathrm{var}(n) = \lambda T + \beta\, (\lambda T)^2 \tag{19}$$

in which β denotes the parameter that quantifies the degree of clustering. When $\beta = 0$, the Polya process reduces to the Poisson process. For λT smaller than about 5, corrections in the ξ and ζ coefficients should be introduced, which will not be discussed herein, resulting in the p and q functions of eqs.(17)–(18). Interested readers may consult [60].

An alternative approach, using concepts from the Theory of Random Processes, has been followed by der Kiuregian [55]. The expected value and variance of the extreme of the process is calculated from the integral between $-\infty$ and $+\infty$ of an integrand involving the point in time probability density under consideration and an exponential function of the square of the variable. For a normal density, this integral does not possess a closed form solution. In fact, due to computational difficulties, the integral should in most cases be obtained numerically. The curves presented by der Kiuregian for the normal density identically coincide with those obtained by Barragán on the basis of eqs. (12)–(13) shown in Figs. 16 and 17. In his original paper [55], which may be considered as establishing the foundation of the present approach, der Kiuregian includes curves for coefficients p and q, both for the Poisson square wave (type a) and the filtered Poisson process (type c).

5.7.3. Analysis of load combinations

By way of introduction to the ensuing discussion of the load combination problem, it is worth mentioning earlier attempts to search for maxima of the combination of action processes in a systematic manner. As described by [61], a procedure proposed by Turkstra [62] has found its way into practice, being known in some European States as *Turkstra's rule.* In this approach, one of the load processes $L_i(t)$ is chosen as the *leading action*. At the point in time when this leading process reaches a maximum, the values of all other *accompanying actions* are read. The leading action, together with its accompanying actions, define a so-called *hazard scenario.*

Each action, in turn, is considered as a leading action. Thus, there are as many hazard scenarios as there are actions that occur simultaneously. Finally, the most unfavourable scenario for the section, element or component under consideration, is the critical one.

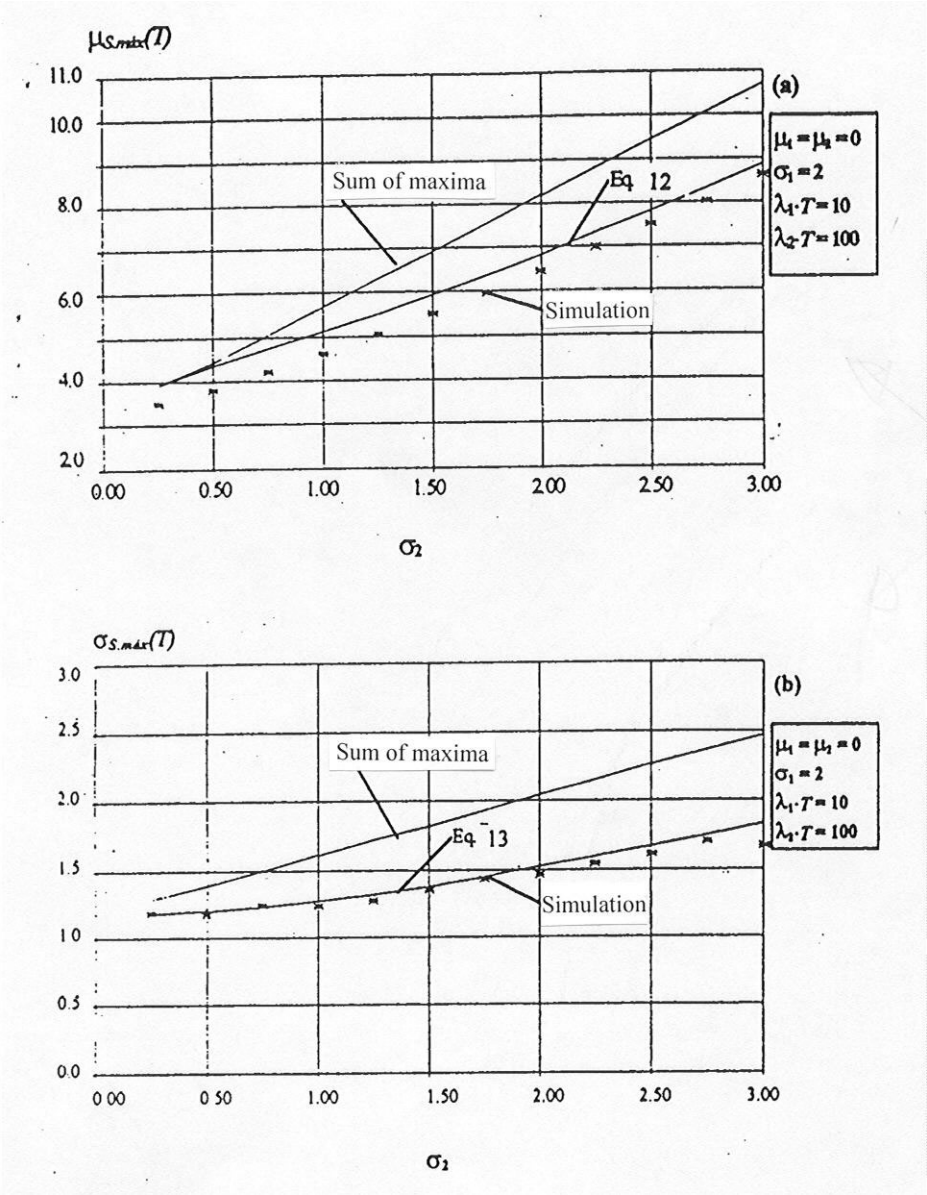

FIG. 16. Combination of a Process type 2 with a Process type 3.

Legend:

μ: mean
α: standard deviation

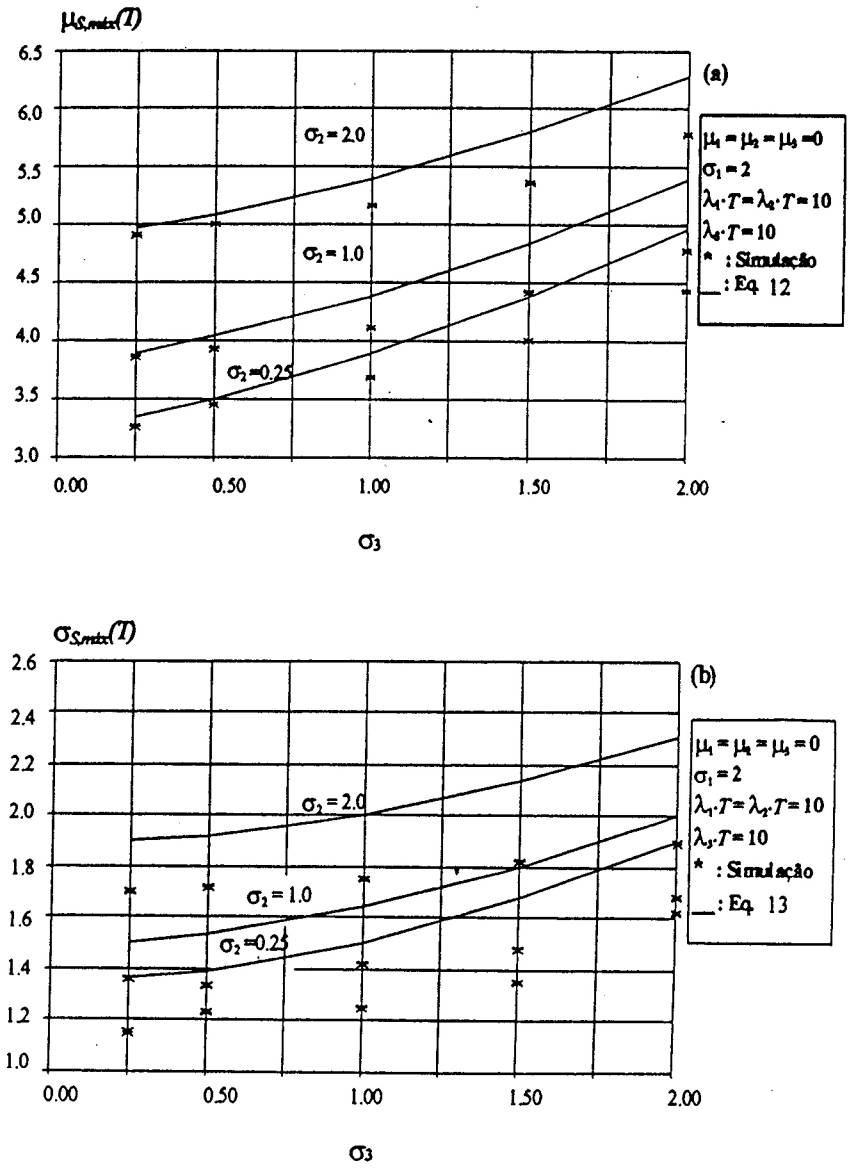

FIG. 17. Combination of two Processes type 2 with a Process type 3.

Legend:

μ: mean
α: standard deviation

Turkstra's rule leads to results that, from a theoretical standpoint, are not always on the safe side, because it is possible that the most unfavourable situation does not occur at the time when one of the individual actions presents its maximum value. In addition, the statistical characterization of the accompanying actions remains a difficult issue. The approach is nevertheless intuitively appealing and constitutes the underlying concept behind the Swiss standard SIA 160 (1989), first introduced in SIA 260 (1980); moreover, the same concept can be applied in a more general context.

Returning now to the mathematical evaluation of peak values of combined processes, it has to be noted that in the analysis of linear structures, the net effect S(t) at any arbitrary point of the structure due to the simultaneous action of N loads L_i(t) may be expressed in the form:

$$S(t) = \Sigma_i c_i L_i(t) \ (i = 1,\ldots N) \tag{20}$$

It will be herein assumed, as usual in most structural codes, that the load/effect conversion coefficients c_i are deterministic, i.e. present no uncertainty[4]. In addition, it will be further assumed that the load processes can be classified as types (a), (b) or (c). Similarly to the previous developments for a single process, discussed in para 5.7.2, the expected value and the standard deviation of the maximum value of S(t) in a time interval T will be sought next. For such purpose, some well known results of the Theory of Probability will first be recalled.

The expected value and the standard deviation of the combined process S(t) are given by:

$$\mu_S = \Sigma_{i=1} c_i \mu_i \tag{21}$$

$$\sigma_S = [\Sigma_{i=1} c_i^2 \sigma_i^2]^{1/2} \tag{22}$$

Now, if the load processes are Gaussian, any linear combination will also be Gaussian and equations (21)–(22) define completely the two parameters of the point in time distribution of S(t). In other cases, the distribution of S(t) will remain, more often than not, undetermined, but an *approximate* upper bound may be obtained by assuming that it may be modelled by a Type I distribution. Thus, a reasonable assumption for codified structural design may be to assign a Type I distribution to load combinations judged to have a heavy tail distribution.

In order to make use of the previously determined p and q coefficients, eqs. (17)(18), to evaluate the combined load effect, the *effective frequencies* $\lambda_{p,S}$ and $\lambda_{q,S}$ should next be determined. The estimators:

$$\lambda_{p,S} = \Sigma_{i=1} \lambda_i c_i \sigma_i / \sigma_S \tag{23}$$

$$1 / \lambda_{q,S} = \Sigma_{i=1} (1/\lambda_i) (c_i \sigma_i / \sigma_S)^2 \tag{24}$$

have been extensively tested by simulation and appear to be adequate for design applications [60].

The equations given above may be used to combine any number of Poisson square wave load processes (type a), with **one** process of type (b) or (c). For such purpose, the p and q coefficients in the equations:

$$\mu_{peak} = \mu_S + p(\lambda_{p,S}) \sigma_S \tag{25}$$

[4] EN 1990 gives the possibility of introducing an additional partial factor γ_{Sd} to account for model uncertainty in action and action effects.

$$\sigma_{peak} = q(\lambda_{q,S}\, T)\, \sigma_S \qquad (26)$$

are evaluated in terms of effective rates, using the functions in Fig. 16.

Alternatively, instead of determining the first two moments using effective rates, as indicated in eqs. (25)–(26), deer Kurgan [55] proposes calculating p and q as *weighted averages* of the appropriate coefficients for the individual loads p_i and q_{uip} :

$$p = \Sigma_{i=1}\, p_i\, (\sigma_i / \sigma_S)^2 \qquad (27)$$

$$q = \Sigma_{i=1}\, q_{uip}\, (\sigma_i / \sigma_S)^2 \qquad (28)$$

These approaches are compared in Section 4 with statistics of peak values determined through numerical simulation, for a number of situations of practical interest [63].

It should be noted, at this point, that *for the determination of peak values of the combination of Gaussian continuous random processes, with continuous derivatives,* der Kiuregian resorts to equations of the form (25)–(26), with effective rate given by:

$$\lambda_S = [\, \Sigma_{i=1}\, \lambda_i^2\, (\sigma_i / \sigma_S)^2\,]^{1/2} \qquad (29)$$

in which the rate of the individual processes λ_i are given by the ratio between the standard deviation of the process and the standard deviation of its derivative, divided by 2π.

5.7.4. Comparison of peak statistics obtained by different methods

Menger in [63] present results of Monte Carlo simulations for normal load processes, of both types (a) and (b), acting simultaneously with other normal or arbitrarily distributed processes. These are compared with the load combination criteria defined by eqs. (25)–(26) [60] and by eqs. (27)–(28), due to der Kiuregian [55]. It may be seen that both schemes appear to work well, yielding correct or slightly conservative results. Much work remains to be done, however, to qualify both approaches in terms of the final reliability of codified designs. In this context, the problem of load definition should be simultaneously addressed. A brief overview of the subject is given in the next paragraph.

5.7.5. Structural loads as random processes

The practical application of the previous or similar results from Random Process Theory requires the specification of all actions of interest as random processes. The adoption of a few, *simple* models, might allow code writers to define loads in a more complete and appropriate manner. Significant effort has been devoted by various authors in this direction, in spite of which little or no effect is perceptible in structural codes.

In connection with live loads in buildings, Harris *et al* [64] suggest peak values, standard deviations and rates of change λ for some loads occurring both in residential and office buildings, to be represented as type (a) processes. For the same application, earlier results from [65] provides the first two moments of the point in time distributions of vertical loads in public and private buildings. Similar information is due to [66–68].

The specification of wind loads as types (a), (b) or (c) processes has also received some attention in the last decade. In [69] Belk and Bennett evaluate, for a number of weather stations in the continental USA, the distributions of the time lag, the event duration and the amplitude for model (c). The so-called clustering effect, already mentioned in para. 5.7.2 is also examined in connection with the data analysed by these authors. The mean of the time lag varies, for a group of nine stations, between 36 and 127 hours, the standard deviations being approximately 25% larger than the respective means, suggesting that the time processes are not Poisson, exhibiting a perceptible clustering effect. The duration presents a mean value of 5.4 hr and a standard deviation of only 1.2 hr, which indicates a remarkable homogeneity among the weather stations. In addition, the standard deviation for each station has an expected value of 5.8 hr, that is approximately equal to the expected duration. Belk and Bennett observe that the Fisher–Tippett I (Gumbel) distribution shows the best fit to the amplitude data, but make no reference whatsoever to the storm type. It has been widely acknowledged that the type of meteorological phenomenon that gives rise to the wind, i.e. the storm type, is a governing factor in the problem [70]

It has already been shown that in temperate climates, thunderstorm winds (TS) and extra-tropical storm winds (usually designated EPS, for *extended mature pressure systems*) should be dealt with separately. In areas affected by tropical cyclones, (typhoons), these should also be treated as processes with different characteristics. Preliminary studies suggest that TS winds may be described as Poisson pulse processes (type b), because the mean duration, about 5 min, is negligibly small in comparison with the mean duration of most loads in structural engineering. The same model is applicable for tornado winds. The risk of overlapping with other short duration, low frequency of occurrence loads, such as earthquakes, may in general be neglected. Type (c) processes constitute an interesting model for EPS storms, with preliminary values of the parameters given by [69]. It has top be noted that, in connection with the load combination problem, if $1/\lambda$ for the other processes is larger than twice the mean duration of each EPS wind storm, then these winds might also be represented, approximately, by Poisson pulse processes.

5.7.6. Extreme loads derived from scenarios

There are cases of truly exceptional events for which no statistics are possible: this is e.g. the case of terrorist attacks. There are other cases, not infrequent, in which the engineer faces the task of estimating actions on the basis of short time records, which are not compatible with the desired or target reliability of the structure: for instance, the risk of tornado winds at a given site can hardly be estimated from 20 or 30 years wind series at the location of interest, which will usually contain *no record or measurement* of the type of storm under consideration. Similar situations arise in connection with extreme rain, floods or earthquakes, or — outside natural phenomena — impacts from falling aircraft or off course vessels.

If these cases would occur, a value L_k of the action should be included in the calculations that may still be defined ‘characteristic value’ but is merely a ‘scenario value’: it should be evaluated as the ‘largest possible’ value (which is possible for some natural phenomena or some accidents, at least assuming that the present conditions do not vary in time: e.g. that the size of commercial aircraft do not increase) or the more vaguely defined ‘as large as reasonable’ or ‘as large as credible’ value. In any case, it should be clear that no statistical meaning or ‘probability of occurrence’ can be attached to such values.

Note that this problem *should not* be confused with the estimation of the distribution of extremes from short duration records, which is related to the large *statistical uncertainty* of the estimates and is further discussed in paras 5.7.7 and 5.7.8.

5.7.7. Models of rare events

Sometimes, in particular in the case of meteorological phenomena, the scarcity or non-existence of observations of rare events may be overcome by the development of *models of the meteorological phenomenon*, such as a tornado, which is then *coupled* with statistics of *the rate of occurrence of the phenomenon* in the region. The latter are normally available, and allow the evaluation of extreme loads statistics at any specific site by simulation. Such an approach has been applied by Riera and Rocha [70] to obtain simulated series of the annual maxima of thunderstorm (TS) winds, resorting for such purpose to a modified Zhu and Etkin [71] model of the wind field during a downburst.

In connection with TS winds, which are responsible for extreme velocities in temperate climates, relevant applications to transmission line systems of models of the wind field have been recently reported. Holmes and Oliver [72] discuss a model similar to that employed by Riera and Rocha [70], that is applied by Oliver *et al* [73] in a risk analysis of transmission lines. Wood *et al* [74] in addition to a numerical model of the wind field, conducted laboratory tests in a specially designed wind tunnel. It may be envisaged that, after these models are fully characterized and tested by comparison with full scale observation, all that is required to generate representative wind series at a given location is the mean number of storms per unit area in the region.

5.7.8. Statistics of extremes based on short duration records

Often only short duration records, of the order of, or less than ten years long series of yearly maxima of the variable under study, are available for the assessment of extreme values. It is known that in such situation the statistical uncertainty in the estimation of peak values associated with low probabilities of occurrence, as required in NPP design, is just too large and makes a purely statistical evaluation of the desired parameters of little practical use. The approach outlined in the previous Section may be resorted to, but for most external actions it may be not ready for immediate use. In the following, a simpler method is suggested, which complements the recorded data with *prior* information.

Assuming that the extreme annual wind, precipitation, or other meteorological variable, V, has to be evaluated, a *prior* probability distribution $P_V(v)$ of V should be proposed, on the basis of (a) models available for regions with similar climate, (b) records obtained at neighbouring sites, or (c) a combination of (a) and (b). The variable V is observed at the site, resulting in a set of *recorded* values V_i, (i= 1, N). When N is small, the possibility of establishing $P_V(v)$ by statistical analysis of the records should be ruled out. A Bayesian approach to *update* the parameters of $P_V(v)$ is possible and constitutes an attractive alternative.

For the basic cases in which $P_V(v)$ is *assumed* normal or log normal, [75] provides the necessary equations to update the mean value and the standard deviation of the variable under consideration once N samples V_i are available. Similar developments are still needed for extreme value distributions.

6. CONCLUSIONS

In some cases the differences in engineering tradition, availability of site related data and research progress in Member States prevented a general agreement on the questions arisen at the beginning of the TCM. In these cases however, this report collects the different solutions given in the Member States, as a reference for further discussions. In some other cases common concern was expressed for some safety issues and a more rigorous approach was suggested.

As general recommendations from the TCM to the IAEA for further activities in the field, the following list was collected:

- A major concern dealt with the differences in nuclear standards in many Member States which gives the impression of different safety levels in the respective design. The TCM recommended an effort for homogenization of main assumptions in hazard evaluation, leaving to national practice and experience the selection of the most suitable methodology in relation to data availability. Frequent exchange of experience among Member States, also with the support of IAEA, was encouraged to meet this goal.
- It was noted that in some cases events not considered in the design basis of the plant created major challenge to its safe operation. The TCM recommended a deep use of information exchange and periodic safety reviews in order to prevent such occurrences, according to the most updated state of the art knowledge.
- A review of the hazard evaluation for all the external events was recommended for a more consistent approach which eliminates discrepancies between different sources and which introduces a suitable grading in the design according to the risk of the installation. Such risk based approach had a general consensus at the TCM, even if most of the Member States agreed that it is difficult to be applied in its formal completeness and it might provide the illusion of a more reliable approach, while very often it introduces higher uncertainties. Therefore the TCM encouraged the development of 'trial and error' processes where some conservative hypotheses are assumed at the early design stage for a straightforward deterministic design process, to be confirmed in the safety assessment phase by some probabilistic tools. Such an approach can provide also useful information for prioritization in maintenance, re-evaluation, upgrading etc. and they deemed to be effective also in risk comparison with other installations, with positive outcomes also on public acceptance tasks.
- Application of PSA to external event scenarios was encouraged, but its development should be consistent and fully integrated with the assumptions for internal events.
- Databases of events and consequences have been encouraged by TCM. However, problems the consensus among Member States is still prevented by some confidentiality in the release of information.
- An effort was recommended in the better definition of monitoring system goals, in their operating procedures and in the relevant operator actions to be taken according to forecasting models for the external event scenarios. The list of items to be inspected after major events requires also a better definition to guarantee the preservation of safety levels after major events.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, IRS User's Manual, IAEA, Vienna (2000).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, INES User's Manual, IAEA, Vienna (2001).

[3] PHB Hagler Bailly Inc., Nuclear Performance Experience Database, October 1999.

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Site Evaluation for Nuclear Facilities, Safety Standards Series (to be published).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of Seismic Hazards for Nuclear Power Plants, Safety Standards Series No. NS-G-3.3, IAEA, Vienna (2003).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, External Human Induced Events in Site Evaluation for Nuclear Power Plants, Safety Standards Series No. NS-G-3.1, IAEA, Vienna (2002).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Geotechnical Aspects of Nuclear Power Plant Site Evaluation and Foundations, Safety Standards Series, IAEA, Vienna (in preparation). [OK?]

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Flood Hazards for Nuclear Power Plants on Coastal and River Sites, Safety Standards Series, IAEA, Vienna (to be published).Design Basis Flood for Nuclear Power Plants on River Sites: A Safety Guide, Safety Series No. 50-SG-S10A, IAEA, Vienna (1983).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Meteorological Events in Site Evaluation for Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (2003).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (2003).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (2003).

[13] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Single Failure Criterion: A Safety Practice, Safety Series No. 50-P-1, IAEA, Vienna (1990).

[14] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of Micro-earthquake Surveys in Nuclear Power Plant Siting, IAEA-TECDOC-343, Vienna (1985).

[15] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodology and Procedures for Compilation of Historical Earthquake Data, IAEA-TECDOC-434, Vienna (1987).

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, Quality Assurance for Safety in Nuclear Power Plants and Other Nuclear Installations: Code and Safety Guides Q1–Q14, Safety Series No. 50-C/SG-Q, IAEA, Vienna (1996).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual on Quality Assurance for the Survey, Evaluation and Confirmation of Nuclear Power Plant Sites, IAEA-TECDOC-416, Vienna (1987).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Probabilistic Safety Assessment for Seismic Events, IAEA-TECDOC-724, Vienna (1993).

[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Evaluation of the Safety of Operating Nuclear Power Plants Built to Earlier Standards — A Common Basis for Judgement, Safety Reports Series No. 12, IAEA, Vienna (1998).
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (in preparation).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for NPPs, Safety Standards Series, IAEA, Vienna (in preparation).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection against Fire and Internal Explosions in Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (in preparation).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, Dispersion of Radioactive Material in Air and Water and Consideration of Population Distribution in Site Evaluation for Nuclear Power Plants, Safety Standards Series No. NS-G-3.2, IAEA, Vienna (2002).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, Fuel Handling and Storage Systems in Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (to be published).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, Emergency Power Systems at Nuclear Power Plants: A Safety Guide, Safety Series No. 50-SG-D7 (Rev. 1), IAEA, Vienna (1991).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, Safety Standards Series, IAEA, Vienna (to be published).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Protection Against Internal Hazards (Other than Fire and Explosions), Safety Standards Series, IAEA, Vienna (to be published).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, Safety Standards Series No. NS-G-1.2, IAEA, Vienna (2001).
[30] STEVENSON, J., “Hazard evaluation for NPPs”, presentation made at the IAEA/EBP workshop, BATAN Jakarta, Indonesia (2000).
[31] US/NRC, Perspectives gained from the individual plant examination of external events (IPEEE) programme, (Draft report for Public Comment), NUREG-1742, NRC, Washington, April 2001.
[32] NUREG/CR-6239, Survey of Strong Motion Earthquake Effects on Thermal Power Plants in California with Emphasis on Piping Systems, (Main Report): ORNEL/Sub/94-SD427/2/V1, Vol. 1, Appendices: ORNEL/Sub/94-SD427/2/V2, Vol. 2 (1994).
[33] IPSN, Rapport sur l’inondation du site de Blayais survenue le 27 décembre 1999, IPSN, 17 January 2000.
[34] FORNER, S., Extreme cold weather in France and consequences on PWR NPP: French practice, Autorité de Sûreté Nucléaire, Presentation given at the IAEA/Technical Committee Meeting on Structural safety of NPPs in relation to extreme external loads, IAEA, Vienna, December 2000.

[35] Autorité de Sûreté Nucléaire, La protection contre les risques externs, Contrôle, No. 142, Paris, September 2001.
[36] Atomic Energy Council of the Republic of China, Facsimile to IAEA Emergency response Unit, 23 March 2001
[37] NUCLEONICS WEEK, Special Vol 42, 6 April 2001.
[38] INTERNATIONAL ATOMIC ENERGY AGENCY, Manual for the Classification and Prioritization of Risks due to Major Accidents in Process and Related Industries, IAEA-TECDOC-727, Vienna (1996).
[39] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidelines for Integrated Risk Assessment and Management in Large Industrial Areas, IAEA-TECDOC-994, Vienna (1998).
[40] USA-EPRI, A Methodology for Assessment of Nuclear Power Plant Seismic Margin, Report NP-6041-M, (Revision 1), EPRI, Palo Alto, August 1991.
[41] PRASSINOS, P., et al., Recommendations to the NRC on trial guidelines for seismic margin review of nuclear power plants, NUREG/CR-4482, LLNL, March 1986.
[42] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review of Operational Nuclear Power Plants, Safety Series No. 50-SG-O12, IAEA, Vienna (1994).
[43] ASME Boiler and Pressure Vessel Code, Section III, Div. 1, Appendix F, "Rules for Evaluation of Service Loadings with Level D Service Limits," American Society of Mechanical Engineers, 1998.
[44] NEBUDA, D.T., Protection against malevolent use of vehicles at nuclear power plants, (Alternate title: Vehicle barrier system selection guidance), NUREG/CR-6190 (1994).
[45] CEN, European Committee for Standardization: Draft prEN 1990, Eurocode: Basis of Structural Design; Brussels, January 2001.
[46] CEN, European Committee for Standardization: ENV 1991-2-7:1998, Eurocode 1, Part 2–7: Accidental actions due to impact and explosions
[47] STEVENSON, J.D., et al., "Advances in the analysis and design of concrete structures, metal containments and liner plate for extreme loads", in: Nuclear Engineering and Design, Vol. 134, No.1, **87–109**, North-Holland, Amsterdam (1992).
[48] HADJIAN, A.H., "Issues with partial safety factors", Proceedings of the 8th International Conference on Structural Safety and Reliability (ICOSSAR 2001), Newport Beach, CA, USA, June 2001, BALKEMA, A.A., Publishers (Abstract Volume, p.115; CD-ROM to be published)
[49] ELLINGWOOD, B., GALAMBOS, T.V., MACGREGOR, J.C., CORNELL, C.A., "Development of a Probability Based Load Criteria for American National Standard A58", NBS Special Publication 577 (1980)
[50] RAVINDRA, M., GALAMBOS, T.V., "Load and Resistance Factor Design for Steel", Journal of the Structural Division, ASCE, Vol. 104, No. ST9, **1337–1353**, (1978).
[51] BORGES, J.F., CASTANHETA, M., "Statistical definition of combination of loads", in: Probabilistic Design of Reinforced Concrete Buildings, Publication SP-31, **43–63**, American Concrete Institute, Detroit, Michigan, USA (1972).
[52] WEN, Y.K., "Probability of extreme load combination", Proceedings of the 4th. Int. Conf. on Structural Mechanics in Reactor Technology, (SMiRT 4), Vol. M, San Francisco, California, USA (1977b).

[53] WEN, Y.K., “Statistical combination of extreme loads”, Journal of the Structural Division, Proceedings ASCE, Vol. 103, ST5 (1977a).
[54] DER KIUREGIAN, A., “Second-Moment Combination of Stochastic Loads”, Journal of the Structural Division, ASCE, Vol. 104, No. ST10, Paper # 14056, **1551–1567**, Oct. (1978).
[55] LARRABEE, R.D., CORNEL, A., “Combination of various load processes”, Journal of the Structural Div., **223–239**, 107, ST1, Proceedings ASCE (1981)..
[56] WEN, Y.K., Structural load modeling and combination for performance and safety evaluation, Elsevier, Amsterdam (1990).
[57] BREITUNG K., RECKWITZ, T., “Upcrossing rates for rectangular pulse load process”, Report No. 42, SFB96, Laboratory for Structural Engineering, T.U. Munich, Germany (1979).
[58] GAVER, D.P., JACOBS, P.A., On combination of random loads, Journal of Applied Mathematics, SIAM, Vol. 40, No. 3, June 1981.
[59] ROCHA, M.M., RIERA, J.D., BARRAGAN, G.F.A., Uma proposta para combinar ações em normas de projeto estrutural, in: *Memorias, XXVII Jornadas Sudamericanas de Ingeniería Estructural,* Lab. de Estruturas, UNT, S.M. de Tucumán, Argentina, Vol. 2, **25–36** (1995).
[60] SCHNEIDERT, J., Introduction to Safety and Reliability of Structures, Structural Engineering Documents, Int. Assoc. for Bridge and Structural Engineering, IABSE, Zürich, Switzerland (1997).
[61] TURKSTRA, C.J., Theory of Structural Design Decisions, Study No. 2, Solid Mechanic Division, University of Waterloo, Waterloo, Ontario, Canada (1972).
[62] HARRIS, M.B., COROTIS, R.B., BOVA, C.J., Area-dependent process for structural live loads, Journal of the Structural Division, ASCE Proceedings, Vol. 107, ST5, **857–873** (1981).
[63] MENGER, J.R., Estudo de critérios de combinação de cargas a serem utilizados em normas de projeto estrutural, Master's Thesis, CPGEC, Universidade Federal do Rio Grande do Sul, Porto Alegre, Brazil, (in progress, 1999).
[64] CULVER, C.G., Live-load survey results for office buildings, Journal of the Structural Division, ASCE Proceedings, Vol. 102, ST12, **2269–2284** (1976).
[65] COROTIS, R.B., DOSCHI, V.A., Probabilistic models for live-load survey results, Journal of the Structural Division, ASCE Proceedings, Vol. 103, ST6, **1257–1274** (1977).
[66] CHALK, P.L., COROTIS, R.B., Probabilistic model for design live loads, Journal of the Structural Division, ASCE Proceedings, Vol. 106, ST6, **2017–2031** (1980).
[67] WEN, Y.K., Statistics of extreme live loads in buildings, Journal of the Structural Division, Proceedings ASCE, Vol. 105, ST10, **1893–1900** (1979).
[68] BELK, C.A., BENNETT, R.M., Macro wind parameters for load combinations, Journal of Structural Engineering, ASCE Proceedings, Vol. 117, No. 9, **2742–2756** (1991).
[69] RIERA, J.D., ROCHA, M.M., Load definition for wind design and reliability assessments: Extreme wind climate, in: Int. Conf. on Wind Effects on Buildings and Structures, A.A. Balkema, Rotterdam (1998).
[70] ZHU, S., ETKIN, B., Model of the Wind Field in a Downburst, Journal of Aircraft, Vol. 22, No. 7, **595–601**, July 1985.
[71] HOLMES, J.D., OLIVER, S.E., An empirical model of a downburst, Engineering Structures, Elsevier, Vol. 22, **1167–1172** (2000).

[72] OLIVER, S.E., MORIARTY, W.W., HOLMES, J.D., A risk model for design of transmission line systems against thunderstorm winds, Engineering Structures, Elsevier, Vol. 22, **1173–1179** (2000).

[73] WOOD, G.S., KWOK, K.C.S., MOTTERAM, N.A., FLETCHER, D.S., Physical and numerical modelling of thunderstorm downbursts, Journal of Wind Engineering and Industrial Aerodynamics, Elsevier, Vol. 89, No. 6, **535–552** (2001).

[74] MADSEN, P.H., LIND, N.C., Bayesian Approach to Prototype Testing, Proceedings ASCE, Journal of the Structural Division, Vol. 108, No. ST4, **753–770**, April 1982.

Annex I

A PROPOSAL FOR EXTERNAL EVENT EVALUATION

POSTULATED HAZARDS CONSIDERED IN NUCLEAR FACILITY SITING AND DESIGN BASED ON INTERNATIONAL EXPERIENCE AND PRACTICE*

I.1. INTRODUCTION

Conventional industrial facilities typically divide siting criteria and postulated design loads into two categories. Those loads which have a probability of occurrence per year on the facility greater than 10^{-1} are termed service or normal loads. The second category termed severe or occasional loads are those loads which typically have a mean or median probability of occurrence between 10^{-1} and 10^{-2} per year. In recent years this probability of exceedance for design basis earthquakes for conventional facilities has been extended to 2×10^{-3}/a. Other external hazard loads are typically set at the 5×10^{-2}/a probability of exceedance. If these loads thus defined have the ability to 1) significantly impair the facility's mission, 2) cause significant damage to the physical plant or 3) lead to loss of human life, these postulated loads become design basis loads.

Nuclear facility structures, systems and components, SSC which have a safety related or mission function typically consider a third category of loads termed extreme loads whose combined probability of exceedance and resultant probability of failure would result in radiological consequences to the public in excess of acceptable limits as defined by national regulatory authorities. Most national regulatory authorities have established a safety goal of 10^{-7}/a or less probability of release of undefined amount of radioactive material to the environment for a large nuclear power reactor. This safety goal typically is set at two to three orders of magnitude below what would be established as safety goals for conventional industrial facilities. As a result of this definition, extreme loads and extreme load combinations considered in design have a practical range of occurrence per year between 10^{-3} and about 10^{-6}, depending on the consequence and the credit taken for design features to prevent or mitigate the consequences of the extreme event occurrence.

There are other nuclear facilities such as spent fuel and high level radioactive waste storage facilities, relatively large research reactors and other similar types of nuclear facilities where the postulated radiological hazards are considered to be significantly less than a large >1000 MW(t) nuclear power plant where safety goals have been established at 10^{-6}/a. For even lower hazard nuclear facilities with very limited radioactive inventories such as zero power reactors low level nuclear waste storage and incinerators safety goals equivalent to essential or hazardous conventional facilities have been established at 10^{-5}/a.

Extreme loads mean or median probabilities of exceedance associated with these less stringent nuclear safety goals are typically one to two orders of magnitude less than the extreme load probabilities established for large nuclear power plants and range from about 10^{-2} to 10^{-5} per year.

* This annex has been prepared by J.D. Stevenson, USA.

I.2. PROBABILITY OF FAILURE

Probability of failure assessments or risk informed design are playing an increasingly significant role in defining design load for nuclear facilities. Perhaps its most important role has been in the area of the decision process regarding extreme load design basis. Prior to its employment, nuclear facility design requirements were based to a considerable degree on the 'minimax' decision rule which says the worst possible future is certain to be found so action should be taken that minimizes the maximum possible loss [I.1]. This is popularly referred to as the 'what if' basis for design where loads and particularly their combination would be postulated regardless of their probability of occurrence hence become design bases. These design requirements were typically used in the 1965 to 1971 era of nuclear power plant, NPP design when most of the existing world's nuclear power plants design requirements were established.

The minimax rule was tempered somewhat by the reasonable decision rule which says that any reasonable decision maker under the same circumstances and with the same background would take the same action; hence these decisions tended to be made also considering historical precedents. Finally, there is the acceptable risk decision rule which says take the action where the sum of the products of the probability of exceedance and the consequences of exceedance are equal to or less than a risk associated with some natural phenomena over which society apparently has no control or is less than some human made activity which historically has been accepted by society, considering the actual or perceived cost/benefit to society.

The current tendency in nuclear facility design is a continuing shift away from minimax rule or deterministic based siting and design toward an acceptable risk informed rule tempered with the reasonableness rule. However, it should be understood that there is often an inability to develop an accurate probability assessment in many areas because of the lack of the necessary statistical data or ignorance as to the governing relationships and variability in the phenomena being investigated. For this reason deterministic bounds are often placed on the applicable design criteria which are developed based on the acceptable risk rules.

For other types of extreme loads in some States national jurisdictions there is a reluctance to assign any probability criteria. These typically include airplane crash, external blast, and some design basis accident loads.

I.3. DESCRIPTION OF POTENTIAL DESIGN BASIS HAZARDS

Table I.1 identifies hazard probabilities and performance or design categories which it is recommended be considered in the development of a design basis for external, natural and human induced and facility accident hazards for typical nuclear and other industrial facilities.

In Table I.2 is a list of the hazards which should be evaluated in the siting and design of a nuclear power plant. Many of the hazards listed in Table I.2 appear in the safety analysis report but do not become design basis hazards or loads because of the exclusion criteria which is identified in Table I.2.

Large nuclear power plants have very high radioactive inventories of radioactive decay products in the fuel. In most water cooled reactors the potential for release of the

radioactive inventory in the fuel due to primary confinement (fuel element and vessel) failure is relatively high. However, for gas cooled reactors this potential for failure is typically several orders of magnitude lower. For this reason water cooled reactors typically require secondary containment structures while gas cooled reactors have not. Also because of the high pressures and temperatures associated with most reactor coolant systems there is a high potential for wide spread dispersion are contamination from such materials if energetically released from the core. Suggested design or performance categories for other types of nuclear facilities are also shown in Table I.2. The potential for release and wide spread dispersion as considered in the development of the probabilities given in Table I.1. In my opinion the PBMR should fall into the performance or design Category 4 relative to reactor safe shutdown and into Category 3 for spent fuel and high level waste storage condition as shown in Table I.1.

I.4. LOADS TYPICALLY CONSIDERED IN DESIGN OF NUCLEAR POWER PLANTS

Loads considered in NPP design may be grouped into the following categories, according to their nature and recurrence:

- Seismic loads
- Severe loads
- Extreme loads

Details on the treatment of each category is provided in the following:

I.4.1. SERVICE LOADS

Service or normal loads on a structure such as dead (D) or live (L) loads are usually considered with predetermined design margins in the form of load factors or allowable stresses and are applied as defined in applicable national building codes. Included in live load would be also any buoyancy (B) hydrostatic (H) and lateral earth pressure (Ep) loads. Also included should be normal steady state and anticipated operating transient loads (i.e. startup and shutdown) including operating temperature (To) and reaction (Ro) effects with probabilities of occurrence in the range of 1.0 to 10^{-1}/a.

I.4.2. SEVERE LOADS

The probability of occurrence for severe loads is usually considered in the range 10^{-6}–10^{-3}. They include natural and plant loads.

I.4.2.1. Seismic loads

The severe seismic load is typically defined in national building codes as a general requirement for all buildings. It is often defined as a 2×10^{-3}/a level of probability of exceedance for ordinary buildings and 1×10^{-3}/a for essential or commercially hazardous buildings by use of a 1.25 importance multiplication factor applied to ordinary building seismic loads. Historically, SL-1 or operating basis earthquakes, OBE were also defined severe load category for design purposes. However, recently it has become design practice in some IAEA Member States to eliminate the SL-1, OBE as a design basis since the SL-2 effects essentially envelope the effects of the SL-1, OBE.

I.4.2.2. Flood, wind and precipitation loads

The design basis wind load is also defined on a probabilistic basis. The design basis wind velocity selected is typically based on either a several minute average fastest wind or more recently a maximum 3 second gust wind speed for a 50 to 100 year recurrence interval for the site exposure level based on national building code standards. It should be noted that precipitation (rain and snow) loads are usually defined for design at the 50 to 100 year reoccurrence interval or 2×10^{-2} or 10^{-2} probability of exceedance level.

I.4.2.3. Operating transients — Occasional and upset condition loads

Plant specific expected operational transients are included in this category with 10^{-1} to 10^{-2}/a probability of exceedance levels.

I.4.3. EXTREME LOADS

Consequences of nuclear power plant facility failures differ significantly from those in conventional structures, systems and components. In conventional facilities life safety of the human occupants is usually the primary concern. Nuclear power plants potentially release significant amounts of radioactivity to the environment, hence have both a short term as well as a long term effect public health and safety. The prevention of such failures in nuclear power plants and the mitigation of their potential consequences have been the primary objectives of nuclear facility safety design.

I.4.3.1. SL-2 earthquake hazard

This level of extreme earthquake ground motion should have a very low probability* of being exceeded during the design life of the plant and represents the maximum level of ground motion to be used for design purposes. Its evaluation should be based on the seismotectonic model and/or detailed knowledge of the seismology, geology and engineering parameters of the site region and area.

Regardless of the seismic hazard potential, a design basis ground motion corresponding to the safety level SL-2 earthquake is recommended to be adopted for every nuclear power plant. The recommended minimum level regardless of the site location is a peak ground acceleration of 0.1g (zero period of the design median shaped ground response spectrum).

Historically SL-1 or OBE level earthquake with a peak ground acceleration value of one half, the SL-2 earthquake was applied with more restrictive acceptance criteria. However, recently this requirement has been dropped in some IAEA Member States when the SL-2 earthquake has a PGA of less than 0.5g.

* In IAEA Member States the SL-2 earthquake determined on a deterministic basis corresponds to a level with a probability of 5×10^{-3} to 1×10^{-5} per year of being exceeded. Some Member States have established a probability of event exceedence as low as 10^{-5}/a using median seismic input and 10^{-4}/a using 85th percentile imput of 1×10^{-4} per year.

I.4.3.2. Straight, hurricane, typhoon and cyclonic wind hazard

These winds observed at a fixed weather station generally follow an Extremal Type I or other skew positive probability density function distribution, with the higher observed values in the distribution associated with moderate and larger cyclonic wide area storm systems. Historically, such wind design parameters have been averaged over a relatively long period of time (i.e. 1.0 minute to 1.0 hour) and require a gust factor greater than 1.0 to be applied for design of structures, systems, or components, SSC. More recently the fastest 3 second duration gust wind is being defined for SSC design purposes. A wind speed having a probability of occurrence equal or less than 10^{-5}/a to 10^{-6} should be used to define these wind loads in the Extreme Category.

The applications of hurricane, typhoon and cyclonic storm effects are usually limited to coastal regions of large land masses and islands of the Atlantic East and Gulf of Mexico coasts of North America, Central America Eastern Pacific Coast as well as the Western Pacific and the Indian Ocean.

I.4.3.3. Tornado hazard

Tornadoes which are defined as a very high intensity small radius cyclonic wind occur over large continental land masses which do not have significant natural barriers to the mixing of warm moist air from tropical seas with cold air from the temperature zone. They can also occur within the general circulation of a hurricane, typhoon or cyclone. Historically worldwide they have been considered for design purposes at only relatively few NPP sites. When considered they have typically been defined at the 10^{-6} to 10^{-7} per year probability of exceedance level based on generic or large region tornado statistics. Current design criteria for nuclear power plants on a probabilistic basis ranges from 10^{-5} to 10^{-7}/a event probability level. The very low probability levels (10^{-5} to 10^{-7}) typically established for tornadoes as compared to earthquakes (10^{-3} to 10^{-5}) can be explained at least in part by the potentially wide and rapid dispersion of radionuclides by tornado type wind action where this is generally not the case with earthquakes unless accompanied by fire.

In most of the land territory of Russia wind loading effects will have the greatest effect on nuclear facility design

I.4.3.4. Tsunamis, seiche and flood hazard

I.4.3.4.1. Tsunamis and seiche

Tsunamis (ocean) are the long water waves (with wave periods from 5 to 60 minutes, or longer range) generated impulsively by mechanisms such as exploding islands (volcanic eruptions), submerged landslides, rockfalls into bays or the ocean, tectonic displacements associated with earthquakes, and underwater explosions. Seiches are similar to Tsunamis but typically occur in bays and lakes. When tsunami or seiche waves reach a coast, initially a draw down occurs which has the appearance of a rapidly occurring low tide then water surges back in the form of a ‘tidal wave.’ The elevation above the tide level (at the time of the tsunami or seiche) reached by this water is called the runup elevation. Runup elevations vary considerably from point to point along the coast and are very sensitive to the shape of the coastline as it relates to the direction of the source mechanism for the wave. The Russian Pacific Coast has experienced such phenomena.

I.4.3.4.2. Floods

All NPP located on bodies of water subject to flooding should be designed to survive a design basis flood typically called the probable maximum flood (PMF). The most expedient design solution is to locate plant grade and safety related SSC above the maximum flood level.

I.4.3.4.3. Precipitation (rain, ice and snow)

It is often current design practice not to identify precipitation (rain, ice or snow) as design loads except in the severe load category. It is recommended that they also be included in the extreme load category and they be included in roof design including the effects of blockage of the primary roof drain systems. It should also be understood that storm sewer systems for NPP are typically designed for only a 25 year return period. Excess precipitation beyond the 25 year return period should be capable of surface run off.

I.4.3.5. Missile hazard

In missile protection NPP design probability assessment has played a direct role. In general, all postulated missiles are evaluated as to their potential for becoming design bases missiles on the basis of at least three probabilities in the form:

$$P_u = (P_3/ P_2) \text{ x } (P_2/ P_1) \text{ x } (P_1) < P$$

where:

P_a = the limiting probability as a function of the hazard and consequences. Typically P_a varies from 10^{-5} to 10^{-7}/a. For large nuclear power plants associated with a large loss of coolant accident a value of 10^{-7}/a is often specified.

P_1 = the probability a missile will be generated.

(P_2/ P_1) = the conditional probability a missile will strike a safety class component given a missile has been generated.

(P_3/ P_2) = the conditional probability a missile will break or fail safety class Structure, System or Component, SSC given a missile has impacted the safety class SSC.

P_U = the joint or total probability of P_1, (P_2/ P_1) and (P_3/ P_2)

In most cases the total probability of as the probabilities and the hazard probability will have to be determined by convolution within the integral $\int_0^\infty$ H(a)f(a)da where H(a) is the hazard function (hazard magnitude as a function of probability of exceedance) and f(a) is the probability distribution function typically defined as a fragility function.

In those instances where P_1 is less than 10^{-6}/year, then the postulated missile need not be considered as a design basis missile. Where $(P_2/ P_1) \times P_1$ are less than 10^{-6}/year, then the missile needs to be considered only to the extend that (P_2/ P_1) and P_1 need to be determined.

When the conservation of P_2/P_1 and P_1 is greater than 10^{-6}/a in Eq. (1) a structural evaluation of the target structures, systems and components, SSC required to determine (P_3/ P_2).

In those cases where P_u is greater than 10^{-6}, then some design evaluation is indicated and postulated missile becomes a design basis missile. The changes can take the form of decreasing any or all of the P_1, (P_2/P_1) or (P_3/P_2) so that the 10^{-7} limit can be met. Example of reductions in P_1 would be improved material or control system or use of physical restraints or guard structures around the potential missile source. An example of P_2/P_1) reduction would be relocation or reorientation of target components or potential missile sources to reduce the probability of missile impact on the target. An example of P_3/P_2) reduction would be to increase the structural resistance to missile load of the target component.

I.4.3.5.1. Extreme wind missiles

Extreme wind missiles when they are considered for design typically are associated with two types of missiles, 1) penetrating type with a relatively high velocity, rigidity, small mass and impact area and 2) impact type with somewhat reduced velocity, crushable, large mass and impact area.

I.4.3.5.2. Rotating equipment rupture missiles

Failures of large steam or high velocity gas turbines resulting in throwing parts of the turbines as energetic missiles have been known to occur. The failures generally fall into two categories: failure at operating speed due to design, material, or environmental deterioration factors; or else failure at a high overspeed due to a failure of the speed and load control system.

In recent years steam turbines with 100 percent inspection and quality control and advanced manufacturing procedures, and turbine control systems with double or triple redundancy for nuclear power plants, have become standard. In addition many turbine manufacturers have done reliability analyses of the potential failure modes of the their turbines or the control systems and have predicted rates of failure below that which is considered credible for NPP design or evaluation purposes. However, to reach this conclusion their turbines are generally orientated so that no line of sight missile could strike the containment or confinement of the Reactor Coolant System and other safety related Structures, Systems and Components, SSC.

I.4.3.5.3. Internal missiles

In many NPP designs plant internal missiles have been identified for potential design purposes. These include value stems, instrumentation inserts pump fly wheels and other parts and appurtenances which may be ejected from high energy system failure in close proximity to the reactor coolant system.

I.4.3.6. Aircraft crash hazard

In some IAEA Member States airplane crash are deterministically considered as a design basis. In other states a NPP is considered adequately designed against aircraft hazards

if the probability of aircraft accidents resulting in significant undefined radiological consequences to the public in excess of allowable limits is less than 10^{-6} to 10^{-7}/ year.

The statistical probability of aircraft impacts on a nuclear plant depends on its location with respect to flight paths proximity to commercial or military air fields and upon the accident (crash) rates for different types of aircraft at the site location. The size (mass) and velocity of the various aircraft which are assumed to crash upon a nuclear power plant and the effect of postulated burning fuel and impact shock loads on internal SSC should also be taken into account in assessing the probability of damage or failure if the incident probability is considered high enough to warrant its consideration.

In most States there is an annual census of aircraft as a function of weight, landing, and cruising speed, etc., and annual accident data which can be statistically analysed to determine the probability of an aircraft hitting safety related SSC of a NPP structure. In general aircraft crashes, their physical characteristics and whether or not they should be considered as a design basis is left up to the individual national regulatory authority. It should also be mentioned that there is a growing concern that small aircraft crashes may not be definable on a statistical basis.

The aircraft crash hazard has often received more significant attention in Western Europe.

I.4.3.7. Industrial facility accident

A fixed industrial facility presents several types of potential hazards to a nearby nuclear power plant, including fire (and resulting smoke and combustion gases), explosion (with attendant pressure wave, ground shock, and missiles), and release of toxic or flammable vapours.

The principal hazards posed to a nuclear power plant from an off-site fire are the effects on control room habitability and emergency diesel generator air takes from smoke and combustion gases. The thermal effects of an off-site fire on plant structures would not generally be significant based on current design practice. The effects of fire on control room habitability would be similar to the effects of a postulated toxic gas release by a nearby industrial facility. Since these effects are considered individually in plant design, and since they are not additive with effects of other natural or human made phenomena, it is not normally necessary to consider smoke, combustion gas, and toxic gas in combination with other hazards. The blast wave and missile impact effects of an external explosion could combine to load the target structures. A review of the available literature shows that explosions of the magnitude required to cause significant blast effects at a nearby nuclear power plant are very infrequent.

Design for external explosion effects becomes necessary only when the potential pressure effects on the NPP structures, systems and components exceed the effects of a design basis wind taking due consideration that the wind load effect tends to be statically applied where the blast load dynamically applied.

Current practice in nuclear power plant siting avoids sites very near hazards such as munitions, hazardous chemicals, or petrochemical production or storage facilities. However, assuming one facility having potential for a significant accidental explosion is near a typical

plant site, a conservative estimate of the average annual probability of significant blast effects occurring at an industrial site is about 3.0×10^{-5} in typical industrialized states.

I.4.3.8. Pipeline accident

A pipeline, transporting materials which are in a liquid state under normal temperature and atmospheric pressure, will not cause any substantial hazard condition even if leakage occurs. However, accidents to pipelines transporting gases under pressure can lead to leaks of natural gas, propane, and other flammable, explosive or toxic gases which may have potentially unacceptable consequences to a nuclear plant. The applicable hazards are overpressure due to air blast, thermal load resulting from gas deflagration, missile hazard, and gas concentration within the plant. Most of the parameters involved in determining the effect of a pipeline accident are site related variables and evaluation should be made on a case by case basis. The evaluation involves quantity–distance relationships, site topography, site meteorology, including wind direction, wind speed, and atmospheric stability class.

For the purpose of estimating the upper bound probability of the pipeline accident, the following assumptions are typically made:

(a) Ignition, deflagration or detonation occur.
(b) Meteorology (wind direction, wind speed, and stability) are such that a gas cloud with the proper mixture to detonate is formed. (Very conservative assumption since the necessary meteorological conditions for such cloud formation are rare in most instances).
(c) About 1.5 kilometres of pipeline is assumed to rupture for application to a typical NPP site.

It should be understood that deflagration versus detonation occurring are usually a function of the concentration of the flammable substance in air including the potential for mixing or turbulence. The probability of a deflagration is in general considered higher than a detonation.

I.4.3.9. Retaining structure failure

Retaining structure (dam) failures can result in either abnormally high or low water levels, either of which may be a hazard to the plant.

When dam design, construction, maintenance, and inspection are performed according to acceptable modern standards and practices, the probability of failure should be very small in the absence of overtopping due to flood or landslide or extreme earthquake. Historical statistics show an average frequency of dam failure of one failure per 10 000 dam-years worldwide (for dams greater than 15 meters in height). Such a large probability reflects many instances of poor design, construction, maintenance, or intervening environmental hazard. A frequency of one retaining structure failure in 10 000 years is recommended for use to identify those hazard combinations which are sufficiently large to require consideration by the plant designer. It is up to the plant designer to further investigate the failure probabilities for dams and other water retaining structures in this area to determine whether lower hazard probabilities are justifiable.

In performing these studies, it is recommended that the designer investigate three categories of excessive failure risk: earth fill dams, dams with high seismic risk, and dams located on poor foundation material. If it can be demonstrated that the structure is in none of these three categories, and that it is subjected to regular inspection and maintenance according to accepted professional practice, then a probability of 10^{-6} per dam-year (100 times lower than that indicated by the historical data) is considered representative.

I.4.3.10. Accidental surface vehicle explosion

Surface vehicle explosions (truck, train, barge in river or canal, or ocean ship) present a potential hazard to a nuclear power plant from the standpoint of both blast overpressure and explosion generated missiles.

To determine whether a surface vehicle explosion is likely enough to be considered to occur simultaneously with any other human induced or natural hazard, the probability of occurrence and the duration of the effects should be estimated.

The probability of a surface vehicle explosion can be calculated by

$$P = P_a \times P_e \times L \times f$$

where:

P = probability per year of surface vehicle explosion which may be a hazard to the plant site (a^{-1}).

P_a = probability of surface vehicle accident per mile travelled (mi^{-1}).

P_e = conditional probability of surface vehicle explosion, given the accident has taken place.

L = length of path within which explosion of shipment can be a hazard to the plant site (mi.).

f = frequency of shipment (a^{-1}).

In IAEA some Member States surface vehicle explosion including highway, train and ship or river barge are defined as design bases independent of probabilities. In such instances an investigation of stand off distance is made to determine if the postulated blast warrants being considered as a design basis for the plant.

I.4.4. DESIGN BASIS ACCIDENTS

Also considered in the extreme load design category are design basis accident, DBA loads. Such loads are associated with postulated failure of structures, systems and components, SSC in close proximity to the reactor coolant system or are safety related with respect to the ability to cool and shutdown the reactor and maintain it in a safe shutdown condition. DBAs are also applicable to spent fuel and high level radwaste processing and storage systems.

Four types of design basis accidents are typically associated with the nuclear reactor, spent fuel and radwaste systems. First is the non-mechanistic potential loss of coolant failure

of reactor coolant system such that all of the coolant is released into the containment or confinement space. The second is a single break and resulting effects of any high energy line (P_o > 1.5 MPa or temperature > 120°C) in the plant unless it can be demonstrated that a leak before break would occur as a function of the service conditions and material of the pipe in which case criteria associated with a moderate energy pipe break would be used. A moderate energy pipeline is any line carrying liquids with pressure and temperature less than those used to define a high energy break where resultant sprays and flooding should be evaluated. The third design basis accident would be associated with postulated drop of a heavy load unless the lifting device is designed to be failure proof. The fourth DBA would be the failure of any single active component (move or change states) to perform its required safety function. These four types of DBA also apply to the spent fuel and high level waste storage and processing facilities. However, the performance or design categories to resist these postulated phenomena are typically less stringent than for the nuclear reactor (i.e. PC-3 or PC-4 instead of PC-5).

I.5. DAMAGE STATES

In general, facility designs consider 4 damage states which dictate the acceptance criteria used in applicable design codes and standards. The following are the damage states considered in nuclear facility design.

- Damage State A: Large permanent distortion of structures, systems and components. Probability of failure (rupture or collapse) equal or greater than 10^{-1}. Generally beyond code defined acceptance criteria. Any evaluation in this damage state should consider non-linear response.
- Damage State B: Moderate permanent distortion of structures, systems and components. Probability of failure between 10^{-2} to 10^{-1}. Defined as Service Level D for ASME [I.2] Systems, Components and Abnormal or Extreme for ACI [I.3] and AISC [I.4] designed structures.
- Damage State C: Limited permanent distortion of structures, systems and components. Probability of failure between 10^{-2} to 10^{-3}. Defined as Service Level C for ASME Systems and Components.
- Damage State D: Essentially elastically behaviour. Probability of failure between 10^{-3} and 10^{-4} for acceptance criteria between 0.8 to 1.2 f_y. Probability of failure between 10^{-4} and 10^{-5} for acceptance criteria equal to or less than 0.8 f_y. Defined as Service Levels B and A for ASME systems and components and normal and severe for ACI and AISC structures.

REFERENCES

[I-1] Benjamin, J.R., Shinozuka, M., Shah, H.C., "Acceptable Risk in Reactor Studies," Paper Jl/l, Transactions of the 3rd International Conference on Structural Mechanics in Reactor Technology, London, September 1975.

[I.2] ASME Boiler and Pressure Vessel Code, Section III, Div. 1, Appendix F, "Rules for Evaluation of Service Loadings with Level D Service Limits," American Society of Mechanical Engineers, 1998.

[I.3] ACI-349, "Code Requirements for Nuclear Safety Related Concrete Structures," American Concrete Institute, 1999.

[I.4] AISC N-690, "Nuclear Facilities – Steel Safety Related Structures for Design Fabrication and Erection," American Institute of Steel Construction, 1996.

TABLE I.1. MEAN PROBABILITY OF EXCEEDANCE LIMITS TYPICALLY USED IN DESIGN OR PERFORMANCE CATEGORIZED NUCLEAR STRUCTURES, SYSTEMS AND COMPONENTS

	EXTERNAL								**INTERNAL**		
Performance Or Design Category[4]	**Earthquake[6]**	**Straight Wind[2]**	**Tornado**	**Precipitation[1]**	**Flood**	**Blast[5]**	**Aircraft Crash[5]**	**High Energy System Rupture**	**Design[7] Basis Accident 1**	**Design[7] Basis Accident 2**	**Design[7] Basis Accident N**
5	10^{-5}	1×10^{-6}	$1 \cdot 10^{-6}$	10^{-2}	$1 \cdot 10^{-6}$	$1 \cdot 10^{-6}$	$1 \cdot 10^{-6}$	$1 \cdot 10^{-6}$	As	As	As
4	10^{-4}	$2 \cdot 10^{-4}$	$2 \cdot 10^{-6}$	10^{-2}	$1 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	$1 \cdot 10^{-5}$	Per	Per	Per
3	$4 \cdot 10^{-4}$	$2 \cdot 10^{-3}$	$2 \cdot 10^{-5}$	10^{-2}	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	$1 \cdot 10^{-4}$	SAR	SAR	SAR
2	$1 \cdot 10^{-3}$	$1 \cdot 10^{-2}$	---	$2 \cdot 10^{-2}$	$1 \cdot 10^{-2}$	---	---	---			
1	$2 \cdot 10^{-3}$	$2 \cdot 10^{-2}$	---	$2 \cdot 10^{-2}$	$2 \cdot 10^{-2}$	—	—	—			
0	—	—	—	—	—	—	—	—			

Performance or design category:

5 Safety Related[1] Large Water Cooled Nuclear Power Plants > 1000 MW(t), LNG storage and processing > 200 cu. meters; Safety Significant Items[3]. In general there is no one to one correspondence between Performance or Design Category and Safety Related Classifications.

4 New spent fuel less than 3 years old requiring forced cooling and large quantities of volatile high level radioactive waste, storage or processing facility, Safety Related Items nuclear research or power reactors larger than 100 MW(t) Safety Items

3 Spent fuel dry storage not requiring forced cooling and Type B packaging solid and liquid nuclear waste and material storage, facility Safety Significant Items and research nuclear reactors larger than 1 MW(t) Safety Items[3]

2 Essential or normal hazardous facilities, police stations, hospitals, petrochemical plants, nuclear reactors equal to or less than 1 MW(t) and secondary support Safety Significant Items for DOE Hazard Category 2[3] — National Building Code Requirements

1 Ordinary residential, commercial or industrial facilities — National Building Code Requirements

0 Low cost structures with no permanent human occupancy – Local Building Code Requirements if any

Notes:

(1) Safety Related items are often divided into two classes, Safety and Safety Significant. The design requirements for Safety Significant items are usually one Performance Category less than Safety Class items in the same facility.

(2) Precipitation probability levels shown have often been used in nuclear facility design. It is recommended they be taken equal to flood probabilities of exceedance in future designs.

(3) In U.S. DOE facilities 10^{-4}/a and 10^{-3}/a respectively straight wind exceedance probability are used for PC-4 and PC-3 respectively. U.S. NRC licensed facilities would typically use 10^{-6}/a for PC-5 and 4 items.

(4) Safety Related item functions are serviced by primary and secondary support systems. A primary support system is one that needs to operate with 72 hours of the event and should be classified the same as the safety item it supports. A secondary support system needed after 72 hours can be one Performance Class less than the Safety related items it supports.

(5) In many IAEA Member States these loads in whole or part are defined deterministically.

(6) Median peak ground accelerations and spectral shapes and damping values should be defined for design purposes.

(7) Design Basis Accidents typically are defined as high energy rotating equipment rupture and heavy load drops within the

(8) nuclear facility. 1) high pressure piping system rupture ($P_D \geq$ or $T_D \geq$ moderate energy piping system ($P_D <$, $T_D <$) leakage resulting in flooding and spray.

TABLE I.2. INDIVIDUAL NATURAL AND HUMAN INDUCED EXTERNAL HAZARDS USUALLY EXCLUDED FROM CONSIDERATION AS A DESIGN BASIS FOR NUCLEAR POWER PLANTS

Hazards Natural	Elimination Criteria No.	Remarks
High Summer Temperature[5]	1	Ultimate heat sink conservatively designed for 30 days of evaporation.
Waterspout	4	Considered in conjunction with tornado. Tornado governs. Loading due to water in spout not governing.
Sandstorm	4	Extreme wind should include this phenomena. Blockage of air intakes with particulate matter should be considered separately.
Volcanic Activity	3, 4	Currently there is no criteria for anti-volcanic design.
Fog	2	Could, however, increase probability of human made hazard involving surface vehicles or aircraft.
Forest Fire	2	Site cleared for such fire. Control room habitability required for smoke.
Drought*	1	Assumes multiple source of ultimate heat sink or ultimate heat sink not affected by drought; e.g. cooling tower with adequately sized basin.
Lightning	2	Plant lightning protected by use of a grounding network.
Frost	2,5	Snow and ice govern.
Meteorite	3	Less than 10^{-7} per year depending on latitude.
Hail	2,5	Other missiles govern.
Coastal Erosion	1	See Note 1.
Flood	4	
Tsunami	4	
Retaining Structure Failure	4	

[5]These natural hazards provide some of the design basis for the ultimate heat sink.

TABLE I.2. INDIVIDUAL NATURAL AND HUMAN INDUCED EXTERNAL HAZARDS USUALLY EXCLUDED FROM CONSIDERATION AS A DESIGN BASIS FOR NUCLEAR POWER PLANTS (CONT'D)

Soil Shrink–Swell Consolidation	1	See Note 1.
Low Lake or River Water Level*	1	Ultimate heat sink should be conservatively designed for 30 days of evaporation.
Avalanche	4	
Landslide	4	
Hazards	Elimination Criteria No.	Remarks
Wave Action	4,5	Included under flood.
Seiche	4,5	Included under flood.
Precipitation	4,5	Included under flood.
Storm Surge	4,5	Included under flood.
Ice Cover	2,5	See remark under snow for roof loading. Ice effects on intake structures may require design consideration. Ice blockage of rivers causing flooding is included under river flooding.
Snow	2	When snow (or ice) load in excess of design live loads is considered in the design of power plant structures, the resulting load combination should be treated as an extreme environmental condition with unit load factors.
Aircraft Crash, Large Aircraft Crash, Small	3 5	If more than 10km from commercial airport flyway. Included in tornado design > 100 m/sec.
Surface Vehicle, Pipeline, and Military or Industrial Facility Accident (Explosion)	4	
Toxic and Flammable Gas	5	Control room habitability required for toxic gas accident. This assumes no operator action outside the control room is required to render the consequences of the event acceptable.

Note 1: Site related characteristics, such as subsidence due to subsurface pumping, mining, sink holes, or alteration of groundwater regions; active surface faulting, liquefaction potential, chemically active soils and rocks or volcanic activity which have expansive, heave, shrinkage characteristics, flood plane level are natural phenomena which should be considered and evaluated during the site suitability evaluation process. Such characteristics either result in (1) the site being considered unsuitable, or (2) necessary design consideration and construction techniques are employed to mitigate or present the hazard.

The following exclusion criteria have been used to eliminate postulated hazards from being included as a design basis:

(1) A phenomenon which occurs slowly or with adequate warning with respect to the time required to take appropriate protective action.
(2) A phenomenon which in itself has no significant impact on the operation of a nuclear power plant and its design basis.
(3) A phenomenon which by itself has a probability of occurrence less than the 10^{-7} per year upper limit of acceptable undefined failure probability and consequences.
(4) Locate the nuclear power plant sufficiently distant from the postulated phenomenon to mitigate its effects.
(5) A phenomenon which is included or enveloped by design for another phenomenon. For example, storm surge and seiche are included in lake flooding; toxic gas is included in pipeline accident or industrial or military facility accident.

Annex II

A PROPOSAL FOR A CONSISTENT FORMULATION OF LIMIT STATES AND ACCEPTANCE CRITERIA

A PROPOSAL FOR LIMIT STATES AND ACCEPTANCE CRITERIA IN RELATION TO EXTERNAL EVENTS*

Acceptance criteria for design level of external loads could be obtained from basic safety criteria for NPP. One of the most important safety criteria for NPP is the frequency of maximum accidental radioactive release.

According to the regulatory document [II.1] frequency of maximum accidental radioactive release should not exceed the value of:

$$[p_0] \le 10^{-7} \text{ 1/reactor /year.} \qquad \text{(II.1)}$$

Real value of frequency of maximum accidental radioactive release for some NPP may be represented as product of three probabilities:

$$p_0 = p_l \cdot p_d^l \cdot p_r^d \ , \qquad \text{(II.2)}$$

where p_l = probability of load of level l,

p_d^l = fragility (conditional probability of damage of type d at load level l),

p_r^d = conditional probability of maximum radioactive release at damage d.

In design of NPP external events appear as a source of loads and actions on it's components. So, probabilistic target for external events, which should be accepted in design of NPP, could be obtained from (2) if using for p_0 its limit value $[p_0]$:

$$p_l = \frac{[p_0]}{p_r^d \cdot p_d^l} \qquad \text{(II.3)}$$

Evaluation of fragility p_d^l could be made by approach of limit state method. In Russia this method is prescribed for civil engineering design. So it is used for containment and other safety related structures.

Using limit state approach it is reasonable to consider fragility as a probability of a state, when strength of material in a weak section of construction is exhausted. If we consider acting load as a given value, this probability will be defined only by randomness of strength of material.

As a rule normal distribution with mathematical expectation μ_R and standard deviation σ is used to describe random nature of strength of construction materials R (Fig. II.1).

---

* This annex has been prepared by S.S. Nefedov, E.G. Bougaev, I.V. Kaliberda, GAN, Russian Federation.

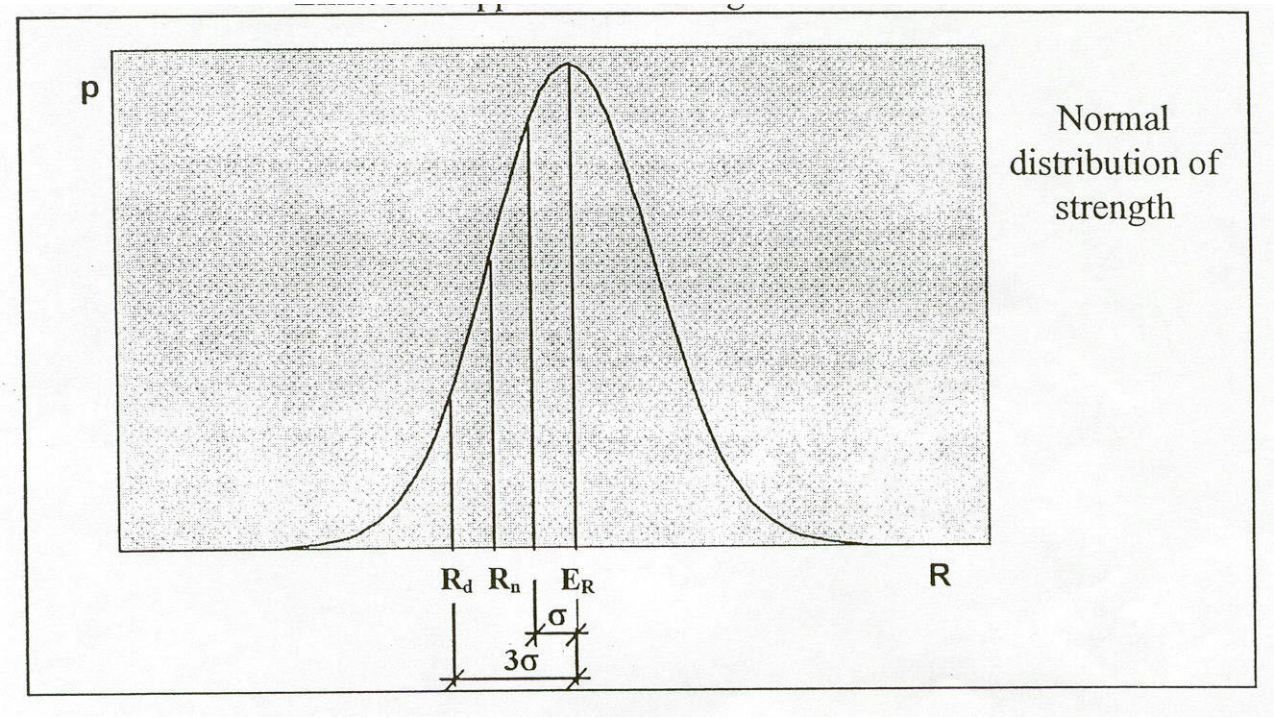

FIG. II.1. Normal distribution of strength.

In norms and standards based on limit state approach for strength parameter of material (yield stress, ultimate stress etc.) is assumed its characteristic value R_c, which is less then mathematical expectation μ_R of R by some number of standard deviations σ:

$$R_c = \mu_R - \alpha_c c \tag{II.4}$$

For concrete this number of standard deviations (see for example [II.2]) $\alpha_c = 1{,}64$. In accordance with the principles of limit state method (see standard [II.3]) in design should be used not the characteristic value of strength parameter R_c, but its design value R_d.

Design value R_d is connected with its characteristic value R_c, via the material safety factor γ_m:

$$R_d = \frac{R_c}{\gamma_m} \tag{II.5}$$

Value of γ_m for different materials is defined in corresponding codes and standards with considering of spread of testing results and other factors, connected with reliability. For normal concrete in accordance with civil engineering code [II.4] $\gamma_m = 1.3$.

So design value of strength parameter R_d is even less then its characteristic value R_c, and lies further from mathematical expectation μ_R on the R axis.

Position of R_d on the axis R may be defined using probabilistic approach analogously to (II.4):

$$R_d = \mu_R - \alpha_d c \qquad \text{(II.6)}$$

Here α_d denotes the number of standard deviations σ, which corresponds to the level of strength, assumed for design. Value of α_d may be defined by equating expressions (II.5) and (II.6). Using the above mentioned values of α_d and γ_m, one may obtain for concrete:

$$\alpha_d \approx 3{,}0\,. \qquad \text{(II.7)}$$

The same results could be obtained also for reinforcing steel and other construction materials. So the level of strength parameter, which is prescribed by limit state codes for design, is less then mathematical expectation of this parameter by approximately three standard deviation of its distribution. Using cumulative function of normal distribution one may conclude, that real strength of weak section of construction will be not less then design strength with the probability ~0,999.

So fragility, which is considered as a probability of a crash of section at given load may be defined as

$$p_d^l \approx 1 - 0{,}999 = 1 \cdot 10^{-3}\,. \qquad \text{(A-8)}$$

Using this result and condition (II.1) we may define probabilistic target for external loads from (II.3) as:

$$p_l \le \frac{10^{-4}}{p_r^d} \text{ 1/reactor/year.} \qquad \text{(II.9)}$$

Expression (II.9) may be considered as probabilistic criteria for loads, accepted in design. However, limit state method is based not on probabilistic but on statistical approach. It requires numerical criterion, which might be compared with results of treatment of load statistics. Such numerical criterion could be obtained from (II.9) by assuming some numerical value for conditional probability of maximum radioactive release at damage d p_r^d.

Numerical estimation of p_r^d is rather difficult and depends very much on essential features of each NPP. Therefore conservative approach is often used for setting of numerical value of p_l.

The maximal conservatism would be in the case, when

$$p_r^d = 1\,. \qquad \text{(II.10)}$$

In this case acceptance criterion for external loads becomes as follows:

$$p_l \le 10^{-4} \text{ 1/reactor/year.} \qquad \text{(II.11)}$$

This criterion is used in existing codes for nuclear engineering and design [II.5, II.6].

Existing analyses show, however, that value of p_r^d is much less then unity. INSAG-3 [II.7] for example even in the case of core damage recommends to assume $p_r^d \approx 1/10$. Taking

into account these reasons criterion (II.11) might be considered as too severe. Therefore more soft criteria could be adopted, which lie in interval:

$$p_l \le [10^{-4};10^{-3}] \text{ 1/reactor/year.} \quad \text{(II.12)}$$

Analogous approach is adopted in the last version of general civil engineering code [II.8], where for seismic loads on especially serious objects is prescribed frequency

$$p_l \le 2 \cdot 10^{-4} \text{ 1/reactor/year.} \quad \text{(II.13)}$$

REFERENCES

[II.1] PNAE G-1-011-97. General Principles of Safety for Nuclear Plants (OPB-88/97).Moscow, Gosatomnadzor, 1997 (in Russian).

[II.2] Civil Engineering Constructions. Ed. by Profs. A.M. Ovechkine, R.L. Mailyan. Moscow, Stroyizdat, 1976 (in Russian).

[II.3] GOST 27751-88. Reliability of the constructions and the foundations. Principal rules of the calculations (in Russian).

[II.4] SNiP 2.03.01-84*. Concrete and Reinforced Concrete Constructions (in Russian).

[II.5] PNAE G-05-35-95. Account of external actions of natural and human induced origin on nuclear and radiation dangerous objects (in Russian).

[II.6] PIN AE-5.6. Norms for civil engineering design of nuclear plants with reactors of different type (in Russian).

[II.7] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, INSAG-3: Basic Safety Principles for Nuclear Power Plants, IAEA, Vienna (1988).

[II.8] SNiP II-7-81*. Construction in seismic regions (in Russian).

Annex III
QUESTIONNAIRE DELIVERED TO THE MEMBER STATES (ADDENDUM)

(Supplement of information according to the TCM recommendations)
(Examples are provided for easy completion)

STATE:	
ORGANIZATION:	

1. External Events and related quantities to be considered in NPP site evaluation, design and safety assessment according to national rules and/or national engineering practice

External event	**Associated site exclusion criterion**	**Hazard screening criterion**	**Hazard definition (If probabilistic, indicate ref. mean probability. If deterministic, indicate probability from PSA)**			**Design basis parameter**	**Safety evaluation**	**Behaviour criteria for design and safety evaluation**
			Deterministic versus probabilistic	**Database characteristics**	**Scenarios and parameters**			
explosion	*None*	*source dist>SDV* *Probability of*	*det*	*analytical simulation*	*quantity of hazardous material, distance*	*pressure wave in time*	*none*	*safety level 'X' (stress<x*yield)*

		explosion< SPL						
earthquake	*Surface faulting*		*det.* *prob.* *prob.*	*historical data (min.200 years), seismotectonics, geology, etc.*	*minimum earthquake=0.1g* *SL-1, P=10E-4/year* *SL-2, P=10E-2/year*	*Response spectra for SL-1 and SL-2*	*RLE = 1.5 * SL-2*	*for design: safety level 'Y' (stress<y*yield)* *for safety evaluation: safety level 'Z' (stress<z*yield)*

2. Describe the relationship (if any) between hazard definition for External events and for Internal events generated as consequence of an external event

External event (initiator)	Internal events (consequence)	Combination rules in the design	Behaviour criteria
Earthquake	• *Pressurized system failure* • *Internal fire* • *Internal flood* • *Internal missiles* • *Falling objects*	*SL-2 is combined with LOCA*	*safety level 'X' (stress<x*yield)*

3. Please provide an explanation of the differences, if any, in the criteria for site evaluation and design of new plants (related to external events) and in the assessment of existing plants, concerning hazard evaluation, design basis, safety margin

CONTRIBUTORS TO DRAFTING AND REVIEW

Aelbrecht, D.	Electricité de France (EDF), France
Ahmad, M.	Pakistan Atomic Energy Commission, Pakistan
Augusti, G.	University 'La Sapienza', Rome, Italy
Bessemoulin, P.	Meteo-France, Toulouse, France
Contri, P.	International Atomic Energy Agency
Deltcheva, V.A.D.	Committee on the Use of Atomic Energy for Peaceful Purposes, Bulgaria
Donald, J.	Nuclear Installations Inspectorate (Health and Safety Executive), United Kingdom
Dundulis, G.	Lithuanian Energy Institute (LEI), Lithuania
Forner, S.	Nuclear Installation Safety Directorate (DSIN), France
Godoy, A.	Autoridad Regulatoria Nuclear, Argentina
Hyun, C.-H.	Korea Institute of Nuclear Safety (KINS), Republic of Korea
Johnson, J.J.	EQE International Inc., United States of America
Jungclaus, D.	Private consultant, Germany
Krytskyy, V.B.	Ministry of Ecology and Natural Resources of Ukraine, Ukraine
Liu, W.	Beijing Institute of Nuclear Engineering (CNNC), China
Momen Beitollahi, M.	Iranian Nuclear Regulatory Authority, Islamic Republic of Iran
Nefedov, S.S.	The Federal Nuclear and Radiation Safety Authority of Russia, Russian Federation
Petrescu, G.	National Commission for Nuclear Activities Control (CNCAN), Romania
Pristavec, M.	Slovenian Nuclear Safety Administration, Slovenia
Ramanujam, S.	Bhabha Atomic Research Centre (BARC), India
Razzaghi Khamsi, A.	Atomic Energy Organization of Iran (AEOI), Islamic Republic of Iran
Rebour, V.	Institut de Protection et de Sûreté Nucléaire (IPSN), France
Riera, J.D.	Laboratorio de Dinamica Estructural e Confiabilidade, Brazil
Soucek, V.	State Office for Nuclear Safety (SUJB), Czech Republic
Stevenson, J.D.	J.D. Stevenson Structural-Mechanical Consulting, United States of America
Sun, Z.	SEPA Nuclear Safety Centre, China
Tajbakhsh, S.	Atomic Energy Organization of Iran (AEOI), Islamic Republic of Iran

Technical Committee Meeting
Vienna, Austria: 4–8 December 2000