

IAEA SAFETY STANDARDS SERIES

External Events Excluding Earthquakes in the Design of Nuclear Power Plants

SAFETY GUIDE

No. NS-G-1.5



IAEA
International Atomic Energy Agency

AV Documents
Document Sharing Hub

IAEA SAFETY RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish standards of safety for protection against ionizing radiation and to provide for the application of these standards to peaceful nuclear activities.

The regulatory related publications by means of which the IAEA establishes safety standards and measures are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety, and also general safety (that is, of relevance in two or more of the four areas), and the categories within it are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Safety Fundamentals (blue lettering) present basic objectives, concepts and principles of safety and protection in the development and application of nuclear energy for peaceful purposes.

Safety Requirements (red lettering) establish the requirements that must be met to ensure safety. These requirements, which are expressed as 'shall' statements, are governed by the objectives and principles presented in the Safety Fundamentals.

Safety Guides (green lettering) recommend actions, conditions or procedures for meeting safety requirements. Recommendations in Safety Guides are expressed as 'should' statements, with the implication that it is necessary to take the measures recommended or equivalent alternative measures to comply with the requirements.

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA.

Information on the IAEA's safety standards programme (including editions in languages other than English) is available at the IAEA Internet site

www-ns.iaea.org/standards/

or on request to the Safety Co-ordination Section, IAEA, P.O. Box 100, A-1400 Vienna, Austria.

OTHER SAFETY RELATED PUBLICATIONS

Under the terms of Articles III and VIII.C of its Statute, the IAEA makes available and fosters the exchange of information relating to peaceful nuclear activities and serves as an intermediary among its Member States for this purpose.

Reports on safety and protection in nuclear activities are issued in other series, in particular the **IAEA Safety Reports Series**, as informational publications. Safety Reports may describe good practices and give practical examples and detailed methods that can be used to meet safety requirements. They do not establish requirements or make recommendations.

Other IAEA series that include safety related publications are the **Technical Reports Series**, the **Radiological Assessment Reports Series**, the **INSAG Series**, the **TECDOC Series**, the **Provisional Safety Standards Series**, the **Training Course Series**, the **IAEA Services Series** and the **Computer Manual Series**, and **Practical Radiation Safety Manuals** and **Practical Radiation Technical Manuals**. The IAEA also issues reports on radiological accidents and other special publications.

—

The following States are Members of the International Atomic Energy Agency:

AFGHANISTAN	GREECE	PARAGUAY
ALBANIA	GUATEMALA	PERU
ALGERIA	HAITI	PHILIPPINES
ANGOLA	HOLY SEE	POLAND
ARGENTINA	HONDURAS	PORTUGAL
ARMENIA	HUNGARY	QATAR
AUSTRALIA	ICELAND	REPUBLIC OF MOLDOVA
AUSTRIA	INDIA	ROMANIA
AZERBAIJAN	INDONESIA	RUSSIAN FEDERATION
BANGLADESH	IRAN, ISLAMIC REPUBLIC OF	SAUDI ARABIA
BELARUS	IRAQ	SENEGAL
BELGIUM	IRELAND	SERBIA AND MONTENEGRO
BENIN	ISRAEL	SEYCHELLES
BOLIVIA	ITALY	SIERRA LEONE
BOSNIA AND HERZEGOVINA	JAMAICA	SINGAPORE
BOTSWANA	JAPAN	SLOVAKIA
BRAZIL	JORDAN	SLOVENIA
BULGARIA	KAZAKHSTAN	SOUTH AFRICA
BURKINA FASO	KENYA	SPAIN
CAMEROON	KOREA, REPUBLIC OF	SRI LANKA
CANADA	KUWAIT	SUDAN
CENTRAL AFRICAN REPUBLIC	KYRGYZSTAN	SWEDEN
CHILE	LATVIA	SWITZERLAND
CHINA	LEBANON	SYRIAN ARAB REPUBLIC
COLOMBIA	LIBERIA	TAJIKISTAN
COSTA RICA	LIBYAN ARAB JAMAHIRIYA	THAILAND
CÔTE D'IVOIRE	LIECHTENSTEIN	THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA
CROATIA	LITHUANIA	TUNISIA
CUBA	LUXEMBOURG	TURKEY
CYPRUS	MADAGASCAR	UGANDA
CZECH REPUBLIC	MALAYSIA	UKRAINE
DEMOCRATIC REPUBLIC OF THE CONGO	MALI	UNITED ARAB EMIRATES
DENMARK	MALTA	UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
DOMINICAN REPUBLIC	MARSHALL ISLANDS	UNITED REPUBLIC OF TANZANIA
ECUADOR	MAURITIUS	UNITED STATES OF AMERICA
EGYPT	MEXICO	URUGUAY
EL SALVADOR	MONACO	UZBEKISTAN
ERITREA	MONGOLIA	VENEZUELA
ESTONIA	MOROCCO	VIETNAM
ETHIOPIA	MYANMAR	YEMEN
FINLAND	NAMIBIA	ZAMBIA
FRANCE	NETHERLANDS	ZIMBABWE
GABON	NEW ZEALAND	
GEORGIA	NICARAGUA	
GERMANY	NIGER	
GHANA	NIGERIA	
	NORWAY	
	PAKISTAN	
	PANAMA	

The Agency's Statute was approved on 23 October 1956 by the Conference on the Statute of the IAEA held at United Nations Headquarters, New York; it entered into force on 29 July 1957. The Headquarters of the Agency are situated in Vienna. Its principal objective is "to accelerate and enlarge the contribution of atomic energy to peace, health and prosperity throughout the world".

© IAEA, 2003

Permission to reproduce or translate the information contained in this publication may be obtained by writing to the International Atomic Energy Agency, Wagramer Strasse 5, P.O. Box 100, A-1400 Vienna, Austria.

Printed by the IAEA in Austria
November 2003
STI/PUB/1159

SAFETY STANDARDS SERIES No. NS-G-1.5

EXTERNAL EVENTS EXCLUDING EARTHQUAKES IN THE DESIGN OF NUCLEAR POWER PLANTS

SAFETY GUIDE

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2003

IAEA Library Cataloguing in Publication Data

External events excluding earthquakes in the design of nuclear power plants : safety guide. — Vienna : International Atomic Energy Agency, 2003.

p. ; 24 cm. — (Safety standards series, ISSN 1020-525X ; no. NS-G-1.5)

STI/PUB/1159

ISBN 92-0-101099-0

Includes bibliographical references.

1. Nuclear power plants—Design and construction. Nuclear power plants — Safety measures. I. International Atomic Energy Agency. II. Series.

IAEAL

03-00340

FOREWORD

by **Mohamed ElBaradei**
Director General

One of the statutory functions of the IAEA is to establish or adopt standards of safety for the protection of health, life and property in the development and application of nuclear energy for peaceful purposes, and to provide for the application of these standards to its own operations as well as to assisted operations and, at the request of the parties, to operations under any bilateral or multilateral arrangement, or, at the request of a State, to any of that State's activities in the field of nuclear energy.

The following bodies oversee the development of safety standards: the Commission on Safety Standards (CSS); the Nuclear Safety Standards Committee (NUSSC); the Radiation Safety Standards Committee (RASSC); the Transport Safety Standards Committee (TRANSSC); and the Waste Safety Standards Committee (WASSC). Member States are widely represented on these committees.

In order to ensure the broadest international consensus, safety standards are also submitted to all Member States for comment before approval by the IAEA Board of Governors (for Safety Fundamentals and Safety Requirements) or, on behalf of the Director General, by the Publications Committee (for Safety Guides).

The IAEA's safety standards are not legally binding on Member States but may be adopted by them, at their own discretion, for use in national regulations in respect of their own activities. The standards are binding on the IAEA in relation to its own operations and on States in relation to operations assisted by the IAEA. Any State wishing to enter into an agreement with the IAEA for its assistance in connection with the siting, design, construction, commissioning, operation or decommissioning of a nuclear facility or any other activities will be required to follow those parts of the safety standards that pertain to the activities to be covered by the agreement. However, it should be recalled that the final decisions and legal responsibilities in any licensing procedures rest with the States.

Although the safety standards establish an essential basis for safety, the incorporation of more detailed requirements, in accordance with national practice, may also be necessary. Moreover, there will generally be special aspects that need to be assessed on a case by case basis.

The physical protection of fissile and radioactive materials and of nuclear power plants as a whole is mentioned where appropriate but is not treated in detail; obligations of States in this respect should be addressed on the basis of the relevant instruments and publications developed under the auspices of the IAEA. Non-radiological aspects of industrial safety and environmental protection are also not explicitly considered; it is recognized that States should fulfil their international undertakings and obligations in relation to these.

The requirements and recommendations set forth in the IAEA safety standards might not be fully satisfied by some facilities built to earlier standards. Decisions on the way in which the safety standards are applied to such facilities will be taken by individual States.

The attention of States is drawn to the fact that the safety standards of the IAEA, while not legally binding, are developed with the aim of ensuring that the peaceful uses of nuclear energy and of radioactive materials are undertaken in a manner that enables States to meet their obligations under generally accepted principles of international law and rules such as those relating to environmental protection. According to one such general principle, the territory of a State must not be used in such a way as to cause damage in another State. States thus have an obligation of diligence and standard of care.

Civil nuclear activities conducted within the jurisdiction of States are, as any other activities, subject to obligations to which States may subscribe under international conventions, in addition to generally accepted principles of international law. States are expected to adopt within their national legal systems such legislation (including regulations) and other standards and measures as may be necessary to fulfil all of their international obligations effectively.

EDITORIAL NOTE

An appendix, when included, is considered to form an integral part of the standard and to have the same status as the main text. Annexes, footnotes and bibliographies, if included, are used to provide additional information or practical examples that might be helpful to the user.

The safety standards use the form 'shall' in making statements about requirements, responsibilities and obligations. Use of the form 'should' denotes recommendations of a desired option.

The English version of the text is the authoritative version.

CONTENTS

[illegible]

5.	EXTERNAL FIRE	46
	General discussion (5.1–5.8)	46
	Loading (5.9–5.10)	47
	Design methods (5.11–5.17)	48
	Means of protection (5.18–5.22)	49
6.	EXPLOSIONS	50
	General discussion (6.1–6.10)	50
	Loading (6.11–6.26)	52
	Design methods and protection measures (6.27–6.39)	56
7.	ASPHYXIAN AND TOXIC GASES	59
	General description (7.1–7.2)	59
	Dispersion (7.3)	60
	Design method (7.4–7.5)	60
	Means of protection (7.6–7.9)	61
8.	CORROSIVE AND RADIOACTIVE GASES AND LIQUIDS ..	62
	General discussion (8.1–8.3)	62
	Design methodology (8.4–8.6)	62
	Means of protection (8.7–8.11)	63
9.	ELECTROMAGNETIC INTERFERENCE	64
	General description (9.1–9.2)	64
	Design methods (9.3–9.4)	64
	Means of protection (9.5–9.7)	64
10.	FLOODS	65
	General description (10.1–10.7)	65
	Loading (10.8–10.15)	66
	Design methods and means of protection (10.16–10.18)	67
11.	EXTREME WINDS	68

General discussion (11.1–11.4)	68
Loading (11.5–11.8)	68
Design methods and means of protection (11.9–11.12)	69
12. EXTREME METEOROLOGICAL CONDITIONS	70
General description (12.1–12.5)	70
Loading (12.6)	71
Design methods and means of protection (12.7–12.12)	71
13. BIOLOGICAL PHENOMENA	72
General description (13.1–13.4)	72
Design methods and means of protection (13.5–13.12)	72
14. VOLCANISM	74
General description (14.1–14.3)	74
Loading and means of protection (14.4–14.8)	74
15. COLLISIONS OF FLOATING BODIES WITH WATER INTAKES AND UHS COMPONENTS	75
General description (15.1–15.3)	75
Loading (15.4–15.5)	76
Design methods (15.6–15.8)	76
Means of protection (15.9–15.12)	77
REFERENCES	79
ANNEX I: AIRCRAFT CRASHES	81
ANNEX II: DETONATION AND DEFLAGRATION	87
ANNEX III: TOXICITY LIMITS	99
CONTRIBUTORS TO DRAFTING AND REVIEW	101
BODIES FOR THE ENDORSEMENT OF SAFETY STANDARDS ..	103

1. INTRODUCTION

BACKGROUND

1.1. This Safety Guide was prepared under the IAEA programme for safety standards for nuclear power plants. It supplements the Safety Requirements publication on Safety of Nuclear Power Plants: Design [1].

1.2. The present Safety Guide is the second revision of a Safety Guide issued in 1982 on the design of nuclear power plants for external human induced events. The main changes are as follows:

- (1) Recommendations on design features relating to all external events¹, excluding earthquakes, have been incorporated into this publication, which makes reference to the Safety Guides on external human induced events, flood hazards and extreme meteorological events [2–4].
- (2) Recommendations on design for protection from the effects of external events, which previously appeared in Ref. [2] and earlier IAEA safety standards², have been included in this publication, with the exception of recommendations on site protection measures which are retained in the relevant Safety Guides on site evaluation.
- (3) The sections dealing with hazardous materials have been reorganized for consistency with Ref. [2]. Two groups of hazardous material are identified: asphyxiant and toxic gases, and corrosive and radioactive gases and liquids.

¹ An external event is an event that originates outside the site and whose effects on the nuclear power plant should be considered. Such events could be of natural or human induced origin and are identified and selected for design purposes during the site evaluation process. In some cases events originating on the site but outside the safety related buildings can be treated as external events if the characteristics of the generated loads are similar to those caused by off-site events.

² Design Basis Flood for Nuclear Power Plants on River Sites, Safety Series No. 50-SG-S10A (1983); Design Basis Flood for Nuclear Power Plants on Coastal Sites, Safety Series No. 50-SG-S10B (1983); Extreme Meteorological Events in Nuclear Power Plant Siting, Excluding Tropical Cyclones, Safety Series No. 50-SG-S11A (1981); Design Basis Tropical Cyclone for Nuclear Power Plants, Safety Series No. 50-SG-S11B (1984); Ultimate Heat Sink and Directly Associated Heat Transport Systems for Nuclear Power Plants, Safety Series No. 50-SG-D6 (1981).

- (4) Operating experience since 1986, as collected in the IAEA Incident Reporting System [5] and as expert experience, has been studied and discussed as guidance for improving the approach to design. A paragraph has been added in several sections with the main outcomes from this experience.
- (5) Section 2, concerning the general approach and the design philosophy for protection against external events, has been considerably expanded, with new information added on structures, systems and components (SSCs) to be protected against external events and on load combinations and acceptance criteria.
- (6) Individual sections have been prepared on aircraft crashes (with a strong emphasis on fuel effects), external fires, explosions, drifting gas clouds, releases of corrosive fluids, collisions with water intakes and all remaining external natural events. The discussion on each of these topics has been expanded and updated. Some material that appeared in the previous Safety Guides on these topics has been deleted.
- (7) The text has been reorganized.

1.3. This Safety Guide provides recommendations for both design basis external human induced events and design basis external natural events³, while the related Safety Guides [2–4] provide recommendations on site evaluation.

1.4. Other Safety Guides relating to the Safety Requirements publication on Safety of Nuclear Power Plants: Design [1] present a discussion on external events and in this sense are complementary to the present Safety Guide — fire effects are in general addressed also in Ref. [6], certain missiles⁴ (as secondary effects of explosions mainly internal to buildings) are treated in Ref. [7], while the effects of earthquakes, vibration and shaking of the ground are discussed in Ref. [8].

³ A design basis external natural event is an external natural event selected for deriving design bases.

⁴ A missile is a mass that has kinetic energy and has left its design location. The term missile is used to describe a moving object in general, but military missiles, whether explosive or not (e.g. bombs and rockets), are specifically excluded from consideration. In general, military projectiles have velocities higher than Mach 1, and are therefore usually beyond the range of applicability of the techniques described in this Safety Guide. However, for non-explosive military projectiles with characteristics lying within the quoted ranges of applicability, the techniques described may be used.

1.5. There are other Safety Guides that deal with the same external event scenarios but in the context of the design of specific plant systems: Ref. [9] deals with the entire reactor cooling system, Ref. [10] with the containment, Ref. [11] with the emergency power system and Ref. [12] with instrumentation and control systems.

OBJECTIVE

1.6. The purpose of this Safety Guide is to provide recommendations and guidance on design for the protection of nuclear power plants from the effects of external events (excluding earthquakes). External events are events that originate either off the site or within the boundaries of the site but from sources that are not directly involved in the operational states of the nuclear power plant units, such as fuel depots or areas for the storage of hazardous materials handled during the construction, operation and decommissioning of units located at the same site. Significant events, either as design basis external human induced events⁵ or design basis external natural events, should be identified and selected as design basis external events (DBEEs)⁶ in the preliminary phases of the site evaluation process, in accordance with Refs [2–4].

1.7. This Safety Guide is intended to provide recommendations on engineering related matters in order to comply with the safety objectives and requirements established in Sections 2 and 3 of the Safety Requirements publication on Safety of Nuclear Power Plants: Design [1].

1.8. This Safety Guide aims to provide the reader with a generally accepted way of defining an appropriate design basis for a nuclear power plant from the site hazard evaluation carried out in the site evaluation phase and according to the specific layout of the plant. Recommendations for methods and procedures

⁵ A design basis external human induced event is an external human induced event selected for deriving design bases.

⁶ A design basis external event is an external event or a combination of external events selected for the design of all or any part of a nuclear power plant, characterized by or having associated with it certain parameter values. Design basis external events should be independent of the plant layout. An engineering analysis may be necessary to develop the loading scheme to be applied to the specific numerical or experimental models selected for the design.

to perform the plant design so as to minimize the probability that the selected DBEEs at the site could jeopardize the safety of the plant are also provided.

SCOPE

1.9. This Safety Guide is applicable to the design and safety assessment of items important to the safety of land based stationary nuclear power plants with water cooled reactors. It covers the safety of new nuclear power plants in relation to the following DBEEs:

Human induced events

- Aircraft crashes;
- Explosions (deflagrations and detonations) with or without fire, with or without secondary missiles, originating from off-site and on-site sources (but external to safety related buildings), such as hazardous or pressurized materials in storage, transformers, pressure vessels or high energy rotating equipment;
- Release of hazardous gases (asphyxiant, toxic) from off-site and on-site storage;
- Release of radioactive material from off-site sources;
- Release of corrosive gases and liquids from off-site and on-site storage;
- Fire generated from off-site sources (mainly for its potential for generating smoke and toxic gases);
- Collision of ships or floating debris with accessible safety related structures, such as water intakes and ultimate heat sink (UHS) components;
- Collision of vehicles at the site with SSCs;
- Electromagnetic interference from off the site (e.g. from communication centres and portable phone antennas) and on the site (e.g. from the activation of high voltage electric switch gear and from unshielded cables);
- Any combination of the above as a result of a common initiating event (such as an explosion with fire and release of hazardous gases and smoke).

Natural events

- Extreme meteorological conditions (of temperature, snow, hail, frost, subsurface freezing and drought);
- Floods (due to tides, tsunamis, seiches, storm surges, precipitation, waterspouts, dam forming and dam failures, snow melt, landslides into water bodies, channel changes and work in the channel);

- Cyclones (hurricanes, tornadoes and tropical typhoons) and straight winds;
- Abrasive dust and sand storms;
- Lightning;
- Volcanism;
- Biological phenomena;
- Collision of floating debris (ice, logs, etc.) with accessible safety related structures such as water intakes and UHS components.

1.10. This list is not exhaustive and other external events, not included in the list, may be identified and selected as DBEEs at the site. All such events should be evaluated in accordance with specific requirements, consistent with the safety requirements established in respect of them by the State concerned.

1.11. The completeness of the definition of hazards due to DBEEs may be affected by possible changes that have occurred in both the industrial environment and the transport environment since the siting process was followed, and also in natural hazards (e.g. because of climate changes), as foreseen in the Safety Requirements for Design [1]. Such changes are mainly considered in periodic safety reviews [13].

1.12. The coverage provided in this Safety Guide for the different scenarios is variable: most emphasis is given to explosions, floods and aircraft crashes. However, this is consistent with the consequences for plant safety expected in the different scenarios and also with the engineering efforts generally expended to protect the plant or to mitigate the consequences of such events.

1.13. Particularly in the case of natural events, some scenarios are treated as exclusion criteria for the site itself (e.g. local volcanism and local active fault) and so they are not discussed here [14]. Other scenarios are dealt with preferably through site protection features (e.g. the ‘dry site’ concept, site drainage, protecting dams and levees) rather than by plant design measures and therefore they are discussed in the relevant publication on site evaluation.

1.14. Throughout this publication the term ‘external events’ always excludes earthquakes and ground shaking scenarios, which are discussed in Ref. [8].

1.15. External human induced events are defined as of accidental origin. Considerations relating to the physical protection of the plant from wilful actions by third parties are outside the scope of this Safety Guide. However, the

methods described herein may also have certain application to problems of physical protection for such scenarios.

1.16. This Safety Guide might be applied also to reactor types other than water cooled reactors at stationary nuclear power plants. However, engineering judgement should be used to assess such applicability, in compliance with the specific safety objectives defined for any plant type.

1.17. This Safety Guide provides recommendations and guidance for design procedures suggesting levels of accuracy consistent with current practice in the design of nuclear power plants, dealing primarily with the application of deterministic methods in design and assessment. Recommendations for the application of probabilistic methods in design and assessment phases are not included here (see Ref. [15]). Moreover, the proposed design method represents a limited number of the many engineering approaches that can be used: other procedures could be applied according to individual circumstances, specific plant layout and safety requirements.

1.18. This Safety Guide is mainly concerned with the design phase, but most of the recommendations could be applied in the safety assessment phase of new installations (described in Ref. [16]), in the periodic safety review phase (described in Ref. [13]) and in the re-evaluation of existing plants by means of extensive use of engineering judgement and in compliance with the relevant regulatory requirements for the specific phase.

STRUCTURE

1.19. The general approach to safety and the design philosophy are presented in Section 2, together with the concepts needed to develop the list of safety related items to be protected. The derivation of the design parameters from the site hazard analysis and the design basis is discussed in Section 3, along with the suitable load combinations and acceptance criteria under these together. Some specific events are treated individually in Sections 4–15. Examples of the design basis for aircraft crashes, solid explosions and gas cloud explosions, and toxicity limits in different States are presented in the annexes. Owing to a lack of general consensus on such issues among States, only examples from practice can be provided. These examples, together with due consideration of the general safety criteria, may help in the selection of the most suitable approach for any specific State.

APPLICABLE DESIGN REQUIREMENTS

“To ensure that the overall safety concept of defence in depth is maintained, the design shall be such as to prevent as far as practicable:

- “All levels of defence shall be available at all times, although some relaxations may be specified for the various operational modes other than power operation.”

“The number of physical barriers that will be necessary will depend on the potential internal and external hazards, and the potential consequences of failures.”

2.2. In order to meet the safety requirements for protection against the external events selected in the site evaluation phase, a classification of the plant items is useful to provide a rational basis for design. In addition to the safety classification, an external event (EE) classification of items may be developed so as to identify the system requirements in a DBEE (for design and maintenance), to estimate the consequences of their failure and to develop

focused post-event operator actions.⁷ The EE classification can also be used within the modification process to ensure that modifications are suitably classified and do not erode the design basis.

2.3. The external event classification, if applied, does not imply different load levels for the external event scenarios and therefore the design of items classified for external events should refer only to the extreme values of DBEEs (as identified in Refs [2–4]), or to a combination of DBEEs where at least one of them is taken at, or close to, its extreme value.⁸ However, lower load intensities could be used in the design for two main reasons:

- for *operational reasons*, in order to identify an operational level for the plant, with associated requirements for shutdown, inspection and emergency procedures in case the load intensities exceed the threshold;
- for *load combinations* with other design basis events, as a consequence of a probabilistic evaluation of the frequency of occurrence of some load combinations (e.g. including frequent wind, normal temperature and normal precipitation).

2.4. When different levels of the same external events are considered in the same load combination, the acceptance criteria of the items classified for external events should refer to the DBEE which in the combination is assumed to be at its extreme value.

2.5. In some cases probabilistic considerations on the probability of the load combination and its associated risk can justify less stringent acceptance criteria

⁷ The EE classification is the process that associates an external event category to any plant item, in addition to other classifications (e.g. for purposes of safety, seismic evaluation, quality assurance (QA) and maintenance), according to its required performance during and after a DBEE. The relevant acceptance criterion associated with the item is part of the classification. The EE classification is a general concept to be applied to all EEs affecting the plant, including earthquakes. A discussion on earthquakes is presented in the Safety Guide on seismic design [8], together with examples and procedures, but fully consistent with the general concepts defined here.

⁸ Some States adopt two levels of classification/load resistance depending upon a deterministic frequent/infrequent categorization: infrequent faults ($<10^{-3}$ per year) require one line of protection, whereas frequent faults ($>10^{-3}$ per year) require two lines of protection.

during short duration DBEEs, provided that the item is not in the safety group for the events in the combination and that post-event inspections are developed to assess the compliance with the reference acceptance criteria (as specified in its classification) after the event (Ref. [1], paras 4.3, 5.7).

2.6. The external event classification should be developed in addition to and to be consistent with the general safety classification of the plant, which identifies those SSCs important to safety (Ref. [1], paras 5.1–5.3). The safety classification covers the following items:

- Items whose failure could directly or indirectly constitute a postulated initiating event (e.g. items protecting the plant from external events are included here);
- Items required for shutting down the reactor, monitoring critical parameters, maintaining the reactor in a shutdown condition and removing residual heat over a required period;
- Items required for preventing radioactive releases or for maintaining releases below limits established by the regulatory body for accident conditions (e.g. all the defence in depth levels and barriers).

2.7. All items assigned to a safety class and possibly other items should be considered in the EE classification, such as:

- the items ‘not important to safety’ which in a DBEE can affect the functionality of a safety classified item (‘interacting items’);
- the items not included in (2) and (3) above that are required for preventing or mitigating plant accident conditions for such a long period that there is a reasonable likelihood that a DBEE may occur during that period.

The EE classification can exclude items not affected by any DBEE (e.g. items located at an elevation higher than the flood level and not affected by any other DBEE).

2.8. The EE classification should be based on a clear understanding of the safety functions required of the items during and after a DBEE or a design basis accident (including the severe accidents if included in the load combinations) not caused by a DBEE. Parts of a system, according to their different functions, may belong to different categories.

2.9. SSCs identified as defined above may be divided into two or more

external event categories in terms of their impact on plant safety in the event of failure caused by a DBEE. A recommended classification for external events, to be reflected in different design requirements, is as follows:

- *External event category 1 (EE-C1)*: Items whose functioning should be maintained in the event of the DBEE and items required for preventing or mitigating plant accident conditions for such a long period that there is a reasonable likelihood that a DBEE may occur during that period (i.e. items ‘important to safety’). These items should be designed in accordance with acceptance criteria corresponding to the safety functions required during and after a DBEE;
- *External event category 2 (EE-C2)*: Items whose loss of functionality may be permitted but should not impair the functionality of EE-C1 items in the event of a DBEE. These items should have acceptance criteria related to their potential interaction with EE-C1 items;
- *External event category 3 (EE-C3)*: Items that are parts of systems that may generate events with radiological consequences different from those generated by the reactor (e.g. spent fuel building and radioactive waste building). These items should have load combination coefficients and acceptance criteria related to their specific potential for radiological accidents, which should be less than those for the reactor;
- *External event, non-classified (EE-NC)*: All other items.

2.10. Within each EE classification category a range of acceptance criteria (according to the required function) and a range of safety margins together with specific construction, operation, inspection and maintenance procedures should be applied to the items depending on their importance or vulnerability in the event of a DBEE.

2.11. Nuclear power plant items of EE-C1 should be designed, installed and maintained in accordance with engineering practice for nuclear applications, for which appropriate safety margins should be established according to the associated consequences. For any item in Category 1, an appropriate acceptance criterion should be established (e.g. functionality, leaktightness and maximum distortion) according to the required safety function.

2.12. Since integrity is required for EE-C2 items and only limited (or, in some cases, no) functionality is required to prevent their interaction with Category 1 items, more simplified and less conservative criteria for design, installation and maintenance may be used, in some cases with a lower intrinsic safety margin than for EE-C1 items, in relation to their probability of being the initiator of an

accident. Often, experience based walkdowns are implemented in response to this concern (see Section 3).

2.13. EE-C3 items should be designed, installed and maintained in accordance with engineering practice for nuclear applications. If their acceptance criteria can be explicitly connected with the specific associated radiological consequences (assumed different from the reactor induced consequences), such criteria could be different from (and in general less conservative than) those defined for EE-C1.

2.14. Nuclear power plant EE-NC items should be designed as a minimum in accordance with engineering practice for non-nuclear applications. For some items of this category of paramount importance for the operation of the plant, it may be reasonable to choose more stringent acceptance criteria, on the basis of operational targets. Such an approach would minimize the need for plant shutdown, inspection and relicensing, thus allowing the plant to continue to operate after a DBEE.

2.15. Typical systems that should be classified as EE-C1 are:

- The reactor system containment structure (including foundations) or the external shielding structure, if any, to the extent necessary to preclude significant loss of leaktightness;
- The structures supporting, housing or protecting items important to safety, to the extent necessary to ensure their functionality;
- Structures protecting the plant from external events;
- The power and instrumentation and control (I&C) cables relevant to safety related items;
- The control room or the supplementary control points, including all equipment necessary to maintain the control room or supplementary control points within safe habitability limits for personnel and safe environmental limits for equipment protected against DBEEs;
- Systems or portions of systems that are required for monitoring, actuating and operating those parts of systems protected against DBEEs;
- The emergency power supplies and their auxiliary systems necessary for the active safety functions;
- The post-accident monitoring system.

2.16. Typical systems that should be classified as EE-C2 are:

- Those parts of SSCs whose continued functionality is not required but whose failure could reduce the functional capability of any plant features

specified above (EE-C1) to an unacceptable safety level or could result in incapacitating injury to occupants of the control room who are necessary to perform a safety function.

2.17. Typical systems that should be classified as EE-C3 are:

- SSCs for spent fuel confinement;
- Spent fuel cooling systems;
- Systems for the containment of highly radioactive waste in gaseous, vapour, liquid and/or solid form.

GUIDELINES FOR SAFETY ANALYSIS FOR DBEEs

2.18. An external event includes any credible consequential effects of that event [2–4]. External events are expected to challenge plant safety by different means, for example: the deterioration of structural capacities, the impairment of equipment operation, the impairment of operator action, the unavailability of the heat sink, and the unavailability of off-site power sources and emergency resources.

2.19. Having selected the external events to be considered for a particular site, the designer should evaluate their effects on the plant, including all credible secondary effects, following the single failure criterion and its limitations as explained in Ref. [1], para. 5.39. To this end, a safety analysis should be carried out, using continuous feedback to optimize the design of the protective measures, as explained in Ref. [16]. Care should be taken in the evaluation of effects on the plant to ensure that realistic and credible scenarios are developed — a single enveloping scenario may be unduly conservative.

2.20. The possibility of common cause failures should also be taken into account.⁹ The single failure criterion is only capable of dealing with random

⁹ In some States the probability of occurrence of certain human induced events, such as external explosions or aircraft crashes, is considered very low, and the passive components are usually assumed to be designed, manufactured, inspected and maintained to an extremely high quality. Therefore, the single failure non-compliance clause (para. 5.39) of Ref. [1] can be applied to the passive components. In some States system outage due to repair, test or maintenance with its associated change in plant configuration is considered one possible mode of a single failure in this context. Other States include the single failure criterion for all DBEEs.

failures and therefore the redundancy, which is the ultimate outcome of such an analysis, may be defeated by common cause failures [17], typically associated with external events that are expected to have adverse effects over relatively large plant areas.

2.21. A DBEE should not be considered in combination with events that may occur independently, such as other external human induced events, natural phenomena, equipment failures and operator errors, unless a combination of these events is shown to have a sufficiently high probability of occurrence. In this assessment, the possibility of a causal relationship should be evaluated, according to Ref. [16].

2.22. A loss of off-site power should be assumed coincident with any extreme DBEE if a direct or indirect causal relationship cannot be excluded. Particularly, for DBEEs that are expected to affect the entire site and, therefore, to give rise to a potential for a common cause failure mode, a loss of off-site power should be combined with the DBEE. For other events, a loss of off-site power should be assumed if the location of the transmission lines or the switchyard is such that the direct effects on them of the DBEE could cause a loss of off-site power. For external events such as ship collisions and internal events such as fire or anticipated operational occurrences, a coincident loss of off-site power should be assumed if the event could be expected to result in an unplanned turbine trip or reactor trip that would increase the potential for grid instability.

2.23. When justified, in the design for protecting against DBEEs that produce primary and secondary effects, the time delay between such effects should be taken into consideration in specifying how the primary and secondary effects are to be combined.

2.24. Phenomena that are expected to show a slow development may receive a lower level of consideration in the safety analysis, provided that it can be demonstrated that corrective actions could be taken before there were serious consequences for plant safety.¹⁰

¹⁰ This is the case, for example, for the design of UHS structures, and particularly of transfer channels, against soil settlement, landslides, subsidence or uplift due to changes in subsurface groundwater, and changes in oil or gas deposits due to natural events or human induced events such as pumping operations.

2.25. Consideration should be given in the safety analysis to the possible duration of extreme events, particularly for extreme weather conditions. Thus if the extreme conditions postulated for the site could endure for a considerable period, the feasibility of providing any backup measure from off the site should be evaluated, in view of the damage that is likely to occur and the probable conditions for the emergency services. Therefore, realistic assessments should be made of the ability to respond off the site under extreme conditions in the site region, when other demands for emergency services may be paramount. Either an adequate capacity should be provided for such circumstances or such backup measures should be excluded from the safety analysis.

2.26. In general, for corrective actions involving the support of off-site facilities, credit for unplanned corrective actions should be based on the analysis of the specific DBEE and particular site conditions, and should include adequate margin for uncertainties. As a minimum, for any event or site, no credit for such action should be taken for at least 48 hours following the onset of the event.

2.27. In particular for the UHS, the need for make-up of heat transport fluids should also be examined. Where a limited quantity of heat transport fluids is stored on site, the capability for make-up should be ensured by either (a) providing an adequate quantity of such fluids to allow time to repair the damaged part of the make-up system, or (b) protecting the make-up system from an external event. In case the make-up facilities cannot be fully protected, they should at least be dispersed or protected in such a way that a minimum capacity remains immediately available after any external event.

2.28. In the design, no credit for operator action should be assumed for any actions that should be taken immediately following the onset of a DBEE: difficulties in operator access at the site, long distances and difficulties in communication at the site may obstruct or prevent a clear diagnosis and local mitigation. No credit for operator actions should be given for the correction of equipment failures or the repair of damage as a consequence of a DBEE, unless there is a clear demonstration that such an action can be reliably accomplished within a time-frame consistent with the complexity and difficulty of the required action. A considerable margin should be applied to account for uncertainties, time needed to diagnose the extent of failure and to develop or modify corrective procedures, and the possible unavailability of appropriate personnel or replacement parts.

2.29. External events may challenge defence in depth at many levels. The basic plant protection should be addressed in the first level of defence either by

means of an adequate design of all the physical barriers or by component qualification. However, all the levels should be designed against external events to guarantee that in the event of an internal design basis accident all levels of defence are in place (Ref. [1], para. 4.4). 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.

2.30. Some external events included in the design basis may be associated with very low probability and catastrophic scenarios: examples include impacts of large aircraft, devastating explosions in the vicinity of the plant 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 a 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 of extreme external events has gross uncertainties associated with it, as discussed in Refs [2–4] for the hazards, but is not explicitly considered in a deterministic design;
- There is an intrinsic lack of operating experience relating to the effects that such extreme events could have on plant safety, owing 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 unfeasible¹¹ and a challenge to one level of defence in depth may be envisaged.

2.31. In these cases some special engineering approaches may be adopted, including all or a selection of the following measures:

- The selection of EE-C1 systems required for the protection of the plant against such events may be less stringent than for other DBEEs, including only a subset of safety classified items, usually only the items in the safety group of the extreme events;

¹¹ This is the case, for example, for a containment building subjected to the crash of a large aircraft: its leaktightness is usually not required.

- 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 DBEEs may be specified for items pertaining to the third or 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.

2.32. 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, supported by adequate warning systems (where possible) and monitoring (see the following subsections). Moreover, a dedicated probabilistic evaluation should be made of the consequences of these special assumptions.

DESIGN SAFETY FEATURES FOR DBEEs

2.33. To perform the safety functions required for DBEEs the designer should 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 show due regard for the single failure criterion; this may be achieved by means of the redundancy of safety systems.

2.34. There are two basic forms of plant protection against external events:

- (1) either the causal influences of an external event are reduced by means of a ‘passive barrier’ (e.g. ‘dry site’ for flood, site protection dam for flood, external shield for aircraft crash, barriers for explosions and building base isolation for earthquake),
- (2) or the ability of the safety systems to resist the effects of EEs is assessed by means of adequate item qualification (including redundancy, diversity or segregation).

2.35. The solution should represent the best balance among safety aspects, operational aspects and other important factors. For example, an inherent capability to withstand localized events (e.g. aircraft crash) can be provided by the 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 is necessary to provide additional protection in the form of barriers or to increase the spatial separation by modification of the plant layout.

2.36. Recommendations for the application of redundancy, diversity and segregation are made in Refs [1, 17]. In particular, special provisions against common cause failure should be made for large and extensive systems, namely the systems used to transport heat to the UHS, pump houses, cooling towers or long piping systems with large ring main systems.¹² A combination of the following protection strategies should be implemented.

- An adequate redundancy of safety related items. The level of redundancy should be an outcome of the application of the single failure approach to the design. Exceptions to the single failure approach may be accepted on a case by case basis where the DBEE has a very low probability and the systems are passive (Ref. [1], para. 5.39).
- Extensive spatial separation between redundant components. This measure should prevent both common cause failures from localized external events (e.g. missile impact) and interactions in the event of failure of one system that could be a source of internal accidents. A detailed analysis of the areas of influence or expected damage from the DBEE should be carried out for the purpose of application of the physical separation.
- Diversity in the redundant components. In the case of external event scenarios with a potential for common cause failures, the benefits of diversity should be evaluated with care. Diversity should be combined with separation when possible.

2.37. To provide additional defence in depth to the basic forms of protection defined above, for some external events proactive, active or administrative measures based on forewarning can also provide safety benefits. Examples of such measures include the reduction of fire loading materials adjacent to or on the nuclear site, the installation of additional barriers (damboards) or the closure of watertight gates in anticipation of flooding, and the inspection of drainage channels. While these measures are not normally as reliable as passive engineered systems, they nevertheless can provide additional safety benefits. The reliability ascribed to such measures should be commensurate with the reliability of the monitoring and forecasting equipment and operator reliabilities.

¹² A ring main system is a piping system that interconnects systems used to transport heat to the UHS.

2.38. The effectiveness of administrative measures is strongly dependent on their enforcement level, particularly when different administrations are involved. Their reliability should therefore be evaluated with care.

2.39. The following aspects should also be considered in a design for safety:

- Following the occurrence of a DBEE the design should ensure accessibility to the main control room, to supplementary control points and to the points, rooms and facilities necessary for meeting the requirements;
- The design should ensure that during the occurrence of a DBEE the plant status does not deteriorate to the extent that it cannot be controlled by the safety measures;
- The systems not protected against DBEEs (i.e. EE-NC items) should be assumed to be ‘operable’ or ‘non-operable’, depending on which status provides the more conservative scenario in the design of protection measures against the DBEE.

2.40. Provisions in the design to protect the plant against DBEEs should not impair its response in the other design basis events. In designing for additional protection, it should be borne in mind that barriers can introduce difficulties for inspection and maintenance, while a greater spread in plant layout may require more staff to handle the increased task of surveillance, as well as longer routing of piping, cable trays and ventilation ducts.

2.41. In the plant design for protection against EEs, adequate robustness should be used to provide the plant with some additional capacity for beyond design basis values for conditions in the selected external event scenarios. In general, this capacity should be provided by a combination of the following: high quality design, low sensitivity to variation in design parameters, and high and demonstrable conservatism in material selection, construction standards and QA. An evaluation of the design conservatism should be carried out either with probabilistic tools or by simplified deterministic bounding analysis.

2.42. Moreover, a special evaluation should be carried out so as to avoid potential small deviations in plant parameters from giving rise to severely abnormal plant behaviour (‘cliff edge effects’) in relation to the specific nature of the external event scenario (e.g. in the case of a site protection dam, if as soon as the dam is overtopped with a small additional steady state water level, the site could be suddenly flooded to the maximum level of the flood). In this case, additional engineering provisions should be implemented on safety systems at least for a safe shutdown mode, such as warning, monitoring and operating procedures.

INTERFACE WITH OPERATIONAL SAFETY FEATURES

2.43. Particular operating limits and conditions (OLCs) (Ref. [18], paras 5.8 and 6.9) should be defined for any external event 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 probabilistic safety assessment (PSA). The OLCs should be associated with dedicated surveillance procedures (pre- and/or post-event), a plant safe state (possibly a reactor shutdown) that is to be reached after such ‘abnormal’ events and a post-event revalidation procedure for any item important to safety that may have been challenged.

2.44. A set of operational limits should be defined for items classified for external events, derived from Ref. [19]:

- Safety limits (safe operating limits — SOLs): these are specified in the safety classification (and also in the EE classification) and represent the design basis conditions for the items. Their exceedance represents a challenge for plant safety and therefore a plant shutdown is required with precise post-event revalidation;
- Limits and conditions for normal operation (NOLs): these represent the limits for safe operation with due consideration of the uncertainties in the design process described above. They do not affect the design being intrinsically related to the uncertainty of the hazard for a 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 conditional on appropriate investigations of causes and effects.

2.45. NOLs should be identified in the hazard evaluation phase. Adequate procedures should be implemented for monitoring and for the prompt evaluation of their exceedance, to be specified in terms of all the parameters affecting the hazard definition. Actions arising from the exceedance of NOLs could include enhanced monitoring, administrative measures and review of forecasts.

2.46. If design provisions to protect the plant against the external events rely on passive barriers to reduce the effects of external events on the plant, NOLs should be referred to the barrier safety function and plant operation can be extended up to SOLs, on the assumption of a high degree of conservatism in the design of the barrier, provided that no cliff edge effects are foreseen for beyond design basis values. However, due account should be taken of the

uncertainties, of the reliabilities of monitoring and forecasting systems and of the margin between the time needed for shutdown and the time before the external event parameters exceed the barrier's capacity.

2.47. In any case, in relation to the development of an external event, plant shutdown should start if any of the following conditions is met [18]:

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

2.48. For most external events with sudden or unexpected effects, the parameters associated with the design basis cannot be monitored: examples would include aircraft impact parameters, blast pressures or impulse. In such cases a precautionary principle should apply and shutdown should be initiated after the event upon the basis of operator judgement.

2.49. To prevent unnecessary trips or demands on safety systems, for those external events whose parameters are continuous variables, such as water level or wind speed, consideration should be given to making routine measurements. The equipment and systems used to measure and report these parameters should have a reliability and accuracy commensurate with the safety claims made upon them.

3. DESIGN BASIS FOR EXTERNAL EVENTS

DERIVATION OF THE DESIGN BASIS FROM THE SITE HAZARD ANALYSIS

3.1. The first step in the design of a nuclear power plant against external events is to identify those events that are considered credible for a particular site. Reference [2] provides a method for selecting those credible human

induced events that should be considered for the site, while Refs [3, 4] present the hazard evaluation for some natural events. For other reasons, such as national safety policy, a certain type of external initiating event may be defined for design on a deterministic basis.

3.2. A general approach in the design is to establish the design input parameters by a combination of deterministic and probabilistic methods and to proceed with the design in a deterministic manner.

3.3. In some cases, even though the combined deterministic and probabilistic approach might identify a specific external human induced event as a potential design basis event, it may still be excluded from specific analysis if it is shown that the corresponding effects are bounded by the effects of other design basis events. However, it should be kept in the design basis to guarantee that potential engineering and administrative measures to be taken for the bounding event are valid for the bounded ones also.

3.4. When the hazard is defined in a probabilistic context, because of the deterministic approach applied in the design, the site hazard should be analysed and a 'single value' on the hazard curve should be selected to be used in the design basis. In this case, the selection of the design basis includes an implicit probabilistic assumption concerning the risk of a radiological accident that a nuclear installation can present, according to the Safety Requirements [1]. Therefore the final target of such an action is to keep the risk acceptably small, which implies an evaluation of the probability that an event will affect safety related items ('design probability values') and then the probability of unacceptable consequences of their failure.

3.5. However, a complete probabilistic analysis is usually carried out only in the framework of a PSA, i.e. in a confirmatory phase of the design. In the early design phase, therefore, assumptions for such conditional probabilities should be made, driven mainly by deterministic calculations (e.g. stress analysis and impact damage evaluation) and expert judgement, so as to select a design basis value on the hazard curve in a reasonable way.¹³ Because of its nature, this process is strictly plant dependent and should be assessed in the design assessment phase [16]. This value should also be compatible with the criteria applied in the probabilistic screening at the site evaluation phase.

¹³ In some States an acceptably small probability of an event generating an unacceptable radioactive release is defined as about 10^{-7} per reactor per year for a new nuclear power plant.

3.6. It may be prudent to specify minimum deterministic design loading conditions for those external events with potentially significant consequences for plant safety. States may wish to specify minimum loading conditions for missile impact, explosions and external fire. To do so provides a degree of confidence that a robustness of design will be ensured over the design lifetime of the plant to take account of unanticipated future scenarios.¹⁴

3.7. A higher probability value for some events may also be extracted from the hazard curve in relation to operational and load combination needs (see Section 2.3). The entire set of values should be consistent with the site hazard evaluation and should be inserted into a monitoring programme for hazard review as part of the process of periodic safety review.

3.8. The entire process should be approved by the regulatory body, and approved also for consistency with other risks from natural and industrial sources.

3.9. The following issues should be considered in the definition of the probability levels for the DBEEs:

- Installed power or hazard characteristic of the radiological source (in some States the spent fuel pool has a different DBEE than the reactor building);
- Concentration of event effects: probability of common cause failures as a consequence of the events (e.g. large fire, flood or extreme ambient temperature would be more prone to develop common cause failures than an aircraft crash);
- The need for active versus passive safety systems to prevent or mitigate unacceptable effects;
- The possible installation of warning systems able to detect in time the potential unfavourable development of an event (e.g. meteorological events versus aircraft crashes);
- The potential for quick dispersion following an event (e.g. explosions, flood and wind might have higher dispersion potential than extreme ambient temperature);
- The kind of potential contamination: long term effects, difficulties in decontamination, dispersed versus concentrated contamination and direct effects on the population;

¹⁴ In some States the following minimum deterministic loads are considered: external fire resistance of safety related buildings at 300°C, longer than 2.5 h; air blast pressure wave at 10 kPa; missile of 510 kg, 0.34 m diameter, 10.7 m long, at speed 25 m/s, rigid.

- Easy implementation of emergency planning in relation to the event: access to the site, availability of evacuation routes and time delay between accident and releases;
- Characteristics of the engineering features that might exhibit some form of cliff edge effect in the event of an accident (e.g. overtopping of a dyke in the event of a flood), without the possibility of preventing a degeneration of the situation with radiological consequences.

3.10. External event PSA, monitoring, inspection, surveillance and periodic safety reviews are the tools that should be used to confirm the selected target probability levels.

OVERALL DESIGN APPROACH

3.11. The initial operational modes to be considered at the time of occurrence of any DBEE, such as power, hot shutdown, cold shutdown, refuelling, maintenance and repair, should be determined in general on a probabilistic basis.

3.12. A typical logic diagram for analysis of the effects of DBEEs on classified items is shown in Fig. 1. The first steps identify the design basis events according to the site evaluation process and the postulated plant conditions (see Boxes 1 and 2 of Fig. 1). Then, probable scenarios of the consequences for the DBEE should be developed and on this basis the list of affected items should be produced and the items should be classified (see Box 3). Afterwards, the corresponding design parameters and loading schemes should be identified (see Box 4).

3.13. The selection of plant locations affected by a DBEE (e.g. site areas, buildings and exposed equipment) should be made carefully, since the possible effects on any particular function caused by the impairment of a system may not be obvious. For example, the repair time for a power line damaged by an event may determine the minimum amount of stored fuel required for the diesel generators, if the supply of diesel oil from sources nearby cannot be guaranteed. Failure of a ventilation system due to an aircraft crash may lead to a temperature rise inside a building, which in turn may cause the malfunctioning of electronic and pneumatic equipment.

3.14. The next step is to determine which items important to safety may be affected by an external event, either directly or by interaction, so as to ensure that the general design requirements can be met (Box 5). The designer should

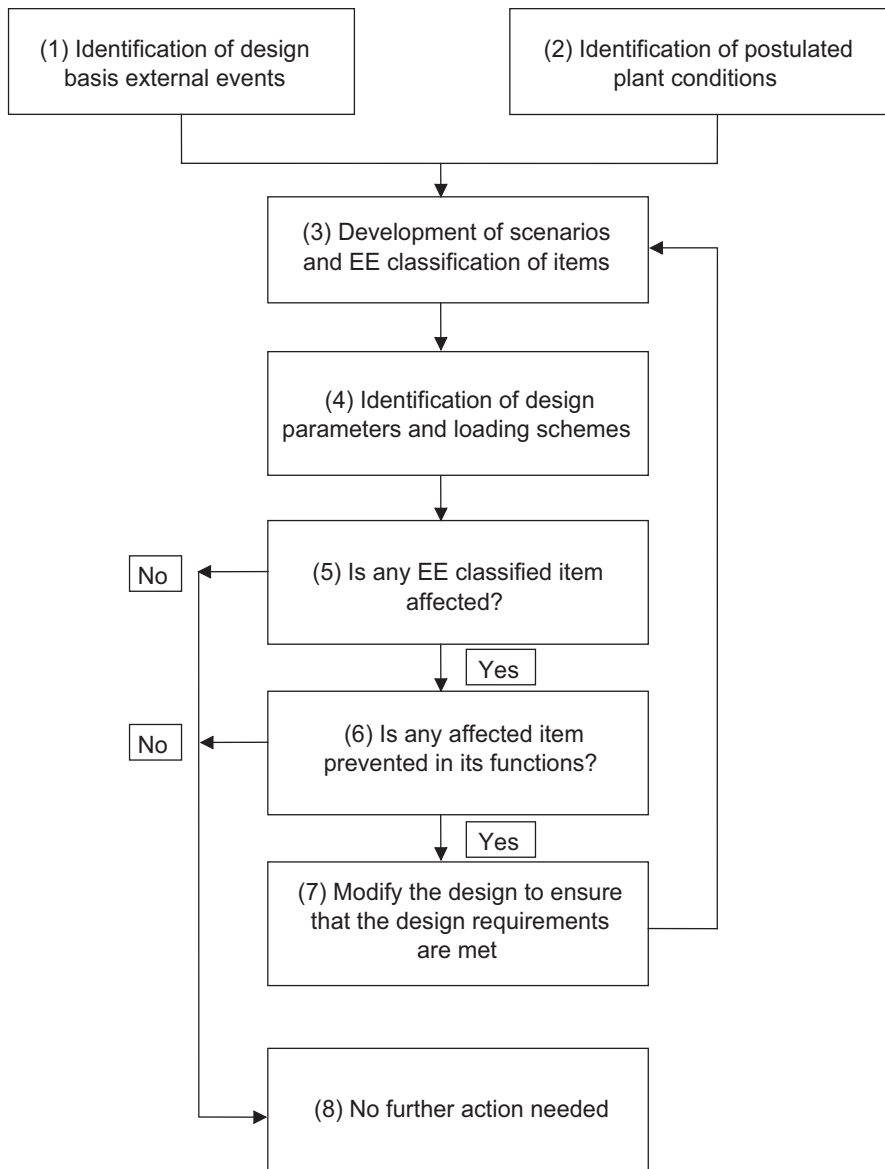


FIG. 1. Logic diagram for the design process in relation to external events.