IAEA TECDOC SERIES

IAEA-TECDOC-1874

IAEA-TECDOC-1874

Hierarchical Structure of Safety Goals for Nuclear Installations

IAEA
International Atomic Energy Agency

IAEA SAFETY STANDARDS AND RELATED PUBLICATIONS

IAEA SAFETY STANDARDS

Under the terms of Article III of its Statute, the IAEA is authorized to establish or adopt standards of safety for protection of health and minimization of danger to life and property, and to provide for the application of these standards.

The publications by means of which the IAEA establishes standards are issued in the **IAEA Safety Standards Series**. This series covers nuclear safety, radiation safety, transport safety and waste safety. The publication categories in the series are **Safety Fundamentals**, **Safety Requirements** and **Safety Guides**.

Information on the IAEA's safety standards programme is available on the IAEA Internet site

http://www-ns.iaea.org/standards/

The site provides the texts in English of published and draft safety standards. The texts of safety standards issued in Arabic, Chinese, French, Russian and Spanish, the IAEA Safety Glossary and a status report for safety standards under development are also available. For further information, please contact the IAEA at: Vienna International Centre, PO Box 100, 1400 Vienna, Austria.

All users of IAEA safety standards are invited to inform the IAEA of experience in their use (e.g. as a basis for national regulations, for safety reviews and for training courses) for the purpose of ensuring that they continue to meet users' needs. Information may be provided via the IAEA Internet site or by post, as above, or by email to Official.Mail@iaea.org.

RELATED PUBLICATIONS

The IAEA provides for the application of the standards and, under the terms of Articles III and VIII.C of its Statute, 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 in nuclear activities are issued as **Safety Reports**, which provide practical examples and detailed methods that can be used in support of the safety standards.

Other safety related IAEA publications are issued as **Emergency Preparedness and Response** publications, **Radiological Assessment Reports**, the International Nuclear Safety Group's **INSAG Reports**, **Technical Reports** and **TECDOCs**. The IAEA also issues reports on radiological accidents, training manuals and practical manuals, and other special safety related publications.

Security related publications are issued in the **IAEA Nuclear Security Series**.

The **IAEA Nuclear Energy Series** comprises informational publications to encourage and assist research on, and the development and practical application of, nuclear energy for peaceful purposes. It includes reports and guides on the status of and advances in technology, and on experience, good practices and practical examples in the areas of nuclear power, the nuclear fuel cycle, radioactive waste management and decommissioning.

HIERARCHICAL STRUCTURE OF SAFETY GOALS FOR NUCLEAR INSTALLATIONS

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

AFGHANISTAN
ALBANIA
ALGERIA
ANGOLA
ANTIGUA AND BARBUDA
ARGENTINA
ARMENIA
AUSTRALIA
AUSTRIA
AZERBAIJAN
BAHAMAS
BAHRAIN
BANGLADESH
BARBADOS
BELARUS
BELGIUM
BELIZE
BENIN
BOLIVIA, PLURINATIONAL STATE OF
BOSNIA AND HERZEGOVINA
BOTSWANA
BRAZIL
BRUNEI DARUSSALAM
BULGARIA
BURKINA FASO
BURUNDI
CAMBODIA
CAMEROON
CANADA
CENTRAL AFRICAN REPUBLIC
CHAD
CHILE
CHINA
COLOMBIA
CONGO
COSTA RICA
CÔTE D'IVOIRE
CROATIA
CUBA
CYPRUS
CZECH REPUBLIC
DEMOCRATIC REPUBLIC OF THE CONGO
DENMARK
DJIBOUTI
DOMINICA
DOMINICAN REPUBLIC
ECUADOR
EGYPT
EL SALVADOR
ERITREA
ESTONIA
ESWATINI
ETHIOPIA
FIJI
FINLAND
FRANCE
GABON
GEORGIA
GERMANY
GHANA
GREECE
GRENADA
GUATEMALA
GUYANA
HAITI
HOLY SEE
HONDURAS
HUNGARY
ICELAND
INDIA
INDONESIA
IRAN, ISLAMIC REPUBLIC OF
IRAQ
IRELAND
ISRAEL
ITALY
JAMAICA
JAPAN
JORDAN
KAZAKHSTAN
KENYA
KOREA, REPUBLIC OF
KUWAIT
KYRGYZSTAN
LAO PEOPLE'S DEMOCRATIC REPUBLIC
LATVIA
LEBANON
LESOTHO
LIBERIA
LIBYA
LIECHTENSTEIN
LITHUANIA
LUXEMBOURG
MADAGASCAR
MALAWI
MALAYSIA
MALI
MALTA
MARSHALL ISLANDS
MAURITANIA
MAURITIUS
MEXICO
MONACO
MONGOLIA
MONTENEGRO
MOROCCO
MOZAMBIQUE
MYANMAR
NAMIBIA
NEPAL
NETHERLANDS
NEW ZEALAND
NICARAGUA
NIGER
NIGERIA
NORTH MACEDONIA
NORWAY
OMAN
PAKISTAN
PALAU
PANAMA
PAPUA NEW GUINEA
PARAGUAY
PERU
PHILIPPINES
POLAND
PORTUGAL
QATAR
REPUBLIC OF MOLDOVA
ROMANIA
RUSSIAN FEDERATION
RWANDA
SAINT LUCIA
SAINT VINCENT AND THE GRENADINES
SAN MARINO
SAUDI ARABIA
SENEGAL
SERBIA
SEYCHELLES
SIERRA LEONE
SINGAPORE
SLOVAKIA
SLOVENIA
SOUTH AFRICA
SPAIN
SRI LANKA
SUDAN
SWEDEN
SWITZERLAND
SYRIAN ARAB REPUBLIC
TAJIKISTAN
THAILAND
TOGO
TRINIDAD AND TOBAGO
TUNISIA
TURKEY
TURKMENISTAN
UGANDA
UKRAINE
UNITED ARAB EMIRATES
UNITED KINGDOM OF GREAT BRITAIN AND NORTHERN IRELAND
UNITED REPUBLIC OF TANZANIA
UNITED STATES OF AMERICA
URUGUAY
UZBEKISTAN
VANUATU
VENEZUELA, BOLIVARIAN REPUBLIC OF
VIET NAM
YEMEN
ZAMBIA
ZIMBABWE

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-TECDOC-1874

HIERARCHICAL STRUCTURE OF SAFETY GOALS FOR NUCLEAR INSTALLATIONS

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2019

COPYRIGHT NOTICE

For further information on this publication, please contact:

Safety Assessment Section
International Atomic Energy Agency
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Email: Official.Mail@iaea.org

Printed by the IAEA in Austria
June 2019

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: Hierarchical structure of safety goals for nuclear installations / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2019. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1874 | Includes bibliographical references.
Identifiers: IAEAL 19-01242 | ISBN 978–92–0–103119–8 (paperback : alk. paper)
Subjects: LCSH: Nuclear facilities. | Industrial safety. | Nuclear engineering — Safety measures.

FOREWORD

Nuclear safety is provided by various means, the effectiveness and sufficiency of which are evaluated by means of safety assessment performed by licensees and reviewed by regulatory bodies. The current approach to safety assessment requires that both deterministic and probabilistic assessments be performed to demonstrate that safety requirements and criteria are met and that risk is acceptably low.

It is an important and at the same time challenging task to determine a set of safety requirements and criteria that would aid in answering the question, How safe is safe enough? In order to achieve the fundamental safety objective of protecting people and the environment from harmful effects of ionizing radiation, a set of detailed technical requirements and criteria, both qualitative and quantitative, can be formulated as safety goals.

The main objective of the present publication is to assist in developing a good understanding of the definition and use of safety goals, and of the process of establishing a consistent and coherent hierarchy of safety goals for nuclear installations. The publication provides nuclear safety specialists and decision makers in operating organizations and nuclear safety regulatory bodies with information on, and examples of, implementation of a hierarchy of safety goals proceeding a range of issues, from high level society-wide considerations to detailed technical issues.

The IAEA thanks those experts who helped prepare this publication for their valuable contributions. The IAEA technical officers responsible for this publication were I. Kuzmina and A. Chekin of the Division of Nuclear Installation Safety.

EDITORIAL NOTE

This publication has been prepared from the original material as submitted by the contributors and has not been edited by the editorial staff of the IAEA. The views expressed remain the responsibility of the contributors and do not necessarily represent the views of the IAEA or its Member States.

Neither the IAEA nor its Member States assume any responsibility for consequences which may arise from the use of this publication. This publication does not address questions of responsibility, legal or otherwise, for acts or omissions on the part of any person.

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.

The authors are responsible for having obtained the necessary permission for the IAEA to reproduce, translate or use material from sources already protected by copyrights.

The IAEA has no responsibility for the persistence or accuracy of URLs for external or third party Internet web sites referred to in this publication and does not guarantee that any content on such web sites is, or will remain, accurate or appropriate.

CONTENTS

1. INTRODUCTION 1

1.1. BACKGROUND 1
1.2. OBJECTIVES 1
1.3. SCOPE 2
1.4. STRUCTURE 2

2. A GENERAL HIERARCHY OF SAFETY GOALS 3

2.1. INTRODUCTORY REMARKS 3
2.2. TYPES OF SAFETY GOALS 3
2.3. HIERARCHICAL APPROACH TO SAFETY GOALS 4
2.3.1. Proposed hierarchy of safety goals 5
2.3.2. Top level safety goals 7
2.3.3. Upper level safety goals 7
2.3.4. Intermediate level safety goals 8
2.3.5. Low level safety goals 8

3. DERIVATION OF SAFETY GOALS 9

3.1. INTRODUCTORY REMARKS 9
3.2. THE ROLES OF STAKEHOLDERS INVOLVED IN THE DEFINITION OF SAFETY GOALS 9
3.3. SAFETY GOALS WITHIN THE HIERARCHY 9
3.3.1. Top level safety goals 10
3.3.2. Upper level safety goals 10
3.3.3. Intermediate level safety goals 10
3.3.4. Low level safety goals 13
3.4. ORGANIZING THE SAFETY GOALS DEFINED WITHIN THE HIERARCHY 14
3.4.1. Labelling scheme for safety goals 14
3.4.2. Table of examples of safety goals within the hierarchy 14

4. APPLICATIONS OF A HIERARCHY OF SAFETY GOALS 18

4.1. INTRODUCTORY REMARKS 18
4.2. COMPLIANCE ASSESSMENT 18
4.2.1. Compliance with top level and upper level safety goals 18
4.2.2. Compliance with intermediate level safety goals 19
4.2.3. Compliance with low level safety goals 19
4.2.4. Compliance with quantitative safety goals 19
4.2.5. Compliance with qualitative safety goals 20
4.2.6. Trade-off and integrated compliance 20
4.3. REGULATORY AND LICENSEE APPLICATIONS 20
4.3.1. Application of safety goals in design 21
4.3.2. Application of safety goals during operations 21
4.4. USE OF SAFETY GOALS IN INTEGRATED RISK INFORMED DECISION MAKING 22

4.5. SAFETY COMMUNICATION 23
4.5.1. Communication between the regulatory body and the public 23
4.5.2. Communication between the regulatory body and the licensee/licence applicant 23
4.5.3. Communication between the operating organisation and the public 24

5. CONCLUDING REMARKS 25

ANNEX I. SAFETY GOALS FOR NUCLEAR INSTALLATIONS IN CANADA 29

ANNEX II. APPLICATION OF THE PROPOSED SAFETY GOALS FRAMEWORK TO THE GERMAN REGULATORY FRAMEWORK FOR NUCLEAR POWER PLANTS 45

ANNEX III. APPLICATION OF THE GENERAL SAFETY GOALS FRAMEWORK FOR NUCLEAR INSTALLATIONS TO SWEDEN 61

ANNEX IV. UK FRAMEWORK FOR NUCLEAR SAFETY GOALS AND TARGETS 77

ANNEX V. DEVELOPMENT OF USNRC SAFETY GOALS FOR LIGHT WATER REACTORS 85

ANNEX VI. EXAMPLES OF SAFETY GOALS HIERARCHIES 91

ANNEX VII. EXAMPLE OF AN APPROACH FOR DEFINING LOW LEVEL PROBABILISTIC SAFETY GOALS 101

1. INTRODUCTION

1.1. BACKGROUND

In 2006, the International Atomic Energy Agency (IAEA) published its Fundamental Safety Principles [1], which states that "The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation", which is to be achieved by adherence to ten safety principles.

Principle 6 of [1], 'Limitation of risks to individuals', states that "Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm." Thus, the risks associated with the operation of nuclear installations must be assessed and controlled, and criteria for what constitutes an 'unacceptable risk' need to be established. These criteria are then used to provide assurance that there are sufficient safety provisions in the design and operational processes to demonstrate that risks are not unacceptable. The IAEA Safety Requirements on Safety Assessment for Facilities and Activities [2] also require to establish criteria for judging safety (Requirement 16).

Several different terms are used for stating or defining safety criteria. In this document, the term safety goal is a necessary characteristic of a structured set (qualitative and/or quantitative), which is expected to be satisfied to assure that an acceptable level of safety is provided. Therefore, a comprehensive set of 'safety goals' is needed. Safety goals may be expressed qualitatively and/or quantitatively, and the term 'risk' is used to cover all situations that have the potential to cause harmful consequences.

The IAEA safety standards (e.g. [1], [3], [4], [5]) define safety principles and some quantitative safety criteria (e.g. dose limits) or semi-quantitative safety criteria (e.g. using terms like 'very low risk'). Particularly important in this context is the concept of Defence-in-Depth (DiD) [6], i.e. a number of consecutive and independent levels of protection which would have to fail before harmful effects could occur. However, safety goals have only been introduced in the IAEA Safety Standards for the probabilistic safety assessment (PSA) of nuclear power plants (NPPs) ([7], and [8]). There is currently no IAEA guidance or publications on how to develop a consistent and coherent set of safety goals in other areas or for nuclear installations other than nuclear power plants.

Several countries refer to the INSAG-12 report [9], as a basis for their national set of quantitative safety goals. Since publication of INSAG-12, there have been considerable developments in the area of safety goals. The integration of qualitative and quantitative safety goals is being pursued by various countries, international organizations and expert groups (see examples in Annexes). The growing importance of establishing a consistent and coherent hierarchy of safety goals for NPPs and other nuclear installations on the basis of the consideration of both quantitative and qualitative concepts has been widely recognized.

1.2. OBJECTIVES

The primary objective of this TECDOC is to assist in creating a greater understanding of the establishment, use and communication of safety goals for nuclear installations in Member States.

This TECDOC sets out the advantages and benefits of developing a hierarchical organization of safety goals. It provides practical guidance and examples on establishing a consistent and coherent hierarchical set of safety goals for nuclear installations. During the initial work, the

word “framework” was used to refer to this hierarchical organization of safety goals. This term is sometimes used in contributions received from some Member States, which are included in the annexes. In the rest of the document, “hierarchy” is used instead of framework. In addition, this TECDOC provides practical guidance on the safety goals that are needed for use in an integrated risk-informed decision making (IRIDM) process[1]. The use of safety goals for communicating with stakeholders and other purposes is also discussed.

This TECDOC discusses the advantages of a hierarchical structure of safety goals and their use but does not recommend any particular set of safety goals because it is the responsibility of each Member State to determine how nuclear safety is assured. A hierarchical structure is proposed as an approach that is consistent and coherent across different nuclear facilities and activities by describing how to develop an appropriate hierarchical structure that may be adopted by different stakeholders in Member States.

1.3. SCOPE

The scope of this TECDOC is concerned only with radiation and nuclear safety. This TECDOC is intended to be applicable with some judgement to all types of nuclear facilities and activities during their lifecycle. However, the examples and specific considerations on safety goals are mainly related to water-cooled NPPs.

1.4. STRUCTURE

Section 2 describes the main elements and a possible hierarchical structure of safety goals. The process for the development of a hierarchical structure of safety goals is described in Section 3. Section 4 discusses applications of the hierarchical structure of safety goals. Section 5 provides concluding remarks. In addition, several Annexes provide supporting information and examples of safety goals developed in Member States and international experts groups, and examples of benchmarking the hierarchy of safety goals suggested in this TECDOC against the existing national safety goals.

[1] IRIDM is a systematic process aimed at the integration of the major considerations influencing nuclear power plant safety. The main goal of IRIDM is to ensure that any decision affecting nuclear safety is optimized without unduly limiting the conduct of operation of the nuclear power plant. It underpins nuclear safety decisions and ensures consistency with the safety goals of the Member State.

Source: A Framework for an Integrated Risk Informed Decision Making Process, INSAG-25, IAEA, Vienna (2011).

2. A GENERAL HIERARCHY OF SAFETY GOALS

2.1. INTRODUCTORY REMARKS

The reason for defining a hierarchy of safety goals is twofold. Firstly, it takes account of the fact that no single safety goal can be used to assess all safety aspects of an installation, but that typically a set of safety goals is needed. Secondly, it makes it possible to present interrelations within the safety goals, which is important in order for different safety goals to give consistent answers when applied to a nuclear installation.

Due to the way safety requirements are typically formulated, it is suitable to structure the safety goals in a hierarchical manner. A number of hierarchical approaches already suggested are discussed in Annex VI. The approaches suggested by MDEP and NPSAG show great similarities, but differ in where the main focus is put. Thus, in the MDEP approach the higher (technology independent) levels have so far been described more in detail, whereas the focus in the NPSAG approach has been on providing a reasonable level of degree in the description of the lower technical levels, which are more technology specific.

The hierarchical approach proposed in this section covers the entire range of levels, from the highest (society) to the lowest (technology and facility specific) level.

2.2. TYPES OF SAFETY GOALS

In principle, the hierarchy of safety goals can be applicable to all nuclear installations during their entire lifetime; the safety goals cover the whole range of conditions of the installation and all relevant sources of radioactivity on the site are expected to be taken into account.

The highest level safety goal would be expected to remain unchanged over all life cycle phases, while lower level safety goals may be different for different life cycle phases, and may also change during the life time of an installation. Both operational states and accident conditions need to be considered[2].

Safety goals are either qualitative or quantitative. Semi-quantitative safety goals typically appear at a high level in the structure and often constitute a bridge between a qualitative and a quantitative safety goal. They include criteria where something is expressed in terms of "frequent/infrequent" or as being "high/low" compared to something else. An example of a semi-quantitative safety goal is the requirement in some Member States that the risk from NPP's shall be low compared to the risk from other viable means of electricity generation.[3]. Quantitative safety goals may be either deterministic or probabilistic, the quantitative deterministic safety goals often being defined as success criteria for a particular assessment.

[2] For NPPs operational states include all modes normal operation and anticipated operational occurrences. Accident conditions comprise design basis accidents and plant conditions beyond them, including severe accidents, for which the plant may be designed or not.

[3] Semi-quantitative safety goals could be another type, but they have generally been considered as quantitative safety goals

The range of application of safety goals and their types is illustrated in Figure 1.

FIG. 1. Types of safety goals and field of application.

2.3. HIERARCHICAL APPROACH TO SAFETY GOALS

For establishing a hierarchical structure of safety goals the following general aspects are expected to be considered:

- The hierarchy is to be applicable to all types of nuclear installations (examples are however often provided for water-cooled NPPs, specifically LWRs).
- The hierarchy is to be applicable to all relevant lifetime stages.
- The hierarchy is to cover the applicable states of the installation, e.g. operational states and accident conditions.
- The hierarchy is to complement and be in agreement with the structure of the IAEA Fundamental Safety Principles and Safety Standards.
- The hierarchy is to be consistent with the structure and intents of defence-in-depth and support its implementation.
- The Top Level safety goals express overall requirements on society level, while lower levels will successively detail the top level goals.
- Safety goals on different levels are to be consistent and traceable, allowing to derive lower level goals from higher level ones.
- Higher level safety goals are as far as possible to be technology neutral, while lower level goals are expected to be increasingly technology specific.
- The hierarchy is to include qualitative as well as quantitative safety goals.
- The structure is to be clearly and unambiguously defined, making it easy to understand, implement and communicate.

It has to be noted that some further considerations may need to be taken into account during the process of applying the actual safety goals forming the hierarchy, which are discussed in Section 4.

2.3.1. Proposed hierarchy of safety goals

The proposed hierarchy of safety goals is shown in Figure 2. The picture also illustrates how the levels of safety goals relate to different aspects of safety (society/site/facility) and to technology (technology independent/specific), and the potential overlaps. In Table 1, each of the levels of safety goals is briefly characterised. A more detailed discussion about each level is provided in the following sub-sections. In addition, in Section 3, the derivation of the hierarchy of safety goals is discussed in more detail and examples are given of specific safety goals on the various levels.

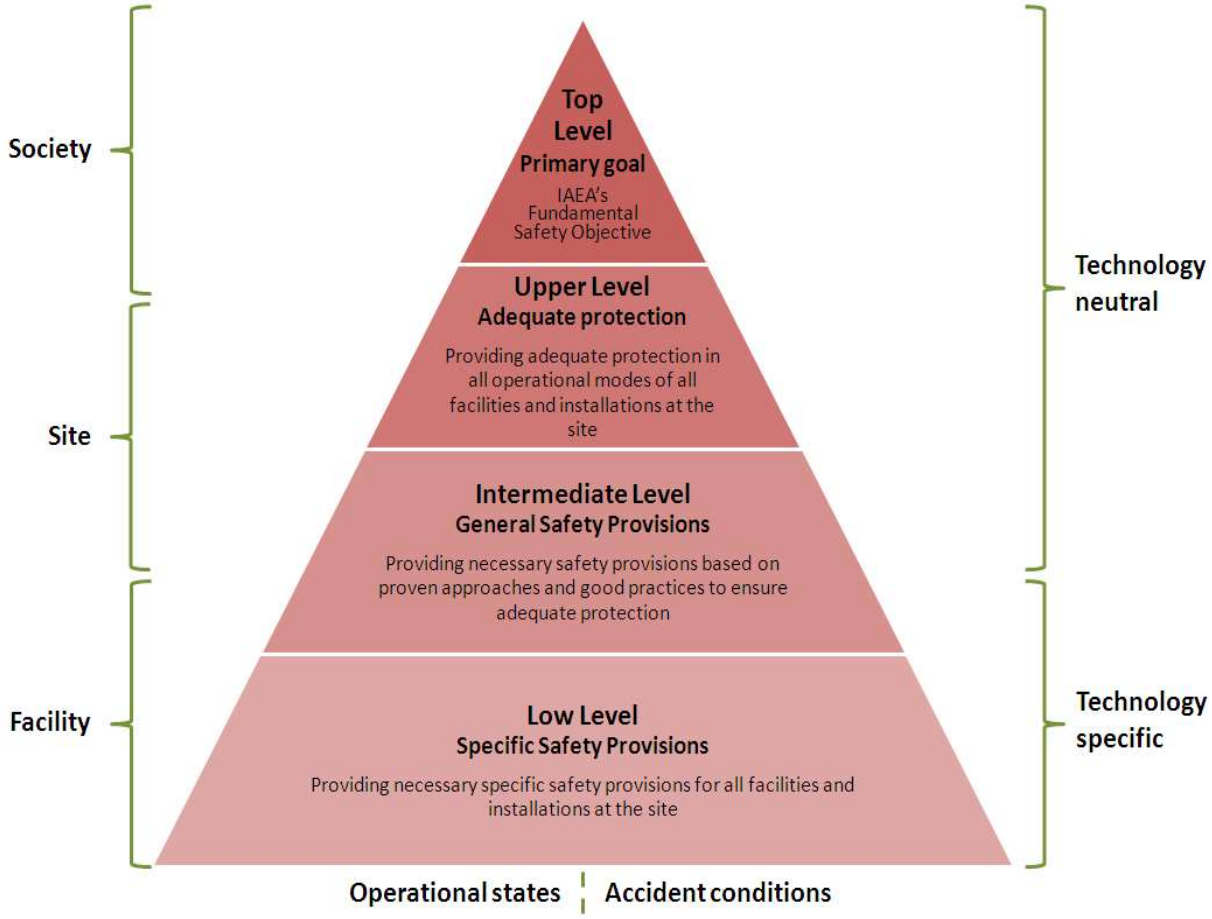

FIG. 2. Proposed hierarchy of safety goals.

TABLE 1. HIERARCHICAL LEVELS OF SAFETY GOALS

Level	Overall Objective	Description	Explanations on the Nature of Safety Goals and Examples[4]
Top Level Primary Safety Goal	Protecting people and the environment from harmful effect of ionizing radiation	Fundamental safety objective as set out in [1] and society level safety goals as defined in national legislation or regulations. The safety goals at this level are society-wide and technology neutral.	Goals at this level are expressed qualitatively and may presuppose, e.g. the prevention of unreasonable harm to the public and the environment. These safety goals may have a wider scope than nuclear.
Upper Level Adequate Protection	Ensuring adequate protection in all states for all facilities and installations at the site	Interpretation of the Top Level safety goal in terms that are defined in more detail at the Intermediate and Low Level. The safety goals at this level are typically technology neutral and have a site-wide scope. They cover operational states and accident conditions.	Upper Level safety goals are high-level and used as a bridge to support the development of Intermediate and Low Level safety goals from the Top Level. In some countries, this is done by relating to levels of risks from other involuntary sources of risk, using quantitative or semi-quantitative expressions of relation between risks from nuclear installations and risks from other involuntary sources of risk, e.g. fatality risks from other sources of energy production.
Intermediate Level General Safety Provisions	Providing general safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection	Formulation of proven approaches and good practices to achieve the higher level safety goals as well as definition of general requirements on site level. The safety goals at this level are still largely technology neutral and site-wide.	Intermediate level safety goals typically include principles related to defence-in-depth, safety margins, physical barriers, considerations related to independence and protection of barriers, redundancy and independence, doses for normal operation, amounts of radioactive waste generated, etc. This level also includes the definition of some high-level quantitative safety goals, e.g. overall large early release frequency (LERF) for the site.

[4] Safety goals mentioned in this table and throughout this section are expected to be seen as examples and do not constitute a complete list of safety goals.

TABLE 1. HIERARCHICAL LEVELS OF SAFETY GOALS (cont.)

Level	Overall Objective	Description	Explanations on the Nature of Safety Goals and Examples
Low Level Specific Safety Provisions	Providing specific safety provisions for each facility and installation at the site to ensure adequate protection	Formulation of technology and facility specific safety goals aimed at assuring that each nuclear facility at the site effectively contributes to meeting the higher level safety goals.	A large number of specific deterministic safety goals are in use, e.g. related to maximum fuel cladding temperature in an LWR. This level may also include quantitative probabilistic safety goals, e.g. for a specific plant unit, the frequency of large release, core or fuel damage, barrier strength, or SSC reliability.

2.3.2. Top level safety goals

Top Level safety goals are the highest level safety goals as defined in national legislation or regulations. In many countries, nuclear safety is ultimately governed by qualitative safety goals at the society level, which are often defined in nuclear legislation but may also be issued by regulatory authorities. These safety goals differ in wording between countries, but generally presuppose the prevention of unreasonable harm to the workers, public and the environment from ionizing radiation, in line with the IAEA Fundamental Safety Objective [1].

Top Level safety goals are important as high-level statements, but may not be sufficient themselves to be used as a basis for defining detailed safety goals.

2.3.3. Upper level safety goals

The Upper Level safety goals provide an interpretation of the Top Level safety goals in terms of overarching requirements to ensure adequate protection and limiting risks of undue harm to people and the environment in operational states and accident conditions. Upper Level safety goals are expressed in more detail than the Top Level safety goals, providing a bridge to the more detailed technical safety goals at the Intermediate and Low Levels. The Upper Level safety goals may also reflect different aspects of risk, such as effects on individuals and society at large.

Upper Level safety goals are typically technology neutral and have a site-wide scope thus providing a basis for Intermediate and Low Level safety goals, which may require an interpretation in numerical terms of what constitutes an unreasonable risk to an individual or to the society.

Upper Level safety goals typically define harmful effects in a way that allows detailed interpretation on the underlying levels. In some countries this is done by comparison with other involuntary sources of risk, e.g., with fatality risks from other sources of energy production or cancer fatality risks from other human-made causes, to which an individual is exposed. In addition, Upper Level safety goals may also be qualitative to draw attention to particular nuclear safety aspects, such as minimisation of radioactive waste, effective leadership and management, etc. Upper Level safety goals may also consider tolerable levels of disruption to the population in the site vicinity, e.g. evacuation, relocation-areas and time scales, and agricultural restrictions.

2.3.4. Intermediate level safety goals

Intermediate Level safety goals are normally to a large extent technology neutral but can include the highest level safety goals for application to specific technologies. This is also the appropriate level to distinguish between facility and site-wide safety goals. Thus, the scope is basically site-wide, but may also include aspects related to specific facilities.

Intermediate Level safety goals are aimed to cover crucial general safety principles and provisions such as defence-in-depth, safety margins, physical barriers (including considerations related to independence and protection of barriers), and redundancy and independence.

Safety goals on Intermediate Level also include site level requirements as appropriate, e.g. related to potential releases (total frequency for the site for large (early) release) or site level capability to handle external hazards with a certain frequency and magnitude.

2.3.5. Low level safety goals

The Low Level safety goals are technical and aim at assuring the nuclear installation meets the higher level safety goals, by addressing siting, design and operational aspects of a nuclear installation. Technical safety goals are also more directly useful as means to evaluate the adequacy of existing or proposed designs of safety related SSCs.

At this level, various aspects of the design and operation of a specific nuclear installation are assessed against safety goals. There is a wide range of safety goals on this level to address both operational states and accident conditions.

Some Low Level safety goals are qualitative and relate to whether a risk, or a condition that may result in a risk, is acceptable. Quantitative deterministic safety goals may relate to maximum or minimum values of crucial parameters, such as fuel temperature, pressure or water levels. Quantitative probabilistic safety goals are expressed as frequencies or probabilities of unacceptable states or consequences. Low level safety goals can constitute requirements or acceptance criteria for design and operation.

3. DERIVATION OF SAFETY GOALS

3.1. INTRODUCTORY REMARKS

This section deals with the derivation of safety goals within the hierarchy of safety goals. Initially, the context and process of defining safety goals is described, i.e. the process through which safety goals on a certain level are defined and the organisation typically defining the safety goals within the hierarchy.

Thereafter, the definition of safety goals on the four levels of the hierarchy is addressed in more detail, also giving examples of potentially relevant safety goals. Where relevant, a discussion is provided on the determination of lower-level safety goals from higher-level safety goals on Top and Upper Levels. These higher-level safety goals could be qualitative and/or quantitative, and aim at helping in making the assessment that nuclear installations have achieved an acceptable level of safety for individuals and society in general. The determination of Intermediate and Low Level safety goals makes possible the coherent use of a set of safety goals at the organisational and technical level that relates to the established safety goals on higher levels.

Although safety goals on Top and Upper Levels are less likely to be changed (particularly if legally established), safety goals on the lower levels may be changed more frequently.

3.2. THE ROLES OF STAKEHOLDERS INVOLVED IN THE DEFINITION OF SAFETY GOALS

Safety goals are intended to reflect the interests of the public, not only those who are directly involved in nuclear safety. At the higher levels (mostly Top and Upper levels), it is the responsibility of Government, or one of its agencies, to define what constitutes an acceptable level of risk. A possibility adopted in some Member States is to take reference with respect to risks from other industries or activities, national accident statistics or death rates from specific causes. These safety goals will be enshrined in legal or other mandatory documents. At levels below the Top Level, as the goals become more technology and facility specific (mostly Intermediate and Low Levels), the role of the regulatory body becomes more important. The input of various expert technical organisations and the licensee becomes more significant in the definition of the two lower level safety goals. In some countries, Low Level safety goals may be defined by the licensees and approved or accepted by the regulatory body.

This progression is outlined in the IAEA Safety Fundamentals [1] which states “The government is responsible for the adoption within its national legal system of such legislation, regulations, and other standards and measures as may be necessary ...” and “Governments and regulatory bodies thus have an important responsibility in establishing standards ...” The Safety Fundamentals [1] also states that the licensee must fulfil its “responsibilities … in accordance with applicable safety objectives and requirements as established or approved by the regulatory body”. Further statements include, “In addition, detailed criteria may be developed to assist in assessing compliance with these higher level objectives, principles and requirements, including risk criteria that relate to the likelihood of anticipated operational occurrences or the likelihood of accidents occurring that give rise to significant radiation risks.”

3.3. SAFETY GOALS WITHIN THE HIERARCHY

This section discusses for each of the four levels of the hierarchy of safety goals, the types of safety goals to be included at a specific level, and the relationship to the previous (higher) level.

3.3.1. Top level safety goals

Top Level safety goals are normally already in place as part of national legislation or regulatory authority requirements. They are generally expressed qualitatively and presuppose the prevention of unreasonable risk to the public and the environment.

No specific recommendations are made regarding the wording or contents of the Top Level safety goal. It is, however, assumed that some safety goal is in place with a scope and aim corresponding to the IAEA Fundamental Safety Objective [1] of protecting people and the environment from harmful effects of ionizing radiation.

3.3.2. Upper level safety goals

Upper Level safety goals are to be defined for both operational states and accident conditions.

The definition of Upper Level safety goals determines the requirements for adequate protection, which requires inter alia the interpretation of the Top Level safety goal in terms of risk, directly or implicitly. This interpretation is an important and key step for the feasibility and acceptability of the hierarchical structure of safety goals.

Upper Level safety goals often express the requirement that risks from the use of nuclear energy are expected to be low compared to other risks to which the public is normally exposed, and are often already in place as part of national law or authority requirements.

It is important in setting Upper Level safety goals that the characteristics of the risks posed by nuclear facilities are taken fully into account. Ionising radiation can lead to a range of effects that can result in restrictions on food production and land occupation to protect public health. High Level quantitative safety goals are expected to encompass these impacts. In terms of public perception, key issues associated with nuclear installations appear to be land contamination and cancer risk. The necessity to provide an emergency response plan is also an upper level requirement.

The Upper Level safety goals imply that justification of the facility or activity in terms of providing an overall benefit is required before a facility can operate or an activity is performed. This justification is generally made at a government or regulatory body level depending on the nature of the facility or activity. Justification requires assessment of the benefit and whether it can be achieved by the facility or activity in a way that does not outweigh the radiation risks.

3.3.3. Intermediate level safety goals

Intermediate Level safety goals aim at providing necessary general safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection such that the higher level goals are adequately addressed, thus achieving the higher level safety goals. At Intermediate Level, some site level issues may also need to be addressed.

Intermediate Level safety goals cover crucial technical safety provisions relating to optimization of protection and limitation of risks such that general safety principles are addressed e.g. defence-in-depth, safety margins, physical barriers (including considerations related to independence and protection of barriers), and redundancy and independence.

Safety goals on Intermediate Level also include site level requirements, e.g. related to risk of total releases from the site rather than from individual facilities on the site (e.g. overall LRF or LERF for the site), or site level requirements related to the capability to handle external hazards (e.g. design of site protective features, effects on shared resources or systems or on emergency preparedness in cases where several facilities are subject to the same event).

Intermediate Level safety goals may include major design requirements such as requirements with respect to diversity, redundancy, structural protection and spatial separation to achieve the required effectiveness and reliability of SSCs, and the single failure criterion. Human factor issues, such as not requiring operator actions within a certain timescale after the occurrence of an abnormal event, will also feature at this level.

The following paragraphs highlight further details for several examples of safety goals corresponding to the Intermediate Level; these include (with no implication for completeness):

A. Radiation Protection Safety Goals for Normal Operation

B. Effective Defence-in-Depth

C. Sufficient Redundancy and Diversity

D. Independence, Protection of Barriers, and Safety Functions

E. Effective Barriers

A. Radiation Protection Safety Goals for Normal Operations

Radiation protection safety goals on the Intermediate Level are generally expressed in the form of dose and contamination levels which are considered to pose acceptable level of risks of latent, stochastic effects (usually cancer) in the exposed persons. These dose and contamination levels are described in the IAEA Requirements for Radiation Protection and Safety of Radiation Sources [3].

Intermediate Level safety goals used to determine whether the protection of workers is optimised include designation of controlled and supervised areas, shielding structures, personal protective equipment including clothing and the control of maintenance activities. Optimisation of protection of the public is based on setting levels of the radioactive discharges and radiation effects from the facility or site.

Intermediate Level safety goals for limitation of risks are usually expressed as dose limits (which are based on the recommendations of the ICRP [11,12]) that are not to be exceeded but with the requirement to reduce doses below these levels ***as low as reasonably achievable*** (ALARA) taking account of societal and economic factors. For workers, the doses are monitored and it is usual to have “action levels” at some fraction of the limit. Dose limits cover specific doses to organs, tissues and extremities as well as whole body levels. Limitation of dose to the public is achieved through setting limits on the liquid and gaseous discharges from the site and radiation which, through analysis of the routes by which this leads to exposure, are shown to not exceed the dose levels in the most exposed individuals.

B. Effective Defence-in-Depth

The IAEA Fundamental Safety Principles [1] state that the application of the DiD concept is the primary means of preventing accidents at a nuclear power plant and of mitigating the consequences of accidents if they do occur. The DiD concept is applied to all safety related activities. This is to ensure that all safety related activities are subject to independent layers of provisions, so that if a failure were to occur, it would be detected and compensated for or corrected by appropriate measures. Application of the DiD concept throughout design and operation provides protection against all types of credible failures, including those resulting from equipment failure or human induced events within the plant, and against consequences of events that originate outside the plant. The brief outline of five DiD levels for NPPs and the essential means by which they are assured from INSAG-12 report [9] are shown in Table 2.

TABLE 2. DiD LEVELS

DiD Levels	Objective	Essential Means
Level 1	Prevention of abnormal operation and failures	Conservative design and high quality in construction and operation
Level 2	Control of abnormal operation and detection of failures	Control, limiting and protection systems and other surveillance features
Level 3	Control of accident within the design basis	Engineered safety features and accident procedures
Level 4	Control of severe plant conditions, including prevention of accident progression and mitigation of the consequences of severe accidents	Complementary measures and accident management
Level 5	Mitigation of radiological consequences of significant releases of radioactive material	Off-site emergency response

C. Sufficient Redundancy and Diversity

Achieving adequate reliability of DiD levels will, in general, require redundancy in the design of plant systems. The application of the single failure criterion provides a deterministic approach for increasing system reliability. In practice however, common cause failures limit the reliability of redundant systems. Protection from such failures involves measures such as diversity, physical separation, and functional isolation of systems and components.

D. Independence and Protection of Barriers, and Safety Functions

Independence and protection of barriers are inherent parts of the DiD safety concept. Another related concept is provision of the fulfilment of a set of fundamental safety functions for the NPP.

Protection of barriers and fulfilment of fundamental safety functions tends to focus on engineered design provisions, though not exclusively. SSCs provided to support these two aspects needs to be sufficiently reliable.

E. Effective Barriers

INSAG-10 [5] notes that generally, several successive physical barriers for the confinement of radioactive material are put in place. Their specific design may vary depending on the activity of the material and on the possible deviations from normal operation that could result in the failure of some barriers. These barriers may serve operational and safety purposes or safety purposes only. The DiD concept applies to the protection of their integrity against internal and external events that may jeopardize it.

The analysis of barriers are expected not only account for the physical barriers but also need to take into account the systems provided to protect these barriers. INSAG-10 [5] identifies four barriers for LWRs, i.e., the fuel matrix, the fuel cladding, the boundary of the reactor coolant system, and the containment structure.

3.3.4. Low level safety goals

Low Level safety goals are technology and facility specific, and are intended to ensure that a nuclear installation meets the higher level safety goals, including requirements in national laws and regulations. This is done by addressing the design and site implementation of a nuclear installation. Low Level safety goals are also more directly useful than the higher levels of safety goals as means to evaluate the adequacy of existing or proposed designs of safety related SSCs.

For operational states, Low Level safety goals are in general related to the performance of SSCs and the provision of the operational requirements, e.g. operating procedures for normal operation and for anticipated operational occurrences. Whilst safety goals related to external hazards at the site level are included in the Intermediate Level safety goals, detailed requirements in the form of Low Level safety goals may be included within the design basis (e.g. seismic fragility-related requirements for SSCs). The Low Level safety goals may include detailed specification of the safety margins. These margins may be dependent on the technical specifications of SSCs, properties of materials used and production processes, etc.

In general, Low Level safety goals related to accident conditions deal with engineered safety features and operator procedures in order to control accidents within the design envelope.

As part of the Low Level safety goals, there may be multiple sub-levels of safety goals, defining ***subsidiary (or surrogate) goals***. These also need to be consistently defined, e.g. regarding safety goals addressing LRF and CDF.

Some examples of Low Level safety goals are provided below. The examples given are for a LWR NPP, but the information may be largely applicable to other types of NPPs, as well as to other types of nuclear facilities.

Thus, Low level safety goals are often defined on one or more of the following headings for an installation or facility:

- Deterministic safety goals may include:
    - required number of trains in safety systems
    - maximum fuel clad temperature
    - design requirements against internal hazards and external hazards

- Probabilistic safety goals, i.e. quantitative safety goals specifying the frequency of a specific consequence, may include:
    - Off-site consequence level (could correspond to PSA Level 3)
    - Radioactive release from plant level (could correspond to PSA Level 2)
    - Core or fuel damage level (could correspond to PSA Level 1)
    - Lower technical criteria; numerous possibilities exist (barrier strength, safety function, safety system, etc.)

3.4. ORGANIZING THE SAFETY GOALS DEFINED WITHIN THE HIERARCHY

3.4.1. Labelling scheme for safety goals

A labelling scheme to provide traceability of safety goals is seen to be useful. Such a scheme has been introduced in the example below. Each level of safety goals is reflected in the designation of the identifier which is composed reflecting the following:

- Top Level safety goal is single and does not need an identifier;
- Upper Level safety goals identifiers point to operational states (O) or accident conditions (A);
- Intermediate Level safety goals identifiers characterize the types of safety goals as qualitative (Q) and quantitative deterministic (D) and quantitative probabilistic (P);
- Low Level safety goals identifiers point to specific installations at the site and specific types of safety goals.

Table 3 provides an overview of the example of labelling scheme for safety goals identifiers.

3.4.2. Table of examples of safety goals within the hierarchy

Based on the safety goal hierarchy defined and the discussion of the relation between levels in the hierarchy and the scope and characteristics of the safety goals to be defined at each of the levels, a summary table has been compiled (Table 4), and populated with some typical examples of safety goals at each level.

It has to be emphasized that the contents of Table 4 are viewed solely as an example; the proper application of the hierarchical structure of safety goals would result in additional or other types of safety goals being identified. In addition, in this example, which serves only for the purpose of the overall concept illustration, not all higher level safety goals are detailed to the level of Low Level safety goals.

TABLE 3. AN EXAMPLE OF LABELLING SCHEME FOR SAFETY GOALS IDENTIFIERS (ID)

Safety Goals Level	Identifiers Used within the Level	Comment	Example
Top Level	None	Not needed	
Upper Level	O – operational states A – accident conditions	Safety goals are labelled by the relevant ID followed by a sequential number within the category, e.g.: O1, O2, A1, A2	**LOW RISK TO PEOPLE'S LIFE AND HEALTH** Risk to life and health of people from the facilities and installations located at the site should be low comparing with risk from other sources to which an individual is generally exposed
Intermediate Level	Q – qualitative P – quantitative probabilistic D – quantitative deterministic	The ID created at the previous level is amended by the relevant ID of the current level followed by a sequential number within the type, e.g.: O1-Q1, O1-Q2, O1-D1, O2-D1 A1-Q1, A1-P1, A1-P2, A2-D1	**A1-P1** Overall L(E)RF for the site for all events and hazards
Low Level	INST# – the identifier of a specific installation, and (TYPE) – type of the safety goal	The ID created at the previous level is amended by the relevant ID of the current level composed of an ID of the specific installation at the site and the ID characterizing the specific type of safety goals, e.g.: A1-P1-INST1(LERF), A1-P1-INST1(CDF), A2-D1-INST1(Fuel Clad T)	**A2-P1-INST1(LRF)** Probabilistic criterion for LRF for Installation #1 on the site **A2-P1-INST1(CDF)** Probabilistic criterion for core damage frequency for Installation #1 on the site.

TABLE 4. AN ILLUSTRATIVE EXAMPLE OF HIERARCHY OF SAFETY GOALS FOR NUCLEAR APPLICATIONS

<table>
<tr><td colspan="10"><u>TOP LEVEL</u> - PRIMARY SAFETY GOAL:

To protect people and the environment from harmful effects of ionizing radiation</td></tr>
<tr><td colspan="10"><u>UPPER LEVEL</u> SAFETY GOALS – ADEQUATE PROTECTION:

Ensuring adequate protection of all facilities and installations at the site</td></tr>
<tr><td colspan="4">Operational States</td><td colspan="6">Accident Conditions</td></tr>
<tr><td colspan="2">O1

RADIATION PROTECTION

To protect workers, the public and the environment</td><td>O2

SECURITY

To provide design features for security</td><td>O3

RADWASTE MINIMIZATION
To minimize radioactive waste</td><td>O4

PROVISIONS FOR

DECOMMISSIONING

To provide design features to facilitate decommissioning</td><td colspan="2">A1

LOW RISK TO PEOPLE’S LIFE AND HEALTH

Risk to life and health of people from the facilities and installations located at the site should be low comparing with risk from other sources to which an individual is generally exposed</td><td colspan="2">A2

LOW RISK TO THE ENVIRONMENT

Large off-site releases leading to land interdiction should extremely unlikely</td><td>A3

SAFETY-SECURITY INTERFACE

Safety-security interface should be addressed</td><td>A4

EMERGENCY RESPONSE

Emergency response should be provided</td></tr>
<tr><td colspan="10"><u>INTERMEDIATE LEVEL</u> SAFETY GOALS – GENERAL SAFETY PROVISIONS:

Providing general safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection</td></tr>
<tr><td><u>Qualitative</u>

O1-Q1

Management, leadership and safety culture</td><td><u>Deterministic quantitative</u>

O1-D1

Meeting ICRP criteria for workers by providing adequate radiation protection measures</td><td>…</td><td>…</td><td>…</td><td><u>Qualitative</u>

A1-Q1

Maintaining effective defence-in-depth</td><td><u>Deterministic quantitative</u>

A1-D1

Maintaining allowed doses for workers in DBAs</td><td><u>Probabilistic quantitative</u>

A1-P1

Overall L(E)RF for the site for all events and hazards</td><td><u>Qualitative</u>

A2-Q1

Providing effective SAM design features and SAMG at the site level</td><td><u>Probabilistic quantitative</u>

A2-P1

Very low likelihood of early or large releases</td><td>A3-Q1

Vital area identification at the site level</td><td>A4-Q1

Detailed emergency plan</td></tr>
</table>

TABLE 4. AN ILLUSTRATIVE EXAMPLE OF HIERARCHY OF SAFETY GOALS FOR NUCLEAR APPLICATIONS (cont.)

<u>INTERMEDIATE LEVEL</u> SAFETY GOALS – GENERAL SAFETY PROVISIONS: *Providing general safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection*											
	O1-D2 Meeting ICRP criteria for discharges to the environment by providing adequate measures for controlling discharges				**A1-Q2** Maintaining sufficient safety margins	**A1-D2** Maintaining allowed discharges to the environment in DBAs	**A1-P2** Frequencies of external hazards/ magnitudes for design of site protective features		**A2-P2** Food ban radioactivity levels and accepted frequency	**A3-Q2** Providing security measures in compliance with safety needs at the site level	**A4-D1** Food ban levels
					A1-Q3 Providing sufficient redundancy and diversity to comply with single failure criterion	**A1-D3** Containment withstanding the crash of a specified size aircraft			**A2-P3** Habitation radioactivity levels and accepted frequency		**A4-D2** Habitation radioactivity levels
<u>LOW LEVEL</u> SAFETY GOALS – SPECIFIC SAFETY PROVISIONS: *Providing specific safety provisions for each facility and installation at the site to ensure adequate protection*											
…	…	…	…	…	<u>Deterministic quantitative (A1-Q2)</u> • Maximum fuel clad temp. (D1): **A1-Q2-INST1(D1)** – for inst. #1 **A1-Q2-INST2(D1)** – for inst. #2 • Maximum coolant pressure (D2): **A1-Q2-INST1(D2)** – for inst. #1 **A1-Q2-INST2(D2)** – for inst. #2 <u>Deterministic quantitative (A1-Q3)</u> • 3 trains of safety systems required: **A1-Q3-INST1, A1-Q3-INST2** …	<u>Probabilistic quantitative (A1-P1)</u> • LERF for each inst.: **A1-P1-INST1(LERF)** **A1-P1-INST2(LERF)** • Supplemental goals on CDF as applicable: **A1-P1-INST1(CDF)** **A1-P1-INST2(CDF)** • Instantaneous risk limit: …	<u>Qualitative (A2-Q1)</u> • Providing effective SAM design measures and SAMG at facility level: **A2-Q1-INST1(SAMG)** **A2-Q1-INST2(SAMG)** …	…	<u>Qualitative (A3-Q1)</u> • Vital area at facility level: **A3-Q1-INST1** **A3-Q1-INST2** <u>Qualitative (A3-Q2)</u> • Security measures at facility level: **A3-Q2-INST1** **A3-Q2-INST2** …	…

4. APPLICATIONS OF A HIERARCHY OF SAFETY GOALS

4.1. INTRODUCTORY REMARKS

As described in previous sections, the hierarchical structure of safety goals provides an approach for developing a structured set of requirements and criteria to support establishing safety during all life cycles of nuclear installations. It promotes a consistent approach to safety so that each facility, of whatever technology, will be required to demonstrate an acceptable degree of safety. In this section, some practical uses of the hierarchy of safety goals are discussed under the following aspects:

1) Compliance assessment: Assessing whether the overall objectives of safety goals are met through assessment of safety cases and on-site inspection;

2) Regulatory and Licensee applications: Consideration of how safety goals can assist in providing assurance of safe design and operational activities, to maintain the required level of safety;

3) Interfacing with Integrated Risk-Informed Decision Making (***IRIDM***) process for regulatory and non-regulatory purposes.

In addition, communication aspects between various stakeholders involved in nuclear safety are discussed.

4.2. COMPLIANCE ASSESSMENT

Safety goals are set to achieve an acceptable level of safety, but it is important that a way to demonstrate they are being met exists, hence they recognise the way in which safety assessment and verification will be carried out. This is partly the driver for developing a hierarchy of safety goals as the higher level goals are difficult to demonstrate directly. By developing supporting lower level goals which are more technical or operational the process of demonstration can be achieved more easily.

Safety of a complex facility or activity requires a range of hazards and risks to be considered. All safety aspects are important. It is necessary to consider the set of factors, at any one level, that contribute to meeting the requirements at a higher level. The general approach for assessing compliance with the hierarchical structure of safety goals is a bottom up process.

In considering the safety of a facility or activity, an assessment of compliance of the design and operations with the safety goals is carried out by the licensee to determine the necessary actions to maintain safety. Regulatory decisions on the adequacy of the safety of the facility or activity will be based on a review of the licensee's assessment. The purpose of developing the hierarchical structure of safety goals is to provide the basis for determining whether adequate safety has been established. The process may be based on qualitative and quantitative considerations. Compliance assessment is expected to take into account the uncertainties associated with safety goals.

4.2.1. Compliance with top level and upper level safety goals

Nuclear safety is generally governed by qualitative safety goals set at the level of the effects on society. Top Level qualitative safety goals are usually defined in the relevant national

legislation or approved by nuclear regulatory authorities. It is not expected that licensees are required to demonstrate compliance directly at these levels.

4.2.2. Compliance with intermediate level safety goals

Upper Level safety goals are refined into a set of Intermediate Level qualitative and quantitative safety goals, which are focussed on proven approaches and good practices including overall site requirements. This set of safety goals allows explicit assessment of compliance of a site's safety performance. Demonstrating compliance with the relevant set of Intermediate Level safety goals ensures compliance with the higher level goals.

Generally, demonstration of compliance at this level is provided by the licensee when seeking approval or renewing an operating licence from the regulatory body. Where necessary, these goals may have to be developed into more technically specific Low Level goals.

4.2.3. Compliance with low level safety goals

Low Level safety goals are usually defined in terms of a specific technology or facility design-related requirements. Technology specific safety goals are related to safety objectives of SSCs, and are partially defined in national and international industrial standards, or national and international nuclear safety standards. Depending on the specific topic, the assessment of meeting nuclear safety standards could be performed by reviewing the underlying quality management processes including activities related to safety assessment and design review.

Compliance with many Low Level safety goals requires the use of analytical techniques (e.g. thermal hydraulic analysis or PSA). These analyses are to be carried out by the licensee and used in the safety management of the facility or activity. The compliance assessment is reviewed by the regulatory body. As technology specific safety goals may be adjusted during the life-cycle phases of a nuclear installation, the quantitative values may change, especially when modifications are implemented. In these cases, more refined safety analyses may be necessary to show compliance with the established quantitative safety goals.

In assessing compliance with technology specific safety goals, there is a need to consider the specific goals for each type of nuclear installation. For each type of installation, the technology specific goals are determined by considering the specific harm that can occur in case of an abnormal situation and, are in general, expected to be quantitative in nature.

4.2.4. Compliance with quantitative safety goals

Quantitative safety goals are defined mainly on the lower levels of the hierarchical structure of safety goals. Examples of quantitative values that can be subject to safety goals are probability/frequency figures for various types of risks or conditions that may result in risk (core damage frequency, barrier strength, release frequencies etc.) and requirements related to different plant states.

Demonstrating compliance with quantitative safety goals is in principle straightforward. It typically involves either deterministic or probabilistic analysis, i.e. a numerical value derived by measurement, analysis, or calculation, is compared to a safety goal which is also expressed numerically. In defining quantitative safety goals, it is also important to define the procedure and assumptions used for the calculations. In practice, compliance assessment needs to provide assurance of basic fulfilment of the safety goal (e.g. comparison of best estimate values or mean

values to the safety goal value) as well as demonstrating robustness. The latter is achieved by taking into consideration various kinds of uncertainties.

For multi-facility sites, compliance with quantitative probabilistic safety goals are expected to be demonstrated by consideration of the risk from individual facilities coupled, where appropriate, with consideration of events that may affect multiple facilities on the site.

4.2.5. Compliance with qualitative safety goals

Demonstrating compliance with qualitative safety goals is not as straightforward as for quantitative safety goals. Concepts such as, effective DiD features, operating procedures including Severe Accident Management Guidelines (SAMG), radioactive waste management policies, and overall requirements for management of safety are important factors. These concepts describe generally accepted practices that, when followed, permit nuclear sites to meet the qualitative safety goals. Assessment of compliance with these goals may be achieved by a review of the licensee's safety analysis, including organisational safety policies that have been established.

Where there are multiple facilities on a site, compliance with qualitative safety goals are expected to consider effects involving incidents or accidents at more than one facility at the same time, to ensure that sufficient equipment and other resources are available.

4.2.6. Trade-off and integrated compliance

In considering safety goals, particularly at an older nuclear facility or site, it is possible that not all the individual safety goals may be fully met. Three possible levels of compliance can be generally defined:

1) Enhanced compliance – where the safety goal is exceeded;

2) Compliance – where the safety goal is fully met;

3) Partial (or reduced) compliance – where the safety goal is not fully met.

It may be possible to compensate for those safety goals where there is reduced compliance by considering whether other safety goals in the same area for which there is an enhanced level of compliance can compensate for a reduced compliance on one safety goal. The consideration of the overall hierarchy of safety goals allows the trade-off to be considered in a consistent manner so that the higher level safety goals can be shown to be complied with. However, it is important to note that any failure to fully comply with a specific safety goal is expected to be considered carefully and certain safety goals must be fully complied with, if they are mandatory requirements. This aspect is dealt in a more comprehensive way in the IRIDM process (see Sub-section 4.4).

4.3. REGULATORY AND LICENSEE APPLICATIONS

This sub-section presents an overview of possible regulatory and licensee applications of safety goals at nuclear facilities. The use of a hierarchical structure of safety goals could be used for informing safety decisions helping to provide confidence to stakeholders, including the public, that safety management is being properly implemented and assured.

It is not the intention here to describe the detailed application of safety goals, but to provide insights on some examples of how a hierarchical structure of safety goals can be used in design and operational activities.

4.3.1. Application of safety goals in design

Once established, the hierarchy of safety goals can be used in the design process of a facility or for considering later design modifications. The hierarchy of safety goals, as an intrinsic part of the design approach, also allows engineering, management and quality assurance processes to be used in demonstrating compliance with safety goal requirements. Some safety goals related to operations may not have been developed at this stage but must be in place before active commissioning (i.e. after introduction of nuclear or radioactive materials).

4.3.2. Application of safety goals during operations

A hierarchical structure of safety goals may facilitate optimisation of operational activities in a number of key areas, such as:

- Operating limits and conditions
- Control of modifications
- Maintenance planning
- Site wide considerations for multi-facility sites
- Emergency preparedness
- Periodic safety review

4.3.2.1. Operating limits and conditions

Operating limits and conditions (OLCs) are defined to ensure the facility is operated in accordance with its design assumptions and intent. Safety goals can be used to support development of the scope and content of the OLCs through, amongst others, engineering requirements, safety analysis, and operational considerations. OLCs are defined for different normal operational modes (e.g., full power, or shutdown modes), and consider effective control of short term risk due to equipment unavailability. The hierarchical structure of safety goals can assist in determining how to handle these situations, e.g. supporting the development of allowed outage times addressing the requirement to control risk increase due to equipment unavailability.

4.3.2.2. Control of modifications

When undertaking modifications to the facility or operational procedures during its lifecycle, safety goals can be used for ensuring that safety is maintained. The modification process (e.g. engineering change control) is expected to consider safety goals in the same way as during the initial design process. This is a rigorous process to address the risks expected from the as-built, as-commissioned and as-operated facility. The consideration of the safety goals in a modification process allows efficient identification of appropriate design features and operating practices to meet the safety requirements.

4.3.2.3. Maintenance planning

Effective maintenance of all SSCs ensures that they meet the functional and reliability requirements to perform their intended functions when required. Safety goals can be used to assist in planning maintenance activities to ensure that safety is maintained when SSCs important to safety are taken out of service. For example, Low Level safety goals formulated as numerical risk metrics (see Sections 4 and 5) can be used as thresholds to ensure that planned maintenance configurations during normal facility operation do not pose unacceptable risks.

4.3.2.4. Site-wide considerations for multi-facility sites

In a hierarchy of safety goals, the identification of safety requirements for a site and the individual facilities on the site allows better understanding of the relative risk posed by each of these facilities. This ensures that the risk of all planned operations at all facilities does not exceed the overall site safety goals. This understanding also provides an informed perspective to facilitate better planning of future developments on the site.

4.3.2.5. Emergency preparedness

The emergency preparedness programme for a nuclear site provides guidance aimed at effective and efficient response to an event with significant off site consequences. The structure of safety goals can provide the basis for developing this programme by setting both high level societal goals and detailed technology requirements. In particular, if a site consists of several facilities, which may be of a diverse nature (e.g. a laboratory complex), the structure of safety goals provides the overarching site requirements as well as the specific lower level goals for each facility in a consistent manner. An understanding of the relative risks posed by the different facilities on a site will allow the emergency preparedness programme to better prioritise and coordinate the deployment of site-wide resources to manage internal and external events affecting multiple facilities.

4.3.2.6. Periodic safety review

When a periodic safety review (PSR) is performed, the safety goals can be used as a baseline, against which to review the current safety provisions and past operating performance. The review of the current safety provisions will indicate whether modifications to the facility or operational procedures are meeting the existing standards which may have changed since the previous safety assessment.

Consideration of the facility performance provides insights on the degree of deviation, if any, from the baseline safety performance. The PSR findings could be used to improve future safety provisions and performance and, therefore, maintain the requirements in the structure of safety goals.

4.4. USE OF SAFETY GOALS IN INTEGRATED RISK INFORMED DECISION MAKING

The use of safety goals in the context of an integrated risk informed decision making (IRIDM) process has evolved over time in several countries (e.g., United States, United Kingdom). An IRIDM process is more effective when combined with a structured hierarchy of safety goals. An IAEA TECDOC on the IRIDM process [10] is currently under preparation based on the framework provided in INSAG-25 [11].

The main goal of the IRIDM process is to define the most balanced decision among several possible options by considering different key elements (e.g. mandatory requirements, deterministic, probabilistic, economical, security considerations). One of the major factors that has to be taken into consideration in the IRIDM process (typically falling in the mandatory requirements considerations) is the level of compliance with existing safety goals.

The safety goals determine a hierarchy in which the Top and Upper Level goals are those that are met to satisfy the protection of society and the Intermediate and Low Levels provide detailed ways to achieve this objective. All these lower level goals can contribute to meeting the higher level goals and can be considered in making a risk-informed decision.

The weighted approach employed in the IRIDM process allows assignment of different importance to the specific levels of safety goals being considered in the decision making.

4.5. SAFETY COMMUNICATION

4.5.1. Communication between the regulatory body and the public

The role of the nuclear safety regulatory body is to regulate activities for the safe operation of nuclear facilities on behalf of the public. Although the nuclear safety regulatory body informs the licensees of all safety concerns through normal communication means, timely communications to legislators as representatives of the public and to the general public are extremely important to assure public confidence on nuclear safety.

IAEA has developed guidance [12] on communications with interested parties. This guidance notes that: “The regulatory body should routinely make as much information as possible available to the public relating to safety, including the radioactive risks associated with facilities and activities, and its independent role to protect people and the environment from harmful effects of ionizing radiation, its responsibilities and activities.” Decision making mechanisms may vary considerably from country to country, depending on cultural aspects, history, government philosophy as well as legal and organisational factors. For the establishment of processes for information and participation, there are factors, such as cultural prerequisites, international conventions, legal frameworks and institutional systems that are expected to be taken into account as they may make the practical activities, even when resting on the same basic principles, quite different between different countries and different situations. There is no ideal or prototypical best practice. Instead ‘best practice’ or rather ‘good practice’ might be nationally or even locally defined to a great extent, given that it fits within an overall regulatory structure.

IAEA recommends [12] that all countries should create and implement instruments that enhance transparency, openness and participation of the interested parties considering the guidance provided by [12]. In this context, the use of safety goals could be an invaluable aid to developing understanding the way in which the risks from ionising radiation are being managed.

4.5.2. Communication between the regulatory body and the licensee/licence applicant

The initial licensing of a nuclear facility, requires the applicant to submit a licence application, which has to meet the regulatory requirements: these may be prescriptive or goal-setting. However, the ultimate responsibility for safety rests upon the licensee to effectively implement all safety requirements. As such, the licensee needs to understand the regulatory requirements to be complied with and how they assure that the higher level safety goals are achieved.

In a prescriptive regime, the regulatory body may also set the lower level goals for the licence application. The structure of safety goals may help demonstrate to the licensee that the goals are both necessary and sufficient to assure safety. In a goal-setting regime, the licensee may be responsible for defining the lower level requirements. Therefore, the structure of safety goals provides an important tool to demonstrate that the lower level goals will satisfy the higher level goals.

4.5.3. Communication between the operating organisation and the public

Communicating the safety goals of the operating organisation to the public in an open, transparent and understandable manner is a key element to enhancing public confidence in nuclear power plant operation. This process cannot be divorced from the communications between the regulatory body and the general public because the regulatory body is seen as an independent arbiter. The operators have to demonstrate that their standards are high and that safety is the overriding priority. Given the complexities of the technologies involved and the potential impacts on the public acceptance of nuclear facility operation, safety goals provide a structure which can demonstrate:

- An adequate level of safety in terms that are understandable and meaningful to the public (the Top and Upper Level goals can assist this);

- A structure for implementation at the technical level which gives confidence that all elements of safety provision are adequately covered.

5. CONCLUDING REMARKS

This TECDOC discusses development and application of a hierarchical structure of safety goals encompassing high level goals and detailed technical requirements that may assist in forming a coherent and consistent approach to nuclear safety. The suggested hierarchy of safety goals provides a practical approach to consistently embrace the set of safety-related requirements, both qualitative and quantitative, and develop the interconnections between them. Specifically, the structure supports adding country-specific safety goals (e.g. risk metrics) to the overall safety considerations in a consistent manner. This process can be aided by reference to the IAEA Safety Standards.

The formalised hierarchy of safety requirements concentrating on technical aspects and design provisions for safety can be applied to a wide range of nuclear installations and multiple-facility sites, covering operational and accidental conditions of the installations. The structure starts from the overarching requirements for safety, that are detailed further in a hierarchical top-down way. A description of the structure and the general features of safety goals at various levels within the suggested four-level hierarchy have been provided. Examples are also presented to illustrate how to derive the detailed safety goals. In addition, compliance assessment and applications of safety goals, including their use within an integrated risk informed decision making process, are outlined.

The hierarchy of safety goals described in this TECDOC considered approaches in several Member States, international organizations and expert groups. The suggested structure has been developed during a series of Consultants Meetings and was discussed at two IAEA Technical Meetings.

The following use of the hierarchical structure of safety goals described in this TECDOC is anticipated:

- For countries which are in the beginning of development of their nuclear power programmes, the approach described in this TECDOC may assist in developing a consistent and coherent view of the safety goals to be pursued.
- For countries with developed nuclear power programmes, this TECDOC may be useful in benchmarking the existing safety goals for consistency and coherence in covering all aspects important to nuclear safety.

In addition, application of the proposed hierarchy of safety goals may provide support in effective communication on the topic of nuclear safety between utility organizations, regulatory authorities and the public.

REFERENCES

[1] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSR Part 4 (Rev. 1), IAEA, Vienna (2016).

[3] EUROPEAN COMMISSION, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Radiation Protection and Safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards Series No. GSR Part 3, IAEA, Vienna (2014).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 (Rev.1), IAEA, Vienna (2016).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna (2009).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Defence in Depth in Nuclear Safety, INSAG-10, A Report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1996).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide SSG-3, IAEA, Vienna (2010).

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide SSG-4, IAEA, Vienna (2010).

[9] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles for Nuclear Power Plants 75-INSAG-3 Rev. 1, INSAG-12, A Report by the International Nuclear Safety Advisory Group, IAEA, Vienna (1999).

[10] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance on Performing Integrated Risk Informed Decision Making, IAEA-TECDOC-XXXX, IAEA, Vienna (in preparation).

[11] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for an Integrated Risk Informed Decision Making Process, IAEA; INSAG-25, IAEA, Vienna (2011).

[12] INTERNATIONAL ATOMIC ENERGY AGENCY, Communication and Consultation with Interested Parties by the Regulatory Body, IAEA Safety Standards Series No.GSG-6, IAEA, Vienna (2017).

ANNEX I. SAFETY GOALS FOR NUCLEAR INSTALLATIONS IN CANADA

I-1. INTRODUCTION

I-1.1. Historical perspective on risk

In Canada, risk concepts have been utilized from the very inception of the nuclear power program with a view to better understand the significance of safety issues, identify potential design weaknesses, and achieve improvements in nuclear safety.

As early as 1957, a numerical frequency ***limit*** of 10-5 per year was proposed for the likelihood of a nuclear accident that might result in significant public health impact on the basis that such an accident should be a factor of five less likely than loss of life due to other forms of electricity production such as coal-fired plants [I-1]. This figure was used to derive reliability requirements for control and safety systems, which were then utilized to guide the design of the 20 MWe Nuclear Power Demonstration (NPD) reactor placed in operation in 1962.

With the prospect of larger power reactors on the horizon in the 1960s, the Atomic Energy Control Board (AECB), now the Canadian Nuclear Safety Commission (CNSC), developed rules for the licensing of power reactors, known as the Siting Guide. The effectiveness of safety systems was required to be such that for any (single) serious process failure requiring safety system action, the exposure of any individual of the population would not exceed 500 milli-rem (5mSv) and of the population at risk 104 person-rem. Further, for any postulated combination of a process failure and failure of a safety system, the predicted dose to any individual was not to exceed 25 rem (250 mSv) whole body, 250 rem (2500 mSv) thyroid, and to the population 106 person-rem. These came to be called the single failure / dual failure criteria of reactor licensing. Even though the criteria did not require a quantitative assessment of public risk, their risk roots are unmistakable.

I-1.2. Safety goals for nuclear power plants

As discussed above, the earliest commercial nuclear plant design approach in Canada recognized the need to establish acceptable levels of risk relative to that of other industries. The drive for formal safety goals came from the increasing use of PSA and the desire to define what constitutes an acceptable level of risk. With the evolution of IAEA guidance on PSA, the CNSC developed Regulatory Standard S-294 [I-2], in 2005, to provide high level requirements for Level 1 and Level 2 PSA development in Canada, following which all utilities were expected to upgrade their probabilistic assessments as part of their licensing basis. Although S-294 does not specify quantitative safety goals as a regulatory requirement for existing nuclear power plants (NPPs), Regulatory Document RD-337 [I-3] specifies quantitative safety goals for new builds (see below). Further, all utilities in Canada have defined quantitative safety goals for their existing nuclear plants (see below). It should be noted that, since the accident at Fukushima Daiichi, the CNSC is re-examining the regulatory framework to strengthen requirements based on lessons learned. In that light, S-294 has been re-examined as part of omnibus regulatory changes, and lessons learned have been formally included in REGDOC 2.4.2 approved by the Commission on March 27, 2014.

I-1.2.1. Safety goals for new builds

The Regulatory Document RD-337 [I-3] for new builds places a limit on the societal risks posed by nuclear power plant operation. For this purpose, the following two qualitative safety goals have been established:

1. Individual members of the public are provided a level of protection from the consequences of nuclear power plant operation such that there is no significant additional risk to the life and health of individuals; and

2. Societal risks to life and health from nuclear power plant operation are comparable to or less than the risks of generating electricity by viable competing technologies, and should not significantly add to other societal risks.

Due to their very general statements, qualitative safety goals need to be translated into numerical objectives that can be compared with experience and with analytical predictions, i.e., for implementation.

RD-337 [I-3] identifies that for practical application, quantitative safety goals are established to achieve the intent of the qualitative safety goals. RD-337 [I-3] defines the quantitative safety goals for new builds as shown in Table I-1.

TABLE I-1. QUANTITATIVE SAFETY GOALS FOR NEW BUILDS (PER UNIT)

Metric	Frequency (/yr)	Description
Core Damage	1E-05	Sum of frequencies from all event sequences that can lead to significant core degradation
Small Release	1E-05	Sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{15} becquerel of I-131. A greater release may require temporary evacuation of the local population.
Large Release	1E-06	Sum of frequencies of all event sequences that can lead to a release to the environment of more than 10^{14} becquerel of Cs-137. The principle concern is the prevention of long-term land contamination where a greater release may require long term relocation of the local population.

In setting the above safety goals, the CNSC considered experience from the Three-Mile Island and Chernobyl accidents which demonstrated that the effect of nuclear accidents on the health of the public and on the environment is not limited to the radiological health effects, and that accidents can have indirect psycho-somatic effects on the population and direct effects on their life when ground is so contaminated that permanent relocation of towns and industry is required [I-4]. The same experience applies very well to the Fukushima accident. Although SRF is not common in other jurisdictions, the CNSC rationale for introducing the SRF is that in CANDU reactors, some accident scenarios may result in limited core damage, leading to small releases which can result in severe disruption of public life (these accidents require emergency measures such as sheltering or short term evacuation of an area around the plant) [I-4]. In summary, the RD-337 [I-3] safety goals (i.e., the threshold release values) were based primarily on the conditions that would trigger evacuation and permanent relocation.

I-1.2.2. Safety goals for existing NPPs

This section discusses safety goals for existing plants from the perspective of both the average and instantaneous risk. In 1990, Ontario Hydro (now Ontario Power Generation) established a set of safety goals to be used in conjunction with its PSAs to judge safety adequacy of its plants. Targets and limits for risk to an individual living in the vicinity of a nuclear facility of early or delayed fatality were developed, as was a societal risk goal in the form of the frequency of a large release that could lead to the long-term (months) evacuation of a considerable number of local residents and the need for decontamination or long-term abandonment of local land and buildings.

The basis for these safety goals was the principle that the risk to a member of the public from the operation of nuclear plants should not be more than 1% of the accident risk to which he/she is normally exposed. For the US-NRC, it is 0.1% of other risks for the average member of the public, while in the Canadian documents, it is 1% of the other risks for the individual most at risk.

The Ontario Hydro goals were put in place initially on a trial basis to gain some experience with their use. Subsequent utility and CNSC initiatives provided the basis for the present day set of industry safety goals at the three Canadian utilities that continue to operate nuclear power plants, i.e., Ontario Power Generation, Bruce Power and New Brunswick Power. The regulatory safety goals for new plants and industry's safety goals for the existing plants have similar consequence definitions but the frequency goals for existing plants are an order of magnitude less stringent.

Small Release Frequency (SRF) is generally not utilized by Canadian utilities in their safety goals for existing nuclear power plants as the majority of failures contributing to SRF are already embodied within estimates of Large Release Frequency [I-5]. However, the utilities are evaluating the SRFs and providing the information to the CNSC.

Latent effects (i.e. frequency of late and early fatalities) are generally not included in utility safety goals. Given that these are PSA Level 3 measures, there is no requirement (explicit or implicit) derived from Regulatory Standard S-294 [I-2] that necessitates the calculation of this safety goal. In the Canadian regulatory environment, the safety goals for limiting societal risk are qualitative in nature. Moreover, the latent effects safety goals have not been widely adopted by nuclear safety organizations around the world, by regulators and utilities [I-6]. A practical reason is that Level 3 measures are associated with inherently higher uncertainties than Level 2 measures.

While there is some variability amongst Canadian nuclear utilities on their established safety goals, Table I-2 shows the common safety goals that apply to each Canadian utility[5].

[5] Individual Canadian utilities may choose, for business reasons or otherwise, to define additional safety goals.

TABLE I-2. AVERAGE SAFETY GOALS PER UNIT

Safety Goal	Average Risk (per year)	
	Target	Limit
Large Release Frequency (LRF)	10^{-6}	10^{-5}
Severe Core Damage Frequency (SCDF)	10^{-5}	10^{-4}

The above safety goals are consistent with IAEA INSAG-12, which is referenced in SSG-3 [I-7].

The safety goal *limit* represents the limit of tolerability of risk exposure above which action shall be taken to reduce risk. The safety goal *target* represents the desired objective towards which the facility should strive, provided that measures to further reduce risk are cost effective, such as when benefits are comparable to, or greater than, the cost of implementing the measure.

The safety goals pertaining to Severe Core Damage are intended to help the nuclear facilities make routine decisions relating to changes in plant operation, configuration or procedures. For proposed changes significantly affecting the integrity of containment, either directly or through crosslink, a further assessment against the Large Release safety goal is required.

Risk based safety goals apply to estimated risk averaged over time, typically one year. This implies that it is permissible for risk to exceed the limit for a short period of time provided that risk increase is controlled, assessed and limited. As such, to ensure that reasonable bounds are placed on the allowable short-term risk, instantaneous limits have also been defined.

I-1.3. Safety goals for non-NPP installations

Within Canada there exist non NPP nuclear installations. The largest and most complex of which is Chalk River Laboratories (CRL), located approximately 200 kilometres north west of Ottawa in the Province of Ontario. It is a multi-facility site unique within Canada where operations are of a heterogeneous nature. There are no common facilities on site although certain elements of the infrastructure are shared, e.g. fire protection, radiation protection, power supply etc. This poses challenges as the site cannot really be compared to a multi-unit homogeneous site, such as a NPP, where two or more identical units may occupy the one site.

I-1.3.1. Safety goals for new build research reactors

Regulatory Document (RD) 367 [I-8] is entitled “Design of Small Reactor Facilities” and sets both qualitative and quantitative safety goals for new build research reactors and these are reproduced below.

Qualitative safety goals

A limit is placed on the societal risks posed by reactor facility operation. For this purpose, the following two qualitative safety goals have been established:

> 1. Individual members of the public are provided a level of protection from the consequences of reactor facility operation such that there is no significant additional risk to the life and health of individuals; and

2. Societal risks to life and health from reactor facility operation should not significantly add to other societal risks.

Due to their very general statements, qualitative safety goals are not directly enforceable. Therefore, they have to be translated into numerical objectives that can be compared with experience and with analytical predictions.

Quantitative safety goals

RD-367 [I-8] identifies that for practical application, quantitative safety goals are established to achieve the intent of the qualitative safety goals. Three quantitative safety goals are:

1. Core damage frequency[6];
2. Small release frequency; and
3. Large release frequency

A core damage accident results from a postulated initiating event followed by failure of one or more safety system(s) or safety support system(s). Core damage frequency is a measure of the plant's accident preventive capabilities. Small release frequency and large release frequency are measures of the plant's accident mitigative capabilities. They also represent measures of risk to society and to the environment due to the operation of a research reactor.

RD-367 [I-8] defines the quantitative safety goals for new build research reactors as shown in Table I-3.

TABLE I-3. QUANTITATIVE SAFETY GOALS FOR NEW BUILD RESEARCH REACTORS

Metric	Frequency (/yr)	Description
Core Damage	1E-05	Sum of frequencies from all event sequences that can lead to significant core degradation.
Small Release	1E-05	Sum of frequencies of all event sequences, whose release to the environment requires temporary evacuation of the local population.
Large Release	1E-06	Sum of frequencies of all event sequences, whose release to the environment requires long term relocation of the local population.

At the CRL site only two of the 16 facilities listed in the site licence are research reactors. The other 14 facilities either use, process or store nuclear substances that is not in a fissionable state but also pose risk. Thus for the majority of the facilities at CRL, the CDF safety goal of 10^{-5} per reactor year as stated in RD-367 [I-8] would not be applicable.

[6] In Canada the term Core Damage Frequency (CDF) is interpreted to mean Severe Core Damage Frequency (SCDF)

I-1.3.2. Safety goals for existing non-NPP installations

The existing CRL site license makes a number of references to the use of safety goals as a means to managing safety on site. However, it is stated that these are only one method that the licensee may adopt and as such few definitive goals are given. What is stated is very much at the high level and of a qualitative nature such as the licensee's responsibility to protect people and the environment from harmful effects of ionizing radiation as taken from the Nuclear Safety and Control Act [I-9]. Reference is also made to a number of IAEA guidance documents. Within Canada it is the responsibility of the licensee to demonstrate safety. It is left up to the licensee to develop a set of safety goals should they wish to do so.

The majority of safety analysis conducted at the CRL is based on deterministic arguments such as the defence-in-depth principle since PSA's do not exist for all but one of the facilities on site.

Examples of existing safety goals for non-NPP installations

The following safety goals are taken from the current CRL site license:

- For satisfying the requirement applied to long-term effects, the frequency of a large release of typically 10^{15} Bq of Cs-137 should not exceed 10^{-6} per year. The combined fall-out consisting of nuclides, other than cesium-isotopes, shall not cause, in the long term, starting three months from the accident, a hazard greater than would arise from a cesium release corresponding to the above-mentioned limit.
- The upper sub-critical limits established in the criticality safety documents will not be exceeded under both normal and credible abnormal conditions (events or event sequences having the frequency of occurrence equal to or more than 10^{-6} per year) during operations with fissionable materials outside reactors.
- The dose limits in Table I-4, written into the CRL licence, are taken from the Radiation Protection Regulations [I-10].

These criteria refer to the committed whole-body dose for average members of the critical groups who are most at risk, at or beyond the site boundary, as calculated in the deterministic safety analysis, for a period of 30 days after the analyzed event.

TABLE I-4 DOSE LIMITS TAKEN FROM THE RADIATION PROTECTION REGULATIONS

	Normal Operation[7]	**AOO**[8]	**DBA**[9]
Dose	The design shall be such that during normal operation, including maintenance and decommissioning, doses are controlled to remain below the limits prescribed in the Radiation Protection Regulations. In addition, radiation doses to the public and to site personnel shall be As Low As Reasonably Achievable (ALARA).	0.5 mSv	20 mSv

I-1.4. System-level risk management

To provide assurance that proactive measures are taken prior to safety goal limits being exceeded, Canada applies a concept where reliability of risk-significant systems (i.e. systems important to safety) is managed and controlled within system-specific targets that are derived from the PSA. The regulatory requirements for utility reliability programs are embodied in regulatory document RD/GD-98 [I-11]. From a high level perspective, the Canadian industry has adopted a concept where the reliability of a system important to safety is set at about 120% of the nominal reliability included in the PSA. However, on a case by case basis deviation from this approach is permissible provided the proposed methodology is accepted by the CNSC.

In each case it is necessary to ensure that system-level reliability targets do not become "moving targets" during periodic PSA re-quantification as required by Regulatory Standard S-294 [I-2]. Therefore, in addition to establishing system reliability targets, the Canadian industry also provides the following information in annual reliability reports submitted to the CNSC:

1. Component failure rate trends for systems important to safety
2. Comparative system-level reliability indices including both predicted and observed reliability relative to derived system targets
3. Operational performance including any impairments of the system that may have occurred
4. Changes that were made to design and operation of the systems including any changes to PSA models
5. Comparative initiating event frequency indices relative to the frequency used in PSA.

[7] Operation within specified operational limits and conditions.

[8] An operational process deviating from normal operation which is expected to occur at least once during the operating lifetime of a facility but which, in view of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

[9] Accident conditions against which a facility is designed according to established design criteria, and for which the damage to the fuel and the release of radioactive material are kept within authorized limits.

I-1.5. Recent developments

PSA safety goals have been set and analyzed as one method of demonstrating reactor safety, within the safety goal concept of "how safe is safe enough". However, the conventional manner by which safety goals are treated in current practice is based on application of the safety goals for a single NPP, although certain multi-unit interactions may have been accounted for (in multi-unit CANDU PSAs, for instance). To date, safety goals are commonly defined on a "per reactor year" basis.

In past years, and again recently in Canada (especially in light of Fukushima lessons learned), consideration has been given to the development of more comprehensive, site-based PSA methodologies that address the aggregation of risks across multiple reactor units, other on-site radiological sources (i.e., spent fuel pools), different hazard types (internal and external, such as seismic, fire, flood, high wind, etc.), and various NPP operating modes. Thus far, these aspects have not been explicitly included within safety goal definitions or in the manner by which the safety goals are implemented. At present, there is no international consensus on these long-standing issues.

It is important to note that risks are not fully quantifiable via PSA, and that PSA is often applied in such a manner as to introduce conservative biases that tend to yield overestimations of the actual risk. A comprehensive approach to whole-site risk characterization and assessment should therefore not be solely based on PSA methods, rather, other complementary methods should be employed as well to address uncertainties and omissions.

Moreover, beyond these analytical/assessment type of methods, there are a myriad of programmatic activities and defence-in-depth principles that assure NPP risks are maintained acceptably low. In the grander scheme of nuclear safety assurance, PSA represents one of multiple lower-tier supporting elements of an overall safety goals hierarchal framework. The sub-sections below discuss the *preliminary* Canadian nuclear *industry* perspective on the concept of a safety goals hierarchy and its relation to risk management.

I-1.5.1. Concept of safety goals framework

There is general international consensus that achieving the overall Safety Objective and the ten Safety Principles articulated in the IAEA's Fundamental Safety Principles document [I-13] requires a hierarchy of safety goals, rather than one single safety goal or quantified value. The concept of a hierarchical framework of safety goals is discussed in the main body of the IAEA TECDOC.

The basic notion is that, collectively, the set of safety goals and their supporting elements serve to assure that an acceptable level of safety is provided and that the overall safety objective is met, namely, the protection of the life and health of the public. It is noted that safety goals may be qualitative or quantitative in nature. Furthermore, the term "goals" is synonymous with "criteria", "objectives", or "targets", and exceeding any one does not necessarily mean that the high-level health objectives are not met.

Consistent with these international activities, the Canadian nuclear industry has proposed to develop a hierarchal framework of safety goals that is an adaptation of the more generic framework proposed by other international agencies or groups. Conceptually, as depicted in Figure I-1, the proposed safety goals framework is structured into four levels along with suggested objectives, principles, and elements. The sample shown below is for illustrative purposes only; it is preliminary in nature and not exhaustively detailed, however, it serves to

introduce the concept and offers some suggested possible elements of such a framework. Further detailed development and rationalization of the elements and their logical linkages are proposed to be conducted as part of future work.

Following is a brief and preliminary discussion of the various levels of safety goals and the suggested possible descriptions, including supporting elements.

Top level safety goal

The top level safety goal is a qualitative statement of the fundamental health objective such as articulated in the IAEA Fundamental Safety Principles document, namely:

"*The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation."*

The focus in the Canadian nuclear industry initiative is on protection of life and health of the public. However, it is recognized that protection of the environment is also important; this issue is normally addressed in the Environmental Assessment process.

Upper level safety goals

At the second level in the hierarchy, a set of safety goals are defined that, in a semi-quantitative manner, further characterize the health objectives. Another important objective at this level relates to the practical elimination of extensive social disruption due to off-site releases of radioactive materials.

A major purpose of the safety goals at this level is to facilitate risk communication that supports risk-informed decision-making at senior levels in the CNSC, the licensees and ultimately the Commission members, and potentially the public. This decision-making is a process of deliberation that is in accordance with the Oxford dictionary definition of the term, viz. "*long and careful consideration or discussion*" and is similar to that described in the US NRC document NUREG-2150 [I-12].

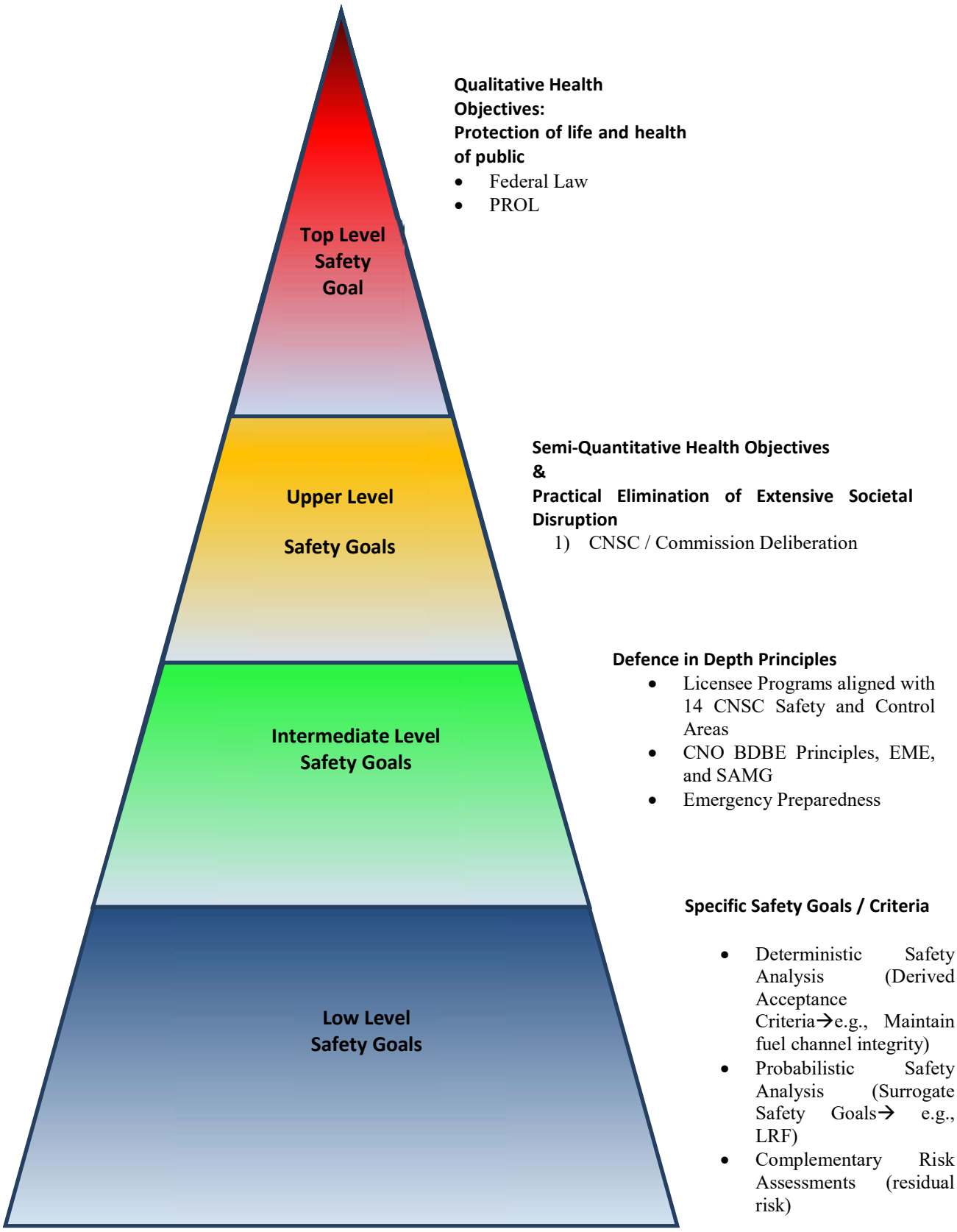

FIG. I-1. *Preliminary Concept-Level Safety Goals Framework.*

Intermediate level safety goals

The third level safety goals are focused on programs, measures and actions that provide defence in depth for design basis events and for events that may progress beyond the design basis. The principles that guide the safety goals at this level in the hierarchy relate broadly to risk management and, as such, are action-oriented. For example:

- aligning licensee programs with the 14 CNSC Safety and Control Areas (SCA);
- aligning with the 14 safety factors articulated in the IAEA periodic safety review process (IAEA SSG-25);
- aligning safety goals with the licensee Chief Nuclear Officer (CNO) principles for addressing Beyond Design Basis Events (BDBEs);
- provision and deployment of Emergency Mitigation Equipment (EME) to prevent accident progression to BDBEs, or to help mitigate BDBEs should they occur;
- implementation of Severe Accident Management Guidelines (SAMG), and;
- implementation of an Emergency Preparedness program.

The action-oriented elements include comprehensive maintenance and testing programs, rigorous training and qualification of personnel, proven procedures and procedural adherence, periodic self-assessments, audits, and continual improvement. This helps to support fostering of a healthy nuclear safety culture, backed up by (deterministic and probabilistic) safety analysis, severe accident management guidelines and emergency preparedness, demonstrated by periodic drills. All of the above processes are managed through an integrated management system, and reflected in operating licenses and subjected to periodic regulatory evaluation. Such regulatory evaluations by the CNSC include the performance of licensee programs in 14 SCAs, namely: Management system, Human performance management, Operating performance, Safety analysis, Physical design, Fitness for service, Radiation protection, Conventional health and safety, Environmental protection, Emergency management and fire protection, Waste management, Security, Safeguards and non-proliferation, and Packaging and transport. Programs aligned with the SCAs are an integral part of a conceptual safety goals framework that assures adequate protection of public health and safety.

Defense-in-depth principles particular to beyond design basis events are further captured in principles stated by the Canadian utilities' senior executives, whereby, in recognition of the high level of public interest and concern following the Fukushima accident, the Canadian nuclear utilities developed a set of principles to guide their response and reassure the public. The Chief Nuclear Officers and Chief Nuclear Engineers have formally committed to these principles, where the objective is to: "practically eliminate the potential for societal disruption due to a nuclear incident by maintaining multiple and flexible barriers to severe event progression". The means by which this objective is met (e.g., via the diverse use of portable emergency mitigation equipment to provide fuel cooling and containment protection) is also an integral part of a conceptual safety goals framework.

Low level safety goals

The fourth level in the hierarchy consists of a set of specific quantitative safety goals and criteria which include those that have been traditionally employed in deterministic safety analysis and probabilistic safety analysis. These goals are focused on risk characterization and analysis. For example, they include:

- Acceptance criteria applied in deterministic safety analysis to meet regulatory requirements and define the Safe Operating Envelope (SOE);
- Surrogate safety goals used in PSA: and
- Application of complementary risk assessment methods that systematically address in either a semi-quantitative or qualitative manner the contributors to residual risk that are difficult to capture in PSA.

In summary of the basic idea, it is the licensee that predominantly works in the intermediate and lower levels of the safety goals framework. Collectively, the qualitative (action-oriented) elements of the intermediate level, together with the low-level specific (quantitative) goals and criteria, support the case that the top-level health objectives are met. This safety case is not solely based on numerical values, rather it needs to take into consideration the robustness of the plant design and operation, as founded on defence-in-depth principles, as well as uncertainties and mitigating factors. The Regulator generally works in the top and upper levels to make licensing decisions, based on the above and the licensee's input that stems from the elements of the intermediate and lower levels of the safety goals framework. The Regulator establishes the safety goals at the higher levels, and the licensee’s objective is to meet them.

Further work is needed to develop the hierarchy of safety goals and the details and relative positioning of all of the key supporting elements (generic and site-specific) as well as the logical linking between goals at each of the different levels.

I-1.5.2. Site safety goals

The primary focus of site-based safety goals should be the protection of the life and health of the public, and that by also focusing on limiting the potential for extensive long-term relocation (as a major form of societal disruption and more stringent consequence goal), the public health risk can be limited to within acceptable levels. To this end, the prevention of long-lived radionuclide releases is a very important objective for protecting the public since these releases can result in unacceptable, long-term contamination of the land surrounding the plant. This view is consistent with the Canadian utilities’ CNO/CNE principles that were established post-Fukushima. Furthermore, consideration of the release of I-131 to account for early effects is also important. Moreover, while focusing on protection of human health, in so doing the potential environmental impacts due to nuclear accidents are also covered to a large extent. On this basis, qualitative safety goals for a NPP site have been proposed by industry [I-1].

To implement these, a quantitative definition of the site safety goals is necessary, at a lower level, so as to facilitate a numerical evaluation and comparison of some form, e.g., via PSA. Quantitative site-based safety goals have been proposed [I-1] by industry for use at the lower level; these include release-based and core-damage based goals expressed in generalized notation.

The release-based safety goal involves evaluations of both the frequency and consequences of radiological accidents that lead to off-site radioactive releases. As such, quantitatively, the site safety goal is evaluated based on results from Level 2 PSA and dose dispersion analysis (where required). The key terms (parameters) in the general quantitative safety goal definition must be determined such that the top-level safety goal is met, i.e., the qualitative health objectives, whilst also supporting the upper-level goal for practical elimination of extensive societal disruption.

Supplementary to the frequency calculation for the safety goal evaluation, a consequence assessment should be considered to *confirm* that the main intent of the upper-level qualitative safety goal has been met, taking into account the full radionuclide mix of releases. The confirmatory assessment is meant to check that smaller releases (below the release threshold value) indeed do not result in "extensive" societal disruption, i.e., no extensive long-term relocation as well as a check for no extensive/widespread temporary evacuation.

Key considerations

Targets vs. Limits

The treatment of very low likelihood hazards in PSA often requires use of simplifying models and assumptions that can result in conservative estimates of the risk from these sources. This, coupled with the fact that NPP risks are not always fully quantifiable via PSA (e.g. due to some factors as incompleteness of knowledge, lack of data), suggests that PSA numerical results must be carefully interpreted when comparing them against quantitative safety goals. In this context, and considering the role of other supporting elements within the overall safety goals framework, it is not considered appropriate to impose hard "limits" for safety goals defined in the lower tier. Instead, utilities should strive to meet "targets" (consistent with the notion of safety "goals"), whether for single-unit NPP sites or multi-unit sites. Historically, plants have been licensed based on deterministic defence-in-depth provisions, and PSA has been used to augment insights concerning design vulnerabilities, not as the sole and hard measure of the safety of the plant. PSA provides an indicator of risk, not a measure of risk.

Limits are more appropriate in the context of design basis accidents – "for which the damage to the fuel and the release of radioactive material are kept within authorized limits" (CNSC RD-310). *Goals* (or targets) are used in the context of beyond design basis accidents, the analysis for which, e.g., via PSA – "shall be performed as part of the safety assessment to demonstrate that:

1) The nuclear power plant as designed can meet the established safety goals; and

2) The accident management program and design provisions, put in place to handle the accident management needs, are effective." (CNSC RD-310)

Nevertheless, utilities would still need to have programmatic guidance in place to take action if the computed safety goal is exceeded. This could include an examination to better understand the insights generated in the PSA, including sources of potential conservatism and/or possible improvements to the design and operation of the plant.

Risk aggregation

Risk Aggregation refers to the process whereby risk metrics (i.e., SCDF, LRF) calculated using PSA for various hazards, plant states and multiple units, are combined together to generate a value for the site as a whole. Factors to consider in performing such an aggregation are that: a) there appears to be an international consensus that risk aggregation for the purposes of comparison with site safety goals should include the risks from all hazards, sources of radioactivity and all phases of plant operation that have the potential to exceed the LRF release threshold, b) significant technical issues have been identified in the simple addition of contributions from these disparate risk contributors, and c) it appears that simple addition would

receive widespread acceptance if PSAs for different hazards were of comparable maturity and level of uncertainty.

A number of options have been identified by the Canadian nuclear industry [I-1]. It is considered prudent to further explore the viability of these options in concert with ongoing international efforts (i.e., by the IAEA, EPRI, etc.). Additional work is necessary to further develop and support risk aggregation concepts. Once there is widely-accepted guidance on site risk aggregation methods, then whole-site risk estimation can be pursued.

I-1.6. Summary

This annex identifies how safety goals are defined and applied in Canada for nuclear installations. Average safety goal targets and limits have been established as a "measuring stick" to determine if station design, operation and maintenance practices fall within international guidelines for existing nuclear power plants, and to propose and rank modifications to reduce risk estimates. Overall, average risk is managed at the system level through application of reliability targets based on PSA for systems identified important to safety. Further, a decision-making process has been developed when goals or limits are exceeded.

As a recent development in Canada, greater interest and consideration is being given to whole-site risk assessment and site-based safety goal definitions within the context of a hierarchal safety goals framework. As well, the topic of whether/how to aggregate risks across different hazard types (internal and external hazards) is being explored. Canada is taking a lead role in these areas, working in consultation with the broader PSA community at both the industry and regulatory levels.

Acknowledgment

This annex contains text that has been largely extracted, either verbatim or modified, from References [I-1] and [I-5].

REFERENCES TO ANNEX I

[I-1] VECCHIARELLI, J., DINNIE, K., and LUXAT, J., Development of a Whole-Site PSA Methodology, COG report no. COG-13-9034 R0, Ontario (2014).

[I-2] CANADIAN NUCLEAR SAFETY COMMISSION, Regulatory Standard S-294, Probabilistic Safety Assessment (PSA) for Nuclear Power Plants, Ottawa (2005).

[I-3] CANADIAN NUCLEAR SAFETY COMMISSION, Regulatory Document RD-337, Design of New Nuclear Power Plants, Ottawa (2008).

[I-4] CANADIAN NUCLEAR SAFETY COMMISSION, E-DOCS-#3336969-v1, Staff Position on Safety Goals, Ottawa (2007).

[I-5] D. MULLIN et al., Application of Safety Goals in Canada, IAEA Technical Meeting on Development and Application of Safety Goals Framework for Nuclear Installations, Vienna (2013).

[I-6] NUCLEAR ENERGY AGENCY, NEA/CSNI/R(2009)16, Probabilistic Risk Criteria and Safety Goals, Committee on the Safety of Nuclear Installations, Paris (2009).

[I-7] INTERNATIONAL ATOMIC ENERGY AGENCY, Specific Safety Guide No. SSG-3, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Vienna (2010).

[I-8] CANADIAN NUCLEAR SAFETY COMMISSION, Design of Small Reactor Facilities, RD 367, Ottawa (2011).

[I-9] MINISTER OF JUSTICE CANADA, Nuclear Safety and Control Act, S.C. 1997, c.9, Ottawa (2012).

[I-10] MINISTER OF JUSTICE CANADA, Radiation Protection Regulations, SOR/2000-203, Ottawa (2007).

[I-11] CANADIAN NUCLEAR SAFETY COMMISSION, Regulatory Document RD/GD-98, Reliability Programs for Nuclear Power Plants, Ottawa (2012).

[I-12] NUCLEAR REGULATORY COMMISSION, A Proposed Risk Management Regulatory Framework, NUREG 2150, Washington, DC (2012).

[I-13] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

ANNEX II. APPLICATION OF THE PROPOSED SAFETY GOALS FRAMEWORK TO THE GERMAN REGULATORY FRAMEWORK FOR NUCLEAR POWER PLANTS

II-1. INTRODUCTION

In the past, the safety concept of nuclear power plants as well as licensing and supervising decisions by the competent authorities and their experts in the Federal Republic of Germany were mainly based on deterministic principles. Safety-related decision-making during design and licensing has essentially been based on the verification of compliance with the German regulations pre-describing technical requirements as laid down, e.g., in the German nuclear safety standards.

A probabilistic safety assessment has been essentially performed in the framework of the periodic safety reviews as a supplement to the deterministic safety analysis. Currently, no specific probabilistic quantitative safety goals for nuclear power plants or other nuclear facilities and no site-wide safety goals are determined within the German regulatory framework. However, a recent document requires that modifications of measures, equipment or the operating mode of a nuclear power plant, compared with the unchanged condition of this plant, must not lead to an increase in the average core damage frequency and the average frequency of large and early releases, neither for full power operation nor for low-power and shutdown states, considering all plant-internal events as well as all internal and external hazards as well as very rare man-made external hazards.

II-2. CURRENT GERMAN SAFETY REQUIREMENTS FOR NUCLEAR POWER PLANTS

The German nuclear regulatory framework has been elaborated over a long time period consisting of the Atomic Energy Act (AtG) [II-1], ordinances such the Radiation Protection Ordinance (RPO) [II-2], regulatory guidelines such as Guidelines for Periodic Safety Reviews and a Guide for the Decommissioning, the Safe Enclosure and the Dismantling of Facilities as well as guidelines and recommendations of the German Reactor Safety Commission (RSK).

Detailed technical requirements are laid down in about 100 German nuclear safety standards (KTA safety standards), elaborated by German experts from authorities, technical support organizations, utilities and vendors, issued by the German Nuclear Safety Standards Commission and announced by the Federal Ministry for the Environment, Nature Conservation and Nuclear Safety in the Federal Gazette.

Recently, the "Safety requirements for nuclear power plants" [II-3] have been issued containing fundamental and general safety-related requirements within the framework of the non-mandatory safety standards and rules that provide more details regarding the required precaution that – pursuant to § 7 para. 2 no. 3 of the AtG – is necessary according to the state of the art in science and technology in order to prevent any damage caused by the construction and operation of a nuclear power plant. As far as necessary from a safety-related point of view, document [I-2-3] shall also be applied to nuclear power plants that pursuant to § 7 (1a) AtG have had their power operating licences revoked or which due to a decision taken by the licensee are in their post-operational phase.

This new regulatory document is now part of the German regulatory framework as shown in Figure II-1. Requirements for physical protection are not included in [II-3], but provided

separately. A further document [II-4] is issued to enable the uniform enforcement of these requirements.

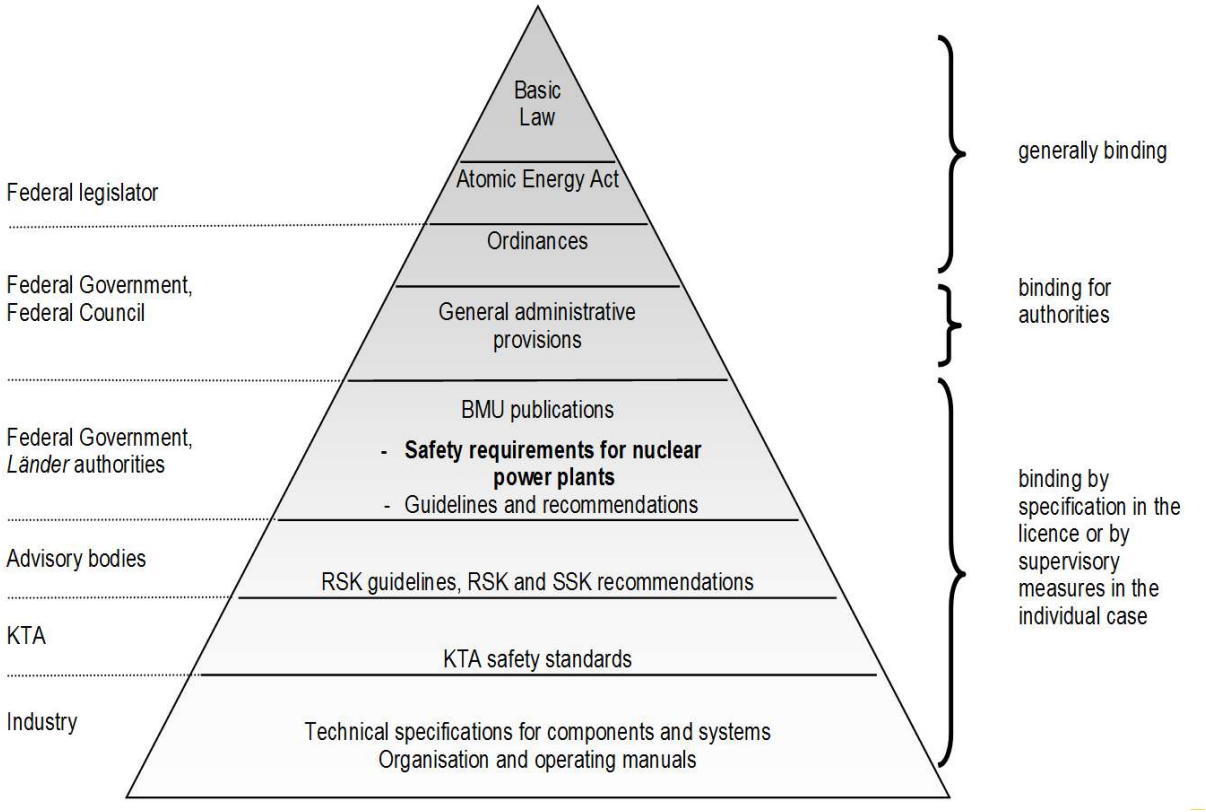

FIG. II-1. German regulatory framework.

II-3. SAFETY GOALS IN GERMAN REGULATIONS

Because the regulatory framework in Germany is very prescriptive compared to other countries like the UK, specific safety goals are also provided in each level of the German regulatory framework. Moreover, technical and radiological safety goals are formulated for all level of defence in depth for all operational states, accident conditions and beyond design basis conditions.

In the German Atomic Energy Act [II-1] it is stated in the first paragraph that the aim of the act is to protect life, health and real assets against the hazards of nuclear energy and the harmful effects of ionising radiation and to provide compensation for damage and injuries caused by nuclear energy or ionising radiation. Moreover, it is stated that the purpose of this act is to prevent danger to the internal or external security of the Federal Republic of Germany from the application or release of nuclear energy or ionising radiation.

§ 7d of [II-1] requires that the holder of a licence to operate an installation for the fission of nuclear fuel for commercial electricity production shall provide the realisation of safety measures according to the ongoing state-of-the-art of science and technology which are developed, suitable and adequate for providing not only an insignificant contribution to further precaution against risks for the public.

The purpose of the Radiation Protection Ordinance [II-2] is to regulate principles and requirements of preventive and protective measures which apply to the use and effects of man-

made and naturally occurring radioactive substances and ionizing radiation in order to protect man and the environment from the harmful effects of ionizing radiation.

The fundamental safety objective in [II-3] is the protection of man and environment against the harmful effects of ionising radiation. Guidelines for the assessment of the design of nuclear power plants are provided in [II-3] and the correspondent spectra of incidents have originally been defined in the Radiation Protection Ordinance [II-2].

Those events, which are relevant concerning their radiological impacts and against which precautions must be taken in terms of engineered safeguards or countermeasures are defined in [II-3] for nuclear power plants. For these events it must be demonstrated by means of computational analyses that the requirements specified in [II-3] are met. Especially, it has to be demonstrated that the safety-related acceptance targets and acceptance criteria applicable to the different levels of defence in depth are achieved and maintained for these events.

For defined events whose occurrence can be prevented by special measures and equipment – in the following referred to as precautionary measures – it shall be demonstrated that the requirements for the effectiveness and reliability of these precautionary measures are fulfilled. For these events computational analysis is only required if it cannot be demonstrated that the specified precautionary measures have been met. The verifications of fulfilment of the acceptance criteria shall consider the assignment of load levels of the reactor coolant pressure boundary, the systems outside the primary circuit and the containment, presented in [II-3] to the events included in the event lists.

The confinement of the radioactive materials present in the nuclear power plant shall be ensured. In order to achieve this safety goal, a safety concept shall be implemented in which measures and equipment are allocated to different levels of defence in depth (DiD) [II-3]:

- Level of DiD 1: normal operation (specified normal operation)
- Level of DiD 2: anticipated operational occurrences (specified normal operation, incident)
- Level of DiD 3: accidents
- Level of DiD 4a: very rare events
- Level of DiD 4b: events involving the multiple failure of safety equipment
- Level of DiD 4c: accidents involving severe fuel assembly damages.

Recently, the German Reactor Safety Commission described its understanding of safety philosophy including orientation values for the four levels of defence in depth [II-5].

Furthermore, additional measures and equipment to identify and limit the consequences of plant conditions that are not allocated to the abovementioned levels of defence 1 – 4a due to their low probability of occurrence shall be provided to an adequate extent as a precaution. Therefore, measures and equipment of the internal accident management shall be provided and planned in supplement on levels of defence 4b and 4c of the defence in depth concept. Therefore, a safety goal on the intermediate level, e. g, is to maintain effective defence in depth.

A further safety goal is to provide effective features to support the external accident management in order to assess the consequences of accidents for accidents involving severe fuel assembly damages with potential or actually occurred releases of nuclear materials into the environment and to mitigate as far as possible their effects on man and the environment.

All equipment that is necessary for shutting the reactor down safely, for maintaining it in shutdown condition, for removing the residual heat or for preventing a release of radioactive materials shall be designed and maintained in such a condition that they fulfil their safety-related functions even in the case of internal and external hazards as well as very rare man-made external hazards.

Radiological safety goals are set for the different levels of defence in depth:

- On levels of DiD 1 and 2

    - radiation exposure of the personnel shall be kept as low as achievable for all activities, even below the limits of the Radiation Protection Ordinance, taking into account all circumstances of each individual case,

    - any discharge of radioactive materials with air or water shall be controlled via the specially provided discharge paths; the discharges shall be monitored as well as documented and specified according to their kind and activity, and

    - any radiation exposure or contamination of man and the environment by direct radiation from the plant as well as by the discharge of radioactive materials shall be kept as low as achievable, even below the limits of the Radiation Protection Ordinance, taking into account all circumstances of each individual case.

- On level of DiD 3

    - the maximum radiation exposure limits for the personnel in connection with the planning of activities for the control of events, the mitigation of their effects or the removal of their consequences shall not exceed the relevant limits of the Radiation Protection Ordinance,

    - the maximum design limits for the plant for protecting the population against any release-induced radiation exposure shall not exceed the relevant accident planning levels of the Radiation Protection Ordinance,

    - any release shall only happen via specially provided release paths; the release shall be monitored and shall be documented and specified according to its kind and activity; and

    - the on-site and off-side radiological consequences shall be kept as low as possible, taking into account all circumstances of each individual case.

- On level of DiD 4

    - the planning of activities to control events of level of defence 4a as well as for the planning of activities in connection with internal accident management measures shall be based the relevant requirements of the Radiation Protection Ordinance regarding the anticipated radiation exposure of the personnel,

- the monitoring of releases of radioactive materials from the plant according to their kind and activity shall be ensured and

- the on-site and off-side radiological consequences shall be kept as low as possible,

Taking into account the measures and equipment for the internal accident management provided on levels of DiD 4b and 4c,

- any releases of radioactive materials into the environment of the plant, caused by the early failure or bypass of the containment and requiring measures of the external accident management for the implementation of which there is not sufficient time available (early release), or

- any releases of radioactive materials into the environment of the plant requiring wide-area and long-lasting measures of the external accident management (large release)

- shall be excluded, or their radiological consequences shall be limited to such an extent that measures of the external accident management will only be required to a limited spatial and temporal extent. The occurrence of an event or event sequence or a state can be considered as excluded if it is physically impossible to occur or if it can be considered with a high degree of confidence to be extremely unlikely to arise.

Moreover, intervention reference levels are set in [II-6] for

- Sheltering: 10 mSv from external exposure in seven days and effective dose commitment resulting from radionuclides inhaled during this period.

- Evacuation: 100 mSv from external exposure in seven days and effective dose commitment due to the radionuclides inhaled during this period.

- Temporary resettlement: 30 mSv external exposure in one month,

- Long-term resettlement: 100 mSv external exposure in one year due to deposited radionuclides.

With regards to intervention in supplies of foodstuffs for the population, a distinction is made between (precautionary) warning of the population against eating freshly harvested foods and fresh milk on the one hand, and intervention in supplies of food-stuffs and feeding stuff on the basis of maximum contamination levels on the other. The warning to the population is issued in the area surrounding an emission source no later than the beginning of a hazardous release or in unclear radiological situations, or in more distant areas in the event of substantial radionuclide concentrations in the air. The maximum radioactivity levels in foodstuffs and feeding stuff in the event of a nuclear accident are laid down in EU regulations.

As prerequisite for the limitation of radiation exposure of the general public and of discharges of radioactive substances (see Table II-1 below), general technical safety goals are described in [II-3] to ensure sufficient reliability of the equipment of level of defence 3 (safety equipment) such as providing sufficient redundancy, diversity, segregation and physical separation of

redundant subsystems, and automation (i.e. not requiring operator actions within 30 minutes after an initiating event).

The safety equipment necessary for the control of events on level of defence 3 shall be available redundantly and segregated in such a way that the safety functions necessary for controlling events are still sufficiently effective if it is postulated that, in the event of their required function,

- a single failure of a safety equipment with the most unfavourable effects occurs due to a random failure, and

- there is at the same time an unavailability of a safety equipment due to maintenance measures with the most unfavourable effects in combination with a single failure.

Single failures are generally postulated for active as well as for passive equipment, exceptions shall be justified.

According to [II-3] specific requirements for the protection against internal and external hazards as well as very rare man-made external hazards have to be fulfilled, among others the following specified requirements: A design basis earthquake and the associated impacts shall be determined for the site under investigation based on site-specific deterministic and probabilistic seismic hazard analyses. For the determination of the seismic engineering parameters of the design basis earthquake, the intensity and, corresponding to the associated seismo-tectonic conditions, the range of magnitudes, distances and focal depths of the earthquake shall be indicated. Irrespective of any site specific hazard analysis, the design shall at least be based on the intensity VI EMS (European Macroseismic Scale).

A further intermediate level safety goal is to ensure that the safety of the plant is not inadmissibly impaired by an aircraft crash. The design shall be based on the load assumptions provided in [II-3] describing the impact-load time diagram, impact area and impact angle.

Suitable protection measures and equipment shall ensure that postulated plant external explosions do not inadmissibly impair the safety of the plant. Apart from chemical explosions, explosions of vapour, gas or liquid clouds, deflagration-to-detonation transition and physical explosions shall be considered. For the structural design, the pressure time diagram according to the guideline for the protection of nuclear power plants against pressure blast waves from chemical explosions [II-7] shall be postulated, unless there are indications of higher pressure time curves to be expected.

The goal to maintain the integrated management system and to maintain and enhance safety culture is addressed in [II-3].

Typical deterministic examples for deterministic low level safety goals which have to be fulfilled are:

- No critical boiling at cladding tube or maintenance of an appropriate temperature-time criterion of the cladding tube,

- Cladding tube temperature < 1200 °C or

- Amount of shutdown reactivity.

The recently issued German safety requirements for nuclear power plants [II-3] extend the use of probabilistic safety assessment to supplement deterministic safety demonstrations to assess the safety significance in case:

- of modifications of measures, equipment or the operating mode of the plant, as well as
- of findings that have become known from safety-relevant events or phenomena that have occurred and which can be applied to the nuclear power plants in Germany that are referred to in the scope of application of the "Safety Requirements for Nuclear Power Plants"

for which a significant influence of the results of the PSA can be expected.

Compared with the unchanged condition of the plant, modifications of measures, equipment or the operating mode of the plant must not lead to an increase in the average core damage frequency and the average frequency of large and early releases, neither for power operation nor for low-power and shutdown states, considering all plant-internal events as well as all internal and external hazards as well as very rare man-made external hazards.

Comparison with the unchanged condition refers to the actual core damage frequency evaluated within the (periodic) safety review of the respective plant. If the unchanged condition was not modelled in the safety review, the unchanged condition as well as the planned modification has to be analysed and compared.

In the following, as a detailed example for low-level safety goals, the procedure in case of storage and handling of fuel assemblies and associated items in nuclear power plants with light water reactors is given. Table II-1 below shows as an example the safety-related acceptance targets and criteria for fuel element storage and handling according to [II-3].

According to [II-3] criteria for the handling and storage of the fuel elements are provided. On levels of DiD 1 to 4a, the control of reactivity during fuel element storage is ensured for all operating phases. Measures and installations for the handling and storage of non-irradiated and irradiated nuclear fuel are provided such that a criticality event in the storage facilities is not to be postulated even under accident conditions or events on the level of DiD 4a. Fuel cooling (heat removal from the facilities for the storage of fuel elements) is ensured on levels of DiD 1 to 4a. The general criteria for the handling and storage of fuel elements in a nuclear power plant for level of DiD 1 are described in [II-3].

As preventive accident management measures according to [II-3] it is necessary to demonstrate the effectiveness of the accident management measures for cooling of the fuel elements in the fuel pool for the representative event sequences considered if the fuel elements are covered with coolant and measures for maintenance or restoration of the required sub-criticality of the fuel elements in the fuel pool is demonstrated for the representative event sequences if long-term sub-criticality of $k_{eff} < 0.999$.

TABLE II-1. SAFETY-RELATED ACCEPTANCE TARGETS AND CRITERIA OF LEVEL OF DEFENCE IN DEPTH 2 TO 4A FOR FUEL ELEMENT STORAGE AND HANDLING [II-3]

Level of defence in depth	**Anticipated operational occurrences (2)**	**Accidents (3)**	**Very rare events (4a)**
Protection goal	control of reactivity		
Acceptance target	ensuring sub-criticality		
Acceptance criterion: neutron multiplication factor k_{eff}	< 0.95	< 0.95; for special events < 0.98	< 0.99
Protection goal	cooling of the fuel elements		
Acceptance targets	(1) Limitation of the pool water temperatures to values which ensure accessibility of the pool area with customary measures (2) Sufficient water coverage for ensuring the required inlet condition for the pool pumps	(1) Limitation of the pool water temperatures to values below the design temperature of the pool (2) Sufficient water coverage for ensuring fuel element cooling	(1) Limitation of the pool water temperatures to values which ensure pool integrity (2) Sufficient water coverage for ensuring spill or evaporation cooling (maintenance of fuel rod integrity)
Protection goal	confinement of radioactive material		
Acceptance targets	(1) see criteria for fuel element cooling (2) maintenance of the retention functions of buildings and systems		

TABLE II-1. SAFETY-RELATED ACCEPTANCE TARGETS AND CRITERIA OF LEVEL OF DEFENCE IN DEPTH 2 TO 4A FOR FUEL ELEMENT STORAGE AND HANDLING [II-3] (cont.)

Level of defence in depth	Anticipated operational occurrences (2)	Accidents (3)	Very rare events (4a)
Acceptance criteria	Compliance with the limit values according to §§ 46, 47 RPO (per one calendar year) (1) Limitation of radiation exposure of the general public (a) 1 mSv (b) eye lens 15 mSv; skin 50 mSv (2) Limitation of the discharge of radioactive substances (a) limits of the radiation exposure of individual members of the general public: effective dose 0.3 mSv; (b) organ specific absorbed doses, e.g. for gonads, uterus, bone marrow (red) 0.3 mSv	Compliance with the accident planning levels according to § 49 RPO (1) Safety-related design for the operation of NPP for the proximate storage of irradiated fuel elements and for Federal facilities for the safeguarding and final disposal of radioactive waste an effective dose of 50 mSv, organ specific absorbed doses, e.g., for the gonads, uterus and bone marrow (red) of 50 mSv each.	-

II-4. APPLICATION OF THE PROPOSED SAFETY GOALS FRAMEWORK

This annex was primarily aimed at tentatively applying the proposed safety goals framework on the situation in Germany, taking into consideration mainly laws and regulations.

Table II-2 provides the application of the safety goals framework proposed in this TECDOC. The top level, upper level and part of the intermediate level safety goals like the radiological limits could in general also be applied to other nuclear installations than nuclear power plants. However, the safety goals, exemplary illustrated in Table II-2, are focussed on German nuclear power plants because they are explicitly described in the several documents within the German regulatory framework.

As can be seen from Figure II-2 [II-8], there is only one site in Germany with three nuclear power plants where two of them are still in operation and one site in Eastern Germany with five nuclear power plants, all of them are shutdown since 1990.

At all other sites only one nuclear power plant is operating or only one plant has been built; a further nuclear installation is only an intermediate storage facility for the spent fuel, sometimes separated by its own fence.

The number of further nuclear installations in Germany is limited: one facility for production of fuel elements for light water reactors, one enrichment plant, one pilot conditioning plant and two centralized interim storage facilities. Only the pilot conditioning plant and one centralized interim storage facility are at one site.

Different types of nuclear installations are only at the two research centres in Germany with research reactors (already shutdown) and with operating facilities for conditioning of radioactive waste and its storage. The still operating research reactors are gain at sites without any other nuclear installation.

Therefore, most of the intermediate level safety goals and the low level safety goals are only formulated exemplary for nuclear power plants. Moreover, no site-wide safety goals have been developed.

It is important to recognise that the application was not aimed to be complete. In particular, a large set of low level safety goals exists.

However, it can be illustrated from Table II-2 how the German safety goals can be integrated in the safety goals framework as proposed in Section 4 of this TECDOC.

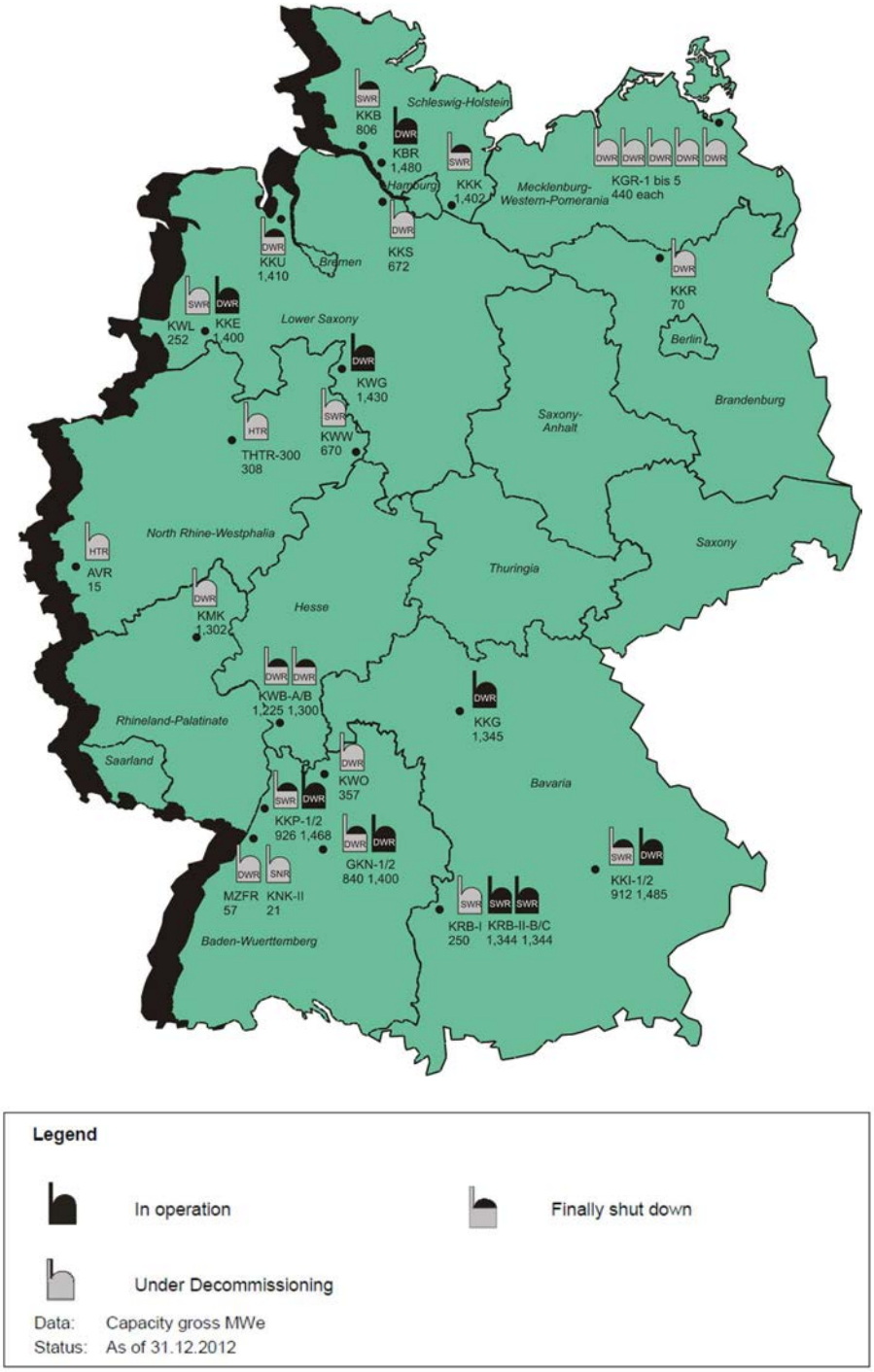

FIG II-2. Location of nuclear power plants in Germany.

TABLE II-2. SAFETY GOALS FOR NUCLEAR INSTALLATIONS WITH MAIN FOCUS ON NUCLEAR POWER PLANTS

<table>
<tr><td colspan="11"><u>TOP LEVEL</u> - PRIMARY SAFETY GOAL: To protect people and the environment from harmful effects of ionizing radiation</td></tr>
<tr><td colspan="11"><u>UPPER LEVEL</u> SAFETY GOALS: Ensuring adequate protection in the nuclear installations</td></tr>
<tr><td colspan="5">Operational states</td><td colspan="6">Accident conditions</td></tr>
<tr><td colspan="2">O1

RADIATION ROTECTION

To protect workers, the public and the environment</td><td>O2

SECURITY

To provide design features for security</td><td>O3

RADWASTE

To avoid or reduce radioactive waste</td><td>O4

DECOMMI SSIONING

To provide design features to facilitate decommis-sioning</td><td colspan="3">A1

LOW RISK TO PEOPLE’S LIFE AND HEALTH

Reducing risk to life and health of people from nuclear installations</td><td colspan="2">A2

LOW RISK TO THE ENVIRONMENT

Any early or large releases of radioactive materials into the environment of the plant shall be excluded, or their radiological consequences limited to such an extent that measures of the external AM will only be required for a limited spatial and temporal extent</td><td>A2

SAFETY-SECURITY INTERFACE

Safety-security interface should be addressed</td><td>A4

EMERGENCY RESPONSE

Emergency response should be provided</td></tr>
<tr><td colspan="11"><u>INTERMEDIATE LEVEL</u> SAFETY GOALS: Providing necessary safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection</td></tr>
<tr><td><u>Qualitative</u>

O1-Q1

Maintain integrated management system and safety culture</td><td><u>Deterministic quantitative</u>

O1-D1

Meet radiological criteria for workers by providing adequate radiation protection measures</td><td>…</td><td>… …</td><td>…</td><td><u>Qualitative</u>

A1-Q1

Maintain effective defence-in-depth</td><td><u>Deterministic quantitative</u>

A1-D1

Maintain allowed doses for workers in design basis accidents</td><td><u>Probabilistic quantitative</u>

A1-P1

Verify the balance of the safety-related design by probabilistic safety analyses</td><td><u>Qualitative</u>

<u>A2-Q1</u>

Provide effective SAMG</td><td><u>Deterministic quantitative</u>

<u>A2-D1</u>

Food ban radioactivity levels</td><td></td><td>A4-Q1

Provide detailed emergency plan</td></tr>
</table>

TABLE II-2. SAFETY GOALS FOR NUCLEAR INSTALLATIONS WITH MAIN FOCUS ON NUCLEAR POWER PLANTS (cont.)

INTERMEDIATE LEVEL SAFETY GOALS: *Providing necessary safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection*											
	O1-D2 Meet radiological criteria for discharges to the environment by providing adequate measures for controlling the discharges				**A1-Q2** Maintain sufficient safety margins	**A1-D2** Maintaining allowed discharges to the environment in design basis accidents s	**A1-P2** Assess the safety significance of plant modifications and findings by probabilistic analyses for which a significant influence can be expected		**A2-D2** Evacuation radioactivity levels		
					A1-Q3 Provide sufficient redundancy and diversity to comply with single failure criterion	**A1-D3** Containment withstanding an aircraft crash according to a specified impact-load-time diagram	**A1-P3** Plant modifications must not lead to an increase of the core damage frequency		**A2-D3** Habitation radioactivity levels		
						A1-D4 Frequencies of external hazards/ magnitudes for design of site protective features	**A1-P4** Plant modifications must not lead to an increase of L(E)RF				

TABLE II-2. SAFETY GOALS FOR NUCLEAR INSTALLATIONS WITH MAIN FOCUS ON NUCLEAR POWER PLANTS (cont.)

LOW LEVEL SAFETY GOALS: *Providing necessary specific safety provisions*									
				Deterministic quantitative **A1-D1** Nuclear and thermo hydraulic design parameters of the reactor core, such as maximal fuel clad temperature and oxidation depth, fuel rod damage extent	Probabilistic quantitative **A1-P1** Criteria for the assessment of the balance of the safety-related design	Qualitative **A2-Q1-** Provide effective SAM measures			
				A1-D2 Number of trains of safety systems (application of single failure criterion including superposition of maintenance procedure) e	**A1-P2** Decision criteria related to the safety significance of plant modifications and findings	**A2-Q2-** Radiological protection monitoring			
				A1-D3 Automatic systems to control design basis accidents, i.e. no need for manual interaction within 30 minutes after event occurrence	**A1-P3** Criteria and process for integrated evaluation of all safety impacts of plant modification				

REFERENCES TO ANNEX II

[II-1] FEDERAL REPUBLIC OF GERMANY, Act On The Peaceful Utilisation of Nuclear Energy and the Protection Against its Hazards (Atomic Energy Act), 23 December 1959, as amended and promulgated on 15 July 1985, last amendment of August 28, 2013 (2013).

[II-2] FEDERAL MINISTER OF THE INTERIOR (BMI), Ordinance on the Protection against Damage and Injuries Caused by Ionizing Radiation (Radiation Protection Ordinance) of July 22, 2001, last amendment of February 22, 2012, Berlin (2012).

[II-3] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION AND NUCLEAR SAFETY (BMU), Safety Requirements for Nuclear Power Plants, Federal Gazette, Berlin (2013).

[II-4] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION AND NUCLEAR SAFETY (BMU), Interpretation of the Safety Requirements for Nuclear Power Plants, Berlin (2013).

[II-5] GERMAN REACTOR SAFETY COMMISSION (RSK), RSK's Understanding of Safety Philosophy, Federal Gazette (2013).

[II-6] FEDERAL MINISTRY FOR THE ENVIRONMENT, NATURE CONSERVATION AND NUCLEAR SAFETY (BMU), Radiological Fundamentals for Decisions on Measures for the Protection of the Population against Accidental Releases of Radionuclides, Gemeinsames Ministerialblatt 2008, No. 62/63, Berlin (2008).

[II-7] FEDERAL MINISTER OF THE INTERIOR (BMI), Guideline for the Protection of Nuclear Power Plants against Pressure Waves from Chemical Reactions by Means of the Design of Nuclear Power Plants with Regard to Strength and Induced Vibrations and by Means of the Adherence to Safety Distances, Federal Gazette No. 179 (1976).

[II-8] BREDBERG, I. et al., State and Development of Nuclear Energy Utilization in the Federal Republic of Germany, BfS-SK-22/13, Bundesamt für Strahlenschutz, Salzgitter (2013).

ANNEX III. APPLICATION OF THE GENERAL SAFETY GOALS FRAMEWORK FOR NUCLEAR INSTALLATIONS TO SWEDEN

III-1. INTRODUCTION AND BACKGROUND

This section is an attempt to apply the TECDOC framework of safety goals to the existing situation in Sweden, taking into account mainly laws and regulations but also covering low level probabilistic requirements defined by utilities.

The application was done using the hierarchy of safety goals defined as well as the matrix presented in the TECDOC, aimed at being an aid in the practical application of the Safety Goals Framework in a national context.

For reference, the TECDOC hierarchy of safety goals is shown in Figure III-1. It is described in detail in Section 2 of the TECDOC.

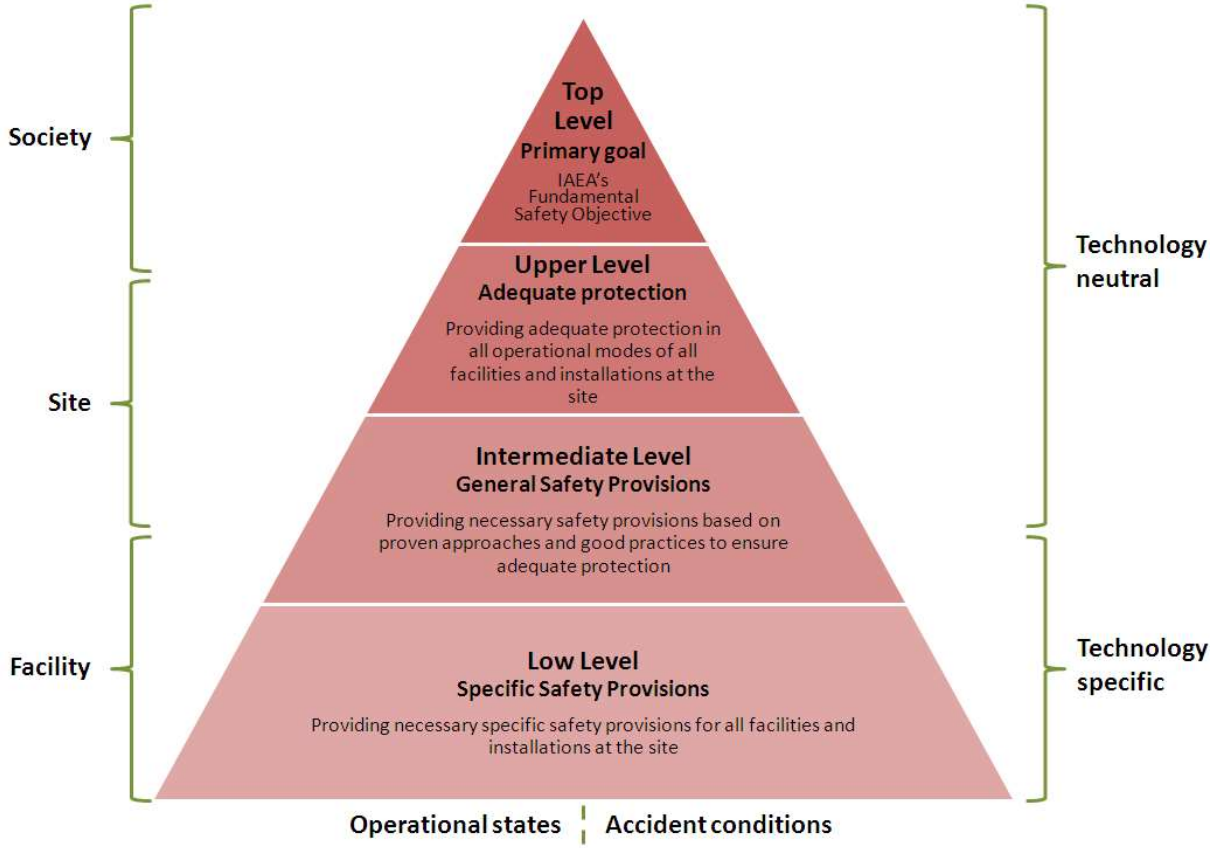

FIG. III-1. Hierarchy of Safety Goals.

As a basis for the application, a matrix has been developed showing an early example of a hierarchy of safety goals for a nuclear installation, see Figure III-2. The example was developed in preparation for the Technical Meeting held in July 2013.

Just as the safety goals hierarchy shown in Figure III-1, the matrix includes four levels, and is split into the main parts "Operational States" and "Accident Conditions". It has been detailed by defining a number of examples of upper level safety goals that are expected to exist in most frameworks. However, it must be stressed that the matrix contents is an example, and that a proper application of the framework would result in further types of safety goals being added.

<table>
<tr><td colspan="11"><u>TOP LEVEL</u> - PRIMARY SAFETY GOAL:
To protect people and the environment from harmful effects of ionizing radiation</td></tr>
<tr><td colspan="11"><u>UPPER LEVEL</u> SAFETY GOALS – ADEQUATE PROTECTION:
Ensuring adequate protection in all operational modes of all facilities and installations at the site</td></tr>
<tr><td colspan="5">Operational states</td><td colspan="6">Accident conditions</td></tr>
<tr><td colspan="2">O1
RADIATION PROTECTION
To protect workers, the public and the environment</td><td>O2
SECURITY
To provide design features for security</td><td>O3
RADWASTE MINIMIZATION
To minimize radioactive waste</td><td>O4
PROVISIONS FOR DECOMMISSIONING
To provide design features to facilitate decommissioning</td><td colspan="3">A1
LOW RISK TO PEOPLE'S LIFE AND HEALTH
Risk to life and health of people from the facilities and installations located at the site should be low comparing with risk from other sources to which an individual is generally exposed</td><td colspan="2">A2
LOW RISK TO THE ENVIRONMENT
Large off-site releases leading to land interdiction should be practically eliminated</td><td>A3
SAFETY-SECURITY INTERFACE
Safety-security interface should be addressed</td><td>A4
EMERGENCY RESPONSE
Emergency response should be provided</td></tr>
<tr><td colspan="11"><u>INTERMEDIATE LEVEL</u> SAFETY GOALS – GENERAL SAFETY PROVISIONS:
Providing general safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection</td></tr>
<tr><td><u>Qualitative</u>
O1-Q1
Management, leadership and safety culture</td><td><u>Deterministic quantitative</u>
O1-D1
To meet ICRP criteria for workers by providing adequate radiation protection measures</td><td>…</td><td>…</td><td>…</td><td><u>Qualitative</u>
A1-Q1
Maintaining effective defence in depth</td><td><u>Deterministic quantitative</u>
A1-D1
Maintaining allowed doses for workers in DBAs</td><td><u>Probabilistic quantitative</u>
A1-P1
Overall L(E)RF for the site for all events and hazards</td><td><u>Qualitative</u>
A2-Q1
Providing effective SAM design features and SAMG at the site level</td><td><u>Probabilistic quantitative</u>
A2-P1
Probabilistic interpretation of practically eliminated</td><td>A3-Q1
Vital area identification at the site level</td><td>A4-Q1
Detailed emergency plan</td></tr>
<tr><td></td><td>O1-D2
To meet ICRP criteria for discharges to the environment by providing adequate measures for controlling the discharges</td><td></td><td></td><td></td><td>A1-Q2
Maintaining sufficient safety margins</td><td>A1-D2
Maintaining allowed discharges to the environment in DBAs</td><td>A1-P2
Frequencies of external hazards/ magnitudes for design of site protective features</td><td></td><td><u>A2-P2</u>
Food ban radioactivity levels and accepted frequency</td><td>A3-Q2
Providing security measures in compliance with safety needs at the site level</td><td>A4-D1
Food ban levels</td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>A1-Q3
Providing sufficient redundancy and diversity to comply with single failure criterion</td><td>A1-D3
Containment withstanding the crash of a specified size aircraft</td><td></td><td></td><td><u>A2-P3</u>
Habitation radioactivity levels and accepted frequency</td><td></td><td>A4-D2
Habitation radioactivity levels</td></tr>
<tr><td colspan="11"><u>LOW LEVEL</u> SAFETY GOALS – SPECIFIC SAFETY PROVISIONS:
Providing specific safety provisions for each facility and installation at the site to ensure adequate protection</td></tr>
<tr><td>…</td><td>…</td><td></td><td>…</td><td>…</td><td><u>Deterministic quantitative</u>
A1-Q2-INST1(D1) – max fuel clad temp. for INST1
A1-Q2-INST1(D2) – … for INST1

A1-Q2-INST2(D1) – max fuel clad temp. for INST2
A1-Q2-INST2(D2) – … for INST2</td><td rowspan="2"><u>Probabilistic quantitative</u>
• LERF for each installation:
A1-P1-INST1(LERF),
A1-P1-INST2(LERF),
• Supplemental goals on CDF as applicable:
A1-P1-INST1(CDF),
A1-P1-INST2(CDF), …
Instantaneous risk limit
….</td><td rowspan="2"><u>Qualitative</u>
A2-Q1-INST1(SAMG)
A2-Q1-INST2(SAMG)
Providing effective SAM design measures and SAMG at the facility level</td><td></td><td>A3-Q1-INST1
A3-Q1-INST12
…
Vital area identification at facility level</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td>A1-Q3-INST1 - required three trains of safety systems</td><td></td><td></td><td></td><td>A3-Q2-INST1
…..</td><td></td></tr>
</table>

FIG III-2. Example of Hierarchy of Safety Goals for Nuclear Installations.

The result of the application is summarised in a 2-page attachment to this annex, using the same matrix format as shown in Figure III-2 above. A more detailed discussion of the contents of the matrix and of the results of the application is provided in the coming four sections, one for each level of the Safety Goals Framework.

III-2. APPLICATION TO THE GENERAL SAFETY GOALS FRAMEWORK

III-2.1. Top level safety goals

These are presented in the Safety Goal Framework as being the highest level safety goals, as defined in national legislation or regulations. They generally presuppose the prevention of unreasonable harm to the public and the environment. Top level safety goals are important as high-level statements, but cannot in themselves be used as a basis for defining detailed safety goals. In a Swedish context, Top Level Safety Goals are expressed in a number of laws, and to some extent also regulations.

On the highest level are the Act 1984:3 on Nuclear Activities (Lagen om kärnteknisk verksamhet) and the Radiation Protection Act 1988:220 (Strålskyddslagen), expressing the aim to protect people, animals and the environment from harmful effects of radiation.

Another important top level document is the Regulation on Handling of Radioactive Waste and Spent Fuel from Nuclear Installations (SSMFS 2008:22), which includes requirements on minimisation of the amounts of waste and on avoiding harmful impact from radiation now and in the future. This regulation also includes a requirement stating that radioactive releases shall not cause worse effects on health and environment outside the borders of Sweden than would be accepted within Sweden.

Further high level requirements (but less specific) are expressed in, e.g., the Environmental Code 1998:808 and in the Act 2006:263 on Transportation of Dangerous Materials.

III-2.2. Upper level safety goals

This level provides an interpretation of the Top Level safety goals in terms of risks of undue harm to people or the environment. Upper Level safety goals are the implicit basis for Intermediate and Low level safety goals, which may require an interpretation in numerical terms of what constitutes an unreasonable risk (or dose) to an individual or to society.

The matrix includes the following typical examples of Upper Level safety goals, all of which are covered in a number SSM regulations as well as (in a few cases) in laws.

Operational states

O1 To protect workers, the public and the environment

O2 To provide design features for security

O3 To minimize radioactive waste

O4 To provide design features to facilitate decommissioning

Accident conditions

A1 Risk to life and health of people from the facilities and installations located at the site should be low comparing with risk from other sources to which an individual is generally exposed

A2 Large off-site releases leading to land interdiction should be practically eliminated

A3 Safety-security interface should be addressed

A4 Emergency response should be provided

A more specific example will be given describing the basis for the quantitative requirements (safety goals) related to unacceptable radioactive releases.

The focus of the SSM is on avoidance of radiological accidents, i.e., requirements have been directed towards protection of the public rather than towards avoidance of core damage. This became evident in the discussions related to the government decisions following the Reactor Safety Investigation [III-1] requiring the introduction of severe accident mitigation system first at the Barsebäck plants 1981 [III-2] and then at all other NPPs in 1986 [III-3]. Basically, these government decisions define the conditions for allowing continued operation of the plants. On the basis of the government's proposition [III-4] regarding guidelines for the national energy policy, it was stated that in spite of the fact, that the risks for uncontrolled radioactive release from nuclear power plants is extremely small, measures shall be taken to further reduce such risks.

The FILTRA system in Barsebäck was taken into operation in October 1985; for the remaining Swedish NPPs severe accident mitigating systems including filtered venting were to be installed by the end of 1989. The document that served as a basis for the decision in 1985 had the title "Release mitigating measures after severe accidents" [III-5]. Based on the document, a number of acceptance criteria for the mitigating systems after a severe accident were defined:

- Events with extremely low probabilities (extremt låga sannolikheter) can be neglected.
  It is accepted that the filtered venting system cannot handle a reactor vessel rupture.
- The same requirements on maximum acceptable release of radioactive substances apply to all NPPs, regardless of location.
  The justification for this requirement is that the same level of individual risk shall be achieved at all sites, regardless of population density and property values.
- Long-term ground contamination of large areas shall be avoided.
  This is judged to be fulfilled if the radioactive release after a severe accident is limited to below 0,1 % of the inventory of the caesium isotopes Cs-134 and Cs-137 in a core of 1800 MW, excluding noble gases.
- There shall be no short-term fatalities in acute radiation syndrome (akut strålsjuka).
  This is judged to be fulfilled if the radioactive release after a severe accident is limited to below 1 % of the inventory of a core of 1800 MW, excluding noble gases.
- The containment shall remain intact for 10-15 hours after a core melt.

A simplifying interpretation of part of the requirements is given by stating that these requirements can be considered fulfilled if the radioactive release after a severe accident is limited to

below 0,1 % of the inventory of the caesium isotopes Cs-134 and Cs-137 in a core of 1800 MWt, provided all nuclides causing unacceptable ground contamination are limited correspondingly. Considering the fact, that the inventory of Cs-134 is 89 TBq/MW and of Cs-137 is 57 TBq/MW, the 0,1 % / 1800MW requirement corresponds to a release of 160 TBq of Cs-134 and of 103 TBq of Cs-137. The requirement that the containment shall remain intact for 10–15 hours after a core melt implies that mitigating measures protecting the containment from over-pressurisation and by-pass shall be designed in a way that practically eliminate the possibility of early releases.

III-2.3. Intermediate level safety goals

Intermediate Level safety goals cover crucial safety provisions such as defence-in-depth, safety margins, physical barriers (including considerations related to independence and protection of barriers), and redundancy and independence.

Requirements on the Intermediate level are typically stated in a set of regulations, including the following important examples:

- SSMFS 2008:1 Regulations concerning Safety in Nuclear Facilities
- SSMFS 2008:12 Regulations (and general advice) on the Physical Protection of Nuclear Installations
- SSMFS 2008:13 Regulations on the Mechanical Devices in Nuclear Installations
- SSMFS 2008:15 Regulations concerning Emergency Preparedness at Certain Nuclear Facilities
- SSMFS 2008:17 Regulations (and general advice) concerning the Design and Construction of Nuclear Power Reactors
- SSMFS 2008:22 Regulations Regulation on Handling of Radioactive Waste and Spent Fuel from Nuclear Installations,
- SSMFS 2008:23 Regulations on Protection of Human Health and the Environment in connection with Discharges of Radioactive Substances from certain Nuclear Facilities
- SSMFS 2008:26 Regulations on Radiation Protection of Individuals Exposed to Ionizing Radiation at Nuclear Facilities

To give some specific examples from two of these regulations, the “Regulations concerning Safety in Nuclear Facilities” (SSM FS 2008:1), includes requirements related to Defence in depth, Organisation and management, Safety criteria and guidelines, Safety analysis, Review activities, Periodic Safety Reviews, and Technical Specifications.

In another regulation, the “Regulations concerning the Design and Construction of Nuclear Power Reactors” (SSM FS 2008:17) includes requirements related to redundancy, functional and physical separation, single failures, requirements on capacity and robustness of various safety functions. The latter requirements are related to event classification, which includes the following classes:

– Normal operation (H1)

  Includes disturbances successfully managed by regular operations and control systems without interrupted operation

– Anticipated events (H2)

  Events that can be expected to occur during the lifetime of a nuclear power reactor

– Unanticipated events (H3)

  Events that are not expected to occur during the lifetime of a nuclear power reactor, but which can be expected to occur if several reactors are taken into account

– Improbable events (H4)

  Events that are not expected to occur; this also includes a number of postulated events that are analysed to verify reactor robustness independently of the event frequency. These events are often called 'design basis events'.

– Highly improbable events (H5)

  Events that are not expected to occur; if the event should nevertheless occur, it can result in major core damage. These events are the basis of the nuclear power reactor's mitigating systems for severe accidents.

– Extremely improbable events (residual risks)

  Events which are so improbable that they do not need to be taken into account as initiating events in connection with safety analysis

These event classes have been given the following approximate interpretation by the industry (expressed per reactor year):

H2		F >	1E-2
H3	1E-2	> F >	1E-4
H4	1E-4	> F >	1E-6
H5	1E-6	> F >	1E-7

III-2.4. Low level safety goals

Low level safety goals are technical and operational, and aim at assuring the nuclear installation meets the higher level safety goals, by addressing the design and site implementation of a nuclear installation. Technical safety goals are also more directly useful as means to evaluate the adequacy of existing or proposed designs of safety related SSCs. Some Low Level safety goals are qualitative and relate to whether a risk, or a condition that may result in a risk, is acceptable. Quantitative deterministic safety goals may relate to maximum or minimum values of crucial parameters, such as fuel temperature, pressure or water levels. Quantitative probabilistic safety goals are expressed as frequencies or probabilities of unacceptable states.

On this level there will be a large number of specific safety goals related to the higher level safety goals that have been defined.

Example – Low level probabilistic safety goals in Sweden

As a specific example, the probabilistic safety goals defined by the industry related to core damage frequency and frequency of unacceptable releases will be presented in some detail. This has been based on the outcome of the first phase of the Nordic PSA Group project "The Validity of Safety Goals" [III-6] which included, inter alia, a detailed description of the background and basis for probabilistic safety goals in Sweden and Finland. This means that the developments since the publication of this report are not fully covered.

Requirements from authorities

As evident from the section, describing the basis for defining Upper Level safety goals regarding unacceptable radioactive releases, no frequency requirement was included in the requirements.

Thus, the interpretation by the industry of the frequency requirement, i.e., converting "extremely low probabilities" into a frequency of occurrence, was done by relating to the concept of residual risk, which at that time was suggested to correspond to an event with a frequency of about 10^{-7} per year. However, this frequency was not spelled out in any of the government decisions, neither in [III-5].

It is worth mentioning in this context, that the Regulation concerning Safety in Nuclear Facilities (SSMFS 2008:1) requires the licensees to have clearly defined goals for their activities. The regulation mentions documented safety goals, which is commented in the following way in the general advice accompanying the SSMFS: "The safety goals may be both quantitative and qualitative. Goals should be formulated so that they can be followed up." The basis for the safety assessment is deterministic, but in the view of SSM, PSA can and should be used to verify the deterministic requirements. SSMFS 2008:1 states: "In addition to deterministic analyses … the facility shall be analyzed by probabilistic methods in order to obtain as comprehensive a view as possible of safety."

The use of safety goals at the utilities

The Swedish nuclear power plants are operated by companies belonging mainly to the Vattenfall group (Ringhals 1 BWR, Ringhals 2-4 PWR, and Forsmark 1-3 BWR:s) and to the EON group (Oskarshamn 1-3 BWR:s and the decommissioned Barsebäck 1-2 BWR:s).

At Vattenfall, safety goals were first discussed at the end of the 1980s, resulting in the publication of a company policy for reactor safety in 1990 [III-7]. PSA related issues in the safety policy have been continuously discussed through the years, and minor revisions of the policy, not affecting the PSA related safety goals, were made from time to time. The policy states that high priority is given to safety enhancing measures if probabilistic analyses indicate that the core damage frequency is above 10^{-5} per year or above 10^{-7} per year for an unacceptable release. An "unacceptable release" is defined as above 0,1 % of the inventory of the caesium isotopes Cs-134 and Cs-137 in a core of 1800 MWt; the plant specific percentage is calculated based on the actual power rating of each NPP.

The latest version of the policy [III-8] is part of the management system for electrical production. The policy stresses the integrated aspects of safety assessment, stating that the

planning of safety improvements shall be based on a combination of deterministic criteria, probabilistic methods, human factors analysis and utilisation of experience feedback. The numerical safety goals have remained unchanged relative to the previous policy. The safety policy on company level has been converted to site specific policies at the Ringhals and Forsmark plants, with more specific evaluation criteria including a graded approach similar to the one outlined in the IAEA Safety Report 12, IAEA (1998) [III-9].

The Sydkraft group (now part of EON Nordic) issued a safety policy in 1995, which included safety goals for the frequency of core damage and large releases [III-10]. The levels defined were 10^{-5} per year for core damage and 10^{-7} per year for an unacceptable release, with an "unacceptable release" defined in the same way as defined above for Vattenfall. The safety goals were not mandatory, but in case of PSA results above these levels, safety enhancing measures were to be prioritised. The policy was effective until 2004 when it was updated and re-issued as the EON Nordic Safety Policy [III-11 and III-12]. As part of the update, the quantitative safety goals were slightly revised; the core damage criterion kept at 10^{-5} per year but applied to *severe* core damage, and the criterion for unacceptable releases stating that the frequency shall be *considerably lower* than the core damage criterion of 10^{-5} per year, which was suggested to imply at least a factor of 10 (the factor is not defined in the policy).

The EON group policy is the basis for the local policy applied by the OKG utility operating the three Oskarshamn NPPs. Detailed local criteria for interpretation and judgement of PSA results have been developed, including a graded approach similar to the one outlined in the IAEA Safety Report 12, IAEA (1998) [III-9]. In addition, probabilistic criteria have been defined with a focus on assessment of the remaining system barrier after an initiating event. These are typically applied for rare initiating events with large uncertainties in the event frequency, such as internal fires or external events.

Table III-1 provides a summary of Swedish probabilistic Low Level safety goals.

Summary of experiences

PSA results and fulfilment of safety goals has been important in some applications and influenced the decision taken by the SSM, e.g., in the FENIX project (mid-90s) for restart of Oskarshamn 1 after a major upgrade including considerable improvements of some safety related systems and functions.

At the utilities, the use of probabilistic safety goals is judged to have triggered a number of important safety improvements. PSA has generally provided an aspect on safety that has been valuable for the total activities at the plants, but this has largely been achieved independently of the safety goals. A general concern with formal probabilistic safety goals was the risk of these being seen as absolute limits, as it was feared that this might indirectly have an impact on the quality and relevance of the PSA models.

Some utilities have moved from a rather negative impression of PSA to a more positive one. PSA in the right context and accompanied by other relevant information is now generally seen to give a very valuable contribution to safety analysis, and PSA has become an integrated part of the total safety analysis concept. Safety goals have contributed to an increased awareness of the usefulness of PSA. They have also increased the focus on the correctness of the PSA models. Another experience is that the quality requirements on PSA increase in risk-informed applications.

TABLE III-1. SUMMARY OF SWEDISH (PROBABILISTIC LOWER LEVEL) SAFETY GOALS

<table>
<tr><th>Authorities</th><th>Vattenfall</th><th>EON (Sydkraft)</th></tr>
<tr><td rowspan="2">1985

Core damage

No numerical criteria defined.

Release

No numerical criteria defined.

”Extremely unlikely” release of more than 0,1 % of the inventory of the caesium isotopes Cs-134 and Cs-137 in a core of 1800 MWt.

No frequency defined, but interpreted by industry as implying < 10^{-7}/year.</td><td>1990

Core damage

10^{-5}/year with a high degree of confidence

Release

10^{-7}/year for a release involving more than 0,1% of the core inventory of substances causing ground contamination.</td><td>1995

Core damage

10^{-5}/year

Release

10^{-7}/year for release involving more than 0,1% of the core inventory excluding noble gases.</td></tr>
<tr><td>2006

Core damage

10^{-5}/year

Release

10^{-7}/year for a release involving more than 0,1% of the core inventory of substances causing ground contamination</td><td>2006

Core damage

10^{-5}/year for severe core damage

Release

Frequency of release involving more than 0,05-0,1% (depending on thermal effect) of the core inventory excluding noble gases shall be considerably lower than 10^{-5}/year.</td></tr>
</table>

III-2.5. Conclusions

This annex was primarily aimed at tentatively applying the proposed Safety Goals Framework on the situation in Sweden, taking into consideration mainly laws and regulations, but also addressing some utility requirements.

It is important to recognise that the application was not aimed to be complete. Still some general conclusions can be drawn. Thus, existing laws and regulations seem to provide a good coverage of the four layers of the Safety Goals Framework, including demonstrating adequate coverage of different types of facilities and covering the entire life span.

The application of the Safety Goals Framework to Swedish conditions was quite easily done, i.e., it seems the framework and work process suggested in the TECDOC are quite easily applied.

It is clear from the review (and from the previous Nordic PSA Group project), that there is still only limited use of probabilistic criteria, and that the most detailed ones are defined by the utilities.

The triangle depicting the framework is judged to fully capture the conceptual aspects of the framework and hierarchy, and the matrix provides specific examples. It is, however, important not to see the matrix as a complete checklist. Additional work is needed as part of any application to prepare relevant matrix contents.

Finally, the safety goals matrix, once it has been developed, can serve as a completeness check, i.e., it indicates areas that are lacking or unclearly defined.

REFERENCES TO ANNEX III

[III-1] SOU; Final report from the Reactor Safety Investigation (Reaktorsäkerhets-utredningen "Säker kärnkraft?"), SOU 1979:86 (1979).

[III-2] INDUSTRIDEPARTEMENTET, Conditions for continued operation according to atomic energy act (Villkor för fortsatt tillstånd enligt 2 § atomenergilagen (1956:306) att driva atomreaktor), Industridepartementet 1183/81 1981-10-15; Industridepartementet, (1981).

[III-3] INDUSTRIDEPARTEMENTET; Conditions for continued operation according to act on nuclear activities (Villkor för fortsatt tillstånd enligt 5 § lagen (1984:3) om kärnteknisk verksamhet för att driva kärnkraftreaktorerna Oskarshamn I, II och III); Industridepartementet 2717/85 1986-02-27 (dossier 8523), Industridepartementet (1986).

[III-4] SVERIGES RIKSDAG, Guidelines for the national energy policy (Riktlinjer för energipolitiken), Proposition 1980/81:90, Stockholm, Sweden (1981).

[III-5] SKI/SSI, Release mitigating measures after severe accidents (Utsläppsbegränsande åtgärder vid svåra härdhaverier), SKI ref 7.1.24 1082/85 (1985).

[III-6] HOLMBERG, J-E., KNOCHENHAUER, M., Probabilistic Safety Goals. Phase 1 — Status and Experiences in Sweden and Finland. SKI Report 2007:06, Swedish Radiation Safety Authority (SSM), Stockholm (2007).

[III-7] VATTENFALL; Company policy for reactor (Koncernpolicy Vattenfall / P-riktlinjer Reaktorsäkerhet) PK 301:1, Sweden (1990).

[III-8] VATTENFALL; Vattenfall policy for nuclear safety (Vattenfalls policy för kärnkraftsäkerhet), Sweden (2006).

[III-9] 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).

[III-10] AHLSTRÖM, G., The Sydkraft safety policy for nuclear power (Sydkrafts säkerhetspolicy Kärnkraft) (1995).

[III-11] FRITIOF, L., Safety Policy Nuclear Power E.ON Nordic (Säkerhetspolicy Kärnkraft E.ON Nordic), (2005).

[III-12] LARSSON, S-E., E.ON Nordic safety policy for nuclear power (E.ON Nordic Säkerhetspolicy för kärnkraft inkl. förklarande text), SKKÖT-050609-01 (2005).

Attachment

Tentative application of Safety Goals Framework to Swedish conditions

(NB – mapping incomplete)

TOP LEVEL - PRIMARY SAFETY GOAL: *To protect people and the environment from harmful effects of ionizing radiation*

Act on nuclear activities 1984:3

Radiation Protection Act 1988:220

Environmental Code 1998:808

Laws on Transportation of Dangerous Materials 2006:263

SSM Regulation on handling of radioactive waste and spent fuel from nuclear installations, SSMFS 2008:22

UPPER LEVEL: *Ensuring adequate protection in all facilities and installations at the site*

Operational states				**Accident conditions**			
O1 **RADIATION PROTECTION** To protect workers, the public and the environment	**O2** **SECURITY** To provide design features for security	**O3** **RADWASTE MINIMIZATION** To minimize radioactive waste	**O4** **PROVISIONS FOR DECOMMISSIONING** To provide design features to facilitate decommis-sioning	**A1** **LOW RISK TO PEOPLE'S LIFE AND HEALTH** Risk to life and health of people from the facilities and installations located at the site should be low comparing with risk from other sources to which an individual is generally exposed	**A2** **LOW RISK TO THE ENVIRONMENT** Large off-site releases leading to land interdiction should be practically eliminated	**A3** **SAFETY-SECURITY INTERFACE** Safety-security interface should be addressed	**A4** **EMERGENCY RESPONSE** Emergency response should be provided
– *SSMFS*	– *SSMFS 2008:12*	– *SSMFS 2008:22*	– *SSMFS 2008:1*	– *SSMFS 2008:23*	– *SSMFS 2008:23*	– *SSMFS 2008:12*	– *Law 2003:778 on protection against accidents* – *SSMFS 2008:15*

INTERMEDIATE LEVEL: *Providing necessary safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection*
See page 2(2)
LOW LEVEL: *Providing necessary specific safety provisions for all facilities and installations at the site*
Not covered by mapping, but addressed in main text

Titles of SSMregulations (SSMFS YYYY:xx)

SSMFS 2008:1 The Swedish Radiation Safety Authority's Regulations concerning Safety in Nuclear Facilities

SSMFS 2008:12 The Swedish Radiation Safety Authority's Regulations (and general advice) on the Physical Protection of Nuclear Installations

SSMFS 2008:13 The Swedish Radiation Safety Authority's Regulations on the Mechanical Devices in Nuclear Installations

SSMFS 2008:15 The Swedish Radiation Safety Authority's Regulations concerning Emergency Preparedness at Certain Nuclear Facilities

SSMFS 2008:17 The Swedish Radiation Safety Authority's Regulations (and general advice) concerning the Design and Construction of Nuclear Power Reactors

SSMFS 2008:22 The Swedish Radiation Safety Authority's Regulations Regulation on Handling of Radioactive Waste and Spent Fuel from Nuclear Installations,

SSMFS 2008:23 The Swedish Radiation Safety Authority's Regulations on Protection of Human Health and the Environment in connection with Discharges of Radioactive Substances from certain Nuclear Facilities

SSMFS 2008:26 The Swedish Radiation Safety Authority's Regulations on Radiation Protection of Individuals Exposed to Ionizing Radiation at Nuclear Facilities

Attachment

Tentative application of Safety Goals Framework to Swedish conditions

(NB – mapping incomplete)

INTERMEDIATE LEVEL: *Providing necessary safety provisions including technical and organizational measures based on proven approaches and good practices to ensure adequate protection*											
Operational states					**Accident conditions**						
Qualitative **O1-Q1** Management, leadership and safety culture	Deterministic quantitative **O1-D1** To meet ICRP criteria for workers by providing adequate radiation protection measures	…	…	**…**	Qualitative **A1-Q1** Maintaining effective defence in depth	Deterministic quantitative **A1-D1** Maintaining allowed doses for workers in DBAs	Probabilistic quantitative **A1-P1** Overall L(E)RF for the site for all events and hazards	Qualitative **A2-Q1** Providing effective SAM design features and SAMG at the site level	Probabilistic quantitative **A2-P1** Probabilistic interpretation of practically eliminated	**A3-Q1** Vital area identification at the site level	**A4-Q1** Detailed emergency plan
– SSMFS 2008:1					– SSMFS 2008:17	– SSMFS 2008:26		– Government letter regarding Filtra			– SSMFS 2008:15
	O1-D2 To meet ICRP criteria for discharges to the environment by providing adequate measures for controlling the discharges				**A1-Q2** Maintaining sufficient safety margins	**A1-D2** Maintaining allowed discharges to the environment in DBAs	**A1-P2** Frequencies of external hazards/ magnitudes for design of site protective features		**A2-P2** Food ban radioactivity levels and accepted frequency	**A3-Q2** Providing security measures in compliance with safety needs at the site level	**A4-D1** Food ban levels
					– *SSMFS 2008:13*	– Government letter regarding Filtra *SSMFS 2008:23*					

					A1-Q3 Providing sufficient redundancy and diversity to comply with single failure criterion	**A1-D3** Containment withstanding the crash of a specified size aircraft			**<u>A2-P3</u>** Habitation radioactivity levels and accepted frequency		**A4-D2** Habitation radioactivity levels
					– *SSMFS 2008:17*	– *SSMFS 2008:17 (indirectly)*					

ANNEX IV. UK FRAMEWORK FOR NUCLEAR SAFETY GOALS AND TARGETS

IV-1. NTRODUCTION

The health and safety regulatory system in the UK is based on a goal-setting approach and nuclear safety follows the same principles that are used in regulating health and safety in industrial situations across virtually all types of work. Thus the regulatory body does not set prescriptive requirements but determines broad safety goals which the licensee has to comply with and hence its own detailed requirements. However, the overall effect of this regulatory approach can be seen to fit the general approach described in this report.

IV-2. TOP LEVEL SAFETY GOAL

The top level safety requirement is promulgated in the Health and Safety at Work etc Act, 1974 (HSWA) [IV-1] which sets a requirement on employers to carry out their work in such a way that the health, safety and welfare of employees is ensured and that risks to the health and safety of those not in their employ are controlled "so far as is reasonably practicable". This phrase is also used in relation to importers, designers, manufacturers in relation to risks to the users of the equipment they provide. The acronym SFAIRP is usually used instead of the full phrase "so far as is reasonably practicable", but even more common is the acronym ALARP which stands for "as low as reasonably practicable"[10] as in the expression "risks should be ALARP". The requirement to demonstrate reasonable practicability is fundamental and the only test in law. This requirement has been included in various UK laws for well over 100 years.

Any organisation wanting to install or operate a prescribed nuclear installation will need a nuclear site licence issued under the Nuclear Installations Act 1965 [as amended] (NIA) [IV-2] by the Health and Safety Executive (HSE), the prime body for regulating health and safety at work in the UK: this power is delegated to the Office for Nuclear Regulation (ONR), which is an agency of HSE. The safety parts of the NIA are now a Statutory Provision of the HSWA ie subsidiary legislation under this Act. The NIA also requires the protection of other people's property. Thus the two acts provide obligations to protect people and the environment. They also place the prime responsibility for safety on the licence holder, who must do all that is reasonably practicable to reduce the risk posed to both employees and the public from the operation of the installation.

UK law is based on precedent i.e. what has been decided in the courts – until there has been a decided case, the precise meaning the law is considered to be "undetermined". The definition of what is necessary to demonstrate reasonable practicability derives from a legal case in 1949 [IV-3]. The judgement stated it was necessary to compare the sacrifice, in terms of money, time and trouble, of implementing further safety measures to reduce risks with the risks that have

---

[10] The requirement for risks to be as low as reasonably practicable (ALARP) is fundamental and applies to all activities within the scope of the Health and Safety at Work (etc) Act 1974 [HSWA] in the UK. In simple terms it is a requirement to take all measures to reduce risk where doing so is reasonable. In most cases this is not done through an explicit comparison of costs and benefits, but rather by applying established relevant good practice and standards. The development of relevant good practice and standards includes ALARP considerations so in many cases meeting them is sufficient. In other cases, either where standards and relevant good practice are less evident or not fully applicable, the onus is on the licensee to implement measures to the point where the costs of any additional measures (in terms of money, time or trouble – the sacrifice) would be grossly disproportionate to the further risk reduction that would be achieved (the safety benefit).

Source: ONR, Guidance on the demonstration of ALARP, NS-TAST-GD-005 Revision 6, September 2013

been averted. If the comparison showed that it would be grossly disproportionate to implement the measures, then they did not need to be implemented. It was noted that this comparison had to been done before any accident or incident occurred. It was also stated that the higher the risk, the less important the cost should be.

No legal meaning has been put to the term "grossly disproportionate"; though it is clear the judge was looking for an imbalance on the side of safety, which has been upheld in later cases. At a public inquiry into a new nuclear power plant at Sizewell in the early 1980s, the Director-General of HSE, gave figures of between 2 and 10 for the public, depending on the risk, and about 3 for workers, which was not questioned. This was also stated without challenge at a later public inquiry.

A later legal judgement [IV-4] defined the meaning of the word "risk", which clearly, given the date of the former case, was not the output of a PSA. Risk was defined as the "possibility of danger" which is some way from a probabilistic definition and also moves the meaning more towards the hazard, i.e. what poses the potential for harm, rather than the chance of harm which is the more common modern definition of risk.

It is a consequence of this goal-setting approach that older facilities, built to different standards, may pose a greater risk than modern ones as the sacrifice in bringing the older facility up to modern standards would be too great. However, it is expected that the older facility will be modified to achieve as near modern standards as possible, within the requirements of reasonable practicability.

Explaining the top level safety goal

Thus in the UK the top level safety goal, and the only one enshrined in law, is about demonstrating that it is not reasonably practicable to do more to prevent harm to people. At the same inquiry into the NPP at Sizewell, the Inspector asked what the application of this requirement meant in terms of risk to people. He specifically asked what was a tolerable risk and what was an acceptable risk? HSE were asked to set this down so that Parliament and the public could consider the position.

This resulted in a document called "Tolerability of Risk from Nuclear Power Plants" (ToR) [IV-5], which was published in its final form in 1992. ToR provided a background discussion of risk, separating individual risk from societal risk (the latter was a comprehensive facet covering multiple casualties through effects on land to more intangible effects on society).

The document also gave statistics on accidents both in the UK and elsewhere from accidents and natural events to both workers and the public. From this data, it was deduced that for workers, the upper level of fatality was around 1x 10^{-3}, yr for industries such as mining, quarrying and deep-sea fishing, whereas in most other occupations the level was nearer to 10^{-4}/year. From data on such activities as car driving, a similar figure of 10^{-4}/yr was derived. These figures were considered "tolerable" as there were no attempts to ban the activities but there were several pressures to get the rates lower. At the other extreme, the deaths from events such as lightning strikes or influenza were of order 10^{-6}/yr, and these seemed to be "broadly acceptable" as there was little pressure to reduce them. It was suggested a similar figure should apply to workers.

On societal risks there was little information, but based on industrial hazards and the case made for erecting the Thames Barrier to protect London a figure of around 10^{-4}/yr to prevent about 100 -1000 deaths was considered tolerable, though the document was not as explicit as this statement suggests.

Subsequently, in 2000, HSE published a further document, Reducing Risk, Protecting People (R2P2) [IV-6] which widened the application of the ToR concept to other industries. This endorsed the individual risk values and set a firmer "tolerable" level of societal risk as a frequency no higher than $2x10^{-4}$/yr for a single accident causing 50 or more deaths, but did not suggest a "broadly acceptable" figure.

Note that these are expectations from applying the requirement of reasonable practicability and are not legal values: they are a guide to health and safety inspectors in carrying out their work. In particular, "broadly acceptable" should be interpreted as meaning that, provided the safety measures are secure the inspectors will turn their attention to other higher risks, but the employer must still implement further measures if they are reasonably practicable. Equally, risks higher than the "tolerable" level may be allowed in specific situations.

IV-3. UPPER LEVEL SAFETY GOALS

In the UK, the nuclear safety regulator has developed an approach based on reasonable practicability, or in the case of environmental regulation on a similar concept of Best Available Technology (BAT) not entailing excessive cost, in line with that used in other industrial sectors. The first aspect is that, wherever possible, relevant good practice should be used to determine the necessary safety measures.

ONR has produced Safety Assessment Principles for Nuclear Facilities (SAPs) [IV-7] to assist its staff in applying consistent judgement on whether the licensee has demonstrated reasonable practicability. The SAPs describe some fundamental safety expectations, which are largely based on the recommendations of the ICRP [IV-8] and the IAEA Fundamental Safety Principles [IV-9], for example:

1. No person shall receive doses of radiation in excess of the statutory dose limits as a result of normal operation.
2. The exposure of any person to radiation shall be kept as low as reasonably practicable (ALARP).
3. The collective effective dose to operators and to the general public as a result of operation of the nuclear installation shall be kept as low as reasonably practicable.
4. All reasonably practicable steps shall be taken to prevent accidents.
5. All reasonably practicable steps shall be taken to minimise the radiological consequences of any accident.

The ONR also uses conditions attached to the Nuclear Site Licence (NSL) to promote Upper Level Safety Goals. Licence conditions [IV-10, 11] can be attached to the NSL, under the powers in the NIA, which makes them legal requirements. The 36 conditions are added to all licences, regardless of the type of facilities on the site, and require the licensee to make and implement arrangements to meet them: in many cases these are approved by the ONR which means they cannot be changed without a further approval process. Licence conditions cover production of safety cases, emergency arrangements, modifications of plant or management arrangements, minimisation of waste etc. The site licence is issued to a single licensee and covers all facilities and activities on the site.

Since the operators have the prime responsibility for safety, the legal requirements set goals, rather than prescribing detailed requirements. Operators in the UK have in the past set down

their own framework for meeting the top level goals for the specific activities they are carrying out. These provide the starting point for the detailed technical requirements for the activities to be carried out, but must also ensure that this delivers a safe operating plant, which meets the regulators expectations. The regulator in turn must be satisfied that the licensee is adequately discharging its responsibility for safety.

IV-4. INTERMEDIATE LEVEL SAFETY GOALS

At the intermediate level, it is necessary to consider the differences between the role of the nuclear regulator and the licensee.

Within the SAPs, ONR sets out its expectations for modern nuclear installations in relation to, *inter alia*: the importance of considering inherent safety, fault tolerance, defence in depth in the design; the application of segregation, redundancy, diversity to safety systems; the need for strong leadership and management for safety in operation; and a sound demonstration of the adequacy of safety in design and operation. Whilst the SAPs are intended for use by ONR's own staff, they are published so that licensees are aware of their expectations. The SAPs are, in general, technology neutral applying to the whole range of facilities that ONR regulates.

The SAPs also contain certain numerical targets which follow the general structure of the ToR framework and are intended to ensure a similar level of risk as in ToR. These targets are not mandatory (unless legislation such as the Ionising Radiation Regulations, 1999 [IV-12], which set upper levels for doses, is invoked – these are based on the ICRP recommendations) and cover: normal operational doses to workers, persons on site and the general public due to activities on the site; design basis doses to the public and workers; total risks of fatalities to workers and the public both for the site and an individual facility; and, societal risk which covers fatalities to the workers and public. Note that in considering the site, simple addition of individual facility risks is not acceptable unless there is complete independence of the facilities. The Annex 2 of Reference [IV-13] explains in more detail the derivation of the numerical targets.

As part of the Licence Condition arrangements for producing and assessing safety cases, the licensee defines standards against which it will assess the acceptability of the safety of any plant or installation, which it will be procuring. This would then be incorporated into the tender specification as well as forming the assessment criteria. The design safety criteria set down fundamental principles, engineering principles and radiological assessment targets. Within the current operator of NPPs these exist for the existing AGRs and PWR as well as for new nuclear plants. The safety requirements for new plants are based on the European Utilities Requirements Document, but use UK specific numerical targets, consistent will the regulators assessment principles. It should be noted that although the requirements are generally consistent the regulator does not formally approve them. They are intended to be demanding requirements for use by the operator in design assessment and safety case production; the regulator independently assesses the outcomes of these processes using their own assessment principles.

The UK numerical targets are generally set in terms of doses to operators or members of the public or in terms of risks. Underlying the approach used by the operators of civil nuclear power stations has been a target level for the individual risk of death to the most exposed individual, below which the risk is considered to be "acceptable/tolerable": i.e. 10^{-6}/yr. To achieve this the design target was that the total probability of exceeding the design basis should be less than this and that no individual fault group should contribute more than 10% i.e. should be $<10^{-7}$. The design basis in the UK is defined in terms of fault sequences derived from initiating faults or hazards, rather than single Postulated Initiating Events (PIE). The design basis covers all

initiating faults or hazards with a frequency $>10^{-5}$/yr, based on best estimate considerations, except for natural external hazards where a cut-off at 10^{-4}/yr is used, but this should be based on conservative judgements.

As part of the implementation of defence in depth it is recognised that common cause failures may limit the reliance that can be placed on redundant systems. Limits are therefore applied to allow for common cause failure. This results in a requirement for diverse protection for PIEs with frequencies > 10^{-3}/yr. Thus some design extension condition faults are already included in the design basis.

In addition to the requirements derived from individual risks there are also requirements related to societal impacts. The modern plants were all designed to ensure that there should be no need to evacuate personnel outside the site fence as a result of any (UK) design basis fault. In addition even for beyond design basis faults it is necessary to show that there is not a "cliff-edge" immediately beyond the design basis, Level 3 PSA analysis has been used to help define what represents an unacceptable cliff edge in terms of disruption of the population, land contamination and agricultural restrictions. Based on this, a societal risk measure has been defined to bound a whole range of consequences and is expressed in terms of the frequency of exceeding 100 fatal cancers. In practice this is not broken down into more detailed design goals because it is used as part of the overall assessment of the design to ensure that a balanced design has been achieved and that all reasonably practicable measures have been taken to reduce the risk. The PSA will help identify the main contributors to each measure of risk but they are often different for each measure of risk.

IV-5. LOW LEVEL SAFETY GOALS

The use of doses and risks to workers and the public provides a generic safety framework, which is technologically neutral; it is left to the licensee to define lower level technology specific targets to ensure that during operation all that is reasonably practicable is done to meet these generic targets. This will include targets for Core Damage Frequency [CDF] for reactors and targets for accidental criticality for fuel processing plants. As an example some of the lower level targets used for PWRs and the way in which they are derived are described.

As was noted above, one of the upper level goals is to ensure that the risk of death to the most exposed person as a result of the operation of a nuclear power station is less than 10^{-6}/yr. Assuming there is no threshold for radiation effects (which is probably conservative), this risk comes from both normal operation and from accidents. Controls on normal discharges and operator doses are set to provide the assurance for normal operation and in general these are based on Ionising Radiation Regulations.

The high level approach to accident conditions requires the probability of accident sequences exceeding the design basis to be reduced below 10^{-7}/yr and the total probability of exceeding the design basis to be less than 10^{-6}/yr. If exceeding the design basis is interpreted as core damage then this leads to a very demanding target for CDF of 10^{-6}/yr. In practice it has been shown that this is very conservative and much higher core damage frequencies result in consequences below the individual risk target so the targets which have been used for CDF are 10^{-5}/yr for new plants and 10^{-4}/yr for older plants.

Core damage is assumed to occur if the secondary fuel limits are exceeded since these are precursors to the loss of coolable geometry. The commonly used temperature limit of 1204C (2300F) is empirically based and represents the temperature at which breakaway oxidation of the cladding occurs. This roughly corresponds to a phase transition in ZrO_2 and is probably due

to the protective oxide layer spalling off the surface. Thus this limit applies to Zirconium based alloys and would not be expected to be the same for stainless steel, say. The limit is conservative since the fuel melting will not have occurred but the progression is likely to be rapid.

Protection systems are provided to detect faults and provide the necessary protective measures to achieve the reliabilities required. This will lead to increased redundancy. In addition conservative rules are applied to allow for potential failures and differences in the plant states. The single failure criterion represents a way to allow for potential unreliability and to permit maintenance it is assumed that one train of protection will be out for maintenance. Combining this with the potential effects of the initiating fault on the protective systems generally leads to a requirement for 4 trains of safety equipment for each safety function.

As part of the implementation of defence in depth it is recognised that common cause failures may limit the reliance that can be placed on redundant systems. In general a reliability limit of between 10^{-3} and 10^{-5} is used. Thus using the central estimate implies that for frequent faults ($>10^{-3}$/yr) diverse protection is required. Thus frequent initiators plus the failure on the first line of protection are design basis faults in the UK. However there will be some relaxation in the analysis assumptions (e.g. limiting heat sink temperatures) to reflect the lower frequency of occurrence.

REFERENCES TO ANNEX IV

[IV-1] UK GOVERNMENT, Health and Safety at Work etc Act, (1974). http://www.legislation.gov.uk/ukpga/1974/37/contents

[IV-2] UK GOVERNMENT, Nuclear Installations Act, (1965). http://www.legislation.gov.uk/ukpga/1965/57/contents

[IV-3] UK COURT OF APPEAL, Edwards v NCB, 1 KB 704, 1 ALL ER 743, (1949).

[IV-4] UK COURT OF APPEAL, The Court of Appeal in Regina vs Board of Trustees of the Science Museum,1 WLR 1171 at Page 117, (1993).

[IV-5] HEALTH AND SAFETY EXECUTIVE, The tolerability of risk from nuclear power stations, HMSO, ISBN 0118863681, Revised (1992). http://www.onr.org.uk/documents/tolerability.pdf

[IV-6] HEALTH AND SAFETY EXECUTIVE, Reducing Risk, Protecting People – HSE's Decision Making Process, HMSO ISBN 0717621510, HSE Books, London (2001). http://www.hse.gov.uk/risk/theory/r2p2.pdf

[IV-7] OFFICE FOR NUCLEAR REGULATION, Safety Assessment Principles for Nuclear Facilities, 2014 Version, Revision 0, (2014). http://www.onr.org.uk/saps/saps2014.pdf

[IV-8] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, Recommendations of the International Commission on Radiological Protection, ICRP Publication 26, Ann. ICRP, 1, 3, Pergamon Press, Oxford (1977).

[IV-9] EUROPEAN ATOMIC ENERGY COMMUNITY, FOOD AND AGRICULTURE ORGANIZATION OF THE UNITED NATIONS, INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL LABOUR ORGANIZATION, INTERNATIONAL MARITIME ORGANIZATION, OECD NUCLEAR ENERGY AGENCY, PAN AMERICAN HEALTH ORGANIZATION, UNITED NATIONS ENVIRONMENT PROGRAMME, WORLD HEALTH ORGANIZATION, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).

[IV-10] OFFICE FOR NUCLEAR REGULATION, Licence Condition Handbook, ONR (2011). http://www.onr.org.uk/silicon.pdf

[IV-11] OFFICE FOR NUCLEAR REGULATION, Compliance inspection - Technical inspection guides, ONR (2019). http://www.onr.org.uk/operational/tech_insp_guides/index.htm

[IV-12] HEALTH AND SAFETY EXECUTIVE, Work with ionising radiation Ionising Radiations Regulations 1999 Approved Code of Practice and guidance L121 HSE Books 2000 ISBN 0717617467, United Kingdom (2000).

[IV-13] OFFICE FOR NUCLEAR REGULATION, Numerical Targets and Legal Limits in Safety Assessment Principles for Nuclear Facilities: An Explanatory Note. HSE (2006). http://www.onr.org.uk/saps/numerical-targets-limits-explanatory-note.pdf

ANNEX V. DEVELOPMENT OF USNRC SAFETY GOALS FOR LIGHT WATER REACTORS

In a 1986 Safety Goal Policy Statement [V-1], the U.S. Nuclear Regulatory Commission (USNRC) described safety goals to help articulate a level of acceptable risk for safe operation of U.S. commercial nuclear power plants. The Commission established two goals that are stated in terms of public health risk – one addressing individual risk and the other addressing societal risk. The risk to an individual is based on the potential for death resulting directly from a reactor accident, i.e., a prompt fatality. The societal risk is stated in terms of nuclear power plant operations, as opposed to accidents alone, and addresses the long-term impact on those living near the plant. In both cases, the Commission based its acceptable level of risk on a comparison with other types of risk encountered by individuals and by society from other causes, applying the rule that the consequences of nuclear power plant operation should not result in significant additional risks to life and health. The safety goals were expressed in qualitative terms, so that the philosophy could be understood by all. In both cases, however, the Commission also expressed the qualitative goals for the safety of nuclear power plants in terms of individual and societal "quantitative health objectives" or "QHOs." These QHOs were established at one-thousandth of the risk arising from other causes presenting the same type of risk.

The established QHOs were based on these assumptions:

- The risk to an average individual in the vicinity of a nuclear power plant of prompt fatalities that might result from reactor accidents should not exceed one-tenth of one percent (0.1 percent) of the sum of prompt fatality risks resulting from other accidents to which members of the U.S. population are generally exposed.

- The risk to the population within the area near a nuclear power plant of cancer fatalities that might result from nuclear power plant operation should not exceed one-tenth of one percent (0.1 percent) of the sum of cancer fatality risks resulting from all other causes.

The Commission believes that this ratio of 0.1 percent appropriately reflects both of the qualitative goals, i.e., to provide that individuals and society bear no significant additional risk. However, this does not necessarily mean that an additional risk that exceeds 0.1 percent would by itself constitute a significant additional risk. The 0.1 percent ratio to other risks is low enough to support an expectation that people living or working near nuclear power plants would have no special concern due to the plant's proximity.

It should be noted that the QHOs *per se* have never been directly reflected in the USNRC regulations, but were promulgated to provide guidance as to the level of public protection which nuclear plant designers and operators should strive to achieve. The QHOs were also meant to provide guidance to the USNRC staff to use in the regulatory decision-making process. However, the Commission was clear that the safety goals were not meant to serve as a sole basis for licensing decisions. In fact, the Commission disclaimed the intent to use safety goals in making plant-specific regulatory decisions. While the safety goals provided a metric to address the question of "how safe is safe enough", practical implementation of the Commission's guidance proved to be difficult. This was due to the large uncertainties involved in calculation of risk in the mathematical sense of multiplying probability with consequences. As a result, the USNRC staff began looking for other metrics to use as surrogates for the QHOs in regulatory decision-making.

In 1990, the Commission provided additional guidance regarding the USNRC Safety Goals, endorsing surrogate objectives concerning the frequency of core damage accidents and large releases of radioactivity [V-2]. The numerical value of one-in-ten-thousand for core damage frequency (CDF) was cited as a "very useful subsidiary benchmark." In addition, a conditional containment failure probability of one-tenth was approved for application to evolutionary light water reactor designs. This resulted in a large early release frequency (LERF) of one-in-one-hundred-thousand, since containment failure is necessary for a large release to occur. The following two numerical objectives have currently been adopted as surrogates for the two QHOs:

- A CDF of $<10^{-4}$ per year as a surrogate for the latent cancer QHO.
- A LERF of $<10^{-5}$ per year as a surrogate for the early fatality QHO.

These numerical objectives are used in support of risk-informed regulatory decision-making [V-3]. However, some groups challenge the complex calculations that go into predicting such accident frequency estimates, contending that accidents with serious public health consequences may be more frequent. Nevertheless, the above two numerical objectives can be derived from QHOs as shown below:

Surrogate for the Early QHO

The individual risk of a prompt fatality from all "other accidents to which members of the U.S. population are generally exposed," such as fatal automobile accidents, etc., is about $5x10^{-4}$ per year. The safety goal criterion of one-tenth of one percent of this figure implies that the individual risk of prompt fatality from a reactor accident should be less than $5x10^{-7}$ per reactor year (ry); i.e.: $(1/10 * 1\% * 5x10^{-4}) = 5x10^{-7}$. The "vicinity" of a nuclear power plant is understood to be a distance extending to 1 mile from the plant site boundary. The individual early risk (IER) is determined by dividing the number of prompt or early fatalities (societal risk) to 1 mile due to all nuclear power plant accidents, weighted by the frequency of each accident, by the total population to 1 mile and summing over all accidents.

It can be shown that if a plant's LERF is 10^{-5} per year or less, the early fatality QHO is generally met. This acceptance can be demonstrated numerically using the results of probabilistic consequence assessments carried out in Level 3 PSAs as follows:

a) assuming that one accident sequence "n" dominates the early fatality risk and the LERF

b) assuming the accident sequence dominating the risk is the worst case scenario:

   - a large opening in the containment which occurs early in the accident sequence
   - an unscrubbed release that also occurs early before effective evacuation of the surrounding population

c) using results from NUREG-1150 [V-4] for the Surry PRA (Table 4.3-1)

   the largest conditional probability of early fatality (CPEF) within 1 mile radius of the plant for internal initiators is $3x10^{-2.}$

   This conditional risk value corresponds to a large opening in containment and a very large release that is assumed to occur early before effective evacuation of the

surrounding population. The definition of an early release is based on no effective evacuation. Consideration of when or if the vessel is breached as a result of the core melt is not directly pertinent to the definition for early release. Therefore, a "late release" is one where there is effective evacuation. It is consistent with the worst case assumptions for accident scenario "n".

Using the above value of CPEF and assuming a LERF goal of 10^{-5} per year, an estimate of the individual early risk (IER) can be calculated as:

$IERy = (3x10^{-2}) * (10^{-5}) = 3x10^{-7}$/year.

The IER corresponding to a LERF = 10^{-5} per year is less than the early fatality QHO of $5x10^{-7}$ per year by a factor of about two. Using a LERF goal of 10^{-5} per year will thus generally ensure that the early fatality QHO is met. Therefore a LERF of 10^{-5}/year is an acceptable surrogate for the early fatality QHO.

Surrogate for the Latent QHO

The risk to the population from cancer "resulting from all other causes" is taken to be the cancer fatality rate in the U.S. which is about 1 in 500 or $2x10^{-3}$ per year. The safety goal criterion of one-tenth of one percent of this figure implies that the risk of fatal cancer to the population in the area near a nuclear power plant due to its operation should be limited to $2x10^{-6}$/ry; i.e.: 1/10 * 1% * $2x10^{-3}$ = $2x10^{-6}$.

The "area" is understood to be an annulus of 10-mile radius from the plant site boundary. The cancer risk is also determined on the basis of an average individual risk, i.e., by evaluating the number of latent cancers (societal risk) due to all accidents to a distance of 10 miles from the plant site boundary, weighted by the frequency of the accident, dividing by the total population to 10 miles, and summing over all accidents.

It can be shown that if a plant's CDF is 10^{-4} per year or less, the latent fatality QHO is generally met. This acceptance can be demonstrated numerically using the results of probabilistic consequence assessments carried out in Level 3 PSAs as follows:

(1) assuming that one accident sequence "m" dominates the latent fatality risk and the LLRF

(2) assuming the accident sequence dominating the risk is the worst case scenario:

- a large opening in the containment

- an unscrubbed release that occurs after effective evacuation of the surrounding population (i.e. no early fatalities occur)

(3) assuming that the accident occurs in an open containment, the conditional probability of large late release (CLLRPm) is 1.0

(4) using results from NUREG-1150 (Table 4.3-1) [I-5-4] for the Surry PRA

the largest conditional probability of latent fatality (CPLF) within a 10-mile radius of the plant for internal initiators is $4x10^{-3}$.

The calculated CPLF values are very uncertain and therefore the approach adopted was to select a conservative estimate of CPLF. A CPLF value was therefore selected from the high consequence-low frequency part of the uncertainty range. This CPLF value corresponds to a large opening in containment and a very large release. It is therefore consistent with the worst case assumptions for accident scenario “m”.

Using the above value of CPLF and assuming a CDF goal of 10^{-4} per year, an estimate of the individual latent risk (ILR) can be calculated as:

$$ILRm = (4x10^{-3}) * (10^{-4}) = 4x10^{-7}/year.$$

The ILR corresponding to a CDF = 10^{-4} per year is less than the latent cancer QHO of $2x10^{-6}$ per year by a factor of about five. Using a CDF goal of 10^{-4} per year will thus generally ensure that the latent cancer QHO is met. Therefore a CDF of 10^{-4}/year is an acceptable surrogate for the latent cancer QHO.

The application of the USNRC safety goals has evolved over time to serve as the basis for many USNRC regulatory initiatives, with the explicit consideration of risk as only one factor among many in making regulatory decisions. The consideration of risk information in regulatory decision making processes is consistent with the risk-informed approach to balance risk insights from PSAs with safety insights from deterministic analyses to assure activities at nuclear power plants are conducted safely. In this context, USNRC has continued ongoing activities in many risk-informed regulatory applications that help the agency to achieve a high level of confidence in public health and safety.

REFERENCES TO ANNEX V

[V-1] U.S. NUCLEAR REGULATORY COMMISSION, Safety Goals for the Operations of Nuclear Power Plants; Policy Statement, 51 Federal Register 30028, (1986).

[V-2] U.S. NUCLEAR REGULATORY COMMISSION, Staff Requirements Memorandum on SECY-89-102, Implementation of the Safety Goals, (1990).

[V-3] U.S. NUCLEAR REGULATORY COMMISSION, Regulatory Guide 1.174, An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, (1998).

[V-4] U.S. NUCLEAR REGULATORY COMMISSION, NUREG-1150 Severe Accident Risks: An Assessment for Five U.S. Nuclear Power Plants, (1990).

ANNEX VI. EXAMPLES OF SAFETY GOALS HIERARCHIES

This annex provides an overview of three examples of safety goals hierarchies developed by expert groups within other projects:

VI-1: Western European Nuclear Regulators Association

VI-2: Multinational Design Evaluation Project

VI-3: Nordic PSA Group

VI-1. DEVELOPMENTS BY WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION

The Western European Nuclear Regulators Association (WENRA) has the aim of developing a common approach to nuclear safety amongst its members. In 2006 it published a detailed set of Reference Levels for Existing Reactors [VI-1], which all participating nuclear regulators agreed to encompass in their regulatory requirements. WENRA then considered new reactors, defined as those in a final design or early construction stage, with the aim of developing a common position on Safety Objectives so that new nuclear power plants, licensed across Europe in the next few years, will be safer than existing ones.

WENRA's expectation [VI-2] is that compared to currently operating nuclear power plants, new nuclear power plants are to be designed, sited, constructed, commissioned and operated with the objectives of:

O1. Normal operation, abnormal events and prevention of accidents

- reducing the frequencies of abnormal events by enhancing plant capability to stay within normal operation.
- reducing the potential for escalation to accident situations by enhancing plant capability to control abnormal events.

O2. Accidents without core melt

- ensuring that accidents without core melt induce no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation).
- reducing, as far as reasonably achievable,
    - the core damage frequency taking into account all types of credible hazards and failures and credible combinations of events;
    - the releases of radioactive material from all sources.
- providing due consideration to siting and design to reduce the impact of external hazards and malevolent acts.

O3. Accidents with core melt

- reducing potential radioactive releases to the environment from accidents with core melt, also in the long term, by following the qualitative criteria below:
    - accidents with core melt which would lead to early or large releases have to be practically eliminated;
    - for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures.

O4. Independence between all levels of defence-in-depth

- enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately as addressed in the previous three objectives), to provide as far as reasonably achievable an overall reinforcement of defence-in-depth.

O5. Safety and security interfaces

- ensuring that safety measures and security measures are designed and implemented in an integrated manner. Synergies between safety and security enhancements should be sought.

O6. Radiation protection and waste management

- reducing as far as reasonably achievable by design provisions, for all operating states, decommissioning and dismantling activities:
    - individual and collective doses for workers;
    - radioactive discharges to the environment;
    - quantity and activity of radioactive waste.

O7. Leadership and management for safety

- ensuring effective management for safety from the design stage. This implies that the licensee:
    - establishes effective leadership and management for safety over the entire new plant project and has sufficient in house technical and financial resources to fulfil its prime responsibility in safety;
    - ensures that all other organizations involved in siting, design, construction, commissioning, operation and decommissioning of new plants demonstrate awareness among the staff of the nuclear safety issues associated with their work and their role in ensuring safety.

The objectives do not constitute a structure in themselves but do represent a set of higher level goals which are either technologically neutral or applicable to LWRs. However many of the terms used, which are generally defined in footnotes in reference [VI-2] need further amplification and are still under discussion.

The WENRA Reactor Harmonisation Working Group has published a further report [VI-3]. This report sets out the common positions established by the Reactor Harmonisation Working Group (RHWG) of WENRA on the selected key safety issues. The work was initiated and also a major part of the work was carried out before the Fukushima Dai-ichi accident. Therefore, the report also discusses some considerations based on the major lessons from the Fukushima Dai-ichi accident, especially concerning the design of new nuclear power plants, and how they are covered in the new reactor safety objectives and the common positions.

VI-2. DEVELOPMENTS BY THE MULTINATIONAL DESIGN EVALUATION PROJECT

The Multinational Design Evaluation Project (MDEP) is a group of nuclear regulatory authorities from fifteen countries, which have firm plans for new nuclear programmes: members are from North America, Europe and Asia. As part of their aim to get greater harmonisation of regulatory requirements and practices, a group was tasked with considering how to harmonise Safety Goals. A report [VI-4] and a position paper [VI-5] have been produced and published.

The MDEP work has two major differences from that of WENRA: firstly, it is explicitly intended to both apply to current technologies but also to advanced designs and, secondly, it attempts to set out a hierarchical approach. The hierarchy (Figure VI-1) starts from a practical statement of the requirements embodied in the Fundamental Safety Objective of the IAEA (protecting people from radiation risks), to which everyone subscribes. The second level, based partly on the basic defence-in-depth approach, introduces fourteen goals. The intention is that from these, lower level goals, probably still to some extent technology independent can be derived, which eventually can be technology specific. The claim is that by using this approach the level of safety achieved should be similar across different technologies and, perhaps more importantly, there is a clear connection between detailed Safety Goals and the overall safety aims.

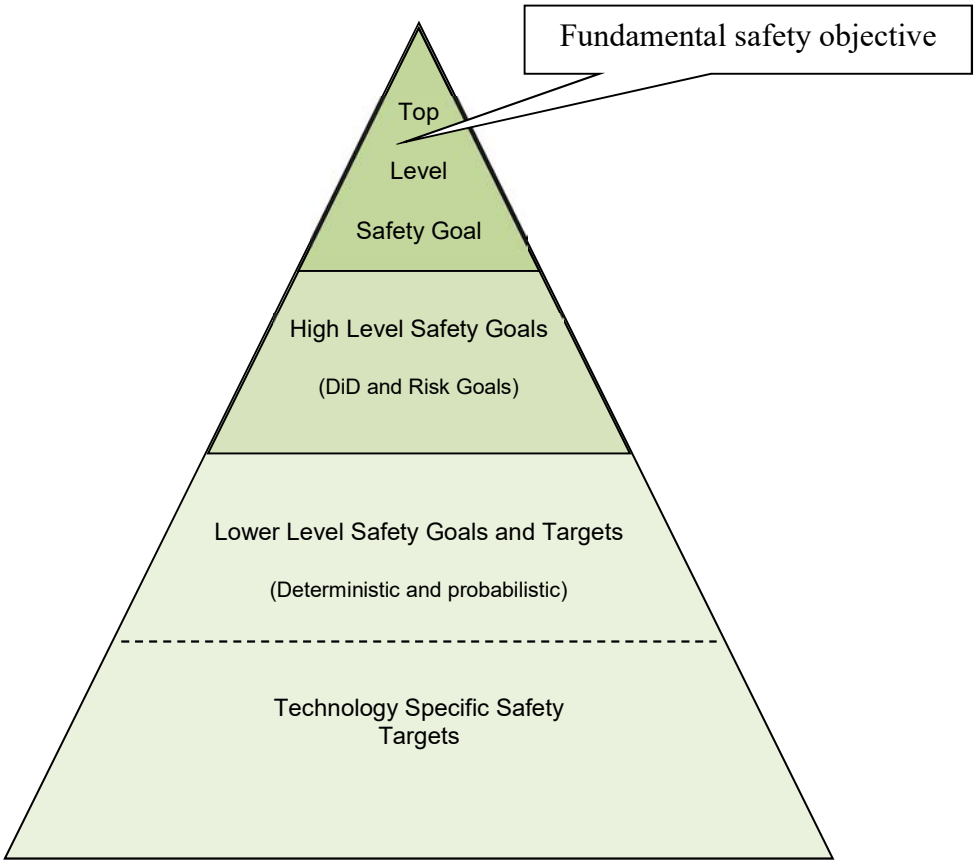

FIG VI-1. MDEP Hierarchy of Safety Goals.

MDEP has decided not to develop the structure further, although some suggested goals have been considered, but to encourage the IAEA to make use of it and the insights gained for its further work.

VI-3. NORDIC PSA GROUP PROJECT ON SAFETY GOALS FOR NUCLEAR POWER PLANTS

The project 'The Validity of Safety Goals' was initiated in 2006 by the Nordic PSA Group (NPSAG) composed by the utilities in Sweden and Finland and the Swedish Radiation Safety Authority. It is a four-year Nordic project dealing with the use of probabilistic safety criteria for nuclear power plants, and was documented in three project reports, [VI-6], [VI-7] and [VI-8]. An overview of the entire project is given in Figure VI-2.

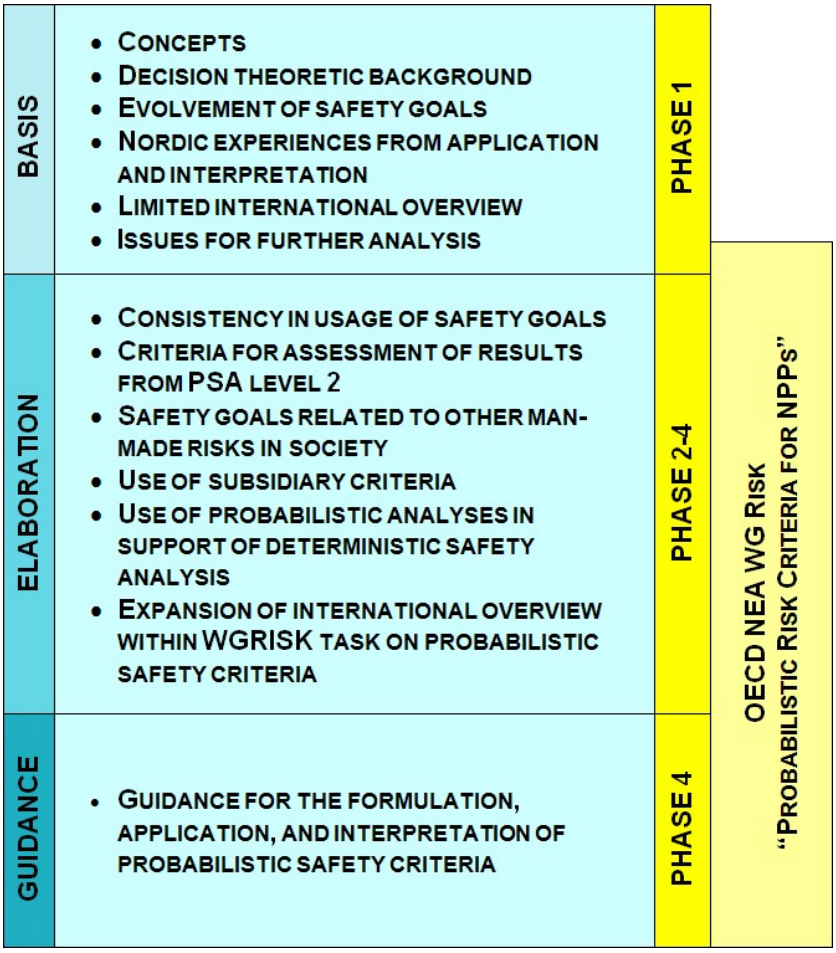

FIG. VI-2. Overview of the 4-year NPSAG project "The Validity of Safety Goals" (2006–2009).

The first phase of the project ("BASIS") was carried out with the aim to discuss and document current views, mainly in Finland and Sweden, on the use of Safety Goals, including both benefits and problems. The work has clarified the basis for the evolution of Safety Goals for nuclear power plants in Sweden and Finland and of experiences gained. This was achieved by performing a rather extensive series of detailed interviews with persons who are or have been involved in the formulation and application of the Safety Goals. The project report [II-6] presents the project context and a background to Safety Goals, as well as a historical review describing reasons for defining Safety Goals, context of goals and experiences. A number of specific issues related to the definition, interpretation and use of probabilistic Safety Goals were also identified and discussed. Towards the end of project phase 1, the OECD/NEA Working Group RISK started preparations for carrying out a task aimed at mapping probabilistic safety criteria in use in the member countries, and at collecting experiences from application of probabilistic criteria. The OECD/NEA task was defined and carried out in co-operation with the NPSAG project.

The second, third and fourth project phases ("ELABORATION") increased the scope and level of detail of the project by addressing a number of specific issues related to the application and use of Safety Goals, i.e.: consistency in the usage of Safety Goals, usage of probabilistic analyses in support of deterministic safety analysis, criteria for assessment of results from PSA Level 2 (criteria for off-site consequences), and the use of subsidiary criteria and relations between these. These phases also included the addition of a more systematic overview of international Safety Goals and experiences from their use, including participation in the OECD/NEA WGRISK Task 2006:2 'Probabilistic safety criteria' [VI-9], and a concise review

of Safety Goals related to other man-made risks in society, with focus on the railway and oil and gas industries. The fourth and final project phase has resulted in a final report summarising results from project phases 2-4 [VI-7].

The fourth project phase also included a "GUIDANCE" element aimed at providing practical guidance for the formulation, application and interpretation of probabilistic safety criteria. This was documented in a separate guidance document [VI-8].

The safety goals hierarchy suggested within the NPSAG project is comprised of four levels as shown in Figure VI-3.

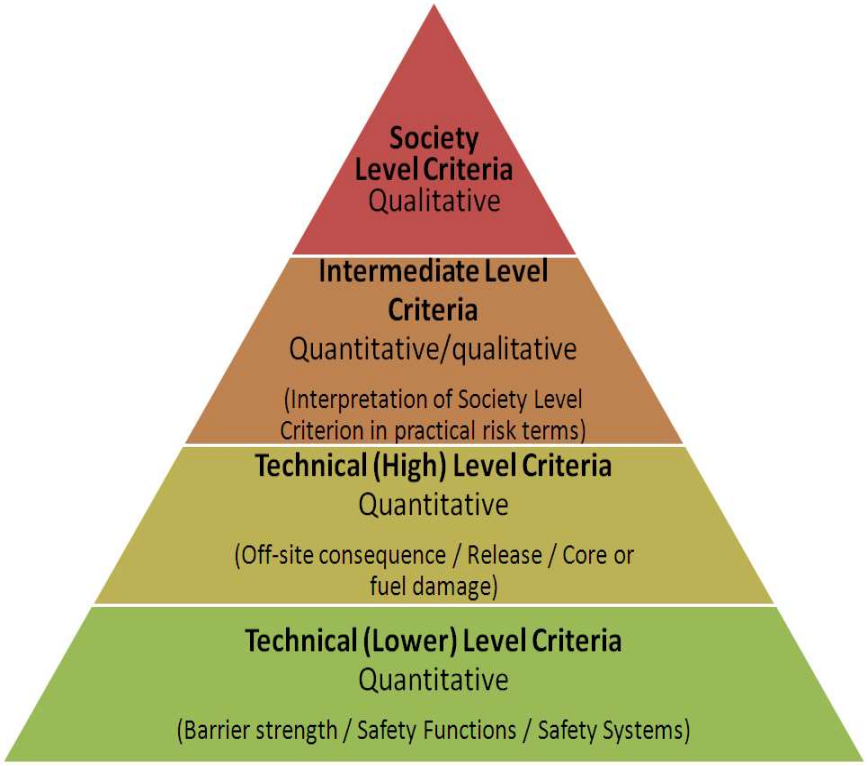

FIG. VI-3. Hierarchy of Safety Goals as described in Nordic NPSAG project.

The focus of the NPSAG project was on probabilistic safety goals, and the following summarises the way the four levels were defined in the project.

Society level

In many countries, nuclear safety is ultimately governed by qualitative criteria on society level, which are defined in nuclear legislation or issued by regulatory authorities. These criteria differ in wording between countries, but generally presuppose the "prevention of unreasonable risk to the public and the environment". Society level criteria are important as high-level statements, but cannot in themselves be used as a basis for defining numerical criteria.

Intermediate level

Intermediate level criteria are more precise and can be both qualitative and quantitative. They typically define "unreasonable" risk by comparison with the levels of risks coming from other involuntary sources of risk, e.g., with fatality risks from other sources of energy production or cancer fatality risks from other unnatural causes to which an individual is generally exposed.

Generally they express the requirement that “risks from use of nuclear energy shall or should be low compared to other risks to which the public is normally exposed”. Thus, intermediate level criteria are the implicit basis for defining the primary safety goal, which requires an interpretation in numerical terms of what constitutes an unreasonable risk to an individual or to society.

Technical level (high / low)

Criteria on technical level are quantitative, and always in some way or other aim at deciding whether a risk is acceptable or not. Criteria on technical level are typically defined on one or more of the following levels:

Higher technical level

- Off-site consequence level (corresponding to PSA level 3)
- Radioactive release from plant level (corresponding to PSA level 2)
- Core or fuel damage level (corresponding to PSA level 1)

Lower technical level (examples)

- barrier strength,
- reliability of safety function
- reliability of safety system

REFERENCES TO ANNEX VI

[VI-1] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Reactor Safety Reference Levels for Existing Reactors WENRA (2014). http://www.wenra.org/media/filer_public/2014/09/19/wenra_safety_reference_level_for_existing_reactors_september_2014.pdf

[VI-2] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, WENRA Statement on Safety Objectives for New Nuclear Power Plants, WENRA, (2010). http://www.wenra.org/media/filer_public/2012/11/05/wenra_statementonsafetyobjectivesfornewnuclearpowerplants_nov2010.pdf

[VI-3] WESTERN EUROPEAN NUCLEAR REGULATORS ASSOCIATION, Report: Safety of new NPP designs - Study by Reactor Harmonization Working Group RHWG, WENRA (2013). http://www.wenra.org/media/filer_public/2013/08/23/rhwg_safety_of_new_npp_designs.pdf

[VI-4] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, NUCLEAR ENERGY AGENCY - OECD/NEA, The Structure and Application of High Level Safety Goals – A Review by the MDEP Sub-committee on Safety Goals, OECD (2011).

[VI-5] MULTINATIONAL DESIGN EVALUATION PROGRAMME, Position Paper on Safety Goals, MDEP (2011). http://www.oecd-nea.org/mdep/documents/position-paper-on-safety-goals.pdf

[VI-6] HOLMBERG, J-E. and KNOCHENHAUER, M., Probabilistic Safety Goals. Phase 1 — Status and Experiences in Sweden and Finland. SSM Research Report 2007:06 (2007).

[VI-7] HOLMBERG, J.-E. and KNOCHENHAUER, M., Probabilistic Safety Goals – Phases 2-4 / Final Report; SSM Research Report 2010:35 (2011).

[VI-8] HOLMBERG, J.-E. and KNOCHENHAUER, M., Guidance for the Definition and Application of Probabilistic Safety Criteria; SSM Research Report 2010:36 (2011).

[VI-9] HESSEL, P. et al., Probabilistic Risk Criteria and Safety Goals; Nuclear Energy Agency Committee on the Safety of Nuclear Installations; NEA/CSNI/R(2009)16, NEA (2009).

ANNEX VII. EXAMPLE OF AN APPROACH FOR DEFINING LOW LEVEL PROBABILISTIC SAFETY GOALS

The approach described in this annex is based on the approach defined in the guidance for the definition and application of probabilistic safety criteria issued by the Nordic PSA Group [VII-1].

VII-1. MAIN CONSTITUENTS OF A PROBABILISTIC SAFETY GOAL

Defining low level probabilistic safety goals involves a number of steps. After the important initial definition of the basis for the safety goal, i.e., stating why it is needed and what it is expected to bring, defining a probabilistic safety goal on a technical level typically consists of four parts as described below.

Please note that the examples given are not recommendations, but rather hypothetical examples of how each part might be defined in a specific case.

- The definition of the safety goal

  This states the safety goal, e.g., "the core damage frequency of a nuclear power plant shall be $< 10^{-5}$/year".

  NB: In order for the safety goal to be relevant, further definition is required, e.g., of "core damage", and of "$< 10^{-5}$/year".

- The scope of the safety goal

  This defines what the safety goal is to be applied on, e.g., "a full scope PSA for the power operation mode".

- The target of the safety goal

  This defines the facility to which the safety goal applies, e.g., "the safety goal applies to new NPPs only" or "the safety goal applies on a per reactor-unit basis where the facility is a multi-unit site"

- The application procedure

This defines how the safety goal is to be applied, including when to apply it, how to apply it and the consequences of not meeting the safety goal, e.g., "The safety goal is to be applied in connection with every major PSA update. In case the safety goal is not met, the reason shall be identified and, if needed and justified corrective actions related to the PSA model (addressing, e.g., simplifications, conservative assumptions, or completeness issues), or plant design or procedures, shall be initiated".

VII-2. DEFINITION OF A PROBABILISTIC SAFETY GOAL

A probabilistic safety goal is generally defined by a *consequence*, a *metric* for the consequence, a *risk metric*, and a *frequency or probability*.

- The *consequence* is the ***end state*** considered for a specific probabilistic safety goal, e.g., the consequence may be "core damage" for a safety goal related to PSA Level 1.
- The *metric* is needed in order to define the consequence further, e.g., by characterizing the nature or extent of fuel damage or by defining "core damage" to have occurred if the local fuel cladding temperature in any part of the core has exceeded e.g. 1204 ºC for a LWR NPP using Zr based fuel clad material.

- The *risk metric* is defined by assigning a frequency of occurrence or probability to the metric, e.g., by measuring the risk of “core damage” in terms of the “core damage frequency”.
- The *frequency or probability* define the acceptance level for the risk metric, e.g., by stating that the “core damage frequency shall be shown to be < 10^{-5} per reactor year of operation”.

Some further definitions relate to the presentation and interpretation of the risk metric, i.e.:

- Consideration of uncertainties

  The safety goal should state whether the application relates to the best estimate (or mean value) of the frequency or probability, or if it shall be related to some level of confidence. The definitions for “best estimate”, “confidence level”, etc., requested in the application should be provided.

- Justification of the definitions made

  Reference documents or supporting analyses are needed to justify the selected definitions, e.g., in order to justify why the metric "core damage" is interpreted (for LWR’s) as "fuel cladding temperature > 1204 °C".

This section provides guidance on the definition of PSA-based low level safety goals. The examples given are for a LWR NPP, but the information given should be largely applicable to other types of NPPs as well, and partly applicable to other types of facilities.

Thus, low level safety goals are often defined on one or more of the following rubrics:

- Off-site consequence level (could correspond to PSA Level 3)
- Radioactive release from plant level (could correspond to PSA Level 2)
- Core or fuel damage level (could correspond to PSA level 1)
- Lower technical criteria; numerous possibilities exist in terms of PSA and/or non-PSA criteria (barrier strength, reliability of safety function, reliability of safety system, etc.)

Below, some general considerations are given for each of these criteria levels; this is largely based on the NPSAG guidance document [VII-1].

VII-3. DISCUSSION ON OFF-SITE CONSEQUENCE SAFETY GOALS

Off-site consequence safety goals are most closely related to the higher level safety goals, related to off-site health, societal and environmental effects. In terms of application to a NPP, a PSA Level 3 may be used to address off-site consequence safety goals.

Health risks are divided into fatal acute or fatal late health risks and these can be calculated for an individual or a group. In both cases, risk is defined as the risk to the member of a critical group that receives maximum exposure from an accident. Typically acute health effects have a threshold dose value under which the probability of health effect is not considered, but above which the probability of acute health effect is increased with increasing dose. Most late health effects are assumed not to have threshold values for dose. Based on these assumptions acute health effects can be expected in the vicinity of the release point if the release is above the threshold value, whereas late health effects potentially appear in the public exposed to radiation over larger areas.

The societal and environmental effects of a severe reactor accident include temporary evacuation and permanent relocation of the population, restrictions to the land use and effects on biosphere. The qualitative safety objective is to reduce the need for off-site countermeasures such as permanent relocation, emergency evacuation outside the immediate vicinity of the plant, limited sheltering, and long term restrictions in food consumption. Quantitative safety goals, related to the release criteria, could include the chance of not meeting timescales for initiation of countermeasures and limitations of the areas involved.

Safety goals defined on this level deal with risk to individuals or groups of the population or workers as well as with risks to the environment. As safety goals cover both acute and late effects, multiple safety goals need to be defined. In setting the goals consideration needs to be given to the counter-measures assumed and the extent to which their effectiveness will depend on the time of year and the time of day as the hypothetical persons for which the doses are evaluated will behave differently. In addition, the effective timescale for which a calculation is needed and the geographical spread should be defined.

The concepts involved in defining a safety goal for off-site consequences are shown and described in Table III-1, using as an example a set of criteria defined by the UK HSE [VII-2].

TABLE VII-1. CONCEPTS INVOLVED IN DEFINING AN OFF-SITE CONSEQUENCE SAFETY GOAL

Concept	Definition	Example
Consequence	Defines the health effects and the individual/group to which the safety goal applies.	Accident resulting in a dose to individuals off-site.
Metric	Qualifies the consequence (in this case "health effect") in terms of a measurable magnitude.	Dose received in the interval 10 to 100 mSv
Risk metric	Defines how the risk is to be expressed.	Frequency of achieving a dose rate in the interval defined.
Frequency/ probability	Defines specific levels related to the frequency/probability.	The UK approach involves the definition of a basic safety limit (BSL) not to be exceeded (except in exceptional circumstances), and a basic safety objective (BSO), below which the risk is considered to be broadly acceptable. BSL: 1 x E-4 / year BSO: 1 x E-6 / year

VII-4. DISCUSSION ON RELEASE SAFETY GOALS

Release safety goals are related to radioactive releases from the facility. In terms of application to a NPP, a PSA Level 2 may be used to address release safety goals.

Typically, releases for which safety goals have been defined can be expressed in several different ways, some examples being:

- Large release

  Expressed in terms of an absolute threshold magnitude of activity and isotopes released
- Large early release

Usually defined more qualitatively, e.g., “Large off-site releases requiring short term off-site response” or “Significant, or large release of Cs-137, fission products before applying the offside protective measures”.

– Containment failure safety goal (conditional probability)

  Related to robustness of the 4th level of Defence-in-Depth.

The definition of what constitutes an unacceptable release typically differs widely among different countries. Part of the reason for the complexity of the release definition, is the fact that in many countries it constitutes the link between the PSA Level 2 results and an indirect means of assessing health effects from the release. Such consequence issues can be more fully addressed in PSA Level 3.

The definition of release safety goals involves many parameters, the most important ones being the time, the amount, the temperature, and the composition of the release. Additionally, other aspects may be of interest, such as the height above ground of the point of release. This means that multiple safety goals may be defined, which is however unusual.

The concepts involved in defining release criteria are shown and described in Table VII-2, using as an example the release criterion defined by the SSM in Sweden [VII-3] and by STUK in Finland [VII-4].

TABLE VII-2. CONCEPTS INVOLVED IN DEFINING A RELEASE SAFETY GOAL

Concept	Definition	Example
Consequence	Defines the consequence related to the release.	Unacceptable release with respect to long-term ground contamination.
Consequence measure	Qualifies the consequence (in this case “release causing long-term ground contamination”) in terms of a measurable magnitude.	**Sweden:** Release of Cs-137 in excess of an amount corresponding to 0.1% of the core inventory in a 1800 MWt reactor (equivalent to about 103 TBq of Cs-137). **Finland:** Release of > 100 TBq of Cs-137.
Risk metric	Defines how the risk of exceeding the specified consequences is to be expressed.	**Sweden:** No risk metric has been defined by SSM. However, it is stated that a release exceeding the limit shall be “extremely unlikely”, indicating consideration of an occurrence frequency. **Finland:** Frequency of exceeding the release limit.
Frequency/ probability	Defines specific levels related to the frequency/probability.	**Sweden:** “Extremely unlikely” has been interpreted to indicate a limit between 10^{-6} and 10^{-7} per year. **Finland**: The criterion is defined as a frequency limit, which is set to $5 \cdot 10^{-7}$ per year.

VII-5. DISCUSSION ON CORE DAMAGE SAFETY GOALS

Core damage safety goals are related to damage to the fuel in the core. In terms of application to a NPP, a PSA Level 1 may be used to address core damage safety goals. It is worth noting, that there is some vagueness in the use of the concept “core damage”, as fuel may be damaged or overheat in other locations than the core.

The definition of what constitutes a core damage is rather homogenous among countries using the criterion for LWRs, usually defined as local fuel temperature above 1204 ºC, i.e., the limit defined in section 1b of 10 CFR 50.46, Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors [VII-5].

In success criteria analysis for PSA, it can be more practical in some scenarios to use other criteria than local fuel temperature, having, however, the same intention to define a criterion when core cooling is considered lost resulting in fuel melting.

Another question is whether mechanical damage of fuel due to dropped load or fuel handling error should be defined as fuel damage. Such events are relevant to the refuelling outage PSA, and there is a variation regarding the way mechanical fuel damage is accounted.

The concepts involved in defining a criterion for core damage are shown and described in Table VII-3, using as an example criteria defined for the Oskarshamn NPPs by E.ON Nordic [VII-6].

It should also be noted that in some facilities (including NPPs) damage of fuel in different locations is to be included in the safety considerations.

TABLE VII-3. CONCEPTS INVOLVED IN DEFINING CORE DAMAGE SAFETY GOALS

Concept	Definition	Example
Consequence	Defines the consequence related to the fuel overheating.	Severe core damage
Metric	Qualifies the consequence (in this case "severe core damage") in terms of a measurable magnitude.	"Severe" is not qualified, but previous versions of the safety policy have referred to 10 CFR 50.46 (local fuel temperature above 1204 ºC).
Risk metric	Defines how the risk is to be expressed.	Frequency of exceeding the limit. *Note: As long as "severe" is not defined, there is some vagueness in the definition of the risk metric.*
Frequency/ probability	Defines specific levels related to the frequency/probability.	The criterion is defined as a frequency target, which is set to $1 \cdot 10^{-5}$ per reactor year.

VII-6. DISCUSSION ON SSC LEVEL SAFETY GOALS

SSC level safety goals can be useful for assessing barrier strength, especially in the defence in depth context. In order to create a connection with defence in depth, barrier strength safety goals may be defined. Lower level safety goals can also be useful as design guidance.

The concepts involved in defining a lower level safety goal are the same as on higher levels, but the definitions may obviously differ considerably from case to case. In Table VII-4, an example is given for a containment integrity criterion.

TABLE VII-4. CONCEPTS INVOLVED IN DEFINING LOWER LEVEL SAFETY GOALS (EXAMPLE FOR CONTAINMENT INTEGRITY CRITERION)

Concept	Definition	Example
Consequence	Defines the consequence related to the fuel overheating.	Loss of containment integrity (resulting in an unacceptable release) after core damage has occurred.
Metric	Qualifies the consequence (in this case "loss of containment integrity") in terms of a measurable magnitude.	Must be based on the metric already defined for the criteria on the levels of core damage and release.
Risk metric	Defines how the risk is to be expressed.	Probability of exceeding the metric related to the release criterion, after the metric related to the core damage criterion has been exceeded.
Frequency/ probability	Defines specific levels related to the frequency/probability.	The criterion is defined as a conditional probability, with a limit set to 0.1. *Note: This criterion can be used both if the higher level criteria are defined as single criteria and if they are ALARP criteria with a limit and an objective.*

REFERENCES FOR ANNEX VII

[VII-1] HOLMBERG, J.-E. and KNOCHENHAUER, M., Guidance for the Definition and Application of Probabilistic Safety Criteria; SSM Report 2010:36, Swedish Radiation Safety Authority (SSM), Stockholm (2011).

[VII-2] HEALTH AND SAFETY EXECUTIVE, NII Safety Assessment Principles for Nuclear Facilities; HSE 2006; HSE, Health and Safety Executive (2006).

[VII-3] SKI/SSI; Release limiting measures after severe accidents (Utsläppsbegränsande åtgärder vid svåra härdhaverier); SKI ref 7.1.24 1082/85; SKI/SSI,(1985).

[VII-4] RADIATION AND NUCLEAR SAFETY AUTHORITY, Probabilistic safety analysis in safety management of nuclear power plants; GuideYVL-2.8. ISBN 951-712-786-3; STUK, Finland (2003).

[VII-5] NUCLEAR REGULATORY COMMISSION, 10 CFR 50.46, Acceptance criteria for emergency core cooling systems for light-water nuclear power reactors. Washington, DC (2017).

[VII-6] E.ON NORDIC; E.ON Nordic Safety policy for nuclear power plants (Säkerhetspolicy för kärnkraft inkl. förklarande text), EON/ SKKÖT-050609-01, E.ON Kärnkraft Sverige AB, Sweden (2005).

ABBREVIATIONS

AGR	Advanced Gas-Cooled Reactor
ALARA	As Low As Reasonably Achievable
ALARP	As Low As Reasonably Practicable
BWR	Boiling Water Reactor
CANDU	CANada Deuterium Uranium (reactor)
CDF	Core Damage Frequency
DBA	Design Basis Accident
DiD	Defence in Depth
ICRP	International Commission on Radiological Protection
LERF	Large Early Release Frequency
LRF	Large Release Frequency
LWR	Light Water Reactor
MDEP	Multinational Design Evaluation Project
NEA	Nuclear Energy Agency
NPP	Nuclear Power Plant
NPSAG	Nordic PSA Group
OECD	Organization for Economic Cooperation and Development
PSA	Probabilistic Safety Assessment
PSR	Periodic Safety Review
PWR	Pressurized Water Reactor
QHO	Quantitative Health Objective
SAM	Severe Accident Management
SAMG	Severe Accident Management Guidelines
SSC	Systems, Structures and Components
SSM	Swedish Radiation Safety Authority
WENRA	Western European Nuclear Regulator Association

CONTRIBUTORS TO DRAFTING AND REVIEW

Ammirabile, L.	European Commission/Joint Research Centre European Commission, The Netherlands
Ashworth, A.	Chalk River Laboratories, Canada
Azlina, B.M.J.	Malaysia Nuclear Power Corporation (MNPC), Malaysia
Barbaud, J.	Électricité de France (EDF), France
Bellens, V.	GDFSUEZ, Belgium
Berg, H.-P.	Bundesamt für Strahlenschutz, Germany
Berger, J.P.	European Atomic Forum, France
Buttery, N.	EDF Energy Sizewell B Power Station, United Kingdom
Ciurea, C.E.	National Commission for Nuclear Activities Control (CNCAN), Romania
Csaba, B.	Hungarian Power Companies Ltd., Hungary
Dermarkar, F.	Ontario Power Generation, Canada
El-Shanawany, M.	Imperial College London, Centre for Nuclear Safety, UK
Eltawila, F.	Federal Authority for Nuclear Regulation (FANR), United Arab Emirates
Evrard, J.M.	IRSN, France
Feron, F.	Autorité de sûreté nucléaire (ASN), France
Froehmel, T.	World Nuclear Association (WNA), Germany
Giorgi, G.	ENEL, Italy
Godinez, S.V.	CNSNS, Mexico
Golshan, M.	Health and Safety Executive Office for Nuclear Regulation, United Kingdom
Grant, I.M.	Federal Authority for Nuclear Regulation (FANR), United Arab Emirates
Gress, P.	Organization for Economic Co-Operation and Development, France
Gupta, O.	Autorité de sûreté nucléaire (ASN), France
Hellstroem, P.	Swedish Regulatory Safety Authority, Sweden
Huang D.	Support Center of China Atomic Energy Authority (CAEA), China
Hwang, T.S.	Korea Institute of Nuclear Safety, Korea
Ibrahim, M.A.	Atomic Energy Authority, Egypt
Johnston, A.	AECL, Canada
Kimtys, E.	State Nuclear Power Safety Inspectorate (VATESI), Lithuania
Knochenhauer, M.	Swedish Radiation Safety Authority, Sweden
Krauss, M.	Bundesamt für Strahlenschutz (BfS), Germany
Krenicky, L.	World Association of Nuclear Operators, United Kingdom
Kuzmina, I.	International Atomic Energy Agency
Lankin, M.	Federal Environmental, Industrial and Nuclear Supervision Service of Russia (Rostechnadzor); Scientific and Engineering Centre for Nuclear and Radiation Safety (SEC NRS), Russia

Lignini, F.M.	AREVA, France
Lorencez, C. M.	Ontario Power Generation, Canada
Lyubarskiy, A.	International Atomic Energy Agency
Mertins, M.	Gesellschaft für Anlagen- und Reaktorsicherheit (GRS), Germany
Mishra, L.	NRB Office, India
Nagy, S.	Hungarian Power Companies Ltd., Hungary
Nguyen, A.T.	Ministry of Science and Technology (MOST), Vietnam
Pouget-Abadie, X.	EDF, France
Rashid, S.	Pakistan Nuclear Regulatory Authority (PNRA), Pakistan
Reiman, L.	Radiation and Nuclear Safety Authority (STUK), Finland
Rodeghiero, P.	Tractebel Engineering, Belgium
Sekkouri, A.R.	Office national de l'électricité (ONE), Morocco
Shi, G.	SNERDI, China
Sholly, S.	Institute of Safety and Risk Sciences, Austria
Spitzer, C.	International Atomic Energy Agency
Steyn, I.	QSS; South African Nuclear Energy Corp. (NECSA), South Africa
Tombuyses, B.	Federal Agency of Nuclear Control, Belgium
Toth, A.F.	Hungarian Atomic Energy Authority (HAEA), Hungary
Toth, C.	Hungarian Power Companies Ltd., Hungary
Travers, W.D.	Federal Authority for Nuclear Regulation (FANR), United Arab Emirates
Tronea, M.C.	National Commission for Nuclear Activities Control (CNCAN), Romania
Van Doesburg, W.	RESUN AG, Switzerland
Vaughan, G.	Consultant, United Kingdom
Vecchiarelli, J.	Ontario Power Generation, Canada
Wallin-Caldwell, L.	SSM, Sweden
Webster, P.	Canadian Nuclear Safety Commission, Canada
Wong, S.-M.	US Nuclear Regulatory Commission (USNRC), United States of America
Zawadka, D.	Polish Energy Group (PGESA), Poland
Zhang, S.	China Power Investment, China
Zheng, H.	CGNPC, China

IAEA
International Atomic Energy Agency

No. 26

ORDERING LOCALLY

IAEA priced publications may be purchased from the sources listed below or from major local booksellers.

Orders for unpriced publications should be made directly to the IAEA. The contact details are given at the end of this list.

NORTH AMERICA

Bernan / Rowman & Littlefield

15250 NBN Way, Blue Ridge Summit, PA 17214, USA
Telephone: +1 800 462 6420 • Fax: +1 800 338 4550
Email: orders@rowman.com • Web site: www.rowman.com/bernan

Renouf Publishing Co. Ltd

22-1010 Polytek Street, Ottawa, ON K1J 9J1, CANADA
Telephone: +1 613 745 2665 • Fax: +1 613 745 7660
Email: orders@renoufbooks.com • Web site: www.renoufbooks.com

REST OF WORLD

Please contact your preferred local supplier, or our lead distributor:

Eurospan Group

Gray's Inn House
127 Clerkenwell Road
London EC1R 5DB
United Kingdom

Trade orders and enquiries:

Telephone: +44 (0)176 760 4972 • Fax: +44 (0)176 760 1640
Email: eurospan@turpin-distribution.com

Individual orders:

www.eurospanbookstore.com/iaea

For further information:

Telephone: +44 (0)207 240 0856 • Fax: +44 (0)207 379 0609
Email: info@eurospangroup.com • Web site: www.eurospangroup.com

Orders for both priced and unpriced publications may be addressed directly to:

Marketing and Sales Unit
International Atomic Energy Agency
Vienna International Centre, PO Box 100, 1400 Vienna, Austria
Telephone: +43 1 2600 22529 or 22530 • Fax: +43 1 26007 22529
Email: sales.publications@iaea.org • Web site: www.iaea.org/books

International Atomic Energy Agency
Vienna
ISBN 978–92–0–103119–8
ISSN 1011–4289