IAEA TECDOC SERIES

IAEA-TECDOC-1902

INPRO Methodology for Sustainability Assessment of Nuclear Energy Systems: Safety of Nuclear Reactors

INPRO Manual

IAEA
International Atomic Energy Agency

INPRO METHODOLOGY FOR SUSTAINABILITY ASSESSMENT OF NUCLEAR ENERGY SYSTEMS: SAFETY OF NUCLEAR REACTORS

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-1902

INPRO METHODOLOGY FOR SUSTAINABILITY ASSESSMENT OF NUCLEAR ENERGY SYSTEMS: SAFETY OF NUCLEAR REACTORS

INPRO MANUAL

INTERNATIONAL ATOMIC ENERGY AGENCY
VIENNA, 2020

COPYRIGHT NOTICE

For further information on this publication, please contact:

INPRO 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
March 2020

IAEA Library Cataloguing in Publication Data

Names: International Atomic Energy Agency.
Title: INPRO methodology for sustainability assessment of nuclear energy systems: safety of nuclear reactors / International Atomic Energy Agency.
Description: Vienna : International Atomic Energy Agency, 2020. | Series: IAEA TECDOC series, ISSN 1011–4289 ; no. 1902 | Includes bibliographical references.
Identifiers: IAEAL 20-01301 | ISBN 978–92–0–102720–7 (paperback : alk. paper) | ISBN 978–92–0–102820–4 (pdf)
Subjects: LCSH: International Project on Innovative Nuclear Reactors and Fuel Cycles. | Nuclear energy. | Nuclear reactors — Safety measures. | Sustainable energy strategies.

FOREWORD

The International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) was launched in 2000, based on resolutions of the IAEA General Conference (GC(44)/RES/21). One of the INPRO objectives is to help to ensure that nuclear energy is available in the twenty-first century in a sustainable manner. To meet this objective, INPRO has been proceeding in steps.

In Phase 1, INPRO developed a methodology for assessing the long term sustainability of a national or international nuclear energy system. This entailed establishing a set of basic principles pertaining to system sustainability, a set of user requirements in support of each basic principle, and a set of criteria for meeting each user requirement. The resulting INPRO methodology was documented in the form of a sustainability assessment guidance manual consisting of an overview volume and eight volumes covering economics, infrastructure, waste management, proliferation resistance, physical protection, environment, safety of reactors and safety of nuclear fuel cycle facilities. The first edition of that manual was published in 2008 as IAEA-TECDOC-1575/Rev.1.

In Phase 2, Member States participating in INPRO have been performing national and international nuclear energy system assessments (NESAs) using the INPRO methodology. The results of those NESAs completed by 2009 were published at the end of 2009 as IAEA-TECDOC-1636. Included in that IAEA publication were several proposals on how to update the INPRO methodology based on the experience of the assessors. Further recommendations on how to update the methodology were developed in parallel by the INPRO steering committee, IAEA experts and the INPRO group.

All the proposals and recommendations were evaluated by internal and external experts at an IAEA consultancy meeting in 2012, and IAEA technical meetings in 2013 and 2016. Based on the outcomes of those meetings, the INPRO sustainability assessment methodology was updated. This publication covers the updated INPRO methodology for the area of safety of nuclear reactors.

The IAEA officers responsible for this publication were A. Korinny and J. Phillips of the Division of Nuclear Power.

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

SUMMARY 1
1. INTRODUCTION 4
1.1. Background 4
1.2. Objective 5
1.3. Scope 5
1.4. Structure 6
2. GENERAL FEATURES OF NUCLEAR ENERGY SYSTEMS SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY 11
2.1. Existing requirements for reactor safety 11
2.2. Requirements for future reactors 12
2.3. The concept of sustainable development and its relationship to the INPRO methodology area of reactor safety 13
2.4. The concept of defence in depth and its relationship to the INPRO methodology area of reactor safety 17
3. NECESSARY INPUT FOR INPRO SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY 20
3.1. Definition of nuclear energy system 20
3.2. INPRO assessment by a technology user 20
3.3. Results of safety analyses 21
3.4. INPRO assessment by a technology developer 21
3.5. Other sources of input 21
4. INPRO BASIC PRINCIPLE, USER REQUIREMENTS AND CRITERIA FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY 22
4.1. Introduction 22
4.2. INPRO basic principle for sustainability assessment in the area of safety of nuclear reactors 22
4.3. UR1: Robustness of design during normal operation 23
4.3.1. Criterion CR1.1: Design of normal operation systems 25
4.3.2. Criterion CR1.2: Reactor performance 28
4.3.3. Criterion CR1.3: Inspection, testing and maintenance 31
4.3.4. Criterion CR1.4: Failures and deviations from normal operation 32
4.3.5. Criterion CR1.5: Occupational dose 33
4.4. UR2: Detection and interception of anticipated operational occurences 35
4.4.1. Criterion CR2.1: I&C system and inherent characteristics 36
4.4.2. Criterion CR2.2: Grace periods after AOOs 37

4.4.3. Criterion CR2.3: Inertia 38
4.5. UR3: Design basis accidents 38
4.5.1. Criterion CR3.1: Frequency of DBAs 40
4.5.2. Criterion CR3.2: Grace period for DBAs 40
4.5.3. Criterion CR3.3: Engineered safety features 41
4.5.4. Criterion CR3.4: Barriers 42
4.5.5. Criterion CR3.5: Subcriticality margins 43
4.6. UR4: Severe plant conditions 44
4.6.1. Criterion CR4.1: Frequency of release into the containment/ confinement 45
4.6.2. Criterion CR4.2: Robustness of containment/ confinement design 46
4.6.3. Criterion CR4.3: Accident management 48
4.6.4. Criterion CR4.4: Frequency of accidental release into environment 48
4.6.5. Criterion CR4.5: Source term of accidental release into environment 50
4.7. Emergency preparedness and response 51
4.8. UR5: Independence of DID levels, inherent safety characteristics and passive safety systems 52
4.8.1. Criterion CR5.1: Independence of DID levels 55
4.8.2. Criterion CR5.2: Minimization of hazards 56
4.8.3. Criterion CR5.3: Passive safety systems 58
4.9. UR6: Human factors related to safety 58
4.9.1. Criterion CR6.1: Human factors 59
4.9.2. Criterion CR6.2: Attitude to safety 60
4.10. UR7: Necessary RD&D for advanced designs 60
4.10.1. Criterion CR7.1: Safety basis and safety issues 62
4.10.2. Criterion CR7.2: RD&D 62
4.10.3. Criterion CR7.3: Computer codes 65
4.10.4. Criterion CR7.4: Novelty 66
4.10.5.Criterion CR7.5: Safety assessment 67
4.11. Concluding remarks 70
APPENDIX I: EXAMPLES OF REFERENCE REACTORS FOR INPRO ASSESSMENT 71
APPENDIX II: EXAMPLE OF APPROACH TO THE ASSESSMENT OF REACTOR CORE DESIGHN MARGINS 72
APPENDIX III: EXAMPLES OF MONITORING SYSTEMS 74
APPENDIX IV: FREQUENCIES OF DBA 76
APPENDIX V: ENGINEERED SAFETY FEATURES 78

APPENDIX VI: CONFINEMENT BARRIERS 81
APPENDIX VII: ACCIDENT MANAGEMENT 82
APPENDIX VIII: ESTIMATION OF CONSEQUENCE OF EXTERNAL RELEASE 84
APPENDIX IX: HUMAN FACTOR CONSIDERATION 86
APPENDIX X: SAFETY CULTURE CONSIDERATION 88
REFERENCES 90
GLOSSARY 96
LIST OF ABBREVIATIONS 98
CONTRIBUTORS TO DRAFTING AND REVIEW 99

SUMMARY

This report, which is part of the INPRO methodology manual, provides guidance for assessing sustainability of a nuclear energy system (NES) in the area of safety of nuclear reactors. The sustainability assessment approach described is not an application of the IAEA safety standards and in no way replaces the safety assessments to be performed as part of the pre-licensing and licensing processes for a nuclear reactor. The manual focuses instead on the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) methodology for sustainability assessment requirements in the area of reactor safety that need to be fulfilled to demonstrate the long term sustainability of the NES assessed by primarily focusing on selected areas of reactor safety that are important for public acceptance.

The INPRO methodology for assessing NES sustainability in the area of safety of nuclear reactors consists of one INPRO basic principle, seven INPRO user requirements, and twenty-eight criteria.

The INPRO basic principle for sustainability assessment in the area of nuclear reactor safety sets the goal for designers/developers to achieve an advanced nuclear power plant (NPP) design that is demonstrably safer than a comparable reference NPP design now in operation and can thus prevent or mitigate off-site releases of radionuclides more efficiently. To approach this high level goal, the INPRO methodology encourages the designer to:

- Incorporate enhanced defence in depth (DID) into an advanced nuclear reactor design as part of the fundamental safety approach and ensure that the levels of protection in DID are more independent from each other than in a reference plant;
- When appropriate to minimize hazards, incorporate inherently safe characteristics and passive systems into advanced designs as part of a fundamental approach to excelling in safety and reliability;
- Take human factors into account in the design and operation of a nuclear reactor.
- Perform sufficient research, development and demonstration (RD&D) work to bring the knowledge of nuclear plant characteristics and the capability of analytical methods used for design and safety assessment of an assessed plant with innovative features to at least the same confidence level as for a reference plant.

In addition, the INPRO methodology encourages all organizations involved in a nuclear power programme to establish and maintain a strong safety culture.

The first four INPRO user requirements (UR1 to UR4) for sustainability assessment in the area of safety of nuclear reactors are linked to the DID concept, in particular levels 1 through 4. Level 5 of the DID concept is dealt with in the INPRO methodology area of Infrastructure [1].

The first user requirement for sustainability assessment in the area of safety of nuclear reactors, UR1, is related to the first level of DID, which is focused on preventing deviations from normal operation and preventing failures of items important to safety. UR1 asks for an increase of robustness in the design assessed relative to a reference design with regard to system and components failures as well as operation. The major means to achieve robustness are to ensure high quality in design, construction and operation, including human performance. UR1 further asks for an efficient implementation of the concept of optimization of worker radiation protection through the use of automation, remote maintenance and operational experience from existing designs.

The second user requirement for sustainability assessment in the area of safety of nuclear reactors, UR2, involves limited consideration of selected provisions in the first DID level and

mostly relates to the second level of DID, which deals with detection and control of failures and deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. UR2 asks for inherent safety characteristics to compensate for deviations and for an adequate or improved instrumentation and control (I&C) system that can detect anticipated operational occurrences (AOOs) and return the plant to normal operation. Additionally, the I&C system should detect failures and initiate mitigating measures.

The third user requirement for sustainability assessment in the area of safety of nuclear reactors, UR3, is mostly related to the third level of DID, which concentrates on controlling accidents, preventing damage to the reactor core, preventing radioactive releases that would require off-site protective actions and ultimately returning the plant to a safe state. UR3 asks for new designs to have less frequent design basis accidents (DBAs), longer grace periods for operator actions after DBAs, and greater reliability of engineered safety features than in a reference design. UR3 further stipulates that a defined number of barriers against an accidental release of radioactivity should remain intact in all potential DBAs and design extension conditions (DECs).

The fourth user requirement for sustainability assessment in the area of safety of nuclear reactors, UR4, is focused on accident conditions more severe than DBAs. UR4 is mainly related to the design extension conditions (DECs) in the third level of DID. UR4 also relates to the fourth level of DID, which aims to mitigate the consequences of accidents that result from failure of the third level of DID by preventing the progression of such accidents and mitigating the consequences of severe accidents. UR4 asks for assessed designs that, relative to a reference design, have a reduced frequency of accidents with release of radioactivity into the containment due to severe core damage. UR4 further stipulates the existence of sufficient natural or engineered processes to control the system and adequate on-site accident management measures to prevent or mitigate radioactive releases to the environment after such a severe accident.

The fifth user requirement for sustainability assessment in the area of safety of nuclear reactors, UR5, asks for increased independence of each DID level to be confirmed using appropriate methods (e.g. probabilistic and deterministic analysis) and for minimization of hazards by incorporating, when appropriate, inherently safe characteristics and passive systems into the design assessed.

The sixth user requirement for sustainability assessment in the area of safety of nuclear reactors, UR6, asks that the safe operation of the assessed plant be supported by an improved human-systems interface and by the establishment and maintenance of a strong safety culture in all national organizations involved in a nuclear power programme.

The seventh user requirement for sustainability assessment in the area of safety of nuclear reactors, UR7, asks the nuclear technology developer to perform sufficient RD&D for innovative design features to bring the knowledge of advanced plant characteristics and the capability of analytical methods to at least the same confidence level as for existing nuclear plants.

INPRO methodology user requirements on nuclear energy system sustainability related to nuclear law, institutional arrangements including the regulatory body, and emergency preparedness and response have been considered as part of the national infrastructure necessary to create and maintain a sustainable nuclear energy system and are therefore published in the INPRO manual covering the infrastructure area [1].

INPRO methodology user requirements on nuclear energy system sustainability in the area of safety can be interpreted as proposals to the designers of new nuclear technology on how to

increase the safety level of a new design in comparison to a reference design (as targeted in the basic principle). The INPRO methodology justifies the requested increase in safety by noting that an assumed significant increase of installed nuclear power during the twenty-first century would theoretically increase the risks of nuclear power, unless nuclear technology is developed further with regard to enhanced safety. Therefore, the overall objective of the INPRO methodology in the area of safety of nuclear reactors is to demonstrate continuous improvement of the safety characteristics of nuclear reactor designs. This implies that the INPRO assessment will be carried out successfully for new reactors that are expected to contribute to the assumed expansion of nuclear power and requires a coordinated global effort to ensure that new reactor designs are sufficiently safe to avoid or minimise a potential increase in the global risks of nuclear power.

In summary, the elements of the INPRO methodology described in this publication (i.e. sustainability assessment in the area of reactor safety) evaluate enhancements in the safety of new reactor designs but do not evaluate compliance with national or international safety standards. The INPRO assessment is performed with respect to a reference design that is assumed to comply with applicable safety standards. The assessed design is likewise assumed to comply with applicable safety standards. Confirmation of compliance of the reference or new design with national or international safety standards is outside the scope of the INPRO methodology. If such confirmation is needed, a separate assessment or peer review should be performed[1].

[1] Peer review of the safety assessment report should be performed based on applicable national regulations and IAEA safety standards. The IAEA's Technical Safety Review (TSR) service can assist in this regard.

1. INTRODUCTION

1.1. BACKGROUND

This publication is an update of Volume 8, Safety of Nuclear Reactors, of the INPRO manual published as IAEA-TECDOC-1575 Rev.1, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems [2]. The update is based on recommendations presented by Member States participating in the International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) and supplemented by IAEA experts. The information presented in the INPRO methodology overview manual published in Volume 1[2] of Ref [2] should be considered as an integral part of this publication and the user is invited to become familiar with that information.

The concept of sustainable development was originally introduced in the 1980s. It defines sustainable development as development that meets the needs of the present without compromising the ability of future generations to meet their own needs. This concept embraces all environmentally sensitive areas of human activities, including different types of energy production. In the area of nuclear energy, the focus of sustainable development is on solving key institutional and technological issues including nuclear accident risks, health and environment risks, proliferation risks, economic competitiveness, radioactive waste disposal, sufficiency of institutions and public acceptability. Sustainable development implies demonstration of progress in the key issue areas. The INPRO methodology is the tool for assessing the sustainability and sustainable development of a nuclear energy system, that was originally created in 2003 under the aegis of the IAEA using broad philosophical outlines of the concept of sustainable development.

INPRO basic principles, user requirements and criteria have been defined for assessing NES sustainability in different areas, i.e. economics, infrastructure (legal and institutional measures), waste management, proliferation resistance, environmental impact of stressors, environmental impact from depletion of resources, safety of nuclear reactors and safety of nuclear fuel cycle facilities. The INPRO basic principles establish goals that should be met in order to achieve long term sustainability of a NES. An INPRO user requirement of sustainability defines what different stakeholders (users) in a NES should do to meet the goal defined in the basic principle. A criterion enables the assessor to check whether a user requirement has been met. The ultimate goal of using the INPRO methodology is to determine whether the NES assessed fulfils all the criteria and meets the INPRO user requirements and basic principles of NES sustainability and therefore represents a long term sustainable system for a Member State (or group of Member States).

One possible output from an assessment of a NES is the identification of areas where a given NES needs to be improved. Given the comprehensive nature of an assessment using the INPRO methodology, such an assessment would be expected to indicate clearly the specific attributes of a NES that need to be improved. An assessor in a country embarking on a nuclear power programme has several options in using the INPRO methodology depending on the stage of the programme [1] (see also the introductory manual of the updated INPRO methodology).

Updated INPRO methodology manuals which have been already published can be found in Refs [1, 3-6].

[2] An update of this publication is in preparation at time of press.

1.2. OBJECTIVE

This volume of the updated INPRO manual for sustainability assessment provides guidance to the assessor of a planned NES (or a nuclear reactor) on how to apply the INPRO methodology for sustainability assessment in the area of safety of nuclear reactors. The INPRO assessment is expected either to confirm the fulfilment of all INPRO methodology criteria in the area of reactor safety, or to identify which criteria are not fulfilled and note the corrective actions (including potential RD&D) that would be necessary to fulfil them.

This publication discusses the INPRO sustainability assessment method for the area of safety of nuclear reactors. The INPRO sustainability assessment method for safety of nuclear fuel cycle facilities is discussed in a separate report of the INPRO manual.

This publication is intended for use by organizations involved in the development and deployment of a NES including planning, design, modification, technical support and operation for nuclear power plants. The INPRO assessor (or a team of assessors) is assumed to be knowledgeable in the area of nuclear safety and/or may be using the support of qualified organizations (e.g. the IAEA) with relevant experience. Two general types of assessors can be distinguished: a nuclear technology holder (i.e. a designer, developer or supplier of nuclear technology), and a (potential) user of such technology. The current version of the manual includes a number of explanations, discussions, examples and details so it is deemed to be used by technology holders and technology users.

1.3. SCOPE

The INPRO methodology presented in this manual is internationally developed guidance for assessing NES sustainability and is intended for use in support of NES planning studies by focusing on selected areas of reactor safety that are important for public acceptance (see Chapter 2). This manual deals with the long term sustainability of a NES comprised of different types of nuclear reactors. The INPRO methodology user requirements and criteria for sustainability assessment are formulated in this manual in a generic manner to make them applicable to both evolutionary and innovative reactors based on different technologies. However, the major contributions to the INPRO methodology update project have been obtained from the INPRO assessments of evolutionary water-cooled reactors and sodium cooled fast reactors. Other types of innovative reactors with a lower level of design maturity may require modifications or clarifications of selected criteria. Such potential changes will be considered in future revisions of the INPRO methodology after sufficient experience has accrued from INPRO assessments of such reactors.

This manual does not establish any specific safety requirements, recommendations or guidance. IAEA safety requirements and guidance are only issued in the IAEA Safety Standards Series. Therefore, the basic principles, user requirements and associated criteria contained in the INPRO methodology should only be used for sustainability assessments. The INPRO methodology is typically used by Member States in conducting a self-assessment of the sustainability and sustainable development of nuclear energy systems. This manual should not be used for formal or authoritative safety assessments or safety analyses to address compliance with the IAEA Safety Standards or for any national regulatory purpose associated with the licensing or certification of nuclear facilities, technologies or activities.

In the current version of the INPRO methodology, the sustainability issues relevant to safety of reactors and safety of nuclear fuel cycle facilities (NFCFs) are considered in separate manuals. The current methodology does not specifically address innovative integrated system designs (e.g. molten salt reactors with liquid fuel and integrated fast reactors with metallic fuel) whose

reactors are combined or co-located with fuel fabrication and/or reprocessing facilities. Reactor and NFCF installations of such integrated systems should be assessed separately against corresponding criteria in the INPRO areas of reactor safety and safety of NFCFs[3]. When more detailed information on the safety issues in integrated systems has been acquired, this approach can be changed in the next revisions of the INPRO methodology.

This version of the INPRO methodology manual for the area of reactor safety is focused on those nuclear power plants that produce primarily electricity, heat and combinations of the two[4]. This publication does not explicitly consider safety issues related to other non-electric applications (hydrogen production, desalination, etc.) or to cogeneration involving such energy products. It is expected that as more detailed information is acquired on the interactions between a reactor and industrial facilities located on the same site, the INPRO criteria may be modified when the methodology is next revised.

1.4. STRUCTURE

This publication follows the relationship between the concept of sustainable development and different INPRO methodology areas. Section 2 describes the linkage between the United Nations Brundtland Commission's concept of sustainable development and the IAEA's INPRO methodology for assessing the sustainability of planned and evolving NESs. Section 2 also considers how the INPRO sustainability assessment methodology in the area of reactor safety relates to the DID concept. Section 3 identifies the necessary inputs for an INPRO assessment in the area of reactor safety. This includes information on design and safety analyses[5] for the planned reactor and for the reference design. Section 4 presents the rationale and background for the INPRO sustainability assessment methodology in the area of reactor safety in terms of the selected basic principle, user requirements and assessment criteria, which consist of indicators and acceptance limits. On the criterion level, guidance is provided on how to determine the values of the indicators and acceptance limits, i.e. how to assess the potential of a NES to fulfil the INPRO methodology criteria. Appendix I presents a list of potential reference reactor designs to be used in the INPRO assessment. Appendices II through X provide complementary information which can be useful for the INPRO assessment of NES against different criteria discussed in the report.

Table 1 provides an overview of the INPRO user requirements and criteria that stem from the INPRO basic principle for sustainability assessment in the area of reactor safety.

[3] In this case, the potential for accidents in one facility to influence parameters or conditions in another has to be considered for the second facility independently or in combination with other external events (e.g. earthquakes and resulting explosions).

[4] Most NPPs sell relatively small amounts of energy in a form of heat used for district heating, greenhouse heating, etc., by local communities.

[5] It is assumed that design information and safety analysis results that are needed to perform the INPRO sustainability assessment are readily available.

TABLE 1. OVERVIEW OF THE INPRO METHODOLOGY FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF SAFETY OF NUCLEAR REACTORS

INPRO basic principle for sustainability assessment in the area of safety of nuclear reactors: *The safety of the planned nuclear installation is superior to that of the reference nuclear installation[a] such that the frequencies and consequences of the accidents are greatly reduced. In the event of an accident, off-site releases of radionuclides[b] are prevented or mitigated so that there will be no need for public evacuation[c].*		
INPRO user requirements	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR1: Robustness of design during normal operation: The nuclear reactor assessed is more robust than a reference design with regard to operation and systems, structures and components failures.	CR1.1: Design of normal operation systems	IN1.1: Robustness of design of normal operation systems.[d] AL1.1: More robust than that[e] in the reference design.
	CR1.2: Reactor performance	IN1.2: Reactor performance attributes. AL1.2: Superior to those of the reference design.
	CR1.3: Inspection, testing and maintenance	IN1.3: Capabilities to inspect, test and maintain. AL1.3: Superior to those in the reference design.
	CR1.4: Failures and deviations from normal operation	IN1.4: Expected frequency of failures and deviations from normal operation. AL1.4: Lower than that in the reference design.
	CR1.5: Occupational dose	IN1.5: Occupational dose values during normal operation and AOOs. AL1.5: Lower than the dose constraints.
UR2: Detection and interception of AOOs: The nuclear reactor assessed has improved capabilities to detect and intercept deviations from normal operational states in order to prevent AOOs from escalating to accident conditions.	CR2.1: Instrumentation and control (I&C) system and inherent characteristics	IN2.1: Capabilities of the I&C system to detect and intercept and/or capabilities of the reactor's inherent characteristics to compensate for deviations from normal operational states. AL2.1: Superior to those in the reference design.
	CR2.2: Grace periods after AOOs	IN2.2: Grace periods until human actions are required after AOOs. AL2.2: Longer than those in the reference design.
	CR2.3: Inertia	IN2.3: Inertia to cope with transients. AL2.3: Larger than that in the reference design.
UR3: Design basis accidents (DBAs): The frequency of occurrence of DBAs in the nuclear reactor assessed is reduced. If an accident occurs, engineered safety features are able to restore the reactor to a controlled state, and subsequently to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention is minimal, and only required after a sufficient grace period.	CR3.1: Frequency of DBAs	IN3.1: Calculated frequencies of occurrence of DBAs. AL3.1: Frequencies of DBAs that can cause plant damage are lower than those in the reference design.
	CR3.2: Grace period for DBAs	IN3.2: Grace periods for DBAs until human intervention is necessary. AL3.2: At least 8 hours and longer than those in the reference design.
	CR3.3: Engineered safety features	IN3.3: Reliability and capability of engineered safety features. AL3.3: Superior to those in the reference design.
	CR3.4: Barriers	IN3.4: Number of confinement barriers maintained (intact) after DBAs and DECs. AL3.4: At least one and consistent with regulatory requirements for the type of reactor and accident under consideration.
	CR3.5: Subcriticality margins	IN3.5: Subcriticality margins after reactor shutdown in accident conditions. AL3.5: Sufficient to cover uncertainties and to maintain shutdown conditions of the core.

TABLE 1. OVERVIEW OF THE INPRO METHODOLOGY IN THE AREA OF SAFETY OF NUCLEAR REACTORS (cont.)

INPRO user requirements	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR4: Severe plant conditions: The frequency of an accidental release of radioactivity into the containment / confinement is reduced. If such a release occurs, the consequences are mitigated, preventing or reducing the frequency of occurrence of accidental release into the environment. The source term of the accidental release into the environment remains well within the envelope of the reference reactor source term and is so low that calculated consequences would not require evacuation of the public.	CR4.1: Frequency of release into containment / confinement	IN4.1: Calculated frequency of accidental release of radioactive materials into the containment / confinement. AL4.1: Lower than that in the reference design.
	CR4.2: Robustness of containment / confinement design	IN4.2: Containment loads covered by the design, and natural or engineered processes and equipment sufficient for controlling relevant system parameters and activity levels in containment / confinement. AL4.2: Larger than those in the reference design.
	CR4.3: Accident management	IN4.3: In-plant accident management (AM). AL4.3: AM procedures and training sufficient to prevent an accidental release outside containment / confinement and regain control of the reactor.
	CR4.4: Frequency of accidental release into environment	IN4.4: Calculated frequency of an accidental release of radioactive materials into the environment. AL4.4: Lower than that in the reference design. Large releases and early releases are practically eliminated.
	CR4.5: Source term of accidental release into environment	IN4.5: Calculated inventory and characteristics (release height, pressure, temperature, liquids/gas/aerosols, etc) of an accidental release. AL4.5: Remain well within the inventory and characteristics envelope of the reference reactor source term and are so low that calculated consequences would not require public evacuation.
UR5: Independence of DID levels, inherent safety characteristics and passive safety systems: An assessment is performed to demonstrate that the DID levels are more independent from each other than in the reference design. To excel in safety and reliability, the nuclear reactor assessed strives for better elimination or minimization of hazards relative to the reference design by incorporating into its design an increased emphasis on inherently safe characteristics and/or passive systems, when appropriate.	CR5.1: Independence of DID levels	IN5.1: Independence of different levels of DID. AL5.1: More independence of the DID levels than in the reference design, e.g. as demonstrated through deterministic and probabilistic means, hazards analysis, etc.
	CR5.2: Minimization of hazards	IN5.2: Characteristics of hazards. AL5.2: Hazards smaller than those in the reference design.
	CR5.3: Passive safety systems	IN5.3: Reliability of passive safety systems. AL5.3: More reliable than the active safety systems in the reference design.

TABLE 1. OVERVIEW OF THE INPRO METHODOLOGY IN THE AREA OF SAFETY OF NUCLEAR REACTORS (cont.)

INPRO user requirements	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR6: Human factors (HF) related to safety: Safe operation of the nuclear reactor assessed is supported by accounting for HF requirements in the design and operation of the plant, and by establishing and maintaining a strong safety culture in all organizations involved.	CR6.1: Human factors	IN6.1: HF considerations are addressed systematically throughout the life cycle of the reactor. AL6.1: HF assessment results are better than those for the reference design.
	CR6.2: Attitude to safety	IN6.2: Prevailing safety culture. AL6.2: Evidence is provided by periodic safety culture reviews.
UR7: Necessary RD&D for advanced designs: The development of innovative design features of the nuclear reactor assessed includes associated research, development and demonstration (RD&D) to bring the knowledge of plant characteristics and the capability of analytical methods used for design and safety assessment to at least the same confidence level as for operating plants.	CR7.1: Safety basis and safety issues	IN7.1: Safety basis and a clear process for addressing safety issues. AL7.1: The safety basis for advanced designs is defined and safety issues are addressed.
	CR7.2: RD&D	IN7.2: RD&D status. AL7.2: Necessary RD&D is defined and performed, and the database is developed.
	CR7.3: Computer codes	IN7.3: Status of computer codes. AL7.3 Computer codes or analytical methods are developed and validated.
	CR7.4: Novelty	IN7.4: Pilot or demonstration plant. AL7.4: In case of a high degree of novelty: a pilot or demonstration plant is specified, built and operated, lessons are learned and documented, and results are sufficient to be extrapolated to a full-size plant. In case of a low degree of novelty: a rationale is provided for bypassing a pilot or demonstration plant.
	CR7.5: Safety assessment	IN7.5: Adequate safety assessment involving a suitable combination of deterministic and probabilistic methods, and identification of uncertainties and sensitivities. AL7.5: Uncertainties and sensitivities are identified and appropriately dealt with, and the safety assessment is approved by a responsible regulatory authority.

[a] Within this publication, a reference reactor (or design) is a reactor of the latest design operating in 2013. It should preferably be designed by the same corporate designer as the reactor assessed and using the same technology. For innovative reactors that may have no operating prototypes in 2013, the latest design that has been safely operated, or at least licensed, can be used as the reference design.
Based on previous experience with INPRO assessments, the definition of date for the selection of the reference design helps to avoid potential misinterpretations of terms. Note that 2013 was the date selected at the beginning of the latest methodology update. This date should be revised periodically along with the rest of methodology.

[b] If significant amounts of toxic chemicals are used in the reactor design (e.g. as coolants or fuel forms in the innovative reactors) or can be generated during the reactor operation or accidents, then potential accidental releases of toxic chemicals have to be considered as part of the INPRO assessment. The INPRO criteria used for the assessment of potential releases of toxic chemicals should be similar to those developed for the assessment of radioactive releases.

[c] Other protective measures may still be needed. Effective emergency planning, preparedness and response capabilities will remain a prudent requirement. This is covered in the Infrastructure area of the INPRO methodology.

[d] In this publication, 'robustness of design' is considered for DID Levels 1 to 4. However, this criterion CR1.1 is focused only on normal operation systems (Level 1 of DID).

[e] The requirement of superiority in the INPRO acceptance limits generally means an expected improvement of a given characteristic of the new design compared with the reference design. However, in cases where this specific characteristic in the reference design has already incorporated the best international practice available at the moment of assessment, the confirmation of equivalent characteristics in a new design will be sufficient for the positive assessment of a specific criterion or evaluation parameter. In this case, the assessor needs to prove both that the reference design is state of the art in relation to a given characteristic and that the new design characteristic is equivalent to that in the reference design.

2. GENERAL FEATURES OF NUCLEAR ENERGY SYSTEMS SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

This section provides an overview of the existing requirements for reactor safety, describes how the INPRO methodology supports the concept of sustainable development, and summarizes how the INPRO methodology follows the DID concept.

2.1. EXISTING REQUIREMENTS FOR REACTOR SAFETY

The INPRO methodology's basic principle, user requirements and criteria for sustainability assessment in the area of reactor safety have been established taking into account the large body of existing work on the safety of reactors operating today, as well as previous work on establishing the requirements for next generation (advanced) reactors.

The IAEA has produced internationally endorsed requirements and published them as the IAEA Safety Standards. These publications define the elements necessary to ensure the safety of nuclear power plants.

National regulatory bodies determine the licensing requirements that must be met by all national or foreign organisations involved in the design, construction, operation, decommissioning etc. of a nation's NPPs.

Various utility groups have developed corresponding utility requirements documents reflecting their experience from the construction, licensing and operation of NPPs over the past several decades, representing over 10 000 reactor-years of operating experience. Documents have been prepared for evolutionary[6] and innovative designs[7] by organizations such as EPRI (Advanced Light Water Reactor Utility Requirements Document – ALWR-URD), Japanese Utilities (JURD), Korean Utilities (KURD), Chinese Utilities (CURD) and the European Utilities (European Utility Requirements – EUR). These documents were authored primarily by electricity-generating utilities whose experiences with well-characterized reactor designs could be used to inform the development of modern (advanced) nuclear designs.

In 2004, the IAEA [7] presented an overview of these utility documents. A summary of the essence of these utility requirements for advanced reactor designs is presented below:

- A design life of 60 years;
- Reliable and flexible operation, with high overall plant availability, low levels of unplanned outages, short refuelling outages, good controllability (e.g. 100–50–100 % load following capability), and operating cycles extended up to 24 months;
- Increased margins to reduce sensitivity to disturbances and to reduce the number of safety challenges;
- Improved automation and man-systems interface, which, together with the increased margins, provide more time for the operator to act in accident/incident situations and reduce the probability of operator errors;

[6] An evolutionary design achieves improvements over existing designs through small to moderate modifications with a strong emphasis on maintaining proven technology to minimize technological risks.

[7] An innovative design incorporates radical conceptual changes in design approaches or system configurations in relation to the designs operating today.

- Calculated core damage frequency – less than 10^{-5} per reactor-year; cumulative frequency of accidental releases to the outside following core damage – less than 10^{-6} per reactor-year; and
- Design measures to cope with severe accidents.

In one specific area, there is a distinct difference between utility requirements for Europe and for the United States. This difference is attributed to the higher population density in Europe leading to more restrictive release targets for the European Utility Requirements as follows:

- To limit emergency protection actions beyond 800 m from the reactor to a minimum during early releases from the containment;
- To avoid delayed actions (temporary transfer of people) at any time beyond about 3 km from the reactor;
- To avoid long term actions, involving permanent (longer than 1 year) resettlement of the public, at any distance beyond 800 m from the reactor; and
- To ensure that restrictions on the consumption of foodstuffs and crops will be limited in terms of time and geographical area.

These requirements have been developed by utilities and are to be considered primarily as design targets. They should not be interpreted as requirements for the emergency preparedness arrangements to be implemented.

2.2. REQUIREMENTS FOR FUTURE REACTORS

The scope of the INPRO methodology covers nuclear reactors expected to come into service in the twenty-first century, together with the associated fuel cycles. It is recognized that a mixture of evolutionary and innovative designs will be brought into service and will co-exist within this period.

The 'Three Agency Study' [8] published in 2002 provides an overview of trends in the development of advanced (innovative) NESs. The range of reactors with advanced design features includes water-cooled, gas-cooled, liquid metal-cooled systems and molten salt reactors of various sizes to be used for various purposes.

In the global nuclear community, it is generally assumed that for widespread and long term use of nuclear power to be sustainable, a nuclear fuel strategy is required that utilizes, at least as a component, breeding, reprocessing and recycling of fissile material. In some countries or regions and for intermediate time scales, it is expected that advanced once-through (open) fuel cycle strategies featuring improved safety, proliferation resistance and physical protection will be followed. Ultimately, however, the development and implementation of advanced reactors and fuel strategies will include closed fuel cycles that make better use of uranium (and thorium) resources.

The Generation IV International Forum (GIF) [9] has defined six advanced (innovative) nuclear reactors and their associated fuel cycles that are to be developed in a joint effort by the countries participating in that programme with the aim of achieving full commercialization of these designs. The innovative reactor designs considered are a fast sodium cooled reactor, a fast gas cooled reactor, a molten salt reactor, a supercritical water-cooled reactor, a lead cooled reactor, and a very high temperature gas-cooled reactor. The 14 members participating in the GIF programme are: Argentina, Australia, Brazil, Canada, China, EURATOM, France, Japan, Republic of Korea, the Russian Federation, Republic of South Africa, Switzerland, the United Kingdom, and the United States. The GIF's risk and safety working group developed the Integrated Safety Assessment Methodology (ISAM) to be used continuously by the developers

of the innovative reactor designs. This methodology is based principally on probabilistic safety assessment and offers assessment tools well suited to all stages of design development.

National licensing requirements are well established for currently operating nuclear power reactors. A vendor of a given reactor design is expected to meet all these requirements at all levels that are specific to that reactor type, and exceptions, even at the detailed level, are unusual.

As mentioned before, this report discusses INPRO methodology criteria for nuclear reactors; INPRO criteria for safety of nuclear fuel cycle facilities are treated in a separate report of the updated INPRO manual. The INPRO methodology user requirements for sustainability assessment in the area of reactor safety are intended to be as generic as possible; where they cannot be made fully generic, this has been noted.

2.3. THE CONCEPT OF SUSTAINABLE DEVELOPMENT AND ITS RELATIONSHIP TO THE INPRO METHODOLOGY AREA OF REACTOR SAFETY

The United Nations World Commission on Environment and Development Report [10] (often known as the Brundtland Commission Report) defines sustainable development as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs" (para. 1). This definition:

> "contains within it two key concepts:
> - the concept of 'needs', in particular the essential needs of the world's poor, to which overriding priority should be given; and
> - the idea of limitations imposed by the state of technology and social organization on the environment's ability to meet present and future needs."

Based on this definition of sustainable development a three-part test of any approach to sustainability and sustainable development was proposed within the INPRO project: 1) current development should be fit for the purpose of meeting current needs with minimized environmental impacts and acceptable economics, 2) current research development and demonstration programmes should establish and maintain trends that lead to technological and institutional developments that serve as a platform for future generations to meet their needs, and 3) the approach to meeting current needs should not compromise the ability of future generations to meet their needs.

The definition of sustainable development may appear obvious, yet passing the three-part test is not always straightforward when considering the complexities of implemented nuclear energy systems and their many supporting institutions. Many approaches may only pass one or perhaps two parts of the test in a given area and may fail the others.

The Brundtland Report's overview (para.61 in Ref. [10]) of nuclear energy summarized the topic as follows:

> "After almost four decades of immense technological effort, nuclear energy has become widely used. During this period, however, the nature of its costs, risks, and benefits have become more evident and the subject of sharp controversy. Different countries world-wide take up different positions on the use of nuclear energy. The discussion in the Commission also reflected these different views and positions. Yet all agreed that the generation of nuclear power is only justifiable if there are solid solutions to the unsolved problems to which it gives rise. The highest priority should be accorded to research and development on environmentally sound and ecologically viable alternatives, as well as on means of increasing the safety of nuclear energy."

The Brundtland Commission Report presented its comments on nuclear energy in Chapter 7, Section III [10]. In the area of nuclear energy, the focus of sustainability and sustainable

development is on solving certain well-known problems (referred to here as 'key issues') of institutional and technological significance. Sustainable development implies progress and solutions in the key issue areas. Seven key issues are discussed in Ref [10]:

1) Proliferation risks;
2) Economics;
3) Health and environment risks;
4) Nuclear accident risks;
5) Radioactive waste disposal;
6) Sufficiency of national and international institutions (with particular emphasis on intergenerational and transnational responsibilities);
7) Public acceptability.

The INPRO methodology for self-assessing the sustainability and sustainable development of a nuclear energy system is based on the broad philosophical outlines of the Brundtland Report's concept of sustainable development described above. Although three decades have passed since the publication of the Brundtland Commission Report and eighteen years have passed since the initial consultancies on development of the INPRO methodology in 2001 the definitions and concepts remain valid. The key issues for sustainable development of NESs have remained essentially unchanged over the intervening decades, although significant historical events have starkly highlighted some of them.

During this period, several notable events have had a direct bearing on nuclear energy sustainability. Among these were events pertaining to non-proliferation, nuclear security, waste management, cost escalation of new construction and, most notably, to reactor safety.

Each INPRO methodology manual examines a key issue of NES sustainable development. The structure of the methodology is a hierarchy of INPRO basic principles, INPRO user requirements for each basic principle, and specific INPRO criteria[8] for measuring whether each INPRO UR has been met. Under each INPRO UR, the CR includes measures that take into consideration the three-part test based on Brundtland Report definition of sustainable development which was described above.

This INPRO manual focusses on the key issue of nuclear reactor safety. In the Brundtland Commission Report [10] section on nuclear energy (Chapter 7, Section III), the most detailed discussion is on the key issue of reactor safety. The report justified its principal focus on reactor safety with the following argument:

> "Nuclear safety returned to the newspaper headlines following the Three Mile Island (Harrisburg, United States) and the Chernobyl (USSR) accidents. Probabilistic estimates of the risks of component failure, leading to a radioactive release in Western style light water reactors were made in 1975 by the U.S. Nuclear Regulatory Commission. The most serious category of release through containment failure was placed at around 1 in 1,000,000 years of reactor operation. Post-accident analysis of both Harrisburg and Chernobyl - a completely different type of reactor - have shown that in both cases, human operator error was the main cause. They occurred after about 2,000 and 4,000 reactor-years respectively. The frequencies of such occurrences are well-nigh impossible to estimate probabilistically. However, available analyses indicate that although the risk of a radioactive release accident is small, it is by no means negligible for reactor operations at the present time."

[8] INPRO basic principles, user requirements and criteria for NES sustainability assessment.

In addition, the Brundtland Commission Report [10] noted that national governments were responding to nuclear accidents by following one of three general policy directions:

> "National reactions indicate that as they continue to review and update all the available evidence, governments tend to take up three possible positions:
> - remain non-nuclear and develop other sources of energy;
> - regard their present nuclear power capacity as necessary during a finite period of transition, to safer alternative energy sources; or
> - adopt and develop nuclear energy with the conviction that the associated problems and risks can and must be solved with a level of safety that is both nationally and internationally acceptable."

These typical national policy directions remain consistent with practice to the current day. Within the context of a discussion on sustainable development of nuclear energy systems, it would seem that the first two policy positions cannot result in development of a sustainable nuclear energy system in the long term since nuclear energy systems are either avoided altogether or phased out over time. However, it is arguable that both policy approaches can meet the three-part Brundtland sustainable development test if technology avoidance or phase-out policies are designed in a way that avoids foreclosing or damaging the economic and technological opportunity for future generations to change direction and start or re-establish a nuclear energy system. This has certain specific implications regarding long term nuclear education, knowledge retention and management and with regard to how spent nuclear fuels and other materials, strategic to nuclear energy systems, are stored or disposed of.

The third policy direction proposes to develop nuclear energy systems that 'solve' the problems and risks through a national and international consensus approach to enhance safety. This is a sustainable development approach, in which the current generation has decided that nuclear energy is necessary to meet its needs, while taking a positive approach to developing enhanced safety to preserve the option in the future. In addition to the general outlines of how and why nuclear reactor safety is a principal key issue affecting the sustainability and sustainable development of nuclear energy systems, the Commission Report also advised that key institutional arrangements should be developed. Since that time, efforts to establish such institutional arrangements have achieved a large measure of success. The Brundtland Commission Report was entirely clear that enhanced reactor safety is a key element of the sustainable development of nuclear energy systems. It is not possible to measure nuclear energy system sustainability apart from direct consideration of certain safety issues.

Understanding the psychology of risk perception in the area of nuclear safety is critical to understanding nuclear energy system sustainability and sustainable development. In a real measured sense, taking into account the mortality and morbidity statistics of other non-nuclear energy generation technology chains (used for similar purpose), nuclear energy has an outstanding safety record, despite the severe reactor accidents that have occurred. However, it should not be presumed that this means that reactor safety is not a key issue affecting nuclear energy system sustainability. How do dramatically low risk estimations (ubiquitous in nuclear energy system probabilistic risk assessment) sometimes psychologically disguise high consequence events in the minds of designers and operators, while the lay public perception of risk (in a statistical sense) may be tilted quite strongly either toward supposed consequences of highly unlikely, but catastrophic disasters, or toward a complacent lack of interest in the entire subject? This issue has been studied for many years [11, 12]. What should be the proper metrics for the INPRO sustainability assessment methodology given that the technical specialist community has developed an approach that may seem obscure and inaccessible to the lay public?

For example, if the radioactive dose consequence of a severe reactor accident is calculated in terms of mortality/morbidity estimates in the known exposed public, the outcomes may seem far less than catastrophic. However, if the impacts of economic and population dislocations that can be attributed directly or indirectly to the severe reactor accident (such as Chernobyl and Fukushima) are estimated and these figures are converted (using the methods of cost benefit analysis) into 'total costs' and 'years of life lost', a severe reactor accident can take on an epic scale – as has been observed in practice in the severe cases. The apparent paradox is that both estimates (dose and other collateral impacts) measure something that has occurred, and both are 'true' in their own sense. The paradox is resolved by noting that, while public exposures to radiation may be kept small and inconsequential through a combination of plant design, other technical measures and emergency responses, experience demonstrates that the perception of a population about an event is at least as important to the overall outcome as are measured evidences of radioactive dose. The affected population will have thoughts and feelings and will take actions based on their individual intellectual and emotional judgements about the accident – whether those judgements are technically informed or not.

It is both unrealistic and unhelpful to suppose that a massive public education campaign can eliminate the difference between the judgments of experts and those of the lay public. Continuous communication and education programmes can help, but there are also limits to what can be achieved. Reactor designs, construction and operations, decommissioning, and emergency planning and response must therefore be reconciled to the reality of the current public mindsets. The close relationship between public perception of risk and public acceptance should be considered universal with regard to the key issue of nuclear safety. It can have tremendous impact across national and regional boundaries and even on different continents – in a psychological sense, a severe nuclear accident anywhere is a nuclear accident everywhere.

With regard to nuclear reactor safety, the public are principally focussed on the individual and collective risks and magnitude of potential consequences in case of reactor accidents (radiological, economic and other psychosocial consequences taken together). Considering the experience of all reactor accidents to date it is clear that a few key issues are central to positively influencing the public debate over nuclear safety and improving public acceptance of nuclear energy:

1. Significant radioactive releases need to be avoided, avoiding the need to relocate significant populations even in the case of a severe nuclear accident.
2. In the extremely unlikely event of a significant release of radioactivity, fully competent emergency planning, preparedness and response capabilities are expected to be in place and available for immediate action[9].
3. Design basis accidents need to be made even more unlikely than in previous designs, even if releases of radioactivity are insignificant and dose to the most exposed public is inconsequential (from a regulatory limit perspective).
4. Facility upsets and failures that could cause a departure from normal safe operations are expected to be rarer than in previous designs. Regular upsets and failures and/or difficult recoveries tend to undermine public confidence in both worker safety and public safety.
5. Where practicable, inherent and passive safety features could be incorporated to reduce risks posed by active system faults and human operator error.
6. Unacceptable occupational doses and hazards need to be avoided. Unacceptable doses and hazards to nuclear workers undermine public confidence in safety and health.

[9] Emergency preparedness and response issues are discussed in the INPRO methodology manual on Infrastructure.

7. Superior performance in the overall reactor plant lifecycle risk posed to the public needs to be demonstrated in comparison to previous reactor designs. Inferior performance on overall risk undermines public confidence in safety.
8. Continuing improvements in safety by design through research and development programmes need to continue and be practically applied in new reactor designs. Continuing improvements help support public confidence in the safety of nuclear energy.
9. Stakeholder communication and public outreach and education on all principal aspects of facility safety listed above (at a minimum) need to be continuous, accurate and transparent[10]. Without an effective communication and education programme, it is very difficult to influence the stakeholder and public mindsets.

In the current INPRO manual, the URs and CRs focus on assessment of the NES characteristics associated with the majority of these issues. Unlike several other key sustainability issues assessed in other areas of the INPRO methodology, Brundtland sustainability in the area of reactor safety is intimately tied to public perception of consequence and risk. Continuously allaying public concern about nuclear reactor safety is central to sustainability and sustainable development of nuclear energy systems.

2.4. THE CONCEPT OF DEFENCE IN DEPTH AND ITS RELATIONSHIP WITH THE INPRO METHODOLOGY AREA OF REACTOR SAFETY

The DID concept provides an overall strategy for designing safety measures and features of nuclear installations [13-15]. The concept is twofold: firstly, to prevent accidents and, secondly, if prevention fails, to mitigate their potential consequences and prevent any evolution to more serious conditions. Accident prevention is the first priority, because provisions to prevent deviations of the plant state from well-known operational conditions are generally more effective and more predictable than measures aimed at mitigation of such departures – plant performance generally deteriorates when the status of the plant or a component departs from normal operating conditions. Thus, preventing the degradation of (normal operation) plant status and performance generally will provide the most effective protection of workers, the public and the environment.

The objectives of implementing DID in a design are as follows:

- To compensate[11] for potential failures of humans, systems, structures and components;
- To maintain the effectiveness of the barriers by averting damage to the plant and to the barriers themselves; and
- To protect the public and the environment from harm in the event that these barriers are not fully effective.

When properly implemented, DID ensures that no single technical, human or organizational failure could lead to harmful effects, and that the combinations of failures that could give rise to significant harmful effects are of very low probability.

DID is characterized by five levels of protection, with the top level being prevention, and the remaining four levels representing the response to increasing challenges to plant and public safety [15]. Ref [15] states:

> "The purpose of the first level of defence is to prevent deviations from normal operation and the failure of items important to safety. This leads to requirements that the plant be

[10] Political support and public acceptance issues are discussed in the INPRO methodology manual on Infrastructure.
[11] Compensate fully or at least minimise effects.

> soundly and conservatively sited, designed, constructed, maintained and operated in accordance with quality management and appropriate and proven engineering practices"

For example, design features that reduce the potential for internal hazards, e.g. fire, contribute to the prevention of accidents.

The purpose of the second level of DID is to "detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions" [15]. The second level "necessitates the provision of specific systems and features in the design, the confirmation of their effectiveness through safety analysis, and the establishment of operating procedures to prevent such initiating events, or otherwise to minimize their consequences, and to return the plant to a safe state".

The purpose of the third level of defence is the control of postulated accidents[12], preventing damage to the reactor core, i.e. assuring its structural integrity, preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state. To achieve this objective, inherent safety features, engineered safety systems and accident procedures have to be provided.

The purpose of DID Level 4 is [15]:

> "… to mitigate the consequences of accidents that result from failure of the third level of defence in depth. This is achieved by preventing the progression of such accidents and mitigating the consequences of a severe accident."

It is related to the control of potential severe plant conditions and the minimisation of off-site contamination.

The purpose of the fifth level of defence is to mitigate the consequences of potential accidental radiological releases. This requires adequate emergency plans, procedures and emergency response facilities.

Ensuring the independence of the different levels of protection in the DID concept is key to avoiding the propagation of failures into subsequent levels.

Based on the DID concept, the INPRO methodology has developed general proposals for designers/developers to meet the INPRO user requirements of sustainable development in the area of safety of nuclear reactors. These proposals are based on extrapolations of trends published in Section 5 of Ref [13] and are presented in Table 2. These proposals are focused on the prevention, reduction and containment of radioactive releases. INPRO NES sustainability assessment user requirements related to the off-site emergency preparedness and response measures, which are focused on reducing the consequences of a potential accidental release of radioactivity from the NPP, are considered in the INPRO area of infrastructure [1].

[12] Accidents can be initiated by single or multiple events.

TABLE 2. INPRO PROPOSALS FOR APPLYING THE DEFENCE IN DEPTH CONCEPT TO NES SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

Level	DID level purpose	INPRO methodology proposals for nuclear reactors
1	Prevention of deviations from normal operation[13] and the failures of items important to safety	Enhance prevention by increased emphasis on robustness of the design of normal operation systems, and further reducing the probability of human error in the routine operation of the plant. Enhance the independence among DID levels.
2	Detect and control deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions.	Give priority to inherently safe design characteristics and advanced control and monitoring systems with enhanced reliability, intelligence and the ability to anticipate and compensate abnormal operational states. Enhance the independence among DID levels.
3	Control of accidents. Preventing damage to the reactor core and preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state	Decrease expected frequency of accidents. Achieve fundamental safety functions by an optimized combination of active and passive design features; limit and mitigate consequences; minimize reliance on human intervention, e.g. by increasing grace period. Enhance the independence among DID levels.
4	Mitigate the consequences of accidents that result from failure of the third level by preventing the progression of such accidents and mitigating the consequences of a severe accident.	Decrease expected frequency of severe plant conditions; increase reliability and capability of systems to control and monitor severe accident sequences[14]; reduce the characteristics of source term of the potential emergency off-site releases of radioactivity. Avoid 'cliff-edge' failures of items important to safety. Enhance the independence among DID levels.
(5)	Mitigation of radiological consequences of radioactive releases	Emergency preparedness is covered in another area of the INPRO methodology called Infrastructure [1].

The first four sustainability assessment user requirements of the INPRO methodology in the area of safety of nuclear reactors are directly linked to the first four levels of the DID concept. The rest of the user requirements are related to specific aspects of this concept. A nuclear power plant is considered as having an acceptable level of safety if it fulfils all applicable (national and international) safety related standards and regulations, i.e. when it is licensed for operation. In fact, the reference design is assumed to be compliant with these standards and regulations. The INPRO methodology intends to go beyond these standards and regulations by taking into account trends and anticipated future directions of development (Section 5 of Ref [13]) to achieve safety enhancements in the assessed new design that contribute to the long term sustainability of the nuclear energy system.

[13] Deviations from normal operation and the failures of items important to safety are considered as the anticipated operational occurrences.

[14] Control and monitor severe accident sequences on both short and long term.

3. NECESSARY INPUT FOR INPRO SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

This section gives guidance on the information needed by an assessor to be able to perform an INPRO sustainability assessment in the area of safety of nuclear reactors. As explained earlier, an INPRO sustainability assessment is not an assessment of compliance with the IAEA Safety Standards.

3.1. DEFINITION OF NUCLEAR ENERGY SYSTEM

Clear definition of the nuclear energy system (NES) is needed for an INPRO assessment. As described in the overview manual of the INPRO methodology, the NES will be selected, in general, based on an energy planning study. This study should define the role of nuclear power (amount of nuclear capacity to be installed as a function of time) in an energy supply scenario for a country (or a region or globally). Using the results of such a study, the next step is the choice of facilities of the NES selected that fits to the determined role of nuclear power in the country. The NES definition should include a schedule for deployment, operation and decommissioning of the individual facilities.

In the INPRO methodology area of safety of nuclear reactors, the design of the reactor assessed is generally to be compared to a reference design. The goal of the INPRO assessment in this area is then to demonstrate an increased safety level in the assessed reactor design in comparison to the reference design. The nuclear reactor assessed, and the reference reactor should preferably be of the same lineage and from the same designer. Examples of potential reference reactors are presented in Annex I.

3.2. INPRO ASSESSMENT BY A TECHNOLOGY USER

As a technology user, an INPRO assessor needs rather detailed design information on the nuclear reactor to be assessed. This includes information relating to: the design basis of the plant; design information on the reactor core, fuel, primary circuit, reactor heat removal system, engineered safety systems, containment systems, human system interfaces, control and protection systems, etc. The design information needs to highlight the structures, systems and components that are of evolutionary or innovative design and these would be the focus of the INPRO assessment.

In addition to the information on the nuclear reactor to be assessed, the INPRO assessor needs the same type of information on a reference plant design in order to perform a comparison of both designs. Details of the information needed are outlined in the discussion of the INPRO methodology criteria in the following sections of this report.

If not available in the public domain, the necessary information is to be provided by the designer (potential supplier). Therefore, a close cooperation between the INPRO assessor as a technology user and the designer (potential supplier) is necessary (as discussed in the overview manual of the INPRO methodology).

The role of technology user in the INPRO assessment is primarily to check in a simplified way whether the designer (supplier) has appropriately taken into account the nuclear safety aspects in its design as defined by the INPRO methodology. A technology user is assumed – in order to minimize its risk – to be primarily interested in installing reactors based on proven technology with designs that have been licensed (at least in the country of the supplier) and that have operated successfully for a sufficiently long time.

3.3. RESULTS OF SAFETY ANALYSES

The INPRO assessor will need access to results of a safety assessment[15] that includes a safety analysis which evaluates and assesses challenges to safety under various operational states, anticipated occurrences and accident conditions using deterministic and probabilistic methods; this safety assessment is expected to be performed and documented by the designer (potential supplier) of the reactor to be assessed and the reference reactor.

For the reactor to be assessed, the safety assessment would need to include details of the research, development and demonstration (RD&D) carried out for advanced aspects of the design. Such information is usually found in a preliminary safety analysis report (PSAR) available in the public domain and is otherwise to be provided by the designer (potential supplier) of the reactor.

3.4. INPRO ASSESSMENT BY A TECHNOLOGY DEVELOPER

In principle, an INPRO assessment can be carried out by a technology developer at any stage of the development of an advanced reactor design. A designer (developer) can use this report to check whether its new design under development meets the INPRO methodology sustainability criteria regarding nuclear safety but can additionally initiate modifications during early design stages if necessary to improve the safety level of its design. However, it needs to be recognized that the extent and available level of detail of design and safety assessment information will increase as the design of an advanced nuclear reactor progresses from the conceptual stage to development of the detailed design. This will need to be taken into account in drawing conclusions on whether an INPRO methodology criterion in the area of safety has been met by the advanced design.

One potential mode of the INPRO methodology application by a technology developer is to perform a limited scope assessment. Limited scope INPRO assessments can be focused on the specific areas and specific installations in a nuclear energy system having different levels of maturity. Limited scope studies may assess reactor designs under development, including innovative designs, and may help to highlight gaps to be closed by on-going R&D studies and to define the scope of data needed for making a future judgement on system sustainability.

3.5. OTHER SOURCES OF INPUT

The NESA support package introduced in the overview manual of the INPRO methodology includes information on safety related issues that were collected form the public domain. This includes preliminary safety analysis reports from several advanced reactor designs, exemplary limited scope assessments performed by designers participating in INPRO activities, etc.

The final report of the nuclear energy system assessment (NESA) of the planned nuclear energy system in Belarus is documented in Ref [16]; it includes an assessment of the WWER reactor AES-2006 using the INPRO methodology.

[15] In this document ‘safety assessment’ means “assessment of all aspects of a practice that are relevant to protection and safety” as defined in the IAEA Safety Glossary and covered in the IAEA Safety Standards.

4. INPRO BASIC PRINCIPLE, USER REQUIREMENTS AND CRITERIA FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

4.1. INTRODUCTION

The INPRO methodology for assessing NES sustainability in the area of nuclear reactor safety defines one INPRO basic principle and a supporting set of INPRO user requirements and criteria and focuses on examining the expected safety impact of future changes in nuclear technology. Using the INPRO methodology to assess the sustainability of a NES is a bottom-up exercise. It consists of determining for each INPRO methodology criterion the value of each of the INPRO methodology indicators for that criterion and comparing that value with the corresponding INPRO methodology acceptance limit. The comparison then provides a basis for judging the capability of the assessed NES to meet the respective sustainability criterion. As will be shown in discussing the INPRO basic principle and user requirements for this assessment area, the methodology encourages innovations that enhance the safety of nuclear reactors.

One of the basic assumptions of the INPRO methodology is the expectation that – to fulfil the needs of sustainable energy supply in the twenty-first century – the global number of nuclear reactors in operation will have to increase considerably compared to the situation today. Keeping the safety level of newly deployed reactors (after 2013) at the same level as the global operating systems today would lead to an overall increase in the numerical risk of nuclear accidents. It is expected, however, that this increase in calculated risk would be compensated by the increased safety level of the newly deployed reactors, based in part on lessons learned from systems in operation. Therefore, the INPRO methodology evaluates enhancements in the safety of new reactor designs but does not evaluate compliance with national or international (e.g. IAEA) safety standards. The reference design is assumed to comply with applicable safety standards because it is an operating plant. Similarly, a new reactor is assumed to be designed so that it complies with applicable safety standards. Confirmation of compliance of the reference or new design with national or international safety standards is outside the scope of the INPRO methodology. If such confirmation is needed, a separate peer review (e.g. using IAEA review services such as TSRs[16]) should be performed.

The INPRO methodology's basic principle and its set of user requirements and criteria for sustainability assessment in the area of reactor safety are expected to apply to any type of advanced design and should foster appropriate developments and improvements that can be communicated to and be accepted by all stakeholders in nuclear energy.

The legal and organizational framework related to safety of nuclear reactors is dealt with in another report of the updated INPRO methodology focused on infrastructure.

4.2. INPRO BASIC PRINCIPLE FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF SAFETY OF NUCLEAR REACTORS

INPRO basic principle for sustainability assessment in the area of nuclear reactor safety: The safety of the planned nuclear installation is superior to that of the reference nuclear installation such that the frequencies and consequences of the accidents are greatly reduced. In the event of

[16] Technical Safety Reviews offered by the IAEA Department of Nuclear Safety and Security

an accident, off-site releases of radionuclides are prevented or mitigated so that there will be no need for public evacuation[17].

Currently, nuclear facilities have significant restrictions with regard to siting, primarily due to the perceived high risk of potential consequences during severe accidents but also to a lesser degree due to the perceived risk of radioactive releases during normal operation. An advanced design is expected to allow – after achieving public acceptance of this development –a reduction of the restrictions on NPP siting. This is a long term objective to be achieved during the twenty-first century.

To approach the goal of the INPRO basic principle, the INPRO methodology proposes that designers/developers undertake the following key measures:

- Incorporate enhanced DID into an advanced nuclear reactor design as a part of the fundamental safety approach and ensure that the levels of protection in DID are more independent from each other than in a reference plant;
- Incorporate, where appropriate, inherently safe characteristics and passive systems into advanced nuclear reactor designs as a part of a fundamental safety approach to excel in safety and reliability;
- Take human factors into account in the design and operation of a nuclear reactor;
- Perform sufficient RD&D work to bring the knowledge of nuclear plant characteristics and the capability of analytical methods used for design and safety assessment of a plant with innovative features to at least the same confidence level as for a reference plant.

In addition, the INPRO methodology encourages the establishment and maintenance of a strong safety culture in all organizations involved in a nuclear power programme.

The INPRO methodology has developed seven INPRO user requirements for NES sustainability assessment in the area of reactor safety to specify in more detail the main measures presented above. These INPRO user requirements are to be fulfilled primarily by the designer (developer, supplier) of the NES. As stated before, the role of the INPRO assessor is to check, based on evidence provided by the designer, whether the designer has implemented the necessary measures as required by the INPRO methodology. The assessor's product is therefore not an assessment of compliance with the IAEA Safety Standards but rather a sustainability assessment against the INPRO user requirements and criteria.

The following sections present the rationale and background information for each INPRO NES sustainability user requirement and criterion and then describe how indicators and acceptance limits are used to determine whether each CR has been met.

4.3. UR1: ROBUSTNESS OF DESIGN DURING NORMAL OPERATION

INPRO user requirement UR1 for sustainability assessment in the area of safety of nuclear reactor: The nuclear reactor assessed is more robust than a reference design with regard to operation and systems, structures and components failures.

This sustainability assessment INPRO user requirement mostly[18] relates to the first level of the DID concept, which has the objective of preventing anticipated operational occurrences (AOOs). The objective is met if the plant stays in normal operation.

---

[17] Other protective measures may still be needed. Effective emergency planning, preparedness and response capabilities will remain a prudent requirement as discussed in the INPRO methodology manual for the area of infrastructure.

[18] UR1 also involves consideration of selected provisions in Level 2 of DID.

AOOs are those conditions of operation caused by plant internal and external events, and probable combinations thereof, that are expected to occur one or more times during the life of a nuclear reactor but neither cause significant damage to items important to safety nor lead to accident conditions that would rely on safety systems (Level 3 of DID) for coping. Examples of AOOs caused by internal or external events in a nuclear power plant [17] include faults such as a turbine trip, malfunction of individual items of a normally running plant, failure to function of individual items of control equipment, trips of a feedwater pump, loss of power to a main (reactor) coolant pump, etc.

The major means to achieve robustness of a reactor design are to ensure a high quality of design, manufacture, construction, and operation (and decommissioning), including adequate attention to human performance. It is important to note that for the assessment of all criteria of INPRO user requirement UR1 the assessor (a technology user) needs information on the reactor to be assessed and on a reference reactor design. The reactor assessed needs to be shown to be safer than the reference reactor.

For operating and evolutionary reactors, the requirements for design, manufacturing and operation are usually specified in (extensive) national standards or adopted standards from other countries; the most widely known and used standards are the Nuclear Codes and Standards published by the American Society of Mechanical Engineers (ASME) and for electric components and I&C the standards published for NPPs by the Institute of Electrical and Electronics Engineers (IEEE). For (innovative) designs still under development and for which no standards may yet exist, at least for the first plant to be installed, a conservative design approach according to existing standards can be proposed as discussed in more detail in the INPRO manual sections for sustainability assessment user requirement UR7.

INPRO assessment of a NES against criteria CR1.1 and CR1.2 of UR1 involves the consideration of multiple technical parameters. For these two criteria the INPRO methodology has developed a series of evaluation parameters (EPs) which are intended as recommendations to the INPRO assessor on how to assess the criteria. Criteria CR1.3, CR1.4 and CR1.5 do not require development of evaluation parameters.

TABLE 3. CRITERIA FOR USER REQUIREMENT UR1 FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

INPRO user requirement	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR1: Robustness of design during normal operation: The nuclear reactor assessed is more robust than a reference design with regard to operation and systems, structures and components failures.	CR1.1: Design of normal operation systems	IN1.1: Robustness of design of normal operation systems. AL1.1: More robust than that in the reference design.
	CR1.2: Reactor performance	IN1.2: Reactor performance attributes. AL1.2: Superior to those of the reference design.
	CR1.3: Inspection, testing and maintenance	IN1.3: Capabilities to inspect, test and maintain. AL1.3: Superior to those in the reference design.
	CR1.4: Failures and deviations from normal operation	IN1.4: Expected frequency of failures and deviations from normal operation. AL1.4: Lower than that in the reference design.
	CR1.5: Occupational dose	IN1.5: Occupational dose values during normal operation and AOOs. AL1.5: Lower than the dose constraints.

The INPRO methodology criteria for UR1 are presented in Table 3.

4.3.1. Criterion CR1.1: Design of normal operation systems

Indicator IN1.1: Robustness of design of normal operation systems.

Acceptance limit AL1.1: More robust than that in the reference design.

In the following, several design related aspects that, if enhanced, would increase the level of robustness of a nuclear reactor design during normal operations are discussed.

It is acknowledged that increasing the robustness of a reactor design is a challenging task for a designer because enhancing one aspect could have a negative influence on other aspects. Thus, an optimum combination of design measures is necessary to increase the overall robustness of a design.

The INPRO methodology has defined several design related aspects as evaluation parameters (EP1.1.1 to EP1.1.5) for criterion CR1.1:

- EP1.1.1: Margins of design
- EP1.1.2: Design simplification
- EP1.1.3: Improved fabrication and construction
- EP1.1.4: Improvement of materials
- EP1.1.5: Redundancy of operational systems.

The use of inherent safety characteristics is an additional means of achieving robustness (discussed separately under UR5). As stated above, these evaluation parameters are meant to be examples for a designer on how to achieve a higher level of robustness in a reactor design by looking for an optimum combination of these parameters.

A detailed safety guide for the design of the core of water-cooled reactors is provided in Ref [18].

4.3.1.1. Evaluation parameter EP1.1.1: Margins of design

The term *margin of design* is defined here as the difference in absolute or relative values between the limiting value of an assigned safety related parameter, such as stress, temperature, etc, the surpassing of which leads to the failure of a structure, system or component (safety limit) and the design value of the corresponding parameter, calculated using conservative approach. Loads and resulting stresses have a great influence on robustness of components, because a design with higher margins against overstressing and fatigue (due to cycling loads) can reduce the (expected) failure rates substantially. An increase of design margins will increase the robustness of a design.

Refs [19–21] give detailed explanation on the application of different margins in the reactor design, operation and safety assessment.

According to Ref [13], Level 1 of DID should also provide the initial basis for protection against external hazards. The design of the reactor assessed is expected to be made more robust against relevant external hazards[19] by an increase of design margins[20]. The robustness of the design against external hazards can involve two aspects: selection of the reactor site and the characteristics of plant systems, structures and components relevant to the external hazards. The selection of site normally can help to eliminate or minimize the frequency and magnitude

[19] When external events or hazards relevant to the reactor assessed have not been considered in the reference design, e.g. tsunami for inland sited NPP, reference margins have to be taken from another operating NPP design, preferably of the same type, considering such hazards.

[20] In this evaluation parameter INPRO asks the assessor to compare design margins associated with specific parameters, which is different from the comparison of parameters.

of some of the external hazards. However, the plant has to be designed against all potential external events at a given site with sufficient margins. Examples of such external natural hazards are extreme meteorological conditions (e.g. frost, snow, drought, etc.), flooding (e.g. tsunamis, dam failures), storms (e.g. hurricane) and earthquakes. Examples of external human induced hazards are aircraft crashes, explosions outside the plant site, etc [22, 23]. However additional protection may be required at higher levels of defence to cope with these hazards.

Based on lessons learned from the Fukushima Daiichi accident [24–28], probable combinations of external events (e.g. an earthquake plus a fire and/or tsunami) need to be considered in the design.

Appendix II gives an example of basic approach to the assessment of design margins of the reactor core.

Acceptability of EP1.1.1 *(design margins):* Evidence available to the INPRO assessor shows that design margins are larger than those in the reference design.

4.3.1.2. Evaluation parameter EP1.1.2: Design simplification

In general, the higher the complexity of a system, the higher the probability that something may fail or malfunction in the system. Thus, an increase of simplicity, i.e. a reduction of complexity, can increase the robustness of a design.

One of the potential options for simplifying the reactor design is to reduce when possible the length of primary circuit pipes and the number of bends. Another simplification option could be to reduce the number of main cooling system components. The design of cooling systems for reactors (used for the transport of energy from the core to a turbine or other energy-converting processes) ranges from a single direct cycle (e.g. high temperature gas cooled reactors - HTGRs) or several parallel direct cycles (e.g. BWRs) up to two (e.g. pressurized water reactors (PWRs) and heavy water reactors (HWRs)) or three (e.g. sodium cooled reactors) separate cycles in series with heat exchangers in between. A designer has to consider several trade-offs in reducing the complexity: reducing the number of loops (e.g. for PWRs) for a given core power will result in larger steam generators; this may possibly result in thermal-hydraulic instabilities or the need for new materials. On the other hand, these considerations may lead to innovative designs, e.g. special heat exchangers for sodium cooled reactors to reduce the number of loops in series to two loops; this reduction could also be supported by a development of a non-flammable sodium coolant.

If appropriate, reducing the numbers of other lines in a reactor system, such as feed water trains and main steam lines, may also be considered. Another option is to reduce the number of active components (e.g. motor operated valves and pumps) in a system.

However, increasing simplicity by reducing active components or reducing the number of lines must not compromise reactor safety and has to be considered carefully for its potential to negatively influence the redundancy of the system.

Acceptability of EP1.1.2: Evidence available to the INPRO assessor demonstrates less design complexity than in the reference design.

4.3.1.3. Evaluation parameter EP1.1.3: Improved fabrication and construction

The basis of improved fabrication and construction is the establishment of an adequate management programme in the organizations involved in NPP design, fabrication and construction [29–31], which is a topic covered in another INPRO manual focused on infrastructure [1]. Improving the fabrication and construction of NPP systems, structures and components can improve plant performance of plant, including safety characteristics, and is linked to progress in fabrication and construction technologies.

An example of improved fabrication concerns the issue of welding and is discussed in the following. Every weld in a pipe or vessel can be a source of failure; therefore, a reduction of welds in piping or vessels clearly results in an increase of robustness of the design of a reactor. In addition, fewer welds require fewer in service inspections and thus lead to reduced doses for the personnel. As in other areas, progress in welding engineering and the fabrication of pipes exists. Progress in welding engineering includes the application of automatic welding machines during fabrication, which results typically in weld characteristics better than those achieved with manual welding procedures. Progress in pipe fabrication includes the elimination of longitudinal welds through the use of a cold-drawing (extrusion) process.

Acceptability of EP1.1.3: Evidence available to the INPRO assessor demonstrates methods of fabrication and construction better than those in the reference design.

4.3.1.4. Evaluation parameter EP1.1.4: Improvement of materials

Mechanical failures of reactor components comprise a significant part of initiating events. For operating reactors many efforts have been undertaken on national and international levels to advance the knowledge of failure mechanisms and to improve the properties of materials. Experiences have shown operational benefits (e.g. improved material behaviour) achieved with only minor changes to materials or specifications (likewise for environmental conditions, e.g. coolant pH). Much emphasis with considerable success has been put on the feedback of operating experience into design solutions. The improvements achieved up till now promise that further advances in material properties will lead to better designs with increased robustness.

Acceptability of EP1.1.4: Evidence available to the INPRO assessor demonstrates the use of materials better than those in the reference plant.

4.3.1.5. Evaluation parameter EP1.1.5: Redundancy of operational systems

Increased redundancies of operational systems may help to avoid transients (e.g. caused by faulty control system actions, trips and setbacks) by reducing the probability of degradation or loss of a function. Provided that redundant operational systems are sufficiently independent, increased redundancy can reduce effects from common cause failures. It can also provide better flexibility during operation, e.g. through different capacities of redundant pumps in a PWR's chemistry and volume control systems.

It is acknowledged that an increase of redundancy may increase the complexity of a system as discussed in evaluation parameter EP1.1.2 above. Thus, as mentioned at the beginning of Section 4.3.1, the design has to be optimized in this respect. Design simplification generally cannot be used as justification for reducing the redundancy of operational systems.

Acceptability of EP1.1.5: Evidence available to the INPRO assessor demonstrates that the redundancy of operational systems is greater than that in the reference design.

4.3.1.6. Final assessment of CR1.1: Design of components and systems for normal operation

The **acceptance limit AL1.1** (*design of normal operation systems is more robust than that in the reference design*) of CR1.1 is met if evidence available to the INPRO assessor shows that an optimized combination of the recommendations proposed in evaluation parameters EP1.1.1 to EP1.1.5 qualitatively shows the new design to be more robust than the reference design during normal operation and deviations from normal operation.

A quantitative increase of robustness can only be demonstrated via the assessment of criterion CR1.4 (failures and deviations from normal operation), i.e. providing arguments that the frequency of AOOs is lower than in the reference design.

For a reactor under development, the developer is to describe measures and features that ensure that the robustness of the innovative design will be comparable or superior to that of the reference design.

4.3.2. Criterion CR1.2: Reactor performance

Indicator IN1.2: Reactor performance attributes.

Acceptance limit AL1.2: Superior to those of the reference design.

An improvement of performance attributes in normal operation are expected to increase the robustness of a nuclear reactor. Aspects that are linked to the characteristics of operation of the nuclear reactor assessed are defined as evaluation parameters (EP1.2.1 to EP1.2.8) for CR1.2 and discussed as follows:

- EP1.2.1: Margins of operation;
- EP1.2.2: Reliability of control systems;
- EP1.2.3: Ageing management;
- EP1.2.4: Impact from incorrect human intervention;
- EP1.2.5: Sufficient technical documentation;
- EP1.2.6: Appropriate training programmes;
- EP1.2.7: Plant management organization;
- EP1.2.8: Use of worldwide operating experience.

4.3.2.1. Evaluation parameter EP1.2.1: Margins of operation

An increase of the difference between an operating level and automatic reactor shutdown (scram) level for reactor conditions resulting in scram, e.g. high power, low flow, low pressure, etc, leads to an increased operational margin. Increased operational margins [32] are expected to contribute essentially to the reduction of occurrence of deviations from normal operation and component failures leading to scrams. An example is the power level (trip level), which initiates scram; sometimes this level is itself power-dependent. Before this trip level is actually reached, operational control systems are to be capable of reducing the power increase. In principle, the difference between an operating level and trip level could be set at a higher value and thus the operational margin would be increased (in this case for an overshooting of power). However, it is pointed out that this increased margin may result in a lower power output of the plant.

Acceptability of EP1.2.1: Evidence available to the INPRO assessor demonstrates operational margins larger than those in the reference design.

4.3.2.2. Evaluation parameter EP1.2.2: Reliability of control systems

Advanced self-checking control systems with increased reliability could help to avoid deviations from normal operation. Such advanced control systems could reduce the frequency of anticipated operational occurrences (AOOs) as well as the demand on operators.

Acceptability of EP1.2.2: Evidence available to the INPRO assessor demonstrates that the control systems of the reactor assessed are more reliable than those in the reference design.

4.3.2.3. Evaluation parameter EP1.2.3: Ageing management

The strategy of ageing management normally has to cover all relevant stages in the NPP lifecycle, including design, manufacture, construction, commissioning, commercial operation and decommissioning, all normal operational states, AOOs and accidents influencing a given system, and all relevant mechanisms of ageing including but not limited to embrittlement, fatigue and wear.

The NPP designer has to determine the design life of items important to safety, to provide appropriate design margins to take due account of age-related degradation and to provide methods and tools for assessing ageing during the NPP operation [15, 33]. The NPP operating organization has to develop a plan for preparing, coordinating, maintaining and improving activities for ageing management implementation at the different stages of the NPP lifecycle. Implementation of this plan involves activities on managing ageing mechanisms, detecting and assessing ageing effects, and managing ageing effects [33].

Ref [33] provides detailed guidance on the establishment, implementation and improvement of ageing management programme.

Acceptability of EP1.2.3: Evidence available to the INPRO assessor demonstrates an improvement of the ageing management strategy of the reactor assessed compared to the reference design.

4.3.2.4. Evaluation parameter EP1.2.4: Impact from incorrect human intervention

Impact from incorrect human intervention needs to be reduced. Reduced impact means the reactor systems are more tolerant to operator mistakes during normal operation and AOO conditions. This important characteristic is an expected corollary of having advanced fault tolerant control systems and/or passive features (see also UR6, human factors related to safety).

Acceptability of EP1.2.4: Evidence available to the INPRO assessor demonstrates that incorrect human intervention during normal operation has less impact on reactor operation than in the reference design.

4.3.2.5. Evaluation parameter EP1.2.5: Sufficient technical documentation

Sufficient technical documentation (mostly to be provided by the designer) including manuals have to be available when the plant is close to starting operation and further on. It should be noted that high performance requires knowledge of the actual state as well as documentation of all modifications since the beginning of operation [34], taking into account a planned service time of 60 years. Continuous documentation from the start of operation is important, e.g. to keep records of abnormal occurrences, accumulated loads on components, etc. In the following some important documentation is briefly discussed.

Technical documentation normally includes:

- Design documentation containing information necessary for plant operation, maintenance, tests, ageing management, potential modifications, etc;
- Documentation which has been developed (received) during purchasing of the plant, plant systems structures and components, nuclear fuel and services;
- Plant documentation including plant modifications documentation which is required for verifying fulfilment and compliance with statutory and regulatory requirements and for evaluation of supplies and services;
- Safety and licensing documentation including compilation of licensing notices and documents for verifying fulfilment of safety rules and commitments;
- Quality assurance and quality control documentation including a compilation of the quality control records;
- Documents developed during NPP commissioning and operation: safety-related operating records; records of the plant maintenance; records of radiological protection of personnel and environment;
- Working documentation including technical specifications, manuals and other technical documents for systems, structures and components.

A series of manuals is needed for an NPP, e.g. operating, chemistry, nuclear testing, and conventional testing manuals (see also Ref [35]). In the following a brief description of these manuals is given.

The *operating manual* contains all operating and safety-related instructions for the control room (shift personnel) that are necessary for normal operation of the plant and for mitigating the consequences of transients and accidents.

The *chemistry manual* describes general and specific aspects of chemical-related conditions and actions, as well as chemistry monitoring. The main goal of the chemistry manual is to maintain chemistry conditions in relevant power plant systems and components that ensure a high corrosion resistance. It also provides a basis for establishing proper chemical operating conditions in auxiliary systems and in radioactive waste processing systems.

The *nuclear testing manual* contains the programme of periodic testing. The objective is to verify, at regular intervals or as a consequence of certain plant events, availability, performance, and quality features of systems, components and structures important for safety of the plant.

The *conventional testing manual* encompasses mandatory periodic tests of systems, structures and components necessary to ensure compliance with non-nuclear standards and regulations, e.g. pressure vessel codes.

Currently, computerized manuals are becoming state of the art. Taking advanced system modelling and computer capabilities into account, advanced control systems including expert systems (based on artificial intelligence methods) are expected to be implemented in new designs.

Acceptability of EP1.2.5: Evidence available to the INPRO assessor shows that sufficient (as described above) technical documentation including manuals are (or will be) available prior the start of operation and will be continuously updated.

4.3.2.6. Evaluation parameter EP1.2.6: Appropriate training programmes

Appropriate training on the safety aspects of the nuclear power plant must be provided to all personnel who are directly involved in plant operation and plant and system maintenance, including those who hold responsible positions within the power plant management [36]. The vendor of a nuclear power plant usually offers training programmes and associated courses to the operator/owner of the plant. Training involves group and modular training. It is important to provide well-written training material. The use of simulators for operator training is mandatory.

Acceptability of EP1.2.6: Evidence available to the INPRO assessor shows that appropriate training programmes are established and will be implemented for the reactor assessed.

4.3.2.7. Evaluation parameter EP1.2.7: Plant management organization

A clear plant management organization with defined responsibilities (see Refs [35, 37] for international experience) is a prerequisite for high performance of the plant.

A pre-condition for granting a construction permit for a nuclear installation is that the applicant has the necessary expertise for start-up and operation, and that the competence of the operating personnel and the operating organization is appropriate and meets all licensing requirements. In addition to the organization's structure, functions and the number of personnel required, the owner/operator defines qualification requirements in sufficient detail and corresponding recruitment activities during the construction phase. The organization's structure, job descriptions, qualification requirements, authority and responsibility of personnel and the lines

of management are described by the owner either in the administrative rules or in the plant manual.

Examples of plant operational functions that have to be addressed within the plant management organization are: responsible plant managers for operation, maintenance, technical support, quality assurance, environmental protection, nuclear and industrial safety, and administration (see also CR6.2, safety culture).

Acceptability of EP1.2.7: Evidence available to the INPRO assessor shows that a clear plant management organization with defined responsibilities will be established before start-up.

4.3.2.8. Evaluation parameter EP1.2.8: Use of worldwide operating experience

Operational experience and related evaluations of existing NPPs are collected by international organizations. Examples are the European BWR Forum, BWR Owners Group, Joint IAEA and Nuclear Energy Agency (Organization for Economic Co-operation and Development) International Reporting System for Operating Experience [38], World Association of Nuclear Operators, CANDU Owners Group, etc. As discussed in the introduction section of this report, national utility organizations in several countries (China, European Union, Japan, Republic of Korea, USA) have prepared documents that describe requirements for new designs based on experience with operating plants.

Consequently, this experience needs to be taken into account in the design of a new reactor. An overview of international activities in this area is presented in Ref [39].

Acceptability of EP1.2.8: Evidence available to the INPRO assessor shows that experience from operating nuclear power plants has been taken into account in the reactor design.

4.3.2.9. Final assessment of criterion CR1.2: Reactor performance

The **acceptance limit AL1.2** (*reactor performance attributes are superior to those in the reference design*) of CR1.2 is met, if evidence available to the INPRO assessor shows that the assessment of the above defined evaluation parameters confirms that the reactor design assessed shows:

- Sufficient operational margins to ensure that key system variables relevant to safety do not exceed limits acceptable for continued operation;
- Reduced impact of incorrect human action by appropriate design;
- Use of advanced control systems;
- Planned implementation of a clear management organization with defined responsibilities;
- Sufficient technical documentation including manuals;
- Appropriate training provisions;
- Planned sharing of operating experience and use of it in the reactor design.

For a (innovative) reactor under development, the developer is to describe measures and features to ensure that reactor performance will be comparable or superior to that in operating plants.

4.3.3. Criterion CR1.3: Inspection, testing and maintenance

Indicator IN1.3: Capabilities to inspect, test and maintain.

Acceptance limit AL1.3: Superior to those in the reference design.

To meet this criterion, the reactor design is expected to permit more efficient and intelligent inspection, testing and maintenance. The criterion cannot be fully met by merely requiring more inspections and more testing. The programmes of inspection, testing and maintenance need to

be driven by a sound understanding of failure mechanisms (corrosion, erosion, fatigue etc) so that the right locations are inspected, and the right systems, structures and components are tested and maintained at the right time intervals.

Appropriate inspections, testing and maintenance are important for keeping and improving the level of safety [40]. Because the methods of inspection, testing and maintenance and their effectiveness, efficiency and accuracy are continuously improving, the acceptance limit AL1.3 mostly requires the state of the art[21].

General prerequisites for an appropriate inspection, testing or maintenance programme for a reactor include:

- Knowledge about materials and manufacturing processes, weld locations, non-destructive testing results, locations with high stresses and high cycling frequencies, operating conditions (including chemistry), damage mechanisms (causes and consequences), field experience on similar components (to be documented in a 'living' documentation);
- Implementation of an inspection, testing or maintenance programme including risk-informed approaches (see also criterion CR7.5) taking into account the knowledge as defined above, such as damage mechanisms, design specifics (e.g. stress locations) and operating conditions;
- Decrease of individual and collective doses caused by inspections, testing or maintenance through design provisions, e.g. choice of materials in connection with adequate water chemistry (to avoid radioactive corrosion products), shielding devices, and easy serviceability. This includes also easy access to working locations, appropriate environmental working conditions and the development of specific tools and robotics in order to reduce dose rates and/or durations of inspections, testing or maintenance (see also criterion CR1.5).

It is recognized that in the early operational stages of an innovative reactor, before the technology (experience) base is fully established, more inspection, testing and maintenance, may be required.

The **acceptance limit AL1.3** (*capability to inspect, to test and to maintain superior to that in the* reference design) of CR1.3 is met, if evidence available to the INPRO assessor confirms that in the reactor assessed:

- Inspections, testing and maintenance are (will be) more effective and efficient than those in the reference plant;
- An appropriate inspection, testing and maintenance programmes are (will be) established;
- Design features to facilitate the performance of inspections, testing and maintenance have been demonstrated.

For a (innovative) reactor under development, measures and features are to be described that ensure that the capability to inspect, test and maintain will be comparable or superior to that in operating nuclear reactors.

4.3.4. Criterion CR1.4: Failures and deviations from normal operation

Indicator IN1.4: Expected frequency of failures and deviations from normal operation.

Acceptance limit AL1.4: Lower than that in the reference design.

[21] 'State of the art' means that the latest available technology needs to be used in the design of the reactor assessed.

For the reactor design assessed, the expected frequencies of initiating events leading to anticipated operational occurrences (AOOs) are supposed to be lower than those in the reference design.

The frequency of these initiating events for operating reactors is determined from operational experience and probabilistic analyses. Apparently, for more robust designs the reduction of these frequencies relative to those for the reference design is possible. However, the frequencies of such initiating events are usually defined as licensing requirements by national regulatory bodies based on detailed national probabilistic studies (see for example Refs [41–45]). Thus, they cannot be easily reduced by a designer because such a reduction would need approval by the responsible regulatory authority.

However, for an INPRO assessment. technical arguments can be presented by the designer/ developer that support a reduction of these frequencies of AOOs. Examples of arguments to support such a reduction of frequencies could be a positive judgment on criteria CR1.1 to CR1.3: improved materials, simplified designs (e.g. less valves), improved design margins (e.g. against overstressing and fatigue, against departure from nuclear boiling, etc.), increased operating margins, increased redundancies of operational systems, less impact from incorrect human intervention (the reactor systems need to be tolerant to human mistakes), more effective and efficient inspections, a continuous monitoring of the plant health, etc.

It is to be mentioned that the frequency of external events per se cannot be influenced by the designer or operator for a given site. An appropriate selection of the site for the nuclear reactor assessed could have a positive effect. However, the frequency of AOOs caused by external events can be influenced by the designer or operator. For some particular external events and NPP locations, the comparison of frequencies of AOOs of the planned reactor against those of the reference design involves comparison against relevant national regulatory requirements.

The **acceptance limit AL1.4** (*reduced expected frequencies of failures and deviations from normal operation)* of CR1.4 is met if technical arguments available to the INPRO assessor show that fewer failures and deviations from normal operation (per year and unit) are expected than in the reference design.

4.3.5. Criterion CR1.5: Occupational dose

Indicator IN1.5: Occupational dose values during normal operation and AOOs.

Acceptance limit AL1.5: Lower than the dose constraints.

This criterion focuses on radiation protection of NPP workers. It is important to note that criterion CR1.5 does not consider radiation exposure of workers during accidents; it considers only plant states corresponding to Levels 1 and 2 of DID, i.e. normal operation and anticipated operational occurrences. The issue of avoiding undue burdens from radiation exposure to the public and environment during normal operation and AOOs is covered in a separate area of the INPRO methodology called environmental impact of stressors; after accidents this issue is covered via INPRO NES sustainability user requirement UR4 for the area of reactor safety, which states that accidental releases outside the plant are prevented or mitigated.

The recommendations of the IAEA Safety Standards for considering radiation protection in NPP design are provided in Ref [46]. Ref [47] recommends the use of dose constraints “for optimization of protection and safety, the intended outcome of which is that all exposures are controlled to levels that are as low as reasonably achievable, economic, societal and environmental factors being taken into account”.

The role of dose constraints is explained in Ref [48]:

> "3.31. To apply the optimization principle, individual doses should be assessed at the design and planning stage, and it is these predicted individual doses for the various options that should be compared with the appropriate dose constraint. Options predicted to give doses below the dose constraint should be considered further; those predicted to give doses above the dose constraint should normally be rejected."

Known occupational doses from normal operation and AOOs in modern NPPs are already very low, so this INPRO criterion CR1.5 does not go beyond asking for further *ad hoc* exposure reduction in dose. Fig. 1 shows accumulated yearly occupational doses in operating NPPs versus year of reporting. It is evident that the occupational doses decreased continuously with increasing lifetime and improved NPP designs. This was achieved by such measures as minimizing source terms (e.g. avoiding cobalt impurities in materials, using erosion/corrosion resistant materials for steam line designs to limit deposits, achieving adequate coolant chemistry), incorporating layout features that reduce the collective dose (e.g. strict physical separation/shielding of systems, accessibility, separation, shielding, handling, set down areas), and using maintenance friendly designs of equipment. It is expected that these features can be implemented in new (advanced) designs and thus – with further improvements – actual doses in new reactors may be further decreased.

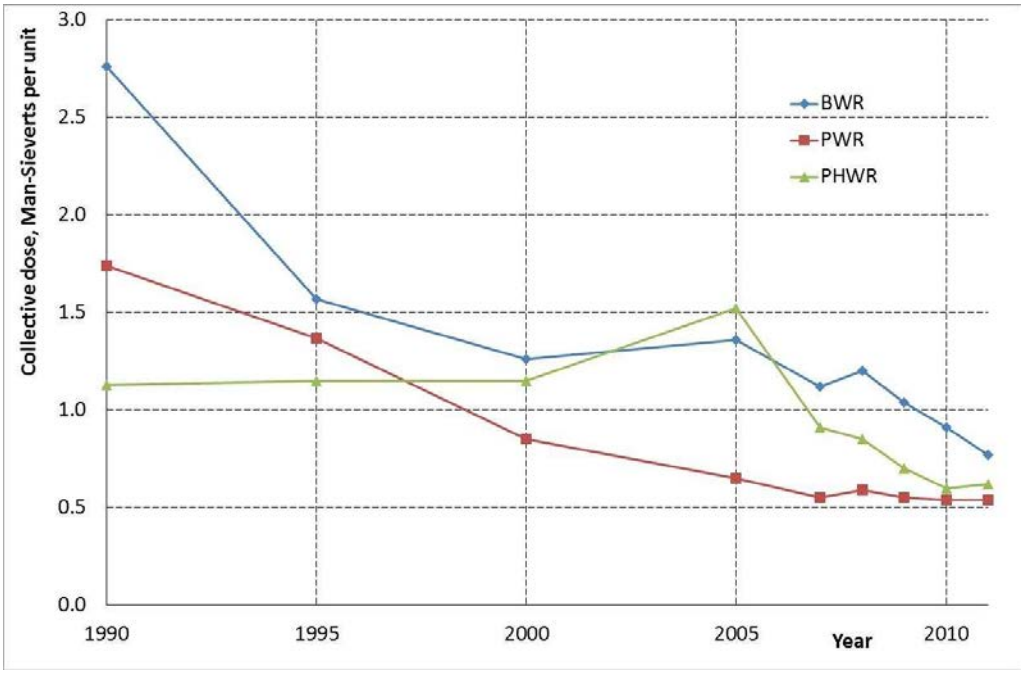

FIG. 1. Accumulated yearly occupational dose (modified from Ref [49]).

The reactor assessed needs to ensure an efficient implementation of the concept of optimization of radiation protection for workers during design, commissioning, operation, and decommissioning through the use of automation, remote maintenance and operational experience from existing designs. Experience in operating reactors shows that maintenance, i.e. in-service inspection and periodic tests and repairs (including replacement), are the sources of most occupational doses. Criterion CR1.5 anticipates that new (advanced) reactors can take advantage of design concepts to achieve occupational dose reduction as a zero-cost side-effect of measures such as automated inspection and maintenance. New reactor designs are expected to be maintenance-friendly through careful layout, reliable equipment, and electronic availability of maintenance procedures at the work-face to guide those charged with performing maintenance duties.

In the INPRO methodology, the dose constraints concept is discussed in more detail in the manual on environmental impact of stressors.

The **acceptance limit AL1.5** (*occupational doses lower than dose constraints*) is met if evidence available to the INPRO assessor shows that doses to workers during normal operation and AOOs have been optimized and are (will be) less than the dose constraints defined or accepted by national regulatory bodies.

4.4. UR2: DETECTION AND INTERCEPTION OF ANTICIPATED OPERATIONAL OCCURENCES

INPRO user requirement UR2 for sustainability assessment in the area of nuclear reactor safety: The nuclear reactor assessed has improved capabilities to detect and intercept deviations from normal operational states in order to prevent AOOs from escalating to accident conditions.

This INPRO NES sustainability user requirement UR2 mostly[22] relates to the second level of the DID concept, which has the purpose of detecting and controlling deviations from normal operational states in order to prevent anticipated operational occurrences at the plant from escalating to accident conditions. The purpose is achieved if the plant returns to normal operation and the progression of AOOs to more severe conditions avoided.

In the design of new reactors, priority is given to advanced instrumentation and control (I&C) systems, and improved reliability of these systems. Optimization of a combination of reliable passive and active systems is important. When appropriate, priority can be given to (design-specific) inherent limiting characteristics (sometimes called 'self-controlling properties' or 'inherent safety features', see INPRO NES sustainability user requirement UR5 in this publication and Ref [50] for more detailed discussions) and to robust and simple (possibly passive) control systems and advanced monitoring systems.

The main function of the I&C system in this level of DID is to detect AOOs and enable the rapid return of the plant to normal operation conditions with, ideally, no consequences, e.g. no need for follow up inspections or regulatory event reports. I&C system data processing involves measurement data from several different sets of instrumentation, e.g. conventional process instrumentation, in-core instrumentation, ex-core instrumentation, rod position measurement instrumentation, reactor vessel water level measurement instrumentation, loose parts and vibration monitoring instrumentation, radiation monitoring instrumentation, accident instrumentation, hydrogen detection instrumentation, and boron instrumentation. These instrumentation sets may contain channels of different importance to safety. For innovative reactor designs, inherent characteristics and/or passive systems (or components) may be able to assist or even partially replace certain capabilities of the I&C system.

In addition to those AOOs that can influence the nuclear fuel in the reactor core, the design also has to cover the potential AOOs that involve the on-site handling and storage of fresh fuel and spent fuel outside the reactor core.

The INPRO methodology criteria for UR2 are presented in Table 4.

[22] UR2 also involves consideration of selected provisions in Level 1 of DID.

TABLE 4. CRITERIA FOR USER REQUIREMENT UR2 FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

INPRO user requirement	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR2: Detection and interception of AOOs: *The nuclear reactor assessed has improved capabilities to detect and intercept deviations from normal operational states in order to prevent AOOs from escalating to accident conditions.*	CR2.1: I&C system and inherent characteristics	IN2.1: Capabilities of the I&C system to detect and intercept and/or capabilities of the reactor's inherent characteristics to compensate for deviations from normal operational states. AL2.1: Superior to those in the reference design.
	CR2.2: Grace periods after AOOs	IN2.2: Grace periods until human actions are required after AOOs. AL2.2: Longer than those in the reference design.
	CR2.3: Inertia	IN2.3: Inertia to cope with transients. AL2.3: Larger than that in the reference design.

Improved I&C systems, improvements in the reactor's inherent characteristics, longer grace periods and increased system inertia make the reactor more robust against AOOs.

4.4.1. Criterion CR2.1: I&C system and inherent characteristics

Indicator IN2.1: Capabilities of the I&C system to detect and intercept and/or capabilities of the reactor's inherent characteristics to compensate for deviations from normal operational states.

Acceptance limit AL2.1: Superior to those in the reference design.

INPRO has defined the following evaluation parameters for CR2.1:

- EP2.1.1: Continuous monitoring of plant health.
- EP2.1.2: Capability of I&C system
- EP2.1.3: Compensation of deviations from normal operation.

Inherent safety characteristics[23] of a nuclear reactor, such as a negative reactivity feedback, influence the dynamic behaviour of the plant in a positive way, and can lead to reduced design requirements for the I&C systems.

4.4.1.1. Evaluation parameter EP2.1.1: Continuous monitoring of plant health

Monitoring of operational data is important for early detection of the onset of integrity loss in reactor system components and avoiding a complete failure of the component. For this purpose, several monitoring systems[24] have been developed.

The installation of monitoring systems can help justify a reduction of design requirements for a nuclear reactor. As an example, the introduction of a leak-before-break (LBB) concept with the corresponding monitoring concept could justify elimination of a large break loss of coolant accident (LB-LOCA) as a design basis accident in water-cooled reactors. Elimination of LB-LOCA would lead to a significant reduction of accident loads on reactor pressure vessel internals to be considered in the design. In addition, the number of pipe restraints to cope with pipe whipping due to jet forces (break flow) could be reduced.

Appendix III gives examples of monitoring systems for water cooled reactors.

[23] See also UR5 in Section 4.8.

[24] Monitoring systems listed in this section are generally normal operation systems used mostly in Level 1 of DID in currently operating reactors. Some of these systems can help to detect AOOs.

Acceptability of EP2.1.1: Evidence available to the INPRO assessor shows that the reactor design includes systems for continuous monitoring of plant health and computerized aids for the operators.

4.4.1.2. Evaluation parameter EP2.1.2: Capability of the I&C system

The capability of the I&C system of advanced reactors to detect and control AOOs needs to be improved over that of the reference plant. Improved capability is expected to involve improvements of system efficiency, effectiveness and reliability achieved for example through increased redundancy and diversity.

Acceptability of EP2.1.2: Evidence available to the INPRO assessor shows that the I&C system of the reactor assessed is superior to that of the reference plant.

4.4.1.3. Evaluation parameter EP2.1.3: Compensation of deviations from normal operation

An analysis of the nuclear power plant dynamics is required to show how the different events causing a deviation from normal operation are compensated by the I&C system and inherent safety features. The dynamic plant model used in the analysis needs the capability to accurately simulate trip parameters, control and auxiliary systems operational behaviour, reactor protection system and safety systems variables, reactor feedbacks and other inherent safety characteristics. When practicable, the reactor design's compensation of AOOs can give priority to reliance on well-developed inherent safety characteristics. For an I&C system to be acceptable, the results of the analyses demonstrate that all limitations and safety limits are met in case of assumed deviations from normal operation.

Acceptability of EP2.1.3: Evidence available to the INPRO assessor shows that a plant analysis has been performed and that its results confirm that key system variables relevant to safety (e.g. heat flux, flow, pressure, temperature) do not exceed limits acceptable for continued operation and do not result in any short-term consequences affecting normal operation.

4.4.1.4. Final assessment of criterion CR2.1: I&C and inherent characteristics

The **acceptance limit AL2.1** (*superior behaviour of I&C in AOOs)* is met if evidence available to the INPRO assessor shows that EP2.1.1, EP2.1.2 and EP2.1.3 above have been met.

4.4.2. Criterion CR2.2: Grace periods after AOOs

Indicator IN2.2: Grace periods until human actions are required after AOOs.

Acceptance limit AL2.2: Longer than those in the reference design.

The 'grace period' for normal operation is defined as the time available, in case of a failure or the beginning of an AOO, before human (operator) action is required. The appropriate value of the grace period depends on the type of nuclear facility, the ease of diagnosis of the failure and the complexity of the human action to be taken.

In case of deviations from normal plant states, the time period for the operator to cope with such deviations can be divided into three different parts:

1) Time to detect;
2) Time to diagnose the deviations and to initiate the necessary countermeasures; and
3) Time for manual control actions, i.e. time for a repair or other measures.

The time needed by the operator for *detecting* a deviation is dependent on the situation and alarm signals.

The time to *diagnose* the situation appropriately is mainly dependent on the time and aids available to operators to identify the plant state. In addition, reliability of the I&C system is important.

It is common practice to assume that, within a time period no longer than 30 minutes, the operator will have detected and identified the situation sufficiently to perform appropriate *manual actions* based on the fact that operators are trained to cope with anticipated operational occurrences. Therefore, the design of the reactor needs to be such that all necessary safety related actions within this time period are automated.

The **acceptance limit AL2.2** (*sufficient grace periods after AOOs*) is met if evidence available to the INPRO assessor shows that grace periods are longer than those in the reference design and amount to at least 30 minutes after detection of a failure or AOO.

4.4.3. Criterion CR2.3: Inertia

Indicator IN2.3: Inertia to cope with transients.

Acceptance limit AL2.3: Larger than that in the reference design.

The term 'inertia' means the capability of a nuclear reactor to cope with AOOs; the main objective of a high inertia is to avoid consequences with safety implications that could delay a return to normal operation.

A nuclear reactor is usually designed to stay within the design limits (e.g. temperatures, pressures, stresses, etc.) for all AOOs, taking into account also a single failure and the repair status of components. Nevertheless, slower transients of system parameters (e.g. slower changes in temperature or pressure) are generally considered preferable.

A high inertia resulting in a slow response to initiating events is usually achieved by sufficiently large mass within the primary system (e.g. in HTGRs), sufficiently large primary water inventory (e.g. in water-cooled reactors), small excess reactivity (e.g. in HWRs), and a large secondary side mass (e.g. in PWRs and liquid metal cooled reactors).

For example, in a PWR with a sufficiently large pressurizer, an AOO with a primary pressure increase (e.g. after a loss of load) will result in no loss of primary coolant mass via the valves of the pressurizer. Any contamination of the confinement/containment by radioactive coolant will thus be avoided due to sufficient inertia of the system.

To demonstrate the adequacy of the nuclear reactor design, the system behaviour for all AOOs has to be analysed with validated and verified computer models (see also EP2.1.3 of criterion CR2.1 and criterion CR7.3).

The **acceptance limit AL2.3** (*inertia is higher than that of the reference design*) of CR2.3 is met if evidence available to the INPRO assessor shows that the assessed reactor has a system inertia higher than that of the reference design.

4.5. UR3: DESIGN BASIS ACCIDENTS

INPRO user requirement UR3 for sustainability assessment in the area of nuclear reactor safety: The frequency of occurrence of DBAs in the nuclear reactor assessed is reduced. If an accident occurs, engineered safety features are able to restore the reactor to a controlled state, and subsequently to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention is minimal, and only required after a sufficient grace period.

This INPRO user requirement UR3 for sustainability assessment in the area of reactor safety mostly relates to the third level of the DID concept, which has the purpose of controlling

accidents, preventing damage to the reactor core and preventing radioactive releases requiring off-site protective actions and returning the plant to a safe state.

The ‘design basis’ of a plant comprises the conditions and events taken into account in the design of the nuclear reactor such that the plant can withstand them by the planned operation of safety systems without exceeding authorized limits. Hence, a DBA is an accident causing conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which the damage to the fuel and releases of radioactive material are kept within authorized limits [17].

The NPP design has to consider potential DBAs in all relevant operating stages of the nuclear reactor (e.g. commissioning, commercial operation and decommissioning) and operating phases (e.g. reactor start-up, power operation, hot stand-by, system shutdown, refuelling outage). In addition to accidents impacting the nuclear fuel in the reactor core, the design has to cover also accidents endangering the fresh fuel storage, on-site fuel transportation systems and the corresponding near reactor spent fuel pool.

The term ‘frequency of occurrence’ used in UR3 means the number of events per reactor year leading to a DBA as determined via probabilistic methods (probabilistic risk assessment).

An NPP has to be designed against DBAs caused by internal and external events (design basis external events – DBEE) and probable combinations thereof. A DBEE is “an external event or a combination of external events selected for the design of all or any part of a nuclear power plant, characterized by or having associated with it certain parameter values” [23]. DBEEs are the external events considered in the design basis of the plant and “to perform the safety functions required for DBEEs the designer should use either systems specific to external events or the safety systems already present in the plant for internal events” [23]. Examples of external events to be considered in the design are earthquake, flooding, external explosion, severe storm, airplane crash, sabotage, etc. [22, 23]. As mentioned above, the frequency of external events per se cannot be influenced by the designer or operator for a given site. An appropriate selection of the site for the nuclear reactor assessed could have a positive effect. However, the frequency of DBAs caused by external events can be influenced by designer or operator. Based on lessons learned from the accident in Fukushima [24–28], also probable combinations of external events should be considered in the design such as an earthquake plus a fire and/or tsunami.

The term ‘controlled state’ is characterized by a situation in which the engineered safety features are able to compensate for the loss of functionality resulting from the DBA. An optimized combination of active and passive engineered safety features is expected to be used.

For advanced (innovative) reactor designs using passive design features to achieve almost all of the fundamental safety functions may be possible. These features could include passive shutdown, passive decay heat removal systems and passively operated coolant injection systems.

A reduced frequency of occurrence of DBAs, longer grace periods after detection of DBAs, enhanced reliability and capacity of engineered safety features, and increased subcriticality margins after DBAs will make the reactor design more robust against DBAs. The INPRO methodology criteria for UR3 are presented in Table 5.

TABLE 5. CRITERIA FOR USER REQUIREMENT UR3 FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

INPRO user requirement	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR3: Design basis accidents: *The frequency of occurrence of DBAs in the nuclear reactor assessed is reduced. If an accident occurs, engineered safety features are able to restore the reactor to a controlled state, and subsequently to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention is minimal, and only required after a sufficient grace period.*	CR3.1: Frequency of DBAs	IN3.1: Calculated frequencies of occurrence of DBAs. AL3.1: Frequencies of DBAs that can cause plant damage are lower than those in the reference design.
	CR3.2: Grace period for DBAs	IN3.2: Grace periods for DBAs until human intervention is necessary. AL3.2: At least 8 hours and longer than those in the reference design.
	CR3.3: Engineered safety features	IN3.3: Reliability and capability of engineered safety features. AL3.3: Superior to those in the reference design.
	CR3.4: Barriers	IN3.4: Number of confinement barriers maintained (intact) after DBAs and DECs. AL3.4: At least one and consistent with regulatory requirements for the type of reactor and accident under consideration.
	CR3.5: Subcriticality margins	IN3.5: Subcriticality margins after reactor shutdown in accident conditions. AL3.5: Sufficient to cover uncertainties and to maintain shutdown conditions of the core.

4.5.1. Criterion CR3.1: Frequency of DBAs

Indicator IN3.1: Calculated frequencies of occurrence of DBAs.

Acceptance limit AL3.1: Frequencies of DBAs that can cause plant damage are lower than those in the reference design.

This criterion CR3.1 asks for a reduced frequency of occurrence (probability) of NPP DBAs caused by both internal and external events and probable combinations thereof.

The frequency of occurrence of DBAs is to be determined via a probabilistic risk assessment. Based on design and confirmed by operating experience (more than ten thousand reactor years of operation) and analytical assessments, the correlation between the frequency of occurrence and the value of consequences (e.g. damage or dose) is such that consequences increase with decreasing frequencies of occurrence.

The approach to assessment of CR3.1 for accidents caused by internal events is discussed in Appendix IV.

The frequency of accidents caused by external events depends heavily on the site selected for the plant and can therefore be influenced both by the NPP designer and the (future) owner/operator of the plant. Such accidents need to be discussed during the INPRO assessment with reference to the national safety standards regulating these issues.

The **acceptance limit AL3.1** (*Reduced frequency of DBAs that can cause plant damage relative to that of a reference plant*) of CR3.1 is met if evidence available to the INPRO assessor shows lower frequencies of design basis accidents than in the reference design.

4.5.2. Criterion CR3.2: Grace period for DBAs

Indicator IN3.2: Grace periods for DBAs until human intervention is necessary.

Acceptance limit AL3.2: At least 8 hours and longer than those in the reference design.

The criterion CR3.2 'grace periods for DBAs' is applicable in Level 3 of DID and implies a similar concept as introduced earlier for control of AOOs (see CR2.2) in Level 2 of DID. For DBAs (caused by internal and external events and probable combinations thereof) the criterion requires that actions of automatic active and/or passive safety systems provide an adequate grace period for the operator before intervention is necessary.

Because the control of DBAs is very important – the next DID level would be the potential for a highly degraded core – the grace period available for operators during the DBA are longer than for AOOs. For the purpose of INPRO assessment of NES sustainability, a basis for the definition of an adequate grace period may be the shift change of operators, usually, taking place every 8 hours, because a new operator crew will take over responsibility and possibly bring fresh insights into accident diagnosis.

There are a few points which may further contribute to the discussion of adequate grace period: shift change after 8 hours may be undesirable for the sake of accident progression knowledge continuity; the next shift may need to be called earlier; accident diagnosis in advanced reactors may be made more efficient, etc. However, these points are deemed to be considered rather as an input for developing efficient operation manuals and accident management procedures whereas 8 hours can be proposed as a limit for design provisions on the adequate grace period for DBAs.

Such a longer grace period results in extended design requirements as compared with those for AOOs, mainly longer fully automated system responses (e.g. emergency power supply, residual heat removal, battery power for I&C, etc.). Sufficient battery power (DC) is required for the I&C systems to identify and assess the plant state and initiate necessary actions. Usually battery power is used for many purposes (e.g. instrumentation, valves, lighting, etc.). The capacity of batteries in most operating reactors is usually designed to use this power for all purposes for about 2–4 hours[25]. For innovative designs, passive safety systems may reduce the need for emergency power supply (via diesels or turbines) for residual heat removal systems.

The **acceptance limit AL3.2** (*increased grace period for a DBA relative to a reference plant*) of CR3.2 is met if evidence available to the INPRO assessor shows that the reactor assessed in case of DBAs has grace periods longer than those of the reference design and at least 8 hours long.

4.5.3. Criterion CR3.3: Engineered safety features

Indicator IN3.3: Reliability and capability of engineered safety features.

Acceptance limit AL3.3: Superior to those in the reference design.

The capability of the engineered safety features is characterized by their sufficiency to restore the reactor to a controlled state after DBAs without operator action. The term 'controlled state' is characterized by a situation in which the engineered safety features are able to compensate for loss of functionality resulting from a DBA (caused by internal and external events and probable combinations thereof). The reactor has to be taken to a safe shutdown state at least within the designed grace period (see CR3.2) with the assurance that sufficient core cooling

[25] Stretching the battery power for a longer period is possible, if the power supply of components not necessary to cope with an accident is interrupted and the remaining power is used for absolutely needed functions such as monitoring purposes. In addition, in accident conditions more severe than DBAs, a recharge of batteries via mobile equipment is expected to be possible in new reactor designs in cases where access to the reactor compartments with the batteries is not possible.

exists. For this purpose, an optimized combination of active and passive engineered safety features is expected to be used.

A probabilistic safety assessment [51] (together with an uncertainty analysis) for the safety-related part of the I&C system needs to be performed with high quality to demonstrate calculated high reliability (low unavailability) of the safety related I&C for all states of the nuclear reactor (full and reduced power operation, shutdown state).

Complementary information on engineered safety features is provided in Appendix V.

The **acceptance limit AL3.3** (*reliability and capability of engineered safety features*) of CR3.3 is met if evidence available to the INPRO assessor shows that the reactor assessed, in case of a DBA (caused by internal or external events and probable combinations thereof), shows an increased reliability of its safety systems compared to the reference plant and the engineered safety features in the reactor assessed are sufficient to reach a controlled state after a DBA based on automatic actions within a grace period of at least 8 hours (as defined in CR3.2).

4.5.4. Criterion CR3.4: Barriers

Indicator IN3.4: Number of confinement barriers maintained (intact) after DBAs and DECs.

Acceptance limit AL3.4: At least one and consistent with regulatory requirements for the type of reactor and accident under consideration.

The indicator IN3.4 'number of barriers maintained' and the corresponding acceptance limit AL3.4 'at least one and consistent with regulatory requirements for the type of accident under consideration' mean that the safety systems and safety features are expected to deterministically provide for continued integrity at least of one barrier (containing the radioactive material) following any accident caused by internal or external events and probable combinations thereof. However, when national regulatory documents or international safety standards require to maintain more than one barrier after a certain type of accidents these requirements are to be used as the acceptance limit values (for this type of accidents) for INPRO assessment.

The indicator IN3.4 consists of two parameters that are considered on different levels of DID: number of barriers after DBAs and number of barriers after DECs. The latter requires to demonstrate the maintenance of at least one barrier (e.g. containment) after all DECs including those with the severe damage of reactor core. For existing and evolutionary water-cooled reactors, it overlays the first part of indicator that focuses on DBAs unless national regulations or international safety standards require to maintain more than one barrier after a certain type of DBAs. Moreover, the existing and evolutionary water-cooled reactors are usually designed to maintain integrity of the reactor core[26] (and corresponding barriers) after DBAs, which is the part of their licensing requirements. Thus, the INPRO assessment of evolutionary water-cooled reactors against this criterion can be focused only on the number of confinement barriers maintained intact after DECs unless national regulations or international safety standards require to maintain more than one barrier after a certain type of DBAs. However, the innovative reactors may involve different layout of physical barriers (e.g. molten salt reactors) and different number of co-located fuel cycle steps[27] (e.g. on-site reprocessing and re-fabrication) with different requirements on confinement barriers. Thus, the INPRO assessment of innovative

[26] I.e. maintain integrity of the reactor core within authorized limits, e.g. limited number of fuel rods failures depending on the size of a break can be acceptable after LOCA in PWR.

[27] Nuclear fuel cycle facilities normally have less barriers than reactors. For more details see the INPRO methodology manual on safety of nuclear fuel cycle facilities.

reactors against this criterion has to be focused on the number of confinement barriers maintained intact after DBAs and DECs.

Complementary information on the confinement barriers is provided in Appendix VI.

The **acceptance limit AL3.4** (barriers) of CR3.4 is met if evidence available to the INPRO assessor confirms, deterministically after all DBAs and DECs (caused by internal or external events), that number of confinement barriers maintained intact in new design is consistent with regulatory requirements[28] for the type of reactor and accident under consideration and in any case at least one (intact) barrier remains against an accidental release of radioactivity (fission products) to the environment.

4.5.5. Criterion CR3.5: Subcriticality margins

Indicator IN3.5: Subcriticality margins after reactor shutdown in accident conditions.

Acceptance limit AL3.5: Sufficient to cover uncertainties and to maintain shutdown conditions of the core.

Indicator IN3.5 'Subcriticality margins after reactor shutdown in accident conditions' refers to the magnitudes of reactivity of the shutdown reactor core when these parameters are supposed to be negative. Reactivity is a core characteristic related to the increase (positive reactivity) or decrease (negative reactivity) of the neutron population driven by the ongoing chain fission reactions[29]. The value of reactivity and its behaviour as a function of time depends primarily on the core size and geometry, fuel[30] composition (enrichment, burn-up, burnable poisons, etc), fuel structure, geometry and temperature, coolant and moderator parameters (temperature, density, poison concentration), and control rod positions and characteristics.

Shutdown system designs may vary greatly depending on the reactor type. Most designs involve inserting control rods into the core and/or the neutron reflector. Many designs involve a combination of control rod insertion and soluble neutron poison injection. To obtain necessary reliability of the shutdown function, the primary shutdown system can be supplemented by one or more back-up systems with a different physical mechanism. Shutdown systems can also use physical mechanisms based on passive components to increase their reliability.

In accident conditions caused by external or internal events, sufficient shutdown reactivity has to be available to make the core subcritical in the shortest possible time and to reliably keep it subcritical over a long period of time. The generally agreed value of the calculated minimum shutdown reactivity margin including a consideration of uncertainties (i.e. margin defined in addition to uncertainties) and a worst single failure in the shutdown system (e.g. most effective control rod stuck) is 1 % $\Delta k/k$[31].

The **acceptance limit AL3.5** (sufficient subcriticality margins) of CR3.6 is met by the reactor assessed if evidence available to the INPRO assessor confirms a calculated shutdown reactivity margin of at least 1 % $\Delta k/k$, including consideration of uncertainties and a worst single failure.

---

[28] If such requirements exist for a given type of reactor at the moment of INPRO assessment.

[29] Situations with neutron flux growth in a subcritical core are possible, e.g. during the reactor start up after refuelling or during rapid variations of core power, however these specific processes are not discussed in this publication.

[30] Including blanket fuel when used.

[31] The term k is the neutron multiplication factor. The reactivity, $\Delta k/k$, is the relative change.

4.6. UR4: SEVERE PLANT CONDITIONS

INPRO user requirement UR4 for sustainability assessment in the area of safety of nuclear reactor: The frequency of an accidental release of radioactivity into the containment / confinement is reduced. If such a release occurs, the consequences are mitigated, preventing or reducing the frequency of occurrence of accidental release into the environment. The source term of the accidental release into the environment remains well within the envelope of the reference reactor source term and is so low that calculated consequences would not require evacuation of the public.

This INPRO user requirement UR4 for sustainability assessment in the area of reactor safety is mostly[32] related to the prevention of accident progression and the mitigation of severe accident consequences. An accidental release of radioactivity from the reactor fuel into the containment/ confinement could occur if, after an initiating (internal or external) event, additional failures of safety systems would occur and lead to severe core damage, i.e. loss of integrity of the fuel cladding in a majority of nuclear fuel elements of water-cooled reactors (coated fuel particles in the case of HTGRs). Potential reasons for reaching severe plant conditions include reaching a so-called cliff edge effect during the progression of certain external and internal events or probable combinations thereof. Ref [52] defines a cliff edge effect as "an instance of severely abnormal plant behaviour caused by an abrupt transition from one plant status to another following a small deviation in a plant parameter, and thus a sudden large variation in plant conditions in response to a small variation in an input". In addition to accidents impacting the nuclear fuel in the reactor core, the design has to cover also accidents endangering the spent fuel in the corresponding spent fuel pool.

Mitigating the consequences means that the radioactivity released from the core during severe accidents needs to be kept safely inside the containment/ confinement of the reactor. For new reactors, the reliability of safety systems for controlling such complex accident sequences with severe core damage is expected to be increased, including their instrumentation, control and diagnostic systems, and appropriate severe accident management procedures are developed. By these measures, the frequency of occurrence of severe accidents with an emergency radioactivity release into the environment can be reduced.

The design of NPPs has to consider potential severe plant conditions in all relevant operating stages of the nuclear reactor (e.g. commissioning, commercial operation and decommissioning) and operating phases (e.g. reactor start-up, power operation, hot stand-by, system shutdown, refuelling outage). Indications of increased design robustness against severe accidents with severe core damage include: (i) a reduced frequency of severe accidents caused by internal and external events and probable combinations thereof, (ii) existence of sufficient engineered processes and equipment to control relevant system parameters and activity levels in the containment/ confinement, (iii) sufficient in-plant accident management to prevent or mitigate an accidental release of radioactivity from the plant to its environs and (iv) increased design margins of the containment/ confinement against internal and external loads. Based on the lessons learned from the accident at Fukushima Daiichi in 2011, the design of new reactors needs to demonstrate an increased robustness against some extreme situations (with more than one initial event and multiple failures).

The INPRO methodology requirements for NES sustainability assessment that relate to emergency preparedness and response, i.e. Level 5 of DID, have been considered as part of the

[32] UR4 discusses accident conditions more severe than DBA, including DEC and accident conditions associated with Level 4 of DID.

national infrastructure necessary to create and maintain a sustainable nuclear energy system. Such requirements are therefore described in the INPRO manual covering the Infrastructure area [1].

The INPRO methodology criteria for UR4 are presented in Table 6.

TABLE 6. CRITERIA FOR USER REQUIREMENT UR4 FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

INPRO user requirements	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR4: Severe plant conditions: The frequency of an accidental release of radioactivity into the containment / confinement is reduced. If such a release occurs, the consequences are mitigated, preventing or reducing the frequency of occurrence of accidental release into the environment. The source term of the accidental release into the environment remains well within the envelope of the reference reactor source term and is so low that calculated consequences would not require evacuation of the public.	CR4.1: Frequency of release into containment / confinement	IN4.1: Calculated frequency of accidental release of radioactive materials into the containment / confinement. AL4.1: Lower than that in the reference design.
	CR4.2: Robustness of containment / confinement design	IN4.2: Containment loads covered by the design, and natural or engineered processes and equipment sufficient for controlling relevant system parameters and activity levels in containment / confinement. AL4.2: Larger than those in the reference design.
	CR4.3: Accident management	IN4.3: In-plant accident management (AM). AL4.3: AM procedures and training sufficient to prevent an accidental release outside containment / confinement and regain control of the reactor.
	CR4.4: Frequency of accidental release into environment	IN4.4: Calculated frequency of an accidental release of radioactive materials into the environment. AL4.4: Lower than that in the reference design. Large releases and early releases are practically eliminated.
	CR4.5: Source term of accidental release into environment	IN4.5: Calculated inventory and characteristics (release height, pressure, temperature, liquids/gas/aerosols, etc) of an accidental release. AL4.5: Remain well within the inventory and characteristics envelope of the reference reactor source term and are so low that calculated consequences would not require public evacuation.

4.6.1. Criterion CR4.1: Frequency of release into the containment/ confinement

Indicator IN4.1: Calculated frequency of accidental release of radioactive materials into the containment / confinement.

Acceptance limit AL4.1: Lower than that in the reference design.

An accidental release of radioactivity into the containment/ confinement could occur if the integrity of a major part of nuclear fuel in the reactor core or in the spent nuclear fuel pool is lost during an accident. Table 7 gives examples of very low core damage frequencies (CDFs) claimed by the designers of AP1000 [53], EPR [54] and KERENA (SWR1000) [55].

During an accident, a highly degraded core with an accidental release of volatile fission products from the damaged nuclear fuel elements (or coated fuel particles in the case of an HTGR) will result if safety systems are not able to restore (and keep) the core in a safe state (e.g. cooled and subcritical). Usually, the volatile fission products will be released into the containment/confinement atmosphere. Depending on the design, molten and solid core material

may enter the containment/confinement after destruction (failure) of the reactor pressure vessel (RPV); the integrity of the containment/confinement may thus be threatened, e.g. for light water reactors (LWRs) by core/concrete-interactions or hydrogen (or steam) explosions.

TABLE 7. FREQUENCY FOR A HIGHLY DEGRADED CORE PER UNIT AND YEAR

Type of reactor	Frequency of core damage per year
AP1000	
- Internal events during power operation	$2.4\ 10^{-7}$
- Internal events, fires and floods during power operation and shutdown	$5.1\ 10^{-7}$
EPR (power operation plus shutdown)	
- Internal events	$6.1\ 10^{-7}$
- Internal and external events,	$2.0\ 10^{-6}$
KERENA (with AM measures)	
- Shut down	$4.1\ 10^{-8}$
- Power operation	$4.3\ 10^{-8}$

Note: AM - accident management (see CR4.3).

To reduce the releases of fission products from the RPV into the containment/ confinement, a failure of the RPV needs to be avoided. Examples of potential countermeasures against RPV failures which have been proposed to be included in new reactor designs are vessel-internal core catchers, outside cooling of the RPV by flooding of the RPV cavity, and RPV venting systems.

The frequency of an accidental release of radioactivity into the containment/ confinement has to be determined via probabilistic methods. A probabilistic safety assessment (PSA) checks the balance of the safety concept (no single accident dominates the core damage frequency) and the overall level of safety (risk) via a qualitative and quantitative assessment of active (and passive) safety systems. Additionally, a PSA achieves the key objective of reviewing the complete plant design, which is otherwise generally performed by separate analyses according to deterministic principles.

It is to be noted that not only during full power operation but also during shutdown, an accident with a highly degraded core may occur due to failures of safety systems. Therefore, for both a new reactor and a reference design, normal operation as well as shutdown states have to be analyzed.

The **acceptance limit AL4.1** (reduced frequency of accidental release into containment/ confinement) is met if evidence available to the INPRO assessor shows that calculated frequencies of a highly degraded core (CDF) are significantly lower than in the reference plant and below the best estimate value recommended by the International Nuclear Safety Advisory Group (INSAG) of 10^{-5} per year and unit [13], taking uncertainties into account.

4.6.2. Criterion CR4.2: Robustness of containment/ confinement design

Indicator IN4.2: Containment loads covered by the design, and natural or engineered processes and equipment sufficient for controlling relevant system parameters and activity levels in containment / confinement.

Acceptance limit AL4.2: Larger than those in the reference design.

Typical lists of internal and external events that should be considered in the design of containment/ confinement systems are provided in Ref [56].

If a plant reaches a state with a highly degraded core and/or degraded fuel in the spent fuel pool, active and/or passive engineered or natural processes are normally available to mitigate

consequences including those to avoid loss of containment/ confinement integrity. An example of such an engineered process is a spray system to reduce the load (temperature and pressure) on the containment/ confinement – the last barrier – and to reduce and/or control the activity in the containment/ confinement atmosphere, thereby also reducing the potential for a complete failure of the containment/ confinement leading to an accidental release outside containment/ confinement. In Table 8 some relevant system parameters and mitigating measures (processes) in some water-cooled reactors are presented as examples.

TABLE 8. EXAMPLES OF MITIGATING PROCESSES USED IN WATER-COOLED REACTORS

Relevant System Parameter	Engineered Mitigating Processes	Explanations
Water level inside RPV	System for water injection from sources inside and outside containment.	The core melt might be stopped (as occurred in the Three Mile Island Unit 2 accident).
Water level in the containment	System for water injection into RPV cavity from sources inside and outside containment.	The RPV could be cooled from the outside; the melt progression might be at least delayed; the melt could be retained within the RPV.
Activity level in containment	Designed path of fission products through water pools inside containment to enable scrubbing. Containment spray system for scrubbing of fission products. Containment internal filters between compartments.	Scrubbing means retention of fission products in water; it is a very effective method to reduce the activity level in the containment atmosphere. Containment internal filters will reduce the activity level
Containment pressure	Outside or inside cooling of containment. Venting to the environment via filter. Hydrogen re-combiners or igniters (in case the containment is not inerted)	Outside or inside cooling of containment will limit the pressure. Venting reduces the load on the containment. Hydrogen re-combiners or igniters avoid hydrogen explosion.

Processes to mitigate consequences including those to avoid loss of containment/ confinement integrity can be very reactor design-specific, e.g. for molten salt reactors and HTGRs they are quite different from those for water-cooled reactors. During the design phase of new reactors special attention needs to be given to considering related preventive and mitigative measures in a balanced way. To avoid a loss of containment/ confinement integrity due to, e.g. overpressure and high temperatures – compared to operating reactors – the containment/ confinement of new reactors is expected to be designed against higher loads caused by an accident with an accidental release of radioactive material into the containment/ confinement. Closure of containment penetrations such as steam or feed water lines in LWRs can be designed with higher reliability, e.g. by increasing the reliability of valves. In addition to loads on the inside of the containment/ confinement (e.g. overpressure) also loads on the outside caused by external events (e.g. tsunami) are expected to be covered with greater margins in new designs.

The **acceptance limit AL4.2** (containment loads larger than those in the reference design) is met if evidence available to the INPRO assessor shows that assessed design employs superior mechanisms and systems (processes) to control and mitigate accidents with a highly degraded core to avoid loss of integrity of the containment/ confinement, and / or the containment/ confinement has been designed demonstrating greater margins between calculated peak accident loads and design loads than in the reference design.

4.6.3. Criterion CR4.3: Accident management

Indicator IN4.3: In-plant AM.

Acceptance limit AL4.3: AM procedures and training sufficient to prevent an accidental release outside containment / confinement and regain control of the reactor.

In accidents more severe than DBAs, the in-plant AM measures provide tools to the operator for preventing a further release into the containment/confinement, and/or for reducing the air concentration of radio-nuclides already there, in order to prevent an accidental release of radioactivity to the outside of the plant (into the environment) [57] that would need emergency response measures.

The in-plant AM measures and actions in case of a highly degraded core are very plant-specific [58]. Off-site provisions needed for AM measures are only necessary after a sufficient period to enable their successful implementation, e.g. by bringing mobile equipment to the plant site, i.e. the plant needs to be self-sufficient for an extended period relying for instance on passive safety features. The consideration of potential cliff-edge effects in the scenarios of accidents is expected to be taken into account in the development of AM procedures. Experiences from operating reactors with installed AM measures have shown that the feasibility and effectiveness of these measures have to be demonstrated and operators have to be trained sufficiently.

Complementary information on the accident management measures is provided in Appendix VII.

The **acceptance limit AL4.3** (sufficient AM measures to prevent accidental release to the outside) is met in the reactor assessed if evidence available to the INPRO assessor shows that procedures and trainings are available, sufficient to maintain the integrity of the containment/ confinement, i.e. prevent major releases of radioactivity to the environment and regain control of the reactor after an accident.

4.6.4. Criterion CR4.4: Frequency of accidental release into environment

Indicator IN4.4: Calculated frequency of an accidental release of radioactive materials into the environment.

Acceptance limit AL4.4: Lower than that in the reference design. Large releases and early releases are practically eliminated.

An accidental release of radioactivity to the environment can occur if the containment/ confinement loses its integrity after an accident with severe core damage. Examples for causes of containment failures are overpressure due to hydrogen or steam explosion and penetration of the base plate by a molten core-concrete interaction (mainly in water-cooled reactors[33]) [59]. Scenarios of a containment/ confinement failure need to be prevented or mitigated by design measures as discussed above, e.g. by increasing the design pressure of the containment. Other examples for design measures to prevent containment failure due to melt-through of the basement floor of advanced water reactors are the core catchers in the EPR or advanced WWER designs, the reactor pressure vessel internal (corium) retention device for the KERENA (SWR1000), and the water-filled calandria vessel and vault in the Enhanced CANDU-6 (EC6) reactor. Examples for design measures to prevent containment failures due to over

[33] Reactor containments of currently operating reactors were not originally designed to cope with loads resulting from core melts.

pressurization are the inclusion of containment cooling systems, and hydrogen catalytic re-combiners or igniters.

Different reactor designs may place different emphasis on specific preventive or mitigative measures. The most widespread currently operating reactor designs, water cooled reactors, include robust containment buildings as part of their system of barriers necessary to keep the calculated frequency of an accidental release sufficiently low. Other designs, e.g. HTGRs, may place major emphasis on retention of the radioactivity inside the fuel matrix (TRISO particles).

INPRO sustainability criteria call for the calculated frequency of accidental release to be lower than in the reference design. It is assumed that the calculated frequency of accidental release from the reference NPP design is lower than 10^{-6} per unit-year. Via a probabilistic safety analysis, the frequency of an accidental release of radioactivity into the environment including uncertainties is expected to be determined covering all plant states (normal operation, shut down) and internal as well as external events and probable combinations thereof leading to accidents; the probabilistic analyses has to use best estimate methods and consider associated uncertainties (see criterion CR7.5).

Modern reactor designs have significantly reduced the potential for a containment failure that would lead to accidental releases of radioactivity. Table 9 gives examples of very low calculated frequencies of containment failures claimed by the designers.

TABLE 9. CALCULATED FREQUENCIES OF CONTAINMENT FAILURES IN MODERN REACTORS

Plant	Frequency/a of sum of containment failure modes
EPR [54]	
- early containment failure	$4\ 10^{-8}$
- late containment failure	$6\ 10^{-8}$
AP1000 [53]	
- large release (internal events at power)	$2\ 10^{-8}$
- large release (internal events at low power and shutdown)	$2\ 10^{-8}$

However, it is worth noting that the calculated frequency of accidental release to the environment depends on the assumed reliability of the reactor components and the assumed reliability of human performance. The former may theoretically vary depending on preventive maintenance management and the latter may theoretically depend on social conditions [60]. Therefore, detailed calculations involve human factor related data based on data appropriate for a given organisation and / or country.

In 2015 the Contracting Parties of the Convention on Nuclear Safety adopted the Vienna Declaration on Nuclear Safety. The first principle of this declaration states:

> "New nuclear power plants are to be designed, sited, and constructed, consistent with the objective of preventing accidents in the commissioning and operation and, should an accident occur, mitigating possible releases of radionuclides causing long-term off site contamination and avoiding early radioactive releases or radioactive releases large enough to require long-term protective measures and actions."

In 2016 this principle was incorporated in the revised IAEA Safety Standards [15] in requirements associated with Level 4 of DID:

> "The safety objective in the case of a severe accident is that only protective actions that are limited in terms of lengths of time and areas of application would be necessary and that off-site contamination would be avoided or minimized. Event sequences that would lead to an early radioactive release or a large radioactive release[3] are required to be 'practically eliminated'[4].

Footnote 3: An 'early radioactive release' in this context is a radioactive release for which off-site protective actions would be necessary but would be unlikely to be fully effective in due time. A 'large radioactive release' is a radioactive release for which off-site protective actions that are limited in terms of lengths of time and areas of application would be insufficient for the protection of people and of the environment.

Footnote 4: The possibility of certain conditions arising may be considered to have been 'practically eliminated' if it would be physically impossible for the conditions to arise or if these conditions could be considered with a high level of confidence to be extremely unlikely to arise."

It is recognised that the existing reference plant selected for the INPRO assessment of a new reactor design might not comply with this new requirement. However, the new reactor designs are expected to demonstrate practical elimination of large releases and early releases[34] (see summary report of the Diplomatic Conference held in the IAEA [61]).

The **acceptance limit AL4.4** (frequency of accidental release into environment) is met if evidence available to the INPRO assessor shows with a high level of confidence that the calculated (best estimate) frequency for an accidental release of radioactivity to the environment due to a failure of the containment/ confinement is lower than in the reference design and well below 10^{-6} per unit-year [13]. For potential sites located close to densely populated areas, e.g. with urban district heating facilities, a lower value than 10^{-6} per unit-year might be required by regulatory authorities. In the assessed reactors large releases and early releases have to be practically eliminated (Ref [19] provides detailed interpretation of this concept).

4.6.5. Criterion CR4.5: Source term of accidental release into environment

Indicator IN4.5: Calculated inventory and characteristics (release height, pressure, temperature, liquids/gas/aerosols, etc) of an accidental release.

Acceptance limit AL4.5: Remain well within the inventory and characteristics envelope of the reference reactor source term and are so low that calculated consequences would not require public evacuation.

Radiological criteria for evacuation of population are normally formulated in terms of projected dose [62]. The calculated consequences (public dose) of radioactive releases to the outside of the NPP after severe accidents need to be kept sufficiently low (lower than the levels defined for evacuation) to avoid the necessity for commencing the evacuation of people living in the vicinity of the plant [63].

Estimation of the consequence of the accidental external release involves the accident modelling within the containment/ confinement to determine the source term for the release and occasionally the modelling of transport of the radionuclides outside of the NPP. The magnitude of given radioactivity inventories and the physical and chemical form of given inventories define the source term for determining atmospheric dispersion of radioactive material as well as radiation exposure.

Since the results of modelling of radionuclide transport in the environment may heavily depend on a series of assumptions such as weather conditions (wind directions in different altitudes, humidity etc) the first part of the acceptance limit in this INPRO criterion requires that source term characteristics in the new reactor including the inventory of released radionuclides remain well within the envelope of the reference reactor source term. In this context 'well within the

[34] The INPRO methodology user requirements and criteria are developed for the assessment of sustainability of nuclear energy systems and may incorporate new developments from different areas, not to be confused with the Vienna Declaration on Nuclear Safety.

envelope' means that all source term characteristics for the new design will be equal to or lower than those for the reference design and at least some of them will be lower by more than the level of uncertainties associated with accident consequence modelling within the reactor containment/ confinement.

For new NPPs the capability and reliability of natural and/or engineered processes for controlling complex accident sequences with severe damage is expected to be increased through improved instrumentation, control and diagnostic systems and the development of appropriate severe accident management procedures. By these measures, the frequency of accidental release of radioactivity can be reduced and the inventory and conditions of release can be kept lower than in the reference design.

It is noted that to meet the objective of Level 5 of DID, emergency protection and response measures have to be planned around the NPP [1] commensurate with the hazard of the accidental release of radioactive and chemically toxic material to the environment. This issue is covered in another report of the updated INPRO methodology called infrastructure.

Complementary information on the estimation of consequence of the accidental external release is provided in Appendix VIII.

The **acceptance limit AL4.5** of **CR4.5** is met if evidence available to the INPRO assessor shows that the calculated inventory and characteristics of the accidental release source term remain well within those of the reference reactor and are low enough so that calculated consequences would not require evacuation of the population.

4.7. EMERGENCY PREPAREDNESS AND RESPONSE

The accidents at Three Mile Island Unit 2 (with an intact containment and no significant accidental release of radioactive materials to the environment), Chernobyl and Fukushima [24] (with large accidental releases of radioactive materials to the environment) have sensitized the public regarding the releases of radioactive elements to the environment. Moreover, if nuclear energy is to play a major role in the future, many more plants will have to be installed, and these are expected to be of designs that can be easily sited. Some countries have the good fortune to have numerous large remote sites available for nuclear power plants to be located, but many countries do not; hence design of a new nuclear plant does not need to rely too heavily on distance from the population. Therefore, it is generally agreed that new nuclear reactors are expected to be designed in such a way that for any postulated accident even with a highly degraded core, a significant release of radioactive material to the environment will be impossible or extremely unlikely.

As discussed in the previous Section 4.6, the INPRO methodology in effect asks the designer to prevent or mitigate the scenarios of accidental release to assure that projected doses to the public will be lower than the dose criteria for emergency evacuation.

To achieve this goal, engineered safety features of new reactors (as discussed for UR4) need to be able to control scenarios of accidents more severe than DBAs and mitigate their consequences, e.g. to prevent complete containment/ confinement failure that results in accidental radioactive releases. Control and mitigation measures need to address all threats (caused by internal and external events and probable combinations thereof). New reactor designs are expected to show that an accidental release of radioactivity into the environment requiring evacuation of population has been practically eliminated, e.g. through use of inherent safety characteristics. It is however acknowledged that also for new (and advanced) reactors emergency preparedness arrangements will have to be established to meet the objective of the fifth level of DID.

Level 5 of DID assumes that an accidental release of radioactivity into the environment will occur during an accident with severe core damage due to a failure of the containment/ confinement. The objective of this fifth DID level is to ensure that necessary emergency response measures such as sheltering, distribution of iodine, evacuation, relocation, etc. can be taken to protect the people and the environment after such an accidental release. The INPRO methodology NES sustainability requirement on emergency preparedness is discussed in another manual [1] focused on Infrastructure (see EP1.2.4 in Ref [1]).

4.8. UR5: INDEPENDENCE OF DID LEVELS, INHERENT SAFETY CHARACTERISTICS AND PASSIVE SAFETY SYSTEMS

INPRO user requirement UR5 for sustainability assessment in the area of reactor safety: An assessment is performed to demonstrate that the DID levels are more independent from each other than in the reference design. To excel in safety and reliability, the nuclear reactor assessed strives for better elimination or minimization of hazards relative to the reference design by incorporating into its design an increased emphasis on inherently safe characteristics and/or passive systems, when appropriate.

As discussed in Section 2.2 the different levels of DID range from operating to accident plant states. They are arranged with increasing severity from operational states (Level 1) to the mitigation of radiological consequences of significant releases of radioactive material to the environment (Level 5). As stated in Ref [13] the general goal of DID is to ensure that even a combination of equipment or human failures at one level of defence will not progress to subsequent DID levels and jeopardize DID at those levels. Thus, the independence of safety systems designed to cope with different levels of defence is key in meeting this goal.

Ref [19] explains that "the full independence of the levels of defence in depth cannot be reached, due to several constraints, such as the common exposure to external hazards, the unavoidable sharing of some SSCs, e.g. the containment or the control room and ultimately the operating crew". INPRO methodology in the area of reactor safety is focused on the improvement or expansion of the independence of DID levels in new reactors rather than on achievement of full independence. To confirm sufficient independence of the DID levels of the reactor assessed a safety assessment had to be performed using a suitable combination of deterministic and probabilistic approaches, or hazards analysis.

Design assessments regarding the DID concept could be quite different for different reactor designs. It is evident that inherent safety characteristics increase the independence of the different DID levels since "inherent safety feature represents conclusive, or deterministic safety, not probabilistic safety" [64] unlike engineered systems, structures and components that "remain in principle subject to failure (however low the probability of such failure)" [64].

The second part of INPRO user requirement UR5 for sustainability assessment in the area of reactor safety is focused on the role of inherent safety and passive safety features in new nuclear designs. Some background on these safety features is provided as follows.

Inherent safety characteristics

An increased use of inherent safety characteristics in the design will strengthen accident prevention in advanced nuclear plants by reducing hazards. A plant design possesses an inherently safe characteristic against a potential hazard if the hazard is rendered technically impossible. An inherent safety characteristic in a reactor design can be achieved through the choice of nuclear physics, and the physical and chemical properties of nuclear fuel, coolant and other components. The term inherent safety is normally used with respect to a particular characteristic, not to the plant as a whole. For example, an area is inherently safe against internal

fire if it contains no combustible material; a reactor is partially inherently safe against reactivity insertion if the physically available amount of excess reactivity is small and overall reactivity feedback is negative so that no large power excursions can occur; a reactor is inherently safe against loss of the heat sink if decay heat can be removed by conduction, thermal radiation and natural convection to the environment without fuel damage, etc.

Examples of reactor concepts with increased robustness against certain potential hazards are designs with all cooling loops inside the pressure vessel (avoidance of loss of coolant in case of loop breaks), use of liquid metals or molten salts (avoidance of high system pressures), use of small excess reactivity (avoidance of large power excursions), low power density cores (limiting fuel temperature in reactivity transients), use of passive safety systems (potentially higher reliability, e.g. natural convection), and use of non-flammable materials (avoidance of fires), etc.

The design of a new reactor is expected to be such that hazards are eliminated (if possible) or minimized, e.g. by limiting the use of explosive gases to the absolute necessary amount, or by using inherent safety features in the core design and operation to limit excess reactivity. If hazards cannot be eliminated, appropriate protective measures have to be installed. In addition, administrative measures need to exist to avoid human errors to the extent possible (e.g. by limiting the transport of hazardous material inside the containment/confinement during shutdown periods).

The analysis of hazards and their consequences are performed using deterministic and probabilistic approaches. For the deterministic approach, engineering judgment, operating experience, validation of design tools and a continuous exchange of information also with other industries is mandatory. For probabilistic approaches, the methods need also to be validated, and the data used have to be reliable. Analyses need to cover all operating states including full power, shutdowns, and maintenance and repair intervals.

There are also external hazards associated with the site of an NPP. Examples of such hazards related to the siting are earthquakes, flooding, storms, and explosions outside the plant. By selecting an appropriate site for an NPP these hazards can be minimized.

The analysis of an inherent safety characteristic is difficult but is possible by the application of adequate mathematical models and, in some cases, by experimental investigations. The necessary RD&D effort to achieve sufficient confidence in advanced designs with increased inherent safety characteristics is discussed in UR7.

Passive safety systems

Passive safety systems can provide additional safety margins; in such cases, deterministic (conservative) design requirements such as the single active failure criterion may not be necessary (since safety will not depend as much on active components), assuming that reliability models are developed for passive systems. Nevertheless, failures in passive systems due to human error in design or maintenance, the presence of unexpected phenomena, and potential adverse system interactions, need to be analysed and may need to be compensated by other design measures.

Safety systems with passive components are very often deemed more reliable due to missing (or a reduced number of) active components; in addition, no (or very limited) human actions are needed and thus, the likelihood of human errors is very low.

A comprehensive description of passive safety systems for water cooled reactors including the associated physical phenomena is provided in the IAEA report [65].

The following passive safety systems are discussed [65]:

- For core heat removal: accumulators, core make-up tanks, elevated gravity drain tanks, passively cooled steam generator natural convection, passive residual heat removal heat exchangers, passively cooled isolation condensers and sump natural circulation device;
- For containment cooling and pressure suppression: containment pressure suppression pools, containment passive heat removal/pressure suppression systems, and passive containment spray systems.

In addition, in Ref [65] the specific designs of twenty advanced reactors are presented with emphasis on passive safety systems. The IAEA has defined four categories of passive systems, as indicated in Table 10 below.

TABLE 10. CATEGORIES OF PASSIVE SYSTEMS IN REACTORS [65].

Needed function	Category			
	A	B	C	D
I&C Signal.	-	-	-	X
External power source or forces.	-	-	-	Batteries or compressed fluids or gravity driven injections.
Moving mechanical parts.	-	-	X	(X)
Moving working fluids.	-	X	(X)	(X)
Examples	*Fuel cladding, pressure boundary.*	*Cooling system based on natural circulation.*	*Accumulators, filtered venting activated by rupture discs.*	*Emergency core cooling, based on gravity driven fluids and activated by battery-powered valves.*

Note: X = function included

For example, category A is characterized by:

- No signal input of intelligence (I&C signal);
- No external power source or forces;
- No moving mechanical parts; and
- No moving working fluid.

Typical examples of category A are physical barriers against fission product release, such as the fuel cladding and the pressure boundary system. The reliability data of a passive safety system or a passive component have to be taken from operating experience and analyses[35]; it is evident that moving parts (e.g. valves) might decrease reliability of such systems.

The INPRO methodology criteria for UR5 are presented in Table 11.

[35] Currently operating experience of passive systems is limited and analyses methods are still under development.

TABLE 11. CRITERIA FOR USER REQUIREMENT UR5 FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

INPRO user requirement	Criteria	Indicators (IN) and Acceptance Limits (AL)
UR5: Independence of DID levels, inherent safety characteristics and passive safety systems: An assessment is performed to demonstrate that the DID levels are more independent from each other than in the reference design. To excel in safety and reliability, the nuclear reactor assessed strives for better elimination or minimization of hazards relative to the reference design by incorporating into its design an increased emphasis on inherently safe characteristics and/or passive systems, when appropriate.	CR5.1: Independence of DID levels	IN5.1: Independence of different levels of DID. AL5.1: More independence of the DID levels than in the reference design, e.g. as demonstrated through deterministic and probabilistic means, hazards analysis, etc.
	CR5.2: Minimization of hazards	IN5.2: Characteristics of hazards. AL5.2: Hazards smaller than those in the reference design.
	CR5.3: Passive safety systems	IN5.3: Reliability of passive safety systems. AL5.3: More reliable than the active safety systems in the reference design.

4.8.1. Criterion CR5.1: Independence of DID levels

Indicator IN5.1: Independence of different levels of DID.

Acceptance limit AL5.1: More independence of the DID levels than in the reference design, e.g. as demonstrated through deterministic and probabilistic means, hazards analysis, etc.

A deterministic method for assessing the DID capabilities of a nuclear reactor design is described in Ref [66]. The method is based on objective trees for each level of DID that define the following elements from top to bottom: the objective of the DID level, the relevant safety functions to be met, identified general challenges to the safety functions based on specific root mechanisms for each of these challenges and a list of provisions in design and operation for preventing the mechanism from occurring.

New reactor designs are expected to strive to the extent practicable to achieve greater independence of DID levels than in the reference design. Special attention should be demonstrated in the design to such hazards as fire, flooding or earthquakes that could potentially impair several levels of DID (for example, they could bring about accident situations and, at the same time, inhibit the means of coping with such situations) [13]. Moreover, for some events (such as sudden reactor pressure vessel failure), where it is not feasible to have independent levels of DID, several levels of precautions need to be demonstrated in the design (e.g. selection of materials, periodic inspection, additional margins of safety, etc.) to make this event practically eliminated.

For design extension conditions the analyses undertaken for the design needs to include identification of the safety features designed for use in such conditions or needs to demonstrate that safety features are capable of mitigating consequences of core damage and of preventing release of radioactivity. These safety features need to be independent, to the extent practicable, from those used in more frequent accidents.

A probabilistic safety assessment (PSA) [51], if done carefully, will highlight systems and elements that are not sufficiently independent, and identify cross-links that compromise the independence of the levels of DID. The nuclear reactor assessed is expected to demonstrate

calculated frequency ranges of reaching the different levels of DID after an initiating event below (superior to) those of the reference reactor.

The **acceptance limit AL5.1** (*independence of DID levels*) is met for the reactor assessed if evidence available to the INPRO assessor demonstrates that the different levels of DID (at least in several selected aspects) are more independent than in the reference plant based on a deterministic assessment and probabilistic analyses.

4.8.2. Criterion CR5.2: Minimization of hazards

Indicator IN5.2: Characteristics of hazards.

Acceptance limit AL5.2: Hazards smaller than those in the reference design.

In this publication hazards are generally interpreted as potential sources of danger. Examples of hazards include overheating, fire, explosions, criticality, release of radioactive material, radiation exposure, etc. This criterion CR5.2 encompasses five evaluation parameters focussed on specific groups of hazards and formulated as follows:

- EP5.2.1: Stored energy;
- EP5.2.2: Flammability;
- EP5.2.3: Excess reactivity in the core;
- EP5.2.4: Reactivity feedbacks;
- EP5.2.5: Criticality outside the reactor core.

In addition to hazards jeopardizing the nuclear fuel in the reactor core the assessment of criterion CR5.2 has to cover also potential hazards endangering the on-site storage and handling of fresh fuel and spent fuel in the corresponding near reactor spent fuel pool.

As stated before the EPs are meant to be examples for a designer on how to minimize hazards in a new design. It is expected that designers will come up with additional examples of reducing hazards.

4.8.2.1. Evaluation parameter EP5.2.1: Stored energy

The stored energy in a power generating system after an operating disturbance or accident can create a hazard: Component damage due to overheating can occur iff the removal of stored energy in the system fails. Thus, a reduction of stored energy in a reactor leads to a reduction of the corresponding hazard of overheating.

A well-known example within a nuclear power plant is the stored energy in the fuel and in the primary coolant mass. While advanced (innovative) approaches may reduce the amount of stored energy in the fuel (e.g. by increased conductivity of the fuel or reduced specific power) the stored energy (enthalpy) in the primary coolant (determined by pressure and temperature level and mass of coolant) of power reactors could only be changed (reduced) within a narrow range for a chosen coolant (e.g. light or heavy water), because of optimization of thermal efficiency, core layout and geometries. It is also obvious that a potential reduction of primary coolant mass in a reactor would decrease the inertia of the system regarding transients, which is a negative effect[36] (see criterion CR2.3).

Acceptability of EP5.2.1: For the reactor design assessed, the amount of stored energy within the fuel and enthalpy in the primary coolant system has been limited to the minimum amount

[36] When minimisation of energy stored in the coolant may involve the reduction of reactor inertia (e.g. through reduction of coolant mass) a quantitative analysis should be performed to estimate and summarise the safety relevant effects.

possible to reduce the hazard of overheating of the core. When practicable the stored energy[37] is to be less than in the reference design.

4.8.2.2. Evaluation parameter EP5.2.2: Flammability

The possibility of a fire in a nuclear reactor represents a considerable hazard (e.g. the fire in Browns Ferry [67]). Consequently, the design of advanced NPPs is expected to minimize this hazard by reducing the amount of flammable material.

The fire protection concept has to include an alarm and suppression system; smoke and heat removal has to be taken into account. The concept of separation of systems with redundant safety functions by distance and barriers normally ensures that a fire remains localized and does not lead to accidents.

For metal (e.g. sodium) cooled reactors, some measures could be developed such as additives to the coolant that suppress the exothermic reactions in case of a leakage (e.g. water-sodium reaction in a steam generator).

The use of explosive gases (e.g. hydrogen in the chemical and volume control system) needs to be limited to the minimum necessary amount. For systems containing explosive gases, protection measures need to be taken to ensure that no explosive mixture of gases in the atmosphere can occur (e.g. by inerting the atmosphere, using re-combiners, etc.).

Acceptability of EP5.2.2: For the reactor assessed, minimization of flammable material has been considered in the design to reduce the hazard of fire. When practicable the amount of flammable material in the systems, structures and components relevant to safety and in the systems related to them is less than in the reference design.

4.8.2.3. Evaluation parameter EP5.2.3: Excess reactivity in the core

To avoid unintended reactivity transients the excess reactivity in the core is expected to be kept to the minimum possible. However, some excess reactivity (or power control) is necessary to cope with fuel burn-up, to reach full power operating conditions and to compensate for xenon and samarium build-up after temporary shutdown.

Acceptability of EP5.2.3: For the reactor assessed, excess reactivity in the core is kept as low as practicable to reduce the hazard of reactivity transients. When practicable the excess reactivity in the core is less than in the reference design.

4.8.2.4. Evaluation parameter EP5.2.4: Reactivity feedbacks

During normal operation the reactivity feedbacks of changing conditions in the core are expected to lead to self-compensation – e.g. negative feedback (reduction of reactivity) on a temperature increase. This can be achieved by a core design with sufficiently negative resonance adsorption effects (Doppler), a negative moderator temperature and void coefficient, and the control of the power distribution (see also criterion CR1.1). However, the core design needs to take into account that a too negative moderator temperature feedback may worsen the situation in accidents with deep cooling of the primary coolant, e.g. in LWRs.

Acceptability of EP5.2.4: During normal operation and AOO of the reactor assessed, changing conditions in the core lead to compensatory reactivity feedbacks that reduce the hazard of power transients.

[37] Per unit of energy produced, per unit of fuel mass or per unit of coolant mass.

4.8.2.5. Evaluation parameter EP5.2.5: Criticality outside the core

To reduce the hazard of criticality outside the core (e.g. in fuel storage), any geometry and material configuration that could create criticality needs to be avoided (e.g. by using fixed poisoned material, administrative measures for (neutron) poisoning of coolants, inherently safe geometries, etc.).

Acceptability of EP5.2.5: For the reactor assessed, the possibility (hazard) for criticality outside the core is less than in the reference design.

4.8.2.6. Final assessment of criterion CR5.2: Minimization of hazards

The **acceptance limit AL5.2** (*reduced hazards)* is met if evidence available to the INPRO assessor shows that the reactor design assessed demonstrates a reduction (or elimination) of hazards compared to those in the reference design.

4.8.3. Criterion CR5.3: Passive safety systems

Indicator IN5.3: Reliability of passive safety systems.

Acceptance limit AL5.3: More reliable than the active safety systems in the reference plant.

This criterion needs to be assessed only when the new reactor design incorporates passive safety systems or components to perform safety functions where the reference design uses active systems/ components.

The advantages and disadvantages of passive safety systems are discussed in Ref [68]. The essential advantages of passive systems are their independence from external support systems such as electric power, their generally greater simplicity and their potential for increased reliability. Disadvantages may include lower driving heads in fluid systems (compared to pumps) and potentially reduced flexibility in the definition of operator / control system actions at abnormal operating conditions of the plant.

Thus, safety systems that use passive components are expected to be more reliable than those using purely active components. However, the use of passive components in safety systems does not eliminate potential hidden failures potentially caused by inappropriate maintenance. Moreover, special considerations are necessary for certain reactor states in which passive safety systems may require specific working conditions to start and operate correctly, e.g. sufficient temperature differences for natural convection.

As described in the introduction to this section, the IAEA report Ref [65] discusses all technical aspects of passive safety systems in water cooled reactors.

The **acceptance limit AL5.3** (increased reliability of passive safety systems) is met if evidence available to the INPRO assessor shows that the use of passive components makes the affected safety systems more reliable than the reference plant's corresponding systems with active components.

4.9. UR6: HUMAN FACTORS RELATED TO SAFETY

INPRO user requirement UR6 for sustainability assessment in the area of reactor safety: Safe operation of the nuclear reactor assessed is supported by accounting for HF requirements in the design and operation of the plant, and by establishing and maintaining a strong safety culture in all organizations involved.

There are two aspects of safety covered in this INPRO user requirement for NES sustainability assessment. The first one is focused on the design of equipment related to safety, especially the

control room, to minimize human errors, and the second one covers the attitude to safety of people in nuclear facilities and related organizations.

The INPRO methodology criteria for UR6 are presented in Table 12.

TABLE 12. CRITERIA FOR USER REQUIREMENT UR6 FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

INPRO user requirement	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR6: Human factors related to safety: Safe operation of the nuclear reactor assessed is supported by accounting for HF requirements in the design and operation of the plant, and by establishing and maintaining a strong safety culture in all organizations involved.	CR6.1: Human factors	IN6.1: HF considerations are addressed systematically throughout the life cycle of the reactor. AL6.1: HF assessment results are better than those for the reference design.
	CR6.2: Attitude to safety	IN6.2: Prevailing safety culture. AL6.2: Evidence is provided by periodic safety culture reviews.

4.9.1. Criterion CR6.1: Human factors

Indicator IN6.1: HF considerations are addressed systematically throughout the life cycle of the reactor.

Acceptance limit AL6.1: HF assessment results are better than those for the reference design.

The importance of the human factor for safe and reliable operation of NPPs is globally recognized and is an issue that needs to be dealt with systematically in a reactor design [59]. Thus, the designer of a new reactor is expected to place increased emphasis on human factors to minimize the possibilities for human (e.g. operator or maintainer) error. The experience available from operating nuclear plants and the best practices from other industries such as aircraft and chemical plants needs to be taken into account for this process.

A human factor engineering programme plan is an essential part of reactor design. Listed below are examples of some design and operational features and assessments. Some of these have already been implemented in existing reactors but can be subject to further improvements in new reactors:

(1) Feedback of experience including a formal methodology;
(2) A PSA taking human error into account;
(3) Use of adequate (and quantitative) models considering the causes of human error, which may assist to find appropriate design measures to avoid the causes and thus minimize human errors;
(4) Existence of a main control room, a remote shutdown station and a technical support centre;
(5) Using visualizations of plant equipment status (components, systems, etc.), the dynamics of processes, the performance of automated processes and their relation with the state of the plant to help guide operator actions;
(6) Monitoring by knowledge-based (expert) systems;
(7) Appropriate ambient conditions in the relevant rooms (e.g. main control room);
(8) Appropriate plant operating procedures (e.g. alarm sheets, procedures for normal operation, incident and accident situations);
(9) Appropriate organisational and administrative structure;
(10) Existence of a verification of design implementation adequacy;
(11) Control of human reliability (e.g. personnel selection, periodic training, etc.);
(12) Application of formal human response models.

Complementary information on human factor consideration is provided in Appendix IX.

The **acceptance limit AL6.1** (systematically addressed human factors) is met for the reactor assessed if evidence available to the INPRO assessor shows that human factors are considered during the lifetime of the reactor including the planning, construction, operating and decommissioning phases, i.e. evidence of improvement of the design and operational features listed above (bullets 1 to 11) is available to the assessor.

4.9.2. Criterion CR6.2: Attitude to safety

Indicator IN6.2: Prevailing safety culture.

Acceptance limit AL6.2: Evidence is provided by periodic safety culture reviews.

The periodic reviews concerning safety culture have to cover not only the operating organization but also regulatory and other responsible government authorities as well as industrial entities. The assessment of this criterion CR6.2 is based on the outcome of safety culture reviews of at least the following organisations: operating organisation, regulatory body, NPP developer and supplier, and fuel suppliers.

The assessment of CR6.2 regarding safety culture of an operating organisation can only be performed once the organization is actually operating a facility. But the need to inculcate a safety culture within an organization and the need for a safety management system need to be recognized in the planning phase for nuclear power. Furthermore, the proposed policies and management structure of the owner/operator can be assessed before operation to determine if they are consistent with a safety culture.

Complementary information on safety culture consideration is provided in Appendix X.

The **acceptance limit AL6.2** (evidence that a safety culture prevails) of CR6.2 is met for the nuclear energy system assessed if evidence available to the INPRO assessor shows that safety culture reviews are being (or planned to be) performed at appropriate intervals.

The INPRO methodology recommends using the support of experienced organizations for such reviews. IAEA offers a service to its Member States called ISCA (Independent Safety Culture Assessment) that can assist with evaluating the status of safety culture. Another method of safety culture assessment is provided in Ref [69].

4.10. UR7: NECESSARY RD&D FOR ADVANCED DESIGNS

INPRO user requirement UR7 for sustainability assessment in the area of reactor safety: The development of innovative design features of the nuclear reactor assessed includes associated research, development and demonstration (RD&D) to bring the knowledge of plant characteristics and the capability of analytical methods used for design and safety assessment to at least the same confidence level as for operating plants.

INPRO user requirement UR7 for sustainability assessment in the area of reactor safety discusses the necessary research, development and demonstration (RD&D) effort for development of nuclear reactors with primarily innovative[38] but also evolutionary[39] design features.

[38] An innovative design is an advanced design that incorporates radical conceptual changes in design approaches or system configuration in comparison with existing practice.

[39] An evolutionary design is an advanced design that achieves improvements over existing designs through small to moderate modifications, with a strong emphasis on maintaining proven design elements to minimize technological risks.

It is well-known that intensive research is needed to bring the level of knowledge of plant behaviour and the capability of computer codes to model phenomena and system behaviour for innovative reactor designs to at least the same confidence level as for operating plants.

A sound knowledge of the phenomena, component, and system behaviour is required to develop computer models for accident analysis of reactors. Hence, the more a plant differs from operating designs, the more RD&D is required. RD&D provides the basis for understanding events that threaten the integrity of barriers defined by the DID concept. RD&D can also provide information to reduce allowances for uncertainties in design, operating envelopes, and in estimates for accident frequencies and consequences.

As the development of an innovative design proceeds, RD&D is carried out to identify phenomena important to plant safety and operation and to develop and demonstrate an understanding of such phenomena. At any given point in the development process the current understanding is incorporated into (computer or analytical) models that form the basis for design and for safety assessments. Such models are then used as a tool for sensitivity analyses to identify important parameters and to estimate safety margins. The results of such analyses are also used to identify coupled effects and interactions among systems that are important to safety. It is not unusual to obtain unexpected results, particularly in the early stages of development. The results, whether expected or not, are used to guide the RD&D programme to e.g. improve conceptual understanding, obtain more accurate data, confirm the extent of system interactions/independence, and characterize the design. The RD&D, in turn, leads to improvements in understanding and in the analytical tools used in design and in safety analyses.

TABLE 13. CRITERIA FOR USER REQUIREMENT UR7 FOR SUSTAINABILITY ASSESSMENT IN THE AREA OF REACTOR SAFETY

INPRO user requirement	Criteria	Indicator (IN) and Acceptance Limit (AL)
UR7: Necessary RD&D for advanced designs: The development of innovative design features of the nuclear reactor assessed includes associated research, development and demonstration (RD&D) to bring the knowledge of plant characteristics and the capability of analytical methods used for design and safety assessment to at least the same confidence level as for operating plants.	CR7.1: Safety basis and safety issues	IN7.1: Safety basis and a clear process for addressing safety issues. AL7.1: The safety basis for advanced designs is defined and safety issues are addressed.
	CR7.2: RD&D	IN7.2: RD&D status. AL7.2: Necessary RD&D is defined and performed, and the database is developed.
	CR7.3: Computer codes	IN7.3: Status of computer codes. AL7.3 Computer codes or analytical methods are developed and validated.
	CR7.4: Novelty	IN7.4: Pilot or demonstration plant. AL7.4: In case of a high degree of novelty: a pilot or demonstration plant is specified, built and operated, lessons are learned and documented, and results are sufficient to be extrapolated to a full-size plant. In case of a low degree of novelty: a rationale is provided for bypassing a pilot or demonstration plant.
	CR7.5: Safety assessment	IN7.5: Adequate safety assessment involving a suitable combination of deterministic and probabilistic methods, and identification of uncertainties and sensitivities. AL7.5: Uncertainties and sensitivities are identified and appropriately dealt with, and the safety assessment is approved by a responsible regulatory authority.

The process is iterative: At the *pre-conceptual stage* of development, physical understanding, analytical models, supporting data bases, and codes may be simplistic and involve significant uncertainties; but as development proceeds, understanding increases and uncertainties (both in

conceptual understanding and in data) are reduced, and the validation of analytical models and codes improves. At the *time of commercialization*, all safety relevant phenomena and system interactions need to be identified and understood and the associated codes and models need to be adequately qualified and validated for use in the safety analyses, which in turn demonstrates that the plant design is safe. Complementary aspects are outlined in Ref [70].

INPRO methodology criteria for UR7 are presented in Table 13.

4.10.1. Criterion CR7.1: Safety basis and safety issues

Indicator IN7.1: Safety basis and a clear process for addressing safety issues.

Acceptance limit AL7.1: The safety basis for advanced designs is defined and safety issues are addressed.

The term 'safety basis' or 'safety case' is understood to be the documentation of safety requirements and safety analyses of a new reactor design before it is being constructed and operated. It is a structured argument, supported by evidence, intended to justify that a system is acceptably safe. It is acknowledged that the safety basis of evolutionary designs is usually covered by established mechanisms; the safety basis of innovative designs has to be developed based on intensive RD&D.

The safety basis includes a well-defined concept for achieving safety with a logical and auditable process for determining design and safety requirements for the new nuclear reactor. Licensing authorities need to be contacted early during the development phase to achieve a common basis of understanding during the development of an innovative design. To develop innovative reactor designs, there is a need for technology specific (or ideally technology-neutral) safety goals to be developed by regulatory (licensing) authorities. These safety goals will then be used by developers for the establishment of a safety concept. One of the main requirements for an adequate safety concept is a complete implementation of the DID concept into an innovative reactor design.

Iteration among design, RD&D and safety analysis is a necessary part of this process to achieve an optimized design. Once the safety requirements have been defined, it has to be demonstrated and documented in the safety basis that they are met. Of high importance are sensitivity analyses to study the important parameters and to confirm that specified safety limits are covering identified uncertainties.

For the final design it has to be demonstrated that in the safety basis all safety issues are covered, and the results are well documented. Pre-operational tests and tests during operation (especially when they are easily possible) are expected to be performed to confirm the adequacy of an innovative design and to supplement the experimental database used for computer codes validation.

The **acceptance limit AL7.1** (safety basis defined, and safety issues addressed) for the reactor assessed is met if evidence available to the INPRO assessor confirms that a safety basis with a consistent safety concept has been developed that demonstrates the appropriate safety goals are met. Results of the process addressing all safety issues including sensitivity and uncertainty analyses and independent reviews are properly documented.

4.10.2. Criterion CR7.2: RD&D

Indicator IN7.2: RD&D status.

Acceptance limit AL7.2: Necessary RD&D is defined and performed, and the database is developed.

Research, development and demonstration (RD&D) on the reliability of innovative components and systems, including passive systems and inherent safety characteristics, need to be performed to achieve a thorough understanding of all relevant physical and engineering phenomena required to support the safety assessment. At least the following are expected to be met by the RD&D programme of a developer for an innovative design:

- All significant phenomena, affecting safety, associated with design and operation of an innovative nuclear plant are identified, understood, modelled and simulated (this includes the knowledge of uncertainties, and the effect of scaling and environment);
- Safety-related system or component behaviour is modelled with acceptable accuracy, including knowledge of all safety-relevant parameters and phenomena, and validated with a reliable database.

It is common practice to assess nuclear system or component behaviour on the basis of code calculations, operating experience and commonly accepted engineering practice. For innovative designs, there is currently limited operating experience. Innovative designs may use new core materials, employ fluids in new thermal-hydraulic regimes, and use radically different fuel and coolants. Development of computer codes to model such innovative designs can proceed in parallel. These computer codes need to be formally verified and validated defining their regions of applicability, using state-of-the-art techniques established in international standards (e.g. validation matrices, uncertainty quantification, proof of scalability, automated verification tools, code qualification reports, etc.) and need to be well documented (e.g. software requirements specifications, theory manuals, user manuals, flow charts, etc.).

Usually, uncertainties are taken into account in a design by applying safety margins. Computer codes and analytical methods need to be based on models that have been validated against experimental data, but this is possible to a lesser extent for innovative designs at early stages of development than for operating designs. In addition to model validation by separate effect tests, plant behaviour calculations are subject to validation against system response (integral) tests. Where such tests are conducted in small-scale facilities, it is necessary to adopt appropriate scaling philosophies.

The design process may involve several iterative RD&D cycles, design modifications and verifications of compliance with the design objectives including safety objectives. Standard safety assessment is based on deterministic and probabilistic techniques and requires essential efforts and detailed information on system design and operating conditions that may not be fully available for innovative systems at the early design stages. However, if the design process is organised correctly the level of design maturity can be expected to grow along with the knowledge accrued in RD&D and verification studies. A few formal approaches applicable at different design stages have been developed to define necessary RD&D in an efficient and effective manner.

An overview of tasks to be performed at the conceptual design stages for defining necessary RD&D is given in Figure 2. For an innovative design the first task is to identify all technology differences from operating designs. To identify the knowledge state and the importance of phenomena and system behaviour an appropriate tool has to be used, e.g. the Phenomena Identification and Ranking Table (PIRT) process which is a structured expert elicitation process based largely on engineering judgment. In addition, adequacy and applicability of the design and safety computer codes have to be assessed. Both the PIRT and the assessment of the adequacy and applicability of related computer codes lead to the required RD&D efforts and a priority list. An additional peer review by RD&D experts would strengthen the choice of the selected tasks. Besides phenomenological data, reliability data including uncertainty bands for

designated components need to be evaluated to the extent possible. This is especially valid for passive safety systems.

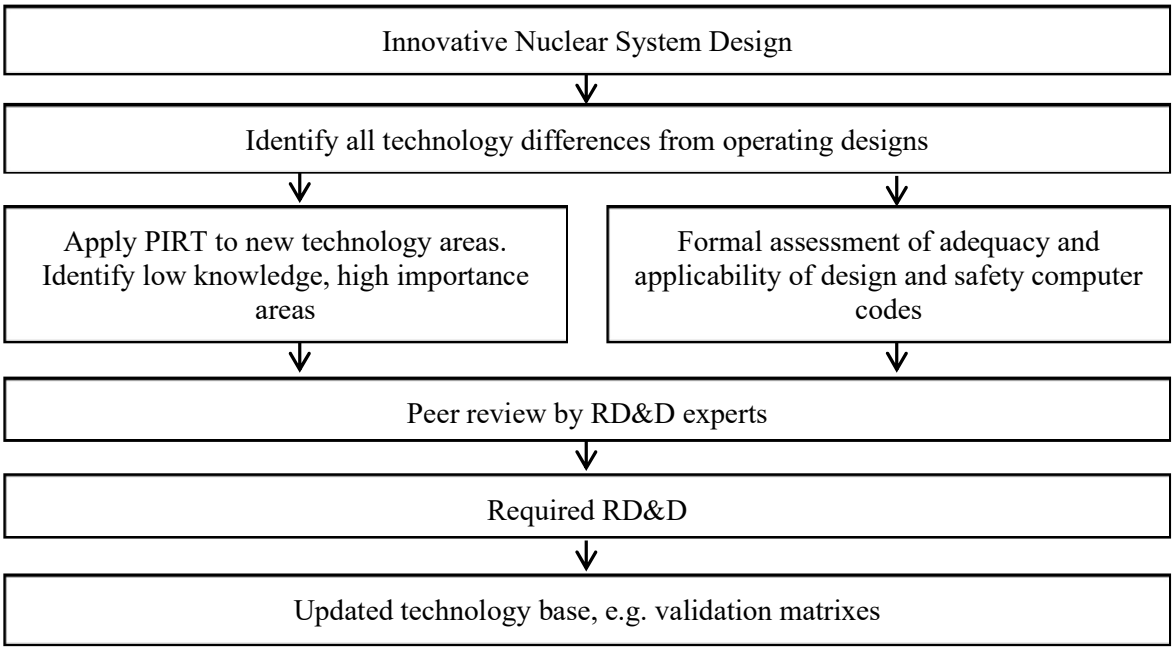

FIG 2. Overview of the different tasks for definition of RD&D.

The Objectives Provisions Tree (OPT) tool of the IAEA [71] uses the structured hierarchic DID framework to examine safety provisions (inherent features, equipment, and procedures) in innovative reactors. The OPT approach considers every DID level by defining objectives to be achieved, safety functions to be implemented, challenges to overcome, potential safety function failure mechanisms and the provisions incorporated to prevent or compensate failures. Figure 3 shows a diagram demonstrating the OPT approach and an example displaying its application.

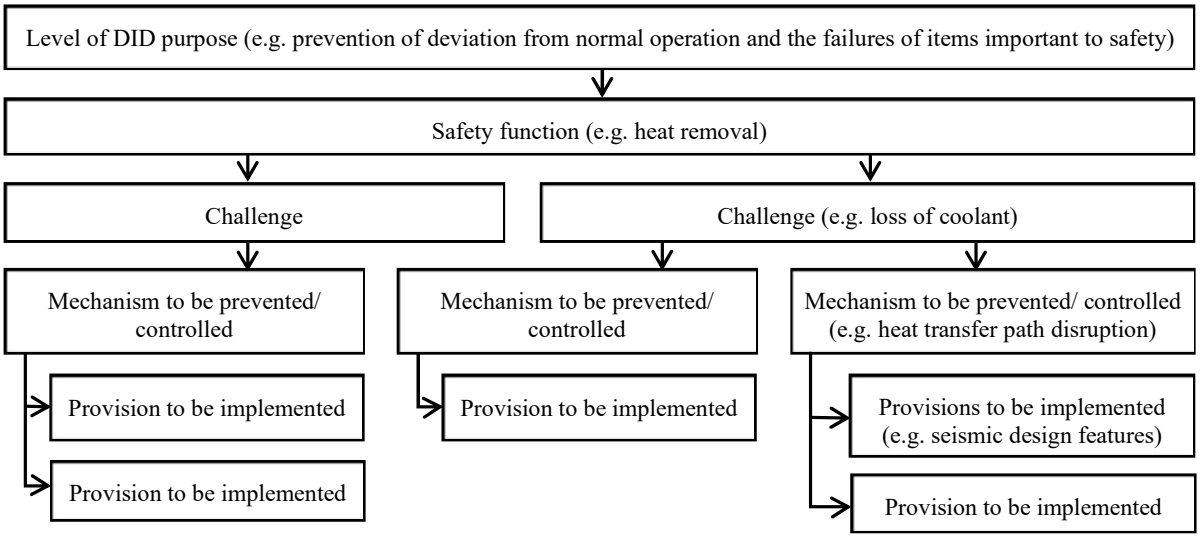

FIG 3. Objectives Provisions Tree approach (modified from Ref [71]).

Implementation of the OPT approach will help to define technology specific RD&D necessary to develop reliable and efficient provisions preventing or controlling safety functions failures.

During the process of generating new and/or more detailed data (e.g. for computational fluid dynamics codes) the selected RD&D tasks should be repeatedly assessed, and necessary

changes adopted. Qualified data should be included in a technology base, e.g. validation matrices (see also criterion CR7.3).

Some innovative reactor components cannot be tested in full size and not with the appropriate boundary and initial conditions, e.g. because of power limitations, or for core melt scenarios tests have to be performed always at a smaller scale and mostly also without using radioactive material. Thus, to reach sufficient confidence in the interpretation of such test results appropriate 'scaling' effects have to be taken into account.

Scaling investigations can be performed with analytical methods and by carrying out experiments with different sizes. To the extent possible both methods should be combined.

In the past large efforts have been undertaken to provide reliable thermal-hydraulic system codes for the analyses of transients and accidents in operating nuclear power plants with water cooled reactors. Many separate effects tests and integral system tests were carried out to establish a data base for code development and code validation.

In this context the question has to be answered as to what extent the results of down-scaled test facilities represent the thermal-hydraulic behaviour expected for a full-scale nuclear reactor under accidental conditions. Scaling principles provide a scientific-technical basis and a valuable orientation for the design of down-scaled test facilities. However, it is impossible for a down-scaled facility to reproduce all the physical phenomena of a full-scale plant in the correct timely sequence and significance. The designer/ developer needs to optimize a scaled-down facility for the processes (phenomena) of primary interest. Consequently, this leads to scaling distortions of other processes with less importance. Taking into account these issues, a goal-oriented code validation strategy is required, based on the analyses of separate effects tests and integral system tests as well as transients occurring in full-scale nuclear reactors. The validation matrices developed in the Committee on the Safety of Nuclear Installations of the Nuclear Energy Agency of the Organization for Economic Co-operation and Development may be a good basis for the realization of these tasks for LWRs (see details in CR7.3). In certain cases, separate effect tests in full scale could play an important role.

For innovatively designed reactors special attention should be directed to detect, study and model new phenomena, as well as to perform scaling considerations during the experimental and analytical work. In any case, code calculations with respect to scaling should always be performed with 'best-estimate models' along with a capability to perform uncertainty analysis.

The **acceptance limit AL7.2** (RD&D defined, performed and database developed) for the reactor assessed is met if evidence available to the INPRO assessor indicates that:

- Measured data are available in the region of application;
- Scaling considerations including uncertainty analyses have been performed and well documented;
- It was demonstrated that all phenomena are understood, data uncertainties are quantified, and documented in reports.

For probabilistic analyses the availability of reliability data with uncertainty bands is required.

4.10.3. Criterion CR7.3: Computer codes

Indicator IN7.3: Status of computer codes.

Acceptance limit AL7.3: Computer codes or analytical methods are developed and validated.

It is common practice to design and assess the behaviour of structures, systems and components of nuclear energy systems on the basis of code calculations. For operating nuclear facilities many suitable, i.e. verified and validated, computer codes are available.

For an innovative nuclear reactor new or more detailed models – established analysis methodologies, analytical models of systems, structures and components behaviour, developed using a representative database based on RD&D programme results – have to be implemented in computer codes, verified and validated. To confirm applicability of these computer codes to the design of systems, structures and components of the innovative reactor, the region of code application has to be covered by the validation matrixes used for quantifying uncertainties and sensitivities.

International standards, e.g. validation matrices, uncertainty quantification approaches combined with scaling considerations, etc, should be used. For example, agreed validation matrices exist for the thermal-hydraulic behaviour of water-cooled reactors. International experts within the Committee on the Safety of Nuclear Installations of the Nuclear Energy Agency of the Organization for Economic Co-operation and Development have selected well documented and accurate separate and integral experiments and plant behaviour data for these validation matrices. The selection process put emphasis on the inclusion of at least two test facilities of different size for each phenomenon or system behaviour. These test matrices are reconsidered periodically.

The computer codes need to have detailed documentation (code manuals) covering the theoretical basis of code development, a list of restrictions or application ranges, and a user guide. In addition to that an independent peer review of the computer codes and their applicability should be performed.

The **acceptance limit AL7.3** (validated computer codes and analytical methods) is met if evidence available to the INPRO assessor shows that for computer codes used in design and analysis of innovative reactors:

- The region of code application is covered by the code validation matrix so that the validation results can be used to quantify uncertainties and sensitivities;
- Independent reviews have been performed;
- Complete code documentation including detailed code manuals is available.

4.10.4. Criterion CR7.4: Novelty

Indicator IN7.4: Pilot or demonstration plant.

Acceptance limit AL7.4: In case of a high degree of novelty: a pilot or demonstration plant is specified, built and operated, lessons are learned and documented, and results are sufficient to be extrapolated to a full-size plant. In case of a low degree of novelty: a rationale is provided for bypassing a pilot or demonstration plant.

The demonstration of an innovative technology typically progresses from bench-scale experiments, to small-scale industrial tests, to large-scale tests, to (possibly) small pilot plants, to large-scale demonstration plants, and finally to full commercialization. The need for a pilot plant or a demonstration plant will depend on the degree of novelty of the processes and the associated potential risk to the owner and the public.

Pilot plants are small compared to demonstration or commercial plants. Not all components of a full-size power plant need to be installed in a pilot plant; at a later stage the rest of the components may be added. For example, a pilot plant may consist of a segment of the core, reactor coolant system and important (possibly new) components. Pilot plants are supposed to be designed such that new phenomena and major interactions thereof can be studied and/or demonstrated. It should be noted that (additionally) installed instrumentation in pilot plants may influence the thermal-hydraulic behaviour due to possible disturbances caused by this instrumentation (not foreseen for the full-size plant).

It is recognized that a small pilot plant can be used only to demonstrate adequate safety features for anticipated occurrences corresponding to Levels 1 and 2 of the DID concept. The safe behaviour of an innovative nuclear reactor during accidents (with a potential for radioactive release) cannot be sufficiently studied in a pilot plant and has to be demonstrated as defined in the CR7.3 above, using codes or analytical approaches validated against suitable experiments, e.g. integrated multiple-effects tests. These methods are covered in CR7.5. Nonetheless, pilot plants should be able to demonstrate the ability to cope with potential accident initiators.

It is important that the pilot plant facility is of adequate scale, such that the results and experience gained from the facility could be extrapolated with a reasonable degree of accuracy to the full-scale plant.

Demonstration plants are usually intended to demonstrate that safety, operational (and to a certain degree economic) targets are achieved or achievable and that the (possibly complex) interactions between (new) components in different operational states and sequences behave as predicted by codes.

For both types of plant, it is important to document their operation for a sufficiently long time to achieve adequate confidence in a new design. It is also evident that some innovative components don't need to be tested in a nuclear environment.

Pilot as well as demonstration plants are not intended to be commercially viable.

It is evident that a design-specific project plan (roadmap) with a well-defined process for the demonstration of innovatively designed components or systems has to be established and reconsidered periodically or after the accomplishment of milestones. There are examples showing that the application of larger sized test facilities resulted in the detection of new phenomena not seen in smaller ones.

Examples of significant novelty in advanced reactor components include: the supercritical-water cooled power reactor, additives to coolant fluids (e.g. sodium) with the characteristic to avoid an exothermic reaction with the fluid (e.g. water) on the secondary side of heat exchangers, radical new fuel and core physics, new concepts for shutdown/control concepts, new heat removal systems, etc.

The result of the decision process for whether to build and operate a pilot plant depends on several issues, e.g. the amount of available separate effects and integral tests, the degree of novelty, the available budget, the experience of operating crews, the overall time schedule up to commercialization, etc.

If a pilot plant has been (will be) built, the INPRO methodology recommends an independent peer review of this plant to support confidence in the adequacy of the pilot plant.

The **acceptance limit AL7.4** (adequate pilot or demonstration plant built or rationale for not building provided) for the reactor assessed is met if evidence available to the INPRO assessor shows that the degree of novelty of innovative safety components and systems has been identified and depending on the novelty a pilot or demonstration plant has been built, operated as part of the RD&D programme and an independent peer review about the adequacy of the pilot plant has been performed. Otherwise a rationale needs to be provided for bypassing a pilot or demonstration plant and going directly to an FOAK plant.

4.10.5. Criterion CR7.5: Safety assessment

Indicator IN7.5: Adequate safety assessment involving a suitable combination of deterministic and probabilistic methods, and identification of uncertainties and sensitivities.

Acceptance limit AL7.5: Uncertainties and sensitivities are identified and appropriately dealt with, and the safety assessment is approved by a responsible regulatory authority.

The safety assessment is expected to be performed using a suitable combination of deterministic and probabilistic evaluations and documented in an appropriate format [72]. The analysis needs to cover all modes of operation of the installation to obtain a complete assessment of conformance with the DID concept. Deterministic safety assessment [52] uses a pre-defined set of accidents to define the design of the safety systems. Normally pessimistic assumptions on accident initiation and evolution, plant state, and plant response are applied. Probabilistic safety assessment (PSA) [73, 74] calculates the frequency and consequences of all accidents down to very low probability of occurrence. Best estimate analyses are commonly used in PSA because a realistic response to an initiating event is needed to estimate the risk and to determine the margins in predicted plant behaviour between a conservative deterministic safety assessment and a best estimate result.

A deterministic safety assessment needs a sound data base and incorporates some conservatism (margins) by using pessimistic assumptions to cover uncertainties in input data such as model parameters and plant state. The value of a PSA depends also very much on the availability of well-based data on, primarily, the reliability of components. Because all data (including experimental data) are somewhat uncertain, PSA normally includes uncertainty analyses.

It is commonly accepted that PSA provides a broader and deeper understanding of safety and risk relevant issues than deterministic methods alone (see above); therefore, PSA is increasingly used for optimization of the various levels of DID, and the optimal allocation of available resources.

The extent to which each method is used needs to be consistent with the confidence in the method for the particular application in terms of reliability data, failure modes and physical phenomena. In some innovative systems, the application of probabilistic methods could be more restricted in comparison with those accepted for operating reactor types, as a consequence of changes in technology and the resulting limited availability of data.

The degree of conservatism in a deterministic safety assessment is commensurate with the uncertainties in the technology evaluated; thus, when the important phenomena are well known, and codes are validated a realistic hypothesis (best estimate) could be considered in the assessment. A best estimate assessment needs to be accompanied by a consideration of the uncertainties of experimental data used for the code models, and uncertainties of the plant status. Where the technology itself is uncertain, a more traditional approach is normally taken: for example, when other liquid metals than those used today are foreseen in a reactor, the currently available codes are not sufficiently developed to simulate all phenomena. Until these tools are available and proven accurate enough, additional or extended safety margins and conservatism are expected to be implemented in the simulations of plant behaviour.

In addition to the assessment of the vulnerability of a nuclear reactor to severe accidents and accidental releases, a probabilistic safety assessment is used starting at the design stage to:

- Determine more realistic loads and conditions for mitigation systems, including containment;
- Assess the balance of the design and possible weakness;
- Integrate human factors into the safety assessment;
- Identify safety margins;
- Help to define operational safety requirements;
- Identify sensitivities and uncertainties.

In principle, a PSA is expected to investigate all possible accident scenarios. Practically, all scenarios involve phenomena associated with some uncertainty; therefore, there exists a fundamental uncertainty in the results of these analyses. A thorough uncertainty analysis can identify areas that need further investigation. Furthermore, if the PSA generates 'point' estimates, an uncertainty analysis may contribute to the credibility of these results.

Sensitivity studies – determining the difference in results using a defined value of a variable and a given deviation from that reference value – are a tool to define the required accuracy (or allowable uncertainty) of a variable.

Typically, three classes of uncertainties are identified:

- Parameter (data) uncertainty, like initiating event frequencies, component failure rates, human error probabilities, etc. The uncertainties are propagated through the assessment steps to generate a probability distribution of the end result.
- Model uncertainty associated with phenomenological models of the physical-chemical processes and related assumptions. They are treated similar to the parameter uncertainties.
- Completeness uncertainties reflect limitations of the scope or truncation effects. In principle, such uncertainties cannot be quantified within a given PSA scope, but by performing additional analyses of excluded events their significance can be evaluated.

In case a required accuracy has not been achieved, either additional experiments have to be performed or design provisions have to be implemented to cope with these uncertainties. Detailed consideration of uncertainties in reliability data of components and human performance involves human factor related data appropriate for a given organisation and / or country.

Safety assessment has to cover all relevant operating stages of the nuclear reactor and its operating phases. In addition to AOOs and accidents which may influence the nuclear fuel in the reactor core, the safety assessment has to cover also potential AOOs and accidents in the near reactor handling and storage of fresh fuel and spent fuel.

For assessing the adequate performance of NPP safety analyses, there exist a number of IAEA publications, e.g. Refs [75, 76]. The safety assessment should be periodically re-examined and updated [77].

'Risk informed decision making' [78–83] includes design criteria that implicitly involve probabilistic considerations and that are complemented by explicit probabilistic arguments for clarifying design objectives. Weaknesses and vulnerabilities of a design can be identified and judged against design objectives. Various options available for improving safety can be quantitatively assessed and compared also with respect to cost effectiveness. Decisions concerning reliable assurance of safe operation and control of risk can be based on such additional justification.

In Ref [78] various publications, national positions and examples of such options for several reactor designs are provided, e.g. the implementation of strategies for fission product retention in a faulted non-isolated steam generator, modification and back fits to PWR and BWR containments, provisions against LOCA outside BWR containments, protection of suction strainers against clogging, etc. The listed examples demonstrate substantial use of PSA in safety relevant decisions by regulators and licensees.

It is, however, evident that, due to the non-availability of experience-based data on the behaviour of innovative designs, a risk-informed approach is more appropriate for operating (or evolutionary) reactor designs with well recorded operational behaviour than for innovative designs.

The **acceptance limit AL7.5** (adequate safety assessment covering uncertainties and sensitivities) is met if evidence available to the INPRO assessor shows that an adequate safety assessment involving a suitable combination of deterministic and probabilistic methods, and a thorough analysis of uncertainties including complementary sensitivity studies[40] has been performed for the facility assessed and was accepted by the responsible regulatory authority in the country of origin.

4.11. CONCLUDING REMARKS

To achieve long term sustainability for nuclear reactors to be installed after 2013 one basic principle has been formulated by the INPRO methodology along with seven user requirements for sustainability assessment in the area of reactor safety. The approach to safety is based on the application of an enhanced DID strategy compared to reference designs, supported by increased emphasis on inherent safety characteristics and passive features. Greater independence of the different levels of DID is considered a key element to avoid failure propagation from one level to the subsequent one. The number of physical barriers in a nuclear facility that are necessary to protect the environment and people depends on the potential internal and external hazards and the potential consequences of failures; therefore, the barriers will vary in number and strength depending on the type of nuclear reactor (e.g. with high or very low power density cores).

The end point of the enhanced DID strategy is that, even in case of accidents with severe core damage, emergency radioactivity releases from the plant large enough to require evacuation of population must be made very unlikely.

The developer of a new reactor design needs to consider the objectives of nuclear safety together with those of physical protection and proliferation resistance during all design stages.

[40] An independent peer review is recommended.

APPENDIX I
EXAMPLES OF REFERENCE REACTORS FOR INPRO ASSESSMENT

Using of the INPRO methodology in the area of reactor safety requires a reference reactor design in addition to the reactor design being assessed. The reference design should represent the latest design operating in 2013 designed preferably by the same designer as for the plant assessed. For innovative reactors which may have no operating prototypes in 2013, the latest design that has been safely operated or at least licensed can be used as a reference - designed preferably by the same designer as the reactor assessed and using the same technology.

In the following Table 14 potential reference designs are proposed for some novel water-cooled reactor designs.

TABLE 14. REFERENCE PLANTS FOR INPRO ASSESSMENT OF WATER COOLED REACTORS

Designer	Reactor assessed	Reference plant
Gidropress	AES-2006/V-491	WWER1000/V-320
Westinghouse	AP1000	SNUPPS, Sizewell B (UK)
AREVA	EPR	N4, Civaux 1,2 (France)
Hitachi-GE	ABWR	BWR5, Kashiwazaki Kariwa (Japan)
Candu Energy Inc.	EC6	CANDU6, Point Lepreau (Canada)
GE-Hitachi	ESBWR	BWR6, Leibstadt (Switzerland)
KEPCO	APR1400	OPR1000, Shin Kori 2 (Republic of Korea)
Mitsubishi	US-APWR	PWR (four-loop), Ohi 4 (Japan)

In the following Table 15 potential reference designs are proposed for some innovative sodium cooled fast reactors.

TABLE 15. REFERENCE PLANTS FOR INPRO ASSESSMENT OF SODIUM COOLED FAST REACTORS

Designer	Reactor assessed	Reference plant
IGCAR	CFBR	PFBR (India)
OKBM	BN-1200	BN-800 (Russian Federation)
CIAE	CFR-1000	CEFR

APPENDIX II
EXAMPLE OF APPROACH TO THE ASSESSMENT OF REACTOR CORE DESIGHN MARGINS

The following discusses an example of how to approach the INPRO assessment of reactor core design and other safety related components with respect to design margins (robustness).

The nuclear fuel in the reactor core generates heat that has to be transported out of the core in normal operation conditions by the primary coolant. Different types of reactors use different coolants, e.g. water, sodium, lead, helium, and molten salt, at different temperatures and pressures. Natural flow through the core during normal operation, as used in some boiling water reactors (BWRs), has the advantage that no active re-circulation pumps are necessary, which is clearly a simplification of the design in comparison to a reactor with forced flow. However, every reactor design with forced flow has also a capability to remove some power produced within the core by natural convection; the ease of transition (from forced flow to natural convection) depends on the design and transition sequence. An increase of the fraction of core heat that can be removed by natural circulation is therefore regarded as an increase of robustness.

The reactor design incorporates systems to control power distribution in the core and the overall power level, e.g. by control rods, liquid poison, and/or reactivity feedbacks[41], and a diverse and redundant safety system to shut down the reactor to decay heat generation level. An appropriate instrumentation and control (I&C) system has to be included to measure and control local and integral physical (neutron flux), thermal (temperature) and thermal-hydraulic states (pressure, flow). Most values measured by the I&C system will also be used by the reactor protection system, possibly with different instruments.

The core design may be divided into several areas:

- Thermal and mechanical fuel design;
- Neutronic core design; and
- Thermal-hydraulic core design including the core's cooling circuit.

The *thermal fuel design* determines the margins of the fuel against specified limits on such quantities as centerline fuel temperature, fission gas release, or maximum fuel cladding temperature. In the *mechanical fuel design*, it has to be shown that the fuel and the core internals can cope with loads resulting from operational states (fission gas pressure, vibrations, lift-up, etc.) as well as with external loads, e.g. from earthquakes and hydraulic forces (in case of pipe breaks).

The *neutronic design* of the core is focused on the optimization of power distribution and burnup of the fuel but includes also the demonstration of sufficient safety margins during operation and transients.

The *thermal-hydraulic core design* has to demonstrate that primarily the fuel is sufficiently cooled during normal operation, transients and accidents. The goal is to avoid exceeding such design limits as (in water cooled reactors) departure from nucleate boiling (DNB) or dry out (i.e. exceeding the critical heat flux, CHF) during normal operations and transients and to at least limit the exceeding of those limits during DBAs. In non-water-cooled reactors, a comparable design limit is typically the maximum allowable fuel element temperature.

[41] Void and temperature in a BWR core is changed also via the core coolant flow, i.e. by the main coolant pumps.

For example, important design parameters for the core of an advanced heavy water reactor (AHWR) include the following:

1. Neutronic characteristics:
    a) Doppler, void and power coefficients of reactivity;
    b) Efficiency of the regulating group of control rods;
    c) Shutdown margins.
2. Fuel thermal design margins:
    a) Fuel centerline temperature (normal operation);
    b) Stored energy in fuel;
    c) Linear heat generation rate; and
    d) Design margins on clad temperature (for corrosion and oxidation considerations).
3. Fuel mechanical design margins:
    a) Design margins on clad stress and strains; and
    b) Fission gas release.
4. Thermal hydraulic design margins:
    a) Minimum Critical Heat Flux Ratio (MCHFR);
    b) Margins to instability (margin on sub-cooling);
    c) Decay heat ratio; and
    d) Fraction of core heat that can be removed by natural circulation.

This list can be used by the INPRO assessor to compare the core design of the reactor to be assessed with that of the reference design.

APPENDIX III
EXAMPLES OF MONITORING SYSTEMS

Examples of monitoring systems for water cooled reactors are given below, some of which may also be applicable to various non-water-cooled designs.

Leakage monitoring. The leakage monitoring system is designed to be able to adequately detect and localize leakages in the reactor coolant pressure boundary during plant operation. This system is sensitive enough to detect those leakages that would not yet lead to an automatic activation of safety measures (e.g. due to pressure build-up, etc). Measured values include air humidity or dew point temperature; air temperature; radioactivity of compartment exhaust air; and condensate in recirculation air coolers. There are also leak monitoring systems based on acoustics, i.e. the noise caused by leakage.

Loose parts monitoring. Experiences in operating nuclear power plants have shown that the occurrence of loose parts in the primary circuit cannot be completely eliminated. Parts carried away by the coolant medium may cause damage to the fuel rods or other in-vessel components. A loose-parts monitoring system is used to detect such incidents.

Vibration monitoring system of RPV internals. This system measures and analyses continuous and cyclic characteristic vibration values.

Diagnostics of rotating machinery. Increasing plant availability and plant safety, as well as reducing costs of maintaining rotating machinery, such as fans, pumps and turbines, requires reliable information on the condition of these components. For example, the basic monitoring of pumps is usually done by monitoring the pump house vibrations and, for re-circulation pumps, the shaft vibration.

Chemical monitoring. The aim is to maintain chemistry conditions that ensure a high corrosion resistance in parts of the power plant systems and components, something which is essential for safe and economic plant operation. The chemistry manual[42] describes water chemistry aspects for relevant plant systems such as the reactor coolant system; reactor auxiliary systems; the steam, condensate and feed water cycles; non-nuclear auxiliary systems and the radioactive waste processing system.

Seismic monitoring. The seismic instrumentation informs the operator if a significant seismic event occurs and records the seismic characteristics (acceleration, frequency, etc.).

In-core monitoring. The importance of in-core monitoring systems and their relevance to reactor safety may be different in different reactor designs. Such systems may be designed to determine the power distribution in the reactor core, to confirm that power distribution characteristics stay within regulatory limits at different power levels and that deviation from the originally calculated distribution does not exceed prescribed uncertainty limits. Theoretically, discrepancies of core power distribution can be caused by different potential errors, e.g. errors in the core calculations, errors during the reactor reloading etc However, different reactor designs may have several alternative tools and methods for protecting against such errors. In-core monitoring systems are normally based on temperature distribution measurements and/ or neutron flux distribution measurements and involve detectors, signal transfer and processing, and the analysis of 3-D power distribution.

[42] See also evaluation parameter EP1.2.5, sufficient technical documentation, of criterion CR1.2.

Monitoring environmental impacts of radioactive releases. A special computer system archives and processes all radiological data from various plant systems in order to obtain a comprehensive overview of the radiological situation of the plant and its environment.

Monitoring supported by computerized aids to operators. State-of-the-art I&C systems are digital. This allows – in combination with the progress in computer speed and capacity – the installation of advanced real-time aids for operators, e.g. screens showing a failure location, prognosis of possible system behaviour as a consequence of this failure, and a list of possible countermeasures. In addition, computerized manuals are becoming the state of the art. Taking advanced system modelling and computer capabilities into account, advanced control systems including expert systems (artificial intelligence methods) may be implemented in the longer term.

APPENDIX IV
FREQUENCIES OF DBA

In the following, the approach to assessment of CR3.1 for accidents caused by internal events is discussed.

For the design of safety systems, a limited number of DBAs has been defined. The selection of different accident sequences is based on operating experience and analytical evaluations. For operating water-cooled reactors, DBAs caused by internal events range from operational transients (e.g. total loss of feed water) without loss-of-coolant up to medium and large break LOCAs (guillotine break of main coolant pipe).

The correlation between the probability of occurrence (i.e. the calculated frequency) and dose or damage to an individual or the public (and environment) is schematically shown in Figure 4, which illustrates three aspects:

- The higher the consequences (damage) the lower is the frequency of occurrence. Note that medium and large break LOCAs have not occurred at all to date in operating reactors;
- The frequency of accidents in the (new) NES assessed is lower than in operating designs (the reference plant);
- Large radioactive releases (see discussion of CR4.4) are practically eliminated in the (new) NES.

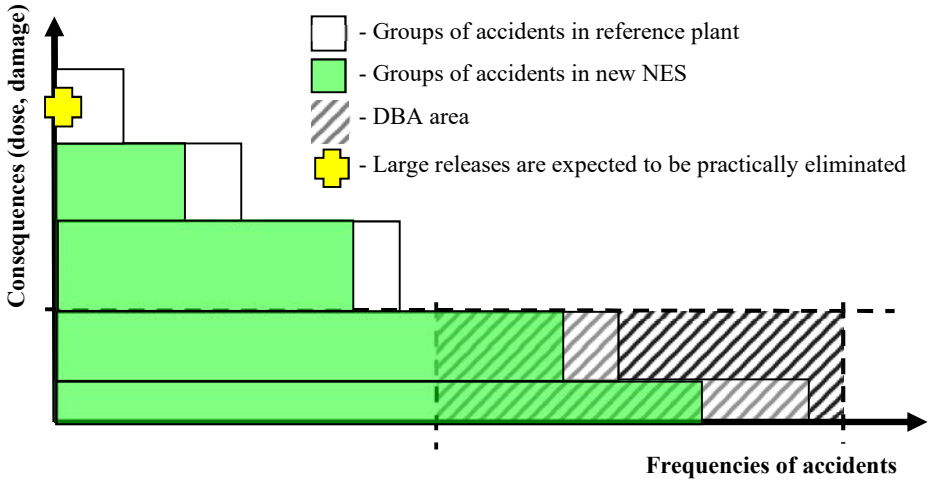

FIG. 4. Correlation between the frequency of accidents and dose or damage in reference NPPs and in new NESs, respectively.

It has to be mentioned that a DBA may be caused either by a sequence of events, i.e. in such a case the frequency of an initiating event is not necessarily equal to the frequency of the DBA, or by a single initiating event (e.g. large pipe break) causing the DBA immediately. The frequencies of several internal initiating events of DBAs to be used in probabilistic analyses – similar to the frequencies of AOOs (see CR1.4) – are usually postulated by national regulatory bodies based on comprehensive (national) risk studies [41, 44, 45]. Thus, a change (reduction) of these values would need the approval of licensing authorities as part of a licensing process. However, for the purpose of INPRO assessment of NES sustainability, technical arguments can be developed by the designer/developer that support potential expected reduction of the frequencies of these specific internal initiating events of DBAs in the new reactor compared to the reference plant. Arguments to support such a reduction include those based on: improved

materials (e.g. with higher strength), improved design margins (e.g. against overstressing and fatigue, against departure from nuclear boiling, etc.), more effective and efficient inspections (e.g. introduction of a leak before break concept), and continuous monitoring of plant health, etc. Thus, for the purpose of INPRO assessment of NES sustainability, lower frequencies of occurrence of the group of DBAs discussed above in a new reactor design could be tentatively justified by provisions implemented in Level 1 of DID.

As an example of frequencies of occurrence of DBAs for new LWRs, INPRO methodology proposes for a small break (SB) LOCA[43] the value of F_{SB}:

$$F_{SB} < 10^{-2} \text{ per unit-year,}$$

and for a medium or large break (LB) LOCA:

$$F_{LB} < 10^{-4} \text{ per unit-year.}$$

These frequencies F_{SB} and F_{LB} could be used as INPRO methodology acceptance limits for those specific DBAs of LWRs when the corresponding frequencies of the reference design are higher than F_{SB} and F_{LB} or not available to the INPRO assessor.

[43] A LOCA is an accident with a break flow out of the primary coolant system that cannot be compensated by the reactor make-up system. For example, SB-LOCA is defined (by the U.S. NRC) as a break of a pipe connected to the primary pressure boundary with a diameter of about 1.3 to 5 cm (for a PWR), for a medium break LOCA the pipe diameter is about 5 to 15 cm, and for a LB-LOCA it is from 15 cm up to the guillotine break of the main coolant line.

APPENDIX V
ENGINEERED SAFETY FEATURES

Engineered safety features (safety systems) are designed to ensure the fundamental safety functions by providing the safe shutdown of the reactor, the removal of the residual heat from the reactor core, and confinement of radioactive material to limit the consequences of DBAs (caused by internal and external events and probable combinations thereof). Engineered safety features and protection systems should be provided to prevent evolution towards severe accidents and to prevent core damage in particular [13], and also to confine radioactive materials within the containment system.

Ref [68] states:

> "171. Initiation and operation of the engineered safety features are highly reliable. This reliability is achieved by: the appropriate use of fail-safe design; by protection against common cause failures; and by independence between safety systems and plant process systems. The design of these systems ensures that failure of a single component would not cause loss of the function served by a safety system (the single failure criterion)."

It also claims that "in current and future plants, consideration is given to improving safety systems in terms of reliability and response time" [68].

To provide the necessary level of reliability of safety systems it is common engineering practice to cover a 'single failure' in the design of a safety system; the 'single failure' is usually selected to represent the worst failure of an active component in the system.

The coincidence of several identical component failures due to common cause (dependencies) is called a common cause failure (CCF). Physical or spatial separation, structural protection and diversity can be used to prevent potential CCF [13]. CCFs have to be taken into account especially for the safety systems designed to be redundant. For example, for the assessments of evolutionary PWRs it was underlined that "the unavailability of a redundant safety system consisting of identical trains probably cannot be demonstrated to be less than 10^{-4} per demand" [84].

As in other facilities, operator intervention is necessary in nuclear plants for plant operating purposes at least some time after a DBA has occurred. There are evaluation methods available to assess the reliability of intervention of plant operating staff [85].

The consideration of potential cliff-edge effects in the scenarios of accidents needs to be taken into account in the selection of design strategy for the fulfilment of fundamental safety functions, e.g. removal of the residual heat, and in the design of safety systems.

Another issue influencing the reliability of safety systems is the necessary maintenance/repair period of safety system components. In principle, there are three options for maintenance of the necessary level of system reliability in this situation:

- Provision of an additional parallel system (as it was done in several NPPs in Germany);
- Provision of redundant 'active' components (e.g. pumps) but no redundancy for passive components (e.g. pipes); this approach has been chosen e.g. for the EPR design;
- Definition by the regulator of (short) acceptable specific maintenance/repair periods for safety systems of reactors without additional systems or components. For most operating reactors these periods have been licensed because, during these (short) periods of maintenance/repair, the overall safety risk is assumed to be only marginally increased.

Enhanced reliability of engineered safety features may be achieved by inclusion of passive systems into (advanced) reactor designs, although other methods can also be effective, e.g.

increased redundancy and diversity of active systems. Advanced reactors might include such passive design features as passive shutdown, passive decay heat removal and passively operated coolant injection systems. Even the use of exclusively passive systems might be possible for an innovative design. In the design of new reactors, the passive safety systems are expected to be given priority only when they are at least as capable and reliable as active systems.

The engineered safety features generally include a mechanical part and I&C. The latter normally controls the mechanical equipment to implement a given safety function and provides operator with necessary information on the process and status of the system. The I&C encompasses all associated equipment including individual measuring instruments for process parameters and component actuation devices. One of the most notable safety related I&C is the safety protection system (SPS) which consists of the reactor protection system (RPS) and the actuation system of engineered safety features. In a typical water-cooled reactor, the SPS controls implementation of the most important safety functions:

- Shutdown of the reactor;
- Residual heat removal from the reactor core;
- Containment isolation.

The design of SPS normally incorporates the following principles:

- Fail-safe principle. If the system fails, it settles in a safe state;
- Single-failure criterion: SPS retains its functional capability even in case of a single failure accompanied by unavailability of another component due to repair or maintenance;
- Diversity principle and diverse process variables: SPS measures at least two different process parameters for one objective. Passive signal indicators possible for an innovative design;
- Redundancy principle: Sufficient redundancy of SPS components to perform safety function in case of failure of components;
- Common mode failure principle: Common mode failure due to internal or external hazards prevented to the extent possible by physical/ spatial separation and structural protection;
- Qualification for operation in harmful environments: SPS designed for environment characteristics of DBAs – temperature, humidity, chemical hazards, radiation etc;
- Automation principle: Automatic initiation and operation at least in the initial phase of an accident to reduce necessity of human intervention;
- Independence from other systems including other I&C: SPS functionally and physically separated from other systems including the control system and other automation systems;
- Control and monitoring: operators in the main control room continuously provided with reliable information on the status of SPS;
- Periodic testing: SPS functions can be tested during operation of the plant. Tests ensure that the design basis functional requirements are met;
- Self-diagnosis, validation of input and actuation signals: SPS monitors the validity of input and output signals and internal processes, and issues alarm signals when needed. Adequate self-diagnosis capability covers all potential hardware and software faults.

The IAEA published a safety guide on the design of I&C systems for NPPs [86] providing detailed recommendations on the design basis, architecture, safety classification, management system, software and human-machine interface for the I&C systems.

The probabilistic methodology to evaluate the reliability (or unavailability) of safety systems comprises the following main steps:

- Identification of initiating events and their frequencies of occurrence;

- Determination of the unavailability of system functions considered in the event sequences, taking human factors and common cause failures into account;
- Determination of the frequency for a highly degraded core (with either a destruction of fuel elements (LWRs, HWRs), the loss of retention capabilities for normally contained fission products (HTGRs), or the loss of the integrity of the primary circuit (molten salt reactors) without and with accident management (AM) actions.

The fault tree analysis is a systematic method of determining the dependency between the failure of a system and failure of its components. The result of such an analysis is the probability of system failure. This method is used for components of engineered safety systems as well as for the I&C systems.

Table 16 presents some examples of reliability data (probability for failure) of engineered safety systems for different initiating events in an operating PWR (Germany).

TABLE 16. RELIABILITY OF ENGINEERED SAFETY SYSTEMS [42]

Event	**Probability of failure of engineered safety system* per demand and unit**
Loss of heat sink	$8.0\ 10^{-6}$
Loss of feed water supply	$2.1\ 10^{-5}$
Breaks in reactor coolant pipe > 200 cm^2	$< 3.0\ 10^{-3}$
Breaks in reactor coolant pipe 80 to 200 cm^2	$3.5\ 10^{-3}$
Breaks in reactor coolant pipe 2 to 12 cm^2	$1.1\ 10^{-3}$
ATWS** during loss of main feed water	$8.4\ 10^{-3}$

Notes: * - loss of safety function, ** - anticipated transient without scram (ATWS)

APPENDIX VI
CONFINEMENT BARRIERS

The general strategy for DID is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution of accidents to more serious conditions, i.e. Levels 4 and 5 of DID. Should preventive measures fail, mitigatory measures, in particular a well-designed containment/confinement can provide the necessary final protection of the public and environment. Generally, several successive physical barriers for the confinement of radioactive material are put in place. Their specific design may vary depending on the radioactivity of the material, on the possible loads on the different barriers and, evidently, on the reactor design itself.

For water cooled reactors, barriers confining the fission products are typically the fuel matrix[44] (partially), the fuel cladding, the pressure boundary of the reactor coolant system (during power operation, but not during shut down), and finally the containment system.

INPRO methodology requirements on the integrity of confinement barriers for the reactor core are summarised in Table 17. For the near reactor spent fuel pools the requirements and barriers depend on the design and generally remain the same except for the primary circuit boundary[45].

TABLE 17. MINIMUM NUMBER OF BARRIERS FOR THE REACTOR CORE IN DIFFERENT LEVELS OF DID

DID Levels	INPRO requirement on minimum number of barriers maintained	Minimum number of barriers maintained (example of operating PWR)
1	All barriers provided by the design for normal operation	4 - fuel matrix, fuel cladding, primary circuit boundary, containment
2		
3	At least one	3[a] - fuel matrix[b], fuel cladding[b], containment
4	At least one	At least one

Notes:
a – assuming that primary coolant boundary was damaged after LOCA.
b – limited number of fuel rods may fail.

Examples of minimum number of barriers maintained for different accidents in PWR are presented in Table 17.

Because the last barrier against a release of radioactive material into the environment is so important, the containment/ confinement system has to be well designed (against internal and external events and probable combinations thereof) and carefully maintained. An additional requirement for water-cooled reactors is the permanent or periodic confirmation of leak tightness of the containment.

For HTGRs the main barrier against an accidental release of radioactivity is the coated fuel particle [87]. For molten salt reactors the fuel rod integrity is not relevant, and the main barriers are the primary circuit boundary and containment. Different barriers exist also for designs with a double walled pressure vessel or designs with submerged (in water) pressure vessels [7, 88].

[44] In some Member States the fuel matrix is not considered as a barrier.
[45] In pool-type sodium-cool fast reactors the spent fuel is normally stored within the reactor vessel.

APPENDIX VII
ACCIDENT MANAGEMENT

The AM is defined in the IAEA Safety Glossary [17] as follows:

> "The taking of a set of actions during the evolution of an accident:
> (a) To prevent escalation to a severe accident;
> (b) To mitigate the consequences of a severe accident;
> (c) To achieve a long term safe stable state."

The IAEA published a safety guide on the AM programmes for NPPs [58] providing detailed recommendations on the development of such programmes, on the structure of AM guidance, and on the AM strategies to be developed for different accidental scenarios. Ref [58] states:

> "2.10. The accident management programme should be developed and maintained consistent with the plant design and its current configuration …
>
> 2.11. The accident management programme should address all modes and states of operation and all fuel locations, including the spent fuel pool, and should take into account possible combinations of events that could lead to an accident …
>
> 2.12. A structured top-down approach should be used to develop the accident management guidance. This approach should begin with the objectives (including the identification of plant challenges and plant vulnerabilities) and the strategies, followed by measures to implement the strategies. In combination, these strategies and measures should include consideration of plant capabilities. Finally, procedures and guidelines should be developed to implement these strategies and measures …
>
> …
>
> 2.14. Multiple strategies should be identified, evaluated and, when appropriate, developed to achieve the objectives of accident management, which include:
>
> (a) Preventing or delaying the occurrence of fuel rod degradation;
> (b) Terminating the progress of fuel rod degradation once it has started;
> (c) Maintaining the integrity of the reactor pressure vessel …;
> (d) Maintaining the integrity of the containment and preventing containment bypass …;
> (e) Minimizing releases of radioactive substances …;
> (f) Returning the plant to a long term safe stable state in which the fundamental safety functions can be preserved."

The in-plant AM measures and actions in case of a highly degraded core are very plant-specific. For water-cooled reactors, examples for in-plant AM measures which can be initiated by the operator when appropriate include:

- Monitoring of RPV, plant systems, structures and components status, and the containment environment;
- Projection on the development of accident scenario;
- Injection of boron into the core (e.g. in case of ATWS);
- Depressurization of RPV to avoid high pressure failure of RPV;
- Restoration of heat removal from the core;
- Spraying into the containment atmosphere when it is necessary and allowed (i.e. does not compromise safety characteristics);
- Prevention of the containment bypass (trough the potential rupture of SG tube);
- Supply of AC/DC power (e.g. via mobile equipment from outside the containment);
- Removal of hydrogen from the containment atmosphere;

- Flooding of the reactor cavity to remove the heat from RPV from outside (when appropriate);
- Filtered containment venting.

In the past – based on experience from the accidents at Three Mile Island and Chernobyl[46] – some operating reactors had to be back-fitted (improved or modified), e.g. enhancing ranges of instrumentation, installing filtered containment venting systems and hydrogen recombiners etc. Besides the use of designated safety features, all types of nuclear power plants have the potential to use other (operational) systems to regain control of the facility after an accident with severe core damage and/or heavily degraded fuel in the spent fuel pool.

Ref [58] provides the recommendations on organization of trainings for the personnel involved in the AM programme including the following:

> "2.95. A list of persons who will be part of accident management should be established, and these persons should be designated as emergency workers. This list should take into account accidents developing over a long period so that adequate shift staffing is maintained at the plant (e.g. during holidays and overnight).
>
> 2.97. Appropriate training should be provided to members of the operating organization personnel responsible for accident management; the training should be commensurate with their roles and responsibilities."

[46] It is expected that after the severe accident in Fukushima Daiichi the operating plants will also need backfitting of their safety features especially with regard to the control of accidents with prolonged station blackout [19].

APPENDIX VIII
ESTIMATION OF CONSEQUENCE OF EXTERNAL RELEASE

International Commission on Radiological Protection [89] recognises three types of radiation exposure situations that for the case of NPP can be presented as follows:

- A *planned radiation exposure* situation that arises from the planned (normal) operation of the NPP. For public exposure the dose limit is defined as an effective dose of 1 mSv in a year. In this situation to determine the actual licensed public dose limit the concept of dose constraint has to be taken into account;
- An *emergency exposure* situation that arises as a result of an accident. In this situation a *reference level* expressed in terms of residual dose shall be defined, typically an effective dose in the range 20 – 100 mSv that includes dose contributions via all exposure pathways. The protection strategy shall be optimized by planning for residual doses to be as low as reasonably achievable below the reference level;
- An *existing exposure* situation that arises from natural background radiation, past practices outside regulatory control, or after an emergency exposure situation.

Evacuation of population is a protective action in an emergency that can reduce the risk of stochastic effects, i.e. reduce consequences of the accident. Radiological criteria for evacuation of population are normally formulated in terms of projected dose. Dose calculations need to be performed with validated computer codes; these calculations have to include uncertainty analyses. To avoid the necessity for protective actions such as evacuation of people around an NPP the calculated public dose after a severe accident needs to be below the criteria for evacuation of population for emergency exposure situations.

Estimation of the consequence of the accidental external release can be divided into two major parts. The first part is focused on the definition of the characteristics of the release source term. These characteristics can be calculated as the result of the accident consequence modelling within the reactor containment/ confinement either deterministically or as a part of PSA Level 2 analysis. The second part models the transport of the radionuclides to the population outside of the NPP through different potential routes and scenarios (PSA Level 3). In addition to exposure due to releases of radioactivity to the environment, radiation transport from the damaged reactor core through the containment/ confinement wall, i.e. irradiation from the reactor building, has to be considered in the calculation of consequences (dose).

The latter part of estimation of the consequence of the accidental external release, the modelling of the radionuclides transport to the population outside of the NPP involves simulation of environmental dispersion and transfer, identification of exposure pathways, selection of population groups and evaluation of doses [90].

The definition of source term for an accidental release to the environment is the prerequisite to the modelling of the radionuclides transport. Source term definition involves the inventory of radioactive materials released, the description of physical and chemical forms of release and other release characteristics such as the height of damaged zone of the confinement wall, pressure and temperature of the released gas and aerosols (including potential explosions).

Accident sequences within the reactor building resulting in the release of radioactivity to the environment may involve containment/ confinement failures or may maintain some of the confinement barriers intact. Containments, e.g. of water-cooled reactors, are designed to be nominally leak-tight. However, leak tight means a small leakage rate that stays within specified limits. During a severe accident, increasing containment pressures and leakages (usually specified between 0.25 – 1 volume % per day) may result in radioactive material first being

released to compartments outside the containment, usually in a surrounding building or annulus, and then released to the environment either through a stack (about 100 m high) or directly through other small leakage paths. In the analysis of consequences after an accident with severe core damage, filter efficiencies and natural fission product retention mechanisms (e.g. scrubbing in pools) are usually taken into account but are conservatively neglected in some countries (e.g. Germany).

In some designs with confinements, e.g. for HTGRs, temporary openings will allow a pressure reduction, and therefore, for such designs an accidental release of radioactivity (fission products) into the confinement is expected to be kept very low.

APPENDIX IX
HUMAN FACTOR CONSIDERATION

There are two perspectives of the human factor: On the one side, the operating staff is seen as a valuable resource that is playing an important role in plant operation, testing, maintenance and inspection of the plant, and sometimes compensating deficiencies in automatic systems. On the other side, human intervention has also to be seen as a factor of disturbance and of limited reliability, the consequences of which have to be taken into account in the design of all plant systems and functions, to ensure a sufficient level of safety and availability of the plant.

There are three possible (negative) contributions of human interventions to accident hazards:

- Human errors during plant operation, testing or maintenance, contributing to the failure of safety systems or to their unavailability;
- Human errors during plant operation, testing or maintenance giving rise to an initiating event; and
- Human interventions during incident or accident situations, negatively influencing the sequence of events.

As a common design principle, it has to be ensured that:

- Functions, assigned to the operating staff, constitute consistent tasks and correspond to the abilities and strengths of the operating staff (e.g. appropriate degree of automation, appropriate number of tasks, appropriate sharing among centralized and local operating actions); and that
- The man-systems interface (i.e. control room, screen-based and conventional control means, processing of information to be presented to the operators) optimally supports the tasks of operators and minimizes the potential for a human error.

It is expected that the ability to predict human response to both normal and abnormal situations will improve much over the next decades and will have a major impact on plant design and operation. Simulator technology and the capacity (e.g. speed and memory) of computers are constantly improving and thus will allow more realistic representation (and prediction of development) of transient and accident plant states in expert systems.

An increased use of expert systems (artificial intelligence) and real-time operator aids will lower the burden on operators during normal operation and short-term response to abnormal and accident situations. Although the necessity of human action in plant operation is expected to be minimized for a new reactor, knowledge about human behaviour is nevertheless very important.

The history of human errors by reactor personnel during operation is usually found in documented reactor operating experience; however, similar data from non-nuclear facilities must also be applied with due care to the evaluation of human factors for reactors. The human response to expected and unforeseen situations is investigated in all industries. However, the time available or the complexity of necessary actions may vary, e.g. seconds or minutes for aircraft pilots or hours for the operating personnel of a nuclear power plant. Nevertheless, data of human responses can be exchanged between different industries such as aircraft, space flight and chemical plants. This is also true for human response models. It is, however, difficult to make any generalizations; this is due to the variety of processes and a very limited number of published applications.

Human interventions prior to an event have usually not been found to be among the dominant risk contributors; this is based on observations and assessments of different industrial facilities

[85]. But human (erroneous) interventions after an initiating event in a nuclear reactor represent the greatest challenge. Ref [85] describes relevant research and developmental work in different countries, reviews the applied approaches to human reliability assessments and their limitations, surveys the results of human reliability assessments, and outlines related developments and trends.

Less dependence on operators for normal operation and short-term accident management and the use of expert systems for early diagnosis and real-time operator aids may help to reduce the likelihood of human errors.

Formal human response models need to be used to estimate the likelihood of human errors after an initiating event. These models can either be adapted from other industries or developed specifically for use in the nuclear industry. To further develop confidence in human performance models, the use of simulators needs to be encouraged. Although environmental conditions (especially the human stress factors) in simulator training are not equivalent to real situations, a thorough evaluation of the results can assist model development.

APPENDIX X
SAFETY CULTURE CONSIDERATION

The term ‘safety culture’ was introduced in 1986 by the International Nuclear Safety Advisory Group in a summary report on the post-accident review meeting on the Chernobyl accident [91] and was further elaborated in a report dealing with safety principles for nuclear power plants [92]. In 1991 an additional report from the International Nuclear Safety Advisory Group was published describing the concept of safety culture [93] in more detail. The latter report defined safety culture in the following way:

> “Safety culture is the assembly of characteristics and attitudes in organizations and individuals, which establish that, as an overriding priority, protection and safety issues receive the attention warranted by their significance.”

A similar definition is given by the Advisory Committee on the Safety of Nuclear Installations (ACSNI) [94].

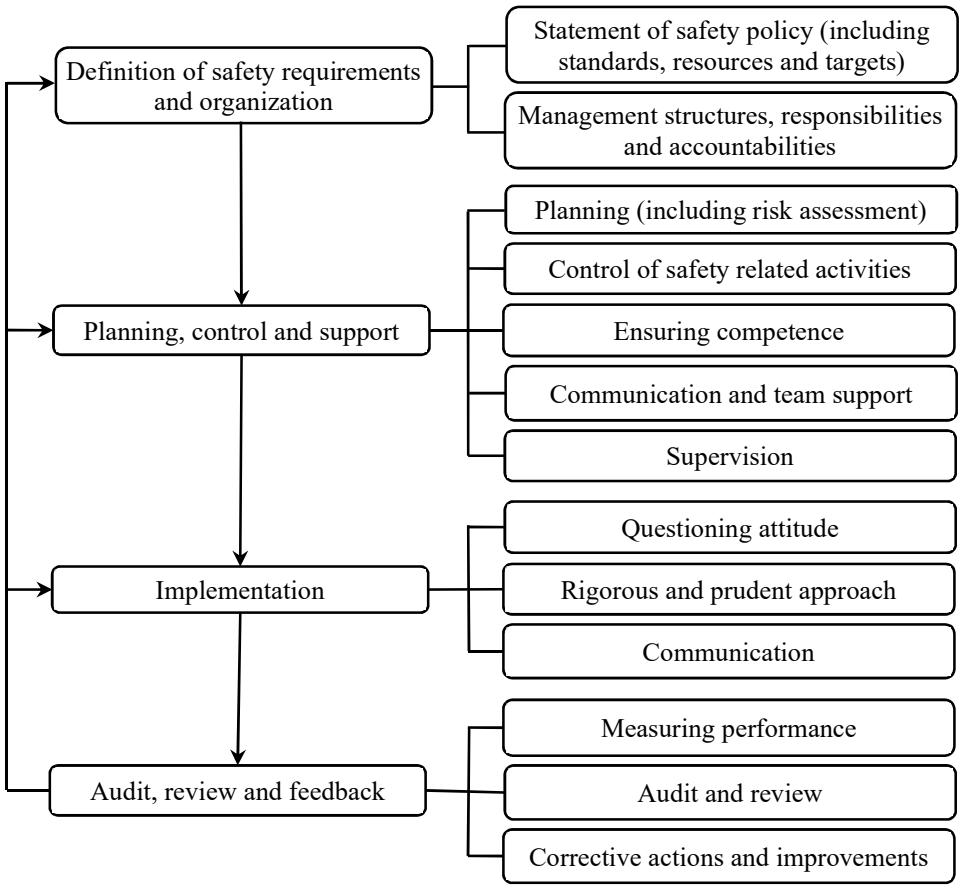

FIG. 5. Components of safety management [35].

This definition emphasizes that safety culture relates to the structure and style of organizations (governmental institutions, owner/operator, and industrial entities) as well as to the habit and attitude of individuals (managers and employees). Safety culture needs a commitment to safety on three levels: policy, management and individual. The policy level requires a clear statement of safety policy, adequate management structures and related resources, and establishment of self-regulation (by regular review). To fulfil their commitments, managers need to clearly define the responsibilities, accountabilities and safety practices for the control of work, ensure that staff are qualified and trained, establish a system of rewards and sanctions, and perform

audits, reviews and benchmarking comparisons. In carrying out their tasks, individuals need to maintain an attentive and questioning attitude, adopt a rigorous and prudent approach, and participate in effective communications (see Figure 5 taken from Ref [35]).

The importance of the management system for safety culture in NPPs has been described in Ref [35], which defines this system as "those arrangements made by the organization for the management of safety in order to promote an adequate safety culture and achieve good safety performance".

Practical recommendations on the implementation of safety culture in a given organization are provided in Refs [95, 96]. Organizations go through a number of stages in developing their safety cultures. These stages are [95]:

- Safety is compliance driven and is based mainly on rules and regulation.
- Good safety performance becomes an organizational goal.
- Safety is seen as a continuing process of improvement to which everyone can and should contribute.

Safety culture is a complex concept (see also Ref [97]) and there is no simple indicator that can be used as a yardstick for determining its status. The multilevel nature of culture, and the tacit nature of some of the levels (basic assumptions), increases the difficulty of measurement. Therefore, to capture both observable behaviour and people's attitudes and basic beliefs, several methods need to be applied including interviews, focus groups, questionnaires, observations and document reviews.

When applying these assessment tools, the key safety culture characteristics and attributes described in Ref [35] can be used for the identification of strengths and weaknesses in an organization's safety culture. Annex 1 of Ref [35] sets out a series of questions for each of the major areas of concern – safety requirements and organization, planning, control and support, etc. – that are helpful in assessing the effectiveness of a safety management system and the status of the safety culture of an organization. Monitoring and measurement of the established and implemented management system effectiveness, self-assessment performance evaluation of management at all levels, independent assessments conducted regularly, management system review, identification of non-conformance and establishment of corrective and preventive actions, and finally identification of improvement opportunities are important elements to consider in assessing whether there is evidence that safety culture prevails.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, INPRO Methodology for Sustainability Assessment of Nuclear Energy Systems: Infrastructure, IAEA Nuclear Energy Series No. NG-T-3.12, Vienna (2014).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual, Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2008).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, INPRO Methodology for Sustainability Assessment of Nuclear Energy Systems: Economics, IAEA Nuclear Energy Series No. NG-T-4.4, IAEA, Vienna (2014).

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, INPRO Methodology for Sustainability Assessment of Nuclear Energy Systems: Environmental Impact from Depletion of Resources, IAEA Nuclear Energy Series No. NG-T-3.13, IAEA, Vienna (2015).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, INPRO Methodology for Sustainability Assessment of Nuclear Energy Systems: Environmental Impact of Stressors, IAEA Nuclear Energy Series No. NG-T-3.15, IAEA, Vienna (2016).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, INPRO Methodology for Sustainability Assessment of Nuclear Energy Systems: Waste Management, IAEA-TECDOC (in publication), IAEA, Vienna (2017).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Cooled Reactor Designs - 2004, IAEA-TECDOC-1391, Vienna (2004).

[8] OECD INTERNATIONAL ENERGY AGENCY, OECD NUCLEAR ENERGY AGENCY, INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Nuclear Reactor Development Opportunities for International Cooperation, OECD/IEA, Paris (2002).

[9] UNITED STATES DEPARTMENT OF ENERGY, A Technology Roadmap for Generation IV Nuclear Energy Systems, GIF-002-00, USDOE, Washington (2002).

[10] UNITED NATIONS, Our Common Future (Report to the General Assembly), World Commission on Environment and Development, UN, New York (1987).

[11] CHOI, Y.S., KIM, J.S., LEE, B.W., Public's perception and judgment on nuclear power, Annals of Nuclear Energy, Volume 27, Issue 4, Elsevier (2000).

[12] SJÖBERG, L., DROTTZ-SJÖBERG, B.M., Knowledge and risk perception among nuclear power plant employees, Risk Analysis, Volume 11, Issue 4, Society for Risk Analysis (1991).

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

[14] CARNINO, A. GASPARINI, M. Defence in depth and development of safety requirements for advanced nuclear reactors, Proceedings of an OECD/NEA Workshop on Advanced Nuclear Safety Issues and Research Needs, Paris, 18 – 20 February (2002).

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

[16] INTERNATIONAL ATOMIC ENERGY AGENCY, INPRO Assessment of the Planned Nuclear Energy System in Belarus, IAEA-TECDOC-1716, IAEA, Vienna (2013).

[17] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safety Glossary, Terminology used in Nuclear Safety and Radiation Protection 2018 Edition, IAEA, Vienna (2018).

[18] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Core for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. NS-G-1.12, IAEA, Vienna (2005).
[19] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations on the Application of the IAEA Safety Requirements for the design of Nuclear Power Plants, IAEA-TECDOC-1791, IAEA, Vienna (2016).
[20] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Margins of Operating Reactors. Analysis of Uncertainties and Implications for Decision Making, IAEA-TECDOC-1332, IAEA, Vienna (2003).
[21] INTERNATIONAL ATOMIC ENERGY AGENCY, Implications of Power Uprates on Safety Margins of Nuclear Power Plants, IAEA-TECDOC-1418, IAEA, Vienna (2004).
[22] INTERNATIONAL ATOMIC ENERGY AGENCY, Seismic Design and Qualification for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. NS-G-1.6, IAEA, Vienna (2003).
[23] INTERNATIONAL ATOMIC ENERGY AGENCY, External Events Excluding Earthquakes in the Design of Nuclear power Plants, IAEA Safety Standards Series, Safety Guide No. NS-G-1.5, IAEA, Vienna (2003).
[24] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Report on Protection against Extreme Earthquakes and Tsunamis in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting Vienna, 4-7 September 2012, IAEA, Vienna (2012).
[25] INTERNATIONAL ATOMIC ENERGY AGENCY, A Methodology to Assess the Safety Vulnerabilities of Nuclear Power Plants against Site Specific Extreme Natural Hazards, International Experts Meeting, 19-22 March 2012, IAEA, Vienna (2012).
[26] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Report on Reactor and Spent Fuel Safety in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, International Experts Meeting, 19-22 March 2012, IAEA, Vienna (2012).
[27] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Report on Preparedness and Response for a Nuclear or Radiological Emergency in the Light of the Accident at the Fukushima Daiichi Nuclear Power Plant, IAEA, Vienna (2013).
[28] INTERNATIONAL ATOMIC ENERGY AGENCY, Mission Report, The Great East Japan Earthquake Expert Mission, IAEA International Fact Finding Expert Mission of the Fukushima Daiichi NPP Accident following the Greta East Japan Earthquake and Tsunami, 24 may – 2 June 2011, IAEA, Vienna (2011).
[29] INTERNATIONAL ATOMIC ENERGY AGENCY, Leadership and Management for Safety, IAEA Safety Standards, General Safety Requirements No. GSR Part 2, Vienna (2016).
[30] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the Management System for Facilities and Activities, IAEA Safety Standards Series, Safety Guide No. GS-G-3.1, Vienna (2006).
[31] INTERNATIONAL ATOMIC ENERGY AGENCY, The Management System for Nuclear Installations, IAEA Safety Standards, Safety Guide No. GS-G-3.5, IAEA, Vienna (2009).
[32] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Standards Series, Safety Guide No. NS-G-2.2, IAEA, Vienna (2000).
[33] INTERNATIONAL ATOMIC ENERGY AGENCY, Ageing Management and Development of a Programme for Long Term Operation of Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide No. SSG-48, IAEA, Vienna (2018).

[34] INTERNATIONAL ATOMIC ENERGY AGENCY, Modifications to Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. NS-G-2.3, IAEA, Vienna (2001).
[35] INTERNATIONAL ATOMIC ENERGY AGENCY, INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Management of Operational Safety in Nuclear Power Plants, INSAG-13, INSAG Series No. 13, IAEA, Vienna (1999).
[36] INTERNATIONAL ATOMIC ENERGY AGENCY, Recruitment, Qualification and Training of Personnel for Nuclear Power Plants, Safety Standards Series, Safety Guide No. NS-G-2.8, IAEA, Vienna (2002).
[37] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Commissioning and Operation, IAEA Safety Standards, Specific Safety Requirements No. SSR-2/2 (Rev.1), IAEA, Vienna (2016).
[38] INTERNATIONAL ATOMIC ENERGY AGENCY, IRS Guidelines, Joint IAEA/NEA International Reporting System for Operating Experience, Service Series 19, IAEA, Vienna (2010).
[39] INTERNATIONAL ATOMIC ENERGY AGENCY, Improving the International System for Operating Experience Feedback, A Report by the International Nuclear safety group, INSAG-23, IAEA, Vienna (2008).
[40] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, Safety Standards Series, Safety Guide No. NS-G-2.6, IAEA, Vienna (2002).
[41] NUCLEAR REGULATORY COMMISSION, Reactor Safety Study: An Assessment of Accident Risks in U.S. Commercial Nuclear Power Plants, WASH-1400 (NUREG-75/014), US NRC, Washington (1975).
[42] GESELLSCHAFT FUER REAKTORSICHERHEIT, German Risk Study: Nuclear power Plants, Phase B – A Summary, GRS-74, Munich (1990).
[43] GESELLSCHAFT FUER REAKTORSICHERHEIT, Safety Analysis for Boiling Water Reactors – A Summary, GRS-98, Munich (1993).
[44] NUCLEAR REGULATORY COMMISSION, Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants, NUREG/CR-6928 (INL/EXT-06-11119), US NRC, Washington (2007).
[45] IDAHO NATIONAL LABORATORY, Initiating Event Rates at U.S. Nuclear Power Plants: 1988 – 2015, INL/EXT-16-39534, INL, Idaho Falls (2016).
[46] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection Aspects of Design for Nuclear Power Plants, IAEA Safety Standards, Safety Guide No. NS-G-1.13, IAEA, Vienna (2005).
[47] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiation Protection and safety of Radiation Sources: International Basic Safety Standards, IAEA Safety Standards, General Safety Requirements Part 3, No. GSR Part 3, IAEA, Vienna (2014).
[48] INTERNATIONAL ATOMIC ENERGY AGENCY, Occupational Radiation Protection, IAEA Safety Standards Series, General Safety Guide No. GSG-7, IAEA, Vienna (2018).
[49] WORLD ASSOCIATION OF NUCLEAR OPERATORS, Performance Indicators 2011, WANO, London (2011).
[50] INTERNATIONAL ATOMIC ENERGY AGENCY, Design Features to Achieve Defence in Depth in Small and Medium Sized Reactors, IAEA Nuclear Energy Series, No. NP-T-2.2, IAEA, Vienna (2009).
[51] INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the quality of probabilistic safety assessments (PSA) for applications in nuclear power plants, IAEA-TECDOC-1511, IAEA, Vienna (2006).

[52] INTERNATIONAL ATOMIC ENERGY AGENCY, Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide No. SSG-2, IAEA, Vienna (2010).
[53] UK HEALTH AD SAFETY EXECUTIVE, Generic Design Assessment – New Civil Reactor Build. Step 3 Probabilistic Safety Analysis of the Westinghouse AP1000, Division 6, Assessment Report No. AR 09/017-P, Merseyside, UK. http://www.onr.org.uk/new-reactors/reports/step3-ap1000-probabilistic-safety-analysis-report.pdf
[54] AREVA, UK-EPR. Fundamental Safety Overview. Report, Volume 2: Design and safety. Chapter R: Probabilistic Safety Assessment. http://www.epr-reactor.co.uk/ssmod/liblocal/docs/V3/Volume%202%20-%20Design%20and%20Safety/2.R%20-%20Probabilistic%20Safety%20Assessment/2.R.2%20-%20Level%202%20Probabilistic%20Safety%20Assessment%20(PSA)%20-%20v2.pdf, and http://www.epr-reactor.co.uk/ssmod/liblocal/docs/V3/Volume%202%20-%20Design%20and%20Safety/2.R%20-%20Probabilistic%20Safety%20Assessment/2.R.1%20-%20Level%201%20Probabilistic%20Safety%20Assessment%20-%20v2.pdf
[55] BRETTSCHUH, W. MESETH, J. Design Features, Safety Assessments and Verification of Key Systems, and Economic Advancements for SWR1000, presented at the IAEA Consultancy Meeting on Recent Developments in Evolutionary Reactors (LWR), Vienna, (2004).
[56] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Reactor Containment Systems for Nuclear Power Plants, IAEA Safety Standards, Safety Guide No. NS-G-1.10, IAEA, Vienna (2004).
[57] INTERNATIONAL ATOMIC ENERGY AGENCY, Implementation of Accident Management Programmes in Nuclear Power Programmes, IAEA Safety Reports Series No. 32, IAEA, Vienna (2004).
[58] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. SSG-54, IAEA, Vienna (2019).
[59] OECD NUCLEAR ENERGY AGENCY, Level 2 PSA Methodology and Severe Accident Management, NEA/CSNI/R(97) 11, OECD/GD(97)198, Paris (1997).
[60] US DEPARTMENT OF ENERGY, Human Performance Improvement Handbook. Volume 1: Concepts And Principles, DOE Standard, DOE-HDBK-1028-2009, Washington (2009).
[61] DIPLOMATIC CONFERENCE TO CONSIDER A PROPOSAL BY SWITZERLAND TO AMEND THE CONVENTION ON NUCLEAR SAFETY, Summary Report, CNS/DC/2015/3/Rev.2, IAEA, Vienna, (2015)
[62] INTERNATIONAL ATOMIC ENERGY AGENCY, Preparedness and Response for a Nuclear or Radiological Emergency, IAEA Safety Standards, General Safety Requirements Part 7, No. GSR Part 7, IAEA, Vienna (2015).
[63] OECD NUCLEAR ENERGY AGENCY, Discussion on Implementation of ICRP Recommendations Concerning Reference Levels and Optimization, Radiological Protection NEA/CRPPH/R(2013)2, OECD/NEA, Paris (2013).
[64] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, IAEA, Vienna (1991).
[65] INTERNATIONAL ATOMIC ENERGY AGENCY, Passive Safety Systems and Natural Circulation in Water Cooled Nuclear Power Plants, IAEA-TECDOC-1624, IAEA, Vienna (2009).
[66] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants, IAEA Safety Reports Series No. 46, IAEA, Vienna (2005).
[67] DINSMORE COMEY, D. The Fire at the Brown's Ferry Nuclear Power Station, Friends of the Earth, California (1976), http://www.ccnr.org/browns_ferry.html

[68] INTERNATIONAL ATOMIC ENERGY AGENCY, Basic Safety Principles, 75-INSAG-3 Rev.1, A Report by the International Nuclear Safety Group, INSAG-12, IAEA, Vienna (1999).
[69] UK HEALTH AND SAFETY EXECUTIVE, Development of a business excellence model of safety culture: Safety culture improvement matrix, Entec UK Ltd, UK HSE, London (1999).
[70] INTERNATIONAL ATOMIC ENERCY AGENCY, Maintaining Knowledge, Training and Infrastructure for Research and Development in Nuclear Safety, INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, INSAG-16, IAEA, Vienna (1999).
[71] INTERNATIONAL ATOMIC ENERGY AGENCY, Considerations in the Development of Safety Requirements for Innovative Reactors: Application to Modular High Temperature Gas Cooled Reactors, IAEA-TECDOC-1366, IAEA, Vienna (2003).
[72] INTERNATIONAL ATOMIC ENERGY AGENCY, Format and Content of the Safety Analysis Report for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. GS-G-4.1, IAEA, Vienna (2004).
[73] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide No. SSG-3, IAEA, Vienna (2010).
[74] INTERNATIONAL ATOMIC ENERGY AGENCY, Development and Application of Level 2 Probabilistic Safety Assessment for Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide No. SSG-4, IAEA, Vienna (2010).
[75] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants, IAEA Safety Reports Series No. 23, IAEA, Vienna (2002).
[76] INTERNATIONAL ATOMIC ENERGY AGENCY, The Role of Probabilistic Safety Assessment and Probabilistic Safety Criteria in Nuclear Power Plant Safety, IAEA Safety Series No. 106, Vienna (1992).
[77] INTERNATIONAL ATOMIC ENERGY AGENCY, Periodic Safety Review for Nuclear Power Plants, IAEA Safety Standards, Specific Safety Guide No. SSG-25, IAEA, Vienna (2013).
[78] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk informed regulation of nuclear facilities: Overview of the current status, IAEA-TECDOC-1336, IAEA, Vienna (2005).
[79] SOUSA, A.L. et al, The Role of Risk Informed Decision Making in the Licensing of Nuclear Power Plants, Academy Publish, Publishing Services LLC, USA, Wyoming (2012).
[80] INTERNATIONAL ATOMIC ENERGY AGENCY, A Framework for an Integrated Risk Informed Decision Making Process, A report by the International Nuclear Safety Group, INSAG-25, IAEA, Vienna (2011).
[81] NUCLEAR REGULATORY COMMISSION, Guidance on the Treatment of Uncertainties Associated with PRAs in Risk Informed Decision Making, NUREG-1855 Volume 1, US NRC, Washington (2009).
[82] ELECTRIC POWER RESEARCH INSTITUTE, Risk Informed Regulation: Potential Application to Advanced Nuclear Plants, EPRI, Palo Alto, CA:2000, TP-114441, Palo Alto (2000).
[83] OECD NUCLEAR ENERGY AGENCY, Probabilistic Risk Criteria and safety Goals, NEA/CSNI/R(2009)16, NEA, Paris (2009).
[84] GROUPE PERMANENT CHARGÉ DES RÉACTEURS NUCLÉAIRES, Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, Autorité de Sureté Nucléaire (ASN), Paris (2001).
[85] OECD NUCLEAR ENERGY AGENCY, Critical Operation Actions – Human Reliability Modelling and Data Issues, NEA/CSNI/R(98) 1, OECD, Paris (1998).

[86] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series, Safety Guide No. SSG-39, IAEA, Vienna (2016).
[87] INTERNATIONAL ATOMIC ENERGY AGENCY, Current Status and Future Development of Modular High Temperature Gas Cooled Reactor Technology, IAEA-TECDOC-1198, Vienna (2001).
[88] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends, IAEA-TECDOC-1451, IAEA, Vienna (2005).
[89] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION, The 2007 Recommendations of the International Commission on Radiological Protection, ICRP Publication 103. Annals of the ICRP 37 (2-4). Ottawa (2007).
[90] INTERNATIONAL ATOMIC ENERGY AGENCY, Prospective Radiological Environmental Impact Assessment for Facilities and Activities, IAEA Safety Standards Series No. GSG-10, IAEA, Vienna (2018)
[91] INTERNATIONAL ATOMIC ENERCY AGENCY, Summary report on the post-accident review meeting on the Chernobyl accident, IAEA Safety Series No.75-INSAG-1, IAEA, Vienna (1986).
[92] INTERNATIONAL ATOMIC ENERCY AGENCY, Basic safety principles for nuclear power plants, A report by the INTERNATIONAL SAFETY NUCLEAR ADVISORY GROUP, INSAG-3, IAEA Safety Series No.75, IAEA, Vienna (1988).
[93] INTERNATIONAL ATOMIC ENERCY AGENCY, Safety culture, A report by the INTERNATIONAL SAFETY NUCLEAR ADVISORY GROUP, INSAG-4, IAEA Safety Series No. 75, IAEA, Vienna (1991).
[94] UK HEALTH AND SAFETY EXECUTIVE, ACSNI study group on human factors, third report, organizing for safety, HSE Books, ISBN 0118821040, UK London (1993).
[95] INTERNATIONAL ATOMIC ENERGY AGENCY, Developing safety culture in nuclear activities: Practical suggestions to assist progress, Safety Reports Series No. 11, IAEA, Vienna (1998).
[96] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Key practical Issues in Strengthening Safety Culture, INSAG-15, INSAG Series No. 15, IAEA, Vienna (2002).
[97] INTERNATIONAL ATOMIC ENERCY AGENCY, Safety Culture in Nuclear Installations, Guidance for Use in the Enhancement of Safety Culture, IAEA-TECDOC-1329, IAEA, Vienna (2002).

GLOSSARY

In this publication the safety related terms are used as they defined in the IAEA Safety Glossary [15].

assessment (INPRO assessment of NES sustainability): An assessment using the INPRO methodology is a process of making a judgment about the long term sustainability of a nuclear energy system. In principle, analyses using analytical tools are not part of an INPRO assessment but could provide necessary input for the assessment. The assessment of a nuclear energy system is done at the criterion level of the INPRO methodology. In the case of a numerical criterion, the assessment process consists of comparing the value of an indicator with the value of the acceptance limit of a criterion. In the case of a logical criterion – mostly phrased in the form of a question – the assessment is done by answering the question raised.

assessor: The INPRO assessor is an expert or a team of experts applying the INPRO methodology in a nuclear energy system assessment. The assessor is typically a member of the academic society of the host country (e.g. an academy of science). The assessor may also be from a nuclear research centre, a utility, a supplier, or an organization of the regulator.

basic principle: As defined in the INPRO methodology, an INPRO basic principle is a statement of a general goal that has to be achieved in order to make a nuclear energy system sustainable in the long term. It therefore provides a basic impetus for the development of necessary capabilities and design features.

closed fuel cycle: This is a nuclear fuel cycle that recycles spent fuel. An example of a partly closed fuel cycle is one where spent uranium fuel is reprocessed to (mono) recycle the fuel's bred plutonium for use in producing mixed oxide (MOX) fuel. A completely closed fuel cycle is foreseen in proposed nuclear energy systems where fast breeder reactors would continuously recycle all of their spent fuel.

construction: in the framework of this publication, this is a process of erection, installation, and related tests and inspections of the NPP buildings and systems.

criterion: As defined in the INPRO methodology, an INPRO criterion enables the assessor to determine whether and how well a user requirement for sustainability assessment is being met by a given nuclear energy system. A criterion consists of an indicator (IN) and an acceptance limit (AL). INs may be based on a single parameter, on an aggregate variable, or on a status statement. ALs may be international or national regulatory limits or limits defined by the INPRO methodology. Two types of criteria are distinguished: numerical and logical. A numerical criterion has an IN and AL that is based on a measured or calculated value that reflects a property of a NES. A logical criterion is associated with some important feature of (or measure for) a NES and is usually presented in the form of a question that has to be answered positively. Some criteria have associated evaluation parameters that serve to simplify the assessment process.

evaluation parameter: The INPRO methodology uses evaluation parameters to assist the INPRO assessor in determining whether a criterion has been met. In some cases, these evaluation parameters have their own acceptance limits, in which case they may also be called sub-indicators.

event: In the context of the reporting and analysis of events, an event is any occurrence unintended by the operator, including operating error, equipment failure or other mishap, and

deliberate action on the part of others, the consequences or potential consequences of which are not negligible from the point of view of protection or safety.

internal event: An event that originates inside the plant and potentially affects the safety of the plant. Typical examples of internal events are failures of equipment.

external event: see definition in Ref [15].

evolutionary design: A reactor design that achieves improvements over previous designs through small to moderate modifications, with a strong emphasis on maintaining design features that are proven to minimize technological risks. Examples of evolutionary reactors are Generation III or Generation III+ reactors.

innovative design: This is an advanced nuclear installation design that incorporates radical conceptual changes in design approaches or system configuration in comparison with existing practice. These reactors may comprise not only electricity generating plants but include also plants (of various size and capacity) for other applications, such as high-temperature heat production, district heating and sea water desalination, to be deployed in developed regions as well as in developing countries and countries in transition. Examples of innovative reactors are Generation IV reactors.

nuclear energy system (NES): A NES comprises the complete spectrum of nuclear facilities and associated legal and institutional measures (infrastructure). Nuclear facilities include nuclear reactor facilities as well as facilities for mining and milling, refining, conversion and enrichment of uranium, manufacturing of nuclear fuel, reprocessing of nuclear fuel (if a closed nuclear fuel cycle is used), and facilities for related materials management activities, including transportation and waste management (storage and disposal). Legal measures consist of the national nuclear law and international agreements, treaties, and conventions. Institutional measures include the corresponding national institutions such as regulatory bodies.

open fuel cycle: This is a nuclear fuel cycle that defines spent fuel as waste to be disposed of. It is also called a once through fuel cycle.

reference reactor: Within this publication, a reference reactor (or design) is a reactor of the latest design operating in 2013. The reference reactor should preferably be from the same designer and use the same reactor technology as the assessed design. It should also comply with the current safety standards. This reference design is to be compared in the INPRO assessment to the assessed reactor (assumed to be installed after 2013). For innovative reactors that may have no operating prototypes in 2013, the latest design that has been safely operated, or at least licensed, can be used as the reference design. Note that 2013 was the date selected at the beginning of the latest methodology update. This date should be revised periodically along with the rest of methodology.

sustainability: In the INPRO methodology, sustainability is defined as the ability of a nuclear energy system to operate until at least the end of the twenty-first century.

user requirement: A user requirement defines what should be done to meet the target/goal of an INPRO methodology basic principle. It is directed at specific institutions (users) involved in nuclear power development, deployment and operation, i.e. the developers/designers, government agencies, facility operators, and support industries.

LIST OF ABBREVIATIONS

AL	acceptance limit (INPRO)
AM	accident management
AOO	anticipated operational occurrence
AP1000	advanced PWR (Westinghouse)
ATWS	anticipated transient without scram
BP	basic principle (INPRO)
BWR	boiling water reactor
CANDU	Canada deuterium-uranium reactor
CCF	common cause failure
CR	criterion (INPRO)
DBA	design basis accident
DBEE	design basis external event
DID	defence in depth
EPR	Evolutionary power reactor (pressurised water reactor)
GIF	Generation IV International Forum
HF	human factor
HTGR	high temperature gas reactor
HWR	heavy water reactor
I&C	instrumentation and control
IN	indicator (INPRO)
INPRO	International Project on Innovative Nuclear Reactors and Fuel Cycles
LOCA	loss of coolant accident
LWR	light water reactor
NPP	nuclear power plant
PIRT	phenomena identification and ranking table
PSA	probabilistic safety assessment
PWR	pressurized water reactor
RD&D	research, development and demonstration
RPV	reactor pressure vessel
UR	user requirement (INPRO)
WWER	water cooled water moderated power reactor (pressurized water reactor of Russian design)

CONTRIBUTORS TO DRAFTING AND REVIEW

Akhtar, S.	Pakistan Atomic Energy Commission
Boyle, S.	Candu Energy, Canada
Bykov, M.	Rosatom, Russian Federation
Carlson, D.	International Atomic Energy Agency
Depisch, F.	Consultant (Germany)
Drace, Z.	International Atomic Energy Agency
Fomichenko, P.	Kurchatov Institute, Russian Federation
Fujii, S.	Mitsubishi Heavy Industries, Japan
Grudev, P.	INRNE, Bulgaria
Khartabil, H.	International Atomic Energy Agency
Kolchinskiy, D.	Rosatom, Russian Federation
Korinny, A.	International Atomic Energy Agency
Korobeinikov, V.	IPPE, Russian Federation
Kuznetsov, V.	International Atomic Energy Agency
Maheshvari, N.	BARC, India
Nitoi, M.	Institute for Nuclear Research, Romania
Nugroho, D.	BAPETEN, Indonesia
Okano, Y.	JAEA, Japan
Phillips, J.	International Atomic Energy Agency
Rakitskaya, T.	Rosatom, Russian Federation
Sargsyan, V.	Scientific Research Institute of Energy, Armenia
Tjahjono, H.	BATAN, Indonesia
Yang, P.	CIAE, China

Technical Meetings

Vienna, Austria: 19-22 November 2013 and 15-17 November 2016.

Consultants Meeting

Vienna, Austria: 21-23 November 2012.

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/publications

20-00101

International Atomic Energy Agency
Vienna
ISBN 978–92–0–102720–7
ISSN 1011–4289