

IAEA-TECDOC-1575 Rev. 1

***Guidance for the Application
of an Assessment Methodology
for Innovative Nuclear Energy Systems***

***INPRO Manual —
Safety of Nuclear Reactors***

*Volume 8 of the
Final Report of Phase 1 of the International Project on Innovative
Nuclear Reactors and Fuel Cycles (INPRO)*



IAEA

International Atomic Energy Agency

November 2008

The originating Section of this publication in the IAEA was:

Nuclear Power Technology Development Section
International Atomic Energy Agency
Wagramer Strasse 5
P.O. Box 100
A-1400 Vienna, Austria

GUIDANCE FOR THE APPLICATION OF AN ASSESSMENT METHODOLOGY
FOR INNOVATIVE NUCLEAR ENERGY SYSTEMS
INPRO MANUAL — SAFETY OF NUCLEAR REACTORS

VOLUME 8

IAEA, VIENNA, 2008
IAEA-TECDOC-1575 Rev. 1
ISBN 978-92-0-100509-0
ISSN 1011-4289

© IAEA, 2008

Printed by the IAEA in Austria
November 2008

FOREWORD

The International Project on Innovative Nuclear Reactors and Fuel Cycles (INPRO) was launched in the year 2000, based on resolutions of the IAEA General Conference (GC(44)/RES/21). INPRO intends to help to ensure that nuclear energy is available in the 21st century in a sustainable manner, and seeks to bring together all interested Member States, both technology holders and technology users, to consider, jointly, actions to achieve desired innovations.

INPRO is proceeding in steps. In its first step, referred to as Phase 1A, INPRO developed a set of basic principles, user requirements and criteria together with an assessment method, which taken together, comprise the INPRO methodology, for the evaluation of innovative nuclear energy systems (INS). The results of Phase 1A were documented in IAEA-TECDOC-1362, published in June 2003.

In its second step, referred to as Phase 1B (first part), Member States and individual experts performed 14 case studies with the objective of testing and validating the INPRO methodology. Based on the feedback from these case studies and numerous consultancies the INPRO methodology was revised, as documented in IAEA-TECDOC-1434, published in December 2004.

In its third step, referred to as Phase 1B (second part), INPRO was requested to provide additional guidance in using the INPRO methodology to assess the sustainability of an INS in the form of an INPRO assessment manual. The resulting INPRO manual is comprised of an overview volume (No. 1), and eight additional volumes covering the areas of economics (Volume 2), infrastructure (Volume 3), waste management (Volume 4), proliferation resistance (Volume 5), physical protection (Volume 6), environment (Volume 7), safety of nuclear reactors (laid out in this volume), and safety of nuclear fuel cycle facilities (Volume 9).

The report on the safety of nuclear reactors was drafted by E.F. Hicken (Germany), within the framework of INPRO, based on a special service agreement with the IAEA. The draft report was reviewed in consultancy meetings held at the IAEA's headquarters in Vienna in 2005. The comments and recommendations and various amendments proposed by the consultants were implemented in this report.

The IAEA highly appreciates the contributions made by the INPRO international coordinating group (ICG) members and the participants of the consultancies, and the valuable guidance and advice provided by the Steering Committee. The IAEA would also like to express its thanks to F. Depisch (Germany) for editing the manuscript.

Phase 1B (second part), of the INPRO project was implemented under the IAEA Project Manager Y.A. Sokolov and the Project Coordinators, A. Omoto, A. Rao, J. Kupitz, I. Facer, and T. Ganguly of the Department of Nuclear Energy. As of August 2008, INPRO has 29 Member States (and the EC) supporting the project.

Based on a decision of the 9th INPRO steering committee in July 2006, INPRO has entered into Phase 2. This phase has three main directions of activity: methodology improvement, infrastructure/ institutional aspects and collaborative projects. The ongoing and future activities of INPRO are expected to lead to further improvements in the INPRO methodology, based on the feedback received from Member States in light of their experience in applying the methodology.

EDITORIAL NOTE

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

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

CONTENTS

CHAPTER 1	INTRODUCTION	1
1.1.	INPRO assessment method	1
1.2.	General goals of the manual.....	1
1.3.	Existing requirements	2
1.4.	Future requirements	3
1.5.	Reactor safety requirements defined in the IAEA Safety Standards	3
1.5.1.	IAEA Fundamental Safety Objective	4
1.5.2.	IAEA Safety Principles.....	4
1.5.3.	High level safety requirements	5
1.6.	Derivation of the INPRO basic design principles for safety.....	7
1.7.	Outline of the report.....	10
CHAPTER 2	NECESSARY INPUT FOR AN INPRO ASSESSMENT	21
2.1.	Definition of INS	21
2.2.	Design information	21
2.3.	Results of safety analyses	21
2.4.	Timing of the INPRO assessment.....	21
CHAPTER 3	BASIC PRINCIPLES, USER REQUIREMENTS AND CRITERIA.....	23
3.1.	INPRO basic principles for safety	23
3.2.	INPRO basic principle BP1 (Defence in depth)	24
3.2.1.	User requirement UR1.1 (robustness).....	24
3.2.2.	User requirement UR1.2 (detection and interception).....	35
3.2.3.	User requirement UR1.3 (design basis accidents).....	40
3.2.4.	User requirement UR1.4 (release into containment)	49
3.2.5.	User requirement UR1.5 (release into environment).....	53
3.2.6.	User requirement UR1.6 (independence of DID levels).....	57
3.2.7.	User Requirement UR1.7 (human machine interface).....	59
3.2.8.	Integration of safety, security and proliferation resistance into the INS design.....	62
3.3.	INPRO basic principle BP2 (inherent safety)	62
3.3.1.	User requirement UR2.1 (minimization of hazards).....	62
3.4.	INPRO basic principle BP3 (risk of radiation)	66
3.4.1.	User requirement UR3.1 (dose to workers).....	67
3.4.2.	User Requirement UR3.2 (dose to public).....	69
3.5.	INPRO basic principle BP4 (RD&D)	70
3.5.1.	User requirement UR4.1 (safety basis).....	71
3.5.2.	User requirement UR4.2 (RD&D for understanding).....	72
3.5.3.	User Requirement UR4.3 (pilot plant).....	76
3.5.4.	User requirement UR4.4 (safety analyses)	77
3.6.	Concluding remarks	80
CHAPTER 4	EXAMPLE FOR AN INPRO SAFETY ASSESSMENT OF A NUCLEAR REACTOR.....	81
4.1.	INPRO basic principle BP1 (Defence in depth)	81
4.1.1.	User requirement UR1.1 robustness	81
4.1.2.	User Requirement UR1.2 detection and interception	86
4.1.3.	User Requirement UR1.3 DBA	87

4.1.4.	User Requirement UR1.4 release into containment.....	89
4.1.5.	User requirement UR1.5 release into environment.....	91
4.1.6.	User requirement UR1.6 independence of DID levels	92
4.1.7.	User requirement UR1.7 human machine interface.....	92
4.2	INPRO Basic Principle BP2 (Inherent safety).....	93
4.2.1.	User requirement UR2.1 minimization of hazards	93
4.3.	INPRO basic principle BP3 (Risk of radiation).....	94
4.3.1.	User requirement UR3.1 radiation protection of workers	94
4.3.2.	User requirement UR3.2 radiation protection of the public	94
4.4.	INPRO basic principle BP4 (RD&D	94
4.4.2.	User requirement UR4.2 RD&D.....	95
4.4.3.	User requirement UR4.3 pilot plant.....	97
4.4.4.	User requirement UR4.4 risk and uncertainties.....	98
ANNEX A:	INNOVATIVE BWR DESIGN SWR 1000	99
ANNEX B:	OPERATING BWR PLANT GUNDREMMINGEN UNIT B AND C	111
ANNEX C:	AREAS OF SAFETY RD&D.....	116
ANNEX D:	IDEAS OF FUTURE DEVELOPMENT OF THE INPRO METHODOLOGY IN THE AREA OF SAFETY	118
ANNEX E:	CHECKLIST FOR ASSESSMENT	120
REFERENCES	141
ABBREVIATIONS.....	145
CONTRIBUTORS TO DRAFTING AND REVIEW	147

CHAPTER 1

INTRODUCTION

This document elaborates on the guidance given in the INPRO report “Methodology for the assessment of innovative nuclear reactors and fuel cycles,” IAEA-TECDOC-1434 (2004), Ref. [2], and the previous INPRO report “Guidance for the evaluation for innovative nuclear reactors and fuel cycles,” IAEA-TECDOC-1362 (2003), Ref. [1], in the area of safety of nuclear reactors.

The information presented in Volume 1 of the INPRO manual (Ref. [3]), should be considered to be an integral part of this volume and the assessor should be familiar with that information before using this volume of the INPRO manual. Knowledge and understanding of the IAEA Safety Standard series is also a pre-requisite for the INPRO assessor performing an INPRO assessment in the area of safety.

This document discusses INPRO assessment methods for nuclear reactors. INPRO assessment methods for nuclear fuel cycle facilities are discussed in Volume 9 of the INPRO manual (Ref [9]).

1.1. INPRO assessment method

As noted in Chapter 4 of Volume 1 of the INPRO manual (Ref. [3]), the INPRO method of assessment is a bottom-up exercise. Basic principles, user requirements and criteria have been defined in different areas – economics, infrastructure, waste management, proliferation resistance, physical protection, environment, and safety. For each of the criteria, indicators and acceptance limits have been defined. The starting point for the INPRO basic principles in the area of safety is the current IAEA Safety Standards.

The INPRO assessment process consists of determining the value of each of the INPRO indicators and comparing this value with the corresponding acceptance limit of the given criterion. Based on the comparison, a judgment on the potential, i.e. the capability, of the INS to comply with the criterion is arrived at. The ultimate goal of the application of the INPRO method is to confirm that the INS assessed fulfils all the INPRO criteria and hence the INPRO user requirements and basic principles and therefore represents a sustainable energy supply system for a Member State (or group of Member States). The INPRO requirements in the area of safety are set out in Table 1.2 to 1.5.

The INPRO method also offers the possibility to compare different INS (or different designs of a component thereof). When making a comparative assessment the uncertainty of the judgment arrived at in the assessment also needs to be specified, taking into account the maturity of the INS. If desired, the set of judgments can be aggregated. Additionally, one possible output from an INS assessment is the identification of areas where a given INS needs to be improved. Given the comprehensive nature on an INPRO assessment, such an assessment would be expected to indicate clearly the specific attributes of an INS that need to be improved, and so, would be an important input to identifying necessary or desirable RD&D objectives.

1.2. General goals of the manual

The goal of this volume of the INPRO manual is to provide guidance to the assessor of the safety of a nuclear reactor in a country or region (or even on a global scale) that is planning to install a nuclear power program (or maintaining or enlarging an existing one), how to apply the INPRO methodology in this specific area.

The INPRO assessor is assumed to be knowledgeable in the area of nuclear safety or is using the support of qualified organizations (e.g., IAEA, OECD-NEA) with relevant experience.

The INPRO assessment should either confirm that the INPRO safety requirements are fulfilled by the designer (or developer) of an innovative nuclear energy system (INS), or define the gaps in the design to be closed by corresponding RD&D.

As will be shown in the discussion of the INPRO basic design principle(s) for safety, the derived user requirements and criteria, INPRO encourages the introduction of innovation that enhances the safety of nuclear reactors.

As stated in Ref. [3] basic principles, user requirements and criteria for the safety of innovative nuclear energy systems (INS) have been established in INPRO taking into account the large body of work that already exists dealing with the safety of reactors operating today, and previous work on establishing requirements for next generation reactors.

One of the basic assumptions of INPRO is the expectation that to fulfill the needs of sustainable energy supply within the next 50 years and beyond, the number of nuclear energy systems (NES) in operation will have to be increased considerably compared to the situation today. Keeping the safety level of the newly deployed NES at the same level as the 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 innovative nuclear energy systems, based, in part, on lessons learned from systems in operation.

1.3. Existing requirements

The IAEA has updated documents that define the elements necessary to ensure the safety of nuclear power plants (e.g., Refs [4] and [5]). On the national level, various utility groups have developed corresponding User (or Utility) Requirements Documents supported by experience from construction, licensing and operation of nuclear power plants over the past four decades (representing over 10.000 reactor-operating years).

Such documents have been prepared for evolutionary and innovative designs 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). They were authored largely by electricity-generating utilities and arose from well-characterized reactor designs, reflected operating experience and formed the basis for the development of modern designs.

In 2004 the IAEA [6] presented an overview of these utility documents. A summary of the essence of these requirements 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 the number of safety challenges;
- Improved automation and man-machine 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;
- Core damage frequency less than 10^{-5} per reactor-year and cumulative frequency of large releases 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 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 EUR 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 ground area.

1.4. Future requirements

As mentioned before, the scope of the INPRO project covers nuclear reactors expected to come into service in the next 50 years and beyond, together with the associated fuel cycles. It is recognized that a mixture of existing¹, evolutionary, and innovative designs will be brought into service and co-exist within this period. The ‘Three Agency Study’ [7] provides an overview of trends in the development of INS. The range of reactor systems having innovative design features includes water-cooled, gas-cooled, liquid metal-cooled systems and molten salt reactors of various sizes to be used for various purposes.

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

User requirements are well established for existing nuclear power reactors. A vendor of a given reactor design is expected to meet all user 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 applies user requirements for INS to reactors; fuel cycle facilities are treated in a separate report called INPRO manual for safety of nuclear fuel cycle facilities [8]. The requirements are intended to be as generic as possible; where they cannot be made fully generic, it is so noted.

The scope of this report includes the safety of reactors; it extends to primary spent fuel storage at reactor sites but excludes extended fuel storage and waste management, addressed in another volume, called INPRO manual for waste management [9]. Legal aspects of safety and the concept of safety culture are dealt with in another report, called INPRO manual for infrastructure [10].

1.5. Reactor safety requirements defined in the IAEA Safety Standards

The starting point for the INPRO Basic Design Principles for Safety, the User Requirements and the Criteria defined for the assessment of the safety of innovative nuclear power plants is the current IAEA Safety Standards. The applicable standards are: the Fundamental Safety

¹The term “existing” will be used in this report consistently to refer to the most modern commercially available designs and operating plants as of 2004.

Principles [11], the requirements for the Safety Assessment for Facilities and Activities² and the requirements for the Safety of Nuclear Power Plants – Design [5]. These Safety Standards are applicable to existing, new and innovative designs of nuclear power plants.

1.5.1. IAEA Fundamental Safety Objective

The Fundamental Safety Objective given in the Safety Fundamentals [11] is to “**protect people and the environment from harmful effects of ionizing radiation**”. This is applicable to innovative nuclear reactors and needs to be achieved without unduly limiting the operation of the plant. This objective applies for all stages in the lifetime of the plant from planning through normal operation up to decommissioning and closure.

To meet this Fundamental Safety Objective and achieve the highest standards of safety that can reasonably be achieved the Safety Fundamentals state that measures have to be taken to:

- (a) Control the radiation exposure of people and the release of radioactive material to the environment;
- (b) Restrict the likelihood of events that might lead to a loss of control over the nuclear reactor core and any other source of radioactive material associated with the nuclear reactor; and
- (c) Mitigate the consequences of such events if they were to occur.

1.5.2. IAEA Safety Principles³

The Safety Fundamentals [11] sets out ten Safety Principles that need to be addressed to meet the Fundamental Safety Objective. Six of them are directly applicable to the INPRO assessment of the safety of an innovative nuclear reactor:

- **IAEA Safety Principle 3: Leadership and management for safety:** Effective leadership and management for safety must be established and sustained in organizations concerned with, and facilities and activities that give rise to, radiation risks.
- **IAEA Safety Principle 5: Optimization of protection:** Protection must be optimised to provide the highest level of safety that can reasonably be achieved.
- **IAEA Safety Principle 6: Limitation of risks to individuals:** Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.
- **IAEA Safety Principle 7: Protection of present and future generations:** People and the environment, present and future, must be protected against radiation risks.
- **IAEA Safety Principle 8: Prevention of accidents:** All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.
- **IAEA Safety Principle 9: Emergency preparedness and response:** Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents.

The lower level requirements relating to these Fundamental Safety Principles are given in the Safety Series documents on Safety Assessment and Verification and on the Safety of Nuclear Power Plants – Design [5].

² At the time of publication of this document, the draft Safety Requirements document “Safety Assessment for Facilities and Activities” was being submitted to the Commission of Safety Standards after having been approved by the Committees.

³ A distinction is made between the IAEA safety principles which are defined in the IAEA Safety Fundamentals [11] and the INPRO Basic Design Principles for Safety which have been derived from the IAEA Safety Fundamentals but are specific to the INPRO assessment of the safety of an innovative nuclear reactor.

1.5.3. High level safety requirements

The IAEA Safety Fundamentals and requirements present a number of high level safety requirements. These are requirements that must be met to ensure that a high level of safety is achieved for any nuclear facility or activity. These include the provision of *defence-in-depth* and performing the required safety functions for a nuclear reactor.

Defence-in-depth

Defence-in-depth provides an overall strategy for safety measures and features of nuclear installations (Refs [12] and [13]). The strategy is twofold: first, to prevent accidents and, second, if prevention fails to limit 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 operating 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 conditions. Thus, preventing the degradation of plant status and performance generally will provide the most effective protection of the public and the environment. *For INS, the objective of INPRO is that the effectiveness of preventive measures should be enhanced compared to existing designs and installations.*

Typically defence-in-depth is characterized by five levels of protection, shown in Table 1 and discussed below, with the top level being prevention, and the remaining four levels representing the response to increasing challenges to the plant and to public safety.

Ensuring the independence of the different levels of protection in the defence-in-depth strategy is a key element to avoid the propagation of failure into subsequent levels. In existing reactors, an accident could challenge several levels of defence-in-depth simultaneously. *For an INS, the objective of INPRO is that this is accomplished in part and for some concepts, by more extensive use of inherent characteristics, through more use of passive systems and through greater separation of redundant systems compared to existing designs and installations.*

An increased use of inherent safety characteristics will strengthen accident prevention in innovative nuclear installations. A plant has an inherently safe characteristic against a potential hazard if the hazard is rendered physically impossible. An inherent safety characteristic is 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.

In assessing safety, the scope of the safety assessment should be holistic, covering the effects on people and on the environment (considered in another volume of the INPRO manual, called environment [14]) of the entire integrated fuel cycle. This ensures that an improvement in safety in one area or component of the fuel cycle is not negated by a decrease in safety in another area.

INPRO has developed general directions for innovation to enhance defence-in-depth relative to existing plants and designs. These are presented in Table 1.1. The end point should be the prevention, reduction and containment of radioactive releases to make the health and

environmental risk of innovative nuclear reactor comparable to that of industrial facilities used for similar purposes so that for innovative nuclear reactor there will be no need for relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility.

Table 1.1. INPRO innovations in application of defence-in-depth (DID)

DID Level	INSAG Objectives (see Ref. [12])	Innovation Direction (INPRO)	
1	Prevention of abnormal occurrences and accidents	Enhance prevention by increased emphasis on inherently safe design characteristics and passive safety features, and by further reducing human actions in the routine operation of the plant.	More independence of levels from each other
2	Control of abnormal operation and detection of failures.	Give priority to advanced control and monitoring systems with enhanced reliability, intelligence and the ability to anticipate and compensate abnormal transients.	
3	Control of accidents within the design basis.	Achieve fundamental safety functions by optimized combination of active & passive design features; limit consequences such as fuel failures; minimize reliance on human intervention by increasing grace period, e.g., between several hours and several days.	
4	Control of severe plant conditions, including prevention and mitigation of the consequences of severe accidents.	Increase reliability and capability of systems to control and monitor complex accident sequences; decrease expected frequency of severe plant conditions; e.g., for reactors, reduce severe core damage frequency by at least one order of magnitude relative to existing plants and designs, and even more for urban-sited facilities.	
5	Mitigation of radiological consequences of significant releases of radioactive materials.	Avoid the necessity for evacuation or relocation measures outside the plant site.	

Safety functions

The fundamental safety functions that need to be carried out for any nuclear reactor are:

- control of the reactivity;
- removal of heat from the core; and
- confinement of radioactive materials and shielding of radiation.

For irradiated fuel storage on a nuclear reactor site, the fundamental safety functions are:

- control of the sub-criticality and chemistry;
- removal of decay heat from radio-nuclides; and
- confinement of radioactivity and shielding of radiation.

To ensure that the fundamental safety functions are adequately fulfilled, an effective defence-in-depth strategy should be implemented which, for an innovative nuclear reactor, INPRO

would expect to include an increased use of inherent safety characteristics and passive systems in nuclear designs compared to existing designs and installations.

1.6. Derivation of the INPRO basic design principles for safety

The IAEA Safety Principles and Requirements given in the above mentioned Safety Series publications are used as the basis for defining the INPRO basic design principles used as the starting point for the INPRO process for assessing the safety of innovative nuclear reactors. The way this has been done is described below.

Safety Principle 8: Prevention of accidents: “All practical efforts must be made to prevent and mitigate nuclear or radiation accidents.”

For an innovative nuclear reactor, the most harmful consequences would arise from the loss of control of the nuclear reactor core, from irradiated fuel or radioactive waste. This requires that measures are taken to prevent the occurrence of abnormal or accident conditions (including breaches of security) that could lead to such a loss of control, and prevent them from escalating further.

This is the Technical Safety Objective given in [5] which requires that all reasonably practicable measures are taken to prevent accidents and to mitigate their consequences should they occur. The aim is to ensure with a high level of confidence that the radiological consequences would be minor and below prescribed limits for all the abnormal or accident conditions taken into account in the design which would include those with a very low frequency of occurrence. This will ensure that the likelihood of accidents with serious radiological consequences is extremely low.

The primary means of preventing and mitigating the consequences of abnormal or accident conditions is to apply defence-in-depth which is implemented through the combination of a number of consecutive and independent levels of protection that would have to fail before harmful effects could be caused to people or to the environment. If one level of protection or barrier were to fail, the subsequent level or barrier would be available. When properly implemented, defence-in-depth 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. The independent effectiveness of the different levels of defence is a necessary element of defence-in-depth.

One possible elaboration of Safety Principle 8 could be: **Prevention of accidents – Defence in Depth**, such as *“all practical efforts must be made to prevent and mitigate nuclear or radiation accidents by providing defence in depth as part of the fundamental safety approach.”*

As an objective for designers of INS, INPRO has chosen to emphasize the use of enhanced defence in depth compared to existing designs and installations as a means to improve safety, and has adopted the following **INPRO basic design principle BP1 for safety – Defence in Depth**: *“Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.”*

Safety Principle 5: Optimization of protection: “Protection must be optimised to provide the highest level of safety that can reasonably be achieved.”

The safety measures that are applied in the design of any nuclear reactor are considered optimised if they provide the highest level of safety that can reasonably be achieved throughout the lifetime of the plant without unduly limiting its utilization. The radiation risks

from the plant from abnormal or accident conditions must be reduced to a level that is as low as reasonably achievable. This needs to take account of uncertainties in knowledge.

One possible elaboration of Safety Principle 5 could be: **Optimization of protection**, such as “the safety measures incorporated in the design of an innovative nuclear reactor must be optimised so that they provide the highest level of safety that can reasonably be achieved without unduly limiting its utilisation.”

As an objective for designers of INS, INPRO has chosen to emphasize the use of inherent safety characteristics and passive systems as a means to improve safety compared to existing designs and installations, and has adopted the following **INPRO basic design principle BP2 for safety – Inherent Safety**: “Installations of an INS shall excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach.”

The Safety Fundamentals (paragraph 1.10 of Ref. [11]) also states that safety and security measures must be incorporated in the design and construction of a nuclear reactor to control access and mitigate the consequences of abnormal or accident conditions arising from breaches in security. The safety and security measures must be designed and implemented in an integrated manner. This aspect is addressed in another volume, called INPRO manual for physical protection [18].

For an innovative nuclear reactor, the optimisation of the protection will involve features of the design and operation that are beyond current practices. The safety assessment carried out needs to demonstrate that these innovative features are able to meet their safety requirements. This requires that a programme of research, analysis and testing is carried out complemented by a subsequent programme of monitoring during operation. This is taken forward as part of the **INPRO basic design principle BP4: RD&D** – see below.

IAEA Safety Principle 6: Limitation of risks to individuals: “Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.”

This requires that doses and radiation risks are controlled within specified limits. The optimization of protection (Safety Principle 5) and the limitation of doses and risks to individuals (Safety Principle 6) taken together achieve the desired level of safety.

This is the Radiation Protection Objective given in Ref. [5] which requires that in all operational states radiation exposure within the installation or due to any planned release of radioactive material from the installation is kept below prescribed limits and as low as reasonably achievable, and to ensure mitigation of the radiological consequences of any accidents.

One possible elaboration of Safety Principle 6 could be: **Protection against radiation risk**, such as “The innovative nuclear reactor must be designed and operated to ensure that the risk of radiation exposure to workers, the public and the environment are lower than for current plants and as low as reasonably practicable.”

As an objective for designers of INS, INPRO has chosen as a means to improve safety to adopt the following **INPRO basic design principle BP3 for safety – Risk of radiation**: “Installations of an INS shall ensure that the risk from radiation exposures to workers, the public and the environment during construction/ commissioning, operation, and decommissioning, are comparable to the risk from other industrial facilities used for similar purposes.”

IAEA Safety Principle 3: Leadership and management for safety: “Effective leadership and management for safety must be established and sustained in

organizations concerned with, and facilities and activities that give rise to, radiation risks.”

This requires that a safety assessment has to be carried out. This involves the systematic analysis of normal operation and its effects, of the ways in which failures might occur and of the consequences of such failures. Safety assessments cover the safety measures necessary to control the hazard, and the design and engineered safety features are assessed to demonstrate that they fulfil the safety functions required of them. Where control measures or operator actions are called on to maintain safety, an initial safety assessment has to be carried out to demonstrate that the arrangements made are robust and that they can be relied on. A facility may only be constructed and commissioned or an activity may only be commenced once it has been demonstrated to the satisfaction of the regulatory body that the proposed safety measures are adequate.

One possible elaboration of Safety Principle 3 could be: **Safety assessment and research**, such as *“A rigorous safety assessment must be carried out for an innovative nuclear reactor to provide a demonstration that a high level of safety has been achieved. This includes the research, development and demonstration work to support the safety assessment.”*

As an objective for designers of INS, INPRO has chosen as a means to improve safety of INS compared to existing designs or installation, to adopt **INPRO basic design principle BP4 for safety – RD&D**: *“The development of INS shall include associated Research, Development and Demonstration work 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 existing plants.”*

IAEA Safety Principle 7: Protection of present and future generations: People and the environment, present and future, must be protected against radiation risks.

This states that the safety standards apply not only to local populations but also to populations remote from nuclear facilities and, where effects could span generations, subsequent generations have to be adequately protected without any need for them to take significant protective actions. This needs to be taken into account in judging the adequacy of measures to control radiation risks.

This also requires that the generation of radioactive waste must be kept to the minimum practicable level by means of appropriate design measures and procedures.

These requirements are taken forward as part of the **INPRO basic design principle BP3: Risk of radiation** – see above.

IAEA Safety Principle 9: Emergency preparedness and response: Arrangements must be made for emergency preparedness and response for nuclear or radiation incidents.

Arrangements must be in place on the site and at the local, regional, national and international levels to respond to a nuclear emergency. The safety aims are to ensure that, for reasonably foreseeable incidents, radiation risks would be minor and that, for any incidents that do occur, practical measures are taken to mitigate any consequences for human life and health and the environment.

These requirements are taken forward as part of the **INPRO basic design principle BP1: Defence-in-depth** – see above. In particular this relates to level 5 of defence in depth which requires that all practicable efforts must be made to mitigate the radiological consequences of any releases of radioactive materials that may result from accident conditions.

Hence, based on the IAEA Safety Fundamentals and the associated requirements for safety assessment and design, the four INPRO basic design principles for safety (also called INPRO

basic principles BP1, BP2, BP3 and BP4 in the rest of the document) have been defined for the safety assessment of an innovative nuclear reactor.

1.7. Outline of the report

Chapter 2 sets out the necessary input for an INPRO assessment of the safety of an innovative nuclear reactor. This includes information on the design and safety assessment (including the safety analysis). This chapter also discusses the timing of the INPRO assessment.

In Chapter 3 rationale and background for the INPRO safety related basic principle(s) (BP), user requirements (UR) and criteria (CR) is provided. On the criterion level a procedure is presented how to assess the potential of an INS to fulfil the INPRO criteria.

Chapter 4 demonstrates the application of the INPRO assessment method in the area of safety on an innovative reactor design compared to an existing design.

Annex A provides information on the innovative BWR design of the SWR1000.

Annex B shows design features of an existing (operating) BWR Plant (Gundremmingen).

Annex C is a reproduction from Ref. [2] presenting some examples of anticipated RD&D areas to be investigated in the future.

Annex D lays out some ideas how the INPRO methodology in the area of safety could be made more simple and consistent.

Annex E presents a table that could be used by an assessor to summarize his assessment.

In Ref. [2], the INPRO basic principles and user requirements for nuclear safety have been formulated in terms of “installations of an INS”. As stated before this volume is focussed on innovative nuclear reactor designs; complementary installations of the front end and the back end of the nuclear fuel cycle are treated in a separate volume of the INPRO manual, called safety of nuclear fuel cycle facilities [9].

In the following Tables 1.2 to 1.5 in the area of safety of nuclear reactors an overview is provided on the four INPRO BPs and the corresponding URs and CRs.

BP1 asks for enhancement of the DID concept, BP2 requests elimination of hazards, BP3 covers the aspect of radiological risk to workers and the public, and BP4 focuses on the necessary RD&D effort for the development of innovative designs.

Table 1.2. User requirements and criteria related to INPRO basic principle BP1

INPRO basic principle BP1 (defence in depth): <i>Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.</i>		
User requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR1.1⁴ (Robustness): <i>Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation.</i>	CR1.1.1 robustness	
	IN1.1.1: Robustness of design (simplicity, margins).	AL1.1.1: Superior to existing designs in at least some of the aspects discussed in the text.
	CR1.1.2 operation	
	IN1.1.2: High quality of operation.	AL1.1.2: Superior to existing designs in at least some of the aspects discussed in the text.
	CR1.1.3 inspection	
	IN1.1.3: Capability to inspect.	AL1.1.3: Superior to existing designs in at least some of the aspects discussed in the text.
	CR1.1.4 failures and disturbances	
	IN1.1.4: Expected frequency of failures and disturbances.	AL1.1.4: Superior to existing designs in at least some of the aspects discussed in the text.

⁴ Related to: DID Level 1: Prevention of Abnormal Operation and Failures, Table 1.1.

Table 1.2. User requirements and criteria related to INPRO basic principle BP1 (continued)

INPRO basic principle BP1 (defence in depth): <i>Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.</i>		
User requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR1.2⁵ (Detection and interception): <i>Installations of an INS should detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions.</i>	CR1.2.1 I&C and inherent characteristics	
	IN1.2.1: Capability of control and instrumentation system and/or inherent characteristics to detect and intercept and/or compensate deviations from normal operational states.	AL1.2.1: Key system variables relevant to safety (e.g., flow, pressure, temperature, radiation levels) do not exceed limits acceptable for continued operation (no event reporting necessary).
	CR1.2.2 grace period ⁶	
	IN1.2.2: Grace period until human actions are required.	AL1.2.2: Superior to existing designs in at least some of the aspects discussed in the text.
	CR1.2.3 inertia	
	IN1.2.3: Inertia to cope with transients.	AL1.2.3: Superior to existing designs in at least some of the aspects discussed in the text.

⁵ Related to: DID Level 2: Control of Abnormal Operation and Detection of Failures, Table 1.1.

⁶ CR1.2.2 (grace period) and CR1.2.3 (inertia) of UR1.2 in this report. were originally defined as CR1.1.5 and CR1.1.6 of UR1.1 in Ref. [2]. They were moved to UR1.2 because they relate more to Level 2 of DID.

Table 1.2. User requirements and criteria related to INPRO basic principle BP1 (continued)

INPRO basic principle BP1 (defence in depth): <i>Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.(continued)</i>		
User Requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
<p>UR1.3⁷ (Design basis accidents): <i>The frequency of occurrence of accidents should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.</i></p>	CR1.3.1 frequency of DBA	
	<p>IN1.3.1: Calculated frequency of occurrence of design basis accidents.</p>	<p>AL1.3.1: Reduced frequency of accidents that can cause plant damage relative to existing facilities.</p>
	CR1.3.2 grace period	
	<p>IN1.3.2: Grace period until human intervention is necessary.</p>	<p>AL1.3.2: Increased relative to existing facilities.</p>
	CR1.3.3 safety features	
	<p>IN1.3.3: Reliability of engineered safety features.</p>	<p>AL1.3.3: Equal or superior to existing designs.</p>
	CR1.3.4 barriers	
	<p>IN1.3.4: Number of confinement barriers maintained.</p>	<p>AL1.3.4: At least one.</p>
	CR1.3.5 controlled state	
	<p>IN1.3.5: Capability of the engineered safety features to restore the INS to a controlled state (without operator actions).</p>	<p>AL1.3.5: Sufficient to reach a controlled state.</p>
CR1.3.6 sub criticality		
<p>IN1.3.6: sub criticality margins</p>	<p>AL1.3.6: Sufficient to cover uncertainties and to allow adequate grace period.</p>	

⁷ Related to: DID Level 3: Control of Accidents, Table 1.1.

Table 1.2. User requirements and criteria related to INPRO basic principle BP1 (continued)

INPRO basic principle BP1(defence in depth): <i>Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.(continued)</i>		
User Requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR1.4⁸ ((Release into containment): <i>The frequency of a major release of radioactivity into the containment / confinement of an INS due to internal events should be reduced. Should a release occur, the consequences should be mitigated.</i>	CR1.4.1 frequency of release into containment	
	IN1.4.1: Calculated frequency of major release of radioactive materials into the containment / confinement.	AL1.4.1: At least an order of magnitude less than for existing designs; even lower for installations at urban sites.
	CR1.4.2 processes	
	IN1.4.2: Natural or engineered processes sufficient for controlling relevant system parameters and activity levels in containment / confinement.	AL1.4.2: Existence of such processes.
	CR1.4.3 accident management	
	IN1.4.3: In-plant severe accident management.	AL1.4.3: Procedures, equipment and training sufficient to prevent large release outside containment / confinement and regain control of the facility.

⁸ Related to: DID Level 4: Prevention of Major Radioactivity Release, Table 1.1.

Table 1.2. User requirements and criteria related to INPRO basic principle BP1 (continued)

INPRO basic principle BP1(defence in depth): <i>Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.(continued)</i>		
User Requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
<p>UR1.5⁹ (Release into the environment): <i>A major release of radioactivity from an installation of an INS should be prevented for all practical purposes, so that INS installations would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose.</i></p>	CR1.5.1 frequency of release to environment	
	IN1.5.1: Calculated frequency of a major release of radioactive materials to the environment.	AL1.5.1: Calculated frequency 10^{-6} per unit-year, or practically excluded by design.
	CR1.5.2 consequences	
	IN1.5.2: Calculated consequences of releases (e.g., dose).	AL1.5.2: Consequences sufficiently low to avoid necessity for evacuation. Appropriate off-site mitigation measures (e.g., temporary food restrictions) are available.
	CR1.5.3 risk	
IN1.5.3: Calculated individual and collective risk.	AL1.5.3: Comparable to facilities used for a similar purpose.	

⁹ Related to DID Level 5: Prevention of Containment Failure and Mitigation of Radiological Consequences, Table 1.1

Table 1.2. User requirements and criteria related to INPRO basic principle BP1 (continued)

INPRO basic principle BP1(defence in depth): <i>Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)</i>		
User requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR1.6 (Independence of DID levels): <i>An assessment should be performed for an INS to demonstrate that the different levels of defence-in-depth are met and are more independent from each other than for existing systems.</i>	CR1.6.1 independence of DID levels	
	IN1.6.1: Independence of different levels of DID.	AL1.6.1: Adequate independence is demonstrated, e.g., through deterministic and probabilistic means, hazards analysis etc.
UR1.7 (Human machine interface): <i>Safe operation of installations of an INS should be supported by an improved Human Machine Interface resulting from systematic application of human factors requirements to the design, construction, operation, and decommissioning.</i>	CR1.7.1 human factors	
	IN1.7.1: Evidence that human factors (HF) are addressed systematically in the plant life cycle.	AL1.7.1: - Satisfactory results from assessment.
	CR1.7.2 human response model	
	IN1.7.2: Application of formal human response models from other industries or development of nuclear specific models.	AL1.7.2: - Reduced likelihood of human error relative to existing plants, as predicted by HF models. - Use of artificial intelligence for early diagnosis and real-time operator aids. - Less dependence on operator for normal operation and short-term accident management relative to existing plants.

Table 1.3. User requirements and criteria related to INPRO basic principle BP2

INPRO basic principle BP2 (Inherent safety): <i>Installations of an INS shall excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach.</i>		
User requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR2.1 (Minimization of hazards): <i>INS should strive for elimination or minimization of some hazards relative to existing plants by incorporating inherently safe characteristics and/or passive systems, when appropriate.</i>	CR2.1.1 hazards	
	IN2.1.1: Sample indicators: stored energy, flammability, criticality, inventory of radioactive materials, available excess reactivity, and reactivity feedback.	AL2.1.1: Superior to existing designs.
	CR2.1.2 frequency of AOO &DBA	
	IN2.1.2: Expected frequency of abnormal operation and accidents.	AL2.1.2: Lower frequencies compared to existing facilities.
	CR2.1.3 consequences	
	IN2.1.3: Consequences of abnormal operation and accidents.	AL2.1.3: Lower consequences compared to existing facilities.
	CR2.1.4 confidence in innovation	
	IN2.1.4: Confidence in innovative components and approaches.	AL2.1.4: Validity established.

Table 1.4. User requirements and criteria related to INPRO basic principle BP3

INPRO basic principle BP3 (Risk of radiation): <i>Installations of an INS shall ensure that the risk from radiation exposures to workers, the public and the environment during construction/ commissioning, operation, and decommissioning, are comparable to the risk from other industrial facilities used for similar purposes.</i>		
User Requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR3.1 (Dose to workers): <i>INS installations should ensure an efficient implementation of the concept of optimization of radiation protection for workers through the use of automation, remote maintenance and operational experience from existing designs.</i>	CR3.1.1 occupational dose	
	IN3.1.1: Occupational dose values.	AL3.1.1: Less than limits defined by national laws or international standards and so that the health hazard to workers is comparable to that from an industry used for a similar purpose.
UR3.2 (Dose to public): <i>Dose to an individual member of the public from an individual INS installation during normal operation should reflect an efficient implementation of the concept of optimization, and for increased flexibility in siting may be reduced below levels from existing facilities.</i>	CR3.1.2 public dose	
	IN3.2.1: Public dose values.	AL3.2.1: Less than the limits defined by national laws or international standards and so that the health hazard to the public is comparable to that from an industry used for a similar purpose.

Table 1.5. User requirements and criteria related to INPRO basic principle BP4

INPRO basic principle BP4 (RD&D): <i>The development of INS shall include associated Research, Development and Demonstration work 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 existing plants.</i>		
User Requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR4.1 (Safety basis)¹⁰: <i>The safety basis of INS installations should be confidently established prior to commercial deployment.</i>	CR4.1.1 safety concept	
	IN4.1.1: Safety concept defined?	AL4.1.1: Yes.
	CR4.1.2 safety issues	
	IN4.1.2: Clear process for addressing safety issues?	AL4.1.2: Yes.
UR4.2 (RD&D for understanding): <i>Research, Development and Demonstration on the reliability of components and systems, including passive systems and inherent safety characteristics, should be performed to achieve a thorough understanding of all relevant physical and engineering phenomena required to support the safety assessment.</i>	CR4.2.1 RD&D	
	IN4.2.1: RD&D defined and performed and database developed?	AL4.2.1: Yes.
	CR4.2.2 computer codes	
	IN4.2.2: Computer codes or analytical methods developed and validated?	AL4.2.2: Yes.
	CR4.2.3 scaling	
	IN4.2.3: Scaling understood and/or full scale tests performed?	AL4.2.3: Yes.
UR4.3 (Pilot plant): <i>A reduced-scale pilot plant or large-scale demonstration facility should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience.</i>	CR4.3.1 novelty	
	IN4.3.1: Degree of novelty of the process.	AL4.3.1: In case of <i>high degree of novelty</i> : Facility specified, built, operated, and lessons learned documented. In case of <i>low degree of novelty</i> : Rationale provided for bypassing pilot plant.
	CR4.3.2 pilot facility	
	IN4.3.2: Level of adequacy of the pilot facility.	AL4.3.2: Results sufficient to be extrapolated.

¹⁰ IN4.1.2 in Ref. [2] was deleted because it completely overlapped with IN4.1.1. Consequently, IN4.1.3 of Ref. [2] became IN4.1.2 in this report.

Table 1.5. User requirements and criteria related to INPRO basic principle BP4 (continued)

INPRO basic principle BP4 (RD&D): <i>The development of INS shall include associated Research, Development and Demonstration work 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 existing plants. (continued)</i>		
User Requirements (UR)	Criteria (CR)	
	Indicators (IN)	Acceptance Limits (AL)
UR4.4 (Safety analysis): <i>For the safety analysis, both deterministic and probabilistic methods should be used, where feasible, to ensure that a thorough and sufficient safety assessment is made. As the technology matures, “Best Estimate (plus Uncertainty Analysis)” approaches are useful to determine the real hazard, especially for limiting severe accidents.</i>	CR4.4.1 risk informed approach	
	IN4.4.1: Use of a risk informed approach?	AL4.4.1: Yes.
	CR4.4.2 uncertainties	
	IN4.4.2: Uncertainties and sensitivities identified and appropriately dealt with?	AL4.4.2: Yes.

CHAPTER 2

NECESSARY INPUT FOR AN INPRO ASSESSMENT

This chapter gives guidance on the information needed by the INPRO assessor to be able to perform an assessment of innovative nuclear reactors.

2.1. Definition of INS

A clear definition of the INS is needed for an INPRO assessment. As described in the first volume of the INPRO manual [3], the INS will be selected, in general, based on an energy planning study. This study should define the role of nuclear power (amount of MW_{nuclear} to be installed as a function of time) in an energy supply scenario for a country (or region or globally). Using the results of such a study, the next step is the choice of components of an INS that fits to the determined role of nuclear power. The INS definition should include a schedule for deployment, operation and decommissioning of the individual components.

A country may decide to install or maintain only certain components of an INS within its national borders, e.g., as a minimum, one (or several) nuclear power plant(s) and corresponding nuclear waste facilities. Such a “national” INS would then consist of the components chosen. In principle, the holistic approach of the INPRO methodology requires confirming the safety of the complete fuel cycle of an INS, i.e. also components outside the country are to be assessed, but, as a first step, an assessment of the national components of the INS should be sufficient.

2.2. Design information

The INPRO assessor will need to have access to the design information of an innovative nuclear reactor. This will include information relating to: the design basis for 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 novel or of an innovative design and this would be the focus of the INPRO assessment, and is to be compared to information of existing designs. The information needed is outlined in the discussion of the INPRO criteria in the following sections of this report.

The information is to be provided by the technology developer or supplier, therefore a close co-operation between the INPRO assessor and the designer is necessary.

2.3. Results of safety analyses

The INPRO assessor will need access to results of a safety assessment that has been carried out and includes a safety analysis which consists of a set of different quantitative analyses that evaluate and assess challenges to safety under various operational states, anticipated occurrences and accident conditions using deterministic and probabilistic methods; these analyses are to be performed by the technology developer or supplier.

The safety assessment would need to include details of the research, development and demonstration (RD&D) carried out for innovative aspects of the reactor design.

2.4. Timing of the INPRO assessment

In principle, the INPRO assessment can be carried out at any stage of the development of the design. However, it needs to be recognised that the extent and level of detail of the design and safety assessment information available will increase as the design of an innovative nuclear reactor progresses from the conceptual stage to the development of the detailed design. This

will need to be taken into account by the INPRO assessor in drawing conclusions on whether an INPRO safety requirement has been met.

Thus, if the INPRO assessment is carried out at an early stage in the development of innovative design¹¹, safety analyses might not be available or possible. In such a case the technology developer of the innovative design should provide generic information to the INPRO assessor of a comparable or similar reactor already fully designed or operating (with a safety case established), to be replaced during the development of the design by reactor specific information.

¹¹ As defined in Chapter 4.2.1 of Ref. [3], an innovative design is an advanced design that incorporates radical conceptual changes in design approaches or system configuration in comparison to existing practice.

CHAPTER 3

BASIC PRINCIPLES, USER REQUIREMENTS AND CRITERIA

In the area of safety for innovative reactors a set of INPRO basic design principles (BP), also called INPRO basic principles in the following, user requirements (UR) , and criteria (CR) has been defined, the focus of which is directed to those requirements that would most likely change for innovative nuclear reactors, reflecting the expected changes in the future in nuclear technology.

As stated in the introduction, the concept of ‘safety culture’ (e.g., Refs [15], [16], [17] and [52]) and the legal framework related to safety of nuclear installations is dealt with in another volume of the INPRO manual, called infrastructure [10].

It is also assumed that requirements and practices set out in IAEA Safety Standards and Guides will be followed where applicable, (see e.g., Refs [5], [20] and [21]). These provide detailed guidance, e.g., for allowable fuel failure rates and capabilities for resuming operation following a transient.

The INPRO set of basic principles, user requirements and criteria is expected to apply to any type of innovative design. It should foster an appropriate level of safety that can be communicated to and be accepted by all stakeholders in nuclear energy.

For innovative nuclear reactors, it is expected that INPRO requirements and criteria will eventually become formalized in IAEA Safety Standards and Guides for innovative reactors; and conversely as the INPRO methodology evolves, it will benefit from and reflect advances in the IAEA Standards and Guides.

3.1. INPRO basic principles for safety

INPRO has defined four basic design principles for safety in Ref. [2] which are laid out in the following:

Installations of an Innovative Nuclear Energy System shall:

- (1) Incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.*
- (2) Excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach.*
- (3) Ensure that the risk from radiation exposures to workers, the public and the environment during construction/commissioning, operation, and decommissioning, shall be comparable to that of other industrial facilities used for similar purposes.*

Further, the development of an Innovative Nuclear Energy System shall:

- (4) Include associated RD&D work 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 existing plants.*

From these four BPs a set of fourteen user requirements (UR) has been derived, associated with thirty-seven criteria (CR, consisting of indicators IN and acceptance limits AL) as shown in Tables 1.2 to 1.5 in Chapter 1 of this report.

In the manual for the INPRO area of physical protection (PP) (Ref. [18]), PP user requirement UR2 requests the designer of new designs to consider jointly the objectives of safety with those of PP and proliferation resistance [19] during all design stages. This PP user requirement UR2 is therefore also to be taken into account during an INPRO safety assessment (to be discussed further in Section 3.2.8).

All the INPRO user requirements in the area of safety are primarily to be fulfilled by the designer (developer, supplier) of the INS. The role of the INPRO assessor is to check, based on evidence provided by the designer, whether the designer has performed the necessary measures as required by INPRO.

In the following sections for each BP and its related URs and CRs rationale and background information is provided.; additionally, at the level of CRs a procedure is outlined that allows a judgement on the potential of an INS whether and how well a given acceptance limit is being met.

3.2. INPRO basic principle BP1 (Defence in depth)

Basic principle BP1: *Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.*

To compensate for potential human error or mechanical failures, this BP asks that a Defence-In-Depth (DID) strategy [12] shall be implemented, utilizing several levels of protection and successive physical barriers to prevent the release of radioactive material to the environment. Means should also be provided to protect the barriers themselves. Further accident management measures should be available to protect the public and the environment from undue harm in case a severe accident occurs.

Optimization of the balance among different levels of defence is important – the seven user requirements for this basic principle place more emphasis on preventative than on corrective measures or mitigative barriers.

Thus the first five user requirements of BP1 are directed towards a strengthening of the DID strategy so that for future nuclear reactors – even in the case of severe accidents – evacuation measures outside the plant site are not needed. The sixth user requirement deals with the independence of the levels of DID, and the seventh covers the issue of human machine interface.

3.2.1. User requirement UR1.1 (robustness)

User requirement UR1.1: *Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation¹².*

The major means to achieve an increase in robustness are to ensure a high quality of design, construction and operation, including human performance. For more robust innovative designs the expected frequencies of initiating failures and disturbances should be reduced relative to existing designs. This reduction could be achieved, e.g., by use of: improved materials, simplified designs to minimize failures and errors, improved design margins to overstressing and fatigue, increased operating margins, increased redundancies of systems, less impact from incorrect human intervention (the machine should be tolerant to mistakes), more effective and efficient inspections, a continuous monitoring of the plant health, etc.

¹² UR1.1 is related to level 1 of DID.

Examples of reactor concepts with increased robustness against certain potential hazards are designs with all cooling loops inside the pressure vessel (avoidance 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 the temperature in reactivity transients), extensive use of passive systems (potentially higher reliability, e.g., natural convection), higher reliability self-checking control systems (avoidance of deviations from normal operation), use of non-flammable materials (avoidance of fires), etc.

The use of inherent safety characteristics is a useful means of achieving robustness and has been highlighted as a separate basic safety principle BP2 (discussed in Section 3.3).

INPRO selected the following criteria for UR 1.1:

Table 3.2.1. Criteria¹³ for user requirement UR1.1

UR1.1 (robustness): <i>Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.1.1 robustness	
IN1.1.1: Robustness of design (simplicity, margins).	AL1.1.1: Superior to existing designs in at least some of the aspects discussed in the text.
CR1.1.2 operation	
IN1.1.2: High quality of operation.	AL1.1.2: Superior to existing designs in at least some of the aspects discussed in the text.
CR1.1.3 inspection	
IN1.1.3: Capability to inspect.	AL1.1.3: Superior to existing designs in at least some of the aspects discussed in the text.
CR1.1.4 failures and disturbances	
IN1.1.4: Expected frequency of failures and disturbances.	AL1.1.4: Superior to existing designs in at least some of the aspects discussed in the text.

3.2.1.1. Criterion CR1.1.1 (robustness)

Indicator IN1.1.1: *Robustness of design (simplicity, margins).*

Acceptance limit AL1.1.1: *Superior to existing designs in at least some of the aspects discussed in the text.*

A list of possible evaluation parameters (EP) for this criterion is given below:

EP1.1.1.1: Margins of design

EP1.1.1.2: Simplicity of design

EP1.1.1.3: Quality of manufacture and construction

EP1.1.1.4: Quality of materials

EP1.1.1.5: Redundancy of systems

¹³ The criteria CR1.1.1 till CR1.1.4 deal with robustness of design to prevent failures and/or disturbances in accordance with level 1 of DID; the original criteria CR1.1.5 and CR1.1.6 as defined in Ref. [2] deal with the robustness of design after a failure or an abnormal operational state has occurred, a situation that is more related to level 2 of DID; they were therefore moved in this report to UR1.2.

Use of inherent safety characteristics is an additional means of achieving robustness. This is described separately under BP2.

Evaluation parameter EP1.1.1.1 margins of design

In the following the design of a reactor core and other safety related components is discussed in respect to robustness. The term *margin* is defined here as the difference between a design limit and the actual design value of the corresponding safety related parameter, such as stress, temperature, etc. An increase of design margins will increase the robustness of a design.

Robust reactor core design

The reactor core inside the pressure boundary forms the nuclear heat source of the nuclear power plant. During power operation the function of the reactor coolant system is to remove heat generated inside the nuclear fuel. The fluid used to absorb this heat in the reactor core and transport it out of the core – i.e. the coolant – could be, for example, water, sodium, lead, helium.

A core design incorporates control systems to change the overall or local power level (e.g., by control rods and/or void changes and temperature changes¹⁴) and a safety system to shut down the reactor to decay heat generation level.

The reactor core must also be cooled in the event of abnormal conditions or accidents; for this purpose various active as well as passive safety systems are installed.

An appropriate instrumentation and control (I&C) system has to be installed 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 can be divided into several areas:

- Thermal and mechanical fuel design;
- Neutronic core design; and
- Thermal-hydraulic core design including its cooling circuit.

The *thermal fuel design* determines the margins of the fuel against specified limits of e.g., centerline fuel temperature, fission gas release, or the 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 (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 burn-up 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 and transients avoiding departure from nucleate boiling (DNB) or dry out (exceeding critical heat flux, CHF), and at least limiting occurrence of DNB or CHF during various design basis accidents (DBAs).

In the following a tentative list of design parameters is presented for the core of an advanced heavy water reactor (AHWR):

Neutronic characteristics that stabilize operation:

¹⁴ Void and temperature in a BWR core is changed also via the core coolant flow, i.e. by the main coolant pumps.

- Doppler coefficient;
- Void coefficient;
- Power coefficient; and

Fuel *thermal design* margins:

- Fuel centerline temperature (normal operation);
- Stored energy in fuel;
- Linear heat generation rate;
- Design margins on clad temperature (from corrosion and oxidation considerations); and

Fuel *mechanical design* margins:

- Design margins on clad stress and strains;
- Fission gas release; and

Thermal hydraulic design margins:

- Minimum Critical Heat Flux Ratio (MCHFR);
- Margins to instability (margin on sub-cooling);
- Decay ratio;
- Fraction of core heat that can be removed by natural circulation; and

Some attributes of improved I&C, etc. could be added.

This list could be used to compare the core design of an innovative reactor core with an existing design.

As stated above, the coolant flow through the core is necessary to remove the power produced within the core. Natural flow through the core during normal operation, used in some former 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 sequence. An increase of the fraction of core heat that can be removed by natural circulation is therefore regarded as an increase of robustness.

A detailed safety guide for the design of the reactor core is provided in Ref. [22].

Improved design margins of components to overstressing and fatigue

Loads and resulting stresses have a great influence on robustness, because a reasonable design with low stresses and low numbers of cycling can reduce the failure rate substantially.

For existing plants the requirements for the design, the manufacturing, in-service inspections and operational monitoring are usually specified in (extensive) national standards or adopted standards from other countries; the most known and used standards are those published by the American Society of Mechanical Engineers (Nuclear codes and Standards) (ASME).

For new (innovative) designs for which no standards exist, at least for the first plant a conservative design approach equivalent to existing standards is required; as discussed in the section for basic principle BP4 in more detail, additional and specific tests would be supportive and may decrease conservatism.

Acceptability of EP1.1.1.1: Evidence available to the INPRO assessor that increased design margins in the INS in comparison to existing design have been demonstrated.

Evaluation parameter EP1.1.1.2: Simplicity of design

One of the options to simplify the reactor design is to reduce the number of components of the cooling system.

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., HTGRs) to several parallel direct cycles (e.g., BWRs) up to two (e.g., PWRs and HWRs) or three (e.g., sodium cooled reactors) separate cycles in series with heat exchangers in between.

A designer has to consider several tradeoffs: reducing the number of loops (e.g., for PWRs) for a given power of the core will result in larger steam generators; this may possibly result in thermal-hydraulic instabilities or the need for new materials, etc. 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 could also be achieved with a development of a non-flammable sodium coolant. The number of other lines in a reactor system, such as feed water trains and main steam lines could also be investigated whether a reduction is appropriate.

Another option is to reduce the number of active components (e.g., motor operated valves, pumps) in a system. However, reduction of lines or active components has to be considered carefully because it may negatively influence the redundancy of the system.

Acceptability of EP1.1.1.2: Evidence available to the INPRO assessor that demonstrates increased simplicity of the INS design in comparison to existing designs.

Evaluation parameter EP1.1.1.3: Quality of manufacture and construction¹⁵

Every weld in a pipe or vessel could 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 an INS. In addition, fewer welds require less in service inspections and thus should lead to reduced doses for the personnel. As in other areas, progress in welding engineering and fabrication of pipes exists. Progress of welding engineering includes the application of automatic welding machines during manufacturing, which results typically in a higher quality of welds compared to manual welding procedures. Progress in fabrication of pipes includes the elimination of longitudinal welds by use of a cold-draw (extrusion) process.

Acceptability of EP1.1.1.3: Evidence available to the INPRO assessor that demonstrates increased quality of manufacturing and construction of the INS in comparison to existing designs.

Evaluation parameter EP1.1.1.4: Quality of materials

Mechanical failures of components comprise still a significant part of initiating events. For existing reactors many efforts have been undertaken on national and international levels to advance the knowledge about failure mechanism and to improve the properties of the material itself. Experiences have indicated that already minor changes in materials or specifications (also for the environmental conditions, e.g., pH of the coolant) resulted in operational benefits (e.g., improved material behavior). Much emphasis with considerable success has been put on the feedback of operating experience into design solutions. The improvements achieved up till

¹⁵ (see also Ref. [53] and [54])

now promise for the future that further advances in material properties will lead to better designs with increased robustness.

Acceptability of EP1.1.1.4: Evidence available to the INPRO assessor that demonstrates increased quality of materials used in the INS in comparison to existing designs.

Evaluation parameter EP1.1.1.5: Redundancy of systems

Increased redundancies of systems may reduce the probability of degradation or loss of a function and help to avoid transients (such as those caused by control system actions, trips and set backs).

Acceptability of EP1.1.1.5: Evidence available to the INPRO assessor that demonstrates increased redundancy of system of the INS in comparison to existing designs.

Final assessment of CR1.1.1 robustness

The **acceptance limit AL1.1.1** (robustness of INS superior to existing designs in at least some of the aspects discussed) of CR1.1.1 is met if evidence is available to the INPRO assessor that at least some of the evaluation parameters, discussed above, demonstrate that the design of the advanced nuclear reactor is superior to existing designs; for the rest of the evaluation parameters it should be at least equal.

3.2.1.2. Criterion CR1.1.2 (operation)

Indicator IN1.1.2: *High quality of operation.*

Acceptance limit AL1.1.2: *Superior to existing designs in at least some of the aspects discussed in the text.*

A list of possible evaluation parameters (EP) for this criterion is given below:

- EP1.1.2.1: margins of operation.
- EP1.1.2.2: reliability of control systems.
- EP1.1.2.3: impact from incorrect human intervention.
- EP1.1.2.4: quality of documentation.
- EP1.1.2.5: quality of training.
- EP1.1.2.6: organization of plant.
- EP1.1.2.7: availability/capability of plant.
- EP1.1.2.8: use of world wide operating experience.

Evaluation parameter EP1.1.2.1: margins of operation.

Increased operating margins (see also Ref. [23]) will reduce the occurrence of abnormal plant states leading to a reactor shutdown (scram). 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 may be capable reducing the power increase. In principle, a trip level could be set at a higher value and thus the operating margin (in this case for an overshooting of power) would be increased. More general, an increase of the difference between operating and scram level for reactor conditions resulting in automatic scrams (e.g., low flow, low pressure, etc.) leads to an increased operating margin. It should be pointed out that this increased margin may result in a lower power output of the plant.

Acceptability of EP1.1.2.1: Evidence available to the INPRO assessor that demonstrates increased operating margin in the design of an INS compared to existing designs.

Evaluation parameter EP1.1.2.2: reliability of control systems.

Advanced self checking control systems could help to avoid deviations from normal operation. Such advanced control systems could reduce the frequency of anticipated operational occurrences (AOO) as well as the demand on operators (see also criterion CR1.2.1).

Acceptability of EP1.1.2.2: Evidence available to the INPRO assessor that demonstrates a superior reliability of the control systems of an INS compared to existing designs.

Evaluation parameter EP1.1.2.3: reduced impact of incorrect human intervention

Less impact means the machine should be more tolerant to mistakes. This important characteristic is an expected corollary of having advanced fault tolerant control system and/or passive features.

Acceptability of EP1.1.2.3: Evidence available to the INPRO assessor that demonstrates less impact of incorrect human intervention on operation of an INS compared to existing designs.

Evaluation parameter EP1.1.2.4: quality of documentation

It should be noted that a high quality of operation requires knowledge of the actual state as well as documentation of all modifications since the beginning of operation, taking into account a planned service time of 60 years [55]. The 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 shortly discussed.

Technical documentation

A sufficient technical documentation (mostly to be provided by the designer) must be available when the plant is close to start operation. Such a documentation includes:

- Project documentation: it covers all information that has to be documented of an individual project;
- Processing documentation: it contains all documents which are generated in the course of processing of the plant and plant items;
- Plant documentation: it encompasses all documents of a plant, or plant items, which are required for the verification of fulfillment and compliance with statutory requirements and for evaluation of supplies and services;
- Safety and licensing documentation: it is the compilation of licensing notices and documents. Documents for the verification of fulfillment of safety rules and commitments are also included;
- Quality documentation: it is the compilation of the quality assurance (QA) records – permanent and non-permanent;
- Operating documentation: it is the compilation during commissioning and operation – safety-related operating records/ records of maintenance of the quality of the plant/ documents on radiological protection of personnel and environment; and
- Working documentation: it includes general documents and technical documents for systems and components.

*Manuals*¹⁶

A series of manuals are needed for a nuclear power plant (NPP), e.g., operating, chemistry, nuclear testing, and conventional testing manuals. In the following a short 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 program 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 facilities 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 modeling and computer capabilities into account, advanced control systems including artificial intelligence methods could be implemented in the longer term.

Acceptability of EP1.1.2.4: Sufficient (as described above) technical documentation including manuals is available for the INS at the start of operation and is continuously updated.

Evaluation parameter EP1.1.2.5: quality of training

Appropriate training (see also Ref. [24]) of nuclear power plant operating personnel in regard to safety aspects shall comprise all staff members, who are directly involved in plant operation, plant and system maintenance, including those who hold responsible positions within the power plant management. The vendor of the power plant usually offers the operator/owner of the plant training programs and associated courses. Training involves group and modular training. It is important to provide well-written training material. Use of simulators for operator training is mandatory.

Acceptability of EP1.1.2.5: Evidence available to the INPRO assessor that appropriate training programs are established and implemented.

Evaluation parameter EP1.1.2.6: organization of plant

A clear plant management organization with defined responsibilities (see also Refs [17] and [25] for international experience) is a prerequisite for a high quality of operation.

A pre-condition for granting a construction permit for a nuclear facility 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 meeting all licensing requirements. In addition to the organization's structure, functions and the number of personnel required, the owner/operator should define qualification requirements in sufficient

¹⁶ See also Refs [17] and [25].

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 shall be 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 manager for operation, maintenance, technical support, quality assurance, environmental protection, nuclear and industrial safety, and administration.

Acceptability of EP1.1.2.6: Evidence available to the INPRO assessor that a clear plant organization with defined responsibilities has been established.

Evaluation parameter EP1.1.2.7: availability/capability of plant

The unit capability factor, scram frequency, and a low number of nuclear events (INES) to be reported provide a good indication of the quality of operation of a nuclear plant. These numbers can be only determined for plants in operation, however, already during the development of INS measures and features should be considered that ensure a high availability/capacity factor.

The *unit capability factor* is the percentage of maximum energy generation that a plant is capable of supplying to the electrical grid, limited only by factors within the control of plant management. A high unit capability factor indicates effective plant programs and practices to minimize unplanned energy losses and to optimize planned outages. The following Figure 3.2.1 shows this factor during the period 1990 till 2004 for all nuclear power units represented in the WANO organization.

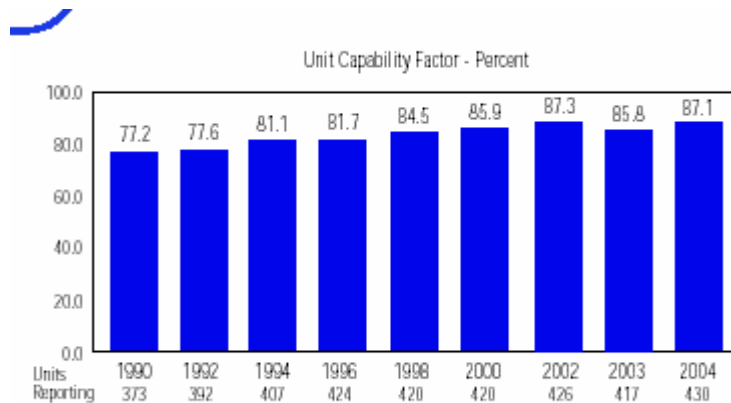


Figure 3.2.1. Unit capability factor [26].

The “unplanned automatic *scrams* per 7000 hours critical” factor tracks the mean scram (automatic shutdown) rate for approximately one year of operation. This factor is shown in the following Figure 3.2.2 based on information from WANO.

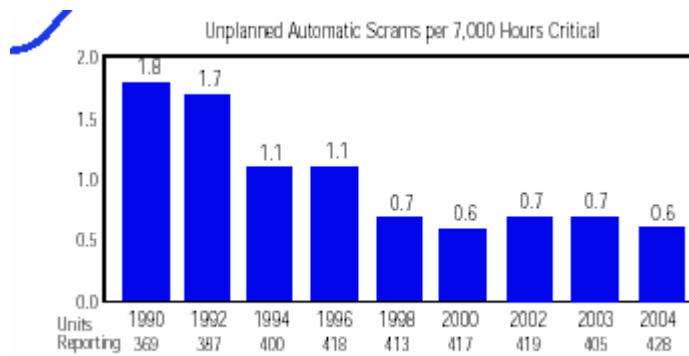


Figure 3.2.2. Unplanned automatic scrams per 7000 hours critical [26].

It is evident that the average scram frequency decreased during the recent years; a similar trend can be expected for an INS. A scram frequency below 0.5 per year is an acceptable value for an INS¹⁷.

Acceptability of EP1.1.2.7: Evidence available to the INPRO assessor that INS in operation demonstrates comparable or superior availability/capacity factors in comparing to existing designs. For INS under development measures and features are described that ensure these factors will remain comparable to existing designs or become superior.

Evaluation parameter EP1.1.2.8: use of world wide operating experience

Operation experience and related evaluations of existing NPPs are collected by international organizations. Examples are the European BWR Forum, BWR Owners Group, Incident Reporting System of IAEA, WANO, CANDU Owners Group (COG), etc. As discussed in the introduction of this report (Section 1.3, existing requirements) 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 should be taken into account in the design of an INS.

Acceptability of EP1.1.2.7: Evidence available to the INPRO assessor that experience of operating nuclear power plants has been taken into account in the design of INS.

Final assessment of criterion CR1.1.2 (operation)

The **acceptance limit AL1.1.2** (quality of operation of INS is superior to existing designs in at least some of the aspects discussed) of CR1.1.2 is met, if evidence is available to the INPRO assessor that the assessment of the above defined evaluation parameters provides positive answers and confirms that the INS design shows:

- Sufficient margins of operation ensuring that key system variables relevant to safety do not exceed limits acceptable for continued operation;
- Reduced impact of incorrect human action by “forgiving” design;
- Use of advanced control systems;
- Existence of a clear management organization with defined responsibilities, sufficient technical documentation including manuals, and of appropriate training provisions;

¹⁷ A similar figure for the frequency of safety relevant nuclear events to be reported (INES) should be available in literature.

- Sharing of operating experience and use of it in design; and
- Number of incidents with the necessity for event reports (INES) kept to a minimum.

3.2.1.3. Criterion CR1.1.3 (inspection)

Indicator IN1.1.3: *Capability to inspect.*

Acceptance limit AL1.1.3: *Superior to existing designs in at least some of the aspects discussed in the text.*

“Capability to inspect” means that the system design should permit more efficient and intelligent inspection, not just require more inspections, i.e. the inspection program should be driven by a sound understanding of failure mechanisms, so that the right locations are inspected at the right time intervals. It is recognized that in early operational stages of an INS, before the technology (experience) base is fully established, more inspection might be required.

Appropriate inspections are very important for keeping and improving the safety level (Ref. [27]). Because the inspection methods and their accuracy are continuously improving, the acceptance limits are mostly “the state-of-the-art”¹⁸.

General prerequisites for an appropriate inspection program for an INS 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 program (including risk-informed approaches, see also criterion CR4.4.1) taking into account the knowledge as defined above, such as damage mechanisms, design specifics (e.g., stress locations) and operating conditions; and
- Decrease of individual and collective doses caused by inspections through design provisions, e.g., choice of materials in connection with adequate water chemistry to avoid radioactive corrosion products, shielding devices, easy serviceability. This includes also easy access to working places, appropriate environmental working conditions and development of specific tools and robotics in order to reduce dose rates and/or durations of inspections (see also criterion CR3.1.1).

Final assessment of criterion CR1.1.3 (inspection)

The **acceptance limit AL1.1.3** (capability to inspect INS is superior to existing designs in at least some of the aspects discussed) of CR1.1.3 is met, if evidence is available to the INPRO assessor confirming:

- More effective and efficient inspections are (will be) performed in an INS compared to existing designs, because the necessary knowledge is available;
- An appropriate inspection program is established; and
- Design features to ease the performance of inspections have been demonstrated.

3.2.1.4. Criterion CR1.1.4 (failures and disturbances)

Indicator IN1.1.4: *Expected frequency of failures and disturbances.*

¹⁸ State of the art means that the latest available technology should be used in the design of an INS.

Acceptance limit AL1.1.4: *Superior to existing designs in at least some of the aspects discussed in the text.*

For innovative designs the expected frequencies of initiating events (failures and disturbances) should be reduced relative to existing designs. Reduction could be achieved via an increased robustness.

For an INS, as a first indication of expected frequencies of failures and disturbances with a potential to disrupt normal operation, the corresponding values for existing reactors with similar designs might be used. In Table 3.2.2 the frequencies of events in existing reactors are given. This list contains only plant internal events because frequencies of external events (e.g., loss-of offsite power, flooding, etc.) are very area-specific, i.e. dependent on local conditions.

Table 3.2.2. Frequency of events per year and unit in existing reactors (some selected sequences)

Event	Reactor-Type	
	PWR[28]	BWR[29]
Loss of heat sink	0,36	0.5
Loss of feed water supply	0,15	0.2
Breaks in reactor coolant pipe > 200 cm ²	$< 10^{-7}$	$< 10^{-7}$ (In feed-water line)
Breaks in reactor coolant pipe 80-200 cm ²	$9,0 \cdot 10^{-5}$	$9,0 \cdot 10^{-5}$
Breaks in reactor coolant pipe 2-12 cm ²	$2,8 \cdot 10^{-3}$	
ATWS during loss of main feed water	$4,7 \cdot 10^{-6}$	
ATWS during loss of main heat sink		$1,0 \cdot 10^{-6}$

Final assessment of criterion CR1.1.4 (failures and disturbances)

The **acceptance limit AL1.1.4** (expected frequencies of failures and disturbances in INS is superior to existing designs in at least some of the aspects discussed) of CR1.1.4 is met, if evidence is available to the INPRO assessor that less failures or disturbances per year and unit in comparison to existing designs are predicted for the INS.

3.2.2. User requirement UR1.2 (detection and interception)

User requirement UR1.2: *Installations of an INS should detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions.*¹⁹

In the design of an INS, priority should be given to advanced control systems, and improved reliability of systems to reduce the need for costly additional equipment because of redundancy and diversity requirements. Optimization of a combination of passive and active systems will be important. In a longer term, priority should be given to (design-specific)

¹⁹ UR1.2 relates to level 2 of DID.

inherent limiting characteristics (sometimes called “self controlling properties”) and to robust and simple (possibly passive) control and advanced monitoring systems.

The main function of the I&C system is to detect anticipated operational occurrences (AOO), and enable 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. For innovative reactor designs inherent characteristics and/or passive systems (or components) could assist or even partially replace certain capabilities of the I&C system.

The set of safety I&C functions to be provided for a NPP can be described from two points of view:

- From the event-based view, showing how the safety I&C initiates required protective actions as a response to postulated initiating events; and
- From the safety goal based view, showing how the safety functions are implemented to achieve these goals (Ref. [30]).

The I&C system processes measurements data from several instrumentations: conventional process instrumentation, in-core instrumentation, ex-core instrumentation, rod position and reactor vessel water level measurement, loose parts and vibration monitoring, radiation monitoring, accident instrumentation, hydrogen detection measurement, and boron instrumentation. These instrumentation contains instrumentation channels of different importance to safety.

For user requirement UR1.2 the following criteria have been selected by INPRO:

Table 3.2.3. Criteria for user requirement UR1.2

UR1.2 (detection and interception): <i>Installations of an INS should detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.2.1 I&C and inherent characteristics	
IN1.2.1: Capability of instrumentation and control system and/or inherent characteristics to detect and intercept and/or compensate deviations from normal operational states.	AL1.2.1: Key system variables relevant to safety do not exceed limits acceptable for continued operation.
CR1.2.2²⁰ grace period	
IN1.2.2: Grace period until human actions are required.	AL1.2.2: Superior to existing designs in at least some of the aspects discussed in the text.
CR1.2.3 inertia	
IN1.2.3: Inertia to cope with transients.	AL1.2.3: Superior to existing designs in at least some of the aspects discussed in the text.

3.2.2.1. Criterion CR1.2.1 (I&C and inherent characteristics)

Indicator IN1.2.1: *Capability of instrumentation and control system (I&C) and/or inherent characteristics to detect and intercept and/or compensate deviations from normal operational states.*

²⁰ CR1.2.2 and CR1.2.3 were originally called CR1.1.5 and CR1.1.6 in Ref. [2]. As they relate to level 2 of DID they were moved to UR1.2.

Acceptance limit AL1.2.1: *Key system variables relevant to safety (e.g., flow, pressure, temperature, radiation levels) do not exceed limits acceptable for continued operation (no event reporting necessary).*

INPRO has defined the following evaluation (EP) parameters for CR1.2.1:

EP1.2.1.1: continuous monitoring of plant health.

EP1.2.1.2: dynamic plant analysis.

Evaluation parameter EP1.2.1.1: Continuous monitoring of the plant health.

Monitoring of operational data (Ref. [22]) is important assuring the integrity of components of a reactor system. For this purpose several monitoring systems have been designed.

Installations of monitoring systems could lead to simplification of the design of an INS. 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 (LOCA) as a design basis accident in water-cooled reactors. In addition, the number of pipe restraints to cope with pipe whipping due to jet forces could be reduced.

Examples of monitoring systems for water cooled reactors are given below; for other reactor designs some of these monitoring systems are also applicable.

Leak monitoring

The leakage monitoring system is designed such that it is capable of detecting and localizing leakages with sufficient accuracy in the reactor coolant pressure boundary during plant operation. This system is sensitive enough to detect those leakages which 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.

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

The system measures and analyzes continuous and cyclic characteristic vibration values.

Diagnostic of rotating machinery

Increasing plant availability and plant safety, as well as reducing cost of maintaining rotating machinery such as fans, pumps, and turbines, requires that reliable information has to be known about 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 on part of power plant systems and components, something which is essential for safe and economic plant operation. The chemistry manual²¹ describes water chemistry aspects for relevant plant

²¹ See also evaluation parameter EP1.1.2.4, *quality of documentation*, of criterion CR1.1.2.

systems as reactor coolant system; reactor auxiliary systems; steam, condensate and feed water cycle; non-nuclear auxiliary systems and the radioactive waste processing system.

Seismic monitoring system

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

Environmental impact 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.

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, i.e. e.g., screens showing a failure location, prognosis of possible system behavior as a consequence of this failure, and a list of possible countermeasures. In addition, computerized manuals are becoming state of the art. Taking advanced system modeling and computer capabilities into account, advanced control systems including artificial intelligence methods could be implemented in the longer term.

Acceptability of EP1.2.1.1: Evidence is available to the INPRO assessor that the INS design includes systems for continuous monitoring of plant health and computerized aids for the operators.

Evaluation parameter EP1.2.1.2: dynamic plant analysis

An analysis of the nuclear power plant dynamics is required to show how the different events causing a deviation from normal operation are detected and mitigated. The dynamic plant model used in the analysis needs the capability to simulate accurately control and reactor protection system variables, trip parameters and safety and auxiliary systems operational behavior. For an I&C to be acceptable, the results of the analyses must demonstrate that all limitation and safety limits are met in case of assumed deviations from normal operation (see also IN1.2.3).

A probabilistic safety analysis [31] (together with an uncertainty analysis) for the safety-related part of the I&C system is to be performed. These analyses should be performed with high quality and demonstrate calculated low un-availabilities of the safety related I&C, e.g., for the shut down state.

Acceptability of EP1.2.1.2: Evidence is available to the INPRO assessor that a deterministic and probabilistic plant analysis has been performed for the INS and the results confirm that key system variables relevant to safety (e.g., heat flux, flow, pressure, temperature, radiation levels) do not exceed limits acceptable for continued operation and do not result in any short term consequences affecting normal operation.

*Inherent characteristics*²² of a reactor, such as a negative reactivity feedback, influence the dynamic behaviour of the plant in a positive way, and could lead to reduced design requirements for the I&C. The following two criteria CR1.2.2 (grace period) and CR1.2.3 (inertia) deal with such inherent characteristics.

²² See also Section 1.7, *defence in depth*, and basic principle BP2 in Section 3.3.

Final assessment of criterion CR1.2.1 (I&C and inherent characteristics)

The **acceptance limit AL1.2.1** (in case of AOO, key system variables relevant to safety do not exceed limits acceptable for continued operation) is met, if evidence is available to the INPRO assessor that the assessment of both EPs above provides positive results.

3.2.2.2. Criterion CR1.2.2 (grace period)

Indicator IN1.2.2: *Grace period until human actions are required.*

Acceptance limit AL1.2.2: *Superior to existing designs in at least some of the aspects discussed in the text.*

The “grace period” for normal operation is defined as the time available, in case of a failure or beginning of abnormal operation, before human (operator) action is required. The appropriate value of this “grace period” could depend on the type of nuclear facility, the ease of diagnosis of the failure, and the complexity of the human action to be taken; simple failures and straightforward actions requiring less grace period.

In case of deviations from normal plant states, it is commonly agreed to divide the time period for the operator to cope with deviations from normal operation into three different time periods:

- (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; usually 5 minutes are assumed.

The time to *diagnose* the situation appropriately is mainly dependent on 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 of no longer than 30 minutes appropriate *manual actions* will be performed by the operator based on the fact that operators are trained to cope with anticipated operational occurrences. Therefore, the design of the reactor should be such that all necessary actions within this time period are automated.

The **acceptance limit AL1.2.2** is met if evidence is available to the INPRO assessor that a grace period of at least 30 minutes is assured by the design of the plant.

3.2.2.3. Criterion CR1.2.3 (inertia)

Indicator IN1.2.3: *Inertia to cope with transients.*

Acceptance limit AL1.2.3: *Superior to existing designs in at least some of the aspects discussed in the text.*

The term “inertia” means the capability of a nuclear reactor system to cope with anticipated operational occurrences; the main objective is to avoid consequences that could delay a restart and a return to normal operation.

A nuclear reactor system is usually designed to stay within the design limits (e.g., temperatures, pressures, stresses, etc.) for all anticipated transients, taking into account also a single failure and repair status of components. Nevertheless, transients of system parameters (e.g., temperature increases, pressure increases) should be as slow as reasonable possible.

A high inertia resulting in a slow response to initiating events is usually achieved by sufficient participating mass within the primary system (e.g., in HTRs), sufficient primary coolant (e.g.,

in water-cooled reactors), small reactivity holdup in the control system (e.g., in HWRs) or additional secondary side mass (e.g., in PWRs and liquid metal cooled reactors).

An additional requirement, primarily for a PWR, is that during an anticipated operational occurrence no coolant mass of the primary coolant system should be lost via the valves of the pressurizer, and thus any contamination by radioactive coolant of the confinement/containment is avoided; this could be achieved by an increased (adequate) size of the pressurizer in an INS.

To demonstrate the adequacy of the design of the nuclear reactor system, the system behavior for these anticipated operational occurrences has to be analyzed with validated and verified computer models, see also criterion CR1.2.1 and CR4.2.2.

The **acceptance limit AL1.2.2** (inertia is superior to existing designs) of CR1.2.2 is met if evidence is available to the INPRO assessor that a higher inertia exists in an INS compared to existing designs.

3.2.3. User requirement UR1.3 (design basis accidents)

User requirement UR1.3: *The frequency of occurrence of accidents should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.*

The term “frequency” used in UR1.3 means the calculated number of events per reactor year using probabilistic methods (PRA). The phrase “if an accident occurs” is to be interpreted that even if the probability for occurrence of a specific accident is extremely low, the plant has to be designed to cope with it.

The term “controlled state” used in the UR1.3 is characterized by a situation in which the engineered safety features are able to compensate for the loss of functionality resulting from the accident. An optimized combination of active and passive engineered safety features should be used. For an INS it might be possible that passive design features could achieve almost all of the fundamental safety functions. For a nuclear reactor these features could include passive shutdown, passive decay heat removal systems and passively operated coolant injection systems.

INPRO has defined the following criteria for UR1.3:

Table 3.2.4. Criteria for user requirement UR1.3

UR1.3 (Design basis accidents): <i>The frequency of occurrence of accidents should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.3.1 frequency of DBA	
IN1.3.1: Calculated frequency of occurrence of design basis accidents.	AL1.3.1: Reduced frequency of accidents that can cause plant damage relative to existing facilities.
CR1.3.2 grace period	
IN1.3.2: Grace period until human intervention is necessary.	AL1.3.2: Increased relative to existing facilities.
CR1.3.3 safety features	
IN1.3.3: Reliability of engineered safety features.	AL1.3.3: Equal or superior to existing designs.
CR1.3.4 barriers	
IN1.3.4: Number of confinement barriers maintained.	AL1.3.4: At least one.

Table 3.2.4. Criteria for user requirement UR1.3 (continued)

UR1.3 (Design basis accidents): <i>The frequency of occurrence of accidents should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.(continued)</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.3.5 controlled state	
IN1.3.5: Capability of the engineered safety features to restore the INS to a controlled state (without operator actions).	AL1.3.5: Sufficient to reach a controlled state.
CR1.3.6 sub criticality	
IN1.3.6: sub criticality margins.	AL1.3.6: Sufficient to cover uncertainties and to allow adequate grace period.

3.2.3.1. Criterion CR1.3.1 (frequency of DBA)

Indicator IN1.3.1: *Calculated frequency of occurrence of design basis accidents.*

Acceptance limit AL1.3.1: *Reduced frequency of accidents that can cause plant damage relative to existing facilities.*

For the design of safety systems a limited number of so-called “Design Basis Accidents (DBAs)” have been defined. The selection of different accident sequences is based on operating experience and analytical evaluations. For existing water-cooled reactors, DBAs range from operational transients without loss-of-coolant up to medium and large break LOCAs.

As mentioned above the frequency of occurrence of DBA is to be determined via probabilistic risk analysis (PRA). From operating experience (more than ten thousand reactor years of operation) and analytical assessments (PSA, see also criterion CR4.4.1) the correlation between the frequency of occurrence and different consequences (e.g., damage or dose) is such that the consequences increase with decreasing frequencies of occurrence (Figure 3.2.3). Note that medium and large break LOCAs have not occurred at all up to date in existing reactors.

As an example of desirable frequencies F of occurrence of design basis accidents for LWRs, INPRO defined for a small break LOCA the value of F_{SB} :

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

and for a large break LOCA:

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

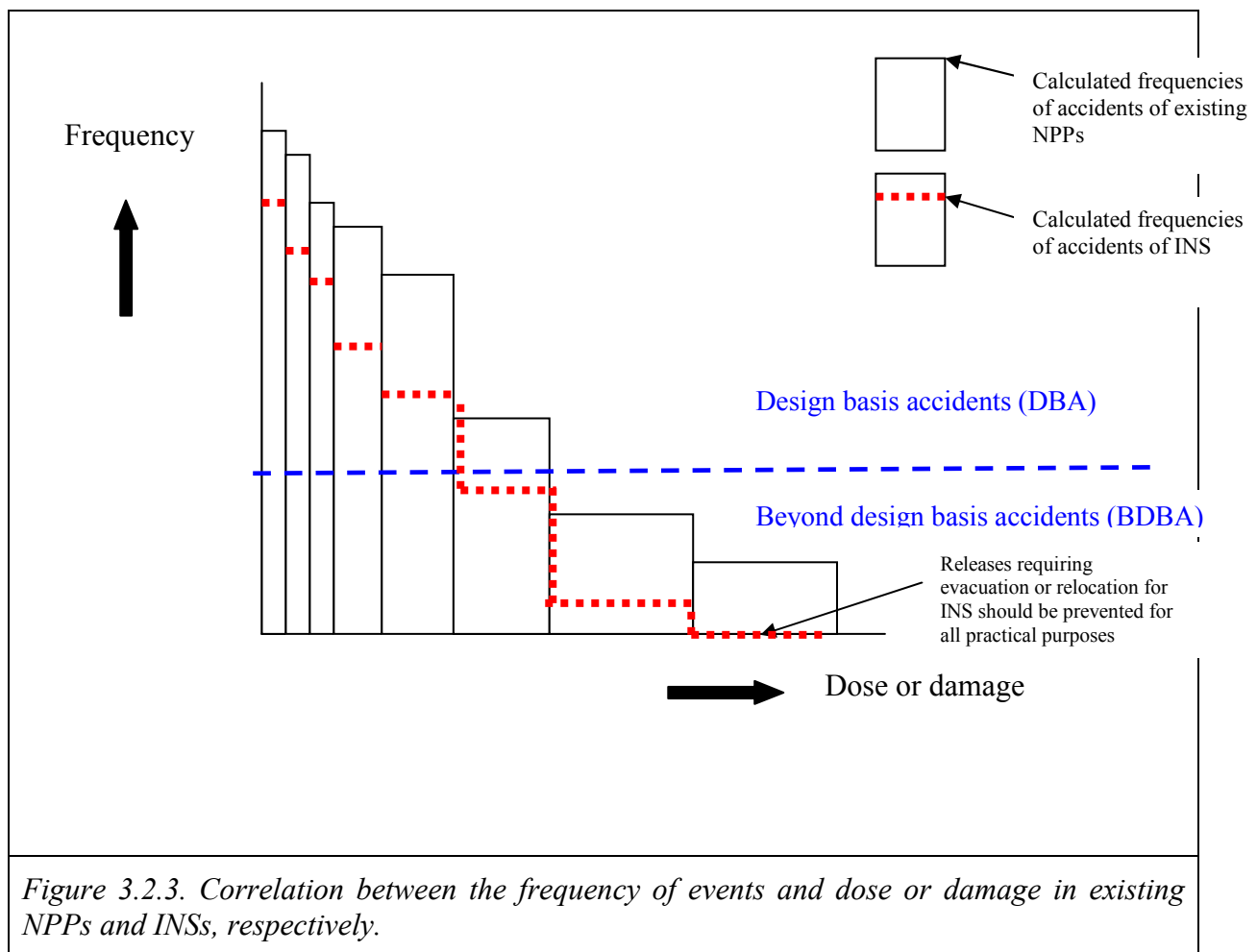
The above defined frequencies F_{SB} and F_{LB} could be used as INPRO acceptance limits for that specific DBA of LWRs.

Because analytical assessments are required besides operating experience, validated computer codes with “best-estimate” models and detailed plant simulation have to be used.

Lower frequencies of occurrence of accidents in INS can be achieved by an increase in robustness (see UR1.1) and improved capability of I&C techniques (see UR1.2).

The correlation between the probability of occurrence (i.e. the calculated frequency) and dose or damage to an individual or the public is schematically shown in Fig. 3.2.3.1. It illustrates three issues:

- The higher the damage the lower the frequency;
- The frequency of transients or accidents in INS are to be lower than in current designs; and
- Releases requiring evacuation or relocation should be prevented in INS for all practical purposes.



The **acceptance limit AL1.3.1** (Reduced frequency of accidents that can cause plant damage relative to existing facilities) of CR1.3.1 is met if evidence is available to the INPRO assessor that the INS shows lower frequencies of accidents with respect to existing comparable designs. For an INS, these frequency values, as well as the consequences of accidents, imply larger uncertainty ranges than those for existing reactors.

3.2.3.2. Criterion CR1.3.2 (grace period)

Indicator IN1.3.2: *Grace period until human intervention is necessary.*

Acceptance limit AL1.3.2: *Increased relative to existing facilities.*

The indicator “grace period until human action is necessary” implies the same concept as introduced earlier for control of abnormal operation (see CR1.2.2). For DBA it requires that actions of automatic and/or passive safety systems provide a grace period for the operator.

Because the control of DBAs has a very high importance – the next DID level would be the potential for a highly degraded core – the grace period available for operators within this DID level should be longer than for abnormal occurrences. An indication may be the shift change of operators every 8 hours, because a new operator crew will take over responsibility and possibly bring fresh insights into accident diagnosis. Such a longer grace period results in extended design requirements as compared with those for abnormal occurrences, mainly longer fully automated system responses (e.g., emergency power supply, residual heat removal, battery power for I&C, etc.).

For innovative designs, passive safety systems may reduce the need for emergency power supply (via diesels or turbines) for active residual heat removal systems.

Sufficient battery power is required for the I&C systems to identify and assess the plant state and execute necessary actions. Usually battery power is used for many purposes (e.g., instrumentation, valves, lighting, etc.). The capacity of batteries in existing reactors is designed to use this power for all purposes for about 2 – 4 hours. It is, however, possible to stretch the battery power for a longer period, if the supply of components not necessary to cope with an incident or accident is interrupted and the remaining power is used for absolutely needed functions such as monitoring purposes. In addition, a recharge of batteries from outside the containment should be possible in case the access to the compartments with the batteries is not possible.

The **acceptance limit AL1.3.2** (increased grace period relative to existing facilities) of CR1.3.2 is met if evidence is available to the INPRO assessor that the INS in case of DBA has a grace period of at least 8 hours.

3.2.3.3. Criterion CR1.3.3 (safety features)

Indicator IN1.3.3: *Reliability of engineered safety features.*

Acceptance limit AL1.3.2: *Equal or superior to existing designs.*

Enhanced “reliability of engineered safety features” may be achieved by inclusion of passive systems into the INS design, although other methods can also be effective.

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

- Identification of initiating reference events and their frequencies of occurrence (see criterion CR1.3.1);
- Determination of the unavailability of system functions considered in the event sequences, taking human factors (see criterion CR1.7.1 and CR1.7.2) and common cause failures (see below) into account; and
- 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 (HTRs), 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 engineered safety systems as well as for I&C systems.

Because the reactor protection system (RPS) is the most important I&C system, some more details will be given below as an example.

The RPS implements the following safety functions:

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

The RPS encompasses all associated equipment including individual measuring instruments for process parameters up to component actuation devices. The RPS has to meet several design criteria:

- Fail-safe principle: The RPS is designed that, if it should fail, it will settle in a safe state;
- Single-failure criterion: The RPS must retain its functional capability even in case of a single failure accompanied by simultaneous unavailability of another component due to repair or maintenance;
- Diversity principle and implementation of diverse process variables: The RPS measures at least two different process parameters for one objective. For an INS passive signal indicators are possible;
- Independence from other systems: The RPS is separated from the control system and other automation systems;
- Control and monitoring: In the main control room, the operators are provided at all times with reliable information on the status of the RPS;
- Periodic testing: The functions of the RPS can also be tested during operation of the plant. These tests ensure that the design basis functional requirements are met;
- Self-diagnosis, validation of input signals and actuation signals: The RPS is designed that it monitors the validity of input and output signals and its internal electronic operation and issues alarm signals when needed. The self-diagnosis capabilities should be adequate and should cover hardware and software faults; and
- Separation from other I&C systems: The RPS should be functionally and physically separated from other systems.

Needed reliability data for an INS are taken from operating experience of similar plants or at least similar components. For new components of an INS, R&D efforts might be necessary, (see criterion CR4.2.1); otherwise conservative data have to be used.

As in other facilities, operator intervention is necessary in nuclear plants for plant operating purposes at least after some time. There are evaluation methods available to assess the reliability of intervention of plant operating staff [32].

Common Cause Failure (CCF) means the coincidence of several identical component failures due to common cause (dependencies). These have to be taken into account especially for redundant safety systems. Therefore, one should assume for redundant safety systems– e.g., for the assessments of LWRs – not a lower frequency than 10^{-4} /yr [33].

The reliability to cope with abnormal operations and accidents can be improved by installing redundant and diverse safety systems and to implement passive components and/or systems.

Systems with passive components are very often more reliable due to missing (or reduced number of) active components; in addition, no human actions are needed and no human errors can occur. IAEA has defined four categories for passive systems [34], as indicated in Table 3.2.5 below.

Table 3.2.5. Categories of passive systems [34] (X = function included)

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)
<i>Examples</i>	<i>Fuel cladding, pressure boundary.</i>	<i>Cooling system based on natural circulation.</i>	<i>Accumulators, filtered venting activated by rupture discs.</i>	<i>Emergency core cooling, based on gravity driven fluids and activated by battery-powered valves.</i>

For instance, category A is characterized by:

- no 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 system or a passive component have to be taken from operating experience or analytical assessments; it is evident that moving parts (e.g., valves) might decrease the reliability.

It is common engineering practice to apply an unidentified “single failure” in the design of a safety system; the “single failure” is selected to represent the worst failure.

For the design of an INS it is important to incorporate the possibility of repair of components. In principle, there are three possibilities:

- provision of an additional system (as has been done in Germany; it is the most expensive solution);
- provision of only redundant “active” components (e.g., pumps) and no redundancy for passive components (e.g., pipes); this design has been chosen for the EPR design;
- For most existing reactors specific repair periods are licensed, i.e. for these repair periods the overall risk is only marginally increased.

In Table 3.2.6 some reliability data for a PWR and different initial conditions (events) are given.

Table 3.2.6. Frequencies of reliability of engineered safety systems [28]

Event	Probability of failure of engineered safety system per demand and unit
Loss of heat sink.	$8,0 \cdot 10^{-6}$
Loss of feed water supply.	$2,1 \cdot 10^{-5}$
Breaks in reactor coolant pipe > 200 cm ² .	$< 3 \cdot 10^{-3}$
Breaks in reactor coolant pipe 80 to 200 cm ² .	$3,5 \cdot 10^{-3}$
Breaks in reactor coolant pipe 2 to 12 cm ² .	$1,1 \cdot 10^{-3}$
ATWS during loss of main feed water.	$8,4 \cdot 10^{-3}$

The **acceptance limit AL1.3.3** (sufficient reliability of engineered safety features) of CR1.3.3 is met if evidence is available to the INPRO assessor that the INS in case of a DBA shows equal or higher reliability than existing designs.

3.2.3.4. Criterion CR1.3.4 (barriers)

Indicator IN1.3.4: *Number of confinement barriers maintained.*

Acceptance limit AL1.3.2: *At least one.*

The indicator “number of barriers maintained” and the corresponding acceptance limit “at least one” means that the design of engineered safety features should deterministically provide for continued integrity at least of one barrier (containing the radioactive material) following any design basis accident. Alternatively, the probability of losing all barriers could be used as an INPRO indicator with a sufficient low value of it as acceptance limit.

The strategy for DID is twofold: first, to prevent accidents and, second, if prevention fails, to limit their potential consequences and prevent any evolution to more serious conditions. 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 activity of the material, on the possible loads on the different barriers and, evidently, on the reactor design itself.

For water cooled reactors at power operation, barriers confining the fission products are typically the fuel matrix (partially), the fuel cladding, the pressure boundary of the reactor coolant system, and finally the containment system.

Because the last barrier against a release of radioactive material into the environment is so important, the containment/confinement system must be well designed and carefully maintained.

As an example the following table shows the minimum number of barriers maintained for different transients or accidents in water-cooled reactors.

Table 3.2.7. Minimum number of barriers maintained for different accidents in water-cooled reactors

Transient or accident	Minimum number of barriers maintained	Examples of barriers
Without loss-of-coolant inside containment.	At least two.	Intact coolant pressure boundary; Intact containment; Depending on the severity of the accident the fuel rods may remain intact.
With loss-of-coolant inside containment.	At least one.	Intact containment; Depending on the severity of the accident the fuel rods may remain intact.
With loss-of-coolant outside containment.	At least two.	Intact containment and isolation valves in the broken pipe and/or confinement of the leakage; Intact coolant pressure boundary; Depending on the severity of the accident the fuel rods may remain intact.

An additional requirement for water-cooled reactors is the permanent or periodic measurement of leak tightness of the containment.

For HTRs the main barrier is the kernel with fuel particles (coated particles) [35]. For molten salt reactors the barriers kept correspond to those in Table 3.2.7, except that fuel rod integrity is not relevant. Different barriers exist also for designs with a double pressure vessel or designs with submerged (in water) pressure vessels (Refs [6] and [36]).

In any case, the **acceptance limit AL1.3.4** (one barrier is to remain after DBA) of CR1.3.4 is met if evidence is available to the INPRO assessor that confirms, deterministically, at least one remaining barrier against a release of fission products to the environment, or, probabilistically, a very low probability of failure of all barriers in an INS.

3.2.3.5. *Criterion CR1.3.5 (controlled state)*

Indicator IN1.3.5: *Capability of the engineered safety features to restore the INS to a controlled state (without operator actions).*

Acceptance limit AL1.3.5: *Sufficient to reach a controlled state.*

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 the accident. The reactor must be taken to a safe shutdown state at least within the designed grace period with the assurance that sufficient core cooling exists. For this purpose an optimized combination of active and passive engineered safety features should be used.

For INS, it might be possible that passive design features could include 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.

The **acceptance limit AL1.3.5** (sufficient capability of engineered safety features) of CR1.3.5 is met if evidence is available to the INPRO assessor confirming that the engineered safety features in an INS are sufficient to reach a controlled state after a DBA based on automatic

actions within a grace period of at least 8 hours. Passive safety systems can be equally capable and should be prioritized.

3.2.3.6. Criterion CR1.3.6 (sub criticality)

Indicator IN1.3.6: *Sub-criticality margins.*

Acceptance limit AL1.3.6: *Sufficient to cover uncertainties and to allow an adequate grace period.*

The indicator “sub-criticality margins” applies (after an accident) both to nuclear reactors (shutdown depth), and to a fuel cycle facility, interpreted as preventing accumulation of fissile material or critical geometries.

Reactivity is an expression for the percentage of excess neutron population in the core. Its magnitude and its behavior as a function of time depend primarily on the composition of the fuel (enrichment, burn-up), the distribution of the fuel within the core and its temperature, on the neutron physics properties of the coolant (temperature, void content), on the positions and heights of insertion of the control rods (if existing) and on the degree of the supplemental burnable poisons (if used).

In designing a reactor core, on the one hand, the core must possess sufficient excess reactivity over the complete cycle to achieve the required cycle length while, on the other hand, sufficient shutdown reactivity must be available to make the core sub-critical in the shortest possible time and to reliably keep it sub-critical.

Shutdown systems are very plant-specific; they range from control rods to be inserted to neutron poison injected or added; in most cases (existing designs) a back-up system with a different physical mechanism is added to the primary shutdown system.

The **acceptance limit AL1.3.6** (Sufficient sub criticality margin) of CR1.3.6 is met if evidence is available to the INPRO assessor that confirms for the minimum shutdown reactivity margin the generally agreed value of 1 % $\Delta k/k$ including a consideration of uncertainties and of a worst single failure in the shutdown system.

3.2.4. User requirement UR1.4 (release into containment)

User requirement UR1.4: *The frequency of a major release of radioactivity into the containment / confinement of an INS due to internal events should be reduced. Should a release occur, the consequences should be mitigated.*

For innovative designed reactors the reliability of systems in controlling complex accident sequences should be increased, including instrumentation, control and diagnostic systems. Thus, the frequency of a major radioactivity release into the containment may be reduced.

INPRO selected the following criteria for user requirement UR1.4:

Table 3.2.8. Criteria for user requirement UR1.4

UR1.4 (Release into the containment): <i>The frequency of a major release of radioactivity into the containment / confinement of an INS due to internal events should be reduced. Should a release occur, the consequences should be mitigated.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.4.1 major release into containment	
IN1.4.1: Calculated frequency of major release of radioactive materials into the containment / confinement.	AL1.4.1: At least an order of magnitude less than existing designs; even lower for installations at urban sites.
CR1.4.2 processes	
IN1.4.2: Natural or engineered processes sufficient for controlling relevant system parameters and activity levels in containment/confinement.	AL1.4.2: Existence of such processes.
CR1.4.3 accident management	
IN1.4.3: In-plant severe accident management.	AL1.4.3: Procedures, equipment and training sufficient to prevent large release outside containment / confinement and regain control of the facility.

3.2.4.1. Criterion CR1.4.1 (major release into the containment)

Indicator IN1.4.1: *Calculated frequency of major release of radioactive materials into the containment / confinement.*

Acceptance limit AL1.4.1: *At least an order of magnitude less than existing designs; even lower for installations at urban sites.*

A probabilistic safety assessment (PSA) determines the balance of the safety concept and the overall level of safety via a qualitative and quantitative assessment of active and passive safety systems. Thus, PSA achieves the key objective to review the plant design, which is performed according to deterministic principles.

After an accident, a highly degraded core with a release of volatile fission products from the core will result if safety systems are not able to keep or restore the core in a safe state. Usually, the volatile fission products will be released into the containment/confinement atmosphere. Depending on the design, liquid or 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 LWR by a core/concrete-interaction. The calculated frequency of the releases into the containment/confinement is a major result of a PSA.

To reduce the releases of fission products from the RPV appropriate countermeasures may be installed in innovative reactor designs, e.g., vessel-internal core catchers or outside cooling of the RPV (see Annex A).

Also during shutdown, a highly degraded core may result due to failures of safety systems. Therefore, during the design phase operational power as well as shutdown states have to be analyzed.

In Table 3.2.9 examples are given for several modern reactor designs (Advanced CANDU reactor ACR, Refs [37] and [38]; EPR [56]; AP1000 [57], SWR1000 [50]).

Table 3.2.9. Frequency for a highly degraded core per unit and year

Type of reactor	Frequency of core damage per year
ACR [37] [38]	
- Shut down	$7.8 \cdot 10^{-9}$
- Power operation	$3.4 \cdot 10^{-7}$
EPR (power operation plus shutdown) [56]	
- Internal events	$6.0 \cdot 10^{-7}$
- Internal and external events,	$2.0 \cdot 10^{-6}$
AP1000 [57]	
- Internal events at power operation	$3.0 \cdot 10^{-7}$
SWR1000 [50] (with AM measures)	
- Shut down	$4.1 \cdot 10^{-8}$
- Power operation	$4.3 \cdot 10^{-8}$

The **acceptance limit AL1.4.1** is met if evidence is available to the INPRO assessor that calculated frequencies of a highly degraded core of an INS are well below the recommended value by IAEA of 10^{-5} per year and unit [12], taking uncertainties into account.

3.2.4.2. Criterion CR1.4.2 (processes)

Indicator IN1.4.2: *Natural or engineered processes sufficient for controlling relevant system parameters and activity levels in containment/confinement.*

Acceptance limit AL1.4.2: *Existence of such processes.*

Releases into the containment can be controlled or mitigated by, e.g., spray systems, thereby reducing the potential for a large release outside containment.

If a plant reaches a state with a highly degraded core, active or passive engineered processes or natural processes should be available to reduce the load on the containment barrier and to reduce and/or control the activity in the containment atmosphere.

Measures to meet these objectives are very reactor design-specific, e.g., measures for molten salt reactors and HTRs are quite different from those for water-cooled reactors. During the design phase of innovative designs special attention should be given to consider related preventive and mitigative processes and measures.

In Table 3.2.10 some measures to meet these objectives for water-cooled reactors are presented as an example.

Table 3.2.10. Relevant system parameters applicable at least for water-cooled reactors

System Parameter	Processes	Explanations
Water level inside RPV.	Restoration of water injection. Water injection from sources outside containment (AM).	The core melt might be stopped. (as occurred in the TMI 2 accident).
Water level in the containment.	Restoration of water injection. Water injection from sources outside containment (AM).	The reactor pressure vessel could be cooled from the outside; the melt progression might be stopped.
Activity level in containment.	Scrubbing of fission products in water pools (potential in some reactors designs). Scrubbing of fission products by sprays (AM). Outside or inside cooling of containments. Containment internal filters or cleaning systems.	Scrubbing is a very effective method to reduce the activity level in the containment atmosphere. Another measure is condensation of steam on cooled structures. Containment internal filters will reduce the activity level.
Containment pressure.	Venting to the environment via filter after about 1 week (in case of no leakages) or earlier in case of leakages; a hydrogen re-combiner should be installed in case the containment is not inerted.	Outside or inside cooling of containments will limit the pressure. Venting should be delayed for pressures below the design pressure and as long as no major release of radioactive material into the environment occurs.

The **acceptance limit AL1.4.2** is met if evidence is available to the INPRO assessor that such mechanisms and systems (processes) are included in the INS design.

3.2.4.3. Criterion CR1.4.3 (accident management)

Indicator IN1.4.3: *In-plant severe accident management.*

Acceptance limit AL1.4.3: *Procedures, equipment and training sufficient to prevent large release outside containment / confinement and regain control of the facility.*

In-plant severe accident management (AM) measures give the operator tools to prevent a further release into the containment/confinement and/or to reduce the concentration of radio-nuclides already there.

Besides the use of designated safety systems all plants have a potential to use other (operational) systems to regain control of the facility. In the past in some cases the components of such systems had to be improved or modified (e.g., ranges of instrumentation) to be used in accident situations.

The in-plant AM measures and actions in case of a highly degraded core are very plant-specific. For innovative reactor designs related measures should be considered from the beginning of the design.

For water-cooled reactors examples for appropriate AM actions are given below:

- Injection of boron (e.g., for ATWS) into the core;
- Depressurization of RPV;
- Restoration of water injection into the RPV as well as into the containment;
- Restoration of heat removal;
- Spraying into the containment atmosphere; and
- Containment venting.

Experiences from existing reactors with installed accident management measures have shown that the feasibility and effectiveness of AM procedures have to be demonstrated and have to be trained sufficiently. The use of a local and/or regional emergency support center (ESC) could be a useful measure; however, it is the national decision to what extent a local and/or regional ESC should influence and guide plant-internal measures.

The **acceptance limit AL1.4.3** is met if evidence is available to the INPRO assessor that procedures, equipment and training are available, sufficient to prevent large releases to environment and regain control of the facility.

3.2.5. User requirement UR1.5 (release into environment)

User Requirement UR1.5: *A major release of radioactivity from an installation of an INS should be prevented for all practical purposes, so that INS installations would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose.*

The user requirement UR1.5 addresses the issue that, if nuclear energy is to play a major role in the future, there will be many more plants, and they must be able to be easily sited. Some countries have the good fortune to have numerous large remote sites, but many do not; hence safety of an innovative plant should not rely heavily on distance from population.

Engineered safety features of innovative reactors and fuel cycle installations should be able to control severe accident (beyond design basis) scenarios and mitigate their consequences, so as to prevent containment failure. Control and mitigation should address all threats (internal and external).

Thus innovative designs should show that:

- The likelihood of a large release is so small that off-site emergency measures, while they may reduce the consequences thereof, do not lead to a significant reduction in risk²³; or
- A large release could be excluded by design for all practical purposes, e.g., through use of inherent safety characteristics.

Consequently, for an INS there should be no need for an offsite emergency plan, which is different in kind from the plan for *any* industrial facility used for a similar purpose.

INPRO selected the following criteria for user requirement UR1.5:

²³ Defined as the product of a calculated frequency multiplied by the potential consequences of this scenario.

Table 3.2.11. Criteria for user requirement UR1.5

UR1.5 (Release to the environment): <i>A major release of radioactivity from an installation of an INS should be prevented for all practical purposes, so that INS installations would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.5.1 major release to environment	
IN1.5.1: Calculated frequency of a major release of radioactive materials to the environment.	AL1.5.1: Calculated frequency $<10^{-6}$ per unit-year, or practically excluded by design.

Table 3.2.11. Criteria for user requirement UR1.5 (continued)

UR1.5 (Release to the environment): <i>A major release of radioactivity from an installation of an INS should be prevented for all practical purposes, so that INS installations would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose. (continued)</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.5.2 consequences	
IN1.5.2: Calculated consequences of releases (e.g., dose).	AL1.5.2: Consequences sufficiently low to avoid necessity for evacuation. Appropriate off-site mitigation measures (e.g., temporary food restrictions) are available.
CR1.5.3 risk	
IN1.5.3: Calculated individual and collective risk.	AL1.5.3: Comparable to facilities used for a similar purpose ²⁴ .

The accidents at TMI-2 (with no major release of radioactive products to the environment) and Chernobyl (with a major release of radioactive products to the environment) have sensitized the public regarding the releases of radioactive elements into the environment. Therefore, it is generally agreed that for any postulated accident in an INS even with a highly degraded core no special offsite emergency plan should be necessary.

3.2.5.1. Criterion CR1.5.1 (major release into environment)

Indicator IN1.5.1: *Calculated frequency of a major release of radioactive materials into the environment.*

Acceptance limit AL1.5.1: *Calculated frequency $<10^{-6}$ per unit-year, or practically excluded by design.*

²⁴ E.g., an oil refinery would be analogous to an enrichment facility; a chemical plant would be analogous to a fuel reprocessing facility; a coal-fired power plant would be analogous to a nuclear power plant.

For innovative designs the calculated radioactive releases to the environment are required to be so low that there is no necessity for evacuation or relocation measures outside the plant site (nevertheless plans for such measures must be provided to gain or increase the public acceptance for deployment of nuclear facilities).

The frequency of a major release of radioactive material into the containment/confinement has been dealt with in criterion CR1.4.1. The frequency of a major release of radioactive products into the environment is the frequency of a major release into the containment/confinement multiplied by the frequency of a containment failure. Examples for causes of containment failures are overpressure, hydrogen burns and penetration of the base plate by a molten core-concrete interaction (mainly for water reactors). Via a PSA the frequency of a containment failure including uncertainties should be estimated.

While the most widespread existing reactor designs (i.e. water-cooled reactors) place emphasis on preventive (i.e. low frequencies of a release into the containment) as well as on mitigative measures (i.e. low frequency of a containment failure) other designs, e.g., HTRs, place the major emphasis on preventive measures. It should also be noted that sabotage and extreme external events also set requirements for the design of containments.

Examples for design measures against melt-through of the basement floor of advanced water reactors are given in Ref. [6], e.g., so-called core catchers in the EPR or advanced VVER 1000 designs, the RPV internal retention device for the SWR1000, and the water-filled shield tank in the ACR.

Existing (i.e. operating at the end of 2004) reactor containments have originally not been designed to cope with loads resulting from core melts. Nevertheless, only a reduced number of sequences with a highly degraded core may result in a major release of fission products into the environment, e.g., failure of the liner, overpressure failure, core-concrete interaction, and hydrogen burn [39].

The following table gives some results of frequencies of calculated containment failures for modern reactor types.

Table 3.2.12. Frequencies of containment failures in modern reactors

Plant	Frequency/yr of sum of containment failure modes
EPR	
- early containment failure	$4.0 \cdot 10^{-8}$
- late containment failure	$6.0 \cdot 10^{-8}$
AP1000	$2.0 \cdot 10^{-8}$

It is evident from the table above that the examples of modern reactors shown above do meet the INPRO requirement to avoid the necessity for evacuation or relocation outside the plant site.

The **acceptance limit AL1.5.1** is met if evidence is available to the INPRO assessor that the frequency for a major release of radioactivity into the environment is well below 10^{-6} per unit-year [12] or practically excluded by design. This acceptance limit allows for enough freedom to put more emphasis on preventive instead of mitigative measures. For an urban site, with for example district-heating facilities, a lower value might be required by local authorities.

3.2.5.2. Criterion CR1.5.2 (consequences)

Indicator IN1.5.2: *Calculated consequences of releases (e.g., dose).*

Acceptance limit AL1.5.2: *Consequences sufficiently low to avoid necessity for evacuation. Appropriate off-site mitigation measures (e.g., temporary food restrictions) are available.*

The dose criteria (mSv) for countermeasures according to ICRP [40] are:

Table 3.2.13. Countermeasures and doses in mSv

Countermeasures	..may be justified in case of a dose of	..almost always justified	Dose of
Short-term sheltering.	5 – 50 mSv	50 mSv	Whole body.
Iodine tablets.	50 – 500	500	Thyroid.
Evacuation (< one week).	50 – 500	500	Whole body.
Evacuation.	500 – 5000	5000	Equivalent dose to skin.
Long-term food-control.		10 in 1 year.	Whole body.
Relocation.	5 – 15 per month.	1000 in 50 years.	Whole body.

Containments, e.g., of water reactors, are nominally leak-tight²⁵. Under severe accident conditions, due to leakages (usually specified between 0.25 – 1 vol.% per day) and a pressure increase radioactive material could be released to compartments outside the containment, usually a surrounding building or annulus and then released to the environment via a stack (usually around 150 m high) or directly through other small leakage paths. In the analysis of consequences after a severe accident filter efficiencies and natural fission products retention mechanism usually are conservatively not be taken into account. Of further importance for calculating dose loads are the magnitude of given activity inventories, the physical and chemical form of given inventories and models and parameters applied as a basis for calculating atmospheric dispersion of radioactive material as well as radiation exposure.

In designs with confinements, e.g., for HTRs, temporary openings allow a pressure reduction and therefore, for those designs release of fission products into the confinement must be low, see also criterion CR1.5.1.

Dose calculations should be performed with validated computer codes; these calculations must include uncertainty analyses (see also CR4.4.2).

The **acceptance limit AL1.5.2** for INS is met if evidence is available to the INPRO assessor that in the design basis of the INS the calculated consequences of releases are sufficient low to meet the requirement that no evacuation or relocation is needed outside the plant site; temporary food restrictions are possible.

3.2.5.3. Criterion CR1.5.3 (risk)

Indicator IN1.5.3: *Calculated individual and collective risk.*

Acceptance limit AL1.5.3: *Comparable to facilities²⁶ used for a similar purpose.*

If nuclear energy is to play a major role in future, the calculated nuclear risk has to be comparable to the risk of other facilities used for the similar purpose.

In a German risk study [28], the health risks of energy conversion systems have been compared. Such a comparison is difficult because use of fossil energy or renewable energy

²⁵ Leak tight means a leakage rate which stays within specified limits

²⁶ E.g., an oil refinery would be analogous to an enrichment facility; a chemical plant would be analogous to a fuel reprocessing facility; a coal-fired power plant would be analogous to a nuclear power plant.

sources cause damages mainly locally within a region and for the present generation while damages from radiation exposures usually are more global and are effecting also future generations. In this study the “Years of Life Lost (YOLL)” for a production of 1 TWh (i.e. 1 Billion kWh) has been selected as the comparative parameter. The Figure 3.2.5 below demonstrates the low risk from power production (no evacuation and relocation has been assumed – as it is required for an INS).

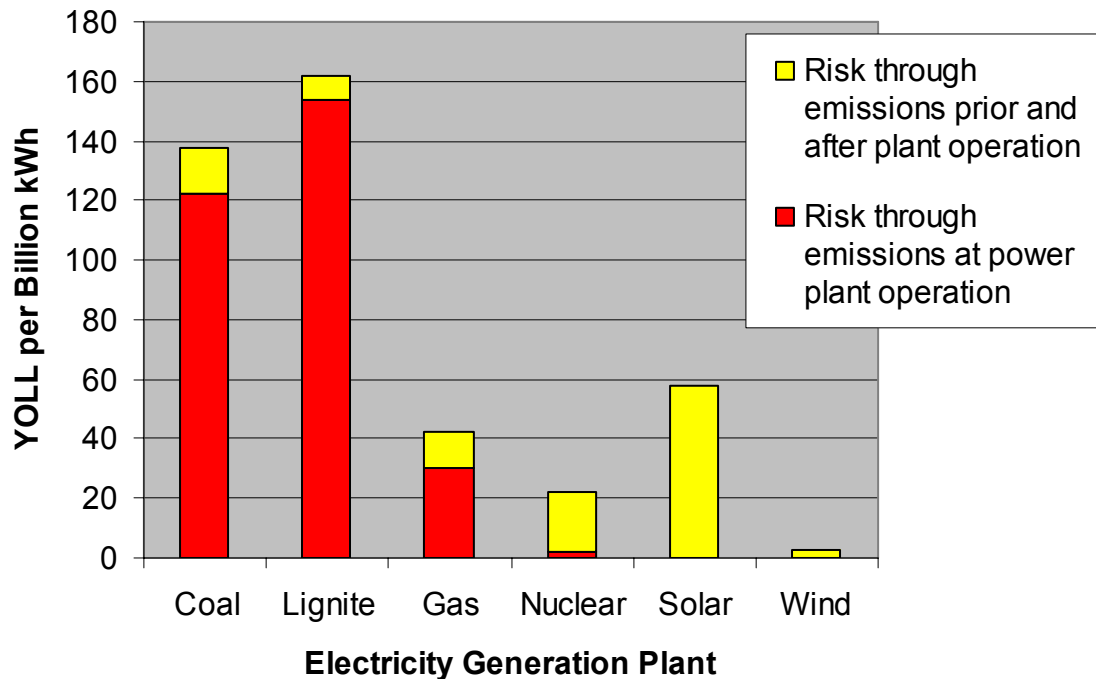


Figure 3.2.5. Cumulative years of lost life (YOLL) per billion of kWh produced by different energy conversion technologies [41].

The **acceptance limit AL1.5.3** is met if evidence is available to the INPRO assessor that the INS shows a risk comparable to other facilities used for similar purposes.

3.2.6. User requirement UR1.6 (independence of DID levels)

User requirement UR1.6: *An assessment should be performed for an INS to demonstrate that different levels of defence-in-depth are met and are more independent from each other than for existing systems.*

A safety assessment should be performed using a suitable combination of deterministic and probabilistic approaches, or hazards analysis.

INPRO has chosen the following criterion for UR1.6:

Table 3.2.14. Criterion for user requirement UR1.6

UR1.6 (Independence of DID levels): <i>An assessment should be performed for an INS to demonstrate that different levels of defence-in-depth are met and are more independent from each other than for existing systems.</i>	
Criterion (CR)	
Indicator (IN)	Acceptance Limit (AL)
CR1.6.1 independence of DID levels	
IN1.6.1: Independence of different level of DID.	AL1.6.1: Adequate independence is demonstrated, e.g., through deterministic and probabilistic means, hazards analysis etc.

3.2.6.1. Criterion CR1.6.1 (independence of DID levels)

Indicator IN1.6.1: *Independence of different levels of DID.*

Acceptance limit AL1.6.1: *Adequate independence is demonstrated, e.g., through deterministic and probabilistic means, hazards analysis etc.*

A method for assessing the DID capabilities of a reactor plant is described in Ref. [42].

The different levels of DIDs 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 (Level 5).

Design assessments could be quite different for different reactor designs. It is evident that inherent safety characteristics (see also CR2.1.1) increase the independence of the different DID levels. Another question is if a system (e.g., I&C or a specific safety system) covers more than one level of defence.

A PSA [31], if done carefully, will quantify the independence of the levels of DID (or more usually will highlight areas where they are not independent).

A PSA should identify:

- Cross-links which compromise the independence of the levels of DID;
- The need for human actions²⁷; and
- The reliability of passive safety systems and inherent characteristics relative to active – redundant and diverse – safety systems.

One result of a PSA are frequency ranges of reaching the different levels of DID; the goal for an INS are frequency ranges below (superior to) those of existing reactors or of recommended values (e.g., by IAEA). PSA can be supplemented by qualitative techniques using experts, such as formal design reviews.

The **acceptance limit AL1.6.1** is met if evidence is available to the INPRO assessor that demonstrates adequate independence of the different levels of DID based on deterministic and probabilistic methods.

²⁷ For INS the grace period ranges from 30 minutes for level 2 up to at least 8 hours for level 3 and 4; inherent safety characteristics will decrease the need for human actions. Note that human actions can both contribute to plant robustness (enhanced DID) and compromise it (via an incorrect accident diagnosis). Longer grace periods increase the chance for correct human actions.

3.2.7. User Requirement UR1.7 (human machine interface)

User Requirement UR1.7: *Safe operation of installations of an INS should be supported by an improved Human Machine Interface resulting from systematic application of human factors requirements to the design, construction, operation, and decommissioning.*

The designer of an INS should 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 should be taken into account in this process.

INPRO selected the following criteria for user requirement UR1.7:

Table 3.2.15. Criteria for user requirement UR1.7

UR1.7 (human machine interface): <i>Safe operation of installations of an INS should be supported by an improved Human Machine Interface resulting from systematic application of human factors requirements to the design, construction, operation, and decommissioning.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR1.7.1 human factors	
IN1.7.1: Evidence that human factors (HF) are addressed systematically in the plant life cycle.	AL1.7.1: Satisfactory results from assessment.
CR1.7.2 human response model	
IN1.7.2: Application of formal human response models from other industries or development of nuclear-specific models.	AL1.7.2: - Reduced likelihood of human error relative to existing plants, as predicted by HF models. - Use of artificial intelligence for early diagnosis and real-time operator aids. - Less dependence on operator for normal operation and short-term accident management relative to existing plants.

3.2.7.1. Criterion CR1.7.1 (human factors)

Indicator IN1.7.1: *Evidence that human factors (HF) are addressed systematically in the plant life cycle.*

Acceptance limit AL1.7.1: *Satisfactory results from assessment.*

The importance of the human factor for safe and reliable operation of NPPs is recognized by everyone and is an issue that should be dealt with systematically for each reactor [39].

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, the 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:

- Errors in plant operation, testing or maintenance, liable to contribute to the failure of systems or to their unavailability;
- Errors in plant operation, testing or maintenance giving rise to an initiating event; and
- Interventions in incident or accident situations, liable to influence the sequence of events with, on the one side, the capability to handle unforeseen situations, but, on the other side, to perform actions only with a limited reliability.

As a common 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-machine 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 the operators and minimizes 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 will improve and thus allow more realistic representation (and prediction) of the transient plant states.

For innovative reactors a human factors engineering program plan (HFEP) is an essential part of the design.

Below some design and operational features and assessments are given, which are implemented in existing reactors but should be subject to further improvements:

- Feedback of experience including a formal methodology;
- A PSA taking human error into account;
- 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;
- Existence of a main control room, a remote shutdown station, a technical support center and the short-term installation of a local and/or regional ESC;
- Visualization of the status of equipment of the plant (components, systems, etc), the dynamics of the processes, the performance of the automated processes and their relation with the state of the plant, resulting in a guidance for operator actions;
- Monitoring by knowledge-based systems;
- Appropriate ambient conditions in the relevant rooms (e.g., main control room);
- Appropriate plant operating procedures (e.g., alarm sheets, procedures for normal operation, incident and accident situations);
- Existence of a verification of adequacy of design implementation; and
- Control of human reliability (e.g., personnel selection, periodic training, etc.).

The **acceptance limit AL1.7.1** is met if evidence is available to the INPRO assessor that human factors are considered during the lifetime of a plant including the planning-, construction-, operating- and decommissioning phase.

3.2.7.2. Criterion CR1.7.2 (human response model)

Indicator IN1.7.2: *Application of formal human response models from other industries or development of nuclear-specific models.*

Acceptance limit AL1.7.2: *Reduced likelihood of human error relative to existing plants, as predicted by HF models; use of artificial intelligence for early diagnosis and real-time operator aids; and less dependence on operator for normal operation and short-term accident management relative to existing plants.*

Although the necessity of human action in plant operation should be minimized for an INS, the knowledge about human behavior is, nevertheless, very important.

The human response to known or 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.

The human interventions prior to an event have usually not been found among the dominant risk contributors, although observations and assessments from different industrial facilities have been used [32].

Errors by personnel during operation are usually taken from documented operating experience; however, the use of data from non-nuclear facilities for evaluation of INS has to be performed carefully.

The human interactions after the initiating event represent the greatest challenge. The relevant research and developmental work in different countries, the currently used approaches and their limitations, the results of human reliability assessments and the current development tendencies are well described in Ref. [32].

To further develop confidence in human performance models, the use of simulators should be encouraged – up to now they are commonly used only for non-severe accidents (DBA). Although the environmental conditions (especially the human stress factor) in simulator training are not equivalent to real situations, a thorough evaluation of the results will assist model development.

As outlined in the sections dealing with criterion CR1.2.1 and CR1.7.1, an increased use of artificial intelligence and real-time operator aids will lower the burden on operators for normal operation and short-term response to accident situations.

The **acceptance limit AL1.7.2** for an INS is met if evidence is available to the INPRO assessor that shows a reduced likelihood of human error relative to existing reactors as predicted by HF models, the use of artificial intelligence for early diagnosis and real-time operator aids and less dependence on operators for normal operation and short-term accident management relative to existing reactors.

3.2.8. Integration of safety, security and proliferation resistance into the INS design

As already mentioned at the beginning of Chapter 3, in the INPRO area of physical protection (PP) [18] a user requirement UR2 is defined calling for the assembling of a joint panel or team of experts in the three areas of safety, proliferation resistance (PR) and PP to review designs and proposed procedures for each of the three INPRO areas to assess their impact on the other areas and on operations, and to look for ways to optimize their synergies. It is therefore recommended to ensure that this PP user requirement UR2 has been taken care of also during an INPRO assessment of nuclear safety.

3.3. INPRO basic principle BP2 (inherent safety)

Basic principle BP2: *Installations of an INS shall excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach.*

Basic principle BP2 is focused on the role of inherent safety and passive safety features in future nuclear designs. If incorporated into a design correctly, an inherent safety characteristic eliminates the cause of the hazard. Passive systems can provide additional safety margins; in such cases, deterministic 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, should be analyzed and may need to be compensated by other design measures.

INPRO has defined a single user requirement for BP1 as discussed in the following.

3.3.1. User requirement UR2.1 (minimization of hazards)

User requirement UR2.1: *INS should strive for elimination or minimization of some hazards relative to existing plants by incorporating inherently safe characteristics and/or passive systems, when appropriate.*

The design of an INS should be such that hazards should be eliminated (if possible) or minimized (e.g., by limiting explosive gases to the absolute necessary amount, or by using inherent safety features in the core design and operation to limit the excess reactivity). If hazards could not be eliminated, appropriate protective measures have to be installed. In addition, administrative measures should 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 an inherent safety characteristic is difficult but should be possible by the application of adequate mathematical models and, in some cases, by experimental investigations. Most inherent safety characteristics of power reactors are expected to be partially effective, i.e. they limit a hazard but do not eliminate it.

The user requirement is one of degree: there are likely fundamental limitations in power reactor type or power range, which prevent absolute inherent safety characteristics (e.g., for many power reactors, one needs to have available enough positive reactivity to compensate for xenon poison).

The assessment of hazards and its consequences should be performed applying deterministic and probabilistic approaches. For the deterministic approach engineering judgment, operating

experience, and a continuous exchange of information also with other industries are mandatory. For probabilistic approaches the methods should be validated (e.g., also for passive systems) and the data used be reliable. All assessments should cover all operating states including shutdowns, maintenance and repair intervals.

INPRO selected the following criteria:

Table 3.3.1. Criteria for user requirement UR2.1

UR2.1 (Minimization of hazards): <i>INS should strive for elimination or minimization of some hazards relative to existing plants by incorporating inherently safe characteristics and/or passive systems, when appropriate.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR2.1.1 hazards	
IN2.1.1: Sample parameters: stored energy, flammability, criticality, inventory of radioactive materials, available excess reactivity, and reactivity feedback.	AL2.1.1: Superior to existing designs.
CR2.1.2 frequency of AOO &DBA	
IN2.1.2: Expected frequency of abnormal operation and accidents.	AL2.1.2: Lower frequencies compared to existing facilities.
CR2.1.3 consequences	
IN2.1.3: Consequences of abnormal operation and accidents.	AL2.1.3: Lower consequences compared to existing facilities.
CR2.1.4 confidence in innovation	
IN2.1.4: Confidence in innovative components and approaches.	AL2.1.4: Validity established.

3.3.1.1. Criterion CR2.1.1 (hazards)

Indicator IN2.1.1: *Sample parameters related to hazards: Stored energy, flammability, criticality, inventory of radioactive materials, available excess reactivity, and reactivity feedback.*

Acceptance limit AL2.1.1: *Superior to existing designs.*

A list of possible evaluation parameters (EP) for this criterion is given below:

EP2.1.1.1: Stored energy.

EP2.1.1.2: Flammability.

EP2.1.1.3: Inventory of radioactive materials.

EP2.1.1.4: Criticality.

EP2.1.1.5: Available excess reactivity.

EP2.1.1.6: Reactivity feed back.

Evaluation parameter EP2.1.1.1 Stored energy

The necessary removal of the stored energy in a power generating system after a disturbance of normal operation creates a hazard. In case the heat removal system fails, damage of

components due to overheating might occur. Thus, a reduction of stored energy in an INS leads to a reduction of the corresponding hazard.

Well known examples for stored energies within the primary system of a NPP are the stored energy in the fuel mass and in the coolant. While innovative approaches may reduce the amount of stored energy in the fuel (e.g., micro particles in HTRs) the decrease of the stored energy in the coolant (mainly the pressure and temperature level and the mass of coolant) for power reactors can only be changed within a narrow range for a chosen coolant (e.g., light or heavy water), because of the design optimization of efficiency, core layout and geometries. For district heating with water reactors, the minimum pressure is determined by a necessary temperature difference (depending on the thermal-hydraulic design of the heat exchanger) between the primary coolant and warm water to be supplied to the customers.

Another well known example for stored energy outside the coolant systems are accumulators for PWRs and HWRs, which are needed for power reactors to cope with specific design basis accidents (e.g., LOCA).

Acceptability of EP2.1.1.1: For advanced reactor designs, the amount of stored energy within or outside the primary coolant system should be limited to the minimum amount possible.

Evaluation parameter EP2.1.1.2 Flammability

The possibility of a fire in a nuclear reactor represents a considerable hazard (e.g., the fire in Browns Ferry [43]). Consequently the design of advanced NPPs should minimize this hazard by reducing the amount of flammable material.

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

For metal (e.g., sodium) cooled reactors, additives to the coolant should be developed 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 CVCS) must be limited to the minimum necessary amount. For systems containing explosive gases, protection measures must 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 EP2.1.1.2: For advanced reactor designs, minimization of flammable material has been achieved.

Evaluation parameter EP2.1.1.3 Inventory of radioactive materials

The radioactive inventory within the reactor should be as low as practicable taking into account its economic purpose, e.g., for power generation (as for most reactors), for process heat, for actinide burning up to plutonium production (as for breeder reactors). In addition, the radioactive material outside the reactor should be minimized to decrease the potential for a major release in accidental situations.

Acceptability of EP2.1.1.3: For advanced reactor designs, the inventory of radioactive material has been minimized.

Evaluation parameter EP2.1.1.4 Criticality

To reduce the hazards of criticality outside the core (e.g., in fuel storages), any geometry and material that could create criticality should be avoided (e.g., by using fixed poisoned material, poisoned coolant administrative measures, inherently safe geometries, etc.).

Acceptability of EP2.1.1.4: For advanced reactor designs, a possibility for criticality outside the core is avoided.

Evaluation parameter EP2.1.1.5 Available excess reactivity

Excess reactivity should be kept to the minimum possible. However, some excess reactivity (or power control) is necessary to cope with the fuel burn-up, to reach full power operating conditions and to compensate for the peak xenon build-up.

Acceptability of EP2.1.1.5: For advanced reactor designs, excess reactivity in the core is kept as low as practicable.

Evaluation parameter EP2.1.1.6 Reactivity feed back

The feedback of changing conditions in the core should lead to self-compensation – e.g., negative feedback on a temperature increase. This could be achieved by a core design with reasonable resonance adsorption effects (Doppler), a negative moderator temperature and void coefficient, and the control of the power distribution (see also criterion CR1.1.1).

Use of passive safety systems or passive components in safety systems may result in an overall reduction of hazards, if these systems are carefully designed and maintained (e.g., capacity, reaction times, etc.); PSA should assist the selection of such systems.

Acceptability of EP2.1.1.6: For advanced reactor designs, changing conditions in the core should lead to a compensatory reactivity feedback.

Final assessment of criterion CR2.1.1 hazards

The **acceptance limit AL2.1.1** is met if evidence is available to the INPRO assessor that the innovative reactor design is superior to existing designs for most of the evaluation parameters listed above.

3.3.1.2. Criterion CR2.1.2 (frequency of AOO and DBA)

Indicator IN2.1.2: *Expected frequency of abnormal operation and accidents.*

Acceptance limit AL2.1.2: *Lower frequencies compared to existing facilities.*

An increased use of inherent safety characteristics will strengthen the prevention of abnormal operation²⁸ and accidents in nuclear reactors and should, therefore, reduce the expected frequencies thereof. The use of passive safety systems (or passive components in safety systems) may increase the reliability of safety systems. However, special considerations are necessary for shutdown states, because passive systems may require specific working conditions, e.g., temperature differences, which might not exist during shutdowns. Examples for expected frequencies of abnormal operation and accidents of existing reactors are given in the section dealing with criteria CR1.1.4 and CR1.3.1.

The **acceptance limit AL2.1.2** is met if there is evidence available to the INPRO assessor that due to the introduction or enhancement of inherent safety characteristics and use of passive

²⁸ The term "abnormal operation" is equivalent to "anticipated operational occurrences". It is to be mentioned that different initiating events (e.g. burnout of switch, electric cable defect, loss of external power, operator error, etc.) can result in the same anticipated operational occurrence (e.g. loss of power to the main coolant pump).

safety systems (or components) lower frequencies of occurrence of AOO and DBA can be expected.

3.3.1.3. Criterion CR2.1.3 (consequences)

Indicator IN2.1.3: *Consequences of abnormal operation and accidents.*

Acceptance limit AL2.1.2: *Lower consequences compared to existing facilities.*

The design of an INS should be such that no undue consequences, i.e. radiation exposures to workers, the public and environment should occur during abnormal operation and accidents. Reducing (see also the earlier section dealing with criterion CR1.1.1 – robustness) or eliminating the hazards in the design, especially by incorporating inherently safe characteristics and/or passive systems to a larger extent than in existing reactors, in an INS the consequences of AOO and DBA should be lower than in existing NPPs. The consequences of abnormal operation and accidents are also discussed in the sections dealing with criteria CR3.1.1, CR3.2.1, and CR1.5.2.

The **acceptance limit AL2.1.3** is met if there is evidence available to the INPRO assessor that due to the introduction or enhancement of inherent safety characteristics and use of passive safety systems (or components) the consequences of abnormal operation and accidents are lower than in existing designs.

3.3.1.4. Criterion CR2.1.4 (confidence in innovation)

Indicator IN2.1.4: *Confidence in innovative components and approaches.*

Acceptance limit AL2.1.4: *Validity established.*

For new concepts of an INS it is of great importance to have confidence in innovative components and approaches. This is especially valid for inherently safe characteristics and for passive systems. For radically new (innovative) designs of reactor components or systems, special attention should be directed to detect, study and model new phenomena as well as scaling considerations within experimental and analytical work. Due to missing operating experiences for completely new passive components or systems, great efforts should be undertaken to evaluate and assess the reliability of such systems, which is needed for a probabilistic safety assessment. For necessary RD&D efforts to achieve sufficient confidence in innovative designs see also basic principle BP4 and especially user requirement UR4.2.

The **acceptance limit AL2.1.3** is met if there is evidence available to the INPRO assessor that before the introduction or enhancement of inherent safety characteristics and use of passive safety systems (or components) in the INS the validity of these approaches has been established by appropriate RD&D programs.

3.4. INPRO basic principle BP3 (risk of radiation)

Basic principle BP3: *Installations of an INS shall ensure that the risk from radiation exposures to workers, the public and the environment during construction/commissioning, operation, and decommissioning, are comparable to the risk from other industrial facilities used for similar purposes.*

The basic principle reflects two concepts:

- It is life-cycle based. This principle asks for the optimization of radiation exposure to people inside and outside of a nuclear facility during the lifetime of a nuclear facility, i.e. during construction, commissioning, operation and decommissioning;

- It is risk-based — i.e. the appropriate figure-of-merit for judging INS is the risk from other industries used for similar purposes.

It is important to note that this basic principle BP3 does not consider accidents; it considers only level 1 and 2 of DID. The requirement to avoid undue burdens from radiation doses to the public during accidents is met via user requirement UR1.5, which states that there should be no need for evacuation.

In this context, it is mentioned that the International Basic Safety Standards for Protection against Ionizing Radiation and for Safety of Radiation Sources are documented in Ref. [44].

INPRO came up with two user requirements for BP3, the first one (UR3.1) dealing with the radiation risk to workers in a nuclear power station, the second one (UR3.2) to the public.

3.4.1. User requirement UR3.1 (dose to workers)

User requirement UR3.1: *INS installations should ensure an efficient implementation of the concept of optimization of radiation protection for workers through the use of automation, remote maintenance and operational experience from existing designs.*

For normal operation, this user requirement repeats the internationally accepted principle of dose optimization for nuclear energy workers. However, doses from operating facilities are already low, so UR3.1 does not go beyond the optimization principle by asking for further *ad hoc* exposure reduction in dose.

The experience in existing reactors is that in-service inspection, periodic tests and repairs (including replacement) are the source of most occupational doses. The user requirement anticipates that INS can take advantage of innovative design concepts to achieve occupational dose reduction as a zero-cost side-effect of measures such as automated inspection and maintenance. Innovative designs should be maintenance-friendly through careful layout, reliable equipment, and availability of maintenance procedures electronically at the work-face to guide the maintainer.

For INPRO user requirement UR3.1 the following criterion has been selected:

Table 3.4.1. Criterion for user requirement UR3.1

UR3.1 (Dose to workers): <i>INS installations should ensure an efficient implementation of the concept of optimization of radiation protection through the use of automation, remote maintenance and operational experience from existing designs.</i>	
Criterion (CR)	
Indicator (IN)	Acceptance Limit (AL)
CR3.1.1 occupational dose	
IN3.1.1: Occupational dose values.	AL3.1.1: Less than limits defined by national laws or international standards and so that the health hazard to workers is comparable to that from an industry used for a similar purpose.

3.4.1.1. Criterion CR3.1.1 (occupational dose)

Indicator IN3.1.1: *Occupational dose values.*

Acceptance limit AL3.1.1: *Less than limits defined by national laws or international standards and so that the health hazard to workers is comparable to that from an industry used for a similar purpose.*

Figure 3.4.1 below shows accumulated yearly occupational doses in existing NPPs versus time. It is evident that the occupational doses decreased continuously with increasing lifetime and improved NPP designs.

This was achieved, e.g., through minimization of 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), layout features which reduce the collective dose (e.g., strict physical separation/shielding of systems, accessibility, separation, shielding, handling, set down areas), and through a maintenance friendly design of equipments. It is expected that these features can be implemented in innovative designs and thus – with further improvements – actual doses in INS may be further decreased.

The health hazards to workers in existing nuclear reactors have been compared with hazards of other energy converting facilities in the section (Figure 3.2.5) dealing with criterion CR1.5.3. The comparison shows very low values for NPPs. At least as good a trend can be expected for INS.

The **acceptance limit AL3.1.1** is met if evidence is available to the INPRO assessor that doses to workers in an INS are less than defined by national or international standards and that health hazards to workers in an INS are comparable to that from other energy converting plants.

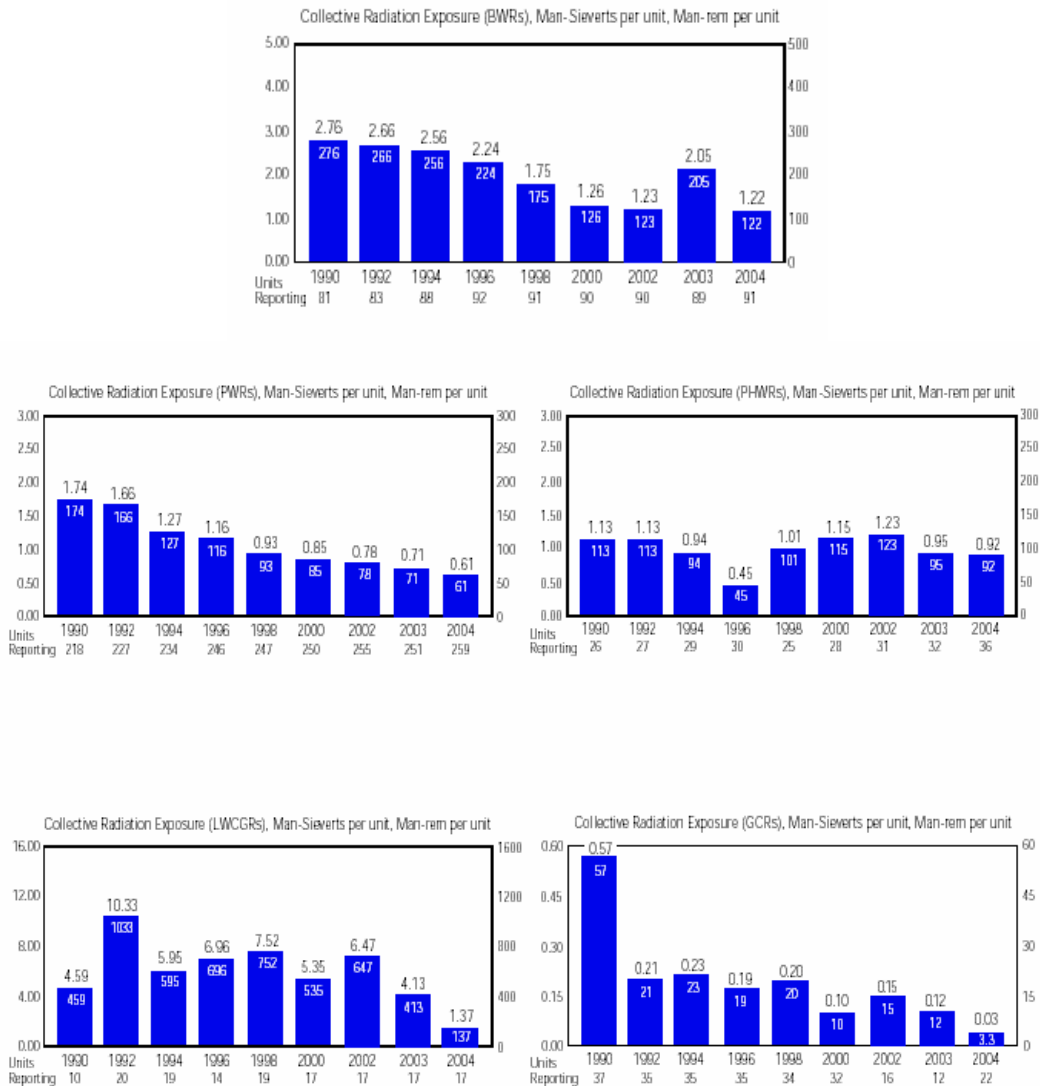


Figure 3.4.1. Accumulated yearly occupational dose [26].

3.4.2. User Requirement UR3.2 (dose to public)

User Requirement UR3.2: *Dose to an individual member of the public from an individual INS installation during normal operation should reflect an efficient implementation of the concept of optimization, and for increased flexibility in siting may be reduced below levels from existing facilities.*

This user requirement applies the same principle to public dose optimization (as in UR3.1) but also asks for no *ad hoc* reduction. Existing nuclear generation plants have a very low risk (compared to other industries) due to radiation exposure in normal operation and no dramatic changes are needed in innovative installations. It notes however that where an INS is located very close to densely populated areas (e.g., local district heating plants) further dose reduction may be required, e.g., by recycling waste streams, consistent with the practice that will be expected of other industries.

In comparing INS of radically different sizes, a more precise indicator than dose for the user requirements UR3.2 and UR3.1 would be “person-Sv per Unit energy”. Also some INS concepts have many units or different facilities co-located at one site. For such scenarios a reduction in dose per unit or facility relative to existing facilities may be necessary to ensure that the dose from the entire site is acceptable.

INPRO has defined one criterion for UR3.2:

Table 3.4.2. Criterion for user requirement UR3.2

UR3.2 (Dose to public): <i>Dose to an individual member of the public from an individual INS installation during normal operation should reflect an efficient implementation of the concept of optimization, and for increased flexibility in siting may be reduced below levels from existing facilities.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR3.2.1 public dose	
IN3.2.1: Public dose values.	AL3.2.1: Less than limits defined by national laws or international standards and so that the health hazard to the public is comparable to that from an industry used for a similar purpose.

3.4.2.1. Criterion CR3.2.1 (public dose)

Indicator IN3.2.1: *Public dose values.*

Acceptance limit AL3.2.1: *Less than limits defined by national laws or international standards and so that the health hazard to the public is comparable to that from an industry used for a similar purpose.*

The radiation exposure of the public from existing nuclear reactors during normal operation is very low compared to existing limits. The dose limit specified by ICRP (Ref. [45]) is 1 mSv per year; this specified limit is generally agreed to be adequate taking in account the effective environmental (natural) radiation load, which ranges from less than 1 mSv up to several mSv depending on the geographic location.

Measured data of operating plants show values well below 1 mSv. However, for a location close to urban sites the specified limits might be lower. For sites with multiple units the calculated doses to the public should concur to the same dose limits outside the fence as a

single unit. This should also be valid for sites with facilities of different type (e.g., reactors for power production or other processes, facilities related to fuel, etc.).

The determination of health hazards of different energy sources requires an intensive analysis. The INPRO assessor needs the results of such a comparative analysis to be provided by the supplier of the INS. In the section dealing with criterion CR1.5.3 it has been shown that the risk (health hazards) from nuclear power plants is mostly lower compared to other industries, taken “Years of Life Lost” as a measure. Hence, there is no need for further lowering the existing radiation protection limits.

The INPRO area of environment [14] and waste management [9] also deal with the issue of public dose. The INPRO methodology related to the environment asks for the control of all stressors (including radiation) to the environment (including the public) to levels meeting or superior to current standards. In the area of waste management a similar requirement is defined specifically for waste management components. At the moment this report was written it is recommended to evaluate public dose within the INPRO environmental assessment. Therefore the role of the INPRO assessor in the area of safety is mainly to assure that the issue of public dose has been covered (but dealt with only once) as part of a holistic assessment of an INS. However, additionally, the INPRO assessor should check here the results of a comparative analysis of all available energy sources regarding health hazards.

The **acceptance limit AL3.2.1** for an INS is met if evidence is available to the INPRO assessor confirming that calculated doses to the public are less than defined by national or international standards and that health hazards to the public are comparable to that from other energy converting plants.

3.5. INPRO basic principle BP4 (RD&D)

Basic principle BP4: *The development of INS shall include associated research, development and demonstration (RD&D) work 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 existing plants.*

More research will be needed to bring the knowledge of plant characteristics and the capability of computer codes to model phenomena and system behavior for innovative reactors to at least the same confidence level as for existing plants (see also Annex C).

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

RD&D and development of safety codes/analytical methods

As the development of an INS 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 parameter 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 program to e.g., improve

conceptual understanding, obtain more accurate data, to 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.

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. [46].

INPRO has defined four user requirements related to technical confidence; the first one dealing with the safety base; the second one with reliability of (radical) new components or systems; the third one with the necessity of a pilot plant; and the fourth one with safety analyses methods.

3.5.1. User requirement UR4.1 (safety basis)

User requirement UR4.1: *The safety basis of INS installations should be confidently established prior to commercial deployment.*

The term “safety basis” is understood to be the documentation of the safety requirements and safety assessment of the plant design before it is being constructed and operated. The safety basis includes a well-defined concept for achieving safety with a logical and auditable process to determine and document all the design and safety requirements for the facility. Iteration among design, RD&D and safety analysis is a necessary part of this process. Once the requirements have been set, it must be demonstrated and documented that they are met.

Table 3.5.1. Criteria for user requirement UR1.4

UR4.1 (safety basis): <i>The safety basis of INS installations should be confidently established prior to commercial deployment.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR4.1.1 safety concept	
IN4.1.1: Safety concept defined?	AL4.1.1: Yes.
CR4.1.2 safety issues	
IN4.1.2: Clear process for addressing safety issues?	AL4.1.2: Yes.

3.5.1.1. Criterion CR4.1.1 (safety concept)

Indicator IN4.1.1: *Safety concept defined?*

Acceptance limit AL4.1.1: *Yes.*

The safety basis is the documentation of the safety requirements²⁹ and safety assessment of the plant design before it is being constructed and operated. The safety basis includes a well-defined concept for achieving safety with a logical and auditable process.

²⁹ The criterion CR4.1.2 consisting of IN4.2.1 in TECDOC-1434 was dropped because it is covered by CR4.1.1.

The safety basis of evolutionary designs is covered by existing mechanisms.

For innovative designs, there is a need for the development of technology-neutral risk-informed safety goals. These goals then lead to the establishment of a safety basis. A framework for assessing the adequacy of such a safety basis is given by the different user requirements in this report; one of the main requirements is the implementation of the DID strategy.

Licensing authorities should be contacted early to achieve a common basis for the innovative design.

The **acceptance limit AL4.1.1** for an INS is met if evidence is available to the INPRO assessor confirming a consistent safety basis that demonstrates the safety goals are met.

3.5.1.2. Criterion CR4.1.2 (safety issues)

Indicator IN4.1.2: *Clear process for addressing safety issues?*

Acceptance limit AL4.1.2: *Yes.*

Iteration among design, RD&D and safety analysis will be necessary to achieve an optimized design with a safety level superior to existing designs. Of high importance are sensitivity analyses to study the sensitive parameters and to confirm that specified limits are covering uncertainties. For the final design it must be demonstrated that all safety issues are covered and the results are well documented. Pre-operational tests should be performed to confirm the design.

The **acceptance limit AL4.1.2** for an INS is met if evidence is available to the INPRO assessor that there are well-documented results of the process addressing the safety issues including sensitivity and uncertainty analyses and independent reviews.

3.5.2. User requirement UR4.2 (RD&D for understanding)

User requirement UR4.2: *Research, development and demonstration (RD&D) on the reliability of components and systems, including passive systems and inherent safety characteristics, should be performed to achieve a thorough understanding of all relevant physical and engineering phenomena required to support the safety assessment.*

It is common practice to assess the system or component behaviour on the basis of code calculations, operating experience and commonly accepted engineering practice. The development of 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 designs should proceed in parallel. These computer codes should 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 should be well documented (e.g., software requirements specifications, theory manuals, user manuals, flow charts, etc.).

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

At least the following requirements should be met:

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

INPRO defined three criteria for user requirement UR4.2 as follows.

Table 3.5.2. Criteria for user requirement UR4.2.

UR4.2 (RD&D for understanding): <i>Research, Development and Demonstration on the reliability of components and systems, including passive systems and inherent safety characteristics, should be performed to achieve a thorough understanding of all relevant physical and engineering phenomena required to support the safety assessment.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR4.2.1 RD&D	
IN4.2.1: RD&D defined and performed and database developed?	AL4.2.1: Yes.
CR4.2.2 computer codes	
IN4.2.2: Computer codes or analytical methods developed and validated?	AL4.2.2: Yes.
CR4.2.3 scaling	
IN4.2.3: Scaling understood and/or full scale tests performed?	AL4.2.3: Yes.

3.5.2.1. Criterion CR4.2.1 (RD&D)

Indicator IN4.2.1: *RD&D defined and performed and database developed?*

Acceptance limit AL4.2.1: *Yes.*

An overview of tasks to be performed for defining necessary RD&D is given in Figure 3.5.2.

For an INS the first task is to identify all technology differences from existing designs. To identify the knowledge state and the importance of phenomena and system behavior an appropriate tool has to be used, e.g., PIRT concept (Phenomena Identification and Ranking Table) that is based mainly on engineering judgment. In addition, the adequacy and applicability of 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 should be evaluated to the extent possible. This is especially valid for passive safety systems.

During the process of generating new and/or more detailed data (e.g., for CFD 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 criterion CR4.2.3).

The **acceptance limit AL4.2.1** for an INS is met if evidence is available to the INPRO assessor that:

- Measured data are available in the region of application; and that
- 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.

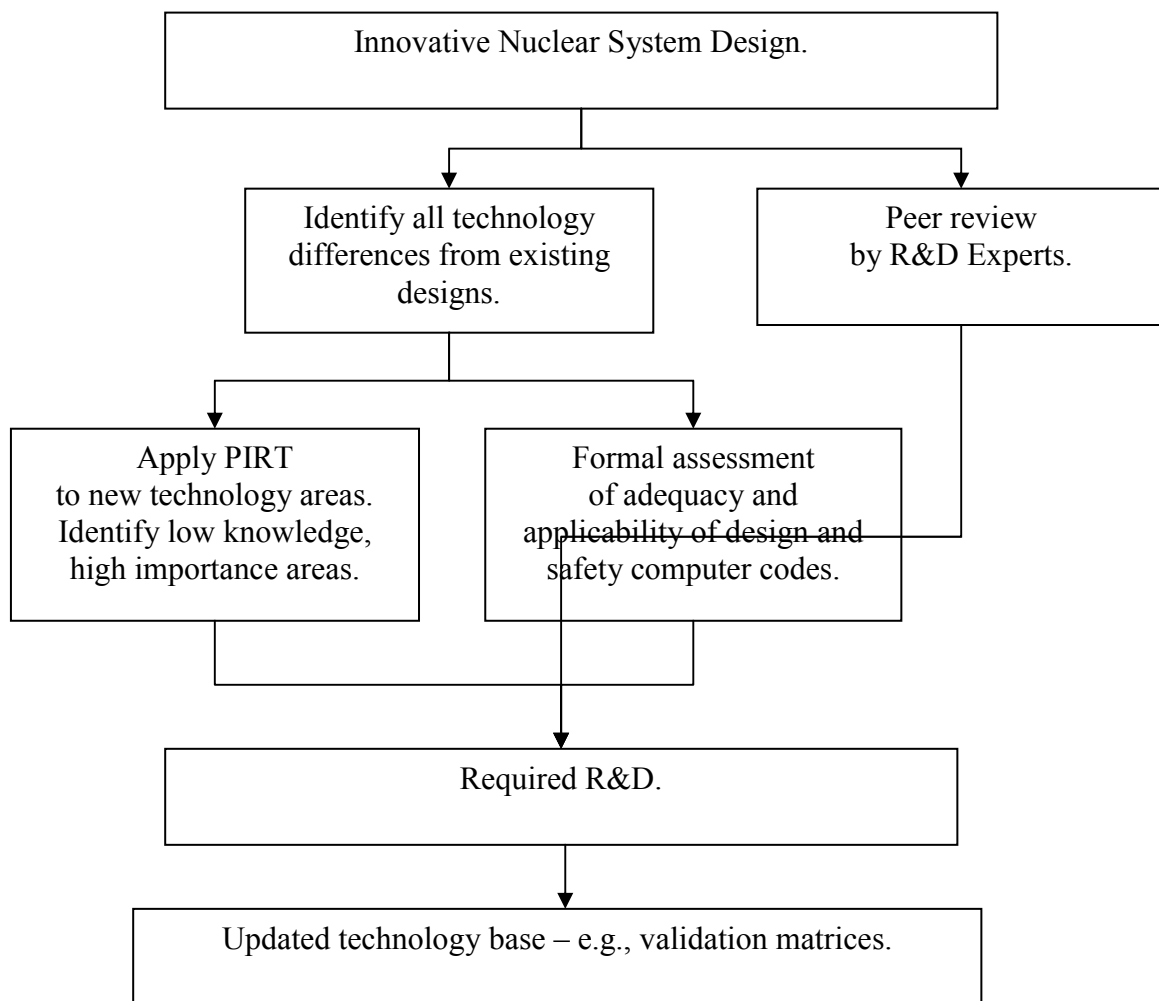


Figure 3.5.2. Overview of the different tasks for RD&D.

3.5.2.2. Criterion CR4.2.2 (computer codes)

Indicator IN4.2.2: *Computer codes or analytical methods developed and validated?*

Acceptance limit AL4.2.2: *Yes.*

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

For an INS new or more detailed models developed using a representative data base must be implemented in computer codes, verified and validated. International standards, e.g., validation matrices, uncertainty quantification approaches combined with scaling

considerations, etc., should be used to the extent possible. For example, agreed validation matrices exist for the thermal-hydraulic behavior of water cooled SSC. International experts within the OECD/NEA/CSNI have selected well documented and accurate separate and integral experiments and plant behavior 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 behavior. These test matrices are reconsidered periodically.

The **acceptance limit AL4.2.2** for an INS is met if evidence is available to the INPRO assessor that for computer codes used in design and analysis of innovative reactors:

- The region of code application is covered by their validation matrix including quantification of uncertainties and sensitivities;
- Independent reviews have been performed: and
- A complete documentation including detailed code manuals are available.

3.5.2.3. Criterion CR4.2.3 (scaling)

Indicator IN4.2.3: *Scaling understood and/or full-scale tests performed?*

Acceptance limit AL4.2.3: *Yes.*

Many components cannot be tested in full size and – in some cases – not with the appropriate boundary and initial conditions, e.g., because of power limitations or – for core melt scenarios – always at a smaller scale and mostly also without radiation. To reach sufficient confidence in the interpretation of results appropriate “scaling” considerations must exist.

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

In the last four decades large efforts have been undertaken to provide reliable thermal-hydraulic system codes for the analyses of transients and accidents in 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 to what extent the results of down-scaled test facilities represent the thermal-hydraulic behavior 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 in the kind and strength of their occurrence. The designer needs to optimize a scaled-down facility for the processes (phenomena) of primary interest. This leads compulsorily to scaling distortions of other processes with less importance. Taking into account these weak points, a goal oriented code validation strategy is required, based on the analyses of separate effects tests and integral system tests as well as transients occurred in full-scale nuclear reactors. The CSNI validation matrices may be a good basis for LWR for the realization of these tasks. Separate effect tests in full scale will play an important role.

For innovatively designed SSC of new 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”.

The **acceptance limits AL4.2.3** for an INS is met if evidence is available to the INPRO assessor showing that scaling considerations including uncertainty analyses have been performed and are well documented.

3.5.3. User Requirement UR4.3 (pilot plant)

User requirement UR4.3: *A reduced-scale pilot plant or large-scale demonstration facility should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience.*

Demonstration of a new 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.

It is recognized that a small pilot plant can be used only to demonstrate adequate safety features for occurrences (abnormal operation and failures) corresponding to level 1 and 2 of the Defence-In-Depth concept. The safe behaviour of an INS during accidents (with a potential for radioactive release) cannot be studied in a pilot plant and has to be demonstrated as defined in the user requirement UR4.2 above, using codes or analytical approaches validated against, e.g., integrated multiple-effects tests. These methods are covered in user requirement UR4.4. 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.

For INPRO user requirement UR4.3 the following criteria have been selected as follows.

Table 3.5.3. Criteria for user requirement UR4.3

UR4.3 (pilot facility): <i>A reduced-scale pilot plant or large-scale demonstration facility should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR4.3.1 novelty	
IN4.3.1: Degree of novelty of the process.	AL4.3.1: In case of <i>high degree of novelty</i> : Facility specified, built, operated, and lessons learned documented. In case of <i>low degree of novelty</i> : Rationale provided for bypassing pilot plant.
CR4.3.2 pilot facility	
IN4.3.2: Level of adequacy of the pilot facility.	AL4.3.2: Results sufficient to be extrapolated.

3.5.3.1. Criterion CR4.3.1 (novelty)

Indicator IN4.3.1: *Degree of novelty of process.*

Acceptance limit AL4.3.1: *In case of high degree of novelty: Facility specified, built, operated, and lessons learned documented. In case of low degree of novelty: Rationale provided for bypassing pilot plant.*

It might be useful to, firstly, describe the objectives for pilot- and demonstration plants. Pilot plants are small compared to demonstration or commercial plants. Not all components of a power plant need to be installed; at a later stage new SSC may be added. For example, a pilot plant may consist of a segment of the core, RCS and important (possibly new) components. Pilot plants should be designed such that new phenomena and major interactions thereof can

be studied and/or demonstrated. It should be noted that installed instrumentation in pilot plants may influence the thermal-hydraulic behavior due to possible disturbances caused by the instrumentation.

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 plants it is important to document the operation for a sufficient long time to achieve adequate confidence in the 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 SSC has to be established and reconsidered periodically or after the accomplishment of milestones.

Examples of a significant novelty of components are, e.g., the containment of the AP 600, the supercritical-water cooled power reactor (SCPR), 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.

There are examples showing that the application of larger sized test facilities resulted in the detection of new phenomena. This is supported by a well developed project plan.

The **acceptance limit AL4.3.1** for an INS is met if evidence is available to the INPRO assessor that the degree of novelty of new SSC has been identified and an appropriate RD&D program has been established.

3.5.3.2. Criterion CR4.3.2 (pilot facility)

Indicator IN4.3.2: *Level of adequacy of the pilot facility.*

Acceptance limit AL4.3.2: *Results sufficient to be extrapolated.*

The objectives to build a pilot (or a demonstration) plant has been discussed in the previous criterion.

The decision process to build and operate a pilot plant depends on several issues, e.g., the amount of available separate effect and integral tests, the degree of novelty, the available budget, the experience of operating crews, the overall time schedule up to commercialization, etc. Independent reviews would support the assessment on the adequacy of a pilot plant.

The **acceptance limit AL4.3.2** for an INS is met if evidence is available to the INPRO assessor that a peer review about the adequacy to build and operate a pilot plant has been performed.

3.5.4. User requirement UR4.4 (safety analyses)

User requirement UR4.4: *For the safety analysis, both deterministic and probabilistic methods should be used, where feasible, to ensure that a thorough and sufficient safety assessment is made. As the technology matures, "Best Estimate (plus Uncertainty Analysis)" approaches are useful to determine the real hazard, especially for limiting severe accidents.*

The safety analysis should be performed using a suitable combination of deterministic and probabilistic evaluations. The analyses should cover all modes of operation of the installation to obtain a complete assessment of the compliance with DID.

Deterministic safety analysis 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 used.

Probabilistic safety analysis (PSA) calculates the frequency and consequences of all accidents down to very low probability of occurrence.

Best estimate analyses are commonly used because a realistic response to an initiating event is needed to estimate the risk and to estimate the margins in predicted plant behavior between a conservative deterministic safety analysis and a best estimate result.

While a deterministic safety analysis incorporates some margins due to pessimistic assumptions, PSA depends very much on the availability of well-based data. Because all data (mainly experimental data) are somewhat uncertain, probabilistic safety analyses should include uncertainty analyses.

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

The extent to which each method is used should 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 existing reactor types, as a consequence of changes in technology and the resulting limited availability of data.

The degree of conservatism in a deterministic safety analysis should be commensurate with the uncertainties in the technology evaluated; when the phenomena are well known and the codes are validated a realistic hypothesis (best estimate) could be considered in the analysis. A best estimate analysis should 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 should be taken: for example, when other liquid metals than those used today are foreseen in a reactor, the existing codes are not sufficiently developed to simulate all phenomena. Until these tools are available and proven accurate enough, safety margins and conservatism should be implemented in the simulations of plant behavior.

In addition to the assessment of the vulnerability of the installation to severe accidents and large releases, a probabilistic safety analysis should be 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 analysis;
- Identify safety margins;
- Help to define operational safety requirements; and
- Identify sensitivities and uncertainties.

For the performance of safety analyses of a NPP, there exists a number of publications, such as, e.g., Refs [20], [21], [47] and [48].

For INPRO user requirement UR4.4 the following criteria have been selected:

Table 3.5.4. Criteria for user requirement UR4.4

UR4.4 (safety analysis): <i>For the safety analysis, both deterministic and probabilistic methods should be used, where feasible, to ensure that a thorough and sufficient safety assessment is made. As the technology matures, “Best Estimate (plus Uncertainty Analysis)” approaches are useful to determine the real hazard, especially for limiting severe accidents.</i>	
Criteria (CR)	
Indicators (IN)	Acceptance Limits (AL)
CR4.4.1 risk informed approach	
IN4.4.1: Use of a risk informed approach?	AL4.4.1: Yes.
CR4.4.2 uncertainties	
IN4.4.2: Uncertainties and sensitivities identified and appropriately dealt with?	AL4.4.2: Yes.

3.5.4.1. Criterion CR4.4.1 (risk informed approach)

Indicator IN4.4.1: *Use of a risk informed approach?*

Acceptance limit AL4.4.1: *Yes.*

A more recent development is called “risk informed decision making” [49]. It includes design criteria that implicitly involve probabilistic considerations and are complemented by explicit probabilistic arguments 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 additional justification.

In Ref. [39] various publications, national positions and examples of such options for existing designs are provided. Examples are, 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 of the behavior of innovative designs a risk-informed approach is more appropriate for existing reactor designs with well recorded operational behavior than for INSs.

The **acceptance limit AL4.4.1** for an INS is met if evidence is available to the INPRO assessor that a careful use of risk informed approaches based on proven data sets has been performed by the designer.

3.5.4.2. Criterion CR4.4.2 (uncertainties)

Indicator IN4.4.2: *Uncertainties and sensitivities identified and appropriately dealt with?*

Acceptance limit AL4.4.2: *Yes.*

In principle, a PSA should 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 which need further investigation. Furthermore, if the probabilistic safety analysis 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 analysis 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 (and possibly new) experiments have to be performed or design provisions have to be implemented to cope with these uncertainties.

The **acceptance limit AL4.4.2** for an INS is met if evidence is available to the INPRO assessor that a thorough analysis of uncertainties including complementary sensitivity studies has been performed by the designer. An independent review is recommended.

3.6. Concluding remarks

For innovative nuclear reactors and fuel cycle installations, four basic principles have been formulated by INPRO along with fourteen user requirements. The approach to safety is based on the IAEA Safety Standards and, derived from those, on the application of an enhanced defence-in-depth strategy compared to existing designs and facilities, supported by increased emphasis on inherent safety characteristics and passive features. Greater independence of the different levels of defence-in-depth 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 defence-in-depth strategy is that even in case of severe accidents there will be no need for evacuation of people living nearby a nuclear facility, apart from those generic emergency measures developed for any industrial facility.

It is recognized that for innovative reactors and fuel cycles, more integration of development is required, to ensure that releases of radioactive material from all components of the system are considered and optimized for a given concept. Ideally, the impact (e.g., dose) of the whole reactor and fuel cycle (including the associated waste treatment installations) should be evaluated at the concept definition stage for innovative nuclear reactors and fuel cycle installations. A balancing of risks, impacts, and economics should be sought to optimize global energy production.

As stated in Section 3.2.8 and in the manual for the INPRO area of physical protection [18], the developer of new designs should consider jointly the objectives of nuclear safety with those of physical protection and proliferation resistance [19] during all design stages.

CHAPTER 4

EXAMPLE FOR AN INPRO SAFETY ASSESSMENT OF A NUCLEAR REACTOR

There are many advanced light water reactor (LWR) concepts, e.g., see Ref. [6], as well as concepts with other fluids (e.g., heavy water, helium, sodium, lead) available. Each design shows benefits as well as drawbacks. The assessment method described in Chapter 3 requires for many INPRO criteria to compare the INS assessed with an existing (operating) plant. Thus, for each advanced design (INS) an appropriate reference design (of an operating plant) is needed.

In the present version of the manual, as an example³⁰, two boiling water reactor (BWR) designs have been selected:

- The operating (existing) NPP Gundremmingen in Germany as the reference plant ; and
- The SWR1000 as an INS to be assessed.

A short description of the SWR1000 (extract from Ref. [6]) is given in Annex A, and a comparable short description of an operating BWR in Germany, the Gundremmingen plant, is given in Annex B [51]. It should be noted that the operation of the existing BWRs started in the early eighties; therefore, documentation and analyses are nearly 30 years old.

Both reactors are large size LWR designs (700 MWe and larger). The selection has been performed because of the availability of sufficiently detailed documentation to the author of the manual, although most documentation and operating or design values are – unfortunately – of proprietary nature.

In the following an example will be presented of a safety assessment of an INS against the INPRO requirements, as described in the previous Chapter 3.

4.1. INPRO basic principle BP1 (Defence in depth)

Basic principle BP1: *Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.*

4.1.1. User requirement UR1.1 robustness

User requirement UR1.1: *Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation.*

4.1.1.1. Assessment against criterion CR1.1.1 robustness

Indicator IN1.1.1: *Robustness of design (simplicity, margins).*

Acceptance limit AL1.1.1: *Superior to existing designs in at least some of the aspects discussed.*

To demonstrate an increase of simplicity and margins in the design of the INS, some examples of design features will be given of the two designs to be compared:

- An operating, conventional BWR (1300 MWe), and
- The innovative SWR1000.

The first example shows a comparison of some systems; the second and third example will be presented in the area of the fundamental safety functions:

³⁰ This chapter was written by E.F.Hicken/Germany; it was not subject of a Peer Review.

- Control of reactivity; and
- Heat removal from the core.

Example No. 1: Comparison of system design:

Table 4.1. Comparison of innovative and conventional system design

Component/System	SWR1000	Conventional BWR
Emergency condenser HPCI-system.	4 x (50 – 100 %)	3 x 100 %
Spent fuel pool cooling system.	cooler inside fuel pool 2 x (50 - 100 %)	2x 100 % +connections to the RHR system (to be operated from the control room)
LPCI-system.	4 x 100 % passive + 2 x 100 % active systems	3 x 100 %
Reactor water cleanup system.	2 x 100 % combined system	2 x 100 %
MCP-seal water system.	“	3 x 100 %
CRD-purging system.	“	2 x 100 %
Boron injection system.	“	2 x 100 %
Main steam lines.	3	4
Feed water lines.	2	4
Feed water heater train.	single train	double train
Reactor building.	109,000 m ³	145,000 m ³
Turbine hall.	157,000 m ³	238,000 m ³
Auxiliary building.	40,000 m ³	70,000 m ³
Switchgear building.	20,000 m ³	65,000 m ³
Electrical-/I&C-systems.	double trains (+ passive systems)	3 trains

The table above clearly demonstrates the increased simplicity of the innovative design in comparison to an operating BWR.

Example No. 2: Control of reactivity

The conventional BWR and the SWR1000 are both BWRs with the control rods inserted from below through a hydraulic system and an electro-driven system. In addition, boron can be injected.

While the operating conventional BWR plant relies on commonly used safety related instrumentation with its signals processed by the Reactor Protection System, the innovative design relies on passive signaling devices, see Figure 4.1 below, in addition to a conventional I&C system proven in the conventional BWR:

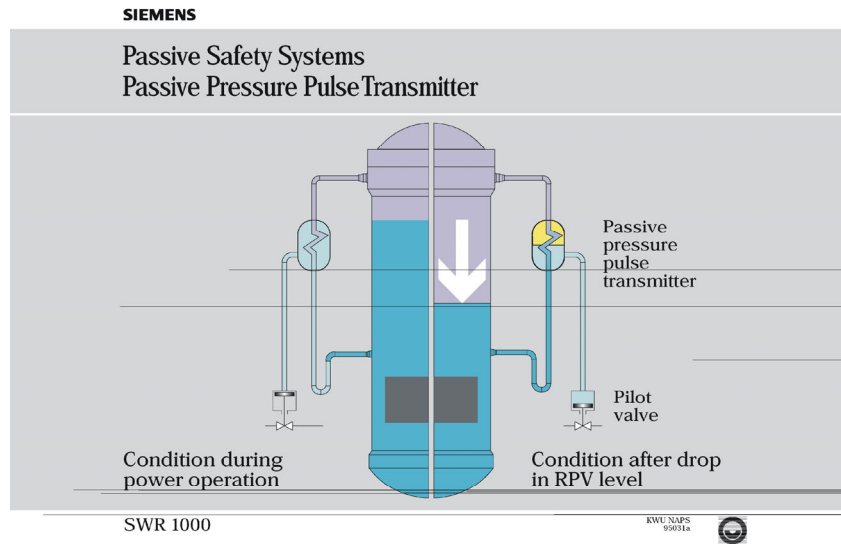


Figure 4.1. Passive signaling device of innovative design.

The system works as follows: During power operation the passive pressure pulse transmitter (PPPT) is flooded with cold water. Because the secondary side of the transmitter is also flooded with cold water, no reaction on the secondary side occurs. In case the water level in the RPV drops, the primary side of the transmitter is heated up by steam resulting in a heat-up - and steam production - of the secondary side. This pressure will be used to initiate some actions, e.g., scram, containment isolation, etc. This system cannot be influenced by operator actions. In addition, the Reactor Protection System (RPS) acts as designed. The system of the innovative design includes passive features for control of reactivity.

Example No3: Heat removal from the core

For the operating conventional BWR the heat removal from the core is achieved by four redundant residual heat removal (RHR) systems with three loops in series, connected through heat exchangers and powered by emergency power – if necessary.

In the innovative SWR1000 the heat removal from the core is achieved by 2 active systems in addition to a passive system; the latter is sketched in Figure 4.2 below:

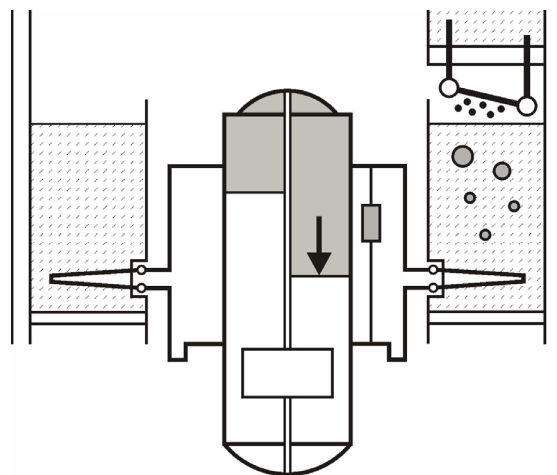


Figure 4.2. RHR system of innovative BWR.

This passive system works as follows: In case of a water level decrease in the RPV (see the right side of Figure 4.2) steam produced in the core region is condensed within the tubes of emergency condensers (EC), and thus the core flooding pool is heated up. Steam produced within this pool will be condensed on tubes of the containment cooling condensers (CCCs), which are cooled by water of the shielding/storage pool. The circulation of the water within these CCCs occurs by natural circulation. The water inventory of the shielding/storage pool allows a heat removal for about three days because this pool is located outside the containment (see also the containment Figure A.5 in Annex A). Refill is easily possible.

The differences in design of the RHR systems are illustrated in the following comparison:

Table 4.2. Comparison of conventional and innovative design of RHR

Component to fulfill functional requirement	Conventional BWR Active System (1 out of 3)*	SWR1000	
		Passive System	Active System (1 out of 2)
Pumps	4	None	2
Heat exchanger.	at least 2	4 emergency condensers 4 containment cooling condenser	at least 2
Diesel.	at least 1	none	at least 1
Check valves.	several	none	several
Isolation valves.	several	several	several
Instrumentation.	extensive	moderate	extensive

Note:

* One system out of three redundant systems available

The table above demonstrates the increased robustness and diversity of the innovative design.

The following Table 4.3 shows a comparison for some variables between a conventional and an innovative BWR regarding features related to the robustness (simplicity and margins) of a design.

Table 4.3. Comparison of an operating design to an innovative design

Design features	Conventional BWR	SWR1000
Core power density (kW/l).	56	51
Water inventory in RPV (kg/MW _{th}).	75	122
Number of active loops:	3	2
Main steam lines.	4	3
Feed water lines.	4	2
Forced or natural flow through the core.	Forced flow.	Forced flow.
Passive components in I&C.	No.	Yes, for signaling device (see example given above).

Table 4.3. Comparison of an operating design to an innovative design (continued)

Design features	Conventional BWR	SWR1000
Redundancy and diversity of safety system for RHR.	Redundancy.	Redundancy and diversity.
Use of passive component in safety systems.	No.	Yes (see examples given above).
Margins against a failure of the leak tight confinement.	Usually the failure pressure of a containment is about 2 – 2.5 times the design pressure.	Usually the failure pressure of a containment is about 2 – 2.5 times the design pressure. The containment is designed for tightness after a severe accident with hydrogen generation from 100 % zirconium oxidation.

The table above clearly demonstrates the increased robustness of the innovative design in comparison to an operating conventional design.

4.1.1.2. Assessment against criterion CR1.1.2 operation

Indicator IN1.1.2: *High quality of operation*

Acceptance limit AL1.1.2: *Superior to existing designs in at least some of the aspects discussed.*

For the SWR1000, the plant management organization and the related responsibilities are clearly described. The technical documentation as well as the monitoring systems described in the criterion and training requirements are available.

The I&C system is digital; all necessary computerized aids to operators (e.g., computerized manuals) are existing.

The predicted scram frequency (SF) for the innovative design is expected to be below 0.5 per year and the number of nuclear events for (INES 2) is expected to be below 0.01 per year.

4.1.1.3. Assessment against criterion CR1.1.3 inspection

Indicator IN1.1.3: *Capability to inspect.*

Acceptance limit AL1.1.3: *Superior to existing designs in at least some of the aspects discussed.*

The capabilities to inspect for the SWR1000 are state-of-the-art and thus superior to existing designs.

4.1.1.4. Assessment against criterion CR1.1.4 failures and disturbances

Indicator IN1.1.4: *Expected frequency of failures and disturbances.*

Acceptance limit AL1.1.4: *Superior to existing designs in at least some of the aspects discussed.*

The frequencies of a conventional BWR and the expected frequencies for the INS (SWR1000) for the operational state are given below:

Table 4.4. Comparison of frequencies of failures and disturbances of conventional and innovative BWR

Event	Conventional BWR (measured)	SWR1000 (conservatively calculated)
Loss of heat sink	0.4 per year and unit	0.5 per year and unit
Loss of heat sink with additional loss of feed water due to common cause failures	0.2	
Loss of feed water supply	0.1	0.3
Loss of offsite power	0.02	0.06
Stuck-open of a safety & relief valve	0.07	0.1
Overfeeding transients	0.2	
Malfunction of turbine or by pass station	0.1	

The differences between the conventional and innovative BWR are small; this is due to the similarity of both designs, and due to the fact that the additional passive systems in the INS are designed mainly for accidents.

4.1.2. User Requirement UR1.2 detection and interception

User Requirement UR1.2: *Installations of an INS should detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions.*

4.1.2.1. Assessment against criterion CR1.2.1 I&C and inherent characteristics

Indicator IN1.2.1: *Capability of I&C system and/or inherent characteristics to detect and intercept and/or compensate such deviations.*

Acceptance limit AL1.2.1: *Key system variables relevant to safety (e.g., flow, pressure, temperature, radiation levels) do not exceed limits acceptable for continued operation (no event reporting necessary).*

The digital I&C system of the SWR1000 is state-of-the-art; plant dynamic analyses show all key system variables stay within prescribed limits.

Regarding the use of passive components in the I&C of the SWR1000, see the example No.2 given in Section 4.1.1.1.

4.1.2.2. Assessment against CR1.2.2 grace period

Indicator IN1.2.2: *Grace period until human actions are required.*

Acceptance limit AL1.2.2: *Superior to existing designs.*

The SWR1000 has a much larger grace period (more than 3 days) than the conventional BWR (30 minutes up to several hours, depending on the sequence).

4.1.2.3. Assessment against CR1.2.3 inertia

Indicator IN1.2.3: *Inertia to cope with transients.*

Acceptance limit AL1.2.3: *Superior to existing designs.*

The INS has a relatively larger water inventory than the conventional BWR and a lower power density and thus more thermal inertia.

4.1.3. User Requirement UR1.3 DBA

User Requirement UR1.3: *The frequency of occurrence of accidents should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.*

4.1.3.1. Assessment against CR1.3.1 DBA

Indicator IN1.3.1: *Calculated frequencies of occurrence of design basis accidents.*

Acceptance limit AL1.3.1: *Reduced frequency.*

Data for frequencies of occurrence as well as reliability data of engineered safety systems are mostly propriety. Therefore, the calculated frequencies are given as Factor x E-nn/year for power states or Factor x E-mm/per refueling for plant shutdown states. To give a better indication of the value of the “factor” the following definition is applied:

- Factor(+) describes a factor between 5 – 9 and
- Factor(-) a factor between 1 – 4.

For shutdown states one refueling per year is assumed.

For the SWR1000 the following values have been calculated:

Table 4.5. DBA to be considered for the SWR1000

DBA	Normal operation	Shutdown/refueling
TRANSIENTS - Loss of auxiliary power - Loss of main feed water supply - Loss of main heat sink - Loss of main heat sink and main feed water supply - Inadvertently opened and stuck-open safety relief valve	Factor(+) x E-2 Factor(-) x E-1 Factor(+) x E-1 Factor(-) x E-1 Factor(-) x E-1	
ATWS	Factor(+) x E-5	
PIPE BREAK ACCIDENTS OUTSIDE CONTAINMENT - Feed water pipe break outside containment - Main steam line break outside containment - Break in the RWCU extraction line outside containment	Factor(-) x E-3 Factor(-) x E-3 Factor(-) x E-3	
LOCA INSIDE THE CONTAINMENT - Small-break LOCA inside containment - Leak at RPV bottom head	Factor(-) x E-3 Factor(-) x E-4	
TRANSIENTS - Loss of residual heat removal (RHR) with reactor vessel closed - Loss of RHR with reactor vessel depressurised but closed - Loss of RHR during flooding/draining of shielding/storage pool - Loss of RHR with shielding/storage pool flooded - Loss of heat sink for active RHR with reactor vessel closed - Loss of heat sink for active RHR with reactor vessel depressurized but closed - Loss of heat sink for active RHR during flooding/draining of shielding/storage pool		Factor(-) x E-7 Factor(-) x E-7 Factor(-) x E-7 Factor(-) x E-4 Factor(+) x E-4 Factor(-) x E-4 Factor(+) x E-4

- Loss of heat sink for active RHR with shielding/storage pool flooded		Factor(-) x E-3
LEAKS AT ELEVATIONS ABOVE THE CORE (with shielding/storage pool flooded) - Very large leak - Large leak - Medium leak		Factor(-) x E-3 Factor(-) x E-4 Factor(-) x E-3
LEAKS AT ELEVATIONS BELOW THE CORE (with shielding/storage pool flooded) - Very large leak - Large leak - Medium leak		Factor(+) x E-8 Factor(-) x E-7 Factor(-) x E-4

A comparison between the values given above for an INS and for an operating BWR is difficult because the time period between the two calculations is more than 20 years. Therefore the calculations for the INS are more detailed, performed with improved codes and based on best-estimate models.

Nevertheless, a comparison shows reduced frequencies of the INS.

4.1.3.2. Assessment against CR1.3.2 grace period

Indicator IN1.3.2: *Grace period until human intervention is necessary.*

Acceptance limit AL1.3.2: *In creased relative to existing facilities.*

For the SWR1000 the grace period is more than 3 days and thus much longer than for the conventional BWR (30 min. and more)

4.1.3.3. Assessment against CR1.3.3 safety features

Indicator IN1.3.3: *Reliability of engineered safety features.*

Acceptance limit AL1.3.3: *Equal or superior to existing designs.*

Due to the use of redundant and diverse systems the reliability of engineered safety systems is higher for the SWR1000 in comparison with the conventional BWR.

4.1.3.4. Assessment against criterion CR1.3.4 barriers

Indicator IN1.3.4: *Number of confinement barriers maintained.*

Acceptance limit AL1.3.4: *At least one.*

The number of confinement barriers maintained is the same for the conventional BWR and the SWR1000.

4.1.3.5. Assessment against criterion CR1.3.5 controlled state

Indicator IN1.3.5: *Capability of the engineered safety features to restore the INS to a controlled state (without operator actions).*

Acceptance limit AL1.3.5: *Sufficient to reach a controlled state.*

For the conventional BWR as well as for the SWR1000 the controlled state is automatically reached with high reliability.

4.1.3.6. Assessment against criterion CR1.3.6 sub criticality

Indicator IN1.3.6: *Sub-critically margins.*

Acceptance limit AL1.3.6: *Sufficient to cover uncertainties and to allow adequate grace period.*

For the conventional BWR as well as for the SWR1000 the sub-criticality is at least 1 % Δ k/k over the cycle with the assumption that the rod with the highest worth is stuck; uncertainties have been considered.

4.1.4. User Requirement UR1.4 release into containment

User requirement UR1.4: *The frequency of a major release of radioactivity into the containment / confinement of an INS due to internal events should be reduced. Should a release occur, the consequences should be mitigated.*

4.1.4.1. Assessment against criterion CR1.4.1 major release into the containment

Indicator IN1.4.1: *Calculated frequency of major release of radioactive materials into the containment / confinement based on frequency calculated for a highly degraded core.*

Acceptance limit AL1.4.1: *At least an order of magnitude less than for existing designs; even lower for installations at urban sites.*

Below figures are given for frequencies with a highly degraded core for:

- Power operation without AM for different sequences; or without AM separated in frequency of occurrence and system unavailability
- After plant shutdown without AM for different sequences

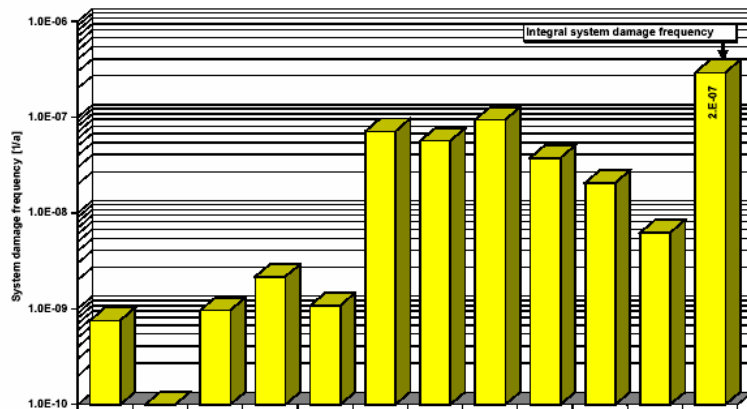


Figure 4.3. Event-related and total frequency for a highly degraded core without AM occurring during power operation.

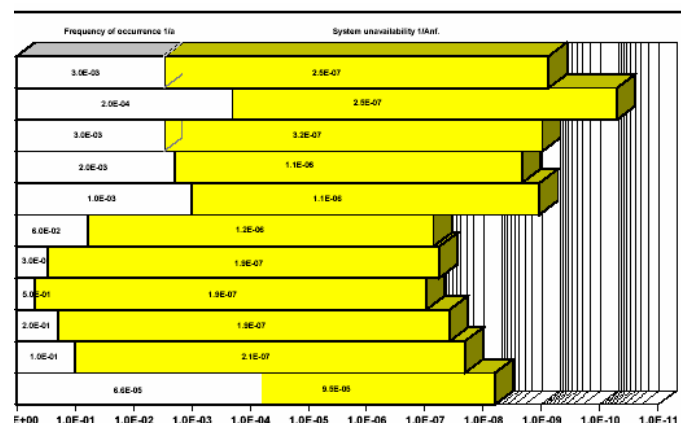


Figure 4.4. Frequencies for a highly degraded core separated into frequencies of occurrence and system un-availabilities during power operation.

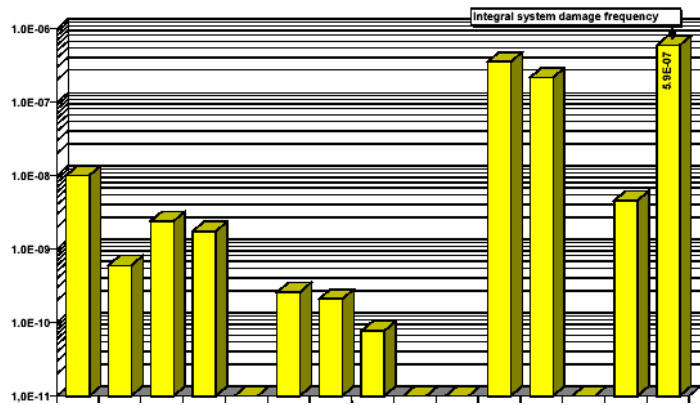


Figure 4.5. Event-related and total frequency for a highly degraded core occurring after plant shutdown.

In Figures 4.3 and 4.5, the vertical bars indicate the contributions of various transients and LOCAs to the integral frequencies illustrated by the bars on the right side.

The calculated integral frequencies for a highly degraded core for the SWR1000 are given in the following Table 4.6:

Table 4.6. Calculated frequencies of a major release into the containment of an INS

Status of plant at start of accident	Frequency without AM	Frequency with AM
Power operation.	$2.9 \cdot 10^{-7}$ /yr	$4.3 \cdot 10^{-8}$ /yr
After plant shutdown.	$5.9 \cdot 10^{-7}$ /refueling	$4.1 \cdot 10^{-8}$ /refueling

The numbers shown in the table above clearly demonstrate for the INS the fulfillment of the corresponding acceptance limit (integral CMF frequencies well below 10^{-5} /year and unit).

4.1.4.2. Assessment against criterion CR1.4.2 processes

Indicator IN1.4.2: *Natural or engineered processes sufficient for controlling relevant system parameters and activity levels in containment/confinement.*

Acceptance limit AL1.4.2: *Existence of such processes.*

The natural or engineered processes are similar for the conventional BWR and the SWR1000.

4.1.4.3. Assessment against criterion CR1.4.3 AM

Indicator IN1.4.3: *In-plant severe accident management.*

Acceptance limit AL1.4.3: *Procedures, equipment and training sufficient to prevent large release outside containment / confinement and regain control of the facility.*

The severe accident management measures in the INS are improved (especially the outside cooling of the RPV) as compared with the conventional BWR.

4.1.5. User requirement UR1.5 release into environment

User requirement UR1.5: *A major release of radioactivity from an installation of an INS should be prevented for all practical purposes, so that INS installations would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose.*

4.1.5.1. Assessment against criterion CR1.5.1 frequency of release

Indicator IN1.5.1: *Calculated frequency of a major release of radioactive material to the environment.*

Acceptance limit AL1.5.1: *Calculated frequency $<10^{-6}$ per unit-year, or practically excluded by design.*

The calculated frequencies of a major release of fission products from the core into the containment have been given in Table 4.6. A major containment failure has not to be assumed in the SWR1000, because an internal molten mass retention device is installed, the RPV is cooled from the outside, and the containment atmosphere is inerted with nitrogen.

4.1.5.2. Assessment against criterion CR1.5.2 consequences

Indicator IN1.5.2: *Calculated consequences of release.*

Acceptance limit AL1.5.2: *Consequences sufficiently low to avoid necessity for evacuation. Appropriate off-site mitigation measures (e.g., temporary food restrictions) are available.*

The calculated dose values outside the vicinity of the plant are shown in Table 4.7:

Table 4.7. Calculated public dose values for the SWR1000 in case of an accident with core melt

Beyond 200 m	Beyond 1000m	Limits for evacuation/relocation Ref. [40]
40 mSv (child) 25 mSv (adult)	15 mSv (child) 0.9 mSv (adult)	50 – 500 mSv / 1 Sv

For the SWR1000 the requirement “no evacuation and no relocation necessary” is met.

4.1.5.3. Assessment against criterion CR1.5.3 risk

Indicator IN1.5.3: *Calculated individual and collective risk.*

Acceptance limit AL1.5.3: *Comparable to facilities used for a similar purpose.*

A comparison of several energy productions has been performed based on the “Years of Life Lost (YOLL)”, see Section 3.2.5.3. It has been shown that for nuclear energy production with the requirement – no evacuation and no relocation – very low risks for the public exist.

The INS clearly fulfils the corresponding acceptance limit of having a risk comparable to other facilities used for similar purpose.

4.1.6. User requirement UR1.6 independence of DID levels

User requirement UR1.6: *An assessment should be performed for an INS to demonstrate that different levels of defence-in-depth are met and are more independent from each other than for existing systems.*

4.1.6.1. Assessment against criterion CR1.6.1 independence of DID levels

Indicator IN1.6.1: *Independence of different levels of DID.*

Acceptance limit AL1.6.1: *Adequate independence is demonstrated, e.g., through deterministic and probabilistic means, hazards analysis etc.*

Based on probabilistic analyses and due to the use of passive safety systems the different levels of the DID are more independent for the SWR1000 than for the conventional BWR. The main reasons are the lower frequencies, less needed human intervention and the use of more passive systems for the SWR1000.

4.1.7. User requirement UR1.7 human machine interface

User requirement UR1.7: *Safe operation of installations of an INS should be supported by an improved Human Machine Interface resulting from systematic application of human factors requirements to the design, construction, operation and decommissioning.*

4.1.7.1. Assessment against criterion CR1.7.1 human factors

Indicator IN1.7.1: *Evidence that human factors (HF) are addressed systematically in the plant life cycle.*

Acceptance limit AL1.7.1: *Satisfactory results from assessment.*

For the SWR1000 the methodology regarding human factors is state-of-the-art.

4.1.7.2. Assessment against criterion CR1.7.2 human response model

Indicator IN1.7.2: *Application of formal response models from other industries or development of nuclear-specific models.*

Acceptance limit AL1.7.2: *Reduced likelihood of human error relative to existing plants, as predicted by HF models; use of artificial intelligence for early diagnosis and real-time operator aids; less dependence on operator for normal operation and short-term accident management relative to existing plants.*

The models used for the SWR1000 are state-of-the-art which implies data from other industries are used to the extent possible.

4.2 INPRO Basic Principle BP2 (Inherent safety)

Basic principle BP2: *Installations of an INS shall excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach.*

4.2.1. User requirement UR2.1 minimization of hazards

User requirement UR2.1: *INS should strive for elimination or minimization of some hazards relative to existing plants by incorporating inherently safe characteristics and/or passive systems, when appropriate.*

4.2.1.1. Assessment against criterion CR2.1.1 hazards

Indicator IN2.1.1: *Stored energy, flammability, criticality, inventory of radioactive materials, available excess reactivity, and reactivity feedback.*

Acceptance limit AL2.1.1: *Superior to existing designs.*

The acceptance limits are fulfilled – in general.

4.2.1.2. Assessment against criterion CR2.1.2 frequency of DBA

Indicator IN2.1.2: *Expected frequency of abnormal operation and accidents.*

Acceptance limit AL2.1.2: *lower frequencies compared to existing facilities.*

See assessment of CR1.1.4 and CR1.3.1.

4.2.1.3. Assessment against criterion CR2.1.3 consequences

Indicator IN2.1.3: *Consequences of abnormal operation and accidents.*

Acceptance limit AL2.1.3: *Lower consequences compared to existing facilities.*

For the SWR1000 the consequences of abnormal operation and accidents without a highly degraded core are well below the limits (1 mSv) as specified by national requirements and ICRP 60 [45].

4.2.1.4. Assessment against criterion CR2.1.4 confidence in innovation

Indicator IN2.1.4: *Confidence in innovative components and approaches.*

Acceptance limit AL2.1.4: *Validity established.*

The acceptance limit is fulfilled for the SWR1000.

4.3. INPRO basic principle BP3 (Risk of radiation)

Basic principle BP3: *Installations of an INS shall ensure that the risk from radiation exposures to workers, the public and the environment during construction/commissioning, operation, and decommissioning, are comparable to the risk from other industrial facilities used for similar purposes.*

4.3.1. User requirement UR3.1 radiation protection of workers

User requirement UR3.1: *INS installations should ensure an efficient implementation of the concept of optimization of radiation protection for workers through the use of automation, remote maintenance and operational experience from existing designs.*

4.3.1.1. Assessment against criterion CR3.1.1 dose to workers

Indicator IN3.1.1: *Occupational dose values.*

Acceptance limit AL3.1.1: *Less than limits defined by national laws or international standards and so that the health hazard to workers is comparable to that from an industry used for a similar purpose.*

It can be expected that the annual dose during normal operation and maintenance will be below a value of 0.25 manSv based on existing operating experience. Source terms have been minimized as well as optimal layout features regarding contributions to the collective doses. The SWSR 1000 has a maintenance-friendly design.

4.3.2. User requirement UR3.2 radiation protection of the public

User requirement UR3.2: *Dose to an individual member of the public from an individual INS installation during normal operation should reflect an efficient implementation of the concept of optimization, and for increased flexibility in siting may be reduced below levels from existing facilities.*

4.3.2.1. Assessment against criterion CR3.2.1 public dose

Indicator IN3.2.1: *Public dose values.*

Acceptance limit AL3.2.1: *Less than limits defined by national laws or international standards and so that the health hazard to the public is comparable to that from an industry used for a similar purpose.*

Calculations for the INS have shown that the doses outside the vicinity of the plant are significantly below those defined by German national regulation.

4.4. INPRO basic principle BP4 (RD&D)

Basic principle BP4: *The development of INS shall include associated Research, Development and Demonstration work 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 existing plants.*

4.4.1. User requirement UR4.1 safety basis

User requirement UR4.1: *The safety basis of INS installations should be confidently established prior to commercial deployment*

4.4.1.1. Assessment against criterion CR4.1.1 safety concept

Indicator IN4.1.1: *Safety concept defined?*

Acceptance limit AL4.1.1: *Yes.*

For the SWR1000 the following guidelines and rules were met:

- German nuclear regulatory codes and standards as well as recommendations issued by the Groupe Permanent Réacteur (GPR) and the German Reactor Safety Commission (RSK) for the future pressurized water reactor designs, insofar as they are applicable for the SWR1000;
- IAEA guidelines;
- European Utility Requirements (EUR);
- US NRC guides; and
- Other national rules.

The safety concept has been published in Ref. [6].

4.4.1.2. Assessment against criterion CR4.1.2 safety requirements

Indicator IN4.1.2: *Design-related safety requirements specified?*

Acceptance limit AL4.1.2: *Yes.*

Design-related requirements have been specified; an independent review has been taken place (in a country not involved in the design).

4.4.1.3. Assessment against criterion CR4.1.3 safety issues

Indicator IN4.1.3: *Clear process for addressing safety issues?*

Acceptance limit AL4.1.3: *Yes.*

Safety issues have been addressed and independently reviewed.

4.4.2. User requirement UR4.2 RD&D

User Requirement UR4.2: *Research, Development and Demonstration on the reliability of components and systems, including passive systems and inherent safety characteristics, should be performed to achieve a thorough understanding of all relevant physical and engineering phenomena required to support the safety assessment*

4.4.2.1. Assessment against criterion CR4.2.1

Indicator IN4.2.1: *RD&D defined and performed and database developed?*

Acceptance limit AL4.1.4: *Yes.*

For the SWR1000 the following components have been studied and modeled [50]:

Model tests in a reduced scale:

- Scram tank with a steam cushion as a driving medium;
- Boron solution tank with a steam cushion as a driving medium;
- Passive core flooding system with a spring supported check valve; and
- Passive flow restrictor without movable parts.

Model tests with original dimensions but a reduced number of heat exchanger tubes or a section of a component:

- Emergency condenser;

- Containment cooling condenser; and
- RPV external cooling for a severe accident.

Full scale tests:

- Passive pressure pulse transmitter;
- Vent pipe which avoids chugging;
- Two-arm quencher attached to a concrete wall; and
- ATRIUM 12 fuel assembly.

4.4.2.2. Assessment against criterion CR4.2.2 computer codes

Indicator IN4.2.2: *Computer codes or analytical methods developed and validated.*

Acceptance limit AL4.2.2: *Yes.*

Computer codes for the operational and accidental behavior exist for the conventional BWRs; most of these computer codes can also be applied for the SWR1000. Computer codes for the passive safety systems of the SWR1000 have been developed; some validation is still needed.

The codes used for the SWR1000 are shown below:

Table 4.8. Codes used for SWR1000 design and analyses

Core Design		
Code Name	Applications	Validation
RAMONA	BWR stability and core physics	Several Experiments
CASMO-4/MICROBURN-2	Burn-up calculations	Worldwide use
ORIGEN-S	Fuel cycle	Worldwide use
KORIGEN	Fuel cycle	Many experiments
Overall System Analysis		
Code Name	Applications	Validation
S-RELAP5	Transient system analysis	Many experiments
WAVCO	Multi-zone containment	Many experiments
Severe accidents associated with a highly degraded core		
Code Name	Applications	Validation
COCOSYS	Lumped-parameter multi-compartment	Many experiments
GASFLOW	Finite-volume containment	Many Experiments
IVA	Melt-water interaction	Existing experiments
MELCOR	Lumped-parameter	Worldwide use
SCDAPSIM	RPV heat-up	Worldwide use
Fluid Dynamics		
Code Name	Applications	Validation
ROLAST-E	Pressure waves	Several experiments
2PHI1K	Pressure transients in pipe networks	Several experiments
S-TRAC	2-phase modelling in systems	Several experiments

Table 4.8. Codes used for SWR1000 design and analyses (continued)

Structural Analysis		
Code Name	Applications	Validation
RSTAB	2D and 3D structural analyses	Many experiments
KWUROHR	Stress and fatigue analysis	Many experiments
STRUDYN	Finite analysis of 3d-structures	Many experiments
ANSYS	Finite elements for different purposes	Many experiments
KWUSTOSS	Fast dynamic analyses	Many experiments
Radiological Consequences		
Code Name	Applications	Validation
PRODOS-B	Dose calculations	Against other codes
ACARE	Radiological consequences	Against other codes
ORIGEN, KORIGEN	See above	See above
Radiation Shielding		
Code Name	Applications	Validation
RANKERN	Gamma dose rates	Many experiments
ANISN/DORT	Anisotropic scattering	Many experiments
MCNP	Monte Carlo Code	Worldwide application

4.4.2.3. Assessment against criterion CR4.2.3 scaling

Indicator IN4.2.3: *Scaling understood and/or full-scale tests performed?*

Acceptance limit AL4.2.3: *Yes.*

Most passive safety systems of the SWR1000 have been experimentally studied at full size but with a reduced number of tubes in the heat exchangers. Problems with scaling are not expected. For those components, which have been tested in a reduced scale, scaling laws are known.

Nevertheless, it is planned to test all passive safety systems or components in full scale.

4.4.3. User requirement UR4.3 pilot plant

User requirement UR4.3: *A reduced-scale pilot plant or large-scale demonstration facility should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience.*

4.4.3.1. Assessment against criterion CR4.3.1 novelty

Indicator IN4.3.1: *Degree of novelty of the process.*

Acceptance limit AL4.3.1: *In case of high degree of novelty: Facility specified, built, operated, and lessons learned documented. In case of low degree of novelty: Rationale provided for bypassing pilot plant.*

It has been shown before that most components of the SWR1000 design represent proven BWR technology, as illustrated in the following Figure 4.6.

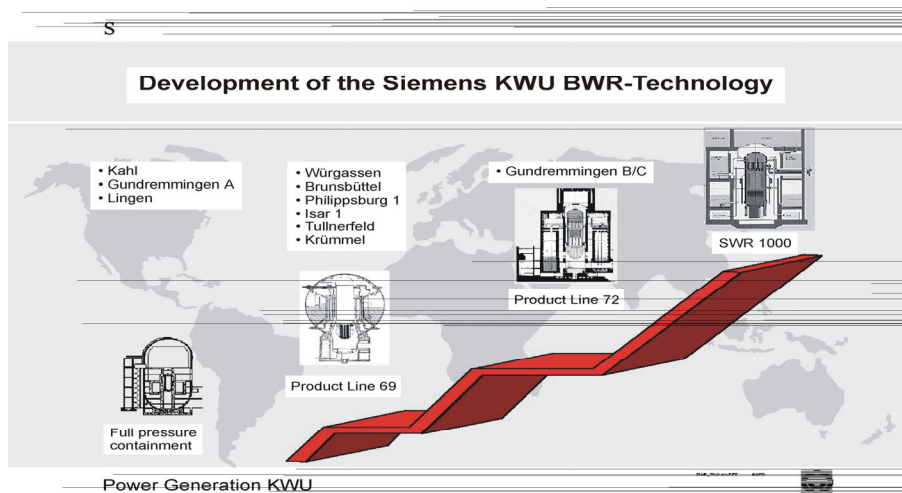


Figure 4.6. Historical development of BWR technology.

For the SWR 1000 the safety concept with active and passive safety systems and the simplicity of the design are indications of the novelty of the plant.

4.4.3.2. Assessment against criterion CR4.3.2 pilot facility

Indicator IN4.3.2: *Level of adequacy of the pilot facility.*

Acceptance limit AL4.3.2: *Results sufficient to be extrapolated.*

For the SWR 1000 no pilot plant is necessary; the rationale for this decision is given in the sections above.

4.4.4. User requirement UR4.4 risk and uncertainties

User requirement UR4.4: *For the safety analysis, both deterministic and probabilistic methods should be used, where feasible, to ensure that a thorough and sufficient safety assessment is made. As the technology matures, “Best Estimate (plus Uncertainty Analysis)” approaches are useful to determine the real hazard, especially for limiting severe accidents.*

4.4.4.1. Assessment against criterion CR4.4.1 risk informed approach

Indicator IN4.4.1: *Use of a risk informed approach?*

Acceptance limit AL4.4.1: *Yes.*

The risk informed approach has been used for some design features and inspections.

4.4.4.2. Assessment against criterion CR4.4.2 uncertainties

Indicator IN4.4.2: *Uncertainties and sensitivities identified and appropriately dealt with?*

Acceptance limit AL4.4.1: *Yes.*

To the extent necessary uncertainty and sensitivity analyses have been performed for the SWR1000, especially for the reliability of passive systems within the calculations and assessments for the PSA Level 2.

**ANNEX A:
INNOVATIVE BWR DESIGN SWR 1000**

A.1. Introduction

In 1992, German utilities awarded FRAMATOME ANP (former Siemens) a contract to develop a new BWR nuclear power plant using passive safety systems, and together with the utilities FRAMATOME started development work on a new BWR with a net capacity of 750 MWe. In the conceptual phase that lasted from February 1992 until September 1993, priority was given to developing passive safety systems to replace or supplement active systems. At the end of the conceptual phase, it was decided that the new requirements for this advanced BWR, especially economic aspects, justified a concept with a higher power output:

- Reactor thermal output 2778 MW.
- Net electric output 977 MW.

Figure A-1 shows the SWR 1000 steam cycle and in Figure A-2 the general plant lay out is illustrated.

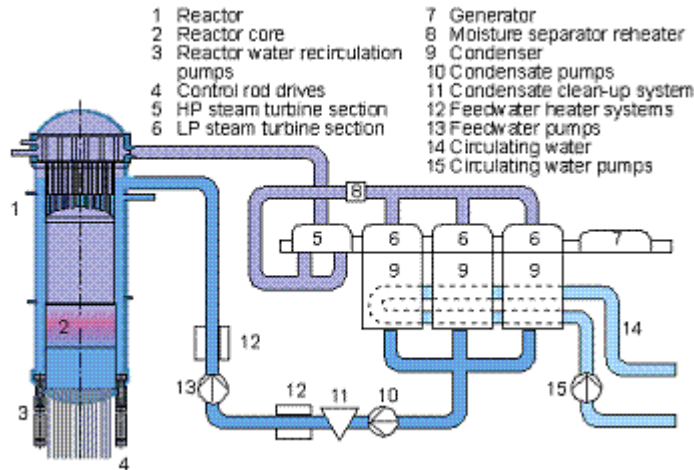


Figure A-1. SWR1000 steam cycle.

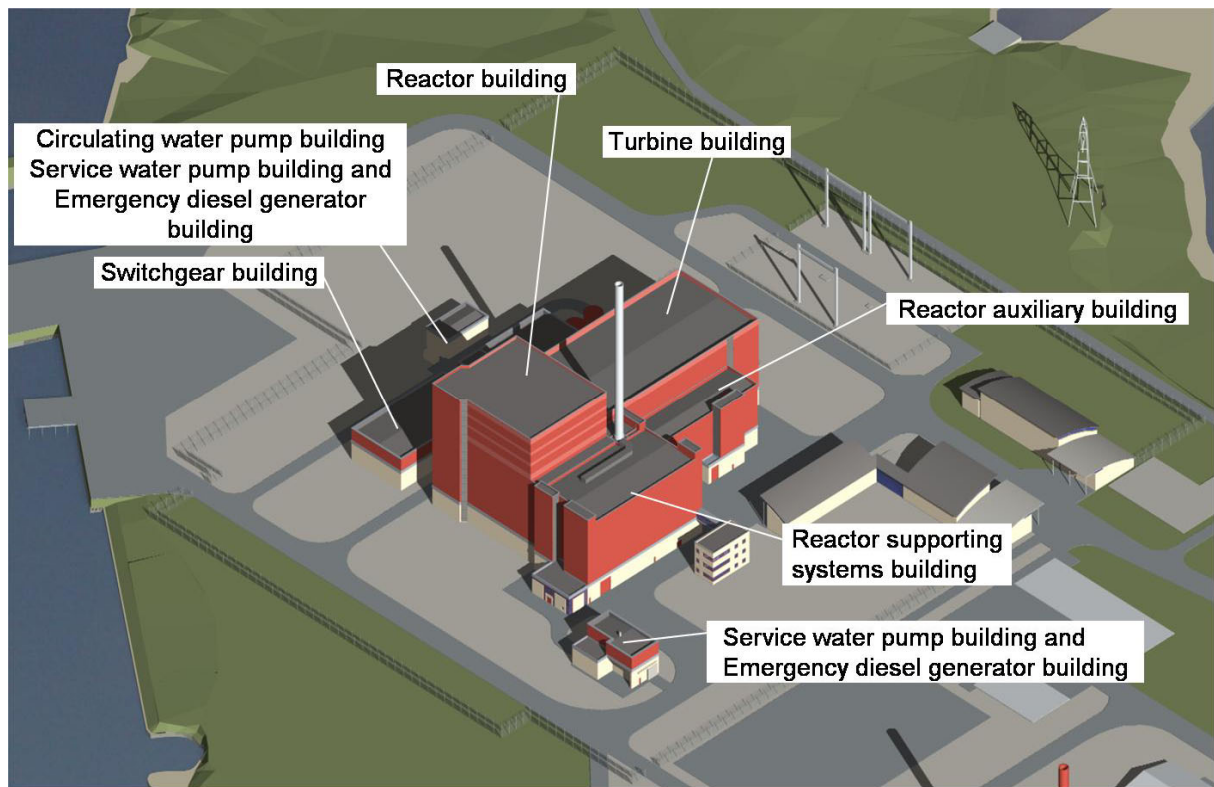


Figure A-2. SWR 1000 general plant layout.

The four-year basic design phase for the resulting "SWR 1000" plant started in mid-1995. In parallel, an experimental testing program was conducted at FRAMATOME's ANP (now AREVA NP) own testing facilities and at other German and European research centers to provide verification of the mode of operation and effectiveness of the SWR1000's passive safety systems.

Since 2000 an extended basic design phase has been underway. At the beginning of this phase it was decided to increase the net electric output to 1254 MW to serve the needs of the nuclear industry with a larger power range.

The main goal of this advanced BWR is to replace the active safety systems used in current designs with passive safety systems enabling:

- Reliable control of the various design basis accidents;
- Low probability of beyond-design-basis accidents (core damage frequency);
- Limitation of the consequences of a core melt accident to the plant itself;
- High plant availability; and
- Economic competitiveness.

The adoption of passive safety systems requires a lot of engineering effort, planning and layout work to modify previous BWR system designs. The passive safety systems replacing and/or supplementing the redundant active safety systems must be capable of ensuring reliable plant operation and accident control. They mainly operate using basic laws of physics such as gravity, natural convection, temperature and pressure differentials.

Various features have been changed compared to existing BWR designs:

- Large water inventory in the reactor pressure vessel (RPV) above the core permits passive core cooling;
- Large water storage capacities inside and outside the reactor containment provide long grace periods and avoid the need for operator intervention, especially during and after accidents;
- For transients as well as for accident control, emergency condensers and containment cooling condensers passively remove decay heat from the core and containment, respectively;
- Activation of key safety functions such as reactor scram, containment isolation and automatic depressurization is backed up by passive systems (passive pressure pulse transmitters);
- Passive cooling of the RPV exterior in the event of a core melt accident ensures in-vessel melt retention;
- Despite the introduction of passive safety systems for accident control the operating experience gained from current BWR plants constitutes the basis for the new concept; and
- Simplification of reactor auxiliary systems and systems used for normal power operation.

The new, innovative design features of the SWR 1000 mark the transition to the next generation of nuclear power plants.

A.2. SWR 1000 Reactor coolant system and its main characteristics

The reactor coolant system is located in the reactor building and is surrounded by a reinforced-concrete containment with steel liner.

Three main steam lines connecting the RPV to the high-pressure turbine section serve to transport the steam generated in the reactor to the turbine. Isolation valves of diverse design are provided in each main steam line inside and outside the containment. The inboard isolation valves are gate valves while the outboard isolation valves are angle-type globe valves.

The function of the feed water system is to receive the water from the main condensate system and to route it to the reactor via two feed water lines. Isolation valves are provided in each feed water line inside and outside the containment. The inboard isolation valves are check valves while the outboard isolation valves are gate valves.

The outboard valves in both the main steam lines and the feed water lines are located immediately adjacent to the containment.

Each main steam line inside the containment is allocated a specific number of safety-relief valves (SRVs) for overpressure protection of the RPV.

For pressure relief, opening of the SRVs is possible when a signal is received from the reactor protection system. If reactor pressure should, however, continue to rise, then all SRVs are mechanically opened by spring-loaded pilot valves. The SRVs close, however, with a corresponding hysteresis.

For automatic depressurization, the SRVs are opened either by solenoid pilot valves or by the passive pressure pulse transmitters (PPPTs) and diaphragm pilot valves, all SRVs being

opened at the same time in this case. Half of the SRVs are designed such that they do not re-close after automatic depressurization. This ensures that the pressure in the reactor remains at a low level.

The steam blown down by the valves is routed downwards into the core flooding pools through discharge pipes. These pipes terminate below the surface of the pool water in specially designed T-shaped quenchers.

A3. SWR 1000 Reactor core and fuel design

The SWR 1000 core represents an "evolutionary" development based on previously common BWR core designs. While no changes have been made to the basic core structure, certain modifications have been introduced. These include a reduced active core height and an enlarged fuel assembly.

A consequence of reducing the active core height is that the core can be positioned lower down inside the RPV. This provides a larger water inventory inside the RPV above the core, a feature which facilitates accident control.

The above-mentioned modification of the fuel assemblies consisted of enlarging the existing ATRIUM™10 fuel assembly design (10x10-9Q) to a 12x12-16 rod array (ATRIUM™12). Fuel rod diameter and pitch, on the other hand, remained the same as in the ATRIUM™10 fuel assembly. As a result of this new design, there are fewer fuel assemblies in the core, which reduces handling times during refueling. Reducing the number of fuel assemblies also reduces the number of control rods, and hence the number of control rod drives as well. The average power density is around 51 kW/l.

A4. SWR 1000 Safety requirements and design philosophy

The safety concept of the SWR 1000 is based on two fundamental principles:

1. Prevention of accidents and environmental impacts
2. Accident control (damage mitigation)

First Safety Principle: "Prevention of accidents and environmental impacts"

This first and most important principle is put into practice by imposing stringent requirements on the design and quality of the plant as well as on the qualifications of personnel, i.e. their competence and reliability.

For this purpose, safety-promoting design, manufacturing and operating principles are pursued on the first level of safety measures.

According to general experience with technical systems, malfunctions of components or systems leading to off-normal operating conditions cannot be entirely ruled out during the service life of a plant, even if the above principles have been observed. In order to control these off-normal operating conditions, systems are designed and measures are taken to control and monitor operation such that the occurrence of accidents as a consequence of off-normal operating conditions is prevented with an adequate degree of reliability (second level).

Second Safety Principle: "Accident Control (Damage Mitigation)"

Despite the precautions taken in compliance with the first safety principle on the two levels described above, it is nevertheless assumed that improbable but hypothetically conceivable accidents may occur during the service life of the nuclear power plant, i.e. accidents which the plant must be designed to control. These accidents – called design basis accidents – include, for example, the following:

- Accidents caused by plant-internal events: main steam line break, feedwater line break, control equipment malfunctions or accidents not involving loss of coolant; and
- Accidents due to natural or external man-made hazards: earthquakes or high water levels.

In order to fulfill the second principle, equipment for accident control is provided on a third level of safety measures. In the case of the SWR 1000, new approaches have been pursued which lead to a significantly higher level of safety.

The safety equipment is designed in such a way that it protects the plant personnel and the population in the vicinity of the plant against the consequences of accidents. For this, the following design principles are applied:

- Redundancy, diversity and independence of subsystems (trains);
- Physical separation of redundant subsystems (trains);
- Safety-oriented system behavior in the case of subsystem or component malfunctions; and
- Passive safety functions given preference over active functions.

Equipment for accident control consists of passive and active safety components.

Passive components, which do not require I&C signals or external power to perform their protective function, take effect solely by virtue of their presence (such as the numerous protective barriers made of concrete or steel) or as a result of basic laws of physics (such as gravity and natural convection). Examples of such equipment are the emergency condenser and the passive pressure pulse transmitter.

Active safety equipment, such as the RHR pumps and the control rods, are controlled and, if necessary, put into operation by the reactor protection system.

In addition to the measures for controlling design basis accidents, features are also provided on a fourth level of safety measures to mitigate the consequences of severe accidents, such as:

- Aircraft crash;
- Explosion pressure waves;
- Combustible and toxic gases; and
- Core melt.

A5. SWR 1000 Safety systems and features (active, passive and inherent)

Passive equipment for accident control

The fundamentally new concept for accident control incorporated into the SWR 1000 includes equipment which, in the event of failure of the active safety equipment, will bring the plant to

a safe condition without the need for any I&C signals or external power. This passive safety equipment (Figure A-3, A-4 and A-5) includes the following:

- *Emergency condensers*
The function of the emergency condenser (EC) system is to remove, in the event of an accident, the decay heat still being generated in the reactor as well as any sensible heat stored in the RPV to the core flooding pools, without any coolant inventory being lost from the RPV. The system thus replaces the high-pressure coolant injection systems used in existing BWR plants. The EC system also provides a means for reactor pressure relief that is diverse with respect to the safety-relief valves.
- *Containment cooling condensers*
The task of the four containment cooling condensers (CCCs) is to remove – by entirely passive means – decay heat from the containment following accidents leading to the release of steam inside the drywell, and in this way to limit buildup of containment pressure. They provide redundancy and diversity with respect to the RHR system.
- *Core flooding system*
The core flooding system is a passive low-pressure flooding system for controlling the effects of loss-of-coolant accidents (LOCAs). It is installed at an elevation which ensures that, following automatic depressurization of the reactor, it can passively flood the reactor core by means of gravity flow. The system provides redundancy and diversity with respect to the core flooding function of the RHR system.
- *Drywell flooding system*
A postulated severe accident involving core melt is controlled such that the molten core is retained inside the RPV. For this purpose the section of the drywell surrounding the RPV is flooded with water in order to cool the RPV exterior and thus remove heat from the reactor.
- *Passive pressure pulse transmitters*
The PPPT is a completely passive switching device which is used to directly initiate the following safety functions (as a minimum), without the need for I&C equipment: reactor scram, containment isolation at the main steam line penetrations, and automatic depressurization of the RPV. The PPPT comes into action as a result of a drop or increase in reactor water level as well as an increase in reactor pressure. For activating the various safety functions, PPPTs of redundant design are installed at two elevations. The upper PPPTs, situated at an elevation beneath that of the normal water level of the RPV, are responsible for initiating reactor scram. The lower PPPTs, arranged at a lower elevation, activate automatic depressurization of the reactor as well as closure of the main steam containment isolation valves. Further PPPTs installed at appropriate locations respond to a rise in reactor water level above the main steam nozzles and likewise activate containment isolation at the main steam line penetrations.

Active safety systems

In order to control the effects of design basis accidents, each nuclear power plant is equipped on the third safety level with a special safety system (see Figure A-3 below) consisting of the reactor protection system and the active safety equipment actuated by it. The reactor protection system is a programmable digital I&C system which continuously monitors all important plant operating parameters, initiates safety-oriented actions if specified limits are

approached and, in this way, takes control over operational disturbances, thus preventing them from developing into accidents. The postulated design basis accidents can thus be controlled to such an extent through activation of the safety equipment that consequences are restricted to the plant itself.

The response of the reactor protection system is not event-oriented but safety-oriented, which ensures that no potential causes of failures or malfunctions can be overlooked when designing the system. The active safety equipment mainly comprises process systems.

As far as the overall safety concept is concerned, it is vitally important that all types of accidents that involve the risk of major release of radioactivity to the environment will be determined.

By far the largest proportion of radioactivity present in the nuclear power plant is located in the reactor core, i.e. contained in the crystal lattice of the fuel and in the fuel cladding tubes. Therefore large releases are only conceivable if these two inner activity barriers should become damaged. The following theoretically conceivable types of accidents involving the risk of an increased release of activity are therefore possible in the event of damage to these two barriers:

- Unallowable rise in reactor power,
- Impaired heat removal from the reactor core,
- Loss of cooling as a result of a loss of coolant.

Among the various active safety systems, a central role is played by the reactor protection system which continuously monitors all important plant operating parameters and, if specified limits are approached, initiates safety actions by actuating other safety equipment as and when required.

The hydraulic scram system employs neutron-absorbing control rods which are kept in the withdrawn position, i.e. at the bottom of the core, during reactor power operation. If a scram is triggered, valves are opened in lines leading to the scram tanks and the energy stored in these accumulators rapidly inserts the control rods into the core from below, thus terminating the chain reaction.

A second, diverse shutdown system is also provided with which the reactor can be shut down by injecting a neutron-absorbing boron solution into the reactor coolant.

If a release of radioactivity into the containment is to be expected during an accident, the containment isolation system allows the containment to be isolated from the plant environs. All pipes, which penetrate the containment wall and belong to systems not required for accident control, can be isolated by containment isolation valves.

The RHR system takes over cooling of the reactor core and/or containment heat removal in the event of an accident.

Finally, mention should be made of the emergency power supply system which supplies power to active safety-related systems if the main generator cannot provide auxiliary power in the event of an accident and if supply from the offsite power system is not available.

ANNEX B OPERATING BWR PLANT GUNDREMMINGEN UNIT B AND C

(A State-of-the-Art Twin-Unit Boiling Water Reactor Plant [51])

In Germany, units B and C of Gundremmingen Nuclear Power Station, are sited right next to Gundremmingen Unit A which was decommissioned in 1980, went on operation in 1984 and 1985, respectively. The two 1310 MW_e units were built by Kraftwerk Union AG for RWE Energie AG and Bayernwerk AG



Figure B-1. Gundremmingen Unit A (left) and Units B and C (right).

Gundremmingen was the first plant to incorporate the full scope of KWU's 1972 BWR Product line.

The principle design of the direct cycle plant is shown in Figure B-2. The water inside the RPV, which has a pressure of 7.06 MPa, is drawn from the down-comer annulus (see the RPV and its internals below) into the lower core plenum by eight reactor water recirculation pumps flanged to the bottom of the vessel. From here the water passes upwards through the core where it is heated to form an steam-water mixture which exits the core at the top. The mixture is then directed through an array of steam separators in which the water is separated from the steam. The steam exiting the steam separators passes through steam dryers and is discharged from the RPV into the main steam piping which routes it to the turbine. It is then exhausted to the condensers.

The core of each unit consists of 784 fuel assemblies.

The inside diameter of the RPV is 6.62 m and its total height 22.68 m; the weight is approximately 785 tons (see Figure B-3).

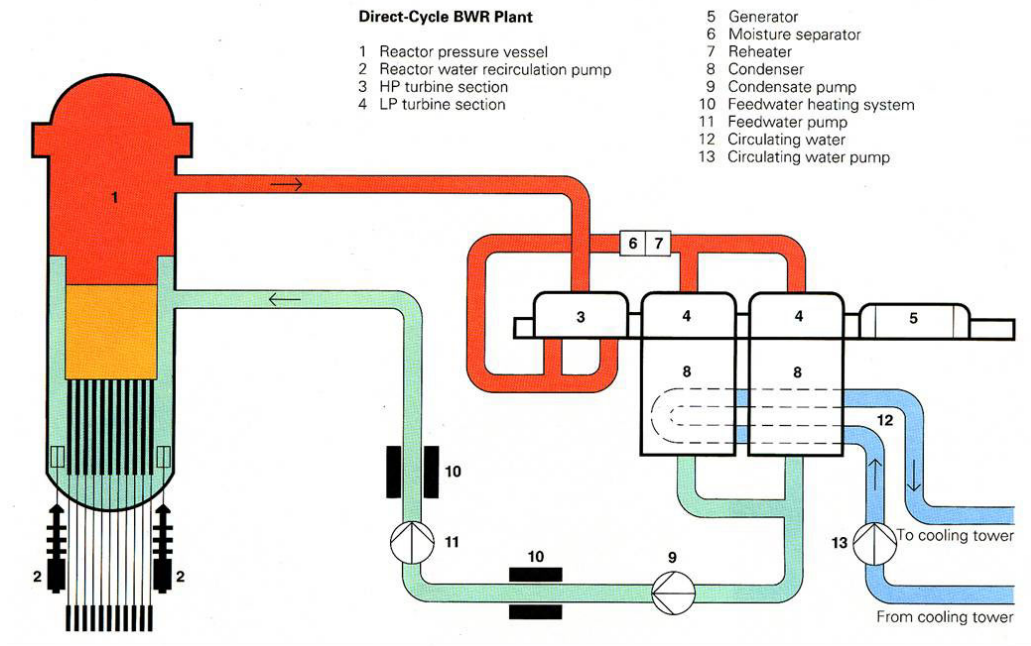


Figure B-2. Direct cycle BWR plant.

Reactor Pressure Vessel and Internals

Eight recirculation pumps draw the reactor water down through the downcomer annulus between the RPV wall and the core shroud and pass it through the reactor core and pass it through the reactor core. The steam generated in the core is dried before being discharged to the turbine through four main steam outlet nozzles.

- 1 Reactor pressure vessel
- 2 Reactor core
- 3 Core shroud
- 4 Downcomer annulus
- 5 Reactor water recirculation pump
- 6 Steam separator assembly
- 7 Steam dryer assembly
- 8 Control rod drives
- 9 Control rods
- 10 Feedwater nozzle
- 11 Main steam nozzle

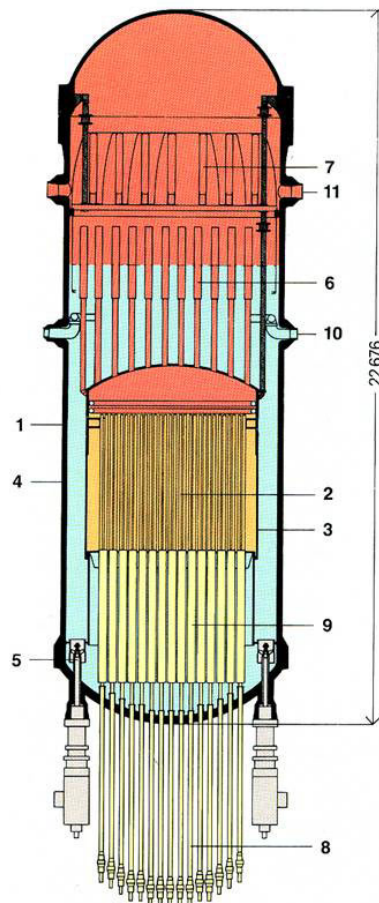


Figure B-3: BWR pressure vessel and internals.

The design of the containment is shown in Figure B-4:

Reactor Pressure Vessel and Containment

The reactor pressure vessel is surrounded by an approximately 1-m-thick biological shield and a cylindrical concrete containment.

- 1 Containment
- 2 Steel liner
- 3 Missile shield
- 4 Biological shield
- 5 Reactor pressure vessel
- 6 Fuel assemblies
- 7 Control rods
- 8 Reactor water recirculation pump
- 9 Feedwater nozzle
- 10 Main steam line
- 11 Pressure suppression chamber
- 12 Vent pipe
- 13 Lock
- 14 Scram accumulator
- 15 Reactor building
- 16 Isolation valve

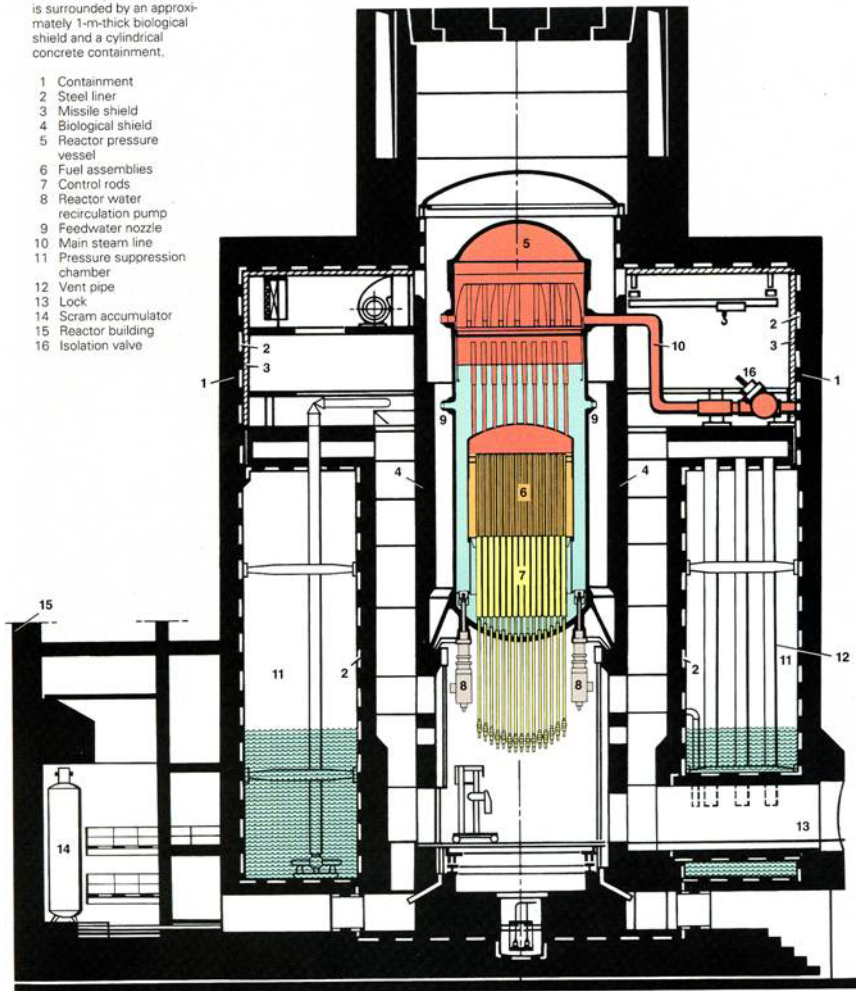
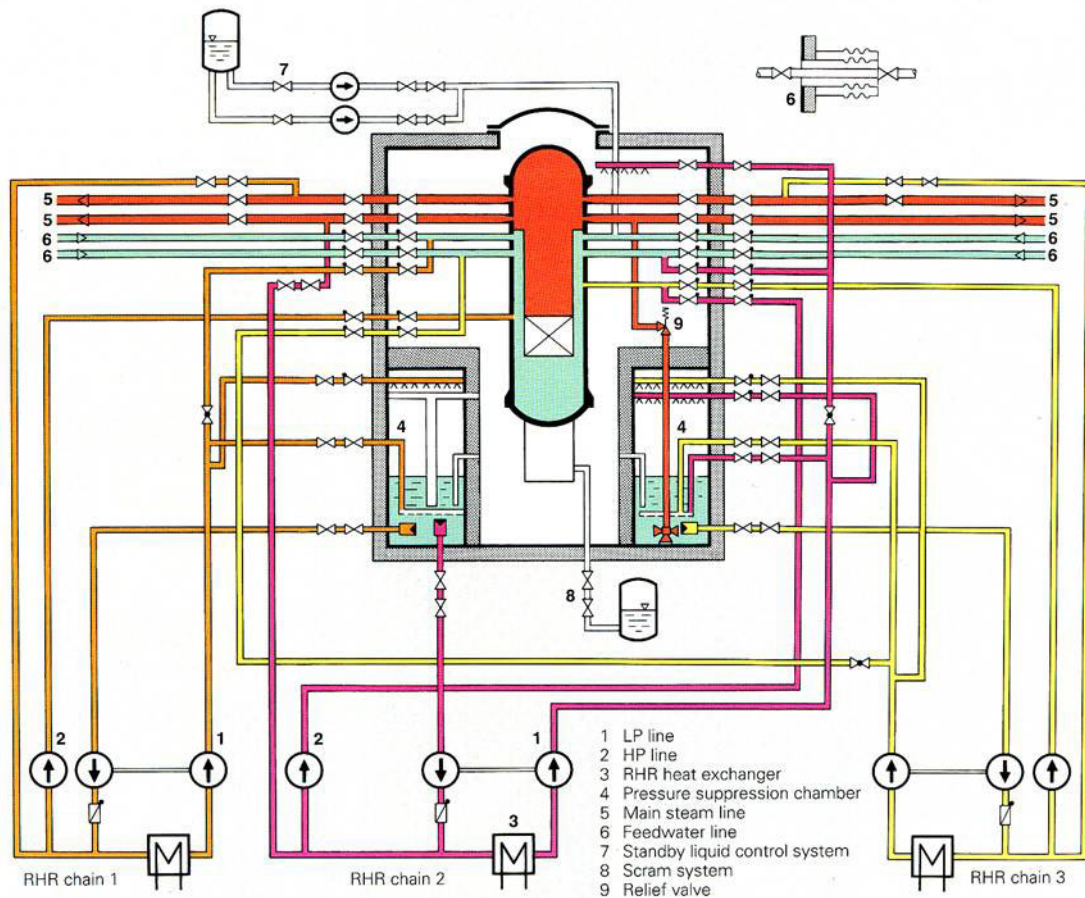


Figure B-4. BWR pressure vessel and containment.

The pressure suppression system which is located inside the cylindrical containment, serves to remove the thermal energy from the reactor whenever the main heat sink is not available. The system is also designed to prevent excessive containment pressure build-up in the event of a main steam or feed water pipe break inside the containment. The pressure suppression system and the containment thus prevent radioactive materials from being released to the environment. In addition, the containment is equipped with a filtered venting system to control the consequences of hypothetical accidents.

In the event of a pipe break in the primary system, the steam released inside the containment flows through vent pipes into the pressure suppression pool where it condenses. If a pipe break should occur outside the containment, the pipes penetrating the containment are closed through closure of the inboard and outboard containment isolation valves.

As illustrated in Fig. B-5, three full-capacity residual heat removal (RHR) chains are provided for tasks associated with normal plant operation as well as for safety-related functions. Each RHR system is divided into a low-pressure (LP) and a high-pressure (HP) line. The LP line contains a heat exchanger for removing heat from the reactor system to the closed cooling water system. This energy is then transferred via a second heat exchanger to the service cooling water system which discharges it to the Danube river.



The three residual heat removal chains serve to cool the reactor both following normal shutdown and after a loss-of-coolant accident.

Figure A-5. Three residual heat removal systems of the BWR Units B and C.

In the event of a loss-of-coolant accident (LOCA), water from the pressure suppression pool is fed by both the HP line and the LP line into the reactor vessel, either via the feed water lines or via separate nozzles connected to the feed water spargers. The components of the RHR systems are designed such that each individual system can provide sufficient water for cooling the fuel assemblies, regardless of whether the LOCA is caused by a small break accompanied by a proportionally small drop in pressure or by a break in the largest-diameter pipe connected to the reactor vessel. To limit the mass outflow out of the pressure vessel a flow limiter is integrated in the RPV wall for each of the steam lines. The steam still being generated by residual heat following a reactor scram is fed to the pressure suppression pool via relief valves installed in the steam lines inside the containment. Coolant lost from the RPV is made up with water supplied by RHR systems. In the event that pressure reduction is required inside the containment, one of the RHR systems LP lines can also be used for drywell spraying.

Residual heat is likewise removed by the RHR systems following normal shutdown and depressurization of the reactor (e.g., for refuelling). In such an event, however, the water is not taken from the pressure suppression pool but from the reactor vessel itself. In addition, one of the RHR systems can be manually lined up to augment the cooling capacity of the fuel pool cooling system if the entire core has been discharged to the pool.

In order to be able to shut down the reactor and maintain it in a sub-critical state even without the use of control rods, a standby liquid control system is provided which injects concentrated boron solution from a storage tank into the reactor vessel for neutron absorption.

ANNEX C AREAS OF SAFETY RD&D

As stated in Ref. [2] the following RD&D areas can be anticipated:

Advanced nuclear power plant designs envisioned today use, besides light or heavy water (up to supercritical states), *liquid metals or gas as working fluids*. Their properties in both normal operation and accident conditions must be determined experimentally. Further work is needed to better understand aspects of natural circulation phenomena such as initiation, stability, etc., especially for two phase flow and flow of supercritical fluid.

Neutronic-thermal-hydraulic interaction is another important area that will need further study, mainly for supercritical water and for fluid states like sub-cooled two-phase fluid with the potential for coupled neutronic and thermal hydraulic oscillations³¹.

Innovative fuel designs will require tests on fuel performance including dimensional and mechanical stability, possible chemical interaction between fuel element and coolant, and mechanical-chemical interaction between fuel material and fuel element cladding.

INS may include *accelerator driven systems* (ADS), which transmute minor actinides and long-lived fission products. The spectrum of unresolved problems for which RD&D is required extends from proton/neutron physics (database) to thermal-hydraulics of a liquid-metal-cooled system. A similar topic of interest is the use of inert fuel matrices for actinide burning in thermal reactors.

Reprocessing is a series of chemical reactions, such as solvent-extraction, oxidation/reduction, electro-refining, ion-exchange, etc. Extensive RD&D in areas as diverse as process control, solvent chemistry, and dry processing (oxidation/reduction reactions) is required. In addition, a method should be developed for quantifying the safety of such facilities.

Digital Instrumentation and Control (I&C) is expected to be used extensively for active control. Again one would expect 'smarter' I&C systems, tied to databases representing the current plant state, operating limits (technical specifications), design and PSA models, using artificial intelligence to control the plant, and diagnose and mitigate accidents. Off-site links would help in plant monitoring and problem solving.

Further development of *Probabilistic Safety Analyses* methods [31], including best estimate plus uncertainty analysis, and their supporting data bases are required and need to be capable of:

- Assessing innovative nuclear designs, which use inherent safety characteristics and passive, as well as active, systems;
- Assessing total risk from various states, full power, low power and shutdown, and considering both internal and most external initiating events;
- Accounting for safety culture and human factors;
- Accounting for ageing effects; and
- Quantifying the effects of random, data and modelling uncertainties.

Finally, the implementation of *defence-in-depth* (DID) for advanced reactors may require a new approach that would be based on a more advanced interpretation of DID fully integrated with PSA insights. DID has been achieved to date primarily through deterministic analyses

³¹ e.g., reactors cooled with supercritical water and BWRs.

based on prevention and/or mitigation. It is expected that risk informed decision-making would play an important role in the development of future reactors and fuel cycle facilities. This will help to achieve high levels of safety while reducing cost, in particular through simplification of safety systems and a sound and well-balanced safety classification of safety systems and components. The challenges for the future are to develop more confidence in the PSA tools, to achieve an appropriate integration of deterministic and probabilistic analyses, and to demonstrate that sufficient DID can be achieved through simpler and cheaper technological solutions.

In summary, RD&D activities on innovative reactor and fuel cycle installations are needed to:

- Identify all important phenomena;
- Validate codes in new regimes of fluid and solid material behaviour;
- Justify scaling to commercial size installations;
- Compensate for lack of operating experience;
- Demonstrate the technology at an appropriate scale, e.g., the pilot plant scale;
- Obtain reliability data; and
- Develop tools for risk-informed decision-making.

ANNEX D
IDEAS OF FUTURE DEVELOPMENT OF THE INPRO METHODOLOGY
IN THE AREA OF SAFETY

In the following some ideas are presented to make the INPRO methodology in the area of safety more simple and consistent.

D1. Reduction of the four INPRO basic principles to a single one

The four basic principles in the INPRO area of safety are:

Installations of an Innovative Nuclear Energy System shall:

BP1: *Incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.*

BP2: *Excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach.*

BP3: *Ensure that the risk from radiation exposures to workers, the public and the environment during construction/commissioning, operation, and decommissioning, shall be comparable to that of other industrial facilities used for similar purposes.*

Further, the development of an Innovative Nuclear Energy System shall:

BP4: *Include associated RD&D work 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 existing plants.*

According to Chapter 4 of Ref. [3] a basic principle should define a goal and provide guidance for RD&D, and a user requirement should define means how to achieve this goal. Looking at BP1 to BP4 it seems that all of them sound more like a kind of user requirement defining what should be done instead of defining a goal to be reached.

All four BPs could be replaced by a single new goal or **BP new** as follows:

INPRO basic principle BP-new (Siting of INS): *Installations of an INS shall be so safe that they can be located at the same site as other industrial facilities used for similar purpose.*

The existing user requirements would be kept (only renumbered). If the new BP is adopted, it must be confirmed that no idea contained in the text of the “old” BPs is lost, i.e. if an idea in a BP is not repeated in the text of its user requirements it must be included into the wording of the user requirements:

- All ideas of BP1 are included in the corresponding URs: UR1.1 to UR1.5 covers enhanced DID, UR1.6 covers independence of DID levels; text on background of “old” BP1 could be moved to UR1.1 and UR1.6 respectively;
- BP2 ideas are completely covered by UR2.1; background of “old” BP2 could be moved to UR2.1;
- In case of BP3 the wording “during construction/ commissioning, operation and decommissioning” has to be added in the UR3.1 and UR3.2; background of “old” BP3 could be moved to UR3.1 and UR3.2 respectively;
- Ideas of BP4 are covered by UR4.1 to UR4.4; background of BP4 could be moved to UR4.2.

D2. Inclusion of BP2/UR2.1 into BP1

BP2 (elimination of hazards) could be integrated into BP1 (or become a UR of BP new). BP2/UR2.1 could become an additional UR for DID level 1 “robustness”. Elimination of hazards and implementation of inherent safety features/passive systems clearly increases robustness.

D3. Inclusion of assessment of safety culture into this volume

As stated in Volume 3 of the INPRO manual [10], it seems appropriate to move the assessment of the safety culture into this volume. One argument for such a change is that the INPRO assessor for this topic needs a general background in nuclear safety.

ANNEX E CHECKLIST FOR ASSESSMENT

In the following pages a checklist (taken from Table.5.4 of Ref. [1]) is provided that could help the assessor to *summarize* the *results* of his assessment and to *check* whether a *complete INPRO assessment* has been done, i.e. whether all INPRO criteria have been assessed. In no way could such a list be sufficient to perform the INPRO assessment. It should be complemented by and referring to comprehensive supporting documentation. It is important to note that an INPRO assessment of a nuclear reactor is not a substitute process for licensing such a plant, i.e. it is not a basis for licensing decision making.

Table E lists all the INPRO basic principles, user requirements and criteria in the area of safety. For the criteria all indicators (IN), and if used also the evaluation parameters (EP), are presented together with the corresponding acceptance limit (AL). The table also provides for a reference where in the report the IN, EP and AL are described. The last four columns could be used to directly document the results of the assessment process.

It is to be noted that the Table E clearly emphasizes that Member States could add their own (country specific) criteria, and, if necessary their own user requirements (as explained in Section 4.3.3 of Ref. [3]).

Table E. Checklist for INPRO assessment

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations.							
User requirement UR1.1 (Robustness): Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation.							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.1.1 robustness							
IN1.1.1: Robustness of design (simplicity, margins). EP1.1.1.1: Margins of design. EP1.1.1.2: Simplicity of design. EP1.1.1.3: Quality of manufacture and construction. EP1.1.1.4: Quality of materials. EP1.1.1.5: Redundancy of systems.	3.2.1.1	AL1.1.1: Superior to existing designs in at least some of the aspects discussed in the text.	3.2.1.1				

122 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.1 (Robustness): Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation. (continued)							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.1.2 operation							
IN1.1.2: High quality of operation EP1.1.2.1: Margins of operation. EP1.1.2.2: Reliability of control systems. EP1.1.2.3: Impact from incorrect human intervention. EP1.1.2.4: Quality of documentation. EP1.1.2.5: Quality of training. EP1.1.2.6: Organization of plant. EP1.1.2.7: Availability / capability of plant. EP1.1.2.8: Use of world wide operating experience.	3.2.1.2	AL1.1.2: Superior to existing designs in at least some of the aspects discussed in the text.	3.2.1.2				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.1 (Robustness): Installations of an INS should be more robust relative to existing designs regarding system and component failures as well as operation. (continued)							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.1.3 inspection							
IN1.1.3: Capability to inspect.	3.2.1.3	AL1.1.3: Superior to existing designs in at least some of the aspects discussed in the text.	3.2.1.3				
CRI.1.4 failures and disturbances							
IN1.1.4: Expected frequency of failures and disturbances.	3.2.1.4	AL1.1.3: Superior to existing designs in at least some of the aspects discussed in the text.	3.2.1.4				

124 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.2 (Detection and interception):							
<i>Installations of an INS should detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions.</i>							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR1.2.1 I&C and inherent characteristics IN1.2.1: Capability of I&C system and/or inherent characteristics to detect and intercept and/or compensate deviations from normal operational states. EPI.2.1.1: Continues monitoring of plant health. EPI.2.1.2: Dynamic plant analysis.	3.2.2.1	AL1.2.1: Key system parameters relevant to safety do not exceed limits acceptable for continued operation.	3.2.2.1				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.2 (Detection and interception):							
<i>Installations of an INS should detect and intercept deviations from normal operational states in order to prevent anticipated operational occurrences from escalating to accident conditions (continued).</i>							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR1.2.2 grace period							
IN1.2.2: Grace period until human interactions are required.	3.2.2.2	AL1.2.2: Superior to existing designs in at least some of the aspects discussed in the text.	3.2.2.2				
CR1.2.3 inertia							
IN1.2.3: Inertia to cope with transients.	3.2.2.3	AL1.2.3: Superior to existing designs in at least some of the aspects discussed in the text.	3.2.2.3				

126 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR3 (Design basis accidents): The frequency of occurrence of accidents should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period.							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
IN1.3.1: Calculated frequency of occurrence of DBA.	CR1.3.1 frequency of DBA 3.2.3.1	AL1.3.1: Reduced frequency of accidents that can cause plant damage relative to existing facilities.	3.2.3.1				
IN1.3.2: Grace period until human intervention is necessary.	CR1.3.2 grace period 3.2.3.2	AL1.3.2: Increased relative to existing facilities.	3.2.3.2				
IN1.3.3: Reliability of engineered safety features.	CR1.3.3 safety features 3.2.3.3	AL1.3.3: Equal or superior to existing facilities.	3.2.3.3				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.3 (Design basis accidents): The frequency of occurrence of accidents should be reduced, consistent with the overall safety objectives. If an accident occurs, engineered safety features should be able to restore an installation of an INS to a controlled state, and subsequently (where relevant) to a safe shutdown state, and ensure the confinement of radioactive material. Reliance on human intervention should be minimal, and should only be required after some grace period. (continued)							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.3.4 barriers							
IN1.3.4: Number of confinement barriers maintained.	3.2.3.4	AL1.3.4: At least one.	3.2.3.4				
CRI.3.5 controlled state							
IN1.3.5: Capability of engineered safety features to restore the INS to a controlled state (without operator actions).	3.2.3.5	AL1.3.5: Sufficient to reach a controlled state.	3.2.3.5				
CRI.3.6 sub-criticality							
IN1.3.6: Sub criticality margins.	3.2.3.6	AL1.3.6: Sufficient to cover uncertainties and to allow adequate grace period.	3.2.3.6				

128 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BPI: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement URI.4 (release into containment): The frequency of a major release of radioactivity into the containment / confinement of an INS due to internal events should be reduced. Should a release occur, the consequences should be mitigated.							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.4.1 major release into containment							
IN1.4.1: Calculated frequency of major release of radioactive materials into the containment / confinement.	3.2.4.1	AL1.4.1: At least an order of magnitude less than for existing designs; even lower for installations at urban sites.	3.2.4.1				
CRI.4.2 processes							
IN1.4.2: Natural or engineered processes sufficient for controlling relevant system parameters and activity levels in containment / confinement.	3.2.4.2	AL1.4.2: Existence of such processes.	3.2.4.2				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.4 (release into containment): The frequency of a major release of radioactivity into the containment / confinement of an INS due to internal events should be reduced. Should a release occur, the consequences should be mitigated. (continued)							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
IN1.4.3: In-plant severe accident management.	CR1.4.3 accident management						
	3.2.4.3	AL1.4.3: Procedures, equipment and training sufficient to prevent large release outside containment / confinement and regain control of the facility.	3.2.4.3				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.5 (release into environment): A major release of radioactivity from an installation of an INS should be prevented for all practical purposes, so that INS installations would not need relocation or evacuation measures outside the plant site, apart from those generic emergency measures developed for any industrial facility used for similar purpose.							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR1.5.1 major release to environment							
IN1.5.1: Calculated frequency of a major release of radioactive materials to the environment.	3.2.5.1	AL1.5.1: Calculated frequency $<10^{-6}$ per unit-year, or practically excluded by design.	3.2.5.1				
CR1.5.2 consequences							
IN1.5.2: Calculated consequences of releases (e.g., dose).	3.2.5.2	AL1.5.2: Consequences sufficiently low to avoid necessity for evacuation. Appropriate off-site mitigation measures (e.g., temporary food restrictions) are available.	3.2.5.2				
CR1.5.3 risk							
IN1.5.3: Calculated individual and collective risk.	3.2.5.3	AL1.5.3: Comparable to facilities used for a similar purpose.	3.2.5.3				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.6 (independence of DID levels): An assessment should be performed for an INS to demonstrate that the different levels of defence-in-depth are met and are more independent from each other than for existing systems.							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.6.1 independence of DID levels							
IN1.6.1: Independence of different levels of DID.	3.2.6.1	AL1.6.1: Adequate independence is demonstrated, e.g., through deterministic and probabilistic means, hazards analysis etc.	3.2.6.1				

132 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement URI.7 (human machine interface): Safe operation of installations of an INS should be supported by an improved Human Machine Interface resulting from systematic application of human factors requirements to the design, construction, operation, and decommissioning.							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.7.1 human factors							
IN1.7.1: Evidence that human factors (HF) are addressed systematically in the plant life cycle.	3.2.7.1	AL1.7.1: Satisfactory results from assessment.	3.2.7.1				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP1: (defence in depth): Installations of an Innovative Nuclear Energy System shall incorporate enhanced defence-in-depth as a part of their fundamental safety approach and ensure that the levels of protection in defence-in-depth shall be more independent from each other than in existing installations. (continued)							
User requirement UR1.7 (human machine interface): Safe operation of installations of an INS should be supported by an improved Human Machine Interface resulting from systematic application of human factors requirements to the design, construction, operation, and decommissioning. (continued)							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CRI.7.2 human response model							
IN1.7.2: Application of formal human response models from other industries or development of nuclear specific models.	3.2.7.2	AL1.7.2: - Reduced likelihood of human error relative to existing plants, as predicted by HF models. - Use of artificial intelligence for early diagnosis and real-time operator aids. - Less dependence on operator for normal operation and short-term accident management relative to existing plants.	3.2.7.2				

Note: User requirement UR2 of the INPRO area of physical protection [18] has to be considered here too (integration of safety, proliferation resistance and physical protection into the INS design).

134 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP2: (inherent safety): *Installations of an INS shall excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach.*

User requirement UR2.1 (minimization of hazards): *INS should strive for elimination or minimization of some hazards relative to existing plants by incorporating inherently safe characteristics and/or passive systems, when appropriate.*

Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR2.1.1 hazards							
IN2.1.1: parameters related to hazards EP2.1.1.1: Stored energy. EP2.1.1.2: Flammability. EP2.1.1.3: Inventory of radioactive materials. EP2.1.1.4: Criticality. EP2.1.1.5: Available excess reactivity. EP2.1.1.6: Reactivity feed back.	3.3.1.1	AL2.1.1: Superior to existing designs.	3.3.1.1				
CR2.1.2 frequency of AOO & DBA							
IN2.1.2: Expected frequency of abnormal operation and accidents.	3.3.1.2	AL2.1.1: Lower frequencies compared to existing facilities.	3.3.1.2				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP2: (inherent safety): Installations of an INS shall excel in safety and reliability by incorporating into their designs, when appropriate, increased emphasis on inherently safe characteristics and passive systems as a part of their fundamental safety approach. <i>(continued)</i>							
User requirement UR2.1 (minimization of hazards): INS should strive for elimination or minimization of some hazards relative to existing plants by incorporating inherently safe characteristics and/or passive systems, when appropriate. <i>(continued)</i>							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR2.1.3 consequences							
IN2.1.3: Consequences of abnormal operation and accidents.	3.3.1.3	AL2.1.2: Lower consequences compared to existing facilities.	3.3.1.3				
CR2.1.4 confidence in innovation							
IN2.1.4: Confidence in innovative components and approaches.	3.3.1.4	AL2.1.4: Validity established.	3.3.1.4				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP3: (risk of radiation): *Installations of an INS shall ensure that the risk from radiation exposures to workers, the public and the environment during construction/ commissioning, operation, and decommissioning, are comparable to the risk from other industrial facilities used for similar purposes.*

User requirement UR3.1 (dose to workers): *INS installations should ensure an efficient implementation of the concept of optimization of radiation protection for workers through the use of automation, remote maintenance and operational experience from existing designs.*

Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR3.1.1 occupational dose							
IN3.1.1: Occupational dose values.	3.4.1.1	AL3.1.1: Less than limits defined by national laws or international standards and so that the health hazard to workers is comparable to that from an industry used for a similar purpose.	3.4.1.1				
User requirement UR3.2 (dose to public): <i>Dose to an individual member of the public from an individual INS installation during normal operation should reflect an efficient implementation of the concept of optimization, and for increased flexibility in siting may be reduced below levels from existing facilities.</i>							
CR3.2.1 public dose							
IN3.2.1: Public dose values.	3.4.2.1	AL3.2.1: Less than the limits defined by national laws or international standards and so that the health hazard to the public is comparable to that from an industry used for a similar purpose.	3.4.2.1				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP4: (RD&D): <i>The development of INS shall include associated Research, Development and Demonstration work 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 existing plants.</i>							
User requirement UR4.1 (safety basis): <i>The safety basis of INS installations should be confidently established prior to commercial deployment.</i>							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR4.1.1 safety concept							
IN4.1.1: Safety concept defined?	3.5.1.1	AL4.1.1: Yes.	3.5.1.1				
CR4.1.2 safety issues							
IN4.1.2: Clear process for addressing safety issues?	3.5.1.2	AL4.1.2: Yes.	3.5.1.2				

138 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP4: (RD&D): <i>The development of INS shall include associated Research, Development and Demonstration work 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 existing plants. (continued)</i>							
User requirement UR4.2 (RD&D for understanding): <i>Research, Development and Demonstration on the reliability of components and systems, including passive systems and inherent safety characteristics, should be performed to achieve a thorough understanding of all relevant physical and engineering phenomena required to support the safety assessment.</i>							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR4.2.1 RD&D							
IN4.2.1: RD&D defined and performed and database developed?	3.5.2.1	AL4.2.1: Yes.	3.5.2.1				
CR4.2.2 computer codes							
IN4.2.2: Computer codes or analytical methods developed and validated?	3.5.2.2	AL4.2.2: Yes.	3.5.2.2				
CR4.2.3 scaling							
IN4.2.3: Scaling understood and/or full scale tests performed?	3.5.2.3	AL4.2.3: Yes.	3.5.2.3				

Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP4: (RD&D): <i>The development of INS shall include associated Research, Development and Demonstration work 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 existing plants.</i>							
User requirement UR4.3 (pilot plant): <i>A reduced-scale pilot plant or large-scale demonstration facility should be built for reactors and/or fuel cycle processes, which represent a major departure from existing operating experience.</i>							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR4.3.1 novelty							
IN4.3.1: Degree of novelty of the process.	3.5.3.1	AL4.3.1: In case of <i>high degree of novelty</i> : Facility specified, built, operated, and lessons learned documented. In case of <i>low degree of novelty</i> : Rationale provided for bypassing pilot plant.	3.5.3.1				
CR4.3.2 pilot facility							
IN4.3.2: Level of adequacy of the pilot facility.	3.5.3.2	AL4.3.2: Results sufficient to be extrapolated.	3.5.3.2				

140 Table E. Checklist for INPRO assessment (continued)

INPRO basic principle BP4: (RD&D): <i>The development of INS shall include associated Research, Development and Demonstration work 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 existing plants.</i>							
User requirement UR4.4 (safety analyses): <i>For the safety analysis, both deterministic and probabilistic methods should be used, where feasible, to ensure that a thorough and sufficient safety assessment is made. As the technology matures, “Best Estimate (plus Uncertainty Analysis)” approaches are useful to determine the real hazard, especially for limiting severe accidents.</i>							
Indicator (IN) or Evaluation Parameter (EP) by INPRO or MS	IN or EP discussed in section	Acceptance Limit (AL) by INPRO or by MS	AL discussed in section	Value of IN or EP for assessed INS	Value of AL for assessed INS	Judgement on potential of INS to meet AL	Basis for judgement
CR4.4.1 risk informed approach							
IN4.4.1: Use of a risk informed approach?	3.5.4.1	AL4.4.1: Yes.	3.5.4.1				
CR4.4.2 uncertainties							
IN4.4.2: Uncertainties and sensitivities identified and appropriately dealt with?	3.5.4.2	AL4.4.2: Yes.	3.5.4.2				

REFERENCES

- [1] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Evaluation of Innovative Nuclear Reactors and Fuel Cycles, IAEA-TECDOC-1362, Vienna (2003).
- [2] INTERNATIONAL ATOMIC ENERGY AGENCY, Methodology for the Assessment of Innovative Nuclear Reactors and Fuel Cycles, IAEA-TECDOC-1434, Vienna (2004).
- [3] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Overview of the Methodology, Volume 1 of the Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2007).
- [4] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, INSAG-12, INSAG Series No. 12, IAEA, Vienna (1999).
- [5] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Design Requirements, Safety Standards Series No. NS-R-1, IAEA, Vienna (2000).
- [6] INTERNATIONAL ATOMIC ENERGY AGENCY, Status of Advanced Light Water Cooled Reactor Designs - 2004, IAEA-TECDOC-1391, Vienna (2004).
- [7] OECD INTERNATIONAL ENERGY AGENCY, OECD NUCLEAR ENERGY AGENCY, INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Nuclear Reactor Development Opportunities for International Cooperation, OECD/IEA, Paris (2002).
- [8] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Waste Management, Volume 4 of the Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2007).
- [9] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Safety of Nuclear Fuel Cycle Facilities, Volume 9 of the Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2007).
- [10] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Infrastructure, Volume 3 of the Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2007).
- [11] INTERNATIONAL ATOMIC ENERGY AGENCY, Fundamental Safety Principles, IAEA Safety Standards Series No. SF-1, IAEA, Vienna (2006).
- [12] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Defence in Depth in Nuclear Safety, INSAG-10, INSAG Series No. 10, IAEA, Vienna (1996).
- [13] 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).
- [14] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Environment, Volume 7 of the Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2007).

- [15] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Safety Culture (A Report by the International Nuclear Safety Advisory Group), INSAG-4, INSAG Series No. 4, (Safety Series No. 75), IAEA, Vienna (1991).
- [16] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Key practical Issues in Strengthening Safety Culture, INSAG-15, INSAG Series No. 15, IAEA, Vienna (2002).
- [17] 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).
- [18] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Physical Protection, Volume 6 of the Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2007).
- [19] INTERNATIONAL ATOMIC ENERGY AGENCY, Guidance for the Application of an Assessment Methodology for Innovative Nuclear Energy Systems, INPRO Manual – Proliferation Resistance, Volume 5 of the Final Report of Phase 1 of the International Project on Innovative Reactors and Fuel Cycles (INPRO), IAEA-TECDOC-1575, Vienna (2007).
- [20] INTERNATIONAL ATOMIC ENERGY AGENCY, Accident Analysis for Nuclear Power Plants, IAEA Safety Reports Series No. 23, IAEA, Vienna (2002).
- [21] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Assessment and Verification for Nuclear Power Plants, IAEA Safety Series No. NS-G-1.2, IAEA, Vienna (2002).
- [22] INTERNATIONAL ATOMIC ENERGY AGENCY, Design of the Reactor Core for Nuclear Power Plants, Safety Guide No. NS-G-1.12, IAEA, Vienna (2005).
- [23] INTERNATIONAL ATOMIC ENERGY AGENCY, Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants, Safety Standards Series No. NS-G-2.2, IAEA, Vienna (2000).
- [24] INTERNATIONAL ATOMIC ENERGY AGENCY, Recruitment, Qualification and Training of Personnel for Nuclear Power Plants, Safety Standards Series No. NS-G-2.8, IAEA, Vienna (2002).
- [25] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety of Nuclear Power Plants: Operation, IAEA Safety Standards Series No. NS-R-2, IAEA, Vienna (2000).
- [26] WORLD ASSOCIATION OF NUCLEAR OPERATORS (WANO), Performance Indicators 2004, London (2005), www.wano.org.uk.
- [27] INTERNATIONAL ATOMIC ENERGY AGENCY, Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants, Safety Standards Series No. NS-G-2.6, IAEA, Vienna (2002).
- [28] GESELLSCHAFT FUER REAKTORSICHERHEIT (GRS), German Risk Study: Nuclear power Plants, Phase B – A Summary, GRS-74, Munich (1990).
- [29] GESELLSCHAFT FUER REAKTORSICHERHEIT, Safety Analysis for Boiling Water Reactors – A Summary, GRS-98, Munich (1993).
- [30] INTERNATIONAL ATOMIC ENERGY AGENCY, Instrumentation and Control Systems Important to Safety in Nuclear Power Plants, Safety Standards Series No. NS-G-1.3, IAEA, Vienna (2002).
- [31] INTERNATIONAL ATOMIC ENERGY AGENCY, Determining the quality of probabilistic safety assessments (PSA) for applications in nuclear power plants, IAEA-TECDOC-1511, Vienna (2006).
- [32] OECD NUCLEAR ENERGY AGENCY, Critical Operation Actions – Human Reliability Modeling and Data Issues, NEA/CSNI/R(98) 1, OECD, Paris (1998).

- [33] GROUP PERMANENT REACTOR, Technical Guide Lines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, Group Permanent Réacteur, Paris (2001).
http://www.irsn.fr/en/index.php?module=presse&action=getCom&com_id=243&lgcode=EN
- [34] INTERNATIONAL ATOMIC ENERGY AGENCY, Safety Related Terms for Advanced Nuclear Plants, IAEA-TECDOC-626, Vienna (1991).
- [35] INTERNATIONAL ATOMIC ENERGY AGENCY, Current Status and Future Development of Modular High Temperature Gas Cooled Reactor Technology, IAEA-TECDOC-1198, Vienna (2001).
- [36] INTERNATIONAL ATOMIC ENERGY AGENCY, Innovative Small and Medium Sized Reactors: Design Features, Safety Approaches and R&D Trends, IAEA-TECDOC-1451, Vienna (2005).
- [37] SANTAMAURA, P., BANASEANU, G., BETTIG, R., HENDERSON, R., ILIESCU, P., MENON, U., OZDEMIR, A.: ACR Level 1 Probabilistic Safety Assessment (PSA) Results – Internal AT-Power Events. 26th Annual Conference of the Canadian Nuclear Society, Toronto, June 12-15 (2005).
- [38] SANTAMAURA, P., KAASALAINEN, S., WEBB, W.A., MCNEIL, S.: ACR Level 1 Internal Events Shutdown State Probabilistic Safety Assessment (PSA). 26th Annual Conference of the Canadian Nuclear Society, Toronto, June 12-15 (2005).
- [39] OECD/NUCLEAR ENERGY AGENCY, Level 2 PSA Methodology and Severe Accident Management, NEA/CSNI/R(97) 11, OECD/GD(97)198, Paris (1997).
- [40] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION (ICRP), Publication 63, Principles for intervention for Protection of the Public in a Radiological Emergency, Annals of the ICRP Vol. 22/4, Pergamon Press, Oxford (1993).
- [41] KREWITT, W., Quantifizierung und Vergleich der Gesundheitsrisiken verschiedener Stromerzeugungssysteme, Thesis (Nov. 1996), University of Stuttgart, Germany.
- [42] INTERNATIONAL ATOMIC ENERGY AGENCY, Assessment of Defence in Depth for Nuclear Power Plants, IAEA Safety Reports Series No. 46, IAEA, Vienna (2005).
- [43] DINSMORE COMEY, D., The Fire at the Brown's Ferry Nuclear Power Station. http://www.ccnr.org/browns_ferry.html.
- [44] INTERNATIONAL ATOMIC ENERGY AGENCY, FAO, ILO, OECD/NEA, PAHO, WHO, International Basic Safety Standards for Protection against Ionizing Radiation and for Safety of Radiation Sources, IAEA Safety Series No. 115, Vienna (1996).
- [45] INTERNATIONAL COMMISSION ON RADIOLOGICAL PROTECTION (ICRP), 1990 Recommendations of the International Commission on Radiological Protection ICRP – Users' Edition, Annals of the ICRP, Vol. 21/1-3, Pergamon Press, Oxford (1992).
- [46] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, Maintaining Knowledge, Training and Infrastructure for Research and Development in Nuclear Safety, INSAG-16, INSAG Series No. 16, IAEA, Vienna (1999).
- [47] 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).
- [48] INTERNATIONAL ATOMIC ENERGY AGENCY, Format and Content of the Safety Analysis Report For Nuclear Power Plants, IAEA Safety Standards Series No. GS-G-4.1, IAEA, Vienna (2004).
- [49] INTERNATIONAL ATOMIC ENERGY AGENCY, Risk informed regulation of nuclear facilities: Overview of the current status, IAEA-TECDOC-1336, Vienna (2005).

- [50] 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, 8-10 Dec. 2004.
- [51] GUNDREMMINGEN, Gundremmingen Nuclear Power Plant Units B and C: Brochure from the Kraftwerk Union (called AREVA NP since 2006), Frankfurt (1985).
- [52] INTERNATIONAL NUCLEAR SAFETY ADVISORY GROUP, The Safety of Nuclear Power, IAEA Safety Series No. 75 - INSAG-5, IAEA, Vienna (1992).
- [53] INTERNATIONAL ATOMIC ENERGY AGENCY, The management system for facilities and activities, IAEA Safety Guide No. GS-R-3, Vienna (2006).
- [54] INTERNATIONAL ATOMIC ENERGY AGENCY, Application of the management system for facilities and activities, IAEA Safety Guide No. GS-G-3.1, Vienna (2006).
- [55] INTERNATIONAL ATOMIC ENERGY AGENCY, The Safety of Nuclear Installations, IAEA Safety Series No. 110, IAEA, Vienna (1993).
- [56] UK-EPR Fundamental Safety Overview; Volume 2 Chapter R – Probabilistic Safety Assessment; Framatome ANP; August (2008).
<http://www.epr-reactor.co.uk/scripts/ssmod/publigen/content/templates/show.asp?P=139&L=EN>
- [57] UK AP1000 Probabilistic Safety Assessment; Westinghouse report UKP-GW-GL-0200
<https://www.ukap1000application.com/AP1000Documentation.aspx>

ABBREVIATIONS

ACR	advanced CANDU reactor
AHWR	advanced heavy water reactor
AL	acceptance limit (INPRO)
ALARP	as low as reasonably practical, social and economic factors taken into account
AM	accident management
AOO	anticipated operational occurrence
ASME	American Society of Mechanical Engineers
ATWS	anticipated transient without failure
BP	basic principle (INPRO)
BWR	boiling water reactor
CANDU	Canada deuterium-uranium reactor
CCC	containment cooling condenser
CCF	common cause failure
CFD	computational fluid dynamics
CHF	critical heat flux
CMF	core melt frequency
COG	CANDU Owners' Group
CR	criterion (INPRO)
CRD	control rod drive
CSNI	Committee on the Safety of Nuclear Installations (NEA)
CVCS	chemical and volume control system
DBA	design basis accident
DID	defence in depth
DNB	departure of nucleate boiling
EC	emergency condenser
ESC	emergency support center
EPR	European pressurized water reactor
EUR	European utility requirements
FCF	fuel cycle facility
FOAK	first-of-a-kind
GC	IAEA General Conference
GIF	Generation IV International Forum
GPR	Groupe Permanent Réacteur
HEU	highly enriched uranium
HF	human factor
HFEP	human factor engineering program plan
HPCI	high pressure coolant injection
HTGR	high temperature gas reactor
HTR	high temperature reactor
HWR	heavy water reactor
IAEA	International Atomic Energy Agency
I&C	instrumentation and control
IEA	International Energy Agency (OECD)
ICRP	International Commission on Radiological Protection
IN	indicator (INPRO)
INES	International Nuclear Event System
INPRO	International Project on Innovative Nuclear Reactors and Fuel Cycles (IAEA)

INS	innovative nuclear energy system (INPRO)
INSAG	International Nuclear Safety Advisory Group (IAEA)
IPCC	Intergovernmental Panel on Climate Change
ISED	indicator for sustainable energy development (IAEA)
LEU	low enriched uranium
LOCA	loss of coolant accident
LPCI	low pressure coolant injection
LWR	light water reactor
MCFHR	minimum critical heat flux ratio
MCP	main coolant pump
MFA	material flow assessment
MS	Member State (IAEA)
MSR	molten salt reactor
NEA	Nuclear Energy Agency (OECD)
NGO	non-governmental organization
NPP	nuclear power plant
NOAK	N th of a kind
NRC	Nuclear Regulatory Commission (USA)
OECD	Organization for Economic Co-operation and Development
O&M	operation and maintenance
P&T	partitioning and transmutation
PHWR	pressurized heavy water reactor
PIRT	phenomena identification and ranking table
PPPT	passive pressure pulse transmitter
PRIS	Power Reactor Information System (IAEA)
PSA	probabilistic safety assessment
PWR	pressurized water reactor
QA	quality assurance
RCS	reactor coolant system
RD&D	research, development and demonstration
RHR	residual heat removal
RPS	reactor protection system
RPV	reactor pressure vessel
RSK	German Reactor Safety Commission
SCPR	supercritical-water cooled power reactor
SF	scram frequency
SRV	safety relief valve
SSC	structures, systems and components
UR	user requirement (INPRO)
VVER	water cooled water moderated power reactor
WANO	World Association of Nuclear Operators
WEC	World Energy Council
WG	weapon grade
WNA	World Nuclear Association
WWER	water cooled water moderated power reactor
YOLL	years of life lost

CONTRIBUTORS TO DRAFTING AND REVIEW

E. Hicken	FzJ, Germany
R. Cirimello	CEA, Argentina
F. Depisch	International Atomic Energy Agency
M.T. Dominguez	Empresarios Agrupados, Spain
M. El Shanawany	International Atomic Energy Agency
P. A. Formichenko	Kurchatov Institute, Russian Federation
B. Kuczera	International Atomic Energy Agency
F. Lignini	International Atomic Energy Agency
B. Raj	Indira Ghandi Centre for Atomic Research, India
C. Shepherd	Corporate Risk Associates, United Kingdom
R. K. Sinha	Bhabha Atomic Research Centre (BARC), India
V.G. Snell	Atomic Energy of Canada Limited (AECL), Canada