The European "Stress test" for Nuclear Power Plants

Expertise on behalf of the Parliamentary Group
of the Greens/EFA in the European Parliament

Bonn, October 2011

drafted by:

büro für atomSICHERHEIT

Renneberg Consult UG
Wolfgang Renneberg
www.atomsicherheit.de

in cooperation with:

intac GmbH
Oda Becker
Wolfgang Neumann
info@intac-hannover.de

with the support of the Greens/EFA Group in the European Parliament

The Greens | European Free Alliance
in the European Parliament

with the individual support of Greens/EFA MEPs

Franziska Brantner
Reinhard Bütikofer
Marije Cornelissen
Bas Eickhout
Jill Evans
Gerald Häfner
Rebecca Harms,
Satu Hassi
Yannick Jadot
Franziska Keller
Jean Lambert
Judith Sargentini
Werner Schulz

Contents

The European "Stress test" for Nuclear Power Plants

Introduction

The most simple, but no less important, lesson to come out of the Fukushima accident is that nuclear accidents really occur - even in developed industrialized countries. The lesson is not a new one; but it has been out of the public domain for some time: Each nuclear power plant operates with a probability of a core melt. The operation of nuclear power plants is always – without any exemption – connected with the residual risk of an uncontrolled nuclear accident.[1] Nuclear safety in the absolute sense does not exist. To say "a nuclear plant is safe" only means that the residual risk is accepted. What was a tsunami in Japan could be the combination of a fire incident, human error, leaking pipes and the clogging of the cooling circuit in a nuclear power plant in Europe or in the United States. It could be any kind of dangerous combinations, anywhere in the World. . An uncontrollable amount of unforeseeable combinations of errors – technical and human ones – cannot be assessed and excluded in advance. It therefore would be a great misunderstanding to believe that a "Stress test" could make nuclear power plants safe. However a sound safety assessment can help to reduce the nuclear risks.

The "Stress test" for Nuclear Power Plants of the European Union formally only affects the member countries of the European Union. The defined "Stress test" specifications and their outcome will eventually serve as an important reference for nuclear safety assessments around the world. A clear understanding of its structure and contents will be required to assess its value for improving nuclear safety worldwide.

The first part of this study considers and analyses the "Stress test" specifications of the European Nuclear Safety Regulators Group (ENSREG) for nuclear power plants in Europe. These "specifications" are the basis for the current investigations of the operators and the nuclear authorities of the member states. This study asks how far these investigations meet the re-

[1] As probabilistic safety objective for the operation of nuclear power plants an average core melt probability of 1: 100.000 per year and per plant is internationally discussed (IAEA, INSAG). For a supposed lifetime of a plant of 50 years this means a probability of 1: 2000 for a core melt to happen.

quirement of the EU Council for a comprehensive risk assessment of the European Nuclear Power Plants (NPP).

The second part of this study recommends measures to compensate the deficits discovered through the analysis in part one.

Summary

The limits of the test

The "Stress test" of the European nuclear power plants as defined by the European Nuclear Safety Regulators Group does not meet the requirements of the EU council nor the expectations of the European public for a comprehensive safety assessment. It doesn't provide a method for comparing the safety of the different plants, nor does it answer how safe European plants actually are.

The prevention of nuclear accidents – which is the centre of the nuclear safety provisions – is practically excluded by the test. The scope of the "test" focuses on which measures are left in the case an accident having happened:

- The scenarios which are under review are incomplete. Internal scenarios such as fire-scenarios, electrical surges, leakage of pipes, malfunction of valves, human failures and combinations of those events are not included in the scope of the test. External scenarios like airplane crashes are also excluded.
- The quality of the safety related systems and components of the plants like the material of pipes, of the reactor vessel, of valves and pumps, of control and instrumentation equipment is not under investigation.
- Degradation effects, in particular those caused by the aging of plants / material fatigue, are not considered
- The safety management of nuclear power plants, which is of utmost importance, is not included.
- The test relies on the safety cases of the licenses of the individual plants, which in many cases are out of date.

The test specifications do not define assessment criteria to check a plant's safety features. No criteria are defined to determine the so-called "robustness" of the plant. Furthermore the "Stress test" does not comply with normally applied qualified and comprehensible methods of technical studies and review practices. It is basically dependent on the confidence in the operators' reports. The experts involved in the "Stress test" are the same experts that have been responsible for nuclear safety in the past. The European Commission is not able to make up for this lack of independence because it has no technical expertise itself. Therefore the whole process is open to abuse, only demonstrating to the public how safe the plants are.

Within this limited scope and taking into account the deficiencies of the method and the process the proposed “Stress test” could nevertheless be useful in giving additional information, and potentially an initial estimation of the ability of individual plants to withstand a few important extreme external events (in particular earthquakes and floods).

The lesson of Fukushima - recommendations

The first practical experience of the Fukushima accident is that nuclear accidents can happen everywhere, and that the residual nuclear risk cannot be eliminated.

Beyond this experience the most important lesson of the Fukushima accident was that a plant and its management must be checked against well-known modern standards for nuclear safety, because in the instance of Fukushima, it was not, and consequences of such a review had not been drawn. Most of the issues concerning the on-going “Stress test“ in the European Union can be deduced from existing codifications of nuclear safety requirements including publications of the International Atomic Energy Agency. Most of the technical safety issues which now appear to as new lessons from the Fukushima accident, have already been discussed in national and international forums. However this knowledge had not been applied to Fukushima and it has not yet been applied to the European plants. The lesson is to apply the knowledge now. This leads to a two-step-approach:

The current limited approach of the “Stress test“ should be complemented by the assessment of aeroplane crashes (see *I.2.3*). Acceptance criteria that enable a classification of different grades of robustness should be defined (see *I.3.4 and II.2.1*). The requirements for the reports on the existing defence- in-depth-concepts of the plants should be structured to give more transparency and to get a sound basis for comparing the safety provisions of the plants (*see I.3.1 and II.2.2*). More precise and more stringent requirements for the underlying data and documents should be defined (see *I.3.5 and II.2.3*). Reports and the main underlying documents should be open to the public. The results of the peer review process (questions and answers) should be completely documented and published (see *I.3.7 and II.2.3*).

The “Stress test“ should be complemented by a second part that assesses the preventive measures of the nuclear power plants against nuclear accidents (*see II.3*).

The safety objectives of WENRA (Western European Regulators Association) for new reactors are an appropriate basis to structure the missing assessment of the preventive measures. Advanced technical safety requirements, which comprise of targets for meeting these objectives, are available (*see Annex I*). For every safety objective the most advanced requirements that are applicable for operating reactors should be applied. As result of such a process a questionnaire which comprises of the most important benchmarks for a safety check of the defence -in-depth system would be a sound basis for the needed second complementary part of the "Stress test". This methodology would provide a comprehensive risk assessment which could inform the European Union about the safety status of its nuclear power plants.

Part I:

The ENSREG Specifications

I.1 Decision of the European Council

On March 25th 2011 the European Council declared that

> *"the safety of all EU nuclear plants should be reviewed, on the basis of a comprehensive and transparent risk assessment ("Stress test"); the European Nuclear Safety Regulatory Group (ENSREG) and the Commission are invited to develop as soon as possible the scope and modalities of these tests in a coordinated framework in the light of the lessons learned from the accident in Japan ….."*[2]

Following on from this declaration EU Commissioner Öttinger said that this risk assessment should enable the EU to reassess the safety of the European nuclear power plants and it should serve as a basis even for decisions on the shutting down of unsafe plants.[3] Therefore it should enable the Euro-

[2] European Council, Conclusions 24/25 March 2011

[3] Oettinger, EU Commissioner for Energy, Interview "Tageschau", 15.03.2011 www.tagesschau.de/redirectid.jsp?id=atomkraft222

pean Union to compare the safety status of European nuclear power plants, at least to a certain degree.

I.2 The approach of ENSREG and of the Commission

Frame of the "Stress test"

The original goal was redefined by ENSREG with the help of the Western European Regulators Association (WENRA):

> *"For now we define a "Stress test" as a targeted reassessment of the safety margins of nuclear power plants in the light of the events which occurred at Fukushima: extreme natural events challenging the plant safety functions and leading to a severe accident."* [4]

By this agreed definition a "comprehensive risk assessment" as was foreseen by the EU-Council had gone out of focus. In principle only initiating events being reviewed are those that have been highlighted by the Fukushima accident: *earthquakes* and *flooding.*

Independent of any special kind of event the loss of the components that are needed to transfer the remaining heat after reactor-shutdown safely into the environment shall be additionally assumed.[5]

According to the Declaration of ENSREG the risk of airplane crashes on nuclear power plants will not be considered:

> *"Risks due to security threats are not part of the mandate of ENSREG and the prevention and response to incidents due to malevolent or terrorists acts (including aircraft crashes) involve different competent authorities, hence it is proposed that the Council establishes a specific working group composed of Member States and associating the European Commission, within their respective competences, to deal with that issues. The mandate and modalities of work of this group would be defined through Council Conclusions."* [6]

Technical Goal of the "Stress test"

Under the limited extreme scenarios of the ENSREG approach the "test" will consist in finding out what means will remain in the case of the narrowly defined Fukushima scenario for each plant, to prevent or to mitigate radioactive

[4] ENSREG (European Nuclear Safety Regulators Group), Declaration of ENSREG, Annex 1, EU "Stress test" specifications, Brussels 31.05. 2011, http://www.ensreg.eu/documents, page 1

[5] That means the loss of the ultimate heat sink, loss of electrical power, ENSREG, page 4

[6] ENSREG (European Nuclear Safety Regulators Group), Declaration of ENSREG, Brussels 31.05. 2011, http://www.ensreg.eu/documents

emissions. This is the main and superordinate target of the whole test. To achieve this goal some key questions need to be answered, in particular how to maintain the three fundamental safety functions, control of reactivity, fuel cooling and confinement of radioactivity. [7]

Therefore a key question of the test will be how the recriticality of the reactor can be avoided even if control systems are no longer available, such was the case with Fukushima. Recriticality means the restart of fission and the additional production of heat that could quickly destroy all barriers.

Another key question will be by what additional devices and procedures the core and the fuel storage pool can be cooled, and what could be done if cooling gets insufficient.

The third key question of the test asks with which devices or procedures the radioactivity can be kept within the containment, or by which means can emissions be mitigated if a plant were faced with the Fukushima scenario.[8]

One important new feature which is applied in this test is the evaluation of the so called “cliff edge effects”. A cliff edge effect is a qualitative degradation of the plant’s safety conditions.

> *“A cliff-edge effect could be, for instance, exceeding a point where significant flooding of plant area starts after water overtopping a protection dike or exhaustion of the capacity of the batteries in the event of a station blackout.”*[9]

Another important feature is the evaluation of how long it takes until critical situations arise when cooling is insufficient, for example, how long it takes before fuel rods start to melt.

Such effects and their consequences for the safety of the plant were – until now – not under consideration in the frame of evidence for licensing conditions or periodic safety reviews. In this respect the “Stress test“ goes beyond the borders of the ordinary safety analysis’ of the past and may give new insights of the plants response on these extreme situations. The test may therefore result in technical and organizational recommendations enabling plants to be better prepared in the case of such accidents.

Structure of the test

The report shall consist of four main parts:[10]

- an up-to-date plant description

---

7 See fn. 4, page 4
8 See id.
9 See id., page 2
10 See id., page 5

- a description of the provisions taken in the design basis of the plant and a description whether the plant copes with its design requirements
- an assessment of the so called "robustness" beyond the design basis in the case of earthquake and flooding and loss of electrical power. The assessment shall give information on how the plant specific defence in depth concept contributes to safety when it faces the scenarios of flooding, earthquake and the loss of electrical power.
- Potential improvements.

The review process of the reports of the 143 European plants shall be finalized within about four months, beginning in January 2012 and ending at the end of April 2012. To assure an equal level of assessment some experts shall be nominated members in each of the peer review teams.[11]

I.3 Limits of the ENSREG - Specifications

The European Council has asked for a comprehensive risk assessment that would allow for a judgment about the safety status of the plants. The assessment of safety margins is something else. Safety margins describe those safety provisions, or better still "safety related attributes", of the plant, that enable the operator to cool down the reactor and to prevent radioactive emissions, even when the existing safety systems have failed and the licensed boundary conditions of the plant are exceeded. The focus of the assessment is on accident management measures that are needed when an accident has happened. For example, if in an aeroplane the engine and electricity supply fails, it is the means to get out of the plane and to come safely to the ground when the engines have stopped working. To take another metaphor, it is whether a ship has a sufficient number of robust life-boats and vests, in case of sinking.

I.3.1 Defence-in-Depth-Concept not under Review

Most of the safety features of the plant that are needed to prevent an accident to occur are not under review. These safety features are those that belong to the so-called design basis of the plant that follows a defence in depth concept.

[11] Fn. 4, page 3

Defence-in-depth means that safety should be guaranteed by independent levels of provisions which shall preclude any accident that may damage human health.[12] The first level of defence shall provide a steady and safe operation within the defined operational data specifications. This is achieved by requirements for reliable function of the instruments, of the components like valves and tubes and electric and electronic devices. It affords a good quality of materials and a lot of defined periodical inspections. The second level of defence serves for those cases when the operational specification data is exceeded. In those cases systems are needed to lead the reactor back into the allowed range of operational limits, such as the limits for pressure, temperature, reactivity. If this second independent level of defence fails because there is, for example, a leak or a valve out of function and the reactor could get out of control, there is the most important third level of defence. This third level of defence consists of independent safety systems that must be able to shut down the reactor to cool the fuel rods and to prevent the reactor from releasing radioactivity out of the limits that are allowed for those cases. How safely a reactor works is mainly dependent on the quality of the installed defence in depth system in total. This is also the view of ENSREG:

> *"It is recognized that all measures taken to protect reactor core or spent fuel integrity or to protect the reactor containment integrity constitute an essential part of the defence-in- depth,* ***as it is always better to prevent accidents from happening than to deal with the consequences of an occurred accident."*** [13]

The safety systems of the defence in depth design are only partly reviewed by the "Stress test". Defence-in-depth is reassessed in a limited approach on "*assumptions of their performance*"[14] for it is assumed that adequate performance of those systems has been assessed in connection with plant licensing.

ENSREG takes for granted that the structures, systems and components to prevent accidents are in place and without deficiencies:

> *"By their nature, the „Stress test" will tend to focus on measures that could be taken* ***after a postulated loss of the safety systems*** *that are installed to provide protection against accidents considered in the design. Adequate performance of those systems has been assessed in connection with plant licensing."*[15]

[12] WENRA (Western European Regulators Association), WENRA Reactor Safety Reference Levels Appendix C, January 2008, http://www.wenra.org/dynamaster/file_archive/080121/1c826cfa42946d3a01f5ee027825eed6/ List of_reference_levels_January_2008.pdf

[13] See fn. 4, page 2

[14] See id.

[15] See id.

By this assumption the “Stress test” excludes the by far most important basis of the safety of nuclear power plants from the safety assessment. The comprehensive basic set of requirements and scenarios the plants has to face and master in order to prevent accidents from happening, and which are central part of any codification of nuclear safety requirements, are not included in the “test”:[16]

- The quality of the material of pipes, of safety relevant components as the reactor vessel, of control and instrumentation equipment is not investigated. The quality varies widely and it makes the difference in the safety of a plant
- Degradation effects caused in particular by the aging of plants / material fatigue are not considered
- The safety management of the plants, which is crucial for safety, is out of the scope. Even not foreseen is a report on whether a safety management corresponding to the state of the art is established and functioning
- Furthermore ENSREG relies on the safety case of the license.[17] This safety case of the plants is in most cases more than two or three, sometimes four, decades old. In the meanwhile a lot of parameters of the plants have been changed, former assumptions have been revised, former calculations methods may be out of date, knowledge about materials, about nuclear systems has developed, and a lot of experience with formerly unforeseen scenarios has been made during operation.[18]

The safety designs of plants are aged and show deficiencies. Especially the independence of the levels of the defence-in-depth-concept as one of the crucial questions of safety is not realised in all plants. Nevertheless all those plants are in a licensed state.[19]

Therefore it is imperative that a risk assessment of a nuclear power plant must include the assessment of the complete design base, an assessment

[16] For example see: Module 4 "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System", Principles of basic safety in connection with design and manufacturing, particularly paragraphs about Material selection No. 2.3.2 (Reactor coolant pressure boundary), No. 3.3.2, (Pressure-retaining walls of components of external systems) No. 5.3 (Small-diameter pipes) and No. 7.4 (Containment system), BMU 2009

[17] See fn. 4

[18] Regular periodic safety assessments do not improve the situation, at least not in every member state. The former safety case that was made for the license is explicitly not under review e.g. within the frame of mandatory periodic safety assessment in Germany but is still the basis of operation. In September 2010 the German nuclear authorities agreed to renew the safety case in a long-term process without a definite time schedule.

[19] see in detail: W. Renneberg, Risks of old nuclear power plants, study on behalf of the Parliamentary Group of the Greens in the German Parliament, July 2010 (Text in German); http://www.atomsicherheit.de/studien-und-statements/risiken-alter-atomkraftanlagen/

which relies on the state of the art and considers the operational experience of the plant under review and of all other comparable plants. Without such an assessment the question of whether a plant is safe or not will remain in the dark.

The importance of defence-in-depth is also addressed in the June 2011 "Report of the Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations". As one the main lessons learned it states: "*Establish safety culture, by going back to the basics that pursuing defence-in-depth is essential for ensuring nuclear safety, constantly learning professional knowledge on safety, and maintaining an attitude for trying to identify weaknesses as well as rooms for improvement for safety.*"[20]

I.3.2 Incomplete Scenarios

For a comprehensive risk assessment, as originally foreseen by the European Council, a broader approach would have been necessary, an approach that starts from the underlying root cause of the Fukushima accident that unexpected events can happen, namely events which have not been foreseen when determining the design and operational safety provisions for a nuclear power plant. Under the experience of the Fukushima accident specific configurations and failure modes typical for an aeroplane crash, for example, or internal fires, or human failures or any combination of these events that until now not have been under consideration within the defence in depth are not covered by the "Stress test". The "Stress test" therefore will not reveal existing "blind areas" within the design of the nuclear power plants that are crucial for their safety.

A necessary broad approach would require looking at all categories of initiating events and possible combinations of events, possible safety systems' failures in each case, and severe accident management issues against the background of the system of levels of defence-in-depth.

In particular aeroplane crashes are to be considered as a relevant *safety* issue in the light of the Fukushima accident. ENSREG regards this scenario under the terms of *security* and therefore claims it not relevant to be included it in the Stress test.[21] This is an evidently misleading argument. The fact that aeroplanes might crash on a nuclear power plant is completely independent of its cause, and might therefore happen without any terrorist background.

[20] Japanese Government, Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations, June 2011

[21] See fn.6

After all there is a clear grounds for ENSREG to address it as a safety issue that might lead to fatal scenarios.

I.3.3 No assessment criteria

The “Stress test“ specifications require descriptions of the plants’ properties and a justification of the chosen safety provisions. Requirements on the quality and the comprehensiveness of those descriptions are not defined. No assessment criteria or bench-marks are defined as a yard stick to assess whether reported provisions of the defence in depth reach a minimum quality.

In the case of earthquake, for example, the “Stress test“ specifications require a description of the up to date level of the assumed peak ground acceleration at the site and the justification of the chosen data.[22] The procedure to determine the peak ground acceleration contains many assumptions in a complex field of investigation. There is no common opinion or commonly accepted rule to determine the basic data for the assessment. There is no common opinion or commonly accepted code to gain the results. The validity of data depends on many factors and the method of assessment depends on many sensitive benchmarks where key predeterminations can be hidden which influence the result significantly. One of many questions for example is what confidence interval the earthquake determination should rely on: it makes a difference whether one can trust the estimated probability of an earthquake of certain strength fully or whether it must be reckoned, that within, for example, a range of 50% the earthquake may be much stronger. The same complexity of finding out the *strength and the probability* of an earthquake is typical for most of the other assessments as for example the adequateness of the “*provisions to protect* the plant” against earthquake[23] or flooding. So far as the “Specifications” rely on the licensed design[24] and its safety case, it relies in many cases on out-dated criteria and methods that may have worked 30 years ago and that differ from plant to plant and from older to younger plant generations.

This insufficiency is characteristic for the whole set of the “Specifications”. Without clear and precise rules for assessment it is possible to generate arbitrary results. This is a major reason why the results of the country reports on the assessment of the 143 European plants will not be comparable.

---

[22] Fn. 4, page 7
[23] To know the loads that must be carried by the structures of the reactor building and its components at each relevant point and to know the load limits that can be carried it needs complex computer based methods of calculation and validated input data. It must take into account the different operation conditions and the interdependency of possible reactions.
[24] Fn. 4, page 7

I.3.4 No acceptance level for "robustness"

The European "Stress test" shall demonstrate how robust the European nuclear power plants are.[25] In the current discussion after the Fukushima accident the term "robustness" is used as the key expression for that what should be required. If you are robust you will never get ill even in bad weather and insufficient clothes. Robustness is meant as something that guarantees a certain kind of additional safety. But there is no definition in the international framework of safety rules or in the "Stress test" specifications, as to what additional level of safety should be achieved, what level of safety would justify saying that a plant is robust or should be backfitted considering the new requirements of the Fukushima accident or should be shut down. Therefore room will be given for incomprehensible and arbitrary assessments of the results of the "Stress test". A transparent method must provide criteria defining what level of safety for a required basic level has to be achieved and what perhaps might be a level that justifies saying "it's a robust plant" with additional safety features.

The German Reactor Safety Commission has defined four levels of robustness, the basic level and three higher levels.[26]

The basic level is chosen as a level that must be fulfilled by all operating plants, taking into account that all plants meet the licensing conditions and have realised all backfitting measures required by the authority. Each of the three levels of robustness defines a larger kind of safety-margin beginning with level 1 of robustness. Level 3 means that the plant is safe even under the defined extreme conditions.

With the example of an earthquake the levels are defined as follows:[27]

Basic level: the plant must be safe in the case of an earthquake that is to be expected with a probability of 10^{-5} per year.

First level of robustness: the plant is safe in the case of an earthquake with an intensity of plus one. Accident management measures may be taken into account.

Second level of robustness: the plant is safe in the case of an earthquake with an intensity of plus two. Accident management measures may be taken into account.

---

25 Id., page 6

26 German Reactor Safety Commission (RSK), Plant specific safety assessment of German NPP in the light of the Fukushima accident (German text, Anlagenspezifische Sicherheitsüberprüfung (RSK-SÜ) deutscher Kernkraftwerke unter Berücksichtigung der Ereignisse in Fukushima-I (Japan), Berlin, 14.05.2011, http://www.bmu.de/energiewende/doc/47398.php

27 See id., page 23

Third level of robustness: the plant is safe in the case of an earthquake with an intensity of plus two even without considering accident management measures.

I.3.5 Assessment methods and data

The "Stress test" does not comply with qualified and comprehensible methods of technical studies and review practices.

The scope of the assessment will require answering new questions. These new questions partly rely on existing documents and partly on new investigations, inspections, assessments and calculations. New documents will be generated. ENSREG requires a classification of the documents:

> *"Documents referenced by the licensee shall be characterized either as:*
>
> - *validated in the licensing process*
> - *not validated in the licensing process but gone through licensee's quality assurance program*
> - *none of the above."*[28]

The "specifications" set the limited timeframe of two and a half months for the operator's first report and one month for the nuclear authority to check it[29]. It is to be expected that a lot of safety relevant documents will be classified in the second or third category. This will significantly weaken the confidence in the used data and - as follows - in the report.

Considering the limited time schedule the "specifications" accept so called "engineering judgments" whenever there is no time for orderly founded assessments[30]. The judgment of an engineer depends on many factors, on his/her experience, on his/her "questioning attitude" and on other subjective factors, especially on his/her subjective perception of the acceptance of risks.[31] It is therefore not a basis for a comprehensible and safety-oriented method for the evaluation of the considered risks.

---

[28] Fn.4, page 5

[29] This is the time schedule for the first report that will be the basis for the report to the EU Council deliberations in December 2011. It is not to be expected that the results of the final report will differ significantly from the first report that is expected in April 2012. The first report will strongly predetermine the second one.

[30] Fn. 4, page 2

[31] Lorenzo Strigini, Engineering judgment and safety and its limits: What can we learn from research in psychology, City University, London 2002;

On the other hand it is completely out of scope for a nuclear authority to check the operator’s report within one month. Considering usual practice it would take at least two years to come to a founded judgment.[32]

I.3.6 Independence of the experts

Independence of the operators

The “Stress test“ specifications require a report of the operators. This report is the most important basis for the final national report that shall be authorized by the nuclear authority of the affected member state.[33]

It is the natural interest of the licensee to operate his/her plant as long as possible and under the best economical boundary conditions. The operator therefore has the natural interest to demonstrate that his/her plant is operating safely and does not need costly backfitting measures. The experts of the operator who are responsible for delivering his/her report in this respect are not independent.

Independence of the authorities

The goal of the “Stress test” is to prepare a paper that can be communicated by the European Union as the sound result from a common assessment of the safety of the European nuclear power plants. It will be authorized by ENSREG and the Commission together with their conclusions.

The problem is that the Commission does not have any independent technical competence among its staff, i.e. people able to assess the safety of nuclear power plants. Therefore it will be ENSREG that will draw the conclusions. ENSREG was created to give technical guidance in particular. Not including the members of those countries without nuclear power plants the ENSREG consists mostly of the leaders of the nuclear authorities of the concerned countries with nuclear power plants. Therefore the ENSREG is not a group that could assess nuclear safety by itself. For a European report on nuclear safety the whole expertise of the authorities and their Technical Support Organizations on the national level are needed.

In the past these experts have legitimated the operation of the power plants under their supervision by giving the license and by issuing other acts admitting the plant’s operation. Hand in hand they have informed the public that the plants were operating safely. With the “Stress test“” they have to ask themselves whether they have not done enough in the past. They have to

[32] The legally mandatory periodic safety assessment in Germany takes not less than two up to five years or more for one plant.
[33] Fn.4, page 3

review their own practice, their own convictions and statements about safety and about acceptable risks. The specifications are addressing this problem:

> *"In order to enhance credibility and accountability of the process the EU Council asked that the national reports should be subjected to a peer review process..*
>
> *[.....]*
>
> *Members of the team whose national facilities are under review will not be part of that specific review."*[34]

I.3.7 Effectiveness of the peer review process

In order to enhance credibility and accountability of the process, the EU Council stated that national reports should be subjected to a peer review process.[35] Peer reviews will start in January and shall be completed by the end of April 2012.

A sound peer review process needs a detailed preparation of its actors, the reviewers. Regarding the short time frame, the immense workload and the limited number of experienced experts able to review the assessments of about 135 plants, it is by no means possible to prepare and proceed a sound in-depth-peer-review-process that could really be able to question the assessments of the different plants. The complexity of data, of calculation methods, of assumptions about the safety parameters and their interdependence within the system of a nuclear power plant is outstanding and nearly unimaginable for the public. There are a lot of very sensitive parameters that significantly influence the result of a risk assessment. A peer review is bound to trust most of these parameters that widely determine the safety of the plant under the level the review is looking at.

It must also be taken into consideration that the peer reviews teams consist of the experts of the involved member countries. It is self-evident that to criticize well-known colleagues within an official process whose results shall be open to the public is always difficult.

Under the given boundary conditions the review process is an instrument by which only evident deficiencies of applied assessment criteria may be identified. By this it will improve the quality of the whole process only to a limited degree.

[34] Fn.4, page 3
[35] Fn. 4, page 3

I.4 Conclusion Part I

The proposed “Stress test“ will not give a comprehensive and transparent risk assessment of the European plants. It is no basis for a judgment about the safety of the European nuclear power plants, especially not a basis for a safety ranking and therefore no basis with which to answer the question as to what nuclear risk should be tolerated in Europe and whether there are nuclear power plants that should be shut down. It will give nearly no information about the reliability of the protections measures of the plants to prevent the supposed failures of the safety systems. It will give nearly no information about all those other scenarios and serious events that could lead to the same safety challenges as the so far supposed extreme events. In particular the consequences of aeroplane crashes on nuclear power plants will not be regarded.

Considering

- the limited scope of the “Stress test“”,
- the lack of clear assessment and acceptance criteria,
- the lack of harmonized assessment procedures and practices in the different member states
- and taking into account the interests of the involved experts of the utilities and nuclear authorities, including their technical support organizations

it should be expected that reports will be made mainly to demonstrate to the public how safely the plants are operating.

Nevertheless the proposed “Stress test” could give more information and to some extent a first estimation of the ability of the individual plants to withstand a few important extreme external events (in particular earthquakes and floods).

Within this limited scope, and taking into account the deficiencies of the method and of the process, the report could give some new information on the robustness of individual plants, and on potential measures going beyond its design basis, in particular on:

- The identification of the step change in the event sequence under which the safety systems will fail completely (cliff-edge effects) and
- time limits until the failure threshold is reached

The proposed “Stress test“ therefore could be a first step towards an harmonized risk assessment of the European nuclear power plants.

Part II

Requirements for a comprehensive risk assessment of the European Nuclear Power Plants

The question has to be answered what would be needed to come to a reliable and comprehensive risk assessment of the European NPP. To identify the conditions it is at first necessary to know about the main obstacles which up until now have been the reason for the current limited approach of the "Stress test" as is analysed above.

Options to rectify the deficits of the current approach of the "Stress test" as far as possible under the current limitations of the European political structures can be divided into those which could improve the current process, and those which can be regarded as a second step that should follow the current process.

II.1 Political, constitutional and administrative restraints

In the political debate in the wake of the Fukushima accident European leaders strongly demanded a complete risk assessment ("Stress test") of the European NPP. Those plants that would not meet the requirements would have to be closed.[36] This was nothing less than a political claim for a European authority to regulate nuclear power even though EU Commissioner Oettinger indicated that the Commission had no power to enforce the shutdown of nuclear power plants.[37]

This political claim does until now not coincide with the reality of the European structures in the field of nuclear safety.[38] Soon it became clear that the national regulators represented in the ENSREG neither wanted to follow that wide scope of a European risk assessment, nor accepted the claim of a European regulatory competence. They refused a comprehensive risk assessment; in particular refusing to investigate the consequences of aeroplane crashes on nuclear power plants.[39]

---

[36] See Fn.3
[37] See id.
[38] Berthelemy, Leveque, Harmonizing Nuclear safety Regulation in the EU: Which Priority?, Intereconomics 2011, 132
[39] Fn. 6, Declaration of ENSREG, 13.05.2011

Until now nuclear safety is regarded as an indispensable part of national responsibility. This national responsibility for nuclear safety has well founded reasons. Nuclear safety and the question 'how safe is safe enough?' are questions that are of the utmost importance for a society that has decided to use nuclear power. Against all earlier attempts of the Commission, the EU Council adopted a Directive on Nuclear Safety that practically does not contain safety rules for nuclear power plants.[40]

Only in the national legislative and administrative frame exists a chain of democratic responsibility that enables the Parliament as highest representative of the people to control the actions of a nuclear authority and to decide on whether or not nuclear power is used. The European Union until now has not developed equivalent or similar democratic structures. A European Constitution does not yet exist. The role of the European Parliament is rather restricted and has practically no means to control the actions of the Commission. The European Union therefore is politically and constitutionally not yet ready to take a leading role in nuclear safety.[41]

A further judicial restraint is the limited competence of the European Union that is given by the Euratom Treaty. In a principle decision the European Court only acknowledged the competence of the EU to regulate the general frame in the nuclear field. Not comprised is a supervisory practice of the European Commission as European regulator in the role to give a license or to regulate the operation of nuclear power plants.[42]

Moreover the European Union by its organizational structures is not yet ready to take direct responsibility for nuclear safety. As member of the Convention on Nuclear Safety the Commission is obliged to be independent from all bodies that promote Nuclear Energy:

> *"Each Contracting Party shall take the appropriate steps to ensure an effective separation between the functions of the regulatory body and those of any other body or organization concerned with the promotion or utilization of nuclear energy."*[43]

Corresponding to the organizational chart of the Commission the responsibilities for nuclear safety and promoting nuclear energy lie within the same Commissioner.[44] The Commission therefore is - under the current organizational structure - not independent in the case of the Nuclear Convention es-

[40] European Council, Council Directive 2009/71/Euratom, 25.06.2009, Official Journal of the European Union, L 172/18

[41] In detail: Renneberg, Regulating Nuclear Safety on the European Level in the view of the Federal Ministry for Environment (German Text, Die europäische Regulierung des Atomsektors aus Sicht des Bundesumweltministeriums), 12. Deutsches Atomrechtssysmposium, Baden Baden 2004, 89

[42] European Court of Justice, Judgment of the Court, C-29/99, I-11310, 10.12.2002

[43] Convention on Nuclear Safety, Art. 8 II, IAEA, INFCRC/449, 5 July 1994

[44] EU Commission for Energy, Directorate for Energy, Organizational Chart, http://ec.europa.eu/dgs/energy/doc/dg_energy_organigram_en.pdf

pecially as far as it takes regulatory competences. This is the result of an organizational change within the Commission in the 2002. Before then the Commissioner for Environment was responsible for nuclear safety.

Another practical reason precludes a direct responsibility of the Commission for Nuclear Safety. The Commission has no independent technical expertise to supervise the member states in questions of nuclear safety. It relies on the technical competence of the member states' authorities. Therefore a strict supervisory independence of a European nuclear "Stress test" from national authorities cannot be realised.

To improve this situation a fundamental change of the structures of the EU would be needed.[45]

On the other hand the European Union can support a European Harmonization Process as done by creating the European Nuclear Regulators Group supported by the WENRA-Group.

The ENSREG is free to define common assessment and acceptance criteria for nuclear safety investigations in consensus with its members and corresponding to their national legislative frames. The ENSREG could in the same way agree on transparent procedures that could partly compensate the lack of independence.

II.2 Recommendations

To compensate the shortcomings of the current process and to enable sound results of the current "Stress test" the following recommendations are given.

II.2.1 Recommendation No. 1: Definition of robustness and its levels:

In adoption of the structure of acceptance criteria of the German Reactor Safety Commission four levels of robustness should be defined.[46] The first level should define the basic scenario (basic safety) and three levels should define additional safety margins corresponding to the inclining Stress-scenarios. The highest level three defines a state where the plant meets the highest standards of robustness. In order to differentiate between the graded levels of robustness, graded requirements

[45] This is not the topic of the present study.
[46] See fn. 26; chapter I.3.4

on the redundancy and diversity or well-founded probabilistic elements, should be applied.[47]

II.2.2 Recommendation No. 2: Comprehensiveness of documentation

Under the given scope of the "Stress test", as defined by ENSREG, the description of the plants' defence-in-depth-concept in the country reports should cover all operational states of the reactor and include spent fuel pools and should document the following issues: [48]

Defence in depth level 1 (normal operation):

- *Description of the existing ageing management program*
- *Description of the existing operating experience feedback program*
- *Quality of the pressure retaining boundary (e.g. material, tolerated flaw indications, status of fatigue analyses)*
- *Status report including an evaluation on number, types and trends of plant specific incidents during the last ten years.*

Defence in depth level 2 (abnormal events):

- *List of postulated initiating events allocated to this Defence in Depth level*
- *Applied acceptance criteria allocated to these events.*
- *Applied requirements for analytical methods, model and boundary conditions for the analyses*
- *Applied requirements for the systems, structures and components (SSCs) needed to fulfil the acceptance criteria in case of these events.*
- *Degree of independence of the SSCs from SSCs of other levels of the Defence in Depth including the reactor auxiliary and support systems (e. g. electrical power supply, cooling systems).*

Defence in depth level 3 (postulated accidents)

- *List of postulated initiating events allocated to this Defence in Depth level*

---

[47] See chapter I.3.4
[48] See e.g. fn..69

- *Applied acceptance criteria allocated to these events*
- *Applied requirements for analytical methods, model and boundary conditions for the analyses (conservative vs. best-estimate approach).*
- *Applied requirements for the systems, structures and components (SSCs) needed to fulfil the acceptance criteria in case of these events.*
- *Degree of independence of the SSCs from SSCs of other levels of Defence in Depth (including the reactor auxiliary and support systems (e. g. electrical power supply, cooling systems)).*
- *Applied requirements for accident procedures (EOPs) needed to fulfil the acceptance criteria in case of these events.*

Defence in depth level 4 (very rare events, multiple failure events and severe fuel damage events)

- List of considered events/states
- Applied acceptance criteria allocated to these events/states
- Applied requirements for analytical methods, model and boundary conditions for the analyses.
- Applied requirements for the systems, structures and components (SSCs) needed to fulfil the acceptance criteria in case of these events/states.
- Degree of independence of the SSCs from SSCs of other levels of Defence in Depth.
- Applied requirements for accident management procedures (SAMGs)

II.2.3 Recommendation No. 3: Quality of documents

It must be guaranteed that documents which are the basis of the assessment refer to the current state of the plant, are checked and confirmed by the authority and are based on valid parameter and verification methods. As far as engineering judgments are used, it must be verified that they are more conservative than qualified exact scientific and technical methods.

II.2.4 Recommendation No. 4: Transparency

The absence of an independent in depth assessment can partly be compensated by procedural rules. The peer review process as proposed by ENSREG is one step to give more transparency to the process.

The peer review process should be strengthened by a clear structure of the reports (recommendation 2), the documentation of the applied assessment criteria, and by an open access not only of the operators' basic reports and of the national-reports but also of the underlying documents for the public, for the non-governmental organizations and their experts. The results of the peer review process (questions and answers) should also be fully documented and be published.

II.2.5 Recommendation No. 5: Prevention of nuclear accidents

The "Stress test" should - in a second phase - assess the ability of the nuclear power plants to prevent accidents. This means the assessment of the defence-in-depth safety provisions to prevent accidents for all foreseeable initiating events and to give an answer to the question whether these provisions meet the current state-of-the-art.

This key question for the safety of nuclear power in the European Union is a crucial one:

Nearly none of the 135 operating European nuclear power plants (NPPs) comply with strict requirements of an accident preventing defence-in-depth concept which corresponds to the up-to-date standards.

The plants differ substantially in age, design and condition. The differences concerning the realisation of the defence-in-depth correspond to substantial differences of their residual risks.

An assessment to reveal residual risks needs testable safety criteria. Binding European criteria for such a safety assessment is currently not available. A commonly agreed and applicable basis for complementing the current "Stress test" are the "*Safety Objectives for New Power Reactors*"[49], published by the Western European Nuclear Regulator's Association (WENRA) in

[49] WENRA: Safety Objectives for New Power Reactors – Study by WENRA Reactor Harmonization Working Group (RHWG), December 2009

2009. The safety objectives for new NPP's[50] were defined on the basis of a systematic analysis of the "Fundamental Safety Principles" developed by IAEA in 2006[51] and some other studies related to safety improvements for new reactors.[52]

The seven "Safety objectives for new reactors" are aimed at the design for new plants. By this they represent the current state-of-the-art safety provisions for nuclear power plants. Beside very few really new requirements, such as measures to cope with a core-melt, they contain safety goals for a strict application of the defence-in-depth concept that can directly be applied to operating plants. As far as new features are required they include those questions that have become relevant with the Fukushima accident and are at least partly addressed in the current "Stress test".

Applying those criteria to existing power plants is apparently not far from WENRA's view. According to WENRA, these safety objectives should also be "*used as a reference for identifying reasonably practicable safety improvements for 'deferred plants'*[53] *and existing plants in case of periodic safety reviews*" [54]. This statement was again strengthened in the WENRA "*Pilot study on Long term operation of nuclear power plants*" published in March 2011.[55]

The safety objectives are not applicable without a set of more precise assessment criteria (benchmarks). These have to be defined. To get the benchmarks for the test, what requirements should be met to achieve the safety objectives as best as possible and to optimise the safety provisions for operating plants, advanced criteria in international and national level are available. Without excluding other technical requirements, rules or guides, the German "Safety Criteria for Nuclear Power Plants"[56] could in a far extent provide testable criteria to assure the level of needed provisions. As a result of that test the deviations ("deltas") of the older plants from current state-of-the-art-requirements on prevention of accidents would be identified.

---

[50] Published in their final wording in WENRA: Statement on Safety Objectives for New Nuclear Power Plants, November 2010

[51] IAEA: Safety Standard Series No. SF-1, Fundamental Safety Principles, 2006

[52] For example:
-NEA/CNRA/R(94)2, A Review for regulatory requirements for advanced nuclear power plants, 1994
-EUR 20163 EN, ISO study project on development of a common safety approach in the EU for large evolutionary pressurized water reactors, October 2001
-Several utilities and individual countries documents of the last 20 years

[53] NPPs originally based on reactor design similar to currently operating plants, the construction of which halted at some point in the past, and now being completed with more modern technology.

[54] WENRA: Statement on Safety Objectives for New Nuclear Power Plants, November 2010

[55] WENRA: Pilot study on Long term operation of nuclear power plants" Study by WENRA Reactor Harmonization Working Group (RHWG), March 2011

[56] Federal Ministry for the Environment, Nature Conservation and Nuclear Safety: Safety Criteria for Nuclear Power Plants, Revision D, June 2009, Note: This is a translation of the German document entitled: "Sicherheitskriterien für Kernkraftwerke", BMU, April 2009.

Annex 1 outlines content and methodology of this missing second phase of the Stress test.

II.3 Conclusions Part II

One of the main lessons of the Fukushima accident is that the plant and its management had not been checked against well-known modern standards for nuclear safety or that the consequences of such a review had not been drawn. Most of the issues of the on-going "Stress test" in the European Union can be deduced from existing codifications of nuclear safety requirements including publications of the International Atomic Energy Agency. Most of the issues that now seem to appear as new lessons of the Fukushima accident have been discussed in national and international forums before. This knowledge however has not been applied. The lesson is to apply the knowledge now.

The on-going "Stress test" is strongly limited in terms of its scope and its methodology, and is by far insufficient at revealing the deficiencies that are relevant for the safe operation of the European plants. It excludes most important areas from investigation that could lead to equivalent scenarios as Fukushima.

This leads to a two-step-approach:

1. The current limited approach of the "Stress test" should be improved by defining acceptance criteria that enables a classification of different grades of robustness. The requirements for the reports on the existing defence-in-depth-concepts of the plants should be structured to give more transparency and to get a sound basis for comparing the safety provisions of the plants. More precise and more stringent requirements for the underlying data and documents should be defined. The reports and the main underlying documents should be open to the public. The results of the peer review process (questions and answers) should be completely documented and published.[57]

2. A comprehensive assessment is needed which includes the prevention of nuclear accidents and corresponds to the state-of-the-art technology in nuclear safety. The safety objectives of WENRA should be a basis for the missing comprehensive risk assessment. Advanced technical safety requirements that include benchmarks representing the state-of-the-art technology are available. For every safety objective the most advanced requirements that are applicable for operating reactors should be applied. As result of such a process a check-list that comprises of the most important benchmarks for a

---

[57] See chapter II.2.4

safety check of the defence-in-depth system would be a sound basis for the needed second complementary part of the "Stress test". This methodology would provide a comprehensive risk assessment, which could inform the European Union about the safety status of its nuclear power plants.

ANNEX I: Criteria for a comprehensive safety assessment

1. Safety objective O1: Normal operation, abnormal events and prevention of accidents

The safety objective "O1" of the WENRA safety objectives for new reactors[58] refers to the first and second level of defence:

> *"WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objectives of:*
>
> - *reducing the frequencies of abnormal events by enhancing plant capability to stay within normal operation.*
> - *reducing the potential for escalation to accident situations by enhancing plant capability to control abnormal events."*

The safety goals of "O1" aim at conceptual measures for new nuclear power plants but they may also be applied to operating plants.

Quality of material

*To reach, for example, the objective "O1" to reduce the frequency of abnor-*mal events, the question, what kind of quality the used material has, is most relevant for safety. The question of how reliable the plant prevents leaks or malfunction of valves or pumps depends strongly on the quality of the material.[59]

The requirements to assure a good material quality comprises of a lot of requirements which include the chemical and physical properties, the kind of manufacturing, the kind of welding, the process of quality assurance from manufacturing until installing the component, the kind and frequency of in-service inspections, and the kind of monitoring of the aging process of the materials.

For testing the quality of the respective plant specific provisions the "Safety Criteria for Nuclear Power Plants" provide benchmarks that can be applied.

---

58 WENRA: Statement on Safety Objectives for New Nuclear Power Plants, November 2010

59 The check of this part of safety objective "O1" is not part of the current „Stress test".

According to those benchmarks specific properties of the material[60] must be given and a quality assurance system has to be installed.

To manage the aging problems it has to be checked whether a comprehensive ageing management system is implemented.[61] The efficiency of such a system must be demonstrated by the licensee.

For an efficient in-service inspection according to "Safety Criteria for Nuclear Power Plants" [62] evidence must be given that all safety relevant equipment is so conditioned and arranged that in-service inspections for the identification of beginning material irregularities can be executed wherever they are needed. If this is not possible, it has to be demonstrated that precautionary measures against irregularities are implemented that guarantee the same level of safety.[63]

Man-machine interface / Design of the control room

The safety objective to reduce the potential for escalation to accident situations by an efficient control of abnormal events means that all should be done to avoid accidental situations by a preventive safety strategy. So whenever the pressure within the reactor vessel rises out of the limit for normal operation or the temperature exceeds normally allowed degrees there have to be intelligent and effective measures to analyse the problem and to lead the plant back into the limits of normal operation. Implementing the best

[60] Module 4 "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System", Principles of basic safety in connection with design and manufacturing, particularly paragraphs about Material selection No. 2.3.2 (Reactor coolant pressure boundary), No. 3.3.2, (Pressure-retaining walls of components of external systems) No. 5.3 (Small-diameter pipes) and No. 7.4 (Containment system). Example: 2.3.2 (2): In combination with the selected construction and the processing techniques applied, the materials used have sufficient resistance against corrosion and other ageing effects under the operating conditions. The water qualities required for corrosion resistance during specified normal operation (levels of defence 1 and 2) are specified. The water quality is monitored and deviations from the specified parameters are detected at an early stage so that disadvantageous impacts on the components are prevented.

[61] Module 4 "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System" Operation, Principles No. 2.5.1 (1+8) (Reactor coolant pressure boundary) No. 3.5.1 (1+9) Pressure-retaining walls of components of external systems) and Handling of indications on components and pipes No. 8 (4), Example: 2.5.1 (8): For systematic identification, observation or prevention of ageing impacts on the integrity of the components of the pressure-retaining walls, an ageing management system is implemented.

[62] Module 1 „Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria"; Technical criteria, No. 3.1 (12)
Module 4 "Safety Criteria for Nuclear Power Plants: Criteria for the Design of the Reactor Coolant Pressure Boundary, the Pressure Retaining Walls of the External Systems and the Containment System", Non-destructive in-service inspections: No. 2.5.3 (Reactor coolant pressure boundary), No. 3.5.4 (Pressure-retaining walls of components of external systems), No. 7.5.2 (Containment system),; Example: 2.5.3 (1) Non-destructive in-service inspections are performed regarding potential damage mechanisms in a representative manner with qualified procedures considering all types of welded joints and base material areas. Selection and suitability of the test procedures and techniques is justified under consideration of the technical progress.

[63] Module 1 „Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria", Technical criteria, No. 3.1 (12a)

available man-machine interface can avoid operating errors. Therefore, one way in which to achieve the defined safety goal is to implement a man-machine interface as regards information and diagnostic instruments[64] that corresponds to the current state-of-the-art technology. For this to be achieved, the requirements on the ergonomic design of the control room play a key role.[65]

The test of these fundamental safety requirements resulting from safety objective O1 is not part of the current "Stress test".

2. Safety Objective O2: Accidents without core melt

"WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objectives of:

- *ensuring that accidents without core melt induce no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation).*
- *reducing, as far as reasonably achievable,*
  the core damage frequency taking into account all types of credible hazards and failures and credible combinations of events;
  - the releases of radioactive material from all sources.
- *providing due consideration to siting and design to reduce the impact of external hazards and malevolent acts.'*[66]

This safety objective is – considering the first two paragraphs – fully applicable to operating nuclear power plants. In the defence-in-depth concept these tools belong to defence-level-3 [67] which has to provide protection against the design basis accidents.

Design basis accidents

[64] WENRA: Safety Objectives for New Power Reactors – Study by WENRA Reactor Harmonization Working Group (RHWG), December 2009, Appendix 3

[65] Module 1 „Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria", Criteria for control rooms, No. 3.8 (4): The ergonomic design of the control room and the emergency control room supports the safety-oriented behaviour of the personnel.

[66] WENRA: Statement on Safety Objectives for New Nuclear Power Plants, November 2010; Note: The complete text of the safety objectives (including footnotes) is given in the Annex .

[67] See chapter I.3.1

To meet this objective, WENRA calls for consideration of a more systematic analysis of critical events and situations in all operating states (operation and shutdown) and not only for the reactor, but also for the spent fuel pool and other facilities of the plant.[68] The fulfilment of these requirements would reduce the frequency of accidents that could lead to uncontrolled scenarios and core melt situations (Fukushima), lower the release rates for radioactive material, and give more provision against core melt accidents.

Corresponding to that goal it must be checked whether all events (internal and external) and particularly credible combinations of events are considered for the plant design according to current state-of-the-art technology. The "Safety Criteria for Nuclear Power Plants", for example, contain a comprehensive list of events the plant has to cope with.[69] Some very important requirements in this context is the assumption of "*long lasting external events*" and of the combination of several natural or other external impacts, as well as the combination of external impacts with internal events.[70]

The implementation of the different levels of the defence-in-depth concept was initially limited to postulated incidents and accidents occurring under full power conditions. Probabilistic Safety Assessments (PSA) show that the contribution of core damage frequency for the shutdown state is in the same order of magnitude as that for operation.[71] Therefore, a systematic consideration of the shutdown state should be a key topic for safety in a second phase of the "Stress test".[72]

For existing reactors the control of accidents is mainly focused on the reactor core. However, the scope of the defence-in-depth has to cover all risks induced by the nuclear fuel, even when the fuel is stored in the spent fuel pool. The accident in Fukushima highlights this deficit of older reactor types. According to the "Safety Criteria for Nuclear Power Plants" the equitable consideration of the spent fuel pool in the safety and accident management has been required a considerable time before the Fukushima accident.[73]

---

[68] WENRA: Safety Objectives for New Power Reactors – Study by WENRA Reactor Harmonization Working Group (RHWG), December 2009, Appendix 3

[69] Module 3 „Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors", Event lists, No. 5

[70] Module 1 „Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria" Postulated operating conditions and events, No. 4.1 (5)

[71] IAEA: "Defence in depth in Nuclear Safety, INSAG 10, A report by the International Nuclear Safety Advisory Group, Vienna, 1996

[72] Module 3 „Safety Criteria for Nuclear Power Plants: Events to be Considered for Pressurised and Boiling Water Reactors", Definitions and classification of the operating phases for PWRs and BWRs, No. 4

[73] Module 1 „Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria", Concept of fundamental safety functions (safety goals), No. 2.3 (2);
Module 7 "Safety Criteria for Nuclear Power Plants: Criteria for Accident Management" Plant conditions, event sequences and phenomena considered in accident management planning, No. 2 (6), Preventive accident management measures, No. 4.1 (4+5)

Human failures and 30 minutes rule

Another area for improvement highlighted by WENRA is the reduction of human-induced failures particularly through more automatic or passive safety systems and longer "grace period" for operators.[74] Human errors bear a potential for jeopardizing defence-in-depth. They have a considerable potential to trigger common cause failures (meaning they affect all redundancies of a specific safety system) as has been seen in many safety significant events, including the Chernobyl accident in 1986.[75] According to the "Safety Criteria for Nuclear Power Plants" no necessity shall be given for manual activation of safety systems during the first 30 minutes of an accident scenario.[76]

Multiple failure situations that exceed the former design basis

Accident conditions which are considered in the WENRA safety objectives for defence- level 3 now include multiple failure situations which were previously considered as "beyond design".[77] Examples of multiple failure situations are station blackout or the total loss of the spent fuel pool cooling system. These scenarios are topics of the current "Stress test".

Common cause failures - Redundancy and diversity

For events which are not controlled by the operational systems and/or limitation functions at defence-in-depth levels 1 and 2, safety systems are required to bring and maintain the plant in a safe state with respect to subcriticality, core cooling and confinement of radioactive materials[78] (defence-in-depth level 3). The reliability of the safety systems has to be achieved through an

---

[74] WENRA: Safety Objectives for New Power Reactors – Study by WENRA Reactor Harmonization Working Group (RHWG), December 2009, Appendix 3

[75] IAEA: Defence in depth in Nuclear Safety, INSAG 10, A report by the International Nuclear Safety Advisory Group, Vienna, 1996

[76] Module 1 "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria", Technical criteria, No 3.1 (3);
Module 5 "Safety Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation", Design, No. 3.2 (6); Module 12 "Safety Criteria for Nuclear Power Plants: Criteria for Electric Power Supply", Design, No. 2 (15): The startup and connection of the emergency power generators runs automatically on demand, so that no manual actions are required within 30 min. Manual startup and connection of the emergency power generators to the bus bars is possible at any time.

[77] WENRA: Safety Objectives for New Power Reactors – Study by WENRA Reactor Harmonization Working Group (RHWG), December 2009, Appendix 2; see Fn. 68, 69, 71

[78] ASN - Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors - adopted during the GPR/German experts plenary meetings held on October 19th and 26th, 2000, p. 7; Module 1 "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria", Concept of the fundamental safety functions (protection goals), No 2.3 (1)

adequate combination of redundancy and diversity [79]. This means the same safety functions are available several times (redundancy) and respectively the safety function is ensured by provisions with different physical or chemical mechanisms (diversity). Particular attention has to be paid to minimising the possibilities of common cause failures[80]. Also these events require physical and spatial separation as far as possible[81]. For example, the safety assessment of fire effects has to clearly identify common mode failure possibilities (including internal flooding risks linked to the use of fire fighting systems) which could result from incomplete separation of equipment that should be redundant.[82] *Special emphasis has to be placed on the redundancy and diversity of electrical power supplies*[83]

---

[79] ASN - Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors - adopted during the GPR/German experts plenary meetings held on October 19th and 26th, 2000, p. 7; IAEA: Defence in depth in Nuclear Safety, INSAG 10, A report by the International Nuclear Safety Advisory Group, Vienna, 1996; These requirements are since long commonly accepted as fundamental principles of reactor designs and can be found in any codification of reactor safety requirements

[80] ASN - Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors, GPR/German experts plenary meetings held on October 19th and 26th, 2000, p. 7; Module 10 "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components". Prevention of multiple failures, No. 1.3 (1-2) Example: No 1.3 (2) Safety installations for which potentials for common-cause failures were identified are designed according to the principle of diversity as far as feasible and technically reasonable..

[81] Module 1 “Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria”, Technical criteria, No 3.1 (3), No. 3.7 (3);

Module 5: "Criteria for Nuclear Power Plants: Criteria for Instrumentation and Control and Accident Instrumentation" No. 6 Redundancy and independence, Example No. 6 (3) To prevent failure-initiating events affecting multiple redundancies within the instrumentation and control installations and within the plant, redundancies are on principle accommodated physically separated from each other.

Module 10 "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components". Prevention of multiple failure No. 1.3 (1-7), Example: No. 1.3 (7) Deficiencies and damages in safety-relevant installations are analysed with regard to their cause. Here, it is clarified, in particular, whether the damage mechanism identified is of systematic nature. If there is suspicion of a systematic failure, it is clarified immediately and corrective measures are taken, if necessary. The necessary safety-related measures when determining redundancy-wide failures are included in the plant operating procedures.

[82] ASN - Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors - adopted during the GPR/German experts plenary meetings held on October 19th and 26th, 2000, p. 57

Module 10 "Safety Criteria for Nuclear Power Plants: Criteria for the Design and Safe Operation of Plant Structures, Systems and Components". Plant internal fire No. 2.2.1 (10-12); Example No. 2.2.1 (10): The layout design of the redundancies of the safety system is generally such in a manner that in case of fire a loss of more than one redundant due to fire-induced heat, fumes or fire extinguishing agents does not have to be postulated

[83] ASN - Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors - adopted during the GPR/German experts plenary meetings held on October 19th and 26th, 2000, p. 11;

Module 12 "Safety Criteria for Nuclear Power Plants: Criteria for Electric Power Supply" Design, No, 2 (10-13); Example: No. 2 (13) The redundants of emergency power supply facilities are physically separated or protected from each other such that any failure-initiating events in the emergency power supply facility will not lead to a loss of several redundants of an emergency power supply facility.

Actuality of the safety case

The methods that were used for the safety case of old plants may be out of date because a renewal process was not performed until now. The confidence in the safety case may therefore be lost. In order to make sure that the plants are operated safely evidence must be given that the safety case is up to date, corresponding to the current state-of-the-art safety requirements, taking into account all changes or corrections of formerly applied data.[84]

3. Safety Objective O3: Accidents with core melt

> *"WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objectives of:*
>
> - *reducing potential radioactive releases to the environment from accidents with core melt, also in the long term, by following the qualitative criteria below:*
> - *accidents with core melt which would lead to early or large releases have to be practically eliminated*
> - *for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures."*[85]

This safety goal refers primarily to new plants. As far as it defines the safety goal to mitigate the consequences of accidents with core melt it is partly applied by the current "Stress test".

In a "Stress test" that aims at revealing the residual risk of nuclear power plants, the provisions in the plant to mitigate core melt scenarios should be

[84] Module 1"Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria", Criteria for documentation, operating rules and safety demonstration No. 5 (7-9), Example No, 5 (9): For the analysis of events and conditions, a) validated calculation methods are used for the respective scope of application, b) any uncertainties associated with the calculation are quantified or considered by suitable methods.
Module 6 "Safety Criteria for Nuclear Power Plants: Criteria for Safety Demonstration and Documentation", Validation of analysis methods, No. 3.1

[85] WENRA: Safety Objectives for New Power Reactors, November 2010. Note: The complete text of the safety objectives (including footnotes) is given in the Annex.

documented. Then the accident scenarios which lead to an early and/or a large release should have to be identified in order to be able to estimate the potential radiological consequences for the affected public.

4. Safety objective O4: Independence of all levels of defence-in-depth

> "WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objectives of:

enhancing the effectiveness of the independence between all levels of defence-in-depth, in particular through diversity provisions (in addition to the strengthening of each of these levels separately as addressed in the previous three objectives), to provide as far as reasonably achievable an overall reinforcement of defence-in-depth."[86]

It is the general objective of defence-in-depth to ensure that a single failure, at one level and even a combination of failures at more than one level of defence, should not propagate and jeopardize defence-in-depth at subsequent levels. "The independence of different levels of defence is a key element in meeting this objective."[87] This safety objective is fully applicable for operating plants. It is in principle a traditional part of the safety concepts of all operating nuclear power plants. The open question only lies in the degree of how consistently this objective is realised practically. Modern safety standards ("for example the "Safety Criteria for Nuclear Power Plant") for operating plants require a consistent separation of all safety levels of the defence-in-depth.[88]

To evaluate the compliance of a plant with this safety objective all safety functions must be proved whether they have duties at two or more levels of defence-in-depth. Components of safety systems of level 3 should not fulfil an operational task. All components of safety features of level 4 which are used at another level of defence-in-depth have to be identified. The result of such a check against current standards would reveal severe differences among the European plants and a big potential for safety improvement.

---

[86] WENRA: Safety Objectives for New Power Reactors, November 2010. Note: The complete text of the safety objectives (including footnotes) is given in the Annex

[87] IAEA: Defence in depth in Nuclear Safety, INSAG 10, A report by the International Nuclear Safety Advisory Group, Vienna, 1996

[88] Module 1 "Safety Criteria for Nuclear Power Plants: Fundamental Safety Criteria", Technical safety concept, defence-in-depth concept No. 2.1 (5 - 8), Technical criteria, No. 3.1 (10) Examples: No. 2.1 (5) On levels of defence 2 and 3, measures as well as installations are provided that are arranged in such a way that upon the failure of measures and installations on levels of defence 1 and 2, the measures and installations on the subsequent level re-establish the required safety-related condition independent of measures and installations of other levels of defence: No. 2.1 (6): It is ensured that a single technical failure or erroneous human action on one of the levels of defence 1 to 3 will not jeopardise the effectiveness of the measures and installations on the next level..

5. Other Safety objectives

The following WENRA safety objectives comprise safety and security interfaces (O5), radiation protection (O6) and safety management (O7).[89] Especially the safety management of nuclear power plants has a significant meaning for operational safety. It is a key element to reduce human failures and to find out failures that have the potential to create serious events or accidents in time. The check of safety objective O7 is not part of the current "Stress test".

89 WENRA: Safety Objectives for New Power Reactors, November 2010. Note: The complete text of the safety objectives (including footnotes) is given in the Annex

ANNEX II

WENRA Safety Objectives for New Nuclear Power Plants

Compared to currently operating nuclear power plants, WENRA expects new nuclear power plants to be designed, sited, constructed, commissioned and operated with the objectives of:

O1. Normal operation, abnormal events and prevention of accidents

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

O2. Accidents without core melt

- ensuring that accidents without core melt induce[90] no off-site radiological impact or only minor radiological impact (in particular, no necessity of iodine prophylaxis, sheltering nor evacuation[91]).
- reducing, as far as reasonably achievable,
  - the core damage frequency taking into account all types of credible hazards, failures, and credible combinations of events;
  - the releases of radioactive material from all sources.
  - providing due consideration to siting and design to reduce the impact of external hazards and malevolent acts.

O3. Accidents with core melt

[90] In a deterministic and conservative approach with respect to the evaluation of radiological consequences

[91] However, restriction of food consumption could be needed in some scenarios.

- reducing potential radioactive releases to the environment from accidents with core melt[92], also in the long-term[93], by following the qualitative criteria below:
    - accidents with core melt which would lead to early[94] or large[95] releases have to be practically eliminated[96];
    - for accidents with core melt that have not been practically eliminated, design provisions have to be taken so that only limited protective measures in area and time are needed for the public (no permanent relocation, no need for emergency evacuation outside the immediate vicinity of the plant, limited sheltering, no long term restrictions in food consumption) and that sufficient time is available to implement these measures.

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

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

O5. Safety and security interfaces

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

O6. Radiation protection and waste management

- reducing as far as reasonably achievable by design provisions, for all operating states, decommissioning and dismantling activities:

---

[92] For new plants, the scope of the safety demonstration has to cover all risks induced by the nuclear fuel, even when stored in the fuel pool. Hence, core melt accidents (severe accidents) have to be considered when the core is in the reactor, but also when the whole core or a large part of the core is unloaded and stored in the fuel pool. It has to be shown that such accident scenarios are either practically eliminated or prevented and mitigated.

[93] Long term: considering the time over which the safety functions need to be maintained. It could be months or years, depending on the accident scenario.

[94] Early releases: situations that would require off-site emergency measures but with insufficient time to implement them.

[95] Large releases: situations that would require protective measures for the public that could not be limited in area or time.

[96] In this context, the possibility of certain conditions occurring is considered to have been practically eliminated if it is physically impossible for the conditions to occur or if the conditions can be considered with a high degree of confidence to be extremely unlikely to arise (from IAEA NSG1.10).

  - individual and collective doses for workers;
  - radioactive discharges to the environment;
  - quantity and activity of radioactive waste.

O7. Leadership and management for safety

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

IV. References

ASN (Autorité de Sûreté Nucleaire): Technical Guidelines for the Design and Construction of the Next Generation of Nuclear Power Plants with Pressurized Water Reactors - adopted during the GPR/German experts plenary meetings held on October 19th and 26th, 2000, www.asn.fr

BMU (Bundesumweltministerium): Safety Criteria for Nuclear Power Plants, Revision D, June 2009,
http://regelwerk.grs.de/downloads/modulerev.d020709em112.pdf
Note: This is a translation of the German document entitled: "Sicherheitskriterien für Kernkraftwerke", Revision D, April 2009,
http://regelwerk.grs.de/downloads/modulerevisiond020709.pdf

Büro für Atomsicherheit (Office for nuclear safety) Renneberg, Wolfgang: Risiken alter Kernkraftwerke (Risks of old nuclear power plants), study on behalf of the Parliamentary Group of the Greens in the German Parliament, July 2010 (note: Text in German)
http://www.atomsicherheit.de/studien-und-statements/risiken-alter-atomkraftanlagen

ENSREG (European Nuclear Safety Regulators Group): Declaration of ENSREG, Annex 1, EU “Stress test” specifications, Brussels 31.05. 2011,
http://www.ensreg.eu/documents

European Commission, Directorate for Energy: Organizational Chart,
http://ec.europa.eu/dgs/energy/doc/dg_energy_organigram_en.pdf

European Council: Conclusions 24/25 March 2011

European Council: Council Directive 2009/71/EURATOM, 25.06.2009, Official Journal of the European Union, L 172/18

European Court of Justice: Judgment of the Court, C-29/99, I-11310, 10.12.2002

IAEA (International Atomic Energy Agency): Defence in depth in Nuclear Safety, INSAG 10, A report by the International Nuclear Safety Advisory Group, Vienna, 1996,
http://www-pub.iaea.org/MTCD/publications/PDF/Pub1013e_web.pdf

IAEA (International Atomic Energy Agency): Safety Standard Series No. SF-1, Fundamental Safety Principles, 2006, http://www-pub.iaea.org/MTCD/publications/PDF/Pub1273_web.pdf

IAEA (International Agency for Atomic Energy): Convention on Nuclear Safety, IAEA, INFCRC/449, 5 July 1994

Japanese Government: Report of Japanese Government to the IAEA Ministerial Conference on Nuclear Safety - The Accident at TEPCO's Fukushima Nuclear Power Stations, June 2011**Öttinger, Günther:** EU-Commissioner for Energy, Interview “Tageschau”, 15.03.2011, www.tagesschau.de/redirectid.jsp?id=atomkraft222

Leveque, Berthelemy: “Harmonizing Nuclear safety Regulation in the EU: Which Priority?”, Intereconomics 2011, 132

OECD-NEA (Organisation for Economic Co-operation and Development-Nuclear Energy Agency): A Review for regulatory requirements for advanced nuclear power plants, CNRA /R (94)2, 1994

Renneberg, Wolfgang: „Die europäische Regulierung des Atomsektors aus Sicht des Bundesumweltministeriums“ (Regulating Nuclear Safety on the European Level in the view of the Federal Ministry for Environment), 12. Deutsches Atomrechtssysmposium, Baden-Baden 2004, 89

RSK (Reaktorsicherheitskommission): „Anlagenspezifische Sicherheitsüberprüfung (RSK-SÜ) deutscher Kernkraftwerke unter Berücksichtigung der Ereignisse in Fukushima-I (Japan)“ (Plant specific safety assessment of German NPP in the light of the Fukushima accident, note: text in German language), Berlin, 14.05.2011,

Strigini, Lorenzo: Engineering judgment and safety and its limits: what can we learn from research in psychology, City University, London 2002

VwVfG (Verwaltungsverfahrensgesetz, German law for administrative procedures): BGBl. I S. 2827

WENRA (Western European Nuclear Regulators Association): Reactor Safety Reference Levels, January 2008, www.wenra.org

WENRA (Western European Nuclear Regulators Association): Safety Objectives for New Power Reactors, Study by WENRA Reactor Harmonization Working Group (RHWG), December 2009, www.wenra.org

WENRA (Western European Nuclear Regulators Association): Statement on Safety Objectives for New Nuclear Power Plants, November 2010, www.wenra.org

WENRA (Western European Nuclear Regulators Association): Pilot study on Long term operation of nuclear power plants Study by WENRA Reactor Harmonization Working Group (RHWG), March 2011, www.wenra.org