Nuclear Regulation

Improving Versus Maintaining Nuclear Safety

NUCLEAR ENERGY AGENCY
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in member countries, while maintaining financial stability, and thus to contribute
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14 December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

NUCLEAR ENERGY AGENCY

The OECD Nuclear Energy Agency (NEA) was established on 1st February 1958 under the name of the OEEC European Nuclear Energy Agency. It received its present designation on 20th April 1972, when Japan became its first non-European full Member. NEA membership today consists of 28 OECD member countries: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, Republic of Korea, Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities also takes part in the work of the Agency.

The mission of the NEA is:

- to assist its member countries in maintaining and further developing, through international co-operation, the scientific, technological and legal bases required for a safe, environmentally friendly and economical use of nuclear energy for peaceful purposes, as well as
- to provide authoritative assessments and to forge common understandings on key issues, as input to government decisions on nuclear energy policy and to broader OECD policy analyses in areas such as energy and sustainable development.

Specific areas of competence of the NEA include safety and regulation of nuclear activities, radioactive waste management, radiological protection, nuclear science, economic and technical analyses of the nuclear fuel cycle, nuclear law and liability, and public information. The NEA Data Bank provides nuclear data and computer program services for participating countries.

In these and related tasks, the NEA works in close collaboration with the International Atomic Energy Agency in Vienna, with which it has a Co-operation Agreement, as well as with other international organisations in the nuclear field.

FOREWORD

The concept of improving nuclear safety versus maintaining it has been discussed at a number of meetings of the NEA Committee on Nuclear Regulatory Activities (CNRA) in recent years. In the summer of 2000, CNRA members were asked to submit their views on the concept in writing. These comments were reviewed and compiled in a paper that was discussed at the December 2000 CNRA meeting. The CNRA then requested two of its expert task groups on regulatory effectiveness and safety backfits to prepare an NEA publication.

The national submissions indicated that there are philosophical differences between member countries about whether their regulatory approaches require licensees to continuously improve nuclear safety or to continuously maintain it. It has been concluded that, while the actual level of safety achieved in all member countries is probably much the same, this is difficult to prove in a quantitative way. In practice, all regulatory approaches require improvements to be made to correct deficiencies and when otherwise warranted. However, the various descriptions of whether safety has to be maintained or improved may cause confusion for the regulator's stakeholders, particularly the licensees and the general public. The CNRA or national regulatory agencies may thus wish to consider what further steps may be taken to reduce such confusion.

This publication was prepared based on contributions from the CNRA members from Finland, France, Germany, Spain, Sweden, the United Kingdom and the United States as well as the work of the expert task groups on regulatory effectiveness and safety backfits. The initial paper written by Dr. Sam Harbison was used as a basis for drafting the publication, which was completed by Dr. G.J. Kurt Asmis.

TABLE OF CONTENTS

INTRODUCTION

The fundamental objective of all nuclear safety regulatory bodies is to ensure that nuclear utilities operate their plants at all times in an acceptably safe way. The problem, of course, is that the timespan covered by a nuclear power plant, from its initial design stages to its eventual decommissioning and dismantling, can be as much as fifty years or more. Over such a long period of time there will certainly be major changes in the engineering and scientific knowledge that underpins the design, construction, operation and maintenance of the plant, as well as a better understanding of the threats that are posed by and to the plant from a variety of internal and external sources. Though improvements in testing and modelling help to reduce the margins of uncertainty in the behaviour of structural components and in the reliability of safety-significant parts of the plant, they also tend to reveal new threats and challenges to its safe operation. In other words the state of the art in science and engineering is constantly changing and presenting new challenges to both the utility and the regulatory body.

An even greater challenge to the regulator is to determine what is the “acceptable” level of safety for a nuclear power plant. What is acceptable is a matter for society to decide by weighing the risks and benefits of any particular activity and judging where the balance lies. Clearly this balance is different for different countries and varies with time in any individual country. The challenge to any regulatory body is to interpret society's answer to the question “how safe is safe enough?” and to reflect it in the regulatory standards and enforcement strategy that it adopts.

These issues are fundamental to the debate about whether regulators should be requiring licensees to continuously improve safety or to continuously maintain safety, which is reflected, in the detailed submissions (see Appendix).

1. LICENSING BASIS

The licensing basis of a nuclear power plant (NPP) is normally established before it goes into operation and consists of: a detailed description of the plant and site facilities; the design safety analysis; applicable codes and standards; operational procedures, rules and limits; emergency procedures, etc. When granting a licence the regulatory authority has to take account of society's views about what level of risk is "acceptable" (see section 3) as well as the current state of the art in science and technology. Once the licensing basis has been established, the regulatory authority requires the plant to remain in conformity with it throughout its operational life, i.e. the level of safety as defined in the licensing basis must be maintained.

However, although the licensing basis stays the same, the scientific and engineering understanding of the various components of it may well change. For example, many older plants were licensed on the basis of a "maximum credible accident" approach, with the design having to show that the plant could withstand such an event. The application of modern probabilistic safety assessment (PSA) procedures to such plants has shown that:

- The "maximum credible accident" is only one of many possible accidents that the plant safety systems might potentially have to cope with; and
- Even for the "maximum credible accident" additional aspects are often identified that were not considered properly at the time the original design basis was agreed.

The question of how far older plants need to be upgraded to conform to the general insights from modern PSAs will be considered further in section 3. However, most regulators have experience of the second point above, which is often revealed when licensees have to upgrade their safety analysis following some unexpected event or when carrying out a major review, such as a Periodic Safety Review (PSR). As an example, the vulnerabilities of certain safety-significant structures and components of the UK's gas-cooled reactors to the

effects of hot gas releases were revealed when PSA techniques were applied to them as part of their first long-term safety reviews. The original, deterministic safety analysis paid most attention to the events within the core and gave little consideration to the potential damage that jets of hot gas, escaping from the pressure vessel or primary coolant pipes, might do to the boilers, control and instrumentation cables and so on. When these effects were fully appreciated the licensees had to make plant modifications and improvements to cope with them. However, such modifications and improvements were strictly to maintain the licensing basis and not to improve safety in line with any new expectations of society. Other examples, which fall into this category, are proper segregation of electrical cabling (after the Brown's Ferry fire); the change of insulation material following the Barsebäck incident in 1992; and the incorporation of steam generator level indicators after TMI.

2. CURRENT STATE OF THE ART IN SCIENCE AND ENGINEERING

Some improvements in the state of the art in science and engineering have a direct impact on the understanding of the safety of the plant. The introduction and development of probabilistic safety assessment (PSA) has had a major impact on both the maintenance of the design basis (as discussed above) and on the whole question of what is acceptable in risk terms (see section 3). Other improvements, however, are more problematical for the regulatory body in terms of whether or not they should be required on older NPPs. For example, many of the developments in instrumentation and control (I&C) that have occurred over the past few years give the potential for more accurate, reliable and "user friendly" monitoring of plant conditions. However, they can be costly to install, in both time and financial terms, and have their own reliability/compatibility problems if mixed with existing analogue systems. The regulator needs to consider carefully the value of requiring the installation of such "state-of-the-art" devices if the existing ones are clearly allowing the plant to operate reliably within its licensing basis.

Similar issues arise from the application of modern inspection techniques to structural components on older plants. The modern equipment often detects cracks and faults in components and welds that were undetectable by the equipment available when the plant was constructed. If the plant has operated safely and reliably for many years, and there is good evidence that the defect is not "growing", should the regulator require the defect to be repaired, especially if the repair might degrade other safety features of the plant? Such questions present a real challenge to the regulator when he has to decide how to react to such new information and he must be clear whether he is requiring the licensee to maintain safety or to improve safety. The costs involved can be very great and, in the present financial climate, utilities are likely to mount strong challenges to requirements which they perceive go beyond the original design basis.

3. AS LOW AS REASONABLY ACHIEVABLE

The various acronyms, such as ALARA, ALARP and SAHARA (safety as high as reasonably achievable), all express essentially the same concept – that the operators and regulators of NPPs should constantly ask themselves the question "how safe is safe enough?" The answer to this question is not fixed but varies with time and, to a certain extent, from country to country. It expresses concepts found in several of the national submissions, such as:

- "the risk from using nuclear power has to be low compared to other risks in society" (Sweden);
- "improving safety is understood to mean reducing the relative risk share of using nuclear energy in relation to the overall risk in the society" (Finland);
- "documented safety reviews [have to show that] all reasonably practicable improvements have been implemented" (UK);
- "an activity is deemed to be safe if the perceived risks are judged to be acceptable" (USA);
- "an acceptable level of risk can only result from a constant confrontation between what is desirable and what is possible" (France).

These last two perceptions give an excellent insight into the process that has to be gone through to answer the question "how safe is safe enough?" Fundamentally, it is for society to answer, on the basis of all the information (technical and otherwise) available to it. The regulatory authority then has to attempt to frame technical safety requirements that accurately reflect society's answer. In some countries, such as the USA, decisions about ALARA are made on a broad, industry-wide basis through the very wide-ranging and open consultation process that is used to obtain the views of all stakeholders (including the utilities) about where the balance lies between risk reduction and cost. The process results in an across-the-board decision about what is acceptably safe and this is normally reflected in a formal regulatory document. The advantage of this approach is that it provides clarity and consistency for both the utilities and the regulatory body though it can appear somewhat rigid (as in the re-licensing requirements).

In other countries, ALARA questions are decided largely between the regulator and the utility on a more ad-hoc, continuous basis. The advantage of this approach is that it is very flexible and can react more or less instantly to new technical information or perceptions of risk. The disadvantage is that there is less certainty for both the regulator and the utilities about where they stand in the ALARA continuum at any particular time. Some countries, such as the UK, have made efforts to restrict this area of uncertainty by attempting to generate public and scientific debates about the limits of acceptable risk, through documents such as the Tolerability of Risk and the associated NII Safety Assessment Principles. It seems that, after a slow start, this approach is gradually gaining a foothold in the public/media debate about risks.

Finally, there is the question of so-called "reverse ALARA". As the state of the art in science and technology improves, especially with the development of more realistic models, longer operating experience and the refinement of PSA, the levels of conservatism built into much of the design and operation of NPPs is becoming clearer. How should regulatory bodies react to such evidence? In the French submission it is stated that:

"The SAHARA principle (safety as high as reasonably achievable) is not paradoxical with the fact that it is possible to relax some regulatory constraints as a better knowledge of the risk is obtained and thus to apparently agree on an increase of the level of risk; but, as the margins are decreased in the same time as their uncertainty is reduced, the actual level of risk accepted by the regulatory body would be maintained."

The key to implementing this precept is how the regulatory body "confirms its acceptability" – is it just a matter for the regulatory body to decide or should it take note of (or consult) its other stakeholders, particularly the public, who may not be prepared to tolerate any increase in the apparent level of risk from NPPs?

In reality, of course, it is extremely difficult for any regulatory body to make an accurate assessment of the level of risk that is deemed to be acceptable by the society it represents. The most reliable indication is usually obtained from the Public Inquiries, parliamentary questions and media coverage that follow any untoward nuclear events – but these are too infrequent and the information comes too late to guide the normal precautionary regulatory approach that is required for nuclear power. It is recommended that further consideration should be given to the general issue of public acceptability as part of the CNRA's further consideration of regulatory effectiveness and regulatory performance indicators.

4. THE HUMAN SIDE OF IMPROVE VERSUS MAINTAIN

In a series of penetrating studies carried out by the High Reliability Group[1], researchers concluded that within the organisations they examined – nuclear power, naval aviation, air traffic control – the one constant was that all were organised for continuous improvement. The warning given was that organising to maintain (rather than to improve) safety would be a difficult prospect. Organising to maintain runs the risk of a dominance of routine and a lapse of mindfulness. The staff at Diablo Canyon, that was the object of one of their studies, were observed to guard against what could be called "business as usual", that is, maintaining what has already been achieved. By a constant and relentless drive for safety improvements the organisation kept itself mobilised in a fairly high state of energy and attention.

Independent of any industry or societal demands to build in new levels of safety, the actual level of safety of any given plant is a constantly shifting condition and never is a single state for any plant. This is so for two broad sets of reasons, the first is technical and the second is organisational:

Technical

- Physically the plant is not a constant over time. It's constantly ageing, which alters some components and performance characteristics. New and updated component parts enter the plant – e.g. valve and other manufacturers alter their products slightly over time as they seek manufacturing cost reductions or upgrades in performance.

1. The High Reliability Group included social psychologist such as Todd LaPorte, Gene Rochlin, Karen Roberts of Berkeley, Paul Schulman of Mills College, Oakland and others. Paul Schulman spent a sabbatical working at Diablo Canyon where he formulated the conclusions reported here.

- New knowledge changes the representation of the plant in analytic models and current "understanding". As we know more about failure probabilities, good practice or characteristics of ageing, the plant isn't the same as in its prior analytical representations.

Organisational

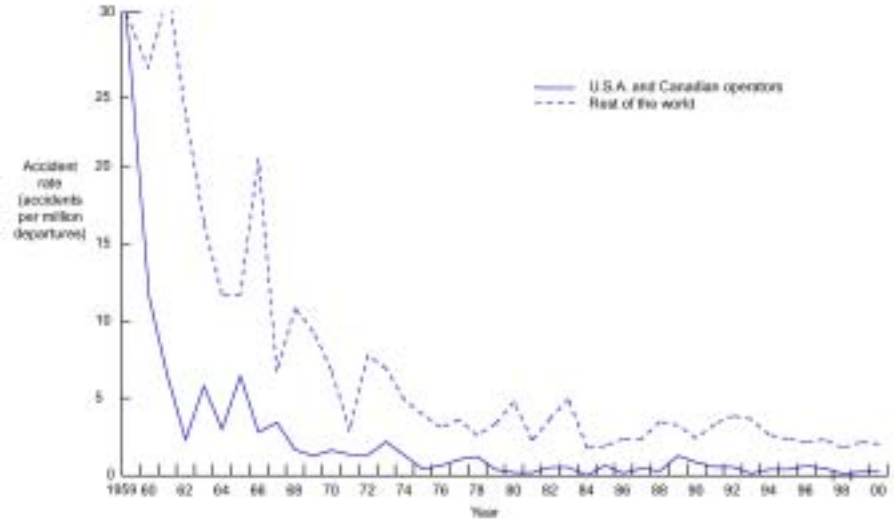
- Organisationally there is no constant level of safety at a plant. Key organisational variables like worker attentiveness and inter-departmental trust can decay over time. Routines, worker turnover and ageing of the workforce can change the ability of the members to cope with surprise. There will be almost imperceptible shifts in standards enforcement as safety becomes taken for granted.

The effort to improve safety was seen as a necessary condition for maintaining some upward equilibrium level of safety – that is, it protected against a downward decay in the trend of cyclical safety fluctuations to which plants are subject. To put it another way, there probably is no zero-slope line or "resting point" for safety equilibria in a high reliability organisation. The aviation industry has data that supports this conclusion.

Changing the Level of Safety: An Example from Civil Aviation

Commercial civil aviation has an exceptional safety record. For the last 20 years a high level of safety has been maintained. The public has found this level of safety acceptable. The concern that the regulator and industry share is that the accident rate has stabilised over the last 20 years and the many improvements in technology and human factors that have been added over that time period have not made a significant change in the safety level achieved.

Commercial Jet Fleet Accident Rate



Source: Airplane Safety, Boeing Commercial Airplane, *Summary of Commercial Jet Airplane Accidents, Worldwide Operations 1959-2000*, page 15, (www.boeing.com/tech/issues)

Air traffic is on the increase. The number of units flying are expected to double over the next few years. This means that the number of accidents will increase proportionally if the current safety levels are kept. The regulator and the industry fear that an increase of the number of accidents will not be accepted by society and are vigorously trying to improve and change the level of safety. National strategies[2] reflect that concern.

The relationship of civil aviation to the nuclear industry debate of improve or maintain is that the aviation industry has tried hard to improve safety over the last 20 years through constant vigilance, experience feedback, addition of new technology and research – particularly in human factors. The reality, however, is that all that improvement effort has only maintained the safety level. The lesson for nuclear safety here may very well be: *qui n'avance pas recule!*

2. Transport Canada, for example, in their current strategic plan are proactively trying to improve the safety levels by providing numerical targets which they hope will cut the accident rate in half within 5 years. See: www.tc.gc.ca/aviation .

CONCLUSIONS

The national submissions indicate that there are differences in how member countries describe their responsibilities to ensure adequate nuclear safety and about whether their regulatory approaches require licensees to continuously improve safety or to continuously maintain safety. It is concluded that, while the actual level of safety achieved in all member countries is probably much the same, this is difficult to prove in a quantitative way. In practice, all regulatory approaches require improvements to be made to correct deficiencies and when otherwise warranted. However, the various descriptions of whether safety has to be maintained or improved may cause confusion for the regulator's stakeholders, particularly the licensees and the general public, and the CNRA or national regulatory agencies may wish to consider what further steps may be taken to reduce such confusion.

In practice there is probably little difference between member countries with regard to the requirement for licensees to operate their plants at all times within the licensing basis. No regulatory authority would allow an NPP to continue to operate to its previous safety standards if some development in the state of the art in science or engineering (such as probabilistic safety assessment) showed clear deficiencies, either in the safety standards or in the extent to which the plant met the standards. However, licensees sometimes fail to appreciate that improvements in the understanding of the science and engineering that underpins the licensing basis may require plant improvements or modifications just to maintain the licensing basis. More difficult questions for the regulatory authority would concern the extent to which licensees should be required to maintain or to improve safety with respect to new developments in the state of the art. In addition, the CNRA or national regulatory agencies may wish to discuss how this can be communicated to the licensees in a better way.

All regulatory authorities recognise that they have to react sensitively to the views of society about the level of acceptable risk from NPPs. Indeed, other safety regulators in civil aviation, food, health and the environment have similar concerns. This is a difficult issue that is tackled in different ways by

different regulatory bodies, depending on the culture and traditions of their particular countries. Nevertheless, regulators need to have some techniques for gauging society's answer to the question “how safe is safe enough?” and for deciding, at any particular time and for any particular plant, whether it means that safety should be improved, maintained or even reduced (in line with a better knowledge of the inherent margins in the models and assumptions). Openness and clarity are important in order that the public can appreciate the technical arguments involved and the licensees can understand the grounds on which the regulator is basing his decision. The regulator must avoid giving the impression of either: allowing the operator carte blanche to run his plant unchanged for a fixed length of time irrespective of the public's view of what is acceptable; or constantly changing the regulatory “goal posts” in an attempt to reflect every swing in the perceived social attitudes to nuclear power.

Throughout the life of a nuclear power plant, changes occur both at the technical and human/organisational level. Regulatory authorities recognise that, in practice, it is very difficult to organise to maintain safety and that improvements to correct deficiencies and when otherwise warranted will continue to be made. Organising to maintain safety brings the risk of a dominance of routine and a lapse of mindfulness.

Appendix

COMPILATION OF COUNTRY CONTRIBUTIONS

In developing its report on Improving Regulatory Effectiveness the CNRA special task group discussed the issue of improving safety versus maintaining safety. CNRA member countries were asked to provide their definitions. The following responses were received:

Finland

What is safe enough?

The constitutional law of Finland stipulates that everyone shall have the right to life and personal liberty, physical integrity and security of person. Also it is stipulated, that the property of every person shall be protected and that public authorities shall strive to ensure for everyone the right to a healthy environment as well as the opportunity to influence decision-making concerning his living environment. Everyone shall be responsible for the natural world and for its diversity, for the environment and for the cultural heritage.

These fundamental rights and responsibilities are reflected in the Nuclear Energy Act defining as the main prerequisite for using nuclear energy, that the use of nuclear energy must be safe; it shall not cause injury to people, or damage to the environment or property. Safety is defined such a way that the activity does not endanger the citizens' health. The use of nuclear energy has to be in line with the overall good of society. This means that only a very low-level risk is considered tolerable. The goal is to keep the risk as low as possible, however, taking into account that the measures needed to meet this goal have to be reasonably achievable. Achievability can often be measured in terms of technical availability, reasonableness in terms of cost and inconvenience.

The safety records show that in reducing the risks of operations the nuclear industry has been a forerunner among the industrial community. That

leads to the conclusion, that in order to be safe enough, the risk stemming from the use nuclear energy has to be low compared to the other risk factors of the society.

Maintaining safety

In modern societies there is a general trend to improve the safety of the society and to minimise all the risks caused by human activities (industry, traffic) as well as by natural hazards (fires, floods, and diseases). This overall risk reduction objective calls for continuous alertness for seeking opportunities to reduce the risks also in nuclear industry. Formal cost-benefit analysis is not used by the licensees nor required by the regulators in Finland.

In Finnish approach "to maintain the safety level achieved" is not considered to mean that the absolute value of risk would be maintained, but instead of that, that the share of the incremental risk from using nuclear power would be maintained unchanged following the overall safety development in the society. This requires constant active efforts to enhance the nuclear safety.

In legal terms, this principle has been manifested in Finnish safety regulations as follows: "Operating experience from nuclear power plants as well as results of safety research shall be systematically followed and assessed. For further safety enhancement, actions shall be taken which can be regarded as justified considering operating experience and the results of safety research as well as the advancement of science and technology". This principle can of course also lead to real safety improvements (see next).

Improving safety

Real improving the safety is understood to mean reducing the relative risk share of using nuclear energy from the overall risk in the society. This interpretation requires that the nuclear industry has a role of a forerunner in safety work, not a role of a follower.

The legislative requirements for reducing the nuclear risk share are somewhat fuzzy and therefore, the driving force behind the safety improvements is more likely to be found in a well-developed safety culture of the licensee. One could say that where the requirements end, the culture begins. The difference of maintaining a safety level already achieved and of really improving it, could also be clarified by an old slogan: When you have done

everything that was assigned you, you should say “We are undeserving slaves; we have simply done our duty”.

France

Acceptable or accepted level of risk?

Determining whether a risk is acceptable is the result not only of a technical decision based on a scientific assessment of the level of risk but also of its acceptability by the society.

An acceptable level of risk can only result from a constant confrontation between what is desirable and what is possible. Consequently the acceptable level of risk can only be assessed by the yardstick of current knowledge and technical means. By definition, this level is changing with time.

At a given moment, and in a fixed technical and social context, it is possible to decide that a certain level of residual risk is acceptable. However it is not possible to decide that this very level of residual risk will remain acceptable later and that it will be enough to maintain it from now on.

A political choice

In France the (implicit) demand from citizens clearly appears as a request for the highest possible reduction of the level of risk. This demand is taken over (also implicitly) by the elected representatives and the government. The regulator must comply with this demand. Even if it is implicit, it really seems that a political consensus exists in France, which considers that the level of nuclear safety must be constantly improved.

As a consequence, despite the fact that regulators can always discuss such a subject, it will be anyway the political aspect that will decide.

A matter of culture

A good safety culture, based on a constant questioning attitude, constitutes a key point of the safety, whether to be improved or maintained. One can doubt whether it is really possible to keep intact such a questioning attitude

without any prospect of progress. Without the willingness to seek for improved safety level, can we really hope to maintain the actual level of safety?

Good principles

The policy of constant safety improvement is absolutely similar to that which is followed as far as radiation protection and environment protection are concerned. The SAHARA (safety as high as reasonably achievable) principle is the "first cousin" of the ALARA principle used in radiation protection and the BATNEEC principle used in environment protection. These three principles, together, make a consistent whole, which by far exceeds the notion of preventing unfavourable consequences of nuclear activities on health and environment. The same concept is presented in some international fora with different and possibly excessive words but, in fact, with the same idea like the willingness to "strive for zero". (What is excessive is not the will to strive for zero, but the fixing of a deadline to that will: the asymptote of zero risk, zero dose or zero release will never be reached).

Periodic safety reviews

In France, the practice is now well established to regularly reassess (about every ten years) the safety reference of existing installations. For PWRs, the homogeneity of the plants and the evolutionary practice among reactor series allow, in fact, to review the safety of a standardised plant series by comparing to following series. This does not mean that the level of safety for a series is considered as insufficient, but as soon as an improvement has been implemented on the most recent reactors, it is necessary to wonder about the possibility to apply it to older ones.

The safety reassessment and the incident operating experience constitute the two driving forces for the policy of improving safety.

This is why the French Safety Authority considers as a key point, not only for the safety of future reactors but also for the safety of present ones, the work performed on new projects like the EPR.

Improving risk knowledge

"The SAHARA principle is not paradoxical with the fact that it is possible to relax some regulatory constraints as a better knowledge of the risk is

obtained and thus to apparently agree on an increase of the level of risk; but, as the margins are decreased in the same time as their uncertainty is reduced, the actual level of risk accepted by the regulatory body would be maintained."

For instance, the agreement given to a new fuel management cycle with a higher burn-up, based on more exhaustive studies showing that previously accepted criteria continue to be satisfied, can be accepted as far as the uncertainty in the risk assessment is itself reduced in order to insure that safety margins are still sufficient to cover "uncertainty". Improving risk acceptability, is also a matter of improving its knowledge.

Germany

Priority to Safety

In Germany, the main safety principle for the peaceful utilisation of nuclear energy is the protection of life, health and property against the hazards of nuclear energy and the detrimental effects of ionising radiation. This principle is established in the Atomic Energy Act and it governs the design and safety concept of the nuclear power plants. These must be equipped with an effective safety system that will protect the plant personnel and the public as well as the environment from the radioactivity related to the operation of the nuclear installation.

Accordingly, nuclear safety has always been considered as the primary objective of the Atomic Energy Act and must at all times be considered in its application. As early as 1972, the supreme administrative court of Germany decreed that nuclear safety has priority over any of the other objectives of the Atomic Energy Act. This decree has always been upheld in later court decisions. The principle of "safety first" has been the guiding theme in any administrative action in the field of nuclear energy. This principle has been concretised with respect to the individual license by the following licensing prerequisite: *"A license may only be granted if the necessary precautions have been taken in the light of the state of the art in science and technology to prevent damage resulting from the construction and operation of the installation."*

An important basis for implementing the safety-first principle is the independent full responsibility of the licensee as the party ultimately responsible for safety (see responsibility of the licensee). The willingness of the licensee to employ an all-encompassing safety management is of crucial importance. This

must comprise all measures required for ensuring the achievement of a sufficient safety level.

Assessment of Safety

The safety assessment during construction, commissioning and essential modifications of a nuclear power plant is performed within the licensing process, continuous safety evaluation during operation is performed within the scope of regulatory supervision.

After the respective license has been granted the safety assessment during construction, commissioning and subsequent power operation of the nuclear power plant is performed in accordance the Atomic Energy Act by the nuclear supervisory authority. This authority verifies that the conditions and prerequisites on which the license was based continue to be maintained during the entire lifetime of a nuclear power plant.

Verification of Safety

Within his independent full responsibility for plant safety each licensee adjusts the safety level of the nuclear power plant to be in correspondence with the state of the art in science and technology over the entire operating life of the plant. If new safety relevant findings come to light, the need for and appropriateness of improvements is evaluated. In addition safety assessments are continuously performed as part of the regulatory supervisory procedure, and discontinuously or periodically as a specific safety review (e.g. probabilistic safety reviews) or risk studies.

Routine verification of safety by the licensee

The licensee submits safety verifications for the first time with the application for construction of a nuclear power plant. These must show that the plant will be in conformity with the valid nuclear safety regulations and will have the necessary safety characteristics.

During operation a regularly repeated verification is required to show that the system functions important to plant safety are executed properly and, also, that the quality characteristics have not deteriorated below acceptable levels (e.g. by in-service inspections, periodical functional tests, and preventive maintenance).

Inspections under governmental supervision

The supervisory activities of the Länder under nuclear legislation include the performance of safety assessments on a continuous as well as discontinuous and periodic basis, both as specific safety reviews and probabilistic safety analyses. They lead to remedial measures wherever appropriate. These continuous supervisory activities assure an intensive assessment of plant safety. Federal supervision is engaged in the analysis of more general safety aspects. The safety reviews performed so far did not reveal the need for any immediate action. However, the plant-specific inspections during operation and the analysis of national and international operating experience have resulted in manifold improvements that have affected specific components and maintenance measures.

Backfitting and safety improvements

The findings of the safety evaluations and the resultant backfitting and safety improvements show that the licensed safety status of the plants have at least been successfully maintained but, also, that newer safety findings were given appropriate consideration during the time of licensed operation.

Conclusions

In Germany, licensees have full responsibility for plant safety. Each licensee adjusts the safety level of the nuclear power plant to be in correspondence with the state of the art in science and technology as long as the plant is in operation.

Accordingly, licensees are required to continuously analyse the safety performance of their NPPs and have to take action (under the supervision of the regulators) if deficiencies are discovered.

Thus, maintaining nuclear safety does not mean to just measure up with the once determined (or required) safety level in a sense of a “steady state” over the lifetime of the plant, but it means to support an ongoing manifold process, in order to achieve the highest possible reduction of risk (in an absolute sense) by improving both, knowledge and technical means.

Sweden

The Act on nuclear activities states that safety shall be maintained by the taking of those measures required to:

- prevent errors in or malfunction of equipment, incorrect handling or anything else that may result in a radiological accidents;
- prevent unlawful dealings with nuclear material or nuclear waste.

It is important to note that the law also says that the licensee of nuclear activities has to ensure that all measures are taken that are needed for maintaining safety.

Looking at the underlying documents to the law one can see that safety is seen in a wide sense, and one can conclude that the SKI cannot easily require a reactor of early design to be upgraded to modern standards just as such. On the contrary, SKI can require a licensee to correct deficiencies in safety, which have been discovered through improved analysis or new knowledge. If the SKI, following the application of such improved analysis of new knowledge sees that a reactor belonging to an earlier design does not meet the licensing conditions, safety has to be improved as a condition for further operation. This means technically improved safety but formally safety is maintained.

SKI also has a duty to "*Initiate safety improvements whenever justified by operating experience, or research and development*". Therefore the SKI requires the licensees to conduct an active safety work including the carrying out of safety analysis using modern analytical tools. Deviations discovered in such analysis have to be assessed and a program for safety upgrading established.

This is taken care of in SKI regulations where we say "licensee has to maintain and develop safety". In the word "develop" we include a continuous work to "hunt" for safety deficiencies in the reactor design and the quality of the safety work and to take actions if deficiencies are discovered.

In summary we can say that we require licensees to continuously analyse safety and take actions if deficiencies are discovered, not to continuously improve safety in an absolute sense. Also, we believe that the risks from using nuclear power has to be low compared to other risks in society. When risks in general are reduced the risks from nuclear power has to be reduced. Finally, it should be said that the licensees themselves have established safety goals, including probabilistic ones. These goals are rather ambitious and push the

owners to modernise their reactors of earlier design. This is according to the SKI part of the responsibility for safety that the licensee has.

Spain

Requirements related to the required safety level for operating nuclear installations in Spain are established in the operation permit. Attached to the permit a set of conditions on Nuclear Safety and Radiation Protection are established. Among these conditions one related to approved Official Documents is included. In this condition are identified revisions of Final Safety Analysis Report (FSAR), Technical Specifications (TS), Emergency Plan and Organisation Manual, used by Regulatory Body to perform safety assessments necessary to release the operation permit. The format and content of both FSAR and TS is based on standards from US Nuclear Regulatory Commission. Emergency Plan and Organisation Manual follow Spanish approach based on national regulations.

From the content of the above mentioned documents the required safety level for the facility is well established as they include Safety analysis, applicable codes and standards and operational limits, so building the licensing base of the plants. Any doubt about which, based in the operating experience of the plant or similar plants, arises on the strict compliance of the licensing base is addressed by CSN, in the framework of the license, as a regulatory control activity. CSN is empowered to set direct requirements, as complementary instructions, to ascertain and restore the licensed safety level.

Also in the operating permit provision for safety improvements are included. All nuclear facilities permits in Spain include a condition requiring licensees to perform an analysis of new regulatory requirements released by the regulatory authority from the country of origin of the technology of Spanish plants (mainly USA and Germany). This analysis should consider both applicability of new requirements to the Spanish plant and provisions for licensee to implement it when found applicable.

CSN perform assessment of licensee's year report related to new requirements. When a new requirement is to be implemented entailing an increase in the plant required safety level, an amendment to the operating permit is released by Ministry of Industry and Energy, following CSN report.

In recent years a new condition has been included in Spanish nuclear power plants, requiring licensees to perform a ten-year based Periodic Safety Review (PSR). CSN assessment of PSR results has become a main input for operating permit renewal. Derived from RPS assessment, safety improvements to

be implemented by licensees are identified. Depending on the scope and nature of the improvements, their implementation is required as conditions to permit renewal or as CSN complementary instructions.

Finally other ways for safety improvement, on a continuous basis, are the so called as "safety improvement programs". These are required directly from CSN to licensees and they do not entail an increase in the licensed safety level, even when from the results of such programs design modifications are implemented in the plants to improve safety. This is the case of programmes, now under way of implementation or close to completion, related to Probabilistic Safety Assessment and its applications, man-machine interface, dose reduction programmes, radwaste management and fire protection.

An economically deregulated electricity market is now in place in Spain. This fact, as recognised in the CSN Strategic Guidance Plan (February, 1998), poses a challenge on CSN to increase its regulatory control specially on potential resource shortages and, at the same time perform an effective regulatory control addressing its activities to the most safety beneficial measures and to perform cost-benefit analysis of the regulatory requirements.

United Kingdom

There is a fundamental duty enshrined in UK safety law (the Health & Safety at Work, etc., Act 1974) for all employers to reduce the risks to their workers and the public "so far as is reasonably practicable". This duty applies to all employers, whether engaged in nuclear operations or, for example oil extraction, construction or agriculture. Combined with the requirement under standard nuclear site licence condition 15 for periodic safety reviews, this places a requirement on licensees periodically (every 10 years) to submit documented safety reviews to the Nuclear Installations Inspectorate (NII) in which it is demonstrated not only that the plant still meets the original design standards, but also that a comparison with modern standards has been made, possible improvements to reduce the gap between these and the original standards have been considered, and all reasonably practicable improvements have been implemented. There is consequently a continuing pressure upon licensees not only to maintain but also to improve safety. This pressure is maintained between the major Periodic Safety Reviews by NII's routine site inspection and technical assessment activities, which include 'minor' safety reviews prior to consent to reactor start-up being granted and assessments of licensees' proposals for plant modifications against the modern standards set out in NII's published Safety Assessment Principles (SAPs). These SAPs are themselves currently under review.

United States

The U.S. Atomic Energy Act of 1954 and Energy Reorganisation Act of 1974 establish the basic regulatory mission of the NRC. This mission is to regulate the civilian use of by-product, source, and special nuclear material to ensure adequate protection of public health and safety, to promote the common defence and security, and to protect the environment. As indicated, "adequate protection" is the standard of safety on which NRC regulation is based. As commonly understood, safety means freedom from exposure to danger, or protection from harm. In a practical sense, an activity is deemed to be safe if the perceived risks are judged to be acceptable. The NRC recognises the risks to the public from nuclear power plant operation. As such, in 1986, it promulgated the Safety Goal Policy, which expresses an acceptable level of the risk from nuclear power plant operation by comparison with other societal risks.

The collective efforts of the NRC and the nuclear industry are needed to maintain safety. NRC licensees have the responsibility to safely design, construct, and operate reactors. Regulatory oversight of licensee safety is the responsibility of the NRC. Thus, safe performance reflects the results of the collective efforts of the NRC and the nuclear power industry.

The safety performance of the U.S. nuclear power industry has improved substantially over the past ten years, and nuclear reactors, collectively are operating above acceptable safety levels consistent with the agency's Safety Goal Policy. The NRC believes this level should be maintained. If substantial safety improvements are identified, additional regulatory requirements should only be imposed consistent with the Commission's Backfit Rule (10 CFR 50.109). Allowing small-risk increases may be acceptable when there is sufficient conservatism and reasonable assurance that sufficient defence-in-depth and safety margins are present. Small-risk changes that reduce unnecessary burden will allow more efficient use of licensee and the NRC resources as well as bring into focus those areas that are more critical to the safety of the public and the environment. We use the body of domestic and international knowledge, experience, and research to determine when changes that could affect risk are acceptable.

NRC licensees will continue to have the primary role in maintaining safety and are expected to identify, through mechanisms such as operating experience feedback and integrated risk assessments, the design and operational aspects of their plants that should be enhanced to maintain acceptable safety performance levels. For nuclear power plants to continue operating, safety performance must be at or above acceptable levels. The NRC will take action to improve safety performance before it falls below acceptable levels and will

require the shutdown of plants when their safety performance is identified as unacceptable. In addition, circumstances may arise, where new information reveals, for example, that an unforeseen hazard exists or that there is a substantially greater potential for a know hazard to occur. In such situations, the NRC has the statutory authority to require licensee action above and beyond existing regulations to maintain the level of protection necessary to avoid undue risk to public health and safety.

Where requirements exist that the NRC concludes have no safety benefit, the NRC can and should take action, as appropriate, to modify or remove such requirements from the regulations or licences. Requirements that are duplicative, unnecessary, or unnecessarily burdensome can actually have a negative safety impact. They also can tend to create an inappropriate NRC and licensee focus on “safety versus compliance” debates. As the NRC has stated in its Principles of Good Regulation, “there should be a clear nexus between regulations and agency goals and objectives, whether explicitly or implicitly stated”.

As some requirements are more important to safety than others, the NRC will use a risk-informed approach, whenever possible when adding, removing, or modifying NRC regulations, as well as when applying NRC resources to the oversight of license activities. Based on the accumulation of operating experience and the increasing sophistication of risk analysis, the NRC will continue to refine its regulatory approach in a manner that enhances and reaffirms our fundamental safety objective. In addition, the NRC recognises that to be a successful regulator we must consider the effects of our decisions on the public and the industries we regulate. Therefore in addition to maintaining safety, our performance goals also include a focus on making our activities and decisions more effective and efficient, reducing unnecessary regulatory burden, and enhancing public confidence.

ALSO AVAILABLE

NEA Publications of General Interest

2001 Annual Report (2002) *Free: paper or web.*

NEA News
ISSN 1605-9581 Yearly subscription: € 37 US$ 45 GBP 26 ¥ 4 800

Safety and Regulation

Advanced Nuclear Reactor Safety Issues and Research Needs (2002)
ISBN 92-64-19781-8 Price: € 75 US$ 65 GBP 46 ¥ 8 700

Nuclear Regulatory Challenge of Judging Safety Backfits (The) (2002)
ISBN 92-64-18484-8 *Free: paper or web.*

Nuclear Fuel Safety Criteria Technical Review (2001)
ISBN 92-64-19687-0 Price: € 20 US$ 19 GBP 12 ¥ 1 900

Investing in Trust: Nuclear Regulators and the Public (2001)
ISBN 92-64-19314-6 Price: € 60 US$ 54 GBP 37 ¥ 6 050

Assuring Nuclear Safety Competence into the 21st Century (2000)
ISBN 92-64-18517-8 Price: € 55 US$ 50 GBP 31 ¥ 5 300

Nuclear Safety Research in OECD Countries – Major Facilities and Programmes at Risk (2001)
ISBN 92-64-18468-6 *Free: paper or web.*

Nuclear Safety Research in OECD Countries – Summary Report of Major Facilities and Programmes at Risk (2001)
ISBN 92-64-18463-5 *Free: paper or web.*

Collective Statement on Major Nuclear Safety Research Facilities and Programmes at Risk (2001)
Bilingual – ISBN 92-64-08476-2 *Free: paper or web.*

Collective Statement on the Role of Research in a Nuclear Regulatory Context (2001)
Bilingual *Free: paper or web.*

Assuring Future Nuclear Safety Competencies – Specific Actions (2001)
ISBN 92-64-18462-7 *Free: paper or web.*

Improving Nuclear Regulatory Effectiveness (2001)
ISBN 92-64-18465-1 *Free: paper or web.*

Nuclear Regulatory Challenges Arising from Competition in Electricity Markets (2001)
Bilingual.
ISBN 92-64-08460-6 *Free: paper or web.*

Order form on reverse side

ORDER FORM

OECD Nuclear Energy Agency, 12 boulevard des Iles,
F-92130 Issy-les-Moulineaux, France
Tel. 33 (0)1 45 24 10 15; Fax 33 (0)1 45 24 11 10; E-mail: nea@nea.fr**,**
Internet: www.nea.fr

Qt	Title	ISBN	Price	Amount
			Total	

❑ Payment enclosed (cheque or money order payable to OECD Publications).

Charge my credit card: ❑ VISA ❑ Mastercard ❑ American Express

(Prices include postage and handling fees).

Card No.	Expiration date	Signature
Name		
Address	Country	
Telephone	Fax	
E-mail		

OECD PUBLICATIONS, 2 rue André-Pascal, 75775 PARIS CEDEX 16
Printed in France.