Nuclear Regulation ISBN 978-92-64-99044-9

The Regulatory Goal of Assuring Nuclear Safety

NEA No. 6273

NUCLEAR ENERGY AGENCY
ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

This work is published on the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Organisation or of the governments of its member countries.

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, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Luxembourg, Mexico, the Netherlands, Norway, Portugal, the Republic of Korea, the 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.

Cover credits: Union Electric Co. (USA) and NEI (USA).

FOREWORD

The Committee on Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency (NEA) is an international committee made up primarily of senior nuclear regulators. It was set up in 1989 as a forum for the exchange of information and experience among regulatory organisations and for the review of developments which could affect regulatory requirements. The Committee is responsible for the programme of the NEA concerning the regulation, licensing and inspection of nuclear installations. In particular, the Committee reviews current practices and operating experience.

Over the past decade the CNRA has produced a series of twelve reports, known as the "green booklets", which look at a number of regulatory challenges. These booklets form part of a mosaic which, when put together, provide most of the major elements of a nuclear safety regime. The objective of this booklet was to bring together these elements and others to show how regulators can develop an overall process for integrated safety assessment. Based on the consensus of the CNRA members at their June 2006 meeting, a Senior-level Expert Group was formed to produce a report on *The Regulatory Goal of Assuring Nuclear Safety*.

The report was prepared by Dr. Thomas Murley and Dr. Samuel Harbison on the basis of discussions with, and input provided by, the members of the Senior-level Expert Group listed below. Dr. Ulrich Schmocker (HSK, Switzerland) skilfully chaired the meetings and the work of the group.

John Loy (ARPANSA)	Australia
Ken Lafreniere (CNSC)	Canada
Petr Brandejs (SONS)	Czech Republic
Marja-Leena Jarvinen (STUK)	Finland
Guillaume Wack (ANS)	France
Michael Herttrich (BMU)	Germany

Lamberto Matteocci (APAT)	Italy
Eiji Hiraoka (NISA/METI)	Japan
Shunsuke Ogiya (JNES)	Japan
Woong Sik Kim (KINS)	Korea
Marli Vogels (KFD)	The Netherlands
Andrej Stritar (UJD)	Slovenia
Lennart Carlsson (SKI)	Sweden
Peter Flury (HSK)	Switzerland
Colin Potter (HSE/NII)	United Kingdom
James Dyer (NRC)	United States
James Wiggins (NRC)	United States
Adriana Nicic	IAEA
Barry Kaufer	NEA-Secretariat

TABLE OF CONTENTS

1. INTRODUCTION

The fundamental objective of all nuclear safety regulatory bodies is to ensure that nuclear facilities are operated at all times in an acceptably safe manner including the safe conduct of decommissioning activities.[1] In meeting this objective the regulator must keep in mind that it is the operator that has the responsibility for safely operating a nuclear facility. The nuclear regulator's responsibility is to oversee the operator's activities in order to assure that the facility is operated safely. Nothing the regulator does should ever diminish that fundamental distinction in roles between the operator and regulator.

Of comparable importance to the regulator's effectiveness in assuring nuclear safety is the need for stakeholder confidence in its technical competence, integrity and sound judgement. Thus, a regulator's decisions must be technically sound, transparent, and consistent from case to case, and seen by impartial observers to be fair to all parties.

To meet its responsibility to proactively promote safety, the regulator will have in place a set of requirements that the operator must follow in order to operate the facility safely, to assure the security of nuclear materials, to protect the environment, and to manage safely radioactive waste and spent nuclear fuel. The regulator conducts oversight activities at facilities to gain assurance that activities are being conducted in a safe manner and, in case they are not, acts to see that the operator takes corrective actions to bring the facility into compliance with requirements and the facility's safety envelope. In the course of its routine activities the regulator makes ongoing judgements on the acceptability of the level of safety of the facilities it regulates. For any regulator one of the most important questions is "How can I judge whether my actions are actually assuring an acceptable level of safety at nuclear facilities?" but this is never a simple or straightforward question to answer.

1. NEA (2002), *Improving Versus Maintaining Safety*, OECD, Paris.

For example, in the weeks and months leading up to the accidents at TMI-2 and Chernobyl, there was no unequivocal evidence that the reactors were skirting on the edge of disastrous accidents. To be sure, in retrospect it was possible to discern several signs of design weaknesses, operator training deficiencies and safety culture problems at both facilities but these did not alert either the operators or the regulators to the impending accidents. A major lesson from both accidents is the need for the regulator to be sensitive to such early signs of weaknesses and problems and to take pre-emptive actions to require improvements before severe accidents can occur.

There are today, many sources of information available to the regulator pertaining to safety at any nuclear facility, such as inspection reports, operating experience reports, research results, periodic safety reviews, probabilistic safety analysis (PSA) results, insights from IAEA reviews and other similar information. A major challenge for the regulator is to systematically collect and analyse this information in order to arrive at an integrated assessment of the level of safety of the particular facility and then to make a judgement about its acceptability.

Clearly, regulatory bodies around the world have been making such judgements for the past five decades, relying mainly on the competence, experience and impartiality of their staff. During that time they have developed criteria and regulations to guide their inspectors in reaching safety judgements. The excellent safety record of the nuclear industry indicates that this process has been generally satisfactory.

More recently, a number of regulatory bodies have started to develop more systematic ways of measuring, recording and analysing safety information in order to arrive at a more quantitative and transparent assessment of the safety level achieved. They recognise the benefits of using a systematic approach but also recognise that, while it is desirable, it is not necessary to have a formal systematic assessment system in order to have an efficient and effective regulatory organisation.

The principal advantages of using such a systematic approach are that it gives an objective, transparent and reproducible snapshot of the safety performance of a facility or a licensee, it provides a basis for trending safety performance at individual facilities, and it assists the regulator in setting safety priorities for future regulatory actions. In addition, it should improve the efficiency of the regulator and, if applied correctly, it should also make the regulator more effective.

The challenge for any regulatory body is to identify an approach that is systematic, comprehensive, has well-defined safety acceptability guidelines and is of practical help in reaching sound, transparent and timely decisions within the laws and regulatory culture of the country in question. In order to assist member countries to address this challenging question, the Committee on Nuclear Regulatory Activities (CNRA) of the OECD Nuclear Energy Agency has sponsored this report.

While this report focuses on the benefits of having an integrated safety assessment system, one must keep in mind that there is no single, right way of carrying out such an integration. This report provides advice on the necessary attributes and basic components of any systematic method, with examples of how the safety components can be integrated and suggestions about the subsequent decision-making process. Clearly, no integrated safety assessment system should be so rigid that it precludes the possibility of individual safety judgements by experienced experts and senior managers in the regulatory body, especially if a facility has been showing an unusual number of events or regulatory non-conformances. Furthermore, it must always be remembered that the safety information available to any regulatory body can only ever be a sample of the total safety picture. Therefore, when using an integrated safety assessment system, regulatory bodies need to beware of assuming, or of giving the impression that the outcome provides an absolute determination of the safety of the facility in question.

The primary focus of this report is on how the regulatory body can systematically collect and make an integrated analysis of all the relevant safety information available to it and arrive at a sound judgement on the acceptability of the level of safety of the facilities that it regulates. It follows, therefore, that the audience for this report is primarily nuclear regulators, although the information and ideas may also be of interest to nuclear operators, other nuclear industry organisations and the general public.

2. THE ELEMENTS OF NUCLEAR SAFETY

"The fundamental safety objective is to protect people and the environment from harmful effects of ionizing radiation."[2] Nuclear safety therefore means the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards. This definition includes the common understanding of nuclear safety as freedom from physical harm, meaning both acute and latent health effects from exposure to radiation. But the regulator must recognise that the general public also expects to be protected against frequent, potentially dangerous events (near misses), and therefore the definition of nuclear safety must include freedom from danger, or unreasonable risk. Furthermore, all stakeholders expect to be protected from environmental damage such as radiological contamination of land, water supplies, buildings and livestock. Therefore, in this report a broader understanding of nuclear safety is used, namely "freedom from physical harm, unreasonable risk and environmental damage due to the operation of nuclear facilities."

Here, operation includes not only facility operation but also the handling and disposal of spent fuel and radioactive waste and the transport of radioactive materials. In principle, safety at nuclear facilities includes protection from harm due to non-radiological accidents (such as falls or chemical spills) but in this report we shall focus solely on radiological protection of workers, the general public and the affected environment. Finally, the term freedom from unreasonable risk is understood to include freedom from security breaches at the facility and from diversion of nuclear materials to unauthorised persons.

Having established this broad understanding of safety, one must examine the elements of the detailed framework of safety. The international nuclear community has developed the fundamentals of nuclear safety in great depth and breadth over five decades of nuclear facility experience. In the early years of nuclear technology, the primary focus was on development of basic physics and

2. IAEA (2006), *Fundamental Safety Principles,* IAEA, Vienna.

engineering principles, safety system design features, codes and standards, and general design criteria governing such matters as redundancy and diversity of safety systems. From the mid-1970s the development of probabilistic safety assessment (PSA) brought important insights into the initiation and progression of potential accident scenarios and the contribution that different systems and components make to the overall safety of a facility. It led to risk-based insights into the operation and maintenance of facilities and gave the possibility of comparing achieved safety against numerical safety goals. As operating experience was gained, it showed the importance of human performance aspects of safety, including operator qualification and training, emergency operating procedures, accident mitigation measures, and emergency planning. In more recent years the importance of operational safety culture has come into clearer focus.[3] A strong safety culture is important to ensure the integrity of the multiple barriers of the entire defence in depth safety fabric. That is, the safety values, norms and attitudes of an entire operating organisation are just as important as the design and construction of the facility.

The defence in depth safety concept has long been recognised as a key element in ensuring safety.[4] After being refined and strengthened through years of application, the concept can best be described as multiple, independent levels of protection (or barriers) that would have to fail before harmful effects from radiation could be caused to the public or the environment. The concept of defence in depth has served safety well over the years and continues to be an effective method of accounting for uncertainties in equipment and human performance. As noted above, it applies not only to barriers and safety functions but also to human factors and organisational aspects.

3. NEA (1999), *The Role of the Nuclear Regulator in Promoting and Evaluating Safety Culture*, OECD, Paris.

4. IAEA (1996), *Defence in Depth in Nuclear Safety, INSAG-10*, IAEA, Vienna.

There is no unique way of grouping the elements of nuclear safety. For the purposes of this report they are grouped under the following three general headings:

1. technical;

2. human factors and organisational; and

3. programmatic and cross-cutting.

Each of these safety elements is made up of a number of safety components, examples of which are listed below. The grouping of these safety components is not unique but the sum of the components is believed to be comprehensive.

Components of technical safety

- A solid foundation of knowledge of the basic physics, chemistry and engineering of nuclear technology.

- A robust facility design which uses established codes and standards that embody design margins, qualified materials, redundant and diverse safety systems, and which protects against the full range of nuclear, conventional and external hazards.

- A robust and properly resourced programme for ensuring that the facilities are designed, constructed, operated, maintained and tested in accordance with the design specifications and safety analyses.

- A strong engineering function that maintains plant, systems and equipment in accordance with the facility design basis, analyses technical and facility ageing issues as they arise, and provides support to operations and maintenance.

- Safety assessments of all changes and backfits made during the life of the facility.

- A radiological protection programme that ensures all personnel are adequately protected against the harmful effects of the ionizing radiations emitted from the nuclear facility and its fuel cycle.

- A programme for utilising the probabilistically-developed risk insights derived from systems analysis and operational experience.

Components of human factors and organisational safety

- Sufficient properly qualified, trained, and fit-for-duty personnel to operate the facility, maintain the equipment, implement the radiation protection programme, and who demonstrate a questioning attitude toward all aspects of operation of the facility.

- An operating staff that follows conservative decision-making principles and has a profound respect for the reactor core and radioactive materials, keeping them under absolute control at all times.

- A comprehensive set of operating, maintenance, and accident management procedures, including severe accident management guide-lines, that have been developed and tested using established man-machine interaction principles.

- A strong corporate management organisation with a leadership that establishes a set of values emphasising the priority of nuclear safety, making it clear that workers should not have a conflict in their daily tasks between safety and other business goals, and that provides adequate resources to ensure that the facility is operated safely.

- A facility management organisation that has clear lines of authority and responsibility for safety and that facilitates openness, a questioning attitude, confidence between employees and managers, control of quality in all activities, and strict adherence to safety procedures.

- A programme and procedures for the management oversight of all safety-related work done by contract workers for or at the facility.

Components of programmatic and cross-cutting safety

- Operational limits and conditions (or technical specifications) that define and govern the safe operating envelope of the facility and ensure that radiation exposures are kept as low as reasonably achievable.

- Programmes such as fire protection and surveillance testing that are critical components of the defence in depth safety philosophy of maintaining multiple barriers, both physical and procedural, against severe accidents.

- A programme of operating experience analysis, trending analysis and feedback to operations.

- A programme of initial and continuing training to ensure an operating staff of qualified workers.

- A configuration management programme that maintains the safety design basis of the facility as approved by the regulatory body.

- An ageing management programme that monitors the potential deleterious effects of ageing on systems, structures and components and requires proactive steps to maintain the safety design basis.

- A change management programme that ensures that organisational changes do not inadvertently diminish operational safety.

- Effective integrated management systems (including quality assurance, self-assessment and corrective action programmes).

- A safety culture that has been instilled throughout the operating organisation based on the highest safety values and that fosters an attitude of conservative decision making.

- Emergency plans, which have been thoroughly reviewed and tested, to enable actions to protect both onsite workers and offsite populations in the event of a nuclear accident.

- Access to a continuing programme of nuclear safety research that is designed to add to the basic knowledge of safety fundamentals.

- Facility siting and environmental policies that promote offsite protection.

- Security plans that are tested and kept current to prevent threats to the facility and to prevent unauthorised use of nuclear materials.

In addition to these safety elements that apply to operation of a nuclear facility, there must be a safety regulatory body that has the legal authority, technical competence and adequate resources to independently assure that nuclear facilities are designed, built, operated and decommissioned safely.

Safety criteria

Regulatory bodies have the legal duty and authority to make final safety judgements on all nuclear activities under their responsibility. In a practical sense a nuclear activity is deemed to be safe if the perceived risks are judged to be acceptable. But the regulator can never have a certain quantitative assessment of the risks involved. Therefore, in arriving at its safety judgements, the regulatory body must be guided by the basic safety criteria embedded in its national laws, regulations and policies. One of these criteria is the level of safety protection required by the regulator. There are various statements of the basic level of safety required by OECD/NEA countries, but they all acknowledge that it is not possible to achieve absolute safety (i.e., zero risk) in nuclear activities. Some of these criteria are:

- no unreasonable risk;
- adequate protection of public health and safety;
- risk as low as reasonably practicable;
- safety as high as reasonably achievable;
- limit risk by use of best technologies at acceptable economic costs.

A related safety criterion is the degree of assurance needed by the regulator that the basic level of safety protection is being met. Here again, there are various formulations of this criterion among OECD/NEA countries, but they all recognise that absolute assurance cannot be achieved. Most countries have some variation of a “reasonable assurance” criterion.

These basic safety criteria are seen to be qualitative, aspirational criteria rather than quantitative safety requirements that must be demonstrated to the regulator. In practice these criteria are what some may call “revealed standards”. That is, the cumulative experience of a regulatory body’s safety judgements over many years will yield a working definition of what these criteria mean.

It is recognised that nuclear facilities generally operate well above the minimally acceptable levels of safety implied by these qualitative safety criteria. Therefore, much of the regulator's oversight actions are directed toward judging compliance with regulations, assessing safety margins and looking for negative or positive safety trends.

Changing level of safety

As a practical matter, the actual level of safety of any given facility is constantly changing, for a number of reasons.

a. Physically the facility is not constant over time. Redundant safety systems are occasionally taken out of service for on-line maintenance during operation, thereby altering the risk profile of the facility in the short term. Over the longer term, as the facility ages and new and updated component parts are introduced, its performance characteristics change.

b. New knowledge about facility performance, such as equipment failure rates or newly discovered and unexpected accident sequences, changes the representation of the facility in analytical safety models and therefore changes the current understanding of the level of safety.

c. Many operators strive to improve the economic performance of their facilities by means of longer fuel cycles, new fuel designs, higher fuel burnups and power uprates, all of which have safety significance.

d. Organisationally there is no constant level of safety performance at a facility. Key organisational variables like interdepartmental co-operation and worker attention to quality can decay or improve over time. Ageing of the workforce and its consequent potential for complacency can change the ability of the workers to cope with unexpected events. Conversely, new managers with fresh ideas can improve operational safety performance.

e. The environment in which the facility operates may change over time. This could be due to nearby industrial, farming or housing developments or because new information emerges about the potential magnitude and frequency of environmental hazards, such as seismic events or severe weather.

This constantly changing level of safety at nuclear facilities presents an obvious challenge to the regulator in reaching its safety judgements. Nonetheless, the consensus among international safety experts is that, if the safety elements and components above are rigorously followed, nuclear facilities can and will be operated safely.[5,6] It is the responsibility of the regulator to continually monitor and assure that the safety elements and components are followed.

5. IAEA (2006), *Fundamental Safety Principles*, IAEA, Vienna.

6. American Nuclear Society (2000), *ANS Position Statement on Reactor Safety*, ANS, USA.

3. MEASURING SAFETY

One of the fundamental challenges that any regulator faces is deciding how to measure[7] the safety elements described in Chapter 2, in order to be satisfied that any particular facility is being operated safely. In meeting this challenge, the regulator must recognise that there is no direct means of measuring the current level of safety at a given facility, nor are there reliable indicators to predict future safety performance. Regulators generally rely on a combination of past experience, sound engineering judgement and risk-based insights to identify a number of safety artefacts which can be used to obtain information about each of the safety elements. This information is then collated and analysed to gauge the integrated safety performance of the facility. The relationship between safety elements, safety components and safety artefacts is shown in Figure 1.

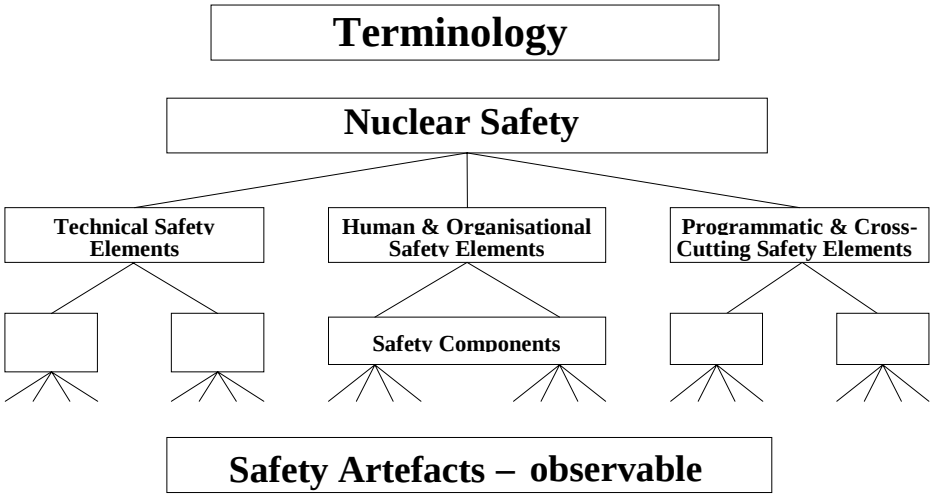


Figure 1: Relationship between safety elements, safety components and safety artefacts

7. In this report the term "measure" includes qualitative as well as quantitative assessments.

The important point is that safety artefacts are the directly observable aspects of the various safety elements and components. They include such things as:

- safety performance indicators;
- inspection findings and observations;
- event findings;
- test results and findings;
- assessment results and findings;
- maintenance results and findings;
- training results, quality and programmes;
- documentation quality and completeness;
- human resources and qualification;
- organisational commitment to safety;
- prompt and accurate responses to regulator's requests.

Some of these artefacts are more quantifiable than others but they all give valuable information to the trained regulator.

Each regulator has to develop its own suite of safety elements, components and artefacts, depending on national circumstances and safety approaches. Clearly it must have a sufficiently competent and experienced staff to be able to comprehend the significance of each piece of safety information and reach a judgement about its implications for the overall safety of the facility. In addition to the normal sources of safety information described above, the regulator's assessment systems should be able to integrate outside information as well. Examples of outside information include foreign operating experience, relevant non-nuclear experience, seismic and severe weather experience, and even anonymously provided information. The regulator's internal systems must be integrated properly so that information passes quickly and accurately between different parts of the organisation and the inputs of all relevant inspectors and technical specialists are taken into account in reaching safety judgements.

Traditionally, regulators have monitored a wide spectrum of safety artefacts to gain assurance about the safe operation of any nuclear facility but they have generally relied on the competence and experience of their staff to make qualitative, engineering judgements about the adequacy of the safety

being achieved at the facility. Over the past few years, some regulators have started to devise systems for measuring and recording safety artefacts in a more systematic way in order to provide a more quantitative and transparent assessment of the level being achieved for each of the elements of safety. The aim is to allow the regulator's safety judgements to be made in a traceable way that stakeholders, especially the licensees and the public, can understand.

It has to be recognised that devising and implementing such a systematic approach to safety assurance has significant resource implications for the regulator. The extent of this additional resource commitment should be analysed and evaluated within the regulator's business plan before any final commitments are made. It may be useful for the regulator to begin with a small pilot programme for one or a few facilities, using the resources at hand, while it develops its methodology and internal processes. After perhaps a year's experience using the pilot programme the regulator can decide whether to expand the programme and perhaps request more resources.

Establishing the safety framework

Regulators do not achieve safety. Their responsibility is to observe the level of safety being achieved by the operators, make a judgement about its adequacy and then take any necessary regulatory action. The information available to them can never be fully comprehensive or complete and so an element of regulatory judgement is always necessary. In order to ensure that this judgement is as objective and reproducible as possible, the regulator should set a framework of safety norms and requirements which, if properly implemented, should ensure an adequate level of safety. Some of the techniques for establishing such a framework are:

- *Setting standards and issuing regulatory guides*

  Most regulators have processes for setting nuclear safety standards which guide both the operators and the regulators on the level of safety that should be regarded as the best that is reasonably achievable. The level of detail varies from regulator to regulator, depending on the regulatory approach and national situation. Irrespective, however, of the level of detail in the standards, most regulators recognise the value and importance of issuing regulatory guides to explain fully the expectations for different facilities, phases of operation, etc. The status of such regulatory guides and the extent to which they will be used to measure safety achievements should be made clear to all stakeholders, especially the operators.

- *Promulgating regulations*

  Some regulators promulgate detailed regulations concerning the practical safety requirements for various systems and processes. In most cases these regulations are generic in the sense that they are applicable to all relevant nuclear facilities but sometimes a regulation is issued to deal with a particular safety issue on a specific cadre of facilities.

- *Issuing licences and amendments*

  The ultimate control of any civil nuclear facility is exercised via a licence which normally contains a number of conditions, with which the facility must comply. The licence and its conditions may be amended from time to time to reflect changing safety knowledge or regulatory requirements, or different phases of the facility's life.

Having established the safety framework that the operator is expected to comply with the next step for the regulator is to measure the extent to which the required safety elements are being adequately met within that framework. This is achieved by observing safety artefacts that give information about the components of each safety element. Safety artefacts are observed during:

- *Inspections (including audits)*

  Central to any regulator's attempts to gain assurance that a facility is being operated safely is the need to "go and see". This requires that the regulator must have complete and unfettered access to all nuclear facilities that it regulates. Actual observation of the performance of the facility and the safety attitudes of its staff by trained, critical, professional regulators is vitally important. Inspections are carried out to verify compliance with licence conditions and other regulatory requirements. There are various types of inspections, including:

  1. the programme of routine inspections;

  2. team inspections or audits targeted at specific parts of the facility or specific technical or human issues;

  3. inspections related to changes in the facility's status, such as commissioning inspections, re-start inspections, etc.;

  4. observation of emergency exercise drills;

5. non-routine (or special) inspections aimed at finding the root causes of apparent declining performance, for instance due to safety culture weaknesses.

Experience has shown that the benefits of any inspection are significantly enhanced by detailed pre-planning to establish clearly the safety artefacts to be measured and the success criteria for each such artefact.

- *Regulatory reviews*

  Regulators carry out a number of safety reviews throughout the life of a facility. Initial safety reviews help to identify the safety significant systems, components and procedures that the regulator will expect to monitor during the commissioning and operation of the facility. During the construction, commissioning and operation of any facility there are usually a considerable number of design changes which the regulator will review to ensure that they do not reduce the overall safety of the facility and that their implementation is properly reflected in operating rules or technical specifications. Proper implementation of the original design requirements and all subsequent design modifications on the facility and in the operating rules is an important safety indicator for the regulator. In addition, most regulators now require periodic safety reviews to give an across-the-board assessment of the safety of the facility and its components compared to the design basis. Such reviews provide the operator and regulator with detailed information about any ageing degradation of structures and components, and inform decisions about replacing obsolete equipment. They also give the regulator a wealth of information about how well the facility has fulfilled the safety expectations built into the original design.

- *Enforcing regulatory requirements*

  Operators are legally obliged to comply with all relevant regulations and regulators are responsible for enforcing such regulations. This requires that the quality of safety information provided by the operator to the regulator must be complete, accurate and timely. When a regulation is breached the regulator normally investigates the reasons for the breach and the extent of any deviation from the required level of safety before deciding what enforcement action to take. Such investigations can provide valuable information on both the technical safety of the facility (e.g. what facility defects or deficiencies allowed

the breach to occur?) and the safety culture of the operator's staff (e.g. did they recognise and report the breach themselves or did they wait until the inspector discovered it?). Regulators can get significant insights from an analysis of the frequency and types of any breaches of regulations that occur at any facility.

- *Reviewing operating experience*

  Operating experience is one of the most reliable indicators of the safety of a facility. One of the most important means for a regulator to assess the level of safety at a facility or a group of facilities should be an evaluation of the frequency and severity of actual past operating events that may be precursors of severe accidents. Inspectors use information on such things as number of scrams, unplanned releases of radioactivity and excessive radiation exposures to give them an ongoing indication of the safety of a facility. They may even carry out their own independent review of a facility's operating experience. They also look closely at how well the operator analyses and reacts to his own operating experience and the operating experience feedback (OEF) from other facilities around the world. The accuracy, completeness and timeliness of statutory reporting of abnormal events by the operator are also important indicators of the overall safety of a facility and its operators.

- *Observing attitudes to safety*

  Safety is achieved on a nuclear facility through a combination of engineering excellence in the design, commissioning and operation of the facility, and a positive safety culture that pervades all members of the staff. The latter aspect is at least as important as the former but it is much more difficult to assess. Inspectors may rely on observation of the operator's attitudes to safety and safety information obtained during meetings with licensee's staff, as well as specific periodic surveys of the overall safety culture.

The following activities are essential and effective supports for the regulator in defining and measuring safety artefacts.

- *Carrying out independent safety analyses*

  In some situations regulators may perform or obtain an independent safety analysis of some critical safety indicator. This allows them to

confirm or question the licensee's analysis and helps to establish the criteria for judging what the acceptable level of safety is.

- *Sponsoring safety research*

  Regulators cannot rely solely on the research sponsored by the licensee. They need to have access to independent research in order to:

  a. have an adequate background to ensure that their safety standards are well-founded and correct;

  b. keep their technical competence up-to-date;

  c. be in a position to challenge the licensee's safety arguments;

  d. be able to make informed judgements about the best indicators of safety performance.

Using a combination of the techniques discussed before to measure safety artefacts the regulator accumulates a considerable variety of measurements related to the safety of any facility. Some will be quantitative, such as the number of unplanned scrams in a particular period, while others will be almost completely qualitative, such as the degree of conservatism demonstrated by the operators. Most will have implications for more than one safety element. For all of them the regulator must have access to all relevant information from the licence holder. Any reluctance on the part of the license holder, or the provision of incomplete or inaccurate information, are additional indicators of a poor attitude to safety. Having obtained all available measurements of safety artefacts, the regulatory challenge is then to arrive at an integrated safety judgement from them.

4. MAKING INTEGRATED SAFETY ASSESSMENTS

In Chapter 2 the safety elements were grouped under three headings: technical; human factors and organisational; programmatic and cross-cutting. Using the techniques outlined in Chapter 3, regulators measure a wide range of safety artefacts related to the components of each of these elements. The challenge is then to find a consistent way of arriving at an integrated safety judgement from all this information. There are a number of factors the regulator needs to consider in developing a framework for integrated safety assessments. These factors include:

- *The extent to which the different components of each element of safety are amenable to quantification*

  The most straightforward aspects for the regulator to assess are the components of the technical safety element. For these there will generally be pre-determined levels of acceptability which can be applied immediately to the measured safety artefacts. The levels of acceptable safety are generally defined in the operating limits, technical specifications requirements, etc., that are derived from the facility's overall safety case, and the extent of any failure to meet one of them is immediately obvious when measured information is available. Next come those safety artefacts where it is possible to set minimum requirements in quantitative terms but where there is at least some subjective judgement in assessing the quality of the safety performance. For example, the necessary components of an acceptable emergency plan can be defined quite closely, as well as the numbers of trained staff that are needed to carry it out. While the regulator can readily check whether these are being complied with, the actual state of emergency preparedness of any facility or site can only be deduced from observations of the behaviour and interaction of staff during emergency exercises. Such observations are essentially subjective and provide qualitative safety information. Finally, there are those safety

artefacts which are almost impossible to assess in a quantitative way. These generally relate to human behaviour and include conservative decision making and safety culture.

- *The timeframe over which safety information is obtained*

  The regulator obtains some safety information continuously (from information provided by the operators, from its inspectors, etc.), some on a frequent basis (from the inspector's regular meetings with site management, from facility modification proposals, from emergency drills, etc.) and other information on an irregular, infrequent basis (such as abnormal events, major facility outages or modifications, surveys of staff attitudes/safety culture, etc.). It can be difficult to keep all such information in mind when making a judgement about the level of safety being achieved at any particular time or when attempting to generate meaningful information about safety trends. Clearly a system that records and organises all the relevant information should be of great help in giving the regulator an accurate overall picture of instantaneous and time-trended safety performance.

- *The importance that should be given to each piece of safety information*

  It is evident that different safety artefacts have different levels of importance when it comes to assessing the overall safety of a facility. For example, if a scram occurred because inadequately trained operators went outside the proper start-up envelope it would probably be of much greater concern than the fact that the licensee had cumbersome work control processes. From their technical competence and regulatory experience regulators attach different importances to different types of safety information and this needs to be reflected in any systematic method for collating and assessing safety.

Bringing the different elements together

At any one time, there will typically be thousands of safety artefacts available to the regulator. Some will be historical, relating to the original design, commissioning, construction and previous operation of the facility. Other information will come from:

- current inspections, including audits;

- licensee reports;

- facility modifications and their close outs;
- analysis of operating experience on the facility in question and elsewhere;
- the licensee's record of compliance with the license and relevant regulations;
- the results of regulatory reviews;
- training records and the maintenance of the necessary cadre of suitably qualified and experienced personnel;
- the safety attitudes of the licensee's staff and contractors;
- emergency exercises.

As noted previously, the regulator's integrated safety assessment system should be capable of combining both quantitative and qualitative information in order to provide a basis for the decision-making process.

In some situations the regulator's judgement about the acceptability of safety at a particular facility will be reached quite quickly on the basis of one or a few pieces of safety information. Consider, for example, the situation where, during a periodic inspection on a PWR, a licensee's NDE (non-destructive examination) discovers cracks in the letdown line upstream of the isolation valves where the cracks are greater than the critical size and have grown significantly since the last inspection. In such a situation the regulator is likely to judge that the situation is unsafe and take immediate regulatory action, without waiting for an analysis of all the other available safety information.

In many situations, however, the regulator will have no specific safety information that demands immediate regulatory action but rather will have information on a number of different safety artefacts that do not individually or collectively yield a clear or complete picture of the safety of a facility. For such situations it is important to have an objective way of organising, integrating and assessing all the safety information for a facility (both good and bad) in order to avoid "cherry picking" those artefacts that, for whatever reason, readily attract inspectors' attention. This helps to avoid biased or arbitrary regulatory decisions and also helps with deciding the extent of any required regulatory actions and the priority areas for future regulatory efforts.

A number of regulatory bodies have recently started to develop systematic ways of measuring, recording and analysing safety elements in order to provide a more integrated, complete and transparent assessment of the safety level being achieved. In the Appendix there are descriptions of five systems that have been developed by national regulatory bodies, plus an illustrative model which uses a "traffic light" system to indicate safety performance.

The desirable attributes of all such systems are:

1. They should be *systematic*. This means that they should be able to include all observations in a pre-determined system which assigns each observation to a defined and reproducible safety "box".

2. They should be *comprehensive*. The models should be capable of encompassing the entire spectrum of safety observations obtained within the three groups of safety elements identified in Chapter 2, namely technical, human factors and organisational, and programmatic and cross-cutting.

3. They should be *consistent*. This means that they should ensure that reproducible and predictable results are generated from any one set of data, irrespective of which staff member enters the data or the circumstances (e.g. time) under which the analysis is carried out. Their treatment of quantitative and qualitative information should be compatible and logical. The results should be coherent in terms of the types of facilities involved and the safety trends predicted.

4. As far as possible, they should contain pre-determined *acceptability guidelines* for safety artefacts which should be based on the regulator's requirements and expectations for safety performance. This is an important though difficult and time-consuming aspect of setting up such systems. The basic framework for acceptability derives from the concepts of defence in depth, safety goals and barriers. The five levels of defence in depth have been defined in INSAG-10 (see Footnote 4). Most regulatory bodies have regulations or criteria which attempt to establish acceptability guidelines, while recognising the challenges of dealing with difficult topics such as human errors and events with only a remote probability of occurrence. For certain types of safety information the acceptability guidelines are immediately defined from the safety case in terms of technical specifications or operating rules. For many others, however, the acceptability guidelines can only be arrived at on the basis of the professional judgement of experienced inspectors with a deep knowledge of the facility in question, taking due account of the relevant regulations or

criteria. This implies a requirement for significant involvement of inspectors during the setting up of such systems and their continuing involvement to assess the safety significance of inspection observations and to help judge acceptability guidelines. Defining such acceptability guidelines often entails a regulatory discussion about the necessary margin of safety above some minimum level, as well as what the regulatory expectations should be, based on previous industry performance.

5. It is very useful for the system to be able to generate information about the *trend* of safety performance with time to enable a graded regulatory response.

6. Finally, the system should generate information in a form that helps the regulator to reach *decisions*. It should provide a methodology for analysing the overall safety significance to a degree sufficient for taking graded regulatory actions before an unacceptable level of safety performance is reached.

There are clearly some challenges involved in setting up and operating such an integrated safety assessment system. To begin with, the regulatory body needs to devote significant time and resources to analysing the many different types of safety information that are available to it and the means by which it is obtained. It then needs to identify the criteria of acceptability (where they exist) for each safety artefact and, if possible, the relative importance of each artefact. A special challenge for the regulator is how to assess the non-technical safety elements, particularly safety culture and organisational safety elements. Earlier NEA reports have described methods for the regulator to recognise early signs of declining safety performance and signs of a weak safety culture.[8,9] Finally, the regulatory staff need to reach a consensus on the criteria for applying the system.

After the initial, resource-intensive set-up phase there will be a continuing commitment on all relevant regulatory staff to report their safety information in a way that allows the system to be operated efficiently and effectively. It seems likely that most regulatory bodies would find it appropriate to have a dedicated resource to input the data and prepare the necessary tables. The information in such tables would then help the regulator to take action and set inspection priorities as discussed in the next chapter.

---

8. NEA (1999), *The Role of the Nuclear Regulator in Promoting and Evaluating Safety Culture*, OECD, Paris.

9. NEA (2000), *Regulatory Response Strategies for Safety Culture Problems*, OECD, Paris.

5. IMPLEMENTING AND COMMUNICATING INTEGRATED SAFETY ASSESSMENTS

In a previous booklet on nuclear regulatory decision making it is stated that, in meeting the goals of technical soundness, consistency and timeliness, the regulator should be guided by an integrated framework for making decisions.[10] Most regulatory decisions relate to or flow from the regulator's fundamental goal of assuring nuclear safety and should be based on a systematic and comprehensive assessment of all the safety elements.

Chapter 4 discussed the main attributes of any systematic method for handling the many safety artefacts that the regulator needs to consider when reaching an integrated safety judgement. The major benefits of using such a system are that it allows the regulator to have a comprehensive, balanced and transparent picture of the state of safety of a facility and facilitates an instant comparison with previous assessments.

The results of any systematic method will normally be presented in a tabular form which identifies where the weak areas of safety performance lie and shows whether safety performance has improved, deteriorated or remained constant since the last assessment. Where the table(s) point to some general area of weakness, such as human factors, the regulator will normally go back to the more detailed tables to identify which particular safety components had been assessed as less than satisfactory. Discussions amongst regulatory staff, supplemented by reference to the relevant safety artefacts, then assist management to determine what actions need to be taken and on what timescales.

There will, of course, be situations where very rapid regulatory action is called for, e.g. where one or more of the safety elements is clearly unacceptable. Consider, for example, the integrated safety assessment that might be generated for a facility that had suffered a significant, uncontrolled leakage from its secondary coolant system due to a long-standing corrosion problem that had been missed by the in-service inspection programme and the negligence of the operators. Clearly this would call for immediate regulatory action, especially if the facility had other signs of a poor safety culture or other unsatisfactory organisational factors. It might also result in the regulator reviewing its own systems to see whether lessons needed to be learned about the efficiency and

10. NEA (2005), *Nuclear Regulatory Decision Making*, OECD, Paris.

effectiveness of its procedures. Nevertheless, even in those situations where immediate action is needed a systematic decision-making framework will benefit the regulator by fostering consistency and efficiency.

All regulatory decisions should be based on the accumulation of systematic, recorded evidence. Normally, the regulator would generate an integrated safety assessment table for each nuclear facility showing, where relevant, the trend of different safety elements with time. In evaluating the significance of this integrated assessment the regulator will ask itself questions such as, “Do we understand the basic reasons why a safety element assessment has changed from satisfactory to marginal or even unsatisfactory?” and “Do we understand why an assessment continues to show marginal or unsatisfactory – that is, why do the operator’s corrective actions appear not to be effective?”.

The outcome of the systematic analysis helps to inform the regulator’s decisions on such things as:

1. the need for enforcement action to ensure compliance;

2. the assessment and inspection priorities for the facility in the next time frame;

3. any industry-wide regulatory initiatives to deal with emerging safety issues or to set an example for all licensees of the consequences of becoming complacent and allowing operational safety to slip below acceptable levels;

4. the need for additional research and safety studies;

5. the need to transmit safety improvement lessons to other facilities and other regulators;

6. the need to transmit lessons to the wider international regulatory community.

Whatever actions the regulator decides to take should be recorded properly and communicated to the operators and other stakeholders, as appropriate. This is an important step in ensuring that the stakeholders have confidence and trust in the regulator's technical competence, integrity and sound judgement.[11]

The stakeholders with a legitimate interest in nuclear regulatory activities are discussed in the NEA booklet on improving nuclear regulatory effectiveness[12] and include: the general public, nuclear licensees, Government departments and agencies, national and international bodies concerned with nuclear power, and concerned action groups.

There is a wide variation among these stakeholders in their level of technical sophistication and understanding of the technical details underlying the regulator's safety judgements. As a consequence the regulator must give careful thought to the challenges of communicating complex safety issues. A special challenge is how to deal with issues that may be of low public health risk but that are of high public concern, such as tritium leakage to groundwater or other small radioactivity releases to the environment.

Some principles the regulator should follow in communicating its safety judgements are the following:

a. Strive for openness, completeness and transparency in giving the full story of the safety issues involved, the basis for the regulatory judgement about them, and what is being done to resolve them. Often it is useful to give a plain language summary that is stripped of technical jargon that may not be intelligible to a general audience.

b. Explain the regulator's conservative safety philosophy, in particular the defence in depth philosophy that requires multiple barriers to protect the public against radiological harm.

c. Give a straightforward, objective technical assessment of the nuclear safety issues involved, trying to achieve a balance which avoids either minimising the safety problems or being unduly alarmist in describing them. If relevant, refer to regulatory acceptability criteria for the elements of safety involved and explain the extent of any deviations from them.

---

11. NEA (2006), *Building, Measuring and Improving Public Confidence in the Nuclear Regulator*, OECD, Paris.

12. NEA (2001), *Improving Nuclear Regulatory Effectiveness* OECD, Paris.

d. Invite licence holders to give their assessments of their own safety performance.

e. Discuss and, if possible, reconcile any differences in perception of performance but, in any case, do not make excuses for weaknesses or misconduct on the part of the licensees.

f. Explain clearly how the regulator and the licensee are separately taking actions to resolve any safety issues.

g. Acknowledge where the regulatory body itself has learned lessons on how it can handle safety issues better in the future.

There are various means for communicating the regulator's safety judgements. The fundamental document is the regulator's record of its safety decision and its basis, produced according to the regulator's standard procedures. This may be made public and may be accompanied by a press release summarising the decision in plain language for a broad audience.

In preparing the written decision on its final safety judgement, the regulator should consider and answer the following questions in order to reassure stakeholders:

- Were normal procedures followed?
- Is there a clear legal basis for the decision?
- Is there a clear safety basis for the decision?
- Were all relevant stakeholders' views considered?
- Was due diligence used in gathering necessary information?
- Is the decision consistent with earlier precedents?

The advantage of having the available information organised in a systematic way, as discussed in the previous chapter, is that it not only allows a balanced, reproducible regulatory decision to be reached but it also gives a sound basis for providing answers to the above questions which are fundamental to reassuring stakeholders.

6. SUMMARY AND CONCLUSIONS

This report addresses the fundamental question facing all nuclear regulatory bodies, “How can the regulator judge whether its actions are actually assuring an acceptable level of safety at nuclear facilities?”

After establishing the broad understanding of nuclear safety to be used in this report, the synthesis of worldwide experience regarding the elements of safety was presented in three broad categories: Technical; Human factors and organisational; and Programmatic and cross-cutting. This was followed by a description of the activities a regulatory body undertakes to measure the detailed components of the various safety elements.

The necessary attributes of any systematic method for organising and evaluating the large amount of safety information available to the regulator are described in detail, followed by a discussion on how a regulator might use this comprehensive assessment information to arrive at the integrated safety judgements that are of vital importance in deciding regulatory actions and setting priorities for future regulatory activities.

Finally, the report discusses the importance of openly communicating the regulator’s safety judgements and suggests some principles for doing so.

The ideas and suggestions in this report cannot be viewed as a rigid formula for all regulators to follow. Indeed it is clear that, while a formal systematic approach is desirable, it is not a necessity for achieving effective and efficient regulation. It has to be recognised that the output of any systematic approach is only as good as the data fed into it and regulators should avoid giving the impression to their staff or stakeholders that it provides a magic formula for assessing safety. Sound safety decisions will continue to rely heavily on the experience, wisdom and good judgement of the regulator’s staff.

However, experience shows that there are clear benefits in having in place a systematic process for collecting and analysing safety information. Not only does it help the regulator to make integrated judgements about the acceptability

of safety at the nuclear facilities it regulates but it also gives a sound basis for communicating and defending its decisions in a transparent way, thereby improving stakeholder confidence. Additionally, it informs future regulatory priorities, facilitates feedback to inspectors, helps promote regulatory consistency and assists knowledge management and knowledge transfer to new inspectors.

When a regulatory body decides to develop such a systematic approach to assist its decision making, it will need to tailor the methodology to be consistent with its national laws, requirements and procedural traditions. Establishing a workable approach will involve a considerable initial resource commitment, followed by a lower-level, but still significant, continuing resource commitment to ensure the system functions effectively and efficiently.

Appendix

DESCRIPTIONS OF SOME INTEGRATED SAFETY ASSESSMENT SYSTEMS

A. Introduction

This Appendix gives a brief description of the main features of five different national integrated safety assessment (ISA) systems. The five ISA systems are broadly consistent with the principles and attributes discussed in this report, but the details of how the systems work are, of course, very different. There is no single right answer for how an ISA system should be developed and implemented. Each regulatory body has to develop its own system based on its national laws, regulations and safety practices. In order to assist regulators, an illustrative system has been developed, based on the three groupings of safety elements defined in Chapter 2, which uses a "traffic light" system to indicate the acceptability of different pieces of safety information. This illustrative system is described at the end of the Appendix, though it has to be recognised that much more development and analysis would be needed before it could be applied in practical situations.

B. National integrated safety assessment systems

1) The system of the Swiss Federal Nuclear Safety Inspectorate (HSK)

Additional information can be obtained by going to: www.hsk.ch

HSK has implemented an integrated safety assessment system for nuclear power plants (called an integrated oversight process) that generally meets the attributes described in this report. The sources of information used in this assessment are inspections, operator licensing data and event analysis data. In the future they plan to include information from licensee reports, safety indicators (i.e. PIs) and insights from plant modification authorisations.

The basic idea behind this system is to assess the design, the operational requirements and operational experience. The assessment of the requirements

includes a thorough check to see if the applied design requirements are still valid in the light of the latest information from research and worldwide operational experience. Another purpose of the assessment is to check if the operational requirements (technical specifications, check lists, operational handbook, emergency guidelines, etc.) correctly reflect the allowed operational regime; if test procedures are complete and steps in the procedures are safe and in the correct order; and if the emergency guidelines are safety goal oriented. Operational experience is assessed by comparing it with operational requirements. Technical aspects are distinguished from human/organisational aspects to recognise that safety is not only dependent on the correct technical design and its implementation but also relies on the correct work of operational and maintenance staff.

To judge the safety importance of the requirements and the operational experience, each aspect is assigned to the corresponding levels of the defence in depth concept, to the corresponding barriers and to the corresponding safety functions. This systematic approach results in a two-dimensional matrix as shown in Table 1. For each NPP, each data point which is based on inspection or assessment findings, on event analysis, etc. is assigned to one of the cells of this table.

The causes of each finding have to be carefully analysed. Experience shows that very often an observation or finding is caused by a number of different contributing factors. Quite often, both technical and human/ organisational aspects play a role. In addition, a technical or human/ organisational aspect can affect more than one level of the defence in depth or more than one barrier or safety function at the same time. Therefore each observation or finding can be assigned to one or several cells in the safety matrix.

The systematic safety assessment system is not only a process that defines how each data point contributes to plant safety; the structure also defines what kind of information has to be gathered to get a complete picture.

Findings are rated on a scale that is based upon the international nuclear event scale (INES). The goal of the scale is to assess all levels of safety performance from good practice to severe accidents on one single scale. The categories are defined as follows:

- **Category G: Good practice**

  All requirements are fulfilled and the practice of other NPPs is clearly exceeded.

- **Category N: Normality**

  All requirements are fulfilled.

- **Category V: Need for improvement**

  Deviations from requirements in documents that do not need formal authorisation by the Swiss Federal Nuclear Safety Inspectorate fall into this category.

- **Category A: Deviation**

  Deviations from normal operation within operational limits and conditions.

- **Categories 1 to 7**

  Rating according to the INES-Manual.

Categories V and A correspond to INES 0. Findings from inspections falling into categories A or higher will be treated as events. Any finding V and higher requires action.

The overall evaluation of the ratings is a resource intensive process whereby each rating (particularly negative ratings) are cross-validated by independent staff and qualitative judgements are made for the sum of the results for design requirements, operational requirements, plant behaviour and human and organisational behaviour. Senior regulatory managers review these quantitative and qualitative ratings and arrive at an overall judgement on the safety performance of the plant being assessed. HSK produces an ISA for each reactor plant annually, and the results are used as a basis for annual reports to the national legislative body as well as for a guide for future inspection plans.

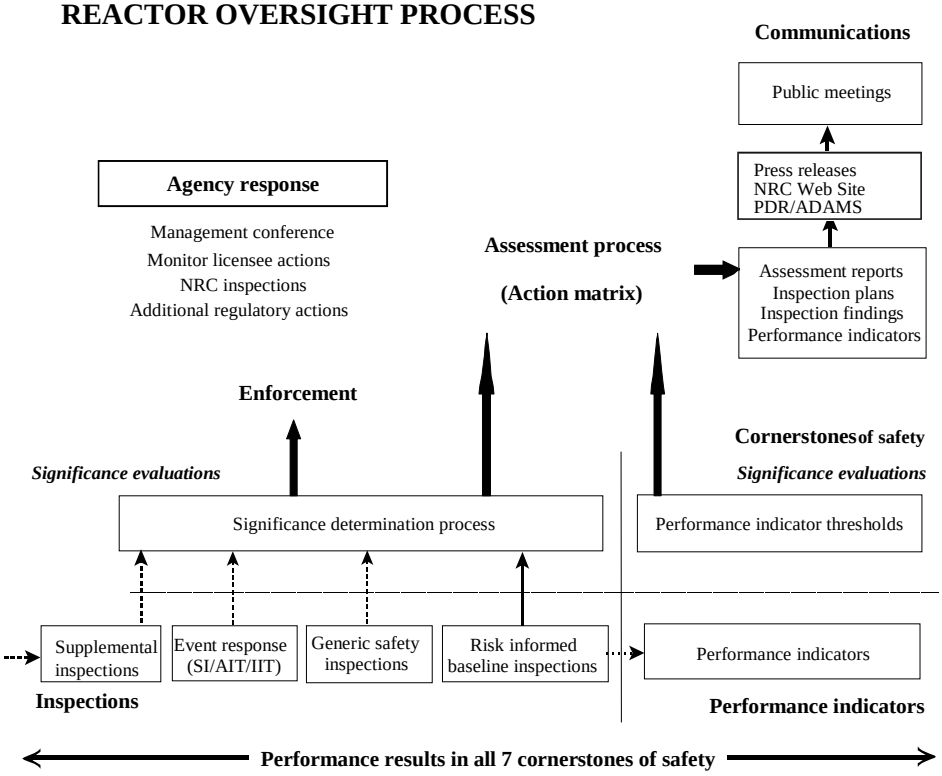
The following table shows the safety matrix used for safety assessment.

Goals \ Subject		Requirements		Operational experience	
		Design requirements	Operational requirements	State and behaviour of the plant	State and behaviour of man and organisation
Safety functions	Controlling reactivity				
	Cooling the fuel				
	Confining radioactive materials				
	Limiting exposure to radiation				
Levels of defence in depth	**Level 1** Prevention of abnormal operation and failures				
	Level 2 Control of abnormal operation				
	Level 3 Control of accidents within the design basis				
	Level 4 Control of severe plant conditions				
	Level 5 Mitigation of the radiological consequences of significant external releases				
Barrier integrity	Fuel integrity				
	Integrity of the primary cooling system boundary				
	Containment integrity				
Overall safety	Multiple level aspects				

2) The system of the United States Nuclear Regulatory Commission (reactor oversight process)

Additional information can be obtained by going to: www.nrc.gov

REACTOR OVERSIGHT PROCESS



US NRC's reactor oversight process (ROP) for nuclear power plants is an integrated safety assessment process that generally meets the attributes described in this report. It is a risk informed and performance based system founded on the premise that NRC's safety mission is composed of three strategic performance areas – reactor safety, radiation safety and safeguards. These qualitative strategic performance areas are made up of seven measurable safety cornerstones: (1) initiating events, (2) mitigating systems, (3) barrier integrity, (4) emergency preparedness, (5) occupational radiation safety, (6) public radiation safety, and (7) physical protection. These safety cornerstones are not congruent with the safety elements and components in this report but are consistent with them.

Each of the cornerstones has associated objective performance indicators (PIs) such as unplanned reactor shutdowns, safety system failures, effluent releases, etc. The PIs, which are compiled and reported regularly by the operators, use a colour-coded system to display safety performance, and they are fed into an action matrix as inputs to NRC's semi-annual plant assessment process.

A parallel source of information for the plant assessments is the findings from regulatory inspections. There are two basic paths for evaluating inspection findings. The first path is for the inspection staff to assign safety significance to each inspection finding. There is formal guidance to enable the inspectors to determine if the finding is greater than minor. If so, the finding is screened through a significance determination process and the resultant findings are assigned a colour-coded rating. Those findings initially given a safety significance rating greater than green are subjected to a separate review by a Significance and Enforcement Review Panel. In a second path the NRC staff looks for cross-cutting issues, so named because they affect, and are therefore part of, each of the cornerstones. The three ROP cross-cutting issues are human performance, management attention to safety and workers' ability to raise safety issues (safety-conscious work environment), and finding and fixing problems (problem identification and resolution). In addition to these three cross-cutting issues and their associated cross-cutting aspects, the NRC believes account-ability, continuous learning environment, organisational change management, and safety policies make up the final components of a licensee's safety culture.

All of this information, namely the objective performance indicators, cross-cutting safety trends, risk informed inspection findings and results from other complementary plant evaluation processes such as operating experience evaluations and accident sequence precursor evaluations, is fed into NRC's assessment process, the action matrix.

The action matrix describes a graded approach in addressing performance issues, such that NRC becomes more engaged as licensee performance declines. At lower levels of safety concern the licensee is encouraged to address its problems through its corrective action programme. At higher levels of safety significance of inspection findings or longer duration of substantive cross-cutting issues, NRC actions become more intrusive. These actions could include additional inspections, a demand for information, a confirmatory action letter or issuance of an order modifying the licence, which could include a plant shutdown.

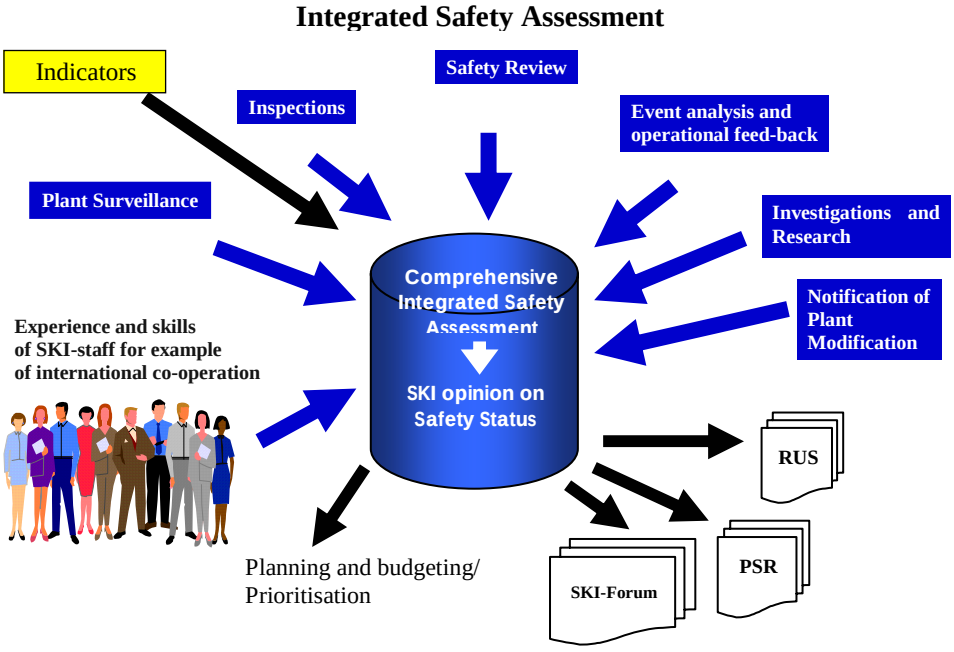
NRC's reactor oversight process is characterised by highly formalised procedures for collecting and evaluating safety information. In particular, the

action matrix assessment process has procedures and guidelines outlining what regulatory actions are to be taken under a given set of circumstances. Nonetheless, the process is not so rigid that it eliminates the judgement of experienced senior regulatory staff and managers in deciding what regulatory actions are appropriate for each licensee.

3) The system of the Swedish Nuclear Power Inspectorate (SKI)

Additional information can be obtained by going to: www.ski.se

SKI conducts an annual integrated safety assessment (called SKI-Forum) for reactor plants it regulates using a process that generally meets the attributes described in this report. The sources of information used in this assessment are plant surveillances, inspections, performance indicators, safety reviews, operating experience evaluations, research results and special investigations. These are supplemented by input from experienced SKI staff. In addition, SKI requires a 10-year periodic safety review for each plant that addresses a broad range of safety issues, including detailed safety analyses of structures, systems and components, such as pressure vessel integrity.



RUS: Annual Safety Report - PSR: Periodic Safety Review - SKI-Forum: Annual Safety Evaluation

SKI uses these sources of safety information to evaluate performance in the following 15 areas:

1. design and construction;
2. management and organisation;
3. competence and staffing;
4. operation and deviations in barrier and defence in depth standards;
5. core and fuel issues;
6. emergency preparedness;
7. maintenance and material control;
8. safety review;
9. experience feedback;
10. physical protection;
11. safety analyses and documentation;
12. safety programme;
13. plant documentation procedure;
14. fuel and waste handling;
15. safeguards.

These 15 safety areas are not congruent with the safety elements and components in this report but are consistent with them, except for the areas of radiation safety and environmental protection for which SKI does not have regulatory responsibility.

SKI analyses the sources of safety information for safety significance using both physical barrier safety standards (fuel, cladding, primary systems, containment and buildings) and defence in depth safety standards. A document covering the 15 safety areas is prepared by the inspection staff and is reviewed

by expert regulatory staff and managers. The final assessment is approved by senior regulatory managers and is discussed with the respective plant management shortly after each SKI-Forum.

The results of the integrated safety assessment are used as a basis for SKI's annual report to its national legislative body as well as for SKI's internal planning, budgeting and prioritisation process.

Based on recent experience SKI is continuing to refine and improve the integrated safety assessment process.

4) The system of the Canadian Nuclear Safety Commission (CNSC)

Additional information can be obtained by contacting:
info@cnsc-ccsn.gc.ca

The Canadian Nuclear Safety Commission (CNSC) has implemented a licensee oversight process for the evaluation of licensee safety performance and the allocation of regulatory resources based on risk. The philosophy behind this process assigns the prime responsibility for safety to the licensee and the oversight function, which ensures that the licensee adequately discharges this responsibility, to CNSC staff. In order for the Commission Tribunal to issue a licence, proponents must demonstrate in their application that they have in place a standard set of programmes and processes which will provide adequate protection to the environment, and the health and safety of workers and the public.

CNSC staff assesses overall licensee performance using a comprehensive set of safety areas, programmes, and review factors and assigns grades (from A through E) to rate each safety area and programme. The Report Card requires integration of information from all activities related to the licensed activity. Supplemental information from ongoing regulatory compliance activities is used to update the ratings.

Evaluation of licensee performance in the safety areas and programmes is integral to the CNSC planning process. This involves linking of licensee performance to regulatory work plans for each facility on an annual basis.

The CNSC rating system consists of five categories: "A-Exceeds requirements", "B-Meets requirements", "C-Below requirements", "D-Significantly below requirements", and "E-Unacceptable". The assessment process collects information from the compliance programme, the licensing and authorisation activities, event analysis and performance indicators such that a

comprehensive picture of safety performance can be obtained. The safety areas and corresponding programmes are:

SAFETY AREAS	PROGRAMMES
1. Operating performance	1.1 Organisation and plant management
	1.2 Operations
	1.3 Occupational health and safety (non-radiological)
2. Performance assurance	2.1 Quality management
	2.2 Human factors
	2.3 Training, examination, certification
3. Design and analysis	3.1 Safety analysis
	3.2 Safety issues
	3.3 Design
4. Equipment fitness for service	4.1 Maintenance
	4.2 Structural integrity
	4.3 Reliability
	4.4 Equipment qualification
5. Emergency preparedness	5.1 Emergency preparedness
6. Environmental performance	6.1 Environmental management systems
	6.2 Effluent and environmental monitoring
7. Radiation protection	7.1 Radiation protection
8. Site security	8.1 Site security
9. Safeguards	9.1 Safeguards

Permanent CNSC site inspectors perform system inspections and audits according to the preplanned annual inspection programme derived from the compliance programme. This programme includes both baseline and augmented inspections for areas of licensee performance which have been identified as not

meeting regulatory requirements. Results are transmitted formally to the licensee and if necessary, corrective actions with target dates are followed up through the CNSC enforcement programme.

The CNSC has developed a set of 17 safety related performance indicators. These indicators are used to benchmark acceptable levels of operational safety. The indicators allow tracking of operational trends important to safety and performance comparisons between stations. These indicators are also used to identify potential problem areas where CNSC staff can redirect regulatory resources to determine whether a safety issue exists.

Analysis of safety significant events is the third component used in evaluating the safety performance. CNSC staff reviews all unplanned events and inputs the information from event reviews into a central tracking database. In addition, CNSC staff carries out detailed independent reviews of the most significant events to ensure that licensee root-cause analysis processes are robust.

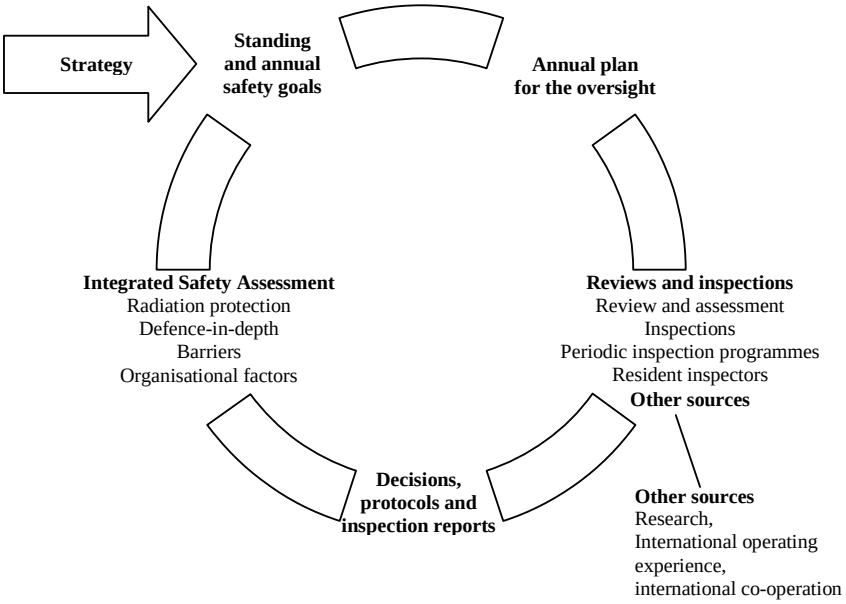
An annual report on the industry safety performance presents the integration of information gathered through CNSC staff assessment activities. The annual report also presents the report card which gives the graded performance of each licensee in the aforementioned safety areas and programmes. The annual report makes comparisons where possible, shows trends and averages and highlights significant issues that pertain to the industry at large.

5) The system of the Finnish Radiation and Nuclear Safety Authority (STUK)

Additional information can be obtained by going to: www.stuk.fi

STUK produces an annual integrated safety assessment for all operating nuclear power plants and plants under construction that it regulates using a process that generally meets the attributes described in this report. The five broad sources of information used in this assessment are (a) oversight of construction and modifications, (b) safety assessments and analyses, (c) oversight of operations, (d) oversight of management, and (e) nuclear safety indicators (PIs). In addition, STUK requires a 10-year periodic safety review that presumably includes more detailed safety analyses of structures, systems and components, such as pressure vessel integrity. The figure below shows that the observations and findings from these sources of information are used in preparing the integrated assessments.

Oversight of Finnish Nuclear Power Plants



STUK FUNCTIONS FOR THE OVERSIGHT OF NUCLEAR POWER PLANTS
Oversight of new plant projects and plant modifications • Changes at the nuclear facility
Safety assessments and analysis • Deterministic safety analysis • Probabilistic safety analysis (PSA) • Safety performance indicators; analysis and feedback
Oversight of operations • Compliance with technical specifications • Incidents • Oversight of outage management • Maintenance and ageing management • Fire protection • Radiation protection • Emergency preparedness • Physical protection
Oversight of management in regulated organisations • Safety management • Management systems and quality management (QM) • Training and qualification of staff • Use of operational experiences • Event investigation • Nuclear liability • Inspection and testing organisations
Oversight of nuclear waste management and nuclear materials • Safeguards of nuclear materials • Nuclear waste management • Control of radioactive materials transport • Licensees for the nuclear materials and nuclear waste

STUK analyses the sources of information and tests the results against radiation protection standards, defence in depth standards, barrier protection standards, and organisational factors. The ISA does not include analyses of emergency preparedness, waste management or nuclear material issues.

The process owners on the STUK staff are responsible for preparing and reporting the results of the assessment of their area of responsibility. The results of the ISA are used as a basis for STUK's annual report to the government.

STUK is continuing to develop its method for making integrated safety assessments in the areas of (a) breadth of coverage of the assessments and (b) methods for handling the safety observations and findings.

C. An illustrative ISA system

One possible approach to making an integrated safety assessment for nuclear power plants would be to use the three groups of safety elements identified in Chapter 2, assigning each safety artefact to one or more of these 3 groups. Each safety artefact could be given one of three possible colours: green, if the result is completely acceptable; amber, if it is questionable or on the margins of acceptability; and red, if it is clearly unacceptable.

This illustrative ISA system is based on the premise that the safety elements are comprehensive, and therefore every piece of safety information (or safety artefact) must fit somewhere in the matrix of safety element components. Frequently, a safety artefact will be relevant to two or even three of the broad safety elements – technical; human factors and organisational; programmatic and cross-cutting.

For example, if an unplanned scram were the result of a maintenance technician's error during a surveillance test, there would likely be no assessment for the technical safety element, but there could be assessments relative to worker qualifications, maintenance procedures and management oversight in the human factors and organisation safety element. Similarly, there may be assessments relative to training, safety culture and quality assurance in the programmatic and cross cutting safety element.

If, on the other hand, the scram resulted from failure of an electronic component, a careful analysis may find contributions from one or more of the following: design weaknesses, poor engineering analysis of replacement parts, inadequate maintenance procedures, inadequate management guidelines on preventive maintenance, inadequate surveillance testing procedures, inadequate

analysis of operating experience with similar components, inadequate ageing management programme, safety culture issues and quality assurance (QA) programme weaknesses. Thus, this single safety artefact could have implications that affect all safety elements. This discussion holds true for every safety artefact that the operator or regulator must consider in this integrated safety analysis system.

Clearly, the effectiveness of this ISA system depends strongly on the quality and thoroughness of the analyses of each safety artefact. A strength of this ISA system is that it forces the operator and regulatory safety analysts to think broadly in terms of the root causes and contributing causes of the safety artefact and how these causes may be related to the entire range of safety elements and components. It is through this broad thinking that hidden (or secondary) safety weaknesses may be revealed.

Table 1 illustrates the approach for the technical safety element. It includes a column allowing the regulator to give each safety component an importance weighting. There is then a column in which the requirements for an acceptable level of safety are specified. For some aspects there would be pre-determined performance indicators to compare against while others might have acceptability guidelines derived by the regulator from past experience and technical judgement. This is followed by a column in which the actual safety performance is given. After that there is a column which shows the status in the "traffic light" system. It would also be useful to have one or more further columns, indicating the status of the safety components at the time of the last and earlier assessments in order to display performance trend information.

The overall status of each component of the technical safety elements would be arrived at by a synthesis of the information from all the relevant safety artefacts. This would nearly always be a matter of judgement for the regulator and would involve the relative importance of each safety artefact as well as its status colour. Naturally, the occurrence of one or more "red" boxes would warrant immediate regulatory action. Having arrived at a status colour for each of the safety components there would then a further synthesis, involving regulatory discussion of the relative importance of each safety component, to generate an overall status for the technical safety elements.

Table 1 – Technical Safety Elements

Safety component	Relative importance	Acceptability criteria	Operational achievement	Status	Previous status
Number of unplanned scrams					
Primary coolant chemistry within specification					
Compliance with technical specifications					
Availability of safety equipment					
Test results					
Plant modification procedures closed out					
Etc.					
Overall status				Red, amber or green	Red, amber or green

The same procedure would then be applied to each of the other two safety element areas, arriving at an overall safety status for each. The three groups would then be grouped together, as shown in Table 2, to give the regulator an integrated safety assessment of the facility.

Table 2 – Integrated safety assessment for facility X

Safety element	Previous status	Current status
Technical	Green	Green
Human factors and organisational	Amber	Amber
Programmatic and cross-cutting	Green	Amber
Overall	Green	Amber

The overview table should help the regulator to establish safety trends and set priorities while the information in the subsidiary tables should assist in identifying individual safety issues that require regulatory attention. The major benefits of such a system are that it allows the regulator to have a simple visual picture of the state of safety of a facility and facilitates an instant comparison with previous assessments.

For example, the first thing the information in the above table tells the regulator is that the overall safety of the facility has deteriorated since the previous assessment. It identifies that the technical safety element is satisfactory but the human factors and organisational safety elements has not improved since the previous assessment while the programmatic and cross-cutting one has deteriorated. At this point the regulator would go back to the detailed tables to identify which particular safety components are assessed as less than satisfactory. Discussions amongst relevant regulatory staff would then assist management to determine (preferably by means of a formal decision-making process) what actions needed to be taken and on what timescales. These proposed actions would then be recorded and transmitted to the operators and other stakeholders, as appropriate.

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