# Three decades of nuclear safety

*Nuclear plant safety has not been a static concept*

**by Pierre Tanguy**

The safety of nuclear power plants has become the focus of the international nuclear community since the Chernobyl accident in 1986. Much has been accomplished in the last 30 years with the IAEA playing a central role in the evolution of safety practices.

Historically, *The Technology of Nuclear Reactor Safety* provides some decisive views in this field, particularly on accidents.* A quotation from the general conclusions of an accident in January 1961 at the 3-megawatt test reactor SL1, has been mentioned several times since Chernobyl:

*"Most accidents involve design errors, instrumentation errors, and operator or supervisors errors. The SL1 accident is an object lesson on all of these. There has been much discussion of this accident, its causes, and its lessons, but little attention has been paid to the human aspects of its causes. There is a tendency to look only at what happened, and to point out deficiencies in the system without understanding why they happen; why certain decisions were made as they were. Post-accident reviews should consider the situation and the pressures on personnel which existed before the accident...."*

That assertion is still relevant today and can help us address current safety issues.

The basic idea for this article is based on the first page of that book, where the evolution of nuclear power is described as occurring over 10-year periods.

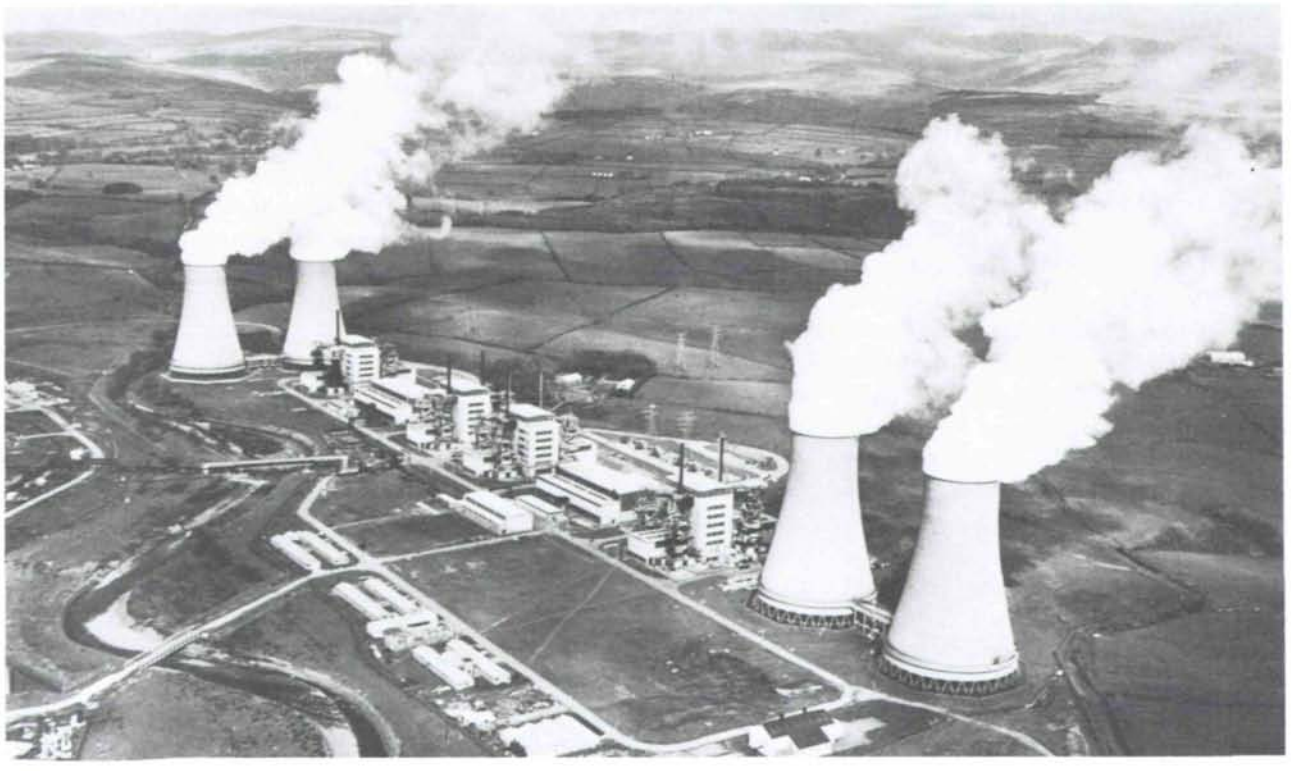
The concept is a good one, as each 10-year period can be characterized by a major emphasis on specific safety aspects. A limited number of safety-significant events could well mark the end of such a period and the beginning of a new era for safety development. It is clear that

---

Mr Tanguy is Inspector General, Sûreté et Sécurité Nucléaires, Electricité de France (EDF), Paris. His article is adapted from an oral presentation at the IAEA in 1987.

* Published by the Massachusetts Institute of Technology Press (1964), edited by Thomson and Beckerly.

**Calder Hall, the world's first large-scale nuclear power station, was officially opened in 1956 at the Windscale Works in Cumbria, UK. (Credit: UKAEA)**



**Safety features are key elements in the design of nuclear power plants. (Credit: UKAEA)**

1979, the year of the accident at Three Mile Island (TMI) and 1986, when the Chernobyl accident occurred, are such reference points. The establishment of the IAEA in 1957 is another landmark.

### "Pre-history" of safety

In 1947, the first event of safety-significance was selected by David Okrent in his book *Nuclear Reactor Safety on the History of the Regulatory Process*. It is used as the starting point of the chapter on historical background in *The Technology of Nuclear Reactor Safety:*

*"At its first meeting in 1947, The Reactor Safeguards Committee considered the first proposal for a contained reactor. From that time on containment for protection of the general public has played an important role in reactor safety in the United States."*

It is still today one of the central issues in reactor safety assessment.

In fact, the history begins earlier, as the book notes:

*"Safety has been an important consideration from the very beginning of the development of nuclear reactors. On 2 December 1942 shortly before the reactor was expected to reach criticality, Fermi noted the mounting tension of the crew. To make sure that the operation was carried out in a calm and considered manner, he directed that the experiment be shut down and that all adjourn for lunch. With such leadership in safety at the very beginning, it is no wonder that the operation of reactors to date (in 1964) has been singularly free of mishaps."*

Perhaps we lack the safety culture of such a supervisor in many plants, since such a large fraction of so-called abnormal occurrences happen during startup after a shutdown period for refueling or maintenance. This is the time when the desire to get the plant on line as soon as possible prevents the people in charge from stopping when they experience minor difficulties, before they get into more serious trouble.

It is coincidence that in 1957 the Windscale accident occurred, with the first, and until Chernobyl, the only one of its time, large-scale radioactive release into the environment: 20 000 curies of iodine. This accident and its potential long-term consequences has been the subject of renewed debates since Chernobyl.

WASH-740 was the first report which gave an evaluation of the maximum consequences of a severe uncontained accident. It became the basis for the liability limits to be included in the Price Anderson Act, which defines the provisions for insurance of nuclear power plants in the United States.

There was a revised version of this report many years later in 1966, but it was not as well known. WASH-740 represented the main reference on what could be the consequences of a very severe nuclear accident until the Rasmussen report (in 1975), and until Chernobyl.

According to Okrent, in the first years, safety priority was on design features, and little attention was given to the other stages — construction and operation. The US Atomic Energy Commission (AEC) issued a first version of the general design criteria in 1965. But the second version of 1967, after discussion with the Advisory Committee for Reactor Safety (ACRS), incorporates important aspects which are still relevant today. The issuance of these criteria represents a decisive step in the deterministic approach of safety. It is a coincidence that, in that same year, the idea of probabilistic safety assessment (PSA) was introduced for the first time in an international meeting in Vienna, Austria. The development of that idea has been extensive.

Before 1957, safety had not reached full recognition, independent from nuclear developments. That was obtained later. Therefore, "pre-history" is a suitable term. Safety was already a primary concern for organizations involved in the development of the peaceful uses of nuclear energy but not fully autonomous. In his paper "Progress in Nuclear Safety", François Cogné mentions that, in the first two Geneva conferences in 1955 and 1958, there was no specific session devoted to safety.* Three important safety developments occurred during the pre-history period in the USA. David Okrent considers that the first official statement on the AEC safety philosophy was made in 1953 by Edward Teller, former chairman of the Reactor Safeguards Committee:

*"In the popular opinion, the main danger of a nuclear pile is due to the possibility that it may explode. It should be pointed out, however, that such an explosion, although possible, is likely to be harmful only in the immediate surroundings and will probably be limited in its destructive effects to the operators. A much greater public hazard is due to the fact that nuclear plants contain radioactive poisons. In a nuclear accident, the poisons may be liberated into the atmosphere or into the*

* Paper in French, in *Revue Générale Nucléaire*, No. 1 (1984).

*water supply. In fact, they will retain a dangerous concentration even after they have been carried downwind to a distance of ten miles. Some danger might possibly persist to distances as great as one hundred miles.''*

This was said 33 years before Chernobyl.

A second point relates to the rule of thumb to define the radius R in miles around the plant for which evacuation should be possible:

$R = 0.01\sqrt{P}$, with P = power in thermal kilowatts.

A 1000 megawatt-electric (MWe) radius is 17.3 miles according to this formula, which is about 30 kilometres. That rule of thumb was established in 1950, 36 years before Chernobyl.

Finally, in 1953, the first civilian nuclear power plant was announced in Shippingport: a containment building was provided around the reactor. The three major aspects that dominated safety for the next years were present: accident prevention, mitigation of consequences by containment, and emergency planning.

### 1957-67: Safety of design

The dominant safety aspect of this period is the importance given to safety of the design. Most of the concepts which are still in use were established about that time including the main safety functions: controlling the chain reaction; cooling the core; and containing the radioactive materials. The concept of defence-in-depth, with the requirement of redundancy to fulfil the single failure criterion, and of postulated initiating events to give the design basis for the safety features, were established. Even if some developments were to occur later, most external events, such as earthquakes and floods, were introduced at that time.

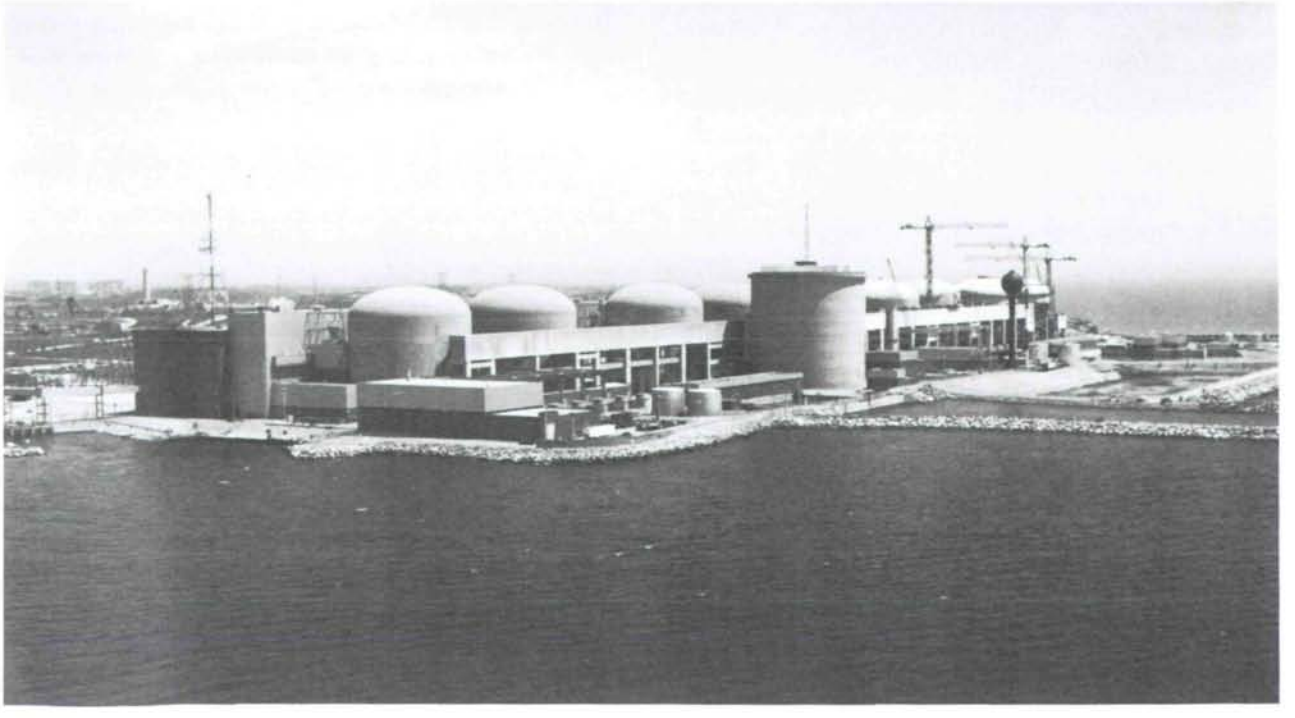
In the AEC approach, the concept of ''maximum credible accident'' was used, presented for the first time in 1959. It was not universally accepted.

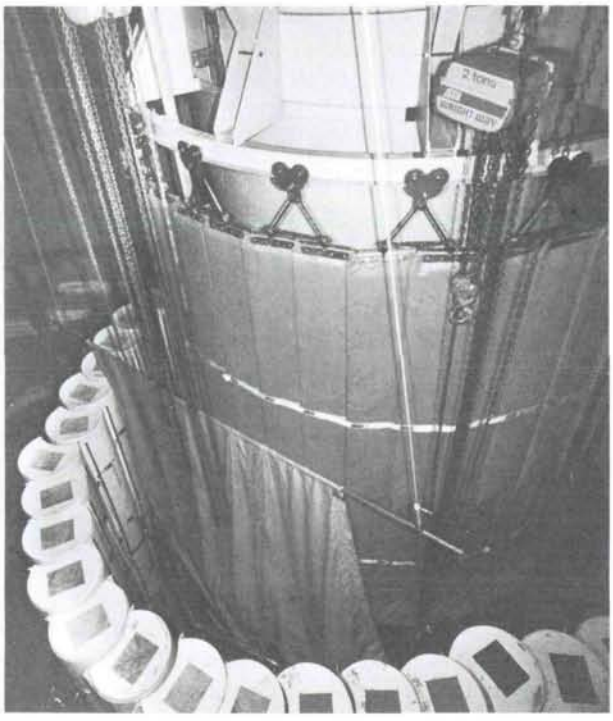
In France, the emphasis was put on the multi-barrier system, between the radioactive materials and the environment, and on an assessment of the possible challenges of these barriers.

Some technical issues which were widely discussed during the period, and which have some relevance today, should be mentioned. The question of pressure vessel integrity was raised in reference to the safety approach, based on prevention of accidents and on mitigation of their consequences should they occur. This approach was fine for pressure tube design where priority was given to prevention of tube rupture; but it also had to be demonstrated that propagation to other tubes would not lead to unacceptable consequences. Was it necessary to provide a containment able to withstand the consequences of rupture for pressure vessel designs? The question was easily answered for gas-cooled reactors, where containment was not considered necessary to keep the consequences of an hypothetical accident at an acceptable level.

The discussion was more difficult for light-water reactors (LWRs). When the AEC deemed such a failure ''incredible'', a report by British experts in 1964 concluded that rapid vessel failure was possible at temperatures above the nominal brittle-ductile transition range — in the operating temperature range where sudden failure was not supposed to occur. A specific research

**The Pickering nuclear generating station nearing completion in the late 1960s.**





**The accident at TMI placed emphasis on operational safety. (Credit: GPU)**

programme was launched in 1965 in the USA and lasted nearly a decade. The Heavy Section Steel Test Programme, conducted by the Oak Ridge National Laboratory, indicated that at operating temperatures thick-walled steel for pressure vessels was very tough and not inclined to undergo rapid fracture.

In parallel, significant improvements were brought to codes and standards, from stress analysis to in-service inspection. Finally, it was considered that the risk of a major rupture from missiles which could breach the containment was very low. Several years later, the Rasmussen report confirmed that conclusion.

Another technical issue is related to the risk of reactivity excursions. Reactor kinetics were subject to extensive studies and research, including the various reactivity coefficients, xenon instabilities, and, for liquid moderators, void effects. Many important experiments were conducted during that period, among them the well-known SPERT programme in Idaho Falls on LWRs.

In the following years, reactivity transients were still the subject of considerable investigations, in particular as regards fuel failure mechanisms, in many research facilities, for example in the USA, Japan, and France, and for several reactor types.

One can consider that it is at the end of this first period that the possibility of urban siting was ruled out. It was first raised in 1963 in the USA with the application for the Ravenswood site: two pressurized-water reactors (PWRs), around 600 MWe each, in the Borough of Queens in New York City, along the East River, with three million people at night within a 5-mile radius, and 5.5 million during the day. The application was withdrawn; the official reason was not related to safety, but to the availability of cheaper power from Labrador.

A similar debate took place several years later in the Federal Republic of Germany with the Ludwigshafen project, for which specific provisions were foreseen to cope with vessel failure. Finally, although there was strong industry pressure for metropolitan siting (in the USA, for example, the Edison Electric Institute wrote in 1967 that "siting of NPPs in metropolitan areas must be a key factor in the design of our future electric power systems"), there was a general consensus to move away from metropolitan sites with the recognition of the relationship between core melt and containment failure.

### 1967-79: Safety of construction

During the second period, from 1967 to TMI, the emphasis was on safety of construction. This may be excessive, since most of the effort was still related to design safety. However, one key safety aspect was introduced at this time: quality assurance.

The importance of safety during the construction stage has always been recognized. As noted in *The Technology of Nuclear Reactor Safety* in 1964:

*"Since many reactor projects have experienced difficulty due to inadequate workmanship, faulty materials, and other construction problems, the importance of this phase (the construction stage) cannot be overemphasized. The execution of a reactor design, if not properly carried out, can nullify the safety features. Very little can be said in the way of guidance except that it is essential to maintain the highest standards of construction and installation."*

A lot of guidance was given later, and quality assurance may have been the source of more paper work than the entire regulatory process. It is now a well-accepted concept, even if its implementation raises problems.

Apart from quality assurance, safety design underwent a considerable evolution during these years. It is important to note that independant regulatory bodies took their full extension during that period. In the USA, the Nuclear Regulatory Commission (NRC) was established in 1974 by the Energy Reorganization Act. Before that, in 1970, a programme of safety guides (later renamed regulatory guides) was initiated by the AEC to implement the design safety criteria.

In France, the safety responsibility shifted from the Commissariat à l'énergie atomique (CEA) to the Service Central de Sûreté des Installations Nucléaires (SCSIN) in 1973. In Great Britain, the Nuclear Installations Inspectorate (NII) was formed in 1975 in the Health and Safety Executive.

Many design safety issues were raised during the period. One issue deals with the specific case of liquid-metal fast breeder reactors (LMFBRs). After the Bethe

and Tait accident, the period was dominated by the Hypothetical Core Disruptive Accident (HCDA). The hypothetical accident involved a core meltdown due to the loss-of-cooling power and failure to scram (shut down the chain reaction), followed by various energetic phenomena. Although core meltdown events for other reactor types were not explicitly considered in the licensing process, HCDA was considered for breeders, for which the negative reactivity coefficient and large thermal inertia were generally considered favourable. There was some apparent lack of coherence here. But, before TMI, there were many discussions on core melt in LWRs (the China syndrome) and important research, for example in the Federal Republic of Germany.

For LWRs, LOCA (loss-of-coolant accident) became the main issue. Results from a research facility (semi-scale) indicated in 1971 that much of the water could leave the reactor vessel under certain conditions involving a pipe break rather than reflood the core immediately. The so-called emergency core cooling system (ECCS) issue was the most controversial one for some time, used by anti-nuclear movements in their actions. It kept the safety emphasis on the large pipe breaks, the so-called guillotine rupture, and unfortunately diverted attention from the more probable small and medium breaks — although the Rasmussen report indicated clearly that they were the risk-dominant sequences. TMI was an unfortunate reminder of the true safety issues.

Among the many other safety issues discussed during this period, fire was recognized as a potential safety concern of considerable importance for at least a decade before the Browns Ferry incident in 1975 in the USA. That event led to a major effort from regulatory bodies, and new requirements were introduced. Other issues of significance to operational safety were resolved as well.

Finally, this period is also characterized by the publication of the Rasmussen report, WASH-1400, in 1975. Forgetting the controversy about its executive summary, and its use in the public debate, what was essential was the general consensus on the benefits for safety which could be gained from a probabilistic approach, as a supplement to the deterministic one used in design. This consensus was worldwide. An excerpt from an ACRS letter, from Okrent's book, articulates this consensus:

*"Reactor Safety Study represents a valuable contribution to the understanding of Light Water Reactor Safety in its categorization of hypothetical accidents, indentification of potential weak links, and its efforts to develop comparative and quantitative risk assessments....The methodology should be applied to other types and designs of reactors, other site conditions, and other accident initiation and sequences."*

On 28 March 1979, the safety scene looked satisfactory on the whole. The safety approach was coherent, and there were no pending serious issues. Contrary to what was said later, severe accidents were not ignored. The probabilistic assessment did confirm that their probability was low, and that one could expect a significant mitigating effect from the containment which would make the probability of severe radiological consequences to the public and the environment much lower. In fact, some members of the nuclear community were even convinced that nuclear power plants might well be not only safe enough, but too safe.

**Emergency preparedness evaluation at a US nuclear plant. (Credit: INPO)**

Maybe at that time it was overlooked that nuclear power plants had evolved over years, and had increased in power capacity. The decay heat levels were much higher. Engineered safety features were added to reduce the likelihood of accidents, but the designs had become more complicated. There were now important relationships between the possible failures of various safety features. And more important, most discussions dealt with design, while not enough attention was given to safety in operation and its human component.

### 1979-86: Safety in operation

The third period is a familiar one and includes the lessons learned from TMI. They were, in most countries, re-emphasized after Chernobyl. Only after TMI, operational safety was given the attention it deserved. Many essential safety aspects played a role in the TMI accident including the importance of adequate operating procedures; the need for appropriate training of operating personnel; the necessary improvement of the man-machine interface; the usefulness of operating experience feedback; the requirement for efficient emergency plans; and the danger of improper "mind-sets" at all levels of the operating organization. These safety

aspects now receive, in most countries, the attention they require. The establishment of the Institute of Nuclear Power Operations (INPO) in the USA is a significant indicator.

Also in this period, probabilistic methodologies were at last used in practice to improve safety. One typical example is the single failure criterion which is useful for safe design, but is not sufficient. There are cases where the complete loss of redundant safety systems has to be taken into account if the corresponding consequences were too large — the "cliff edge" effect. The only decision tool is probabilistic safety assessment (PSA). Complicated safety issues such as total blackout (loss of all electrical sources, external and internal to the plant) and anticipated transient without scram (ATWS) have been solved with the assistance of PSA.

"Safety goals" have to be used, even if implicitly, in the decision-making process. In retrospect, it appears that there was from the beginning a conscious policy of trying to make nuclear power reactors safer than other industrial or technological enterprises. Many countries have attempted to translate this general objective in terms of limited probabilities for harmful accidental consequences. This is not an easy concept, and even if many would agree on the order of magnitude of some safety goals, the discussion would be more difficult on their use, or practical implementation.

Finally, there is no doubt that this period has seen significant improvements in the safety of nuclear power plants. The Chernobyl disaster does not necessarily contradict this statement, but it compels us to proceed to a new and complete review of our safety philosophy and practices.

### 1986 and beyond: International safety

No one can know what will be the main safety trends in the next decade in the technical field. Fashionable concepts such as inherent safety should not have a very bright future; but, international aspects will be prominent.

We did not wait for 1986 before entering into intensive international safety co-operation. In addition to IAEA's role, there are many examples of fruitful international safety co-operation, through international organizations, such as the Nuclear Energy Agency of the Organisation for Economic Co-operation and Development (NEA/OECD), as well as through bilateral or multilateral agreements.

They cover all aspects of nuclear safety, from regulatory matters to exchange of operating experience, including safety research. Much of the safety progress made in the past has been the result of common research programmes, too numerous to mention here.

***IAEA's nuclear safety programme.*** The drafters of the Statute of the IAEA conferred on the Agency the mandate to "seek to accelerate the contribution of atomic energy to peace, health and prosperity throughout the world". The phraseology was widely seen in the early days as giving the Agency a promotional role with respect to the use of nuclear power for electricity generation. At the same time, however, they gave the Agency a specific mission in the field of safety.

The Agency has no actual regulatory powers; it is mandated only to provide advisory services. The only exception is in the case of technical assistance projects, when it is obliged to observe its own safety standards in addition to those of the national regulatory or safety authority, where they do not conflict.

The Agency was established at a time when there were very few nuclear power stations; and the resources devoted to its nuclear safety programme were limited. National authorities took the lead in the development of standards, reflecting their own degree of involvement in nuclear power. The Agency paid close attention to work in areas where international agreement was clearly required.

The 1960s, for example, saw the development of the well-known "regulations" on the transport of radioactive materials across international boundaries. These have been widely adopted as the basis for national legislation, and by bodies which do have regulatory powers. The Agency worked in close collaboration with organizations such as the Central Commission for the Navigation of the Rhine, Central Office of International Railways, Euratom, International Maritime Organization, International Air Transport Assocation, Universal Postal Union, and World Health Organization.

In the 1970s, the number of nuclear power plant projects increased, and it was recognized that harmonization of differing national standards and regulatory requirements — not only in transport but in other areas of nuclear safety — could be valuable in the development of international trade in nuclear power plant services and equipment. The Agency therefore began development of a comprehensive body of safety standards for nuclear plants. Eventually, this programme resulted in the publication of 60 documents in the Agency's Nuclear Safety Standards (NUSS) programme, dealing with siting, design, construction, operation, and quality assurance considerations.

The accident at TMI, and the changing world energy situation, resulted in a fall in the number of orders for new nuclear plants. The Agency reoriented its programmes to place increased emphasis on operational safety. In 1982, it revised its Basic Safety Standards to take account of recommendations of the International Commission on Radiological Protection (ICRP) on dose optimization. During the same period, it published a wide range of technical guidance documents dealing with occupational and public needs in the field of radiation protection, and emergency planning and preparedness.

From the beginning, the Agency carried out ad hoc missions to Member States, especially in connection with services and assistance provided through its techni-

cal assistance programme. Through these missions, developing countries in particular could receive the benefit of expert advice. In 1972, to meet the increasing needs of Member States, the Agency announced the availability of missions for the Integrated Safety Assessment of Research Reactors (INSARR) — many of which are in developing countries.

In 1983, the Agency formally offered the first Operational Safety Review Teams (OSART). OSART missions provide nuclear power plant operators with useful advice, and an exchange of ideas on safety improvement, at the working level. Since Chernobyl, the OSART programme has been expanded greatly; the Agency now fields at least one mission each month.

Also in 1983, the Agency established an international Incident Reporting System (IRS), to enable operators in all participating countries to benefit from "lessons learned." This system complements that operated by the NEA/OECD. In particular, it includes plants in countries outside the OECD area. It is now being expanded to include more "significant events", and to enable a more effective and timely analysis of events. Teams for the assessment of safety-significant events (ASSET) are now offered, to perform on-the-spot, in-depth analysis of the operational experience of nuclear power plants with respect to their safety, focusing particularly on the man-machine interface and human factors.

In 1985, the Agency established the International Nuclear Safety Advisory Group (INSAG) to review the Agency's activities in the field of nuclear safety and to advise on its future work programme. INSAG was active in reviewing data and analyses presented at the Post-Accident Review Meeting convened in Vienna in 1986 in response to the Chernobyl accident.

The Agency also offers Radiation Protection Advisory Team (RAPAT) missions, to help non-nuclear power States develop their radiation protection capabilities; training is expanding in this field.

### Where is the emphasis today?

The emphasis today in nuclear safety efforts is switching from establishment of standards and quality assurance to accident prevention through improved operational safety and accident mitigation. Accident mitigation has three aspects: accident management, containment integrity, and emergency preparedness.

Moreover, the establishment of monitoring networks, the setting of intervention levels, (which demonstrate at the national level that the public can be efficiently protected against the consequences of severe accidents) will have to be included in multinational and multi-agency endeavours.

Finally, from the beginning, the safety priority has always been the prevention of accidents, particularly severe accidents. It is proper to be prepared to face accidents, should they happen, and we should remain convinced that these accidents can be avoided if we take into account the lessons learned from more than 30 years of nuclear safety development.