Rendiconti
Accademia Nazionale delle Scienze detta dei XL
Memorie di Scienze Fisiche e Naturali
121° (2003), Vol. XXVII, t. I, pp. 291-293

MAURIZIO CUMO *

The safety of nuclear power plants

A particular family of large and complex constructions for which the safety is a basic aspect is that of nuclear power plants. They contain radioactive materials which might be released into the environment if the safety barriers failed.

Safety must be assured in the design of plants and in their operation. Safety requires that there is shielding against ionizing radiation, leak – tight enclosure of the highly radioactive fission products in the reactor, effective control of the dynamic process and cooling capacity which can always match the heat generated.

There are four aspects of the fission chain reaction which might be dangerous, but cannot be separated from the peaceful use of nuclear energy and therefore require safety measures:

– the fission chain reaction involves ionizing radiation, which requires shielding;
– highly radioactive fission products are created, requiring tight enclosures;
– it is a dynamic process, requiring control;
– it has effects that cannot be instantly stopped, since radioactive decay continues to produce some heat, reducing gradually, which requires long-term cooling.

There are basic design safety characteristics common to many reactors:

Redundancy – More components or subsystems of a safety system that are needed to make it work are provided – typically two to four – so that safety does not depend on the functioning of single units. For example, one single cooling pump might be enough, but could be under maintenance, so a second is provided. That might fail, so a third is provided.

Diversity – Two or more systems based on different design of functional principles are available for a particular safety function – the belt and braces approach. This protects against all the systems being put out of action all at once for the same reason.

* Uno dei XL. University of Rome «La Sapienza».

Physical separation – Components or systems intended to perform the same function can be separated physically, so that they are protected against simultaneous loss by, for example, fire or flood. Distance or physical barriers can both be used.

The fail-safe principle – Components or systems are designed to fall automatically into the safest conditions if they fail, or if power is lost.

The basic aim in nuclear power plant safety is to maintain the integrity of the multiple barriers. This is assured through the "defence in depth approach", which can be characterized by three levels of safety measures: preventive measures, protective measures and mitigative measures.

First level: preventive measures – These are designed to stop any events that could lead to accidents. Some of these are:
– inherently safe features, which rely on the laws of nature to work, included in the design in order to stabilize and limit reactor power;
– safety margins built in the design of components and systems;
– components and systems tested and inspected during construction and at regular intervals afterwards and suitably maintained so that they are kept in their intended condition during plant operation;
– instruments and controls provided to ensure that operators will at all times know and have control of the operational status of the plant and of its systems.
– Quality assurance methodology is followed throughout the design, construction and operation of the plant. This means that a procedure of independent inspection, testing, checking, counterchecking and documenting is followed to ensure that all components and systems will operate satisfactorily in service. It includes making sure that the design is adequate to meet the defined and agreed requirements and that manufacturing and construction are carried out according to the design.

Second level: protective measures to halt or deal with incidents. Despite the care that is taken at the first level to avoid failures or operating errors that could potentially lead to safety problems, it is accepted that there may be some failures during the life of a nuclear power plant. All reasonably conceivable failures are therefore postulated, and a second level of defence is provided by reliable protective measures designed to stop or to successfully deal with such incidents.

Third level: mitigative measures. These are designed to limit the consequences of accidents if they occur in spite of the preventive and protective measures. Some of these measures are:
– If the regular power supply and its backup fail, there are diverse and redundant emergency power systems to provide electricity for safety systems;
– There is a containment to prevent any radioactive material leaking from the reactor in an accident. The containment is built to very high specifications and

fulfils stringent anti-leakage requirements. It is designed to maintain its integrity not only against internal stresses, but also against external stresses such earth-quakes, aircraft crashes and hurricanes;

Emergency planning: is the last defence, with the removal of nearby population in safer areas.

A top level in safety is reached by the so called "inherently safe" reactors which are exclusively protected by physical laws of nature, completely passive, without any need of active energized systems and of operators to avoid accidents. A design of this type of reactor has been accomplished by a team of the University of Rome La Sapienza, starting since 1983. The reactor, called MARS, is a modular, cogenerative plant of 600 MWth whose components are totally in steel and may be assembled by means of flanged connections.

In this way the reactor may be completely constructed in factories, shortening the time of construction, and then transported in pieces in the selected site to be assembled. Its operating life may exceed the century, due to the easy substitution of all components. The final decommissioning is very quick and cheap, producing a large amount of recyclable steel and a small one of activated melt ingots. Water desalination and electricity are the preferred products of its co-generation. Detailed evaluations of their costs have reached very competitive targets.