14. How Safe is Safe Enough?

Antti Vuorinen
Director General, Emeritus, STUK Finland

How safe is safe enough is a question repeated often, when talking about safety of nuclear power plants; but most often left without clear answer. In the following is an attempt to highlight some key elements, which has to be kept on mind and taken care, when attempting to achieve high level of safety in nuclear technology.

Every incident and accident at nuclear power plant gives a reason to raise this question. It does not matter, what the reason of the abnormal behavior of the facility was. Is the design safe? Is the quality of the plant adequate? Are the operating personnel properly qualified? Is there a qualified independent regulatory authority? Generally speaking, we have to ask at first: Is the safety culture of the country and the operating company at acceptable level?

What are the essentials of good safety culture?

Responsible persons at every level must acknowledge and understand the quality and the magnitude of nuclear risks and commit to act in responsible way. The commitment has to be manifested clearly and openly. At state level, there must be an up-dated nuclear safety regulation assigning clearly the responsibilities of nuclear utilities, licensing system and the full-powered independent regulatory authority as well as on- and off- site rescue organization for emergency situations; provided with sufficient qualified resources. At utility level personnel of nuclear utility from the top management to the operating and maintenance workers have to understand the importance of prioritizing always the safety before economy or other interests and take the actions correspondingly. Especially persons in key positions have to understand the importance of independent quality assurance and to take necessary actions for fulfilling it. To be effective safety culture needs continuous development and follow-up.

What are the safety objectives?

Nuclear safety is finally culminated to the question of radiological safety of personnel of the plant and people in the environment; as well as the radiological contamination of the environment. Technical safety objective is to prevent the release of radioactive materials from the reactor to the environment. To achieve this goal, heat transfer from the reactor core has to be assured in all circumstances. However, unexpected disturbances, incidents and even accidents may happen on the plant. The attempt is to keep the number of all kind of abnormalities to the minimum. And provide the plant with the protection systems to assure safe shut-down, core cooling, monitoring plant conditions and if needed mitigating possible radiological consequences to the minimum.

In plant technology, it means high quality, verified by comprehensive quality assurance program, utilizing defense in depth principle, including multiple-barrier protection, redundant systems working with diverse principles as far as possible. The plant and its system must be tested and analyzed using best estimate and probabilistic approaches to verify plant behavior in normal, transient and accident conditions to make sure that plant meets the preset design objectives. The special values of probabilistic analysis are that these provide information about the internal reliabilities, revealing possible weaknesses. Thus it may enhance towards balanced system.

Modern plant is running utilizing automated systems in normal and into certain extend in abnormal conditions also. However, the role of operator, shift supervisor and safety engineer is crucial in unexpected situations. Operation procedures for unexpected situations and diagnostic, event based or symptom oriented, aids are essential to restoring safe conditions on the plant. Extreme, natural phenomena, such as storms, earthquakes, tsunamis etc. may cause loads exceeding design values of the plant. At least partly, this problem should be taken as an extra margin of certain components and systems. Such components are for example: primary circuit, especially reactor vessel and containment. Systems, which need very special analyses and judgment are: Diagnostic system for abnormal situations, electric power supply, heat removal from primary circuit, water supply, ultimate heat sink, pressure relief-valves of primary system and environmental radiation monitoring system.

Responsibility and authorization for all protective and mitigating actions on the plant must lay on the operating shift. Responsibility for possible rescue actions off the plant lays on the rescue officials. The utility is obliged to arrange immediately an information service for rescue organization, for international collaborators and for public needs. Ageing of the plant and the knowledge of personnel is an important challenge. That requires special emphases in planning and fulfilling maintenance and retraining personnel.

The leading principle in radiation protection with dose limit system is so- called ALARA-principle: Radiation doses should be kept “As low as reasonably achievable”! In practice, it means need for optimization. The leading target of nuclear safety should be SAHARA-principle: “Safety as high as reasonably achievable”! It means that in addition to the well-proven solutions even the latest achievements of science and nuclear technology should be utilized, where applicable. For improving nuclear safety level, one essential way is learning, not only from major accidents but from minor incidents too, at home. Learning should be followed by careful consideration about the need for corresponding back-fitting of the plant, procedures, operator training etc. Decisions on what changes are really improvements are often difficult. Probabilistic cost benefit analyses may be here helpful. However, when it is a question of major accident with a very low probability and possibility for very severe consequences, the uncertainties of analyzes are too big for an analytic decision. That is why the pragmatic approach is preferable. All practicable measures to prevent major radioactive leakages from nuclear power plant must be taken.

August 2011