# What is safety?

The word **safety** is very often used in the everyday life. According to Webster's New World Dictionary the definition can be given as follows:

**safety:**
**1.** the quality or condition of being safe; freedom from danger, injury, or damage; security.

**2.** (technical) the stability of a building, machine or other construction, the tranquillity of its operation and the fact that it does not endanger its environment. Safety is always relative; it can be only defined if the condition of its surrounding is defined as well. It only exists if the object/construction is not bearing force.

## Safety of nuclear power plants

The safety of modern nuclear power plants is better than twenty years ago. The old plants are not only out-of-date but also dangerous. The two reactor accidents (Three Mile Island 1979, Chernobyl 1986) forced the nuclear operators to improve the safety of plants. As a result modern plants have manifold safety systems. In the case of a nuclear power plant safety means that the design of the plant must ensure safety of the environment, even in the case of a serious accident. The modern plants (among them the Paks NPP) fulfil this criterion. The constructors have developed a huge number of accident prevention methods and the safety systems are built so that they can avert several types of accidents. The safety systems are prepared and the personnel are trained to be able to prevent emergency situations. Since it is impossible to consider all the possibilities there is a need for continuous safety enhancement measures and reviews. These are the basic requirements that the nuclear operators have to comply with, including the Paks Nuclear Power Plant in Hungary. The Hungarian Atomic Energy Agency is responsible for its review and also the examination of other nuclear institutions (KFKI research reactor, BME study reactor, Interim Storage Facility for Spent fuel). The responsible agency only issues an operational licence if the nuclear safety of the institution is proved in all areas.

Let us examine why a nuclear power plant is so peculiar in terms of safety.

- In nuclear power plants there is a great amount of radioactive material, against the radiation of which the workers must be protected and in an accident situation the release of these materials to the environment must be prevented.
- In an NPP, a large quantity of heat is generated even after shutdown due to the radioactive decay of the fission product isotopes.

Three basic safety conditions must be fulfilled in a nuclear power plant:

- Efficient control of the nuclear chain reaction (reactivity control).
- Proper cooling of the reactor core.
- Prevention of the release of radioactive materials.

These **safety functions** are implemented in an NPP with the aid of the so-called **defence-in-depth**.

# Defence-in-depth

## Barriers

According to an earlier concept, the above safety functions were fulfilled using so called barriers. In this method, the protection of the public against consequences of an accidental release of fission products rests on the interposition of a series of leak tight barriers, which are:

- the fuel pellets,
- the cladding,
- the primary circuit,
- the containment.

The primary goal of the barriers is to prevent the radioactive materials from reaching the next barrier.

The primarily goal of safety analyses is to ascertain the normal operation of the barriers even in case of emergency.

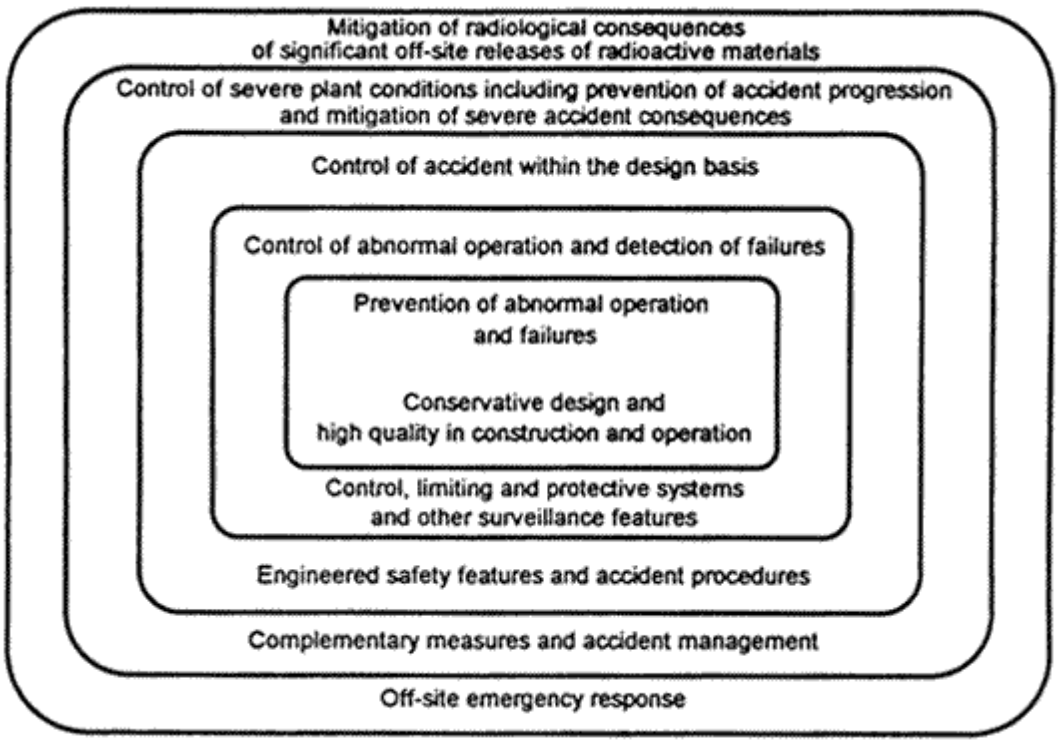
However, the increasing safety requirements urged the development of this concept. The reactor safety systems must cope with a triplet of expectations, namely

- accident prevention,
- monitoring (watching signs that may indicate accidents),
- mitigating of accident consequences.

The principle of defence-in-depth was formulated according to these requirements.

## The principle of defence-in-depth

The principle of defence-in-depth, in contrast to the barriers, does not only consist of actual technical solutions; it is rather a framework that includes the whole plant. The approach combines the prevention of abnormal situations and their degradation with the mitigation of their consequences. The defence in depth concept consists of a set of actions, items of equipment or procedures, classified in levels, the prime aim of each of which is to prevent degradation liable to lead to the next level and to mitigate the consequences of failure of the previous level.




Before describing the different stages involved, the principle can be simply summarized as follows: Although the precautionary measures taken with respect to errors (incidents and accidents) are, in theory, such as to prevent their occurrence, it is nevertheless assumed that accidents do occur and provisions are made for dealing with them so that their consequences can be restricted to levels deemed acceptable.

**First level: prevention of abnormal operation and failures**

The installation must be designed with excellent intrinsic resistance to its own failures or specified hazards in order to reduce the risk of failure. This implies that following preliminary delineation of the installation, an exhaustive study of its normal and foreseeable operating conditions be conducted to determine the worst (mechanical, thermal, pressure) stresses or those due to environment, layout, etc., for each major system and component, for which allowance must be made. The installation components can then be designed and operated by following clearly defined and qualified rules. The selection of appropriate staff, their appropriate training, the overall organization, the sharing of responsibilities or the operating procedures contribute to the prevention of failures throughout plant life.

**Second level: control of abnormal operation and detection of failures**

The installation must be prevented from straying beyond the authorized operating conditions. Control and protection systems must be designed with the capacity to inhibit any abnormal development before equipment is loaded beyond its rated operating conditions. Temperature, pressure and nuclear and thermal power control systems must be installed to prevent excessive incident development. Systems for measuring the radioactivity levels of certain fluids and of the atmosphere in various facilities shall assume monitoring requirements and check the effectiveness of the various barriers and purification systems.

**Third level: control of accidents within the design basis**

The first two levels of defence in depth, prevention and keeping the reactor within the authorized limits, are designed to eliminate the risk of failures with a high degree of reliability. However, a series of incidents and accidents is postulated by assuming that failures could be as serious as a total instantaneous main pipe break in a primary coolant loop or a steam line, or could concern reactivity control. Therefore it is required to install safety systems for limiting the effects of these accidents to acceptable levels. Start-up of these systems must be automatic and human intervention should only be required after a time lapse allowing for a carefully considered diagnosis to be reached. In the postulated situations, the correct operation of these systems ensures that core structure integrity will be unaffected, which means that it can subsequently be cooled. Radioactive releases to the environment will consequently be adequately limited.

**Fourth level: control of severe plant conditions including prevention of accident progression and mitigation of severe accident consequences**

We have to consider the means required to contend with plant situations which have bypassed the first three levels of the defence-in-depth strategy (e.g. cases of multiple failure) or which were considered as part of the residual risk (i.e. the likelihood of such accidents is extremely low). Such situations can lead to higher radioactivity release levels. The concern here is consequently to reduce the probability of such situations by preparing appropriate procedures and equipment to withstand additional scenarios corresponding to multiple failures. Every endeavour would also be necessary to limit radioactive release due to a very serious occurrence and to gain time to arrange for protective measures for the population in the vicinity of the site. It is then essential that the containment function be maintained under the best possible conditions.

**Fifth level: mitigation of radiological consequences of significant off-site releases of radioactive materials**

Population protection measures because of high release levels would only be necessary in the event of failure or inefficiency of the measures described above. The conditions of these measures are within the scope of the public authorities. They are supplemented by the preparation of long- or short-term measures for checking the consumption or marketing of foodstuffs which could be contaminated. Such measures are included in the external emergency plans. Periodical training drills are also necessary in this area to ensure adequate efficiency of the resources and linkups provided.

We have to note here that, according to the recommendations of the International Atomic Energy Agency, the principle is to be applied taking into account the characteristics of the installation. The national authorities should enforce implementation, but safety still remains the responsibility of the operating organization.

# Safety culture

In order to operate a nuclear installation safely, it is not enough to have a technically safe system. For safe operation it is also equally important that the operating personnel should have a proper attitude to safety and the management, as well as the workers must be committed to safety and must realize that safety has the highest priority above all. This is the concept of safety culture.

The International Atomic Energy Agency gives the following official definition: *"Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear power plant safety issues receive the attention warranted by their significance."*

After this hard-to-understand definition, let us see what it means in simpler terms! In all types of activities, for organizations and for individuals at all levels **attention to safety** involves many elements:

- Individuals must be aware of the **importance of safety**.
- **The knowledge and competence** of the personnel must be adequate. This should be conferred by training and instruction of personnel and by their self-education.
- The **management** is required to demonstrate **commitment** to the high priority of safety and individuals should adopt the common goal of safety.
- **Personnel must be motivated to keep to safety regulations**, which the management can achieve by the setting of objectives and systems of rewards and sanctions.
- It is important that the **management supervise** the work of individuals, including audits and review practices, with readiness to respond to individuals' questioning attitudes.
- **Responsibilities must be clearly defined**, through formal assignment and description of duties; the management must make sure that the personnel understand them.

Safety culture has two general components. The first is the necessary framework within an organization and is the responsibility of the management hierarchy. The second is the attitude of staff at all levels in responding to and benefiting from the framework.

Accordingly, the concept of safety culture implies what attitude the individuals working in a nuclear installation and the whole organization have to nuclear safety. Safety culture is also an amalgamation of values, standards. morals and norms of acceptable behaviour. These are aimed at maintaining a self-disciplined approach to the enhancement of safety beyond legislative and regulatory requirements. Therefore, safety culture has to be inherent in the thoughts and actions of all the individuals at every level in an organization. The leadership provided by top management is crucial.
Safety culture applies to conventional and personal safety as well as nuclear safety. All safety considerations are affected by common points of beliefs, attitudes, behaviour and cultural differences, closely linked to a shared system of values and standards.

Below are some questions, to which you have to know the answers, if you want to undertake your duty as regards safety. Let us take a look at each of the above concepts. Before an individual begins any safety related task, his or her *questioning attitude* raises issues such as those listed in the following:

- Do I understand the task?
- What are my responsibilities?

- How do they relate to safety?
- Do I have the necessary knowledge to proceed?
- What are the responsibilities of others?
- Are there any unusual circumstances?
- Do I need any assistance?
- What can go wrong?
- What could be the consequences of failure or error?
- What should be done to prevent failures?
- What do I do if a fault occurs?

# Reactor safety

Since the Chernobil reactor accident it is very probable that there are not many people in the world who have not asked the (otherwise naturally brought up) question "How safe is a nuclear power plant?" Newspapers, magazines and the mass media often publish opinions which are radically different from each other and raise unnecessary and exaggerated fear in people. It is a commonly accepted fact that these kinds of fears are usually based on the lack or inadequacy of knowledge; in other words, if one does not know something, one may obviously be afraid of it. In order to examine how dangerous is the operation of nuclear power plants in our vicinity, let us first take a look at the concepts of safety, danger and risk.

In every minute of our life we are exposed to dangers and in most cases we are not even aware of them. To illustrate this, here are some everyday examples. If you want to go or travel from one place to an other, say from home to the office or school, or maybe to a weekend cottage, you usually take some means of transport . If you take your car, for example, there is a real chance that you might suffer an accident. (Think of the fact that only in Hungary about 1500 people die on the roads every year.) Nevertheless, most of the time you do not even think of it, which means that people consider this kind of risk normally acceptable. Yet the fact that when simply walking in the street- an airplane may fall down on your head- is really not at all considered.

Why? The answer is simple: the likelihood of this latter event is much lower, as everyone feels it somehow. But the way we think is strange. When you take an airplane, it probably occurs to you that the plane might suffer a crash on its way. On the other hand, everybody knows that a mile flown is far safer than a mile taken by car. That is, travelling by air is safer than travelling by car. Then how could we define risk? In the case of fatal car accidents, we can obtain a characteristic measure if we calculate the probability that a person dies sitting in his car during one year. Since about 10 million people live in Hungary and the number of casualties is 1500/year, $1.5*10^3/10^7 = 1.5*10^{-4}$/year is the probability that a person suffers a fatal car accident in a year. This number is approximately 1/10000. This amount of risk is taken as endurable or perhaps necessary, without much thinking. Let us compare this value with the calculated risk of nuclear power plant accidents.

In most states of the USA a nuclear installation can only be commissioned if the risk of a serious accident - i.e. one that has significant effect on the population and environment - is less than $10^{-7}$/year. This number is one-thousandth of the risk of the above mentioned road accidents. Note here that the probability of the most serious accident of the Paks NPP is around this value. How can such a low value be achieved? Accidents can be attributed to two different causes: human error and technical fault. Of course, as a third cause we may add the design error, or we may also consider that the severity of a potential accident is largely determined by the design and elaborate implementation of the system. Just consider how much the car manufacturing companies spend on making cars safer, equipping them with a large number of safety equipment items (airbags, etc.). All these either help avoid the accidents (active elements) or mitigate the severity of these (passive ones). At almost all the modern nuclear power plants there is, for example, a so-called containment,

which is a strong and hermetically sealed reinforced concrete structure around and above the reactor. If such a containment had existed in Chernobil, it is very likely that the environmental impact would have much lower. Moreover, nearly all the newer design (and of course, many of the older) reactors have so-called inherent safety, which means that - even if the worst human error occurs - the laws of physics serve as negative feed-back and, for example, prevent the power of the reactor from getting too high.

# The International Nuclear Event Scale

The International Nuclear Event Scale (INES) is a tool to promptly and consistently communicate to the public the safety significance of reported events at nuclear installations. By putting events into proper perspective, the Scale can ease common understanding among the nuclear community, the media and the public. It was designed by an international group of experts convened jointly by the International Atomic Energy Agency (IAEA) and the Nuclear Energy Agency (NEA) of the Organisation for Economic Cooperation and Development (OECD). The group was guided in its work by the findings of a series of international meetings held to discuss general principles underlying such a scale. Initially applied for a trial period to classify events at nuclear power plants, 32 countries participated in the trial and international agencies, and user countries monitored progress. The Scale operated successfully and now has been made available for formal adoption by each country. The Scale also has been extended and adapted to enable it to be applied to all nuclear installations associated with the civil nuclear industry and to any events occurring during the transport of radioactive materials to and from those facilities. Events are classified on the Scale at seven levels. Their descriptors and criteria are shown below with examples of the classification of nuclear events which have occurred in the past at nuclear installations. The lower levels (1-3) are termed **incidents**, and the upper levels (4-7) **accidents**. Events which have no safety significance are classified as level 0 / below scale and are termed deviations. Events which have no safety relevance are termed out of scale.

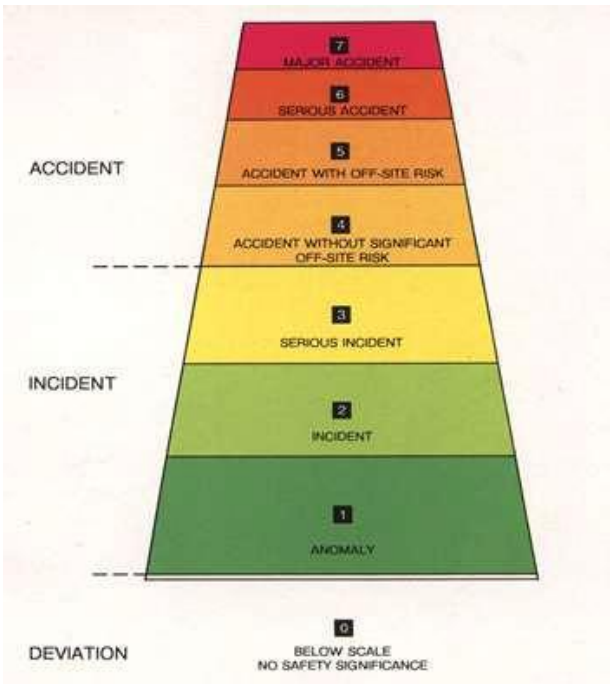
Although the same scale is used for all installations, it is physically impossible for events to occur which involve the release to the environment of considerable quantities of radioactive material at some types of installation. For these installations, the upper levels of the scale would not be applicable. These include research reactors, unirradiated nuclear fuel treatment facilities and waste storage sites. Industrial accidents or other events which are not related to nuclear or radiological operations are not classified and are termed "out of scale". For example, although events associated with a turbine or generator can affect safety-related equipment, faults affecting only the availability of a turbine or generator would be classified as out of scale. Similarly, events such as fires are to be considered out of scale when they do not involve any possible radiological hazard and do not affect the safety layers.

The Scale is not appropriate as the basis for selecting events for feedback of operational experience, as important lessons can often be learnt from events of relatively minor significance. It is not appropriate to use the Scale to compare safety performance among countries. Each country has different arrangements for reporting minor events to the public, and it is difficult to ensure precise international consistency in rating events at the boundary between level 0 and level 1. The statistically small number of such events, with variability from year to year, makes it difficult to provide meaningful international comparisons. Although broadly comparable, nuclear and radiological safety criteria and the terminology used to describe them vary from country to country. The INES has been designed to take account of this fact.

**Examples of classified nuclear events:**

- The 1986 accident at the Chernobyl nuclear power plant in the Soviet Union (now in Ukraine) had widespread environmental and human health effects. It is thus classified as Level 7.
- The 1957 accident at the Kyshtym reprocessing plant in the Soviet Union (now in Russia) led to a large off-site release. Emergency measures including evacuation of the population were taken to limit serious health effects. Based on the off-site impact of this event it is classified as Level 6.
- The 1957 accident at the air-cooled graphite reactor pile at Windscale (now Sellafield) facility in the United Kingdom involved an external release of radioactive fission products. Based on the off-site impact, it is classified as Level 5.
- The 1979 accident at Three Mile Island in the United States resulted in a severely damaged reactor core. The off-site release of radioactivity was very limited. The event is classified as Level 5, based on the on-site impact.
- The 1973 accident at the Windscale reprocessing plant in the United Kingdom (now Sellafield) involved a release of radioactive material into a plant operating area as a result of an exothermic reaction in a process vessel. It is classified as Level 4, based on the on-site impact.
- The 1980 accident at the Saint-Laurent nuclear power plant in France resulted in partial damage to the reactor core, but there was no external release of radioactivity. It is classified as Level 4, based on the on-site impact.
- The 1983 accident at the RA-2 critical assembly in Buenos Aires, Argentina, an accidental power excursion due to non-observance of safety rules during a core modification sequence, resulted in the death of the operator, who was probably 3 or 4 metres away. Assessments of the doses absorbed by the victim indicate 21 Gy for the gamma dose together with 22 Gy for the neutron dose. The event is classified as Level 4, based on the on-site impact.
- The 1989 incident at the Vandellos nuclear power plant in Spain did not result in an external release of radioactivity, nor was there damage to the reactor core or contamination on site. However, the damage to the plant's safety systems due to fire degraded the defence-in-depth significantly. The event is classified as Level 3, based on the defence-in-depth criterion.

The vast majority of reported events are found to be below Level 3.



| Level / Descriptor | Criteria | Examples |
|---|---|---|
| **7. Major accident** | • External release of a large fraction of the radioactive material in a large facility (e.g. the core of a power reactor). This would tipically involve a mixture of short and long-lived radioactive fission products (in quantities radiologically equivalent to more than tens of thousands of terabecquerels of iodine-131 ). Such a release would result in the possibility of acute health effects; delayed health effects over a wide area, possibly involving more than one country; long-term environmental consequences. | Chernobyl NPP, USSR (now in Ukraine), 1986 |
| **6. Serious accident** | • External release of radioactive material (in quantities radiologically equivalent to the order of thousands to tens of thousands of terabecquerels of iodine-131 ). Such a release would be likely to result in partial implementation of countermeasures covered by emergency plans to lessen the likelihood of health effects. | |
| **5. Accident with off-site risk** | • External release of radioactive material (in quantities radiologically equivalent to the order of hundreds to thousands of terabecquerels of iodine-131 ). Such a release would be likely to result in partial implementation of countermeasures covered by emergency plans to lessen the likelihood of health effects.<br>• Severe damage to the nuclear facility. This may involve severe damage to a large fraction of the core of a power reactor, a major criticality accident or a major fire or explosion releasing large quantities of radioactivity within the installation. | Windscale Pile, UK, 1957<br>Three Mile Island, USA, 1979 |
| **4. Accident without significant off-site risk** | • External release of radioactivity resulting in a dose to the most exposed individual off-site of the order of a few milisieverts. * With such a release the need for off-site protective actions would be generally unlikely except possibly for local food control.<br>• Significant damage to the nuclear facility. Such an accident might include damage to nuclear plant leading to major on-site recovery problems such as partial core melt in a power reactor and comparable events at non-reactor installations.<br>• Irradiation of one or more workers which result in an overexposure where a high probability of early death occurs. | Saint Laurent NPP, France, 1980<br>Tokai Mura, Japan, 1999 |
| **3. Serious incident** | • External release of radioactivity above authorised limits, resulting in a dose to the most exposed individual off site of the order of tenths of millisievert. * With such a release, off-site protective measures may not be needed.<br>• On-site events resulting in doses to workers sufficient to cause acute health effects and/or an event resulting in a severe spread of contamination for example a few thousand terabecquerels of activity released in a secondary containment where the material can be returned to a satisfactory storage area.<br>• Incidents in which a further failure of safety systems could | Vandellos NPP, Spain, 1989 |

| | | |
|---|---|---|
| | lead to accident conditions, or a situation in which safety systems would be unable to prevent an accident if certain initiators were to occur. | |
| **2. Incident** | • Incidents with significant failure in safety provisions but with sufficient defence in depth remaining to cope with additional failures.<br>• An event resulting in a dose to a worker exceeding a statutory annual dose limit and/or an event which leads to the presence of significant quantities of radioactivity in the installation in areas not expected by design and which require corrective action. | |
| **1. Anomaly** | • Anomaly beyond the authorised operating regime. This may be due to equipment failure, human error or procedural inadequacies. (Such anomalies should be distinguished from situations where operational limits and conditions are not exceeded and which are properly managed in accordance with adequate procedures. These are typically "below scale"). | |