HADMÉRNÖK

VII. Évfolyam 1. szám - 2012. március

Tamási Béla – Grósz Zoltán
bela.tamasi@hm.gov.hu – grosz.zoltan@uni-nke.hu

NUCLEAR SECURITY – THE ROLE OF THE ENGINEER AT NUCLEAR POWER PLANTS

Absztrakt/Abstract

Minden ország alapvető kötelessége, hogy megóvja a kritikus infrastruktúrák körébe sorolt atomerőműveit, amely során feladatuk biztosítani a környezet megóvását az esetlegesen bekövetkező nukleáris balesetek esetében. A veszélyes nukleáris anyaggal üzemelő erőműveknek működésük során szigorú biztonsági követelményeknek kell megfelelniük. A képzett mérnökök az erőművek biztonságát és a környezet védelmét ötlépcsős műszaki alkalmazással valósítják meg. Az erőművek tervezése során a „mélységi védelem" megvalósítása alapvető követelmény. Ennek során a mérnökök kizárólag olyan erőműveket tervezhetnek, amelyek a katasztrófák negatív hatásainak ellenállnak és az üzemzavarokat is megfelelően tudják kezelni. Vajon, a magas szintű technológiák alkalmazásával elkerülhetőek a nukleáris balesetek?

Each country's fundamental duty is to protect nuclear power plants categorised as critical infrastructure and to ensure the preservation of the environment in case of nuclear accidents. Due to the unstable nature of the materials used within nuclear power plants safety measures utilized by the nuclear energy industry must be rigorous. Highly skilled engineers follow a five step approach to deliver the virtual defence in depth required to maintain a safe and secure environment within a nuclear power plant. One of the fundamental tenets of nuclear power plant design is "Defence in Depth." This approach leads engineers to design a plant that can withstand severe catastrophes, even when several systems fail. Will applying these hi-tech methods really help us avoid nuclear accidents?

Kulcsszavak/Keywords: *nukleárisbiztonság, biztonságosüzemeltetés, biztonságifunkciók, mélységivédelem, biztonságigátak, biztonságirendszerek ~ nuclear security, safety operation, security functions, virtual defence in depth, security measures, security systems*

1. INTRODUCTION

Nuclear power plants are spread all over the world and are involved in the energy production of approximately 30 countries. The world now has 435 operating nuclear power plant units in 190 nuclear power plants.[1]

Reactors however – regardless of their type – have unique design, there are no two nuclear power plants in the world that are the same in every detail. Safety systems of nuclear reactors, just like everything else in the world, are continuously developing. There is more experience in this field for which a high price has been paid unfortunately, since they were obtained at the expense of accidents. It is very important to understand that regardless of the level of development of a nuclear reactor or its security system there is no 100 percent safety or guarantee for safety. The most important thing a security system of a nuclear power plant has to fulfill is to prevent the release of radioactivity into the environment. Let's see how it could be implemented. [1]

2. SAFETY AND THE SAFETY OF NUCLEAR POWER PLANTS

In Hungary, long-term or permanent failure of electric energy production – technically speaking: production safety emergency – may cause a serious electricity supply problem, a temporary energy crisis. The economic damage due to "production safety emergency" means that although a nuclear emergency situation[2] does not exist, but one or more blocks of the nuclear power plant are out of production, or other major economic damage happened that does not affect the production.

The word safety is very often used in everyday life. The meaning of it in general terms and in technical terms is defined as follows[3].

Security is:

- The basic needs of existence and subjective experience and / or in existential situationswhen the person is not threatened by any kind of danger, or if it so, it can be avoided.
- (Technical) strength of a building, machinery, structure, or the safe and smooth operation of it, or the nature of them that they are harmless to the environment in the vicinity or it does not threaten the safety of the occupants. Security is always relative, which means that only among certain environmental conditions or under the maximum output exists. [2]

Studying these two conditions – namely "certain environmental conditions", and "under the maximum output" – from the perspective of nuclear safety, we can determine the safety concept of nuclear power plant, scilicet: safety is that quality of the plant's characteristics, which provides protection for the operational staff and for the public against external and internal exposure, prevention of radioactive contamination of the environment, the avoidance of exceeding the permissible exposure limits written in the relevant standards for either stationary or in emergency situations.

[1] Source: IAEA March 18 2011
[2] means: by radioactive or/and nuclear material caused contamination
[3] Magyar Nagylexikon, AkadémiaiKiadó, Budapest, 1995.

2.1 The safety of nuclear power plants

"Science and technology – I want to say that very clearly – does not solve every problem but without science and technology can not be solved any problem."[4]

The safety level of nuclear power plants nowadays is much higher than twenty years ago. The anachronism of the old developments from the perspective of security and the two major reactor accidents with significant implications – Three Miles Island in 1979 and Chernobyl in 1986 (see below) – has prompted the nuclear power plant owners to significantly increase the safety level of their plants. Therefore, the reactors operating these days are equipped with multiple safety systems. The safety of nuclear power stations means that the plants must be designed with every technical equipment and security system able to guarantee the safety of the plant's environment, in case of a major accident. The review of the security and the continuous development to improve it is an elementary requirement from the owners.

The Government of Hungary delegated control of the nuclear power station to the National Nuclear Energy Authority, similarly to the other nuclear facilities (KFKI Research Reactor, BME Training Reactor, Irradiated Cassettes Transition Storage Facility etc).

The implementation of nuclear safety starts with the planning of the nuclear power plant: it must be built and operated in such way that in case of an accident it guarantees the safety of the environment.Through the operation it should make every effort to increase its' security. It is based on regular overview and reassessment of the security situation in order to ensure that the new scientific achievement and operating experience of other plants are utilized in every nuclear power plant. [3]

2.2. For the safe operation

The safe operation of a nuclear power plants is one of the most important criteria. There is a large amount of radioactive material in a nuclear reactor and against it's radiation the facility staff must be protected. In case of an accident leakage must be prevented.

In the nuclear reactor three basic conditions must be fulfilled.These are:

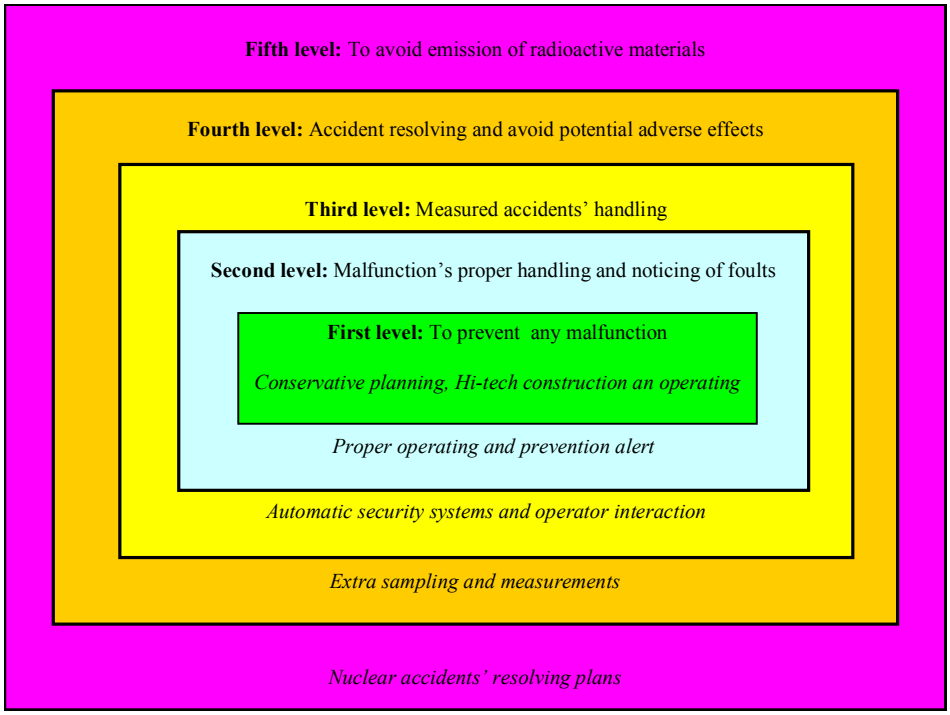
- effective control of the nuclear chain reaction;
- the proper conveyance of generated power;
- prevention of the loss of radioactive material.

The safety functions of nuclear reactors are implemented using the so called ”defence in depth”.

3. THE DEFENCE IN DEPTH

This is a theory developed in the 1990s by the International Nuclear Energy Agency. Every country's authority has to enforce greater effect of this principle. The defence in depth is linked to the relevant level of the above mentioned three conditions. The five levels of defence in depth principle settle the security-related offenses, equipment, procedures. Each is designed to prevent to achieve the next level. [4] (see Figure 1.)

[4] Teller Ede: A biztonságbizonytalansága



1. figure. "Virtual defence in depth"
Forrás: www.agr.unideb.hu/ktvbsc/dl2.php?dl=17/14_eloadas.ppt; (2011. október 24.)

First level: The entire plant must be designed so that it's resistance against the internal faults is the greatest possible or these errors occurs least frequent possible. Then on this basis, the facility must be designed, to ensure of course an adequate safety margin of error. The possibility of human error must be excluded as much as possible or human-managed devices must be transparent and easy to operate. The workers must be selected for the job properly – taking into account the psychological stress also. It must be specified which external events are important to withstand without damage to the system. Another important factor is the selection of the site for future power plants. Clear responsibilities should be determined from the design phase to the operation.

Second level: The facility must be kept within the designed operating limits and a separate device must be provided to prevent any violation of safety constraints. Instruments like this are: constant measurements, periodic testing, constant maintenance, periodic testing of security systems. Care should be taken to display accurate operation of instrumentation, without any delay every error should be fixed, even if this results drops of production. Every effort should be taken in practice to eliminate errors which could be abolished theoretically.

Third level: The aim of the first two levels of defence in depth is to make smaller the chance for errors. In spite of this the potential for malfunctions and accidents can not be excluded. Therefore the system should be prepared for some so-called "plausible accidents". These "plausible accidents" derive from reasons that despite the constant controls can not be excluded. Therefore, we need systems that help manage the expected emergency situation. These security systems shall be designed so that they initiate automatically and human intervention is permitted only after a certain time – when the situation has been cleared, defined and reviewed. In case of any plausible accidents these systems maintain the integrity of the active zone.The leakage of radioactive substances are therefore, constrained to the proper level even in the case of the worst plausible accident.

Fourth level: The system must be prepared for worse case scenarios as well, which lead to accidents formerly classed as non-plausible or more than one error occurs at a time. In this case the security systems do not provide adequate protection, the most dangerous situation for the reactor may occur: “zone melting”, which is is accompanied by highly radioactive emissions. So the goal here is to reduce the chance of these kinds of events among the given conditions and to insert additional systems, which reduce the extent of the zone melting, or at least delay, allow time for any other action (such as evacuation of the population).

Fifth level: Provision must be taken for the event of radioactive emission. These measures are necessary just in case the first four levels’ measures proved ineffective. This level of course is not longer the responsibility of the plant, but requires authorities’ action. These tasks should be incorporated into a contingency plan and all the decisions should be based on this or on the opinion of the subject matter expert team. It is imperative to run the system smoothly in emergency situations, therefore periodic re-training shall take place with the involvement of the applicable agencies (eg: National Nuclear Energy Agency, Disaster, Health).

4. THE ENGINEERING BARRIERS (TECHNICAL SOLUTIONS)

The so-called ”engineering barriers“ prevent the leakage of radioactive substances into the environment either in normal or in emergency situations. The primary role of the certain dams is to prevent the radioactive material from reaching the next dam. The primary aim of safety analysis is to determine whether, these dams work properly in normal mode, in normal operations or in case of an emergency situation.

The first engineering dam is the fuel lozenge itself, the major part of fission products created during the operation embedded into the nuclear fuel matrix which would prevent their evasion.

The second engineering dam is the case of thenuclear fuel rod, in which the uranium dioxide pastilles are filled. These – mostly of zirconium alloy cases – are filled with inert gas and are hermetically sealed. Thus, the jacket locks the gaseous fission products. In normal mode the first two engineer dams are responsible for the retention of radioactive materials.

The third engineering dam in the reactor tank itself, within the tank is the active zone and the primary circuit. The stainless steel reactor tank is calibrated for extreme temperature and pressure thus in case of possible damage to the fuel it gives additional protection against leakage of radioactive materials into the environment.

The fourth engineering dam is the safety building itself that includes the entire primary coolant circuit, the containment, which is calibrated for the over pressure created during a so called scaling accident and continuously kept ventilated controlled manner through filters.

5. INTERNAL AND EXTERNAL SECURITYSYSTEMS

We can speak of internal or inherent safety, if the reactor is designed in such way that the increase of the reactor power reduces the reactivity of the reactor, so the number of the fissions, ergo the output itself. These negative feedback loops based on physical processes therefore it cannot be deactivated, so in case of an accident or in an emergency situation it protects the reactor in the so-called ”run away”.

The aim of the external security systems is to control the reactor’s output, to inactivate if necessary, to remove the released heat and to prevent the leakage of radioactive material. This latter function is fulfilled by the previously mentioned engineering dams. The chain reaction is stopped and controlled in the short term by the control rods, for long term boric acid

dissolved in the primary coolant is used. They absorb free neutrons in the reactor, thereby reducing the number of fissions. [5]

It is the nature of nuclear power plants that the heat generation in the reactor is not finished immediately after the chain reaction was terminated as the generated heat[5] previously to be released. Immediately after termination this residual heat is 7% of the nominal operating output which is decreasing as time passes. Because of this remanentheat effective cooling of the reactor is required not only during normal operation, but even after the termination. The emergency cooling systems are an important part of the external security systems because these perform this task even in the case of damage of the primary cooling circuit. The nuclear power plants nowadays are designed in such a way that even if the largest diameter primary circuit breaks[6] the cooling of the reactor can be provided adequately.

The safety systems are built multiple based on the principle of redundancy so that the defence system remains viable despite the failure of any element. The principle of diversity means that the parts of the system are produced by several different manufacturers or based on different principles of operation so that the common-mode failures can be avoided.

An important component of safety is the operator's commitment to security and the organization's safety culture. It can be strengthened by high standard continuous education of the operators and maintenance personnel and by the strong safety-awareness approach. It is basic criteria for operators of nuclear installations and their leaders that security is considered top priority, and that they remain vigilant in their daily work. The technical systems and the staff together can provide the required safety standards.

6. SECURITY FEATURES OF IMPLEMENTATION

The proper design, engineering dam and defence in depth are illustrated in the two worst nuclear power accidents and the description of the incident in Paks.In 1979 in the United States, in the second block of the Three Mile Island nuclear power plant after the loss of coolant and operator error caused partial zone melting. The melt, however, remained within the reactor tank. The containment fulfilled its function and retained the majority of the radioactive material. Only some radioactive inert gas emissions occurred, but this was only a negligible additional radiation caused to the population. [6]

The other accident was not as lucky. In the fourth block of the Chernobyl Nuclear Power Plant in April 1986 there was a serious reactor “run away” accident. Construction errors made the incident even worse since the reactor did not have negative feedback necessary for inherent security; on the top of it the external security system was deactivated and this led to a reactor explosion. The lack of a heavy duty reactor tank, suitable protective reactor building led to the absence of other safety means which are required in Hungarian or in the western reactors. This resulted in a large environmental release and the population radiation exposure was very significant. [7]

Speaking about nuclear safety, we have to mention the incident that occurred in April 2003 in the second block of the Paks Nuclear Power Plant. In a temporary installed underwater outside cleaning tank of the reactor, thirty heather cases were damaged. The damage was caused by inappropriate cooling. The residual heat was high and the cases became overheated and brittle thus after inundating flooding they became crumbled. Part of the gaseous radioactive fission products from the damaged nuclear case escaped into the environment (the first two engineering dams were damaged), but there was no significant contamination.

[5] or remained heat

[6] so called: pipe breaking or coolent-lost malfunction

7. THE FUKUSHIMA ACCIDENT FROM AN ENGINEER'S POINT OF VIEW

The earthquake that hit Japan in March 2011 was several times more powerful than the worst earthquake the nuclear power plant was built for. When the earthquake hit the nuclear reactors all automatically shut down. Within seconds after the earthquake started, the control rods had been inserted into the core and the nuclear chain reaction stopped. At this point, the cooling system should carry away the residual heat. The earthquake destroyed the external power supply of the nuclear reactor. This is a challenging accident for a nuclear power plant, and is referred to as a "loss of offsite power." The reactor and its backup systems are designed to handle this type of accident by including backup power systems to keep the coolant pumps working. Furthermore, since the power plant had been shut down, it cannot produce any electricity by itself.

For the first hour, the first set of multiple emergency diesel power generators started and provided the electricity that was needed. However, when the tsunami arrived it flooded the diesel generators, causing them to fail. A large tsunami that disables all the diesel generators at once is such a scenario, but the tsunami was beyond all expectations. When the diesel generators failed after the tsunami, the reactor operators switched to emergency battery power. After 8 hours, the batteries ran out, and the residual heat could not be carried away any more. At this point the plant operators begin to follow emergency procedures that are in place for a "loss of cooling event." These are procedural steps following the "Depth in Defence" approach. All of this, however shocking it seems to us, is part of the day-to-day training you go through as an operator.

At this time people started talking about the possibility of core meltdown,[7] because if cooling cannot be restored, the core will eventually melt (after several days), and will likely be contained in the containment. However, melting was a long way from happening and at this time, the primary goal was to manage the core while it was heating up, while ensuring that the fuel cladding remain intact and operational for as long as possible.

Because cooling the core is a priority, the reactor has a number of independent and diverse cooling systems such as the reactor water cleanup system, the decay heat removal, the reactor core isolating cooling, the standby liquid cooling system, and others that make up the emergency core cooling system.

Since the operators lost most of their cooling capabilities due to the loss of power, they had to use whatever cooling system capacity they had to get rid of as much heat as possible. But as long as the heat production exceeds the heat removal capacity, the pressure starts increasing as more water boils into steam. The priority now is to maintain the integrity of the fuel rods by keeping the temperature below 1200°C, as well as keeping the pressure at a manageable level. In order to maintain the pressure of the system at a manageable level, steam and other gases have to be released from time to time. This process is important during an accident so the pressure does not exceed what the components can handle, so the reactor pressure vessel and the containment structure are designed with several pressure relief valves. So to protect the integrity of the vessel and containment, the operators started venting steam from time to time to control the pressure.

During this time, mobile generators were transported to the site and some power was restored. However, more water was boiling off and being vented than was being added to the reactor, thus decreasing the cooling ability of the remaining cooling systems. At some stage during this venting process, the water level may have dropped below the top of the fuel rods. Regardless, the temperature of some of the fuel rod cladding exceeded 1200 °C, initiating a

[7] Note that the term "meltdown" has a vague definition. "Fuel failure" is a better term to describe the failure of the fuel rod barrier (Zircaloy).

reaction between the Zircaloy and water. This oxidizing reaction produces hydrogen gas, which mixes with the gas-steam mixture being vented. This is a known and anticipated process, but the amount of hydrogen gas produced was unknown because the operators didn't know the exact temperature of the fuel rods or the water level. Since hydrogen gas is extremely combustible, when enough hydrogen gas is mixed with air, it reacts with oxygen. If there is enough hydrogen gas, it will react rapidly, producing an explosion. At some point during the venting process enough hydrogen gas built up inside the containment (there is no air in the containment), so when it was vented to the air an explosion occurred. The explosion took place outside of the containment, but inside and around the reactor building there was no safety function.[8]

Since some of the fuel rod cladding exceeded 1200 °C, some fuel damage occurred. The nuclear material itself was still intact, but the surrounding Zircaloy shell had started failing. At this time, some of the radioactive fission products[9] started to mix with the water and steam that was released into the atmosphere.

Since the reactor's cooling capability was limited, and the water inventory in the reactor was decreasing, engineers decided to inject sea water[10] to ensure the rods remain covered with water. Although the reactor had been shut down, boric acid is added as a conservative measure to ensure the reactor stays shut down. Boric acid is also capable of trapping some of the remaining iodine in the water so that it cannot escape, however this trapping is not the primary function of the boric acid.

This process decreased the temperature of the fuel rods to a non-damaging level. Because the reactor had been shut down a long time ago, the decay heat had decreased to a significantly lower level, so the pressure in the plant stabilized, and venting was no longer required. [8]

8. CONCLUSION

To create a safe environment is the task of the operators of the power plant. It is well known that the radioactive material used in power plants has a risk itself to the environment. Having this knowledge the experts are working constantly to ensure nuclear safety. In our analysis we worked out of those technical solutions of the nuclear power plant whose task is during the operational function to prevent the escape of radioactive materials into the environment, thereby ensuring nuclear safety. We reviewed the interpretation of security, the implementation of the safety functions and finally we described the technical solutions used for preventing the leakage of radioactive substances into the environment. The safe operation of the large number of currently operating nuclear reactors in the world demonstrates the precise engineering calculations. "The nuclear energy in the hands of intelligent people is not dangerous."[11] As a matter of fact only one single nuclear accident – the one that happened last year at Fukushima – is able to radically change this view.

Felhasznált irodalom

[1] Aszódi Attila: ATOMERŐMŰVEK AVILLAMOSENERGIA-TERMELÉSBEN Magyar Tudomány 2007/01 p11. ISSN 0025-0325

[2] Holló Előd: ATOMERŐMŰVEK KOCKÁZATÁNAK ÉRTÉKELÉSE; Magyar Tudomány 2007/01 p19.*ISSN* 0025-0325

8This explosion destroyed the top and some of the sides of the reactor building, but did not damage the containment structure or the pressure vessel. While this was not an anticipated event, it happened outside the containment and did not pose a risk to the plant's safety structures.

9 e.g.cesium and iodine

10mixed with boric acid – a neutron absorber

11 source: Teller Ede: visit in Paks NPP

[3] BukovicsIstván - VavrikAntal: INFRASTRUKTÚRÁK KOCKÁZATA ÉS BIZTONSÁGA Hadmérnök I. Évfolyam 3. szám - 2006. december p9. ISSN 1788-1919

[4] Dr. Trampus Péter: A VIRTUÁLI MÉLYSÉGI VÉDELEM KONCEPCIÓ ALKALMAZÁSA A REAKTORTARTÁLY BIZTONSÁGÁNAK IGAZOLÁSÁRA Magyar Energetika 2005/1 ISSN 1216-8599

[5] Hamvas János: FIZIKUSOK A PAKSI ATOMERŐMŰBEN; Fizikai Szemle 2000/11. p 398. *ISSN* 0015-3257

[6] OPEN SOCIETY ARCHIVES; http://www.osaarchivum.org/guide/rip/10/TheExhibitionIII.html; (2011.október 14.)

[7] Kováts Balázs: A NUKLEÁRIS IPAR ÉS A TÁRSADALOM; Magyar Tudomány 2001/11 in1364-1367 *ISSN* 0025-0325 http://www.matud.iif.hu/01nov/kovats.html; (2011. október 21)

[8] Josef Oehmen: INFORMATION ABOUT THE INCIDENT AT THE FUKUSHIMA NUCLEAR PLANTS IN JAPAN; http://mitnse.com/2011/03/13/modified-version-of-original-post/; (2012. november 1.)