The Final Safety Analysis Report and its Safety Analyses Chapter for the Paks Nuclear Power Plant

Sándor Szirmai, HAEA

1. Development of the present form of the Final Safety Analysis Report

The construction and installation procedures of the Paks NPP followed a practice close to the western standards. Based on the Technical Plan presented by the Supplier, a Pre-construction Safety Analysis Report was developed, and later a Pre-operational Safety Analysis Report, which had the same role as the Final Safety Analysis Report (FSAR). The construction and installation procedures formally did not (or not much) differ from the standards accepted elsewhere.

Regarding their content, it is rather difficult to evaluate these Safety Reports. The Pre-construction Safety Analysis Report and later the Pre-operational Safety Analysis Report was convincing for the professionals by presenting the safety of the NPP and by drafting the realisation of the safety goals for several operational occurrences and accidents with the aid of the equipment designed to handle these events. There were although several deficiencies compared to the western requirements.

One of the most important steps in supplying these deficiencies was the AGNES project carried out between 1991 and 1994. The project - being aimed at reassessing the safety of Paks NPP corresponding to the state-of-the-art of those years - had also the goal of establishing the foundation of an up-to-date Safety Report, to eliminate the deficiencies of the Pre-operational Safety Analysis Report. The analyses performed during the project and the prepared documentation served as a good basis for compilation of a state of art new Safety Report.

The analyses carried out to establish the proposed Safety Improving Measures and the compilation of the first PSR report (for units 1 and 2) meant an important leap forward to update and complete the SAR.

The first volume of the new Nuclear Safety Code (an Appendix to the Atomic Act) prescribes the regulatory procedures for the NPPs. For a new plant two safety reports are required: prior to the construction the Preliminary Safety Report and prior to commissioning the Final Safety Analysis Report. The US NRC Reg. Guide 1.70 served as basis of the regulations. The FSAR has to be actualised after the evaluation of the results of commissioning and then, after any modifications related to the safety, on a yearly basis.

In the FSAR - according to an agreement with the licensee - the 4-unit plant is described together, and the unit-specific details are treated separately.

The procedures for editing and modifying the Final Safety Analysis Report was determined to ensure that all the details and peculiarities are described and discussed, which are necessary for judging the safety and for providing up-to-date, valid description of the plant.

2. Regulatory approval and updating of FSAR

The FSAR was submitted to the authority in 2000. The reference date of the FSAR was chosen as March 31, 1998, because this was the reference date of the Periodic Safety Review for the units three and four. Choosing the same reference date made possible to re-use parts without modifications from the Periodic Safety Review. Exception from this reference date is the chapter 15 (Safety Analysis), where the latest PSA results are presented.

The submitted FSAR was reviewed and approved by the Authority, due to its substantially higher standards and deeper analyses compared to the original Pre-operational SAR. At the same time, the Regulator ordered a very deep updating, completion and re-edition work on the report to meet the true internationally acceptable level. To allow enough time for the licensee the next FSAR update is scheduled for year 2003.

3. The contents of the FSAR

The structure of the Final Safety Analysis Report is based on US NRC Reg. Guide 1.70. Rev.3. The chapters of the FSAR are as follows:

1. Introduction and general description of the plant
2. Description of the site
3. Design of systems and components

4. Reactor
5. Reactor coolant system and connected systems
6. Safety protection systems, components
7. Instrumentation and control
8. Electric power supply systems
9. Auxiliary systems
10. Steam and power modification systems
11. Radioactive waste management
12. Radiation protection
13. Conduct of operation
14. Commissioning program
15. Safety analysis
16. Conditions and limitations of operation
17. Quality assurance
18. Preliminary program of decommissioning of the nuclear power plant and its units

4. The Safety analysis chapter

The chapter 15 of the FSAR is a kind of a summary, which contains information enough to judge the design safety of the plant units in various accident situations. This chapter does not contain each analysis and description in full detail, rather it refers to the detailed analyses and descriptions. Therefore this chapter and the background materials consist the whole system of information needed to evaluate in full-scope the safety of the units.

The chapter 15 of the FSAR is mainly based on the results of the AGNES project elaborated in three years, the final report summarising these results, and other safety analyses prepared since then.

The reference unit for the AGNES project is the unit 3. While supplying the input of the analyses and drawing the conclusion in many cases it was possible to take into account the different data of the other units, thus the main conclusions apply to every unit.

Fulfilment of special design principles

This subchapter presents the analyses proving the satisfaction with the single failure criterion and the common cause failures. The common cause failures caused by the spatial position were analysed for fire, flooding, and high energy breaks. Among the external events the seismic risk drew a great attention. As the analysis of the accident situations assumed the realisation of some special safety functions, the cases of the inadvertent decreasing of the boron concentration and the load-bearing capacity of the containment building were presented here.

Accident analysis

The accident analyses have been prepared to cover the full design basis. The original design basis has been extended to a significant degree (e.g. earthquake). This chapter presents the accepted methodology and the results of the analyses. The analyses follow rather closely the logic of the US NRC Reg. Guide 1.70, for chapter 15, touch upon the evaluation of the pressurised thermal shock (PTS), and the investigation of some transients assumed without scram actuation (ATWS). This chapter presents those accident analyses, which have been performed to determine the success criteria for the PSA of non-nominal power cases.

Probabilistic safety analyses

During the level I probabilistic safety analyses the event trees have been prepared for all states of the units for initial events of technology origins, and also the failure trees containing failure-logic relationships. The human factor has also been quantified. The full reliability database has been prepared. Based on these, the core damage frequency could be determined. The PSA analyses include also the sensitivity and uncertainty studies. According to these results and also on the basis of the AGNES deterministic analyses the priorities of the Safety Improving Measures were determined. Since the first PSA analysis prepared in the framework of the AGNES project, the probabilistic analyses are updated every year. As the PSA has been updated since the reference date of the Final Safety Analysis Review, reference date of the PSA is the 1st of January 1999.

Severe Accident Evaluation

The aim of the severe accident evaluation - based on deterministic analyses of some basic accident processes and taking into account the literature of this topic - was to get a realistic view on how the severe accident scenarios can take place on the Paks NPP units. The chapter presents the results of analyses, and draws conclusions on the in-vessel processes and the containment processes, including the spreading of radioactive material. The chapter also contains some strategies of preventive and mitigative procedures, to be worked out.

5. Accident analysis

In this chapter the accident analyses are presented, which were made on the basis of the AGNES project and the Periodic Safety Review, and the extended analyses, which were prepared for establishing the Safety Improving Measures. The structure of the analyses is as follows:

Design Basis Analysis (DBA)

In the Design Basis Analyses it had to be verified that the plant safety systems are suitable to cope with the consequences of such accidents. The aim of the analyses is to prove that the acceptance criteria are satisfied.

The analyses are arranged into three groups: thermohydraulic transients, transients caused by reactivity anomalies, and analysis of auxiliary systems for radioactive release.

For the reactivity transients 1D or 3D core calculations are performed, depending on the type of transient. It is important to take into account the thermohydraulic feedback. For the analysis of thermohydraulic transients different codes were used depending on the processes. In cases involving the failure of the primary circuits, the activity transport and dose calculations were performed as well. For auxiliary system analysis ad hoc methods are used, but for dose calculations the same methods are used as for the LOCA transients.

Anticipated Transients Without Scram

The ATWS analyses have been performed using realistic, nominal operational data as initial state, according to the international practice. The inclusion of this transient vas decided - in spite of its very low probability - to satisfy the international requirements.

Pressurised Thermal Shock (PTS) of the reactor vessel

The thermal shock is important mainly for pressure vessels of older construction, having weak material properties. The Paks NPP vessels have good material properties, nevertheless the accident analyses include the PTS analysis.

During the life-time of the reactor the vessel is exposed to several of anticipated transients causing significant cool-down (thermal shock), possibly while the primary pressure remains high. Therefore it has to be verified that during its design life-time the reactor vessel can not fail during PTS events, even taking into account its embrittlement.

The assumed initial events

The first step of the analysis is to fix the initial events to be analysed. According to the experience of decades of operation and authorisation, the initial event list of the Regulatory Guide 1.70 issued by the US NRC properly covers the expectable transients and accidents, which are the most important for the safety of a PWR plant and its environment, taking into account their probability and consequences. The FSAR contains the analysis of these initial events, completing the list with those initial events, which are specific as expectable for VVER plant's accidents.

According to their expected frequency, the initial events for Design Basis Accidents are grouped into two categories:
1. Anticipated Operational Occurrences (AOO);
2. Postulated Accidents (PA)

The expected frequency for AOO events are greater than 10^{-2}/year, for PA events less than this value.

The groups of initial events are as follows:
1. Increase of heat removal by the secondary system
2. Decrease in heat removal by the secondary system
3. Decrease in primary coolant inventory
4. Reactivity and power distribution anomalies
5. Increase in reactor coolant inventory
6. Decrease in reactor coolant inventory
7. Radioactive release from subsystems and components
8. Anticipated Transient without Scram (ATWS) cases
9. Pressurised thermal shock (PTS) cases

Acceptance Criteria for AOO Cases

Criterion C1

An initiating event shall not generate a plant condition with more serious consequences than permitted for the given category (anticipated operational occurrence) without an additional independent failure.

Criterion C2

An occurrence by itself or in combination with an additional active component failure or operator error shall not result in loss of function of any barrier including the fuel cladding. However, if the combined frequency of an occurrence plus an additional component failure or operator error is below 10-2/unit/year, a limited number of fuel cladding failures may be accepted. Fuel cladding failures are assumed as per Criterion C4.

The most limiting plant system single failure(s) or operator error is identified and assumed in the analysis.

Criterion C3

The probability of experiencing a heat transfer crisis anywhere in the core shall be low. It is required that there be a 95 % probability, at the 95 % confidence level, that the limiting fuel rod does not experience a departure from nucleate boiling (DNB). The applied DNB correlation is based on experimental data that are relevant to the particular core cooling conditions and fuel design.

If the DNB ratio falls below these values, fuel failure (rod perforation) must be assumed for all rods that do not meet these criteria unless it can be shown, based on an acceptable fuel damage model, that fewer failures occur.

Criterion C6

The plant is considered adequately designed and the primary and secondary coolant activities adequately limited, if calculations show that the resulting doses, with an assumed event generated iodine spike and with equilibrium iodine concentration for continued full power operation, are below the limits chosen for AOO. These dose limits are:
- the effective dose equivalent at the plant site is less than 15 mSv/a, the thyroid dose equivalent is less than 150 mSv/a,
- outside the plant site the effective dose equivalent is less than 0.1 mSv/a, the thyroid dose equivalent is less than 1 mSv/a.

Criterion C8

Pressure in the reactor coolant and main steam systems shall be maintained below 110 % of the design value.

Acceptance Criteria for PA Cases

Criterion C1

An initiating event shall not generate a plant condition with more serious consequences than permitted for the given category (postulated accident) without an additional independent failure.

Criterion C4

Fuel cladding failure shall be assumed for all rods where one or more of the following conditions occur:

a) The cladding is overheated. Fuel rods experience a departure from nucleate boiling as per Criterion C3.
b) The fuel pellets are overheated. The fuel pellet temperature reaches melting temperature at any point. (The fuel melting point is 2840 ºC for fresh fuel and 2670 ºC for spent fuel.)
c) Excessive fuel enthalpy is produced. The radially averaged fuel enthalpy exceeds 586 J/gUO2 (140 cal/g) at any axial location in the fuel rod. The reference temperature for enthalpy is 298 K.
d) Other mechanisms. Other possible fuel rod failure modes, e.g. mechanical impact, or ballooning and rupture due to internal pressure.

Criterion C5

In the postulated accident conditions the primary reactor coolant system shall be maintained in a safe state so that short term and long term coolability of fuel can be maintained. It has to be proved that the following requirements shall be met:

a. The emergency core cooling criteria shall be met:

- The calculated maximum fuel rod cladding temperature does not exceed 1200 oC.
- The calculated total oxidation of the cladding does not exceed 17% of the total cladding thickness before oxidation.
- The calculated total amount of hydrogen generated from the chemical reaction of the cladding with water or steam does not exceed 1% of the hypothetical amount that would be generated if all the metal in the cladding cylinders surrounding the fuel, excluding the cladding surrounding the plenum volume, were to react.
- Calculated changes in core geometry are such that the core remains amenable to cooling.

b. The radially averaged fuel enthalpy shall not exceed 963 J/gUO2 (230 cal/g) at any axial location in any fuel rod. The reference temperature for enthalpy is 298 K.

Criterion C7

The plant is considered adequately designed and the primary and secondary coolant activities adequately limited, if calculations show that the resulting doses, with an assumed event-generated iodine spike and with equilibrium iodine concentration for continued full power operation, are below the limits chosen for PA. These dose limits are:

- the effective dose equivalent at the plant site is less than 50 mSv/event, the thyroid dose equivalent is less than 500 mSv/event,
- outside the plant site the effective dose equivalent is less than 5 mSv/event, the thyroid dose equivalent is less than 50 mSv/event.

Criterion C9

Pressure in the reactor coolant and main steam systems is maintained below 135% of design limits, taking into account potential embrittlement as well as ductile failures, and taking into account the fuel.

In certain special cases the above criteria are supplemented with the following:

Criterion C10

The plant technical specifications should include a provision requiring that reactor instrumentation be used to search for potential fuel loading errors after refuelling operations.

Criterion C11

From the time that an alarm makes the operator aware of unplanned moderator dilution the following minimum time intervals must be available before criticality is reached or the shut-down margin of the reactor is completely lost:

a. during refuelling: 30 minutes
b. during start-up, cold shut-down, hot stand-by and power operation: 15 minutes.

Criterion C12

The core shall not be uncovered during accidents in the course of refuelling.

Criteria applied for the PTS analyses

Special criteria were applied for the PTS analyses:

Criterion PTS-1: The crack initiation safety factor shall exceed the value 1.1.
Criterion PTS-2: The pressure at the stable end state of the system shall not exceed the permitted value associated with the given temperature.

6. Conclusions of the safety analyses

According to the initial event list each initial event has been analysed, which is considered important at present in the world.

The results of the analyses verified that there are considerable safety margins on the systems of the units. For most of the initial events studied the plant fulfils the requirements even with the minimal configuration of the safety systems. The strict application of the single failure criterion was only needed to fulfil the criteria at the 200% cold leg break, the inadvertent withdrawal of the control assemblies, and for steam line break. There were weaknesses revealed which have to be followed with attention during the operation, and appropriate measures are needed to avoid the worsening of the situation.

For the 200% cold leg break the minimal configuration has not proved to be satisfactory (the design criterion for the emergency cooling system is that it can perform its function with a single failure).

The inadvertent withdrawal of the control assemblies caused a not too serious violation of criteria only if the reactor period protection was omitted.

The other potentially dangerous group of loss of cooling accidents consists of those when the primary coolant flows outside of the containment (break of steam generator heat exchanger tube, lift-off the steam generator collector lid, flow to the MCP intermediate circuit). In these cases the water does not flow into the sump, and this causes loss of the core integrity when the emergency core cooling tanks inventory is running out and the brake isolation is not completed in time and primary water supply is not available from other sources.

The steam line break study has shown that although recriticality may occur, but the critical heat flux is not exceeded. The reason of the recriticality is that the pressure difference between the steam collector and the steam generator does not initiate the steam generator isolation. (For large steam line breaks, in accordance with the assumed single failure this signal is omitted, for small breaks the signal does not appear at all). There is a measure in progress to apply a new "steam header pressure low" signal on the units.

The study of accidents causing high secondary pressure has shown that even while omitting the reducers to the atmosphere, the secondary pressure increases only slightly above the stem generator safety valve set point, because of the high capacity of the steam generator safety valves.

The study of the feedwater line breaks has shown that steam generator safety signals, which would cause the separation of the steam generator, do not appear, therefore this transient (which belongs to the "Decrease in heat removal by the secondary system" group, actually causes increase in the heat removal. This problem also will be solved by introducing the new "steam header pressure low" signal mentioned above.

For the reactivity transient cases it turned out that in some cases the reactor period protection is indispensable to avoid the violation of criteria. Therefore this protection can not be taken as diverse.

Very interesting and important result of the analysis, that during ATWS the system is not endangered and criteria are not violated, if realistic circumstances are assumed.

The study of the PTS transients led to unambiguous and clear result that in the operation procedures the primary break isolation can not be an absolute priority compared to avoiding the cold overpressurising of the vessel. This have been applied in the development of the new symptom-based operational procedures.

The containment analyses have shown that the containment pressure for design basis accidents remains under the design pressure. The steam line break studied with additional failures results in higher pressures than the design accident. In this case operator intervention is necessary after 30 minutes to avoid the limit violation.

The hydrogen generation is not taken into account in the original Technical Plan. Since then an emergency gas removal system has been installed for the possible generation of in-vessel generated gases, and hydrogen recombiners have been installed for the hydrogen removal from the containment, designed for Design Basis Accidents. The adequate functioning of the gas removal system and the recombiners have been verified by analyses.

For the events causing radiological consequences it has been proved that violation of the criteria does not occur. For the steam generator collector damage it was expected that it could cause problems because of the direct release to the environment, but the analyses have shown that the release of the primary activity even with the expectable spiking does not exceed the environmental limits.