AUSTRIAN REPORT

TO THE

EXPERT MISSION WITH TRILATERAL PARTICIPATION ACCORDING TO CHAPTER IV OF THE PROTOCOLL OF THE NEGOTIATIONS BETWEEN THE CZECH AND THE AUSTRIAN GOVERNMENT LED BY PRIME MINISTER ZEMAN AND FEDERAL CHANCELLOR SCHÜSSEL WITH THE PARTICIPATION OF COMMISSIONER VERHEUGEN

January 2001

CONTENTS

TEMELÍN DOCUMENTATION REVIEW STATUS

(Revision 1, 31 January 2001)

0.0 Executive Summary

In the Framework of the Agreement between the Government of Austria and the Government of the Czech Republic on Issues of Common Interest in the Field of Nuclear Safety and Radiation Protection Temelin issues had been discussed a long time. Since fall of last year the Czech and Austrian side have agreed to an in-depth technical review process which has emerged to a quite fruitful and open process. On 12 December 2000 Austrian Federal Chancellor Wolfgang Schüssel and Czech Prime Minister Milos Zeman agreed with Commissioner Günter Verheugen "to conduct a "trialogue" to find a better mutual understanding on the issue of the Temelin Nuclear Power Plant".

The present document was prepared for this Trialogue and provides a high-level summary of the review of Temelín documentation as well as a preliminary list of issues and indications, which replaces all former lists of questions, issues, etc. submitted to the Czech side. The ongoing intensive study of the plant documents such as POSAR and related literature reveals an unexpectedly growing number of potentially safety relevant indications and issues. This is reflected in the size of the list grown since last summer. Final clarification on the weight and potential resolution of the issues is expected in the forthcoming discussions on bilateral and trilateral expert level. Accordingly, the document is a of the nature of a status report - it is a snapshot in time of an ongoing process, not a final document issued at the completion of a fully realized process with analysis and deliberation on the issues concluded.

Following a bilateral meeting between the Czech and Austrian governments and experts on 2 September 2000, further bilateral interactions were commenced, beginning with a joint Parliamentary site visit to Temelín on 4 October 2000. Beginning on 28-30 November 2000, a review of Temelín documentation was initiated. The documentation consists in the main of the Temelín Pre-Operational Safety Analysis Report (POSAR) and the Temelín Probabilistic Safety Assessment (PSA). Other documents were also reviewed. Only the PSA is in English, while the POSAR and the other reference documentation is in Czech and requires an interpreter to be reviewed. As a result, the review process takes time and is focused on main parts of the section of interest in the documents being reviewed.
Applicable parts of the WENRA report, IAEA Safety issues and other EU funded activity were kept in mind by the experts performing the review work.

The POSAR and PSA document of NPP Temelín were considered for review. Portions of them have been reviewed together with some reference documentation made kindly available by the NPP. Based on the review, preliminary indications (see chapter 2.4) are available which can be summarized as follows:

A) <u>POSAR structure and general content</u>

The POSAR, dated December 1999 (Revision 1), is organized strictly in accordance with US NRC Regulatory Guide 1.70, and corresponds in general (as to structure) to western practice even if in some section the content is more limited compared to others.

B) General safety objectives, safety principles and criteria

General Safety Objectives of the design construction and operation are sufficiently defined, Safety Functions correctly addressed, concepts for safety and seismic classification of structures, systems, adequately introduced even if with no explicit indication of related requirements (covered in some reference documentation which is under review).

C) General conception of Temelin safety features

The general safety conception of Temelin Safety features is mainly based on three trains 100 % each which ensures more than a simple redundancy in front of a single failure. In addition Units 1 and 2 share two non safety diesels which can provide emergency AC power in case of Beyond Design Basis Conditions

D) Equipment seismic and environmental qualification

Equipment seismic and environmental qualification is an unresolved issue at Temelín NPP which is the object of an in–progress complex program to reassess and finalize the qualification of safety and safety related equipment by year 2002. The current status of this program, which does not appear from revised documentation, should be investigated.

E) Safety features design aspects

Indications have been collected about some limitations in the design, capability, or functionality of some safety features which are under review in order to ascertain the existence of real concern about their importance for safety.

F) Site seismic assessment

Assumptions and investigations made in the area of seismic assessment of the site appears to be not always consistent.

G) External events identification and definition

Additional effort for completeness of evaluation and definition of natural and external man-made with related safety provisions appear necessary.

H) Probabilistic Safety Assessment (PSA)

The Temelín PSA performed in 1995 when the construction was still in progress together with some design changes appear as needing to be reviewed for completeness, for more adequate modeling and also for quantification.

I) Miscellaneous

The Temelín plant has a full-time professional fire fighting organization of significant capability.

ISSUE IDENTIFICATION

The issues or areas of issues listed below have been identified due to the relevance for nuclear safety possibly associated with them (see chapter 3 of the report). On the basis of available documents and knowledge a ranking within these issues cannot be made. The issues are however organized into four groups , according to the preparatory effort still needed – minimum, medium and high. The confidence in the analysis of the relevance to nuclear safety is highest for the issues with minimum preparatory effort, the uncertainty whether the issues have a high relevance for nuclear safety or have been sufficiently addressed is greatest in issues with high preparatory effort still needed.

Issues with minimum preparatory effort

1. Containment bypass and primary-to-secondary (PRISE) leakage accidents
2. Natural Gas Pipeline Accidents and Their Effect on Temelín
3. Tornadoes

Issues with minimum to medium preparatory effort

4. Containment Design and Arrangement
5. Probabilistic Safety Assessment and Severe Accidents

Issues with medium preparatory effort

6. Emergency Operating Procedures (EOPs) and Severe Accident Management Guidelines (SAMGs)
7. Seismic Design and Seismic Hazard Assessment
8. Main Steam Line and Feedwater Line Breaks
9. Reactor Pressure Vessel Embrittlement and Pressurized Thermal Shock
10. Main Steam Line Safety and Relief Valves Qualification for Two-Phase and Water Flow
11. Status of IAEA Safety Issues resolution
12. Safety Classification of Components
13. Control Rod Insertion
14. Sump Screen Blocking and Suction Line Integrity
15. Reactor Coolant Pump Seal Integrity
16. Hydrogen Control
17. Limited ECCS/Containment Spray Sump Volume

Issues with high preparatory effort

18. Boron Dilution
19. Environmental and Seismic Qualification of Equipment
20. Ventilation System and Habitability Aspects of Control Rooms
21. Instrumentation and Control (I&C) Reliability
22. Non-Destructive Testing
23. Leak Before Break (LBB)
24. Conception of Safety Features
25. Design Basis Accident Analysis
26. Beyond Design Basis Accident Analysis
27. Safety Culture
28. NPP Organizational Structure and Management of Licensing Activities
29. Technical Basis for Temelín Emergency Planning Zones (EPZs)

1.0 INTRODUCTION

1.1 Background

In the Framework of the Agreement between the Government of Austria and the Government of the Czech Republic on Issues of Common Interest in the Field of Nuclear Safety and Radiation Protection Temelin issues had been discussed a long time. Since fall of last year the Czech and Austrian side have agreed to an in-depth technical review process which has emerged to a quite fruitful and open process. On 12 December 2000 Austrian Federal Chancellor Wolfgang Schüssel and Czech Prime Minister Milos Zeman agreed with Commissioner Günter Verheugen "to conduct a "trialogue" to find a better mutual understanding on the issue of the Temelin Nuclear Power Plant".

The present document was prepared for this ''Trialogue'' and provides a high-level summary of the review of Temelín documentation as well as a preliminary list of issues and indications, which replaces all former lists of questions, issues, etc. submitted to the Czech side. The ongoing intensive study of the plant documents such as POSAR and related literature reveals an unexpectedly growing number of potentially safety relevant indications and issues. This is reflected in the size of the list grown since last summer. Final clarification on the weight and potential resolution of the issues is expected in the forthcoming discussions on bilateral and trilateral expert level. Accordingly, the document is a of the nature of a status report - it is a snapshot in time of an ongoing process, not a final document issued at the completion of a fully realized process with analysis and deliberation on the issues concluded.

Temelín is a VVER-1000/320 pressurized water reactor which has been modified in response to recommendations from a variety of organizations, including incorporation of a revised core and control rod design and digital instrumentation and control (I&C) and protection systems supplied by Westinghouse.

Following a bilateral meeting between the Czech and Austrian governments and experts on 2 September 2000, further bilateral interactions were commenced, beginning with a joint Parliamentary site visit to Temelín on 4 October 2000. Beginning on 28-30 November 2000, a review of Temelín documentation was initiated. The documentation consists in the main of the Temelín Pre-Operational Safety Analysis Report (POSAR) [1] and the Temelín Probabilistic Safety Assessment (PSA). [2] Other documents were also reviewed. Unfortunately, only the PSA is in English, while the POSAR and the other reference documentation is in Czech and requires an interpreter to be reviewed. As a result, the review process takes time and is focused on main parts of the section of interest in the documents being reviewed.
Applicable parts of the WENRA report. IAEA Safety issues and other EU funded activity were kept in mind by the experts performing the review work.

1.2 Bilateral contacts

established have proven very fruitful and are irreplaceable for the development of a climate of mutual understanding between the experts. Furthermore – from an expert view – they constitute an element of utmost importance for the maintenance of trust within the Austrian population. The current document was prepared in the midst of an ongoing review of Temelín documentation, and ongoing bilateral expert contacts on various Temelín issues.

---

[1] POSAR is an English language acronym for Pre-Operational Safety Analysis Report. In the Czech language, POSAR is PpBZ (Predprovozní Bezpecnostní Zpráva). The POSAR is written in the Czech language. The POSAR version reviewed was Revision 1, December 1999.

[2] The PSA was prepared in the English language by a project team consisting of personnel from CEZ-ETE, Nuclear Research Institute Rež, Energoprojekt Praha, RELKO, EQE, Enconet, and other consultants. The PSA was issued in December 1995. Note that a revision of the PSA has recently been undertaken on behalf of CEZ, and that this revision will reflect the as-built and as-operated condition of the plant.

2.0 DOCUMENTATION REVIEW STATUS

This section of the report presents a status of the review of Temelín documentation. In the main, this review has considered the POSAR and the PSA.

2.1 POSAR Desktop Review Status

The portions of the POSAR which have been partially reviewed to date are as follows:

- Chapter 1, introduction, list of safety functions, basic plant data, list of safety systems and safety-related systems.
- Chapter 2, external hazards (natural gas pipelines and aircraft crash), geology, seismology, geotectonics, meteorology, and climatology.
- Chapter 3, Section 3.2, safety classification, Section 3.5, man-induced hazards, Section 3.6, Protection against dynamic impacts due to postulated pipe breaks, Section 3.8, containment design and reactor building layout, 3.10,Seismic input for electrical equipment and I&C systems, Section 3.11, equipment qualification.
- Chapter 4. Reactor (thermal and hydraulic design, reactivity control system), reactor core.
- Chapter 5, reactor vessel materials, reactor coolant pumps, steam generators, pressurizer safety valves, and pressurizer PORV (relief valve).
- Chapter 6, safety system design (containment, containment sprays, containment isolation, hydrogen recombiners, containment leak rate testing, emergency core cooling system, residual heat removal system, makeup pumps, main and emergency control rooms, sump screen blocking, ventilation systems, and emergency feedwater system).
- Chapter 7. Engineered safety features: Instrumentation and controls (engineered safety systems, safe shutdown systems).
- Chapter 8, electrical systems.
- Chapter 9, auxiliary systems design (spent fuel pool cooling system, makeup of spent fuel pool cooling system from containment spray system, spent fuel pool, essential service water system, intermediate cooling system, compressed air and nitrogen systems, fire detection & suppression systems, fire brigade, fire fighting systems, diesel generator systems, fire hazard analysis, and radioactive waste treatment & storage systems).
- Chapter 10, Steam and power conversion systems (main steam supply system, condenser).
- Chapter 13, Section 13.1, NPP organization structure and management, Section 13.5, emergency operating procedures.
- Chapter 15, safety analyses, Section 15.0, plant design conditions, list of design basis events and acceptance criteria for accident analysis, and other sections of Chapter 15 on steam generator tube rupture accident and leakage from primary to secondary system other than via steam generator tube rupture.
- Chapter 18, Section 18.2 concerning reactor operating modes.

2.2 PSA Desktop Review Status

With the exception of the detailed fault trees (only some of them have been studied), the entire PSA has been reviewed to date, some sections in more detail than others.

2.3 Other documents

In addition to the POSAR and the PSA, documents which have been completely or partially reviewed include the following:

- Ondrej Mladý, *NPP Temelín Safety Analysis Reports and PSA Status*, Temelín PSA Manager CEZ-ETE, Czech Republic, in IAEA, International Conference on the Strengthening of Nuclear Safety in Eastern Europe, IAEA-CN-75 (Vienna, Austria), 14-18 June 1999, pp. 235-259.
- Ján Štuller, Petr Brandejs, Alexander Miasnikov & Miroslav Šváb, *Regulatory Aspects of NPP Safety*, State Office for Nuclear Safety, Czech Republic, in IAEA, International Conference on the Strengthening of Nuclear Safety in Eastern Europe, IAEA-CN-75 (Vienna, Austria), 14-18 June 1999, pp. 215-229.

- Karel Krížek, et al., *NPP Temelín, Status of Safety Improvements*, in IAEA, International Conference on the Strengthening of Nuclear Safety in Eastern Europe, IAEA-CN-75 (Vienna, Austria), 14-18 June 1999, pp. 231-234.
- Frantisek Hezoucky, *Temelín NPP Status: The Challenge of Safety Improvements*, The Uranium Institute 25th Annual Symposium (London, United Kingdom), 30 August-1 September 2000.
- International Atomic Energy Agency, Report of the IPERS (International Peer Review Service) Phase 1 Review Mission for the Temelín Nuclear Power Plant Level 1 Probabilistic Safety Assessment in the Czech Republic, IAEA-RU-5628, WWER-SC-128, Division of Nuclear Safety (Vienna, Austria), 24 April to 5 May 1995. [3]
- EGP 4101-6-40396 „ Basic Concept of safety of Temelin Operation“ March ´95 .
- EGP 4101-9-970162 „ List of selected equipment“.
- EGP 4104-6-950004 „List of selected equipment“.
- VUEZ, Levice, Analytical and experimental assessment of the existing solution of the screen construction of the tank GA 201 from the point of view of accumulation of disintegrated insulation type JERZIL-Standard under conditions of maximum design base accident considerations for NPP Temelín, report A-ST-OTS-1126, 1998, main report and attachments.
- Cizek et al, 1993 Details of Tectonic.
- Novak and Jedlicka, 1992, Relations between Temelin NPP site and South Bohemian Basins in respect to usage of underground water sources.
- Pozdunik O., 1997, Geological supervision report on the results of the takeover of the reactor hall 2 , HUB JETE SG Praha p50834.
- Zdenek A. et al. 1993, Hydrogeological Area.
- Safety Issues And Their Ranking for WWER-1000 Model 320 Nuclear Power Plants, IAEA-EBP-WWER-05, March 1996
- Nuclear Research Institute Rez plc, Response to the IAEA document Safety Issues And Their Ranking, WWER-1000 Model 320 NPPs for Temelin NPP, March 2000

2.4 PRELIMINARY INDICATIONS

Based on the review conducted to date, we have the following preliminary indications (note that the review is ongoing, and thus this list is preliminary, subject to change, and subject to addition or deletion as additional review warrants). They are grouped for main areas of review still in progress and represent some first findings whose verification will be additionally addressed in the frame of the review for the overall set of issues identified in par.3 of this interim report.

A) POSAR Structure and general content

1. The POSAR, dated December 1999 (Revision 1), is organized strictly in accordance with US NRC Regulatory Guide 1.70, and corresponds in general (as to structure) to western practice.

2. The treatment of issues in the POSAR is in some instances limited where it should provide a more balanced insight. (For example for measures taken for preventing pipe whip on the 28.8 m level in case of pipe break, for measures taken for avoiding sump screen blocking in case of LOCA, and concerning information about type and qualification of installed safety and relief valves on main steam lines). (See issues 8, 10, 14).

3. According to modern requirements, the POSAR should contain a section dedicated to the general basis for decommissioning, dealing with those aspects which should be considered in advance during the construction and the operation of NPP. It seems that such section is missing from the Temelín POSAR.

[3] The IPERS report cited above is a publicly available document. Note that another IPERS mission, to review the Level 2 and external events analyses, was conducted by the IAEA from 15-19 January 1996. The mission report is not publicly available, and has not been reviewed to date.

B) General safety objectives, safety principles and criteria

4. The general Safety Objectives of the design construction and operation are sufficiently defined also with reference to document ''Basic Concept of safety of Temelin operation'', EGP 4101-6-940396', March '95. The identified Safety Functions necessary to address the safety conception of Temelín structures, systems, and components appears even and detailed.

5. The POSAR introduces basic concepts for safety and seismic classification of structures, systems, and components (SSCs). The concepts of Safety Systems and Safety related systems are introduced, but there is no explicit indication of related requirements (par.3.2.2 dedicated to safety Classification is made of only one page). These aspects are covered in some reference documentation which is under review (see issue 12).

C) General conception of Temelin safety features

6. The general safety conception of Temelin Safety systems is based on three trains 100% each which ensures more than a simple redundancy in front of a single failures.

7. The protection and engineered safety features (ESF) actuation systems are digital, with the Primary Reactor Protection System (PRPS) and the Diverse Protection System (DPS) provided for this purpose. We have found that the emergency control room is also equipped with hardwired controls to one train of essential equipment, as well as hardwired controls to limited non-safety equipment. Thus, in principle, if both the PRPS and the DPS fail, the operators can abandon the main control room, proceed to the emergency control room, and manually actuate one train of essential equipment to manage plant conditions. (In addition, of course, they could cause other plant actions by performing local actions, e.g., pulling fuses and breakers to trip the reactor.) Given the hardwired controls for one essential train of equipment, the situation is better than we had previously thought in terms of dealing with failures of the digital control and protection systems.

8. The ventilation systems for the main and emergency control rooms are separate systems, designed to prevent common mode failures from affecting both control rooms.

9. The Temelín prestressed concrete containment parameters (in terms of failure pressure and volume to thermal power ratio) were compared with comparable parameters for similar containment type PWRs in the US. Compared with recently completed US PWRs with prestressed concrete containments, Temelín compares well in terms of failure pressure and volume to thermal power ratio (assuming that the failure pressure analysis documented in the Temelín PSA is correct).

D) Equipment seismic and environmental qualification

10. Equipment seismic and environmental qualification is an unresolved issue at Temelín NPP which is the object of an in–progress complex program to reassess and finalize the qualification of safety and safety related equipment by year 2002. The content of the POSAR briefly describes the three steps of this program as it was conceived in 1999. The content of the program steps and the current status of the implementation is going to be reviewed based on reference documentation and NPP information. (See issue 19).

E) Safety features design aspects

11. Indications have been collected about some limitations in the design, capability, or functionality of some safety features which are under review (e.g., feed and bleed mode of operation for small break LOCA and loss of feedwater, emergency reactor coolant pump seal injection, steam generator tube rupture safety features, behavior and capability, lack of an intermediate cooling system for residual heat removal heat exchangers, etc.). (See issue 15, 17, 24).

12. Cold overpressure protection is provided by administrative controls, instead of incorporating some automatic features as recommended in IAEA-EBP-WWER-05.

13. The Temelín containment configuration, in which the bottom of the containment is elevated above local grade level, results in a risk of release of core debris outside containment which does not exist for western PWRs. Core debris can penetrate the bottom of the containment, and when it does the resulting depressurization of the containment into the reactor building (which is neither a containment nor a confinement) and structural failure of the reactor building due to pressure from steam and noncondensables, and possibly due to hydrogen combustion/detonation phenomena as well. (See issue 4).

14. The containment sump at Temelín serves as a common reservoir for the high pressure injection, low pressure injection, and containment spray systems. The volume of the Temelín sump is small compared with other VVER-1000 plants and very small compared with western PWRs. The Temelín sump volume is 500 m^3 (about 132,000 gallons), which is less than the Kozloduy 5-6 sump has 800 m^3 of water. Most comparable size western PWRs have "sump" volumes of between 950-1900 m^3 (about 250,000-500,000 gallons, Milstone 3 NPP 1 Millions gallons - more examples to come). This provides Temelín with comparatively less margin to deal with primary to secondary leakage (steam generator tube rupture, steam generator collector head leakage) events. [4] (See issue 17).

15. The ventilation systems for the reactor building (including the main and emergency control rooms) are <u>not</u> protected by automatic isolation in the event of ingestion of combustible gases or toxic gases. Reliance is placed on manual action by the operators to isolate the building ventilation systems under such circumstances. Neither the POSAR nor the PSA provide an analysis of the risks posed to operators by combustible or toxic materials. (See issue 20).

16. The pressurizer is equipped with a relief valve (called a PORV) which is preceded by a block valve. The PORV would be used to relieve overpressure, and to perform so-called feed and bleed cooling (used to cool the reactor when all feedwater is lost). The PORV block valve is always closed except when the primary pressure is in a narrow band (from 16.3-16.7 MPa). If the block valve does not open, it is irrelevant whether the PORV can open or not because flow is blocked. This arrangement introduces additional failure modes into primary pressure relief compared with most western PWRs. (See issue 24).

17. The "high pressure injection" system is in reality a medium pressure injection system which <u>cannot</u> inject emergency coolant into the primary coolant system until the system depressurizes below the shutoff head of the pump. In case feed and bleed cooling is necessary, it must be initiated by operator action within 33 minutes of loss of all feedwater, otherwise the primary system pressure stabilizes at a value above the shutoff head of the high pressure injection pumps, which results in failure of feed and bleed. (See issue 24).

18. The atmospheric dump valves (BRU-A) are still <u>not</u> demonstrated to be capable of passing two-phase flow or water flow while retaining operability of the valve. Failure of the valve in the open position with a leaking or broken steam generator tube (or with any other type of primary to secondary leakage) results in a more severe containment bypass sequence than would be the case from a cycling BRU-A valve. Note that IAEA-EBP-WWER-05, the IAEA's VVER-1000 safety issue ranking report, identified this as a safety issue with high preparatory effort. (See issue 10).

F) Site seismic assessment

19. Data on the design basis earthquake for Temelín differ among various Czech documents (e.g., National Report on the Convention on Nuclear Safety, Environmental Impact Assessment, etc.). An intensity of 6º on the MSK-64 scale is assumed as the design basis earthquake (strongest historical quake), and is said to correspond to a maximum horizontal peak ground acceleration of 0.06g, and for 7º corresponding to 0.1g. These are only global mean values and cannot be accepted as conservative ones. An intensity of 7º corresponds to 0.19g following the Soviet standard PNAE G7-9002-86, and even to 0.25g according to the French SCSIN standard.

[4] Another important factor is that the VVER-1000 SG tubes are larger in diameter than the western PWR SG tubes. Thus, a ruptured SG tube in a VVER-1000 is associated with a larger and therefore faster leak rate than if a tube in a western PWR ruptures. Combining this with the smaller volume in the VVER-1000 sump brings the issue into a more complete perspective.

20. The assumption that no higher earthquake than intensity 6º MSK-64 can be expected at Temelín is based only on isoseismal maps of known historical earthquakes, and not on a paleoseismological investigation including age determination of fault movements, which is the state-of-the-art. (See issue 7).

21. No paleoseismological studies are documented in either the POSAR or the PSA. (See issue 7).

22. The catalogue of historical earthquakes presented to the IAEA Site Safety Review Mission started its record in 1593, thus avoiding to mention the strongest known historical earthquake relevant for the Bohemian Massif (namely the Neulengbach quake of 1590). For this destructive earthquake, for which Gutdeutsch, et al. (1987) identified an epicentral intensity of 9º MSK-64. Because this event cannot be attributed to a fault, it must be considered to be attributed to the zone. For this zone, a maximum intensity of 10º MSK-64 must be assumed. According to Grünthal, et al. (Grünthal, G., Mayer-Rosa, D., Lenhardt, W.A. (1998): Abschätzung der Erdbebengefährdung für die D-A-CH-Staaten - Deutschland, Österreich, Schweiz. Bautechnik Jg.75 Okt 1998, H10, pp.3-17.), the distance between Temelín and the focal region attributed to the Neulengbach quake is 100 km. This results in an assumed intensity of 8º MSK-64 for the Temelín safe shutdown earthquake. Following the zoning model by Lenhardt (Lenhardt, A.(1995): Regional Earthquake hazard in Austria. 10th European Conf. on Earthquake Eng. Duma ed. Balkema, Rotterdam 1995. pp.63-68), the distance between Temelín and the boundary of the Neulengbach zone is only 30 km, which results in an intensity of 9º MSK-64 for the Temelín safe shutdown earthquake. (See issue 7).

23. The map of seismogenic zones in the POSAR differs much from that in the report by Energopruzkum (Simunek P. et al.(1995):NPP Temelin construction site – supplementary geological and seismological surveys, Part A – tectonics, Part B – seismic risk, Energopruzkum Praha, Internal Report for CEZ) and clearly depicts the problems with zoning: Sometimes boundaries of seismic zones follow state boundaries, sometimes they cross main tectonic structures and bend around Temelin (as in Schenkova Z., Schenk, V., Kárník, V. (1981).Seismic Hazard Estimate for a Low Seismicity Region - Example of Bohemia. Pageop., Vol. 119, pp. 1077-1092) or get out of its way stepwise as in the POSAR. Herein a girdle of unrealistic small zones lies between Temelin and the Neulengbach focal area. The POSAR's method of determining Io_{max} and M_{max} for single faults and zones has never been discussed in the international scientific community because it was never published in an international journal. On another map of the POSAR active faults (Rodl, Jachymov) end before they reach the area of Temelín. Despite a suspicious fault scarp of the Jachymov fault (Hluboka fault) a recent tectonic activity is denied in the POSAR. It seems that the investigations carried out for assuming a recent tectonic inactivity (described in the POSAR or in the Energopruzkum reports, Simunek P. et al.(1995):NPP Temelin construction site – supplementary geological and seismological surveys, Part A – tectonics, Part B – seismic risk, Energopruzkum Praha, Internal Report for CEZ) did not use adequate methods (paleoseismology) nor date the late Quaternary units and were not applied on the best locations, e.g. directly across the scarps. The results presented in the Energopruzkum reports rely mostly on intensities assumed from historical reports, boreholes and geoelectric measurements which are not sufficient to determine the location of faults and an age of the last fault activity. In contrast to the assumed tectonic inactivity in the POSAR previous works by Czechoslovakian authors presented indications of a young reactivation of Variscan shear zones with recent horizontal crustal movements along deep faults, active subsidence in the South Bohemian Basins and ongoing uplift in the adjacent mountainous areas e.g. the Bohemian Forest [Stovickova N., (1980): Tectonic Stresses as Determined from the Character of Fault Systems in the Bohemian Massif. Rock Mech., Suppl. 9, pp.125-138; Vyskocil, P., Kopecky (1974): Neotectonics and Recent Crustal Movements in the Bohemian Massif. Research Inst. Of Geodesy, Topography & Cartography, Praha; Vyskocil, P. (1975): Recent Crustal Movements in the Bohemian Massif. Tectonophysics 29, 349-358; Vyskocil, P., Zeman, A., (1979): Recent movements of the earth's crust in the region of the Bohemian Massif and its south-east border. Geodynamic Investigation in Czechoslovakia, VEDA,1979, pp.139-145; Zatopek, A. (1979): On geodynamical aspects of geophysical synthesis in central Europe. Geodynamic Investigation in Czechoslovakia, VEDA,1979, pp.91-104]. The map of Kutina (Kutina, J. (1976): Relationship between the distribution of big endogenic ore deposits and the basement fracture pattern – examples from four continents. Proc. 1st Int. Conf. on the New Basement Tectonics 1974,565-593, Utah Geol. Assoc. Pub.5) depicts microearthquakes lined up along the main deep seated faults. An absence of seismicity within a short period of monitoring cannot constitute a major

indication for the definition of a degree of activity in a given region. The seismic cycle and return period of large earthquakes can extend to several thousand years. (See issue 7).

24. Both POSAR and PSA assume a very low seismicity of the Bohemian region. Although shear zones in the South Bohemian Massif appear to have initiated as a system of conjugate wrench faults (dextral shear zones) in the late Variscan, Southern Bohemia and the adjacent Austrian part of the Bohemian Massif appear to be affected to a much greater extent by Alpine N-S-striking convergence. Because the Southern Bohemian Massif can be classified as part of the Alpine foreland the compressive deformation may represent clear indications for the existence of potential active zones in the Budejovice Basin. Statements in the report by Energopruzkum (Simunek P. et al.(1995):NPP Temelin construction site – supplementary geological and seismological surveys, Part A – tectonics, Part B – seismic risk, Energopruzkum Praha, Internal Report for CEZ) such as „active morpho-structure“, „rectilinear slopes with probable tectonic origin“, western „horst's margin“ of the Lisov threshold, the mentioning of the asymmetric basin, deformed terraces, younger tectonic movements and the existence of a thrust in the Upper Pliocene to late Pleistocene points out the contradictions concerning the assumed tectonic inactivity in the POSAR. A higher seismic hazard than assumed should therefore be taken into consideration. (See issue 7).

G) External events identification and definition

25. Both the POSAR and the PSA are incomplete in their analyses of natural gas pipeline failures and their impact on Temelín. Both documents assume that upon rupture of a natural gas pipeline the gas <u>always</u> immediately burns and is not available for transport. Actual real-world experience with large, high pressure, natural gas pipelines show that this is <u>not</u> always the case. We have identified six such events (in the United States: 07/26/2000 - Corpus Christi, Texas; 11/12/1999 - Oelwein, Iowa; 12/01/1998 - Amarillo, Texas; 1X/04/1997 - Santa Fe, New Mexico; in Canada: 04/15/1996 - Sc. Norbert, Manitoba; 01/23/1994 – Latchford, Canada and Russia), and it appears that no immediate ignition occurs in of the order of one out of 10 to one out of 20 such events. Neither the POSAR nor the PSA document examines the natural gas pipeline(s) which must be present to supply gas to the gas boilers in Building 410. These pipelines are much closer to the reactors than the three gas pipelines discussed in the POSAR and PSA.

26. Both the POSAR and the PSA dismiss tornadoes and high winds out of hand on the basis that tornadoes are very unlikely in the Czech Republic and that when they do occur they are very mild and not capable of damaging nuclear power plant structures, systems, and components (SSCs). Tornado experience in the past two decades in the Czech Republic does not support the first proposition, and photographs of damage do not support the second proposition. Temelín SSCs have been designed for very minimal wind conditions. [5] (See issue 2).

27. The POSAR and PSA assume that a flight exclusion area around the NPP (consisting of a cylinder 4 km in diameter and 1.5 km high) reduces aircraft crash rates at the site. This is an improper assumption, as crashing aircraft (lack of control) can easily move 2 km horizontally, and aircraft can still overfly the site higher than 1.5 km. (See issue 3).

28. The POSAR and PSA analysis of aircraft crash fail to account for skid areas in their analyses, and do not account for all potentially important structures (only considered the ESW spray ponds and the containment/reactor building complex). In addition, the aircraft crash analyses only considered impact, not post-crash fires and explosions.

H) Probabilistic Safety Assessment (PSA)

[5] The PSA indicates that structures within the original Soviet scope of supply [the reactor building (Building 800), the auxiliary building (Building 801), the safety-grade diesel generator buildings (Building 442), and the non-safety diesel generator building (Building 444)] are designed for a maximum windspeed of 44 m/sec (98 mph). The remaining structures were designed to a Czechoslovak national standard from 1973 to a wind speed of 33.8 m/sec (76 mph).

29. The Temelín PSA, which is not a licensing document but a probabilistic study to support licensing and operational activities getting an insight into the plant safety features and weaknesses, has been examined for review. The review has considered according to international practice aspects related to methodology, modeling and quantification. The following remarks have been identified: (See issue 5).

<u>Topics Which Could Increase Risk</u>

- The PSA did not include accident analysis for the containment bypass sequences and those leading to basemat penetration by using modern severe accident codes (e.g. MELCOR).

- The PSA recommends performing an analysis of offsite consequences to establish individual and society risk levels, but no such analysis is provided.

- The core inventory of radioactive materials is not provided in the PSA; only release fractions are provided.

- There are numerous limitations, particularly of the fire and flooding analyses, which reflected the lack of information on cable and instrumentation arrangement (such as in the control room and cable spreading areas), and which need to be corrected in an update of the PSA.

- The PSA analysis of loss of spent fuel pool cooling is incomplete because the PSA considered only <u>shutdown</u> periods, ignoring the potential for such events during power operation.

- The PSA failed to consider the adequacy of spent fuel pool cooling during and following severe accidents when system failures and environmental conditions in the containment and around the plant could prevent or delay repairs, resulting in a spent fuel pool accident as well.

- The PSA failed to quantify the risk posed by concurrent reactor core and spent fuel pool accidents.

- The PSA is incomplete in that it does not include Level 2 analysis of shutdown events, only Level 2 analysis of events at power.

- The Level 2 analysis of full power events fails to take proper account of the possibility of deflagration-to-detonation transition (DDT) phenomena posed by the specific containment configuration present at Temelín. Such events result in shock loading of the containment (compared with hydrogen burning which results in quasi-static loading) for which the containment is not designed and which could result in containment failure. The analysis also failed to consider the larger quantities of hydrogen generated by VVER-1000 reactors due to larger amounts of zirconium and stainless steel in the reactor vessel internals.

- The Level 1 PSA dismisses external fires affecting offsite power by stating that this type of event is included in the data for loss of offsite power generally. The loss of offsite power frequency is based on generic US data, and does not reflect conditions in the region of Temelín. The PSA may be underestimating the risk posed by loss of offsite power events as a result.

- The Level 1 PSA does not include possible core damage accident contributions arising from onsite and nearsite hazardous materials accidents. The PSA did not quantify these possible contributors, and was unable to screen them, because insufficient information was available at the time of the PSA report to analyze these potential contributors.

- The Level 1 PSA analysis of turbine missiles as accident initiators is optimistic and incomplete. The assumed frequency of generating turbine blade missiles is optimistically biased, inconsistent with worldwide experience, and not demonstrable based on VVER-1000 experience (even if all the existing VVER-1000 plants, the two Temelín units, and

Khmelnitsky Unit 2 and Rivne Unit 4 — 24 units total — operate for 60 years this is only 1440 turbine-years of experience, almost a factor of ten less than the assumed failure rate of 10^{-4}/yr). Worldwide experience supports a turbine blade missile accident rate of 10^{-3} per year. In addition, as the PSA noted no analysis has yet been performed of Unit 2 turbine missile impacts on Unit 1. Finally, the PSA failed to consider Unit 1 turbine missile impacts on the emergency diesel generator/essential service water building, the Unit 1 and Unit 2 switchyards, the Unit 2 turbine hall and turbine (possibly resulting in Unit 2 turbine missiles being generated due to impact of Unit 1 missiles on Unit 2), the Unit 2 transformers, and on Building 500 (the non-safety switchgear building).

- The Level 1 PSA excluded from the models test outage events in which the system is automatically reconfigured from the test configuration to the operating configuration in response to a demand signal. The control system which reconfigures the system from test to operation must still work properly or the system will not response automatically.

- The Level 1 PSA excluded from the model all equipment unavailability during logic testing combinations which violate the technical specifications. This modeling is equivalent to saying that the technical specifications are never violated, which is of course not true.

- The Level 1 PSA excluded external hazards consideration of loss of offsite power due to fire or flooding on the basis that these events are included in the frequency of loss of offsite power. However, the loss of offsite power frequency is based on generic US data, not Czech data from the region of Temelín, thus the justification offered for not including these events in the external hazards analysis is invalid.

- The Level 1 assessment of seismic events is based on a technically invalid probabilistic seismic hazard assessment (specifically, it is not physically reasonable for the seismic hazard to be uniform at frequencies below 10^{-3} per year). In addition, some fragility estimates for structures, systems, and components are either optimistic or missing. Finally, there is no indication that the seismic analysis consider seismically-initiated fires or flooding from failure of non-seismically qualified water system (e.g., non-seismically qualified fire suppression water).

- The Level 1 fire PSA (at power and shut down) excluded certain buildings which might be significant to fire risk without adequate justification. Included in this category is Building 594, which provides ESW filtration and is recognized in the aircraft crash analysis as a single point vulnerability for ESW. The fire PSA also excluded Building 586/01, which contains electrical switchgear for the ESW spray pond equipment. Possibly other buildings were incorrectly excluded as well, but the evaluation of this aspect of the analysis is incomplete.

- The Level 1 fire PSA (at power and shut down) improperly assumes that Temelín electrical cable cannot propagate fires. This is incorrect; qualified cable does not burn as easily as unqualified cable, but once it starts burning it behaves similarly to other cable and can certainly propagate fires if not suppressed.

- The fire PSA is not based on actual cable routing of power and control cables.

- The fire PSA does not quantify fire risk associated with fires in the control room nor fires in the containment. The main control room has a relatively high combustible loading, no fire detectors in the cabinets, and cabinets configured to act as a "chimney", thus enhancing fire growth and propagation.

- The fire PSA assumes that all fire barriers (passive and active) are properly designed and installed, and are always maintained in proper working order. No consideration is given to the probability of failure of a fire barrier, regardless of the type of barrier (fire doors, which can be left open; ventilation dampers which can fail to close, etc.). There is no inter-zone fire propagation modeled in the PSA.

- The frequencies of fire initiating events are based on two decade old data not specific to nuclear power plants (taken from a 1973 insurance standard). In general, the initiating event frequencies for fires are low compared with contemporary fire PSAs of western NPPs.

- The fire PSA assumes, but does not justify, that the main and emergency control rooms are completely electrically separated and that a fire affecting I&C in one of the control rooms leaves the I&C in the other control room unaffected.

- The fire PSA screens sequences from the analysis if their frequency is below 10^{-6} per year. The internal events PSA screens sequences if their frequency is less than 10^{-10} per year. Clearly the fire contribution to CDF is underestimated and leaves the impression that fires are less significant to CDF than they really are, even within the constraints of the fire analysis as it was performed.

- The fire PSA does not analyze issues raised in the US NRC-sponsored Fire Risk Scoping Study (NUREG/CR-5088). These issues (including inadvertent actuation of fire suppression systems without a fire) have been found important to fire risk in western PSA studies, and US NRC required all US NPPs to analyze these issues in their fire IPEEE studies.

- The fire PSA screens any area with a combustible loading of less than 5 kg/m^2, regardless of the distribution of combustibles within the fire area. If all the combustibles are located in one small, critical area which can cause damage to one or more trains of safety systems, but the fire area has a large surface area, such fire areas are improperly screened using the combustible loading criterion (which is not a modern criterion, but an artifact of a 22 year old Czechoslovak national standard).

- The PSA assumes that a 7 meter distance (22 feet) between redundant trains of equipment, without intervening combustibles, is adequate to prevent fire propagation. US NRC sponsored research has raised questions about this assumption, but the PSA apparently ignored these research results. Some important fire risk contributors may have been improperly screened as a result.

- The reactor building internal flooding analysis only considered flooding from the ESW system; all other sources were screened. This ignores some very large water tanks (e.g., three 500 m^3 EFW water tanks and the fire protection system piping).

- The assignment of some internal flooding initiators to event trees is inconsistent, and results in considerable underestimates of sequence frequency or even screening of potentially important accident sequences.

- There is an obvious numerical mistake in one fire sequence (the wrong initiating event frequency was mistakenly used), resulting in a significant underestimate of frequency (PSA estimate of 7.16×10^{-8} vs. a correct sequence frequency of 1.3×10^{-6}, which would be one of the top 15 accident sequences).

- Some internal initiating event frequencies are based on generic US data when VVER-1000 specific data (which have higher frequencies) are available; this particularly affects loss of feedwater transients, loss of offsite power transients, and small and very small LOCAs. In addition, the PSA excludes multiple SG tube rupture (stating that it lumped together with SG collector head leakage, but there is no increase in frequency to account for multiple SG tube ruptures), at least one of which has already occurred (Ginna, USA, 1982, although the additional ruptured tube had previously been plugged, this cannot be *a priori* assumed to always be the case). Multiple SG tube rupture accidents represent another class of containment bypass accidents.

- The PSA improperly excludes loss of instrument air as an accident initiating event. Loss of all instrument air would result in a reactor trip (due to the trip of the reactor coolant pumps) and unavailability of some equipment.

- The PSA improperly excludes loss of HVAC systems as an initiating event. Loss of HVAC necessitates the abandonment of the main control room because the I&C

computers will fail, resulting in a reactor trip and the need to control the plant from the emergency control room.

- It is unclear how the PSA dealt possible initiating events such as loss of DC power, leakage through the main coolant pump thermal barrier coolers (potential containment bypass), instrument tube rupture (potential containment bypass), spurious actuation of fire suppression systems, hydrogen leakage and burning/explosion due to generator cooling system failures. Loss of DC power and spurious actuation of fire suppression systems have both been found to be important accident initiators in some PSAs of western PWRs.

- The interfacing LOCA analysis uses parameter values which are considerably lower than contemporary western PSAs. As a result, a lower frequency for such events is calculated for Temelín than would otherwise be the case. If this were corrected, the frequency of interfacing LOCAs would rise, but primary to secondary leakage would still be the dominant source of containment bypass accidents.

- The PSA states that the US NRC's Source Term Code Package (STCP) was used to perform accident progression analyses (to establish event timing and severity) and to quantify the conditional probability of some events in the containment event tree. No results from the STCP analyses are provided; no summary is provided; no indication is provided of what sequences/events were analyzed. The quantification values in the containment event tree cannot be verified or validated.

- The PSA assumes a value of 1.6×10^{-5} per demand for failure of containment isolation. This is based on the sum of the failure of series of isolation valves. The probability ignores failure of the actuation system for containment isolation (failure of PRPS, which actuates the system, is 3×10^{-3} per demand, and the DPS — backup digital system — does not appear to actuate containment isolation). Failure of containment isolation in the event of a core damage accident is equivalent to containment bypass.

- The PSA model improperly concludes that main coolant pump seals will not fail within 24 hours. Even if the Russian manufacturer is correct about the seals not failing for 24 hours given loss of seal cooling/injection (it is not clear that this is so, since the tests upon which the PSA relies did not simulate all relevant conditions, and the Russian manufacturer recommended performance of additional tests), if seal cooling/injection is lost and the pumps are not tripped, the seal will fail very quickly. This results in a loss of coolant accident, which the PSA does not consider.

<u>Topics Which Could Decrease Risk</u>

- The Level 1 shutdown PSA failed to take into account the possibility of providing spent fuel pool makeup (and, by overflowing the pool to the sump, indirect heat removal) by using the containment spray system in a special alignment (a manual action which can be accomplished from the main or emergency control room, by opening three motor-operated valves or MOVs). This makes the loss of spent fuel pool cooling accident frequency unnecessarily conservative and skews the risk perspective of the overall facility.
- The Level 2 PSA does not model the venting system for the reactor coolant system (pressurizer vents and reactor vessel head vent), which could depressurize the primary coolant system in severe accident conditions to reduce the likelihood of energetic interactions within the reactor cavity (which might otherwise occur if the vessel fails with the primary system at high pressure). This is a "conservatism" in the PSA which actually skews the risk perspective for the plant by artificially inflating the fraction of core damage sequences which are assumed to melt at high pressure.
- The Level 1 PSA models failure of the accumulators as leading directly to core damage for large LOCAs. This is an unnecessary and artificial conservatism representing a leftover of design basis accident thinking. Detailed thermal hydraulic calculations on this scenario have been performed on western PWRs which show conclusively that so long as low pressure injection succeeds there is no core damage. There is no reason to

suppose that the same result would not obtain for a VVER-1000 reactor. Thus, even if accumulators fail, if low pressure injection succeeds this is not a core damage sequence. This "sequence" artificially inflates core damage frequency by inserting a "core damage" accident at 3.75×10^{-6} per year, the sixth most likely internal events sequence, when in fact this scenario does not result in core damage. This skews the risk perspective for the plant.

- The fire PSA does not credit operation of the charging pumps or the intermediate cooling system, both of which are non-safety systems but which could be available to help respond to accidents.

The entire PSA assumes that the third train of charging pumps is always unavailable due to maintenance. This is unnecessarily conservative and skews the risk assessment results toward higher frequencies for some types of sequences.

There appears to be a major quantification problem with the Temelín PSA event trees (fault tree quantification has not been checked, but with the problems noted below, it is difficult to not suspect the quantification of fault trees as well). Hand calculation have been made of several dozen event sequences in an attempt to verify that the model is producing correct results and the following discrepancies have been noted:

- The model does not appear to be taking account of success probabilities in event sequences. Normally this is not a problem as failure probabilities are 99% or greater. However, when conditional probabilities are in the range of 5% or greater, and the success probabilities are not included in the calculation, overestimation of sequence frequencies will occur. This can artificially inflate the importance of some sequences in comparison with others. This affects the dominant accident sequence in the PSA (which is a containment bypass sequence), resulting in an overestimate of accident frequency by about 8%.
- The model incorrectly screens sequences (e.g., calculating a sequence frequency below 10^{-10} per year) when the sequences are actually among the dominant accident sequences with frequencies above 10^{-7} to 10^{-6} per year. Some of the affected sequences are containment bypass sequences involving steam generator tube rupture and steam generator collector head leakage (primary-to-secondary leakage or PRISE accidents) and have frequencies totaling nearly 10^{-6} per year but which the PSA screens.
- The model incorrectly quantifies accident sequences at a lower frequency than the model parameters indicate. One of the affected sequences is a loss of all feedwater with failure of feed and bleed cooling (in effect, this is the Three Mile Island Unit 2 accident sequence), which the PSA estimates at 8.41×10^{-7} per year and which in contrast is estimated at 1.27×10^{-5} per year, which would make it the second most likely accident sequence in the model and increase internal events core damage frequency by more than 14%. Another affected sequence is a partial loss of essential service water with failure loss of all feedwater and failure of feed and bleed cooling, which the PSA estimates at 1.71×10^{-8} per year and which again in contrast is estimated at 5.7×10^{-6} per year (which would make it the third — or, if the above sequence is included, the fourth — dominant accident sequence and increase internal events core damage frequency by more than 6%).

30. The Level 2 PSA identifies the possibility of direct core debris contact with the containment liner, and core debris attack on the containment wall concrete. However, this failure mode is not quantified on the basis that there are other containment failure modes (melt-through of the cavity area instrumentation tubes) which occur more quickly. More detailed studies[6] (Kujal, 1998 [1]; Kujal, 1998a [2]; Kujal 1993 [3]) conducted after the PSA was completed appear to cast doubt on the instrument tube failure mode. It is not known whether the PSA update will address the containment wall contact failure mode. (See issue 5).

[6] Literature reference:
[1] B. Kujal & J. Duspiva (1998), Calculation and analysis of scenario of IV type with MELCOR code (interaction of corium with concrete in vertical channels), Report ÚJV Z-346-T, (in Czech).
[2] B. Kujal (1998a), Ex-vessel cooling of WWER-1000 core debris, Sensitivity study of MELCOR analytical model describing corium-coolant interaction, Report ÚJV Z-298-T, (in Czech).
[3] B. Kujal (1993), Analysis of the selected problems of the severe accident for the WWER-1000 unit at the Temelín NPP (in Czech), Phase 2: B. Kujal, Analysis of corium melting through of the containment building foundation slab, NRI Report (in Czech).

I) Miscellaneous

31. The Temelín plant has a full-time professional fire fighting organization consisting of 62 persons, 56 of whom are professional fire fighters. Fire fighting equipment, trucks, fire suppressants, and a hazardous materials response vehicle and trained personnel are available onsite, dedicated to the nuclear power plant facilities. This is well beyond the capabilities of many western NPPs.

32. The POSAR in Chapter 13, Section 13.1, describes the NPP organizational structure. According to R.G. 1.70, this section should cover, among other things, the organizational arrangement (charts) with functional responsibilities and authorities associated to each identified safety position and associated administrative rules. The POSAR does not contain an organizational scheme of Temelín NPP, and it is not simple to understand the safety positions identified as relevant in the organizational structure for the performance of safety activities. These aspects together with the NPP organization for management of licensing activity and interface with SÚJB will be reviewed according to additional documentation and information provided by CEZ a.s. (see issue 28)

33. The size of the Temelín EPZs is rather small (5 km for the "inner zone" and 13 km for an "emergency planning zone") compared with the practice in other countries (e.g., the US, which has a 16 km plume exposure pathway EPZ, which must consider evacuation and sheltering, and an 80 km ingestion exposure pathway EPZ, which must consider implementation of controls on water, milk, crops, etc., for a plant the size of Temelín). We need to understand the technical basis for the Temelín EPZs, which is not discussed in the POSAR (so far as we have reviewed it) nor in the PSA. Inasmuch as the PSA clearly shows the potential for large release accidents at Temelín (such as those due to containment bypass or containment melt-through into a compartment above ground and outside containment), there seems to be little apparent basis for having smaller EPZs at Temelín. (See issue 29).

34. There are two fire suppression water pumping systems. One is a seismically qualified system, which serves safety system compartments in the reactor building and containment. The other is a non-seismically qualified system serving the remainder of the NPP. The failure of the non-seismically qualified system could result in seismically-initiated fires not being suppressed, and could also result in flooding due to pipe breaks in the system. (See issue 19).

35. The Severe Accident Management Guidelines (SAMGs) (which are the accident management procedures which take over where the EOPs leave off) have not yet been implemented at Temelín. (See issue 6).

36. The POSAR states that the service life of the steam generators is 30 years. Among the service life limiting issues is a 70 cycles restriction on 30ºC/hr cooldown rate to reach cold shutdown during the life of the plant. [7] Such restrictions may impose a significant limitation on the ability of CEZ to extend the operating life of the plant beyond 30 years, thus affecting the overall economics of the plant. Replacement of the steam generators is, of course, possible, but this necessitates purchase of four new steam generators and results in a lengthy outage to accomplish the replacement.

37. POSAR contains only an insufficient survey on materials data of the nuclear main components (chapter 5), deviations from Code specifications are not commented.

[7] Other service limiting issue include: 30 hydro tests for leaktightness, and 130 planned heatups at 20ºC/hr from cold temperature. This is discussed in Section 5.4.2 of the POSAR.

3.0 ISSUE IDENTIFICATION

The issues identified below were selected due to the high safety significance possibly associated with them. On the basis of available documents and knowledge a ranking within these issues cannot be made. The issues are however organized in into four groups , according to the preparatory effort still needed – minimum, medium and high. The confidence in the analysis of the relevance to nuclear safety is highest for the issues with minimum preparatory effort, the uncertainty whether the issues have a high relevance for nuclear safety or have been sufficiently addressed is greatest in issues with high preparatory effort:

- Issues with minimum preparatory effort contain sufficiently documented issues with well established high priority. These issues could be pursued in the context of the European Commission - only very limited further preparation seems to be necessary.

- Issues with minimum to medium preparatory effort

- Issues with medium preparatory effort represent potentially important issues for which a significant part of the documentation has already been studied but which would benefit from limited additional effort on bilateral level to enable an efficient treatment within the framework of the European Commission. This includes the possibility that some of the issues have been sufficiently addressed.

- Issues with high preparatory effort represent potentially important issues for which a sufficiently detailed analysis on a bilateral level is still lacking, since a significant part of the documentation has not yet been studied or made available, and which would greatly benefit from further treatment on the bilateral level before they can be either recommended for treatment in the context of the European Commission or be set aside as resolved.

Where possible reference is made in this context to relevant IAEA issues (IAEA-EBP-WWER-05). The IAEA Ranks are as follows:

Rank III issues are of high safety concern, defense in depth is insufficient, immediate corrective actions are required.
Rank II issues are of safety concern, defense in depth is degraded, action is required to resolve the issue.
Rank I issues reflect a deviation from recognized international practices.

Issues with minimum preparatory effort

1. Containment bypass and primary-to-secondary (PRISE) leakage accidents

The Temelín probabilistic safety assessment (PSA) identifies a large absolute and percentage contribution to core damage frequency resulting from primary-to-secondary (PRISE) and containment bypass accidents. (We note that not only would such accidents be accompanied by a large source term resulting from containment bypass, but subsequent to vessel failure containment melt-through would add an additional large source term from material not released during the in-vessel phase of the accident. See the related issue of containment design and arrangement, below.)

This issue includes steam generator (SG) collector leakage, SG collector failure, SG tube rupture (single and multiple), interfacing LOCA, and any other accidents resulting in primary-to-secondary leakage and/or in bypass of the containment (including containment isolation failure). The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— CI4 (Steam Generator Collector Integrity, Rank III)
— CI5 (Steam Generator Tube Integrity, Rank II)
— S2 (Mitigation of a Steam Generator Primary Collector Break, Rank II)
— I&C11 (Water Chemistry Control and Monitoring Equipment, Primary and Secondary, Rank I)

- — Cont1 (Containment Bypass, Rank II)
- — AA7 (Steam Generator Collector Rupture Analysis, Rank II)
- — AA9 (Severe Accidents, Rank I)
- — AA10 (Probabilistic Safety Assessment, Rank I)

2. Natural Gas Pipeline Accidents and Their Effect on Temelín

(See Preliminary Indication 26)

There are three natural gas pipelines located approximately 900 meters from the center point between the two Temelín reactors. CEZ and the PSA have assessed these pipelines as posing no hazard to Temelín, but this is based on a flawed premise (i.e., that in the event of pipeline rupture the natural gas will always burn immediately and not be available for transport to and ingestion into the reactor buildings by the ventilation systems). To the contrary, we have identified a number of large pipeline rupture events in Canada, Russia, and the United States which have not been accompanied by immediate burning of the gas and in which gas transport was possible. Based on data analyzed so far, it appears that the conditional probability of no immediate combustion (given a large, high pressure, natural gas pipeline rupture) is of the order of 0.05-0.10, whereas the POSAR and PSA implicitly assume that the probability of no immediate combustion is very low (approaching zero).

In addition, although not considered in either the POSAR or the PSA, there are three natural gas-fired boilers located at the front of the NPP near the access road and the visitor's center. Clearly, a natural gas pipeline or pipelines feeds these boilers. Any such pipeline is much closer to the reactors than the three pipelines included in the POSAR and PSA. The possible hazards posed by such a pipeline or pipelines has not been assessed in documentation which we have reviewed.

Natural gas pipeline rupture, followed by gas transport to the vicinity of the reactors and ingestion into the reactor buildings could cause multiple fires inside these buildings. Such fires could cause an accident in one or both reactors, and could affect spent fuel pool cooling as well as reactor cooling.

In addition, gas transport and ingestion could affect other buildings (e.g., turbine hall, diesel generator building/essential service water pump compartments, etc.), and it is clear that neither the POSAR nor the PSA considered any building other than the reactor building and containment in its limited assessment of pressure wave impacts.

Note that the reactor building and main and emergency control room ventilation systems do not have combustible gas detection capability, only smoke detectors). Isolation of the ventilation systems in case of a natural gas pipeline accident is thus a manual operator action. There are no systems to alert the operators to a pipeline rupture apart from a telephone call to the plant from the pipeline company.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

- — S14 (Ventilation System of Control Rooms, Rank II)
- — I&C9 (Accident Monitoring Instrumentation, Rank II)
- — IH1 (Systematic Fire Hazards Analysis, Rank II)
- — IH2 (Fire Prevention, Rank III)
- — IH3 (Fire Detection and Extinguishing, Rank II)
- — IH4 (Mitigation of Fire Effects, Rank II)
- — EH3 (Man-Induced External Events, Rank II)
- — AA8 (Accidents Under Low Power and Shutdown Conditions, Rank II)
- — AA9 (Severe Accidents, Rank I)
- — AA10 (Probabilistic Safety Assessment, Rank I)

3. Tornadoes

(See Preliminary Indication 27)

Both the POSAR and the PSA indicate that tornadoes, except for very mild and very rare ones, do not occur on the territory of the Czech Republic. This is not correct, and there is a very easily accessible web site sponsored by the Czech Hydrometeorological Institute which shows tornado damage from the past 10 years which is not consistent with either the proposition that Czech tornadoes are mild nor with the proposition that Czech tornadoes are rare (http://www.chmi.cz/meteo/sat/torn/, tornadoes on the territory of the Czech Republic, Ceský hydrometeorologický ústav). The design basis wind speeds for the Temelín structures, systems, and components are low (34-44 m/sec) compared with even modest tornadoes (Fujita-Pearson Tornado Intensity Scale 2, with winds ranging from 50-70 m/sec, and representing about one fourth of all tornadoes) which have struck NPPs in other countries, causing considerable damage and loss of offsite power. There are a number of potentially vulnerable structures at Temelín (e.g., the turbine hall, the 110 kV and 400 kV switchyards, the ESW intake filtration building, the cooling towers, the auxiliary boiler building, and Building 529, failure of which would result in a complete loss of offsite power). In addition to wind speed, tornadoes are associated with wind-borne missiles, for which the design basis of Temelín structures is not known, but for which there are some clearly vulnerable structures (some of those previously mentioned, such as the turbine hall).

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— EH2 (Analyses of Plant Specific Natural External Conditions, Rank I)
— AA8 (Accidents Under Low Power and Shutdown Conditions, Rank II)
— AA9 (Severe Accidents, Rank I)
— AA10 (Probabilistic Safety Assessment, Rank I)

Issues with minimum to medium preparatory effort

4. Containment Design and Arrangement
(See Preliminary Indication 13)

Temelín has a prestressed concrete containment, a concept employed in many western pressurized water reactors (PWRs), However, contrary to western PWR designs, the Temelín containment is supported more than 10 meters above ground by several levels of the reactor building. What this means is that if a core melt accident occurs and core debris penetrates the bottom of the containment, it is released or expelled (if the containment is pressurized) into a small compartment outside containment, above ground. This results in a release of radioactivity to this compartment outside containment, and subsequently to the environment. (In western PWRs, the bottom of the containment is below ground, and the only release pathway to the atmosphere if the bottom of the containment melts through is via the ground, which acts to "scrub" fission product aerosols before they can be released to the atmosphere in large quantities.)

The Temelín PSA indicates that the reactor cavity area (into which core debris would flow or be expelled when the reactor vessel fails in a severe accident) will be dry in nearly all accident sequences because containment spray water cannot reach this area. In addition, the PSA indicates that the reactor cavity has a small area compared with the area which would be needed to establish a coolable debris bed, and that as a result penetration of the bottom of the containment is almost ensured. We believe this is true at the very least due to bulk melt-through in the time frame of 24-36 hours, and may happen much more quickly as a result of a variety of different penetrations under the reactor vessel or within range of molten core debris in a severe accident. The resulting source terms could be quite high.

Another potential containment arrangement issue is the potential for direct core debris contact with the wall of the containment (resulting in melting of the liner and direct concrete attack). The composition of the wall concrete is unknown to us, but we consider it unlikely that it is the same as the reactor cavity concrete. If the containment wall concrete is more typical limestone concrete, considerable additional hydrogen as well as carbon monoxide (also combustible) could be generated compared with reactor cavity attack by molten core debris.

This issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— Cont1 (Containment Bypass, Rank II)
— AA8 (Accidents Under Low Power and Shutdown Conditions, Rank II)
— AA9 (Severe Accidents, Rank I)
— AA10 (Probabilistic Safety Assessment, Rank I)

5. Probabilistic Safety Assessment and Severe Accidents

(See Preliminary Indication 29, 30)

Severe accident risks arising from Temelín are clearly an important concern for Austria. A probabilistic safety assessment (PSA) has been performed, with results issued in the 1996 time frame. (An update has been under way and may be partially or substantially complete, at least for Level 1 results.) [8] The 1996 PSA results indicate a core damage frequency for events at power marginally meeting or straddling the IAEA INSAG safety target of 1×10^{-4} per year. However, the results also indicate a large release frequency well above the IAEA INSAG safety target of 1×10^{-5} per year. The large release events are dominated by containment bypass and by containment melt-through accidents (see two related issues, containment bypass and primary-to-secondary (PRISE) leakage accidents and containment design and arrangement, above).

The external events results do not include a contribution from natural gas pipeline accidents potentially affecting Temelín (see a related issue, natural gas pipeline accidents and their effect on Temelín, above), nor from onsite or offsite industrial accidents which release toxic substances into the air. In addition, the external events results include a very low result for seismic events, which we believe to be based on a flawed probabilistic seismic hazard assessment (see a related issue, seismic design and seismic hazard assessment, above).

The IAEA has sponsored two IPERS reviews of the Temelín PSA, one of internal events (24 April to 5 May 1995, before the analysis was completed) and one of external events. It is important to understand the results of the IPERS missions and the extent to which the IPERS missions findings are reflected in the version of the PSA which we have been reviewing, and the extent to which the remaining issues will be addressed in an update of the PSA. (We have access to the 1995 IPERS mission report, but not the 1996 IPERS mission report.)

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— G3 (Reliability Analysis of Safety Class 1 and 2 Systems, Rank II)
— EL1 (Off-Site Power Supply Via Startup Transformers, Rank I)
— EL2 (Diesel Generator Reliability, Rank I)
— EL3 (Protection Signals for Emergency Diesel Generators, Rank I)
— EL5 (Emergency Battery Discharge Time, Rank III)
— IH1 (Systematic Fire Hazards Analysis, Rank II)
— IH2 (Fire Prevention, Rank III)
— IH3 (Fire Detection and Extinguishing, Rank II)
— IH5 (Systematic Flooding Analysis, Rank I)
— IH6 (Protection Against Flood for Emergency Electric Power Distribution Boards, Rank II)
— AA8 (Accidents Under Low Power and Shutdown - LPS - Conditions, Rank I)
— AA9 (Severe Accidents, Rank I)
— AA10 (Probabilistic Safety Analysis, Rank I)
— AA11 (Boron Dilution Accidents, Rank I)
— AA12 (Spent Fuel Cask Drop Accidents, Rank I)
— AA13 (Anticipated Transients Without Scram, ATWS, Rank II)
— AA14 (Total Loss of Electrical Power, Rank II)
— AA15 (Total Loss of Heat Sink, Rank II)

The issue also encompasses the use of the PSA in design and operation, feedback from the PSA into the current NPP design and procedures, and the use of the PSA in the plant modification programme (e.g., actions taken to limit core damage frequency and spent fuel pool accident frequency during shutdown, accidents taken to limit core damage frequency and containment bypass/large release frequency from power operations). It also encompasses the analysis of beyond design basis accidents, and the use of these analyses in plant design and operation.

[8] Reportedly the Temelín PSA Level 1 analysis update should have been completed in December 2000; the Level 2 analysis update is scheduled to be performed between March and September 2000; see, Frantisek Hezoucky, *Temelín NPP Status: The Challenge of Safety Improvements* , The Uranium Institute 25th Annual Symposium, 30 August - 1 September 2000, London, p. 11.

Based on up to date review results, a number of concerns about the PSA has been identified, included here as an illustrative list:

- Failure to consider loss of spent fuel pool cooling with the reactor at power (Mode 1)
- Failure to consider the adequacy of spent fuel pool cooling during severe reactor accident conditions
- Failure to consider concurrent reactor and spent fuel pool accidents due to common cause (including cooling dependencies)
- Failure to perform Level 2 analysis for shutdown reactor accidents
- Failure to adequately consider deflagration-to-detonation transition (DDT) phenomena in severe accidents as a possible containment failure mode
- Use of United States data for loss of offsite power and the conditional probability of recovery of offsite power versus time
- Improper screening of external fires as a cause of extended loss of offsite power
- Incomplete and optimistic assessment of turbine missile hazards (including failure to model Unit 2 turbine missile impacts on Unit 1, failure to consider numerous possible missile targets for Unit 1 turbine missiles, and failure to consider large fires which have historically resulted from turbine failures)
- Lack of analysis of risks posed by onsite and nearsite release of hazardous materials to the air
- Failure to model surveillance test outages in which the system is automatically reconfigured from test to operational configuration (the reconfiguration I&C system still has to work, but this was ignored in the models)
- Failure to model violations of Technical Specifications
- Failure to model loss of offsite power due to fire or flooding (these events are inherently local phenomena which are not represented in generic US data used for modeling loss of offsite power)
- Failure to model potentially significant buildings in the fire PSA (e.g., Buildings 586/01 and 594).
- Failure to model potentially significant buildings in the aircraft crash analysis (e.g., Buildings 586/01, 594, the turbine hall, the diesel generator fuel storage tanks, etc.), failure to consider skidding prior to impact as a hazard, and failure to consider the disposition of aircraft fuel after the crash (fire, explosion, etc.; only impact hazards were considered)
- Failure to perform a state-of-the-art probabilistic seismic hazard assessment (the assessed hazard is uniform below 10^{-3} per year, which is clearly not physically possible)
- Inadequate modeling of fire propagation and failure to consider the conditional probability of fire barrier failure (barriers include fire doors, walls, dampers, etc.)
- Lack of modeling of control room fires, despite a high combustible loading, conditions favorable for fire growth and propagation in the control room cabinets, and lack of fire detectors in the cabinets
- Use of optimistic fire initiating event frequencies based on inapplicable non-nuclear data
- Failure to model issues raised in the US NRC's Fire Risk Scoping Study (NUREG/CR-5088), including inadvertent fire suppression system actuation
- Screening of reactor building flood sources other than the ESW system
- Numerical quantification errors in the event tree models for internal events, fires, and flooding (including improper screening of potentially dominant accident sequences, failure to account for success state probabilities, and various examples of over- and under-calculation of sequence frequencies)
- Improper exclusion of loss of instrument air and loss of HVAC systems as initiating events (both result in a reactor trip and failures of some equipment)
- Improper exclusion of loss of DC power, spurious actuation of fire suppression systems, and generator hydrogen leakage as potential initiating events
- Use of optimistic data in the interfacing LOCA analysis
- Optimistic assessment of containment isolation failure probability
- Failure to provide results from accident progression analyses using computer models of severe accidents
- Failure to model the need to trip the reactor coolant pumps to avoid a seal LOCA in the event of loss of seal cooling/injection
- Failure to model use of containment spray to provide spent fuel pool cooling
- Failure to model systems which could provide makeup of water to the containment sump

— Failure to model the reactor vessel and pressurizer vent system
— Equating accumulator failure with core damage (this is not realistic)
— Improper exclusion of natural gas pipeline ruptures, failure to consider natural gas pipelines feeding the auxiliary boilers (Building 410), and improper exclusion of tornadoes

Issues with medium preparatory effort

6. Emergency Operating Procedures (EOPs) and Severe Accident Management Guidelines (SAMGs)
(See Preliminary Indication 35)

This issue includes EOPs (stated by CEZ a.s. to be aimed at "accident prevention") and SAMGs (stated by CEZ a.s. to be aimed at "accident consequences mitigation") as well as any other procedures that would be used by Temelín staff in responding to potential or actual severe accidents. We understand that the EOPs have been implemented, but we have not been able to review them. We also understand that the SAMGs were not implemented for startup of Unit 1, but were scheduled to be completed in February 2001. [9]

The EOPs and SAMGs are extremely important for severe accident risk management purposes. The final version were not available when the PSA was performed, so numerous assumptions were made about the behavior of operators which may or may not ultimately have be reasonable for real operational situations. Thus, the risk profile of the plant may be strongly dependent on the provisions of and quality of the implemented EOPs and SAMGs and operator and management training thereon. A tracking of the EOPs and SAMGs against the PSA-identified dominant accident sequences is a necessary precondition to ascertaining the adequacy of the EOPs and SAMGs.

Also important in this context is the related issue of post-accident monitoring and sampling in terms of design, capability, qualification, and availability of information in the main and emergency control rooms, as well as in the technical support center.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— OP2 (Emergency Operating Procedures, Not Ranked) [10]
— I&C9 (Accident Monitoring Instrumentation, Rank II)
— I&C10 (Technical Support Centre, Rank II)
— EP01 (Emergency Centre, Not Ranked) [11]
— AA13 (Anticipated Transients Without Scram, ATWS, Rank II)
— AA14 (Total Loss of Electrical Power, Rank II)
— AA15 (Total Loss of Heat Sink, Rank II)

7. Seismic Design and Seismic Hazard Assessment
(See Preliminary Indication 20, 21, 22, 23, 24)

The original seismic design of Temelín was for a 0.06g PGA design basis earthquake. The plant design has been reviewed and improved to 0.1g PGA. Although approved by SÚJB, this value has not been reviewed by the IAEA (of course, there is no requirement for such a review under Czech regulations, but such a review has been done in other cases such as Mochovce and Bohunice, for example). It is based, in whole or in part, on a probabilistic seismic hazard assessment (PSHA) which is not state of the art. Indeed, the PSHA results show a nearly vertical seismic hazard curve below 10^{-3} per year, which is simply not physically possible. Thus, there are significant questions about whether the 0.1g PGA value is reasonable and, if not, then there are significant questions about the adequacy of seismic design of the plant structures and equipment.

[9] Frantisek Hezoucky, *Temelín NPP Status: The Challenge of Safety Improvements* , The Uranium Institute 25th Annual Symposium, 30 August - 1 September 2000, London, pp. 9 & 11.

[10] The non ranking should not be understood as an indication of minor safety relevance. Rather, these issues were identified in a different manner (via OSART missions) than the other issues.

[11] The non ranking should not be understood as an indication of minor safety relevance. Rather, these issues were identified in a different manner (via OSART missions) than the other issues.

In addition to the above, we note that the PSA includes a median fragility for offsite power of 0.4g PGA. This is quite optimistic, and contemporary PSAs normally assign a value of 0.2-0.3g PGA for the switchyard (failure of ceramic insulators, resulting in essentially unrecoverable loss of offsite power). A more reasonable fragility for offsite power, combined with a state-of-the-art probabilistic seismic hazard assessment will, we believe, result in a substantial increase in the estimated risk to Temelín arising from earthquakes.

Some component analyses in the POSAR appear to show very little margin. In some cases, a shift was made from the cited French standard and reference was made to Russian normative standards instead.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— EH1 (Seismic Design, Rank II)
— EH2 (Analyses of Plant Specific Natural External Conditions, Rank I)

8. <u>Main Steam Line and Feedwater Line Breaks</u>

(See Preliminary Indication 2)

.

The Temelín main steam lines (MSL) and main feedwater lines (FWL) are arrayed with the MSL on top and the FWL on bottom, in pairs to the respective steam generators. The MSIVs and FW isolation valves are in a special compartment just prior to the exit of these pipes into the turbine hall. Until this point, there are no isolation valves or check valves of any kind.

There are pairs of MSLs which exit on each side of the containment, and run together in pairs until all four MSLs run side by side as they approach the MSIVs. Unless the MSLs are adequately restrained and/or adequately physically separated, if one line rupture it is possible for two lines (or more in some areas) to rupture as a result of pipe whip. These ruptures can occur in areas where the steam lines cannot be isolated. The reactivity effects and the effects on the reactor vessel (pressurized thermal shock due to extreme overcooling) of multiple steam line ruptures are not addressed in the POSAR sections which we have reviewed to date.

It should be borne in mind that multiple steam line rupture events are not an academic concern in general — one of the historical events in the US (at Millstone Unit 3) involved a consequential failure of an adjacent line, and this occurred in an NPP which was licensed to the modern USNRC criteria for such events (which USNRC believed would preclude this sort of consequential failure). Given the arrangement of the MSL and FWL at Temelín, multiple steam line failure is far from an academic concern.

In addition, there are no details in the POSAR sections which we have reviewed to date concerning the erosion-corrosion prevention and mitigation program at Temelín. Given the proximity of the steam lines, erosion-corrosion protection is very important, but there are no details available to us so far about the program implemented for Temelín. This is a very real concern — most of the steam and feedwater line ruptures which have occurred in PWR reactors to date have originated from erosion-corrosion effects resulting in material degradation.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— CI6 (Steam and Feedwater Piping Integrity, Rank III)
— IH7 (Protection Against the Dynamic Effects of Main Steam and Feedwater Line Breaks, Rank II)
— AA5 (Main Steam Line Break Analysis, Rank I)

9. <u>Reactor Pressure Vessel Embrittlement and Pressurized Thermal Shock</u>

The reactor pressure vessel consists of welded ring forgings (three surrounding the active core). There are two circumferential welds at or near the same elevation in the vessel as the reactor core. Neutron irradiation of both the vessel base metal and the welds increases the temperature at which the vessel wall materials experience a transition from ductile to brittle fracture properties. Such temperatures can be reached as the vessel is cooled down. There are certain types of "overcooling" transients, especially when coolant is delivered by high pressure injection and/or makeup pumps, which could — if the transition temperature is high enough — result during pressurized thermal shock in crack initiation and non-arrested crack propagation and therefore vessel failure. Insufficient information on the materials characteristics has been presented in the POSAR from which to make a final assessment of this issue. The brittle fracture safety assessment was neither performed according to the Russian Code, nor according to the IAEA recommendations. More information is needed on the used Westinghouse methodology and the used materials data to evaluate the conservatism of this procedure. Due to the lack of a statistical data basis on VVER-1000 materials' neutron embrittlement there is considerable need of sufficient safety margins. The Czech side is investing many efforts to create a representative surveillance program to compensate the missing statistical data basis with respect to the conservative prediction of neutron embrittlement of the RPV belt line region.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— CI1 (Reactor Pressure Vessel Embrittlement and Its Monitoring, Rank III)
— AA6 (Overcooling Transients Related to Pressurized Thermal Shock, Rank II)

10. Main Steam Line Safety and Relief Valves Qualification for Two-Phase and Water Flow
(See Preliminary Indications 2, 18)

The POSAR describes these valves, but the sections of the POSAR reviewed to date do not address the issue of the qualification of the main steam line safety valves and the atmospheric dump valves (BRU-A) for passing two-phase and water flow. There is no information presented concerning the designer of the valves nor the qualification tests for the valves to demonstrate their ability to pass high velocity two-phase and water flow.

This is potentially significant because in the event of a steam generator tube rupture, steam generator collector failure, or steam generator collector head leakage accident with MSIV closure, the atmospheric dump valves could be challenged and forced to pass two-phase flow or water flow. If a core damage accident occurs under these conditions and the valves cannot close, a containment bypass situation exists. [See the related issues of containment bypass and primary-to-secondary (PRISE) leakage accidents, and emergency operating procedures (EOPs) and severe accident management guidelines (SAMGs) above, and the related issues of probabilistic safety assessment and severe accidents, and , environmental and seismic qualification of equipment, below.]

In addition, there are questions about the design of the compartment containing the main steam and feedwater lines up to the main steam isolation valves and feedwater isolation valves as regards aircraft crash. Aircraft crash beyond the capability of this compartment could result in multiple steam line/feedwater line failures which could cause accident conditions beyond the capacity of installed safety systems.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— CI4 (Steam Generator Collector Integrity, Rank III)
— CI5 (Steam Generator Tube Rupture, Rank III)
— S02 (Mitigation of a Steam Generator Primary Collector Break, Rank II)
— S09 (Steam Generator Relief and Safety Valves' Qualification for Water Flow, Rank III)
— S10 (Steam Generator Safety Valves' Performance at Low Pressure, Rank II)
— EH3 (Man-Induced External Events, Rank II), specifically aircraft crash

11. Status of IAEA Safety Issues resolution

It is important to obtain final information on the status of implementation of plant/procedure modifications to address the safety issues set forth in IAEA-EBP-WWER-05. Although the Nuclear Research Institute Řež report from March provides expanded information in this regard, some issues are left open or their resolution is unclear due to equivocal statements in the report.

12. Safety Classification of Components

The POSAR provides lists of safety systems and safety-related systems, but the explanation of how systems were assigned to one or the other category is unclear. We need a clear understanding of concepts of Safety Systems and Safety related systems with related requirements (par.3.2.2 dedicated to safety Classification is made of only one page). These aspects are covered in some reference documentation which should be reviewed. .

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— G1 (Classification of Components, Rank II)

13. Control Rod Insertion

Further information is needed concerning the experimental and startup testing programs aimed at resolving this issue for the revised Westinghouse core and control rod designs. Little information on this matter is available in the incomplete version of the POSAR to which we have been given access.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— RC2 (Control Rod Insertion Reliability/Fuel Assembly Deformation, Rank III)

14. Sump Screen Blocking and Suction Line Integrity
(See Preliminary Indication 2)

Sump screen blocking can affect, simultaneously, all three trains of high pressure injection, low pressure injection, and containment spray. Loss of integrity on the common suction line from the sump to these system can also affect all three systems simultaneously. In addition, since all three systems use the residual heat removal (RHR) heat exchangers in operation, integrity of the heat exchangers is also a related issue and can affect all three trains of all three systems. Some information is provided in the POSAR. In the verification report the adequacy of the revised sump screen design could not be confirmed for 3×100% operation of the ECCS pumps in case of a large break LOCA. Three solutions to overcome this situation are proposed in this report but they are not reflected or assessed in the related chapter of the POSAR. Thus the implemented solutions on Temelín NPP site is an open issue.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— S05 (ECCS Sump Screen Blocking, Rank III)
— S06 (ECCS Water Storage Tank and Suction Line Integrity, Rank II)
— S07 (ECCS Heat Exchanger Integrity, Rank II)

15. Reactor Coolant Pump Seal Integrity

We understand from the POSAR and PSA that a document from the pump manufacturer exists suggesting that the seals will maintain integrity for 24 hours on loss of seal cooling/seal injection. However, this is only if the pumps are shutdown immediately (e.g., this is discussed in the IPERS Phase 1 mission report at page 99), and no consideration was given to the likelihood that one or more pumps would not automatically shut down.

In addition, we note that the letter relied upon to establish 24 hour seal integrity states that during the test the maximum leakages through the end stage of the sealing was not created and that the environmental conditions were not fully simulated. [12] Thus, even the test which is relied upon may not adequately represent the installed configuration at Temelín. The letter recommends performance of additional tests, but there is no indication that these additional test were performed. Note that the test was with a shutdown coolant pump. No tests were apparently run

[12] International Atomic Energy Agency, Report of the IPERS (International Peer Review Service) Phase 1 Review Mission for the Temelín Nuclear Power Plant Level 1 Probabilistic Safety Assessment in the Czech Republic, 24 April to 5 May 1995, IAEA-RU-5628, WWER-SC-128, p. 100.

with a running pump to ascertain how much time is available within which to shutdown the pump and still maintain seal integrity as assumed in the PSA.

Failure to do so would result in the seals leaking excessively for any pump not promptly tripped after loss of seal cooling/injection. No indication is provided of the resulting LOCA size. In addition, it is noted that the IAEA IPERS mission report (24 April to 5 May 1995) recommended further consideration of pump seal LOCAs, but it is clear that the PSA which we have reviewed (dated December 1995) takes no note of such accidents.

The related emergency operating procedures (EOPs) and severe accident management guidelines (SAMGs) need to be reviewed, as well as the suggested power supply by the fifth (non-safety) diesel generator for the makeup pumps. We also need to review the Diverse Protection System (DPS), which backs up the Primary Reactor Protection System (PRPS), to ascertain whether DPS would provide a signal to promptly trip the reactor coolant pumps on loss of seal cooling/injection or whether instead coolant pump trip would be an operator action if PRPS fails.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— G2 (Qualification of Components, Rank III)
— CI2 (Non-Destructive Testing, Rank III)
— I&C1 (I&C Reliability, Rank II)
— I&C7 (Primary Circuit Diagnostic Systems, Rank II)
— S3 (Reactor Coolant Pump Seal Cooling System, Rank II)
— AA1 (Scope and Methodology of Accident Analysis, Rank II)
— AA9 (Severe Accidents, Rank I)
— AA10 (Probabilistic Safety Assessment, Rank I)
— AA15 (Total Loss of Heat Sink, Rank II)
— Oper.Pro.1 (Procedures for Normal Operation, not ranked) [13]
— Oper.Pro 2 (Emergency Operating Procedures, not ranked) [14]

16. Hydrogen Control

The lower half of the Temelín containment, which includes the reactor cavity area, is extensively compartmentalized. In contrast, the area above the refueling deck is quite open. Under severe accident conditions, it is in principle possible that deflagration-to-detonation transition (DDT) could occur, resulting in impulsive (rather than quasi-static) loads on containment. Such phenomena are beyond the modeling capabilities of most severe accident codes. It is necessary to understand what analyses have been made of hydrogen detonation and DDT phenomena for Temelín in order to assess the adequacy of the containment design for severe accidents.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— S15 (Hydrogen Removal System, Rank II)
— AA9 (Severe Accidents, Rank I)
— AA10 (Probabilistic Safety Analysis, Rank I)

17. Limited ECCS/Containment Spray Sump Volume

(See Preliminary Indication 14)

The Temelín sump volume (which is the source of injection water for low and high pressure ECCS systems and containment spray) is small both in comparison with other VVER-1000 units and especially small in comparison with western PWRs. The Temelín sump volume is 500 m^3 compared with an 800 m^3 sump volume for Kozloduy Units 5 & 6 and compared with typical western sump volumes ranging from 950-1900 m^3. This provides Temelín with comparatively less margin (and time) to deal with primary to secondary leakage (steam generator tube rupture, steam generator collector head leakage) events, for example.

[13] The non ranking should not be understood as an indication of minor safety relevance. Rather, these issues were identified in a different manner (via OSART missions) than the other issues.

[14] The non ranking should not be understood as an indication of minor safety relevance. Rather, these issues were identified in a different manner (via OSART missions) than the other issues.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

- CI4 (Steam Generator Collector Integrity, Rank III)
- CI5 (Steam Generator Tube Integrity, Rank III)
- S2 (Mitigation of a Steam Generator Primary Collector Break, Rank II)
- Cont1 (Containment Bypass, Rank II)
- AA2 (QA of Plant Data Used in Accident Analysis, Rank I)
- AA3 (Computer Code and Plant Model Validation, Rank I)
- AA8 (Accidents Under Low Power and Shutdown Conditions, Rank II)
- AA9 (Severe Accidents, Rank I)
- AA10 (Probabilistic Safety Assessment, Rank I)

Issues with high preparatory effort

18. Boron Dilution

Boron dilution could result in a return to power under conditions in which the necessary reactor heat removal and pressure relief systems are not available. Under such circumstances, core damage could result.

Boron dilution was not addressed in the POSAR sections which we have reviewed, nor was it addressed in the PSA. The Nuclear Research Institute Rež report from March indicates that there are interlocks which on reactor trip close all valves that could supply unborated water to the suction of the makeup pumps. During outages, however, the plant relies on administrative controls to prevent boron dilution accidents. It is well recognized that containment integrity and system operability requirements are relaxed in shutdown compared with operating modes, this boron dilution accidents could be important to risk.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

- RC1 (Prevention of Inadvertent Boron Dilution, Rank II)
- RC3 (Subcriticality Monitoring During Reactor Shutdown Conditions, Rank II)
- AA1 (Scope and Methodology of Accident Analysis, Rank II)
- AA9 (Severe Accidents, Rank I)
- AA10 (Probabilistic Safety Assessment, Rank I)
- AA11 (Boron Dilution Accidents, Rank I)

19. Environmental and Seismic Qualification of Equipment
(See Preliminary Indications 10 , 34)

It is important to identify any safety and safety-related structures, systems, or components which are not environmentally and/or seismically qualified. Specific identification of unqualified equipment is important in order to understand which equipment may not be available in accident conditions.

The content of the in–progress complex program to reassess and finalize the qualification of safety and safety related equipment by year 2002 needs to be reviewed. This, together with information about the current status of the implementation and related outcomes, is an important aspect which affects the operability of safety systems in accident conditions.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

- G2 (Qualification of Equipment, Rank III)
- AA1 (Scope and Methodology of Accident Analysis, Rank II)
- AA2 (QA of Plant Data Used in Accident Analysis, Rank I)
- AA3 (Computer Code and Plant Model Validation, Rank I)
- AA9 (Severe Accidents, Rank I)

20. Ventilation System and Habitability Aspects of Control Rooms
(See Preliminary Indication 15)

We need to verify information concerning the control room ventilation systems and to obtain additional information concerning the air supplies and ventilation intake locations for the main and emergency control rooms. In addition, we need additional information on the habitability of the main and emergency control rooms under a variety of conditions, including the occurrence of a severe accident at the opposite unit (i.e., the impacts of a Unit 2 severe accident on Unit 1 main and emergency control room habitability).

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— S14 (Ventilation System of Control Rooms, Rank II)
— AA1 (Scope and Methodology of Accident Analysis, Rank I)
— AA2 (QA of Plant Data Used in Accident Analysis, Rank I)
— AA3 (Computer Code and Plant Model Validation, Rank I)
— AA8 (Accidents Under Low Power and Shutdown Conditions, Rank II)
— AA9 (Severe Accidents, Rank I)
— AA10 (Probabilistic Safety Assessment, Rank I)

21. Instrumentation and Control (I&C) Reliability

We need to obtain additional information on I&C reliability data gathering, and on the logic used by the PRPS and DPS when one train of components is in test or maintenance. It is important to understand whether the logic reverts to 1-out-of-2 for the remaining two trains, or whether it remains 2-out-of-3 (effectively, 2-out-of-2 with one train in test or maintenance).

It has to be noted that the PSA version which was provided for review does not accomplish fully the goal of evaluating the reliability of the I&C systems. The I&C systems, protection systems, and the corresponding man-machine interfaces were represented in a relatively coarse manner in the PSA. (Indeed, the IAEA IPERS report on this issue states that they were told by the PSA team that the I&C analysis has the character of a "placeholder" in the PSA, and the IPERS report also notes that the interactions between the PSA team and the designers of the reactor protection system were "weak and relatively undefined".) [15]

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— I&C1 (I&C Reliability, Rank II)
— I&C2 (Safety System Actuation Design, Rank I)
— AA8 (Accidents Under Low Power and Shutdown Conditions, Rank II)
— AA9 (Severe Accidents, Rank I)
— AA10 (Probabilistic Safety Assessment, Rank I)
— AA13 (Anticipated Transients Without Scram, ATWS, Rank II)

22. Non-Destructive Testing

We need detailed information on NDT and NDE activities planned to address the risk dominant accidents (SG collector failure, SG collector head leakage, and SG tube rupture). Very little detail has been included in the POSAR concerning the quality of materials in the active core zone, or the quality of welds and main components resulting from NDT results. Where results are reported, there are indications of deviations from normative values without accompanying explanations justifying the deviations.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— CI2 (Non-Destructive Testing, Rank III)

[15] International Atomic Energy Agency, Report of the IPERS (International Peer Review Service) Phase 1 Review Mission for the Temelín Nuclear Power Plant Level 1 Probabilistic Safety Assessment in the Czech Republic, 24 April to 5 May 1995, IAEA-RU-5628, WWER-SC-128, pp. 10 & 11, 20-22.

23. Leak Before Break (LBB)

This issue is addressed in the Nuclear Research Institute Rež report from March, however the POSAR is largely silent on the issue. Inasmuch as the POSAR was structured according to USNRC Regulatory Guide 1.70 and these details should be in the POSAR, it is unclear on what basis the SÚJB approved leak before break application to Temelín.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— CI3 (Primary Pipe Whip Restraints, Rank II)
— I&C7 (Primary Circuit Diagnostic Systems, Rank II)
— I&C8 (Reactor Vessel Head Leak Monitoring System, Rank III)

24. Conception of Safety Features
(See Preliminary Indications 11, 16, 17)

Some of the safety features concepts of the Temelín design appear to have shortcomings. An evaluation of the relevance of these aspects will be addressed in the ongoing review activity. These include: (a) the feed and bleed mode of operation for small LOCAs, loss of feedwater, and other events; (b) emergency reactor coolant pump seal injection; (c) steam generator tube rupture features, behavior, and capability; (d) lack of an intermediate cooling system for cooling the RHR heat exchangers; and (e) design provision to protect safety support systems from external natural and man-made hazards.

25. Design Basis Accident Analysis

Design basis accident analysis and radiological consequences of such accidents could not be reviewed to date since the relevant portions of the POSAR (including the bulk of Chapter 15) were not provided by CEZ a.s. until recently (11 January 2001).

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— AA1 (Scope and Methodology of Accident Analysis, Rank II)
— AA2 (Quality Assurance of Plant Data Used in Accident Analysis, Rank I)
— AA3 (Computer Code and Plant Model Validation, Rank I)
— AA4 (Availability of Accident Analysis Results for Supporting Plant Operation, Rank I)
— AA5 (Main Steam Line Break Analysis, Rank I)
— AA6 (Overcooling Transients Related to Pressurized Thermal Shock, Rank II)
— AA7 (Steam Generator Collector Rupture Analysis, Rank II)
— AA11 (Boron Dilution Accidents, Rank I)
— AA12 (Spent Fuel Cask Drop Accidents, Rank I)
— AA13 (Anticipated Transients Without Scram, ATWS, Rank II)
— AA14 (Total Loss of Electrical Power, Rank II)
— AA15 (Total Loss of Heat Sink, Rank II)

26. Beyond Design Basis Accident Analysis

This issue encompasses the review of evaluations made at Temelín NPP of plant response and management capability for events which are beyond the Design Basis Accidents in terms of frequency of occurrence, source term quantification and accidents which can result from combination of independent failures or extensive common mode failures, e.g., total loss of electrical power (station blackout), total loss of heat sink, multiple steam generator tube rupture, etc.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— AA1 (Scope and Methodology of Accident Analysis, Rank II)
— AA14 (Total Loss of Electrical Power, Rank II)
— AA15 (Total Loss of Heat Sink, Rank II)

27. Safety Culture

As part of the assessment of other issues, the broad issue of safety culture is being assessed. However, there are two specific aspects of safety culture which need to be mentioned here: (a) operating experience feedback, and (b) root cause analysis procedure. How these aspects of safety culture are integrated into the management and operation of the plant has important implications which need to be investigated. Review of the operating experience feedback and root cause analysis processes is needed.

The issue encompasses the following IAEA issues (from IAEA-EBP-WWER-05):

— Man01 (Need for Safety Culture Improvements, Not Ranked) [16]
— Man02 (Experience Feedback, Not Ranked) [17]

28. NPP Organizational Structure and Management of Licensing Activities

Organizational structure with functional responsibilities and authorities associated to each identified safety position and the associated administrative structure, are of significant importance for the management of safety activities of the NPP. These aspects together with the NPP organization for management of licensing activity and interface with SÚJB will be reviewed according to additional documentation and information provided by CEZ a.s.

The issue is not identified in from IAEA-EBP-WWER-05.

29. Technical Basis for Temelín Emergency Planning Zones (EPZs)
(See Preliminary Indication 33)

The size of the Temelín EPZs is rather small (5 km for the "inner zone" and 13 km for an "emergency planning zone") compared with the practice in other countries (e.g., the US, which has a 16 km plume exposure pathway EPZ, which must consider evacuation and sheltering, and an 80 km ingestion exposure pathway EPZ, which must consider implementation of controls on water, milk, crops, etc., for a plant the size of Temelín). We need to understand the technical basis for the Temelín EPZs, which is not discussed in the POSAR (so far as we have reviewed it) nor in the PSA. Inasmuch as the PSA clearly shows the potential for large release accidents at Temelín (such as those due to containment bypass or containment melt-through into a compartment above ground and outside containment), there seems to be little apparent basis for having smaller EPZs at Temelín.

The issue is not identified in IAEA-EBP-WWER-05.

[16] The non ranking should not be understood as an indication of minor safety relevance. Rather, these issues were identified in a different manner (via OSART missions) than the other issues.

[17] The non ranking should not be understood as an indication of minor safety relevance. Rather, these issues were identified in a different manner (via OSART missions) than the other issues.