IAEA-CN-73/46

# TEMELIN NPP PSA AND SAFETY MONITOR™

O. MLADÝ
CEZ a.s., Temelin NPP,
Czech Republic

## Abstract

In the frame of Temelin NPP PSA Project the PSA models have been developed covering Level 1 both at power and shutdown states of operation, external events and the Level 2 analyses. The hierarchical structure established for the performance of the Temelin PSA was determined from the outset by the requirement for the production of a living PSA capable of being used for both an in depth analysis of plant design and operation as well as on-line use in real time. The development, key functional requirements, status and use of Safety Monitor 2.0 for Temelin NPP is described as well as one of the Safety Monitor applications - evaluation of deterministic allowed outage times.

## 1. INTRODUCTION

The Temelin NPP is a WWER-1000/320 two unit plant under construction, originally designed according to the standards of the former Soviet Union. When the Czech Republic became independent, Temelin was still in the early stages of construction, therefore it was decided to upgrade areas of the plant where it was considered that the design standard was below that for other plants, due to come on line in the late nineties. This resulted in the decision to replace the Russian core with a Westinghouse core, retaining the original configuration and rod drive control mechanisms, and at the same time, replace all instrumentation control and protection with that of the latest Westinghouse design, including digital software for the generation of the ESFAS and reactor scram functions. Significant number of other improvements increasing plant safety are being or have been incorporated into the Temelin design already as summarized in Ref. [1].

## 2. TEMELIN NPP LIVING PSA

The utility, CEZ-NPP Temelin also decided, following the recommendations of a number of audits and IAEA pre-OSART mission, that the performance of a PSA would be an integral step in the preparation of the Preliminary Safety Case. The Temelin PSA Project covers both Level 1 at power and non power modes of operation, external events and the Level 2 analysis to determine the source terms. Off-site consequences were not evaluated at this stage. The model structure in NUPRA Ref. [2] greatly facilities the use of the model as a living tool.

It was important for the PSA at Temelin to be as comprehensive as possible otherwise the conclusions regarding the relative contributions to core damage would be incorrect. The hierarchical structure established for the performance of the Temelin PSA was determined from the outset by the objectives above which require the production of a living PSA capable of being used for both an in depth analysis of plant design and operation as well as on line use in real time. The structure had to provide a clear and traceable link between the plant design documentation and operational information and the risk evaluation, both for the performance of the PSA and its continuing use. In addition to the normal management procedures these structural elements were:

- a complete set of task plans delineating the sources of plant information, assumptions to be made, and documentation to be produced within the task.

- a complete set of analysis files giving the results of the analysis in the task including the relationship of the results to existing plant information, other tasks and the computer risk model.
- a document data base showing where all applicable documents were used.
- a quality assurance process and independent review of the work products, including Temelin engineering and operational staff.
- PSA model in sufficient detail to meet the defined objectives.
- Safety Monitor, or PSA model, running in real time useable by plant staff with no knowledge of PSA terminology, for plant evaluation of the current risk level and recommended allowed outage times for a given state.
- the ability to evaluate the risk profile of a refueling outage or maintenance program during power operation.

The key elements for the subsequent use of the PSA are the task plans and analysis files. It is these documents which ultimately define the model and define the end usage. It is therefore essential to know at the outset of the PSA its end usage so that the appropriate methodology and techniques can be used for the development of the final risk model.

## 3. APPLICATIONS

The increasing level of plant design and operational detail which it is now possible to include in the PSA and the ability to relate this directly to the individual model unit has lead to the realization that the PSA can be used in the day to day operation and decision making processes at the plant in the areas like:

- Assessment of modifications (design, operation, testing, procedures, etc.)
- Tech specs issues (LCOs, AOTs, STIs)
- Operating and maintenance strategies based on risk minimization
- Outage Risk Management
- Precursor Analysis
- Risk Profiles

These issues are primarily associated with calculating risk for a given plant configuration or its change. For it to change the risk it must eventually either change the value of the individual elements (basic events) in the PSA or the logic structure in which those elements are arranged. As calculating the risk of a new plant configuration using PSA risk model requires roughly person days, performing a risk assessment sometimes for hundreds of equipment outages, tests, and alignments required for some applications is thus beyond reach.

From that reason, additionally to the completion of Temelin LPSA model, the decision has been made to extend the PSA Project and to implement a real-time risk calculation tool analyzing both real and scheduled plant conditions for determining the impact of plant configurations and on-line maintenance on operational risk level - Safety Monitor™ 2.0

## 4. TEMELIN SAFETY MONITOR

The major purpose of the Safety Monitor at Temelin is to provide an on line measure of risk based on the current plant configuration and testing status so enabling plant staff to plan and perform maintenance activities in such a way that safety is maximized, and at the same time unnecessary plant shutdown is avoided. It is clear that simply no plant would prefer to be uninformed about the risk associated with an upcoming change in plant configuration. The process of obtaining that information using PSA is so arduous that to evaluate every change would be virtually impossible, and such evaluation would be only retrospective in nature. Prior to the Safety Monitor, calculating the risk of a new plant configuration using PSA would have required roughly person days. This level of effort made performing a risk assessment for each of hundreds of equipment outages, tests, and re-alignments using PSA beyond reach. Now the performance of such a calculation is performed in about 4 person minutes, so allowing the hundreds of calculations to be performed. As the model in the Safety Monitor is the same as the PSA model, in fact it contains more information on components than the PSA model, each calculation gives the exact PSA solution appropriate to the particular plant alignment. As the model does not use pre-solved solutions which approximate to the plant alignment, as is used in some plant monitors currently in existence, the determination of the relative contribution to risk can be performed accurately.

Experience in the use of the Safety Monitor at San Onofre [3], [4] has clearly shown that quarterly plant risk, which had been tracked for the past ten years, began to decrease after the Safety Monitor was introduced. Not only was safety improved but also direct cost savings were achieved and in the near future it is expected that real savings of $500,000 per day will be achieved for the number of days the refueling outage is shortened.

## 4.1 Safety Monitor key functional requirements

The key functional requirements for Safety Monitor are as follows:

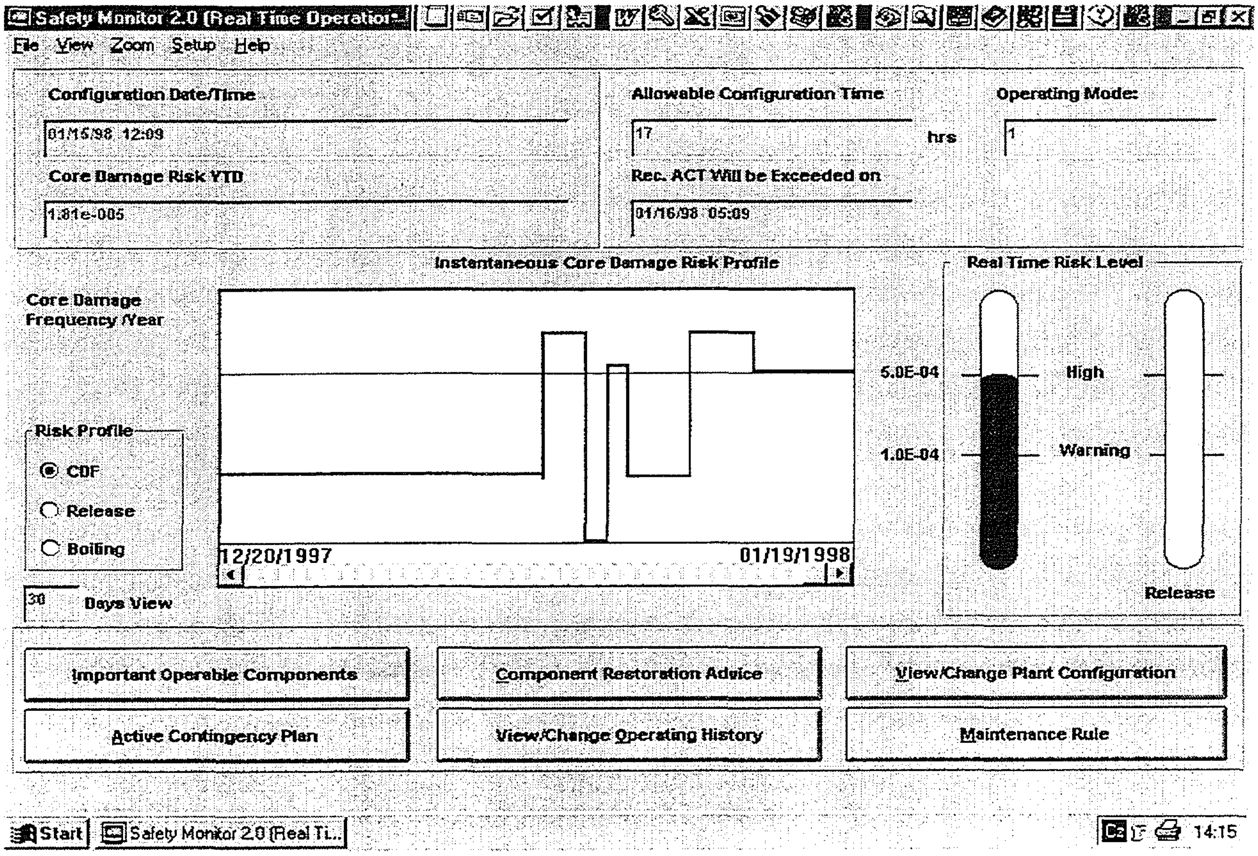
1. Must operate in a multi-user PC environment under Microsoft Windows with security access features enabling access of multiple users at the same time.
2. Software must be usable by plant personnel without knowledge of PSA techniques.
3. Must resolve the complete PSA model within several minutes for each plant configuration/maintenance/testing activities to reflect current (or proposed) plant conditions.
4. Must be designed to provide virtually identical results to the original PSA models.
5. Re-quantification of cut set libraries is not used, thereby eliminating the risk of truncation errors in the results.
6. Must support risk calculations also for other than Level 1 models (external events, shutdown, Level 2 and 3).
7. Must provide the following information:

    - Actual plant risk (displayed in a "gauge" display) as a function of given actual plant configuration and conditions
    - Allowed Configuration Time
    - Risk profile over the operating cycle
    - Cumulative risk over the cycle
    - Important equipment in current plant configuration
    - Optimal restoration advice for inoperable components to reduce risk
    - Hypothetical risk profile from scheduled maintenance activities

Some of the significant Temelin Safety Monitor screens illustrating these functional requirements are shown in the Figures 1 and 2. To achieve maximum benefit from using Safety Monitor at the plant the Scientech Safety Monitor™ 2.0 has been customized to meet Temelin specific needs, e.g. Temelin specific Safety Monitor model, component naming conventions, Czech language displays and documentation.

## 4.2 Intended use of Safety Monitor at Temelin

It is expected that the Safety Monitor will be used extensively by the maintenance division in scheduling preventive maintenance activities, both at power and during refueling. The planner can enter



Safety Monitor 2.0 (Real Time Operation)
File View Zoom Setup Help
Instantaneous Core Damage Risk Profile
Core Damage Frequency /Year
12/20/1997
01/19/1998
Real Time Risk Level
5.0E-04
1.0E-04
High
Warning
Release
Important Operable Components
Component Restoration Advice
View/Change Plant Configuration
Active Contingency Plan
View/Change Operating History
Maintenance Rule
Start
Safety Monitor 2.0 (Real Ti...
14:15

Configuration Date/Time: 01/15/98 12:09

Core Damage Risk YTD: 1.81e-005

Allowable Configuration Time: 17 hrs

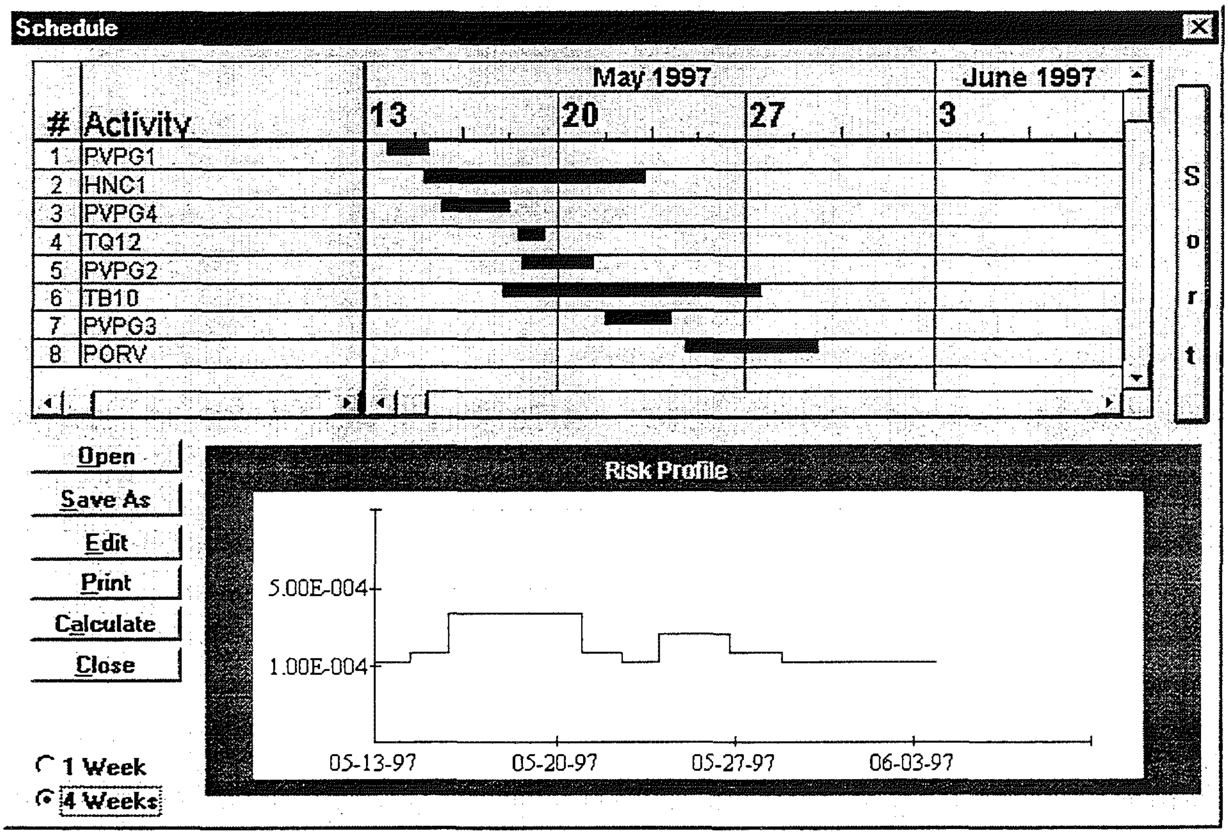
Rec. ACT Will be Exceeded on: 01/16/98 05:09

Operating Mode: 1

Risk Profile: ● CDF ○ Release ○ Boiling

30 Days View

*FIGURE 1 - TEMELIN SAFETY MONITOR MAIN SCREEN*



| # | Activity |
|---|---|
| 1 | PVPG1 |
| 2 | HNC1 |
| 3 | PVPG4 |
| 4 | TQ12 |
| 5 | PVPG2 |
| 6 | TB10 |
| 7 | PVPG3 |
| 8 | PORV |

○ 1 Week
● 4 Weeks

*FIGURE 2 - TEMELIN SAFETY MONITOR SCHEDULER SCREEN*

specified equipment outages several weeks in advance and if the calculated risk for these hypothetical configurations is high, then equipment outages can be rearranged within the schedule until the risk is sufficiently low. Similarly for operator personnel would definitely be an advantage to be informed about a risk associated with an upcoming plant configuration prior such configuration will be entered, including recommended limiting time to be allowed for such configuration or to provide risk reduction advise for such configuration. The intended use of Safety Monitor, in general form, is briefly summarized below:

- Provide an easy-to-use tool for operator/maintainer plant staff to obtain insights from the PSA without detailed knowledge of PRA techniques and terminology
- Provide a PSA oriented tool for active influence on risk level of plant operation
- Provide a means to optimize safety within Technical Specifications constraints
  - Identify requirements that are too restrictive given their risk significance or
  - Identify Tech Specs required testing that may be adverse to the plant safety
- Provide a means to optimize planed maintenance activities through:
  - Import of maintenance schedule into the Safety Monitor
  - Risk profile calculation over the entire maintenance schedule
  - Schedule adjustment/editing from acceptable risk level point of view
  - Optimized schedule export back into the plant maintenance scheduler
- Provide history of plant configuration changes and component outages with associated risk levels

## 5. EVALUATION OF ALLOWED OUTAGE TIMES

One of the key applications at Temelin will be the evaluation of the allowed outage times (AOTs) recommended in the Technical Specifications and Limiting Conditions of Operation. The current AOTs are usually based on the engineering judgment of the designer, and approved by the regulator, as part of the overall licensing process. This may result in wide differences in the actual risk contribution of one AOT vis a vis another. There is many approaches how to evaluate TS requirements using PSA. A general discussion on quantitative and qualitative measures and approaches is given e.g. in sections 3.1.3 and 3.2.1 of the IAEA-TECDOC-729 [5].

The allowed outage times for the various systems and components at Temelin have not yet been fixed as Temelin is still under construction. Provisional values are under development, and it has been decided to use risk based analysis to evaluate the final deterministic AOTs that will be included in the licensing to the regulatory body. As the Temelin PSA and Safety Monitor models are available it will be possible to determine which ones will result in an over prescriptive limit on time out of service and also any in which the proposed time would result in a high level of risk. It should be emphasized that the final AOTs will still be deterministic in nature at the present time. The model developed for the Safety Monitor will be used to perform this evaluation as the solution time of 4 minutes will enable the 300 or more calculations to be done in a reasonable period of time. Also by using the full PSA model rather than the cut set solution a number of inaccuracies will be avoided. For example many single component failures are not in the cut sets when the random failure rate is used but would be in if the value was set to 1 (in maintenance). It can be seen from Table I. that there are a number of ways in which the risk contribution of an equipment outage can be compared. Column C represents the incremental level without consideration of time of outage, whereas column D the risk contribution of the outage. This is dimension less so in order to find the annual contribution this number is multiplied by the frequency of component outage per year (combined planned and unplanned maintenance). The annual risk contribution is shown in column F.

What is not possible is to evaluate in this way the impact of other events taking place at the same time as these individual outages. Ultimately the on line use of the Safety Monitor will allow the determination of the risk contribution for the unique circumstances at any time in operation.

TABLE I. EXAMPLE OF ALLOWED OUTAGE TIME EVALUATION

| A | B | C | D = (B x C) | E | F = (D x E) |
|---|---|---|---|---|---|
| COMPONENT(s) | AOT | RISK LEVEL INCREMENT | RISK CONTRIBUTION | COMPONENT FAILURE/YEAR | ANNUAL RISK CONTRIBUTION |
| LHSI PUMP 10 | 48 hr | 2.7E-11 | 1.3E-9 | 0.3 | 3.7E-10 |
| LHSI PUMP 20 | 48 hr | ... | ... | ... | ... |
| LHSI PUMP 30 | 48 hr | ... | ... | ... | ... |
| BATTERY CHARGER | 24 hr | 3.8E-10 | 9.12E-9 | 0.8 | 7.3E-9 |
| ... | ... | ... |  |  | ... |
| ... | ... | ... |  |  | ... |
| ... | ... |  |  |  | ... |
| ... | ... |  |  |  | ... |
| TOTAL Σ |  |  |  |  | 1.2E-6 |

THE TOTAL SUM OF ANNUAL CDF FROM COMPONENTS SHOULD BE HIGHER THAN PSA ANNUAL CDF AS THE ACTUAL TIME IN MAINTENANCE IS USUALLY LESS THAN AOT (COLUMN E IS EXACT IF PLANT MAINTENANCE INFORMATION IS USED).

## REFERENCES

[1] Design Modifications of Temelin WWER-1000 NPP, Information material for IAEA meeting in Vienna, Nov. 28 - Dec. 2, 1994, Temelin, Czech Republic.

[2] NUPRA - The NUS Probabilistic Risk Assessment workstation, Version 2.2, March 1994. NUS, Gaithersburg, MD, USA.

[3] Integration of PSA into the Regulatory Framework of the U.S. NRC. IAEA-CN-61/34 International Conference on Advances in Operational Safety of Nuclear Power Plants, Vienna, 4-8 September, 1995.

[4] MORGAN, T., HOOK, T.G., LEE, R., „Risk Management Insights from the Development and Use of the San Onofre Safety Monitor“, International Meeting of Thermal Hydraulics, Taipei, Taiwan 1994.

[5] IAEA-TECDOC-729, Risk Based Optimization of Technical Specifications for Operation of NPPs, IAEA, Vienna, 1993