TEMELIN SAFETY MONITOR

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

Abstract

Temelin NPP is a WWER-1000/320 two unit plant under construction, originally designed according to the standards of the former Soviet Union. After a series of reviews in the 80s, a decision was taken to upgrade the design of Temelin, including the supply of fuel and instrumentation and instrumentation and control system (I&C). Details on the current design and other related safety matters were presented to the nuclear community in a meeting organized by the IAEA in November 1994.

Based upon recommendations of IAEA OSART missions, post TMI requirements and Temelin Risk Audit recommendations it was decided to perform a Probabilistic Safety Assessment within the Temelin PSA Project. The general purpose of this project was to perform systematic examination of the Temelin Unit 1 NPP for severe accident vulnerabilities by performance of a Level 1 and 2 PSA study.

In addition to the completion of Temelin documented living PSA model, the decision was to develop and implement a PSA based software tool able to analyze real and scheduled plant conditions for determining the risk impact of plant configurations and on-line maintenance activities. This paper provides an overview of the key features of the Temelin Safety Monitor, describes its development activities and its current status and intended use at Temelin NPP for PSA applications.

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. After series of reviews in the 1980s, a decision was taken to upgrade the design of Temelin, including the supply of fuel and instrumentation and instrumentation and control system (I&C). Details on the current design and other related safety matters were presented to the nuclear community in a meeting organized by the IAEA in November 1994.

At the present time, a significant number of safety improvements are being or have been incorporated into the Temelin design already. Among most significant measures are: replacement of old core and fuel by new WEC VVANTAGE 6 core, new WEC core monitoring system "BEACON", replacement of I&C by new WEC I&C (PRPS, DPS, RLCS, ESFAS), development of new symptom based emergency operating procedures using COMPRO (computerized procedures system), improved MCR and ECR design and TSC development, two additional non safety grade diesel generators supplying AFW, normal charging system and ADV implemented into design, SGs design modified in terms of the primary header cracking and primary to secondary leak flow rate improvement, enhanced batteries life, replacement of rectifiers and inverters, flame-retardant cables replaced by flame-resistant, containment sump screens and common ECCS suction modified, ECCS/RHR

heat exchanger material improved, equipment/structures seismic requalification for 0.1g SSE, PORV fitting into the design, etc.

Based upon recommendations of IAEA OSART missions, post TMI requirements and Temelin Risk Audit recommendations it was decided to perform Probabilistic Safety Assessment within the Temelin PSA Project. The general purpose of this project was to perform systematic examination of the Temelin Unit 1 NPP for severe accident vulnerabilities by performance of a Level 1 and 2 PSA study. The work on the Temelin PSA began in 1993 and it was completed by June 1996. The Project was accomplished by a team consisting of NUS Corporation, NPP Temelin PSA staff and other subcontractor project personnel (EQE International, UJV Rez, EGP Prague, etc.) under the overall direction and responsibility of the NUS.

In addition to the completion of Temelin documented living PSA model, the decision has been made at the plant to develop and implement a PSA based software tool analyzing real and scheduled plant conditions for determining the impact of plant configurations and on-line maintenance on actual operational risk level - Scientech Safety Monitor^{TM} 2.0.

Temelin NPP PSA Project Key Features

Scope:	Level 1 - internal initiating events, external initiating events (fire, floods, seismic, others), Level 2, Living PSA (Temelin Safety Monitor)
Operating modes:	Full power, shutdown (outages, refueling)
Supplier:	NUS Corporation, direct involvement of NPP Temelin
Subcontractors:	EGP Praha, UJV Rez (NRI), RELKO, EQE, others
Client:	NPP Temelin
Financing:	CEZ, a.s. - NPP Temelin
Current status:	All models completed, Safety Monitor - ongoing task

Methodology:

The approach used for the PSA project is given by Temelin PSA Project Plan. Temelin PSA model has been developed using standard small event tree/large fault tree linking methodology using the NUPRA code. The event trees are "Plant Damage State" event trees which have been developed with the Level 2 in mind, to give a smooth interface between Level 1 and Level 2.

Quality Assurance:

As it was intended from the project beginning that the results of the study should be incorporated in a living PSA one of the most important issues was quality assurance. The safety guidelines issued by the IAEA and Decree No 436/90 issued by the State Office for Nuclear Safety both indicate that a quality assurance program should be implemented for activities associated with the design and operation of Nuclear Power Plants. Therefore, a Quality Assurance Program and Plan for the performance of the Temelin PSA Project was developed incorporating the elements of an acceptable NUS QA Program designed to meet 10 CFR 50, Appendix B requirements to the extent possible. The key features of the program involves: design, documentation and software control, verification, review of interim and final work products, and software control.

Independent review:

The key area of independent review was performed at three basic levels. NPP Temelin engineers performed a review of all models and documentation to ensure that the details of the model and assumptions conform with what is known about the plant design. At the second level all work products underwent several stages of verification and review. All system models were independently checked by another analyst within the Project team and designated by the Project manager before their incorporation in the final overall model. All calculations, documents, and computer code inputs and outputs were checked for accuracy by another member of the Project team. The verification was done in accordance with NUS Quality Assurance Program. At the third level an independent review by the IAEA was envisaged. Such independent review of the Temelin PSA Level 1 (internal events) model conducted by IPERS team from the IAEA in the frame of IAEA 1995-1996 TC Biennial Program took place in April/May 1995 at Temelin and the second IAEA IPER mission reviewing external events and Level 2 models proceeded in January 1996. The results and recommendations are summarized in the IAEA reports from these IPER missions.

Features and Development Activities of Safety Monitor^{TM} for Temelin NPP

Temelin PSA staff intends to support actively plant staff in analysis of day-to-day issues related to the areas like:

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

To achieve such day-to-day support of the plant staff requires a dynamic and flexible use of plant specific current PRA models, which is not realistic because of following reasons:

- Extensive scope of PRA models (thousands of BEs, and MCSs)
- Special knowledge of PRA techniques, software and for all the plant specific PRA model(s) is required
- Number of PRA models could potentially exist - Level 1/2, Shutdown, External Events
- Reflection of a current plant status/configuration in the PRA model is time consuming, often requiring large number of PRA model modification steps (model extension, house event settings, CCF and HEPs modification, etc.)
- Quantification process is running for a certain time period itself, depending on the PRA hardware, software used and scope of the plant specific model
- The interpreting of the results obtained requires knowledge of PRA techniques again

Therefore, plant PRA staff decided to extend the PSA project and to implement a real-time risk calculation tool at Temelin analyzing both real and scheduled plant conditions for determining the impact of plant configurations and on-line maintenance on actual operational risk level - Safety Monitor^{TM} 2.0.

Temelin Safety Monitor Key Functional Requirements

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 PRA techniques
3. Must resolve the complete PRA model(s) 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 PRA models
5. Re-quantification of cutset 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
   - Recommended 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 Safety Monitor screens are shown in the Appendix A.

Temelin Safety Monitor Development

The Scientech Safety Monitor™ 2.0 has been modified to meet Temelin specific needs:

- Temelin specific Safety Monitor model development
- Data for Safety Monitor development using Temelin component naming conventions
- Development of Czech language displays
- Development of Czech language documentation
- Running software under Temelin LAN Environment
- Testing of completed SM (software and model) at Temelin to ensure proper operation

Status of Temelin Safety Monitor Development Activities

Safety Monitor Model Development

Temelin PSA Level 1 model conversion to a SM master fault tree logic for total core damage risk from all sequences was performed. System fault trees were expanded to consider all possible operating alignments. Safety Monitor models were optimized for fast solution retaining full PSA model fidelity. Optimized SM model results have been carefully validated against the original plant PSA model results.

Safety Monitor Data Development

Plant specific data were developed for Temelin SM including over 25 main database tables, e.g. master system/train/component lists, component to PRA logic mapping list, mutually exclusive events, system alignment list, equipment tag out boundaries, maintenance activities, in addition testing and some other external conditions (e.g. severe weather) that could alter the likelihood of an initiating event, using Temelin specific component naming conventions. Currently, only PSA and some other equipment is included in Temelin Safety Monitor databases.

Development of Czech Language Displays and Documentation

All Safety Monitor 2.0 resource files were translated into Czech language enabling full understanding of Safety Monitor screens and functions by the plant personnel. These files are currently under compilation process. Czech version of Safety Monitor user and administrator documentation will be developed from English version following software final V&V.

Testing of completed SM

Currently, as the software is still under development, it is running for testing at Temelin PSA Dept. LAN computers.

Intended Use of Safety Monitor at Temelin

- 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

- Serve as a means to optimize safety within Technical Specifications constraints

    - Identify requirements that are too restrictive given their risk significance
    - Identify Tech Specs required testing that may be adverse to plant safety

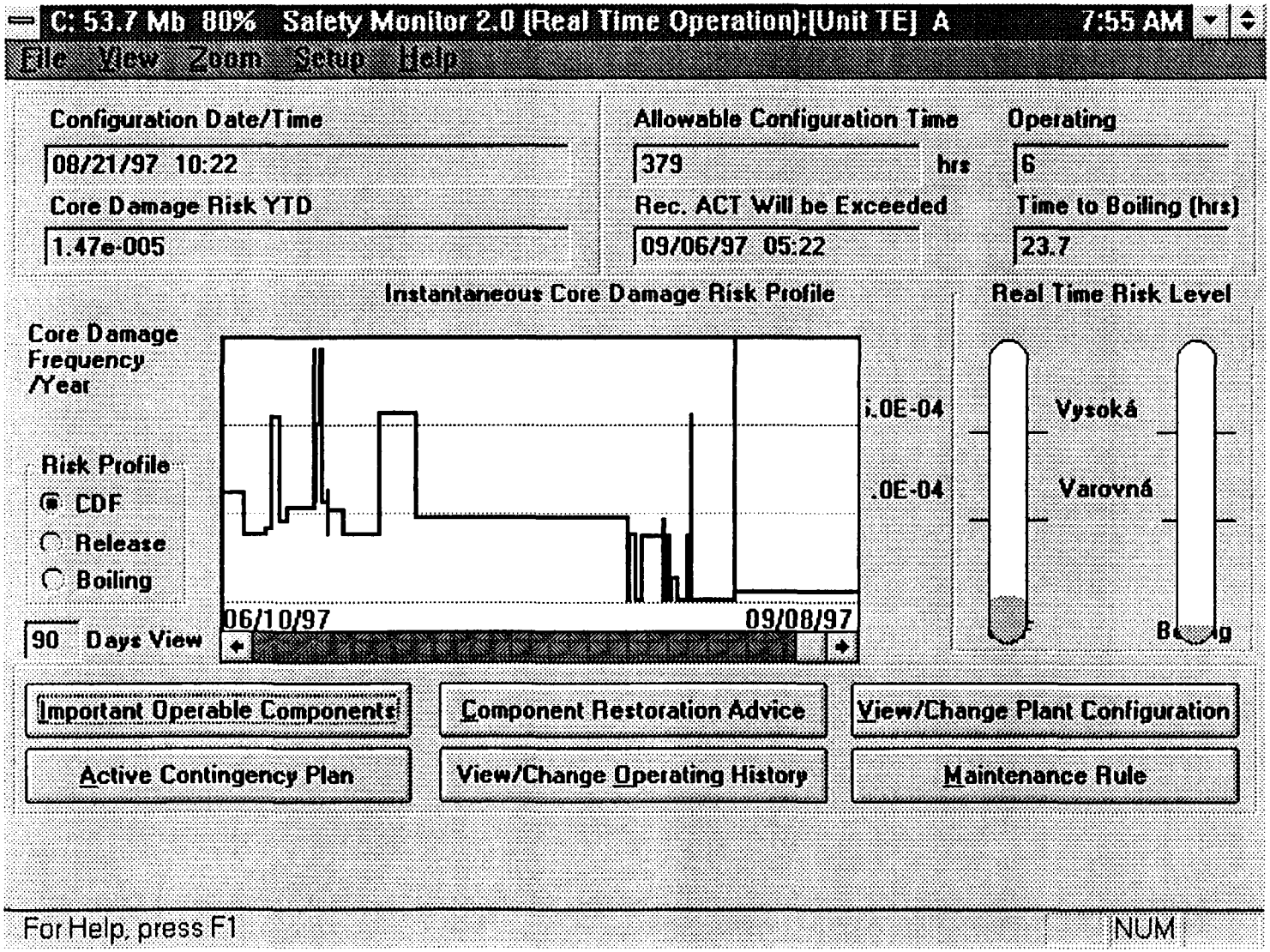
- Serve as a means to optimize planed maintenance activities through:

    - 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

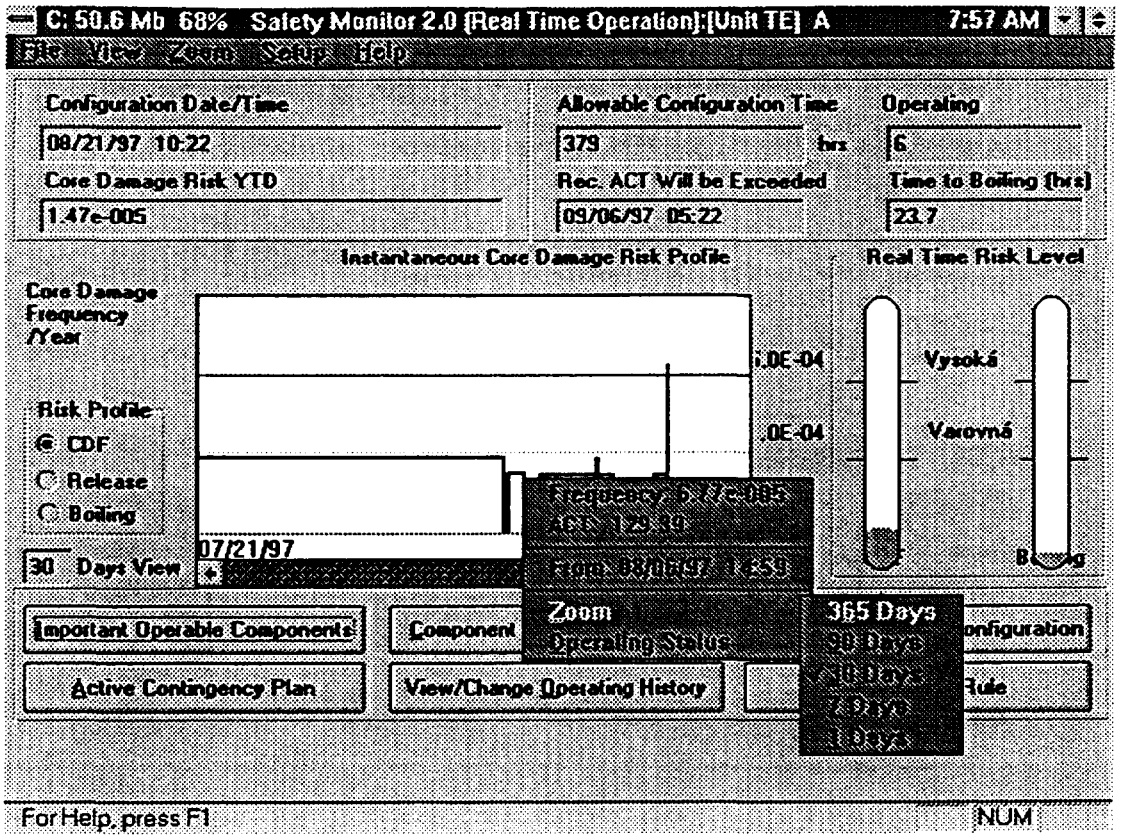
- Provide history of plant configuration changes and component outages with associated risk levels

The following figures present the "Temelin Safety Monitor Screens".

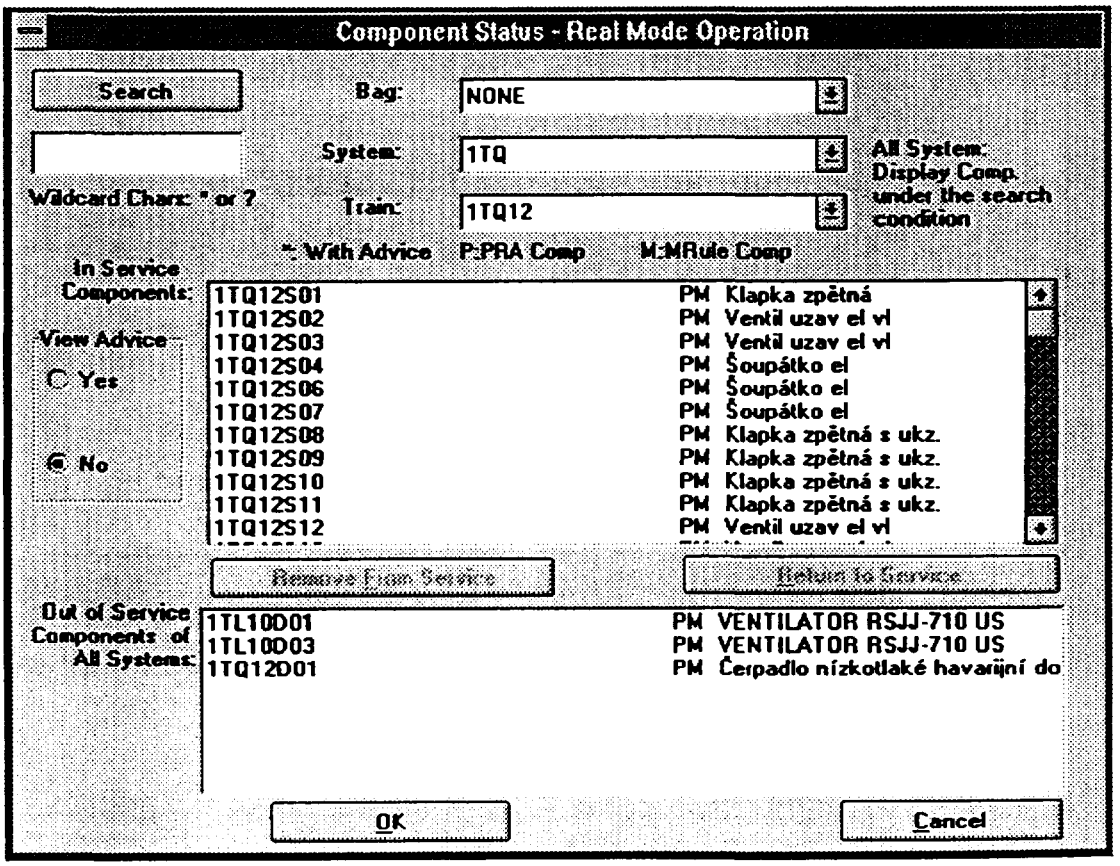
SAFETY MONITOR MAIN SCREEN



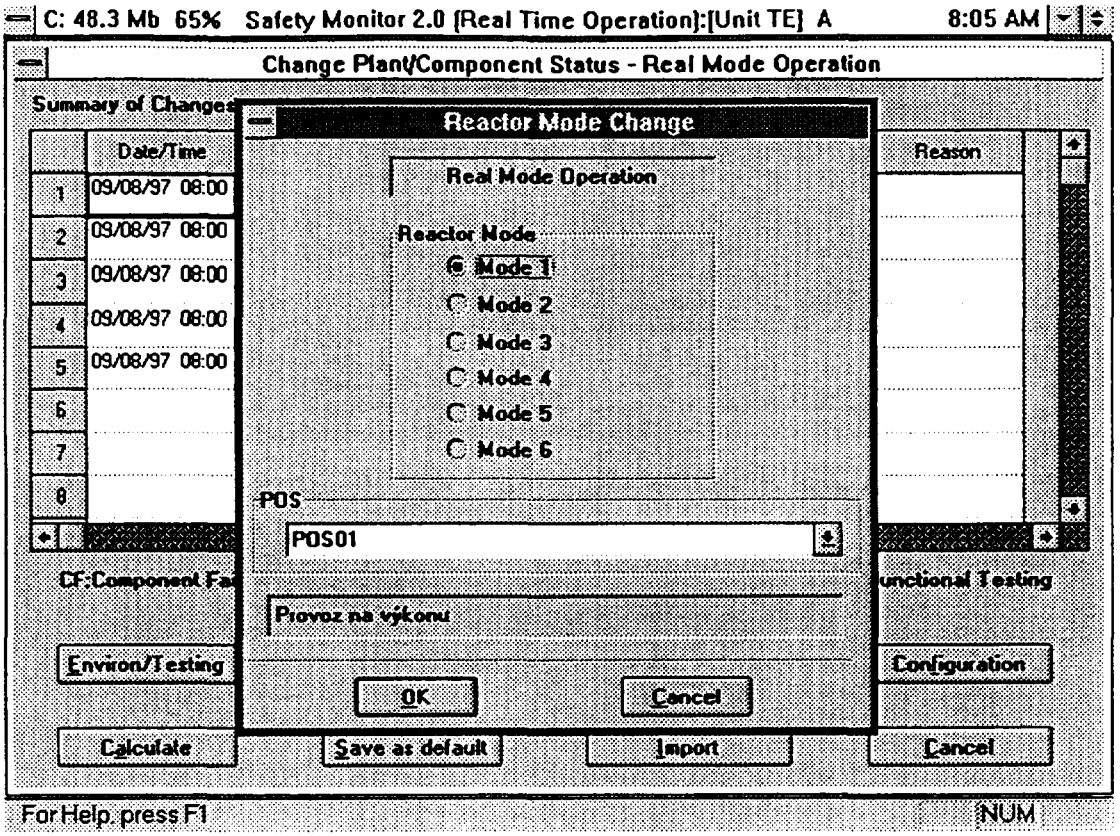
SAFETY MONITOR SCREEN - RISK PROFILE MENU



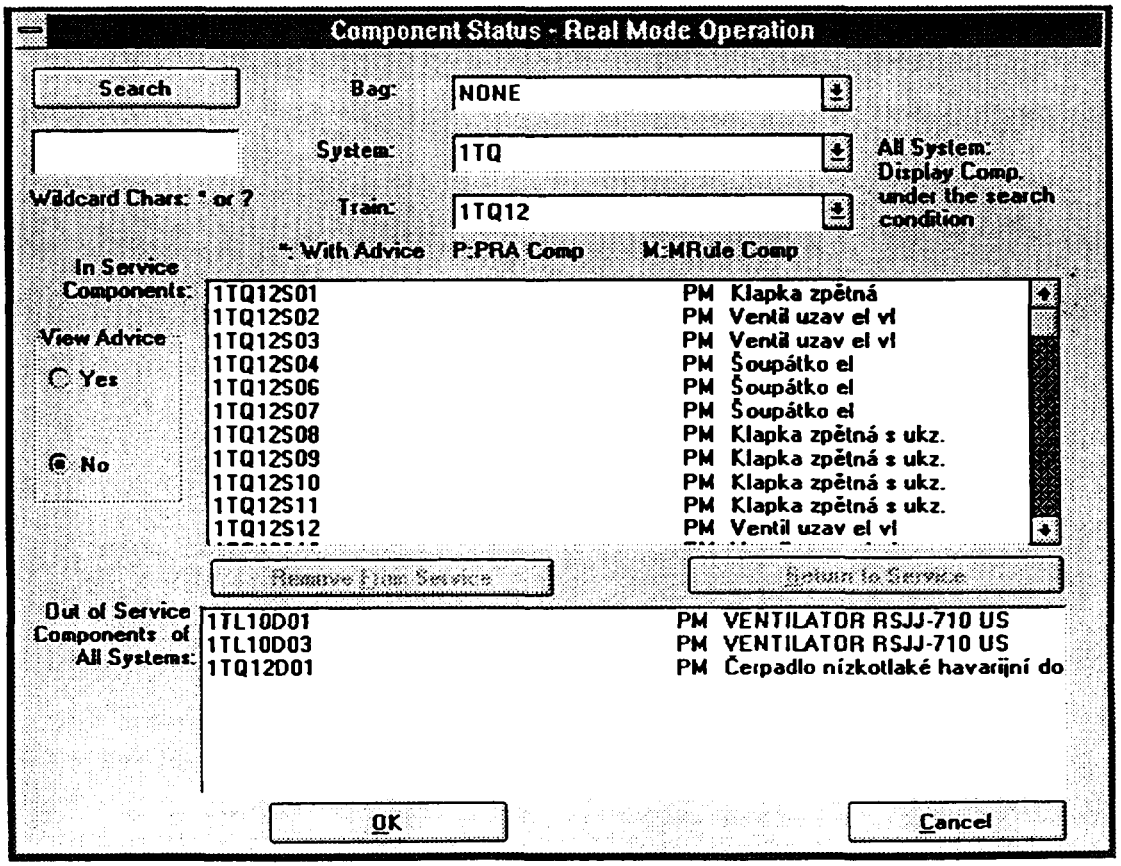
OPERATING STATUS SCREEN



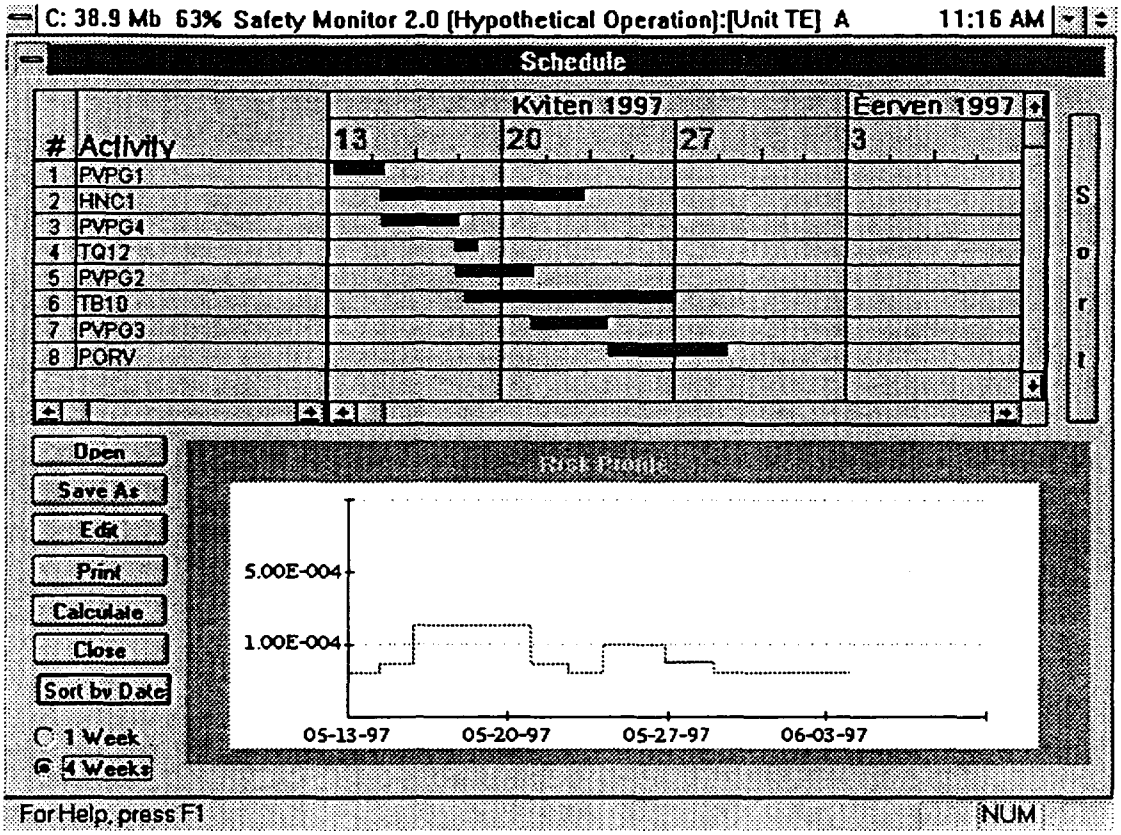
REACTOR MODE CHANGE SCREEN



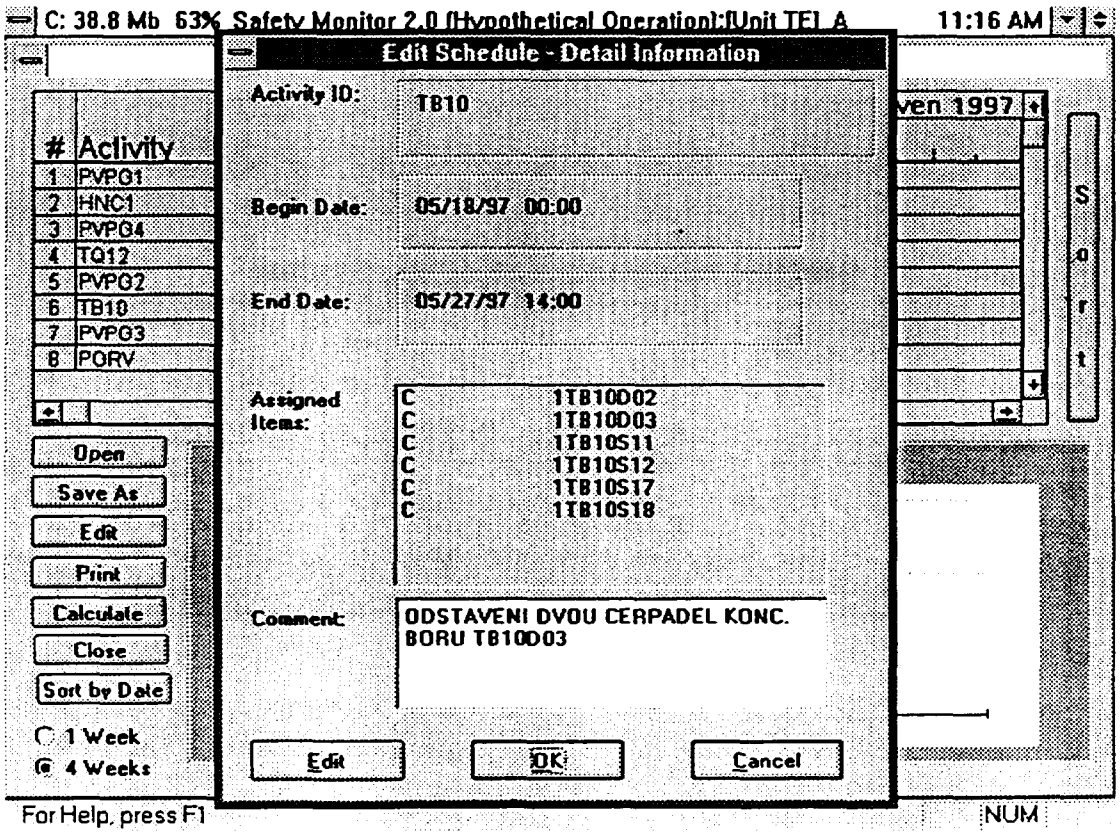
COMPONENT STATUS CHANGE SCREEN



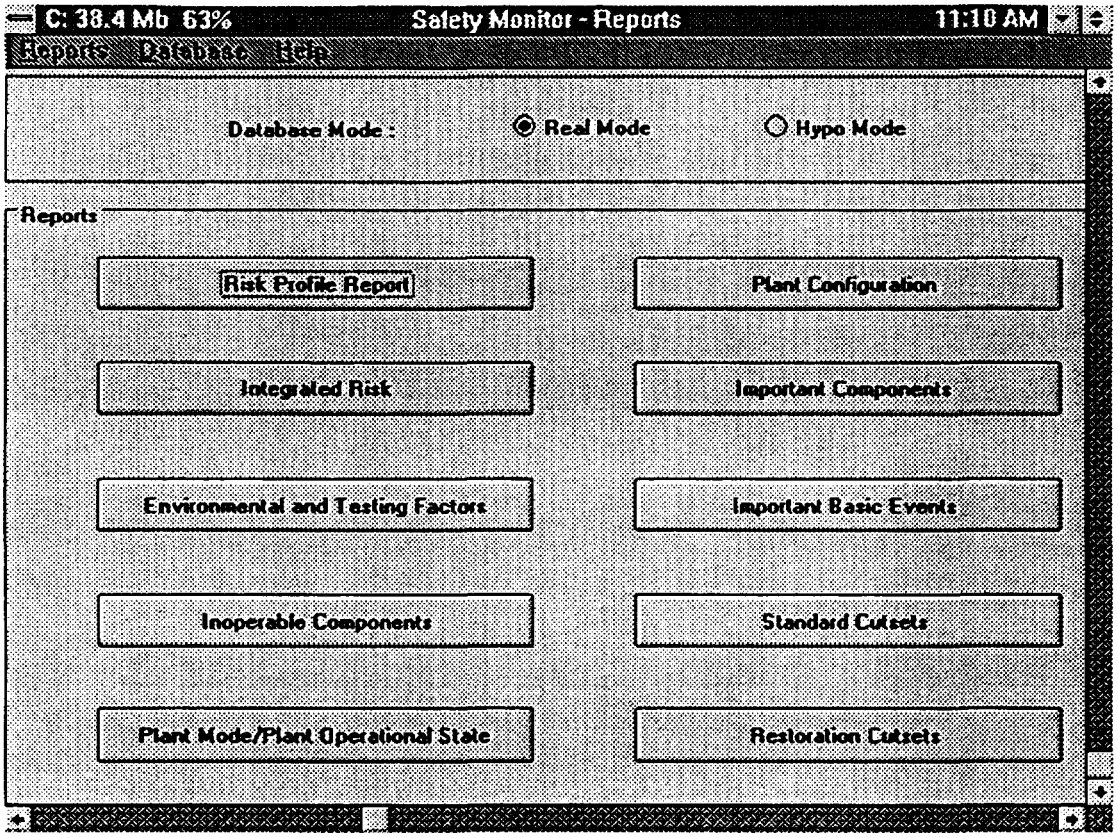
SAFETY MONITOR SCHEDULER SCREEN



SAFETY MONITOR SCHEDULER - EDIT ACTIVITY SCREEN



SAFETY MONITOR REPORT SCREEN



SAFETY MONITOR MAINTENANCE RULE REPORT