Current state of verification for safety relevant software with regard to the change of the millennium in German nuclear power plants.

IMPACT OF YEAR 2000 ON NUCLEAR INDUSTRY

8 to 10 February 1999, Ottawa

H. Heinsohn

Content:

- Procedure pursued by the authorities
- Year-2000 catalogue of requirements
- Status of implementation by the power stations
- Systems that will expectedly remain unaffected
- Systems that may be affected
- First results and already identified problem areas
- Summary and outlook

Procedure pursued by the authorities and their experts

- Measures taken so far
  - June 15,1998: Information Notice issued by GRS
  - July/98: Utilities ordered by the *Länder* (states) authorities to check the systems
  - October 28, 1998: "Hearing of the utilities on the principle procedure“ in front of committees of the Reactor Safety Commission (RSK)
  - October 28, 1998: Formation of the RSK Working Group Year 2000 Programme (RSK-WG-Year-2000)
  - December 2, 1998: Publication of the Year-2000 catalogue of requirements by the RSK-WG-Year-2000.
  - December, 1998: Supplement to the Information Notice by GRS with a recommendation for the 12 German states authorities and the operators to proceed according to the Year-2000 catalogue of requirements.

Procedure pursued by the authorities and their experts (2)

- Dates planned:
  - February, 1999: 2nd Meeting of the WG-Year-2000
    Assessment of the listed systems
  - April 1999: 3rd Meeting of the WG-Year-2000
    Assessment of the assigned conformity stages
  - June 1999: 4th Meeting of the WG-Year-2000
    Assessment of the upgrading measures
  - July 1999: Planned date of conclusion of the project to all in accordance with the Year-2000 catalogue listed systems.
  - Assessment by the licensing authorities and their experts

Year-2000 catalogue of requirements

- Objective:
  Uniform procedure to demonstrate Year-2000 conformity

- Definition of Year-2000 conformity:

  BSI DISC PD2000-1

- Application field:
  - Systems to control design bases accidents and processes of abnormal operation.
  - Systems which on their failure to function demand immediate or short-term termination of power operation (up to about 12 hours).
  - Other safety-significant systems (like e.g. fire alarm system, radioactivity monitoring system).
  - Systems used for physical plant protection.

The Year-2000 catalogue of requirements (2)

- Project organisation
  Fixation of the Objectives, project management and performance, competencies and responsibilities, frame schedule, project execution scheme.

- Project performance
  - Registration:
    The software based systems and components are to be fully registered.
  - Categorisation:
    The systems are to be categorised according to their possible influence on plant operation:
    - S: systems to control design basis accidents and processes of abnormal operation
    - V: systems which on their failure to function demand immediate or short-term termination of power operation (up to about 12 hours)
    - B: systems that have to be registered but do not have to be categorised into S or V.

Year-2000 catalogue of requirements (3)

- Conformity stages
  For the systems and components, the individual conformity stages are to be defined:
  - Conformity stage 1:
    the system or component is Year-2000-conform
  - Conformity stage 2:
    the system or component is Year-2000-conform following a single modification
  - Conformity stage 3:
    the system is not Year-2000-conform, but the effects are tolerated.

- Analysis:
  - Recommended check lists fore the year-2000 conformity analysis are the check lists of NEI/NUSMG 97-07, Appendix H
  - It is also allowed to take an other check list if they is equivalent to the recommended check list.

Status of implementation by the power stations

- Year-2000 projects exist in all plants
- Registration is nearly completed
  (final date is January 1999)
- A categorisation with regard to a possible impairment of plant operation is also nearly completed.
- The analyses of Year-2000 conformity are going on.
- Utilities have planned the system tests; the intention is to perform these tests during plant outages wherever this is possible.
- The final date planned by all plants for the systems to be analysed according to the catalogue of requirements is end of July 1999.

Systems that will expectedly remain unaffected

- Safety system
  - There are only few components with embedded systems, e.g. speed measuring transducer, neutron flux instrumentation
  - The components are qualified according to KTA Standards, which involves i.a.
    - detailed documentation,
    - a type inspection by independent experts, and
    - the demonstration of a quality system by the component manufacturers.
- Limitation systems
  - In the first line hard-wire technology is used in these systems.
  - 2 plants use the computer based system Teleperm XS (Siemens-made); however, Year-2000 conformity has been demonstrated in the qualification.
- Conventional alarm system

Systems that may be affected (1)

- Operational systems that interfere directly with plant operation
  - reactor control
  - neutron flux measurement
- Computers used for in-service inspections
- Component monitoring systems
  (e.g. pump monitoring system, loose-parts monitoring system, leakage monitoring system, vibration monitoring system)
- Computers used for servicing, diagnosis and archiving
  (e.g. programming devices for SPSs or service computers for Teleperm XS)
- Measuring and information systems
  (aeroball system, computer annunciator system, accident consequence computer)
- Alarm systems
  (fire protection and fire alarm systems, activity and local dose monitoring systems)

Systems that may be affected (2)

- Systems organising plant operation
  (operational management systems, access control systems, telephone systems)
- Digital component controls
  (lifting gear, handling equipment, elevator controls)
- Meteorological monitoring systems
- Systems not belonging to the power plant itself
  (power supply grid, nuclear power plant simulators, remote monitoring systems of the authorities)

First Results and Already Identified Problem Areas

- As expected, the review of the safety systems and the systems involved in dealing with abnormal operation uncovered only two component groups where the year-2000 conformity had to be checked.
  - Rotational speed transducers (Jaquet) on a few primary coolant pumps and on the overspeed governors of the emergency power diesel generators.
    - The company Jaquet has issued a year-2000 conformity declaration for these transducers.
  - Special types of neutron flux measuring lances
    - The year-2000 conformity checks of this equipment by the manufacturers are still under way.

First Results and Already Identified Problem Areas (1)

- The remaining systems relevant to safety
  - I&C equipment employed within the plant controls, a year-2000 conformity declaration is available for Contronic 3 by ABB;
    the conformity checks for the other systems are still under way.
  - In the control rooms problems were identified for a few types of paper recorders.
    It was found that at the change of millennium these recorders would automatically switch to a rapid paper advance.
    However, after activating the reset function, this problem would be solved and should not reoccur.
  - Process computers (for physics calculations and handling of alarms).
    The examination has not yet been completed.
    Nevertheless, software updates were carried out in the older types.
  - Findings have been identified in the fields of radioactivity measurements and personal dosimetry, in the access control systems, fire alarm systems and the meteorological computers;
    these problems have not yet been completely solved

Summary and outlook

- Year-2000 projects have not yet been completed
  (The requisite demonstrations are not yet available or have not yet been checked by the independent experts)

- So it is not yet possible to make a final assessment

- But even so, on the basis of the already available information, we expect:
  - The safety of the German nuclear power plants will not be jeopardised at the change of the millennium.
    - Only a few, specially qualified components are affected
    - The Year-2000 conformity is systematically demonstrated
    - The demonstrations are checked by independent experts;
  - As regards the remaining large number of components and systems to be examined, there still exists the principle possibility that there may be individual disturbances despite the systematic examination within the framework of the Year-2000 programmes. For these cases, all nuclear power plants have provided contingency plans as a supplement to the Year-2000 conformity demonstrations.