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

Content:

1 Introduction

The year-2000 issue has been intensively addressed in German nuclear power plants for about a year. Aside from the power utilities operating these plants, the manufacturers and expert organisations as well as the German Reactor Safety Commission (RSK) - an advisory commission to the Federal Minister for Environment, Nature Conservation and Nuclear Safety (BMU) - all have been involved in this subject matter. However, due to the change of government last Fall the RSK was dissolved by the end of 1998.

At the time this paper is being prepared, neither have new members of RSK nor its working groups has yet been appointed. Thus, the RSK Working Group on the Year-

2000 Issue (*RSK-WG-Jahr-2000*) does not exist at this time, but it is expected that a new advisory group will be formed in the near future to continue the work.

2 Procedure pursued by the authorities and their experts

An outline of the procedure pursued by the authorities shall stand at the beginning of this paper. In this context, the most important measures shall be introduced, divided into a description of the measures that have already been implemented and an outlook on those that will still have to be taken during what remains of 1999.

The measures taken by the authorities to analyse the Year-2000 issue with regard to German nuclear power plants were sparked off by an Information Notice issued by *Gesellschaft für Anlagen- und Reaktorsicherheit (GRS)* in May 1998. These Information Notices are part of a proven procedure by which GRS, on behalf of the Federal Minister for Environment, Nature Conservation and Nuclear Safety (BMU), informs the 12 licensing authorities of the German Federation, their expert organisations as well as the power utilities on events of general safety significance and makes recommendations of measures derived from the analysis of these events. It is then up to the utilities to demonstrate to the respective licensing authorities how they have implemented the recommendations of GRS on a plant level.

At the end of October 1998, all utilities reported to committees of the German Reactor Safety Commission (RSK) on the state of the work and the scheduled final dates of the respective Year-2000 programmes. They had been asked to address a previously specified catalogue of questions of the RSK on project structures. Details of the state of the activities performed by the utilities will be described in the following section.

Also in October 1998, an RSK Working Group on the Year-2000 issue (*RSK-WG-Jahr-2000*) was formed on request of the BMU. This working group was to meet about every 2 months and in order to define requirements, monitor the state of the activities and prepare as early as possible a final assessment for the BMU of the Year-2000 programmes of all power utilities.

At the 1st meeting of the *RSK-WG-Jahr-2000* at the beginning of December 1998, a "Compilation of the information necessary for the safety-related assessment the programmes scheduled by the German nuclear power plant operators to ensure Year-2000 software conformity„ (catalogue of requirements) was worked out. This catalogue of requirements contains the criteria for the assessment of the Year-2000 conformity demonstrations to be checked by the German supervisory authorities. Details of the essential requirements of this catalogue will be presented in a following section.

At the end of December 1998, GRS issued a supplement to its June 1998 Information Notice in which the latest developments in Year-2000 conformity demonstrations were considered. On account of the December Information Notice, the catalogue of requirements became part of the supervisory procedure of the authorities. In addition, the December Information Notice also sets deadlines for information to be provided on the progress made by the projects.

The planning for the remaining time until the change of millennium is governed mainly by the scheduled meetings of the *RSK-WG-Jahr-2000* and the final assessments by the local licensing authorities. The schedule of meetings of the *RSK-WG-Jahr-2000* is largely in line with the expected progress of the projects. The current schedule calls for three meetings until the middle of 1999:

- end of February 1999: assessment of the listed systems,
- April 1999: assessment of the conformity stages assigned to the systems,
- June 1999: assessment of the upgrading measures and submission of a final assessment.

By end of July 1999, the projects to be carried out according to the catalogue of requirements should be concluded. Purely operational systems do not fall under the catalogue of requirements; in many cases, the projects relating to these systems are scheduled to continue until November 1999.

Beginning in August 1999, detailed checks will be performed by the local supervisory authorities and their experts relating to the Year-2000 conformity demonstrations prepared by the power utilities for the systems and components with safety

significance. However, local experts will already begin assessing certain projects as they are getting underway.

3 Year-2000 catalogue of requirements

As already mentioned in the previous section a catalogue of requirements exists that represents the basis for the Year-2000 conformity demonstrations in Germany. The most essential requirements shall be briefly described.

The aim of the catalogue of requirements is to define the necessary requirements for the Year-2000 conformity demonstrations and a standardised procedure in Germany from the specific point of view of safety. Based on the definition of Year-2000 conformity according to the British Standards Institute (BSI; DISC PD2000-1), all necessary requirements regarding project organisation, project management, depth of demonstrations and documentation, and the additional contingency planning are covered. The information needed for a general assessment is also specified. The general assessment should lead to the achievement of a uniform safety level preventing any safety-relevant operational disturbances.

The catalogue of requirements deals with the relationship between the power utilities and the supervisory authorities. Also for this reason, it contains only those systems and components that may impede the safe operation of nuclear power plants. Although other systems, e.g. office communication systems, are in fact included in the Year-2000 programmes of the power utilities, their checks remain solely in the responsibility of the utilities themselves. The scope of the catalogue of requirements specifies the systems for which demonstrations have to be furnished. Corresponding to their respective safety significance, the catalogue of requirements applies to

- systems to control accidents (safety systems),
- systems to control processes of abnormal operation,
- operational systems which upon functional failure may directly result in a disturbance of power operation lasting up to a maximum of about 12 hours,
- other safety relevant systems (e.g. fire alarm systems, radioactivity monitoring system),

– systems used in physical plant protection.

The general requirements for project organisation and project performance contained in the catalogue requirements are generally in line with common procedures as laid down, e.g., in the publication on "Nuclear Utility Year 2000 Readiness" (NEI/NUSMG 97-09). However, a few special issues have been added.

For example, the systems are classified according to their possible influence on plant operation, with a distinction being made between the following categories:

– S: Systems to control design basis accidents (e.g. reactor protection system) and processes of abnormal operation (e.g. limitation systems),

– V: Systems which upon functional failure demand immediate or short-term termination of power operation (e.g. control systems, components protection system),

– B: Systems that shall be registered but do not belong into categories S or V.

For those systems that may have a direct influence on the safety systems or on plant operation - categories S and V - a demonstration of Year-2000 conformity is an absolute necessity. This means that it must be demonstrated without any restrictions that neither performance nor functionality is affected by any dates prior to, during or after the year 2000.

Restrictions with regard to the demonstration of Year-2000 conformity are admissible only in the case of systems that have no direct influence on the safety system or on plant operation - category B. In practice it will thus be possible to, e.g., postpone some upgrades to the first half of the year 2000, allowing for a better use of the available resources. For this reason, two sub-categories of absolute Year-2000 conformity have been defined:

– The system or the component shows Year-2000 conformity following one single modification carried out after the change of date.

– The system or the component does not show Year-2000 conformity, however, the consequences are tolerated.

In this connection, proof also has to be furnished - apart from the Year-2000 conformity demonstrations - that the organisation of the necessary one „single modification" is ensured or that the consequences can actually be tolerated.

A general requirement is that the demonstrations must be performed in accordance with the original quality system demonstrations. In the case of the I&C equipment of the safety system, for example, this means that proof has to be furnished that the authorised expert will be able to convince himself of the Year-2000 conformity of this equipment. Here, a declaration of conformity by the system manufacturers alone does not usually suffice. In the case of an operational control system (BOP), on the other hand, it is usually sufficient if the system manufacturer alone presents a declaration of conformity.

If upgrading measures are taken to reach Year-2000 conformity, these have to be performed in line with the applicable standards for the respective component groups.

4 Status of implementation by the power stations

The status of implementation concerning the checks of Year-2000 conformity on a plant level is currently changing from day to day. This means that the information has to be constantly updated. This rapid change is caused by the fact that all Year-2000 projects are currently in the "hot phase". Based on the statements by the power utilities to the committees of the RSK in October 1998, the following picture emerges:

- Year-2000 projects exist in all plants.
- Registration and categorisation with regard to the possible effects on operation of the software-based systems has largely been completed. The planned final date is end of January.
- The analyses of Year-2000 conformity and the possibly required upgrading measures are currently in progress.
- The system tests that are necessary to demonstrate Year-2000 conformity are presently in the planning stage. Here, risks have to be minimised under consideration of possible perturbations of plant operation. Therefore, the utilities' intentions are to perform these system tests during plant outages.

– The final date planned by all plants for the systems to be analysed according to the catalogue of requirements is end of July 1998.

5 Systems that will expectedly remain unaffected

Systems which from our point of view will not be affected are the safety system and the limitation systems as well as the conventional alarm systems.

The safety system uses hard-wire technology. Depending on the date of plant construction, there exist only a few measuring transducers and electronic calculation circuits that will have to be examined also with regard to embedded systems. For these components, Year-2000 conformity has to be demonstrated in the same way as the original demonstration of their proven qualification for operation in the safety system. This means that a detailed demonstration is required and that every detail has to be clear to the authorised experts.

As regards the limitation systems, there are two plants which, for one year, have been using modern digital instrumentation and control systems (TELEPERM XS made by Siemens). In the qualification of TELEPERM XS, Year-2000 conformity has already been demonstrated. In all other German nuclear power plants, the limitation systems use hard-wire technology, which means that here, too, there are only a few components with embedded systems where an examination is required. For these as well as for the components of the safety system, the rule also applies that the examinations have to be well documented, that they must only be made by specially qualified manufacturers, and that the demonstrations have to be checked by authorised experts.

The conventional alarm system receives and processes all the important signals from the safety system. It is designed as a hard-wire annunciator panel.

6 Systems that may be affected

Generally, one can say that the number of possibly affected systems and components in a plant depends on the date of plant construction or plant modifications. In this connection it has to be taken into account that, in Germany, the most recent plants

are already ten years old. The following list therefore contains systems that are classified as software-based that are available maybe in only a single plant.

- Operational systems that interfere directly with plant operation (reactor control and neutron flux measurement),
- Computers used for in-service inspections,
- Component monitoring systems
  (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 PLS's or service computers for TELEPERM XS),
- Measuring and information systems
  (aeroball system, computer annunciator system, incidence sequence computer),
- Alarm systems
  (fire protection and fire alarm systems, activity and local dose monitoring systems)
- Systems required for 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)

7 Already identified software problems

As this paper had to be prepared in early January and the first concrete results of the registration in Germany were only provided by the operators at the end of January, this section will be presented orally at the Ottawa conference. It will then include all the latest information available.

8 Summary and outlook

Since the Year-2000 projects have not yet been completed and the requisite demonstrations are not yet available or have not yet been checked by authorised experts, it is not possible to make a final assessment of the situation. However, on the basis of the information already available GRS is of the opinion that

- the safety of the German nuclear power plants is not in jeopardy at the change to the Year-2000; this judgement is based on the fact that only a few, specially qualified components in this area are affected whose Year-2000 conformity is systematically demonstrated within the framework of the Year-2000 programmes as well as on the circumstance that these demonstrations will be checked by authorised experts;
- as regards the remaining large number of components and systems to be examined, it is principally still possible 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.