XA9642715 - 725

IAEA-IWG-NPPCI-96/3
LIMITED DISTRIBUTION

WORKING MATERIAL

MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEMS IN NUCLEAR POWER PLANTS

REPORT OF AN ADVISORY GROUP MEETING ORGANIZED BY THE INTERNATIONAL ATOMIC ENERGY AGENCY AND HELD IN VIENNA, AUSTRIA, 25-29 MARCH 1996

Reproduced by the IAEA
Vienna, Austria, 1996

Table of Contents

MEETING REPORT

The need for frequent backfitting of instrumentation and control systems arises from specific conditions such as: rapid obsolescence of technologies as a consequence of which new designs with new operational characteristics have to be employed; the high potential for improving and broadening I&C application to achieve improved on-site operational benefits at relatively low cost; and new regulatory requirements.

The reasons for upgrading the instrumentation and control systems in nuclear power plants are to take advantage of modern technology to improve plant availability and to reduce instrumentation and control's contribution to escalating operating and maintenance costs. Modern instrumentation and control technology, using analogue and digital equipment to the best advantage, brings increased reliability, safety and cost-effective plant operation.

The Advisory Group Meeting on "Modernization of Control and Instrumentation Systems in Nuclear Power Plants" was held in Vienna, Austria, from 25 to 29 March 1996 and was attended by 21 experts from 14 countries. The meeting was organized jointly by the Department of Nuclear Energy and the Department of Nuclear Safety.

The objectives of the meeting were:

- To solicit and analyze information from Member States regarding their experience in modernization of I&C in nuclear power plants.
- To identify requirements for the system modernization.
- To initiate the development of an IAEA TECDOC on "Modernization of I&C in Nuclear Power Plants"
- To consider and approve the Objectives of the TECDOC.

5. To prepare the extended outline of the TECDOC.

The new technical document on the subject has to be produced as a consequence of the recommendations of the International Working Group on Nuclear Power Plant Control and Instrumentation to produce a guidance on NPP C&I modernization.

The participants agreed to the fact that the new technical document has to help plan, develop, and implement I&C systems for operating nuclear power plants, help develop cost effective approaches in qualification, verification and validation to address regulatory approval for new (digital) systems, guide for research and development of advanced technologies for improvements of safety, reliability, and productivity of present and future nuclear power plants.

The time schedule for the preparation of the first draft of the report was agreed as follows:

1) Material from the Contributors to Technical Leaders: **15 June 1996**
2) Material from Technical Leaders tot he Project Leader: **15 August 1996**
3) First draft report to the IAEA: **15 October 1996**
4) Draft report to the project team members: **15 November 1996**
5) Next meeting: **2-6 December 1996**

The participants of the meeting suggested that the technical report should be published as a TECDOC and distributed to all nuclear utilities in Member States as well as to main design organizations.

The extended outline of the document was prepared and further responsibilities of the technical report were discussed and agreed upon (see Table 1).

Table 1

TECDOC on Modernization of I&C in Nuclear Power Plants

Contributors and Their Responsibilities

(29 March 1996 Status)

Names/Chapters	1	2	3	4	5	6	7
Mr. Miliovsky, Bulgaria					+		
Mr. Karpeta, Czech Rep.					TL		
Mr. Wahlström, Finland					+		TL
Mr. Dall'Agnol, France			+				+
Mr. Bastl, Germany	TL	TL			TL		
Mr. Toth, Hungary			+	+	+		+
Mr. Kim, Rep.of Korea						+	
Mr. Koo, Rep. of Korea				+			+
Mr. Pobodonostsev, Russian Fed.		+	+	+	+		+
Mr. Arbiza Berregui, Spain				+		+	
Mr. van Gemst, Sweden				TL	+		
Mr. Clarke, U.K.						TL	+
Mr. Wall, U.K.				+	+		
Mr. Yastrebenetsky, Ukraine		+		+	+		
Mr. Naser, U.S.A. (**PL**)			TL				

TL - Technical Leader

+ - Contributors

PL - Project Leader

Technical Document
on

MODERNIZATION OF CONTROL AND INSTRUMENTATION SYSTEMS IN NUCLEAR POWER PLANTS

Extended Outline prepared by the AGM Meeting held in
Vienna, Austria,
25-29 March 1996

1. INTRODUCTION

This report has been produced in response to the perceived need for collective consideration of the issues and approaches to plant modernisation that is becoming necessary as many operating power reactors approach their 20th to 30th year of operation. The need for the activity, particularly for Instrumentation and Control systems was indicated by the IWG during its general meeting. Further discussion of the topic at Garching confirmed this need and international support that would be available for such an activity.

The report attempts to address a very wide range of circumstances from, old plant operating at very low powers that face major ageing issues, to new potentially high performance plant for which it has been decided I&C improvements are required to resolve safety issues. The process of change raises many issues as to what potentially might be achieved by such a change to overcome obsolescence, economic and safety problems. The report must also include appropriate consideration of the increasingly international nature of the instrumentation and control system supply industry. Consequently it does not ignore the different national approaches that are used to demonstrate the systems are suitable to be brought into service. The report does not seek to provide advice on how the different national licensing processes should be approached.

The audience for the report is all those considering Instrumentation and Control system change. It is hoped that by identifying the issues and giving examples of cases where change has been successfully achieved and indicating where and why difficulties have been encountered, that others starting on such changes can benefit from experience.

The report is structured to follow the probable lifecycle of a modernisation exercise and thus starts by considering the things driving change and the strategy to be adopted to make the change. Thus chapters 2 and 3 of the report includes a discussion of continued maintenance of ageing equipment, as well as issues such as choice of technology if the conclusion is that change is required. The engineering issues are discussed in chapters 4, 5 and 6. These examine the process from initiation to commissioning on the plant and identifies some of the issues arising from choice of technology. Chapter 7 discusses human issues, this is considered to be particularly important as if the change is not managed correctly then many benefit could be lost indeed the change may be detrimental to plant operation. The issues treated in this section include the management of the old and new equipment on the plant and the very different interface it has to the operations and maintenance staff.

2. PRESENT SITUTAION AND THE NEEDS FOR MODERNIZATION

The present situation is that many reactors are approaching mid life and some of the systems particularly vital instrumentation and control systems are approaching the end of their life. The plant operators are faced with crucial decisions as to the strategy for continued operation of the plant, recontinued system maintenance, system replacement or system upgrade. These decisions are to be made in an increasingly competitive environment as electricity supply is deregulated and so enhancement of plant performance as well as achieving cost reduction becomes paramount.

In practice the situation is different from one plant to the other, so that the aspects for refurbishment vary in priority. Some typical examples may demonstrate the basic differences:

- Ageing: Towards the end of the life time (for I&C typically 20 years) more inspection and repair work has to be performed in order to keep the necessary reliability of the system. Furtheron the original vendor may not produce any more systems of the old technology or may have disappeared from the market. Though partly powerful workshop installed on-site, and partly special vendors are financed by the utilities, a situation like this causes rising maintenance costs and moreover the risk of spare part delivery, so that an exchange of the concessed systems becomes highly necessary despite the fact that the availability or safety targets are still achieved.

- Quality Assurance: Adequate QA plays an important role for high integrity systems. For older systems - regardless of their real quality - this vigorous QA process is missing or the quality of documentation does not meet the standard of today. In this case the lack of confidence in the quality of systems which are applied in sensitive areas of the plant provide the prime impact to the decision for modernization. Those decisions mostly go along with the expectation of an improved availability.

- Progress in technology. Computer-based digital I&C systems have many advantages when compared with the analogue technology. Performing of complex calculations, high flexibility and easy adaption to later changes are basic advantages. Extended self-testing during operation reduces the amount of manual repetitive testing, can make the best coverage more complete and reduces the potential for human error. Improvement of MMI not only comprises the use of screens in the control room, but also the presentation of complex situations by means of specialized graphs and diagrams. In all this there is a gain of functionality which in many cases drives the decision for improving I&C systems.

- Operator support systems / diagnosis systems. methodologies developed for operator support, e.g. SPDS, success pass monitoring, or for diagnosing the mechanical health of the plant, e.g. loose parts monitoring, vibration monitoring, can be realized in an effective manner by means of computer based systems only. They offer a vast field of providing useful information to the operator and making the operation of a plant more effective and safer. These systems are most of the time stand-alone systems, they are comparably loosely coupled to traditional existing I&C and hence are add-ones which do not call for extensive installation efforts.

- Sensors and actuators. Protection systems have to be tested repeatedly with great care, with a special issue being the demonstration of the accidental resistance of the concerned components. For this purpose special test procedures have to be applied, e.g. by taking specimens from the relevant components of the plant and performing tests reproducing the stress under accidental conditions or to test components in situ by means of special procedures like spray testing etc. It is important to note that by means of these procedures, relevant faults can be timely detected and repaired; moreover an insight into the overall status of these components is achieved which ultimately determines the decision if replacement by new items has to be performed.

In summary, most of the time it is a combination of the reasons given above, which lead to the decision of modernization. Safety issues are not the prime motivation for considering a large refurbishment, it is rather system obsolescence, the reducing availability of spare parts and the potential gain in system performance and functionality which drive the utilities' decision towards application of modern I&C technology in existing plants. The completion of such a change will bring safety benefit as reduction of operator action for testing, and repair will reduce the number of human errors and potential challenges to the safety systems.

3. STRATEGY

Instrumentation and control systems in nuclear power plants need to be modernized in a systematic, reliable, and cost-effective manner to replace obsolete equipment, to reduce operations and maintenance costs, to improve performance, and to enhance safety. To achieve the maximum benefits from I&C modernization, it is important for the utility to develop long-term planning and implementation strategies which include the definition of the vision for the plant at the end of the planning horizen. The strategy will be to look at the I&C systems in the context of the entire plant to determine which ones should be maintained, replaced, or upgraded. The strategy will prioritize the I&C modernization activities. It will identify the infrastructure required to implement the modernization so that the vision will be achieved in a systematic manner.

3.1. GENERAL APPROACH

As the problems mostly arise at the maintenance level of the given I&C system or component, the utilities, in the past, have tended to handle the question on that particular equipment without taking into consideration the plant as a whole. It is important to make modernization decisions based on the overall vision for the plant so that a particular modernization supports that vision.

- comprehensive
- systematic
- life cycle
- reasons for this approach
- goals to be reached
- based decisions on justifiable arguments
- participants involved

3.2. CURRENT STATE OF I&C SYSTEMS IN PLANT
(information obtained here will be useful for the future requirements)

Since their commissioning, I&C equipment have been modified. It is necessary to know precisely the present state of the I&C systems and their operating history in order to make appropriate decisions for the modernization of them.

- definition of the I&C systems
- collect documented information to support the decisions (adequacy and quality)
- description of I&C systems (limits, boundaries, environment, location, power supply, grounding, operating characteristics, suppliers supports, ...)

3.3. PLANT POLICIES AND EXTERNAL REQUIREMENTS

The main goal of the plant policy is to cost-effectively produce power through incresing power production, decreasing O&M costs, and enhancing safety. The plant policy will identify the goals and objectives of the utility that will effect I&C modernization. The external requirements that effect I&C modernization must all be identified. This combination of plant policy and external constraints will determine the plant vision and drive the modernization activities.

- other projects presently ongoing and planned (safety reassessment, fire sectorization reassessment, ...)
- long term business plan objectives
- external requirements (regulatory issues, load following capability)

3.4. UTILITY DEFINED CONSTRAINTS

There are several constraints defined by the utility internally that must be satisfied by the I&C modernization activities. These constraints must be identified and satisfied in the implementation plans for I&C modernization.

- develop plant specific guidelines for consistent modernization
- stepwise versus global modernization
- physical constraints (including technological constraints)
- economic constraints
- safety constraints
- technology constraints
- human constraints

3.5. DEFINITION OF VISION FOR I&C SYSTEM

A global vision of the overall future I&C configuration is to be defined at the beginning of the modernization activities in order to coordinate the activities and the implementation of the new equipment. I&C modernization can effectively be carried out during several years based on the needs and constraints of the utility. This global vision includes foreseeable new functionality to support the goals for the plant. It includes consideration of the MMI, system boundaries, process data storage, database management, etc.

- define the desired level of automation
- creating new functionalities
- global view of I&C (communication, man machine interfaces, process data storage, life duration of the I&C systems, database management, I&C systems management)
- desired availability of functions

3.6. DETERMINE WHAT TO DO WITH SPECIFIC I&C SYSTEMS

It is necessary to determine what is the proper thing to do with each piece of I&C equipment based on an integrated assessment of the plant and I&C systems. A criteria for this assessment is required to allow informed decisions. A preliminary decision for each piece of I&C equipment is made based on this criteria.

- to keep
- to replace
- to upgrade
- full system or components only modernization
- make preliminary decision for each system based on integrated evaluation
- choice of the systems which need detailed observations

3.7. OBSERVATION IN DEPTH

By detailed analysis of the selected system, the optimal solution must be defined. After comparison with the original decision, the reason of the difference must be found, if any. Then the necessary corrections muct be done.

- evaluate each I&C system in depth
- determine if preliminary decision is correct

3.8. Definition of migration paths

After the appropriate modernization activities have been determined, whatever the modernization will be, major or minor, the activities must be carried out in the correct order to maximize benefits and support the vision for the plant. This order will be determined not only by the I&C renovation but it must also take into account global services (ventilation, power supplies, etc.) and concurrent existing projects which may impact the I&C systems. Relevant activities such as operations and maintenance staff training must be taken into account.

- prioritisation
- develop plan to implement decision
- scheduling

4. ENGINEERING REQUIREMENTS AND CONSTRAINTS

This chapter has been prepared under the assumption that the strategy analysis has concluded that the that old technology is to be replaced by a newer one. The addition of improved functionality within the same technology in the plant is not within the scope.

This chapter will summarise the the important differences between characteristics and performance of different types of technology that is available including:

- relays
- solid state electronics
- computers
- programmable logic controllers PLC
- field programmable gate arrays FPGA
- programmable logic devices PLD
- communication links

In addition to considering the use of new technology to deliver the required functionality its ability to form part of a system, through integration with other information systems for maintenance, engineering, refuelling planning, component database, is described.

References are made where new technology is used in existing nuclear power plants.

The advantages and disadvantages relating to the introduction of new technology for safety and non-safety functions will be discussed briefly.

The consequences of introducing new technology in terms of its influence on the training of personnel, the organisation of the maintenance and the staffing of the control room will be discussed.

In order to have a complete discussion of the engineering process it will be necessary to consider change at:

- the module level
- the system level
- total integrated I&C

The chapter includes a discussion of standards and guidelines that are an important input to the engineering process. It is noted that total compliance to modern safety standards while highly desirable cannot always be achieved when completing plant improvements. Some discussion of the issues is present along with recommendations of how safety evaluation with other methods can be used.

The different schools of thought regarding modernisation as nuclear unique or off-the shelf products are indicated.

Indicate issues to be treated e.g. engineering process, requirements capture and constraints

4.1. SCALE

The section above on strategy identified the different possibilities for upgrade and indicated the great range of size of systems that are the subject of this document. The size of a system along with the degree of complexity will need to be considered when identifying the engineering approach to a replacement or modernisation exercise.

The scale of the change and the time scales for change will also impact on the engineering process. For example if the system change is only part of a major programme it may enforce the inclusion in the requirements of measures to accommodate the changing nature of the environment into which the system is to be placed and the changes in the systems to which it is connected.

4.2. GENERIC REQUIREMENTS

4.2.1. **Recovery of Old Requirements**

The requirements of the old system that is to be replaced has to be generated from existing information to define the starting point for generation of the requirements for the replacement system. In order to assemble the old requirements the following issues must be addressed:

- The characteristics of the old system including: functional requirements, safety requirements, licensing limitations.
- The complete list of inputs and outputs and the links between them. The connections to all external systems must be clearly characterised.
- Evaluation of the operating experience of the old system. Much of this should be available directly from the analysis undertaken to determine if the system in question should be kept under maintenance, replaced or upgraded.
- The threats and challenges to the system should be identified by analysis i.e. the expected challenges, and inspection of the operating history of the current system.

4.2.2. Generation of the new requirements

The requirements of the new system can be grouped for convenience under four headings.

4.2.2.1. *Functional requirements*

The functional requirements should be set down using the requirements of the original system as a basis. Additional functionality should be clearly identified as should unintended but exploited functionality as identified by operations staff.

4.2.2.2. *Deterministic Safety Requirements*

The system safety requirements should be set down, these include:

- original and current licensing requirements
- environmental including EMC/EMI defensive measures
- system tolerances
- the defensive measures to protect system integrity should be set down. These will include measures to prevent unauthorised access and change. In the case of computer based systems security and anti virus measures will need to be identified.

4.2.2.3. *Maintenance Requirements*

The deployment of a new system even one with nominally identical functionality is expected to introduce improved diagnostic and maintenance measures. These measures are expected to include:

- continuous on line diagnostics working either as part of the operating cycle or on operator demand.

- periodic proof test capability of major functions should be provided.

- bypass / override functions should be provided for the duration of testing these would expected to be under strict key control.

- The procedures to be used for system change and upgrade should be set down as part of the maintenance strategy

- periodic and preventiv maintenance

4.2.2.4. *Balance between Automation and Human Actions*

.2.2.5. *Probabilistic Requirements*

- This chapter will cover requirements for both hardware and software.

- Verification methods shall be described.

- Especially it has to be verified that the modernisation of I&C will not decrease availability of safety systems and plant production compared with the existing systems.
- Definitions will be described.

.3. LIMITATIONS AND CONSTRAINTS

Modernisation of the power plant is carried out when installation of the "old" system has been finished.

The specification for the new equipment shall consider the existing design as for:
- physical space
- layout
- ventilation
- area environment
- cabling, connectors
- access
- ranges of in and output signals
- power supplies
- qualification
- environmental accident survival
- cables
- accuracy

This chapter will analyse the consequences of these limitations and describe methods how to take care of these.

4.4. IMPACT OF AND ON OTHER SYSTEMS

Although the basic idea for modernisation is to adapt the new equipment to the existing ones changes to existing systems must be considered.

Existing I&C must be changed for interfacing the new one

Other , non I&C systems, must be changed to provide service functions as:
- quality and ranges for power supplies
- environmental control (cooling, ventilation)
- EMC environment (grounding, screening)

Other impact can be for organisation of and staffing for operation and maintenance

This section will identify possible impacts and describe methods to solve the problem

- availability of data
- timeliness of the data

4.5. OTHER FEATURES

This chapter will cover special features which have not been described in previous chapters including:

- Flexibility, the ability to introduce new functions within the same equipment to meet new requirements
- Expandability, the ability to use the same type of equipment to perform other functions
- Use and qualification of commercially available off-the shelf products e.g. PLCs
- Integration of I&C systems of different technology
- The problem for the operating staff and the maintenance department to live with a mixture of new and old technology.
- Validation of the system functions and man machine interface using simulators
- Strategy for step by step modernisation without degrading plant availabilityor safety
- Interfacing new and old equipment

4.6. COMPLIANCE WITH SAFETY STANDARDS AND GUIDES

The current standards and guides relating to I and C equipment are an expression of the consensus of the best approach to or features of a device, system or systems. In many cases the total compliance with a standard or guide is not required but justification is required for any significant departures. When a replacement I&C system is introduced it would be expected to comply with the requirements of the current standards and guides not those applied when the system was first built. It is often the case that during a backfit to an old plant the demands of the latest standards and guides cannot be met, these circumstances may for example due physical or other restrictions. A common problem in this context is the inability to have the required degree of isolation due to cabling and space considerations. In these circumstances special pleading must be made to justify that safety is not compromised, quite often such pleading appeals to mitigating features such as the presence of fire barriers and fail safe, or known state, design.

Typical examples of deviations and methods how to evaluate these will be given e.g:

- single failure criteria

- physical and functional separation (dependent)

- initiating events combined with related failures
- bypasses for maintenance and testing

5. IMPLEMENTATION OF AN I&C MODERNIZATION PROJECT

Depending on its scope and extend, modernization of the I&C systems at a NPP will be implemented either as one project or as a series of projects. Typical participants in this type of projects will be the utility, design companies, vendors, consulting and service companies. The project should be built according to normal project management practices. A modernization project is however special in that considerable efforts may be needed to regenerate the design basis for the systems. It is also necessary to take the specific structure of the modernization into account and to schedule all tasks in relation to the plant operational schedules with a specific consideration of the planned outages. It may also be important to consider a parallel operation of the old and the new systems.

5.1. PARTICIPANTS IN THE PROJECT

There are many parties involved in a modernization project that may take up varying roles depending on the scope and the allocation of responsibilities in the project. The modernization project is different from projects for building new systems in that the plant operator will have a crucial role of integrating the operational experience in the project. A modernization project will therefore rely on efficient communication between all parties involved.

Roles and responsibilities of the involved parties

Communication procedures

5.1.1. Vendor-utility cooperation

Since most upgrading projects will rely on some available I&C platform it may be advisable to use the same platform as broadly as possible for the modernization. This has regularly been realized as a precompetition project where one vendor has been selected for the final part of the modernization project. This arrangement has the advantage that the utility and the vendor can engage in a close cooperation for adapting the solutions to the plant.

5.1.2. Utility participation in systems design

Sometimes utilities have participated to a relatively large extend in systems design. This effort is mostly then directed towards the application design. Such an effort has a benefit of providing an efficient training for the utility personnel that later on is assigned the responsibilities for maintaining the modernized systems.

5.2. MANAGERIAL ASPECTS OF THE PROJECT

A modernization project will follow the general logic of any project. It will be initiated by the operator of the NPP who in a pre-project phase will evaluate the feasibility of the proposed solutions. This implies the allocation of necessary staff from the operator for various roles in the project.

5.2.1. Project management plan

Reconstruction of the plant I&C systems original design basis

Acqisition of documentation on changes performed on the I&C systems

Individual system requirements specification

Pre-selection of vendors

Sending out questionnaires to the pre-selected vendors

Guidelines for bids evaluation

Issuance of the call for tenders

Bids evaluation

Concluding of contracts

Acceptance of equipment (site acceptance tests)

Storage of equipment

Training of personnel

Equipment installation

Testing and commissioning

Trial operation

Handing over the systems to the operator

Time schedules for individual activities

5.2.2. Project quality assurance plan

Purpose

Items and activities covered QA

Organizational structure of the project's QA/QC

Tasks and responsibilities

Reviews and audits

.Documentation

5.3. PHASES OF THE PROJECT

Design

Manufacture

Site preparation

Installation

Commissioning

5.4. LICENSING ASPECTS OF I&C MODERNIZATION PROJECTS

5.4.1. Review of the country regulatory environment

Identify differences, if any, that exist in the country licensing process of the plant I&C systems when licensing assessment is performed for a new plant and when it is performed for changes in the plant which affect the plant safety.

Identify safety principles and regulatory requirements applicable to your target I&C system.

Based on the classification scheme adopted in the existing licensing process assign safety classes to the I&C systems to be modernized with respect to their importance to nuclear safety.

Identify applicable requirements and design criteria for individual systems included in the modernization project.

Identify quality assurance requirements applicable to individual systems included in the project.

Conduct a comparison of the licensing environment under which the plant operating license was issued with current licensing environment.

5.4.2. Communication with the regulatory body

Two basic options exist.

- The regulatory body is contacted at the project start and is kept involved throughout the whole project implementation.

The regulatory body is approached at the moment when documentation required for licensing assessment is submitted.

Some advantages of the 1st option:

The regulatory body gets familiar with the project in its broader context.

The regulatory body is kept informed right from the project start on both the safety and technical aspects of the proposed changes to the I&C systems.

Timely feedback is obtained with respect to safety aspects of the project

One of the risks associated with the project is kept under control.

Some shortcomings of the 1st option:

Too close involvement of the regulatory body is not desirable because of an increasing potential for a biased assessment of the proposed engineering solutions.

Some advantages of the 2nd option:

The regulatory body preferences do not affect the engineering solutions to be implemented in the project

Some shortcomings of the 2nd option:

An increased risk of nonacceptance of the proposed technical solutions.

Much more time consuming licensing process which may result in delays in the project implementation.

5.4.3. Licensing issues to be addressed in the safety case

Justification of exemptions to the existing regulatory requirements.

New technical specifications and their justification.

Qualitative reliability analysis to demonstrate that the new systems do not introduce new failure modes which were not considered in the plant original accident analysis.

Justification of the adequacy of the new system characteristics such as functionality, performance and reliability with respect to the plant original accident analysis.

If some protective functions of the I&C part of the plant safety systems (reactor trip system, engineered safety features actuation system) have been removed or replaced by other functions or if some performance characteristics of the new I&C part of the plant safety systems such as the response time or accuracy are poorer than those of the original system then a new accident analysis of the same level of rigor as the original one shall be performed and documented.

If the modernization project introduces software-based technology to the plant I&C system then the following issues shall be addressed to the level of rigor commensurate with the importance to safety of the systems involved:

The way the potential for common mode failure in those systems have been considered.

Measures taken to ensure adequate quality of the system software.

Qualification of the computer system equipment.

6. TESTING, COMMISSIONING AND SETTING TO WORK

6.1. STRATEGY

Describe a typical system.

Describe the differences between a refurbishment system and a new system.

Break the problem into smaller parts.

Ensure tests cover the interface between parts.

Run old and new systems in parallel.

Record behaviors of old system.

Consider way to transfer control loops from old system to new 'bumplessly'.

Compare performance of old and new systems.

Integrated testing of complete system.

Issues of RFI testing.

6.2. DATA INPUT / OUTPUT SUBSYSTEMS

Testing connection to original system.

Interactions between old and new system.

Secure changeover points.

Check health monitoring facilities.

Check functionality of subsystem.

Check performance of subsystem.

6.3. COMPUTER HARDWARE AND COMMUNICATIONS NETWORKS

Environmental checks

Performance checks

Health monitoring and error reporting

Main/standby changeover
Links to subsystem

Synchronization and transport delays

6.4. CONTROL SYSTEMS

Consider the way to decommission the old system.

This includes, open loop control, closed loss control and protection systems.

Check the output chain.

Check any feedback checks.

Check any interlocks.

Check other health checks.

Check Changeover mechanism (old to new).

Progressively test the loops.

Variation in loop dynamics - may be an issue.

Need to check any standby channel.

6.5. SYSTEM SOFTWARE

May require special software to link old and new part of the system together.

The use of interface simulation or the availability of spare system for testing the software.

Should seek evidence of the quality of the software including test coverage V&V and evidence of wide usage with error reporting and correction mechanisms.

Need to check functionality and performance of the software and also the error reporting and health checking mechanisms.

6.6. APPLICATION LEVEL SOFTWARE

This can include:

Operation formats - can be derived from data tables.

Database identifiers and alarm levels.

Alarm conditioning - do not usually have time to repeat all the original tests.

Any fault or error reporting system.

Control loops. - Separate.

6.7. INTEGRATED TESTING

Once all the subsystems have been tested there is still a need for complete start to end tests of the system and where possible this should include the parts of the old system which interface to the new one of the subsystem checks have been thorough then sample checks may be adequate at this stage.

Tests should be carried out to confirm that the required system performance has been achieved.

Tests should be conducted to confirm the operation of any facility that could not be tested during the manufacturer's factory acceptance test.

6.8. PARALLEL RUNNING

Definition of parallel running.

Need to be aware of interference between the two systems.

May need buffer amplifiers or special interfaces.

Need to be aware of data skew / latency and sampling error when comparing results.

Need to be aware of any offsets or drift if comparing control loop outputs.

Can take significant effort to explain genuine differences between the old and new system.

Parallel running can be used to validate, formats, alarm levels, alarm logic, etc.

6.9. LABELS AND DOCUMENTATION

Check that all the equipment is correctly labelled and documented.

The documents should allow the utility to operate and maintain the equipment.

Depending on the operator's strategy for long term maintenance and change design information will also be required.

7. PERSONNEL AND OPERATIONS ISSUES

The effective use of control and information systems is dependent on the human interface. The use of equipment particularly that with extensive operator involvement will evolve as the operation staff learn to exploit a systems strengths and compensate for its weaknesses. This will impact upon requirements capture and on the subsequent efficient introduction of new systems. The involvement of the operations personnel must be managed through the change process to ensure that their knowledge is exploited and their confidence gained. Due consideration must be given to operator, and other staff, training to ensure the new systems are correctly used and problems with the management and use of interfaces belonging to the different generation of plant equipment does not compromise the plant.

7.1. OPERATIONAL PHILOSOPHY

It is necessary to have a description of the operational philosophy to be used in the main control room and also in other places where plant staff will interact with the new systems. This philosophy should be based on the task analysis performed for the original control room construction with due consideration of changes in the automation level and task allocations. The involvement of the end users in the development of this general control philosophy shouldbe ensured. Suitable guidelines to ensure the ergonomic quality of the control rool design should be adopted. A special consideration should be given to possible problems of operating the old and new systems in parallel. If major parts of the old control room equipment are left unchanged and the new systems are brought into the middle of the old equipment a special care of harmonization the systems should be exercised.

Staffing

Positions and their responsibilities

Plant operational states

Task analysis

Ergonomic considerations

7.2. APPLIED STANDARDS AND PRACTICES

A large modernisation of the control room eg. the introduction of VDU based information presentation either as a replacement or as a complement to existing information presentation will need decisions on standards to be applied. Such standards are among others color codes, used symbols, use of special effects, etc. The principles and possible problems of operating through VDUs should beconsidered. A special consideration should be given to the time for looking up required displays and information before actions could be initiated.

Project internal standards

Principles for operating through the VDUs

7.3. DISPLAY HIERARCHY

The use of a VDU based control room relies on an easy access to a large number of various displays. The hierarchy of these displays and the principles of transfer between them has to be laid out.

Alarms and events

Overview displays

Detailled displays

Zooming principles

Methods for ensuring availability of important information

7.4. OPERATOR SUPPORT SYSTEMS

A modernisation project will often involve upgrades in the control room providing the operators with specific support systems. The implementation of these support systems should as well as for other systems follow the general control philosophy as laid out for the control room (7.1). The detailed implementation of the operator support systems should also be in accordance with the general standards and principles as laid out (7.2).

SPDS

Early fault detection

Diagnosis systems

Component performance evaluation

Computerized operational procedures

7.5. VERIFICATION AND VALIDATION OF CONTROL ROOM SOLUTIONS

The design should be verified in various stages to make sure that the general design principles are adhered to. Typically this means that agreed quality assurance procedures will be followed. There are various standards and guidelines available for this purpose. Some of the guidlines have been implemented as special tools to support the V&V process. The verification prrocess should be ended with a validation of the new systems using a simulator and operators from the plant demonstrating that they are able to handle the functions of the new systems in an intended way also during major plant transients.

Available guidelines and standards

Methods for the V&V process

7.6. OTHER MAN-MACHINE INTERFACES

In the design of the new systems a special consideration should be given also to the indirect users of the system functions. This means maintenance people, plant I&C engineers and other technical staff. Changes in the systems should be supported through design databases and specific planning tools. The new systems may also provide more functionality in supporting the communication between control room operators, auxiliary operators, maintenance people and technical staff.

Technical support centre

Emergency operating facility

Field communication stations

Control engineering tools

Design databases

7.7. TRAINING AND PROCEDURES

Before the implementation of the system the operators should be given appropriate training. Maintenance people should also be given the necessary training to understand the new system and to diagnose possible malfunctions. The procedures and instructions should also be updated to reflect the changes introduced. Necessary checks should be implemented according to the agreed commissioning plan for the new systems. A special consideration shouldbe given in the case the new and old systems are expected to beoperated in parallel. The implementation will be dependent on the scope and the details of project plans.

Scope and depth of training

Commissioning tests and their instructions

Needs of a possible period of parallel operation

Interpretations of test results and other V&V evidence

Control room arrangements during parallel operation

7.8. DOCUMENTATION

The changes in the systems should be brought into the documentation as early as possible, but at the latest when the new systems are taken into operation.

- Documentation principles

  Use of modern information technology

  Ensuring that all relevant parts are updated

7.9. REFERENCES

NUREG-0700 (updateddraft), papercopy available and software in a beta version provided from BNL.

Other NUREGs

IEC standards

IEEE standards

8. CONCLUSIONS AND RECOMMENDATIONS

NATIONAL PRESENTATIONS

ACTIVITIES RELATED TO THE MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEMS IN THE UNITED STATES AT THE ELECTRIC POWER RESEARCH INSTITUTE

Joseph Naser

Electric Power Research Institute
3412 Hillview Ave
P. O. Box 10412
Palo Alto, California 94303
U.S.A.

Abstract

Most nuclear power plants in the United States are operating with their original analog I&C equipment. This equipment requires increasing maintenance efforts to sustain system performance. Decreasing availability of replacement parts and support organizations for analog technology accentuate obsolescence problems and resultant O&M cost increases. Modern technology, especially digital systems, offers improved functionality, performance, and reliability; solutions to obsolescence of equipment; reduction in O&M costs; and the potential to enhance safety. Digital I&C systems with their inherent advantages will be implemented only if reliable and cost-effective implementation and licensing acceptance is achieved and if the upgraded system supports reduced power production costs. EPRI and its member utilities are working together under the Integrated I&C Upgrade Initiative to address I&C issues.

Introduction

Operating nuclear power plants in the United States were designed 20 to 40 years ago with analog instrumentation and control (I&C) technology. Today, most plants continue to operate with much of their original I&C equipment. This equipment is approaching or exceeding its life expectancy, resulting in increasing maintenance efforts to sustain system performance. Decreasing availability of replacement parts and the accelerating deterioration of the infrastructure of manufacturers that support analog technology accentuate obsolescence problems and resultant operation and maintenance (O&M) cost increases.

Instrumentation and control systems in nuclear power plants need to be upgraded in a reliable and cost-effective manner to replace obsolete equipment, to reduce operation and maintenance costs, to improve plant performance, and to enhance safety. The major drivers for the replacement of the safety, control, and information systems in nuclear power plants are the obsolescence of the existing hardware and the need for more cost-effective power production. Digital I&C systems need to play a major role in nuclear power plants to achieve real productivity improvements needed for increased competitiveness. The procurement of replacement modules and spares under current requirements, for hardware that is no longer fully supported by the original equipment manufacturer, is costly, time consuming and, in some cases, not even possible. Competition between power producers is dictating more cost-effective power production. The increasing O&M costs to maintain many of the analog systems is counter to the needs for more cost-effective power production and improved competitiveness. The reluctance to implement new digital I&C systems to address O&M cost concerns is also counter to the needs for more cost-effective power production and improved competitiveness.

Technological improvements, particularly the availability of digital systems, offer improved functionality, performance, and reliability; solutions to obsolescence of analog equipment; reduction in O&M costs; and the potential to enhance safety. Modern digital technology holds a significant potential to improve cost-effectiveness and productivity of nuclear power plants. Digital systems have the potential for solving the utilities' current problems of increasing analog equipment obsolescence; rapidly escalating O&M costs; lost generation due to system unavailability, spurious operation, and human error; and the inability to increase plant capacity due to equipment limitations. All of these problems contribute to reduced competitiveness with other power production sources and could lead to premature plant closures.

Reliance on custom designed systems coupled with new licensing and design issues have resulted in high implementation costs when digital upgrades have been performed in nuclear power plants. There is a need for a systematic approach leading to the identification, prioritization, and implementation of I&C solutions in nuclear power plants. Viable alternatives range from extending the useful life of existing equipment to the complete replacement of systems in a cost-effective manner when vulnerability to obsolescence or the need for increased productivity so dictates.

Reliable, integrated information is a critical element for protecting the utility's capital investment and increasing availability and reliability. Integrated systems with integrated information can perform more effectively to increase productivity, to enhance safety, and to reduce O&M costs. A plant communications and computing architecture is the infrastructure needed to allow the implementation of I&C systems in an integrated manner. Current technology for distributed digital systems, plant process computers, and plant communications and computing networks support the integration of systems and information. The test for future digital I&C system upgrades will be whether they are cost beneficial to the plant and if they can offer a payback to the utility in an acceptable time period.

EPRI Nuclear Power Plant Instrumentation and Control Upgrade Program

Nuclear utilities are confronted by a growing equipment obsolescence problem which is a significant contributing factor to increasing costs for plant operation and maintenance. Plant age combined with the rapid pace of evolution of electronic technology is a significant factor in equipment obsolescence. The flexibility and performance of modern digital technology could be used as the basis for replacing obsolete modules or systems in a cost-effective manner in nuclear power plants. The realization of the benefits of digital technology is currently restrained by the relatively high cost of initial applications of new technology in a highly regulated environment. Work is needed to establish reliable and cost-effective methodologies for the design, qualification, and implementation of digital I&C systems in nuclear power plants. This work should utilize, as much as possible, relevant information and experience from other process industries where digital I&C systems are commonly used. Commercial-grade digital I&C systems have proven reliable in other process industries for applications including safety-related systems. Cost-effective approaches are needed to implement and qualify commercial-grade hardware and software for nuclear power plant applications. To address these issues and facilitate the upgrading of I&C systems in nuclear power plants, the Electric Power Research Institute (EPRI) has put together an industry-wide instrumentation and control program. This program is documented in the Integrated Instrumentation and Control Upgrade Plan (1)

The EPRI Instrumentation and Control Upgrade Program has developed a life-cycle management program for I&C systems. Life-cycle management involves the optimization of maintenance, monitoring, and capital resources to sustain safety and performance throughout the plant life. Life-cycle management for I&C systems and components additionally may require the use of digital technology, when analog equipment cannot be cost-effectively maintained or when an improvement in performance is desired. The main product of the life-cycle management program is a set of methodologies and guidelines that, as part of the utility's overall life-cycle management effort, will enable nuclear power plants to fully consider I&C cost and performance improvements including the application of digital technology. Specific examples of system specification and designs will also be developed through the application of the upgrade implementation guidelines to safety-related and non safety-related systems and system prototypes.

Planning Methodologies

Four strategic planning methodologies are being developed under the I&C Upgrade Program. The first two methodologies enable the utility to prepare an I&C life-cycle management program plan and a plant communications and computing architecture plan. The last two methodologies enable the utility to perform long-term maintenance planning and detailed upgrade evaluation for I&C systems or components.

The Life-Cycle Management Plan is a long term strategic plan for managing a power plant's I&C systems over the planning period selected by the utility. The Life-Cycle Management Plan Methodology (2) guides a designated team of utility personnel through a comparison of I&C life-cycle management strategies and through existing and planned life-cycle management program activities to identify interfaces and integration options. On the basis of this comparison, the I&C Life-Cycle Management Plan is prepared. This plan includes the identification of systems and components to be included in the program; the development of bases for upgrade or long term maintenance options; the initial cost and performance improvement estimates, prioritization for detailed upgrade evaluation, and deferred-upgrade maintenance planning; and the identification of related programs and organizational interfaces including key personnel and responsibilities. The methodology is accompanied by a workbook which contains various outlines, worksheets, and generic interview questions and topics that aid in the development of a Life-Cycle Management Plan. The document describing the methodology also explains the overall process for planning and implementing the various elements of I&C life-cycle management, and the relationship of the other EPRI planning methodologies and guidelines.

The Plant Communications and Computing Architecture Plan Methodology (3,4) provides utilities with a detailed set of instructions for preparing a Plant Communications and Computing Architecture Plan that will allow them to upgrade their I&C systems in a logical, cost-effective, and non-disruptive fashion. The Plant Communications and Computing Architecture Plan Methodology provides all of the information necessary to allow utilities to develop their strategic architecture plans in the most cost-effective manner possible. It guides a designated team of utility personnel through an assessment of the existing plant data network architecture, corporate communications architecture life-cycle management plans, and I&C life-cycle management implementation guidelines with respect to the communications architecture. On the basis of the assessment results, a Plant Communications and Computing Architecture Plan is prepared to address a characterization of the existing network architecture; a characterization of the future network architecture in terms of a network model and communication standards for connectivity and interoperability of network elements; a set of network architecture requirements regarding the physical configuration, network access, network add-on provisions, network performance monitoring, and I&C equipment communications interfacing; and a set of consistent human-machine interface requirements for I&C systems.

The Systems Maintenance Plan Methodology (5) addresses long-term maintenance planning for systems or components where the initial screening in the Life-Cycle Management Plan indicates that detailed upgrade evaluation is not justified, over the planning period, by cost and performance improvement potential. The Systems Maintenance Plan Methodology contains a process for developing a comprehensive System Maintenance Plan for each identified system. The Systems Maintenance Plan will present the most efficient approach for maintaining the operational goals and life expectancy of the system. The Systems Maintenance Plan Methodology will describe how to develop long range maintenance objectives, to baseline and analyze the existing maintenance process, to analyze failure rates, inventory practices, and obsolescence issues, and to implement maintenance related problem solving techniques.

The Upgrade Evaluation Methodology addresses (6) a detailed evaluation of I&C system and components when upgrading is indicated by the cost and performance screening in the Life-Cycle Management Plan. The Upgrade Evaluation Methodology is used to analyze each candidate system upgrade to determine if the upgrade is justified from a cost benefit perspective. The Upgrade Evaluation Methodology is used to produce an Upgrade Evaluation Report for each candidate upgrade. The Upgrade Evaluation Report describes high level system functionality, upgrade alternatives and associated cost benefit evaluations, and the recommended alternative. The upgrade evaluation process includes detailed cost and performance analysis; conceptual design options analysis; cost/benefit analysis; and upgrade recommendations. Analysis of conceptual design options includes the consideration of digital design basis changes, associated technical specification changes, and equipment selection candidates. Where an upgrade is to proceed, the Upgrade Evaluation Report is used as input to the Functional Requirements Specification.

Integrated Plant Systems

While analog equipment is becoming obsolete and more costly to maintain, the requirements on nuclear power plant personnel to improve availability, reliability, and productivity and to reduce safety challenges to the plant have increased. These personnel are working with more complex systems, and responding to increasing operational, regulatory and productivity demands. As tasks become more complex, involving large numbers of subsystem interrelationships, the potential for human errors increases. Therefore, reliable, integrated information is a critical element for protecting the utility's capital investment and increasing availability and reliability. Integrated systems with integrated information access can perform more effectively to increase productivity and enhance safety.

Traditionally systems have been implemented in a stand-alone manner which has resulted in increased O&M costs. This approach has also reduced the effectiveness, and in some cases the possibility, of new and upgraded systems. An integrated approach is essential to maximize the effectiveness of new and upgrades systems. The modern technology available for distributed digital systems, plant process computers, and plant communications and computing networks is fully capable of supporting integration of systems and information. This capability and its effectiveness has been proven in other process industries.

Productivity Enhancement Systems

Digital technology can support improved power output from nuclear power plants. The improved accuracy of digital systems and the associated reductions in uncertainties can allow the utility to increase its plant's power rating. Digital I&C systems also have the potential to support faster startups for increased power output. They can also support the faster determination of the root causes of an unanticipated trip. At the same time, they can support the faster evaluation of the performance of the equipment and systems during the unanticipated trip. Both of these will allow a faster return to power after an unanticipated trip and; therefore, allow more power to be produced by the plant.

The technological advances of the last few years have made it possible to develop sophisticated digital I&C systems, which can not only process and present information, but can also give advice to the human. With appropriately implemented digital I&C systems, humans can be augmented substantially in their capacity to monitor, process, interpret, and apply information; thus reducing errors and increasing reliability and availability. These digital I&C systems can increase productivity by eliminating routine human-power-intensive efforts such as recording, collecting, integrating, and evaluating data; and by assisting in monitoring and control activities. These systems can improve the consistency and completeness of decision-making activities by performing the role of diagnostic and decision-support advisors. Digital I&C systems can assist in reducing safety challenges to the plant by presenting more complete, integrated, and reliable information to plant staff to better cope with operating and emergency conditions. Reducing safety challenges leads directly to improved reliability and availability and hence productivity. It can also reduce the maintenance activities, which would have been required, for equipment that would have been unnecessarily challenged. Functional requirements for an environment that would support these capabilities is given in reference 7.

Advances in technological and human engineering offer the promise of helping nuclear power plant staff to reduce errors, improve productivity, and minimize the risk to plant and personnel. A plant-wide infrastructure for coordinated computerized support systems should be created to enhance these systems and to reduce their implementation costs. This infrastructure will include information communication capabilities, database and knowledge base managers, and a unified human-machine interface. This infrastructure, which is the plant communications and computing architecture discussed above, will permit incremental additions of I&C systems in all domains.

Implementation Guidelines

Design and licensing issues have inhibited access to cost and performance improvements possible with digital technology. Examples of the areas of concern for digital systems in nuclear power plants are licensing, software verification and validation (V&V), hardware qualification including electromagnetic interference compatibility and seismic, reliability, performance, separation, redundancy, fault-tolerance, common-mode failures, diversity, human-machine interfaces, and integration of systems and information through communications networks. Use of commercially available digital systems is an approach for more cost-effective implementations that is of considerable interest to the nuclear utilities. The development of good functional specifications and bid specifications for digital systems is essential to assure that the system will behave as desired. As part of the EPRI Instrumentation and Control Upgrade Program, guidelines to address many of these concerns have been developed.

The Guideline on Licensing Digital Upgrades (8) was developed to be consistent with the established 10 CFR 50.59 process. It helps utilities design and implement digital upgrades, perform 10 CFR 50.59 safety evaluations, and develop information to support licensing submittals. It suggests a failure analysis-based approach that encompasses digital-specific issues and other possible failure causes, addressing both according to their potential effects at the system level. Abnormal Conditions and Events (ACES) (9), as described in IEEE ANS 7-4.3.2-1993 "Application Criteria for Programmable Digital Computer Systems in Safety Systems of Nuclear Power Generating Stations", play an integral role in this approach.

Guidance for electromagnetic interference susceptibility testing of digital equipment (10) and a handbook for electromagnetic compatibility of digital equipment (11) have been developed. These reports integrate the current knowledge and understanding of the electromagnetic issues concerning the installation of digital equipment in power plants. They direct the utility toward practical and economical solutions for dealing with electromagnetic interference. The handbook also helps eliminate some misconceptions that questioned the reliability of digital equipment subjected to the electromagnetic environment of nuclear power plants.

Guidelines and a handbook for software V&V have been developed (12-14). These describe approaches to categorize the software systems in terms of criticality and consequences of failure. They then identify levels of V&V commiserate with these categorizations. The guidelines for V&V in reference 13 developed a set of 16 V&V guideline packages based on the system category, development phase, and software system component which is being tested. For V&V methods in the guidelines that do not have a good description elsewhere in literature on how to use them, 11 sets of procedures have also been developed. The guidelines developed were based on the attempt to identify the methods which were most successful in finding various types of defects, on the attempt to assure that the different guidelines catered to the different needs of different systems, and on the attempt to emphasize the practicality and cost-effectiveness of the methods recommended.

Experience with digital upgrades in nuclear plants has shown that there is significant room for improvement in predicting upgrade costs and in anticipating the types of technical problems that will be encountered. Often the problems can be traced to deficiencies in the specifications that govern the design, development, installation and testing activities that must be done properly to ensure success. While proper specification of requirements has always been an area where plant upgrade projects are vulnerable, the introduction of digital technology has exacerbated the situation through its need for new types of requirements with which utility engineers and operators typically have limited experience and expertise. A guideline (15) is being developed to help utilities create better requirements specifications for digital upgrades.

The use of commercially available digital equipment in nuclear safety applications continues to be a controversial issue. A process for the commercial-grade dedication of hardware was developed several years ago (16,17) and has proven very successful. The basic concepts of this process are being used as the starting point to formulate an approach for evaluation and acceptance of commercial grade microprocessor-based equipment. EPRI is working with a group of utility representatives to develop industry consensus guidelines (18). These guidelines will help the utility engineer determine what activities to undertake to establish adequate assurance that a commercial grade digital device used in a safety-related system will perform its safety function. The approach will extend the traditional commercial dedication process to include digital-specific issues, such as software configuration management, unanticipated functions and failure modes, and the software development process. Guidance will be provided to help determine appropriate technical and quality requirements and to help confirm that such requirements have been met.

Demonstration Plant Projects

The utility demonstration plants essentially are the laboratories where I&C cost and improvement options are being researched and developed. There are six utility demonstration plant projects in progress which are providing the primary inputs, as well as testing, validation and refinement activities for the methodology and guideline development under the I&C Upgrade Program.

Activities at each of the six demonstration plants may include the preparation of I&C life-cycle management plans and plant computing and control architecture plans; system screening, deferred-upgrade maintenance planning, and detailed upgrade evaluations; testing, validation, and refinement of various plant-specific methodologies and guidelines; and development of options and plans for integration of I&C cost and performance improvement activities with related life-cycle management efforts. The activities at these demonstration plants, as well as at other nuclear power plants, include implementations of new and upgraded systems.

Demonstration project activities are presently being pursued at the Tennessee Valley Authority's Browns Ferry Unit 2, Baltimore Gas and Electric Company's Calvert Cliffs Units 1 and 2, Northern States Power Company's Prairie Island Units 1 and 2, Entergy Company's Arkansas Nuclear One Units 1 and 2, Omaha Public Power District's Fort Calhoun, and Taiwan Power Company's Chinshan.

Strategic Alliance Teams Working Together to Develop Modern I&C Systems

The EPRI I&C Upgrade Program requires the cooperation of all elements of the nuclear industry to achieve full success. This is especially true under the current competitive environment which reduces the resources utilities, suppliers, government agencies, and EPRI have to develop new systems to overcome obsolescence issues and to increase productivity. In general, no single organization has the resources or is willing to take the risks of first-of-a-kind engineering for the implementation of major digital I&C systems. A five year Joint Nuclear Power Industry/DOE I&C Upgrade Program has been developed to support the development and implementation of major new systems. This industry-driven and industry-led program is built around the concept of strategic alliance teams working together to share resources, risks, and benefits to achieve a common goal. The purpose of this joint program is be to improve the competitiveness of nuclear power plants through the use of digital I&C technology.

EPRI has worked with various segments of the nuclear power industry and the United States Department of Energy (DOE) to develop the detailed description for the joint program. This description includes vision and mission statements, objectives, driving issues, strategies, road blocks, and a project screening criteria. An initial fast start project has been identified. Under this project, three diverse modern forms of I&C technologies are being studied and prototyped for application to safety systems in nuclear power plants.

The first is the use of commercially available programmable logic controllers (PLCs). PLCs with appropriate qualification programs appear to be ideally suited for a large number of nuclear power plant applications. PLCs have proven highly reliable in many industrial applications and can be used to replace aging analog and electromechanical equipment to solve the obsolescence problem, improve operation and productivity, and reduce O&M costs.

Areas that must receive careful attention when adopting commercially available PLCs include software verification and validation, hardware qualification, and regulatory acceptance. Standardized designs of PLC-based systems for safety system applications offer the opportunity for increased cost-effectiveness in implementations.

The second is the use of application specific integrated circuits (ASICs). Due to the stringent and, from past history, costly requirements for licensing digital systems for reactor protection systems, cost and regulatory risk are major concerns with licensing a digital reactor protection system. To satisfactorily insure that a microprocessor-based reactor protection system will perform as desired, be highly reliable, and not have unintended functions may be very costly. A potentially cost-effective alternative is to develop an ASIC-based reactor protection system. In this case, the ASIC is designed to perform only the needed functionality of the reactor protection system. This reduces the effort required to assure the reactor protection system's performance in protecting the plant and public. This technology can also be used for other safety and control systems.

The third is the use of dynamic safety system (DSS) technology. Most of the key safety systems in US Light Water Reactor (LWR) nuclear power plants use analog technology operating in a static mode. Although these static systems are highly reliable, they require periodic manual testing to demonstrate that they maintain functionality. These systems have become obsolete and replacement parts are either not available or available only at high cost. DSS technology operates with the insertion and processing of test signals for continuous verification of both hardware and software components. Although DSS is computer-based, the final checking of signal patterns is performed by a solid state hardware component. Thus DSS offers the benefits of computer based functionality and reliability while avoiding concerns about undetected software problems. The United Kingdom developed DSS technology has been demonstrated in advanced gas cooled reactor (AGR) plants. This project is to develop the DSS technology for LWRs.

Conclusions

The implementation and integration of digital I&C systems enhance the ability to achieve the goals of improved availability and reliability, enhanced safety, reduced operations and maintenance costs, and improved productivity in nuclear power plants. The plant communications and computing architecture provides the infrastructure which allows the integration of systems and information. The modern technology of distributed digital systems, plant process computers (both monolithic and distributed), and plant communications and computing networks have proven their ability to achieve these goals in other industries. The use of this modern, proven technology is a key contributor to improved competitiveness in nuclear power plants. EPRI has established an Integrated Instrumentation and Control Upgrade Program to support its member nuclear utilities in developing strategic plans and taking advantage of this modern technology to improve nuclear power plant competitiveness. Strategic alliances are being put together to reduce the costs and risks of first-of-a-kind development, implementation, and licensing.

References

1. "Integrated Instrumentation and Control Upgrade Plan, EPRI NP-7343 Revision 3, December 1992.

2. "I&C Life Cycle Management Plan Methodology", EPRI TR-105555, Vols. 1&2, August, 1995.

3. "Plant Communications and Computing Architecture Plan Methodology", EPRI TR-102306, Vols. 1&2, November 1993.

4. "Plant Communications and Computing Architecture Plan Methodology Revision 1", EPRI TR-104129, Vols. 1&2, December 1994.

5. "Systems Maintenance Plan Methodology", EPRI TR-106029, to be published in 1996.

6. "Upgrade Evaluation Methodology", EPRI TR-104963, to be published 1996.

7. "Plant-Wide Integrated Environment Distributed on Workstations (Plant-Window) System Functional Requirements", EPRI TR-104756, Draft Report, 1994.

8. "Guideline on Licensing Digital Upgrades", EPRI TR-102348, December 1993.

9. "Abnormal Conditions and Events Analysis for Instrumentation and Control Systems", EPRI TR-104595, Vols. 1&2, to be published in 1996.

10. "Guidelines for Electromagnetic Interference Testing in Power Plants", EPRI TR-102323, September 1994.

11. "Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants", EPRI TR-102400, Vols. 1&2, June 1994.

12. "Handbook of Verification and Validation for Digital Systems", EPRI TR-103291, Vols. 1-3, December 1994.

13. "Guidelines for the Verification and Validation of Expert System Software and Conventional Software", EPRI TR-103331, Vols. 1-8, April 1995.

14. "Verification and Validation Guidelines for High Integrity Systems", EPRI TR-103916, Vols. 1&2, December 1995.

15. "Requirements Definition Guideline", EPRI Draft Report, December 1995.

16. "Guideline for the Utilization of Commercial Grade Items in Nuclear Safety Related Applications (NCIG-07)", EPRI NP-5652, June 1988.

17. "Supplemental Guidance for the Application of EPRI NP-5652 on the Utilization of Commercial Grade Items", EPRI TR-102260, March 1994.

18. "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", EPRI Draft Report, January 1996.

EPRI/NPG

Activities Related to the Modernization of Instrumentation and Control Systems in the United States at the Electric Power Research Institute

Joseph Naser

Advisory Group Meeting on Modernization of Instrumentation and Control Systems in Nuclear Power Plants

March 25-29, 1996

Vienna, Austria

I&C Obsolescence Cost Control

I&C Mod IAEA 1

EPRI/NPG

Aging I&C Equipment

- Analog I&C equipment designed 20 to 40 years ago is in general use
- Equipment is approaching or exceeding its life expectancy
- Increasing O&M costs to maintain system performance
- Less than optimal performance
  - Power output
  - Personnel productivity

I&C Obsolescence Cost Control

I&C Mod IAEA 2

EPRI/NPG

Digital Technology

- Address equipment obsolescence issues
- Increased functionality for improved performance
- State-of-the-practice in other process industries
- Demonstrated cost and performance improvements

I&C Obsolescence Cost Control

I&C Mod IAEA 3

EPRI/NPG

Digital Technology Supports

- Increased reliability and availability
- Reduced O&M costs
- Enhanced safety
- Increased competitiveness

I&C Obsolescence Cost Control

I&C Mod IAEA 4

EPRI/NPG

US NRC Staff Positions (Early '90s)

- US NRC Staff's concerns with digital technology led to:
  - Increased scrutiny and requirements with regard to regulatory acceptance of safety-related digital retrofits
  - Publication of a draft Generic Letter on 8/14/92
    - "...the installation of digital based safety systems (1) is an unreviewed safety question, (2) will require a review by the NRC staff, and (3) cannot be performed under the 10 CFR 50.59 rule."

EPRI/NPG

Utility Reactions

- Regulatory reviews perceived as rapidly escalating and open-ended with no clear acceptance criteria
- Chilling effect on I&C replacement activities
  - postponement or cancellation of proposed improvements
  - implementation of retrofits using old, less reliable technology

National Energy Strategy Act (1992)

- Promotes competition between utilities
- Generation is very much impacted as electricity becomes a commodity
- Becoming a low-cost producer becomes a matter of economic survivability
  - Experience with profit-making process industries shows that successful performance of I&C systems is essential for economic survivability

Effects on I&C Upgrades

- Resources much tighter
- Shorter payback periods required for new systems
- Major emphasis on extending useful life of existing equipment
- Upgrades as last resort with typically "like-for-like" capabilities
- Not taking full advantage of digital technology to support improved performance and reduced costs

EPRI/NPG

EPRI I&C Program

- Working with nuclear power industry to address I&C issues
- Digital I&C technology
- Planning and implementation strategies
- Licensing stabilization
- Plant demonstrations

EPRI/NPG

Objectives

- Address obsolescence
- Reduce O&M costs, improve functionality
- Provide strategies for integrating, over a period of years, digital systems/subsystems/modules/components into operating plants
- Promote stable regulatory approach for digital technology
- Provide capability for implementing digital I&C systems
- Reduce costs and shorten the learning curve for modernizing or maintaining I&C systems

EPRI/NPG

Economic Survival

- Emphasis on cost-effective equipment decisions (maintain vs. upgrade)
  - Various levels of "upgrade"
- Greater use of off-the-shelf, rather than custom, equipment
- Use of approaches that reduce licensing and technology risks
- Use of digital I&C systems to improve productivity
- Cost sharing through joint projects and strategic alliances

I&C Obsolescence Cost Control

I&C Mod IAEA 11

EPRI/NPG

Planning Methodologies

Objective is to support I&C planning to ensure that:

- Obsolescence is addressed
- Only cost-beneficial replacements/upgrades are performed
- Replacements/Upgrades are performed in optimum order
- All upgraded systems work together; have a consistent human-machine interface; and contain the right functionality
- Information is where it is needed, when it is needed to allow operators, engineers, and management to make well-informed decisions
- The process to develop bid specifications is consistent and streamlined

I&C Obsolescence Cost Control

I&C Mod IAEA 12

EPRI/NPG

Planning Methodologies

- EPRI TR-105555 (August 1995)
  Life-Cycle Management Methodology
- EPRI TR-102306 (November 1993)
  EPRI TR-104129 (December 1994)
  Plant Communications and Computing Architecture Plan Methodology
- EPRI TR-106029 (to be published in 1996)
  System Maintenance Planning Methodology
- EPRI TR-104963 (to be published in 1996)
  System Upgrade Evaluation Methodology

I&C Mod IAEA — I&C Obsolescence Cost Control — 13

EPRI/NPG

Implementation Methodologies

- Provide support for addressing design and licensing issues
- Developed with utility working groups and/or through iteration with utility use

I&C Mod IAEA — I&C Obsolescence Cost Control — 14

Requirements Specification

- EPRI Draft Report (December 1995) Requirements Definition Guideline
- Digital systems requirements different from those previously used for analog systems

Verification and Validation

- EPRI TR-103291 (3 Volumes) (December 1994) Handbook for Verification and Validation of Digital Systems
- EPRI-TR-103331 (8 Volumes) (April 1995) Guidelines for Verification and Validation of Expert System and Conventional Software
- EPRI TR-103916 (2 Volumes) (December 1995) V&V Guideline for High Integrity Systems

EPRI/NPG

Electromagnetic Interference Compatibility

- EPRI TR-102323 (September 1994)
Guide to Electromagnetic Susceptibility Testing for Digital Safety Equipment in Nuclear Power Plants

- EPRI TR-102400 (2 Volumes) (June 1994)
Handbook for Electromagnetic Compatibility of Digital Equipment in Power Plants

I&C Obsolescence Cost Control

I&C Mod IAEA 17

EPRI/NPG

Abnormal Conditions and Events

- EPRI TR-104595 (to be published in 1996)
Abnormal Conditions and Events Analysis for Instrumentation and Control Systems

I&C Obsolescence Cost Control

I&C Mod IAEA 18

EPRI/NPG

Use of Commercially Available Digital Equipment

- EPRI Draft Report (January 1996)
  Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications

I&C Mod IAEA

I&C Obsolescence Cost Control

19

EPRI/NPG

Licensing Stabilization

- EPRI TR-102348 (December 1993)
  Guideline on Licensing Digital Upgrades
- Generic Letter published on 4/26/95
- Renewed interest in digital upgrades

I&C Mod IAEA

I&C Obsolescence Cost Control

20

EPRI/NPG

Objectives of Plant Demonstrations

- Address obsolescence
- Improve functionality, reduce O&M costs
- Integrated implementation of modern technology
- Test bed for generic methodologies, guidelines, and information (all four NSSS types)
- Support the development of a stable regulatory approach for digital upgrades
- Obtain feedback for needed R&D projects

I&C Obsolescence Cost Control

I&C Mod IAEA 21

EPRI/NPG

I&C Plant Demonstration Participants

Plants:

- Browns Ferry Unit 2
- Calvert Cliffs Units 1 & 2
- Prairie Island Units 1 & 2
- ANO Units 1 & 2
- Fort Calhoun
- Chinshan

I&C Obsolescence Cost Control

I&C Mod IAEA 22

EPRI/NPG

Some Lessons Learned

1. Importance of baseline interviews including plant personnel
2. Structured upgrade planning
   - can postpone need for upgrade capital
   - benefits from supplier participation
3. Planning and implementation methodologies
   - can be generic
   - improve with trial use
4. Need to coordinate I&C upgrade planning with
   - plant strategic plan
   - site computer network

I&C Mod IAEA — I&C Obsolescence Cost Control — 23

EPRI/NPG

Some Lessons Learned (cont'd)

5. Strategic upgrade planning
   - must accommodate known short-term upgrades
   - identifies some immediate needs
   - causes focus on maintenance effectiveness
6. Importance of network architecture planning
7. O&M cost concern is a major factor in I&C upgrades
8. Licensing cost uncertainty must be eliminated
9. Standardization and use of commercial grade equipment are needed for cost effectiveness
10. More later - stay tuned

I&C Mod IAEA — I&C Obsolescence Cost Control — 24

EPRI/NPG

Strategic Alliances

- Need for various organizations to work together to:
  - Share resources and benefits
  - Reduce first-of-a-kind development, implementation, and licensing costs and risks
  - Develop standardized approaches
  - Reduce duplication of effort
  - Increase new systems available for use

I&C Mod IAEA I&C Obsolescence Cost Control 25

EPRI/NPG

Joint Industry/DOE I&C Program

- Catalyst to resolve industry's major I&C problems
- Industry led and driven program
- Strategic alliances to reduce cost and licensing risks of first implementations
- International program
- More cost competitive generation facilities
- Increased competitiveness for suppliers

I&C Mod IAEA I&C Obsolescence Cost Control 26

Initial Projects

- Application Specific Integrated Circuits for Safety and Control Systems
- Commercially Available Programmable Logic Controllers for Safety and Control Systems
- Dynamic Safety System Technology for Reactor Protection Systems

C & I REFITS ON AGR's

R Clarke - Nuclear Electric PLC

Nuclear Electric operates four "first generation" Advanced Gas Cooled reactor stations; Hartlepool, Heysham 1, Hinkley Point B and Dungeness B. Each station has two reactor/turbine units which operate using the original data processing and control computers. At all sites, various peripheral devices such as VDUs and magnetic drums have been replaced by modern equipment. In addition, specific initiatives have been taken at each site to address obsolescence issues as follows;

Hartlepool and Heysham 1 are twin stations and their data processing and control systems are based upon the Ferranti Argus 500 system. A project has recently been completed to develop and install an "emulator" which replaces the original CPU and memory with a VME based system incorporating an Argus 700. The Argus 700 has been modified to run the original Argus 500 instruction set so that the original software can remain unchanged. The use of the VME bus also offers the opportunity to introduce an Ethernet interface card and so provide a potential future upgrade path.

Dungeness B also operates Argus 500 computers; but these have a higher clock rate than those on other stations and an emulator was not viable for these systems. Dungeness B have recently placed a contract with Q Systems to help them produce a maintenance strategy based upon the methodology developed under the auspices of EPRI.

At Hinkley Point B the computer systems are based upon the GEC M2140 and the decision has been taken to undertake a full replacement of these systems with changeover of the first unit planned for the end of 1997. The scope of the project includes:

- The replacement of the on-line computers
- Provision of off-line support facilities
- Provision of new uninterruptible power supplies
- Provision of new computer rooms and HVAC
- Provision of new plant I/O Subsystems
- Retention of the existing plant wiring and transducers
- Upgrade of the training simulator

Four major contracts have been awarded:

Ferranti Syseca Ltd	Main Contractor, computer hardware and software
Instem	Plant I/O Subsystem
Balfour Kilpatrick	UPS, HVAC and general electrical work
SWEB	Plant I/O "Break-In" wiring

Operational stations have a large investment in their computer systems and th objective is to retain this investment whilst upgrading the system.

The issues being addressed as part of the Hinkley Point B project are to:-

a) retain the existing database, alarm logic and control structure
b) minimise changes to the existing plant wiring
c) minimise the changes to the operator interface
d) minimise the need to re-train operational staff
e) provide secure changeover points without affecting plant operation
f) changeover at full power without affecting generation
g) provide facilities for future modifications and changes

These and many other issues apply to all operational plant and need to be considered when undertaking refurbishment projects.

Modernization of the Ukrainian VVER-1000 NPP Instrumentation and Control Systems

Mikhail Yastrebenetsky,
Dr. of Sc., Prof.,

Head of I&C Department
State Scientific Technical Center
of Nuclear and Radiation Safety,
Kharkov, Ukraine, 310002,
Artema str. 17
Tel/fax (038-0572)-47-17-00.

IAEA Advisory Group Meeting on "Modernization of Instrumentation and Control Systems in Nuclear Power Plants".

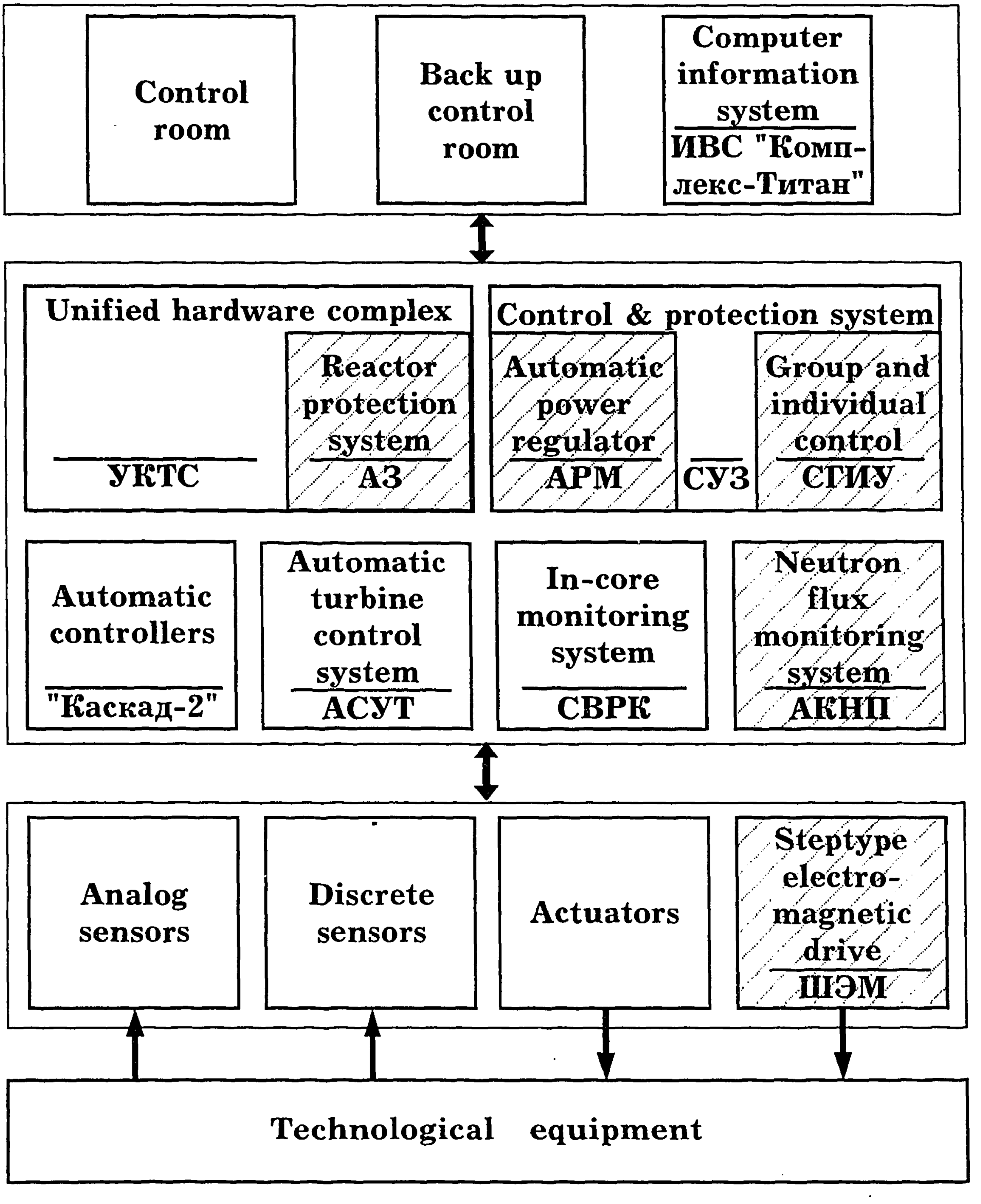
Vienna, 25-29 March 1996.

Operating Units of Ukrainian NPP's

NPP	Number of unit	Type of reactor	Date of commissioning , mm/yy
Zaporozhye	1	VVER-1000	10/84
	2	VVER-1000	07/85
	3	VVER-1000	12/86
	4	VVER-1000	12/87
	5	VVER-1000	08/89
	6	VVER-1000	10/95
Yuzhno-Ukrainsk	1	VVER-1000	12/82
	2	VVER-1000	01/85
	3	VVER-1000	09/89
Rovno	1	VVER-440	12/80
	2	VVER-440	12/81
	3	VVER-1000	12/86
	4	VVER-1000	Under construction
Hmelnitsky	1	VVER-1000	12/87
	2	VVER-1000	Under construction
Chernobyl	1	RBMK-1000	09/77
	3	RBMK-1000	11/81

Common number of NPP Units	-	15
NPP's electricity production share (1995)	-	36,7 %
Number of VVER-1000 units	-	11
Installed VVER -1000 power capacity share (1995)	-	79,7 %

Subsystems of operating VVER-1000 I&C



Reasons for VVER-1000 I&C Modernization

I&C isn't whole system, it's set of subsystems:
- different element bases;
- different technical realisation for decision of same tasks;
- different construction;
- difficulties with interface between heterogeneons components.

I&C is very bulky (near 700 cabinets only of УКТС).

Absence of:
- high (general plant) level cooperated with unit level;
- system for informational personell support.

Lifetime of many instruments ended or near to the end.

Problems with spare parts after USSR desintegration.

Non-complete accordance to safety requirements:
- absence of diagnostics in hardware and software ;
- discrepancy to seismic requirements ;
- low fire resistance .

Big expenses of labour for I&C operation.

Main Actions in USSR for VVER-1000 I&C Modernization

Year	Name of action	Head of action	Main designer
1982	Issue of " Main technical reguirements to new NPP I&C generation"	---	Teploelectro-proekt
1983	Issue of set of 8 USSR Standards "Apparatus for NPP I&C" acted to VVER-1000 I&C with distributing structure	V.Zonov	Teploelectro-proekt
1983	Issue of "Technical task to elaboration of preproduction prototype of I&C of NPP VVER-1000"	V.Gritskov	Central Institute of Complex Auto-matization (CNIIKA)
1986	Issue of "Common technical requirements to NPP VVER-1000 I&C"	G.Shasharin	Ministry of Power Generation
1987	Issue of Recommended document "NPP I&C. Reliability. Common requirements"	M.Yastrebe-netsky	Central Institute of Complex Auto-matization (CNIIKA)
1987-1991	Elaboration preproduction I&C for NPP VVER-1000 (for new Tatarskaya NPP or new Bashkirskaya NPP and for modernization of operating NPP) : - issue of technical task - designing - elaboration of new instruments	I.Prangishvili	Institute of Problems of Control (IPU)

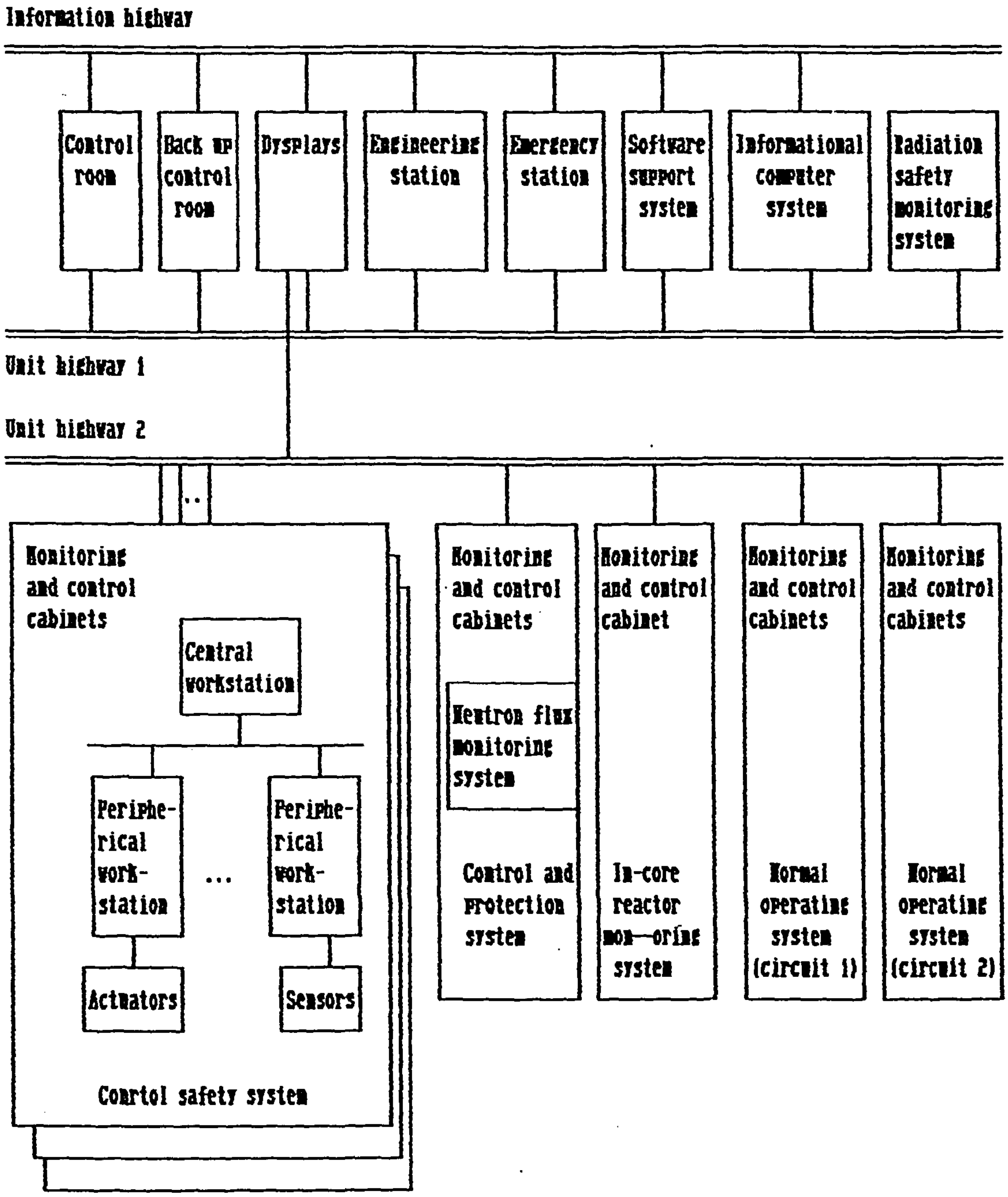
Present VVER-1000 I&C Modernization

Manufacturer	Old system Name	Old system Type	New system	NPP unit	Present state
Khartron (Ukraine)	I&C as whole			Z-3 Z-4 Z-5 H-1 R-3 Y-1 Y-2 Y-3	1-st phase of design are finished. 2-nd phase of design is near to the end
				Z-3	Automatic power regulator and seismic protection equipment are being tested
Westron (USA - Ukraine)	Unit computer information system	Complex Titan 2	WDPF-II	Y-1	Apparatus is prepared for mounting of pilot system
Siemens (Germany)	Reactor protection system	UKTS	Teleperm-XS	R-4	The most part of documentation is prepared. Type testing is fulfilled in Germany
Skoda-YaM (Czeck Republic)	Steptype electromagnetic drive	ShEM	ShEM-M	Y-1	Resurs tests are finished in Skoda
Skoda-Controls (Czeck Republic)	Group and individual control system	SGIU	SGIU	Y-1	V&V of software are being spent in Skoda

Schedule of NPP VVER-1000 I&C Modernization

Name of subsystem	Manufacturer	Year 1997	1998	1999	...	2003
Steptype electromagnetic drive	Skoda	Z-3	Z-4			
	Gidropress		H-1		Z-5	
Group and individual control system	Khartron	Z-3	Z-4 H-1		Z-5	
Reactor protection system	Khartron	Z-3	H-1	R-3 Y-3	Z-4 Z-5	
Automatic power regulator	Khartron	R-3 Z-3	H-1	Y-3	Z-4 Z-5	
Neutron flux monitoring system	SNIIP	Z-3	H-1	Y-3		
	Khartron				Z-4 Z-5	
Safety radiation control system	Khartron		Z-1 H-1 Y-1	Y-2 R-3	Y-3 Z-4 Z-5	
Unit informational computer system (1 phase)	Khartron, Impuls	Z-3	H-1	Y-3 R-3	Z-4 Z-5	
Unit informational computer system (2 phase)	Khartron, Impuls		Z-3	H-1	Z-4 Z-5 Y-3 R-3	
Unit informational computer system (3 phase)	Khartron, Impuls			Z-3	Z-4 H-1 Y-3 R-3	Z-5
Control safety system-1	Khartron		Z-3		H-1 Z-4 R-3	Z-5
	Fiolent		Y-1	Y-2	Y-3	
Control safety system-2	Khartron	Z-1		H-1 Y-3 R-3	Z-4 Z-5	
	Fiolent			Y-1	Y-2	
Control safety system-3	Khartron			Z-3	R-1 H-1 Z-4	Z-5
	Fiolent				Y-1 Y-2	

SUBSYSTEMS OF I&C KHARTRON



Main pecularities of I&C Khartron for modernization VVER-1000

* Distributed hierachical system

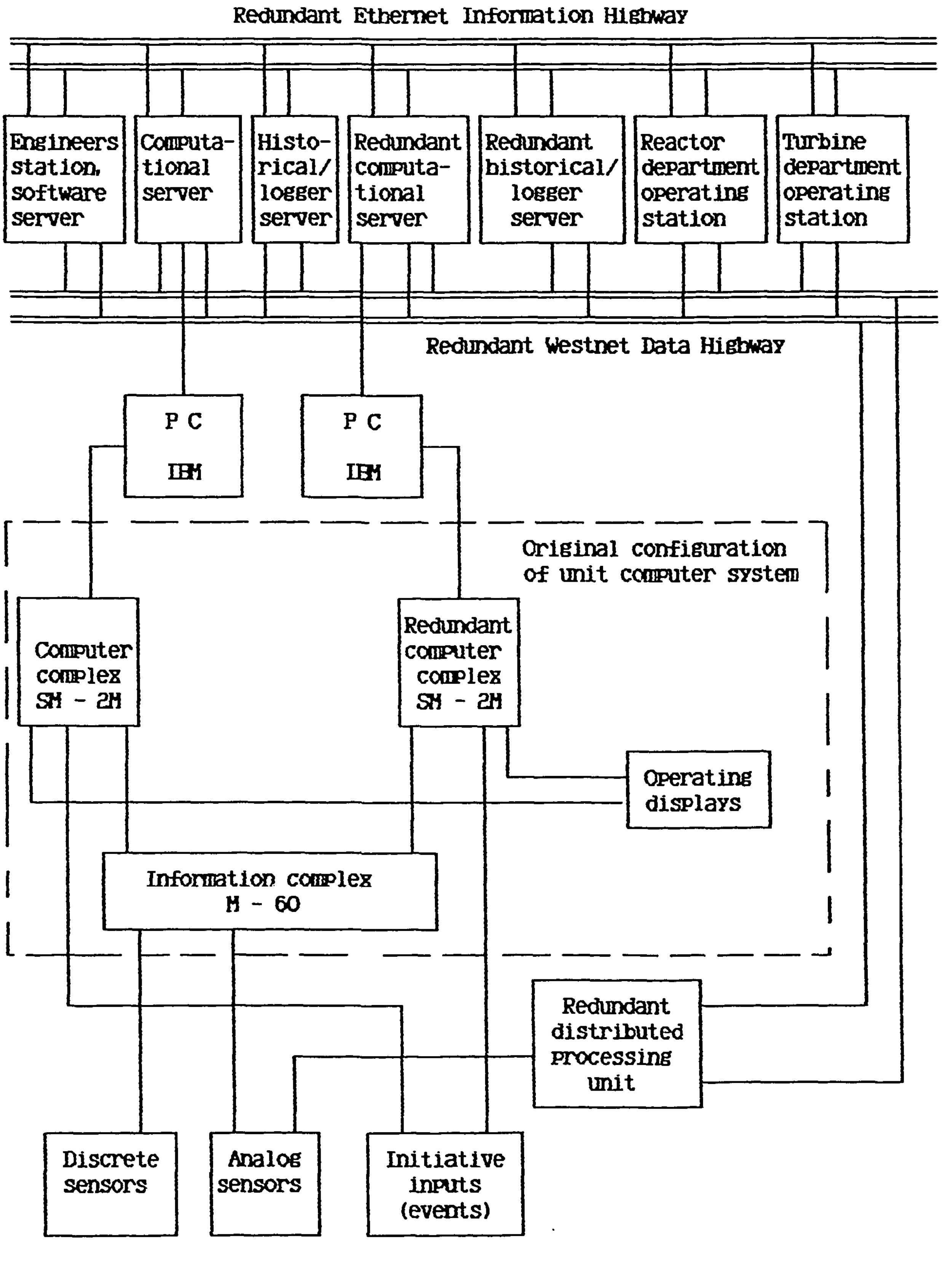
* Wide using of modern computer technique:
  - presence of high productive working stations;
  - presence of local computer nets and unit buses;
  - using of optical-fibre wires for local computer nets;
  - displays with big resolution;
  - high level of diagnostic;
  - possibility of control by display keys;
  - possibility to replace of failured elements without stop of system;
  - ope ning to join with additional instruments and to implement step-by-step.

* I&C consists from programm-technical complexes, what are built similary from different functions.

* Presense of:
  - information system for technical support of personell;
  - possibility of interface as with new foreign technique ("Siemens", "Westinghouse", "Skoda", etc), as with operating system (УКТС,ИВС).

* Saving of operating in NPP:
  - sensors;
  - actuators;
  - cables;
  - parts of control room equipment.

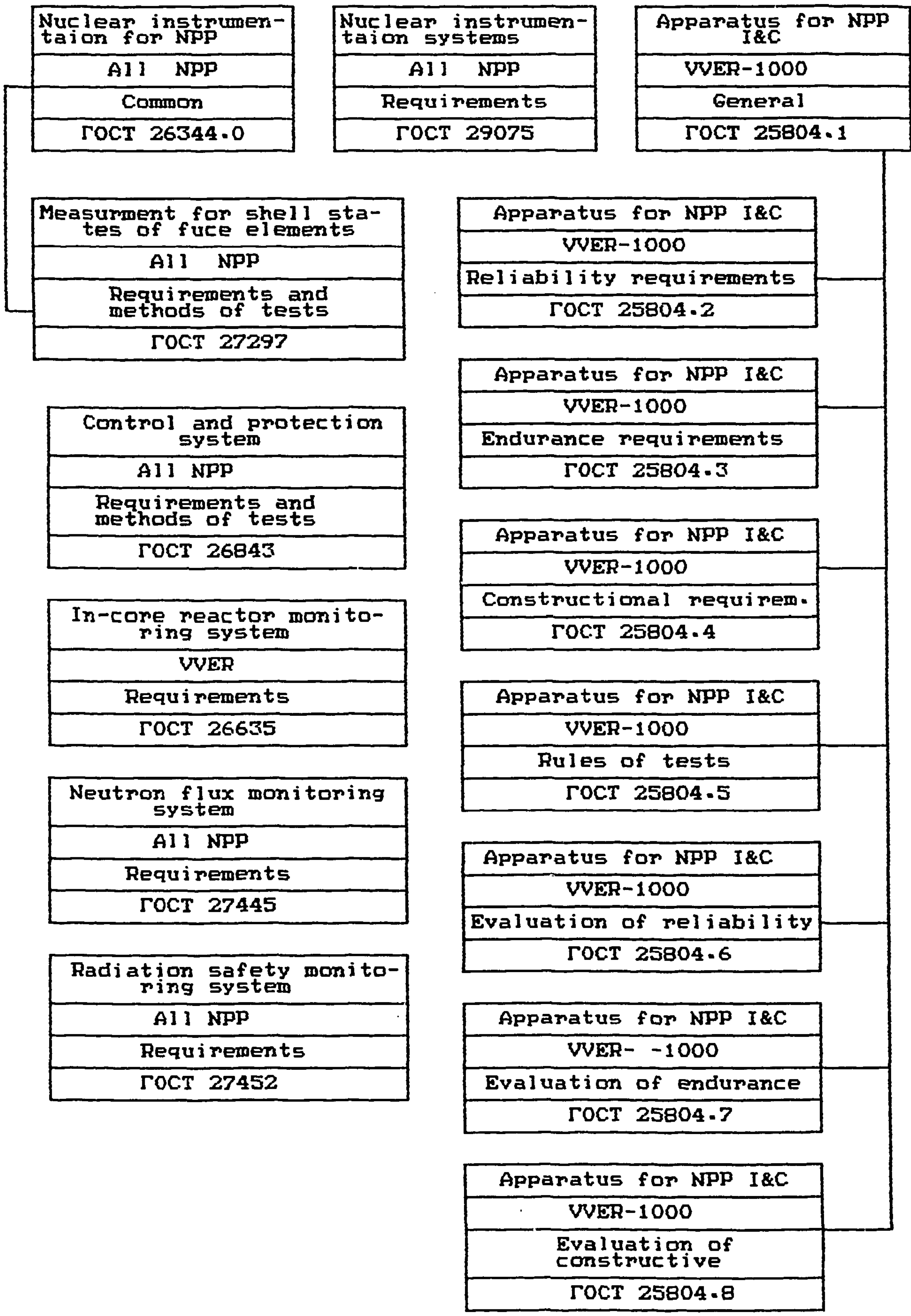
MODERNIZATION OF YUZHNO-UKRAINSK UNIT COMPUTER SYSTEM (PHASE 1)



Standards, Guides and Rulers what are used for Ukrainian NPP's I&C Modernization

USSR Safety Guides and Rulers what are acted to different NPP equipment, including I&C	Ukrainian Regulatory Autority confirmed this list for Ukrainian NPP's (Decision N1 from 4.01.1992)
USSR common technical Standards what are acted to NPP I&C USSR Standards what are acted to I&C in different branches of industry, including NPP USSR Standards what directly are acted to NPP I&C	USSR Standards acted in the Ukraine as International Standards
Ukrainian common technical Standards what are acted to NPP I&C	Ukrainian Standards began to act from 1995 - 1996.

USSR STANDARDS WHAT DIRECTLY ARE ACTED TO NPP VVER-1000 I&C.



Requirements to Expertise of modernized I&C

1. Expertise - continuous process, what have to include all stages of system creation:
   - elaboration of principles of safety assessment (preliminary safety analysis report);
   - design;
   - testing of hardware and software;
   - elaboration of final safety analysis reports;
   - testing on NPP area etc.

2. Expertise have to include analysis system as whole, hardware and software.

3. If foreign manufacturer realise modernization, necessary steps in expertise are:
   - analysis of coordination between Ukrainian standards and standards of country-manufacturer;
   - consideration of results of tests and V&V, what manufacturer and independent company fulfilled by own standards;
   - consideration of results of this system analysis, what were made by Regulatory Autority of country-manufacturer.

4. Expertise have to include analysis interface between modernized and remained parts of I&C.

14

Stages of licensing and list of documents for expertise in the time of modernization

Stage of licensing	Name of document for expertise
Admission on change of design	Technical decision of NPP about modernization Technical task Preliminary safety analysis report (conception, topical report)
Admission on mounting and setgoing	Design (some sections) Quality assurance programm Specification of software and hardware Methodic and results of tests , what have made by manufacturer Methodics and results of V&V Programms of mounting, setgoing and implementation
Admission on operation	Final safety analysis report Methodics and results of test in NPP condition

Structure of the IAEA Technical Document "Modernization of I&C in NPP's" (Proposal)

1. Objective
   1.1. Major goals of I&C modernization
   1.2. Scope and structure of the report
   1.3. Purpose of the report

2. Common principles of modernization
   2.1. Main reasons of modernization
   2.2. Technical posibilities for modernization
   2.3.* Peculiarities of modernization (replacement only part of system; interface with remaining components; short time for working into NPP, etc).
   2.4.* Choice of the prioritites
   2.5. International and national standards

3. Stages of modernization
   3.1. Technical requirements
   3.2. Designing
   3.3. Hardware qualification and testing
   3.4. Software V&V
   3.5. Vendors system testing
   3.6. Erection, setgoing, testing into NPP
   3.7. Personell training

4.* Comparation techical performance of modern and old systems
   4.1. Reliability
      4.1.1. Failures criterions
      4.1.2. Reliability measures
      4.1.3. Assumption for the evaluation
      4.1.4. Initial data
      4.1.5. Methodics for evaluation
   4.2. Accuracy
   4.3. Speed
   ....

5. Regulatory autorities actions
   5.1. Common principles
   5.2. Stages of licensing
   5.3. Requirements to the documents

6. Modernization of typical systems
   6.1. Reactor protection systems
   6.2. Reactor control and limitation systems
   6.3. Incore instrumentation systems
   6.4. Unit computer information systems
   ....

7. Representative systems

8. Conclusions

MAIN TRENDS OF ACTIVITY ON MODERNIZATION OF I&C SYSTEMS AT NPPs IN RUSSIA.

A.B.Pobedonostsev
OKB Mechanical engineering
Nizhny Novgorod, Russian Federation

A.G.Chudin
Russian Federation Ministry for Atomic Energy
Moscow, Russian Federation

INTRODUCTION

There are more than 20 nuclear power reactors in operation in Russia, which had operated over 10 years. (see table) [5.6]. Running time of I&C systems of these NPPs is ordered as a rule about 30 years, but lifetime of individual parts of I&C systems is limited by 10-15 years.

I&C systems was designed in the 60-70-th years in accordance with existed regulation `and scheme-technical decisions. Moral and physical obsolence of these I&C systems require the reconstruction of existing systems. Therefore the problem of replacement of I&C systems apparature and equipment which lifetime has been exhausted is very actual. At the same time there are some reasons that don't allow to perform equipment replacement to similar one but require to modernize I&C systems at NPP.

REASONS FOR I&C SYSTEMS MODERNIZATION

There are some reasons for I&C systems modernization at NPP. One of them is equipment and apparature obsolence of I&C systems. In most cases it is not possible to perform equipment replacement to similar one. It is conditioned by the next reasons:

* qualitative changes was happend in the field of I&C systems. Analogue equipment had been replaced by apparature on the base of microprocessors and computers;
* cell base and hardware had been produced with the usage of this cell base became moral obsolete;
* in many cases the serial of complecting components has already been stopped to be produced by Manufacturer that begin to produce modern equipment.

Next reason to make modernization of I&C systems is the changes of regulations, including more hard requirements related to guality, safety and reliability. Codes OPB-88 and PBY RU AS-89 contain the new requirements to NPP I&C systems such as:

* requirement of diagnostic performance related not only to technological equipment but to I&C systems hardware and software too;
* requirement to operator information support provision;
* requirement to independence and redundancy of protection system channels and etc.

One more reason for I&C systems modernization is the experience of I&C systems operation at running NPPs and the requirements and proposals of NPP staff for operational index and consumers properties improvement of I&C systems.

GENERAL APPROACH TO MODERNIZATION ACTIVITY

The foundation of I&C system modernization at NPP is the complex approach to modernization.
Complex approach to I&C systems modernization concerning to projects for new NPPs consist in taking into account the ability for I&C systems modernization in future.

I&C systems design should be satisfied the next main requirements that promote the I&C systems modernization in future:

* I&C systems structure should be decentralized and opened to increasing of structural units number;
* I&C systems hardware should be realized on the modern cell base and has module-unit construction;
* standard (including international) interfaces should be applicated to connect separate components of I&C systems with each other as well as individual units and modules into apparature cabinets;
* I&C systems hardware should be designed with taking into account it's ability to increase the number of processing input/ontput signals without additional hardware changes including absence of structure-hardware decisions changes.

Complex approach to modernization of running NPP consist in development of longtime shedule of I&C systems modernization for each NPP power unit. This shedule should provide step by step modernization activity.

Modernization should be related not only to hardware but to functional part of I&C systems proiect as well. For example, during process of reactor control protection system (CPS) modernization it is necessary to analyze accordance of CPS design to regulation requirements (single failure criteria, common reason failures). It could require to add protection signal list and to change the measurement channel schems and etc.

Modernization of running regulation systems, including the introduction of new loops, reguires calculated substantiation of this one. When they modernize systems that are realized on the base of computer technic, for example, in-core monitoring system, it is necessary to modernize hardware as well as software and mathematic. [7].

For modernization process it is necessary to take into account the human factor influence. At the earliest stage of requirements development to system modernization appropriating NPP personnel should take part in the development of this requirements and agree the final version of requirements.

Sometimes the modernization is related to changing of operator interface, in this case the operator interface changes should be discussed and agreed by NPP operators.

NPP operators training for familarization gaining with modernized man-machine interface should precede the infroduction of modernized inferface at running NPP.

It seems expedient NPP maintenance personnel to take part in modernized hardware assembling and factory acceptance testing at the I&C system factory.

CURRENT PRACTICE OF OPERATING NPP MODERNIZATION

Modernization of I&C systems at operating NPP are performed in Russia now.

Modernization usually consist in individual system hardware replacement or addition to existing I&C systems project of new additional systems. Such activity is not intended for largescale modernization and lead in the first turn to autority requirements accordance and safety and effectivity improvement of operation.

Great efforts are undertaken in the field of operator support system (OSS) development and implementation.

The working group composed by the specialists of several russian organizations on the request of Concern Rosenergoatom developed the concept of an information support system for operational personnel of operating NPP.

The main objective of an information support system is to help an operator in the main control room to evaluate a safety status of power unit.

The first priority functions of operator support that intended for the implemantation at the running NNPs are a critical safety functions display, intellectual annunciation system, early fault detection and diagnosis. Information support system of operator can be implemented as a separate computer module integrated in operating process control system of a power unit. The work of the implememtation of an information support system is being carried out in the framework of modernization of operating process control system. It is supposed to introduce OSS at running NPP by sereral stages, step-by-step. The implementation of OSS should be performed on the basis of the analysis for every power unit of available information system, personnel activity and determination of a set of the OSS functions to be developed, of these functions realization methods and their integration ways with existing running information system [1].

Development of OSS are fulfilled by many russian organizations. Such developments are performed not only for I&C systems modernization but for new NPP projects as well. For example, the OSS design for Voronezh nuclear heating plant are developed by OKB Mechanical engineering; there is operating model of OSS that is realized on the base of PC. Such experience of russian organizations on OSS development creates the foundation for information systems modernization of operating NPPs.

One of the directions in the field of OSS is the development of Safety Parameters Display Systems (SPDS).

The pilot program for SPDS design and implementation at Balakovo NPP (PWR) and Lenningrad NPP (RBMK) are developed in Russia.

The russian organizations and american firm (Westinghouse) take part in SPDS development in the framework of this program.

Westinghouse-firm has successful experience in the area of development and implementation of SPDS systems in USA [2].

Activity for diagnostic system development and implementation for NPP technological equipment and processes diagnosis are performed in Russia.

Diagnostic systems are realized as hardware-software sets for vibration monitoring, equipment lifetime assessment, leakage montoring, loose parts monitoring.

These systems are implemented as local autonomous information systems. Data of technologial process are received by diagnostic system from existing information system and it's own additional sensors.

The diagnostics systems begin to be implemented at NPP. At the beginning of 1993 the expert on-line diagnosis system was put into trival operation at Leningrad - 1 NPP. At present this system is used to diagnose 11 technological subsystems. The diagnosis system provide:

* to monitor the process state of the diagnosed technological subsystems at the macrolevel (healthy-unhealthy);
* to determine the type of malfunction, its cause and location, if there is any trouble;
* to represent on the display screen digital and graphic data on any subsystem being diagnosed;
* to record the diagnosis result in the archive on the user request.

The foundation of this diagnosis system is the software program block that is running in the operating system MS DOS for IBM PC and compatible computers [3].

Moscow science and research centre SNIIP developed new modern hardware complex for VVER-440 reactor control and protection system (AKNP-7, AZTP, ALOS, AOP and AKNP-7-02 for VVER-1000) that is conformed to modern normative requirements and is performed neutron flux monitoring, logistic process of data and protection signal formation, representation and recording of information. This modern control and protection system hardware are installed and operate at South-Ukraine NPP and Rovno NPP in the Ukraine as well as at Kola NPP-1.2 and Novo-Voronezh NPP in Russia.

Such activity related to reactor control & protection system (CPS) modernization nad been performed for the 3th power unit of Beloyarskay NPP (fast type reactor) by NPO, "Avtomatika" (Omsk, Russia).

Equipment for control rods motors control concerning VVER-type operating reactors are modernizing as well.

Modernization generally is performed at the level of individual units and modules and is related to cell base replacement and sometimes scheme decisions improvements [7].

Russian organizations take part in CPS systems' modernization for Ukraine NPPs as well. It is supposed for South-Ukraine NPP several CPS subsystem (ROM, ARM, control of control rods motors) to realize on the base of microprocessers.

The putting of these systems into operation should be possible after the software licencing as well as hardware [7].

It is necessary to note that the level of production technology of reactor control & protection systems in Russia does not always correspond to the level of the system development. This one is the main reason why foreing firms co-operate in a number of CPS designs.

The successful experience of russian and french firm collaboration has been already presented while development of functional part of CPS reconstruction project for Kola NPP-3 and 4 [4].

Collaboration of russian organizations with foreing firms has some features. Project of I&C systems modernization always is designed by russian organization that is specialized in the field of I&C systems for NPPs development. Russian design organization defines the modernization strategy, key technical decisions, performes safety provision substantiation and is responsible for correctness of design. Such approach is conditioned by russian organizations large experience and knowledge in the field of NPP technological processes, russian standards and regulations related to I&C systems for NPPs, current practice of I&C systems development and operation in Russia. Collaboration of russian organizations with foreing firms consist in combined development of metodology for individual tasks solving (for example, SPDS). Russian organizations perform in this case the analisys of methods for problem solving and their adaptation for russian conditions. Sometimes it is supposed to use foreing hardware for I&C systems modernization. In this case it is expedient to involve foreing firms that have the experience in such technic application in the works on modernization. Collaboration provides to chouse the optimal technical decisions and to eliminate design errors related to foreing hardware application.

CONCLUSION

* It is supposed to modernize I&C systems of NPP on the base of complex approach. The longtime shedule of I&C systems modernization for each NPP power unit should be developed. Such shedule should provide stage-by-stage modernization.

Modernization should be related not only to hardware but to functional part of I&C system project as well.

* Current practice of information system modernization usually consist in adding to existing I&C systems new systems (OSS, SPDS, diagnostic systems) that are realized as local systems connected with existing I&C systems for process information acquisition . It is supposed to introduce new systems into operation gradually and increase their functionability step-by-step.

* Control system modernization is performed in the first turn for safety important systems including reactor control and protection systems.

* Project of I&C systems modernization for russian NPPs is developed by russian organizations that are specialized in the field of I&C systems for NPPs development. The main reason for such approach is conditioned by next circumstance. Russian design organizations have large experience and knowledges in the field of NPP' technological processes, russian standards and regulations related to I&C systems for NPPs, current practice of I&C systems development and operation in Russia. When it is expedient from economical and technical point of view foreing firms together with russian organizations take part in the works on I&C systems modernization.

REFERENCES

1. V.G.Dounaev, V.V.Golovanov. The concept of an information support system for operational personnel of operating nuclear power plants. Operator support systems in nuclear power plants. IAEA, Vienna, 1994, IAEA-TECDOC-762.
2. J.Boucau, S.Smirnov, A.I.Gorelov and all. The SPDS as a tool to improve post-accident strategy on VVER and RBMK reactors. Operator support systems in nuclear power plants. IAEA, Vienna, 1994, IAEA-TECDOC-762.
3. E.O.Adamov, O.N.Glazov, A.P.Eperin, N.V.Strepetov. The design concept of an on-line diagnosis system of a sophisticated technological object: the shell of expert diagnosis system "Dasha". Operator support systems in nuclear power plants. IAEA, Vienna, 1994, IAEA-TECDOC-762.
4. G.I.Biryukov, N.P.Konoplev, I.V.Pogorelov. Reconstraction of control and protection systems of VVER-type reactors in Russia. Instrumentation and control of WWER type nuclear power plants. Proceedings of the IAEA meeting, Prague. Czech Republic, 27-29 September 1994, Nuclear Research Institute REZplc, 1995.
5. Nuclear Power Reactors in the World. Reference Data Series №2. IAEA, Vienna, 1992.
6. Instrumentation and control of WWER type nuclear power plants. Proceedings of the IAEA meeting, Prague, Czech Republic. 27-29 September 1994, Nuclear Research Institute REZplc,1995.
7. D.A.Anufriev, A.M.Afrov. N.P.Konoplev, I.V.Pogorelov. Main trends of VVER-type RP control, monitoring and protection systems modernization. OKB "Gidropress", 1996.

OPERATING NUCLEAR POWER PLANTS IN RUSSIAN FEDERATION

Table

SITE	REACTOR TYPE	UNIT NUMBER	COMMERCIAL OPERATION START
BALAKOVO	VVER	1	1986
		2	1988
		3	1989
		4	1993
BELOYARSKY	BN-600	3	1981
BILIBINO	RBMK	1	1974
		2	1975
		3	1976
		4	1977
KALININ	VVER	1	1985
		2	1987
KOLA	VVER	1	1973
		2	1975
		3	1982
		4	1984
KURSK	RBMK	1	1977
		2	1979
		3	1984
		4	1986
LENINGRAD	RBMK	1	1974
		2	1976
		3	1980
		4	1981
NOVOVORONEZH	VVER	3	1972
		4	1973
		5	1981
SMOLENSK	RBMK	1	1983
		2	1985

XA9642720

Replacement of I&C Systems in WWER-1000 of Kozloduy NPP

V. Miliovsky, Committee on the Use of Atomic Energy for Peaceful Purposes, Bulgaria

Abstract

Significant improvements in the Control and Instrumentation Systems are proposed by the Modernization Programme of Kozloduy units 5 and 6. The approach in the development of the modernization programme is given in this paper. The proposed improvements in I&C are described and a correspondence with the recommendations of the IAEA draft report "Ranking of Safety Issues for WWER-1000 Model 320 NPPs" WWER-SC-104 is evaluated.

1. Introduction

The Kozloduy units 5 and 6 were put in commercial operation on 20 September 1988 and 30 December 1993, respectively. Both units have the same design elaborated in accordance with general rule OPB-73 and with norms/standards in force at that time. The design of the plant does not entirely comply with the current safety standards and the utility decided to implement modernization programme to upgrade the plant. In 1993 discussions were initiated by the Bulgarian utility to carry out a modernization programme in order to obtain funding from the banks. This was the reason why the utility with the engineering assistance of the local engineering organizations, ENERGOPROEKT and RISK ENGINEERING LTD, has decided to introduce additional improvements that are consistent with the present version of the Kozloduy 5/6 modernization programme.

The basis of assessment of the initial safety level of Kozloduy 5/6 were the safety analysis of the IAEA OSART and ASSET missions conducted at Kozloduy in 1991 and 1994 added with IAEA Safety Review Missions done on other WWER-1000 units, evaluations made by IPSN and GRS (French and German nuclear safety expert organizations so called RISKAUDIT) and recommendations made by the IAEA and the Main Designer in the draft report WWER-SC-104.

Based on this approach the safety reassessment and availability analysis of Kozloduy 5/6 includes three different stages:

- the first is concerned with the identification and prioritization of weaknesses in relation to safety and availability while making sure of the systematic scope of the reassessment;
- the second is concerned with the appraisal of how to resolve each safety-related and availability problems raised by the weaknesses on the basis of feasibility studies of corrective actions complying with safety principles and of availability-benefits evaluation whenever possible;
- the third is for implementation of corrective actions, according to a schedule which takes into account priorities as well as the studies, the implementation means and the NPP operating schedule.

Experience feedback of similar PWR unit operation (WANO - Users group), consideration of international programs led by IAEA or the EEC (PHARE and TACIS programs) may lead to propositions for new safety improvements.

In terms of reference rulings, not only for improvement studies but also for assessment of the final safety level, one could mention:

- the fundamental safety rules of the Bulgarian Regulatory Authority;
- the internationally recognized IAEA documents such as "Basic Safety Principles for Nuclear Power Plants" (INSAG-3 publication) and the "IAEA Safety Guides - 50 - SG";
- the French rules related to design or construction (French RCC);
- some of the American NRC Regulatory Guides like the NUREG 1.70 for the drawing up of the safety report.

2. General Safety of units 5/6

The initial WWER 1000/V-320 design dates back to the mid of the 1970's, 8 V-320 reactors are either in operation or near to completion in the former USSR and Eastern European countries. The Kozloduy reactors are among the most recent put in operation and they get a benefit from all implemented upgradings.

The Kozloduy units 5/6 design is, in general, consistent with standard international practices for safety systems and safety related systems. The basic safety concept of defence-in-depth is realized by fundamental principles including the use of redundancy, diversity, physical separation, fail safe design and a pressure-resistant confinement.

During construction, commissioning and operation of units 5/6 more than 1600 changes to hardware and to documentation had been implemented with the aim of improving the reliability and safety of plant operation. The most important safety improvements are design changes in steam generators, emergency core cooling system and control rod position indication system. The main improvements in the area of analysis and documentation are amendments in safety analysis reports reflecting start-up and operational experience, finalization of PSA (level 1) and a fully computerized system for reporting and recording of events. The most significant modifications of I&C are:

- updating of SG "level" protections;
- replacement of motor - actuated SG feedwater control valves with pneumoactuated ones;
- application of accelerated reactor power reduction;
- application of gas fire - fighting in electronic circuitry cabinets;
- applications of new three channel reactimeters;
- installation of an automatic radiation monitoring system in 3 km area around the site.

A smaller number of shortcomings identified at Kozloduy 5/6 include findings known also from operation of other WWER-1000 NPPs. The majority o shortcomings identified at Kozloduy 5/6 are mainly related to those topics which reflect the evolution in safety standards within the last two decades.

The evaluation of the impact of all issues on plant safety considers thei influence on the fulfilment of the main safety functions and the underlying overal plant defence-in-depth. In addition, the existing design issues in some areas are considered separately because they affect nearly every system or equipment and thus influence the capability of the main safety functions.

Because of importance of I&C systems on the fulfilment of the main safety functions their issues are considered separately.

3. Shortcomings of existing I&C systems

I&C systems important to safety covers those for safety systems and those for safety-related systems. The I&C safety classification should be completed and approved for both cases and should be carried out into the procedures for maintenance of the I&C important to safety. The qualification list of I&C equipment important to safety should be reviewed for all design conditions.

The qualification of I&C equipment for LOCA conditions cannot be checked, since neither specifications regarding test procedures and sequences nor test reports are available at the site.

I&C equipment has a design lifetime of ten years. Failure analysis discovered relay contact oxidation, low insulation resistance of wiring and terminals, etc. Without major efforts in maintenance the I&C reliability may has a serious impact to the safety.

The accident monitoring instrumentation in the control rooms is not properly designed. The information needed during and after an accident is distributed throughout the control room and is not organised in a way that would support rapid and accurate diagnosis of an accident condition. Reactor pressure vessel level indication is currently not provided and the level could be estimated only by indirect means. The I&C for monitoring and diagnosing state of systems important to safety needs to be improved. The original design does not provide for adequate diagnostic systems to monitor the reactor coolant pressure boundary integrity and the mechanical equipment.

The chemical monitoring system currently used is of the 1970's era. Assurance of reliable and accurate results requires a lot of maintenance efforts. An accurate and preferably on-line chemical monitoring system is important to give the operator a possibility for in time response to deviations in primary coolant water-chemical conditions.

The current in-core monitoring and control system can detect and manually suppress xenon oscillations in base load operation and infrequent power changes. However, if the plant will be used in load follow mode, the system needs to be improved.

Recent international practice is to design an NPP with a room (technical support centre) where current plant data and status is compiled to display to technical experts who will support the operators during the management of an accident.

4. *Proposed measures in the modernization programme for I&C systems.*

I&C Reliability

The proposed measure are as follows:

- Improvement of ECCS accumulator isolation. At present, a spurious signall or loss of power to one sensor can fail the accumulator isolation function of all four accumulators;
- Classification of the equipment according to its importance for safety in accordance with OPB-88 and PNAEG 007-09-89 and evaluation of deviations from NUSS;
- Collection and evaluation of existing documentation concerning equipment qualification and development and implementation of a programme for additional qualification;
- Verification of earthquake resistance of main control room recorders and mounting or replacement;
- Determination of service life of cables, including development of diagnosis, algorithms and software;
- Replacement of Sapphire dP sensors due to susceptibility of the rupturing of their membrane;
- Replacement of actuator limit switches using 220 AC to avoid personnel and equipment hazard;
- Replacement of TITAN computer with a more modern system with higher capacity in speed and memory;
- Development of a Failure Mode and Effects Analysis (FMEA) for the control and safety I&C. This should include both the effects of shorts or voltage disturbances on the protection system and possible failure modes of the control systems;
- Development of reliability - based maintenance methods;
- Development of maintenance instructions in accordance with IAEA recommendations;
- Development of "Rest Life Time" evaluation model.

The Kozloduy NPP strategy for long term I&C upgrades in that one must determine weak points and keep them working and then determine priority and schedule for evolution and technology. The replacement listed above (other than the TITAN replacement) are immediate requirements to replace unsatisfactory components. Replacement of the TITAN computer is the biggest issue. Presently, it has been under study for about one year. There are many organisational interfaces within the plant and off-site. The computer must be compatible with existing systems which must connect with it, and must support future I&C upgrades.

The Failure Mode and Effects Analysis should be co-ordinated with the deterministic safety analysis. Generally it is acceptable in western practice that control I&C failures cause a plant transient requiring protection, provided that:

- the frequency of failure is low such that undesirable thermal transients and challenges to the protection system are minimised, and
- the transient caused by the failure is conservatively addressed in the safet analysis and shown to have acceptable consequences.

The above series of actions are all based on feedback from experience, regarding inadequate quality or reliability or function. They will all provide improvements in plant safety as well as plant availability and meet the intend of the IAEA recommendations.

Safety System Actuation Design.

The reliability of the current design approach has already been assessed and compared against a fail-safe design, where actuation takes place at loss of power.

Engineering safety features actuation on loss of instrument power is not an absolute rule in western countries. The risk of spurious actuation must be balanced against the risk of failure to actuate on demand. For example, it is common practice in the US to use "energise-to-actuate" for confinement spray. On Temelin, loss of I&C power to one Division (sensing, signal conditioning, and comparing) causes the system to drop from 2-of-3 to 1-of-2; loss of a second Division drops actuation to 1-of-1; and loss of third will cause actuation.

Loss of all electric power, of course, will render the ESF useless. However, there are ways in which instrument power could be lost without loss of AC power to the ESF. A reliability assessment has been made regarding the likelihood of loss of instrument power, with the resulting recommendation that the electric power supply to the I&C important to safety should be upgraded with additional and more reliable inventors, and by backfitting other equipment of the uninterruptable power supply system.

Segregation of the Protection System and Safety System Actuation.

The proposed modification in the IAEA draft report is to install new sensing lines to assure no reduction in safety margin or reliability. Since neither safety problem nor operational problem (lower availability due to spurious action) has yet been identified, the measure is not included in the present modernization programme.

The present system could cause spurious action of reactor trip if one sensing line breaks, or possibly if one line becomes plugged. However, no single failure can defeat safety action if needed, from either reactor trip or ESF actation system.

In western countries, reactor trip and ESF actuation systems (and often control systems) often share the same tap, sensing line and sensor). The issue is more directly related to the need to minimise spurious actuations due to a single failure than to segregation of systems. These areas should be incorporated into other specifics in which design or operating deficiencies have been identified. For example, Kozloduy proposal to improve ECCS accumulator isolation appears to be a similar area in which a design deficiency (one which does not meet single failure criterion) was identified and is planned for upgrade.

Human Engineering of the Control Rooms.

The proposed measures are:

- A structured, in-depth design review of the control room, similar to those done for western plants, should be conducted. The objective of this review would be to identify the specific deficiencies of the control room and to establish a modification plan to improve the safety situation. The recommendations of the control room design review should be prioritised according to their importance to safety and interim modifications should be made as soon as practical.

- A Safety Parameter Display System (SPDS) should be added to provide the operator with the information needed to assess the critical safety functions of the plant.

- Installation of Post-Accident Monitoring System (PAMS).

In-depth design review of the control room has been accomplished under an existing programme with Gilbert-Commonwealth. A preliminary study has been completed and continued progress is expected. The SPDS and PAMS are two different systems, and both are recommended by the IAEA draft report. The purpose of SPDS is to provide an information display to the operator that helps him rapidly to diagnose an event (transient or accident). PAMS, on the other hand, provides highly reliable, safety-grade wide-range instrumentation to the operator that is necessary for:

- diagnosing an event and taking manual action prescribed in the EOPs;
- monitoring the critical safety functions (criticality, decay heat removal);
- monitoring the extend of breaches in fission product barriers;
- monitoring the status of safety systems;
- monitoring radioactive releases.

Water Chemistry Control and Condition Monitoring for Mechanical Equipment

The proposed measures are:

- Installation of an on-line RCS chemistry monitoring system.

- Implementation of a system for continuos chemistry monitoring and control of SG blowdown water.

- Installation of a system for continuos diagnosis monitoring for main circulation pump vibrations.

- Inspection/diagnosis for main circulation pump stators winding insulation.

- Reliable control of operating temperatures of winding of main transformers and house transformer.

- Replacement of sensors and analysis system for present turbine vibration monitoring.

The main coolant pump vibration monitoring system replacement is already in progress on units 5 and 6 (by the Russian supplier AMRAIN) and will be finished in 1996.

The proposed measures address the safety issues and the intend of the IAEA recommendations have been met.

Primary Circuit Diagnostic Systems

The proposed measures are:

- Installation of a system for detection of a loose parts in primary circuit;

- Installation of a system for quick detection and localisation of a leakage from primary to secondary circuit;

- Modification of existing radwaste collection system (TZ) for continuous operation with increased sensitivity and monitoring to distinguish secondary from primary leaks;

- Installation of means for leak detection in upper reactor vessel head at control rod drive mechanism and instrument flange.

The intended modification of the existing radwaste system is relatively simple and will be implemented much earlier than the proposed upper head leak detection system. The Kozloduy NPP staff has already installed a humidity detector to enhance reliability of general leak detection in the upper vessel head but further tests/inspections can not be devised that would identify the location of a leak. Therefore that need will be avoided by improving the existing seals of the instrument flange connections and by installation of leak detection at control rod drive mechanism and instrument flange. Systems of two principles (acoustic and humidity) are presently being evaluated. A N 16 system is now being studied for detection of primary to secondary leaks. Improvements are desired to enhance reactor operator ability to manage the accidents.

Accident Monitoring Instrumentation

The proposed measures are:

- Installation of a steam-gas mixture detector in reactor vessel to measure the level of coolant under accident conditions;
- Installation of a hydrogen detection & recombination system;
- Replacement of equipment to monitor radioactivity in gas releases to improve accuracy, equipment qualification and service life;
- Installation of a sampling system for accidents;
- Modernization of radiation monitoring facilities.

A systematic review of accident monitoring should be conducted to identify the parameters necessary to monitor an accident and to verify that the instrument ranges are adequate to cover all design basic events. This review should also confirm that the sensor channels for the accident monitoring instrumentation are sufficiently independent from the environmental conditions that result from the accident. The following measures are also included:

- Installation of a fibre optics cable for rapid transmission of PAMS and SPDS information in the Technical Support Center;
- Installation of an automated independent radiation monitoring system for each safety system train;
- Development and installation of a centralized radiation monitoring system;
- Installation and operation of a meteorological station;
- Replacement of installed radiation monitoring system detectors which have proved unreliability;
- Provision of the metrology laboratory with the capability to maintain ionizing radiation measuring equipment.

Automatic Reactor Protection for Power Distribution and DNB in Base Load Operation

The measure proposed is:

- The neutron monitoring system AKNP, now near to the end of its service life, may be replaced with one that is more sensitive. Improved information processing, alarm and display would also be intended.

The performance of the AKNP excore nuclear monitoring system is considered satisfactory for the present base load operation. Since it is within 3 years of the end of its warranted 10 year service life for unit 5, the Russian manufacturer, SNIIP, will study it to see if its warranty can be extended. If it is decided to be replaced it will be replaced with more sensitive detectors. At present no need has been identified for axial offset monitored by the excore nuclear instrumentation and it is not a consideration for an upgraded system. The adverse power distributions will be considered in the upgraded safety analysis. On that basis the BNSA will decide whether administrative control provides adequate protection.

Incore Monitoring of Power Distribution in Load Follow Mode

The proposed measure is:

- Replacement of the incore monitoring system including thermocouples, neutron detectors and computer processor. (This may be done as part of conversion to a three year fuel cycle.)

A decision on replacing the incore detectors must be made before the end of the 10 year service life of the present detectors and system. If the plant will be converted to load follow operation new/different fuel would be required and different incore detectors and computer processor would be provided.

5. Conclusions

The intended programmes in the area of I&C together with other upgrades either completed or already in progress address all the IAEA I&C issues of higher safety significance. Two of the IAEA I&C issues of low safety significance are not addressed: potential for spurious actuation due to a single failure and core axial power protection against DNB during base load operation. Kozloduy NPP should monitor progress on these issues in other WWER-1000/320 NPPs and consider their applicability to Kozloduy NPP.

Modernization of Kozloduy 5/6 would provide a power generation source where one could expect a very high level of reliability. The targeted safety improvements can only go to increasing these factors, the in-service availability and load factors. Successful completion of the modernization programme in good time would therefore constitute a considerable beneficial contribution to means of energy production in Bulgaria in safe and reliable conditions.

IAEA ADVISORY GROUP MEETING
ON
MODERNIZATION OF INSTRUMENTATION AND CONTROL SYSTEMS
IN NUCLEAR POWER PLANTS
VIENNA, 25 TO 29 MARCH 1996

NPP I&C SYSTEM INNOVATIONS IN THE CZECH REPUBLIC A REGULATORY PERSPECTIVE

PRESENTED BY C. KARPETA
SONS
PRAGUE, CZECH REPUBLIC

<u>The goal of this presentation is to describe:</u>

- the on-going I&C system replacement project at the NPP Temelin
- the preparatory phase of a project for I&C system innovation at the NPP Dukovany
- licensing aspects of NPP I&C system replacement/innovation projects in the Czech Republic

I&C system replacement project at the NPP Temelin

Topics to be addressed:

- **brief description of the NPP Temelin**
- **I&C system upgrades**
- **diagnostic system upgrades**
- **quality assurance aspects of the I&C system replacement**

Brief description of the NPP Temelin

- general information about the plant
- the plant NSSS
- the plant secondary side
- the plant original I&C system
- a summary of deficiencies of the original I&C system design

- 96 -

I&C design upgrades

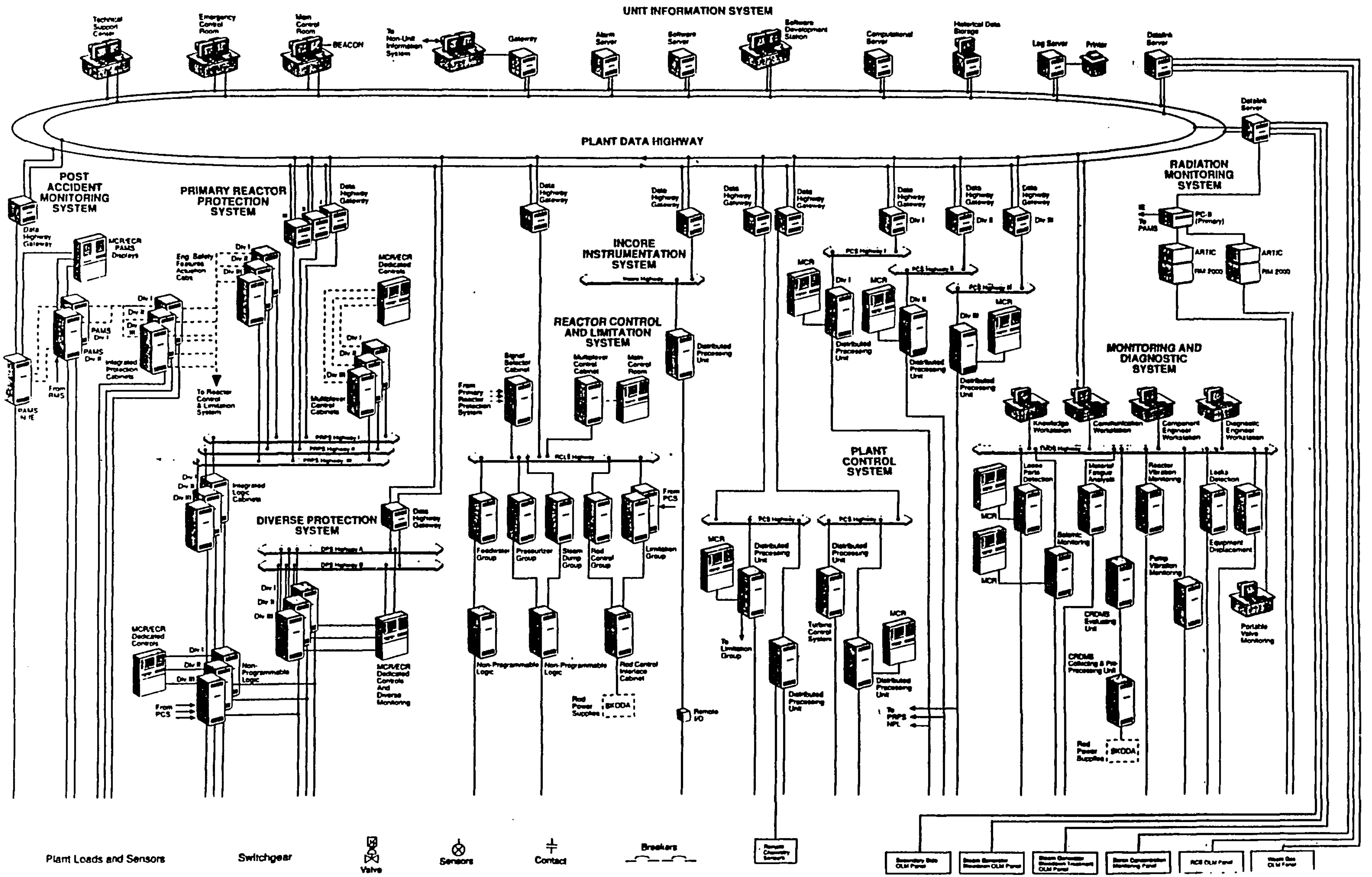
- overview of the adopted approach
- I&C system architecture

  * unit information system

  * I&C parts of the plant safety systems

    ⇒ Primary Reactor Protection System (PRPS)
    ⇒ Diverse Protection System (DPS)
    ⇒ Post-Accident Monitoring System (PAMS)
    ⇒ Non-Programmable Logic (NPL)

Westinghouse Temelín I&C System Architecture



I&C design upgrades (cont.)

* Reactor Control and Limitation System (RCLS)

* Plant Control System (PCS)

* Plant Control Centers (MCR, ECR, TSC)

Diagnostic systems

- Control Rod Drive Monitoring System (CRDMS)
- Digital Metal Impact Monitoring System (DMIMS)
- Rotating Equipment Vibration Monitoring System (RECOP)
- Material Fatigue Evaluation System (MAFES-TSF)
- Material Fatigue Evaluation System (MAFES-DMS)
- Reactor Vibration Monitoring System (RVMS)
- Leakage Monitoring System of Pipes (LEMOP)

Quality assurance of the I&C system replacement project

Topics to be addressed:

- **basic provisions of the Regulation No. 436/1990**
- **QA programs of organizations involved in the replacement project**
- **QA policy adopted in the I&C area**

Basic provisions of the Regulation No. 436

- items important to safety are classified into three safety classes
- three types of QA programs are identified (general, partial, and individual)
- both organizational and technical aspects of QA programs implementation are addressed
- format and contents of documentation on implementation of each type of QA programs are defined

QA programs of organizations involved in the replacement project

- the utility - Czech Power Company (CEZ)
- the general supplier - SKODA Company
- subcontractors of the general supplier
  - * Westinghouse Electric Corporation (WEC)
  - * Energoprojekt (EGP)
  - * Regula Praha, Metra Blansko, VUMS, Diamo, I&C Energo and others

QA policy adopted in the I&C area

- the role of EGP and WEC in the I&C system design
- manufacture of the I&C equipment
  * in the USA
  * outside the Czech Republic territory
  * in the Czech Republic
- installation

Preparatory activities for I&C system innovation at the NPP Dukovany

Topics to be addressed:

- brief description of the NPP Dukovany and its I&C system
- overview of findings of the plant I&C system evaluations
- outline of a proposal for I&C system replacement project

Brief description of the NPP Dukovany

- general information on the plant
- NSSS of the plant
- plant secondary side
- plant I&C systems
    - * I&C parts of safety systems
    - * control systems
    - * information systems

Overview of the I&C system evaluations

- IAEA extrabudgetary program on the safety of VVER model 213 NPPs
- basic engineering for replacement of the I&C system for V 213 nuclear reactors - phase 1
- SONS findings from evaluation of the operational SAR for Unit No. 1
- results of PSA - level 1 study

Outline of a proposal for I&C replacement

Recommendations for I&C system replacement generated by the PHARE project - phase 2

- **objectives of the replacement project**
- **definition of the final design concept**
- **formulation of detailed system requirements**
- **specification of the project QA program**
- **inquiry documentation**
- **planning documentation**

Licensing aspects of I&C system replacement projects in the Czech Republic

Topics to be addressed:

- **the existing regulatory framework**
- **specific aspects of the NPP Dukovany case**
- **specific aspects of the NPP Temelin case**
- **database of licensing issues to be considered in the assessment of new I&C systems**

Regulatory framework for I&C system replacement projects

- the role and responsibilities of SONS as per provisions of the Act No. 28/1984
  - * upon request of the licensee and after assessment of the submitted documentation SONS will grant its consent
    - ⇒ to local authorities as a binding position for decision taking in the proceedings concerning the construction and commissioning of nuclear facilities
    - ⇒ to individual phases of putting a nuclear facility into operation
    - ⇒ to implementation of changes affecting the nuclear safety of nuclear facilities

- **the role and responsibilities of SONS as per provisions of the Act No. 28/1984 (cont.)**

  * **on the basis of a substantiated proposal submitted by the licensee for each individual nuclear facility SONS will approve**

  ⇒ **a set of limits and conditions imposed upon the operation of this nuclear facility**

  ⇒ **quality assurance programs for items important to safety**

  ⇒ **programs for putting the facility into operation**

  ⇒ **changes of limits and conditions**

SONS requirements relating to the NPP Dukovany I&C system innovation

Two groups of requirements were set forth by SONS based on the findings from its review of the operational SAR for Unit No. 1:

- **specification of the replacement system general characteristics**
  - **well structured defense-in-depth**
  - **sufficient diversity among the individual echelons of defense**
  - **independence between the individual echelons of defense, between safety systems and other plant systems, between**

individual divisions of redundant safety systems, and between plant control centers

* high reliability documented by a systematic qualitative and quantitative analysis

* efficient testability and maintainability

* post-accident monitoring

* efficient operator information, control and support system

* unit control system for load-follow operation

* on-line and off-line diagnostic systems

- **specification of design and quality assurance requirements**

  * **conformance to the applicable provisions of the Regulation No. 2/1978**

  * **conformance to the applicable provisions of the Regulation No. 436/1990**

  * **compliance with the current internationally recognized design criteria for assurance of nuclear safety**

SONS requirements set for the NPP Temelin I&C system replacement

Topics to be covered:

- **general acceptability requirements**
- **requirements pertinent to computer-based safety systems**
    - **requirements for hardware**
    - **requirements for software**

General acceptability requirements

The NPP Temelin I&C replacement system

- shall be licensable in the country of its design origin
- shall meet applicable requirements stated in internationally recognized codes, guides and standards
- the issue of the potential for a common mode failure in the computer-based reactor protection system shall be addressed by providing a diverse system capable of taking the plant to safe shutdown conditions and maintaining the plant in those conditions with the assistance of the operational personnel

General acceptance criteria for HW of computer-based parts of safety systems

- compliance of the hardware design, development and manufacture activities at the supplier and installation, commissioning and maintenance activities at the plant operator with IEC 987/1989

- environmental, seismic and EMC qualification of the computer system hardware according to regulatory guides, IEC and IEEE standards

- implementation of quality assurance program in conformance with Czech regulation No. 436/1990 and ANSI/ASME NQA-1b/1992

General acceptance criteria for PRPS SW

- compliance of the software development activities at the supplier and maintenance activities at the plant operator with IEC 880/1986, ASME NQA-2a/1990 part 2.7 and IEEE 7- 4.3.2/1993

- carrying out independent audits which provide evidence that the requirements and recommendations of the above mentioned standards have been met and followed during the software development

- performing independent verification and validation (IV&V) of the delivered software product which shall provide reasonable assurance that it is free from faults that could impair accomplishment of the system safety functions

General acceptance criteria for DPS SW

- conformance of the software development activities at the supplier and maintenance activities at the plant operator to IEC 880/1986, ASME NQA-2a/1990 part 2.7 and IEEE 7-4.3.2/1993

- special attention shall be paid in the development process to the reduction of the potential for CMFs similar to those postulated in the PRPS software

- conducting independent audits which provide evidence that the development process is in compliance with the provisions of the above mentioned standards

- performing IV&V of the delivered software product which provides reasonable assurance that the product is free from faults that could impair accomplishment of the system safety functions

General acceptance criteria for PAMS SW

- compliance of the software development activities at the supplier and maintenance activities at the plant operator with IEC 880/1986, ASME NQA-2a/1990 part 2.7 and IEEE 7-4.3.2

- performance of independent audits which provide evidence that the requirements and recommendations of the above mentioned standards have been met and followed during the software development

- independent verification of system requirements and their complete and correct translation into software requirements and specifications

Guidelines for IV&V of the PRPS software

- General

  * verification of system requirements and their complete and correct translation into software requirements and specifications
  * static analysis of selected parts of the software
  * dynamic testing of the software as a whole

- Specific

  * system software
  * application software
  * data

Guidelines for IV&V of the DPS software

- General

  * verification of system requirements and their complete and correct translation into software requirements and specifications
  * static analysis of selected parts of the software
  * analysis of the potential for CMFs similar to those of the PRPS

- Specific

  * system software
  * application software
  * data

Guidelines for IV&V of the PAMS software

- **verification of system requirements shall be performed against applicable Czech and US regulations**

- **verification of software requirements and specifications against system requirements should be carried out using a qualified tool; if a tool employment is not feasible manual techniques are also acceptable**

Guidelines for the scope of an independent audit

- **assessment of the development process implementation**
  - * **QA, V&V, CM and software safety analysis should be examined**
  - * **particular attention should be paid to questions raised during the review of relevant documentation**
- **assessment of the design outputs**
  - * **for a number of individual safety system functions the implementation of the associated functional requirements should be traced from top level system requirements to design documentation and testing**

  * evaluation of the employed development processes including the ACEs analysis should be performed

  * the assessment should include a review of Temelin specific reactor trip functions, samples of diagnostic software, the automatic surveillance testing provisions and provisions for confirming system return to service

- assessment of design output translation to executable code

  * documentation of the process for qualifying the employed tools should be inspected

  * both commercial off-the-shelf products as well as developer's in-house products should be covered

Database of licensing issues

A database of licensing issues has been developed because of:

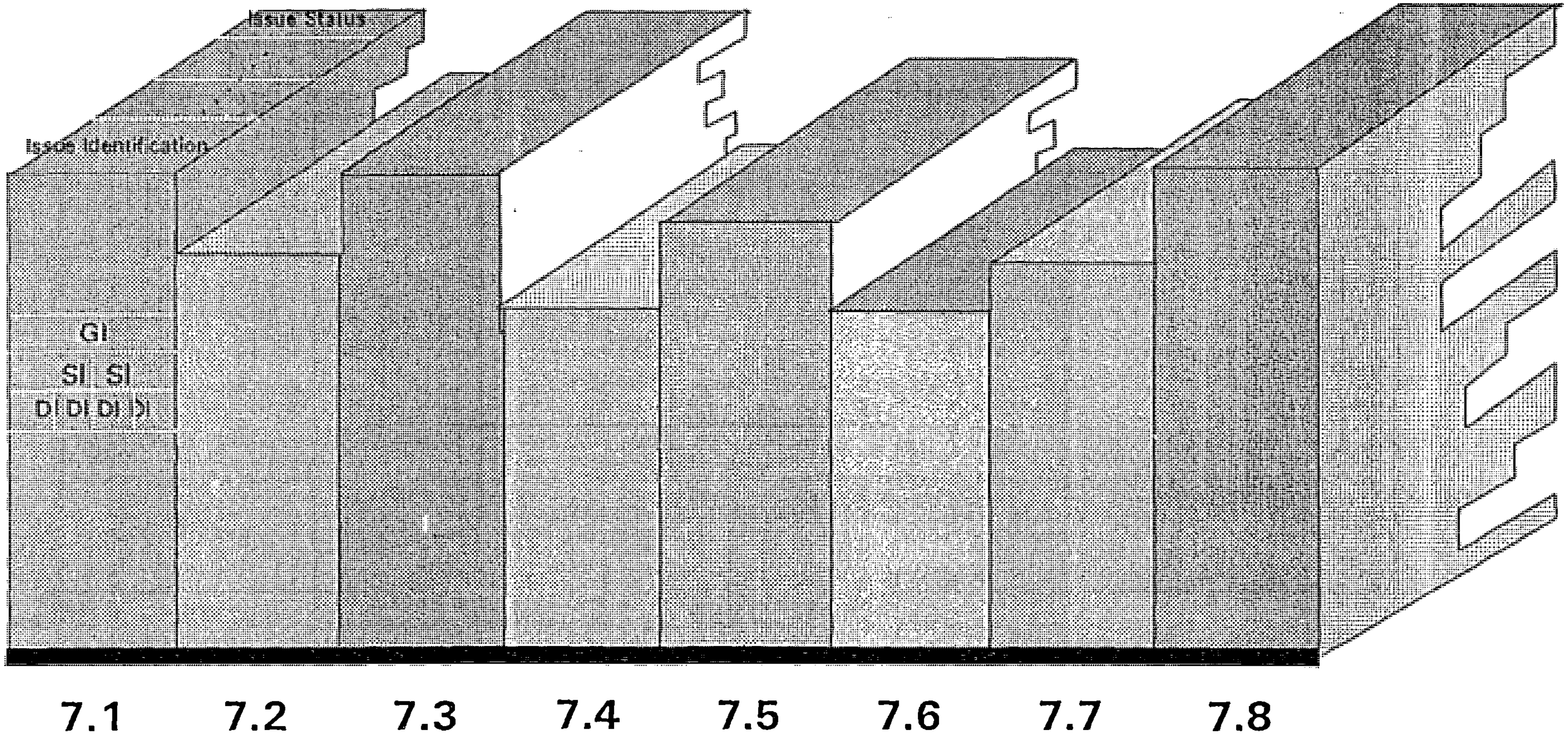
- **the need for a tool for organizing, documenting, and reporting of the NPP Temelin I&C licensing review process**
- **SONS position on licensibility of the NPP Temelin I&C systems**
- **specific characteristics of the NPP Temelin I&C system design**
- **adopted review methodology**

The licensing methodology for which the Temelin Licensing Database was designed consists of a bottom up review and evaluation structured into 3 layers:

- Lower layer
- Middle layer
- Upper layer

-127-

The structure of the I&C licensing database may be represented by a 3-dimensional figure consistent with Chapter 7 of the PSAR.



-128-

Examples

ISSUE IDENTIFICATION NUMBER: 07 . 208 . 000 . 000

ISSUE: Adequacy of the PRTS design for test and calibration

Source of the ISSUE: NUREG 0800/81(7.2 II.1; 7.2 III.3; 7.1 App.B.11); 10 CFR 50/93 App.A(III.11); Reg.2/78(16.2); IAEA 50-SG-D3/80(7.10); IEEE 603/91(5.7); IEEE 7-4.3.2/93(5.7); BTP ICSB 22

ISSUE IDENTIFICATION NUMBER: 07 . 208 . 001 . 000

ISSUE: Adequacy of provisions for periodic on-line and/or off line testing to detect PRTS failures

Source of the ISSUE: RG1.22; RG1.118; IAEA 50-SG-D3/80(7.10.1); IEEE 338/87(6)

ISSUE IDENTIFICATION NUMBER: 07 . 208 . 002 . 000

ISSUE: Adequacy of provisions for periodic test to confirm and/or adjust performance characteristics of the PRTS

Source of the ISSUE: RG1.22; RG1.118; IAEA 50-SG D3/80(7.10.2); IEEE 338/87(6)

ISSUE IDENTIFICATION NUMBER: 07 . 208 . 003 . 000

ISSUE: Adequacy of test coverage

Source of the ISSUE: RG1.22; RG1.118; IAEA 50-SG D3/80(7.10.3); IEEE 338/87(5, 6)

Examples (continued)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 000 . 000

ISSUE: Adequacy of the verification and validation process for a computer system used as part of a safety system

Source of the ISSUE: RG 1.152/85 ASME NQA-1/89, suppl. 35-1 (4) ASME NQA-2a/90, part 2.7 (3.4,4) IEC 880/86 (6.8) IEC 987/89 (6) SUJB requirements (letters to CEZ: Feb. 94, Aug. 94)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 100 . 000

ISSUE: Adequacy of planning for V&V activities for the development process of the computer system

Source of the ISSUE: ASME NQA-1/89, Suppl. 35-1 (4.0) ASME NQA 2A/90, part 2.7 (4.0, 3.4)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 101 . 000

ISSUE: Adequacy of the HW verification and validation plan

Source of the ISSUE: IEC 987/89 (6.1)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 102 . 000

ISSUE: Adequacy of SW verification and validation plan

Source of the ISSUE: IEC 880/89 (6.2.1, 8) IEEE 1074/91 (7.3.1) IEEE 1012/92 (3.0, 3.1 to 3.7)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 103 . 000

ISSUE: Adequacy of the integrated computer system (HW&SW) verification and validation plan

Source of the ISSUE: IEC 880/86 (7.5)

Examples (continued):

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 300 . 000

ISSUE: Adequacy of coverage of the computer system development process by V&V activities and adequacy of results obtained

Source of the ISSUE: IEEE 1012/92 (3.5) IEC 987/89 (6) IEC 8880/86 (6, A1) IEEE 7 4.3.2/93 (E.2)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 301 . 000

ISSUE: Verification of safety system requirements allocation to the computer system

Source of the ISSUE: IEEE 7-4.3.2/93 (E.2.2.1 to E.2.2.5) IEEE1012/92 (3.5.3) IEEE 830/84 (4.3)IEC 880/86 (4) IEC 987/89 (6.0)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 302 . 000

ISSUE: Verification of the design phase

Source of the ISSUE: IEEE 7-4.3.2/93 (E.2.2.8.1, E.2.2.7) IEEE 1012/92 (3.5.4) IEEE 1016/87 (5.1 to 5.3) IEC 880/86 (6.2.2) IEC 987/89 (6.1, 5.7.1)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 303 . 000

ISSUE: Verification of the implementation phase

Source of the ISSUE: IEEE 7-4.3.2/93 (E.2.2.8.2) IEEE 1012/92 (3.5.5) IEEE 1008/87 (3) IEC 880/86 (6.2.3) IEC 987/89 (6.1, 5.7.2)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 304 . 000

ISSUE: Verification of the integration phase and validation of the computer system

Source of the ISSUE: IEEE 7-4.3.2/93 (E.2.2.9, E.2.2.10) IEEE 1012/92 (3.5.6) IEC 880/86 (7.5.8) IEC 987/89 (6.7, 6.8)

Examples (continued)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 200 . 000

ISSUE: Acceptability of the range of V&V activities performed during the development cycle of a computer system.

Source of the ISSUE: ASME NQA-1/89, Suppl. 35-1 (4.2) ASME NQA-2a/90, part 2.7 (4.1, 4.2)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 201 . 000

ISSUE: Independent reviews of documented work

Source of the ISSUE: IEC 880/86 (6.2.2) IEC 987/89 (6.3) IEEE 7-4.3.2/93 (E.2.1.1)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 202 . 000

ISSUE: Independent witnessing of design activities

Source of the ISSUE: IEEE 7-4.3.2 (E.2.1.2)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 203 . 000

ISSUE: Independent inspections of generated products, such as design/test documentation, code, etc.

Source of the ISSUE: IEEE 7-4.3.2/93 (E.2.1.3) IEC 987/89 (6.3)

ISSUE IDENTIFICATION NUMBER: 07 . 111 . 204 . 000

ISSUE: Independent analysis of development process products

Source of the ISSUE: IEEE 7-4.3.2/93 (E.2.1.4) IEC 987/89 (6.2)

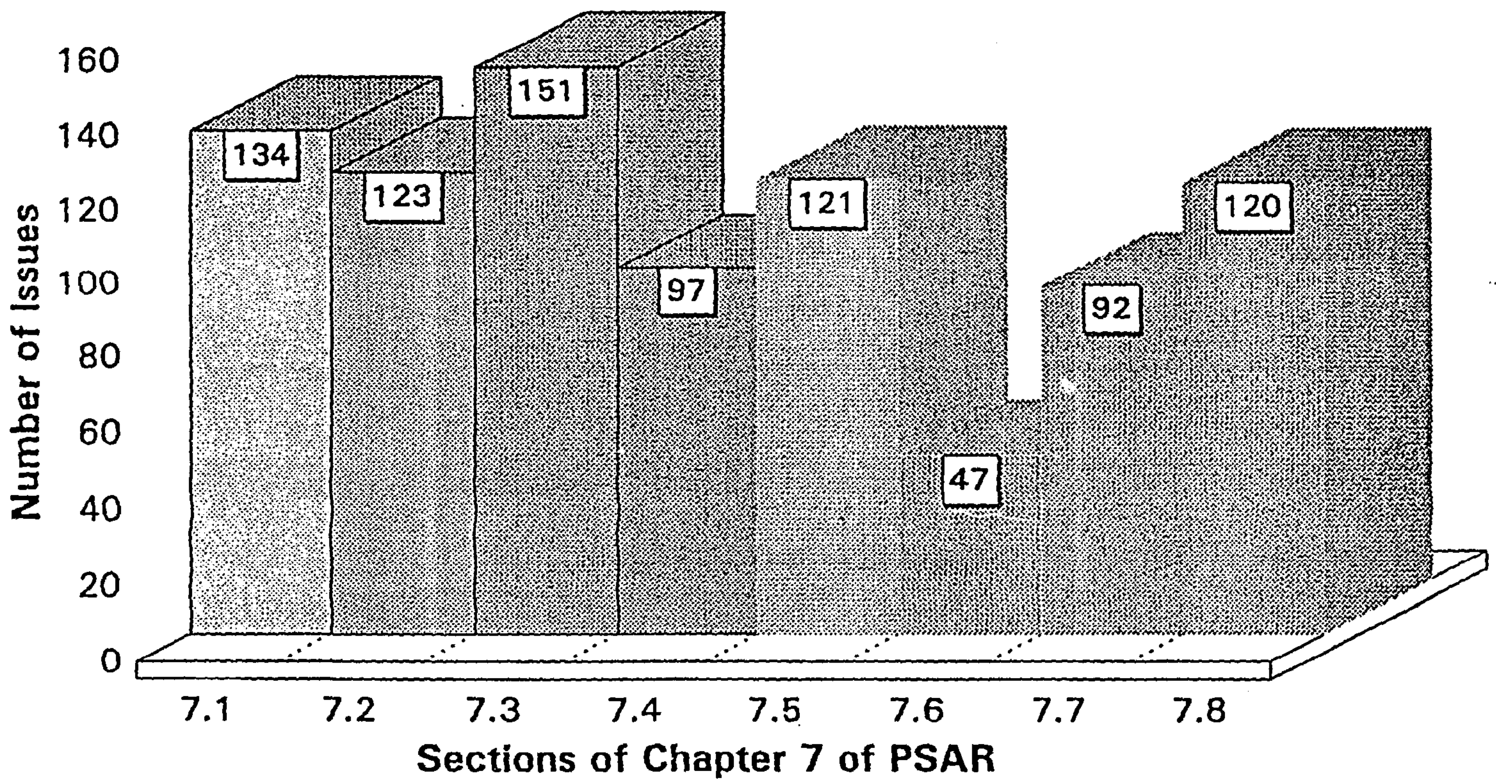
ISSUE IDENTIFICATION NUMBER: 07 . 111 . 205 . 000

ISSUE: Testing of products of the development process

Source of the ISSUE: IEEE 7-4.3.2/93 (E.2.1.5) IEEE 1008/87 (3) IEC 880/86 (6.2.3.1) IEC 987/89 (6.3)

Number of licensing issues identified in the licensing database for individual sections of Chapter 7 of the NPP Temelin PSAR

Total: 885



MMIS Development: *its status*

IAEA Advisory Group Meeting

on

"Modernization of Instrumentation and Control Systems in Nuclear Power Plant"

25-29 March 1996

Vienna/Austria

In Soo Koo/ Chang Hwoi Kim

Man-machine Interface System Development/Advanced I&C Systems Development

Korea Atomic Energy Research Institute

BACKGROUND

1. PROBLEMS OF OPERATING PLANTS

Existing I&C systems for nuclear power plants

- obsolescence
- burden on maintenance and testing activities
- inaccuracy
- unreliability
- to adopt new technologies

The outage reports of nuclear power plants

The percentage of failures caused by I&C:	about 17% of duration
	about 44% of numbers.

2. TMI ACTION PLAN

Operator's burden at emergency: very high

3. POTENTIAL LICENSING ISSUE

- IEEE 7-4.3.2, "Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations", 1993.
- NUREG-0711, “Human Factors Engineering Program Review Model”, 1994.
- NUREG-0700, “Human-System Interface Design Review Guideline, draft”, 1995.

GOAL

- Improvement of plant availability and reliability
- Improvement of the maintainability
- Software quality improvement and hardware qualification
- Improvement of the operator support functions
- Development of MMIS(= MMI + I&CS)

DEVELOPMENT APPROACH

- Advanced design

  To improve safety, reliability and availability, advanced digital technology is applied in the design of MMIS.

- Adoptive design

  To provide flexibility in the design of MMIS, standardization and modular design is applied

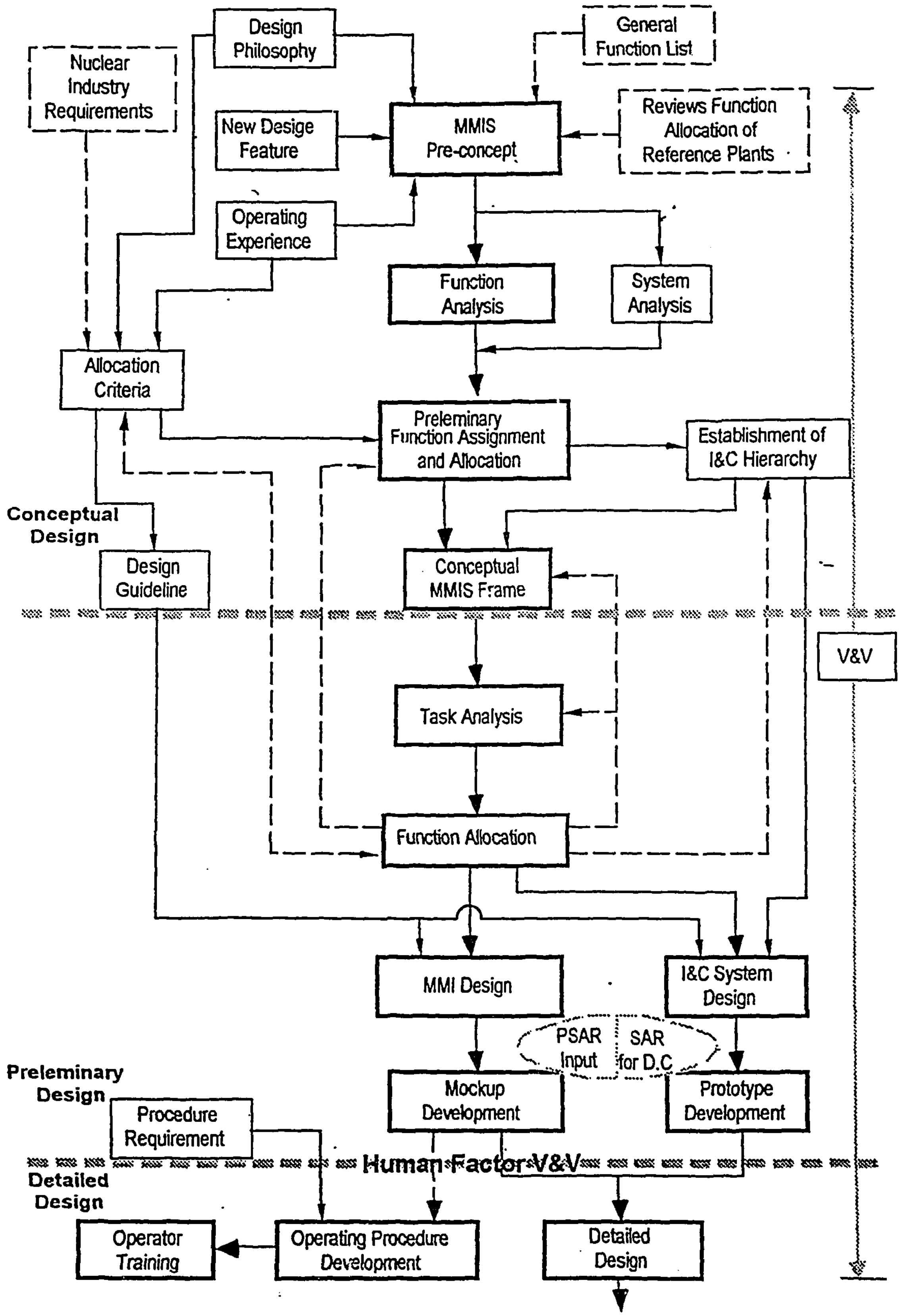
- Intelligent design

  To achieve human error-free MMIS, operator aids functions and automation of I&C systems are provided.

- Integrated design

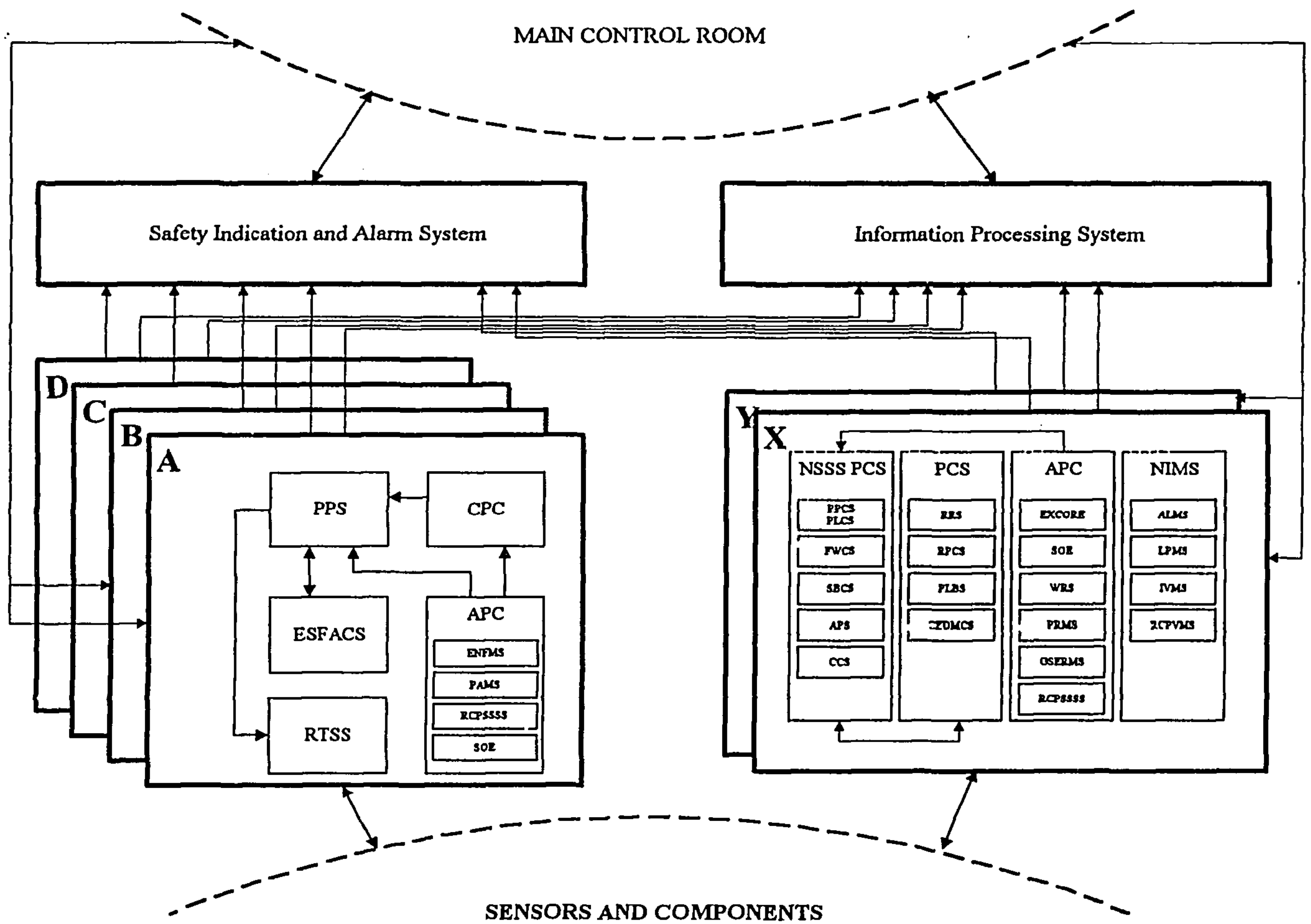
MMIS DEVELOPMENT METHOD

1. MMIS Pre-concept
2. Function Analysis
3. Preliminary Function Assignment and Allocation
4. Conceptual MMIS Frame
5. Task Analysis
6. Function Allocation
7. MMI Design and I&C System Design
8. Mock-up Development and Prototype Development


Design Philosophy
General Function List
Nuclear Industry Requirements
New Desige Feature
MMIS Pre-concept
Reviews Function Allocation of Reference Plants
Operating Experience
Function Analysis
System Analysis
Allocation Criteria
Preleminary Function Assignment and Allocation
Establishment of I&C Hierarchy
Conceptual Design
Design Guideline
Conceptual MMIS Frame
V&V
Task Analysis
Function Allocation
MMI Design
I&C System Design
PSAR Input
SAR for D.C
Preleminary Design
Procedure Requirement
Mockup Development
Prototype Development
Human Factor V&V
Detailed Design
Operator Training
Operating Procedure Development
Detailed Design

DEVELOPMENT OF NEXT GENERATION REACTOR

1. Main Control Room
2. Information Processing System
3. Safety Indication and Alarm System
4. Plant Protection System
5. ESF Actuation Control System
6. Core Protection Calculator System
7. Process Control System
8. Power Control System
9. Misc. System


MAIN CONTROL ROOM
Safety Indication and Alarm System
Information Processing System
D
C
B
A
PPS
CPC
ESFACS
RTSS
APC
ENFMS
PAMS
RCPSSSS
SOE
Y
X
NSSS PCS
PPCS
PLCS
FWCS
SBCS
APS
CCS
PCS
RRS
RPCS
PLBS
APC
EXCORE
SOE
WRS
PRMS
OSERMS
RCPSSSS
NIMS
ALMS
LPMS
IVMS
RCPVMS
SENSORS AND COMPONENTS

On Going Project

1. Automatic Startup Intelligent Control System(ASICS)

- Goal

  Development of automatic heat-up control system from cold shutdown to 5% Rx power

- Automation Mode

  - Heating I : RCS temp. 60 - 176°C, RCS Pr. 27Kg/cm^2

  - Heating II : RCS temp 176 - 292°C, RCS Pr. 27 - 157Kg/cm^2

  - 2nd Mode : SG level 100 - 50%, 2nd Pr. 1 - 76.6Kg/cm^2

  - Critical Mode : 1770 - 0PCM

2. Alarm and Diagnosis-Integrated Operator Support System(ADIOS)

- To filter or suppress unnecessary or nuisance alarms
  - Mode and state dependency
  - Hierarchical and functional relation alarm
  - Dynamic priority dependent on plant state
  - Status-Alarm separation

- Analysis plant model : KORI 3 & 4
  - Object-oriented knowledge representation scheme
  - Prototype implementation and human-performance evaluation using HFEITF

- Model-based fault detection and diagnosis
- Operator response model using cognitive mental model

I&C Test Facility

- Goal

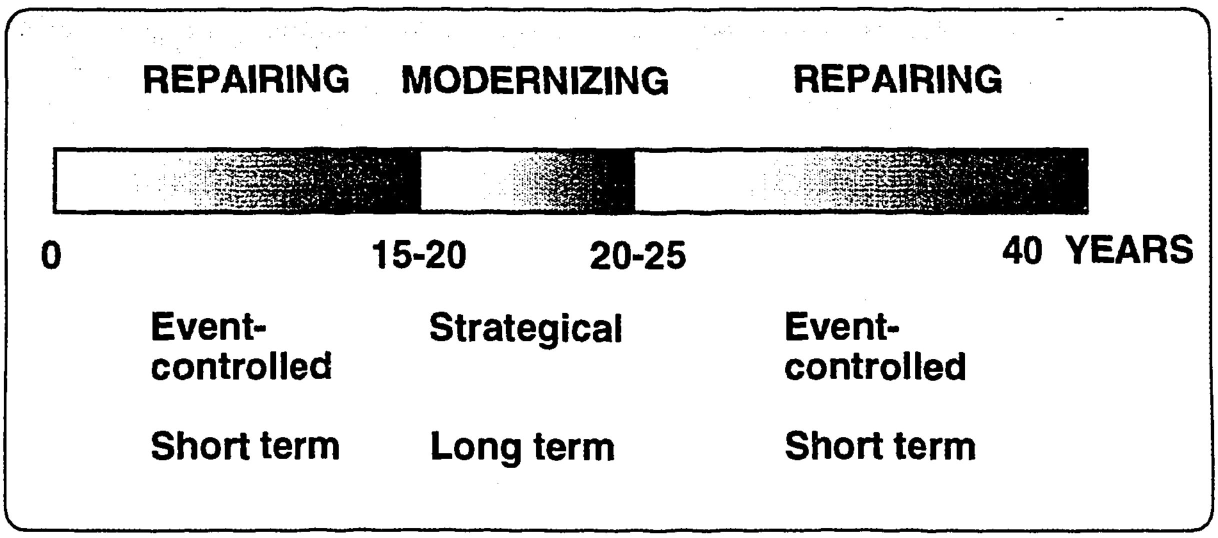
  Developing 3-loop 993MWe PWR code, GUI, and hardware interface

- Main Function

  - Function and performance test for developed I&C system
  - Store certain operational condition to file
  - Only one step run the dynamic process
  - Insert malfunction
  - Print out continuously specified variables with changeable time step to certain file
  - Automatically show certain situation by scenario

= MODERNIZATION of I&C =

A stepwise learning process with a final vision



IAEA Advisory Group Meeting on:
Modernization of Instrumentation and Control Systems in Nuclear Power Plants

Wien, 25-29 March 1996.

Paul van Gemst
ABB Atom
Sweden

Summary

In spite of some political signals it is expected that the life time o nuclear power plants in the Nordic countries will be as designed for. As the economical life time of the I&C equipment is less than the corresponding life time of the plant a strategy for modernisation of it must be developed.

To modernise equipment during ongoing operation of the plant is not onl a technical challenge but also a challenge to human relations. It will give a unique chance for the old generation, who built the plants, and the young generation, who have to modernise the plants, t discuss common problems and new ideas.

The purpose of this paper is to summarise some important aspects whic can be included in the content of the planned IAEA book.

Lifetime phases

During the first lifetime phase of the power plant the I&C equipment is repaired and modified on an "event" controlled way. What I am meaning with the word "event" is that repairs and modifications are decided and carried out when component faults or design errors are detected. These activities are carried out on a short term basis. As the equipment became older such short term activities will increase until a moment that some drastically and other methods have to be decided.

Such decision must be taken before the costs for repairing became so high that it is difficult to "free" capital for investments in new equipment.

This is the situation for many nuclear power plants in the Nordic countries. In order to quarantee the safe, reliable and economical operation of the power plant strategies for modernisation of I&C equipment are developed, initiated and carried out. Such strategies will often cover a long time period of several, up to, 10 years.

Strategy.

Depending on the age of the plants and the type of technology of the I&C equipment different types of strategies are developed. A common element for all strategies is that modernisation shall be prepared during plant operation and be carried during the normal planned refuelling outages. The main goal is that modernisation shall not reduce the plant availability.

The plans include a learning process with a stepwise replacement of equipment. The most important decision from the start is that all modernisation shall be a logical part of the final I&C integrated configuration after the modernisation process during many years.

How this final "vision" can be reached has been the subject fo different studies.

It is obvious that two different strategies are possible.

The first one is to replace systems one by one and provide possibilitie to connect these later into a final integrated I&C system. The advantage is, of course, that systems and the later network can be purchased with the latest technology in free competition. The disadvantage is that much software engineering is required to integrate the systems with the network. Solutions for such integration are often unique and not supported as a standard design.

Another strategy is to establish the infrastructure "network" for the I&C from the beginning and to connect systems stepwise later. The advantage is that integration costs are reduced because the structure is an well proven standard design.
The disadvantage is of course that often standard systems must be purchased from the same manufacturer as for the network. The choice of technology is not longer totally free. This option seems to be the most economical one today.

Common for both strategies is that the first modernisation step must be selected with regard to:

- the best spin-off for learning of the application and the operation of new technology
- the volume of communication for establishing the requirements for and installation of the infrastructure

A typical example for this first step is the plant process computer with control room MMI and communication to other computers and to the process I&C.

As a minimum following aspects shall be included in the strategy:

- the final I&C structure "vision"
- the method for integration
- selection of the first step
- limitation and restrictions
- safety and licensing
- functional upgrading
- step by step implementation
- new technology
- products
- design requirements
- project organisation
- Budgeting

Vision

It is clear that the modernised equipment shall be based on digital technology. The different systems shall be connected with each other by networks.
Different types of networks shall be available as for:

- process control and supervision
- control room MMI
- plant technical and administration servers and computers

A example of such an infrastructure is enclosed.

Limitation and restrictions.

Modernisation of I&C for an existing plant must take care of some limitations. Such limitations must be defined as a policy in the beginning of the modernisation process.
The limitations can be a result of:

- limitation of plant layout
- integration philosophy
- available free spaces
- existing process systems
- existing control room and maintenance organisation and staffing
- available time during refuelling outages
- money

Safety and licensing.

The main safety goal is to increase safety by using more modern safety requirements. Requirements can be obtained by reading formal criteria and standards or by executing a PSA (Probabilistic Safety Assessment). However, as the plant was designed for many years ago, it can be problem to meet all modern requirements.
The limitations and restrictions as mentioned before can put limits on the modernisation of the safety. Deviations between the modernisation gaols and formal modern requirements must be listed, evaluated and agreed upon with the licensing authorities. For some old power plants in Sweden such deviations against formal requirements are evaluated with a PSA (Probabilistic Safety Assessment). The PSA methods can also successfully be used to identify weak points in the existing design.
Another input for increasing safety are the evaluation reports for transients, incidents or accidents.
An important discussion point in the Nordic countries is what type of safety standards shall be used. IEEE, which was used for the original design, or the newer IEC? Very often IEEE is selected as the other mechanical and process systems are also following USA criteria and standards.

Functional upgrading.

The main reason for modernisation is to replace an obsolete equipment. To increase functions is often not foreseen but can identified later.

Typical new functions are:

- increasing the degree of automation
- improving the operational support
- improving the administration of maintenance
- reducing manpower
- specialist engineering support
- better process transient management

A normal input for the decision for upgrading functions is to study operational reports or to interview operation and maintenance personnel. Interviewing personnel is also a good method to engage the plant personnel as early as possible in a modernisation process.

Step by step implementation.

As mentioned before a step by step modernisation is required for different reasons.
For most of the plants to start with a few stand-alone steps is preferable to gain experiences for modernisation and to increase the competence of the staff. In order to guarantee the learning aspects formal agreements can be signed between the original builder of the plants and the utilities.
Another point is of course that the size of the individual modernisation has to be limited in order to make it possible to install them during a normal refuelling outage. An important aspect is to provide space for new equipment by step by step removal of old equipment.
Modernisation can be carried out for components, systems or integrated I&C systems. An important gaol to let all modifications be a part of the final, long term, I&C configuration.

In order to make the step by step approach possible the new equipment must communicate with the existing equipment. This must be planned very carefully. Consequences for the personnel to operate and maintain two type of technologies at the same time must be clarified.

New technology.

New technology can solve current problems in a better way and in this way increase the safety and improve the plant availability. It can further include the best of the existing equipment. The new equipment has also possibilities to include new or improve old functions.

However, a new equipment has new characteristics different from the existing equipment. Such new characteristics have to be identified and the influences on safety and operation must be evaluated.

Typical new characteristics for digital equipment are:

- Functions are carried sequentially and the load vary depending on the plant situation. There is a risk for overloads during big transients in the plant if the software system is not designed properly.

- Software can be complex and risk for common design errors are increased. This can increase the volume of CMF (Common Mode Failures) if counter measures are not planned or implemented properly.

- Due to the sequential way of working the time response for the new equipment differs from the existing analogue or relay equipment

- Concentration of many functions in fewer hardware units makes it difficult to analyse consequences of hardware faults. Such faults can influence the operation of more process systems as before.

- Modern equipment includes methods and tools which are not suitable for nuclear safety systems. Examples are downloading of data and programs and open communication. Security ("sabotage") can be a problem if such new methods are allowed in safety systems.

- Elder plants are not provided with sufficient grounding or other measures for reducing electrical and magnetic interferences. Before installation of modern equipment this problem has to be studied and suitable counteractions to be taken. Due to European laws standard equipment purchased within Europe has been tested for EMC thoroughly.

Products.

As mentioned before the strategy must include a vision of the final and long term I&C configuration. This is only possible by using off the shelf products with standardised hardware and software communication modules.
The manufacturer of the products must quarantee a long term support. Special products only for nuclear application cannot be supported in a long term.

Using standard products with operating experience will also reduce development costs and delivery times and increase availability of systems.

The nuclear application will therefor be designed with standard hardware and software modules from an industrial standard product family. Typical nuclear requirements will be designed into the target system by using the standard modules in specified way.

Above mentioned reason is the background for the decision of some utilities in the Nordic countries to base the long term modernisation on products of the same manufacturer.

Design requirements.

Design requirements must be specified early in the modernisation project. They must be under QA control.

They must include following aspects:

- Reconstruction of the original requirements
- Adaptation to new technology
- Adaptation to newer safety requirements
- Increasing of operational and maintenance functions or support
- Methods for coexistence of new and old equipment
- Use of modern methods as for:
  Human factor engineering
  Verification and validation
  PSA (Probabilistic Safety Analysis)
  Full scale simulation training and validation
  FMEA (Failure Mode and Affect analysis)
  Reliability analysis
- Environmental characteristics, separation, earthquake and other typical nuclear requirements

Requirements are divided into general requirements valid for the whole I&C and requirements for standalone systems.

General requirements will often result in the design of configurations "infrastructures" for:

- whole I&C system
- the control room complex
- auxiliary electrical power system.

A point that has already being identified in current projects is that new equipment and new safety rules need other types of power supplies and will require changes in the electrical power supply system.

Project organisation and budgeting.

Modernising I&C during continuous operation is not easy. It need a well structured project and project organisation.
Strategies have to be decided and plans to made up for a stepwise introduction of new systems. Different types of experts from different organisations have to be contracted.

The project must be authorised by and accepted in the whole organisation of the utility. Especially the end users within the operation and maintenance departments must be engaged from the beginning.

Informal information meetings with regulatory authorities have to be organised and formal licensing process must be planned and carried out.

Personnel has to be trained on new equipment.

In order to install and commission the new equipment during a short refuelling outage it is necessary to prepare for installation already during the operation of the plant. This must be done without jeopardising safety or plant availability.

All these aspects together make it sometimes more difficult to modernise an existing plant than to build a new one.

By means of informal quotations price levels for equipment has to be estimated and a long term budget must be worked out. This budget is approved by the management of the plant.

References:

[1] Lars-Erik Häll
TVO
Modernisation of the control and instrumentation in the TVO BWR power plant.
IAEA specialist meeting, Munchen 1995

[2] S Börlin, Å Bäck
ABB Atom
Backfitting a digital class 1E system
ENC'94
Transaction volume 2

[3] A Laryd
ABB Atom
Operating experience of software in programmable equipment used in ABB Atom nuclear I&C applications
VTT Symposium 147
Helsinki, Finland

Acknowledgement:

I want to thank my colleagues for useful suggestions and comments and especially following persons:

Einar Ströbeck	Ringhals Sweden
Bo Sandin	Forsmark Sweden
Lars-Erik Häll	TVO Finland
Lars Engdahl	ABB Atom Sweden
Per Balldin	ABB Atom Sweden
Anders Ericsson	ABB Atom Sweden.

MORE

Other aspects which can be part of the new IAEA book are:

- Case examples for modernisation of:
  - components
  - systems
  - integrated I&C
- An example for a typical nuclear I&C configuration based on off-the-shelf products.

ABB Nuclear Power Plant Control System Structure - Overview

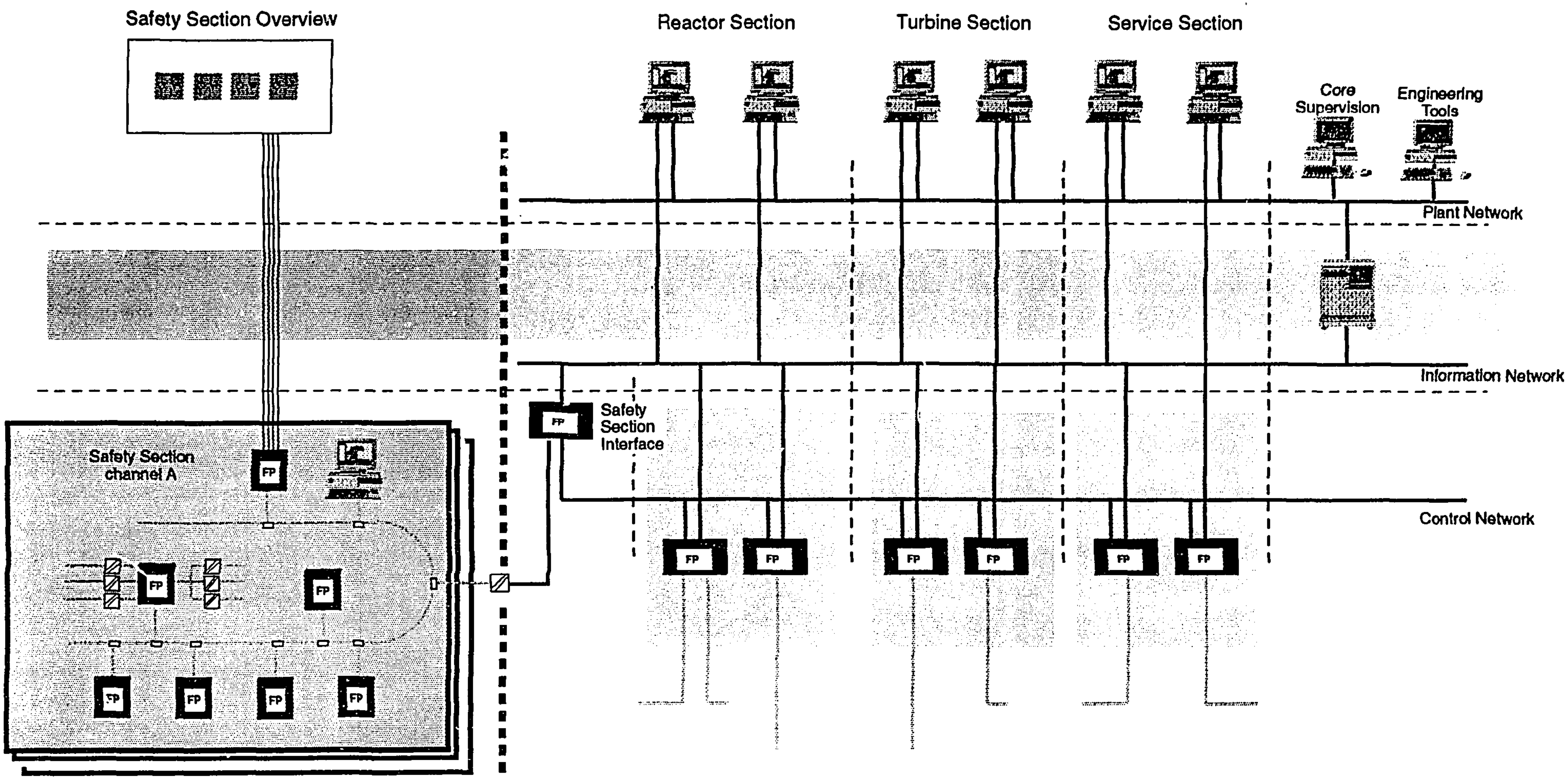


ABB *Nuclear Advantage*

ABB

ABB Nuclear Power Plant Control Room - Overview

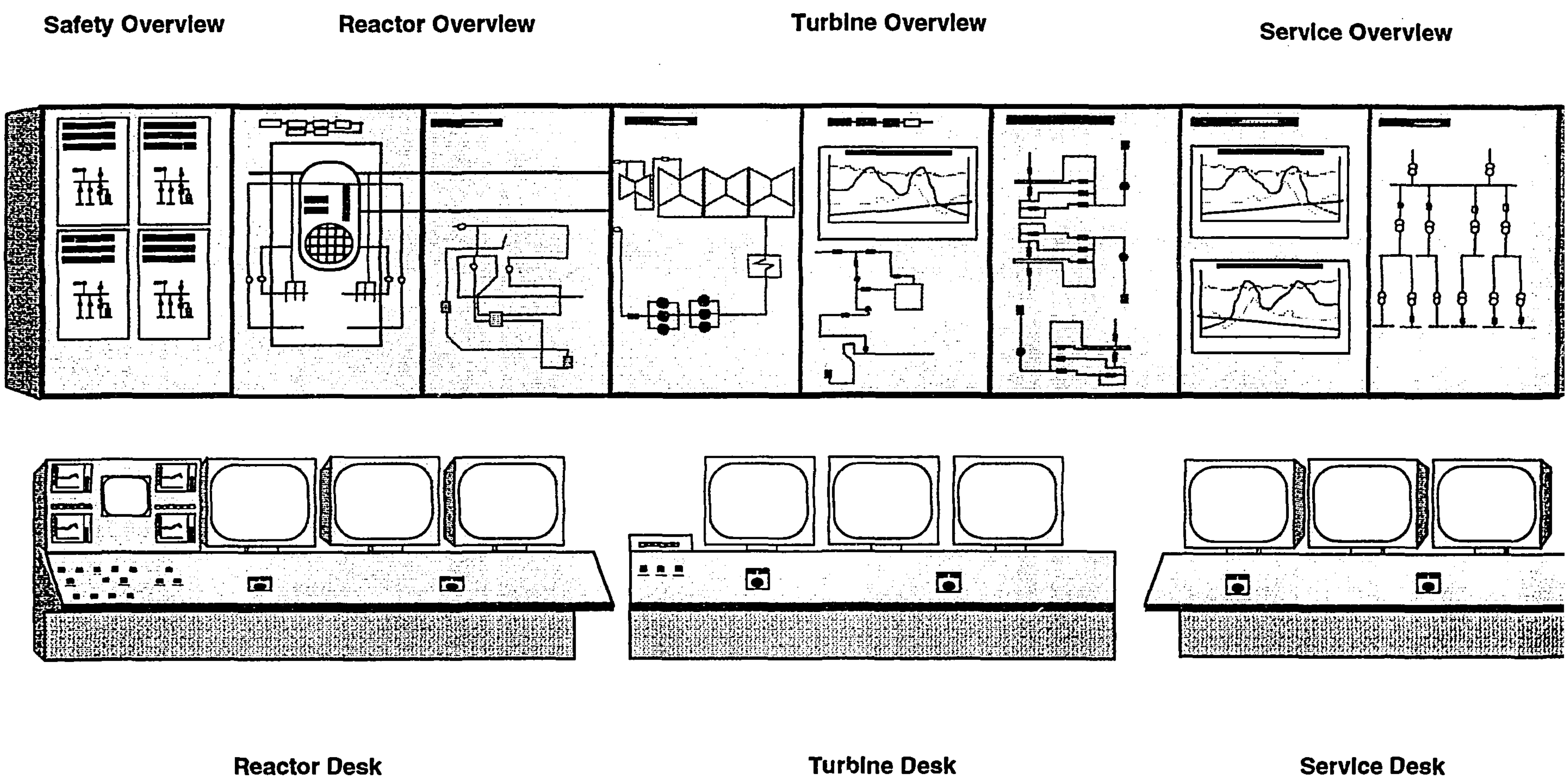


ABB *Nuclear Advantage*

The phases of the R2C Project

4 phases

definition of the Project Specifications (working group from April to July 1993)

Observation phase | **Basic Preliminary Project studies**

from 01/09/93 to 01/12/94

Synthesis
from 01/01/95
to 01/04/95

R2C Project

- **Start up decision : April 1993**
- **Aims :**
  - **to help in deciding to keep or to replace equipment groups**
  - **to identify the studies to be launched afterwards according to the results of the Project**
- **EDF Divisions involved**
  - **Generation and Transport Division (final client)**
  - **Engineering and Construction Division**
  - **Research and Development Division**
- **Participation of equipment suppliers**

Project management

- studies by equipment groups
  - the minimal set of equipment that cannot be split for the studies
- documents
  - approval process
- financial management
  - one reference as a national project
  - 3 kinds of budgets
    - ✳general studies
    - ✳studies entrusted to the Engineering Division
    - ✳studies entrusted to the Research and Development Division
- management of the man hours by account

Project organization

- Project manager : member of the Generation Division (final client)
- Observation phase manager : member of the Generation Division
- Basic Preliminary Project manager : member of the Engineering Division
- one Project Correspondent for each department or plant
- role of the suppliers :
  - preparing an answer for EDF concerning the feasibility of keeping and maintaining their equipment after the 2nd ten-yearly outage

Limits of the R2C Project

- equipment dealt with by the Project :
  - equipment for which replacement during a partial outage does not seem possible at first glance
  - other equipment closely linked to it
- main other concurrent studies to take into account :
  - reassessment of the nuclear safety of some 900 MW plants
  - Fire Protection Action Project (PAI)
  - studies related to the enhancement of computerized aids for operators

Strategic choices of the R2C Project

- priority : replacement of obsolete equipment
  - equipment that cannot be maintained until the 3rd ten-yearly outage
- keeping cables and relay racks
- implementation of renovations partially and step by step :
  - before, during and after the 2nd ten-yearly outage
- keeping a "traditionnal" control room

Content of the first phase

- writing :
  - the Specifications of the preliminary studies
  - the Project manual
- the Specifications detail the aims of the Project :
  - hypothesis
  - constraints
  - contents
  - results to be reached
- the Project manual details the operation of the Project :
  - organization
  - leading of the Project
  - management
  - for all the Divisions involved

Brief description of the control of the EDF plants

- 900 MW series (34 units)
  - electromagnetic relays for on/off automatic control
  - analog technology for closed loops control
- 1300 MW series (20 units)
  - on/off controls : programmable controllers
  - protection system : integrated digital system
  - closed loops control : programmable controllers (P'4) or analog systems (P4)
- 1400 MW series (4 units)
  - a fully computerized control room

Observation of equipment group X

- global behaviour
- visual examination
- difficulties encountered within the plants
- status of the stocks of spare parts
- support of the suppliers
- sensitiveness of the equipment to the obsolescence of components
- anticipation of ageing problems
- *inventory of functional modifications*
- identification of the margins
- keeping the qualification
- technical synthesis
- economic synthesis

Definition of observation phase

- AIM
  - to establish a technical and economic assessment of the feasibility and the actions to launch for keeping the equipment until the 3 rd ten-yearly outage
- LIMITS
  - in connection with the Basic Preliminary Project (APS)
  - the time and the schedule
- ACTIONS CARRIED OUT
  - specific to each equipment group
  - others

Observation phase : qualitative results

- good behaviour for
  - cabinets, wiring, electronic boards
  - proficiency level on plants
  - documentation statement
  - suppliers support including answers for components obsolescence
- good : these aspects have had low impacts on failure rate and no consequence on availability nor on safety

Observation phase : maintenance

- high availability of control equipment
  - except for some modules
  - higher risks with analog control equipment (not redundant)
- very few production losses due to the control equipment
  - mainly due to nuclear instrumentation system (RPN)
  - mainly due to human error during periodic tests or maintenance
- maintenance costs are relatively low :
  - higher for the oldest plants and for computerized aids
  - it seems they do not increase

Observation phase : other studies

- faster ageing than forecasted :
  - can be reduced by ageing tests carried out on strategic components
- supplier vanishing :
  - can be managed on a mid term for simple components
  - otherwise periodic assessment of the suppliers' health must be made
- unforeseeable losses can be mitigated by limited spare parts stocks

Observation phase : functional enhancement needs

- a very small number of functional needs for the 2nd ten-yearly outage
  - improvement in alarms processing and display
  - improvement in steam generators feedwater control
  - in addition for the oldest plants :
    - analog part of protection system
    - failure rate of nuclear instrumentation system (RPN) considered too high
- sufficient margins exist for integration of impacts due to non I&C modifications

Observation phase : actions to be launched

- some recommendations have been made about :
  - solutions to anticipate components obsolescence
  - the carrying out of ageing tests
  - the carrying out of exceptional maintenance interventions
  - the reducing of hot local spots on the boards
  - the improvement of repair quality

Observation phase : a good safety level

- Safety level is guaranteed by :
  - functionalities are unchanged
  - a reference file exists for each equipment group
  - a good initial qualification
  - periodic tests
  - good experience feedback
  - preventative maintenance
- if necessary, seismic tests will be made for single modules
  - performed on a whole cabinet
  - with up to date standards (IEC) with more severe criteria

Constraints of the Basic Preliminary Project (1)

- duration of the works : they must not increase the duration of the outages
- scheduling according to the type of outage :
  - to take advantage of the long outages
  - to schedule the works for one unit during one or several outages
  - to maintain operational systems and functions necessary during the outages
- a validation period must be respected on the first renovated unit (10 months)

Aims of the Basic Preliminary Project

- to establish a technical and economic assessment for the replacement of complete groups of equipment :
  - specification of a target architecture to be reached when all the possible equipment renovation will be performed
  - specification for renovation of each complete group of equipment
  - to establish a program for the assessment of more recent equipment available in the market

Contents of the Basic Preliminary Project

- description of the existing situation
- definition of the nuclear safety level to be reached for each group of equipment
- definition of the target architecture
- study for the renovation of each group of equipment
- study of the consequences in the main control room
- global study of the installation and the erection
- synthesis and optimization
- definition of the specifications for the renovation of each group of equipment

Constraints of the Basic Preliminary Project (2)

- constraints proper to each plant :
  - only one technical solution
  - to generalize the renovation quickly on all the units of the plant
  - decisions taken for the oldest plants may be different from the ones taken for the others
  - to avoid too many different types of equipment on the same unit
- keeping the principle of standardized plant series :
  - only one technical solution for the plants of the series

-166-

Safety approach

- only the equipment which will be upgraded is concerned
- conservation of present safety approach for 1E equipment
- case by case requirements definition for safety related equipment
  - comparison to the newest standardized plants series (N4)

Recommendations for the construction of the target architecture

- an integrated off-the -shelf system is recommended for :
  - controllers, computers, database management
  - off-the-shelf equipment must be assessed
- the necessary new functions must be integrated
- functions allocation in new equipment is almost unchanged

R2C Project : abstract

- most equipment has shown correct behaviour :
  - low failure impact on nuclear safety and availability
  - moderate failure rate
  - generally moderate maintenance costs
- a very few functional improvements
- the studies now carried out aim to minimize the impact on the existing equipment and control room

What is happening now ?

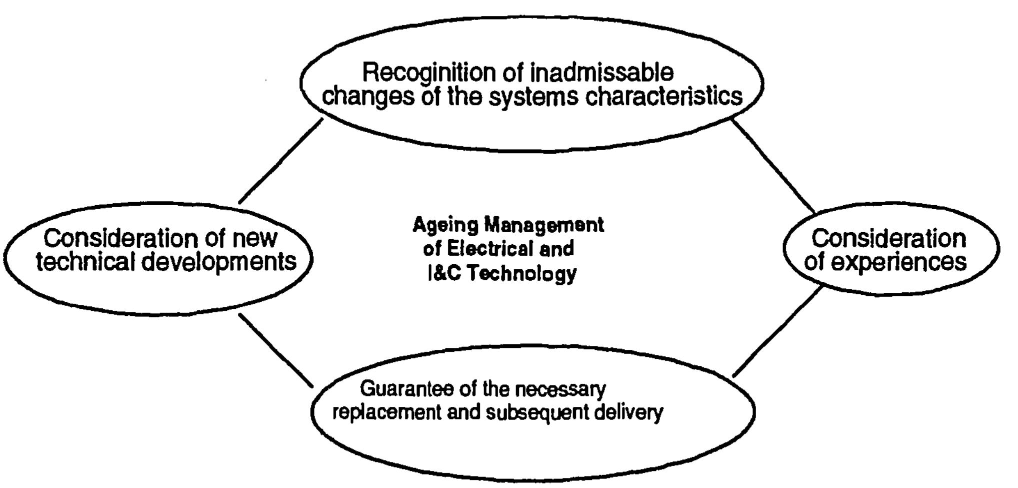
- steam generator feedwater control
  - bids are now under examination
- alarms
  - studies are in progress
  - smaller annunciators to replace some existing ones
- for the oldest plants :
  - protection system
    - improvement of the existing boards to withdraw hot spots
  - nuclear instrumentation system
    - writing of functional specifications with the help of the boiler vendor is in progress
    - use of digital technology ?
- works are scheduled for the 2nd ten-yearly outage

Ageing Diagnosis, Prediction and Substitute Strategies for I & C

R. Heinbuch, J. Irlbeck (Bayemwerk AG München)
W. Bastl (Institut für Sicherheitstechnologie GmbH Garching)

Measures for the maintenance and renewal of older instrumentation and control (I&C) technology are described regarding the technical standard in German nuclear power plants as it exists today. The basic duties and goals of the management of ageing, recognition of inadmissable changes of system characteristics and the guarantee of the required spares and replacement deliveries, taking into consideration experience and innovative progress, are illustrated using some basic examples, like the continuing resistance to accidents, use of computer-based digital I&C and alternative systems, e.g. application specific integrated circuits (ASICs).

Tasks and Goals of the Ageing Management in the Electrical (Electronic) and I&C Technology



1 Introduction

The German nuclear power plants that are in operation today were built in the years from the mid 60's till the end of the 80's. During this time, several I&C generations were developed by the industry which are used in the power plants today. With the exception of the process computer based information system, there are fixed wired electronic systems built up in discreet semiconductor technology. I&C of todays conventional power plants and backfittings in the conventional areas of nuclear power plants are principally being realized in digital I&C technology. In future, this technology will also be favoured by the supplier industry, so that the traditional I&C systems receive increasingly less supplier support.

The proof of functioning of the operational and safety relevant I&C is ensured by extensive repetitive tests. With these tests it was assumed until now that the proof for resistance to accidents, attained at the plant erection within the frame of the type tests with timelapsing ageing simulation, wouldn't have to be repeated for the remaining lifespan of those particular tested components. In the last couple of years extensive discussions and investigations took place, about the period of confidence of the accident resistance proof carried out within the frame of the type testing. The results of these tasks are recognized in the KTA-Regulations draft 3706 (13.06.1994). In this paper the consequences drawn for the repetitive proof of the LOCA (loss of coolant accident) proofness of I&C components of the safet system are discussed.

However, the ageing condition of the systems will not only be measured by whether the demands set at the time of construction are still fulfilled, but also whether today more efficien and more reliable systems are on hand than those used during plant construction. The experience gained from the renewal of these systems is described with the aid of concrete ex amples for enhancing of the man-machine interface and for improving the system availability. Furthermore, from the demands of the longterm functional upkeep of the ol I&C technology and the guarantee of subsequent delivery of suitable replacement systems, basic tasks result for the management of ageing.

2 Present situation

The production of the I&C technology as used when building the plants has practically come to a standstill. The supply of spare parts can momentarily only be assured by way of special productions, reserve of spares, new generation of instruments with similar properties. These special productions live from a stack of components (transistors, diodes, etc.) which is not refilled anymore. In our opinion, the availability of the remaining stocks and the arising costs thereof are not determinable anymore.

Ageing effects are noticeable in the older plants (drift phenomena, electrolyte capacitors). The failure rates still lie within the normal range. Until now, the maintenance measures needed for the functional upkeep, could still be executed with reasonable expenditure in the old technology.

The exchange of the I&C systems will be necessary up to three times during the lifespan of the power plants. Exchange actions are currently performed. For I&C expansions in the operational and safety relevant areas (requirement class 3), computer based digital I&C systems are basically being engaged. It is to be expected that an increasing need for suitable new I&C systems will arise, with which the safe and reliable continued operation of the power plants can be secured.

2.1 Proof of the functional capability

2.1.1 Recurring tests

The proof of the required functional capabilities and constancy in use of the electrical and I&C components is performed during manufacture, construction and commencement of operation. The preservation of these characteristics is being proven by repeated testing, which is carried out either during operation or shutdown of the plant.

These tests require a relatively large personnel effort, if testing has to be manually. So, as far as possible, automatic testing equipment is used. As a rule computerized testing aids are used to which high quality requirements are made. Of course, special attention is paid to the software.

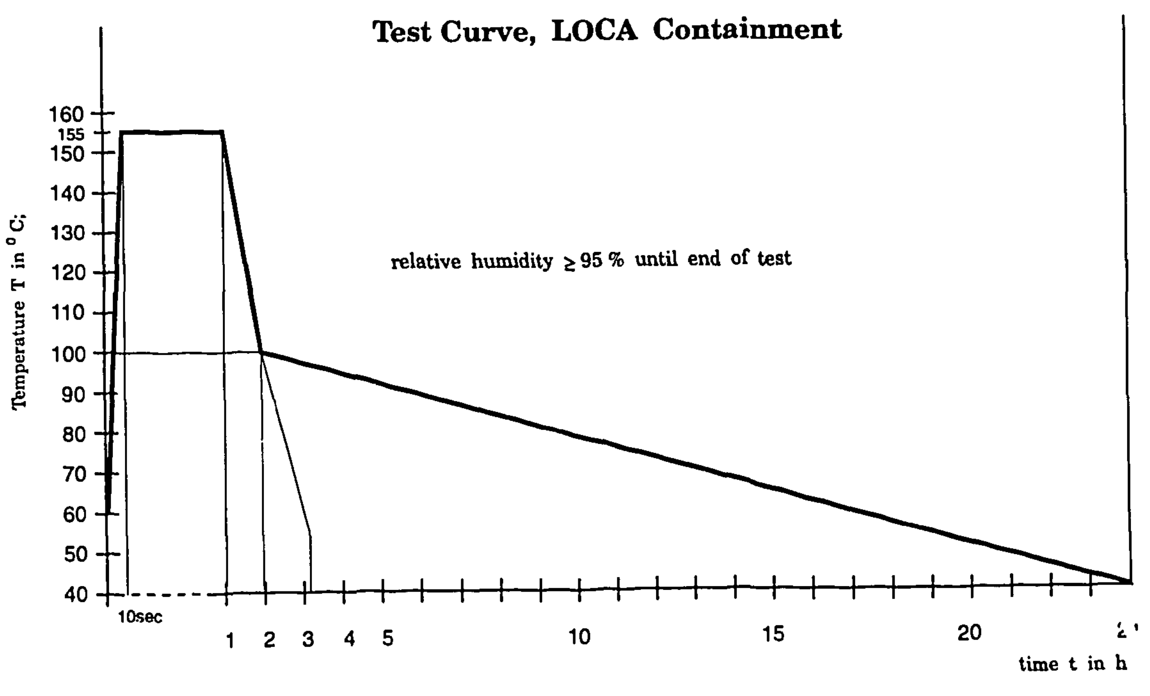
2.1.2 Proof of the resistance to accidents

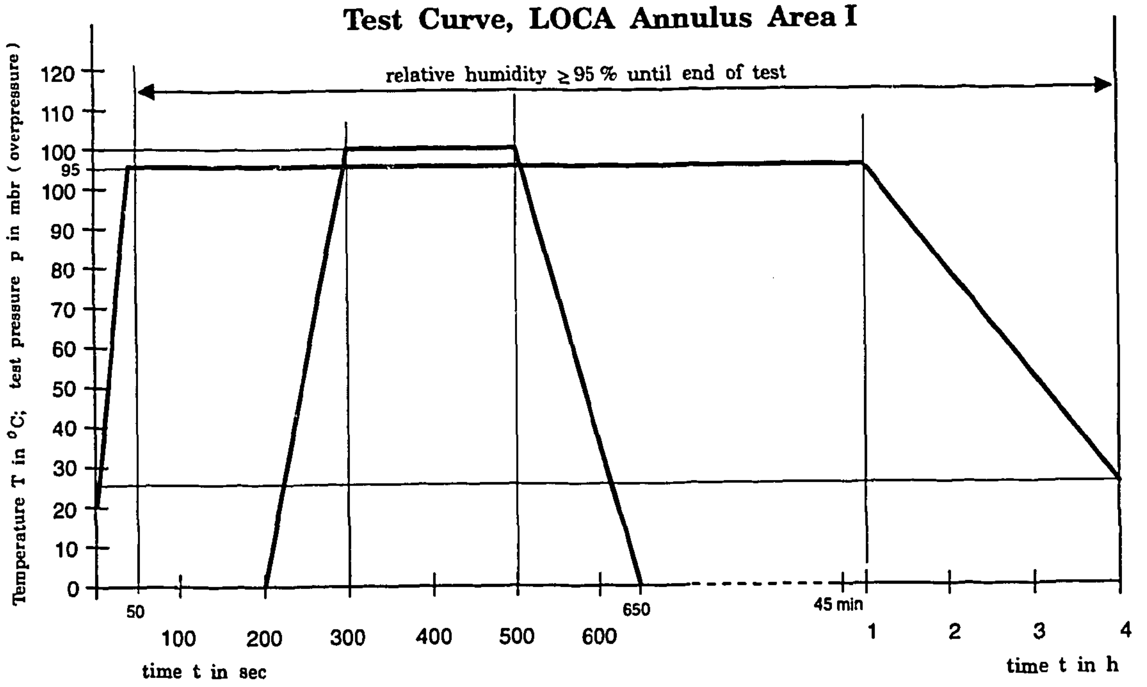
It was already clear during construction of the plant, that a complete repetitive test for the preservation of performance under accidental conditions on the built-in components could not be considered.

Therefore the following measures had to be observed, in order to achieve the longterm performance with respect to the accident resistance of electrical and I&C components, within the frame of the plant specifications:

- application of suitable materials with regard to the expected operational temperature and radiological dose rate at the installation sites.
- construction related measures regarding mechanical stability and humidity protection
- experimental proof within the framework of type and suitability tests on artificially preaged specimens.

An essential part of the type tests is the experimental reproduction of the stress under accidental conditions on corresponding specimens. Test curves have been defined on the basis of accidental sequences simulated as realistically as possible. In the following diagrams, the presently used test curve for the LOCA in the containment and those for the LOCA in the annulus area I are shown.





Both curves can be used for the qualification of I&C components in the corresponding PWR and BWR building areas (containment, PWR-annulus or reactor building areas outside the containment for the BWRs). A single proof demonstrating lower values at the respective installation site is thereby not excluded. Also, shortly before expiration of the working lifetime of the components it should be assured by means of preageing within the framework of the type test, that the experimental proof is still valid.

Especially for synthetics it has not been possible to achieve valid theoretical ageing predictions. Because of time and expenditure for the simulation of 40 years of reactor operation, accelerated artificial preageing was carried out in periods of up to one year. Such an accelerated thermal and radiological preageing can be too short for the age dependent decomposition of synthetics, because, e.g., the oxidation process of oxygen cannot be simulated realistically enough in this short period.

A reduction of accelerated artificial preageing may become useless if, during or shortly after completion of the type test, further developed modern instruments are already on the market.

For all these reasons the continuing resistance to accident conditions of the I&C components should be secured during their operation. Prerequisite is a basic accident proof design in the sense of the abovementioned measures.

2.2 Preservation of the accident resistance

The accident resistance of the concerned electrical and I&C components must be secured during the entire life cycle of the plant. From todays knowledge, the thermal and radiological preageing methods from the type tests do not cover an operating period of 40 years safely. Hence it needs to be ascertained, if a still sufficient accident resistance is given.

Thereby, the inspection performed after a certain time for the actuators of older plants, was focused especially to valve positioners, magnetic positioners including the matching cables, plugs, terminals and containment penetrations. It was discussed that different components of the older generation within the containment were to be proven through corresponding special testing to preserve their accidental resistance. But because better and more suitable components are available in the meantime, for example motor positioners, magnetic positioners, terminals and penetrations, these components were exchanged.

The exchange was supported by aspects like:

- future delivery of older equipment only with higher expenditure guaranteed
- rechecking of valve specification and design
- proof deficiencies from the type test, especially for penetrations

For the motors required during a LOCA in the annulus, theoretical proof showed that by the temporarily rising environmental temperatures in the annulus no undue shortening of the lifespan of the windings was to be expected.

At the moment the transducers of the oldest generation for the reactor safety instrumentation, are being exchanged for more suitable ones. The advanced age of the mechanical gauges and electrolytic condensors were reasons for this exchange.

Within the framework of the revision of positioners (8 year period), on-site tests for leaks in the housing of the switches were performed for accident proof positioners of the next generation.

On detection of undue leaks, cable connections including grouting were changed. Together with the rules given in the specification (like changing of seals, oil and lubricants) as well as the recurring tests regarding the mechanical forces, it has been and is being secured that these valve positioners retain their accident resistance up to the next revision. From our point of view, as long as the delivery of the positioners and subparts is secured under reasonable conditions in future, then these can be operated using this procedure for a long time without ageing problems.

For a particular cable type used in our plant, a R&D program of the manufacturer has come up with a noticeable radiation dosis effect after a few years of in plant use. Within the framework of special tests on I&C cables, which are in use near the primary circuit of the plant, and which were further preaged in order to obtain a representative ageing profile on the primary circuit, the load limit regarding dose rate was established by the manufacturer. Cables in locations near loops, which have reached or are reaching their load limit because of operational radiation dose rates such that they cannot withstand the dose due to a subsequent loss of coolant, have been exchanged for more suitable cables.

Tests on selected 61 pole resin penetrations carried out within a special test using realistic conditions for a computed accident course (BWR) gave a satisfactory seal tightness. Further tests with 4 pole resin penetrations ar planned.

Especially through exchange but also through the theoretical proof, as well as partially performed special tests, also within the framework of the prescribed component revisions, the preservation of the LOCA stability has been ensured also for the older component generation.

Therefore, there exists at this time for all component generations considerable confidence periods. Proof for the preservation of accident stability must be given in time before the expiration of these confidence periods, be it by theoretical proof, special tests, substitute tests, parts or component exchange or combined procedures. A significant part is played by the measurement of the stress due to real temperature and radiation at the location of the component in order to obtain the real ageing. This can be done through subsequent use of, e.g., analyn dosimeters and max thermometers over a reactor cycle with a follow-up extrapolation over past and future time spans. Recent measuring results on BWR (penetrations) are available and are being evaluated at the moment.

Further research and development programs for proof procedures have been initiated.

2.3 Research and development programs

Experience so far shows, that accident proof I&C components of the older generation have mostly been exchanged, also for other reasons like ageing effects and shortcomings in the type tests. This experience, however, does not contradict that certain electrical and I&C components can remain in use for periods which lie in the range of the life expectancy of the whole plant. An exchange of all accident proof cables or large components like motors is not necessary because of the small accident stress.

For this reason, for equipment which is basically qualified as accident proof it seems appropriate to develop procedures which make possible an in-use control about the preservation of the accident proofness. In a VGB working group such activities have taken place since 1988.

Parallel to this utility working team, the completion of KTA 3706 "Recurrent proof of the accident resistance of electrical and I&C components of the safety system" was forced. Besides the already mentioned possibilities of exchange of components, two further paths are kept open in this KTA standard for proving the preservation of accident stability, i.e. substitute and special tests.

In the course of the substitute tests, construction parts which have to cope with accidents should be tested locally by means of relevant procedures like spraytesting, dive-pressure tests etc.. The execution of spraytesting on terminals has been assured experimentally by the manufacturer on order of the VGB working group. The associated procedure (VESPA) is being assessed at the moment by TÜV Rheinland. Further substitute tests cited by KTA are sealing and heating tests.

In the special tests, the relevant steps of type testing have to be repeated. For this, specimens have to be taken from the plant, for example three or six specimens, in order to form a large enough sample.

In both procedures, care has to be taken on how to assure a large enough load precursor, either by testing in a shorter time span (substitute testing) or by application of additional artificial ageing.

TÜV Nord investigated the ageing and the lifetime of electrical equipment of the safety system and the accident instrumentation in nuclear facilities under operational conditions. Apart from exceptions they observed no ageing relevant changes in the failure behaviour of the investigated nuclear power plant components. Regarding valve positioners and magnets aged in use, there exist safety margins under accident conditions. Further relevant results were:

- electronic components have an innovation cycle which, with the exception of a few parts, is shorter than the residence time
- the basis for assessing the ageing behaviour of accident proof, electrical components was not enough

It is planned to continue this project with the cooperation of the utilities.

According to KTA 3706, the point in time for the start of the recurring tests of the LOCA proofness is to be fixed for each nuclear power plant. Test instructions must be set up before the test begins and they must be approved by independent experts. The testing strategies, relating to component groups which should be put down in the test instructions, are being worked on by a VGB working group.

The VGB in continuation of his research and development project on cables has given specific aims to the plant manufacturer.

The setting up of testing strategies is still in the beginning phase. In order to reach meaningful procedures first of all adequate component samples must be established for all facilities.

3 Strategies for maintenance and renewal of old I&C

To preserve the function of older I&C systems, so far required a reasonable effort for all facilities in Germany. In spite of not foreseeing a drastic aggrevation for the delivery situation regarding the old I&C technology, foresight strategies must be developed to ensure the longterm preservation of I&C performance.

From a current view the following alternatives can be seen for the renewal of the old I&C systems:

- spare part keeping and special productions for old I&C systems (current practise)
- substitution of old I&C through new digital I&C for operational systems (partially practised)
- use of new digital I&C for safety systems
- substitution of old I&C by means of functionally equivalent circuitry which is realised in modern micro electronics (ASICs).

3.1 Spare part keeping and special productions of old I&C

This method is currently being practised especially in the area of safety relevant I&C. The quality assurance of the manufacturers and the observation of the statistical failure behaviour of the old I&C is being intensively supported by common actions of the utilities within the framework of the VGB (working group "Qualification of electrical and I&C components" and working group "I&C failure statistics").

In spite of the fact that failure behaviour is currently still normal, and that the delivery o spares is still assured to a large extent, in the mediumterm one must count on the renewal of these systems in the old plants.

3.2 Digital safety systems

Digital I&C for the application in safety systems has been developed or is being develope in several countries. In Germany, Siemens/KWU, with the support of the German utilities, has developed TELEPERM XS for the longterm exchange of old safety I&C technology and TELEPERM XP for operational systems.

An assessment of the TELEPERM XS concept performed by GRS has established its suitability for use in nuclear facilities under highest safety demands.

For the PWR plants GKN1 and KKU, it is planned to replace the rod control and limitation system. The technical specifications for these systems will be delivered to the customer in the near future, they are also the basis for the licensing procedure. TELEPERM XS will also be offered to the high flux research reactor FRM-2 at Garching.

Furthermore, TELEPERM XS will be used for the safety systems in Rovno. It is in the manufacturing process and installation is presently planned for the end of next year. The new system has also been offered to PAKS in Hungary.

Presently, type-testing of the system components is being performed. It will be completed by the end of this year. For these particular tests, the basic requirements for traditional systems (as laid down in the KTA rules) were followed. According to these rules, there are:

- theoretical checks (e.g. regarding functional description, specification, load)
- practical checks (e.g. regarding functionality, electromagnetic compatibility, environmental conditions).

In analogy to these traditional rules, type-testing has been also applied to the new digital system. This was possible because

- the system (regardless of its specific application) consists of approximately the same hard- and software components
- the system applies re-usable software components (configurable and parameterised according to plant specific needs)
- hard- and software interfaces can be uniquely and completely described.

For software components, the following analyses have been performed:

- assessment of the development process and its measures for quality assurance
- trace of functions from requirements definitions via software specification, design, implementation to the code by desk inspection and static analysis
- verification of software interfaces

- conformity with standards, mainly IEC 880
- conformity with project internal guidelines
- assessment of failure and error analysis

Finally, a system type testing is performed to check the typical system properties:

- correctness of operational behaviour
  - correct functional behaviour
  - no feedback of fuctions with respect to other functions
  - temporal behaviour
  - deterministic behaviour of the system (reproducible results)
  - ability to be assessed, maintained, diagnosed
- tolerable stress and failure behaviour
  - failure and error tolerance
  - independent behaviour of the I&C system from the technical process (resistance to input data overload)

3.3 Renewal of old safety relevant instrumentation and control by copy of function equivalent circuits (ASICs)

The use of ASICs could be another solution for the replacement of old I&C. The development of micro-electronics has led to revolutionary changes in the production of electronic systems. This means in micro-electronics, a large amount of circuits can be built up monolithically (on the silicium basis), in contrast to old I&C, where the single parts (transistors, diodes, resistors, condensors) are put onto printed circuit boards.

These developments, which worldwide are used in great numbers, open up a new perspective for the renewal and extension of old instrumentation and control systems. In this new technology of micro-electronics, the switching circuits of the old I&C are copied exactly, i.e. a new integrated circuit "made to measure" is produced.

The application of ASICs offers the following basic perspectives:

Safety

- the user-proven fixed switching structures remain
- parallel signal processing
- optimal protection against unnoticed changes
- high degree of integration (therefore fewer contacts)
- design and testing tools proven in mass fabrication
- software problems reduced because only basic procedures of automation theory is being used during design.

Functionality

- all required analog and binary signal functions can be realized
- the interface to the computer can be directly intergrated
- the test logic can be integrated directly onto the chip
- a high function density and consequently a small volume can be obtained

Compatibility/Flexibility

- pin-compatible assemblies can be realized
- the required flexibility for the protection function during the planning can be ensured through design tools

At the moment, the VGB Working Group "I&C in NPPs" is testing the possibility of applying ASICs to replace old instrumentation and control systems. The applicability is being tested in a pilot utilization. It is expected that qualification requires less effort in relation to software solutions.

4 Improvement of performance through the new instrumentation and control technology

A system can be out of date in spite of it still fulfilling the originally specified properties. This is especially true for areas where today much more powerful systems are available and an improvement of plant availability or plant safety can be achieved.

The following measures (already taken in several German NPPs) can serve as examples for such improvements:

- the exchange or expansion of plant computers are realized in most plants which are older than 10 years. The marked aims of these measures are
  - improvement of the man-machine interface
  - improvement of plant disturbance diagnosis
  - expansion of the extent of information
- renewal of the refuelling platform with the aim of
  - improving the functionality and the man-machine interface
- renewal of the turbine I&C with the aim of
  - improving the availability and the man-machine interface.

5 Summary

The main aims of the tasks for the ageing management in the electrical and instrumentation and control technology are in the longterm preservation of function while considering technical development, experience and the guarantee of relevant continuing deliveries.

The functionality is proven by means of repetitive testing. A special problem is the proof for accident resistance. In extended research and development programs, solutions have been achieved which have been taken up in the KTA rule 3706.

For the longterm preservation of the function of instrumentation and control, strategies fo the replacement of old I&C systems are required. The tendency is to replace old I&C

technology in the area of process instrumentation and control and safety relevant instrumentation and control by computer-based systems.

The new digital safety instrumentation and control technology requires, like any computer based system, a high degree of formality to describe the process relevant demands. When defining these demands, experience and latest developments can be used for improvements.

On the other hand the establishment of the formal descriptions and their assessment require a high effort. Therefore further alternatives for the replacement of old instrumentation and control technology is being searched for, where the development of the new system is based on the proven circuit design of the old I&C. In this context ASICs appears to provide promising solutions.

The use of the new I&C technology contributes today in essential areas of nuclear power plant instrumentation and control to the improvement of performance, e.g. with regard to the man-machine interface and the diagnostic abilities.

Department of Nuclear Energy and Safety
Division of Nuclear Power

Issue No. 3
29 March 1996
621-12-AG-928

NOTIFICATION OF AN AGENCY SPONSORED MEETING

Title of meeting: Advisory Group Meeting on "Modernization of Instrumentation and Control Systems in Nuclear Power Plants"

Opening Meeting: 9:30 a.m.

Dates, inclusive: 25-29 March 1996

Scientific Secretary:
A. Kossilov, A2543, X22796

Place: IAEA Headquarters
C07, Mtg. Room No. II, X4641

Secretary:
R. Wehofsitz, A2549, X22801

PARTICIPANTS AND PARTICIPATING MEMBER STATES AND ORGANIZATIONS	ADDRESSES Official Mailing Address	Temporary Address	FOR THE PERIOD
BULGARIA Mr. V. MILIOVSKY	Committee on the Use of Atomic Energy for Peaceful Purposes Nuclear Facilities Department 69 Shipchenski Prokhod Blvd. 12574 Sofia Tel.: 70 05 14 Fax: 3592 702143		25-29 March 1996
CZECH REPUBLIC Mr. Č. KARPETA	State Office for Nuclear Safety Dept. of Nuclear Systems and Components Slezska 9 120 29 Prague 2 Tel.: 42 2 2417 2445 Fax: 42 2 2417 2627		25-29 March 1996

PARTICIPANTS AND PARTICIPATING MEMBER STATES AND ORGANIZATIONS	ADDRESSES Official Mailing Address	Temporary Address	*FOR THE PERIOD*
FINLAND Mr. B. WAHLSTRÖM	Technical Research Centre of Finland VTT Automation Otakaari 7B P.O.Box 13002 FIN-02044 VTT Tel.: + 358 0 4566400 Fax: 358 0 4566475 E-mail: Bjorn.Wahlstrom@.vtt.fi		27-29 March 1996
FRANCE Mr. DALL'AGNOL	EdF-SEPTEN 69628 Villeurbanne Cedex 12-14 avenue Dutrievoz Tel.: 33 72 82 72 28 Fax: 33 72 82 77 04		25-29 March 1996
GERMANY Mr. W. BASTL *Chairman*	Institute for Safety Technology (ISTec) GmbH Forschungsgelände D-85748 Garching b. München Tel.: (089) 32004-531 Fax: (089) 32004 300		25-29 March 1996

PARTICIPANTS AND PARTICIPATING MEMBER STATES AND ORGANIZATIONS	ADDRESSES Official Mailing Address	Temporary Address	FOR THE PERIOD
HUNGARY			
Mr. Z. TOTH	Head of Process Computer Department Paks Nuclear Power Plant Postfach 71 7031 Paks Tel.: (36) 75 31 85 47 Fax: 36 1 553 894 E-mail: Tothzs@tea.mailgate.npp.hu		25-29 March 1996
KOREA, REP. OF			
Mr. Chang-Hwoi KIM	KAERI P.O.Box 105 Yousong, Taejon 305-600 Tel.:+ 42-868-2927 Fax: + 42-868-8357 E-mail: Chkim2@nanum.kaeri.re.kr		25-29 March 1996
Mr. In-Soo KOO	KAERI P.O.Box 105 Yusong, Taejon 305-600 Tel.: + 42-868-2905 Fax: + 42 861 1388 E-mail: Iskoo@nanum.kaeri.re.kr		25-29 March 1996
RUSSIAN FEDERATION			
Mr. A.G. CHUDIN (Observer)	Ministry for Atomic Energy Staromonetny 26 109180 Moscow Tel.: (095) 239 27 95 Fax: (095) 233 30 53		25-29 March 1996

-187-

PARTICIPANTS AND PARTICIPATING MEMBER STATES AND ORGANIZATIONS	ADDRESSES: Official Mailing Address	ADDRESSES: Temporary Address	FOR THE PERIOD
RUSSIAN FEDERATION (cont.)			
Mr. A. POBEDONOSTSEV	OKB Mechanical Engineering 603603 Nizhny Novgorod Byrnakovsky proezd, 15 Tel.: (8312) 418902 Fax: (8312) 418772		25-29 March 1996
SLOVAK REPUBLIC			
Mr. J. DOLEŽAL (Observer)	NPP Mochovce 935 39 Mochovce Tel.: 0042-813-36-3994 Fax: 0042-813-391		25-29 March 1996
Mr. V. HORVATH (Observer)	Mochovce NPP 93539 Mochovce Tel.: 0042-813-36-3992 Fax: 0042-813-391-128		25-29 March 1996
Mr. S. UŠKERT (Observer)	Mochovce NPP 935 39 Mochovce Tel.: 0042-813-36-3603 Fax: 0042-813-391 128		25-29 March 1996
SPAIN			
Mr. J.A. ARBIZA BERREGUI	INITEC Gran Via Carlos III-124-3° 08034 Barcelona Tel.: 34-3-2050862 Fax: 34-3-2054908		25-29 March 1996

-188-

PARTICIPANTS AND PARTICIPATING MEMBER STATES AND ORGANIZATIONS	ADDRESSES Official Mailing Address	Temporary Address	FOR THE PERIOD
SWEDEN			
Mr. P. van GEMST	ABB Atom AB Nuclear Services Division S-721 63 Vasteras Tel.: 46 (0) 347035 Fax: 46 (0) 347318 E-mail: Atopage@qm.ato.abb.se		25-29 March 1996
U.K.			
Mr. R. CLARKE (Observer)	Nuclear Electric plc. Barnett Way Barnwood Glochester GL4 7RS Tel.: (1452) 653177 Fax: (1452) 552 600		25-29 March 1996
Mr. N. WALL	Nuclear Installations Inspectorate St. Peters House Stanley Precinct Bootle, Merseyside L20 3LZ Tel.: 0151 951 3193 Fax: 0151 922 5980, 0151 951 3942		25-29 March 1996
UKRAINE			
Mr. M.A. YASTREBENETSKY	Ukrainian Committee of Nuclear and Radiation Safety Scientific Technical Center, I&C Dep. Artema str., 17 Kharkov 310078 Tel. + fax: 380(572)471700		25-29 March 1996

PARTICIPANTS AND PARTICIPATING MEMBER STATES AND ORGANIZATIONS	ADDRESSES: Official Mailing Address	ADDRESSES: Temporary Address	FOR THE PERIOD
U.S.A. Mr. J. NASER	Electric Power Research Institute Nuclear Power Division 3412 Hillview Avenue P.O.Box 10412 94303-0813 Palo Alto Tel.: (415) 855-2107 Fax: (415) 855-2774 E-mail: jnaser@msm.epri.com	Hotel Pension Elite Wipplingerstr. 32 A-1010 Vienna Tel.: 533 25 18-0 Fax: 535 57 53	25-29 March 1996
I.A.E.A. Mr. A. KOSSILOV Scientific Secretary	Division of Nuclear Power Reactor Engineering Section P.O.Box 100 Wagramerstrasse 5 A-1400 Vienna Room No. A2543 Tel.: + 43 1 2060 22796 Fax: + 43 1 2060 7 E-mail: Kossilov@nepo1.iaea.or.at		

PARTICIPANTS AND PARTICIPATING MEMBER STATES AND ORGANIZATIONS	ADDRESSES Official Mailing Address	Temporary Address	FOR THE PERIOD
I.A.E.A. (cont.)			
Mr. M. DUSIC	Division of Nuclear Installation Safety Safety Assessment P.O.Box 100 Wagramerstrasse 5 A-1400 Vienna Room No. B0872 Tel.: + 43 i 2060 22522 Fax: + 43 1 2060 7 E-mail: Dusic@nepo1.iaea.or.at		

c:\wpwin\kossdocs\ag928.ntf