ADVANCED I&C SYSTEMS FOR NUCLEAR POWER PLANTS

H.-W. BOCK, A. GRAF, H. HOFMANN
Siemens AG,
Erlangen, Germany

Abstract

Advanced I&C systems for nuclear power plants have to meet increasing demands for safety and availability. Additionally specific requirements arising from nuclear qualification have to be fulfilled. To meet both subjects adequately in the future, Siemens has developed advanced I&C technology consisting of the two complementary I&C systems TELEPERM XP and TELEPERM XS. The main features of these systems are a clear task related architecture with adaptable redundancy, a consequent application of standards for interfaces and communication, comprehensive tools for easy design and service and a highly ergonomic screen based man-machine-interface. The engineering tasks are supported by an integrated engineering system, which has the capacity for design, test and diagnosis of all I&C functions and the related equipment. TELEPERM XP is designed to optimally perform all automatic functions, which require no nuclear specific qualification. This includes all sequences and closed-loop controls as well as most man-machine-interface functions. TELEPERM XS is designed for all control tasks which require a nuclear specific qualification. This especially includes all functions to initiate automatic countermeasures to prevent or to cope with accidents. By use of the complementary I&C systems TELEPERM XP and TELEPERM XS, advanced and likewise economical plant automation and man-machine-interfaces can be implemented into Nuclear Power Plants, assuring compliance with the relevant international safety standards.

1. CONCEPT

A process control system covering all automation tasks in nuclear power plants requires equipment for automation, communication, operator control and monitoring, engineering, diagnosis and maintenance. The features of this equipment and the manner in which it interacts characterize the process control system. As innovation cycles in software and hardware development become shorter, process control systems will only have any chance on the market in future if they are based on standards because standards usually have a longer life than individual components. For this reason the extensive use of standards was determined as fundamental principle of the common concept behind TELEPERM XP and TELEPERM XS.

However, because standard components are naturally unable to cover all the requirements specific to power plant I&C, it is necessary to superimpose specific characteristics. This is done in a way that is transparent to the user by means of engineering tools which together form an engineering system. This allows unrestricted exploitation of the technical and cost advantages associated with the use of standards while enjoying a previously unavailable comfort during engineering, maintenance and diagnosis as well as consistency in documentation.

2. ENGINEERING, MAINTENANCE, DIAGNOSIS

The central interface between the equipment for automation, operator control and monitoring, and communication and the personnel responsible for running the I&C system is the engineering system. It is an integral part of the I&C system and supports not only engineering tasks but also maintenance and diagnosis of all I&C components, i.e. both the plant specific software functionality for automation, operator control and monitoring, communication and the hardware functionality of the entire I&C system. The most important feature is that all activities - the specification of the control functions as

well at the design of the hardware architecture - can be performed through the same graphic user interface by means of standardized symbols.

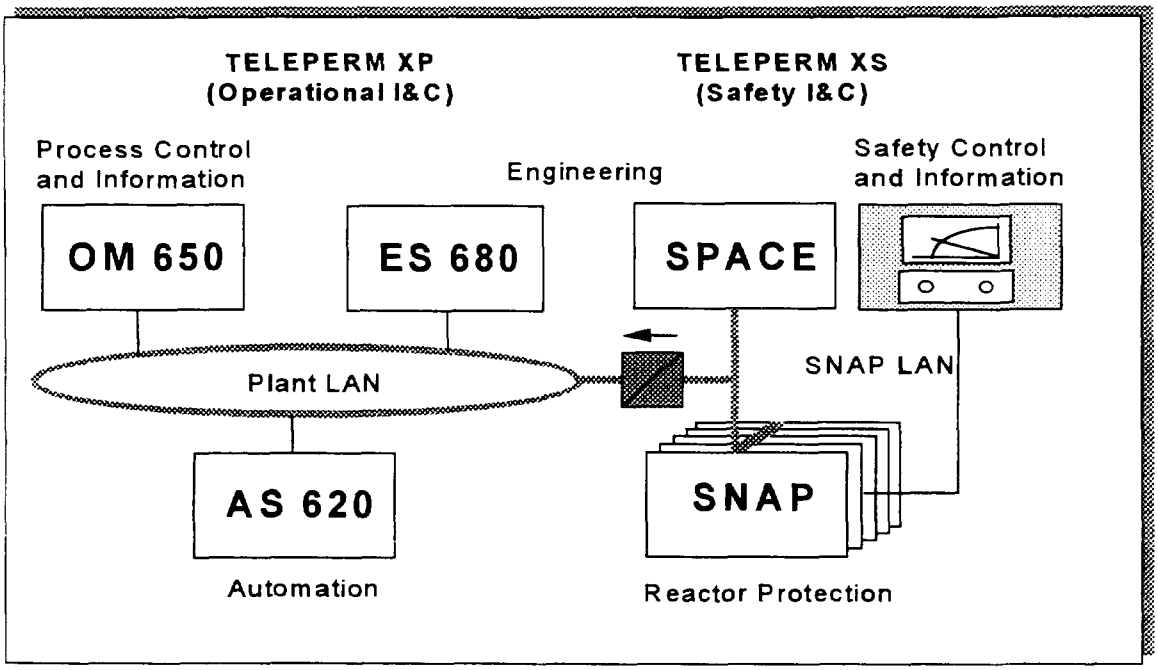

FIG. 1 Advanced I&C systems for nuclear power plants.

This means that the entire plant-specific functionality of the hardware and the software is specified in graphics using the engineering system and stored centrally in a database. To enhance clarity the engineering tool supports hierarchical structures with several levels. The engineering data created as part of the normal plant design serves as a reference for all further activities. It is used not only to derive the construction documents for cabinet fabrication but also to automatically generate the entire plant-specific software code. It also forms the basis of complete function- and location-oriented documentation, thereby ensuring that the documentation of all components of the I&C system is always up to date and complete. The graphic user interface behind which the specific data and mechanisms of the I&C system are concealed is in itself an important step into the future and permits the process engineer to specify the functional requirements on the I&C system without any software knowledge.

Although an integrated engineering support considerably simplifies commissioning, the real advantages of the engineering tool become apparent later when the plant is in operation. The strong consistency of the plant documentation with the I&C functionality actually implemented, which is ensured by the consistent use of strict feedforward documentation, is especially important if frequent modifications and expansions are required during the plant operation time. The engineering system is also used for maintenance and diagnosis during operation of the I&C system. For example, internal states such as fault signals from modules or simply the current values of variables can be scanned and visualized on the graphic user interface of the engineering tool. Furthermore overview pictures describing the I&C structure together with the ergonomic user interface assure quick and direct identification of all module faults, so that specific repair measures can be taken in time and service costs reduced.

3. OPERATOR CONTROL AND MONITORING

Operator control and monitoring of the process is performed using the process control and information system. It is characterized by a client-server concept based on international standards that permits distribution and scaling of the functionality in a way that no other architecture can. Clients and servers communicate via a common, open terminal bus so that all information is available everywhere. This permits adapted implementations, ranging from low-cost minimum configurations as they are necessary for example for local control stations up to screen-based complete control rooms with overview displays and one or more control consoles.

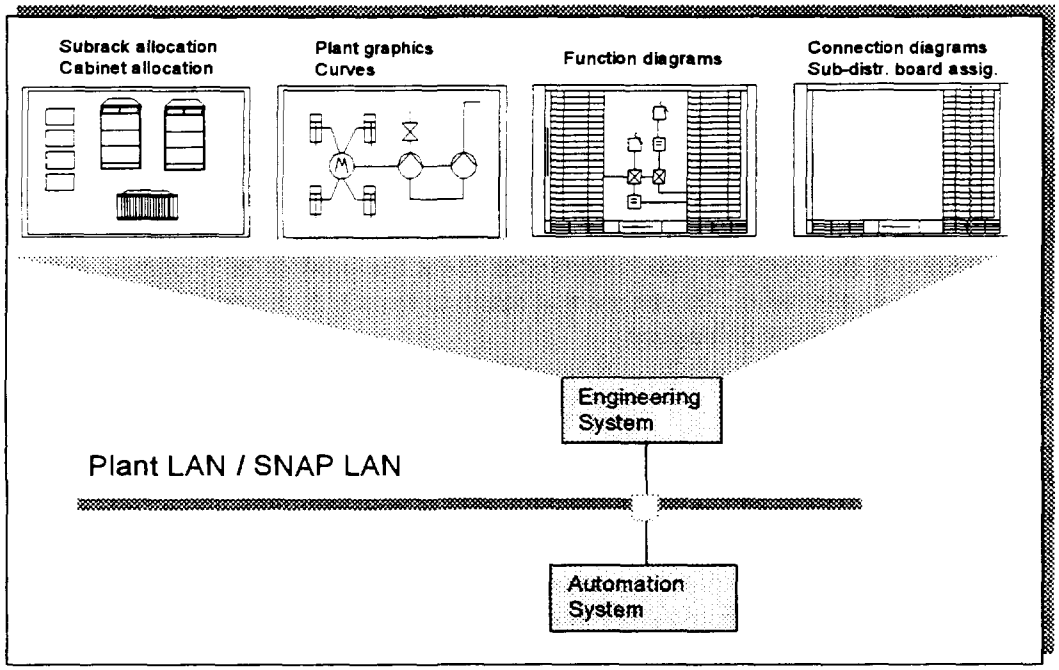

FIG. 2 Tasks of the engineering system.

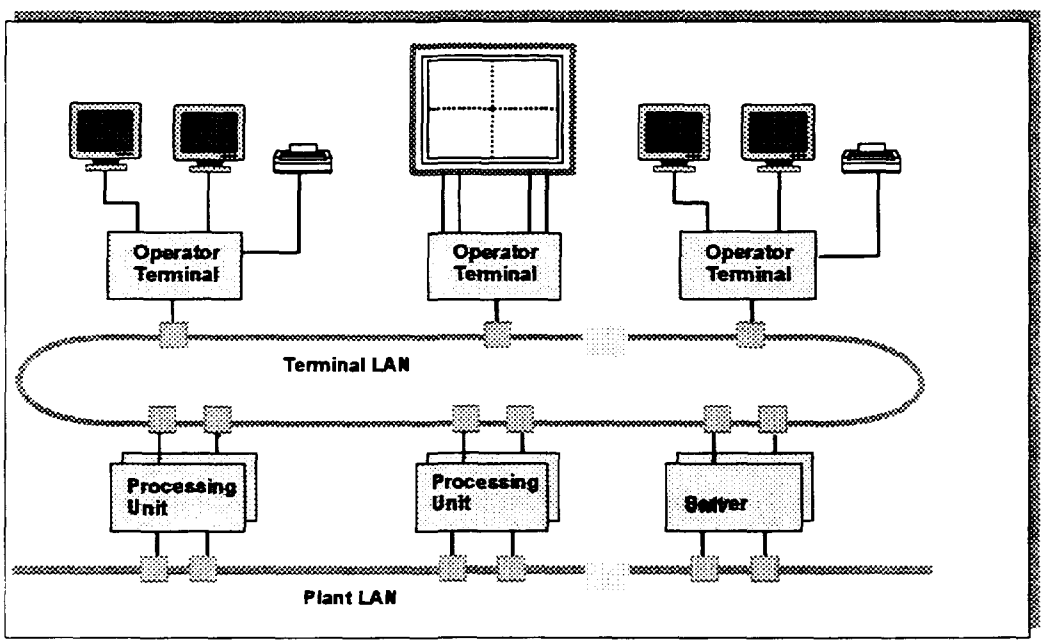

FIG. 3 TELEPERM XP process control and information.

The display devices used are high-quality graphics monitors and large-area displays allowing information about the process, about the plant and about the process control system to be displayed graphically or alphanumerically. Operator input is made using an input device that is in wide-spread and successful use in the PC world, the mouse.

A screen-based control room necessarily involves a greater information density than a conventional control room. For this reason, ergonomic display of information and operator guidance are especially important. The visualization of functionally coherent process complexes in conjunction with a hierarchically structured organization of the process display has proven especially advantageous. This method of representation is supported by the process control and information system by surrounding each display with an identical frame containing selection fields with which the operator can request

additional information and navigate his way through the displays to request additional information and navigate his way through the displays to obtain the required information. Extensive case studies have shown that this concept can provide the operator with all the necessary information even under stressful conditions.

In addition to these classic processing functions for process control and information, other future-oriented function modules can be integrated into the server computer. One example of this is the "forecasting computer" function module that calculates process behaviour in advance on the basis of the current plant state to provide the operators with information about the profiles of important process variables for a certain time into the future. This means that action to remedy faults can be taken in good time, thereby enhancing the availability of the plant.

4. COMMUNICATION

Open communication between systems and components of different manufacturers is the aim pursued by international standardization activities in communication technology. The most important standard for open networks is the OSI reference model from the International Standardization Organization. It provides an abstract description of the network architecture and the associated protocols. All other standards are based on the functions defined in this model. This also applies to the SINEC (Siemens Network Communication) local area networks used with TELEPERM XP and TELEPERM XS.

The relevant requirements for electromagnetic compatibility and decoupling are met by the choice of the transmission medium:

- Triaxial cable;
- Optic fibers;

and relevant requirements for transmission performance by the choice of the bus type

- Ethernet (IEEE 802.3);
- Profibus (DIN 19 245).

In applications where insensitivity to electromagnetic interference, galvanic isolation, or bus lengths of up to 4000 meters are required, optic fibers are used as transmission medium.

The great significance that communication between the I&C components has for the safety and availability of the power plant demands an extremely high degree of reliability for data transmission. In order to meet this demand the buses themselves used must be as a matter of principle of fault tolerant design.

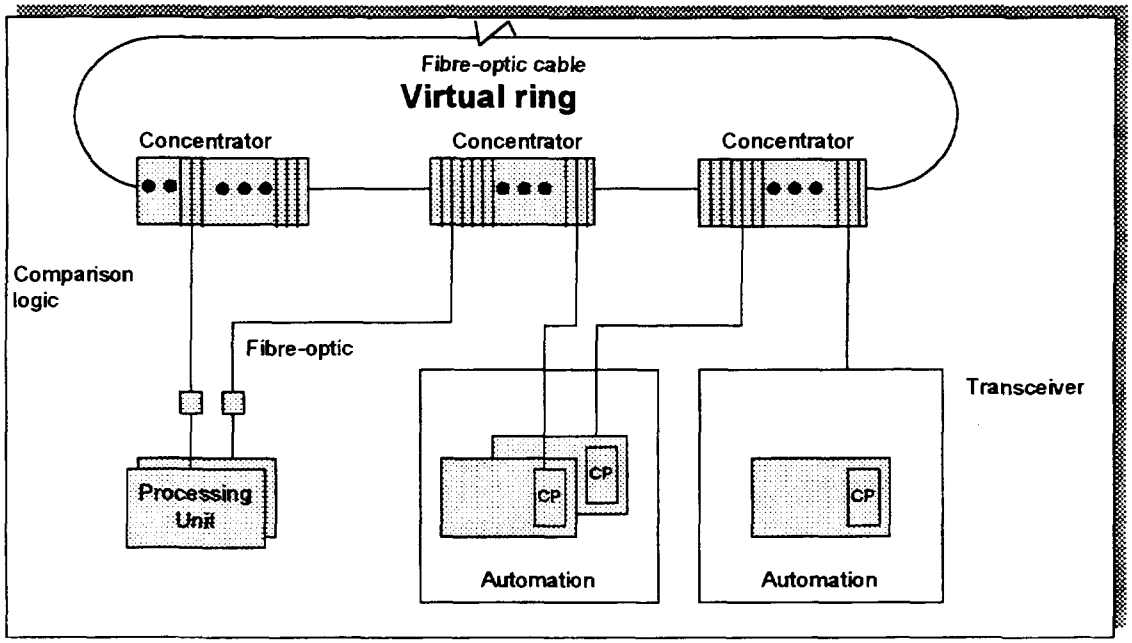

FIG. 4 TELEPERM XP open communication acc. to ISO/OSI.

5. AUTOMATION

In automation, the I&C tasks of closed-loop control, open-loop control, signaling, monitoring and protection are implemented. To achieve this, the automation equipment acquires measurements signals from the process using analog or binary input modules, perform the necessary data processing and output commands to the actuators in the plant (motors, valves, etc.) via analog or binary output modules. In this way, start-up and shut-down sequences are implemented, load changes are made, appropriate action is taken in response to disturbances and, if necessary, protection trips are initiated.

For economic implementation of a process control system it is of paramount importance to be able to adapt the structure of the automation to the requirements of the plant flexibly. This means that the automation must be structured in a task-oriented way. TELEPERM XP and TELEPERM XS both provide the freedom to meet all demands economically. The scalability of the systems assures that individual autonomous control loops, medium-sized systems with local control stations, or complete nuclear power plants with a large-scale screen-based control room can all be implemented just as economically. Fail-safe or fault-tolerant systems can also be implemented, thanks to provision made for planned degrees of redundancy throughout the process control system.

All automation equipment can be connected to a common plant LAN so that all available information about the process can be evaluated centrally. This renders possible effectively to monitor the consistency of the information continuously so that only validated information is passed on to the operator.

The concept described forms the basis of both the TELEPERM XP and TELEPERM XS digital I&C systems. Both systems can be used independently or together. TELEPERM XP is intended for all automation tasks for which no specific qualification for nuclear applications is required. This is the case for the control of essential process variables, for almost the entire man-machine interface as well as for the extensive open-loop controls of the auxiliary systems. This delimitation means that TELEPERM XP can be used for all the automation tasks of a fossil-fired power plant as well as for functions not important to safety in nuclear power plants.

TELEPERM XS, on the other hand, is intended for the safety I&C of a nuclear power plant. Its typical applications are reactor protection and ESFAS functions. The scalability of the system permits automation of other safety-related tasks, such as control of the refuelling machine or the control rod

movement computer. To cover all these tasks, TELEPERM XS is qualified for use in the highest safety category.

Teleperm XP

The TELEPERM XP process control system is designed to perform all automation tasks in the power plant for which no specific qualification for nuclear applications is required. In order to perform these tasks, TELEPERM XP is scalable in large extents so that economic solutions can be ensured both for very small application and for complete plants.

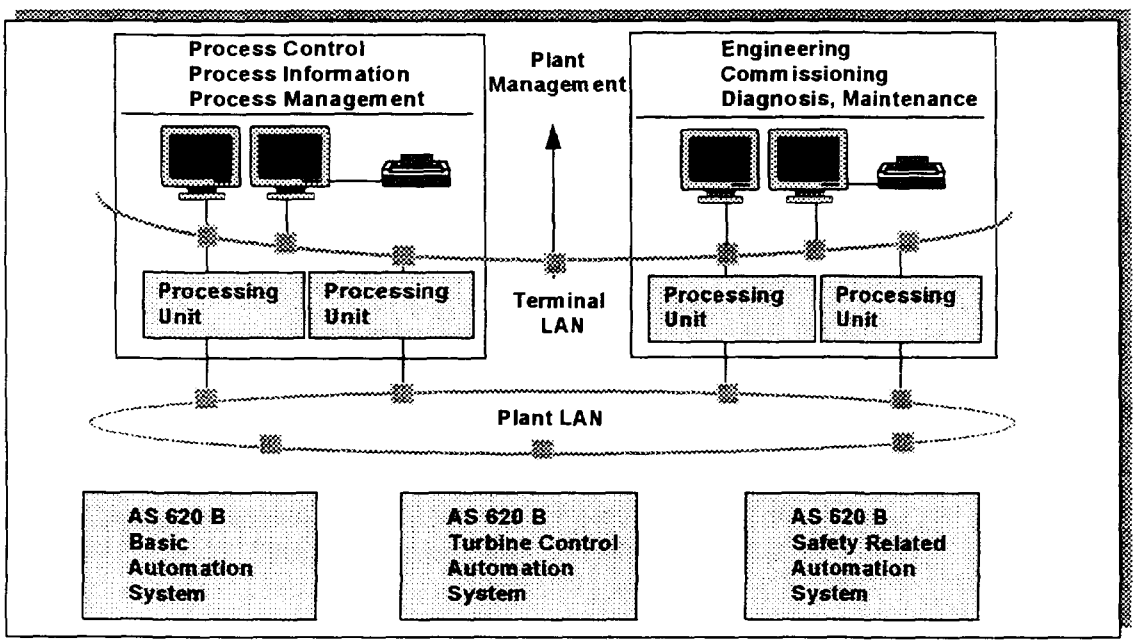

FIG. 5 TELEPERM XP overview.

For engineering, maintenance and diagnosis, TELEPERM XP contains the ES 680 engineering system. All components of TELEPERM XP, i.e. the equipment for automation, operator control and monitoring, and for communication can be handled in every phase of the engineering process in accordance with the general concept. Configuration and documentation of the plant-specific software functionality, of the process I/Os or of communication is possible. After commissioning, the same system is used to make modifications to the software or to locate failures of hardware components.

TELEPERM XP includes the OM 680 process control and information system for operator control and monitoring. This system features a user-friendly man-machine interface, the use of modern visualization media, high availability and a modular hardware and software concept. OM 680 meets the above mentioned requirements to user friendly and ergonomic information displays and supports manual control. Appropriate configuration with just a few basic hardware components such as PC, monitors and local area networks permit compact solutions which can be expanded right up to large-scale man-machine interfaces.

The hierarchically structured automation system fulfills the most varied demands in a power plant with its three function-oriented system types:

- Basic functions (AS 620B);
- High availability and fail-safe applications (AS 620S);
- Increased dynamics, e.g. for turbine control (AS 620T).

The system types AS 620B and AS 620S can be used at the individual control level with function modules on a parallel, redundant cabinet bus. Additionally the AS 620B signal modules can be

connected via the SINEC L2 DP serial peripheral bus. In this way, it is possible to implement future-oriented field bus concepts with TELEPERM XP at the automation level.

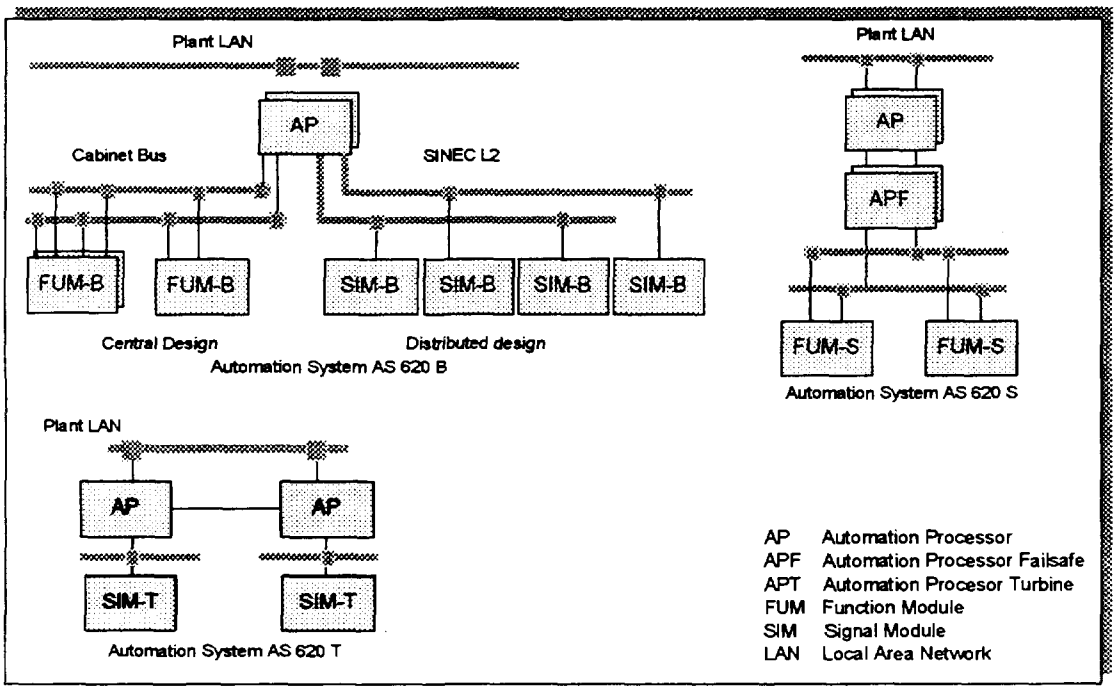

FIG. 6 variants of automation.

To increase availability, all automation processors and the function modules can be implemented redundantly. Not only is the use of future field bus technology being prepared - a precondition of this are intelligent and bus capable field devices - but the use of fuzzy logic has also been planned for new closed-loop control tasks.

All components of TELEPERM XP intermesh fully and they together form a modern process control system with which the various process control tasks of a power plant can be implemented in a future-oriented and economic way. The modular system structure permits adequate solutions for all types and sizes of power plants.

Teleperm XS

National and international codes and standards impose special requirements on the safety I/C of a nuclear power plant. These concern:

- Fault tolerance;
- Robustness;
- Qualification.

In order to be able to meet these requirements to the full without making operational automation tasks unnecessarily expensive by excessive conservatism, the TELEPERM XS I&C system was developed to complement the TELEPERM XP system. It is largely based on standard devices selected for their quality characteristics and adapted by specific design measures. The qualification required by nuclear codes and standards is achieved by supplementary type tests and extended factory tests.

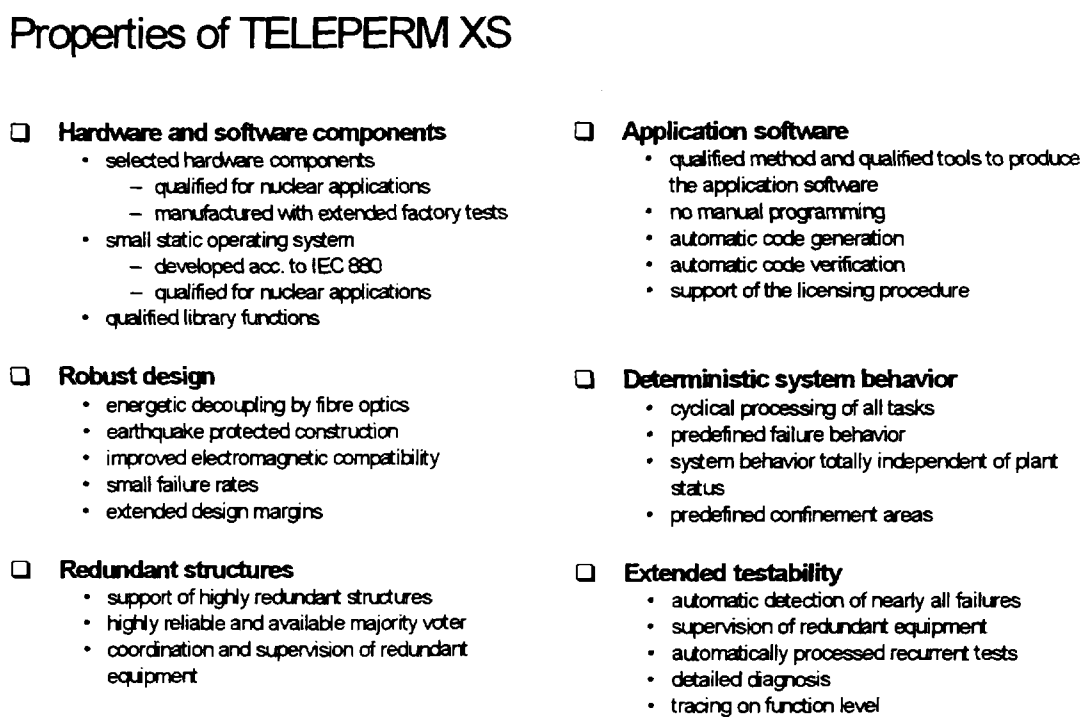

FIG. 7Properties of TELEPERM XS.

6. REACTOR PROTECTION

The most important requirements on safety I&C in nuclear power plants concern the automation equipment for reactor protection. The required fault tolerance characteristics demand for a distributed multicomputer system. The automation devices used must permit the implementation and supervision of widely distributed topological structures.

Superimposing the functional requirement that some protective actions must be initiated very rapidly so as to prevent unsafe states reliably to the above mentioned characteristic, leads to very high performance requirements.

TELEPERM XS fulfills these requirements and also has system characteristics that support the implementation and operation of highly redundant, spatially distributed architectures. For example, highly reliable and highly available I/C systems consisting of two, three of four redundant trains can be implemented with each required topology within the trains. The electrical isolation of automation units is mainly achieved by the use of fiber optics for communication. To avoid a reliability bottleneck in the interface between the redundant I&C trains and the individual control level, a highly available architecture has been applied for the associated voting processor.

Robustness demands design measures that affect both hardware and software. The use of modified packaging hardware allows TELEPERM XS to withstand accelerations such as during an earthquake or in the event of an aircraft crash. Appropriate shielding measures for the cabinets ensure that the stringent requirements on electromagnetic compatibility are also met. In addition to design measures for the hardware, special design rules are also applied on the software. One important rule demands the effective decoupling of the plant process from the behavior of the I&C system because it must be guaranteed that a disturbance or accident in the plant process cannot under any circumstances cause an impact on the safety I&C. For this reason, the computers of TELEPERM XS process all tasks cyclically and do not use event-controlled programs. This means: measurement signals are read in, limit signals formed and control commands output in a never varying sequence regardless of whatever happens in the plant or in other computers.

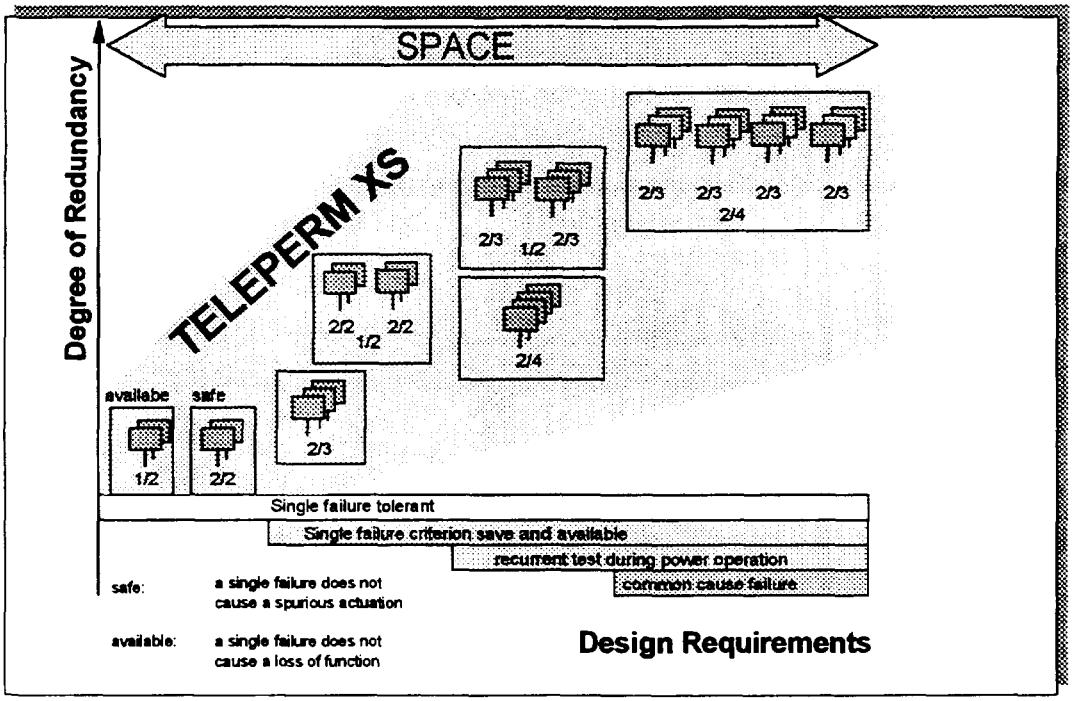

FIG. 8 Structure of safety I&C.

7. SAFETY CONTROL AND INFORMATION

Operator control inputs in nuclear power plants mostly involve operational tasks. Safety related manual intervention such as manual input to the safety I&C system is very limited in scope. Moreover, the low market potential does not justify the development and qualification of a screen-based user interface via which safety-related manual intervention could be implemented. TELEPERM XS therefore does not have dedicated equipment for operator control and monitoring. Instead, the hardwired control room instrumentation is used for safety-related manual command input. However, TELEPERM XP equipment can be used, for example, to display or archive process variables acquired via the safety I&C as part of normal process control. For this purpose, the safety I&C system is connected to the plant LAN of the operational I&C via a uni-directional gateway.

Local control stations for safety-related equipment are only used operationally as well and can therefore be implemented using TELEPERM XP devices.

8. ENGINEERING

The development of plant-specific application software is generally considered the most error-prone activity during the implementation of safety-related I&C systems. For this reason, for TELEPERM XS the production of application software is strongly formalized. In this way, problems related to individual working methods of the staff members can effectively be avoided. Not only the production but also the verification process can be automated to a remarkable high degree. In addition to the function described, the tools required for verification and validation have also been integrated into SPACE, the engineering system of TELEPERM XS, so that its function scope is far greater than that of any previously known engineering aid.

With SPACE the following process model is used to developed plant-specific application software: the task specifications are mainly laid down by mechanical engineers, process engineers and physicists - as always - in prose, diagrams, equations and tables, and are passed on to the I&C specialists in this form. These problem definitions are read and understood by I&C specialists - i.e. control engineers, communications engineers, physicists, computer engineers and mathematicians. Queries for better understanding develop into system discussions. The I&C specialists then prepare all the data and information in a pre-defined way before using the editor of the engineering system SPACE to specify the I&C functions in the form of function diagrams. These function diagrams with well-defined presentation

conventions are readable and understandable for the parties that originated the task specifications for verification purpose and also serve as documentation for the customers. A format recommended by VGB is used which was the result of contracted development of the institute of Prof. Welfonder, Stuttgart.

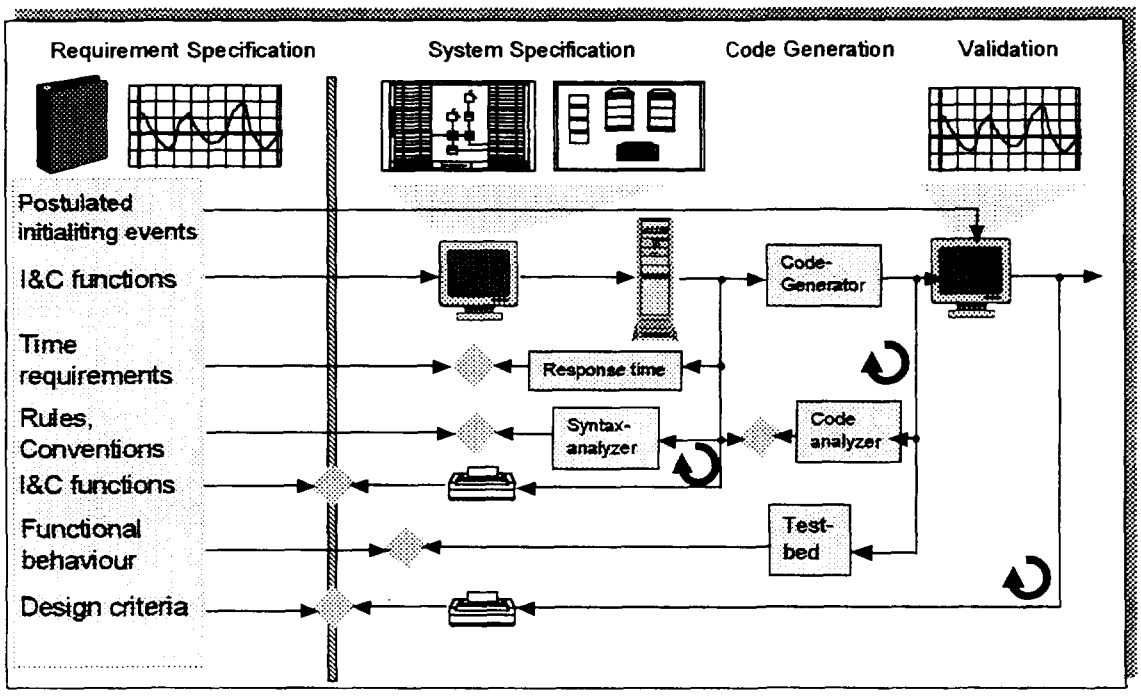

FIG. 9 The system design process.

Once the specification is complete, it can be checked automatically according to various criteria using analysis tools. This analysis includes such important characteristics as completeness and the absence of ambiguity. This has only been made possible by the use of rigorously formal methods. The formally correct specification is then passed on for verification by the originators of the requirement specification who are also responsible for its release. For the quality of the application software it is of decisive significance that the application software is automatically derived from the formal specification by qualified generators. Because the software was generated by an automatic tool, it is possible to verify the consistence of the generated code with the formal specification using a second automatic tool. One consequence of this method is that quality verification of the code generator can be kept economically viable.

After this verification step, the code is ready for testing. As an option to facilitate testing, a test environment can be generated by the code generator. This provides all the aids required for efficient testing. For example, arbitrary signal transients can be generated in order to provoke specific responses and all internal signals and memories can be accessed in order to evaluate the functional behavior.

If realistic feedback from the process is required to evaluate functional behavior, the generated code can be linked to a partial area simulator. In such functional tests the partial area simulator simulates the thermohydraulic power plant process and provides the I&C functions with the required measured data. The I&C function, i.e. the test object, responds to this measured data with commands to the final control elements which in turn affect the thermohydraulic power plant process. If necessary, power transients as well as malfunctions or accidents can be simulated by the partial area simulator.

9. QUALIFICATION

Especially when developing new technology systems which are to perform important safety functions, it is essential to take care of safety requirements from the beginning in order to avoid problems which in

later stages of the development process might lead to costly changes or even redesign. Therefore a development accompanying assessment has been decided.

Accompanying evaluations and concept assessment of the whole system **by GRS ISTec.** Since 1988, continuous evaluations of the development on behalf of the Bavarian licensing authority (BStMLU). In June 1992, acceptance of the concept to realize I&C systems for safety functions of the highest category

a) Type testing

Type testing has to demonstrate the compliance of the modules with the data specified in the corresponding data sheet. It consists of a theoretical and a practical part. Essential issues of the theoretical assessment are the failure effect analysis, the critical load analysis and the program for the practical tests, which comprise functional tests and robustness tests (internal and external influences/events). The role of an authorized expert (independent institute) is the assessment of the documents as prepared by the manufacturer, the evaluation of the practical test program, the participation in the practical tests (to the extent considered necessary) and the assessment of the test results. Software type testing is performed in analogy to hardware type testing. This can be done because as a rule we are facing distributed systems with reusable software modules which can be configured and parameterised according to their envisaged application.

b) Type testing of the software modules

Since October 1992, contracted to GRS ISTec, which is supported by TÜV-Nord. In June 1996, the qualification of the system software and the application modules was finished. One new aspect is that all re-usable software is subject to a type test "analogous to the stipulations of KTA 3503". This method is of special advantage to the TELEPERM XS concept because the entire application software is made up of re-usable software modules combined by generators, i.e. software modules are used in the same way as hardware modules in hardwired systems. A software module has a well-defined functionality and a well-defined interface that can both be checked against the pecification. Whereas in the hardware type test, greater emphasis is placed on practical testing, in the software type test equal emphasis is placed on theoretical and practical testing.

c) Type testing of the hardware modules

Since February 1994, contracted to TÜV-Nord to elaborate the module analysis and the test specifications. The practical testing was delegated to the test institute of TÜV Rheinland (ISEB).
In October 1996, the practical tests of the hardware modules for the qualification were finished.

d) Plant Independent System test

proving the main system features with participation of GRS ISTec and TÜV Nord as independent assessors. These tests are scheduled for November 1996.

The main system features to be proven by this tests are: checking the specified system performance, e. g. the strict cyclic processing of the application code and proving the correctness of the recalculation of processor and bus loads as well as of the response time for the specified application code by the engineering tool SPACE, validation of the process of generating the application code, system behaviour independent of the application software and its allocated input data trajectories.

Fig. 10 gives an overview on the main standards relevant as well for the development as for the qualification.

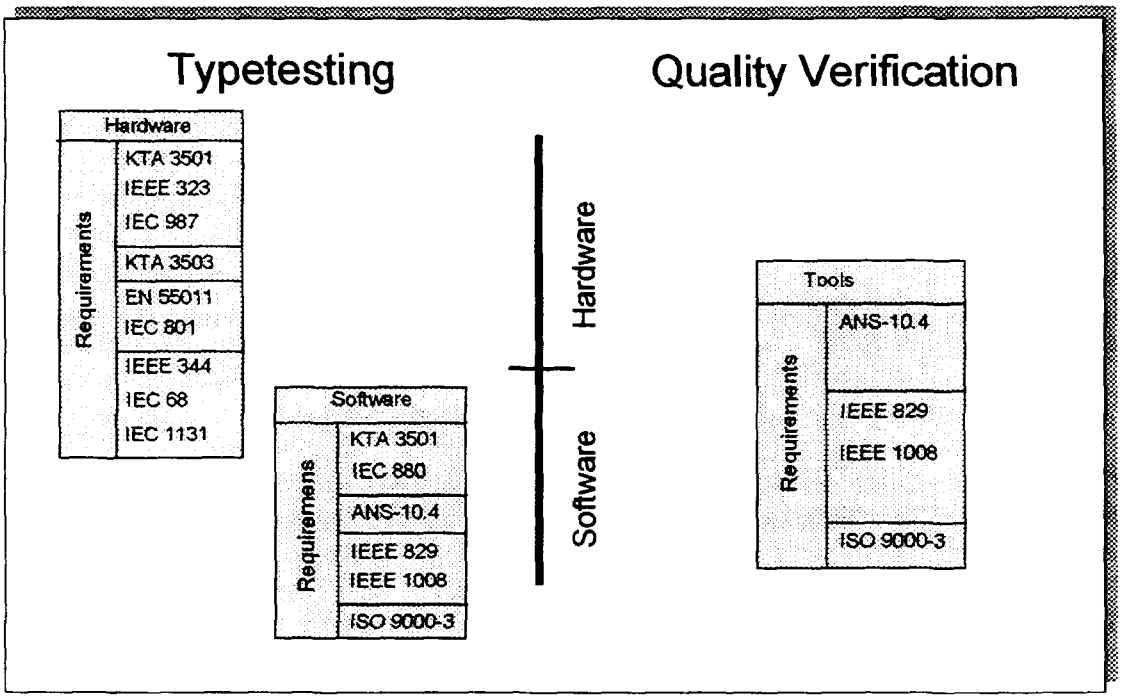

FIG. 10 Basis of qualification.

Abbreviations

ANS	American National Standard
AS	Automation System
CP	Communication Processor
DIN	Deutsche Industrie Norm
EMC	ElectroMagnetic Compatibility
ES	Engineering System
GRS	Gesellschaft für ReaktorSicherheit
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standardization Organization
ISTec	Institut für SicherheitsTechnologie
KTA	KernTechnischer Ausschuß
LAN	Local Area Network
OM	Operation and Monitoring
OSI	Open System Interconnection
SNAP	Siemens Nuclear Automatic Protection
SPACE	SPecification And Coding Environment
TÜV	Technischer ÜberwachungsVerein
VGB	Verband der GroßkraftwerksBetreiber