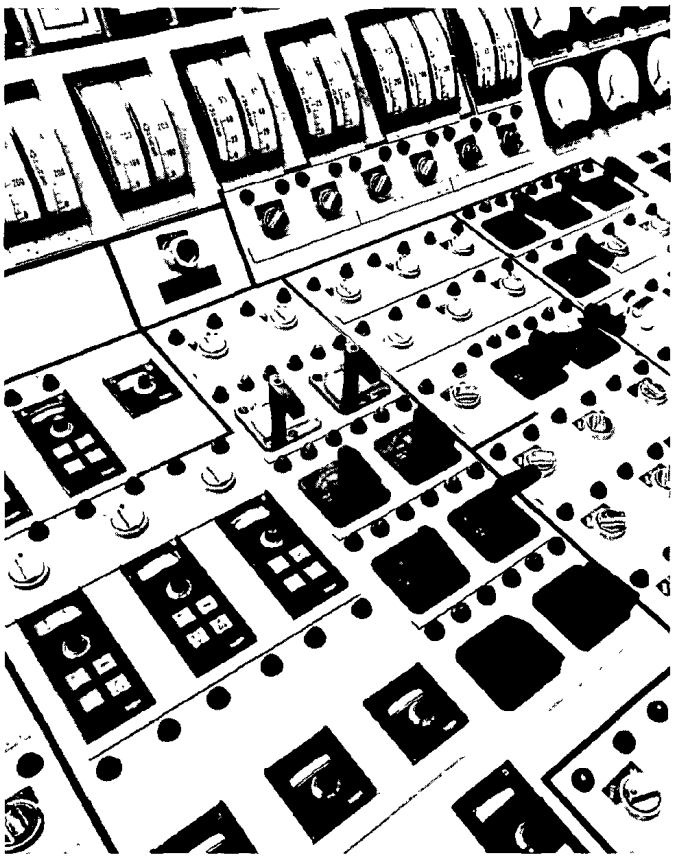
Advanced computerized operator support systems in the FRG

In the Federal Republic of Germany, automation carries increasing emphasis

by W. E. Büttner



Control-room panel

During the course of the development of nuclear power plants, the instrumentation and control systems – and the information displays, annunciator windows, and devices inside the control room – have been increasing substantially. In a present modern 1300-megawatt pressurized-water reactor (PWR) in the Federal Republic of Germany, there are about 7500 control interface modules, 12 000 binary indications or displays, 1400 measured value recorders, 10 cathode-ray tube (CRT) displays, and 8 logging devices in the control room and local control stations.

So as not to overburden the shift personnel, the degree of automation has been increased essentially to assist personnel during normal operation, as well as during incidents and accidents. In German nuclear power plants, the degree of automation is higher than in nuclear plants in the English-speaking world. Nevertheless, the exigency to develop further operator support systems for information processing, compression, and presentation is generally recognized, as the development of such systems is recognized worldwide.*

This article describes the development of some computerized operator support systems in the FRG with the main emphasis on safety aspects. The tasks of the systems are to:

- Log and record disturbances and accidents
- Reduce the information load and present only essential alarms and messages
- Improve signal supervision and verification
- Enable a fast survey of the plant status (especially in case of accidents) and of the character and location of a disturbance
- Carry out automatic diagnosis of disturbances
- Compute process parameters that cannot be measured directly
- Support operators as they follow procedures in the operating manual.

Review of operator tasks

A task analysis of the operator's job is the basis for development and implementation of these computerized operator support systems. Therefore, a short description of operator tasks will be given with regard to the automatic protection and limitation systems.

The minimum size of the control crew depends on plant organization and management. The crew normally consists of at least one shift leader, two reactor operators (of which one has shift leader qualifications and is the shift leader substitute), two shift electricians, and two shift mechanics. In practice, there are more shift personnel in modern nuclear plants – instead of two reactor

Mr Büttner is a project leader with the Gesellschaft für Reaktorsicherheit in Garching, Federal Republic of Germany.

* See the author's report of the IAEA Symposium on Nuclear Power Plant Control and Instrumentation in Munich (October 1982) and "Leichttechnik in Kernkraftwerken – eine Übersicht", by P. Freymeyer, etz. 102 (March 1981) for further information.

operators, there are three or four. In addition to them, there are one or two control board operators and four electrical charge hands. The reason is that shift personnel are occupied by many organizational and administrative tasks (for example, defining work permit sheets for maintenance and the necessary disconnections), or they must perform functional tests or retests.

Shift personnel have to operate the plant during power, start-up, and shutdown operations and down-time, and they are responsible for co-ordinating all operational activities of the power station unit, including the associated auxiliary installations, under both normal and accident conditions. In case of incidents and accidents, they have to:

- Prevent undue disturbance consequences during a short time period
- Bring the plant into long-term guaranteed safe and stable conditions
- Mitigate disturbance consequences and master complex disturbance situations.

According to the German KTA-Rule 3501, it is a design criterion that the reactor protection system should automatically initiate the required protection actions.* Hence, provisions for manual interventions are an exception and must not be necessary in the first 30 minutes (nevertheless, manual operator actions will be possible). This is to keep operators free to recognize the plant state (knowledge-based behaviour).

During the short-term period, the operators should analyse the causes of an accident, supervise the safety actions automatically started, and prepare actions necessary to bring the plant into safe and stable conditions. However, the shift is subjected to further actions, such as:

- Releasing alarms (e.g., fire alarm for buildings affected)
- Checking whether persons are within a danger zone
- Initiating first aid or rescue operations if necessary
- Informing the emergency service on call and the plant management if necessary
- Logging the events (e.g., within the shift log-book or switching log-book).

Computerized operator support systems

In the course of this article, only computerized operator support systems will be described that concern safety-related aspects. Some systems may be useful for both normal and disturbance or accident conditions. In this case, the aiding functions for normal operation modes remain unmentioned. All systems described are under development, test, or commissioning.

* Reactor Protection System and Monitoring of Engineered Safeguards, KTA 3501 (March 1977).

Log and record systems for disturbances, accidents

Switching and alarm logs and incident reviews available in present plants are useful for later disturbance analysis and clearing up, as well as for continuous observation of incidents and accidents. By using more typewriters, the switching and alarm logs can be split up into, for example, a separate log for all messages of electrical and control facilities (about 50% of the messages in present switching and alarm logs). It also might be possible to call up separate alarm logs and messages of subsystems (via the system identification number).

A second idea is to plot trend curves of important process variables (in a first step about 200). By this means, it is much easier to check the process variables against safety limits and to compare them with each other. Also, the time resolution is much better than in the tabulated list of the present incident reviews. Such intentions can be realized within a short time and without great expense. But ideal conditions for such projects call for a separate group within the utility for maintaining, updating, and developing the computer software.

Reduction of information load

In present nuclear power plants almost every event, independent of its importance, is announced to operators and has to be evaluated and classified by them. It is left to their skill, knowledge, and flexibility to pick the really important ones out of the flood of messages. In particular, the information load will increase very much in case of incidents. This situation is considered as unsatisfactory.

Therefore, a filtering method is under development to limit the number of messages and alarms issued by the process computer.* It must be assured that the presentation of messages remains feasible and makes sense, even if major or unexpected disturbances affect the plant.

The reduction of information load will be realized by:

- Suppression of consequential alarms. This means alarms that will necessarily and unavoidably follow an event already announced.
- Suppression of superfluous alarms. This means alarms from subsystems not available for further actions within the present plant operation mode, or from subsystems not, or no longer, required.

Both procedures are used in combination. The final remaining alarms are then displayed. This suppression will not affect the alarm recording.

* See "KWU Alarm Analysis Concept: A Means to Reduce Information Load for the Operators in Nuclear Power Plants", by J.R. Goethe, at IFAC Workshop Modelling and Control of Electric Power Plants, Como (September 1983).

Signal verification and sensor surveillance

It is required that all information displayed via advanced operator support systems must be safe and trustworthy. To increase the reliability of primary information – particularly by the intensive way of mixing, combining, and compressing data by computers – new methods will be adapted to signal verification and sensor surveillance. Research for application of such methods in nuclear plants is in an early stage. Three methods seem to be promising.

One method is to monitor sensors or measuring chains by means of plausibility investigation using logical or physical dependencies of signals. Another method is to use the noise analysis by comparing the statistical information of the measuring signals or channels with their typical signal patterns. Finally, it is possible to compute process states by means of mathematical models (analytical or functional redundancy) and to compare them with the measured ones in a logical or voting sense. It is possible to combine the methods – for example, to use an analytical redundancy of process parameters that cannot be measured directly for a plausibility check.

Plant overview: PRINS

Different efforts are proposed to enable operators to get a quick overview of plant status. There is also a close connection to the alarm-reduction and alarm-analysis projects described in this article.

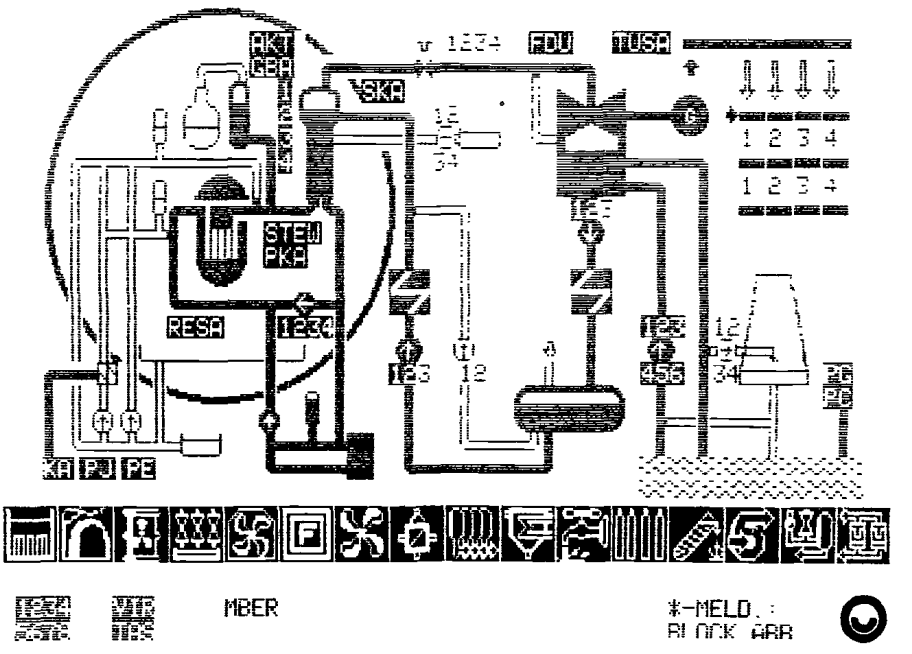
Kraftwerk Union (KWU) has a new process information system called PRINS under design for the three German Konvoi-reactors.* PRINS is an integrated system providing information for all modes of plant operation. It includes the functions of safety parameter display systems, as well as of disturbance analysis and operation monitoring systems.

For information display there will be available up to 32 colour video display units (VDU). The scope of display formats mainly includes system overviews and diagrams, but trend logs, bar graphs, alphanumerics, alarms, and logics also are covered. The objectives for information display are to:

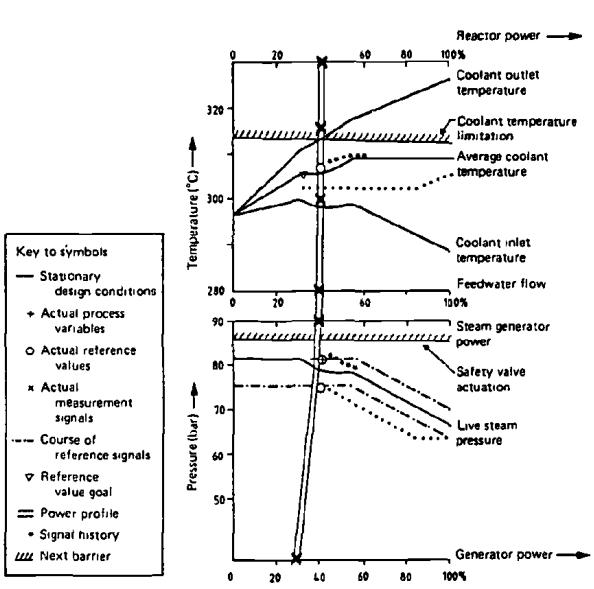
- Make possible qualified manual operations to bring the plant to a safe status in case of accidents
- Maintain the plant in a safe status
- Confine the consequences of an accident or incident
- Make transparent the behaviour of complicated automatic systems (particularly for the limitation systems)
- Facilitate and assure operation, such as for retests or start-up and shutdown procedures
- Enable an easy post-mortem analysis.

Some examples of information presentation by PRINS are shown in illustrations accompanying this

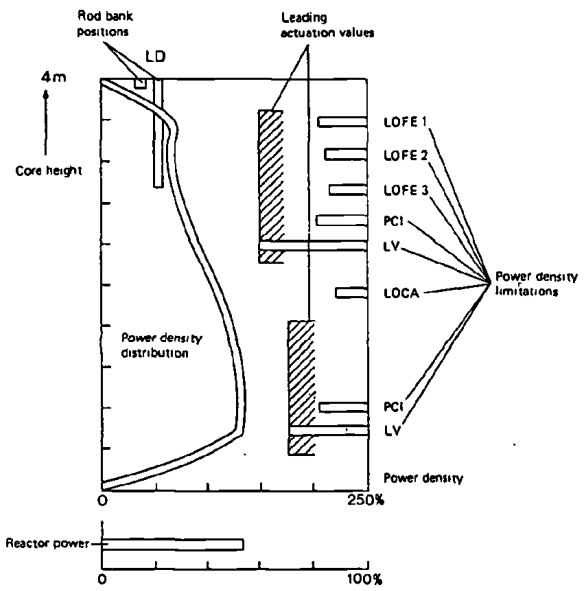
* See "Safety Parameter Display Functions are Integrated Parts of the KWU-Konvoi-Process Information System (PRINS)", by W. Aleite and K.H. Geyer, paper for presentation at the Fifth International Meeting on Thermal Nuclear Reactor Safety, Karlsruhe (September 1984); and "Video Display Units in Nuclear Power Plant Main Control Rooms: The Process Information Systems KWU-PRINS", by W. Aleite, H.W. Bock, and E. Rubbel, Siemens Forschung- und Entwicklungsbericht Bd. 13, No. 3 (1984).



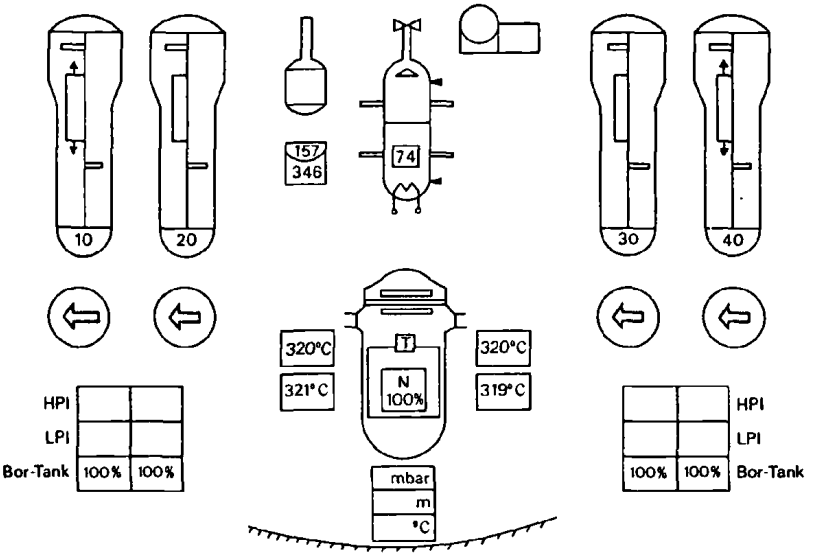
PRINS displays the status of all important systems. Auxiliary systems which are not directly involved (such as ventilation or the fuel-pit cooling loop), are displayed by symbols at the bottom.



In the part-load diagram of PRINS, all stationary design conditions, as well as actual process parameters and process history, are shown.



The power density distribution and limitation diagram of PRINS gives the updated rod bank positions, the reactor power, the power density distribution with respect to the core height, and the power density limitations for the upper and lower core.



All important process parameters that are necessary to identify whether the safety-related functions, "coolant inventory" and "heat removal" are guaranteed are faded into the information PRINS provides.

article. In each of these displays, an average of 100 binary and 30 analog signals are processed. Thus a reduction of information load could be obtained.

Another pilot project is now under test with the aim of achieving a quick overview of the plant status. In checking whether the behaviour of a system is such as designed or not, it should not be necessary to check all the switching messages and process variables to assure the regular operation of a safety system. The check will therefore be done automatically and a message will be given at inadequate results only. The same holds for shutdown procedures. For example, in case of a turbine trip many messages have to come within a fixed sequence. To check this manually is very time consuming, so it will be done automatically in a similar way as described above.

Disturbance analysis: STAR

A second pilot project has been started in the Biblis nuclear power plant for testing the disturbance analysis system called STAR.* The first pilot application was in the Grafenrheinfeld nuclear plant.** Many publications have been issued on disturbance analysis and the STAR system, so it will be outlined only briefly.

* "STAR – A Concept for the Orthogonal Design of Man-Machine Interfaces with Application to Nuclear Power Plants", by W.E. Büttner, L. Felkel, R. Manikarnika, and A. Zapp, IFAC Conference on Analysis Design and Evaluation of Man-Machine Systems, Baden-Baden (September 1982).

** "STAR Disturbance Analysis System: Results from the Grafenrheinfeld PWR Application", International Symposium on Nuclear Power Plant Control and Instrumentation, Munich (October 1982).

To detect disturbances, so-called disturbance models are used. These are represented by logical models (e.g., cause-consequence diagrams), by physical models (e.g., mass balances, system, or component characteristics) or by mathematical models (e.g., five-point, fixed-memory linear filtering). The models contain the anticipated appearance of events during disturbances and are started in a background data base. They are overlaid by the actual plant data.

The disturbance analysis routine scans the models and detects disturbances, if there are any. The main objectives of the STAR system are to:

- Recognize plant disturbances as early as possible, determine the prime causes and possible propagation, and provide information about the process status
- Announce the best or suitable recovery action to master the disturbance if it is unambiguously possible (these hints should not force operator actions)
- Enable supplying of information to the disturbance analysis system
- Provide flexible models that can be extended or modified easily, which may be necessary to take account of experience or plant modifications.

Support of operating manual procedures

Many procedures described in the operating manual consist of checking the value or status of specific plant variables, combining them in a logical way, and performing actions required by the results of the check. For such procedures an opportunity for application of computerized aid systems is obvious. Preparatory research for pilot application was done for the supervision of safety systems in boiling-water and pressurized-water reactors.*

The main objectives for such a system follow:

- The reactor safety systems, together with their power supply and auxiliary systems, will be supervised so that in case of component failures or unavailabilities a check will be performed to determine whether remaining systems fulfil safety requirements in the operating manuals.
- In case of failures, the counter-actions or necessary preventive measures should be announced if safety requirements are violated (e.g., admissible repair time, shortening of retest intervals of redundant systems).
- A supervision of remaining repair time should be performed.
- The operator will be supported by drawing up working or disconnection sheets for maintenance procedures, and by the documentation of retests or functional test results (e.g., according to the German KTA-rules 1202 and 3506).* How the requirements of the operating manual can be transferred to and supervised by a computer can be logically presented.

Conditions for successful development

To summarize, the reasons for all the activities in the field of computerized operator support systems are the substantial increase of instrumentation and control equipment; the necessity to remove the burden of routine tasks from the operators and to leave them to the intrinsic tasks of plant control and supervision; the requirement to reduce and to compose the information quantity; and the intention to support the operators in case of incidents and accidents by diagnosis and supervision.

Most of the tasks cannot be solved by means of conventional equipment. New systems, however, must be consistent with the conventional control-room design, information display, and the operating manual procedures. It must be guaranteed that all the systems, the old ones as well as the new ones, act together and are fitted in an overall conception. A test phase on a plant simulator should complete the pilot application and the shift operators should be extensively included in the development. This is necessary to overcome the difficulty of having the advanced systems act together, though they will be developed individually for reasons of quality assurance, documentation, test, or expert opinion.

A further necessary condition for successful development is a detailed operator task analysis and a clear definition of the system tasks. The support systems have to give the operators new facilities. Aids are not needed where there are systems or procedures already available and handy. The systems should not give orders to the operators but should advise them.

Finally, attention must be paid to ergonomic aspects.

* "Überwachung von Sicherheitsparametern durch Prozessrechnereinsatz", by H. Schüller and W.E. Büttner, GRS-A-Report No. 916 (March 1984).

* Requirements for the Inspection Manual, KTA 1202, (June 1984), and Test of Electrotechnical Control Systems of the Safety System of Nuclear Power Plants, KTA 3506, (November 1984).