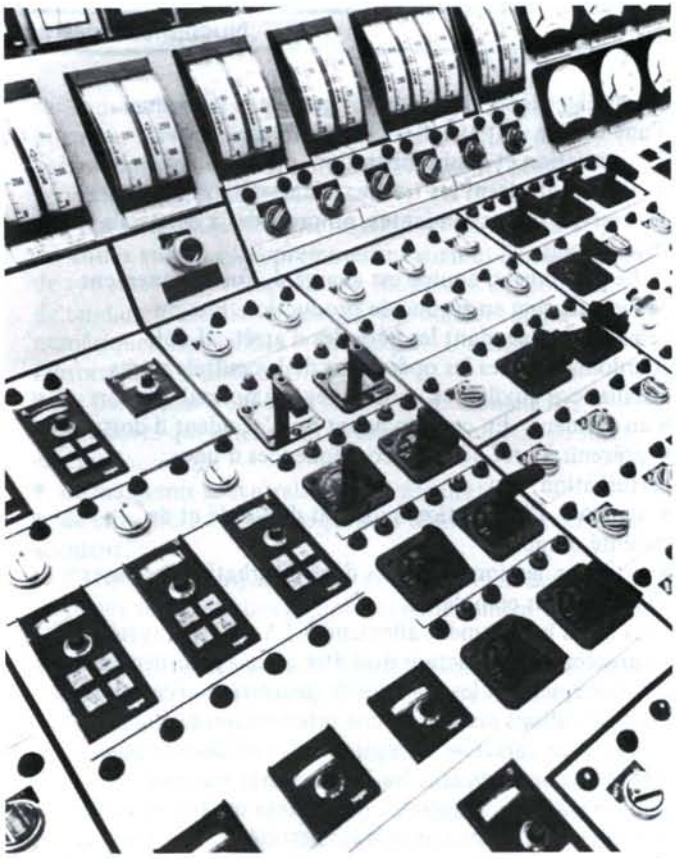
# Systèmes informatiques avancés pour opérateurs en RFA

*En République fédérale d'Allemagne, l'automatisation va de l'avant*

par W.E. Büttner



Panneau-pupitre de la salle de commande

L'évolution des centrales nucléaires s'accompagne d'un développement remarquable de l'instrumentation dont disposent les salles de commande, tels les dispositifs d'affichage, les écrans de signalisation et autres appareils. Une centrale moderne à réacteur à eau pressurisée de 1300 mégawatts, actuellement en service en République fédérale d'Allemagne, comporte environ 7500 modules de contrôle en interface, 12 000 indicateurs ou affichages binaires, 1400 enregistreurs de valeurs mesurées, 10 affichages à tubes cathodiques et huit dispositifs d'enregistrement, situés dans la salle de commande et ses postes annexes.

C'est avant tout pour éviter de surcharger les équipes et les aider en période normale et en cas d'incident ou d'accident qu'on a mis l'accent sur l'automatisation; aussi est-elle plus largement utilisée dans les centrales nucléaires d'Allemagne que dans celles des pays anglophones. Le monde entier convient d'ailleurs de la nécessité de pousser plus loin le progrès des systèmes qui aident les opérateurs à traiter, à condenser et à présenter l'information.*

Le présent article décrit l'évolution de certains systèmes informatisés d'appui aux opérateurs en République fédérale d'Allemagne, notamment en ce qui concerne la sûreté. Ces systèmes ont pour fonction:

- de relever et d'enregistrer les incidents et accidents;
- d'alléger l'information en ne présentant que les alertes et messages essentiels;
- de perfectionner le contrôle et la vérification des signaux;
- de permettre une détection rapide de l'état de l'installation (notamment en cas d'accident) ainsi que du caractère et de l'emplacement d'un incident;
- de procéder à un diagnostic automatique de l'incident;
- de déterminer par le calcul les paramètres de fonctionnement qui ne se prêtent pas à une mesure directe;
- d'aider les opérateurs à exécuter les instructions données dans le manuel d'exploitation.

### Les tâches de l'opérateur

L'élaboration et la mise en œuvre de systèmes informatisés d'appui aux opérateurs exige une analyse préalable de la tâche de ces derniers. Nous en donnons ci-après une brève description en ce qui concerne les systèmes automatiques de protection et de limitation.

L'importance des effectifs du personnel de commande dépend de l'organisation et de la direction de la centrale. Chaque équipe comprend normalement au moins un chef d'équipe, deux opérateurs de réacteur, dont l'un possède les qualifications de chef d'équipe et peut le remplacer, deux électriciens et deux mécaniciens. En pratique, les équipes des centrales modernes sont plus nombreuses et comprennent trois ou quatre opérateurs de réacteur au lieu de deux. Il y a en outre deux opérateurs de tableau de commande et quatre personnes affectées à la

---

M. Büttner est directeur de projets à la Gesellschaft für Reaktorsicherheit, Garching (République fédérale d'Allemagne).

* Voir le rapport de l'auteur au Colloque international de l'AIEA sur la commande et l'instrumentation des centrales nucléaires, tenu à Munich en octobre 1982, ainsi que "Leittechnik in Kernkraftwerken – eine Übersicht» par P. Freymeyer, e t z. 102 (mars 1981) pour tout complément d'information.

charge électrique. La raison en est que le personnel d'une équipe doit assumer de nombreuses tâches d'organisation et d'administration, par exemple établir les fiches autorisant les travaux d'entretien et les mises hors service correspondantes, ou procéder à des essais fonctionnels.

Le personnel d'équipe est chargé du fonctionnement de l'installation en régime de production, lors du démarrage et pendant les périodes d'arrêt. Il doit coordonner toutes les opérations de la centrale et ses installations auxiliaires, tant en régime normal que lors d'un accident. En cas d'incident ou d'accident il doit:

- prévenir à bref délai les conséquences d'une perturbation;
- ramener l'installation à un état de sûreté et de stabilité durable;
- atténuer les conséquences des perturbations et parer aux situations complexes.

D'après le règlement allemand KTA 3501, le système de protection du réacteur doit être conçu pour déclencher automatiquement les mesures de protection nécessaires.* Les dispositions prévoyant une intervention manuelle ont donc un caractère exceptionnel et ne doivent pas être nécessaires pendant les 30 premières minutes (l'intervention manuelle de l'opérateur est toutefois possible). Cette prescription est destinée à laisser aux opérateurs le loisir de constater l'état de l'installation pour pouvoir agir en connaissance de cause.

Pendant cette brève période, les opérateurs doivent analyser les causes de l'accident, vérifier l'exécution des mesures de sûreté automatiques, et préparer les interventions nécessaires pour restaurer la sûreté et la stabilité de l'installation. L'équipe a toutefois aussi d'autres obligations, à savoir:

- donner l'alarme (par exemple en cas d'incendie dans les bâtiments concernés);
- vérifier s'il reste des personnes dans la zone dangereuse;
- commencer les opérations de premiers secours ou de sauvetage en cas de besoin;
- informer le service d'intervention de garde et la direction de la centrale en cas de besoin;
- consigner les événements dans le journal de bord de l'équipe ou dans le registre de commutation.

### Systèmes d'appui informatisés

Ne seront décrits dans le présent article que les systèmes d'appui informatisés. Certains d'entre eux peuvent rendre service non seulement en cas d'incident ou d'accident, mais aussi en régime normal et nous ne parlons pas du rôle qu'ils jouent dans ce dernier cas. Tous les systèmes décrits sont à l'étude, à l'essai ou en service.

### Systèmes d'enregistrement des incidents et accidents

Les registres de commutation et d'alarme et les relevés d'incidents dont disposent les centrales actuelles rendent des services quand on veut analyser et élucider les incidents ultérieurs, et observer en continu des incidents et accidents. En employant plusieurs machines à écrire, on peut répartir l'enregistrement et consacrer par exemple un journal séparé pour tous les messages provenant des installations électriques et des postes de commande (qui représentent actuellement 50% du total des messages). On pourrait aussi appeler des journaux particuliers d'alarme et de messages provenant des sous-systèmes au moyen de leur numéro d'identification.

Il serait également possible de tracer les courbes de l'évolution des variables importantes (200 environ pour commencer). Ceci permettrait de les comparer beaucoup plus facilement aux limites de sûreté et entre elles. La résolution en temps serait aussi bien meilleure qu'avec la présentation actuelle sous forme de tableaux. Ces idées pourraient se concrétiser en peu de temps et à peu de frais, mais pour créer les conditions optimales à cet effet il serait bon de créer dans la centrale un groupe spécialement chargé de la gestion du logiciel.

### Allègement de l'information

Dans les centrales nucléaires actuelles, presque tous les événements, quelle que soit leur importance, sont annoncés aux opérateurs, qui doivent les évaluer et les classifier. A eux d'avoir l'habileté, les connaissances et la souplesse nécessaires pour choisir les messages vraiment importants dans cet afflux d'information, particulièrement en cas d'incident. Il faut porter remède à cette situation.

C'est pourquoi l'on étudie actuellement une méthode de filtrage permettant de réduire le nombre des messages et des alarmes émis par l'ordinateur d'exploitation.* Il faut s'assurer que la présentation des messages restera possible et utile même en cas d'incidents graves ou inattendus.

Pour alléger l'information, il y a lieu:

- De supprimer les alarmes conséquentes, c'est-à-dire celles qui suivent nécessairement et inévitablement un événement déjà annoncé.
- De supprimer les alarmes superflues, à savoir celles qui proviennent de sous-systèmes qui ne peuvent servir à intervenir dans le contexte du mode d'exploitation en cours, ou de sous-systèmes qui ne sont pas ou ne sont plus utiles.

Les alarmes sont alors affichées. Ce filtrage des alarmes ne supprime pas leur enregistrement.

### Vérification des signaux et surveillance par détecteur

Toute information affichée par les systèmes perfectionnés d'appui aux opérateurs doit être sûre et fiable. Afin d'améliorer la fiabilité de l'information primaire, notamment par l'emploi intensif de l'ordinateur pour la composition, la combinaison et la condensation des données, il faudra adopter de nouvelles méthodes de vérification des signaux et de surveillance des détecteurs. Des recherches sur l'application de ces méthodes dans les centrales nucléaires viennent d'être entreprises.

Trois d'entre elles paraissent intéressantes. La première consiste à surveiller les détecteurs ou les chaînes de mesure

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

* Voir «KWU Alarm Analysis Concept: A Means to Reduce Information Load for the Operators in Nuclear Power Plants» par J.R. Goethe, IFAC Workshop Modelling and Control of Electric Power Plants, Côme (septembre 1983).

au moyen d'une recherche de plausibilité qui fait appel à la dépendance logique ou physique des signaux. La seconde consiste en une analyse des bruits qui rapporte l'information statistique fournie par les signaux ou circuits de mesure à leurs modes caractéristiques de signalisation. Enfin, on peut aussi calculer les états de fonctionnement au moyen de modèles mathématiques (rendondance analytique ou fonctionnelle) et les comparer logiquement ou sélectivement avec les valeurs mesurées. Les deux méthodes peuvent être combinées, par exemple en faisant appel à une redondance analytique des paramètres dont la plausibilité n'est pas vérifiable au moyen d'une mesure directe.

### Examen de la situation de la centrale: PRINS

Plusieurs procédés différents ont été proposés pour permettre aux opérateurs de connaître rapidement l'état de la centrale, préoccupation d'ailleurs étroitement liée aux projets d'allègement et d'analyse des alarmes exposés dans le présent article.

La Kraftwerk Union (KWU) est en train d'élaborer un nouveau système d'information sur le fonctionnement, dénommé PRINS, à l'intention de trois réacteurs allemands.* PRINS est un système complet qui renseigne sur tous les modes de fonctionnement de la centrale. Il porte sur les fonctions de systèmes d'affichage de paramètres de sûreté, l'analyse des incidents et la surveillance du fonctionnement.

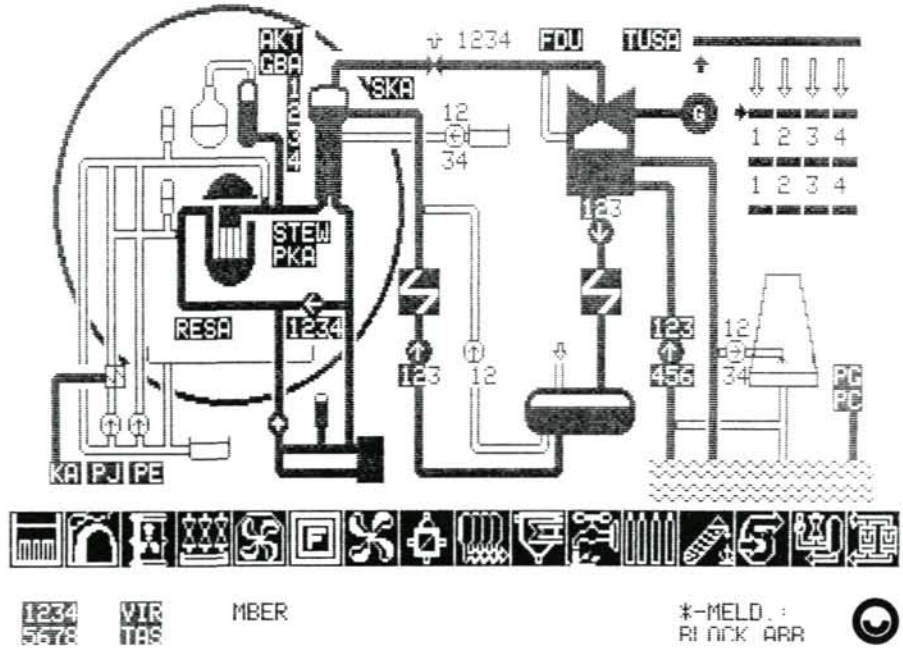
Pour l'affichage de l'information on aura jusqu'à 32 unités video. Elles présenteront surtout l'examen de systèmes et des diagrammes, mais aussi des courbes de tendance, des histogrammes, des données alpha-numériques, les alarmes et la logique. L'affichage de l'information a pour but:

- de permettre d'exécuter les opérations manuelles déterminées qui amèneront la centrale à un état de sûreté en cas d'accident:
- de maintenir la centrale en état de sûreté;
- de circonscrire les conséquences d'un incident ou accident;
- d'assurer la transparence du comportement des systèmes automatiques complexes (notamment de limitation);
- de faciliter et d'assurer le fonctionnement, par exemple pour les répétitions d'essais ou les opérations de démarrage ou d'arrêt:
- de faciliter l'analyse après coup.

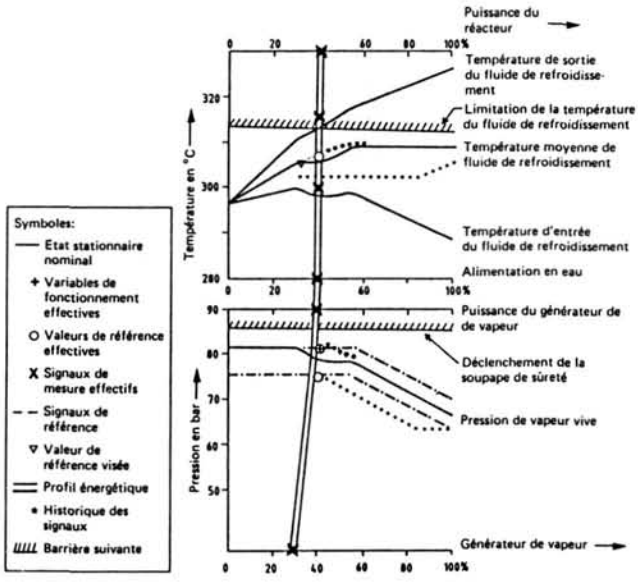
Les illustrations qui accompagnent le présent article montrent quelques exemples de présentation d'information par le système PRINS. Chacun de ces affichages traite en moyenne 100 signaux binaires et 30 analogues. C'est ainsi qu'on a pu obtenir un allègement de l'information.

Un autre projet pilote visant à permettre un examen rapide de l'état de l'installation est en cours. Quand on veut savoir si le comportement d'un système correspond à ce qu'on en attend, il ne devrait pas être nécessaire de vérifier tous les messages de commutation et variables de

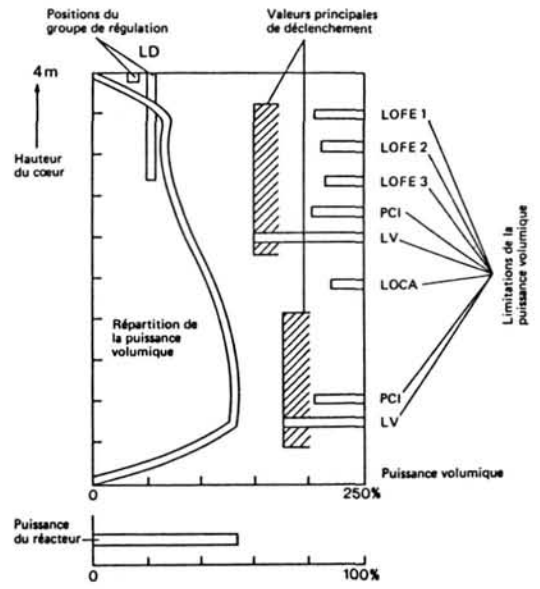
* Voir: «Safety Parameter Display Functions are Integrated Parts of the KWU-Konvoi-Process Information System (PRINS)» par W. Aleite et K.H. Geyer, communication présentée à la Cinquième réunion internationale sur la sûreté des réacteurs thermiques tenue à Karlsruhe en septembre 1984, et «Video Display Units in Nuclear Power Plant Main Control Rooms: The Process Information System KWU-PRINS» par W. Aleite, H.W. Bock et E. Rubbel, Siemens Forschungs- und Entwicklungsbericht Vol.13, N° 3 (1984).



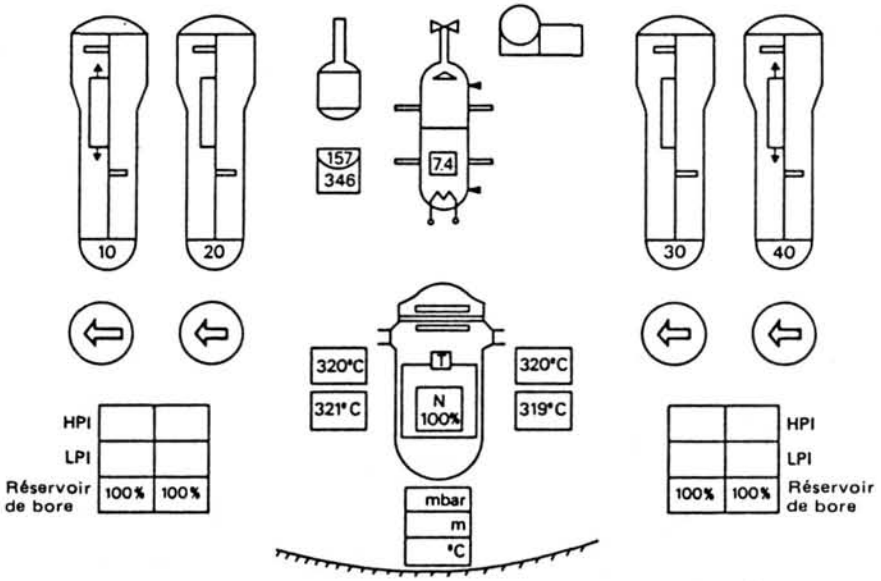

**PRINS présente l'état de tous les systèmes importants. Les systèmes auxiliaires sans relation directe avec l'exploitation — par exemple la ventilation ou le circuit de refroidissement de la fosse à combustible — sont représentés par des symboles au bas de la figure.**




**Ce diagramme de charge partielle de PRINS montre tous les états stationnaires nominaux, ainsi que les paramètres réels du fonctionnement et son historique.**




**Le schéma de la répartition et des limitations de la puissance volumique de PRINS donne les positions à jour du jeu de barres, la puissance du réacteur, la répartition verticale de la puissance volumique dans le cœur et les limitations de la puissance volumique pour les parties supérieure et inférieure du cœur.**




**L'information fournie par PRINS contient tous les principaux paramètres de fonctionnement nécessaires pour savoir si les fonctions de sûreté, la quantité requise de fluide de refroidissement et l'évacuation de la chaleur sont assurées.**

fonctionnement pour s'assurer du bon fonctionnement d'un système de sûreté. La vérification s'opérera donc automatiquement et un message ne sera émis qu'en cas de non conformité. Il en va de même en ce qui concerne les manœuvres d'arrêt. Par exemple, dans le cas d'un arrêt d'urgence de la turbine, de nombreux messages doivent arriver dans un ordre déterminé. La vérification manuelle prendrait beaucoup de temps, et c'est pourquoi elle se fera automatiquement comme on l'a vu plus haut.

### Analyse des perturbations: STAR

Un deuxième projet pilote a été entrepris à la centrale nucléaire Biblis afin de mettre à l'épreuve le système d'analyse des perturbations dénommé STAR.* Le premier essai a eu lieu à la centrale nucléaire de Grafenrheinfeld.** Vu l'abondance des publications sur l'analyse des perturbations et le système STAR nous nous bornerons ici à un bref exposé.

* «STAR – A Concept for the Orthogonal Design of Man-Machine Interfaces with Application to Nuclear Power Plants», par W.E. Büttner, L. Felkel, R. Manikarnika et A. Zapp, Conférence IFAC sur l'analyse, la conception et l'évaluation des systèmes homme-machine, Baden-Baden, septembre 1982.

** «STAR Disturbance Analysis System: Results from the Grafenrheinfeld PWR Application», Colloque international sur la commande et l'instrumentation des centrales nucléaires, Munich, octobre 1982.

La détection des incidents s'effectue au moyen de modèles. Ce sont des modèles logiques (par ex. diagramme cause-effet), physiques (équilibres des masses ou caractéristiques des systèmes ou composants), ou mathématiques (par exemple filtrage linéaire à mémoire fixe). Les modèles contiennent l'aspect attendu des événements en cas d'incident et ont leur point de départ dans une base de donnés fondamentales. Les données effectives de la centrale s'y superposent.

Le sous-programme d'analyse balaie les modèles et détecte les perturbations éventuelles. Le système STAR a pour principaux objectifs:

- de déceler les incidents le plus tôt possible, d'en déterminer les causes premières et l'évolution possible et de renseigner sur l'état du fonctionnement;
- d'annoncer l'action la plus apte à remédier à l'incident si c'est possible sans ambiguïté (cette indication ne doit pas engager l'opérateur);
- de fournir des informations au système d'analyse des perturbations;
- d'établir des modèles souples faciles à agrandir ou à modifier, qui seront peut être nécessaires pour tenir compte de l'expérience ou des modifications de la centrale.

### A l'appui du manuel d'exploitation

De nombreuses procédures figurant dans le manuel d'exploitation consistent à vérifier la validité ou l'état de certaines variables de la centrale, à les combiner de façon logique et à exécuter les actions dictées par les résultats de cette vérification. Dans ce domaine, l'emploi de systèmes informatisés s'impose à l'évidence. Des recherches préparatoires en vue d'un emploi pilote pour la surveillance des systèmes de sûreté ont été faites dans des réacteurs à eau sous pression et à eau bouillante.*

Ce système a pour principaux objectifs:

- de surveiller les systèmes de sûreté du réacteur, y compris leur alimentation en courant et leurs systèmes auxiliaires, de manière à ce que, en cas d'absence ou de défaillance d'un composant, l'on puisse déterminer si les systèmes restants répondent aux prescriptions de sûreté du manuel d'exploitation;
- en cas de défaillances, indiquer les mesures correctives ou préventives nécessaires lorsque les prescriptions de sûreté sont violées (par exemple durée admissible de la réparation; réduction des intervalles entre essais répétés des systèmes redondants);
- contrôler le temps qui reste pour réparer;
- aider l'opérateur en établissant des fiches d'exécution et de mise hors service pour les opérations d'entretien et en le renseignant sur les résultats des essais répétés ou fonctionnels (par exemple conformément aux règles KTA 1202 et 3506).* On peut montrer logiquement comment les prescriptions du manuel d'exploitation peuvent être transférées à un ordinateur et surveillées par lui.

### Conditions du succès

En résumé, ce qui justifie les activités dans le domaine des systèmes informatisés d'appui aux opérateurs, c'est la multiplication de l'instrumentation et du matériel de commande; la nécessité de décharger les opérateurs de leurs tâches de routine et de les laisser à leurs tâches de conduite et de contrôle de la centrale; la nécessité de réduire et d'aménager l'information; l'intention d'aider les opérateurs en cas d'incident ou d'accident en leur fournissant des diagnostics et des moyens de surveillance.

Dans la plupart des cas, ces tâches ne peuvent être assurées au moyen d'un matériel traditionnel. Il faut toutefois que les systèmes nouveaux soient compatibles avec la conception traditionnelle de la salle de commande, avec l'affichage de l'information et avec les prescriptions du manuel d'exploitation. Il faut avoir la certitude que tous les systèmes, les anciens comme les nouveaux, agissent de concert et s'insèrent dans un ensemble. Une phase d'essai sur simulateur de centrale devrait compléter l'expérimentation et il serait bon que les opérateurs participent activement au projet, afin d'obvier à la difficulté que présente l'action simultanée de systèmes perfectionnés qui, pour répondre aux impératifs de l'assurance de qualité, de la documentation, des essais ou des avis des spécialistes, ont été mis au point séparément.

Une autre condition indispensable du succès est l'analyse détaillée des tâches des opérateurs et la définition précise des missions des systèmes. Il faut que les systèmes d'appui offrent aux opérateurs des possibilités nouvelles. Ils ne sont pas nécessaires lorsqu'on dispose déjà de systèmes ou de procédures commodes. Les systèmes ne doivent pas donner d'ordres aux opérateurs, mais les conseiller.

Enfin il ne faut pas négliger les aspects ergonomiques.

* «Überwachung von Sicherheitsparametern durch Prozessrechnereinsatz» par H. Schüller et W.E. Büttner, Rapport GRS-A N° 916 (mars 1984).

* Prescriptions relatives au manuel d'inspection, KTA 1202 (juin 1984); Essai des commandes électrotechniques du système de sûreté des centrales nucléaires, KTA 3506 (novembre 1984).