Analyse du travail de pilotage d'une centrale nucleaire (I) : le systeme socio-technique

P. Alengry

INRIA

UNITÉ DE RECHERCHE
INRIA-ROCQUENCOURT

Institut National
de Recherche
en Informatique
et en Automatique

Domaine de Voluceau
Rocquencourt
B.P.105
78153 Le Chesnay Cedex
France
Tel.(1) 39 63 55 11

Rapports de Recherche

N° 989

Programme 8

ANALYSE DU TRAVAIL DE PILOTAGE D'UNE CENTRALE NUCLEAIRE (I) : LE SYSTEME SOCIO-TECHNIQUE

Pierre ALENGRY

Mars 1989

ANALYSE DU TRAVAIL DE PILOTAGE D'UNE CENTRALE NUCLEAIRE (I) : LE SYSTEME SOCIO-TECHNIQUE

Pierre ALENGRY

Programme 8

Ce rapport a été rédigé dans le cadre d'une recherche réalisée par le Projet de Psychologie Ergonomique de l'INRIA, et financée en partie par le Comité des Etudes Médicales d'EDF-GDF (contrat n° : 1 86 D098 00 21123 01 1).

Analyse du travail de pilotage d'une centrale nucléaire:
(I) : Le système socio-technique

Résumé:

Ce rapport présente un premier volet de l'analyse du travail de pilotage d'une centrale nucléaire, décrivant l'environnement socio-technique du pilotage. Nous décrivons successivement: (1) le processus technologique lui-même; (2) l'organisation du travail; (3) la qualification et la formation des opérateurs de conduite; (4) l'organisation de la salle de commande; (5) les outils de travail disponibles en salle de commande. Lorsque les outils sont spécifiques au domaine, nous décrivons leurs modalités d'utilisation. Une analyse des inadéquations du système homme-machine est ensuite présentée; cette analyse repose sur des observations réalisées en salle de commande ou bien sur des interviews effectuées auprès des différents opérateurs.

Mots-Clés: Conduite de centrale nucléaire - Organisation du travail - Structure de la salle de commande - Formation des opérateurs - Structure des outils de travail - Inadéquations du système homme-machine.

Work Analysis of the Nuclear Power Plant Control Room Operators
(I): The Socio-Technical System

Abstract

The aim of this report is to present a first part of the work analysis of the nuclear power plant operators. This work analysis focuses on the socio-technical environment. We describe (1) the process itself; (2) the work organization; (3) the nature of the operators' training; (4) the structure of the control room; (5) the tools used by the operators in order to control the functioning of the power plant. Some inadequations of the man-machine system, collected by observation of the operators' activity in control room, are reported.

Keywords: Nuclear power plant control activity - Work organization - Control room structure - Operators' training - Man-machine inadequations.

TABLE DES MATIERES

I - INTRODUCTION

Nous présentons dans ce rapport un premier volet de l'analyse du travail de pilotage d'une centrale nucléaire, portant sur l'environnement socio-technique du pilotage. Nous décrivons successivement: (1) le processus technologique lui-même; (2) l'organisation du travail; (3) la qualification et la formation des opérateurs de conduite; (4) l'organisation de la salle de commande; (5) les outils de travail disponibles en salle de commande. Une analyse des inadéquations du système homme-machine est ensuite présentée; cette analyse repose sur des observations réalisées en salle de commande ou bien sur des interviews effectuées auprès des différents opérateurs.

II - LE PROCESSUS TECHNOLOGIQUE

1. Fonctionnement du processus

1.1 Principe de base

Le principe de base d'un processus de production d'électricité est d'avoir en entrée une énergie donnée (hydraulique, thermique...) et en sortie une énergie électrique. Dans le cas du processus nucléaire de production d'électricité, l'énergie d'entrée est nucléaire: dans le cœur du réacteur, le combustible (les pastilles d'Uranium) est le siège de réactions en chaîne qui provoquent un important dégagement de chaleur, évacuée par caloporteur (l'eau primaire) à un échangeur de chaleur appelé Générateur de Vapeur (GV). Le GV transfère cette chaleur à un circuit d'eau (eau alimentaire) qui est transformée en vapeur. Cette vapeur est amenée sous une forte pression à la turbine où elle va se détendre et entraîner l'arbre. La turbine entraîne à son tour un alternateur qui produit l'électricité distribuée au réseau (c'est-à-dire aux consommateurs). Le cycle de transformation d'énergie est donc le suivant:

Figure 1: Cycle de transformation d'énergie

1.2 Niveau d'automatisation

La part la plus importante du fonctionnement du processus est automatisée. En fonctionnement normal à pleine puissance, l'opérateur peut n'avoir aucune action à effectuer. Mises à part les actions sur des organes (ouverture de vannes, mise en route de

pompes), les actions consistent à mettre en route des automatismes ou bien à ajuster leur fonctionnement, par la modification des points de consignes à l'aide de Relais de Commande à Main (RCM). Cependant, dans certaines configurations, l'opérateur peut avoir à conduire manuellement des sous-systèmes du processus: par exemple, lorsque la puissance est inférieure à 10% de la puissance nominale (PN), l'opérateur doit maintenir manuellement les niveaux d'eau des GV.

2. Structure du processus

Le processus peut être décrit du point de vue des systèmes qui le compose. Le nombre de ces systèmes est relativement élevé: on comptabilise environ 180 systèmes. Par exemple: le circuit primaire pressuriseur inclus constitue un système (système RCP); le circuit de ventilation continue du Bâtiment Réacteur (BR) constitue également un système (système EVR); la salle de commande elle-même est considérée comme un système (système KSC). Un système n'est donc défini ni par sa fonction générique (une pompe assure un débit, par exemple), ni par sa position dans la hiérarchie des systèmes, ni par ses caractéristiques topologiques. Un système est défini par rapport à la **fonction spécifique** qu'il exerce: un système réalise une fonction qui ne peut être réalisée par un autre système.

Un moyen pratique pour décrire le processus de production nucléaire d'électricité consiste à distinguer les 2 principaux circuits: le circuit primaire, dont la fonction est de produire de la chaleur et le circuit secondaire dont la fonction est de transformer cette chaleur en électricité. A l'interface entre les deux circuits se trouve le GV. Ces deux circuits avec leurs principales composantes sont représentés à la Figure 2.

2.1 Le circuit primaire

L'eau primaire entre à 280°C dans le cœur et en sort à 320°C et circule dans le circuit primaire dont les composantes sont: le cœur dans le réacteur; les tuyauteries (branches froides amenant l'eau primaire dans le cœur et branches chaudes évacuant l'eau primaire du cœur); le pressuriseur; les pompes primaires et la partie primaire des GV (les tubes GV en forme d'épingle). La fonction de chacune de ces composantes est la suivante: le cœur fournit la chaleur; le pressuriseur maintient une pression constante à 150 bar dans le primaire; les pompes primaires assurent la circulation de l'eau primaire et donc le refroidissement permanent du cœur; les tubes GV constituent la source chaude à laquelle la source froide va extraire les calories nécessaires pour produire de la vapeur.

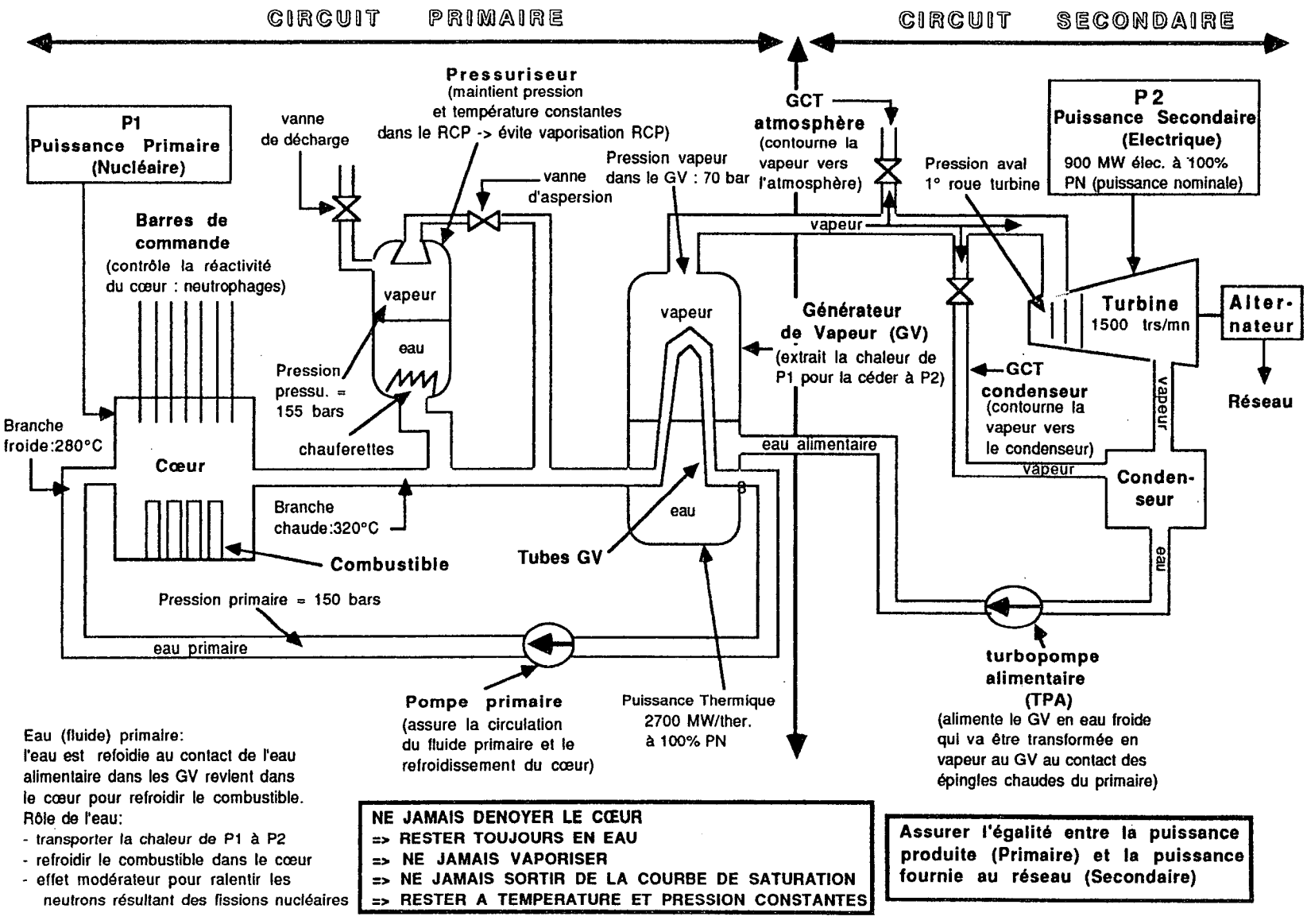

Figure 2: Représentation schématique des deux grands circuits (primaire et secondaire) et de leurs principales composantes

2.2 Le circuit secondaire

L'eau alimentaire pénètre sous pression dans les GV et, au contact de la source chaude amenée par les tubes GV, commence à se vaporiser. La sortie du GV est de la vapeur qui est amenée à une turbine. La détente de la vapeur dans la turbine provoque l'entraînement de l'arbre par l'intermédiaire des ailettes de la turbine. L'énergie ainsi obtenue est ensuite transformée, par l'alternateur, en énergie électrique qui est diffusée au réseau (c'est-à-dire aux consommateurs). La vapeur une fois passée par la turbine est amenée au condenseur d'où elle ressort en phase liquide pour être de nouveau transportée au GV. Les principales composantes du circuit secondaire sont: les tuyauteries d'eau alimentaire à l'entrée du GV et de vapeur en sortie; la turbine et ses différents organes de détente et de régénération de la vapeur (séparateurs-surchauffeurs); le condenseur et sa source froide; les Turbo-Pompes Alimentaires (TPA); un circuit de contournement de la vapeur à l'atmosphère (GCTatm.); un circuit de contournement de la vapeur au condenseur (GCTcond.). La fonction de chacune de ces composantes est la suivante: les tuyauteries transportent l'eau ou la vapeur; la turbine fournit une énergie cinétique; le condenseur condense la vapeur en eau; les TPA assure le débit d'eau alimentaire entrant dans le GV; les circuits de contournement ont pour fonction d'une part d'absorber les excédents de vapeur, par exemple lorsque la puissance électrique diminue, et d'autre part de refroidir le circuit primaire.

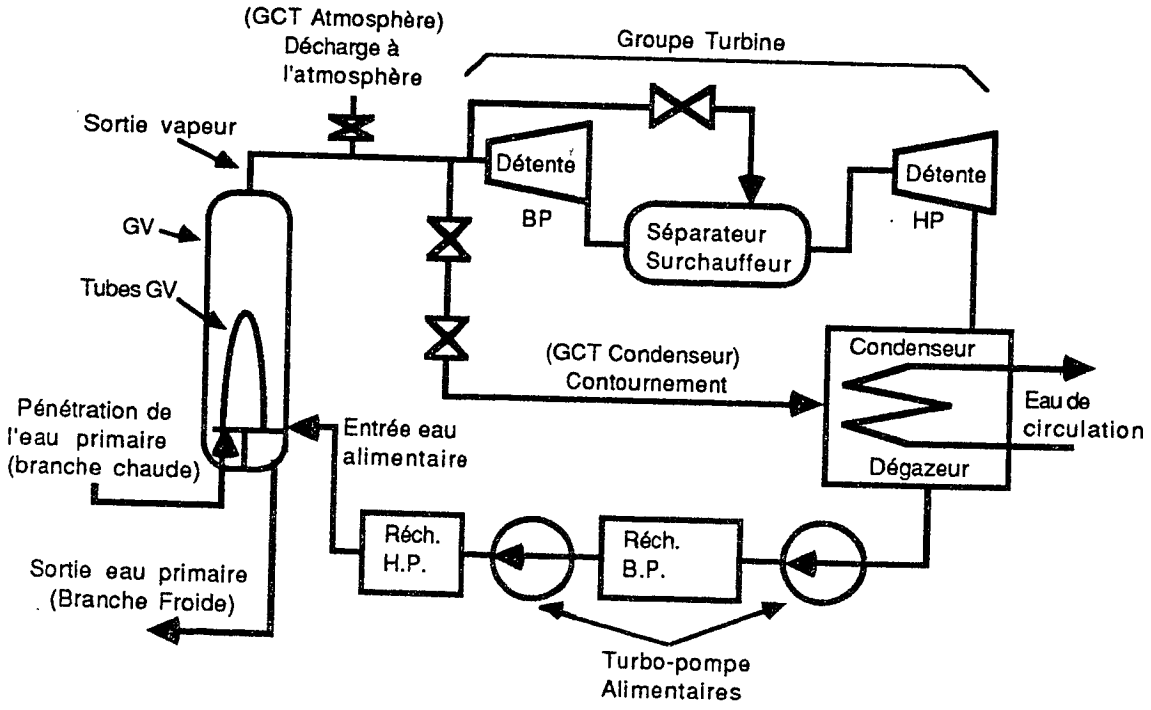

Figure 3: Représentation schématique des principales composantes du circuit secondaire

3. Objectif du processus

L'objectif général du processus est de fournir la puissance électrique exigée par le réseau de consommateurs. Cet objectif dépend de la réalisation des principaux sous-objectifs suivants: (1) équilibre des puissances primaire et secondaire; (2) respect des fonctions de sûreté; (3) maintien du circuit primaire aux conditions optimales de saturation.

3.1 Equilibre des puissances primaire et secondaire

La puissance exigée par le réseau peut être soumise à des fluctuations auxquelles doit s'adapter le processus, par la mise en œuvre de boucles internes de régulation (Figure 4).

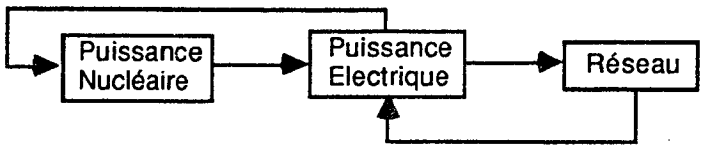

Figure 4: Schématisation des principales boucles de régulation

Le processus fonctionne en **boucle fermée** du point de vue des puissances primaire et secondaire: en toutes circonstances (par exemple, même lorsque le processus est découplé du réseau: cas de l'ilôtage) l'**équilibre** entre la puissance produite par le réacteur (appelée puissance primaire) et la puissance fournie par la turbine au réseau (appelée puissance secondaire) doit être maintenu. Le rôle des automatismes est de maintenir cet équilibre constant: des boucles internes de régulation agissent en régulant les variations de l'équilibre entre les puissances primaire et secondaire.

Les variations de cet équilibre global du processus (par exemple, lorsqu'une augmentation ou une diminution de la puissance électrique est demandée par le réseau) a pour conséquence de provoquer une succession d'états de **déséquilibres intermédiaires**[1] avant que soit atteint un nouvel état d'équilibre. Certains de ces déséquilibres intermédiaires sont régulés automatiquement par les régulations et d'autres doivent être régulés manuellement par les opérateurs. Nous avons montré (Alengry, 1988a) que la connaissance de ces états de déséquilibre est importante car elle permet aux opérateurs de prévoir, d'anticiper ou de surveiller des déséquilibres qui peuvent, s'ils ne sont pas contrôlés, empêcher l'atteinte de l'état final d'équilibre global désiré.

Dans certaines situations (accident, arrêt...), où les puissances primaire et secondaire sont nulles, cet équilibre n'est plus un objectif. L'objectif est de contrôler la réactivité résiduelle

[1] Intermédiaires parce que se produisant entre un état initial de déséquilibre et un état final d'équilibre des puissances.

du cœur afin d'éviter les problèmes de surchauffe. Ce contrôle est déterminé par les fonctions de sûreté.

3.2 Respect des fonctions de sûreté

Les critères de sûreté imposent d'éviter de relâcher des produits de fissions radioactifs dans l'environnement. 3 fonctions de sûreté doivent être en permanence maintenues pour respecter les critères de sûreté:

- refroidir le cœur
- confiner la réactivité
- contrôler la réactivité

Ces 3 fonctions sont obtenues par un ensemble de sous-fonction. Le **refroidissement** nécessite d'avoir (1) une masse d'eau; (2) une circulation; (3) une source froide. Le **confinement** dépend de l'intégrité des 3 barrières biologiques, à savoir (1) les gaines qui enveloppent le combustible; (2) le circuit primaire lui même ; (3) l'enceinte de confinement qui intègre le circuit primaire. le **contrôle de la réactivité** est réalisé par l'utilisation de produits neutrophages qui ont pour propriété d'absorber les neutrons et donc de diminuer la réactivité du cœur; ces produits sont (1) les grappes (ou barres) de commande qui peuvent être insérées ou extraites dans le cœur; (2) l'acide borique dont l'opérateur peut faire varier la dilution dans l'eau primaire.

Une cause grave pouvant conduire au rejet de produits de fissions radioactifs dans l'environnement est la montée à très haute température du combustible dans le cœur du réacteur, conduisant à la perte de l'intégrité de barrières biologiques. Pour éviter une telle montée en température, une exigence fondamentale est de maintenir les conditions de saturation dans le primaire.

3.3 Maintien des conditions optimales de saturation

Le processus nucléaire considéré est de type REP (Réacteur à Eau Pressurisée): par construction, une exigence est de rester en permanence en phase liquide dans le circuit primaire. Cela signifie d'éviter que l'eau primaire se vaporise, ce qui peut être une cause de surchauffe conduisant à des conséquences graves telles que la fusion des gaines du combustible entraînant la rupture de la première barrière biologique. Ceci implique d'avoir de l'eau qui soit sous-saturée restant en phase liquide. Les conditions de fonctionnement en sous-saturation sont établies, pour le circuit primaire:

- température moyenne (T branche chaude + T branche froide / 2) = 304°C
- pression = 150 bar

Le pressuriseur qui est connecté hydrauliquement au primaire a pour fonction de maintenir ces conditions. Cette fonction implique que les conditions du pressuriseur soient :
- température = 345°C
- pression = 155 bars

Un paramètre physique donne une indication sur les conditions de saturation dans le primaire: l'écart de température par rapport à la température de saturation (Δ T Sat.). Nous décrivons dans Alengry (1988b) comment ce paramètre est utilisé par les opérateurs en situation accidentelle.

Les objectifs décrits ci-dessus correspondent aux exigences les plus abstraites du système. L'atteinte de ces objectifs nécessite la mise en œuvre de sous-fonctions impliquant d'autres objectifs (sous-buts). Par exemple, le contrôle de la masse d'eau dans le primaire et les actions de borication dépendent d'un système: le système RCV (système de contrôle chimique et volumétrique) qui lui même met en œuvre d'autres sous-fonctions. Par ailleurs, une fonction indisponible peut être réalisée par des fonctions de substitution: par exemple, la perte de la fonction de circulation par déclenchement des pompes primaires peut être recouvrée par d'autres fonctions comme: la circulation en thermosiphon monophasique ou la création d'une brèche au pressuriseur. La mise en œuvre d'une hiérarchie de fonctions et sous-fonctions ou la recherche de fonctions de substitution peuvent être effectuées automatiquement ou bien par action de l'opérateur. Cet aspect de l'activité des opérateurs est développé dans Alengry (1988b).

III - L'ORGANISATION DU TRAVAIL

1. Structure des équipes de conduite

Le pilotage de la centrale est centralisée, c'est-à-dire que les décisions et les actions de contrôle sont prises à partir des informations et des commandes reportées en salle de commande. Cependant, un certain nombre d'informations et de commandes ne sont accessibles qu'à partir de dispositifs décentralisés situés, par exemple, en salle des machines ou dans le Bâtiment des Auxiliaires Nucléaires (BAN). Une première distinction à faire est celle des opérateurs situés en salle de commande et de ceux situés en local.

1.1 Les opérateurs de conduite en salle de commande

Un Chef de Quart (CDQ) assure la supervision des équipes de conduite; il transmet les ordres de consignation et d'essai périodique et fournit des compléments de formation sur le tas au cours de l'exécution de certaines procédures. Il participe également directement à la résolution des incidents et accidents: son rôle consiste par exemple à coordonner les actions des différents opérateurs en situation accidentelle. Il est assisté par un Adjoint Chef de Quart (ACDQ). Généralement, les CDQ et ACDQ sont des exploitants qui ont été auparavant Chefs de Bloc.

La tâche de conduite proprement dite est répartie entre les deux Chefs de Bloc (CDB) qui sont postés en permanence en salle de commande: le Chef de Bloc Principal (CDBP) et l'Assistant Chef de Bloc (ACB). Le CDBP est plutôt focalisé sur la conduite du circuit primaire et l'ACB est plutôt focalisé sur le circuit secondaire.

1.2 Les opérateurs en local

Il s'agit essentiellement des Rondiers et Agents Techniques (AT). Une caractéristique du travail de ces agents est qu'ils ont accès aux informations en local, c'est-à-dire concernant l'état physique des appareils pour lesquels les CDB n'ont pas d'information suffisamment précise ou pas d'information du tout. Leur activité se traduit par des allers et retours de la salle de commande aux différents secteurs accessibles (i.e., sauf zone rouge): Bâtiment des Auxiliaires Nucléaires (BAN), salle des machines, Bâtiment Réacteur (BR) si la centrale est à l'arrêt. Selon la zone où ils se déplacent, ils doivent ou non prendre les mesures de radio-protection nécessaires.

Un agent local est posté en permanence à la salle de commande du BAN où il dispose de moyens de contrôle et de commande (qui peuvent être redondants avec ceux centralisés en SDC ou bien spécifiques). Ils ont en outre accès à des verrines d'alarme en local concernant des appareils spécifiques. Lorsque des alarmes apparaissent en local, le rondier prévient le CDB qui décide de l'intervention à réaliser; l'alarme est acquittée par le rondier à la demande du CDB lorsque celui-ci s'est assurée que le problème est résolu. Inversement, une alarme en salle de commande peut amener le CDB à demander à un rondier d'intervenir sur un appareil en local; lorsque celui-ci a terminé son intervention, il prévient le CDB que l'alarme peut être acquittée ou devrait avoir disparu.

Parmi les actions qu'un rondier peut avoir à réaliser, on distingue:

- des actions ponctuelles, à la demande des CDB consistant à effectuer des relevés ou des vérifications sur l'état physique de certains appareils ou circuits à propos desquels le

CDB sait ou suppose qu'il se produit quelque chose d'anormal. Il peut également s'agir de réaliser certaines opérations (consignations, lignages...).

- des actions de routine consistant en des rondes systématiques pour surveiller l'état de certains appareils. Cette phase de l'activité des agents en local constitue un élément important du point de vue de la prévention et de la régulation: en effet, ils peuvent détecter certaines dérives qui ne sont pas répercutées en salle de commande (par exemple: des vibrations sur une pompe, un niveau d'huile trop bas...) et intervenir avant qu'une alarme n'apparaisse en salle de commande et que la dégradation ne s'aggrave.

Le rôle des agents locaux est essentiel dans une équipe de quart: ils constituent le prolongement perceptif et moteur de l'équipe de conduite centralisée. Ils peuvent fournir des diagnostics élémentaires et permettre d'anticiper sur des dysfonctionnements.

1.3 L'Ingénieur Sécurité Radioprotection (ISR)

La fonction de l'ISR a été instituée à la suite du retour d'expérience de l'accident de Three Mile Island. En effet, lors de cet accident, on a observé que les opérateurs pouvaient travailler sur la base d'un consensus erroné, à la fois pour ce qui est de l'état effectif de l'installation et pour la stratégie de conduite à appliquer. Le rôle de l'ISR est de scruter en permanence un certain nombre de variables d'état cruciales du point de vue de la sûreté tout en restant strictement indépendant de l'activité de l'équipe de conduite. Il n'intervient auprès d'elle que lorsque l'une des variables d'état qu'il scrute est hors de sa plage de variation autorisée: il indique alors à l'équipe ce qui ne va pas et quoi faire. L'ISR n'est en aucun cas un super CDQ mais un élément parallèle dans l'établissement du diagnostic et de la conduite accidentelle.

2. Services techniques

De nombreux opérateurs interviennent en permanence sur le processus, appartenant à différents corps de métiers tels que: les chimistes, les électriciens, les automaticiens, les mécaniciens... Ces opérateurs peuvent intervenir à la demande de l'équipe de conduite (par exemple, lorsqu'il est nécessaire de contrôler l'état chimique d'un ballon, lorsque des relayages des panneaux de contrôle sont en panne...). Ces opérateurs peuvent avoir à effectuer des essais périodiques et pour cela demander à l'équipe de conduite de disposer, à partir de la salle de commande des organes ou des circuits dans une position qui leur permet de réaliser leur travail. Lors des arrêts de tranche et des redémarrages, les interactions entre toutes les catégories d'opérateurs sont particulièrement nombreuses.

3. Les relèves

Les équipes de conduite effectuent le quart selon le principe des 3 X 8. Dans ce mode de fonctionnement, les relèves entre équipes constituent des phases cruciales du travail. Le contenu des relèves porte essentiellement sur l'état général de la centrale et de ses composantes. Les opérateurs mettent l'accent sur les matériels qui ont été rendus indisponibles au cours de leur vacation, des raisons de cette indisponibilité et des travaux qui ont été effectués. Les informations concernant des interventions d'autres services (chimistes, électriciens) en cours ou prévues sont également transmises. En général, la synthèse des informations ne reprend pas des informations anciennes, sauf s'il s'agit de problèmes importants qui sont difficiles à solutionner.

Des documents papier sont à la disposition des opérateurs pour faciliter les relèves (cf ci-dessous: § VI. 1.). Une partie du travail de la vacation consiste à remplir ces documents. Cependant, les opérateurs effectuent une transmission orale des informations importantes qui est redondante avec les informations écrites sur les documents papier. En outre, des informations n'apparaissant pas sur ces documents sont transmises, notamment pour ce qui est des alarmes présentes en salle de commande, c'est-à-dire: leur origine; le moment où elle est apparue; le contexte dans lequel elle est apparue; les actions qui ont déjà été entreprises; s'il y a un opérateur qui travaille dessus en local...

Les relèves se font à un niveau horizontal: chaque opérateur occupant un poste informe son successeur qui va occuper le même poste. on a donc l'ensemble des relèves suivantes: CDQ -> CDQ; ACDQ -> ACDQ; CDBP -> CDBP; ACDB -> ACDB; rondier -> rondier; AT -> AT. Le CDBP et l'ACDB procèdent ensuite à une synthèse.

En général, le début d'une vacation en salle de commande se décompose de la façon suivante:

- communication orale entre les opérateurs
- lecture de la main courante (état des principaux circuits (Marche/Arrêt/Indisponible)
- test systématique de l'état des voyants des verrines d'alarmes
- vérification de la position des boutons poussoirs (manu/auto)
- lecture de tout document papier se trouvant sur la table de quart (bons de Demande de Travaux, demande d'action de la part du service technique...)
- planification et préparation des interventions éventuelles devant être réalisées dans la journée (essais périodiques, modification de l'état de la centrale...).

IV - QUALIFICATION ET FORMATION

1. Qualification

Actuellement, les CDB sont généralement embauchés avec un niveau Bac ou Bac + 2 (BTS). Les rondiers sont embauchés au niveau Bac. Cependant, le recrutement peut être variables. Par exemple, des exploitants ayant une expérience des centrales thermiques peuvent être embauchés après une formation particulière. De même, un opérateur a pu être embauché comme rondier sans avoir le niveau Bac puis suivre différents échelons jusqu'aux postes de conduite en salle de commande. De manière générale, la mobilité est importante et des opérateurs de conduite peuvent devenir instructeur sur simulateur puis revenir à l'exploitation avec la qualification d'ingénieur conduite ou d'ISR.

2. Formation

Les opérateurs de conduite suivent une formation qui s'échelonne sur une série de stages comprenant des contenus théoriques et pratiques. La partie théorique des stages porte sur les phénomènes physiques sous-jacents au fonctionnement du processus (thermodynamique, neutronique, électricité, notions de régulation...). Elle peut être dispensée uniquement en salle pour les formations techniques de base ou bien en alternance avec des exercices sur simulateur. La partie pratique porte sur des exercices de pilotage soit sur des simulateurs pleine échelle, soit sur des simulateurs de fonction (c'est-à-dire d'un système particulier). Les exercices de pilotage sur simulateur sont organisés selon un plan de formation décomposé en modules (1) de pilotage en fonctionnement normal; (2) de pilotage en fonctionnement incidentel; (3) de pilotage en fonctionnement accidentel. Chacun de ces modules est d'une durée de 15 jours. En outre, les opérateurs ayant suivi tous ces modules continuent régulièrement à suivre des modules de recyclage ou de mise en situation qui sont d'une durée d'un semaine.

Un module de formation regroupe 4 stagiaires et un instructeur technique. Le principe de ces modules de formation est d'alterner les périodes en salle de cours et sur simulateur. Une situation de pilotage est d'abord préparée par les stagiaires en salle, où ils étudient la procédure de conduite qui leur semble appropriée à la situation de pilotage proposée. Cette procédure est ensuite appliquée sur simulateur par deux des stagiaires, les deux autres ayant pour fonction d'observer les deux qui pilotent afin de relever les difficultés qu'ils rencontrent. L'exercice sur simulateur est suivi d'un retour en salle où une analyse critique de la procédure de pilotage est proposée par les stagiaires observateurs sous la supervision de l'instructeur. A cette occasion, des connaissances nouvelles sont présentées par l'instructeur ou bien des connaissances supposées déjà acquises sont revues et mises à

jour. Ces connaissances portent sur la structure du processus, sur les boucles de régulation, sur les principes de la physique et sur l'utilisation des différentes consignes de pilotage.

Le contenu des modules de formation à la conduite normale, incidentelle et accidentelle est prédéfini. La formation est basée sur la compréhension par les opérateurs des phénomènes sous-jacents à la situation de pilotage étudiée. L'accent est notamment mis sur les conditions d'utilisation des consignes incidentelles et accidentelles ainsi que sur la justification de la stratégie qu'impose de suivre une consigne à un opérateur.

Le contenu des modules de recyclage est plus variable et est organisé en fonction des desiderata d'une équipe de conduite qui propose des situations pour lesquelles un approfondissement des connaissances est souhaité.

Les modules de mise en situation proposent à une équipe de conduite complète (ISR compris) des situations accidentelles complexes. Lors de ces modules, des connaissances acquises à l'occasion des autres modules peuvent être revues mais également de nouvelles comme, par exemple, l'utilisation de consignes accidentelles adaptées à des situations accidentelles les plus graves et les moins probables.

A l'occasion des différents modules de formation certains points importants de l'organisation du travail sont abordés et notamment la répartition des rôles et la coordination entre les différents opérateurs en situation accidentelle. Par exemple, c'est l'occasion pour un CDQ d'apprendre à utiliser le document coordinateur des consignes accidentelles pour synchroniser l'activité respective des autres opérateurs. C'est aussi l'occasion pour l'ISR de mettre au point l'exercice de sa fonction et d'éviter des pièges tels que l'implication dans l'activité de l'équipe de conduite proprement dite.

Par ailleurs, l'acquisition de connaissances ne se limite pas aux stages de formation mais continue sur le lieu de travail où, soit à l'occasion de l'exécution d'une procédure nouvelle, soit à l'occasion de périodes calmes, les opérateurs peuvent consulter les différents documents disponibles en salle de commande (schémas de principe, consignes de conduite, courbes descriptives de l'évolution de certains phénomènes...).

V - STRUCTURE DE LA SALLE DE COMMANDE

1. Fonction de la salle de commande

La fonction de la salle de commande (SDC) est de regrouper les organes de commande, de contrôle, de signalisation et de surveillance nécessaires au pilotage décentralisé du processus. Cependant tous ces organes ne sont pas centralisés. On peut distinguer les contrôles et commandes selon qu'ils sont centralisés ou non.

1.1 Commandes et contrôles centralisés

Une fois le matériel configuré avant le démarrage, l'opérateur peut, à partir de la salle de commande, contrôler et commander les différents matériels afin de:

- préserver le matériel lui-même, le personnel et la population environnante
- éviter des déclenchements intempestifs
- modifier le régime de fonctionnement du processus.

1.2 Commandes décentralisées et contrôles centralisés

Entre dans cette catégorie le matériel qui fonctionne entièrement en automatique et indépendamment -ment de l'état du processus.

1.3 Commandes et contrôles décentralisés

Entre dans cette catégorie le matériel qui fonctionne de manière totalement ou en grande partie découplé du fonctionnement du processus.

2. Principaux supports des contrôles et des commande

La SDC comprend deux principaux panneaux de contrôle/commande: le pupitre avant et le tableau arrière, et des synoptiques. La Figure 5 présente une vue de la salle de commande.

2.1 Organisation topologique du pupitre et du tableau

L'organisation topologique du pupitre et du tableau correspond à un double découpage, vertical et horizontal:

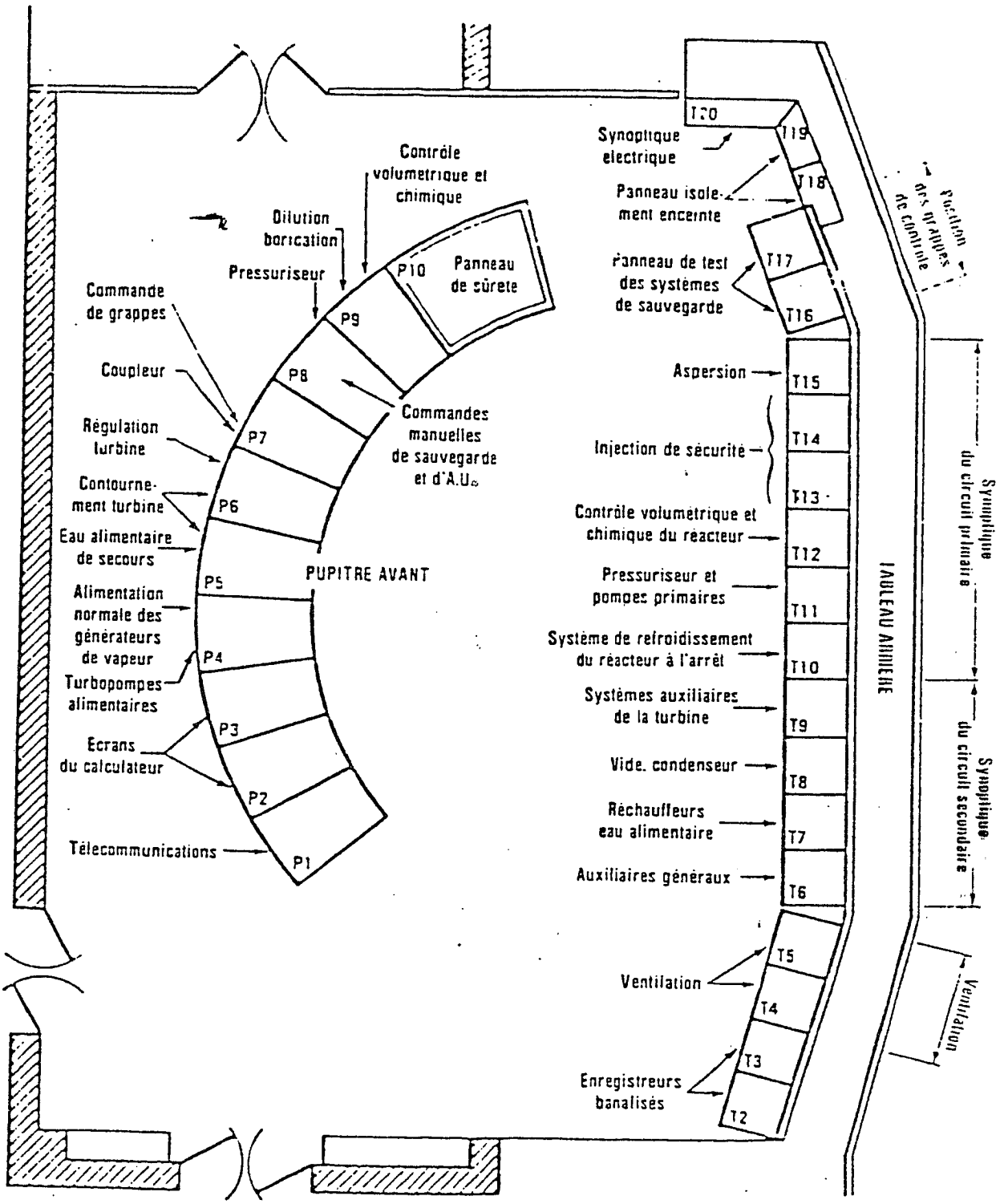

Figure 5: Organisation topologique de la salle de commande

- verticalement, le pupitre est décomposé en zones (platines) regroupant chacune des fonctions spécifiques (une dizaine de zones pour le pupitre et une vingtaine pour le tableau).

- horizontalement, trois zones peuvent être distinguées, respectivement du haut vers le bas:
    * les verrines d'alarmes (signalisation de défauts)
    * les indicateurs (enregistreurs, cadrans numériques, camemberts, échelles...)
    * les commandes (Tourner-Pousser-Lumineux - TPL-; Boutons Poussoirs - B.P. -; Relais de Commande à Main - RCM -).

2.2 Fonctions et paramètres physiques regroupés sur le pupitre et le tableau

Le **pupitre** intègre les organes de commande et de contrôle utilisés pour le pilotage en situation normale ainsi que pour les manœuvres urgentes ou fréquentes. Il met à disposition des opérateurs toutes les informations pouvant être fournies par le calculateur. Il regroupe, par platine, les principales fonctions suivantes: refroidissement; groupe turbo-alternateur; grappes de commande; pressuriseur-RCV. Du point de vue des paramètres physiques essentiels, le pupitre restitue les valeurs des: niveaux GV; débits GV et pression GV; gradient de température; niveau pressuriseur; pression primaire.

Le **tableau** intègre les organes de commande et de contrôle utilisés pour le pilotage de manœuvres exceptionnelles et peu fréquentes ainsi que les différents synoptiques. Le tableau regroupe, par platine, les fonctions suivantes: auxiliaires primaires; auxiliaires secondaire; GV alimentation en eau; poste d'eau-vide au condenseur; vapeur; pompes primaires; pressuriseur-RCV; IS-EAS, tests permissifs; isolement enceinte. Du point de vue des paramètres physiques essentiels, le panneau restitue les valeurs des: alarmes activité; indicateurs GV (niveaux + débits); indicateurs pressuriseur (niveau + pression); température branche chaude; niveau PTR; débit IS; pression enceinte.

On remarque que des indications communes à certaines fonctions sont dispersées à différents endroits du pupitre et du tableau, ce qui entraîne certains problèmes (cf ci-dessous § VII. 2.4).

2.3 Synoptiques

Les synoptiques fournissent une présentation schématique des principaux circuits du processus avec leurs connections. Des croix-morses pouvant prendre deux couleurs: rouge et vert, indiquent respectivement l'ouverture et la fermeture d'une partie d'un

circuit. La partie haute du tableau reçoit des synoptiques non actifs. Les parties latérales du tableau reçoivent les synoptiques de distribution électrique.

3. Salle de commande inter-tranches

Une tranche est une unité de production qui comprend un processus complet de production d'électricité tel qu'il a été décrit au § II. Les tranches sont couplées deux à deux et les SDC de deux tranches sont communicantes. Un local inter-tranche permet de faciliter la conduite et reçoit certains contrôles concernant du matériel commun aux deux tranches.

4. Redondance de certaines chaînes d'instrumentation

Les systèmes qui sont considérés comme critiques du point de vue de la sûreté nucléaire sont instrumentés par des chaînes dédoublées (voie A-voie B). Pour cette raison, certaines platines sont divisées en deux zones identiques reproduisant les mêmes indications pour le même système. Un commutateur permet à l'opérateur de passer d'une voie à l'autre. Cela lui permet, lorsqu'il a un doute sur la réalité d'une valeur qui lui est donnée par une voie, de confirmer ou d'infirmer cette valeur par l'autre voie: il a donc la possibilité de tester l'hypothèse d'une déficience de capteur.

VI- LES OUTILS DE TRAVAIL

Dans les outils de travail, nous distinguons: (1) les documents papier utilisés dans le travail de pilotage; (2) les commandes; (3) les contrôles; (4) les systèmes spécifiques regroupant à la fois des contrôles et des commandes. Lorsque des renseignements sur les modalités d'utilisation de ces outils ont été observés ou recueillis à partir d'une documentation, ils sont fournis.

1. Les documents papier

Différents documents papier sont à la disposition des exploitants en salle de commande.

1.1 Main courante des Chefs De Bloc

Cette main courante est utilisée: (1) en début de journée pour prendre connaissance de l'état du système; (2) en cours de journée où diverses observations sont annotées; (3) en fin de journée où les opérateurs remplissent une check-list.

1.1.1 Début de journée

Les CDB vérifient et remplissent les parties réservées aux essais périodiques (EP) concernant:

- les différents systèmes d'instrumentation
- les fuites, volumes, débits

Les appréciations possibles sont les suivantes:

- RAS (Rien A Signaler)
- DT (Demande de Travaux)
- fait (ou vu)
- indications numériques (m3/h (débit); m (niveau))

Les opérateurs procèdent également à la lecture des parties résumant l'état des principaux circuits (remplies par l'équipe précédente).

1.1.2 Cours de journée

Les CDB retranscrivent sur la main courante les différentes manœuvres d'exploitation qui sont effectuées en cours de journée, avec la date, l'heure, le système concerné et la nature de la manœuvre. Ils reportent également des indications concernant les fuites éventuelles et l'état des pompes.

1.1.3 Fin de journée

En fin de journée, les CDB remplissent les parties concernant l'état des circuits principaux, à savoir: RCP; RCV; RRA; REA; RRI; RIS; EAS; RPN; SEB; EAS; LHG; LHH; SEC; SEA; ANG; ASG; CRF; CVI; SAP. Les appréciations possibles sont les suivantes:

- M(arche)
- A(rrêt)
- I(ndisponible)

1.2 Formulaire synthétisant l'état de la tranche

Par ailleurs, l'état de la tranche est synthétisé à l'aide d'un formulaire rempli par les opérateurs en fin de journée et qui décrit l'état général de la tranche avec le matériel qui fonctionne et la valeur de certains paramètres. Ce formulaire a pour intitulé: "Etat Tranche X et communs - Situation à X heures". Ce formulaire est transmis au CDQ.

L'utilisation de ce formulaire par les opérateurs est organisée de la façon suivante:

(1) Les premières informations lues sont celles qui fournissent une description générale de la tranche:
- l'état de fonctionnement de la tranche dans les 24 heures précédentes (page 1)
- les matériels disponibles ou indisponibles en relation avec des spécifications techniques ou bien avec des critères de sûreté (page 4).

(2) Sont ensuite lues les informations décrivant de manière plus détaillée l'état de la tranche (pages 2 et 3). Cette description est hiérarchisée:

- au plus haut niveau de la hiérarchie, sont représentés les deux principaux circuits du processus: le circuit primaire et le circuit secondaire
- au niveau inférieur, sont représentées les sous-fonctions qui permettent de réaliser les fonctions remplies par les circuits primaire et secondaire
- à un niveau encore inférieur, sont représentés les matériels (ou sous-systèmes) qui permettent de réaliser les sous-fonctions avec, comme attributs:
    * leur disponibilité (disponibles, consignés, condamnés...)
    * leur état de marche (En Service/Hors Service)
    * la valeur de certains paramètres caractérisant leur fonctionnement

1.3 Main courante des agents locaux

Cette main courante reporte l'état des circuits et appareils en local. Elle est accessible aux CDB. De manière générale, la plupart des documents se trouvent à un moment où à un autre disponibles en salle de commande et tous les opérateurs peuvent y avoir accès.

1.4 Bons divers pour l'exécution de manœuvres

Ces documents concernent des consignes d'exécution de manœuvres et décrivent les spécifications pour leur réalisation; les consignes peuvent être demandées par les CDB aux agents locaux (consignation d'une vanne, par exemple) ou bien par les services techniques aux CDB (mise en recirculation d'un circuit par exemple).

1.5 Consignes d'exploitation

Les consignes d'exploitation décrivent, pour chaque système, circuit ou appareil, les rubriques suivantes:

- astreinte (électrique, mécanique...): indique les états du système qui sont exigés pour la mise en œuvre du circuit concerné (conditions de pression, de température, de volume...). Il s'agit en fait des prérequis pour l'utilisation d'un système
- préparation (électrique, mécanique...) du système: indique les action à entreprendre préalablement à la mise en route du circuit
- mise en service du système: indique les action à entreprendre pour la mise en route du circuit (instructions pas à pas, accompagnées d'observations diverses retranscrites par les opérateurs pour indiquer certaines difficultés et comment les éviter)
- arrêt du système: indique les action à entreprendre pour l'arrêt du circuit
- surveillance du système (en fonctionnement normal)
- gestion des incidents pouvant se produire sur le système
- alarmes associées au circuit avec les codes des alarmes tels qu'ils sont visualisés sur les verrines, les libellés des alarmes et leurs codes d'entrée dans le calculateur
- schéma logique décrivant le système
- courbe d'évolution des paramètres concernés
- observations diverses concernant les points suivants:
    * localisation des appareils
    * vérifications supplémentaires à entreprendre
    * consignes particulières sur une instruction
    * codes (armoires locales, verrines locales)
    * glossaire explicitant la nature des alarmes

1.6 Procédures de conduite incidentelle et accidentelle

Les procédures de conduite en situation dégradée se décomposent en deux éléments:
- une consigne cartonnée indiquant pas-à-pas, à l'aide d'un arbre de décision, les tests et actions qui doivent être réalisés pour:
    * établir un diagnostic
    * conduire une situation accidentelle.
- une règle de conduite, qui est un document pédagogique expliquant la nature des tests et actions qui sont demandés aux opérateurs.

L'entrée dans une consigne accidentelle se fait à partir d'alarmes (alarmes codées DEC - Document d'Entrée en Consigne -) ou de la mise en service de protections automatiques (Injection de Sécurité). Les consignes sont organisées en une structure hiérarchisée qui permet le passage d'une consigne à une autre.

Une consigne comprend trois phases principales:
- recherche ou confirmation des conditions (symptômes) d'entrée dans une consignes
- actions immédiates consistant à vérifier ou à confirmer le fonctionnement des automatismes
- actions différées pour atteindre deux buts successifs:
    * amener le processus dans un état stabilisé standard ou proche
    * amener le processus dans un état de repli

L'utilisation des procédures fait l'objet d'une formation très poussée dans les modules de formation à la conduite incidentelle et accidentelle. L'objectif est d'amener les stagiaires à comprendre, sur la base du comportement physique de l'installation ainsi que des stratégies relatives aux fonctions de sûreté, la stratégie qu'ils doivent appliquer dans une procédure.

1.7 Schémas de principe

Ces schémas décrivent par exemple la structure d'un circuit ou la logique utilisée dans une régulation automatique. Les opérateurs s'y réfèrent lorsqu'ils doivent exécuter certaines manœuvres, soit en temps réel, c'est-à-dire au cours du déroulement même de la manœuvre, soit pour préparer une intervention. Ces schémas sont essentiels car, selon les opérateurs, il est très difficile d'avoir une représentation exacte et exhaustive de la structure du processus. On peut ainsi observer des situations où un opérateur guide l'activité d'un autre par l'intermédiaire d'un schéma de principe:

Observation 32:
Un CDB, qui a demandé à un agent local d'effectuer une intervention sur un circuit, suit les actions de ce dernier en communiquant avec lui par téléphone et lui fournit, à l'aide d'un schéma de principe, des informations complémentaires concernant la localisation des organes sur lesquels il faut intervenir.

Enfin, dans les périodes calmes, les opérateurs consultent fréquemment ces schémas afin de parfaire leur connaissance du système; de manière générale, les documents qui sont disponibles en salle de commande constituent un support permanent pour la formation des opérateurs.

1.8 Les fiches d'alarmes

Les fiches d'alarmes sont des documents archivés auxquels les opérateurs peuvent se référer pour avoir des informations complémentaires sur une alarme. La recherche d'une fiche fiche d'alarme s'effectue selon les codes d'accès suivants:

- un chiffre indiquant la tranche sur laquelle est implantée l'alarme
- un trigramme désignant le circuit concerné par l'alarme (RCV, RRI...)
- des caractères alphanumériques complémentaires (00AA19)

Le contenu d'une fiche d'alarme indique:

- le ou les défaut(s) pouvant être à l'origine de l'alarme
- les conséquences possibles de l'apparition de l'alarme
- les actions à entreprendre

2. Les commandes

L'ordre de grandeur du nombre de commandes disponibles en salle de commande (toutes voies confondues) est d'environ 500.

Les commandes disponibles en salle de commande sont essentiellement de 3 types: Relais de Commande à Main (RCM); Relais de Commande Intermédiaire (RCI); Tourner-Pousser Lumineux (TPL); Boutons Poussoirs (BP).

Les RCM et RCI sont des organes de commande qui envoient des ordres pris en compte par des régulations automatiques (par exemple, modifier un point de consigne). Les BP interviennent dans les procédures d'acquittement des klaxons et des verrines d'alarmes. Les BP sont utilisés également pour l'enclenchement de protections automatiques (Arrêt

d'Urgence, par exemple): dans ce cas, ils sont protégés par un cabochon. Les TPL constituent des organes de commande dont l'apprentissage est un peu plus complexe: nous en décrivons les modalités d'utilisation ci-dessous.

La position d'un TPL à 9 heures correspond à un mode d'arrêt et, à 12 heures, à un mode de marche. Cependant, l'ordre de marche n'est effectif que si il a été confirmé par une action "pousser". La signalisation lumineuse d'un TPL comprend 2 états: "plein feu" et "feu éteint". L'état "feu éteint" indique une concordance entre la position du TPL et celle de l'actionneur commandé. L'état "plein feu" indique une discordance entre la position du TPL et celle de l'actionneur commandé. Une discordance peut signifier:

- le mauvais positionnement d'un actionneur dont le TPL est positionné correctement (cas d'un déclenchement sur défaut)
- le bon positionnement d'un actionneur dont le TPL est mal positionné (cas d'un ordre automatique)
- la préparation d'un ordre par l'opérateur
- une manœuvre en cours d'exécution due à un ordre de l'opérateur depuis le TPL.

L'une des actions systématiques que réalisent les opérateurs lorsqu'ils prennent leur quart est de vérifier l'état des TPL de la salle de commande.

3. Les contrôles

Les informations retransmises en salle de commande concernent:

- des valeurs de paramètres physiques
- des positions d'organe

3.1 Nombre et type d'informations retransmises en salle de commande

Environ 5800 sorties binaires (TOR) et 950 sorties analogiques sont retransmises en salle de commande.

Les sorties TOR concernent:

- les alarmes
- les voyants
- les croix-morses des synoptiques
- les signalisations des TPL

Les sorties analogiques concernent les paramètres physiques dont les valeurs sont affichées sur les enregistreurs, indicateurs analogiques et alphanumériques.

Une sortie analogique peut être traitée par le calculateur comme une sortie TOR (par exemple, quand un paramètre physique dépasse un seuil et fait apparaître une alarme).

Une sortie analogique peut être calculée à partir d'autres sorties analogiques (par exemple, la température moyenne est calculée à partir de la température des 3 branches chaudes).

On distingue les valeurs analogiques selon que leur instrumentation est simple ou complexe. Par exemple, une pression est une valeur analogique simple: elle est calculée directement à partir des variations de l'état d'une membrane. Un niveau est une valeur analogique complexe: le calcul d'un niveau est en effet calculé à partir d'une pression puis est pondéré par des facteurs de variations thermiques, car un niveau ne peut être calculé dynamiquement. Cette distinction est importante car elle détermine (par exemple dans la stratégie prescrite par les consignes accidentelles) le choix des valeurs qui doivent être prises en compte pour faire un diagnostic. Ceci explique l'écart qu'on peut observer entre la stratégie de diagnostic mise en œuvre dans une consigne et la stratégie explicitée par les opérateurs: ceux-ci peuvent traiter informellement des valeurs analogiques différentes d'une consigne, parallèlement à l'utilisation de celle-ci. Nous présentons dans Alengry & Pierret (1988) quelques éléments montrant que la logique du diagnostic représentée par les consignes et la logique du diagnostic des opérateurs peuvent différer. Nous montrons notamment que les opérateurs utilisent une représentation hiérarchique des classes d'accident ainsi que des heuristiques permettant d'explorer cette hiérarchie. Ces heuristiques portent sur des valeurs analogiques non prises en compte par les consignes.

3.2 Types de présentation d'information

3.2.1 Enregistreurs

L'évolution de certains paramètres est enregistrée sur des rubans papier. Environ 100 enregistreurs[2] sont réparties sur les différentes platines de la salle de commande. Les opérateurs y ont recours dans les principaux cas de figure suivants:

- après avoir lancé une commande, pour vérifier que celle-ci:
    * est effectivement suivie d'un effet et/ou

[2] La comptabilisation des contrôles et des commandes a été faite sur un simulateur pleine échelle (simulateur CP2 du Centre de Formation du Bugey d'EDF). Selon les estimations ces chiffres doivent être augmentés de 20% pour avoir une approximation quantitative par rapport aux salles de commande réelles.

* pour contrôler que l'action n'entraîne pas une dérive trop importante par rapport au seuil requis
* s'assurer que le système rejoint bien l'état désiré

- lors de contrôles de routine pour identifier d'éventuelles dérives
- dans un objectif de planification, par analyse des évolutions passées pour en extrapoler une évolution future

3.2.2 Indicateurs numériques

Le nombre d'indicateurs numériques s'élève à environ 40. Ils donnent une valeur pour les paramètres physiques suivants: Δ TSat.; T RIC Max.; pression primaire; borication/dilution; 16 indicateurs de position des sous-groupes des barres de commande; puissance électrique (MW); puissance nominale (%); vitesse turbine; pression vapeur barillet & pression consigne; vitesse TPA (X 2); taux de fuite RCP; boremètre; vitesse pompes primaire (X 3).

3.2.3 Indicateurs analogiques

On comptabilise environ: 160 camemberts ou échelles et 50 ampèremètres. Certains de ces indicateurs analogiques fournissent un information équivalente à celles fournie par certains indicateurs numériques.

Un autre type de support d'information sont les alarmes.

3.3 Les alarmes

Les alarmes sont des sorties TOR (qui peuvent être issues de sorties analogiques). Le nombre des alarmes potentiellement actives en salle de commande est de l'ordre de 1200. Sur un accident, il peut y avoir jusqu'à 200 alarmes allumées simultanément.

L'exhaustivité des alarmes n'est pas centralisée en salle de commande. Cet aménagement permet de réduire la quantité d'information en salle de commande mais pose un problème lié à la dispersion des contrôles (cf § VII. 2.4.1.).

3.3.1 Codage couleur des alarmes

Quatre couleurs sont utilisées pour coder les alarmes selon leur degré de gravité et de l'urgence des interventions que doivent réaliser les opérateurs.

a) Alarmes blanches

Ce sont les moins prioritaires: elles fournissent plutôt une information concernant l'état d'un circuit (par exemple qu'un circuit est passé sur un système de secours).

Observation 33:
Une alarme blanche apparaît: "Niveau anormal réchauffeur 3 file 1". Cette alarme signifie que pour le circuit concerné, l'évacuation des purges se fait par le système de secours (ordre automatique). Ceci entraîne des pertes de calories et un opérateur conclut qu'il faut voir ce qui se passe effectivement, mais n'entreprend pas d'action immédiate ("à la fin de la journée, cette alarme doit disparaître").

b) Alarmes jaunes

L'intervention peut être différée mais moins que pour les alarmes blanches (30 mn - 1h).

c) Alarmes rouges

Ces alarmes nécessitent un intervention immédiate. Par exemple, l'alarme indiquant l'ouverture du sas du bâtiment réacteur nécessite une intervention d'urgence.

d) Alarmes vertes

Une alarme verte indique la mise en service d'une protection automatique (IS, EAS, AU...). Lorsqu'une alarme de cette couleur apparaît, il est trop tard pour les opérateurs. Cependant, cela ne signifie pas qu'ils ne font rien: ils doivent vérifier le fonctionnement de l'automatisme et confirmer certaines actions pour s'assurer que l'automatisme dispose bien des conditions logiques qui lui sont nécessaires et qui pourraient être absentes.

3.3.2 Codage alphanumérique des alarmes

Chaque alarme a un code alphanumérique (par exemple: 4 RCP 0019AA) qui permet au CDB d'identifier le libellé exact de l'alarme en se référant aux fiches d'alarmes.

Le premier chiffre indique la tranche à laquelle appartient le système concerné par l'alarme. Par exemple: le chiffre 4 indique qu'il s'agit d'un système spécifique à la tranche 4, un 5 à la tranche 5 et un 9, un système commun aux deux tranches.

Le trigramme qui suit le premier chiffre désigne le système concerné. Par exemple: RCP pour circuit primaire.

3.3.3 Libellé des alarmes

Les libellés des alarmes peuvent être retranscrits par un mot entier ou bien par une abréviation, comme, par exemple: PISC. REACT (pour piscine réacteur) ou PISC. DESAC. (pour piscine de désactivation).

Des icônes peuvent être présentés sur les alarmes. Par exemple, une flèche montante indique qu'un niveau, une pression, un volume ou une activité augmentent.

Parfois l'indication fournie sur une alarme ne spécifie pas le sens d'une évolution anormale. On peut trouver, par exemple: "niveau anormal". Pour connaître dans quel sens évolue le paramètre concerné, le CDB doit prélever des informations complémentaires (indicateurs, informations locales).

3.3.4 Alarmes regroupées

Certaines alarmes indiquent que plusieurs défauts peuvent être à l'origine de leur apparition en SDC. Les différents défauts pouvant être à l'origine d'une alarme regroupée sont recensés dans les fiches des alarmes. Lorsqu'une alarme regroupée apparaît, le CDB (même s'il a une idée assez précise du défaut qui peut être en cause) demande à un rondier d'aller effectuer des vérifications en local afin d'identifier plus précisément la cause de l'alarme. Les alarmes regroupées peuvent être une source de difficultés pour l'analyse de l'état du processus (cf § VII. 2.3.1).

3.3.5 Conditions d'activation des alarmes

Une alarme peut être activée:

- sur une information brute indiquant:
    * un dépassement de seuil
    * un mauvais positionnement d'organe

- sur une conjonction des deux types d'informations ci-dessus. Par exemple: bas niveau ET pompe en service.

3.3.6 Comportement et acquittement des alarmes

Une alarme se signale par la mise en service d'un avertisseur sonore (klaxon) et par l'allumage de la lampe d'une verrine. Des boutons poussoirs (BP) permettent d'acquitter respectivement le klaxon et la verrine.

Trois cas de figure doivent être vus pour le comportement d'une alarme selon que le défaut en cause est (1) fugitif; (2) permanent; (3) annulé.

a) Défaut fugitif

L'apparition d'un défaut fugitif se manifeste par un klaxon et par un clignotement lent de la verrine. L'acquittement du klaxon provoque l'extinction de celui-ci puis l'acquittement de la lampe provoque l'extinction de la verrine.

b) Défaut permanent

L'apparition d'un défaut permanent se manifeste par un klaxon et par un clignotement rapide de la verrine. L'acquittement du klaxon provoque l'extinction de celui-ci puis l'acquittement de la lampe fixe la verrine en position allumée.

c) Défaut annulé

L'annulation d'un défaut se manifeste par un klaxon et par un clignotement lent de la verrine. Au bout de 3", le klaxon disparaît puis l'acquittement de la lampe fixe la verrine en position éteinte.

3.3.7 Traitement des alarmes

Une alarme est rarement traitée seule: elle est analysée en relation avec d'autres alarmes ou indicateurs pour être validée et pour en extraire la signification effective du point de vue de l'état du processus. Le traitement d'alarme procède donc par construction de l'information pertinente et par recoupement de plusieurs sources d'information. Par exemple, si une alarme n'est pas concordante avec une évolution attendue du paramètre physique associé, l'opérateur peut faire des tentatives de commutation de voies pour vérifier qu'un capteur n'est pas hors-service. Ce traitement implique une bonne connaissance à la fois des principes de fonctionnement du processus et des éléments de l'interface homme-machine.

Dans certaines situations (incident, arrêt de tranche) de nombreuses alarmes peuvent apparaître. Dans ce cas, la difficulté pour les opérateurs réside dans la densité des

informations et dans la possibilité de discriminer les alarmes pertinentes des autres. Une alarme n'est pas pertinente lorsqu'elle n'a pas de défaut réel à l'origine. Par ailleurs, une alarme peut être pertinente mais n'être que la conséquence d'un défaut en amont déjà signalé par une autre alarme: dans ce cas, le problème réside dans les ordres de priorité à accorder aux alarmes. Les opérateurs sont aidés dans cette tâche par un dispositif, le panneau de sûreté (cf ci-dessous, § 4.1), qui fournit entre autres le premier défaut.

La situation la moins confortable est celle où les sources d'alimentation électrique des panneaux de contrôle sont perdues. Dans un incident réel et assez grave de ce type, il y a eu environ 250 alarmes qui se sont allumées simultanément avec impossibilité de recouper ces alarmes avec les informations fournies par les indicateurs, également alimentés par la source perdue. Des procédures accidentelles existent qui fournissent aux opérateurs une stratégie à laquelle ils peuvent se raccrocher dans ses situations. Cependant ces procédures, comme les autres, ne prennent en considération que des cas enveloppe, c'est-à-dire bien modélisés, et ne traitent pas les situations intermédiaires ou les cumuls d'incidents qui sont des situations floues et complexes (cf Alengry & Pierret, 1988). Dans l'incident mentionné ci-dessus, les opérateurs avaient des consignes d'exploitation qui ne s'adaptaient pas à la situation effective: ils ont réussi à résoudre l'incident en utilisant deux principes fondamentaux:

- laisser au maximum fonctionner les automatismes (le principe de base étant que tant que l'état effectif du processus n'est pas connu, toute action réalisée en aveugle risque de dégrader encore plus l'état du processus)
- appliquer une conduite par état (suivi de la température primaire et de la marge à la saturation).

Par ailleurs, l'acquittement trop systématique des verrines peut entraîner des problèmes comme, par exemple, faire disparaître des alarmes qui sont des conditions pour entrer dans une consigne incidentelle. C'est par exemple le cas des alarmes codées DEC (Document d'Entrée en Consigne).

3.3.8 Fonction des alarmes

L'apparition d'une alarme a pour fonction essentielle d'activer l'opérateur et de lui signaler que quelque chose d'anormal est peut être en train de se produire.

Par construction, les centrales de ce type ont été étudiées pour fonctionner à "schéma éteint", c'est-à-dire sans alarme allumée. Par construction toute alarme allumée est donc a priori "anormale".

Cependant, la normalité d'une alarme est relative. En effet, des alarmes peuvent être normales selon la configuration actuelle du processus. Ainsi, en arrêt de tranche, des alarmes peuvent signifier non pas un défaut mais la mise hors-service d'un système qui doit normalement être dans cet état dans la configuration donnée. Des aménagements ont été réalisés pour faciliter la conduite en arrêt de tranche: un panneau regroupant les contrôles spécifiquement appropriés à cette situation est ajouté aux autres panneaux pour permettre aux opérateurs de se focaliser sur les informations essentielles.

L'observation reportée ci-dessous montre un cas de figure où des impératifs de productivité et de coût amène les opérateurs à conduire en situation normale à pleine puissance avec des alarmes allumées:

> Observation 34:
> Sur un panneau de contrôle d'une tranche fonctionnant à pleine puissance, 5 alarmes restent allumées en permanence: elles correspondent à une action de déconnection d'une chaîne de mesure intermédiaire qui est usée et que les opérateurs veulent ménager. Cette chaîne de mesure n'est pas utile en puissance et peut rester inutilisée jusqu'à une prochaine baisse de puissance.

4. Dispositifs spécifiques

4.1 Panneau de sûreté (KPS)

Ce dispositif a été implanté depuis peu en salle de commande. Le principe sous-jacent à sa conception est de fournir à l'opérateur en situation accidentelle un regroupement des contrôles considérés comme essentiels du point de vue des fonctions de sûreté.

Dans sa partie haute, le KPS reçoit 12 voyants sur deux voies et 2 indicateurs numériques. Les voyants donnent les informations suivantes: aspersion; isolement enceinte 1° phase; isolement enceinte 2° phase; isolement vapeur; Injection de Sécurité; Arrêt d'Urgence; arrêt pompes primaires; isolement ARE & déclenchement TPA; démarrage MPS-ASG; démarrage TPS-ASG; déclenchement Turbine; ilôtage. Les indicateurs numériques donnent une information sur la marge à la saturation (Δ TSat) et sur la température du cœur (T RIC Max.). Par ailleurs 2 voyants intitulés "Marge à la saturation" et "Surchauffe" donnent une information redondante par rapport aux 2 indicateurs numériques.

Les parties médiane et basse du KPS sont réservées à une zone de dialogue. Dans sa partie médiane, le KPS reçoit 2 écrans où les opérateurs peuvent appeler différentes informations (premier défaut, consigne de diagnostic A.0; grilles d'arrêt de l'Injection de

Sécurité...). Dans sa partie basse le KPS reçoit deux claviers alphanumériques permettant d'appeler les images des écrans, de valider la consigne A.0...

4.2 Kit d'imprimantes

Le kit est un ensemble constitué de trois imprimantes ayant chacune une fonction particulière:

- mis en suivi de l'évolution de certains paramètres. Lorsqu'ils effectuent certaines manœuvres, les opérateurs peuvent avoir besoin de surveiller à fréquences régulières et rapprochées l'évolution des paramètres concernés par la manœuvre
- relevé systématique des paramètres hors-tolérance. L'apparition d'un paramètre hors-tolérance au kit est accompagné d'un signal sonore
- retranscription du libellé des défauts corrélés avec certaines alarmes (codées K).

4.3 Téléphones

Sept moyens de communication téléphonique sont à la disposition des opérateurs en salle de commande; ils sont repérés par leur couleur:

- Orange: reliée au dispatching
- Orange (2): reliée aux services du dispatching
- Blanc et gris: communications internes
- Interphone: BR, BAN, SAS, poste du CDQ
- Petit orange: Plan d'Urgence Interne
- Rouge (hors platine): incendie

4.4 Tableau indicatif des régimes de repli relatifs à la sûreté

L'existence de ce tableau est justifiée par les consignes de maintenance préventive en fonctionnement en puissance. Ces consignes concernent les états de sûreté du matériel définies par la consigne I.0. Cette consigne intègre les différentes contraintes administratives réglant juridiquement le fonctionnement d'une centrale nucléaire: par exemple, pour un appareil indisponible, une date limite est requise au-delà de laquelle on ne peut plus accepter de fonctionner en puissance à l'état-standard n°9. Ces consignes indiquent les régimes de repli de l'installation en cas d'indisponibilité des matériels relatifs à la sûreté nucléaire.

Ce tableau constitue une mémoire permanente de l'état de l'installation en relation avec la sûreté. La figure 6 représente les informations qui peuvent être retranscrites par les opérateurs sur ce tableau dans une situation où la tranche avait commencé son démarrage quelques jours auparavant.

CONSIGNE I0 - Respect du domaine de fonctionnement autorisé
Tr. 4

Syst	Evènement	Date	Heure	Etat Initial	Etat à Rejoindre	Date Heure	Observations
LHH	Consigna°	5/11	1h00	9	5	8/11 1h00	rentré le 5/11 à 14h20
LHG	Consigna°	5/11	15h00	9	5	8/11 15h00	rentré le 5/11 à 15h40

CHIMIE

	Date	Co
REA 04BA	5/11	7460 ppm
REA 03BA	25/11	8380 ppm
PTR BK	5/11	2240 ppm
RIS 04BA	4/11	21880 ppm
RCP	6/11	auto 978
Bormètre	6/11	manu 1100

ligne sur boucle 2
Activité 23/10
(RCP EQI 131) 26.10 -3 C/m

PILOTAGE

	Date	
burn up		MWJ/T
limite mini inser°	31/10	212pas

INFORMATIONS SURETE

INFORMATIONS DIVERSES

BR Salle des machines BAN

CARTE DE FLUX

Effectuée le 2/11/85 N° 4 à 87% PN
Réglage coeff. chaînes RPN
fait le :

Figure 6: Exemple d'un état possible du tableau I.0

4.5 Ecrans d'aide à la conduite immédiate et différée

2 écrans vidéo fournissent des informations soit directement, par affichage automatique, soit à la demande des opérateurs, par un système de dialogue commandé par clavier alphanumérique. Les informations affichées automatiquement concernent: (1) les variables analogiques qui dépassent un seuil fixé; (2) les variables TOR entrant dans les automatismes et expliquant les discordances signalées par les TPL. Les informations affichées à la demande de l'opérateur concernent tout ce qui a trait au fonctionnement instantané du processus en vue d'une action différée (suivi des variables en évolution, fonctions spécifiques...).

VII - INADEQUATIONS DU SYSTEME HOMME-MACHINE

Nous recensons ci-dessous quelques-unes des inadéquations du système homme-machine qui ont été identifiées au cours d'observations menées en salle de commande ou qui ont été rapportées dans des interviews avec les différents opérateurs. Ces inadéquations concernent principalement la structure des communications et des outils de travail. Il s'agit d'un diagnostic succinct du système socio-technique. L'objectif n'est pas ici de faire une analyse exhaustive de ces difficultés ni d'identifier systématiquement les solutions qui pourraient leur être apportées. Cependant les points relevés ci-dessous nous semblent importants, car ils sont susceptibles d'avoir une influence sur la qualité du travail de pilotage et donc sur la sûreté.

1. Inadéquations liées à la structure des communications

Les communications peuvent être internes à la salle de commande ou s'étendre aux opérateurs en local ou encore à des services administratifs et techniques. Nous nous intéressons ici aux communications "salle de commande" <-> "local".

La fréquence des communications dans la salle de commande est relativement élevée selon la configuration de la tranche ou bien le moment de la journée. Les facteurs qui peuvent faire varier cette fréquence sont les suivantes:

- relèves
- ordres de consignation
- incidents
- arrêts de tranche
- exécution des essais périodiques

Les supports de ces communications sont soit les échanges téléphoniques, soit les échanges verbaux directement entre opérateurs. Les communications ont essentiellement un aspect opératif: elles correspondent à quatre principaux objectifs que ce soit dans le sens salle de commande -> local ou inversement:

- demander des informations
- demander une intervention sur un système
- confirmer qu'une opération demandée a bien été effectuée
- prévenir que l'état d'un système a été (ou risque d'être) modifié.

Par exemple:

Observation 1:
- "je fais une soudure. Si vous avez une détection incendie, ne vous inquiétez pas" (local - > salle de commande).
Observation 2:
- (à propos d'une chaudière) "la une est plantée" (salle de commande - > local).
Observation 3:
- "tu peux me mettre le RRI en manu, j'ai une régu à changer" (local - > salle de commande); "j'ai vu que ce matin il y a eu des manips; ok, tu la reprends en bas" (salle de commande - > local).
Observation 4:
- "c'est bon avec les alarmes, j'ai fini" (local - > salle de commande).
Observation 5:
- "sur TEG on a un défaut, tu peux regarder ce que c'est?" (salle de commande - > local).

Les difficultés et problèmes relatifs à la structure des communications sont les suivants.

1.1 Ambiguïté des messages

Les messages peuvent être ambigus ou peu explicites et risquer d'entraîner l'exécution d'actions non désirées comme on le voit dans l'exemple qui suit:

Observation 6:
Un chef de bloc reçoit en salle de commande un appel d'un opérateur situé en local qui lui demande s'il lui a bien demandé d'inverser les circuits 2 et 3. Celui-ci répond par la négative et se retourne vers son assistant pour lui demander si c'est bien lui qui a envoyé cet ordre. Ce dernier lui répond que non.

Ce que suggère ce type de situation, c'est qu'il peut y avoir des confusions soit sur le destinataire ou l'émetteur d'un message soit sur la terminologie utilisée par les opérateurs. Dans ce second cas de figure, le problème peut traduire une absence de phraséologie: les opérateurs n'utilisent pas un lexique identique pour désigner les mêmes objets.

1.2 Non transmission de l'information pertinente

Ce problème apparaît surtout lorsque plusieurs relais interviennent dans la transmission de l'information. Il s'agit de situations qui peuvent être illustrées par l'exemple suivant, qui implique au moins quatre relais de communication:

Observation 7:
"Si tu vois untel tu le préviens que s'il a besoin de vapeur, que quelqu'un est en train d'intervenir sur l'évap".

Un exemple est donné par les demandes de modification dont la transmission passe par plusieurs personnes:

> Observation 8:
> Un opérateur remarque qu'entre le moment où une demande de modification est partie et son retour, elle subit des transformations telles qu'il peut se produire que la modification effectuée ne corresponde plus à ce qui a été initialement demandé.

Le risque est qu'à chaque relais, l'information est susceptible d'être tronquée, déformée voire non transmise. Cette multiplication des relais peut être mise en relation avec la difficulté que rencontrent parfois les CDB à localiser les opérateurs dont ils ont besoin pour effectuer une intervention en local.

1.3 Difficulté de localisation des opérateurs

> Observation 9:
> Il est apparu que lorsque les CDB ont besoin d'un opérateur pour réaliser une intervention, ils ne parviennent pas toujours à le localiser. Ils sont alors contraints de multiplier les appels pour retrouver l'opérateur concerné.

La conséquence est que les CDB ne sont pas toujours en mesure d'effectuer les actions nécessaires au moment approprié et que les délais d'intervention peuvent augmenter.

1.4 Identification d'un opérateur par rapport une tranche

Ce problème concerne les communications dans le sens local -> salle de commande. Lorsque les agents en local contactent un CDB en salle de commande, ils ont besoin de s'assurer que le CDB avec lequel ils communiquent est bien celui qui pilote la tranche sur laquelle ils sont en train d'intervenir. Or il peut parfois y avoir des confusions comme par exemple dans la situation suivante:

> Observation 10:
> Un CDB Principal de l'une des deux tranches remplace momentanément son collègue sur l'autre tranche. Un agent en local appelle cette tranche mais identifie la voix du CDB remplaçant et croit s'être trompé de tranche. L'agent en local interrompt la communication et refait son appel.

Il existe d'autres problèmes de ce type qui sont liés au couplage des tranches, comme on le voit ci-dessous.

1.5 Identification de la tranche sur laquelle une intervention est nécessaire

Le fait que certains circuits et appareils soient communs aux deux tranches peut être une source de confusion:

> Observation 11:
> Selon les commentaires des opérateurs, il s'est déjà produit qu'en intervenant à la demande d'un CDB sur un circuit commun aux deux tranches un opérateur en local ait effectué un lignage dans le mauvais sens, c'est-à-dire, par exemple, orienté un débit vers la mauvaise tranche.

Les opérateurs ont développé spontanément des moyens du type de ceux mis en œuvre dans l'aéronautique pour atténuer les confusions inhérentes aux deux problèmes décrits ci-dessus:

> Observation 12:
> Lors des appels téléphoniques, le opérateurs associent systématiquement à leur nom le numéro de la tranche qui est sous leur responsabilité. De même, ils confirment à plusieurs reprises un message pour s'assurer qu'il a été bien compris.

1.6 Interférences avec d'autres équipes intervenant sur le système

Certaines interventions réalisées en local peuvent modifier l'état du système et déclencher des alarmes en salle de commande:

> Observation 13:
> Un CDB voit apparaître une alarme (activation importante des purges GV1). Il entreprend diverses actions, notamment sur le circuit APG. Il finit par apprendre qu'une équipe est en train de souder à l'argon dans le secteur: les chocs provoqués par la soudure ont été enregistrés par les instrumentations et ont déclenché l'alarme.

Les interférences créées par des équipes intervenant sur le système ont pour conséquence de faire apparaître des "fausses" alarmes, c'est-à-dire qui ne sont associées à aucun défaut effectif. Ce type de situation se produit souvent selon les opérateurs, par exemple:

> Observation 14:
> Une intervention locale engendre de la fumée: celle-ci est détectée par des capteurs qui déclenchent une alarme incendie.

La conséquence est que si le CDB n'est pas prévenu que des interventions risquent de déclencher des alarmes, il peut mettre en œuvre des procédures de diagnostic et de régulation qui ne sont pas justifiées. Cependant, un risque plus important est que ces "fausses" alarmes peuvent masquer des alarmes réelles apparaissant simultanément.

1.7 Augmentation de la charge de travail mental

Une remarque générale que l'on peut faire à propos du travail des CDB est que dans certaines situations, même en fonctionnement normal, leur charge de travail peut être relativement élevée:

> Observation 15:
> Plusieurs tâches peuvent être effectuées simultanément: essai périodique, intervention à la demande du service technique, contrôle de la réalisation d'une consignation, surveillance de l'évolution d'une dérive, check-list...

Le traitement en temps partagé de plusieurs tâches constitue, selon certains opérateurs, l'une des principales difficultés pour le CDB novice qui débute en salle de commande: la difficulté est d'apprendre à attribuer des ordres de priorité aux différentes tâches.

La fréquence élevée des communications peut être un facteur d'augmentation de la charge de travail mental:

> Observation 16:
> Lorsqu'ils sont sollicités par un appel téléphonique ou directement par un opérateur, les CDB doivent interrompre l'action qui est en cours et mémoriser l'état dans lequel ils ont abandonné cette action pour pouvoir la reprendre une fois terminée l'intervention relative à l'interruption.

Les CDB mettent particulièrement l'accent sur ce problème pour les situations d'arrêt de tranche (où ils soulignent qu'il y a en moyenne 50 ordres de consignation donnés dans la même journée) ou bien pour celles qui nécessitent des interventions complexes et pour lesquelles ils souhaiteraient ne pas être constamment interrompus.

Il apparaît que le téléphone est un outil de travail fondamental dans une salle de commande; il peut cependant, dans certains cas, être une source importante de perturbation du travail des CDB.

2. Inadéquations liées à la structure des outils de travail

Certaines caractéristiques des outils de travail peuvent constituer des obstacles pour la réalisation optimale des objectifs de pilotage.

2.1 Densité des informations

Ce qui est immédiatement remarquable en salle de commande c'est la surinformation qui est présentée aux opérateurs. Selon la configuration de l'installation, le traitement des informations est sélectif, c'est-à-dire que certaines informations sont privilégiées au détriment d'autres:

> Observation 17:
> En arrêt de tranche toutes les alarmes qui apparaissent ne sont pas utiles: les opérateurs indiquent en effet qu'ils se focalisent principalement sur les alarmes qui concernent le circuit primaire. De même, en situation dégradée, les interviews montrent que les opérateurs travaillent sur une quantité restreinte d'informations.

Ceci signifie que selon la situation, les opérateurs n'ont pas besoin de toutes les informations en permanence. Des aménagements basés sur ce principe ont été réalisés comme par exemple le panneau de sûreté qui regroupe les informations essentielles en situation accidentelle ou le panneau d'arrêt de tranche.

En outre, du fait de l'absence d'informations de synthèse, les opérateurs sont continuellement amenés à construire, à partir de plusieurs indicateurs, l'information dont ils ont besoin pour prendre leurs décisions.

2.2 Construction de l'information pertinente

Les opérateurs indiquent en effet qu'ils prennent rarement leurs décisions sur la base d'une information unique. D'une part, plusieurs paramètres doivent bien sûr être pris en compte pour identifier exactement la situation dans laquelle se trouve le système. D'autre part, ils tendent à remettre en question la fiabilité de certaines informations: l'évaluation de la crédibilité d'une information est effectuée par un recoupement avec d'autres sources d'information. Par exemple:

> Observation 18:
> Dans une situation rapportée ci-dessus (Observation 13), un opérateur est confronté à l'alarme "activité importante des purges GV1". L'opérateur estime qu'il ne faut pas accorder d'importance à cette alarme car si un défaut s'était réellement produit, une indication complémentaire serai présente sur l'alarme CVI.

Il semble qu'il puisse y avoir dans certains cas un problème de cohérence entre différentes sources d'information; par exemple:

> Observation 19:
> Un indicateur donne une différence entre la température moyenne et la température de référence égale à -0,4°C, alors que sur une vidéo les deux températures sont cotées à des valeurs identiques.

De fait, les résultats du dépouillement de la carte de flux n'étaient pas encore disponibles au moment de la phase d'observation et les opérateurs soulignent que, pour cette raison, le recalibrage des indicateurs n'avait pas pu être effectué.

2.3 Informations ambiguës ou incomplètes

Ce problème apparaît surtout pour les alarmes regroupées et pour les informations retranscrites sur le kit d'imprimantes.

2.3.1 Les alarmes regroupées

Ce type d'alarmes indique que plusieurs défauts peuvent être à l'origine de leur apparition. Il s'agit pour l'opérateur d'identifier quel est, parmi tous les défauts envisageables, celui qui est en cause. Pour cela, il peut se référer aux fiches d'alarmes.

Si cet aménagement peut avoir comme avantage de réduire la quantité d'informations qui est présentée aux opérateurs, il a comme inconvénient de ne pas fournir toute l'information utile à la conduite. La conséquence est que les opérateurs ne sont pas toujours en mesure de réaliser l'analyse de l'état du système. Pour avoir une information plus précise, ils doivent dépêcher un agent afin de contrôler les verrines d'alarmes situées en local.

Les conséquences de cette décentralisation des informations sont les suivantes: d'une part les délais nécessaires à l'identification de la cause d'un dysfonctionnement augmentent et ceci d'autant plus si l'on recoupe ce problème à un autre évoqué plus haut qui traduit la difficulté des CDB à avoir rapidement à leur disposition un opérateur en local. D'autre part, le CDB n'est pas en mesure de savoir ce qui se passe réellement: il n'est pas susceptible de connaître la nature du défaut ni sa gravité.

> Observation 20:
> Par exemple, l'alarme regroupée "Défaut station de pompage" peut avoir au moins deux causes à son origine: un simple filtre encrassé ou bien une pompe cassée. L'état de la situation diffère sensiblement selon la cause en présence.

De fait les CDB traitent avec prudence cette catégorie d'alarmes et lorsqu'une alarme regroupée apparaît, ils demandent systématiquement à un rondier d'aller effectuer des vérifications sur place afin d'identifier plus précisément la cause de l'alarme[3].

Il se peut en effet qu'une alarme regroupée apparaisse à plusieurs reprises sur des intervalles de temps assez rapprochés mais que le défaut en cause ne soit pas toujours identique. Dans ce cas, le risque est que les opérateurs traitent la situation en se basant sur la connaissance du dernier défaut en cause alors que le défaut réel est d'une autre nature.

Observation 21: Un incident assez grave (perte du 48 volts annulant la source d'alimentation des dispositifs de contrôle en salle de commande) a eu à son origine un problème de cet ordre.

2.3.2 Les informations fournies par le kit d'imprimantes

Le kit est un ensemble constitué de trois imprimantes (cf § VI. 4.2.).

Les problèmes de présentation d'information sur le kit sont les suivants:

Observation 22: Les interviews effectués auprès des opérateurs indiquent que toutes les informations qu'ils désirent ne sont pas reportées sur l'imprimante. Observation 23: La densité des informations pose aux opérateurs des problèmes de discrimination de l'information utile. Ceci est particulièrement le cas lorsque les opérateurs ont besoin de consulter des listings archivés. Pour discriminer les informations qui les intéressent, le opérateurs procèdent par identification de patterns: les indices utilisés sont la longueur des chaînes de caractères qui représentent une information ainsi que la position relative d'une chaîne d'une longueur donnée par rapport à la longueur des chaînes dont ils savent qu'elles sont limitrophes. Observation 24: Lorsqu'une succession importante d'informations doit être affichée sur le kit, il peut se produire que certaines informations ne soient pas imprimées.

[3] Et ceci même s'ils ont une idée assez précise du défaut qui peut être en cause.

2.4 Dispersion des contrôles et des commandes

2.4.1 Alarmes centralisées et alarmes décentralisées

L'exhaustivité des alarmes n'est pas centralisée en salle de commande. Si cet aménagement peut avoir comme avantage de réduire la quantité d'informations qui est à la disponibilité des opérateurs, il a comme inconvénient de ne pas fournir toute l'information utile. La conséquence est que les opérateurs ne sont pas toujours en mesure de réaliser l'analyse de l'état d'un circuit et qu'ils doivent pour cela dépêcher un agent afin de contrôler les alarmes spécifiques situées en local. La conséquence est que les relais de transmission d'information sont multipliés: les difficultés liées à ce problème se traduisent par l'augmentation des délais nécessaires à l'identification de la cause d'un dysfonctionnement ainsi que par les divers problèmes, étudiés ci-dessus, relatifs à la structure des coordinations.

2.4.2 Inadéquation de la localisation des contrôles/commandes dans la réalisation de certaines tâches

La réalisation de certaines actions de régulation nécessite d'utiliser plusieurs organes de contrôle et de commande. Or dans certains cas, les contrôles et les commandes qui interviennent dans une même séquence d'actions de régulation sont dispersés sur les différentes platines du pupitre avant et du tableau arrière de la salle de commande.

Observation 25:
Par exemple, pour l'activité de surveillance des niveaux GV, les enregistreurs reproduisant les courbes d'évolution sont situées sur le panneau avant et le commutateur de capteur sur le panneau arrière. Dans certains cas, le opérateurs sont contraints d'aller au panneau avant pour surveiller les courbes d'évolution et, s'ils détectent une valeur anormale, d'aller au panneau arrière pour commuter un capteur, puis de revenir au panneau avant pour surveiller les courbes d'évolution.
Observation 26:
Le problème est identique pour la régulation du niveau du pressuriseur.
Observation 27:
De même, les enregistreurs et les alarmes des niveaux des Générateurs de Vapeur ne sont pas localisés au même endroit.
Observation 28:
Un cas cité mais qui ne doit plus exister est celui des pompes ASG: la tâche de mise en service de ces pompes impliquait de les démarrer à un endroit de la salle de commande, puis de contrôler leur prise de charge sur un amèremètre à un deuxième endroit et enfin de contrôler la valeur de leur débit à un enregistreur situé à un troisième endroit.

Cette dispersion ne pose pas trop de problème pour les tâches de régulation simples (peu d'actions successives à effectuer) ou qui ne nécessitent pas des délais trop courts entre chaque action. Cependant, lorsque la régulation se complexifie, cette dispersion est un

facteur d'augmentation de la charge de travail mental, les opérateurs étant obligés de mémoriser l'état des commandes et des contrôles lorsqu'ils passent des uns aux autres. Le risque est d'oublier certaines valeurs et d'être obligé de revenir à des états antérieurs de la procédure pour les retrouver.

La dispersion des contrôles et des commandes pose également des difficultés aux opérateurs lorsque la séquence de régulation exige d'effectuer des actions simultanées. C'est le cas dans l'exemple suivant:

> Observation 29:
> Lorsque les opérateurs doivent intervenir sur l'ouverture des orifices de détente sur le circuit RCV (commande située sur le panneau arrière), il est nécessaire de réguler simultanément le débit par une commande de vanne (localisée sur le panneau avant). Les opérateurs doivent obligatoirement être deux pour réaliser cette action.

2.5 Procédures complexes

Certaines activités s'avèrent, selon les opérateurs, complexes à réaliser. Par exemple:

> Observation 30:
> L'action de régulation manuelle des GV (à Puissance Nominale (PN) < 10%) constitue selon les opérateurs une opération délicate. L'objectif est de maintenir les niveaux GV dans des limites définies; cependant, la régulation manuelle de l'appoint d'eau pour compenser une baisse de niveau peut créer un refroidissement qui risque de faire évoluer le paramètre de niveau dans le sens inverse de celui qui est désiré.

De même, les opérateurs sont amenés à réaliser des calculs relativement complexes compte tenu du nombre de variables à prendre en considération:

> Observation 31:
> Par exemple lorsqu'ils doivent réaliser un bilan de réactivité ou bien, après un arrêt, lorsqu'ils doivent identifier la valeur précise de la concentration en bore à laquelle il sera possible de rediverger.

Pour ce qui est de l'élaboration de ces calculs, le problème réside surtout dans le fait qu'ils sont effectués dans un contexte qui, selon les opérateurs, n'est pas toujours favorable du fait des interruptions fréquentes dues aux communications ou de la nécessité de réaliser en même temps d'autres tâches qui exigent une vigilance particulière.

Par ailleurs, la prévision de l'évolution de certaines variables peut être complexe: c'est le cas par exemple de l'évolution du xénon suite à des modifications successives du régime de fonctionnement du processus (cf Alengry, 1988a).

VIII - CONCLUSION

Nous avons décrit dans ce rapport le contexte socio-technique dans lequel est élaboré le travail de pilotage d'une centrale nucléaire. Les caractéristiques et fonctions des principaux opérateurs ont été définies ainsi que la nature et le support des informations sur lesquelles est basé le travail de pilotage. Dans certains cas, les modalités d'utilisation d'informations importantes ont été décrites. Certaines des inadéquations du système homme-machine les plus significatives ont été relevées.

Nous présentons dans un autre rapport (Alengry, 1988b) les classes de situation auxquelles sont ou pourraient être confrontés les opérateurs au cours de leur travail de pilotage.

Références bibliographiques

Alengry, P. (1988a) *Représentation des Modes Opératoires et des Connaissances Evoqués par des Opérateurs de Centrale Nucléaire dans une Tâche de Pilotage Simulée*. Rapport INRIA, Décembre 1988.

Alengry, P. (1988b) *Analyse du Travail de Pilotage d'une Centrale Nucléaire (II): Les Classes de Situation*. Rapport INRIA, Décembre 1988.

Alengry, P. & Pierret, C. (1988) *Formalisation des Connaissances et du Raisonnement dans une Activité de Diagnostic: Le cas des Accidents par Brèche dans les Centrales Nucléaires*. Rapport INRIA, Décembre 1988.

Imprimé en France
par
l'Institut National de Recherche en Informatique et en Automatique