L'APPROCHE PAR ETAT: UNE NOUVELLE CONCEPTION DES PROCEDURES DE CONDUITE POST-ACCIDENTELLE

H. SUREAU, G. DEPOND
Service Etudes et projets thermiques et nucléaires,
Electricité de France,
Paris La Défense

A. OLIOT
Société Framatome,
Paris La Défense,

France

Abstract–Résumé

PLANT STATE APPROACH: A NEW CONCEPT IN POST-ACCIDENT OPERATION PROCEDURES.

Normal accident procedures are based on a diagnosis of the accident-initiating incident and on a predetermined succession of events in the most probable sequences. This 'event' approach does not allow all conceivable accident situations to be taken into account or the diagnosis to be reviewed and updated in the event that the system deviates from the pattern predicted by the first diagnosis. These shortcomings can be overcome by a 'state' approach based on the observation of physical parameters, analysis of the thermohydraulic status of the system and definition of operator action. This is done continuously throughout the post-accident phase. Studies carried out have identified all the cooling states of a PWR boiler, revealed the need for additional instrumentation to give a comprehensive description of these states and indicated that it is possible to establish a direct relationship between a state and the appropriate action. The procedures used in French power plants have benefited from this work: a number of important mechanisms such as the safety injection system have been made independent of accident-initiating events and accident sequences through the use of continuous plant state criteria. A further application of the state approach, which is still restricted by existing instrumentation, is effected by the safety engineer who exercises continuous post-incident surveillance. Based on very precise plant state criteria, this approach makes it possible either to confirm the main safety measures dictated by the sequential procedure being applied or to decide to use the emergency procedure which defines the action required as a function of the state of the boiler and the available systems and is used where the normal procedures are no longer valid. Work is continuing to achieve more systematic application of the state approach with additional instrumentation.

L'APPROCHE PAR ETAT: UNE NOUVELLE CONCEPTION DES PROCEDURES DE CONDUITE POST-ACCIDENTELLE.

Les procédures accidentelles habituelles sont basées sur un diagnostic de l'incident initiateur et sur un déroulement prédéterminé des séquences les plus probables. Cette approche «par événement» ne permet pas de couvrir toutes les situations accidentelles imaginables et de réactualiser le diagnostic pour une évolution du système non conforme aux prévisions du premier diagnostic. Ces lacunes peuvent être comblées par une approche «par état», basée sur l'observation des paramètres physiques, l'analyse de l'état thermohydraulique du système et la définition des actions de l'opérateur, et ceci d'une manière permanente pendant toute la phase post-accidentelle. Les études effectuées ont permis d'identifier l'ensemble des états de refroidissement d'une chaudière REP, de faire apparaître la nécessité d'une instrumentation complémentaire par la caractérisation complète de ces états, et de montrer la possibilité d'établir une relation directe état-actions. Les procédures utilisées dans les centrales françaises bénéficient, entre autres, de ces travaux: certaines actions importantes, par exemple sur l'injection de sécurité, ont été rendues indépendantes des événements initiateurs et des séquences accidentelles, par utilisation de critères permanents d'états. Une autre application de l'approche par état, encore limitée par l'instrumentation actuelle, est confiée à l'ingénieur de sûreté qui exerce une surveillance permanente après incident. A partir de critères très précis d'états, elle permet soit de confirmer les principales actions de sûreté demandées par la procédure séquentielle en cours d'application, soit de décider d'utiliser la procédure d'urgence qui définit les actions requises en fonction de l'état de la chaudière et des systèmes disponibles, au-delà du domaine de validité des procédures habituelles. Les travaux se poursuivent pour une utilisation plus systématique de l'approche par état avec une instrumentation complémentaire.

1. L'INTERACTION HOMME-MACHINE EN SITUATION ACCIDENTELLE

La sûreté du refroidissement des produits radioactifs du combustible nucléaire en situation accidentelle repose, au-delà des premières minutes redevables aux automatismes, sur une bonne conception de l'interaction homme-machine.

Les événements perturbateurs induisent une dégradation de l'état du système qui est appréhendée par l'opérateur grâce aux informations délivrées par des capteurs et présentées, après traitement, en salle de commande. L'opérateur doit alors effectuer un diagnostic et engager les actions requises pour ramener le système dans un état sûr.

Les processus de diagnostic et d'action correspondants sont précisés dans des procédures post-accidentelles écrites. Une conception cohérente de l'ensemble de ces procédures permet de structurer les autres éléments de l'interaction homme-machine: capteurs et actionneurs nécessaires et leur qualification aux conditions post-accidentelles, traitements et présentation des informations et des commandes en salle de commande, organisation de l'équipe de conduite, formation et entraînement des opérateurs sur simulateurs, etc.

La nécessité d'améliorer l'ensemble de ces éléments en situation accidentelle est apparue depuis 1979 après l'accident de Three Mile Island, la mise en service de nombreuses tranches et l'analyse des incidents réels et des tests effectués sur

simulateur: si le système REP semble bien doté des moyens potentiels de sortir correctement d'un très grand nombre de situations dégradées, le problème est de savoir quand et comment les mettre en œuvre. La conception du processus de diagnostic des situations et de décision des actions s'est avérée être le point essentiel à améliorer, les moyens matériels et humains permettant une application correcte de ce processus devant ensuite être adaptés à cette conception.

2. INSUFFISANCE DES PROCEDURES POST-ACCIDENTELLES PAR EVENEMENT

Les procédures post-accidentelles à la disposition de l'opérateur étaient basées, jusqu'en 1980, sur une analyse séquentielle pessimiste des accidents «enveloppe» servant au dimensionnement des protections et des systèmes de sauvegarde.

Ces procédures par événement ont été depuis améliorées, dans leur contenu technique, à partir d'études post-accidentelles plus réalistes, et, dans leur forme, à partir du retour d'expérience des centrales et des tests sur simulateurs.

Le diagnostic de l'événement initiateur doit être effectué entre 5 et 15 min environ après le déclenchement d'une protection du réacteur ou d'une alarme, délai nécessaire à une première «stabilisation» de l'état du système après fonctionnement des automatismes de sécurité dont le bon déroulement est vérifié.

Le diagnostic de l'événement initial conduit au choix d'une procédure séquentielle d'actions prédéfinies correspondant au déroulement d'une séquence accidentelle préétudiée.

Cette approche séquentielle par événement a conduit à un jeu de procédures accidentelles, dites I, A ou H, couvrant l'ensemble des séquences prises en compte dans la conception des tranches REP.

Mais la réalité à laquelle peut être confronté l'opérateur ne se conformera probablement à aucune des séquences préétudiées. En effet, une procédure spécifique à un événement initiateur peut difficilement coller de manière réaliste à l'ensemble des situations pouvant résulter à moyen terme de différences dans l'état initial de la tranche, dans le comportement des matériels ou dans les délais d'action des opérateurs. Il en résultera un flou croissant dans l'application de la procédure au cours du développement de l'incident. L'opérateur risque de se perdre sans savoir ce qu'il doit faire et l'incident risque de dégénérer en accident plus sérieux.

Par ailleurs, les procédures par événement ne peuvent pas couvrir toutes les combinaisons possibles d'événements correspondant à des cumuls de défaillances matérielles et/ou humaines, simultanées ou étagées dans le temps, telles que, par exemple, l'erreur de diagnostic initial, la mauvaise application d'une procédure, le cumul de plusieurs accidents, la perte totale d'un système de sauvegarde, etc. La tentation de multiplier les séquences préétudiées conduirait à multiplier

corrélativement le nombre des procédures de conduite et rendrait le diagnostic, et donc le choix de la bonne procédure, pratiquement impossibles.

L'approche séquentielle par événement, qui permet d'optimiser la conduite spécifique à certains événements accidentels, conduit à une impasse relative: impossibilité de réactualiser le diagnostic en cas d'évolution du système non conforme aux prévisions du premier diagnostic et impossibilité de couvrir toutes les situations accidentelles imaginables.

Cette critique est bien illustrée par l'accident de Three Mile Island en 1979: l'erreur de diagnostic initial, faite par l'opérateur sur la base d'une instrumentation délivrant des informations ambiguës en situation perturbée, a conduit à des actions inadéquates et transformé un accident mineur en accident majeur. L'opérateur, pris à contre-pied par des réactions inattendues du système à ses actions, a appliqué successivement sept procédures différentes et jamais la bonne. Ce n'est qu'après plusieurs heures que l'exploitant prit conscience du fait que le fluide primaire de réfrigération était passé à la saturation puis en diphasique avec dénoyage et dégradation du cœur du réacteur.

Suite à cette expérience malheureuse, la première idée a été d'ajouter rapidement en salle de commande une information sur la marge à la saturation, première manifestation d'un diagnostic permanent d'état, puis d'essayer de généraliser une surveillance des états du système en situation post-accidentelle.

En effet, si les séquences accidentelles peuvent être multipliées à l'infini, les états de refroidissement et de confinement possibles du système peuvent par contre être dénombrés. De plus, les actions requises de l'opérateur, à un instant donné et à l'échelle de temps de son intervention, peuvent en général être déduites de la connaissance de cet état du système sans que l'enchaînement des événements antérieurs y ayant conduit ait nécessairement été identifié. Une approche par état de la conduite post-accidentelle devrait donc permettre de sortir de l'impasse relative de l'approche séquentielle par événement.

comment ça ?

3. DEVELOPPEMENT DE L'APPROCHE PAR ETAT

3.1. Objectif

L'objectif de l'approche par état est d'expliciter une relation directe états→actions de l'opérateur, c'est-à-dire:

1) Identifier tous les états de refroidissement possibles de la chaudière, leurs domaines de stabilité, leurs transitions, en recherchant une exhaustivité qu'il n'est pas possible d'atteindre par l'approche séquentielle par événement et indépendamment de leur probabilité d'occurence.

2) Caractériser ces états par des grandeurs physiques mesurables.

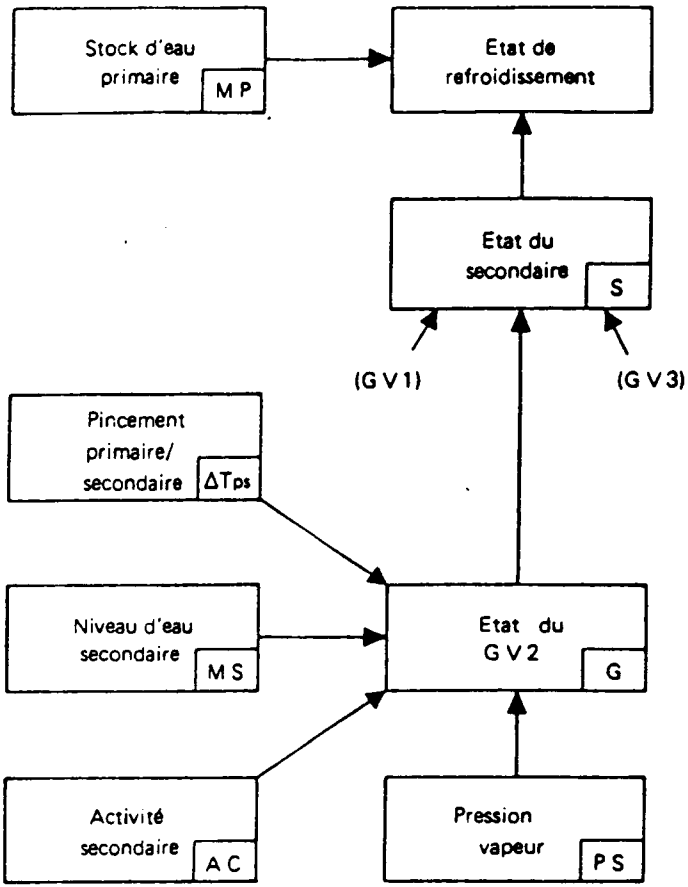

FIG. 1. Analyse des états de refroidissement du coeur et de la chaudière.

3) Identifier pour chacun de ces états les actions correctives et/ou réparatrices requises de l'opérateur.

4) Construire une synthèse des points précédents où ne sont plus discriminés les uns des autres que les sous-ensembles d'états nécessitant des actions différentes.

5) Expliciter le processus de diagnostic d'état correspondant et les règles de conduite associées.

6) Identifier les mesures physiques complémentaires et les traitements d'information en salle de commande nécessaires à la mise en œuvre de ce processus de diagnostic d'état et d'action.

3.2. Analyse des états de refroidissement de la chaudière

Le fonctionnement d'une chaudière nucléaire est analysé à partir des bilans fondamentaux de masse, énergie, impulsion appliqués aux différents éléments de celle-ci et qui font apparaître:

– le cheminement de l'énergie: production, extraction du combustible, transport, transfert hors circuit primaire;
– le stockage, déstockage d'énergie dans les circuits primaire et secondaire;
– le stockage, déstockage des masses d'eau dans les circuits primaire et secondaire.

Ces différentes «catégories» physiques sont analysées. Pour chacune d'elles différentes configurations sont retenues, couvrant l'ensemble des possibilités, et identifiées par des paramètres mesurables (pression, niveau, température et leurs dérivées, etc.).

Les combinaisons possibles de ces configurations sont regroupées et montrent que (figure 1):

– le stock de masse du fluide primaire (MP) et l'extraction de chaleur du circuit primaire définissent le comportement de la chaudière, en particulier la circulation du fluide primaire et l'extraction de chaleur du combustible;
– l'extraction de chaleur du circuit primaire est fonction de la présence éventuelle de gaz incondensables dans le circuit, identifiée par le pincement primaire-secondaire (ΔTPS), et de l'état du circuit secondaire (S);
– l'état du secondaire (S) dépend lui-même de l'état de chacun des générateurs de vapeur défini à partir de la masse du fluide secondaire (MS), de la pression vapeur (PS) et du niveau de radioactivité éventuel du fluide secondaire (AC).

3.3. Synthèse: grille états/actions (figure 2)

Les résultats de l'analyse précédente permettent de construire une grille d'états pour la chaudière et une grille d'états pour chaque générateur de vapeur.

Chaque état défini dans ces grilles est identifié à partir de paramètres physiques mesurés et de leur évolution: masse de fluide primaire (taux de vide, niveau cuve), températures et pressions primaire et secondaire, niveaux d'eau, pression vapeur, radioactivité des générateurs de vapeur. Chaque état requiert des actions de sûreté spécifiques sur les différents actionneurs en fonction de leur disponibilité (injection de sécurité, circuit de charge et décharge, aspersion et décharge pressuriseur, eau alimentaire de secours des générateurs de vapeur, décharge vapeur au secondaire, isolement vapeur et eau du secondaire, etc.). Ces actions sont à optimiser afin de stabiliser et si possible restaurer le système afin de retrouver des états de moins en moins dégradés.

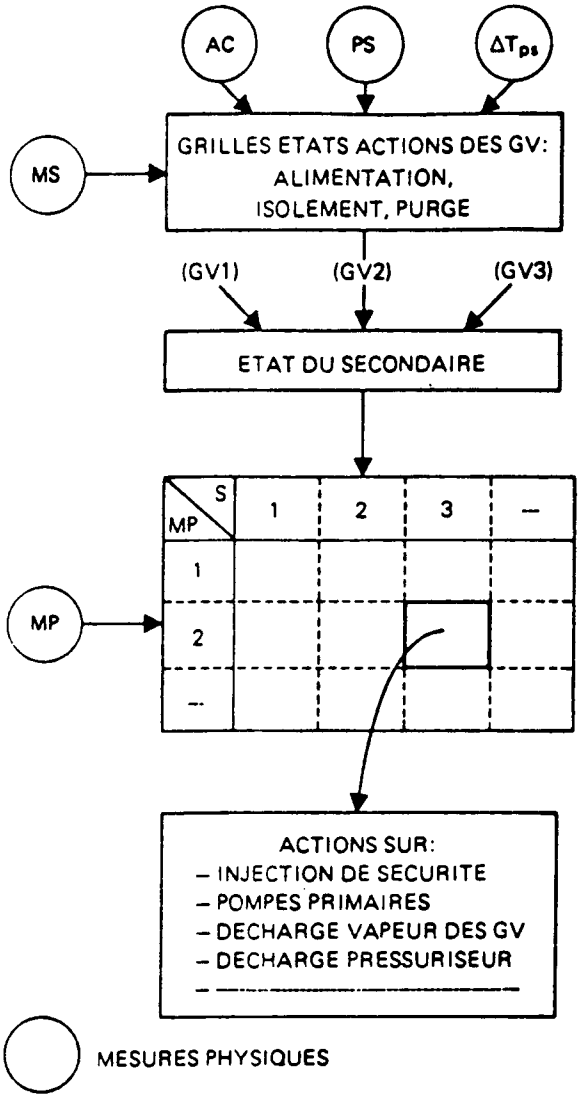

FIG.2. Synthèse: grilles états/actions.

3.4. Mesures physiques complémentaires

Pour être totalement opérante, et notamment permettre des ripostes graduées même après passage en régime diphasique, une telle approche nécessite une instrumentation complémentaire à celle existant actuellement sur nos réacteurs: des mesures de taux de vide dans les branches chaudes et de niveau dans la cuve, plus particulièrement dans le plénum supérieur. En effet, les mesures existantes (pression et température primaire, niveau pressuriseur) ne sont pas suffisantes pour connaître la masse d'eau primaire et sa tendance en situation diphasique.

Les actions de développement de cette instrumentation complémentaire ont été engagées en liaison avec Framatome et le CEA. Des mesures de niveau cuve par poids de colonne seront opérationnelles pour le démarrage du premier ou du deuxième réacteur 1300 MWe de Paluel. Les études de faisabilité de mesures de taux de vide en branche chaude se poursuivent avec des tests de capteurs à ultrasons haute fréquence sur une tranche du Blayais et sur la boucle d'essai diphasique Super Moby Dick à Grenoble. Des conclusions seront tirées avant la fin de 1983.

Cependant, sans attendre les résultats des développements de cette instrumentation complémentaire et des procédures par états associés, l'approche par état a déjà été utilisée dans le cadre de la formation du personnel de conduite, et pour améliorer et compléter les procédures actuelles par événement.

4. PREMIERES APPLICATIONS DE L'APPROCHE PAR ETAT

4.1. Amélioration des procédures par événement

Les améliorations apportées dans la révision en cours des procédures I, A et H et provenant de l'approche par état visent:

1) D'une part, à rendre les critères d'action des principaux systèmes de sauvegarde aussi indépendants que possible des séquences. Pour cela, on assure une surveillance constante des principaux paramètres, ou combinaisons de paramètres, qui permettent de discriminer à chaque instant les actions d'activation et de désactivation de ces systèmes. Ce type d'amélioration porte sur les actions de démarrage et d'arrêt des pompes d'injection de sécurité, sur la mise en service de l'aspersion de l'enceinte de confinement, sur l'isolement des générateurs de vapeur contaminés et, dans une moindre mesure, sur l'arrêt des pompes primaires.

2) D'autre part, étant donné le constat de non-exhaustivité des procédures actuelles, à les compléter par des garde-fous, qui confirment ou redéfinissent les actions essentielles, indépendamment du diagnostic initial et de l'évolution qui en était attendue (ce qui permet de couvrir les séquences hors procédures). Ce deuxième type d'amélioration concerne des renvois entre procédures et surtout

la surveillance permanente après incident (SPI) et l'élaboration d'une nouvelle procédure d'urgence (U1).

A titre d'exemple du premier type d'amélioration, la conduite de l'injection de sécurité est précisée dans le paragraphe suivant.

4.2. Conduite de l'injection de sécurité (IS)

L'injection de sécurité sert essentiellement à compenser les pertes d'eau du circuit primaire lorsque le circuit de charge n'est plus suffisant pour assurer cette fonction.

La conduite de l'injection de sécurité dépend donc d'une évaluation du stock d'eau qui est sûre et dénuée d'ambigüité. Le critère pour évaluer ce stock est le niveau pressuriseur représentatif du volume liquide, validé toutefois par une condition de sous-saturation en sortie cœur (ΔTsat), pour couvrir le cas des brèches en phase vapeur du pressuriseur (y compris les ouvertures intempestives de soupapes du pressuriseur). Le principe général de la conduite de l'IS est l'arrêt progressif des files si le stock est suffisant, ou excessif, et la (re)mise en service si le stock est insuffisant.

La grille états/actions de l'injection de sécurité présente une combinaison des seuils de niveau pressuriseur et de ΔTsat de manière à éviter dans la plupart des cas les pompages entre arrêt et redémarrage des pompes. De plus le déplacement du point représentatif de l'état (niveau, ΔTsat) dans cette grille permet de suivre et mieux comprendre l'évolution de la situation, et donc de vérifier la cohérence et l'efficacité des actions de sauvegarde entreprises par ailleurs.

Cette grille de conduite, indépendante de la séquence accidentelle est incorporée dans toutes les procédures (version 1982) où l'injection de sécurité intervient.

Les images correspondantes seront présentées sur les panneaux de sûreté en cours d'installation (voir le mémoire IAEA-SM-268/56, présents comptes rendus, volume I).

4.3. Procédures de surveillance permanente et d'urgence

La procédure de surveillance permanente après incident (SPI), basée sur l'approche par état, permet de réactualiser continuement le diagnostic initial et éventuellement d'adopter la procédure d'urgence (U1) qui sert de «garde-fou» aux procédures par événement.

La procédure U1 est prévue pour assurer les meilleures conditions possibles de refroidissement de la chaudière et de sauvegarde du cœur dans des situations où les procédures I, A ou H, propres à des séquences accidentelles bien identifiées, s'avèrent inadaptées et inefficaces. L'objectif de cette procédure U1 est d'éviter, ou de limiter, ou de retarder l'endommagement du cœur et ses conséquences

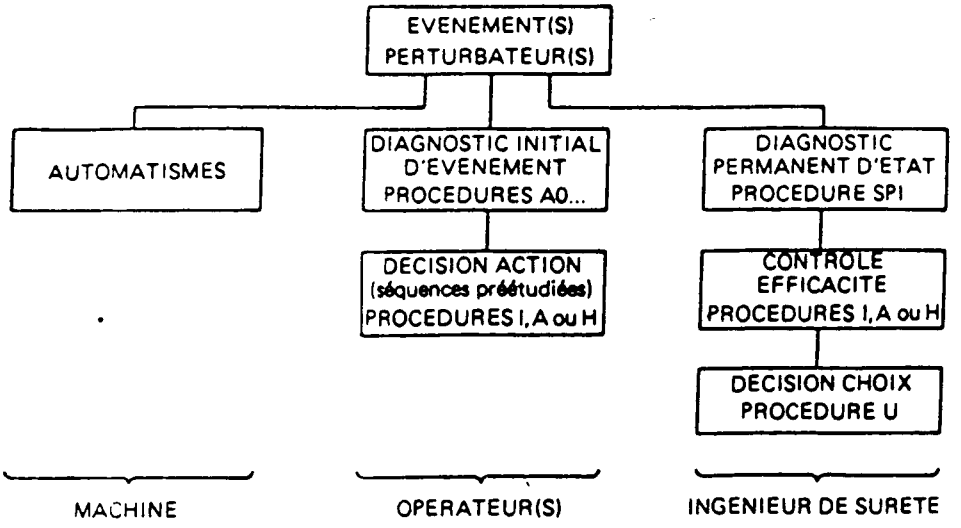

FIG. 3. Interaction homme-machine en situation accidentelle.

radiologiques, selon la gravité de la situation et l'importance des moyens restant disponibles.

Par quel processus peut-on arriver à la décision d'abandonner une procédure I, A ou H en cours d'application au profit de la procédure U1? C'est-à-dire comment détecter, à n'importe quel moment et quelles qu'en soient la ou les causes, que le système ne suit pas ou ne suit plus la séquence accidentelle initialement diagnostiquée, et/ou que la procédure appliquée par l'opérateur n'est pas ou n'est plus efficace?

Il est apparu inopportun d'effectuer ce processus à l'intérieur des procédures «séquentielles» I, A et H pour trois raisons:

1) Difficulté de concevoir les critères précis à l'intérieur de chaque procédure et à chaque étape de leur déroulement permettant de détecter une évolution non conforme à l'attente et potentiellement dangereuse.

2) Difficulté de demander à l'opérateur un processus d'auto-contrôle et la remise en question constante de ses décisions et de ses actions antérieures.

3) Difficulté d'introduire ce processus dans les procédures actuelles dont la conception et la rédaction devraient alors être reprises entièrement.

Il est par contre apparu plus intéressant et techniquement possible de procéder à un diagnostic permanent:

– selon une logique indépendante, redondante et extérieure aux procédures existantes, qui restent alors inchangées et qui pourront évoluer ultérieurement de façon autonome si besoin est;

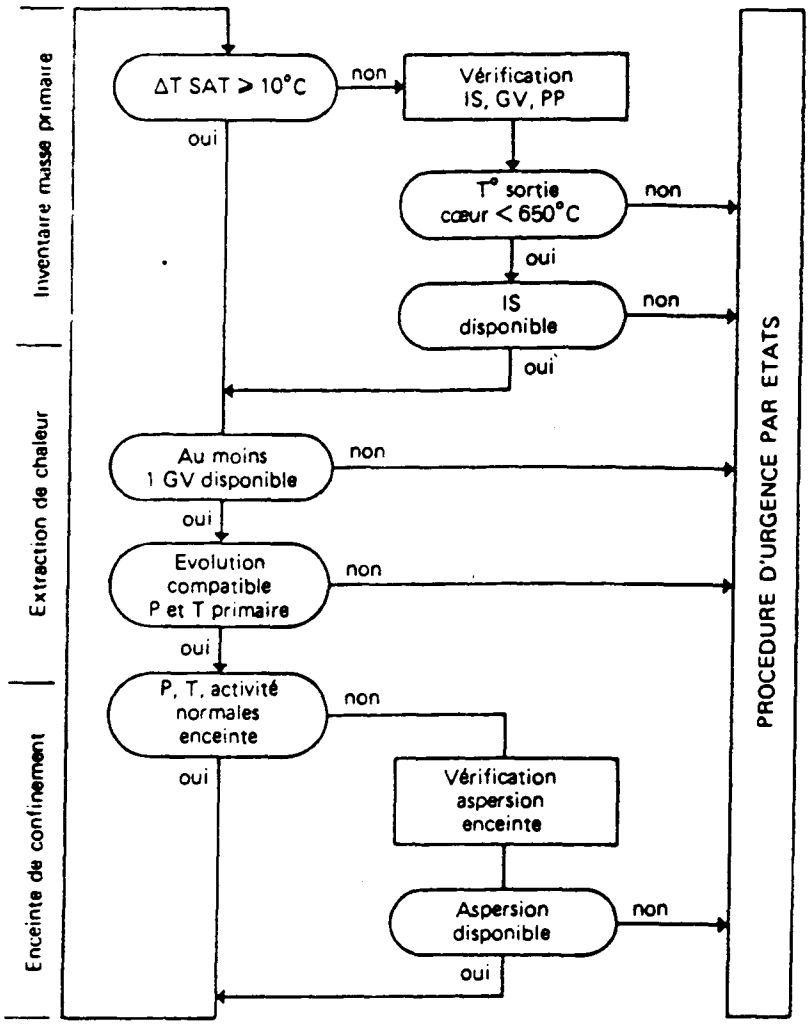

FIG.4. Surveillance permanente par états.

– en faisant appel à l'ingénieur de sûreté et de radioprotection (ISR), ce qui assure une redondance humaine par rapport à l'opérateur;
– en s'appuyant sur l'analyse des états de refroidissement de la chaudière, complétée par l'analyse de la disponibilité des systèmes de sauvegarde utilisés, et mise en œuvre avec l'instrumentation actuelle.

Cette logique conduit l'ISR à exercer une surveillance permanente après incident (SPI) qui permet, à partir de critères très précis d'état (figure 3):
– soit, si le système suit la séquence initialement diagnostiquée, de suivre, et éventuellement de confirmer à l'opérateur, avec un léger décalage dans le temps, les principales actions déjà demandées par la procédure séquentielle en cours d'application;
– soit, dans certains cas de défaillances cumulées non prises en compte dans les séquences, de demander à l'opérateur des actions complémentaires limitées (isolement d'un GV) sans pour autant abandonner la procédure en cours;
– soit, dans certaines situations encore plus dégradées, de prendre la décision d'abandonner la procédure en cours et de passer à l'application de la procédure U1 qui définit alors les actions requises en fonction de l'état du système et des moyens disponibles à chaque instant.

Un logigramme très simplifié de la surveillance permanente après incident (SPI) est présenté figure 4. La SPI porte sur les paramètres suivants:
– disponibilité de chaque générateur de vapeur, c'est-à-dire sa capacité à évacuer la puissance résiduelle sans que la vapeur évacuée soit contaminée;
– le stock d'eau primaire et la température sortie cœur;
– l'efficacité globale du secondaire sur le primaire, c'est-à-dire sa capacité à refroidir et dépressuriser le primaire;
– la mise en service effective des systèmes de sauvegarde appelés (ASG, ISHP, ISBP, EAS, etc.);
– la pression, la température et l'activité dans l'enceinte de confinement;
– la criticité du cœur (flux nucléaire, position des barres de contrôle, concentration en bore, etc.).

La procédure U1 elle-même permet, en fonction de l'évolution des températures sortie cœur et de la disponibilité des générateurs de vapeur et de l'injection de sécurité, de préconiser les meilleures actions pour:
– l'utilisation des générateurs de vapeur,
– l'injection de sécurité,
– les soupapes de décharge du pressuriseur,
– les pompes primaires,
pour arrêter, atténuer ou retarder les évolutions dangereuses (donnant ainsi du temps pour retrouver des systèmes défaillants).

Les logigrammes des procédures SPI et U1 sont programmés sur les panneaux de sûreté en cours d'installation dans toutes les tranches REP (voir le mémoire IAEA-SM-268/56,présents comptes rendus,·volume I).