CEA-N-2008

- Note CEA-N-2008 -

Centre d'Etudes Nucléaires de Saclay
Services d'Electronique de Saclay
Service du Matériel Electronique

# ETUDE DE LA SURETE DU PCC 2140 ET DE L'ALILOG 21 CONSIDERES COMME CHAINE DE MESURE DE SECURITE

par

Pierre MERIAUX, Serge ADNOT, Catherine RAYROLLES

- Mars 1978 -

*Edité par*
*le Service de Documentation*
*Centre d'Etudes Nucléaires de Saclay*
*Boîte Postale n° 2*
*91190 - Gif-sur-YVETTE (France)*

Note CEA-N-2008

**DESCRIPTION-MATIERE** *(mots clefs extraits du thesaurus SIDON/INIS)*

| *en français* | *en anglais* |
|---|---|
| INGENIERIE DE LA SECURITE | SAFETY ENGINEERING |
| MONITEURS DE RAYONNEMENT | RADIATION MONITORS |
| DISPOSITIFS D'ALERTE | ALARM SYSTEMS |
| CHAMBRES D'IONISATION | IONIZATION CHAMBERS |
| CIRCUITS ELECTRONIQUES | ELECTRONIC CIRCUITS |
| FIABILITE | RELIABILITY |

- Note CEA-N-2008 -

Centre d'Etudes Nucléaires de Saclay
Services d'Electronique de Saclay
Service du Matériel Electronique

# ETUDE DE LA SURETE DU PCC 2140 ET DE L'ALILOG 21 CONSIDERES COMME CHAINE DE MESURE DE SECURITE

par

Pierre MERIAUX, Serge ADNOT, Catherine RAYROLLES

CEA-N-2008 - MERIAUX Pierre, ADNOT Serge, RAYROLLES Catherine,

ETUDE DE LA SURETE DU PCC 2140 ET DE L'ALILOG 21 CONSIDERES COMME CHAINE DE MESURE DE SECURITE.

Sommaire.- L'ensemble PCC 2140 et ALILOG 21 peut être utilisé au C.E.A. ou à l'E.D.F. comme chaîne de mesure de Sécurité. A la suite d'une étude effectuée sur un équipement similaire mais ancien, il avait été constaté que certaines défaillances commutaient le préamplificateur sur la gamme de mesure la moins sensible, ce qui allait à l'encontre de la Sûreté de l'équipement. Ce rapport analyse les modes de défaillance conduisant aux pannes "non sûres" et évalue les risques encourus compte tenu des tests possibles par l'utilisateur.

1978 21 p.

Commisseriat à l'Energie Atomique - France.

---

CEA-N-2008 - MERIAUX Pierre, ADNOT Serge, RAYROLLES Catherine.

SAFETY STUDY OF PCC 2140 AND ALILOG 21 USED AS PART OF SAFETY MEASUREMENT SYSTEMS.

Summary.- The PCC 2140 and ALILOG 21 equipment may be used at C.E.A. or E.D.F., as part of safety measurement systems. In a study of a similar, but earlier equipment, it was noticed that certain types of failures caused the system to switch to the least sensitive measurement range, which was detrimental to safety. This report analyses failure modes leading to unsafe failures and evaluates the risks ran into when taking in account tests during use.

1978 21 p.

Commissariat à l'Energie Atomique - France.

- PLAN -

# I - INTRODUCTION

## I.1 But de l'ETUDE

La chaîne de mesure constituée par un PCC 2140 et l'ALILOG 21 est un ensemble électronique recommandé au C.E.A. auprès des installations nucléaires, pour tableaux de contrôle de Radioprotection (voir Catalogue Electronique 77 édité par le GEC - Tome 1 - F05; Utilisée en voie logarithmique, elle peut-être considérée comme équipement de sécurité.

Elle est issue du développement du PCC 1140 et de l'ACC 1140 pour lesquels une étude particulière avait été effectuée pour le CEA/DAM. Cette étude avait amené le constructeur français : MERLIN GERIN a revoir le dispositif d'alarme car un certain nombre de modes de défaillances de composants conduisait à la commutation systématique sur la gamme la moins sensible du préamplificateur PCC 1140, ce qui ne semblait pas aller dans le sens de la sûreté. L'accord, donné par le GEC au constructeur, de garder le contact repos du relais RX1 du PCC 2140 pour la gamme de sensibilité la moins grande était conditionné par le lancement d'une étude ultérieure sur la chaîne PCC 2140 et ALILOG 21. Ceci a d'ailleurs été confirmé par des groupes de travail.

## I.2 Objet de l'ETUDE

L'objet de ce rapport était donc d'analyser cette nouvelle chaîne de mesure pour voir si les modifications apportées par le constructeur allaient dans le sens de l'amélioration de la sûreté.

La valeur du risque encouru, pendant une période donnée étant l'expression mathématique de la Sûreté, nous la calculerons pour un niveau de rayonnement créant dans la chambre d ionisation un courant allant de 10-13 à 10-11 A correspondant à la gamme la plus sensible du PCC 2140. Le critère de non-Sûreté retenu est le suivant :

- franchissement du premier Seuil S1 sans déclenchement de l'alarme correspondante, à l'insu de l'utilisateur.

Il s'agira en fait de calculer la probabilité conditionnelle de la défaillance du circuit de seuil S1, la visualisation de l'état de bon fonctionnement "BF" restant correct et rassurant, par le fait, l'expérimentateur.
Une étude antérieure effectuée sur le PCC 1140 et l'ACC 1140 dont la diffusion du rapport a été confidentielle, estimait le risque d'avoir le "Silence Injustifié" à : 0,126 pour une période égale à un an et dans desconditions d'environnement similaires.
Ce rapport permettra donc de justifier le bien-fondé des modifications effectuées et de chiffrer la diminution du risque encouru.

* GEC : Groupe de Gestion centralisée d'Electronique aux S.E.S. Ce Catalogue, présenté en 3 Tomes, est un receuil des matériels recommandés. Il constitue une sélection établie par des groupes de travail spécialisés; elle est faite à la suite d'essais et d'examens technologiques, selon des critères de performances, de prix, d'assurance de qualité et de coût de maintenance.

## II - DESCRIPTION DU CIRCUIT

### II.1 Définition des éléments étudiés

L'ALILOG 21 et le PCC 2140 associés à une chambre d'ionisation permettent la mesure des rayonnements $\beta$ et $\gamma$ dans deux modes de fonctionnement : linéaire et logarithmique et éventuellement en combinant les deux modes : fonction LIN-LOG.

Seule la fonction LOG, associée à des déclencheurs réglables, permet la commande des circuits de sécurité et en particulier le déclenchement des Alarmes à distance. Les circuits contribuant à la réalisation de cette fonction LOG

ALILOG 21 - VUE GENERALE : Figure 1

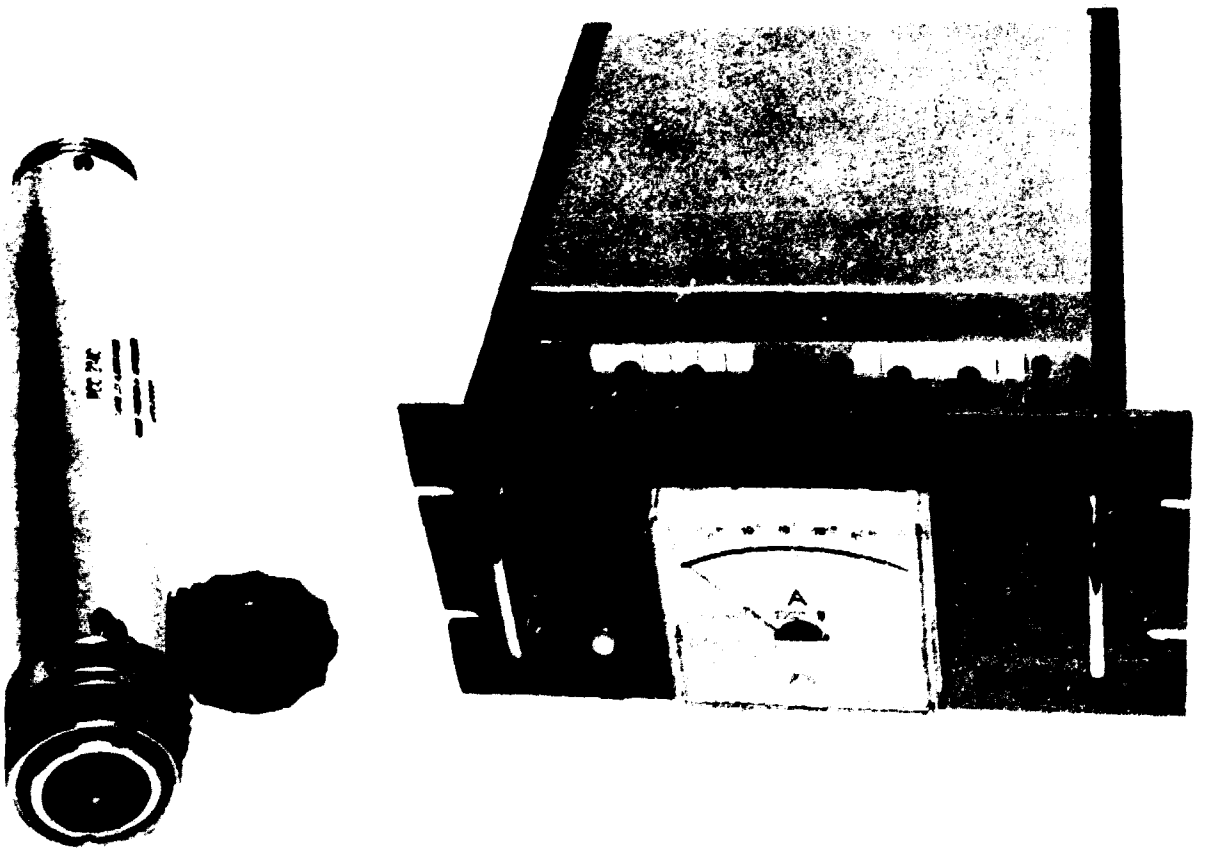


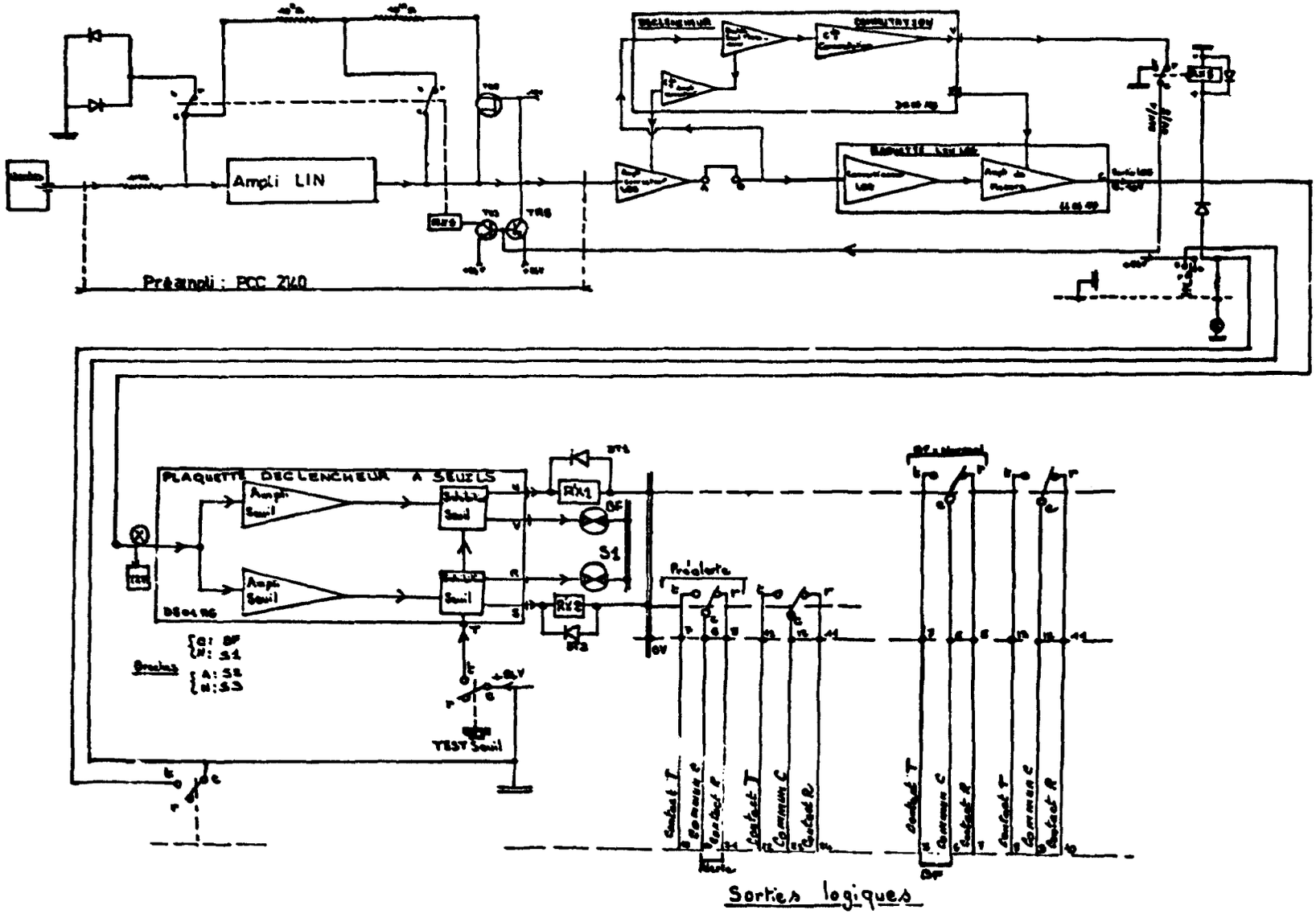
Figure 2

# 2 - ELECTRONIQUE AUPRES DES INSTALLATIONS NUCLEAIRES POUR TABLEAUX DE CONTROLE DE RADIOPROTECTION - T.C.R.

Une nouvelle génération de matériel est en cours d'élaboration. Pour l'établissement d'un projet et/ou la réalisation d'un T.C.R. il est recommandé de prendre contact avec les SES/SAI - M. COCHINAL (Saclay – poste 3455).

## 2.1 - Version "MONOBLOC"

| Nomenclature | Désignation | Type Article | Prix HT | Fournisseur |
|---|---|---|---|---|
| 61 47 07 58 | **Amplificateur pour courant continu à réponse linéaire ou logarithmique**<br>Cet appareil associé au préamplificateur PCC 2140 est destiné à la mesure et au contrôle de l'activité en radioprotection.<br>- Fonctionnement linéaire :<br>- 6 calibres de mesure commutables de 0 à $10^{-12}$ A, $10^{-13}$ A, $10^{-11}$ A, $10^{-10}$ A, $10^{-9}$ A, $10^{-8}$ A.<br>- précision relative : ± 2 % pour Ie ⩾ $10^{-12}$ A<br>- fluctuations : < 50 mV c. à c. pour Ie = 0<br>- Fonctionnement logarithmique :<br>- étendue de mesure : $10^{-10}$ A à $10^{-8}$ A<br>- précision relative : 9 à 20 % entre $10^{-12}$ A et $10^{-8}$ A<br>- fluctuations : < 200 mV c. à c. pour Ie = $10^{-10}$ A<br>- temps de réponse de $10^{-12}$ à $9.10^{-12}$ A : < 15 s<br>En fonctionnement LIN-LOG, le dépassement de la gamme fait passer automatiquement la sortie qui est en fonctionnement linéaire en fonctionnement logarithmique.<br>- Sortie directe : 0 à –10 V, 5 mA<br>- Sortie enregistreur : 0 à –50 mV ± 1 mV<br>- 4 déclencheurs à seuil, connectés en sortie logarithmique, réglables de 0 à –10 V, sortie 2 inverseurs.<br>- Haute tension : ± 600 V<br>- Alimentation : 220 V/50 Hz<br>- Consommation : < 20 VA<br>- Présentation en minichâssis autonome dont l'encombrement est la moitié de celui d'un châssis 3 U3 - Possibilité de deux voies de mesure par châssis 3 U3<br>- Masse : 5,5 kg<br>NB : 1) Connecteur de liaison avec préamplificateur : SOCAPEX 319 L<br>2) Le préamplificateur utilisable, non fourni avec l'appareil, est du type PCC 2140<br>3) Appareil livré avec cordon de 5 m permettant la liaison au préamplificateur. | ALILOG 21 | | MG |
| 51 47 37 21 | **Préamplificateur pour ALILOG 21**<br>Cet appareil est normalement prévu pour être associé à l'amplificateur ALILOG 21.<br>- Fonctionnement linéaire<br>- Résistances de mesure : $10^9$ Ω (± 1 %)<br>$10^{12}$ Ω (± 2 %)<br>- commutables à partir de l'ALILOG 21.<br>- Courant de fuite à l'entrée : ⩽ $5.10^{-13}$ A<br>- Sorties hautes tensions (± 600 V) pour polarisation des chambres<br>- Raccordements : entrée PF 34/37 BKB (SOCAPEX)<br>sortie PM 319 L (SOCAPEX)<br>- Dimensions : boîtier cylindrique L = 280 mm<br>Ø = 48 mm<br>- Masse : 0,6 kg | PCC 2140 | | MG |
| 61 28 41 40 | **Intensimètre linéaire et logarithmique**<br>Cet appareil associé au préamplificateur PIL 1[illegible] permet la mesure du débit de flux entre 0,1 c/s et $10^6$ c/s<br>- soit sur une échelle logarithmique (6 décades)<br>- soit sur une échelle linéaire (5 calibres)<br>L'ensemble est destiné aux mesures d'activité en radioprotection. Il est conçu pour des détecteurs délivrant des impulsions.<br>En fonctionnement LIN-LOG le dépassement de la gamme fait passer automatiquement la sortie qui est en fonctionnement linéaire en fonctionnement logarithmique.<br>- sortie directe : 0 à –10 V, 1 mA<br>sortie enregistreur : 0 à –50 mV | ILILOG 11 | | MG |




CIRCUIT ALARME

Figure 3

sont donc à considérer pour cette étude. Par conséquent, les circuits de mesure linéaire, les alarmes locales (voyants) et le test ne serontpas pris en compte.

## II.2 Description de la structure considérée

La stucture retenue pour cette étude fait l'objet de la Figure 3. Cette chaîne peut-être décomposée de la façon suivante :

1 - Le préamplificateur PCC 2140 avec ses 2 résistances T.H.V. de $10^9$ et $10^{12}$ ohms.

2 - Le circuit Convertisseur Lin-Log comprenant en série :
- un Ampli-Correcteur Log
- un Ampli-Convertisseur Log et un Ampli de Mesure (soit une plaquette Lin-Log)
- et en parallèle : une plaquette Déclencheur Commutation

3 - Le circuit "Alarme" constitué par :
- les Seuils BF, S1 et S2, S3 cablés sur 2plaquettes "Déclencheur à Seuils" identiques
- la commande des alarmes réalisée par :
- les Relais R'X1, R'X2 et R'X3, R'X4
- les contacts BF, S1 (Préalerte), S2 et S3 (Alertes)

4 - Le circuit à Relais RX1 et RX5 qui commande la commutation automatique des gammes

5 - Toutes les alimentations BT et HT

## II.3 Rappel des conditions de bon fonctionnement

Deux gammes de mesure S et s sont prévues comme suit :

a) Une gamme plus sensible S correspondant à des courants d'entrée allant de 10-14 A à 10-11 A. La mise en service de la résistance T.H.V. de $10^{12}$ ohms est assurée par la position "travail"du relais RX1.

b) Une gamme moins sensible s pour des courants d'entrée allant de $10^{-11}$ A à $10^{-8}$ A. Cette fois-ci la mise en service de la résistance T.H.V. de $10^9$ ohms est

commandée par la position "repos" du relais RX1.

IMPORTANT : Par conséquent, toute défaillance catalectique d'un composant conduisant à la mise au repos du relais RX1 (coupure de la bobine ou absence de 24 volts aux bornes) impose le fonctionnement sur la gamme la moins sensible.

Le tableau ci-après définit la position des relais suivant les différentes situations (T = position "Travail" R = position "Repos").

| FONCTIONS | RELAIS | POSITIONS DES RELAIS | | | |
|---|---|---|---|---|---|
| | | Fonctionnement LOG | | Fonctionnement LIN | |
| | | Gamme S | Gamme s | Gamme S | Gamme s |
| Commutation de gammes | RX1 | T | R | T | R |
| " " " | RX5 | R | R | T | R |
| | | ALILOG 21 en attente | ALILOG 21 en alarme | ALILOG 21 en attente | ALILOG 21 en alarme |
| Seuil BF | R'X1 | T | T | T | T |
| Seuil S1 | R'X2 | T | R | T | T |
| Seuil S2 | R'X3 | T | R | T | T |
| Seuil S3 | R'X4 | T | R | T | T |

inhibition

## III - REMARQUES PAR RAPPORT A L'EXPERTISE TECHNOLOGIQUE (1)

Nous formulerons ici les remarques relatives à l'expertise technologique qui a été faite en Novembre 1974 sur un prototype du PCC 2140 et de l'ALILOG 21. Peu d'améliorations ont été apportées depuis.

On trouve notamment que :

- Il y a toujours des risques de confusion entre plusieurs repères sur les schémas ; par exemple le point A revient plusieurs fois, les relais RX1 et RX2 se retrouvent dans le PCC2140 et l'ALILOG 21. Pour les distinguer nous

les avons surnommés R'X1 et R'X2 dans l'ALILOG 21.

- Le calibre des fusibles FU1 et FU2 n'est toujours pas indiqué, ce qui est gênant pour l'utilisateur.

- Les connexions des résistances de haute valeur, montées sur des isolants en téflon, sont pliées au ras de l'ampoule de verre, risquant d'y provoquer des micro-fêlures.

- Le transformateur touche les composants, de la carte voisine.

- Sur la plaquette HT, il n'y a pas de notation pour repérer les composants.

- Les plaquettes HT et RD se touchent ce qui risque de provoquer à long terme des court-circuits.

- Sur la plaquette BT, le PD2 n'est pas référencé et les transistors TR1, TR2 sont montés sans soin.

- Sur la carte de commutation, le câblage des picôts gêne l'accés aux composants.

- Le châpitre "maintenance" de la notice est incomplet, seules les précautions à prendre pour remplacer le transistor MOS d'entrée sont mentionnées.

- La liaison entre les broches 3 et 4 du connecteur "sorties logiques" n'est pas clairement indiquée dans la notice; elle est obligatoire pour la mise en service de l'équipement.

- Observations particulières :

(1) Une précaution particulière est à prendre pour la maintenance car le voyant bleu, signalant la mise sous tension, s'éteint en cas de défaillance du circuit de redressement BT, par conséquent ne signale plus la présence du réseau. Le voyant devrait être branché au secondaire du transformateur.

(2) Bien que la ligne de continuité ne soit pas effective entre le préamplificateur et l'ALILOG 21, ni sur la plaquette HT, une coupure à ce niveau provoquerait une baisse immédiate du signal d'entrée et serait détectée par le circuit BF. Grâce à cet artifice, nous pouvons dire que cet équipement est conforme aux normes MCH[M], à l'exception de l'isolement des connecteurs de sorties analogiques et logiques.

## TABLEAU B

**EFFICACITE DU SEUIL BF**

| INFORMATION BF BONNE<br>c.c. entre broches 5 et 6 ou 8 et 9<br>c.o. entre broches 6 et 7 ou 9 et 10 | INFORMATION BF MAUVAISE<br>c.c. entre broches 6 et 7 ou 9 et 10<br>c.O; entre broches 5 et 6 ou 8 et 9 |
|---|---|
| Signal en X > Seuil BF<br><br>DC 04 MG en panne (1)<br><br>DS 01 MG en panne (1) | - Pas de strappe entre les bornes 3 et4 du connecteur "sorties logiques"<br>- Signal en X < Seuil BF<br>- Fusibles sautés<br>- pas de ± 15 V<br>- pas de 24 V<br>- pas de HT ou baisse importante<br>- DC 04 MG en panne (2)<br>- LL 04 MG en panne<br>- DS 01 MG en panne (2)<br>- Toutes défaillances catalectiques (ou pannes sures) du PCC2140 et de l'ALILOG 21<br>(Taux de défaillance moyen = $46077.10^{-9}$/H.) |

(1) pour un niveau de signal d'entrée supérieur à $10^{-11}$ A (gamme s)

(2) pour un niveau de signal d'entrée inférieur à $10^{-11}$ A (gamme S)

* MCH (2) Ce sont des normes internes C.E.A. concernant la fabrication des matériels de contrôle de réacteurs nucléaires.

## IV - ETUDE DE SURETE

### IV.1 Principe de fonctionnement de l'information "BF"

Une analyse appronfondie du schéma montre que toutes défaillances catalectiques des composants situés hors du circuit d'alarme provoquent le non-fonctionnement du voyant BF et le repos du relais R'X1 (court-circuit entre les broches 6 et 7, puis 9 et 10 du connecteur "sorties logiques") l'utilisateur est alors averti. Ceci se traduit par l'annulation du niveau du signal sur la broche C de la carte "Déclencheur à Seuils"; ce point (X) est d'ailleurs commun aux entrées des 3seuils S1, S2 et S3. Toutes ces défaillances constituent en fait ce que l'on appelle les "PANNES SURES". Pour mieux montrer l'importance du circuit de "Bon-Fonctionnement" nous dresserons un tableau de validité. Nous nous placerons uniquement dans le cas où l'information est recueillie sur le connecteur "sorties logiques" ce qui est indispensable pour une utilisation en équipement de sécurité. Ces sorties sont inhibés en cas de test et de fonctionnement en "linéaire", ce qui n'est bien sûr pas le cas pour les voyants BF, S1, S2 et S3.

(voir tableauB ci-contre)

### IV.2 Pannes Non-Sûres

Il existe toutefois certains modes de défaillance qui, simultanément :

- ne perturbent pas le circuit de bon fonctionnement (BF)
- interdisent le déclenchement des alarmes (S1, S2 ou S3).

Ces événements concernent les pannes du circuit relatif aux seuils S1 ou S2 ou S3, câblés sur les plaquettes "Déclencheur à Seuils" DS 01 MG soit $\overline{S1}$ ou $\overline{S2}$ ou $\overline{S3}$. L'utilisateur étant assuré du bon fonctionnement de sa chaîne de mesure (voyant BF allumé) ne sera pas, dans ce cas averti du franchissement éventuel du seuil S1 (ou S2 ou S3), par

## TABLEAU C

### ANALYSE DES EVENEMENTS ELEMENTAIRES ET EVALUATION DE LEUR TAUX DE DEFAILLANCE

**PANNES NON-SURES : SILENCE INJUSTIFIE de $S_1$**

| EVENEMENTS CODE | Modes de défaillance | PONDERATION | $\lambda$ GLOBAL en $10^{-9}$/H | TOTAL : $\lambda$ en $10^{-9}$/H |
|---|---|---|---|---|
| | 1 - CONNECTEUR SORTIE ALARME EM 337P | | | |
| 0100 | c.o broches 20 et 21 | 2 | 0,5 | 1 |
| | 2 - CIRCUIT RELAIS sch.912979 | | | |
| | RELAIS R'X2 | | | |
| 0200 | c.o contacts 5 et 6 | 2 | 10 | 20 |
| 0201 | c.o contacts C et R | 1/10 | 230 | 23 |
| | 3 - PLAQUETTE DECLENCHEURS A SEUILS | | | |
| | DS.01 MG | | | |
| 0300 | c.o broches H, R | 2 | 10 | 20 |
| 0301 | c.c BE TR7 | 1/4 | 36 | 9 |
| 0302 | c.o BC TR6 | 1/4 | 36 | 9 |
| 0303 | c.o BE TR6 | 1/4 | 36 | 9 |
| 0304 | c.o R 21 | | 15 | 15 |
| 0305 | c.o R 18 | | 15 | 15 |
| 0306 | A2 sortie +15V | 1/3 | 960 | 320 |
| 0307 | c.o DT6 | 1/2 | 7 | 3,5 |
| 0308 | c.o R16 | | 15 | 15 |
| 0309 | c.o R19 | | 15 | 15 |
| 0310 | c.o PT1 (masse) | 1/3 | 153 | 51 |
| 0311 | c.O PT1 (curseur) | 1/3 | 153 | 51 |
| | | | | Total : 576,5 |

Lexique : c.o = circuit ouvert
c.c = court circuit

# Arbre de défaillance

Evènements conduisant au SILENCE INJUSTIFIE du seuil S1

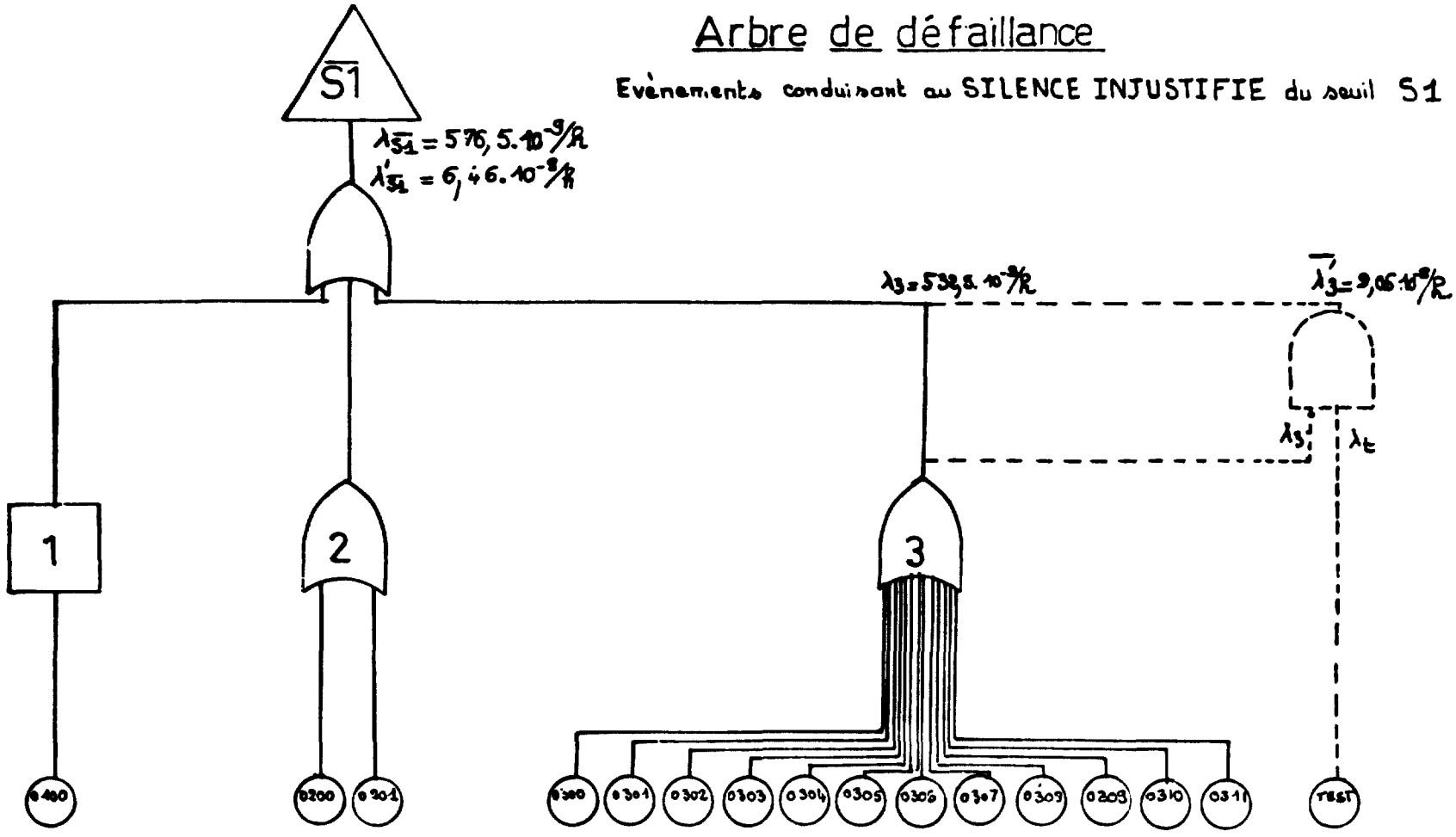



Figure 4

le signal d'entrée.

Nous pouvons dire, que nous nous trouvons en situation de PANNES NON-SURES.

Pour apprécier l'importance du risque encouru par ces incidents, il est indispensable d'établir un arbre de défaillance du circuit "Déclencheur à Seuils" et de rechercher les modes de défaillance qui conduisent au "SILENCE INJUSTIFIE" $\overline{S1}$. Les événements qui conduisent à des fausses alarmes ne sont pas pris en compte.

Les événements élémentaires conduisant aux pannes non-sûres sont classées et codifiés dans le tableau C ci-après. Chacun des modes de panne a été affecté d'un taux de défaillance établi à partir d'une banque de données en usage au C.E.A.

L'arbre de défaillance fait l'objet de la Figure 4 et ne comporte que 15 événementsélémentaires. Cette analyse est identique pour les circuits "seuil" S2 ou S3.

Comme l'arbre de défaillance ne comporte que des "portes OU", le taux de défaillance total pour $\overline{S1}$ est la somme des taux élémentaires. On obtient :

- le taux de défaillance conduisant à la panne non-sûre $\overline{S1}$ est de : $\lambda_{\overline{S1}} = 576,5.\ 10\text{-}9/h.$

Par raison de symétrie, $\lambda_{\overline{S1}} = \lambda_{\overline{S2}} = \lambda_{\overline{S3}}$ car les circuits sont identiques.

## IV.3 Calcul du risque de pannes non-sûres

Pour évaluer le risque suivant le critère défini au paragraphe 1.2, il faut calculer la probabilité conditionnelle suivante :

- risque = $p_r = p_{\overline{S1}} \times R(t)$

= $p_{\overline{S1}}$ = probabilité de pannes non-sûres du circuit "seuil" S1 à un instant donné.

- R(t) = fiabilité de la chaîne PCC 2140 et ALILOG 21 à l'instant t.

En effet, il s'agit de calculer cette probabilité $p_{\overline{S1}}$ alors que l'utilisateur sait que son appareil marche bien. L'information BF correcte correspond en fait à la fiabilité de l'équipement.

Nous calculerons ce risque pour une période de lan, soit 8760 heures. La MTBF de la chaîne PCC 2140 et ALILOG 21 a été calculée par le programme PEFAT. Les résultats font l'objet du diagramme de PARETO (voir Figure 5)

MTBF = 18.613 heures

- Calcul de la fiabilité à 8760 heures :

$$R(t) = e^{-\frac{t}{MTBF}} = e^{-\frac{8760}{18.613}} = 0,625$$

- Calcul de $P_{\overline{S1}}$ :

$$P_{\overline{S1}} = 1 - e^{-\lambda_{\overline{S1}} t} = 1 - e^{-576,5.10-9 \times 8760} = 0,005$$

- Evaluation du risque annuel $P_r$ de pannes non-sûres S1

$$P_r = P_{\overline{S1}} \times R(t) = 0,005 \times 0,625 = 3,13.10-3$$

risque annuel = 3,13.10-3

Nous pouvons également calculer le risque de n'avoir :

- ni l'alarme S1, ni l'alarme S2 : $P_{r2}$
- ni simultanément les alarmes S1, S2 et S3 : $P_{r3}$

$$P_{r2} = P_{\overline{S1}} \times P_{\overline{S2}} \times R(t) = (0,005)^2 \times 0,625 = \underline{1,56.10-5 \text{ à 1 an}}$$

$$P_{r3} = P_{\overline{S1}} \times P_{\overline{S2}} \times P_{\overline{S3}} \times R(t) = (0,005)^3 \times 0,625 = \underline{7,81.10-8 \text{ à 1 an}}$$

IV.4 Proposition de test pour diminuer le risque annuel $P_r$

Revenons à l'arbre de défaillance (Figure 4).

Nous remarquerons que tout le poids de fiabilité provient de la "porte OU" N°3 correspondant aux 12 évènements élémentaires de la plaquette "Déclencheur à Seuils" DS 01 MG.

$$\lambda_3 = 532,5.10-9/h$$

Or le TEST prévu sur l'appareil permet justement de vérifier

----- CARACTERISTIQUES DE L'EXECUTABLE <"1> : PCC2140+ELIOC21 --

LE 12/7/1477 A 9 HEURES 58 MIN.

TEMPS..... = 18613.31 SECONDES.
MAX MOYEN..... = 5.37250E-05 OCTETS/SECONDE.

** DIAGRAMME DE RARETE PAR BLOCS

| BLOC | * NOMBRE * | LA/DA | * % | * DIAGRAMME DE FRAGILITE 0 5 10 15 20 25 |
|---|---|---|---|---|
| B7 | 1 | 1.03350E-05 | 20.35 | [[[[[[[[[[[[[[[[[[[[ |
| B6 | 1 | 9.06600E-06 | 16.87 | [[[[[[[[[[[[[[[[ |
| B4 | 2 | 6.67200E-06 | 12.42 | [[[[[[[[[[[[ |
| B1 | 1 | 6.39400E-06 | 11.90 | [[[[[[[[[[[ |
| B8 | 1 | 5.31000E-06 | 9.88 | [[[[[[[[[ |
| B10 | 1 | 4.85200E-06 | 9.11 | [[[[[[[[[ |
| B5 | 1 | 4.73200E-06 | 8.81 | [[[[[[[[[ |
| B1 | 1 | 3.96000E-06 | 7.37 | [[[[[[[ |
| B9 | 1 | 1.25000E-06 | 2.33 | [[ |
| B3 | 1 | 3.14000E-07 | .58 | [ |

LEGENDE DES BLOCS :

| NUMERO | LIBELLE |
|---|---|
| B1 | PCC2140 |
| B2 | CHASSIS |
| B3 | PD-01-MC |
| B4 | DS-01-IC |
| B5 | DC-04-MC |
| B6 | LL-04-IC |
| B7 | PT-02-MC |
| B8 | PT-02-IC |
| B9 | CIRCUIT RELAIS |
| B10 | CIRCUIT COMMUTATEUR |

toute la chaîne en injectant notamment un courant de 10-10 A à l'entrée du PCC 2140. Ceci permet de vérifier au moins le bon fonctionnement du premier seuil S1 et de l'alarme locale correspondante (voyant S1).

On peut considérer que la fiabilité de la chaîne tend vers 1 juste après ce test et qu'entre 2instants de test, cette fiabilité décroit suivant R(t).

A titre d'exemple, nous supposerons ici un test mensuel. Le taux de défaillance $\lambda_t$ entre 2 tests est celui de l'équipement et calculé par PEFAT sur la Figure 3 :

$$\lambda_t = \text{taux moyen} = 5{,}3721.10\text{-}5/h$$

Si nous procédons systématiquement à ce test mensuel, cela revient à introduire une "porte ET" représentée en pointillée sur la Figure 4 car les évènements conduisant au silence injustifié sur la 3$^{eme}$ branche dépendront des pannes non-sûres du circuit "seuil S1" (Taux = $\lambda_3$ = 532,5. 10-9/h) et de la non-détection de ces dernières, ce qui se traduit par le taux de défaillance entre 2 tests (Taux = $\lambda_t$ = 5,3725. 10-5/h).

Pour un test mensuel soit tous les 720 heures, le taux de défaillance moyen équivalent $\lambda'_3$ devient :

$$\lambda'_3 \# \lambda_3 \times \lambda_t \times 720 = 2{,}06.\ 10\text{-}8/h$$

Dans ces conditions, le taux de défaillance global conduisant au SILENCE INJUSTIFIE du seuil S1 devient :

$$\lambda'_{S1} = 6{,}46.10\text{-}8/h$$

$$P'_{\overline{S1}} = 5{,}65.\ 10\text{-}4/h$$

d'où, le risque annuel de pannes non-sûres $\overline{S1}$ tombe alors à :

$$\text{risque avec test mensuel} = P'_r = P'_{\overline{S1}} \times R(t) = 5{,}65.\ 10\text{-}4 \times 0{,}625$$

$$P'_r = 3{,}54.\ 10\text{-}4$$

Dans ces conditions, on voit que le risque annuel est divisé par un facteur 10.

## V - CONCLUSION

L'absence de tension aux bornes du relais RX1 du PCC 2140

ou la coupure de sa bobine conduit effectivement à la position "repos" des contacts et à la commutation de gamme s, la moins sensible. Cette situation qui paraissait, au moment, de l'étude du PCC 1140 et ACC 1140 Log, ne pas aller dans le sens de la sûreté, devient maintenant sur la chaîne PCC 2140 et ALILOG 21 une panne SURE car l'efficacité de l'information BF prévient l'utilisateur de ce genre d'incident.

Il existe toutefois un certain risque de pannes NON-SURES qui interdisent les alarmes S1, ou S2 ou S3 alors que l'information BF est correcte. Ce risque a été évalué annuellement à 3,13. 10-3 mais peut-être notablement réduit à 3,54. 10-4 en effectuant une fois par mois le TEST prévu par le constructeur, ce qui ne doit pas poser de problème à l'utilisateur. Bien sûr avec un test journalier, on reduirait encore considérablement ce risque de "Pannes Non-Sûres".

Compte tenu de la classe de l'appareil qui ne peut être utilisé comme équipement de surveillance que sur la position LOG, le risque de 0,00035 chance par an nous semble très satisfaisant.

L'accord du GEC donné le 21-12-76 à MERLIN GERIN nous parait donc tout à fait justifié.

*Manuscrit reçu le 21 novembre 1977*

## REFERENCES BIBLIOGRAPHIQUES


(1) J. KERMORGANT et D. KRAKOWSKI "COMPTE RENDU DE MISSION A LA SOCIETE MERLIN-GERIN GRENOBLE" SES/GEC/R.3458

(2) 3ème édition du document MCH/MENT-1 "MATERIEL ELECTRONIQUE NUCLEAIRE POUR TABLEAU DE COMMANDE ET DE CONTROLE" SPECIFICATIONS GENERALES" SES/INT/SAI/75-23

(3) P. MERIAUX "EVALUATION DU RISQUE DANS LE CAS DU SILENCE INJUSTIFIE POUR LA BALISE C/IEP" SES/SGM/R.101

(4) S. ADNOT "ETUDE COMPARATIVE DE TROIS PROGRAMMES POUR L'EVALUATION RAPIDE DE LA FIABILITE" NOTE-CEA-N-1859.


-:-