
Diagnostic d'équipements avioniques par corrélation temporelle

**Arnaud Lefebvre, Zineb Simeu-Abazi, Jean-Pierre Derain,
Mathieu Glade**

*Eurocopter, aéroport Marseille-Provence, Marignane France,
arnaud.lefebvre@eurocopter.com*

*Laboratoire G-SCOP, 46 avenue Félix Viallet 38031 Grenoble, France,
Zineb.Simeu-Abazi@g-scop.inpg.fr*

*Eurocopter, aéroport Marseille-Provence, Marignane France, jean-
pierre.derain@eurocopter.com*

*Eurocopter, aéroport Marseille-Provence, Marignane France,
mathieu.glade@eurocopter.com*

RÉSUMÉ. Cet article présente une méthode de diagnostic d'équipements avioniques basée sur la corrélation temporelle d'événements. Une défaillance est détectée grâce à l'exécution de tests intégrés organisés sous forme d'arbres de tests. La méthode proposée repose sur deux paramètres: la donnée temporelle relative au parcours des arbres de tests et le temps de propagation des défaillances. La fenêtre de corrélation temporelle entre les messages de panne est obtenue grâce à l'analyse des chemins de propagation. L'identification de cette fenêtre temporelle permet de déterminer le degré de corrélation entre panne. Il s'agit là de distinguer les messages de panne dus à des défaillances simples avec phénomène de propagation, et l'occurrence de défaillances multiples.

ABSTRACT. This article presents a method of diagnosis of avionics equipment based on the temporal correlation of events. A failure is detected thanks to the execution of built-in tests organised in test trees. The method proposed is based on two parameters: the temporal data coming from the test tree execution and the propagation time of failures. The temporal correlation window between the failure messages is obtained thanks to the analysis of the ways of failure propagation. The identification of this time window allows determining the degree of correlation between the different failure messages. The goal is to distinguish between single failure occurrence with propagation phenomenon, and multiple occurrences of failure.

MOTS-CLÉS : Equipements avioniques, tests intégrés, arbres de test, diagnostic, propagation de panne, corrélation temporelle.

KEYWORDS: Avionics Equipment, integrated tests, test trees, diagnosis, failure propagation, temporal correlation

1. Introduction

Dans le secteur aéronautique, la maintenance représente à ce jour la tâche la plus coûteuse dans le cycle de vie d'un aéronef (Glade, 2005). Les grandes lignes directrices sont l'amélioration de la disponibilité des appareils et l'optimisation des coûts liés à la maintenance des équipements, et ce, durant tout le cycle de vie de l'appareil. Actuellement, la partie avionique a été dotée d'autotests (BIT : Built In Test). Ces BIT sont présents sur pratiquement toutes les cartes électroniques et ont pour but de délivrer une alarme dès qu'une discordance est observée. Le diagnostic de ces alarmes n'est traité qu'une fois que l'appareil est au sol. Il subsiste alors, des problèmes d'ambiguïtés de localisation qui retardent les actions de maintenance ou provoquent des opérations de maintenance inutiles telles que des fausses déposes, ou demande de longues procédures de test pour isoler la défaillance.

Pour améliorer les opérations de localisation, il convient donc de compléter le système existant par un organe qui analyse les résultats d'autotests qui sont générés automatiquement. En effet, lorsqu'un défaut apparaît, il doit être détecté le plus rapidement possible, localisé et sa cause identifiée. Les étapes classiques d'observation et de suivi doivent être complétées par une étape déductive qui correspond à la recherche de la cause: le diagnostic.

Les méthodes de diagnostic utilisées dans les différents secteurs industriels sont très variées et tiennent compte de la spécificité des matériels qui constituent leurs procédés industriels. L'opération de diagnostic est définie comme étant l'identification de la cause probable de la (ou des) défaillance(s) à l'aide d'un raisonnement logique fondé sur un ensemble d'informations d'une inspection, d'un contrôle, ou d'un test de maintenance (norme AFNOR). Pour certains procédés relativement simples, les relations entre les causes et leurs effets sont biunivoques et le diagnostic par raisonnement inverse est simple. Par contre, pour des procédés plus complexes (Lunze et al., 2001), comme pour les systèmes avioniques, le diagnostic n'est possible qu'en faisant appel à des techniques efficaces qui nécessitent des développements particuliers.

Cet article propose une méthode de diagnostic originale basée sur le modèle dynamique issu de l'analyse temporelle des différents tests exécutés.

Après une brève présentation des méthodes de diagnostic actuelles des équipements avioniques, le principe général de la méthode de corrélation des pannes est proposé.

2. Diagnostic des équipements avioniques : Etat de l'art

Un hélicoptère peut être décomposé 5 grandes parties qui sont:

La partie structure, la partie moteur, la partie hydraulique, la partie rotor et la partie avionique. La partie avionique est responsable d'environ 25% du coût direct induit par la maintenance (Ghelam, 2006).

Dans cet article, on s'intéressera particulièrement aux équipements avioniques et au diagnostic des défaillances apparaissant sur ses équipements.

2.1 Les tests intégrés

Afin de faciliter les opérations de maintenance, la partie avionique est divisée de différents sous-systèmes composés d'équipements appelés LRU (Line replace unit). Un LRU est composé d'un ensemble de cartes électroniques nommées SRU (Shop Replace Unit).

Afin de réaliser un diagnostic rapide et efficace, des tests automatiques (BIT : Built In Test) ont été intégrés sur la partie avionique. Ces BIT sont présents sur la majorité des cartes électroniques et ont pour but de délivrer une alarme quand la valeur mesurée par le test sort des limites de tolérance de l'équipement. L'ensemble des tests implémentés sur un équipement avionique a pour but de donner une information sur l'état de fonctionnement d'un équipement aux équipes de pilotages et de maintenance. De manière générale, on distingue 3 modes de fonctionnements :

- L'état de bon fonctionnement, quand aucun test automatique ne donne d'information de défaillance.
- L'état de fonctionnement dégradé, quand un ou plusieurs tests intégrés remontent un dysfonctionnement ne correspondant pas à une perte de fonctionnalité, mais à une dégradation des performances de l'équipement.
- Un état de mauvais fonctionnement, quand un ou plusieurs tests intégrés d'un équipement remontent un dysfonctionnement correspondant à une perte de fonctionnalité de l'équipement.

Il existe trois types de tests intégrés pouvant générer une alarme

- Le PBIT (Power Up Built In Test): Test perturbant exécuté à la mise sous tension d'un équipement. Le but de ce test est de réaliser un test le plus exhaustif possible des fonctionnalités de l'équipement et de remonter une information sur le fonctionnement des différents équipements au pilote.
- Le CBIT (Continuous Built In Test) : Test non perturbant exécuté durant tout le fonctionnement opérationnel de l'équipement. Ce test est effectué en tâche de fond par rapports aux fonctions de l'équipement. Il a pour but d'informer le pilote en cas de défaillance afin de permettre de réaliser les

4 nom de revue, volume, n°, année de parution

opérations en vol adéquates pour garder un niveau de sécurité suffisant pour les passagers et la machine.

- L'IBIT (Initiated Built In Test) : Test perturbant, effectué sur demande de l'opérateur de maintenance au sol pour confirmer et améliorer les résultats fournis par le PBIT et le CBIT. Lorsqu'une panne a été détectée, l'opérateur de maintenance peut être amené à exécuter un test complémentaire pour confirmer la présence de la panne, ou pour affiner la localisation donnée par l'organe de diagnostic.

Les tests sont organisés par équipement sous forme d'arbres. Ces arbres de test sont exécutés en boucle. L'agencement de ces tests intégrés est défini par l'équipementier en charge du développement de l'équipement. Pour notre étude on s'intéresse essentiellement aux arbres de tests non perturbants (CBIT) qui sont le mode de test réalisé tout au long de la phase de vol de l'hélicoptère.

2.2 Gestion informationnelle

Lorsqu'une défaillance est détectée, une alarme est générée par un équipement, l'information relative à l'alarme est stockée en mémoire non-volatile de l'équipement. L'alarme est aussi envoyée au calculateur de maintenance qui recueille toutes les alarmes des différents équipements et leur affecte une information temporelle correspondant au temps d'apparition de cette alarme. Les informations relatives à une alarme dans le calculateur de maintenance sont :

- Le numéro du vol
- L'équipement émetteur de l'alarme (LRUi, SRUi)
- Le numéro du test qui a généré l'alarme au sein de l'équipement émetteur (Ti)
- Le mode de détection du test ayant détecté l'alarme : PBIT, CBIT, IBIT
- La date d'occurrence de l'alarme (ti)
- Le caractère de la défaillance (panne intermittente, transitoire, constante).
- Les paramètres complémentaires associés à la défaillance (Vitesse rotor, Température, Vibrations...)
- La phase de vol de l'hélicoptère (phase d'allumage sur batterie, phase de vol ascendante, vol stationnaire ...)

Les différents messages de pannes enregistrés dans le calculateur de maintenance sont ensuite exploités pour donner une information opérationnelle au pilote et pour amener une information de maintenance au sol à l'opérateur de maintenance.

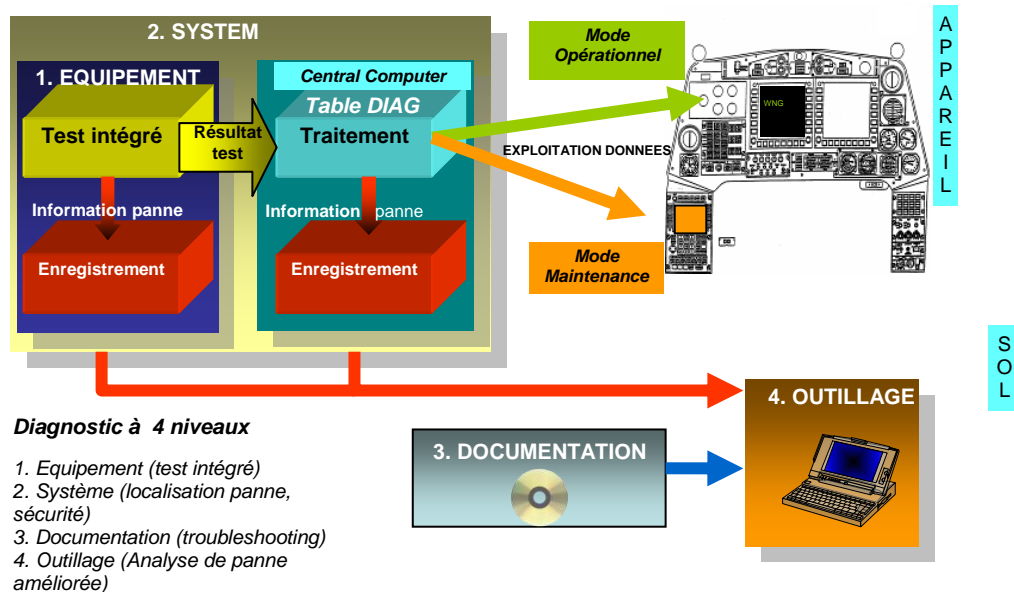


Figure 1. Schéma synoptique du concept de diagnostic sur un hélicoptère

La table de diagnostic nommée « Table DIAG » sur la figure 1, associe à chaque message de panne, un ou plusieurs équipements suspectés d'être défaillants, ainsi qu'une probabilité de défaillance relative pour chacun des « équipements suspects ».

2.3 La problématique diagnostic

L'ambiguïté de localisation des défaillances est une problématique complexe. Elle peut se traduire de deux manières différentes sur un système avionique comme le présente la figure 2.

- Cas a : A une date donnée, un message de panne peut suspecter plusieurs LRU
- Cas b : Plusieurs messages de pannes peuvent suspecter le même LRU.

Dans les deux cas, seule une analyse de la corrélation entre panne avec la prise en compte de la date d'occurrence des défaillances peut lever de telles ambiguïtés de localisation.

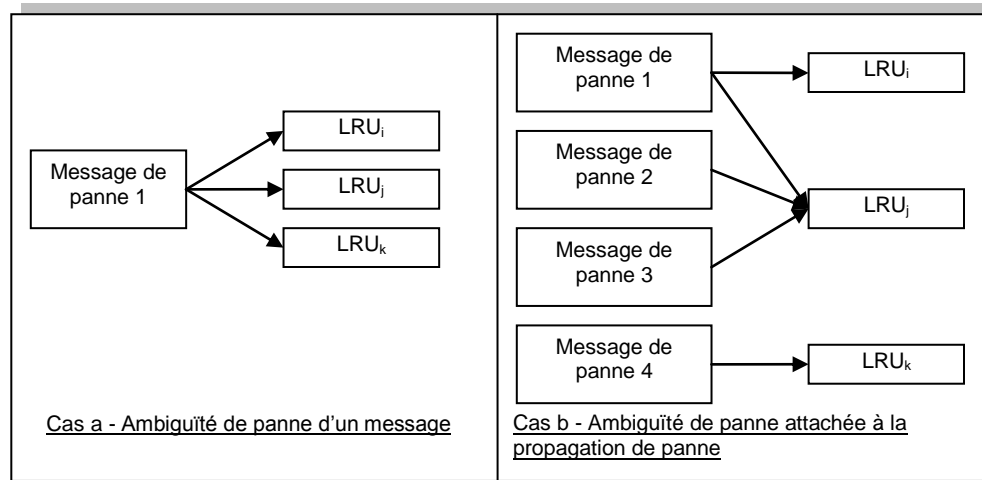


Figure 2. Illustration des deux phénomènes générant des ambiguïtés de pannes

2.4 L'ambiguïté de localisation attachée à un message

Les performances de détection d'une défaillance d'un équipement électronique sont liées à sa testabilité. Les taux de détection et de localisation de pannes servent d'indicateurs sur les capacités de testabilité intrinsèque des équipements. Aujourd'hui l'état de l'art permet de déterminer que le taux de détection des défaillances pour un équipement électronique est d'environ 80%. 60% des pannes détectées sont isolées sur un seul LRU. Donc dans 40% des cas, il existe une ambiguïté de localisation pour la défaillance détectée [GHE 06].

Les exigences données en début de conception d'un équipement définissent des taux de détection et d'isolation des pannes. Si on considère que 100 alarmes peuvent être générées par un équipement, alors :

- 90 alarmes au minimum sont susceptibles d'incriminer un seul équipement
- 5 alarmes sont susceptibles d'incriminer 2 équipements
- 5 alarmes au maximum sont susceptibles d'incriminer 3 équipements.

Pour résoudre ce problème d'ambiguïté de localisation, il est nécessaire de réaliser un suivi proactif des exigences de testabilité par rapport aux résultats obtenus. Cette ambiguïté ne peut être corrigée que par une meilleure définition des tests pendant la phase de conception de l'équipement.

2.5 L'ambiguïté de localisation amenée par la propagation des pannes

Il existe d'autres phénomènes venant perturber le diagnostic au niveau système : la propagation des défaillances. Le phénomène se traduit au niveau système par une

propagation des effets de la panne sur les équipements en aval, comme illustré sur la figure 3.

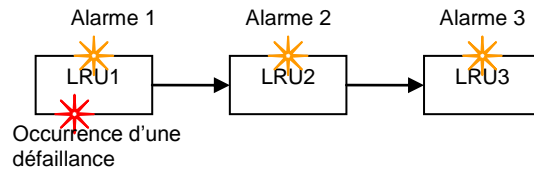


Figure 3. Illustration du phénomène de propagation

Dans le cas de propagation décrit dans la figure 3, il est nécessaire d'isoler les alarmes issues d'une défaillance commune. Les autres alarmes sont alors considérées comme décorrélées.

L'étude proposée dans ce papier présente l'approche temporelle permettant d'identifier les tests qui sont considérés comme corrélés et ceux qui ne le sont pas.

2.6 Hypothèses de travail

Pour modéliser le fonctionnement d'un équipement avionique, nous avons pris dans un premier temps les hypothèses suivantes :

- **Hypothèse 1 :** Les tests intégrés exécutés sur différents LRU.
- **Hypothèse 2 :** Chaque LRU s'autoteste en parallèle sans prendre en compte l'autotest des autres LRUs.
- **Hypothèse 3 :** Les tests d'un même LRU sont organisés en arbres de test dont l'exécution séquentielle génère une alarme lors de la détection d'une défaillance.
- **Hypothèse 4 :** Sur un arbre de test, il existe des tests pour la détection de défaillances (Tdi) et d'autres pour l'isolation de défaillances (Tli).
- **Hypothèse 5 :** L'information intrinsèque d'une alarme (W_i) peut incriminer différents LRU comme potentiellement défaillants. (Cas a et Cas b présentés et illustrés en figure 2)
- **Hypothèse 6 :** Lors de l'occurrence d'une défaillance plusieurs alarmes peuvent être déclenchées en cascade par phénomène de propagation.
- **Hypothèse 7 :** Suivant la configuration ou pour une mission donnée du système, le phénomène de propagation peut avoir lieu ou non.
- **Hypothèse 8 :** La configuration du système ne change pas pendant la durée d'un vol

3. Exploitation de la dynamique temporelle

Avec une problématique aussi complexe que le diagnostic des équipements électroniques, il est difficile de trouver un concept de diagnostic satisfaisant pour la partie avionique d'un hélicoptère.

Il existe aujourd'hui 3 types d'hélicoptères embarquant des capacités d'auto diagnostic. Plusieurs techniques ont été étudiées pour ces différents hélicoptères. On peut citer :

- La corrélation des messages de pannes avec des paramètres contextuels.
- La corrélation temporelle entre les différents messages de panne.
- La corrélation logique entre les différents messages de panne.

Aujourd'hui sur un hélicoptère, la fenêtre de corrélation temporelle entre deux alarmes a été fixée de manière empirique. Ainsi, dans une fenêtre temporelle qui correspond à une tolérance, toutes les alarmes générées par les équipements sont considérées comme corrélées et identifiant une défaillance commune.

Or, il est possible d'avoir une autre défaillance pendant ce même intervalle. De même, il est possible d'avoir des alarmes issues de la propagation des effets de la défaillance apparaissant après cette fenêtre de tolérance.

Dans cette étude, on cherche donc à déterminer comment dimensionner la fenêtre temporelle pour corréliser les alarmes de panne et lever ainsi les ambiguïtés de localisation.

3.1 Principe général du diagnostic

Pour l'identification des causes de défaillances, il existe deux grandes classes de méthodes : les méthodes de diagnostic internes et les méthodes de diagnostic externe. Lorsque l'on dispose d'une connaissance profonde du fonctionnement du système à travers l'analyse fonctionnelle, les méthodes de diagnostic interne sont utilisées. Dans le cas contraire, le diagnostic externe s'oriente vers des techniques du type reconnaissance de forme, l'intelligence artificielle ou aux réseaux de neurones qui nécessitent de disposer d'un retour d'expérience riche est parfaitement documenté. Les méthodes de diagnostic interne sont basées sur les informations d'entrées et sorties fournis par des capteurs ou des données temporelles (Blanke et al., 2003), (Knotek, 2006), (Yovine, 1993), (Zad, 1999).

Suite à une alarme (ou un dysfonctionnement) correspondant à un comportement incorrect, l'opération de diagnostic est déclenchée. Cette phase consiste à diagnostiquer, à localiser la cause du mauvais fonctionnement. La méthode proposée exploite les données temporelles du système. Elle consiste à retrouver l'ensemble des tests ayant provoqué une alarme entre l'instant initial étant t_0 et l'instant t_a correspondant au temps associé à l'occurrence d'un dysfonctionnement ou d'une alarme. L'idée est d'exploiter la notion temporelle (Tripakis, 1998) non

utilisée aujourd'hui du temps d'exécution d'un arbre de test. La corrélation de cette information aux temps d'occurrence des messages de panne permet de dimensionner la fenêtre de corrélation.

3.2 Arbres de test

Sur un équipement avionique, les tests intégrés exécutés en parallèle et pendant toute la durée de la mission sont organisés sous forme d'arbres séquentiels comme le montre la figure 4.

Rappelons que Td est un test de détection, Tl est un test de localisation, W est l'alarme résultante d'un test renvoyant un résultat différent du résultat attendu, comme le montre l'exemple de la figure 3.

Chaque alarme est accessible par un ou plusieurs chemins. Un temps d'exécution propre est associé à chaque test.

Le formalisme d'un arbre de test est très proche de celui d'un automate temporisé. On va donc se servir d'une modélisation à l'aide d'automates temporisés pour reproduire le fonctionnement d'un arbre de test.

Les nœuds de l'arbre sont de 3 types :

- Test de détection Td
- Test de localisation Ti
- Alarmes W.

Chaque test a un temps d'exécution propre qui sert de transition temporisée entre deux nœuds. En cas de dysfonctionnement de l'équipement, on peut atteindre un nœud correspondant à un warning, soit à partir d'un test de détection, soit à partir d'un test de localisation.

Une défaillance peut être caractérisée de trois façons différentes :

- Constante : la panne apparaît et reste présente jusqu'à la fin du vol
- Intermittente : la panne apparaît et disparaît plusieurs fois pendant le vol
- Transitoire : la panne est liée à un caractère transitoire d'un ou plusieurs paramètres pendant le vol d'un hélicoptère

Les alarmes sont considérées comme des « états deadlocks ». Pour le moment nous avons pris comme hypothèse qu'une défaillance est toujours constante (pas d'aspects transitoires ou intermittents), hors l'expérience montre qu'une défaillance peut avoir un caractère intermittent ou transitoire.

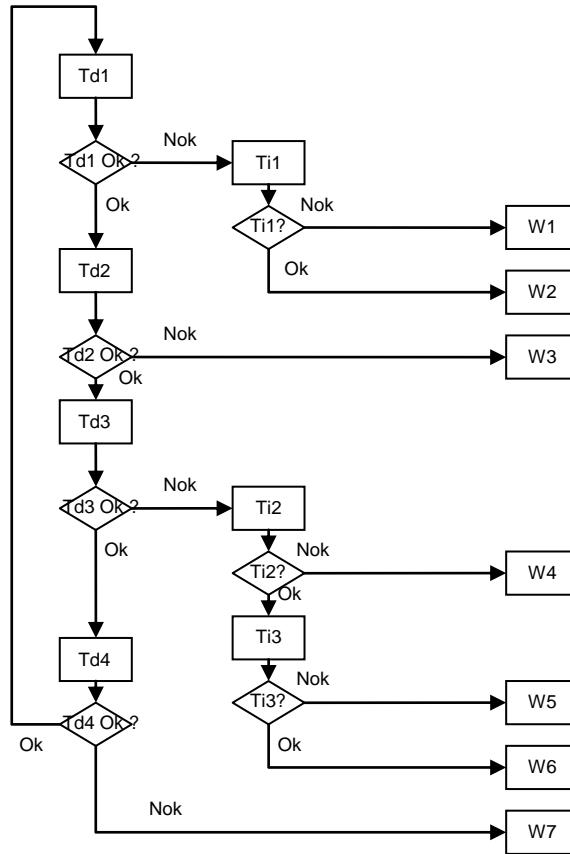


Figure 4. Exemple d'arbre de test

L'utilisation d'un automate temporisé nous permet de modéliser plusieurs arbres de tests s'exécutant en parallèle. Le but est de déterminer comment supprimer une ambiguïté de localisation due à une propagation de panne quand au moins deux alarmes sont générées.

4. Corrélation des messages de panne

Une propagation de panne se traduit par l'apparition en cascade de tests en aval de la défaillance. La principale problématique consiste à déterminer si les alarmes générées en aval de la défaillance sont à corrélérer entre elles, ou si elles témoignent de plusieurs défaillances différentes.

4.1 Corrélation structurelle

L'idée est d'exploiter la notion temporelle non utilisée aujourd'hui du temps d'exécution d'un arbre de test, pour corréler cette information aux messages de panne remontés afin de réaliser la discrimination de ces messages de panne.

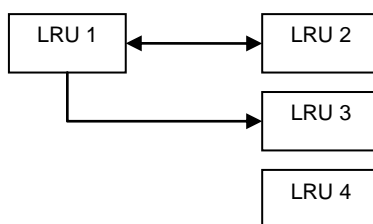


Figure 5. Exemple simplifié de système électronique

La première corrélation entre les messages de panne qui peut être proposé, est une corrélation logique induite par les relations entre les différents équipements constituant le système. L'analyse de l'architecture du système nous permet de déterminer dans quels cas les alarmes peuvent être corrélés et dans quels cas, les alarmes ne peuvent pas être corrélés.

Ainsi de l'exemple de la figure 5 on en déduit qu'il existe une relation entre

- LRU1 et LRU2, LRU1 et LRU3

Mais il n'existe pas de relation entre

- LRU1 et LRU4, LRU2 et LRU4, LRU2 et LRU3, LRU3 et LRU4.

Les relations structurelles permettent de réaliser un premier tri pour déterminer quels sont les messages de pannes qui ne peuvent pas être corrélés entre eux. En prenant pour exemple la figure 5, si un message de panne est généré par le LRU1 et un message de panne est généré par le LRU4, alors les messages de pannes ne peuvent pas être généré par une même défaillance, puisqu'il n'existe pas de lien entre les deux équipements.

4.2 Corrélation fonctionnelle

Afin d'affiner la connaissance des relations entre les équipements on va s'intéresser à la dépendance fonctionnelle des équipements. Cette information n'est pas toujours bien connue par l'équipementier comme par l'intégrateur. Elle ne pourra donc être exploitée que dans la mesure où on connaît les dépendances fonctionnelles des équipements.

Pour illustrer cette dépendance, on va considérer l'exemple figure 6 :

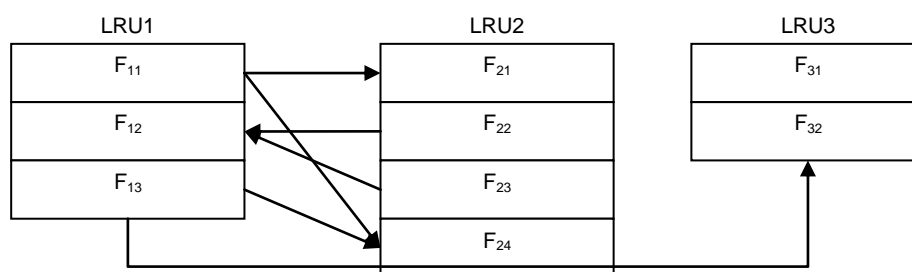


Figure 6. Exemple simplifié de dépendances fonctionnelles entre deux équipements

Soit trois LRU : LRU1 et LRU2, LRU3.

Le LRU1 est constitué de fonctions indépendantes, F11, F12 et F13, le LRU2 est composé de 4 fonctions indépendantes : F21, F22, F23, F24 et le LRU3 est composé des fonctions F31 et F32.

Connaître les dépendances fonctionnelles entre les LRU permet d'établir un tableau de relation entre les deux équipements.

Relation entre	F ₁₁	F ₁₂	F ₁₃	F ₂₁	F ₂₂	F ₂₃	F ₂₄	F ₃₁	F ₃₂
F ₁₁	1	0	0	1	0	0	1	0	0
F ₁₂	0	1	0	0	0	0	0	0	0
F ₁₃	0	0	1	0	0	0	1	0	1
F ₂₁	0	0	0	1	0	0	0	0	0
F ₂₂	0	1	0	0	1	0	0	0	0
F ₂₃	0	1	0	0	0	1	0	0	0
F ₂₄	0	0	0	0	0	0	1	0	0
F ₃₁	0	0	0	0	0	0	0	1	0
F ₃₂	0	0	0	0	0	0	0	0	1

Figure 7. Exemple simplifié de système électronique : tableau de dépendances fonctionnelles

On a pris pour hypothèse que les fonctions à l'intérieur d'un même équipement sont indépendantes les unes des autres. Rajouter une dépendance entre deux fonctions d'un même LRU rend plus complexe le problème de propagation.

Connaître les dépendances entre les fonctions permet de déterminer quels sont les messages de panne potentiellement corrélés, voir figure 6.

Avec l'exemple de la figure 6, si deux messages de pannes sont générés, un par la fonction F22 et l'autre par la fonction F13, ils ne peuvent pas provenir d'une même défaillance.

4.3 Corrélation temporelle

4.3.1 Terminologie

On définit les termes suivants pour la suite de l'étude :

- Temps de latence interne (Tli) : Temps entre l'occurrence d'une défaillance sur un équipement et temps de génération de l'alarme par l'équipement sur lequel la défaillance est apparue.
- Temps de latence externe (Tle) : Temps entre l'occurrence d'une défaillance sur un équipement et le temps de génération d'une alarme sur un autre équipement.
- Temps de détection (td) : Temps de détection d'une défaillance correspondant au parcours de l'arbre de test jusqu'à détection par un test Td.
- Temps d'isolation de la défaillance (ti) : Temps nécessaire une fois la panne détectée pour isoler la panne et générer une alarme.
- Temps de parcours de l'arbre de détection (Tparc) = $\sum td$. Le temps de parcours de l'arbre de test est égal à la somme des temps de tous les tests de détection.
- Temps de propagation d'une défaillance (Tprop)
- Temps entre deux alarmes (ΔT) : Temps entre deux messages de pannes issus de deux équipements différents relatifs à la même panne

4.3.2 Evaluation de la fenêtre temporelle pour le cas a

Pour parvenir à affiner la dépendance entre les messages de pannes on cherche à utiliser l'information temporelle non exploitée du temps d'occurrence des défaillances, et du temps de parcours des arbres de tests avant génération d'alarme.

Lors de l'occurrence d'une défaillance, il existe un certain temps de latence avant qu'un test détecte la défaillance et génère un warning.

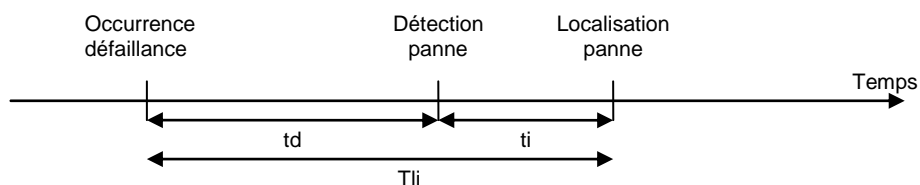


Figure 8. Illustration du phénomène de latence d'émission de l'alarme

Ce temps de latence interne à l'équipement peut varier entre un temps nul, si la défaillance apparaît à l'instant où le test est réalisé et peut être infini s'il n'existe pas de test interne capable de détecter la défaillance.

On détermine que la formule permettant de calculer le temps de latence interne à l'équipement est la formule suivante, voir figure 8 :

$$Tli = td + ti$$

On cherche à borner le temps de latence interne.

Le temps de latence interne maximum est le temps le plus long avant qu'une alarme ne soit générée suite à l'occurrence d'une panne interne à l'équipement. On se place donc dans le cas où le test de détection de la défaillance vient juste d'être effectué quand arrive la panne.

$$Tli_{max} = td_{max} + ti_{max} = T_{parc} + ti_{max}$$

Le temps de latence interne minimum est le temps le plus court avant qu'une alarme ne soit générée suite à l'occurrence d'une panne interne à l'équipement. On se place donc dans le cas où la panne arrive au moment où le test de détection va s'effectuer.

$$Tli_{min} = td_{min} + ti_{min}$$

4.3.3 Evaluation de la fenêtre temporelle pour le cas b

Si un phénomène de propagation de défaillance apparaît, il existe un temps de latence entre le temps d'occurrence et le temps d'émission de « l'alarme de propagation ». Ce temps de latence, est appelé temps de latence externe.

On détermine que la formule permettant de calculer le temps de latence interne à l'équipement est la formule suivante, voir figure 9 :

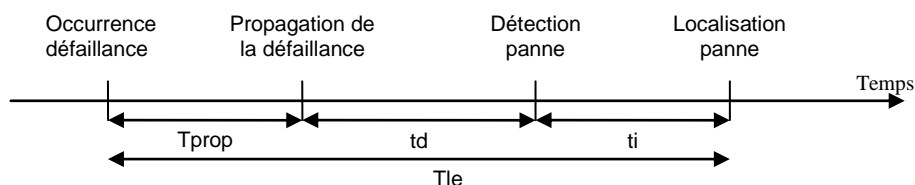


Figure 9. Illustration du phénomène de propagation

Le temps de propagation d'une défaillance peut être déterminé par analyse structurelle et fonctionnelle de l'équipement. Ce temps de propagation est le temps que mettent les effets d'une défaillance pour impacter le fonctionnement des équipements situés en aval de la défaillance.

On cherche à borner le temps de latence externe.

$$T_{le} = T_{prop} + t_d + t_i$$

Le temps de latence externe maximum est le temps le plus long avant qu'une alarme ne soit générée suite à une propagation de panne. On se place donc dans le cas où le phénomène de propagation est le plus long et où le test de détection de la défaillance vient juste d'être effectué quand arrive la panne.

$$T_{le \max} = T_{prop \max} + t_{d \max} + t_{i \max} = T_{prop} + T_{parc} + t_{i \max}$$

Le temps de latence externe minimum est le temps le plus court avant qu'une alarme ne soit générée suite à une propagation de panne. On se place donc dans le cas où le phénomène de propagation est le plus court et où la panne arrive au moment où le test de détection va s'effectuer.

$$T_{le \min} = T_{prop \min} + t_{d \min} + t_{i \min}$$

4.3.4 Evaluation du degré de corrélation entre les défaillances.

Le but est de déterminer quelle est la valeur maximale de ΔT pour parvenir à déterminer si deux alarmes sont corrélées ou décorrélées voir figure 10.

$$\Delta T = \text{Max} (T_{le} - T_{li}; T_{li} - T_{le})$$

Soit si on cherche à trouver l'écart maximal entre deux défaillances on obtient

$$\Delta T_{\max} = \text{Max} (T_{le \max} - T_{li \min}; T_{li \max} - T_{le \min})$$

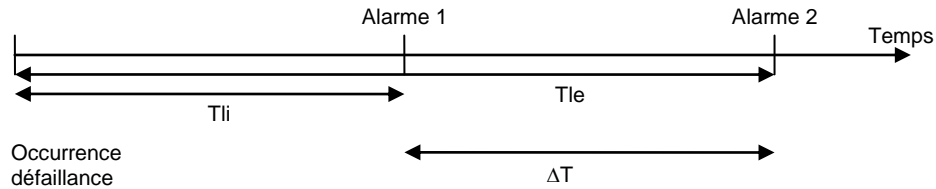


Figure 10. Calcul de l'écart entre de messages de pannes par phénomène de propagation

A partir de la valeur calculée de l'écart maximum entre deux alarmes, on parvient à la conclusion que deux alarmes ayant pour temps d'occurrence un temps supérieur au temps ΔT max calculé ne sont pas corrélées, et identifient deux défaillances différentes.

Si on a un temps entre les deux messages de panne inférieur au temps ΔT max calculé, alors les deux alarmes sont peut être corrélées, et peuvent être les résultantes d'une même défaillance.

4.3.5 Exemple

Considérons 2 arbres de tests de structure identique a celle de la figure 4.

Pour le premier arbre de test, on fixe les temps d'exécution des tests aux valeurs suivantes :

$td1 = 3 \text{ ut}$; $td2 = 4 \text{ ut}$; $td3 = 2 \text{ ut}$; $td4 = 1 \text{ ut}$; $ti1 = 4 \text{ ut}$; $ti2 = 2 \text{ ut}$; $ti3 = 3 \text{ ut}$. (ut: unite de temps)

Pour le second arbre de test on fixe les temps d'exécution des tests aux valeurs suivantes:

$td1' = 6 \text{ ut}$; $td2' = 2 \text{ ut}$; $td3' = 3 \text{ ut}$; $td4' = 4 \text{ ut}$; $ti1' = 2 \text{ ut}$; $ti2' = 4 \text{ ut}$; $ti3' = 1 \text{ ut}$.

On décide pour cet exemple de déterminer qu'une même défaillance D peut se propager de l'équipement testé par l'arbre de test 1 à l'équipement testé par l'arbre de test 2 en un temps de propagation fixe : $T_{prop} = 5 \text{ ut}$.

La défaillance D génère l'alarme W2 sur l'arbre de test 1 et l'alarme W6' sur l'arbre de test 2.

De ces données on déduit les temps de parcours pour chaque arbre ainsi que les temps d'isolation des alarmes voir le tableau figure 11:

Temps	Arbre 1	Arbre 2
T _{parc}	td1+ td2+ td3+ td4= 10 ut	td1'+ td2'+ td3'+ td4'=15 ut
t _i	ti1 = 4 ut	ti2' + ti3' = 5 ut
T _{li max}	T _{parc1} + ti = 14 ut	
T _{li min}	td1 + ti = 7 ut	
T _{le max}		T _{prop} + T _{parc2} + ti = 25 ut
T _{le min}		T _{prop} + td3' + ti = 13 ut

Figure 11. Calcul des temps de latence

On détermine que la fenêtre temporelle maximale de corrélation pour les 2 warning est:

$$\Delta T_{\max} = \text{Max} (T_{le \max} - T_{li \min}; T_{li \max} - T_{le \min}) = \text{Max} (25-7 ; 14-13) = 18$$

A partir de ce calcul si on détermine que le temps d'occurrence de l'alarme W2 est de 54 et le l'alarme W6' est enregistré au temps 61, alors les 2 alarmes appartiennent à la même fenêtre temporelle et peuvent être corrélées entre eux, une seule défaillance peut être la cause de l'apparition des 2 warnings.

Si on le temps d'occurrence de l'alarme W2 est de 34 et celui de l'alarme W6' est de 61, le temps d'occurrence entre les deux alarmes est supérieur à la fenêtre maximale calculée, on en déduit donc que les alarmes ne peuvent pas être corrélées entre elles et qu'il y a une occurrence multiple de défaillances.

5. Conclusion

Les phénomènes de propagation de pannes sont des phénomènes complexes pour un équipement avionique. La propagation des effets des défaillances entraîne des ambiguïtés de localisation entre les alarmes générées par les systèmes avioniques dotés de capacités d'autotest. On a vu qu'il était possible en ayant une connaissance de la structure du système observé de trier les messages de pannes pour ne garder que les messages de pannes ayant une probabilité d'être corrélés entre eux. Cette connaissance du système d'étude peut être complétée en ajoutant l'information temporelle amenée par les arbres de test.

Grâce à cette information, et à l'information relative au temps de propagation, on peut déterminer une fenêtre de corrélation entre deux messages de panne. Les tests générés à l'extérieur de la fenêtre de corrélation ne sont pas résultants d'une seule défaillance, mais de plusieurs défaillances. Les tests générés à l'intérieur de la fenêtre de corrélation temporelle peuvent avoir été générés par une même défaillance.

Plusieurs hypothèses ont été proposées afin de répondre à la problématique de discrimination entre des défaillances simple avec phénomène de propagation et des défaillances complexes.

Les hypothèses 1 à 5 ont été définies afin de retraduire le fonctionnement des tests d'un système avionique, tel qu'il est défini aujourd'hui.

L'hypothèse 6 qui définit que suite à l'occurrence d'une panne un phénomène de propagation des effets peut apparaître traduit la mauvaise ou 0 isolation des fautes.

Les hypothèses 7 et 8, qui définissent les modes de propagation des pannes, traduisent qu'une défaillance donnée pourra ou 0 se propager en fonction de la configuration du système. Par contre la configuration n'évolue pas durant un vol. Hors, sur un hélicoptère, la dépendance fonctionnelle peut évoluer suivant les phases de vol. En effet, certains équipements électroniques ne sont sollicités que pendant certaines phases de vol et ne sont pas sollicités durant le reste du temps. Ce qui se traduit par des phénomènes de propagation changeants au cours du vol. La suppression de l'hypothèse 8 est un cas plus général, dans lequel le phénomène de propagation peut arriver avec un délai qui vient s'ajouter au temps de latence externe. Ce délai correspond au temps de 0-propagation d'une panne induit par la configuration de vol ne permettant pas de propager la panne. Afin d'évaluer ce délais il est nécessaire d'avoir la connaissance de la configuration d'un hélicoptère tout au long du vol.

Pour répondre à cette problématique, on se propose dans un second travail de recourir à la simulation à l'aide d'automates temporisés, en intégrant la connaissance de la configuration du système.

L'autre travail consiste à identifier comment corréliser les messages de pannes entre eux pour fournir l'information de diagnostic. La méthode envisagée pour réaliser cette seconde étape est d'utiliser les arbres de défaillance dynamiques (Manian et al., 1999), en utilisant la notion temporelle, ainsi que les automates temporisés pour réaliser la simulation des résultats des méthodes proposées (Tripakis, 2002).

6. Références

- Blanke M., Kinnaert M., Lunze J. and Staroswiecki M., *Diagnosis and Fault-tolerant Control*, Springer Verlag, 2003.
- Ghelam S., Implémentation d'une fonction de maintenance prédictive appliquée aux systèmes avioniques, Thèse de doctorat, Univ. Joseph Fourier, Grenoble, France, 2006.
- Glade M., « Modélisation des coûts de cycle de vie : prévision des coûts de maintenance et de la fiabilité. Application à l'aéronautique ». Thèse de doctorat, 2005.
- Knotek M., Fault diagnostics based on temporal analysis, Thèse de doctorat, Univ. Joseph Fourier, Grenoble, France, 2006

- J. Lunze, J. Schröder, and P. Supavatanakul. *Diagnosis of discrete event systems: the method and an example*. In Proceedings of the Workshop on Principles of Diagnosis, DX'01, pages 111–118, ViaLattea, Italy, 2001.
- R. Manian, D.W. Coppit, K.J. Sullivan, J.B. Dugan, *Bridging the gap between Fault Tree Analysis Modeling Tools and the Systems being Modeled*, PROCEEDINGS Annual RELIABILITY and MAINTAINABILITY Symposium, 1999.
- Tripakis S., *L'Analyse Formelle de Systèmes Temporisés en Pratique*, Thèse de doctorat Université Joseph Fourier, Grenoble, France, 1998.
- Stavros Tripakis, *Fault diagnosis for timed automata*, In Proc. 7th Int. Symp. Formal Techniques in Real-Time and Fault Tolerant Systems (FTRTFT 02) (Springer, ed.), vol. 2469 of LNCS, 2002, pp. 205–224.
- Yovine S., *Méthodes et outil pour la vérification symbolique des systèmes temporisés*, Thèse de doctorat, VERIMAG Institut National Polytechnique de Grenoble France, 1993.
- Zad S.H., *Fault diagnosis on discrete-event and hybrid systems*, Thèse de doctorat, Univ. Of Toronto, 1999.