(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) **N° de publication :** ***2 976 377***

(à n'utiliser que pour les commandes de reproduction)

(21) **N° d'enregistrement national :** **11 55084**

(51) Int Cl[8] : ***G 06 F 17/18*** *(2012.01), G 06 F 17/50, G 06 N 7/00*

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt :** 10.06.11.

(30) **Priorité :**

(43) **Date de mise à la disposition du public de la demande :** 14.12.12 Bulletin 12/50.

(56) **Liste des documents cités dans le rapport de recherche préliminaire :** *Ce dernier n'a pas été établi à la date de publication de la demande.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *EUROPEAN AERONAUTIC DEFENCE AND SPACE COMPANY EADS FRANCE Société par actions simplifiée* — FR.

(72) **Inventeur(s) :**

(73) **Titulaire(s) :** EUROPEAN AERONAUTIC DEFENCE AND SPACE COMPANY EADS FRANCE Société par actions simplifiée.

(74) **Mandataire(s) :** CABINET SCHMIT CHRETIEN.

(54) PROCEDE D'AMELIORATION DE LA FIABILITE D'UN RESEAU DE CONTROLE COMMENDE MULTIPLEXE.

(57) L'invention concerne un procédé pour l'évaluation de la fiabilité d'une transmission entre deux terminaux i et j interconnectés d'un réseau de contrôle commande multiplexé, lequel réseau comporte plus de deux composants, chaque composant dudit réseau comprenant un état dit de fonctionnement et une pluralité d'états dits de défaillance, lequel procédé comportant les étapes consistant à, séquentiellement :

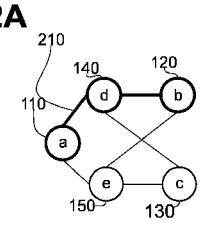
a. déterminer les chemins de longueur minimale entre les terminaux i et j ;

b. rechercher pour chaque chemin déterminé à l'étape a) des combinaisons d'états des composants du réseau telles que la transmission par ledit chemin soit possible ;

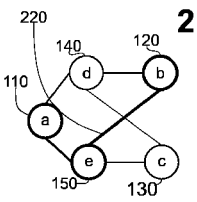
c. déterminer à partir des combinaisons identifiée à l'étape b) un ensemble correspondant aux états admissibles des composants du réseau tels que la transmission par n'importe quel des chemins déterminé à l'étape a) soit possible ;

d. déterminer la probabilité de défaillance de la transmission en fonction de la combinaison des probabilités des états de l'ensemble déterminé à l'étape c).

2A



2B



FR 2 976 377 - A1

L'invention concerne un procédé d'amélioration de la fiabilité d'un réseau de contrôle-commande multiplexé. L'invention est applicable dans tout dispositif de contrôle-commande multiplexé, plus particulièrement mais non exclusivement, dans les domaines du transport et de l'énergie, l'invention visant plus spécifiquement le domaine aéronautique.

Dans ce domaine aéronautique, les dispositifs de contrôle-commande évoluent dans le sens d'une complexité croissante avec l'intervention prépondérante de l'informatique. Parallèlement la demande de fiabilité s'accroît et tout ceci doit être réalisé dans le respect de contraintes de masse assez sévères. Les composants de la chaîne de contrôle-commande deviennent également plus complexes et ladite chaîne intègre des composants logiciels en plus des composants matériels lesquels composants logiciels ajoutent des modes de défaillance supplémentaires. Pour des contraintes de masse, les dispositifs de contrôle-commande basés sur des connexions point à point cèdent la place à des dispositifs mettant en oeuvre des bus multiplexés. Ainsi, la chaîne de contrôle commande d'un aéronef comprend des composants interconnectés, parmi lesquels des émetteurs et / ou récepteurs de données tels que des contrôleurs , capteurs ou actionneurs et des équipement de transmission de données tels que des concentrateurs ou des commutateurs. La conception d'une telle chaîne, et notamment le choix de ses composants nécessitent une analyse de fiabilité. Le calcul de la fiabilité d'une transmission entre deux terminaux d'un réseau est défini selon l'art antérieur comme la probabilité qu'il existe au moins un chemin entre ces deux terminaux ne comportant que des composants non défaillants. Lorsque le réseau ne comprend que des composants matériels, chaque composant ne comprend qu'un seul mode de défaillance: le composant fonctionne ou ne fonctionne pas. Un tel composant est, selon l'art antérieur modélisé par une chaîne de Markov comprenant deux états, associant à chacun de ces états une probabilité d'occurrence. L'analyse de la fiabilité repose sur l'analyse des chaînes de Markov représentatives du comportement des chemins considérés. Cependant, lorsque le réseau comprend à la fois des composants logiciels et des composants matériels, des modèles de défaillance plus élaborés doivent être considérés. Ainsi, pour chaque composant il est nécessaire de considérer :

- des défaillances liées à la transmission d'informations : absence intempestive ou présence intempestive de transmission d'information, ce type de défaillance est couramment désigné par la présence d'un composant bavard ou au contraire d'un composant muet ;
- des défaillances liées à la valeur de l'information transmise, c'est à dire des défaillances liées à l'intégrité des données ;
- des défaillances liées à la date de transmission : transmission tardive ou prématurée de données.

La prise en compte de cette pluralité de modes de défaillance dans l'analyse de la fiabilité du réseau, implique la prise en considération de chaînes de Markov beaucoup plus complexes. De plus, certains modes de défaillance peuvent être propageants, c'est à dire qu'une telle défaillance d'un composant affecte la capacité de transmission de données d'autres composants alors que ceux-ci ne sont pas, eux mêmes, défaillants. C'est par exemple le cas d'un composant dit bavard, qui en transmettant sans interruption des données sur le réseau obère toute transmission de données d'autres composants. L'analyse de la fiabilité d'un réseau de contrôle-commande de ce type par les méthodes connues de l'art antérieur, conduit à une explosion combinatoire et ne peut être réalisée y compris par la mise en oeuvre de moyens de calcul puissants. Ainsi, il est très délicat, voir impossible d'optimiser le choix des composants et l'architecture d'un tel réseau pour en assurer la fiabilité de fonctionnement.

L'invention vise à résoudre les inconvénients de l'art antérieur en proposant un procédé pour l'évaluation de la fiabilité d'une transmission entre deux terminaux *i* et *j* interconnectés d'un réseau de contrôle commande multiplexé, lequel réseau comporte plus de deux composants, chaque composant dudit réseau comprenant un état dit de fonctionnement et une pluralité d'états dits de défaillance, lequel procédé comportant les étapes consistant à, séquentiellement :

a. déterminer les chemins de longueur minimale entre les terminaux *i* et *j* ;

b. rechercher pour chaque chemin déterminé à l'étape a) des combinaisons d'états des composants du réseau telles que la transmission par ledit chemin soit possible ;

c. déterminer à partir des combinaisons identifiées à l'étape b) un ensemble correspondant aux états admissibles des composants du réseau tels que la transmission par n'importe quel des chemins déterminés à l'étape a) soit possible ;

d. déterminer la probabilité de défaillance de la transmission en fonction de la combinaison des probabilité des états de l'ensemble construit à l'étape c).

Ainsi, ce procédé séquentiel qui consiste, par l'analyse de la topologie du réseau, à concentrer l'attention sur les groupes de composants pertinents à chaque étape, permet de réduire de manière considérable le nombre de combinaisons à étudier et évite l'explosion combinatoire du problème. Ainsi, une expression analytique de la fiabilité du réseau en fonction des caractéristiques des composants dudit réseau est obtenue à l'issue de l'étape d), laquelle expression analytique est avantageusement utilisée pour sélectionner les composants les plus critiques en fonction de leurs modes de défaillance les plus critiques également.

L'invention peut être mise en oeuvre selon les modes de réalisation avantageux, exposés ci-après, lesquels peuvent être considérés individuellement ou selon toute combinaison techniquement opérante.

Avantageusement, chaque composant est modélisé par un chaîne de Markov comprenant plus de deux états, lesdits états étant regroupés en 3 sous-ensembles :

- un sous ensemble des états de bon fonctionnement ;
- un sous ensemble des états de défaillance non propageante ;
- un sous ensemble des états de défaillance propageante, tel que la défaillance propageante n'a d'effet sur les composants adjacents du composant considéré.

Ainsi, l'analyse conduite à l'étape b) du procédé objet de l'invention, est simplifiée et rapide. En effet, selon un mode de réalisation particulier de ce procédé, la combinaison d'états obtenue à l'étape b) est déterminée par :

b1 tous les composants du chemin entre *i* et *j* sont dans leur état de fonctionnement, et ;

b2 tous les composants adjacents à un composant se trouvant sur le

chemin entre *i* et *j* sont dans leur état de fonctionnement ou dans un état de défaillance non propageante ;

b3 les combinaisons d'états ainsi déterminées étant stockées pour chaque chemin.

Avantageusement, l'étape c) est réalisée en effectuant l'union des ensembles stockés à l'étape b3).

L'invention est exposée ci-après selon ses modes de réalisation préférés, nullement limitatifs, et en référence aux figures 1 à 3, dans lesquelles :

- la figure 1 représente un exemple schématique de réseau de contrôle-commande comportant cinq composants représentés par des noeuds dudit réseau ;
- les figures 2A et 2B illustrent deux exemples de chemins de longueur minimale entre deux des noeuds du réseau de la figure 1 ;
- la figure 3 est un tableau montrant l'ensemble des états admissibles des composants du réseau de la figure 1 pour que la transmission de données soit possible par les chemins de la figure 2.

Figure 1, selon un exemple illustratif, un réseau (100) de contrôle-commande comprend 5 composants, dont 3 terminaux (110, 120, 130), représentés respectivement par les noeuds *a,b* et *c*, et deux concentrateurs (140, 150) représentés respectivement par les noeuds *d* et *e*. Selon un exemple de réalisation du procédé objet de l'invention, celui-ci porte sur l'analyse de la transmissions des données entre le terminal *a* (110) et terminal *b* (120).

Selon une notation généralisée, le k^{ième} chemin de longueur minimale entre les noeuds *i* et *j* est noté $P_{ij}^{\ k}$.

Figure 2, entre les terminaux a et b, un premier chemin P_{ab}^{1} (210) de longueur minimale passant par le noeud *d* peut être défini ainsi qu'un second chemin P_{ab}^{2} (220) passant par le noeud *e* peuvent être définis.

En désignant par :

- X_i^0 l'ensemble des états de bon fonctionnement du composant i ;:
- X_i^F l'ensemble des états de défaillances non propageantes du

composant i ;

- et par X_i^P l'ensemble des états de défaillances propageantes du noeud *i*.

Les états de bon fonctionnement étant limités à un seul état, soit $card(X_i^0) = 1$.

Figure 3, le tableau donne les combinaisons d'ensemble d'états admissibles pour les deux chemins (210, 220) de longueur minimale déterminés ci-avant, le signe $\cup$ désignant l'union des ensembles d'états.

Ainsi, les composants *a* (110) et *b* (120) doivent être dans leur état de fonctionnement X_a^0 et X_b^0 quelques soit le chemin. A contrario, le composant *c* (130) qui n'est jamais sur un chemin de transmission mais qui est systématiquement adjacent à un composant du chemin, quelque soit le chemin, ne doit pas se trouver dans un état de défaillance qui se propage. Ainsi, si l'ensemble des états tels que la transmission entre les noeuds *i* et *j* est possible par le chemin P_{ij}^k pour un composant l est noté $X_l^{P_{ij}^k}$ alors :

$X_c^{P_{ab}^1} \notin X_c^P$ c'est à dire $X_c^{P_{ab}^1} \in X_c^0 \cup X_c^F$

L'état du réseau à un instant donné est la combinaison des états actifs des composants à cet instant. Une combinaison caractéristiques comporte donc autant de termes que de composants du réseau. L'ensemble $C_{ij}^{P_{ij}^k}$ des combinaisons admissibles pour une transmission selon un chemin P_{ij}^k est donné par :

$$C_{ij}^{P_{ij}^k} = \prod X_l^{P_{ij}^k}$$

L'ensemble des états admissibles pour tous les chemins, noté C_{ij} s'obtient en réalisant l'union des ensembles de combinaisons admissibles pour chaque chemin, soit :

$$C_{ij} = \bigcup C_{ij}^{P_{ij}^k}$$

Ainsi cet ensemble des états admissibles pour tous les chemins entre *a* (110)

et *b* (120) est donné par :

$$C_{ab} = X_a^0 \times X_b^0 \times \left(X_c^0 \cup X_c^F\right) \times \left[\left(X_d^0 \cup X_e^0\right) \times \left(X_d^F \cup X_e^0\right) \times \left(X_d^0 \cup X_e^F\right)\right]$$

Ainsi, cet ensemble ne comprend que 6 combinaisons d'états parmi les 3^5 soit 243 états que contient la chaîne de Markov décrivant le comportement de ce réseau. Ainsi, la réalisation des étapes a) à c) du procédé selon l'invention permet de réduire considérablement la dimension du modèle.

L'étape d) du procédé objet de l'invention est réalisée en effectuant la somme des probabilités de chacune des combinaisons d'états admissibles. En notant $\pi_i^{X_i^0}$ la probabilité de l'ensemble de l'état de fonctionnement X_i^0 du composant i et π_{ij} la fiabilité de la transmission entre les noeuds *i* et *j*, alors la fiabilité de la transmission entre les noeuds *a* (110) et *b* (120) du réseau (100) s'écrit :

$$\pi_{ab} = \pi_a^{X_a^0} \cdot \pi_b^{X_b^0} \cdot \left(\pi_c^{X_c^0} + \pi_c^{X_c^F}\right) \cdot \left[\left(\pi_d^{X_d^0} \cdot \pi_e^{X_e^0}\right) + \left(\pi_d^{X_d^F} \cdot \pi_e^{X_e^0}\right) + \left(\pi_d^{X_d^0} \cdot \pi_e^{X_e^F}\right)\right]$$

Connaissant, par l'intermédiaire des données constructeur, ou à partir d'essai les valeurs des probabilités de défaillances correspondantes de chacun des composant il est alors facile de simuler l'influence des divers composants sur la fiabilité de transmission et ainsi d'optimiser la construction du réseau de contrôle-commande.

REVENDICATIONS

1. Procédé pour l'évaluation de la fiabilité d'une transmission entre deux terminaux *i* et *j* interconnectés d'un réseau de contrôle commande multiplexé, lequel réseau comporte plus de deux composants, chaque composant dudit réseau comprenant un état dit de fonctionnement et une pluralité d'états dits de défaillance, caractérisé en ce que ledit procédé comprend des étapes consistant à, séquentiellement :

a. déterminer les chemins de longueur minimale entre les terminaux *i* et *j* ;

b. rechercher pour chaque chemin déterminé à l'étape a) des combinaisons d'états des composants du réseau telles que la transmission par ledit chemin soit possible ;

c. déterminer à partir des combinaisons identifiées à l'étape b) un ensemble correspondant aux états admissibles des composants du réseau tels que la transmission par n'importe quel des chemins déterminé à l'étape a) soit possible ;

d. déterminer la probabilité de défaillance de la transmission en fonction de la combinaison des probabilités des états de l'ensemble déterminé à l'étape c).

2. Procédé selon la revendication 1, caractérisé en ce que chaque composant est modélisé par un chaîne de Markov comprenant plus de deux états, lesdits états étant regroupés en 3 sous-ensembles :

- un sous ensemble des états de bon fonctionnement ;
- un sous ensemble des états de défaillance non propageante ;
- un sous ensemble des états de défaillance propageante, tel que la défaillance propageante n'a d'effet que sur les composants adjacents du composant considéré.

3. Procédé selon la revendication 2, caractérisé en ce que la combinaison d'états obtenue à l'étape b) est déterminée par :

b1 tous les composants du chemin entre *i* et *j* sont dans leur état de

fonctionnement, et ;

b2 tous les composants adjacents à un composant se trouvant sur le chemin entre *i* et *j* sont dans leur état de fonctionnement ou dans un état de défaillance non propageante ;

b3 les combinaisons d'états ainsi déterminées étant stockées pour chaque chemin.

4. Procédé selon la revendication 3, caractérisé en ce que l'étape c) est réalisée en effectuant l'union des ensembles stockés à l'étape b3)

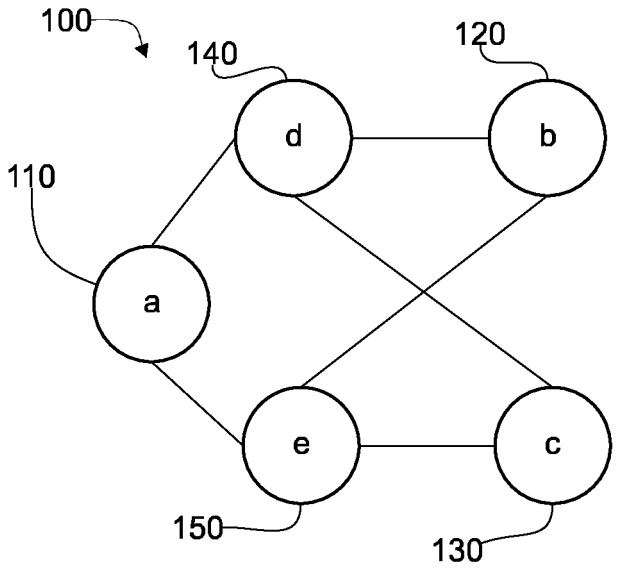


Fig. 1

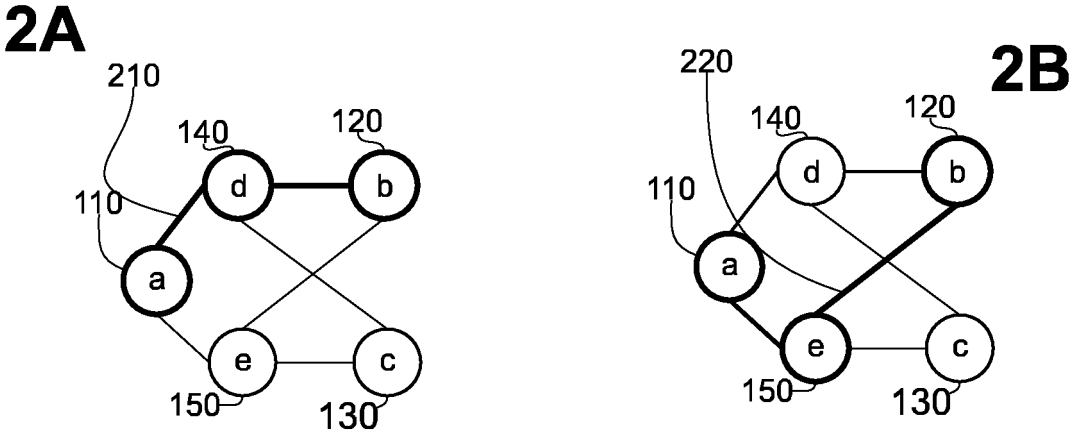


Fig. 2

	P^1_{ab}	P^2_{ab}
a	X^0_a	X^0_a
b	X^0_b	X^0_b
c	$X^0_c \cup X^F_c$	$X^0_c \cup X^F_c$
d	X^0_d	$X^0_d \cup X^F_d$
e	$X^0_e \cup X^F_e$	X^0_e

Fig. 3