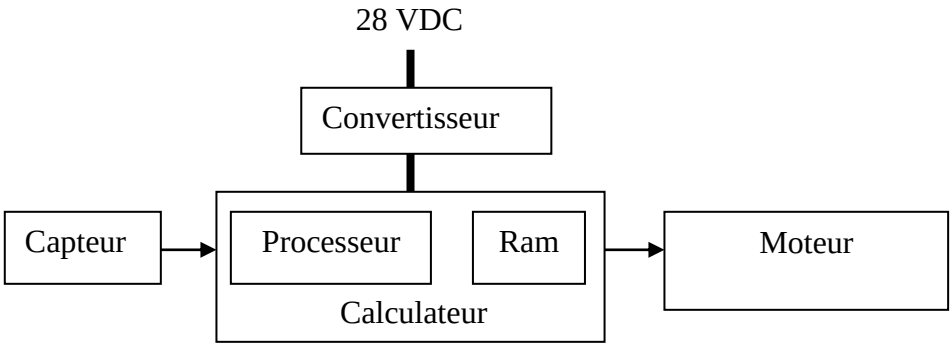
TP SdF N° 3

Analyse de risques et évaluation de fiabilité d'un système mécatronique

A – Analyse de riques

Un calculateur commande un moteur à partir d'une information fournie par un capteur de position. Il comprend un processeur et une mémoire vive (RAM) et est alimenté via un convertisseur de tension à partir d'une barre d'alimentation 28 VDC.



Pour répondre à une exigence de fiabilité, les différents constituants de ce système doivent être redondés, à l'exception de la partie mécanique du moteur.
A partir d'une décomposition fonctionnelle du système, faire une analyse de risques afin d'identifier les événements redoutés et proposer des actions pour les maîtriser.

Arborescence	Evénements redoutés	Effets au niveau système	Actions en diminution de risques	Remarques
1. Convertisseur				
	Perte CV	Perte système	Redondance	
	Court-circuit en entrée	Perte de la barre générale d'alimentation 28 VDC	Disjoncteur ou fusible	
	Surtension en sortie	Destruction des équipements en aval dont éventuellement le moteur	Protection matérielle (inhibition du CV sur détection de surtension)	Ségrégation entre la fonction CV et la protection pour éviter les risques de propagation de panne
2. Calculateur	Perte calculateur	Perte système	Redondance (1)	
2.1. Processeur	Déroutement de programme	Perte système	Détection par chien de garde entainant un réinitialisation du calculateur (Reset) puis une reconfiguration sur la redondance si la panne subsiste (2)	
	Erreur de données (registre)	Perte système	Surveillance logicielle (3)	

2.2. Mémoire	Panne d'un bit	Perte système	Détection par circuit correcteur détecteur d'erreur (EDAC) (4)	Test et correction des pannes fugitives latentes en tâche de fond (scrubbing)
2.3. horloge	Dérive d'horloge	Perte système	Horloge du chien de garde différente de celle du processeur (5)	
3. Capteur	Erreur de mesure	Perte système	Redondance triple + vote (6)	Ségrégation entre les acquisitions pour éviter une propagation de panne entre voies
4. Moteur				
4.1. Mécanique	Panne mécanique	Perte système	Essai de qualification par rapport à la mission	
4.2. Enroulement	Panne enroulement	Perte système	Redondance (surveillance de la réponse du moteur par rapport à sa commande)	Une panne du moteur ou de sa commande ne doit pas conduire à un court-circuit de l'enroulement de la voie défectueuse qui conduirait à la génération d'un couple magnétique perturbateur

(1) Redondance calculateur
Dans les architectures classiques, l'unité de traitement est en redondance passive froide et est munie de moyens de détection de panne matériels (chien de garde) et logiciels, plus ou moins élaborés dont l'efficacité peut atteindre 99 % environ. Seules des contraintes très sévères de sécurité ou de temps de réponse (une navette en phase de rentrée par exemple) peuvent justifier une architecture à vote majoritaire (6) moins fiable, plus lourde et plus consommatrice en énergie. La nécessité de sauvegarder le contexte en cas de reconfiguration (notamment pour rendre celle-ci plus rapide) peut conduire à l'utilisation de mémoires partagées ou à l'observation du contexte par l'unité de traitement en redondance, mise alors à l'état ON.

(2) Chien de garde
Les déroutements de programme permanents ou fugitifs peuvent être détectés par un mécanisme de type chien de garde (watch dog). Celui-ci est constitué d'un compteur réinitialisé périodiquement durant chaque cycle de traitement du logiciel. En l'absence de remise à zéro, une alarme est déclenchée dès que le compteur dépasse une certaine valeur correspondant à une durée supérieure à la période de traitement. L'efficacité du chien de garde peut-être améliorée par divers autotests réalisés par logiciel en tâche de fond durant les durées des cycles de traitement non employées par des tâches opérationnelles. Cette alarme peut réinitialiser le processeur (Reset) afin de pallier une panne fugitive, puis commander la reconfiguration sur un processeur en redondance si la panne subsiste.

(3) Altération de données sans déroutement de programme
Les paramètres critiques peuvent faire l'objet de test de vraisemblance ou être dupliqués.

(4) EDAC :
L'impact des altérations de bits en mémoire peut être limité par l'utilisation de système de détection

et de correction d'erreur (EDAC) associé à une procédure de limitation des pannes latentes (Scrubbing) pour les pannes fugitives. Le système de détection et de correction d'erreur consiste à ajouter un code à chaque mot lors de l'écriture en mémoire et de tester la cohérence entre le mot et le code à la lecture. Les EDAC classiquement utilisés (ajout de 4 bits de code par mot de 16 bits) ont la possibilité de détecter et corriger une erreur de bit de manière transparente et de détecter 2 erreurs. Le scrubbing consiste à lire la mémoire en tâche de fond afin de limiter le risque d'erreurs multiples dans un même mot.

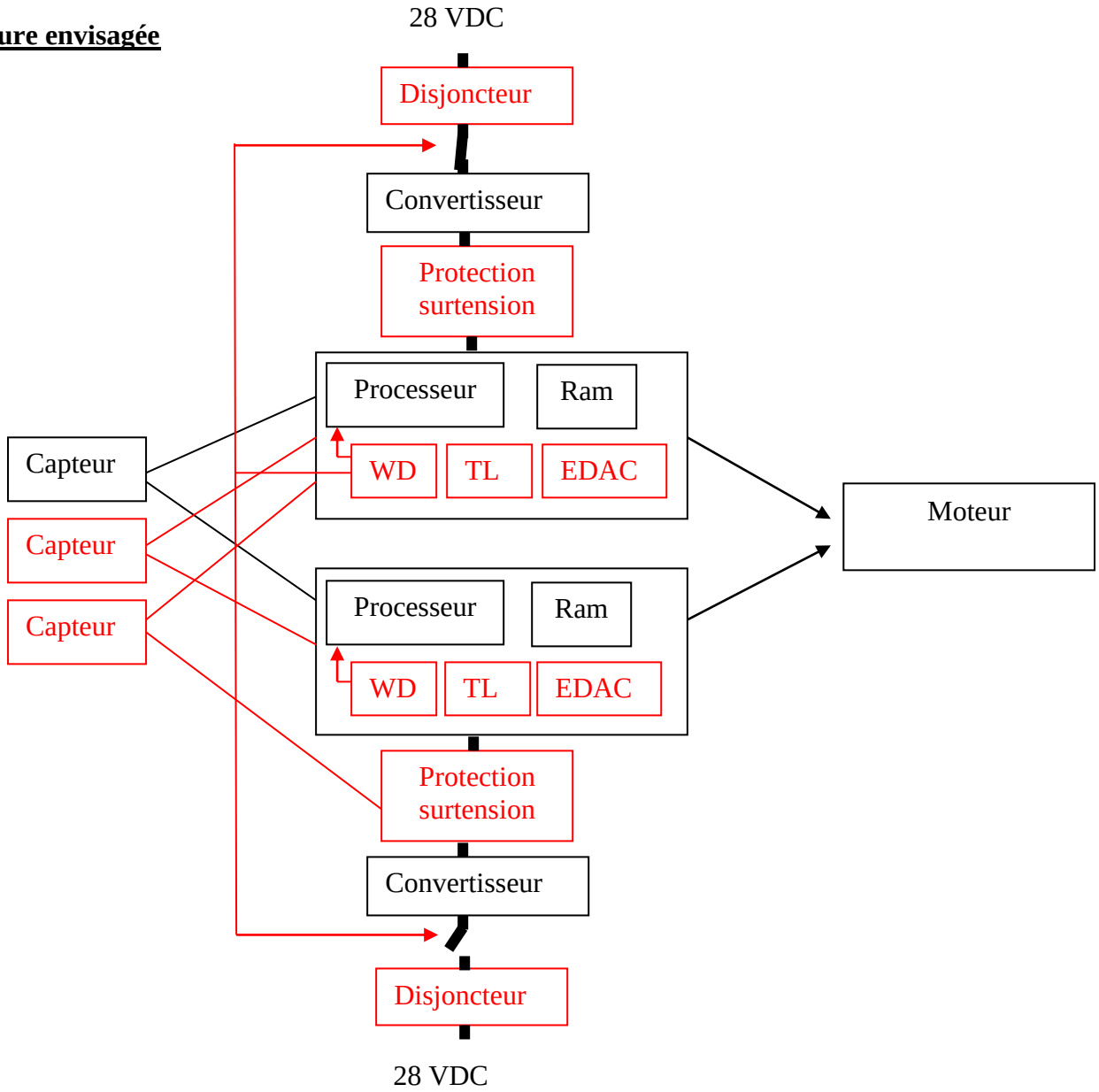
(5) Dérives d'horloge

L'horloge du chien de garde doit être différente de celle du processeur afin de pouvoir détecter une dérive éventuelle de cette dernière.

(6) Vote

Le vote consiste à choisir la médiane parmi trois valeurs. Il permet ainsi de s'affranchir de la localisation de la panne.

Architecture envisagée



B – Evaluation de fiabilité

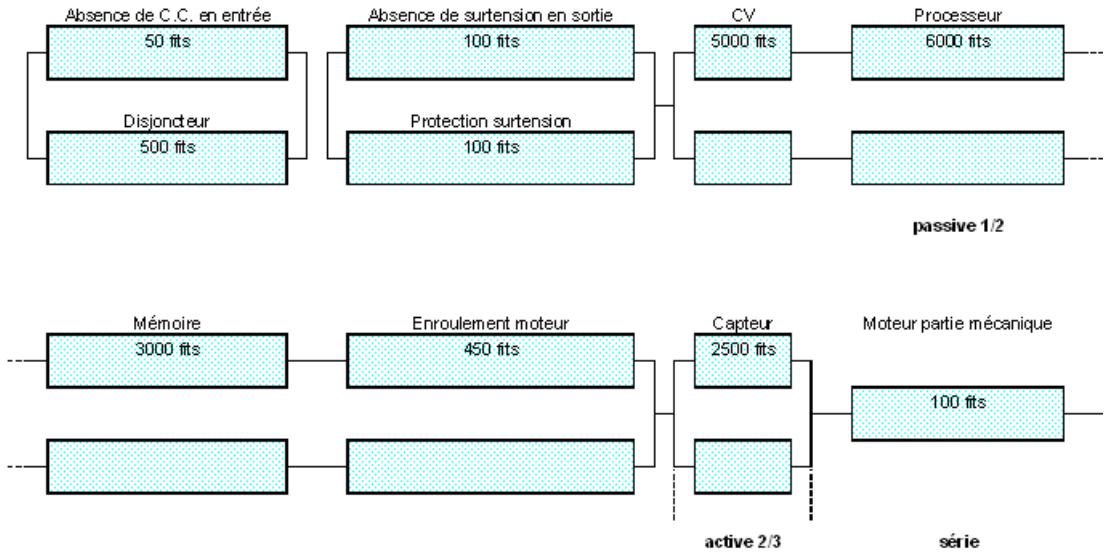
On se propose d'évaluer la fiabilité du système à partir des éléments suivants :

Elément	Mode de défaillance	Taux de défaillance (fit = $hr^{-1} *10^9$)	MTTR (hr)
1. Convertisseur	Perte CV	5000	200
	Court-circuit en entrée	50	Sans *
	Surtension en sortie	100	Sans *
	Protection surtension	100	Sans *
	Perte disjoncteur en amont	500	Sans *
2. Calculateur			
2.1. Processeur	Perte processeur	6000	200
2.2. Mémoire *(100 Kmots de 16 bits + 4 bits de code)*	Perte mémoire	3000	200
	Panne fugitive d'un bit	1bit/semaine	
2.3. Chien de garde	Panne latente du chien de garde	500	Sans *
	Efficacité du chien de garde	90% des pannes du processeur	
3. Capteur	Perte ou erreur de mesure	2500	
4. Moteur			
4.1. Mécanique	Panne mécanique	100	
4.2. Enroulement	Panne enroulement	450	200

*Sans * : panne non détectée ou non réparée (à titre de simplification)*

1- Etablir le Bloc diagramme fiabilité du système sans considérer le chien de garde et les pannes fugitives de la mémoire.
2 - Evaluer la fiabilité du système de 0 à 10 ans.
3 - Etablir un modèle markovien du calculateur en considérant l'efficacité et la panne du chien de garde (λ WD)
4 - Evaluer une période de scrubbing de manière à ne pas dégrader la fiabilité (0,99 à 10 ans)

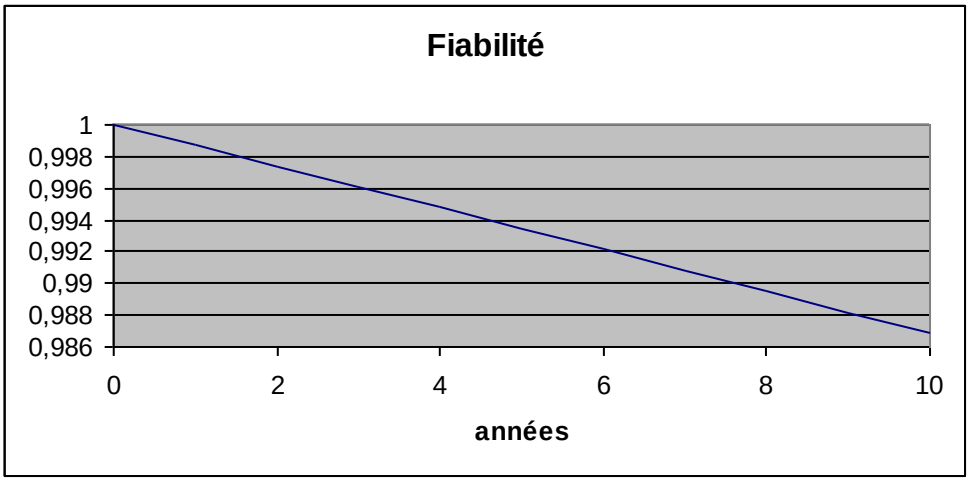
BDF



Remarque : Les modes de défaillance relatifs à la perte de 28VDC, la surtension et la perte de redondance doivent être séparés dans le BDF. Les deux premiers modes ne sont considérés que pour la seule voie active car la voie en redondance est déconnectée par un relais.

Fiabilité

ELEMENTS	Taux de panne ON (fit)	Nb	Type de redondance	Taux de panne OFF(fit)	Taux d' utilisation r (%)	MTTR (heure)
Absence de C.C. en entrée (a)	50					
Disjoncteur (b)	500					
			a+b			
Absence de surtension en sortie (a)	100					
Protection surtension (b)	100					
			a+b			
CV	5000					
Processeur	6000					
Mémoire	3000					
Enroulement moteur	450					
	14450		passive 1/2	1445		200
Capteur	2500		active 2/3			200
Moteur partie mécanique	100		série			
$			Système			



Pour évaluer la fiabilité opérationnelle du système, on utilise les formules de redondance réparable active ou passive avec le dernier état absorbant (voir l'exemple de fonction personnalisée de l'aide en ligne de l'outil SUPERCAB).

Chien de garde

Le chien de garde est utilisé pour la reconfiguration de l'ensemble constitué du CV, du processeur, de la mémoire et de l'enroulement du moteur. En cas de panne latente du chien de garde, le processeur ne peut plus commuter sur la voie redondante, quelque soit la panne détectée notamment par logiciel (le capteur, qui est fiabilisé par un vote, permet de tester la réponse du moteur à sa commande).

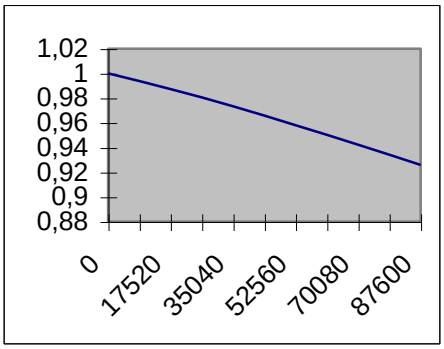
MAT :	1	2	3	4
OK : 1	-	λ WD	λ CV + 90 % λ Processeur + λ Mémoire + λ enroulement + 10% (λ CV + λ Processeur + λ Mémoire + λ enroulement)	10 % λ Processeur
Perte chien de garde : 2		-		λ CV + λ Processeur + λ Mémoire + λ enroulement
Perte une voie : 3	1/MTTR		-	λ CV + λ Processeur + λ Mémoire + λ enroulement
Perte système : 4				-
INIT :	1	0	0	0
ETATS :	1	1	1	0

Un taux $\lambda_{OFF} = \lambda_{ON} / 10$ a été choisi pour la voie redondante et les modes indépendants de défaillance relatifs à la perte de 28VDC, à la surtension et à la partie mécanique du moteur n'ont pas été considérés ici.

MAT :	1	2	3	4
OK : 1	-	0,0000005	0,000015295	0,0000006
Perte chien de garde : 2		-		0,00001445
Perte une voie : 3	0,005		-	0,0000239
Perte système : 4				-
INIT :	1	0	0	0
ETATS :	1	1	1	0

Probabilité : 0,92595507
à t (hr) : 87600

T (hr)	PR
0	1
8760	0,9939041
17520	0,98737127
26280	0,98047757
35040	0,97327747
43800	0,9658189
52560	0,95814393
61320	0,95028955
70080	0,9422882
78840	0,93416838
87600	0,92595507



EDAC

Mémoire 100 de KMots de 16 bits + 4 bits de code
Panne fugitive d'un bit en mémoire par semaine
La probabilité de panne d'un mot en mémoire et de la mémoire complète ($P = p^{100000}$) peut être évaluée par le modèle suivant :

MAT :	1	2	3
OK : 1	-	20/(7*24*100000*20)	
Panne d'un bit : 2	1/Tscrubbing	-	19/(7*24*100000*20)
Perte du mot : 3			-

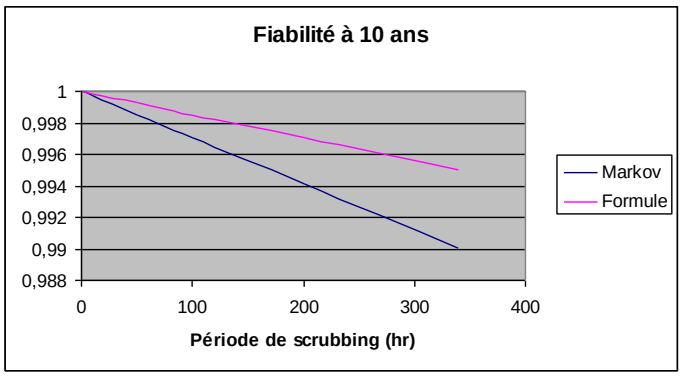
MAT :	1	2	3
OK : 1	-	5,95238E-08	
Panne d'un bit : 2	0,002941176	-	5,65476E-08
Perte du mot : 3			-

INIT :	1	0	0

ETATS :	1	1	0

	Mot	Mémoire	$T_{scrubbing}$ (hr)
Probabilité :	0,9999999001	0,9901	340
à t (hr) :	87600		

Une période de scrubbing inférieure à 340 heures permet d'atteindre une fiabilité de 0,99 à 10 ans relative aux pannes fugitives en mémoire.
Couramment utilisée, la formule suivante donne une valeur approchée du MTTF lié à ce type de panne :
$MTTF \approx 2/B(B-1)\lambda^2TW = 17476161$ heures soit $P = \exp(-10*365*24/MTTF) = 0,995$
Avec B : Nombre de bits dans un mot
λ : Probabilité d'erreur par bit et par heure
T : Période de scrubbing en heure
W : Nombre de mots en mémoire
Pour de longues périodes de scrubbing, les résultats obtenus avec cette formule sont optimistes par rapport à ceux obtenus par traitement markovien.



.