TP N° 40

Evaluation des architectures proposées dans la norme EN 61508

La norme EN 61508 présente, dans sa partie 6, différentes architectures de systèmes de sécurité pour lesquelles elle propose diverses formules pour calculer la probabilité moyenne de défaillance sur demande (PFD) ou la probabilité de défaillance par heure (PFH).

Ce TP a pour objet d'évaluer ces différentes architectures par modélisation markovienne en précisant leurs caractéristiques et les hypothèses opératoires considérées.

Les résultats obtenus sont comparés aux résultats des formules proposées par la norme.

Evaluer les exemples d'architectures présentés dans la norme EN 61508 et comparer les résultats obtenus avec ceux des formules proposées.

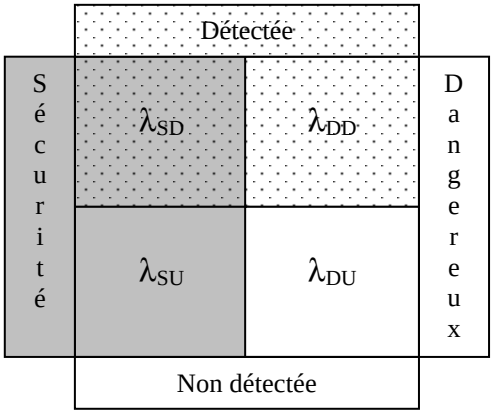
Evaluation des exemples d'architectures de systèmes de sécurité de la norme EN 61508

Les systèmes de sécurité sont des entités de surveillance et de protection d'installations diverses considérés indépendants des systèmes protégés.

Ils comprennent des capteurs, des organes de traitement et des actuateurs, qui sont chacun caractérisés par un taux de défaillance λ.

Ce dernier peut se décomposer de la manière suivante :

$$\lambda = \lambda_D + \lambda_S \qquad \lambda_D = \lambda_{DD} + \lambda_{DU} \qquad \lambda_S = \lambda_{SD} + \lambda_{SU}$$



avec :

- λ_D : taux de défaillance dangereuse rendant le système de sécurité inopérant
- λ_{DD} : taux de défaillance dangereuse détectée par un test de diagnostic (supposé permanent)
- λ_{DU} : taux de défaillance dangereuse non détectée par le test de diagnostic
- λ_S : taux de défaillance en sécurité conduisant à un état de sécurité
- λ_{SD} : taux de défaillance en sécurité détectée par un test de diagnostic
- λ_{SU} : taux de défaillance en sécurité non détectée par le test de diagnostic

Outre les tests de diagnostic, une maintenance supposée parfaite de période T_1 couvre la totalité du produit considéré.

La norme fait l'hypothèse (discutable) d'une répartition équilibrée entre les pannes dangereuses et les pannes en sécurité avec un même taux de couverture DC du test de diagnostic pour chaque type de défaillance.

$$\lambda_D = \lambda_S = \lambda/2 \qquad \lambda_{DD} = \lambda_{SD} = \lambda/2 * DC$$

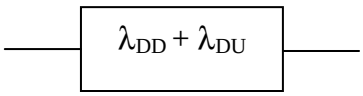
Les évaluations de ce TP sont réalisées par des traitements markoviens. Ceux-ci font l'hypothèse de transitions à taux constants (caractérisées par des lois exponentielles). La méthode des états fictifs (combinaison de lois exponentielles) pourrait cependant être employée pour modéliser d'autres types de transition (loi d'Erlang, etc.).

Les traitements markoviens sont réalisés en régime asymptotique en modélisant la maintenance de période T_1 par des transitions aléatoires de taux $1/(T_1/2 + MTTR)$. En effet, la durée moyenne de non détection d'une panne non détectée par un test de diagnostic est $T_1/2$ et le MTTR correspond à la durée moyenne séparant l'occurrence d'une panne détectée et le rétablissement du service.

Ces traitements sont également réalisés en régime transitoire en modélisant cette même maintenance par un forçage périodique de l'état courant à l'état initial (sans panne).

Considérée parfaite, cette maintenance pourrait être partielle et modélisée comme telle.

1 - Mono chaîne 1001



L'architecture 1001 peut se modéliser par la matrice de Markov suivante :

MAT 1001 :	1	2	3
OK : 1	-	λ_{DD}	λ_{DU}
Panne détectée : 2	1/MTTR	-	
Panne non détectée : 3	$1/(T_1/2+MTTR)$	λ_{DD}	-

- Le système de sécurité n'est disponible que dans l'état 1.
- En cas de panne détectée, la maintenance effectuée recouvre la totalité des pannes dangereuses, détectées (λ_{DD}) ou non détectées (λ_{DU}).
- Les pannes conduisant à un état de sécurité (λ_S) ne sont pas considérées ici car elles n'ont aucun effet sur les pannes dangereuses.

Pour un jeu de valeurs numériques, la probabilité de panne sur demande (PFD), corespondant à l'indisponibilité du système de sécurité, et la probabilité de défaillance par heure (PFH), corespondant à 1/MTTF, sont calculées ci-après par le modèle markovien en régime asymptotique ainsi que par les formules proposées dans la norme.

λ_{DU} :	0,00001	hr-1
λ_{DD} :	0,0001	hr-1
T_1 :	8760	hr
MTTR :	24	hr

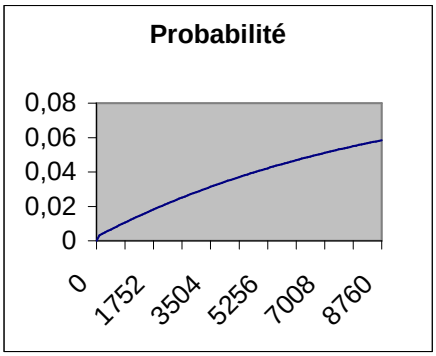
MAT :	1	2	3
OK : 1	-	0,0001	0,00001
Panne détectée : 2	0,041666667	-	
Panne non détectée : 3	0,000227066	0,0001	-
INIT :	1	0	0
ETATS :	1	0	0

	PFD	PFH
Markov :	**0,031990975**	**0,00011**
Formules :	**0,04644**	**0,00011**

L'indisponibilité est également calculée en régime transitoire avec le même modèle markovien auquel a été supprimée la transition relative à la maintenance périodique.

MAT :	1	2	3
OK : 1	-	0,0001	0,00001
Panne détectée : 2	0,041666667	-	
Panne non détectée : 3		0,0001	-
INIT :	1	0	0
ETATS :	0	1	1

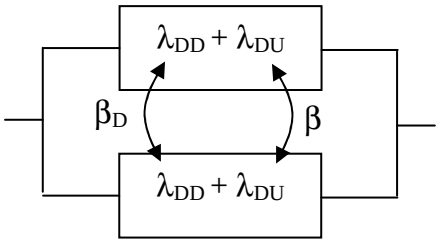
Indisponibilité : 0,05848559
à t : 8760 (hr)
Indisponibilité moyenne entre 0 et t : 0,03480739



La feuille de calcul Excel est disponible par un double clic sur l'icône suivant :


1001

2 – Double chaînes 1002



L'architecture 1002 correspond à la mise en parallèle de deux chaînes de type 1001 (capable chacune de conduire à un état de sécurité) en considérant un taux β_D de défaillance de cause commune des pannes détectées par un test de diagnostic et un taux β de défaillance de cause commune des pannes non détectées.

Chaque chaîne ayant 3 états, l'architecture a $9 = 3^2$ états possibles dont certains peuvent se regrouper en exploitant la symétrie. Elle peut ainsi se modéliser par la matrice de Markov suivante à 6 états :

MAT 1002 :	**1**	**2**	**3**	**4**	**5**	**6**
OK : **1**	-	$2*\lambda_{DD}*(1-\beta_D)$	$2*\lambda_{DU}*(1-\beta)$	$2*\lambda_{DD}*\beta_D$		$2*\lambda_{DU}*\beta$
1 panne détectée : **2**	1/MTTR	-		λ_{DD}	λ_{DU}	
1 panne non détectée : **3**	$1/(T_1/2+MTTR)$	$\lambda_{DD}*(1-\beta_D)$	-	$2*\lambda_{DD}*\beta_D$	$\lambda_{DD}*(1-\beta_D)$	λ_{DU}
2 pannes détectées : **4**		1/MTTR		-		
1 panne détectée + 1 non détectée : **5**	$1/(T_1/2+MTTR)$		1/MTTR	λ_{DD}	-	
2 pannes non détectées : **6**	$1/(T_1/2+MTTR)$			$2*\lambda_{DD}*\beta_D$	$2*\lambda_{DD}*(1-\beta_D)$	-

- Le système de sécurité est disponible dans les états 1, 2 et 3.
- Les taux de défaillance de cause commune β_D et β ne s'applique que sur les éléments dont la panne est détectée (λ_{DD}) ou non détectée (λ_{DU}) par le test de diagnostic.
- Un seul réparateur est considéré pour les 2 chaînes (le taux de transition de 4 vers 2 serait 2/MTTR dans le cas contraire).
- La maintenance de période T1 est réalisée simultanément sur les deux chaînes et est considérée parfaite.

Pour un jeu de valeurs numériques, la PFD et la PFH sont calculées en asymptotique ci-après :

MAT :	**1**	**2**	**3**	**4**	**5**	**6**
OK : 1	-	0,000198	0,0000196	0,000002		0,0000004
1 panne détectée : 2	0,0416667	-		0,0001	0,00001	
1 panne non détectée : 3	0,0002271	0,000099	-	0,000002	0,000099	0,00001
2 pannes détectées : 4		0,0416667		-		
1 panne détectée + 1 panne non détectée : 5	0,0002271		0,0416667	0,0001	-	
2 pannes non détectées : 6	0,0002271			0,000002	0,000198	-

λ_{DU} :	0,00001	hr-1
λ_{DD} :	0,0001	hr-1
T_1 :	8760	hr
MTTR :	24	hr
β_D :	1%	
β :	2%	

INIT :	1	0	0	0	0	0
ETATS :	1	1	1	0	0	0

	PFD	**PFH**
Markov :	**0,0023821**	**7,536E-06**
Formules :	**0,0037979**	**1,12E-05**

T_{CE} : 422,18182 **T_{GE} : 289,45455**

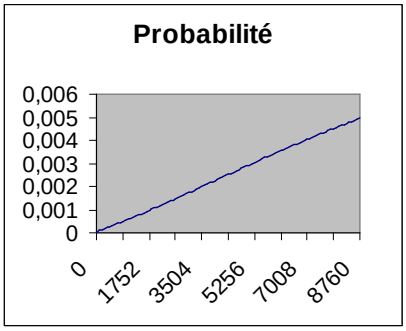
L'indisponibilité est également calculée en régime transitoire avec le même modèle markovien auquel a été supprimé les transitions relatives à la maintenance périodique.

MAT :	1	2	3	4	5	6
OK : 1	-	0,000198	0,0000196	0,000002		0,0000004
1 panne détectée : 2	0,0416667	-		0,0001	0,00001	
1 panne non détectée : 3		0,000099	-	0,000002	0,000099	0,00001
2 pannes détectées : 4		0,0416667		-		
1 panne détectée + 1 panne non détectée : 5			0,0416667	0,0001	-	
2 pannes non détectées : 6				0,000002	0,000198	-

INIT :	1	0	0	0	0	0

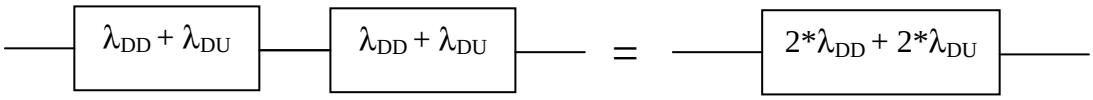
ETATS :	0	0	0	1	1	1

Indisponibilité : 0,0049483
à t : 8760 (hr)
Indisponibilité moyenne entre 0 et t : 0,0025063



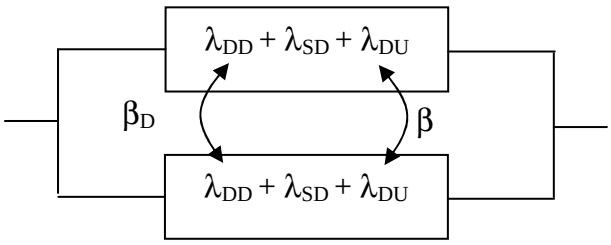

1002

3 – Mono chaîne 2002



Cette architecture correspond à la mise en série de 2 chaînes de type 1001 puisque la mise en sécurité n'est activée que sur demande simultanée des 2 blocs de sécurité.

4 – Double chaînes 1002D



Cette architecture à deux chaînes a un fonctionnement qui diffère de la 1002.

En cas de panne détectée sur l'une des deux chaînes ($\lambda_{DD} + \lambda_{SD}$) la maintenance est effectuée sur l'ensemble de celle-ci et la surveillance est assurée par la seconde.

En cas de panne détectée sur les deux chaînes, la sortie est mise en sécurité.

Le modèle markovien est alors le suivant dans lequel les états de sécurité sont 1, 2, 3 et 4.

MAT 2002D :	1	2	3	4	5	6
OK : 1	-	$2*\lambda_{SD}+2*\lambda_{DD}*(1-\beta_D)$	$2*\lambda_{DU}*(1-\beta)$	$2*\lambda_{DD}*\beta_D$		$2*\lambda_{DU}*\beta$
1 panne détectée : 2	1/MTTR	-		$\lambda_{SD}+\lambda_{DD}$	λ_{DU}	
1 panne non détectée : 3	$1/(T_1/2+MTTR)$	$\lambda_{SD}+\lambda_{DD}*(1-\beta_D)$	-	$2*\lambda_{DD}*\beta_D$	$\lambda_{SD}+\lambda_{DD}*(1-\beta_D)$	λ_{DU}
2 pannes détectées : 4		1/MTTR		-		
1 panne détectée + 1 non détectée : 5	$1/(T_1/2+MTTR)$		1/MTTR	$\lambda_{SD}+\lambda_{DD}$	-	
2 pannes non détectées : 6	$1/(T_1/2+MTTR)$			$2*\lambda_{DD}*\beta_D$	$2*\lambda_{SD}+2*\lambda_{DD}*(1-\beta_D)$	-

La PFD et la PFH sont calculées en asymptotique ci-après :

MAT :	1	2	3	4	5	6
OK : 1	-	0,000398	0,0000196	0,000002		0,0000004
1 panne détectée : 2	0,0416667	-		0,0002	0,00001	
1 panne non détectée : 3	0,0002271	0,000199	-	0,000002	0,000199	0,00001
2 pannes détectées : 4		0,0416667		-		
1 panne détectée + 1 panne non détectée : 5	0,0002271		0,0416667	0,0002	-	
2 pannes non détectées : 6	0,0002271			0,000002	0,000398	-

λ_{SD} :	0,0001	hr-1
λ_{DU} :	0,00001	hr-1
λ_{DD} :	0,0001	hr-1
T_1 :	8760	hr
MTTR :	24	hr
β_D :	1%	
β :	2%	

	1	2	3	4	5	6
INIT :	1	0	0	0	0	0
ETATS :	1	1	1	1	0	0

	PFD	PFH
Markov :	0,0015167	6,657E-06
Formules :	0,00106	2,152E-06

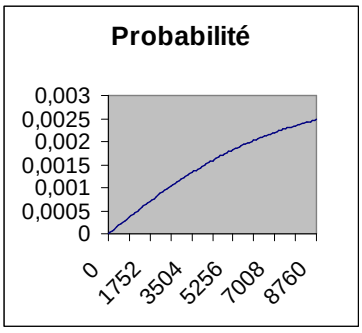
T_{CE}' : 232,57143 T_{GE}' : 163,04762

Et en régime transitoire :

MAT :	1	2	3	4	5	6
OK : 1	-	0,000398	0,0000196	0,000002		0,0000004
1 panne détectée : 2	0,0416667	-		0,0002	0,00001	
1 panne non détectée : 3		0,000199	-	0,000002	0,000199	0,00001
2 pannes détectées : 4		0,0416667		-		
1 panne détectée + 1 panne non détectée : 5			0,0416667	0,0002	-	
2 pannes non détectées : 6				0,000002	0,000398	-

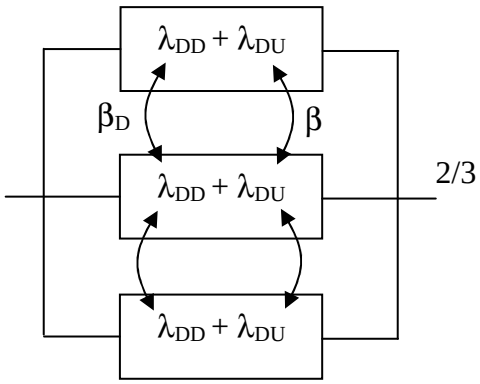
	1	2	3	4	5	6
INIT :	1	0	0	0	0	0
ETATS :	0	0	0	0	0	1

Indisponibilité : 0,0024714
à t : 8760 (hr)
Indisponibilité moyenne entre 0 et t : 0,0014607




1002D

5 – Triple chaînes à vote 2003



L'architecture 2003 correspond à la mise en parallèle de 3 chaînes de type 1001 avec un vote majoritaire permettant de passiver la panne de l'une d'elle.

Les $27 = 3^3$ états possibles de cette architecture peuvent se regrouper en 10 états suivants :

1 : OK
2 : 1 panne détectée
3 : 1 panne non détectée
4 : 2 pannes détectées
5 : 2 pannes non détectées
6 : 1 panne détectée + 1 panne non détectée
7 : 3 pannes détectées
8 : 3 pannes non détectées
9 : 2 pannes détectées + 1 panne non détectée
10 : 1 panne détectée + 2 pannes non détectées

	1	2	3	4	5	6	7	8	9	10
1	-	$3*\lambda_{DD}*(1-\beta_D)$	$3*\lambda_{DU}*(1-\beta)$				$3*\lambda_{DD}*\beta_D$	$3*\lambda_{DU}*\beta$		
2	1/MTTR	-		$2*\lambda_{DD}*(1-\beta_D)$		$2*\lambda_{DU}*(1-\beta)$	$2*\lambda_{DD}*\beta_D$			$2*\lambda_{DU}*\beta$
3	$1/(T_1/2+MTTR)$		-		$2*\lambda_{DU}*(1-\beta)$	$3*\lambda_{DD}*(1-\beta_D)$	$3*\lambda_{DD}*\beta_D$	$2*\lambda_{DU}*\beta$		
4		1/MTTR		-			λ_{DD}		λ_{DU}	
5	$1/(T_1/2+MTTR)$				-		$3*\lambda_{DD}*\beta_D$	λ_{DU}		$3*\lambda_{DD}*(1-\beta_D)$
6	$1/(T_1/2+MTTR)$		1/MTTR	$\lambda_{DD}*(1-\beta_D)$		-	$2*\lambda_{DD}*\beta_D$		$\lambda_{DD}*(1-\beta_D)$	λ_{DU}
7				1/MTTR			-			
8	$1/(T_1/2+MTTR)$						$3*\lambda_{DD}*\beta_D$	-		$3*\lambda_{DD}*(1-\beta_D)$
9	$1/(T_1/2+MTTR)$					1/MTTR	λ_{DD}		-	
10	$1/(T_1/2+MTTR)$				1/MTTR		$2*\lambda_{DD}*\beta_D$		$2*\lambda_{DD}*(1-\beta_D)$	-

- Le système de sécurité n'est disponible que dans les états 1, 2 et 3.
- Il pourrait l'être également dans l'état 4 si le vote prenait en compte les tests de diagnostic, ce qui est exclu dans la norme.
- Les modes communs (β_D et β) affectent simultanément les 3 chaînes.

L'indisponibilité est calculée en régime asymptotique :

MAT :	1	2	3	4	5	6	7	8	9	10
OK : 1	-	0,000297	0,000029				0,000003	0,000001		
1 panne détectée : 2	0,041667	-		0,000198		0,000020	0,000002			0,000000
1 panne non détectée : 3	0,000227		-		0,000020	0,000297	0,000003	0,000000		
2 pannes détectées : 4		0,041667		-			0,000100		0,000010	
2 pannes non détectées : 5	0,000227				-		0,000003	0,000010		0,000297
1 panne détectée + 1 panne non détectée : 6	0,000227		0,041667	0,000099		-	0,000002		0,000099	0,000010
3 pannes détectées : 7				0,041667			-			
3 pannes non détectées : 8	0,000227						0,000003	-		0,000297
2 pannes détectées + 1 panne non détectée : 9	0,000227					0,041667	0,000100		-	
1 panne détectée + 2 pannes non détectées : 10	0,000227				0,041667		0,000002		0,000198	-
INIT :	1	0	0	0	0	0	0	0	0	0
ETATS :	1	1	1	0	0	0	0	0	0	0

λ_{DU} :	0,00001	hr-1
λ_{DD} :	0,0001	hr-1
T_1 :	8760	hr
MTTR :	24	hr
β_D :	1%	
β :	2%	

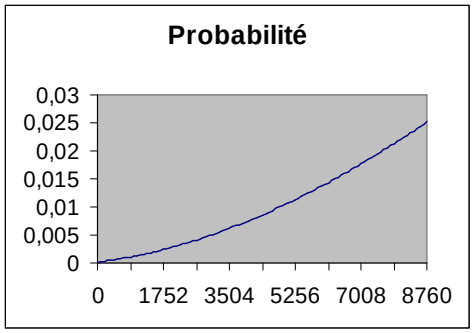
	PFD	PFH
Markov :	0,01212	2,1E-05
Formules :	0,00958	3,1E-05

T_{CE} : 422,182 T_{GE} : 289,455

Et en régime transitoire :

MAT :	1	2	3	4	5	6	7	8	9	10
OK : 1	-	0,000297	0,000029				0,000003	0,000001		
1 panne détectée : 2	0,041667	-		0,000198		0,000020	0,000002			0,000000
1 panne non détectée : 3			-		0,000020	0,000297	0,000003	0,000000		
2 pannes détectées : 4		0,041667		-			0,000100		0,000010	
2 pannes non détectées : 5					-		0,000003	0,000010		0,000297
1 panne détectée + 1 panne non détectée : 6			0,041667			-	0,000002		0,000198	0,000010
3 pannes détectées : 7				0,041667			-			
3 pannes non détectées : 8							0,000003	-		0,000297
2 pannes détectées + 1 panne non détectée : 9						0,041667	0,000100		-	
1 panne détectée + 2 pannes non détectées : 10					0,041667		0,000002		0,000198	-
INIT :	1	0	0	0	0	0	0	0	0	0
ETATS :	0	0	0	1	1	1	1	1	1	1

Indisponibilité : 0,025158337
à t : 8760 (hr)
Indisponibilité moyenne entre 0 et t : 0,009965274




2003

6 – Triple chaînes en redondance 1003

Cette architecture à un fonctionnement identique à la 1002 avec 3 chaînes au lieu de 2.

Elle se modélise comme la 2003 mais est disponible dans les états 1 à 6.

L'indisponibilité est calculée en régime asymptotique :

MAT :	1	2	3	4	5	6	7	8	9	10
OK : 1	-	0,000297	0,000029				0,000003	0,000001		
1 panne détectée : 2	0,041667	-		0,000198		0,000020	0,000002			0,000000
1 panne non détectée : 3	0,000227		-		0,000020	0,000297	0,000003	0,000000		
2 pannes détectées : 4		0,041667		-			0,000100		0,000010	
2 pannes non détectées : 5	0,000227				-		0,000003	0,000010		0,000297
1 panne détectée + 1 panne non détectée : 6	0,000227		0,041667			-	0,000002		0,000198	0,000010
3 pannes détectées : 7				0,041667			-			
3 pannes non détectées : 8	0,000227						0,000003	-		0,000297
2 pannes détectées + 1 panne non détectée : 9	0,000227					0,041667	0,000100		-	
1 panne détectée + 2 pannes non détectées : 10	0,000227				0,041667		0,000002		0,000198	-
INIT :	1	0	0	0	0	0	0	0	0	0
ETATS :	1	1	1	1	1	1	0	0	0	0

λ_{DU} :	0,00001	hr-1
λ_{DD} :	0,0001	hr-1
T_1 :	8760	hr
MTTR :	24	hr
β_D :	1%	
β :	2%	

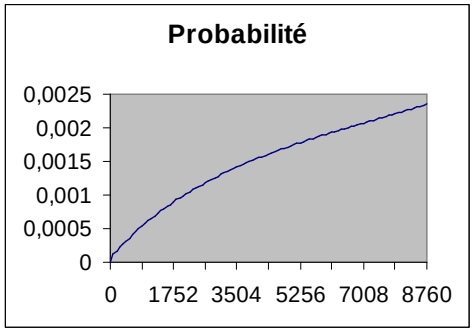
	PFD	PFH
Markov :	0,00142	4,882E-06
Formules :	0,00112	2,851E-07

T_{CE} : 422,182 T_{GE} : 289,455 T_{G2E} : 223,091

Et en régime transitoire :

MAT :	1	2	3	4	5	6	7	8	9	10
OK : 1	-	0,000297	0,000029				0,000003	0,000001		
1 panne détectée : 2	0,041667	-		0,000198		0,000020	0,000002			0,000000
1 panne non détectée : 3			-		0,000020	0,000297	0,000003	0,000000		
2 pannes détectées : 4		0,041667		-			0,000100		0,000010	
2 pannes non détectées : 5					-		0,000003	0,000010		0,000297
1 panne détectée + 1 panne non détectée : 6			0,041667			-	0,000002		0,000198	0,000010
3 pannes détectées : 7				0,041667			-			
3 pannes non détectées : 8							0,000003	-		0,000297
2 pannes détectées + 1 panne non détectée : 9						0,041667	0,000100		-	
1 panne détectée + 2 pannes non détectées : 10					0,041667		0,000002		0,000198	-
INIT :	1	0	0	0	0	0	0	0	0	0
ETATS :	0	0	0	0	0	0	1	1	1	1

Indisponibilité : 0,0023456
à t : 8760 (hr)
Indisponibilité moyenne entre 0 et t : 0,0014832




1003

Conclusions :

La modélisation d'un système requiert une définition très précise des caractéristiques de son architecture et de la manière de l'opérer.

La norme EN 61508 est relativement ambiguë sur le fonctionnement réel des architectures proposées et les formules fournies ne font pas l'objet de justifications rigoureuses. Pour le jeu de valeurs numériques choisi dans ce TP, les ordres de grandeur des résultats obtenus par les formules semblent toutefois corrects à l'exception de la valeur de PFH de l'architecture 1003.

On notera que les canaux en redondance font l'objet d'une maintenance périodique simultanée et, par là même, ne sont pas indépendants entre eux. La probabilité de défaillance multiple juste avant la maintenance peut être sensiblement supérieure à une combinaison de probabilités de panne en valeur moyenne.