ANNEXE 3/1: DEFAILLANCES PERCEPTIBLES ET REPARABLES

(D'après Fiabilité, maintenabilité et Risque de David SMITH)

1 - Probabilité et indisponibilité d'un circuit 1002

Les démonstrations sont réalisées pour un circuit 1002 (1 branche doit fonctionner sur les 2 branches en parallèle). La généralisation à N branches ne sera que mentionnée.

Pour qu'un système 1002 soit défaillant il faut que:

la branche A **OU** la branche B soit défaillante, **ET** que la branche en service devienne défaillante durant le temps d'indisponibilité de l'autre branche.

1.1 – Taux de défaillance par unité de temps de l'ensemble des 2 branches A & B

Prob.de BF de l'ensemble branche = Prob. BF.A **ET** Prob. BF.B = R ensemble = $R_A \times R_B$

(BF = bon fonctionnement)

Prob.de défaillance de l'une ou l'autre branche = F ensemble = Prob. déf.A **OU** Prob. déf.B

(1 – F) ensemble = $(1 - F_A) \times (1 - F_B)$ → F ensemble = $F_A + F_B - F_A \times F_B$ (théorème de Poincaré)

($F_A \times F_B$) négligeable → Prob.de défaillance de l'une ou l'autre branche $\simeq F_A + F_B$

F_A = probabilité de défaillance de la branche A = $1 - e^{-\lambda.t} \simeq e^{-\lambda.t}$

Si A et B identiques: FA = FB $\simeq e^{-\lambda.t}$ → Prob.de défaillance de l'ensemble branche = $2.\lambda$ ①

1.2 – Taux de défaillance du système

λsyst = Taux de défaillance de l'ensemble branche x Taux d'indisponibilité d'un branche

1.3 – Taux d'indisponibilité d'une branche

Le taux d'indisponibilité peut être calculé de la manière suivante:

Taux disponibilité d'une branche = Tps dispo / Tps total = MTBF / (MTBF + MDT)

MTBF temps moyen de bon fonctionnement au sens de la fiabilité.

MDT (Mean Down Time)

Taux d'indisponibilité branche = 1 - MTBF / (MTBF + MDT) = MDT / (MTBF + MDT)

Dans l'hypothèse de $\beta = 1$, MTBF = $1 / \lambda$. De plus MDT négligeable devant le MTBF d'où:

Taux d'indisponibilité branche = λ /MTBF = λ.MDT ②

① & ② → Taux de défaillance du système = $2.\lambda \times \lambda.MDT = 2.\lambda^2.MDT$

1.4 – Probabilité de défaillance du système

La norme utilise le terme d'indisponibilité.

Probabilité = Indisponibilité = Taux de défaillance x Durée critique

On peut admettre, pour un système 1002, qu'en moyenne la défaillance de la branche utilisée en secours aura lieu à la moitié du temps d'arrêt pour réparation de la première branche soit à MDT / 2.

D'où: **Probabilité de défaillance du système = $2.\lambda^2.MDT \times MDT / 2 = \lambda^2.MDT^2$**

2 - Généralisation

Défaillances perceptibles – Système réparable								
Taux de défaillance du système				**N éléments installés**	**Probabilité (indisponibilité) du système**			
λ				**1**	$\lambda.MDT$			
$2.\lambda^2.MDT$	$2.\lambda$			**2**	$\lambda^2.MDT^2$	$2.\lambda.MDT$		
$3.\lambda^3.MDT^2$	$6.\lambda^2.MDT$	$3.\lambda$		**3**	$\lambda^3.MDT^3$	$3.\lambda^2.MDT^2$	$3.\lambda.MDT$	
$4.\lambda^4.MDT^3$	$12.\lambda^3.MDT^2$	$12.\lambda^2.MDT$	$4.\lambda$	**4**	$\lambda^4.MDT^4$	$4.\lambda^3.MDT^3$	$6.\lambda^2.MDT^2$	$4.\lambda.MDT$
1	**2**	**3**	**4**	**MooN**	**1**	**2**	**3**	**4**
M éléments requis					**M éléments requis**			

Tableau 3

ANNEXE 3/2: DEFAILLANCES NON PERCEPTIBLES ET REPARABLES

1 - Défaillances non perceptibles en dehors d'un test et réparables

Par exemple un système de sécurité relatif à une surpression est rarement sollicité et sa défaillance (non réponse) passe inaperçue en dehors de la survenance de l'incident process. Lorsque les défaillances des branches ne sont pas perceptibles en cours d'utilisation de l'installation, un test de bon fonctionnement d'une ou des branches est réalisé suivant une périodicité T.

On trouve différents types de tests. Leur performance est mesurée par la couverture de diagnostic DC.

Tests prévus dès la conception: Durant la durée des tests l'installation peut être dans un état dangereux, de plus les tests risquent de créer des défaillances systématiques en particulier l'intervention d'Opérateurs peut multiplier par 10 le risque de défaillance.

Tests manuels: Parfois ils ne peuvent être réalisés que durant des arrêts complets d'installation (2 ans, 5 ou même 7 ans)

Tests automatiques: Intégrés au matériel et souvent réalisés en ligne. Ils sont propres à chaque composant ou contrôlent le fonctionnement opérationnel d'une partie de l'installation.

Si le système est composé de X éléments il faut que X défaillances surviennent pour rendre indisponible le système.

On pourra admettre que leur distribution est régulière durant l'intervalle de test T et que le temps de réparation d'un élément est faible par rapport à T.

Le tableau ci-dessous donne les valeurs des PDF et PFH fournies par la **SINTEF**: Reliability Prediction Method for Safety Instrumented Systems – PDSMethod Handbook 2010 Edition (PDS = Acronyme en Norvégien de Reliability of computer- based safety systems).

	Défaillances aléatoires		**Défaillances *CC***	
	PFH	**PFD_{avg}**	**PFH**	**PFD_{avg}**
1001	λ_{DU}	$\lambda_{DU}.T/2$	/	/
1002	$(\lambda_{DU})^2.T$	$(\lambda_{DU}.T)^2/3$	$\beta.\lambda_{DU}$	$\beta.\lambda_{DU}.T/2$
2002	$2.\lambda_{DU}$	$\lambda_{DU}.T$	/	/
1003	$(\lambda_{DU})^3.T^2$	$(\lambda_{DU}.T)^3/4$	$C_{1003}.\beta.\lambda_{DU}$	$C_{1003}.\beta.\lambda_{DU}.T/2$
2003	$3.(\lambda_{DU})^2.T$	$(\lambda_{DU}.T)^2$	$C_{2003}.\beta.\lambda_{DU}$	$C_{2003}.\beta.\lambda_{DU}.T/2$
3003	$3.\lambda_{DU}$	λ_{DU}	/	/
MooN	**(A)**	**(B)**	$C_{MooN}.\beta.\lambda_{DU}$	$C_{MooN}.\beta.\lambda_{DU}.T/2$
NooN	$N.\lambda_{DU}$	$N.\lambda_{DU}.T/2$	/	/

(**A**) → $[N\,!\,/\,(N-M+1)\,!\,.\,(M-1)\,!] \times [(\lambda_{DU}.T)^{N-M+1} / T$

(**B**) → $[N\,!\,/\,(N-M+2)\,!\,.\,(M-1)\,!] \times [(\lambda_{DU}.T)^{N-M+1}$

Tableau 4

Le facteur β étant déterminé pour une architecture 1002, la Sintef propose d'appliquer un coefficient C_{MooN} au facteur β suivant les différentes architectures (C_{1002} = 1; C_{1003} = 0.5; etc.).