Convertisseur CAL23DmA rev0

AMDEC Détaillée

DATE	20-09-2010

	NAME	
WRITTEN BY	P.DUMOULIN	
CHECKED BY	R.KIEFFER	
SAFETY CHECKED BY	A.CURULLA	
APPROVED	D.CURULLA	

REFERENCE	LG	REV					*SH/SH END*	*NUM SH*
AMDEC CAL23DmA rev0	fr	A1	-				1/16	16

TABLE OF CONTENTS

Section 1 Généralités

1.1 Documents de référence

[1.]	CEI 60812 – Edition 2 - 2006	Analyse des Modes de défaillance de leurs Effets et de leur Criticité
[2.]	CEI 62380 - 2004	Recueil de données de fiabilité - Modèle universel pour le calcul de la fiabilité prévisionnelle des composants
[3.]	RPA101019 - B	AMDEC Détaillée - Recommandations
[4.]	CEI 61508 – Edition 2.0 – 2010-04	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité

1.2 Abréviations

AMDEC	Analyse des Modes de Défaillance, de leurs Effets et de leur Criticité
SIL	Safety Integrity Level

Section 2 Contexte

Ce document est l'Analyse des Modes de Défaillance, de leur Effet et de leur Criticité (AMDEC) du composant CALD23mA/S2 de la société LOREME.

Outre la caractérisation des informations nécessaires pour la sûreté de fonctionnement (en particulier pour les calculs de disponibilité et de constitution de stock de pièces de rechange), cette étude permet de répondre aux exigences de la norme CEI-61508 en identifiant et quantifiant les défaillances dangereuses du composant, permettant ainsi d'interagir sur la conception afin d'éviter ou de réduire ces risques.

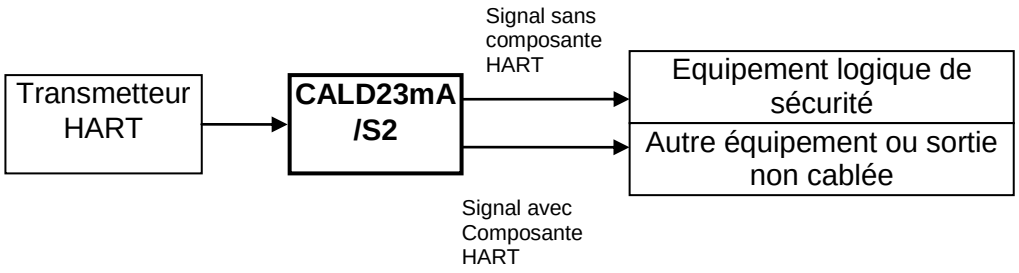
2.1 Circonstances de l'analyse

Cette étude a été réalisée dans le but de vérifier l'aptitude du convertisseur CALD23mA/S2 à être utilisé dans des applications de sécurité SIL3.

2.2 Périmètre de l'analyse

Le composant concerné comprend un ensemble de composants électroniques faisant l'acquisition de signaux d'entrée issus de capteurs analogiques HART et restituant deux signaux de sorties : l'un identique à l'entrée, le 2ème, sans la composante HART.

Généralement, un convertisseur est interfacé entre un capteur HART et un équipement de protection, généralement désigné « Equipement logique de sécurité»



2.3 Tests par injection de défaut

Des tests d'injection de défauts ont été réalisés par la société LOREME, afin de vérifier les hypothèses de détection et de dangerosité.

Rapport de test : AMDEC_CAL23DmA verification par injection defaut.XLS

Section 3 Caractéristiques relatives à la sécurité

Les caractéristiques, relatives à la sécurité, sont définies dans la norme CEI 61508.

3.1 Caractérisation du composant

Le convertisseur CALD23mA est un sous-système de type « A » [CEI61508-2-§ 7.4.3.1.2] :

- Les modes de défaillances des composants nécessaires à la réalisation de la fonction de sécurité sont bien définis,
- Le comportement du convertisseur dans des conditions d'anomalie est entièrement déterminé,
- Le convertisseur bénéficie d'un retour d'expérience dans de nombreuses applications de sécurité.

3.1.1 Défaillance en sécurité

[CEI61508-4-§3,6.8] Défaillance en sécurité: Défaillance qui n'a pas la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.

Une défaillance en sécurité est une défaillance qui n'est pas dangereuse.

On parle aussi de défaillance sûre.

[CEI61508-2-§7.4.3.1.1-d] La proportion de défaillances en sécurité d'un sous-système appelé SFF (Safe Failure Fraction) est définie par le rapport entre la somme des probabilités de défaillances en sécurité λ_S plus les défaillances dangereuses détectées λ_{DD} sur la somme des probabilités de défaillances fonctionnelles total du sous-système (ensemble des « défaillances en sécurité » λ_S et des « défaillances dangereuses » λ_D).

$$SFF = \frac{\lambda_S + \lambda_{DD}}{\lambda_S + \lambda_D}$$

3.1.2 Défaillance dangereuse

[CEI61508-4-§3,6.7] Défaillance dangereuse : défaillance qui a la potentialité de mettre le système relatif à la sécurité dans un état dangereux ou dans l'impossibilité d'exécuter sa fonction.

On parle aussi de panne non sûre.

Section 4 Etude AMDEC

4.1 Analyse fonctionnelle

Le convertisseur se compose :

- D'un étage d'entrée (appelé input stage dans l'AMDEC), commun aux deux sorties
- D'une fonction « alimentation » (appelée Power Supply dans l'AMDEC) en charge de générer des tensions d'alimentation indépendantes : Ve pour alimenter le capteur, V1 pour alimenter la sortie S1 et V2 ppour alimenter la sortie S2.
- D'une sortie S1 (appelée output1 dans l'AMDEC) contenant la composante HART du signal d'entrée
- D'une sortie S2 (appelée output2 dans l'AMDEC) ne contenant pas la composante HART du signal d'entrée.

4.2 Définition de l'évènement redouté

Pour le convertisseur CALD23, l'événement redouté (c'est-à-dire la défaillance dangereuse, telle que définie dans la section précédente) est l'émission d'un courant de sortie erroné :

- Soit un courant de sortie erroné de plus de 2% par rapport à la demande du procédé.
- Soit un courant de sortie, bloqué à une valeur, tel qu'il ne peut prendre une valeur de repli de sécurité: courant de sortie bloqué dans une gamme > 3,6mA ou < 21mA.

4.3 Définition de la position de repli de sécurité

L'état de repli de sécurité est défini par un courant de sortie hors de la gamme 3,6mA – 21mA.

- Soit un courant de sortie < 3,6 mA
- Soit un courant de sortie > 21 mA

Le programme d'application de l'« Equipement logique de sécurité » devra impérativement être configuré pour détecter toute valeur de courant hors gamme (< 3,6 mA - > 21 mA) et les considérées « Invalides ».

De ce fait, dans l'étude AMDEC, cet état est considéré comme non dangereux.

4.4 Description du tableau AMDEC

Afin d'illustrer la méthode décrite précédemment, vous trouverez en annexe un exemple de tableau AMDEC adapté à l'évaluation des caractéristiques de sûreté d'un module.

Les colonnes de ce tableau sont listées et expliquées ci-après :

- ***S. Fonc.* :** Identification de la fonction dont le composant étudié fait parti.
- ***Libellé*** : Libellé abrégé du composant considéré
- ***Repère topo.*** : Repère topographique du composant sur le schéma développé.
- ***Qt* :** Quantité (généralement unitaire -1- sauf pour les fonctions répétitives dont les effets de défaillances sont strictement identiques).
- ***λu*** : Taux de défaillance unitaire du composant. Tous les taux de défaillance sont exprimés en FIT (10-9 panne / heure).
- ***λt*** : Taux de défaillance total (*λu* * Qt)
- **Fail. Mode**: Mode de défaillance propre au type du composant. Six principaux modes de défaillance sont retenus
    - CC: court-circuit
    - CO: Circuit Ouvert
    - Drift : Dérive de la valeur
    - Sortie à la masse
    - Sortie bloquée à la tension d'alimentation
- ***%*** : Répartition, en pourcentage, des modes de défaillance issus exclusivement de la norme CEI 62380.
- ***Effet local*** Effet de la défaillance du composant au niveau de la fonction.
- ***Effet module*** Effet de la défaillance au niveau du module ; en particulier pour les pannes identifiées non dangereuses, décrire comment l'état sûr est obtenu.

Remarque : Cette étude a considéré que tout défaut conduisant à une valeur de courant en sortie du convertisseur < 3,6mA ou > 21 mA devait être considérée comme « invalide » par l'équipement qui en fait l'acquisition et par conséquent qu'il n'était pas dangereux.

Description des categories de défaillances		Classification
Etat de repli de sécurité (Fail safe state)	L'état de repli de sécurité est défini par un courant de sortie hors de la gamme 3,6mA – 21mA - Soit un courant de sortie < 3,6 mA - Soit un courant de sortie > 21 mA	SD: Safe; Detected at system level
Courant de sortie < 3,6mA (Output current < 3,6 mA (Fail safe low))	Tous défauts conduisant à un courant de sortie < 3,6mA, sans demande de la part du procédé	SD: Safe; Detected at system level
Courant de sortie > 21mA (Output current > 21 mA (Fail safe high))	Tous défauts conduisant à un courant de sortie > 21 mA, sans demande de la part du procédé	SD: Safe; Detected at system level

Description des categories de défaillances		Classification
Courant de sortie erroné (Erroneous output current (Fail dangerous))	Défaillance qui conduit à une sortie erronée, c'est à dire qui ne reflète pas la demande du procédé. - Soit la défaillance conduit à un courant de sortie erroné avec plus de 2% d'erreur par rapport à la demande du procédé. - Soit la défaillance empêche le courant de sortie de prendre une valeur de repli de sécurité (courant de sortie bloqué dans une gamme > 3,6mA ou < 21mA)	DU: Dangerous Undetected
Pas d'effet fonctionnel (Not functional effect)	Défaut d'un composant qui n'a pas d'effet sur la fonction de sécurité – Voir note1 De tels défauts sont non fonctionnels. Les défauts peuvent être: - Perte de certaines capacités de découplage - Défaillance de composants non utilisés, ou composants de face avant (tels que les leds…)	Not for SFF calculation; it is also not part of the total failure rate
Pas d'effet (No effect on output current)	Défaut d'un composant qui ne conduit pas à une erreur du courant de sortie de plus de 2%. Pour le calcul du SFF, cela est considéré comme un défaut "sûr" non détecté.	SU: Safe Undetected failure
Dégradation de filtrage ou de protection (Filtering or protection degradation)	- Défaillance de composants de filtrage CEM Voir note2 Du fait de la difficulté à appréhender les conséquences d'un tel défaut, ces derniers sont considérés comme fonctionnels dans 50% des cas. De même, parmi ces derniers, 50% sont considérés potentiellement dangereux.	SU: Safe Undetected failure DU: Dangerous Undetected

Note 1 - Cas particulier des condensateurs de découplage : Les condensateurs de découplage assurant le découplage général d'une carte électronique ; en moyenne, un condensateur de découplage pour un ou deux circuits intégrés. Le nombre total de condensateurs de découplage sur une carte, permet alors de considérer que la défaillance en "circuit ouvert" d'un condensateur n'a pas d'influence fonctionnelle en cas de perturbation extérieure : le découplage est assuré par les autres condensateurs de la carte et par conséquent ce mode de défaillance n'est pas détecté.
En termes de défaillance dangereuse, en plus du fait que la perturbation sera absorbée par les autres condensateurs, sa présence de courte durée ne peut empêcher en permanence une entrée ou une sortie de prendre son état normal ; En conséquence, ce mode de défaillance est non fonctionnel.

Note 2 - Pour assurer l'immunité aux perturbations CEM et aux surtensions exceptionnelles (surtensions en dehors des conditions normales d'exploitation), un certain nombre de composants peuvent être ajoutés au schéma. Les modes de défaillance de ces composants allant dans le sens de la "disparition" du composant (circuit ouvert d'un élément de protection parallèle et court circuit d'un élément série), ne sont généralement pas détectés. Mais les éventuelles perturbations, que la défaillance de ces composants ne permettra plus de filtrer, ne peuvent pas empêcher durablement l'acquisition ou la restitution dans leur état sûr.

En conséquence, pour un système de protection, ces défaillances seront considérées fonctionnelles dans la moitié des cas, toujours non détectées et potentiellement dangereuses dans 50% des cas fonctionnels.

- ***Moyen de détection*** : Le convertisseur ne dispose pas de fonctions d'autotests. Cependant, cette colone permet d'indiquer si le défaut est non détecté, détectable uniquement lors de tests périodiques, ou détectables par l'équipement faisant l'acquisition du signal issu du convertisseur, généralement appelé «solver logique », en charge de détecter toute valeur hors gamme.

Les cinq colonnes [Fct, %DAuto, %Dpério, Ns et MC] sont analysées à la fois dans le cadre d'un module implanté dans une architecture « simplexe » et « redondante ». la colonne [Nv] n'est applicable que pour une architecture « redondante ».

- ***Fct*** : Ce mode de défaillance a-t-il un effet fonctionnel ?
  - "O" pour oui dans tous les cas,
  - "N" pour non dans tous les cas,
  - "X" pour oui dans 50% des cas.
- $\%D_{Auto}$: % de détection par des autotests.
- $\%D_{Perio}$: Dans le cas où la détection par des autotests n'est pas de 100%, indiquer le % de détection total (via autotests + via tests périodiques) qui pourrait être obtenu en considérant des tests périodiques (Ces test seront à décrire).
- ***Ns détecté*** : La défaillance peut-elle avoir un effet non sûr lorsqu'elle est détectée?
  - "O" pour oui dans tous les cas de détection
  - "N" pour non dans tous les cas de détection
  - "X" pour oui dans 50% des cas de détection
- ***Ns non détecté***: Dans le cas où la défaillance n'est pas détectée à 100%, indiquer si elle peut avoir un effet non sûr lorsqu'elle n'est pas détectée ?
  - "O" pour oui dans tous les cas de non détection
  - "N" pour non dans tous les cas de non détection
  - "X" pour oui dans 50% des cas de non détection
- ***MC*** : Identification d'un Mode Commun entre les deux sorties

  Le convertisseur peut être utilisé, en autre, dans les applications suivantes :

  - Une sortie du convertisseur est utilisée dans une application dite « de sécurité », l'autre sortie étant utilisée pour une autre application (de régulation ou supervision par exemple)
  - Les deux sorties du convertisseur sont acquises par un même équipement qui les compare, en 1oo2, afin de vérifier leur cohérence et ainsi réduire le taux de pannes non sûres,

  Il est intéressant de pouvoir distinguer dans l'AMDEC, les défauts affectant les deux sorties de manière commune, des défauts n'affectant que l'une ou l'autre des sorties.

  La colonne MC (Mode Commun) permet d'indiquer si le mode de défaillance du composant affecte les deux sorties (MC = o (oui) ou bien une seule sortie (MC = N (Non) ; dans ce cas, la colonne suivante permet de discriminer la sortie affectée (S1 ou S2).

A partir des informations précédentes, des formules automatiques saisies dans le fichier Excel du tableau AMDEC permettent de quantifier les taux de défaillances suivants, pour chacun des modes de défaillances de chaque composant élémentaire :

λf	Taux de pannes fonctionnelles
λfd	Taux de pannes fonctionnelles détectées Avec $\lambda fd = \lambda fd_{low} + \lambda fd_{high}$
λfd_{low}	Défaillances en position de repli < 3,6mA
λfd_{high}	Défaillances en position de repli > 21mA
λfnd	Taux de pannes fonctionnelles non détectées
λsd	Taux de pannes "sures" détectées
λsnd	Taux de pannes "sures" non détectées
λdd	Taux de pannes dangereuses détectées (1)
λdu	Taux de pannes dangereuses non détectées totales du composant $\lambda du = \lambda du_{mc} + \lambda du_{S2} + \lambda du_{S1}$
λdu_{mc}	Taux de pannes dangereuses non détectées de la partie "mode commun"
λdu_{S2}	Taux de pannes dangereuses non détectées de la sortie S2
λdu_{S1}	Taux de pannes dangereuses non détectées de la sortie S1
MTBF	Temps moyen entre défaillances

(1) Cette étude a considéré que tout défaut conduisant à une valeur de courant en sortie du convertisseur < 3,6mA ou > 21 mA devait être considérée comme « invalide » par l'équipement qui en fait l'acquisition et par conséquent qu'il n'était pas dangereux

Le tableau renseigné nous permet de calculer les caractéristiques élémentaires de sûreté du module:

DC	Taux de couverture fonctionnel (Lambda fonctionnel / lambda fonctionnel détecté)	$\lambda fd / \lambda f$
SFF	Proportion de défaillances en sécurité	$\lambda sd + \lambda snd / \lambda f$

Section 5 Calcul de fiabilité

Les taux de pannes des composants utilisés dans l'AMDEC sont calculés selon la norme CEI 62380 - Recueil de données de fiabilité - Modèle universel pour le calcul de la fiabilité prévisionnelle des composants.

5.1.1 Hypothèses d'étude

Les taux de défaillance des composants sont considérés constants sur toute la durée de vie du système.

L'évaluation des caractéristiques de sûreté d'un module fait intervenir un certain nombre d'hypothèses :

- Seul l'aspect matériel est traité. L'aspect sûreté de fonctionnement du logiciel n'est pas abordé.
- Seules les défaillances catalectiques sont prises en compte : Défaillances franches, soudaines et non prévisibles. Ne sont pas considérées, les défauts qui pourraient être dus à :
  - des erreurs de conception,
  - à des défauts de lot en production,
  - à l'environnement (interférences électriques, cycles de température, vibrations) ; L'équipement et ses modules est généralement conçu pour tenir aux exigences environnementales définies dans la norme automates IEC61131-2.
  - des erreurs humaines en fonctionnement ou en maintenance, (des précautions sont prises pour les éviter : telles que des mots de passe, des vérifications de valeur de gamme, cohérence du matériel détecté...)
- Ne sont traitées que les pannes simples.
- Les défauts de soudure, qui sont généralement dus à une non qualité détectable en fin de fabrication par un déverminage spécifique, ne sont pas pris en compte.
- Tous les aspects touchant aux fonctionnalités spécifiques à la phase de mise sous tension ne sont pas traités.

5.1.2 Hypothèses pour le calcul des taux de défaillance

Température

En phase de fonctionnement, il est fait l'hypothèse que l'équipement est installé dans un local dont la température est régulée, de sorte que la variation de température est inférieure à 3°C. Par conséquent, et en accord avec les hypothèses de la norme IEC62380, le ΔT sera égal à 0, pour la phase de fonctionnement.

L'étude a été réalisée pour deux températures :

- Une température ambiante de 23°C, correspondant à la température d'un local climatisé. L'échauffement dû aux composants électroniques de l'équipement sous-tension en phase de fonctionnement, est estimé à 7°C. Ce qui correspond à une température au droit des composants de 30°C.

- Une température ambiante de 38°C (afin de simuler une panne de climatisation). Ce qui correspond à une température au droit des composants de 45°C.

Profil de mission

Le profil de mission définit les conditions d'utilisations de l'équipement de sécurité. Pour un automate de sécurité, le profil de mission se décompose en phases suivantes :

- Une phase de on/off par an (pour des besoins de maintenance par exemple) ; A cette occasion, l'équipement subit une variation de température Delta ΔT : de 7°C entre les 23°C de température ambiante et les 30°C, température au droit des composants due à leur échauffement.
- Deux phases par an, pour simuler un disfonctionnement du système de climatisation; A cette occasion, on estime que l'équipement subit une variation de température Delta ΔT : de 15°C (Delta entre la température au droit des composants lorsque la climatisation fonctionne, c'est à dire 30°C et la température estimée en cas de perte de climatisation, 45°).
- Une phase de fonctionnement permanent le reste du temps, sans considération de variation de température.

Remarque : En cas de profil différent (température, temps de fonctionnement…) un nouveau calcul est à prévoir avec une éventuelle vérification du respect des contraintes SIL.

Récapitulatif des hypothèses :

Hypothèses	
Tac (Température de l'air ambiant)	23.00
Tae (T° ambiante au voisinage des composants (= T° air ambiant + Delta T° composants 7°C)	30.00
Delta ΔT1°C / cycle (Tae – Tac)	7.00
n1 (Nbre de Cycles de T°/an)	1.00
Delta ΔT2 - Prise en compte d'une différence de température simulant une perte de climatisation du local	15.00
n2 (Nbre de Delta DT2 / an => 2 pertes de climatisation / an)	2.00
τon (Temps pendant lequel l'équipement est sous tension)	1.00
τoff (Temps pendant lequel l'équipement est hors tension)	0.00

5.1.3 Taux de défaillance

Ci après les taux de pannes élémentaires des composants du convertisseur CALD23mA/S2, pour une température au voisinage des composants de 30°C:

Type de composant	*Taux de pannes en Fits (10-9/h)*
Condensateurs	
Condensateur céramique de type II X7R	0.16
Condensateur céramique de type I NPO	0.05
Condensateur ALU - electrolyte liquide	8.00
Condensateur ALU - electrolyte solide	2.05
Résistances & Potentiomètres	
Résistances fixes CMS - faible dissipation	0.02
Résistances fixes agglomérée à piquer	0.74
Potentiomètres - non bobinés	0.45
Transistors	
Transistors MOS basse puissance (2N7002) - non interface - SOT23	0.13
Diodes	
Diodes petit signal – NON utilisée en interface - CMS - SOT23	0.14
Diodes redressement - NON utilisée en interface - CMS - SOT23	0.18
Diode zéner - NON utilisée en interface - CMS - SOT23 BXZ384	0.57
Diode basse puissance (1500W peak) - transient voltage suppressor - DO214 - SMCJ105A - NON utilisée en interface	1.51
Diode de signal - puissance - CMS non interface	0.53
Diodes redressement basse puissance – utilisée en interface - CMS - SOT23	40
Diode basse puissance (1500W peak) - transient voltage suppressor - DO214 - SMCJ105A utilisée en interface	11.51
Diodes redressement puissance - utilisée en interface - CMS - SOT23	41
Circuits intégrés Bipolaires	
Regulator - 78L05 - SO8 - circuit mixtes	12.9
Circuits Linéaires (MOS)	
Amplifier - LM258	3.06
Relais	
Relais electromécaniques - miniatures - type inverseur	11.4
Transformateur	
Transformateur - Puissance	1.60
light indicator	
LEDs	2.0

Section 6 Résultats de l'AMDEC:

L'AMDEC détaillée se trouve dans le fichier : *AMDEC_CAL23DmA.xls*

Les résultats sont exprimés en Fits (10^{-9}/h) pour tous les taux de pannes.

Rappel : température au voisinage des composants de 30°C (23°C ambiante + 7°C de delta T)

Taux de pannes fonctionnelles	265	λf
Taux de pannes fonctionnelles détectées	235	λfd
Défaillances en position de repli < 3,6mA	231	λfd low
Défaillances en position de repli > 21mA	3.9	λfd high
Taux de pannes fonctionnelles non détectées	30	λfnd
Taux de pannes "sures" détectées	235	λsd
Taux de pannes "sures" non détectées	28.2	λsnd
Taux de pannes dangereuses détectées	0.00	λdd
Taux de pannes dangereuses non détectées totales du composant	1.5	λdu
Taux de pannes dangereuses non détectées de la partie "mode commun"	0.6	λdu_{mc}
Taux de pannes dangereuses non détectées de la sortie S2	0.5	λdu_{S2}
Taux de pannes dangereuses non détectées de la sortie S1	0.5	λdu_{S1}
Temps moyen Entre Défaillances (en heures)	3777383	MTBF
Taux de couverture fonctionnel (Lambda fonctionnel / lambda fonctionnel détecté)	88.8%	DC
Proportion de défaillances en sécurité	99.4%	SFF

Ci-après les résultats de l'AMDEC pour une température au voisinage des composants de 45°C (38°C de température ambiante + 7°C de delta T)

Taux de pannes fonctionnelles	307	λf
Taux de pannes fonctionnelles détectées	261	λfd
Défaillances en position de repli < 3,6mA	255	λfd low
Défaillances en position de repli > 21mA	6.1	λfd high
Taux de pannes fonctionnelles non détectées	46	λfnd
Taux de pannes "sures" détectées	261	λsd
Taux de pannes "sures" non détectées	44.4	λsnd
Taux de pannes dangereuses détectées	0.00	λdd
Taux de pannes dangereuses non détectées totales du composant	1.8	λdu
Taux de pannes dangereuses non détectées de la partie "mode commun"	0.7	λdu_{mc}
Taux de pannes dangereuses non détectées de la sortie S2	0.6	λdu_{S2}
Taux de pannes dangereuses non détectées de la sortie S1	0.6	λdu_{S1}
Temps moyen Entre Défaillances (en heures)	3258617	MTBF
Taux de couverture fonctionnel (Lambda fonctionnel / lambda fonctionnel détecté)	84.9%	DC
Proportion de défaillances en sécurité	99.4%	SFF

Section 7 Cas particuliers de certaines défaillances non détectées lors des tests périodiques

L'AMDEC a mis en évidence que certaines défaillances de composants (la dérive de valeur « drift » de certaines résistances) conduisent à une erreur de 0.5% sur le courant de sortie.

Cette erreur sur le courant de sortie étant très faible, il ne peut être affirmé qu'elle sera systématiquement détectée, par les utilisateurs, lors des tests périodiques.

Par conséquent, la première défaillance sera latente et la deuxième défaillance pourrait éventuellement entrainer une erreur de plus de 2% sur le courant de sortie : ce qui correspond à un état dangereux.

Ces défaillances ont été identifiées sur les deux voies « output1 » et « output2 ». Pour chacune des voies, trois résistances sont concernées (R13, R15 et R16 pour la voie1, R3, R5 et R6 pour la voie 2).

Calculons la probabilité, par voie, pour que deux résistances parmi les trois concernées « dérivent » sur une période T.

Le taux de panne fonctionnel d'une résistance, pour une température auprès des composants de 45°C (ce qui correspond à une approche « pire cas ») est de $1{,}74.10^{-11}$ La probabilité du mode de défaillance en défaut « drift » est de : 60%, soit un taux de panne $\lambda_{drift} = 0{,}6 * 1{,}74.10^{-11} = 1{,}04.10^{-11}$p/h.

Si l'on considère une période T de 30 ans, correspondant à une durée de fonctionnement avant remplacement, la probabilité I pour une résistance d'être en "drift" est donnée par $I = \lambda_{drift} * T/2$. En effet, le taux de panne étant faible en regard de la durée, on considère que statistiquement la durée moyenne d'indisponibilité, lorsqu'il y a une panne dans cette durée, est égale à la moitié de la durée considérée.

La probabilité P de défaillance par heure d'avoir deux résistances parmi les 3 dans ce même défaut, pour les deux voies 1 et 2, sur une durée de 30 ans est de :

$P = 2 * 3! * \lambda_{drift} * I = 6 * \lambda_{drift}^2 * T = 1{,}7.10^{-16}$ p/h

On peut donc considérer que, sur une durée d'utilisation de 30 ans, les dérivent de valeur de deux résistances sur les voies 1 et 2 du convertisseur ont un taux de défaillance négligeable devant les défaillances simples des autres composants du module.