Manuel d'installation , d'utilisation de test et de sécurité

INP101
INP101V

SIL2

LOREME 12, rue des Potiers d'Etain Actipole BORNY - B.P. 35014 - 57071 METZ CEDEX 3
Téléphone 03.87.76.32.51 - Télécopie 03.87.76.32.52
Nous contacter: Commercial@Loreme.fr - Technique@Loreme.fr
Manuel téléchargeable sur: www.loreme.fr

REV 2-18/10/19

Sommaire

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

1 Introduction

1.1 Information générale

Ce manuel contient les informations nécessaires à l'intégration du produit afin d'assurer la sécurité fonctionnelle des boucles connexes. L'ensemble des modes de défaillance et la HFT du module sont précisés dans l'Analyse AMDEC référencée AMDEC CNL40ig rev2.XLS (le CNL40ig est convertisseur de mesure incorporé dans l'INP101)

Autres documents Applicables:
- fiche technique INP101 ,
- déclaration CE de conformité INP101 (disponible dans la rubrique CEM de ce manuel)
- Analyse AMDEC CNL40igH (convertisseur incorporé dans l'INP101)
- Manuel de configuration INP101

Les documents mentionnés sont disponibles sur www.loreme.fr

Le montage,l'installation, la mise en service et la maintenance ne peuvent être effectués que par des personnels formés et qualifiés ayant lu et compris les instructions du présent manuel.

Quand il n'est pas possible de corriger les défauts, les appareils doivent être mis hors service, des mesures doivent être prise pour se protéger contre une utilisation accidentelle. Seul le constructeur peut être amener à réparer le produit.

Le non suivi des conseils donnés dans ce manuel peut engendrer une altération des fonctions de sécurité, et causer des dommages aux biens , à l'environnement ou aux personnes.

1.2 Fonction et utilisations prévues

Le transmetteur INP101 assure la mesure de température issu d'une sonde PT100 ou d'un thermocouple et sa retransmission sous forme de signal analogique 4...20 mA avec ou sans protocole Hart, ainsi que l'isolation du signal.
il dispose d'un afficheur permettant la visualisation locale de la mesure.

Les appareils sont conçus, fabriqués et testés en fonction des règles de sécurité applicables.
Ils ne doivent être utilisés que pour les applications décrites et dans le respect des conditions environnementales figurant dans la fiche technique : http://www.loreme.fr/fichtech/INP101.pdf

1.3 Normes et directives

Les dispositifs sont évalués conformément aux normes citées ci-dessous:

• Sécurité fonctionnelle selon IEC 61508 , édition 2000:
Standard de la sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité électronique.

L'évaluation du matériel a été réalisée par Analyse des Modes de défaillance de leurs Effets et de leur Criticité (CEI 60812 – Edition 2 - 2006)
permettant de déterminer la proportion de défaillances en sécurité (SFF) de l'appareil

L'AMDEC s'appuie sur le recueil de données de fiabilité - Modèle universel pour le calcul de la fiabilité prévisionnelle des composants (CEI 62380 - 2004) et sur les données constructeur.

1.4 Information constructeur

LOREME SAS
12, rue des potiers d'étain 57071 Actipole Metz Borny
www.loreme.fr

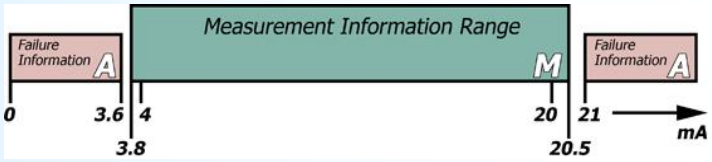
2 Fonction et état de sécurité

2.1 Fonction de sécurité

La fonction de sécurité de l'appareil est remplie, aussi longtemps que la sortie (4 ... 20 mA) reproduit l'image de la mesure d'entrée avec une tolérance de +/-2%. La plage de bon fonctionnement du signal de sortie s'étend de 3.8 mA à 20.5 mA.

2.2 Position de repli de sécurité (suivant NAMUR NE 43)

L'état de repli de sécurité est défini par un courant de sortie hors de la gamme 3,6mA à 21mA.
• Soit un courant de sortie =< 3,6 mA
• Soit un courant de sortie >= 21 mA



L' application devra impérativement être configurée pour détecter toute valeur de courant hors gamme (=< 3,6 mA et >= 21 mA) et les considérés « Invalides ». De ce fait, dans l'étude AMDEC, cet état est considéré comme **non dangereux**.
Le temps de réaction pour toutes les fonctions de sécurité est < 200 ms.

AVERTISSEMENT ! La valeur de repli étant librement programmable, il appartient à l'installateur de vérifier la compatibilité avec la sécurité du process (valeur de repli programmé en sortie usine : 21 mA)

3 Recommandation de sécurité

3.1 Interfaces

Le dispositif est doté des interfaces suivantes:

• les interfaces de sécurité : entrée température, sortie analogique

• interfaces non de sécurité : communication HART (diagnostique et configuration), Liaison série RS232 (configuration de l'appareil), l'afficheur local

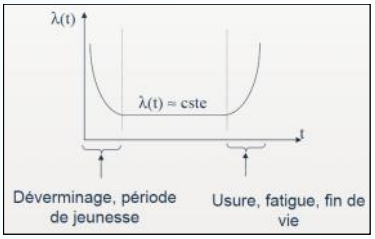
La communication HART n'est pas pertinente pour la sécurité fonctionnelle, la perte de communication est considérée comme étant détectée par l'application, de ce fait, dans l'étude AMDEC, cet état est considéré comme non dangereux.

3.2 Configuration / étalonnage

la configuration de l'appareil est nécessaire pour définir son mode de fonctionnement (type d'entrée, échelle de mesure, valeur de repli) se reporter au manuel de configuration.
le réétalonnage n'est possible que par retour usine. Aucune modification ne doit être effectué sur le module!

3.3 Durée de vie utile

Evolution du taux de défaillance



Bien qu'un taux de défaillance constant est assumé par l'estimation probabiliste, celui ci ne s'applique que pour la durée de vie utile des composants.
Au-delà de cette durée de vie utile, la probabilité de défaillance s'accroit de manière significative avec le temps.
La durée de vie utile est très dépendante des composants eux même et des conditions de fonctionnement tel que la température, en particulier.
(les condensateurs électrolytiques sont très sensibles à la température de travail)

Cette hypothèse d'un taux de défaillance constant est basée sur la courbe en forme de baignoire, qui montre le comportement typique des composants électroniques.
Par conséquent, la validité de ce calcul est limité à la durée de vie utile de chaque composant.
Il est présumé que les défaillances précoces sont détectées pour un très fort pourcentage durant la période de déverminage constructeur et au cours de la période d'installation, l'hypothèse d'un taux de défaillance constant pendant la durée de vie utile reste donc valide.
selon la CEI 61508-2, une durée de vie utile, fondée sur le retour d'expérience, doit être prise en considération.
L'expérience a montré que la durée de vie utile est comprise entre 15 et 20 ans, et peut être plus élevé si il n'y a pas de composants a durée de vie réduite dans les fonctions de sécurité (tels que condensateurs électrolytique, relais, mémoire flash, optocoupleur) et si la température ambiante est nettement inférieure à 60 °C.

Remarque :

La durée de vie utile correspond au taux de défaillance aléatoire constant de l'appareil.
La durée de vie effective peut être plus élevée.
L'intégrateur devra s'assurer que le module n'est plus nécessaire à la réalisation de la sécurité avant sa mise au rebut.

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

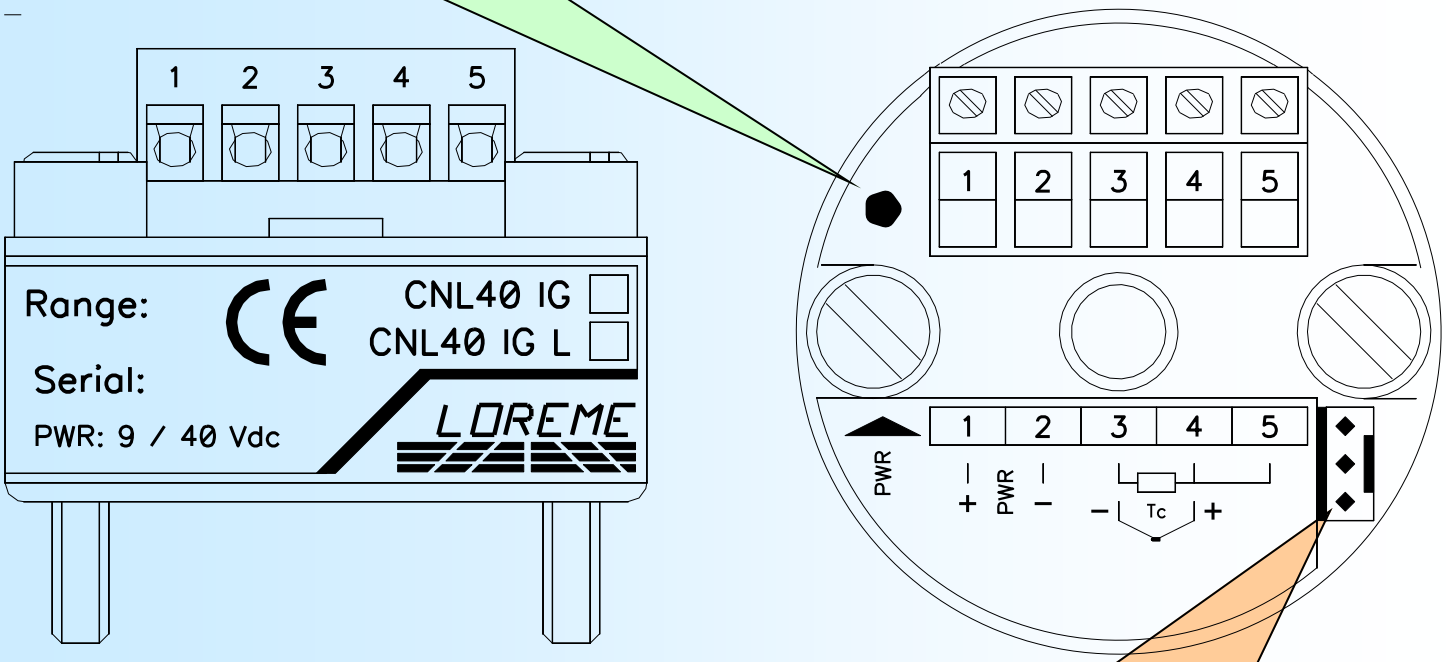
4 Installation , mise en service et remplacement

La capacité de fonctionnement et les courants de signalisation d'erreurs doivent être soumis à un contrôle lors de la mise en service (validation) voir paragraphe : " ***Contrôles périodiques et de mise en service*** "
et à des intervalles adéquats préconisés au paragraphe : " ***Périodicité des contrôles*** "
Tout appareil ne satisfaisant pas le contrôle de mise en service doit être remplacé.

AVERTISSEMENT !
Aucune maintenance utilisateur ne doit être effectuée, un appareil défectueux doit être remplacé par un matériel neuf de même type. Pour un retour en réparation ou un réétalonnage, il est d'une très grande importance que tous les types de défaillances de l'équipement soit signalées en vue de permettre à l'entreprise de prendre des mesures correctives afin de prévenir les erreurs systématiques.

4.1 Descriptif convertisseur de mesure incorporé dans L'INP101

Led jaune traversée par le courant de sortie, signale que la boucle de sortie est fermée et alimentée. (circulation du courant)
s'éteint lors de l'ouverture de la boucle de sortie permet un contrôle visuel rapide du bon fonctionnement



Embase 3 points (liaison RS232) permet le passage en configuration (n'utiliser que le cordon fourni par LOREME à cet effet) Attention : le passage en mode configuration fige le courant de sortie (arrêt de la mesure durant la configuration) Pour des raisons de sécurité le convertisseur quitte automatiquement le mode configuration après 2 minutes d'inactivités et retourne en mode mesure.
cette liaison est également utilisé pour le raccordement de l'afficheur local dans l'INP101.

4.2 Raccordements électriques et configuration

*** Alimentation et sortie analogique du convertisseur :** borne 1 + et borne 2 -
Le module est protégé contre les inversions de polarité de l'alimentation

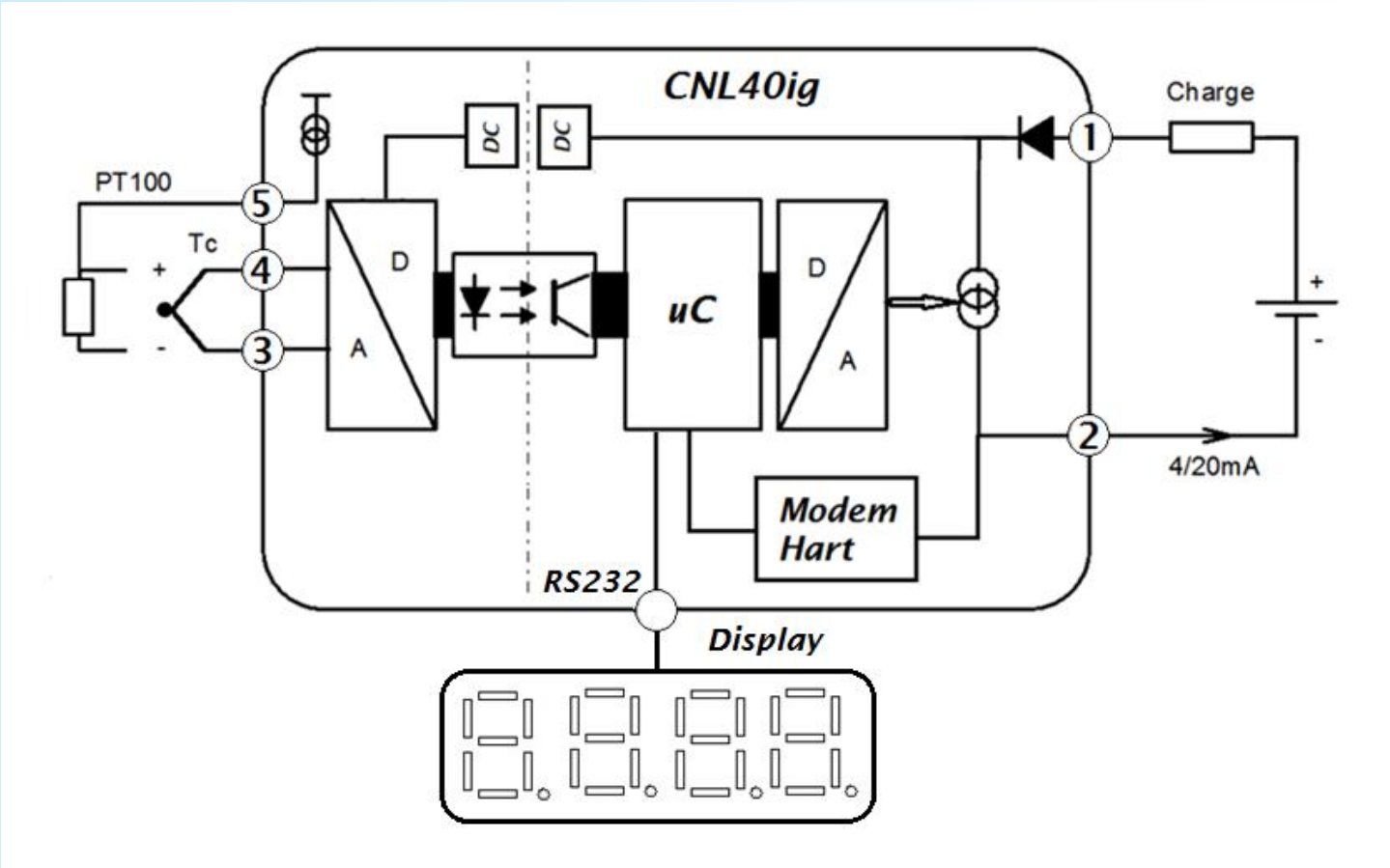
*** Entrée** : deux configuration sont possible , PT100 et thermocouple
- Raccordement en entrée Thermocouple : Tc+ borne 4 ; Tc- borne 3
- Raccordement en entrée PT100 3 fils : fil blanc borne 3 ; les 2 fils rouge en borne 4 et 5

Remarques :
-pour un thermocouple distant, s'assurer que la prolongation soit faite avec du câble d'extension ou de compensation du même type que le thermocouple employé, et de la bonne polarité du câble.
- pour une sonde PT100 distante, s'assurer que le câble de prolongation utilisé dispose de 3 conducteurs de même section pour garantir la meilleur compensation de ligne.
- veiller au bon choix du type de capteur dans la configuration
- l'échelle de température programmé dans l'automate et dans le convertisseur doivent être identique
- la valeur de repli de la sortie analogique doit être programmé < à 3.6mA ou >= à 21mA (21mA sortie usine)

AVERTISSEMENT !

Ne pas dépasser les spécifications de la fiche technique,
pour assurer un fonctionnement sûr de la sortie analogique il faut :
- une tension auxiliaire d'alimentation comprise entre 15 Volts et 40 Volts
- une charge maximum dans la boucle, calculée de sorte que la tension résiduelle aux bornes du convertisseur soit de 15V pour un courant de boucle de 21 mA.
Attention , un dépassement de charge de la boucle 4...20mA peut empêcher le courant de sortie d'atteindre la valeur de repli celui-ci pouvant saturer dans la plage de mesure, et mettre le système dans un état dangereux.

4.3 Schéma typique de raccordement



LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

5 Contrôles périodiques et de mise en service

La procédure de test périodique est définie par LOREME et doit être suivie par l'utilisateur final pour assurer et garantir le niveau SIL dans le temps.
les tests périodiques doivent être réalisés en suivant la procédure définie ci dessous et selon la périodicité définie au paragraphe " ***Périodicité des contrôles*** "

5.1 Procédure de contrôle

Le test périodique permet la détection d'une éventuelle défaillance interne du produit ainsi que l'étalonnage de la boucle.
les conditions d'environnement ainsi qu'un temps de chauffe minimum de 5 minutes doivent être respectés.

Test complet du convertisseur et de la chaîne de traitement du signal *(le système est indisponible pendant le test)*

1. Si nécessaire, contourner le système de sécurité et / ou prendre les mesures appropriées, pour assurer la sécurité durant le test
2. Inspecter l'appareil, absence de dommage visible ou de contamination (oxydation)
3. Insérer un milliampèremètre* dans la boucle de sortie
4. déconnecter le capteur (pt100 ou thermocouple)
5. vérifier que le courant de sortie passe en valeur de repli (<=3.6mA ou >=21mA)
6. connecter un simulateur* à l'entrée du convertisseur (pt100 ou thermocouple) à la place du capteur
7. Simuler les valeurs de température appropriées à l'échelle du convertisseur (sur 5 points : 0%, 25%, 50%, 75%, 100%) et vérifier que le courant de sortie (4..8..12..16..20mA) soit proportionnel à l'entrée à +/-2% près.
8. Débrancher le simulateur et reconnecter le capteur à l'entrée du convertisseur (vérifier que le courant est dans la gamme de mesure)
9. Retirer le milliampèremètre et refermer la boucle de sortie (la Led verte doit être allumée)
10. Après les essais, les résultats doivent être documentés et archivés.

Tout appareil ne satisfaisant pas le contrôle doit être remplacé

*note *: le milliampèremètre et le simulateur doivent être calibré de façon régulière pour ce test (selon l'état de l'art et la bonne pratique)*

5.2 Périodicité des contrôles

Selon le tableau 2 de la CEI 61508-1 le PFDavg , pour les systèmes fonctionnant à faible sollicitation,
doit être ≥ 10^{-3} à <10^{-2} pour les fonctions de sécurité SIL 2 et ≥ 10^{-4} à <10^{-3} pour les fonctions de sécurité SIL 3 .

λ safe detected	λ dangerous detected	λ safe undetected	λ dangerous undetected = PFH	**SFF**
420 FIT	0 FIT	17 FIT	21 FIT	95.4%

conditions : température de 30°C

Valeur du PFDavg **en fonction de la périodicité de test**

T[Proof] **= 1 an**	**T**[Proof] **= 5 ans**	**T**[Proof] **= 10 ans**	**T**[Proof] **= 20 ans**
PFDavg=9.20E^{-05}	**PFD**avg=4.60E^{-04}	**PFD**avg=9.20E^{-04}	**PFD**avg=1.8E^{-03}

approximation : PFDavg = λdangerous x T[Proof] /2 (erreur engendré par l'approximation < 3%)

Les champs marqués en vert signifie que les valeurs calculées du PFDavg sont dans les limites autorisées pour le SIL2

Récapitulatif :

Probabilité de défaut PFD = 9.20 E^{-5} x Tproof [années]

soit pour Tproof = 5 ans , 50 % de SIF en catégorie SIL2

Remarques :

- les intervalles de test doivent être déterminés en fonction du PFDavg requis par l'intégrateur.

- Le SFF, PFDavg et PFH doit être déterminé pour l'ensemble de la fonction instrumentée de sécurité (SIF) en s'assurant que les valeurs de courant hors gamme sont bien détectées au niveau système et qu'elles conduisent effectivement à la position de sécurité.

Transmetteur programmable isolé pour PT100 et thermocouple montage en tête de sonde pyrométrique avec afficheur

DECLARATION CE DE CONFORMITE

REV8
Page 1/1

Aux exigences de protection de la directive 2004/108/CE "Compatibilité ELECTROMAGNÉTIQUE" et aux exigences de la directive 2006/95/CE "BASSE TENSION"

Nous déclarons sous notre seule responsabilité, que le produit :

Désignation: **Convertisseur de température en technique 2 fils**

Type: **INP101** avec transmetteur CNL40igH incorporé

N° de révision : 2 date : 16/12/2008

CE

est conforme aux normes génériques ou spécifiques harmonisées suivantes :

NORMES GENERIQUES :	Test Réalisé	NORMES FONDAMENTALES :	
(SECURITE) : directive 2006/95/CE " BASSE TENSION "			
	X	EN 61010-1	Règle de sécurité pour les appareils électriques de mesurage, de régulation et de laboratoire
NF EN 61000-6-4 Mars 2007 Compatibilité électromagnétique (CEM) - Partie 6-4 : normes génériques - Norme sur l'émission pour les environnements industriels			
	X	EN 55011 Class A	émission rayonnée et émission conduite sur l'alimentation à courant alternatif.
NF EN 61000-6-2 Janvier 2006 Compatibilité électromagnétique (CEM) - Partie 6-2 : normes génériques - Immunité pour les environnements industriels			
	X	EN 61000-4-2	décharges électrostatiques.
	X	EN 61000-4-4	transitoires rapides.
	X	EN 61000-4-5	ondes de choc 1,2/50 (5/20) µs.
	X	EN 61000-4-8	champ magnétique à la fréquence du réseau.
	na	EN 61000-4-11	creux de tension et coupures brèves de tension.
	X	EN 61000-4-3	champ électromagnétique RF modulé en amplitude.
	X	EN 61000-4-6	fréquence radio en mode commun modulée en amplitude.

Metz, le : 16/12/2008

Signé au nom de LOREME ; M. Dominique Curulla

Année d'apposition du marquage CE : 2008

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Technique@Loreme.fr

Annexe 1 : CONSEILS RELATIFS A LA CEM

1) Introduction:

Pour satisfaire à sa politique en matière de CEM, basée sur la directive communautaire 89/336/CE,
la société LOREME prend en compte les normes relatives à cette directive dès le début de la conception de chaque produit.
L'ensemble des tests réalisés sur les appareils, conçus pour travailler en milieu industriel, le sont aux regards des normes
EN 50081-2 et EN 50082-2 afin de pouvoir établir la déclaration de conformité.
Les appareils étant dans certaines configurations types lors des tests,
il est impossible de garantir les résultats dans toutes les configurations possibles.
Pour assurer un fonctionnement optimal de chaque appareil il serait judicieux de respecter certaines préconisations d'utilisation.

2) Préconisation d'utilisation:

2.1) Généralité:

- Respecter les préconisations de montage (sens de montage, écart entre les appareils ...) spécifiés dans la fiche technique.
- Respecter les préconisations d'utilisation (gamme de température, indice de protection) spécifiés dans la fiche technique.
- Eviter les poussières et l'humidité excessive, les gaz corrosifs, les sources importantes de chaleur.
- Eviter les milieux perturbés et les phénomènes ou éléments perturbateurs.
- Regrouper, si possible, les appareils d'instrumentation dans une zone séparée des circuits de puissance et de relayage.
- Eviter la proximité immédiate avec des télé-rupteurs de puissance importante, des contacteurs, des relais, des groupes de puissance à thyristor ...
- Ne pas s'approcher à moins de cinquante centimètres d'un appareil avec un émetteur (talkie-walkie) d'une puissance de 5 W, car celui-ci crée un champs d'une intensité supérieur à 10 V/M pour une distance de moins de 50 cm.

2.2) Alimentation:

- Respecter les caractéristiques spécifiées dans la fiche technique
(tension d'alimentation, fréquence, tolérance des valeurs, stabilité, variations ...).
- Il est préférable que l'alimentation provienne d'un dispositif à sectionneur équipé de fusibles pour les éléments d'instrumentation, et que la ligne d'alimentation soit la plus direct possible à partir du sectionneur. Eviter l'utilisation de cette alimentation pour la commande de relais, de contacteurs, d'électrovannes , ...
- Si le circuit d'alimentation est fortement parasité par la commutation de groupes statiques à thyristors, de moteur, de variateur de vitesse, ... il peut être nécessaire de monter un transformateur d'isolement prévu spécifiquement pour l'instrumentation en reliant l'écran à la terre.
- Il est également important que l'installation possède une bonne prise de terre, et préférable que la tension par rapport au neutre n'excède pas 1V, et que la résistance soit intérieure à 6 ohms.
- Si l'installation est située à proximité de générateurs haute fréquence ou d'installations de soudage à l'arc, il est préférable de monter des filtres secteur adéquats.

2.3) Entrées / Sorties:

- Dans un environnement sévère, il est conseillé d'utiliser des câbles blindés et torsadés dont la tresse de masse sera reliée à la terre en un seul point.
- Il est conseillé de séparer les lignes d'entrées / sorties des lignes d'alimentation afin d'éviter les phénomènes de couplage.
- Il est également conseillé de limiter autant que possible les longueurs de câbles de données.

DECLARATION DE CONFORMITE

La société LOREME déclare sous sa seule responsabilité, que le produit :

Désignation: **Convertisseur de température en technique 2 fils**

Type: **INP101** avec transmetteur CNL40igH incorporé

N° de révision : 2 date : 16/12/2008

Peut être utilisé pour les applications de sécurité fonctionnelle jusqu'à SIL2 selon la Norme IEC61508-2 : 2000 en respectant les consignes de sécurité spécifiées dans le manuel de sécurité.

L'évaluation des défaillances aléatoires et dangereuses pour la sécurité donne les valeurs suivante:

Appareil avec composants du type B , tolérance aux pannes matérielles HFT = 0
valeurs pour le convertisseur seul (cas le plus défavorable)

λ safe detected	**λ** dangerous detected	λ safe undetected	λ dangerous undetected = PFH	**SFF (1)**	**PFD**avg **T**[Proof] **= 1 an**	**PFH**
420 FIT(2)	0 FIT(2)	17 FIT(2)	21 FIT(2)	95.4%	$9.20E^{-05}$	$2.1E^{-08}$ 1/h

(1) selon AMDEC CNL40igH rev2 *établi avec "ALD MTBF calculator" : http://www.aldservice.com/*
(2) FIT = Failure rate (1/h)

Le manuel de sécurité donne les probabilités de défaillance des capteurs associés (pt100 et thermocouple) pour permettre l'évaluation d'une boucle complète.

Metz, le : 26/08/14

Signé au nom de LOREME ; M. Dominique Curulla

Transmetteur INP101 avec convertisseur CNL40igH rev2 incorporé

AMDEC Détaillée

Contexte

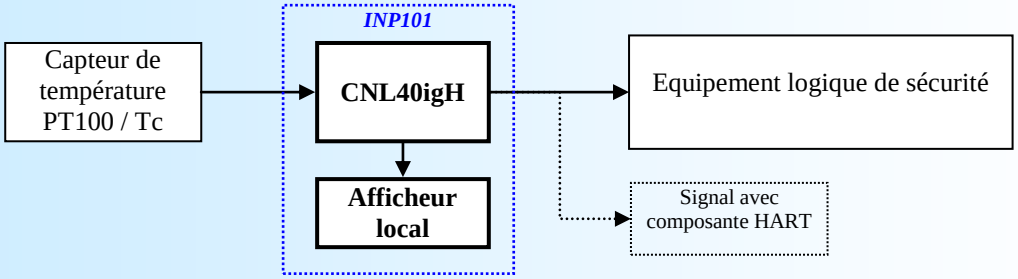
Ce document est l'Analyse des Modes de Défaillance, de leur Effet et de leur Criticité (AMDEC) du composant CNL40igH incorporé dans l'INP101 de la société LOREME.
Outre la caractérisation des informations nécessaires pour la sûreté de fonctionnement (en particulier pour les calculs de disponibilité et 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.

Circonstances de l'analyse

Cette étude a été réalisée dans le but de vérifier l'aptitude du convertisseur CNL40igH à être utilisé dans des applications de sécurité SIL2

Périmètre de l'analyse

Le composant concerné comprend un ensemble de composants électroniques faisant l'acquisition de signaux d'entrée issus de capteurs de température et restituant un signal de sortie analogique (4..20mA) avec ou sans la composante HART.
Généralement, un convertisseur est interfacé entre un capteur et un équipement de protection, désigné « Equipement logique de sécurité»



Caractérisation du composant

Le convertisseur CNL40igH est un sous-système de type « B » [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.

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.

SFF [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 λS plus les défaillances dangereuses détectées λDD sur la somme des probabilités de défaillances fonctionnelles total du sous-système (ensemble des « défaillances en sécurité » λS et des « défaillances dangereuses » λD).

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

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.

Analyse fonctionnelle

Le convertisseur se compose :
d'un étage d'entrée convertisseur analogique numérique
d'un étage d'isolation (alimentation du CAN et de transmission du signal)
d'un microcontrôleur (linéarisation et mise à l'échelle du signal et communication Hart)
d'un étage de sortie (amplificateur de courant)
et d'un modulateur / démodulateur pour signal Hart

Définition de l'évènement redouté

Pour le convertisseur **CNL40igH,** 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.

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
La valeur de repli du convertisseur CNL40igH devra impérativement être programmé pour l'une de ces valeurs.
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 et >= 21 mA) et les considérées « Invalides ».
De ce fait, dans l'étude AMDEC, cet état est considéré comme non dangereux.

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) ;
- des erreurs humaines en fonctionnement ou en maintenance,
(des précautions sont prises pour les éviter : telles que 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.

Taux de défaillance

Ci après les taux de pannes élémentaires des composants du convertisseur CNL40IGH,
pour une température au voisinage des composants de 30°C: (2 pages suivantes)

Transmetteur programmable isolé pour PT100 et thermocouple montage en tête de sonde pyrométrique avec afficheur

AMDEC CNL40ig rev2

Etabli avec "ALD MTBF calculator" : http://www.aldservice.com/

				selon IEC6-2380		répartition		λf = 1/MTBF				
								λfd		λfnd		
Count	RefDes	Pattern-Name	Value	λf (fit)	type	ratio	λf (fit)	λsd	λdd	λsnd	λdnd	effet
1	XC174	1206	0	0,02	co	100%	0,020	0,020				repli sortie > 21 mA
1	73	1206	1M 1% 50ppm	0,21	co	40%	0,084			0,084		drift sortie < 2%
					drift	60%	0,126			0,126		drift sortie < 2%
4	76	1206	1u X7R	0,21	co	30%	0,063			0,063		sans influence découplage vref
					cc	70%	0,147	0,147				repli sortie > 21 mA (vref=0)
	163	1206	1u X7R	0,21	co	30%	0,063			0,063		sans influence découplage modem hart
					cc	70%	0,147	0,147				plus de communication Hart
	XC169	1206	1u X7R	0,21	co	30%	0,063			0,063		plus de passe bas ligne
					cc	70%	0,147	0,147				plus de mesure de ligne (err < 2%)
	XC171	1206	1u X7R	0,21	co	30%	0,063			0,063		plus de passe bas entrée
					cc	70%	0,147				0,147	en tc non detecté / en pt rupture capteur
1	XC172	1206	2k5 1% 50ppm	0,02	co	40%	0,008				0,008	en tc non detecté / en pt rupture capteur
					drift	60%	0,012				0,012	dérive mesure (référence)
3	96	1206	2n2 NPO	0,07	co	10%	0,007			0,007		perte filtre reception Hart
					cc	70%	0,049	0,049				plus de communication Hart
					drift	20%	0,014			0,014		altération filtre Hart
	97	1206	2n2 NPO	0,07	co	10%	0,007	0,007				plus de communication Hart
					cc	70%	0,049	0,049				plus de communication Hart
					drift	20%	0,014			0,014		altération filtre Hart
	100	1206	2n2 NPO	0,07	co	10%	0,007			0,007		pas de filtre HF boucle 4..20 mA
					cc	70%	0,049	0,049				courant sortie > 21 mA (court circuit)
					drift	20%	0,014			0,014		sans influence
2	XC170	1206	5k 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie > 21 mA rupture capteur
					drift	60%	0,012			0,012		sans influence
	XC177	1206	5k 1% 50ppm	0,02	co	40%	0,008				0,008	mesure flottante
					drift	60%	0,012			0,012		sans influence
2	84	1206	7k5 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie < 3.6 mA
					drift	60%	0,012				0,012	dérive sortie
	XC166	1206	7k5 1% 50ppm	0,02	co	40%	0,008	0,008				rupture en PT / sans influence en tc
					drift	60%	0,012				0,012	dérive en pt / sans influence en tc
3	74	1206	10k 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie < 3.6 mA
					drift	60%	0,012				0,012	dérive sortie
	79	1206	10k 1% 50ppm	0,02	co	40%	0,008	0,008				plus de configuration RS232
					drift	60%	0,012			0,012		sans influence
	95	1206	10k 1% 50ppm	0,02	co	40%	0,008	0,008				plus de communication Hart
					drift	60%	0,012			0,012		sans influence
1	81	1206	10M 1% 100ppm	0,02	co	40%	0,008				0,008	plus de détection rupture tc
					drift	60%	0,012			0,012		sans influence
1	99	1206	23.7 1% 50ppm	0,02	co	40%	0,008	0,008				repli sortie < 3.6 mA
					drift	60%	0,012			0,012		dérive < 2%
1	83	1206	47u X7R	0,21	co	30%	0,063			0,063		plus de découplage uC
					cc	70%	0,147	0,147				repli sortie < 3.6 mA
2	67	1206	50k 1% 50ppm	0,02	co	40%	0,008	0,008				rupture capteur (ref à 0)
					drift	60%	0,012				0,012	dérive mesure (référence)
	78	1206	50k 1% 50ppm	0,02	co	40%	0,008	0,008				risque altération com RS232
					drift	60%	0,012			0,012		sans influence
4	77	1206	100n X7R	0,21	co	30%	0,063				0,063	ondulation courant de sortie
					cc	70%	0,147	0,147				repli sortie < 3.6 mA
	103	1206	100n X7R	0,21	co	30%	0,063			0,063		plus de decouplage AD
					cc	70%	0,147	0,147				rupture capteur AD plus alimenté
	105	1206	100n X7R	0,21	co	30%	0,063			0,063		plus de découplage XTR116
					cc	70%	0,147	0,147				courant sortie > 21 mA (court circuit)

Transmetteur programmable isolé pour PT100 et thermocouple montage en tête de sonde pyrométrique avec afficheur

AMDEC CNL40ig rev2

				selon IEC6-2380		répartition		λf = 1/MTBF				
								λfd		λfnd		
Count	RefDes	Pattern-Name	Value	λf (fit)	type	ratio	λf (fit)	λsd	λdd	λsnd	λdnd	effet
	107	1206	100n X7R	0,21	co	30%	0,063	0,063				plus de découplage ref modem Hart, perte com
					cc	70%	0,147	0,147				plus de tension de ref modem Hart, perte com
2	98	1206	250k 1% 50ppm	0,02	co	40%	0,008	0,008				perte polarisation entrée modem hart, perte com
					drift	60%	0,012			0,012		sans influence
	106	1206	250k 1% 50ppm	0,02	co	40%	0,008	0,008				perte polarisation entrée modem hart, perte com
					drift	60%	0,012			0,012		sans influence
1	XC183	1206	500 1% 50ppm	0,02	co	40%	0,008	0,008				plus d'alimentation etage d'entrée rupture capteur
					drift	60%	0,012			0,012		sans influence
1	8	DC/DC 1W	LME1212S	286,00	co	50%	143,000	143,000				plus d'alimentation etage d'entrée rupture capteur
					cc	50%	143,000	143,000				plus d'alimentation etage d'entrée rupture capteur
1	13	LEDC-MSDUAL	LED	2,00	co	20%	0,400				0,400	risque dépassement charge en sortie
					cc	80%	1,600	1,600				plus d'alimentation etage d'entrée rupture capteur
1	2	MSOP10	LTC2402	37,00	out gnd	50%	18,500	18,500				rupture capteur plus de signal AD
					out vcc	50%	18,500	18,500				rupture capteur plus de signal AD
1	16	QFN20 0.65	DS8500	2,00	out gnd	50%	1,000	1,000				plus de communication Hart
					out vcc	50%	1,000	1,000				plus de communication Hart
1	1	QUARTZ HC49 CMS	3.6864 Mhz	5,00	cc	50%	2,500	2,500				plus de communication Hart
					co	50%	2,500	2,500				plus de communication Hart
1	6	SC70	TMP05	37,00	out gnd	33%	12,210	12,210				plus de t° de comensation
					out vcc	33%	12,210	12,210				plus de t° de comensation
						34%	12,580				12,580	dérive mesure erreur compensation
1	75	SO8	385 2v5	15,00	co	50%	7,500				7,500	dérive mesure alim AD non défini
					cc	50%	7,500	7,500				rupture capteur AD plus alimenté
1	18	SO8	ADuM1100A	12,00	out gnd	50%	6,000	6,000				rupture capteur plus de signal AD
					out vcc	50%	6,000	6,000				rupture capteur plus de signal AD
1	69	SO8	XTR116	19,00	out gnd	50%	9,500	9,500				repli sortie > 21 mA
					out vcc	50%	9,500	9,500				repli sortie < 3.6 mA
2	148	SOD8	4148	10,00	co	20%	2,000	2,000				repli sortie < 3.6 mA (ouverture boucle)
					cc	80%	8,000			8,000		sans influence, plus de protection inversion polarité
	149	SOD8	4148	10,00	co	20%	2,000	2,000				plus d'alimentation modem Hart, perte com
					cc	80%	8,000			8,000		tension modem Hart hors spécifications
1	5	SSOP28-0.65	16F886	20,00	outgnd	50%	10,000	10,000				repli sortie < 3.6 mA
					out vcc	50%	10,000	10,000				repli sortie > 21 mA
								420,029	0,000	16,827	20,774	
			somme fit :	457,63			457,63	(verif)		SFF=	95,46%	
			MTBF =	2 185 171	Hrs					DC=	91,78%	

LOREME 12, rue des Potiers d'Etain - 57071 Metz ☎ 03.87.76.32.51 - Fax 03.87.76.32.52 - Email: Commercial@Loreme.fr - Techni-

Annexe 2 :
Utilisation des données de L'AMDEC et information complémentaire sur les capteurs de température.

Le convertisseur de mesure CNL40igH raccordé à un capteur de température dans une canne pyrométrique devient un assemblage. Par conséquent, lors de l'utilisation des résultats de l'AMDEC dans une évaluation SIL,
le taux de défaillance des capteurs (pt100 ou thermocouple) doit être pris en considération pour le calcul de la fonction instrumentée de sécurité (SIF)
Ci-dessous le récapitulatif des modes de défaillance et leur fréquence pour les PT100 et les thermocouples en fonction du type de raccordement et de l'environnement dans lequel ils sont utilisés.

Taux de défaillance typiques de thermocouples et PT100 avec fils d'extension (capteur déporté)

type d'élément de mesure	taux de défaillance (FIT)
thermocouple en environnement de faible stress	1000
thermocouple en environnement de stress élevé	20000
Pt100 montage 2/3 fils en environnement de faible stress	475
Pt100 montage 2/3 fils en environnement de stress élevé	9500
Pt100 montage 4 fils en environnement de faible stress	500
Pt100 montage 4 fils en environnement de stress élevé	10000

Taux de défaillance typiques de thermocouples et PT100 sans fils d'extension (capteur avec transmetteur incorporé)

type d'élément de mesure	taux de défaillance (FIT)
thermocouple en environnement de faible stress	100
thermocouple en environnement de stress élevé	2000
Pt100 montage 2/3 fils en environnement de faible stress	48
Pt100 montage 2/3 fils en environnement de stress élevé	960
Pt100 montage 4 fils en environnement de faible stress	50
Pt100 montage 4 fils en environnement de stress élevé	1000

Répartition typique des modes de défaillance pour les thermocouples

Type de défaillance	Avec fils d'extension	Raccordement direct Sans extension
Circuit ouvert	90%	95%
Court circuit	5%	4%
Dérive *	5%	1%

** le phénomène de dérive des thermocouples est essentiellement du au vieillissement*

Répartition typique des modes de défaillance pour les sonde PT100

Type de défaillance	Avec fils d'extension	Raccordement direct Sans extension
Circuit ouvert	78%	79%
Court circuit	2%	3%
Dérive	20%	18%

La répartition du taux de défaillance dépend légèrement du type de raccordement des pt100 (2,3,4 fils)

les conditions de stress sont : des vibrations importantes sur le process et ou des cycles fréquent de température, ces phénomènes pouvant causer des fissures du substrat et des ruptures de soudure sur les fils de raccordement.

Annexe 3 : termes et définitions.

SIL signifie “Security Integrity Level”, c’est-à-dire le niveau d’intégrité de la sécurité. La notion de SIL a été introduite dans la norme IEC61508 et elle est reprise dans les normes dérivées de l’IEC61508, telles que la norme IEC61511 relative aux systèmes instrumentés de sécurité (SIS) pour les process et l’IEC62061 pour les systèmes de sécurité à électronique programmable pour les machines.
Lorsque l’on veut réaliser une installation de sécurité, il faut commencer par évaluer le risque (sa dangerosité, sa fréquence d’occurrence), ce qui conduit à définir les exigences de sécurité que l’on attends du SIS, c’est-à-dire son SIL.
En définitive, le SIL définit le niveau de fiabilité du SIS. Il existe deux manières de définir le SIL, selon que le système de sécurité fonctionne en mode de faible sollicitation ou si au contraire s’il fonctionne en continu ou à forte sollicitation. Il existe 4 niveaux de SIL (notés SIL1 à SIL4) plus le SIL est élevé, plus la disponibilité du système de sécurité est élevée.
Pour les **systèmes de sécurité fonctionnant en mode de faible sollicitation**,
on parle de probabilité moyenne de défaillance sur sollicitation PFD_{avg} (Probability of Failure on Demand) sur une période de 10 ans.
La relation entre les niveaux SIL et le PFDavg est la suivante :
SIL 4 : PFDavg compris entre 10^{-5} et 10^{-4}
SIL 3 : PFDavg compris entre 10^{-4} et 10^{-3}
SIL 2 : PFDavg compris entre 10^{-3} et 10^{-2}
SIL 1 : PFDavg compris entre 10^{-2} et 10^{-1}
Pour les **systèmes de sécurité fonctionnant en mode de sollicitation élevée,** on parle de PFH, probabilité de défaillance dangereuse par heure. La relation entre les niveaux SIL et le PFH est la suivante :
SIL 4 : PFH compris entre 10^{-9} et 10^{-8}
SIL 3 : PFH compris entre 10^{-8} et 10^{-7}
SIL 2 : PFH compris entre 10^{-7} et 10^{-6}
SIL 1 : PFH compris entre 10^{-6} et 10^{-5}

Échelle des niveaux SIL

	Sollicitations du SIS		
SIL*	rares PFD**	fréquentes PFH***	Facteur de réduction du risque
4	$\geq 10^{-5}$ à $< 10^{-4}$	$\geq 10^{-9}$ à $< 10^{-8}$	10 000 à 100 000
3	$\geq 10^{-4}$ à $< 10^{-3}$	$\geq 10^{-8}$ à $< 10^{-7}$	1 000 à 10 000
2	$\geq 10^{-3}$ à $< 10^{-2}$	$\geq 10^{-7}$ à $< 10^{-6}$	100 à 1 000
1	$\geq 10^{-2}$ à $< 10^{-1}$	$\geq 10^{-6}$ à $< 10^{-5}$	10 à 100

*Safety Integrity level, niveau d'intégrité de la sécurité
**Probability of Failure on low Demand, probabilité d'avoir une défaillance (pour réaliser la fonction de sécurité prévue) au moment d'une sollicitation
***Probability of a dangerous Failure per Hour ou Probability of Failure on High demand, probabilité d'une défaillance dangereuse par heure

Abréviation	Description
HFT	Tolérance matérielle ; capacité d'un module fonctionnel de continuer l'exécution d'une fonction sollicitée en présence d'erreurs
MTBF	Temps moyen entre deux défaillances
MTTR	Temps moyen entre la survenance d'une erreur dans un appareil ou un système et la réparation
PFD	Probabilité de défaillances menaçantes d'une fonction de sécurité en cas de sollicitation
PFDavg	Probabilité moyenne de défaillances menaçantes d'une fonction de sécurité en cas de sollicitation
SIL	Safety Integrity Level (niveau d'intégrité de sécurité) ; la norme internationale IEC 61508 définit quatre Safety Integrity Level (SIL1 à SIL4). Chaque niveau correspond à une plage de probabilité pour la défaillance d'une fonction de sécurité. Plus le Safety Integrity Level des systèmes de sécurité est élevé, plus la probabilité qu'ils n'exécutent pas les fonctions de sécurité sollicitées est faible.
SFF	Partie de défaillances non dangereuses, partie de défaillances ne présentant pas de potentiel pour mettre le système de sécurité dans un état de fonctionnement dangereux ou inadmissible.
TProof	Contrôle répétitif permettant de détecter des défaillances dans un système de sécurité.
XooY	Classification et description du système de sécurité en termes de redondance et de procédé de sélection appliqué. "Y" indique la fréquence à laquelle la fonction de sécurité est exécutée (redondance). "X" détermine le nombre de canaux qui doivent fonctionner correctement.
λsd et λsu	λsd Safe detected et λsu Safe undetected Taux de défaillance ne présentant aucun danger . Une défaillance ne présentant aucun danger (safe failure) est donnée quand le système de mesure passe à l'état sûr défini ou au mode de signalisation d'erreurs sans sollicitation émanant du procédé.
λdd et λdu	λdd Dangerous detected et λdu Dangerous undetected Taux de défaillance dangereuse généralement, une défaillance dangereuse est donnée quand le système de mesure est mis dans un état dangereux ou entravant le fonctionnement.
λdu	λdu Dangerous undetected Une défaillance dangereuse non détectée est donnée lorsque le système de mesure ne passe ni à l'état sûr défini, ni au mode de signalisation d'erreurs en cas de sollicitation émanant du procédé.