MTS SENSORS

Temposonics®

Capteurs de position linéaire magnétostrictif

TH – Conforme SIL 2
Manuel De Sécurité

Table des matières

1. Introduction

Ce manuel donne à l'utilisateur des consignes d'installation électriques et d'utilisation pour les modèles série T Temposonics® à sortie analogique dans les applications de sécurité. Le modèle série T est certifié SIL (Safety Integrity Level, ou Niveau d'intégrité de sécurité) 2 conformément à l'IEC 61508.

IEC 61508	Sécurité fonctionnelle des systèmes de sécurité électriques/électroniques et électroniques programmables

2. Analyse des risques

IEC 61508 SIL	$MTTF_d$	Mode de demande élevée PFH
3	élevé, 30 < 100 ans	$\geq 10^{-8}$ à $< 10^{-7}$
2	intermédiaire, 10 < 30 ans	$\geq 10^{-7}$ à $< 10^{-6}$
1	bas, 3 < 10 ans	$\geq 10^{-6}$ à $< 10^{-5}$
Aucune exigence particulière	-x–x-	$\geq 10^{-5}$ à$< 10^{-4}$

Fig. 1 : Probabilité de défaillance dangereuse

3. Conception du système

3.1 Conception redondante sans diagnostic interne

Une conception redondante comporte deux capteurs, chacun muni d'une sortie indépendante (fonctionnement à sortie inversée). La validation du fonctionnement est effectuée par comparaison croisée, la sortie correcte de deux signaux d'un capteur étant définie par :

Z = CH (A) + CH (–B) = 0
avec : Z = résultat de la comparaison croisée
CH (A) = sortie du signal de position
CH (–B) = sortie du signal de position inversé

Si ce résultat nécessaire n'est pas reçu, le contrôleur interprète cela comme une défaillance du système et le place en arrêt d'urgence.

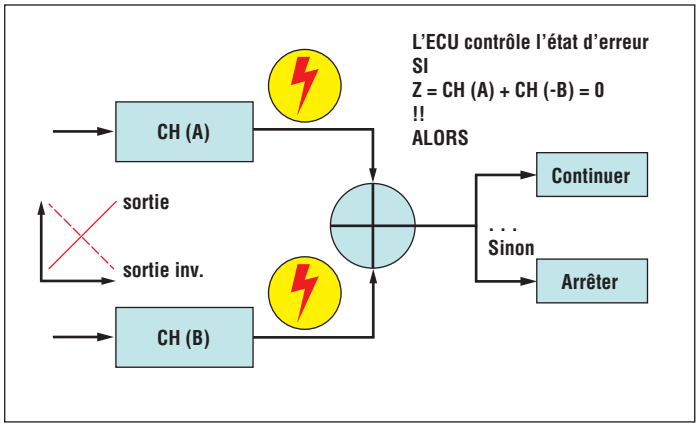

Fig. 2 : Conception redondante sans diagnostic

Sans diagnostics internes des canaux, le système est incapable de détecter le canal défaillant. Le contrôleur est occupé par l'algorithme de comparaison et sa capacité de traitement est réduite.

3.2 Conception redondante avec diagnostic interne

Les capteurs à capacité d'autodiagnostic interne permettent un message de défaillance indépendant de la boucle de traitement du contrôleur. Le capteur se mettra de lui-même en état de sécurité.

Dans ce cas, le contrôleur peut séparer les canaux et le système peut passer en mode de fonctionnement sûr, où la machine peut continuer à fonctionner sur un canal jusqu'à ce que le capteur défaillant soit remplacé.

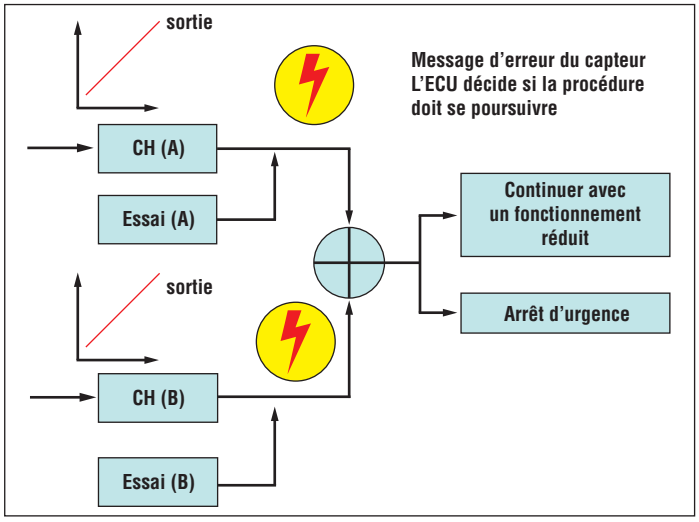

Fig. 3 : Conception redondante avec diagnostic

3.3 La fonction de sécurité

Le capteur série T Sécurité émettra continuellement un signal de position proportionnel à la position de l'aimant, et la fonction de diagnostic interne contrôlera les paramètres de sécurité pertinents dans le matériel. En cas de défaillance, le capteur émettra un signal d'erreur en sortie. L'unité de commande (ECU) reçoit les signaux émis. En cas de défaillance, l'ECU doit réagir de manière appropriée afin de gérer la fonction d'urgence. Le système s'arrêtera ou fonctionnera en mode d'urgence.

Série T Analogique Sécurité	
Sortie de courant	4…20 mA
Sortie d'erreur	< 3,6 mA (près de 0 mA)

Fig. 4 : Fonction de sortie de la série T

Types de défaillances

1. Défaillances sûres (λ_{SD} et λ_{SU}) détectées et non détectées
2. Défaillances dangereuses (λ_{DD} et λ_{DU}) détectées et non détectées IEC 60079-14 et réglementation locale.

Type de défaillances (λ) dans les systèmes de sécurité		
État de défaillance	**Détectée**	**Non détectée**
État de sécurité	λ_{SD} sûre détectée	λ_{SU} sûre non détectée
	Le capteur fonctionnera sans commande du contrôleur à l'état sûr.	
Défaillance dangereuse	λ_{DD} dangereuse détectée : le capteur fonctionne dans un état dangereux (= fonction inopérante)	λ_{DU} dangereuse non détectée : le capteur n'est pas capable de se retrouver dans un état sûr ou defini.

Fig. 5 : Types de défaillances

4. Remarques propres au dispositif

4.1 Détermination et usage prévu/certification

Le modèle série T Sécurité est un capteur de position linéaire magnétostrictif certifié conformément à l'IEC 61508 pour une entrée unique dans les systèmes instrumentés de sécurité SIL 2 en mode de demande faible et en mode de demande élevée. Le capteur mesure la position relative d'un aimant en déplacement par rapport à son ZÉRO. Le signal de sortie est transmis à un contrôleur externe (ECU) et traité conformément à ses exigences.

4.2 Installation mécanique et électrique

Aucune exigence particulière ou supplémentaire d'installation du capteur n'existe outre les pratiques d'installation normales documentées dans le manuel d'utilisation de la série T. Les spécifications de fonctionnement pour l'environnement sont applicables telles que publiées dans la section des spécifications du manuel d'utilisation de la série T (document n° 551513).

4.3 Essais de fonctionnement et hors tension

Pour des informations complètes relatives à la performance, à l'installation, à l'utilisation et aux spécifications des modèles série T Sécurité, consultez notre manuel d'utilisation (document n° 551513). Toutes les recommandations normales d'installation telles que documentées dans le manuel d'utilisation pour les capteurs analogiques série T sont applicables. Toutes les configurations sont permises pour les modèles série T Sécurité. Les essais de fonctionnement des circuits de sécurité donneront une indication fiable pour tous les composants utilisés (capteur, contrôleur et actionneur). L'essai relève de la responsabilité de l'utilisateur (l'intervalle de contrôle est de 1 an).

4.4 Maintenance et réparation

Les modèles série T Sécurité ne sont pas réparables sur site ; les réparations du dispositif doivent être réalisées par MTS. Toute défaillance de borne non suivie de 10 démarrages consécutifs sans défaillance de borne doit être signalée. En cas de défaillance, contactez MTS Sensors.

4.5 Modes de fonctionnement illégaux et dangereux

Aucun mode de fonctionnement hors des spécifications données n'est autorisé. Les limites spécifiques sont valides et elles ne doivent pas être dépassées. Le manuel d'utilisation doit tout particulièrement être pris en compte. Aucune modification du firmware n'est autorisée. Si une température de stockage de 93 °C est dépassée, il convient de remplacer le capteur. Afin de s'assurer des valeurs de sécurité de la fig. 7, il convient de remplacer le capteur si la température de fonctionnement dépasse la valeur indiquée.

4.6 Défaillance de cause commune (CCF, Common Cause Failure)

Les problèmes de CCF suivants ont été pris en compte lors de la conception des modèles de capteurs série T et peuvent être utilisés pour l'analyse des CCF du système global :

1. le capteur est protégé contre la surtension, jusqu'à une tension nominale maximale, et le mauvais câblage (VCC – Masse) ;
2. l'AMDEC est disponible et ses résultats ont été pris en compte pour l'analyse des CCF ;
3. les concepteurs de ce capteur ont été formés pour comprendre les causes et les conséquences d'une défaillance de cause commune ;
4. le capteur a été soumis à l'essai pour : la CEM (émission et immunité), les charges mécaniques (par exemple, vibrations, pression), les influences environnementales telles que la pénétration de fluide et la température. Le capteur est compatible au sein de ces environnements et est prévu pour être utilisé dans ces conditions pourvu qu'il reste étanche à la contamination de ces environnements.

4.7 Mesures contre les usages abusifs prévisibles

Les mesures suivantes ont été prises contre les usages abusifs prévisibles de la série T Sécurité :

1. protection complète contre le mauvais câblage du capteur ;
2. instructions détaillées dans le manuel d'utilisation sur les méthodes de prévention de l'endommagement du capteur pendant son installation ;
3. le contrôle du fonctionnement du capteur après l'installation réduira la possibilité d'endommagement non détecté du capteur pendant le processus d'installation.

4.8 Plan d'action en cas de défaillance

En cas de réponse indiquant la défaillance d'une borne du capteur, celui-ci doit fonctionner sans défaillance de borne (c'est-à-dire que le capteur n'émet pas un courant inférieur à 3,6 mA) lors des 10 démarrages consécutifs suivant la réponse de défaillance initiale. Dans le cas contraire, le capteur doit être retourné à MTS Sensors pour inspection.

4.9 Identification du produit

Les capteurs série T sont proposés dans de nombreuses configurations de longueur, type de bride, type de raccordement, type de protection en cas d'atmosphère explosible et sortie. Le numéro de modèle du capteur comprend le caractère "S" à la position 14, pour indiquer l'homologation SIL 2. Toutes les versions munies de l'option "S" de sécurité fonctionnelle sont compatibles SIL 2.

Exemple pour la série T : TxxxxxxxxxxxxSxxxx

5. Série T Analogique Sécurité

5.1 Description fonctionnelle

Le capteur de position série T Analogique Sécurité est de type B conformément à l'IEC 61508, avec une tolérance nulle à la défaillance matérielle. Le capteur effectue des autodiagnostics et passe à un état de sécurité en cas de détection d'une défaillance, indiquant ainsi l'impossibilité de réaliser la fonction de sécurité. Pour que la sortie du capteur soit considérée valide, la valeur doit être dans la plage 3,8…20,5 mA pendant 10 millisecondes consécutives. Si la valeur de sortie du capteur sort de la plage 3,6…21 mA, et se trouve donc dans un état de défaillance, cet état de défaillance doit être considéré présent jusqu'à ce que la sortie soit dans la plage valide pendant 10 millisecondes consécutives. La plage de mesure active est 4…20 mA (pour la course du capteur définie).

Essai de fonctionnement

Les conditions de déclenchement d'une défaillance sont :
- aimant de position manquant ou endommagé ;
- somme de contrôle invalide pour la mémoire des paramètres ;
- somme de contrôle invalide pour la mémoire du programme ;
- défaillance interne du matériel ;
- position de l'aimant hors de la plage de mesure valide.

5.2 Méthode d'essai hors ligne pour contrôler la fonction de sécurité

L'essai hors ligne peut être appliqué pour contrôler la fonction de sécurité du capteur.

Parmi les essais de fonctionnement hors tension recommandés :

la fonction de sécurité du capteur série T Sécurité est contrôlée en interne, mais l'étendue du diagnostic du capteur peut être augmentée en contrôlant le fonctionnement du capteur en externe.

La méthode recommandée de contrôle du fonctionnement de la série T Analogique Sécurité est la suivante :

1. mettre en bypass la fonction de sécurité et prendre les mesures appropriées pour éviter un déclenchement intempestif ;
2. placer le capteur série T à son zéro ;
3. déplacer l'aimant du capteur série T sur toute sa course jusqu'à sa position extrême pour vérifier son amplitude de mouvement ;
4. ramener le capteur série T à son zéro ;
5. effectuer sur le capteur série T une vérification de l'étalonnage en 3 points répartis sur toute la plage de travail ;
6. supprimer le bypass et reprendre le fonctionnement normal.

Toutes les méthodes appliquées et tous les résultats de l'essai doivent être consignés dans un rapport d'essai. En cas d'échec de l'essai de fonctionnement, le dispositif et le système doivent être mis à l'arrêt. Le processus doit être effectué en mode sûr en raison des actions impliquées. Veuillez consulter le document technique valide : manuel d'utilisation (fonctionnement et installation électriques, document nº 551513).

5.3 Tolérance de sécurité

Consultez le manuel d'utilisation de la série T (document nº 551513) pour la précision de fonctionnement du capteur. La précision de sécurité du capteur analogique série T est de 1 % de la course totale. Voici un exemple des calculs nécessaires pour déterminer la position de sécurité maximale de l'aimant du capteur :

Course totale : 80 mm
Vitesse de l'aimant : 100 mm/s
Temps de réponse le plus défavorable : 10 ms

Tolérance de sécurité
= 1 % × 80 mm
= 0,8 mm

Tolérance du temps de réponse (pour le déplacement)
= 100 mm/s × 10 ms
= 1,0 mm

5.4 Certificat et données sur les taux de defaillance calculés

Les taux de panne sont établis à partir de l'AMDEC conformément à l'IEC 61508. Les hypothèses suivantes sont valides :

– le capteur fonctionne en mode de demande faible et en mode de demande élevée ;
– les taux de défaillance des alimentations externes ne sont pas pris en compte ;
– consultez le rapport AMDEC pour les valeurs de SFF et PFD_{avg} mentionnées ;
– en cas de défaillance, le capteur analogique série T passera à un état de sécurité ;
– le contrôleur doit interpréter le signal de défaillance de la bonne manière ;
– les conditions ambiantes respectent les spécifications issues du manuel d'utilisation valide (document nº 551513) ;
– la valeur de PFD est calculée en supposant un intervalle d'essai de 1 an.

Les taux de défaillance supposent que la durée de vie utile des composants n'a pas été dépassée. La durée de vie utile est définie comme un intervalle de temps opérationnel pendant lequel le taux de défaillance est relativement constant.

Série T (SIL 2 : Analogique Sécurité)	IEC 61508
Niveau de sécurité	SIL 2
Type de dispositif	B
$MTTF_d$	100 ans à 60 °C ; 44 ans à 80 °C
PFD_{avg}	3.49E-04 à 60 °C ; 9.85E-04 à 80 °C
Temps de réponse de diagnostic (temps d'échec de détection)	25 ms (max.) 1 s pour la détection des défaillances CRC
% de la plage SIL 2 pour PFD	3,5 % à 60 °C ; 9,9 % à 80 °C
Tolérance à la défaillance matérielle (HFT, Hardware fault tolerance)	0
Durée de vie utile	50 ans à 60 °C ; 18 ans à 80 °C

Fig. 6 : Paramètres de la série T

Dispositif à une précision de 1 %	λ_{SD}	λ_{SU}	λ_{DD}	λ_{DU}	SFF
Série T à 60 °C	0	100	802	62	93,6 %
Série T à 80 °C	0	283	2 266	175	93,6 %
Série T à 85 °C	0	400	3 205	248	93,6 %

Fig. 7 : Valeurs de sécurité pour la température maximale de fonctionnement

6. Termes et abréviations

Terme	Spécifications
Cat.	Catégorie de sécurité conformément à l'EN 954-1
E/E/PE	Électrique/Électronique/Électronique programmable
FIT	Défaillances dans le temps (1×10^{-9} défaillances par heure)
AMDEC	Analyse des modes de défaillance, de leurs effets et de leur criticité (méthode analytique de détermination des modes de défaillance et des taux de défaillance)
FSM	Gestion de la sécurité fonctionnelle
HFT	Tolérance à la défaillance matérielle, HFT=x où x est le nombre de défaillances que la conception peut tolérer sans perdre sa fonction de sécurité.
Mode de demande élevée	En mode de demande élevée ou continu, la fréquence des demandes de fonctionnement sur un système de sécurité est supérieure à une par an.
Mode de demande faible	Mode dans lequel la fréquence des demandes de fonctionnement sur un système de sécurité n'est pas supérieure à une par an et pas supérieure à deux fois la fréquence d'essai.
$MTTF_d$	Durée moyenne entre les défaillances dangereuses
PFD_{avg}	Probabilité de défaillance en cas de demande
PFH	Probabilité de défaillance dangereuse par heure
SFF	La fraction des défaillances sûres résume la fraction des défaillances qui mènent à un état sûr et la fraction des défaillances qui seront détectées par des mesures de diagnostic et mèneront à une mesure de sécurité définie.
SIF	Fonction instrumentée de sécurité
SIL	Niveau d'intégrité de la sécurité
SIS	Système instrumenté de sécurité – Mise en œuvre d'une ou plusieurs fonctions instrumentées de sécurité. Un SIS est composé de toute combinaison de dispositifs, de solveurs logiques et d'éléments finaux.
SLC	Cycle de vie de sécurité
Composant de type A	Composant "non complexe" (utilisant des éléments discrets) ; pour des détails, voir 7.4.4.1.2 de l'IEC 61508-2
Composant de type B	Composant "complexe" (utilisant des microcontrôleurs ou des automates programmables industriels) ; pour des détails, voir 7.4.4.1.3 de l'IEC 61508-2
V&V	Vérification et validation
Vérification	La démonstration, pour chaque phase du cycle de vie que les livrables (en sortie) de la phase satisfont aux objectifs et aux exigences spécifiés par les entrées de la phase. La vérification est généralement exécutée par analyse et/ou essai.
Validation	La démonstration que le ou les systèmes de sécurité ou la combinaison de systèmes de sécurité et d'installations externes de réduction des risques satisfont, à tous les égards, aux spécifications des exigences d'intégrité de la sécurité. La validation est généralement obtenue par des essais.

Notes

MTS®
SENSORS

Référence du document :
551504 Révision A (FR) 05/2016

SITES

ÉTATS-UNIS
MTS Systems Corporation
Sensors Division
3001 Sheldon Drive
Cary, N.C. 27513, États-Unis
Tel. +1 919 677-0100
Fax +1 919 677-0200
info.us@mtssensors.com
www.mtssensors.com

ALLEMAGNE
MTS Sensor Technologie
GmbH & Co. KG
Auf dem Schüffel 9
58513 Lüdenscheid, Allemagne
Tel. +49 2351 9587-0
Fax +49 2351 56491
info.de@mtssensors.com
www.mtssensors.com

JAPON
MTS Sensors Technology Corp.
737 Aihara-machi,
Machida-shi,
Tokyo 194-0211, Japon
Tel. +81 42 775-3838
Fax +81 42 775-5512
info.jp@mtssensors.com
www.mtssensors.com

CHINE
MTS Sensors
Room 504, Huajing Commercial Center,
No. 188, North Qinzhou Road
200233 Shanghai, Chine
Tel. +86 21 6485 5800
Fax +86 21 6495 6329
info.cn@mtssensors.com
www.mtssensors.com

FRANCE
MTS Systems SAS
Zone EUROPARC Bâtiment EXA 16
16/18, rue Eugène Dupuis
94046 Creteil, France
Tel. +33 1 58 4390-28
Fax +33 1 58 4390-03
info.fr@mtssensors.com
www.mtssensors.com

ITALIE
MTS Systems Srl
Sensor Division
Via Camillo Golgi, 5/7
25064 Gussago (BS), Italie
Tel. +39 030 988 3819
Fax +39 030 982 3359
info.it@mtssensors.com
www.mtssensors.com

AVIS JURIDIQUE

ISO 9001 CERTIFIED

Reg.-No. 003095-QM08

SIL 2 IEC 61508

CE