developing solutions

FISCHER
MESS- UND REGELTECHNIK

IEC 61508
SIL

RoHS III COMPLIANT

Manuel de sécurité

NK10

Limiteur de niveau de remplissage

09015142 • SHB_FR_NK10 • Rev. ST4-C • 08/22

Mentions légales

Fabricant : **FISCHER Mess- und Regeltechnik GmbH**

Bielefelderstr. 37a
D-32107 Bad Salzuflen

Téléphone : +49 5222 974 0
Fax : +49 5222 7170

Mail : info@fischermesstechnik.de
Web : www.fischermesstechnik.de

Rédaction technique : Chargé de documentation : T. Malischewski
Rédacteur technique : R. Kleemann

Historique des versions

Rév. ST4-A 11/18	Version 1 (première édition)
Rév. ST4-B 01/21	Version 2 (correction du domaine d'application : n° U non utilisé))
Rév. ST4-C 08/22	Version 3 (nouvelle certification SIL)

Sommaire

1 Domaine d’application et normes 4
1.1 Normes 4
1.2 Abréviations 4
1.3 Documents également applicables 5
2 Description de l’appareil et domaine d’application 6
2.1 Structure et fonction de sécurité 6
2.2 Schéma de fonctionnement 6
3 Consignes relatives à la conception 7
3.1 Schéma de raccordement pour applications SIL 7
3.2 Maintenance et contrôles récurrents 8
3.3 Critères de sécurité 8
4 Certificat SIL 10
5 Annexe 12
5.1 Glossaire 12
5.2 Taux de défaillances 15
5.3 Types d’appareil 16
5.4 Explication des pictogrammes 17

1 Domaine d’application et normes

Ce document s'applique aux limiteurs de niveau de remplissage de la série NK10.

Ces limiteurs de niveau de remplissage sécurisés ont reçu un certificat du TÜV, conformément à la norme IEC 61508 (partie 1-2 et 4-7 :2010) pour SIL 1 et SIL 2 (SIL 3 en cas d’activation redondante).

1.1 Normes

Directives

Directive sur les appareils sous pression 2014/68/EU
Type d’équipement de sécurité pour l'utilisation dans une chaîne de sécurité comme équipement complet avec fonction de sécurité de catégorie IV

Directive européenne également applicable :
Directive Basse Tension 2014/35/UE

Normes et règlements appliqués :

IEC 61508
Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité - (partie 1-2 et 4-7)

EN 61511
Sécurité fonctionnelle - Systèmes de sécurité pour le secteur des industries de transformation

EN 61010-1
Règles de sécurité pour appareils électriques de mesurage, de régulation et de laboratoire - Exigences générales

DIN 4754-3
Installations de transmission de chaleur avec agents caloporteurs organiques - Partie 3 : Limiteurs de niveau de remplissage

EN 13445-1
Récipients sous pression non soumis à la flamme

1.2 Abréviations

SIL *(en : Safety Integrity Level)*
Niveau d'intégrité de sécurité

La norme internationale IEC 61508 définit quatre niveaux d'intégrité de sécurité discrets (SIL 1 à SIL 4). Chaque niveau correspond à une plage de probabilité pour la défaillance d'une fonction de sécurité. Plus le niveau du système de sécurité est élevé, plus faible est la probabilité que les fonctions de sécurité requises soient défaillantes.

HFT *(en : Hardware Failure Tolerance)*
Tolérance de défaillance du matériel

Capacité d'une unité fonctionnelle à poursuivre l'exécution de la fonction requise en cas de défaillances ou de divergences.

MTBF *(en : Mean Time Between Failures)*

Durée de service moyenne entre deux défaillances.

MTTR *(en : Mean Time To Repair)*

Durée moyenne entre l'apparition d'une défaillance et la réparation.

PFD *(en : Probability of Failure on Demand)*

Probabilité de défaillances dangereuses d'une fonction de sécurité lors d'une sollicitation.

PFD_{AVG} *(en : Average Probability of Failure on Demand)*

Probabilité moyenne de défaillances dangereuses d'une fonction de sécurité lors d'une sollicitation.

PFH *(en : Probability Failure per Hour)*

Probabilité moyenne d'une défaillance dangereuse par heure.

λ_S *(en : Lambda Safe)*

Taux total de toutes les défaillances non dangereuses.

λ_{DD} *(en : Lambda Dangerous Detected failures)*

Taux total des défaillances dangereuses détectées.

λ_{DU} *(en : Lambda Dangerous Undetected failures)*

Taux total des défaillances dangereuses non détectées.

DC *(en : Diagnostic Coverage)*

Le niveau de couverture du diagnostic est une mesure permettant d'identifier des défaillances potentielles à l'aide de tests.

SFF *(en : Safe Failure Fraction)*
Part des défaillances non dangereuses

Pourcentage de défaillances non dangereuses sur le nombre total de défaillances susceptibles de placer le système de sécurité dans un état de fonctionnement dangereux ou non autorisé.

FIT *(en : Failure In Time)*
Fréquence des défaillances

Nombre de défaillances en l'espace de 10^9 heures.

T1 *(en : Test Intervall)*

Intervalle de contrôle de la fonction de protection.

XooY *(en : X out of Y))*
Activation de la sélection :

Classification et description du système de sécurité en termes de redondance et de procédé de sélection appliqué.

- x Indique la fréquence à laquelle la fonction de sécurité est exécutée (redondance).
- Y Détermine le nombre de canaux qui doivent fonctionner correctement.

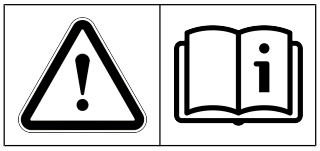
LDM *(en : Low Demand Mode)*

Mode de fonctionnement au cours duquel le taux de sollicitation du système de sécurité n'est pas supérieur à une fois par an et n'est pas supérieur au double de la fréquence du contrôle de redondance.

HDM *(en : High Demand Mode)*

Mode de fonctionnement au cours duquel le taux de sollicitation du système de sécurité est supérieur à une fois par an ou est supérieur au double de la fréquence du contrôle de redondance.

1.3 Documents également applicables



Les notices d'utilisation et les fiches de données contiennent des consignes de sécurité et des caractéristiques techniques importantes qui sont indispensables pour assurer la sécurité du fonctionnement.

Ces documents sont toujours valables dans leur version actuelle disponible sur le site Internet www.fischermesstechnik.de.

Fiche de données standard	09005238	DB_DE_NK10
Fiche de données ATEX	09005535	DB_DE_NK10_H
Notice d'utilisation standard	09005016	BA_DE_NK10
Notice d'utilisation ATEX	09005110	BA_DE_NK10_H

2 Description de l’appareil et domaine d’application

2.1 Structure et fonction de sécurité

Le système de flotteur du limiteur de niveau de remplissage se trouve dans le récipient rempli de fluide (cuve d’expansion). Le mouvement du flotteur provoqué par la modification du niveau de remplissage est transmis directement à un commutateur par l’intermédiaire de la tige du flotteur isolée par un soufflet en acier inoxydable. Le point de rotation de la tige du flotteur se trouve hors de la chambre sous pression.

À l’extérieur de la chambre sous pression se trouve également une touche de contrôle qui permet un contrôle du fonctionnement selon DIN 4754-3 sans baisse du niveau de remplissage. Dès que cette touche de contrôle est actionnée, le corps du flotteur est déplacé dans le sens opposé à sa poussée verticale.

Le point d’activation du commutateur S1 (borne 1, 2, 3) est réglé en usine de telle sorte qu’il se déclenche lorsque la tige de flotteur se trouve en position horizontale. Le commutateur d’avertissement optionnel S2 s’active environ 2,5 mm avant le S1.

La fonction de sécurité est définie comme :

1. Commutation sûre lorsque la valeur limite réglée est atteinte (commutateur S1)
2. Avertissement sûr lorsque la valeur limite réglée est atteinte (commutateur S2) - option

Les contacts de commutation du limiteur de niveau de remplissage doivent alors être surveillés par un dispositif supérieur adapté et sécurisé conformément à la norme EN 61508.

Dans une architecture monocanal (1oo1), les appareils peuvent être utilisés jusqu’au niveau SIL 2. Dans une architecture multicanal et redondante (1oo2), leur utilisation est possible jusqu’au niveau SIL 3.

2.2 Schéma de fonctionnement

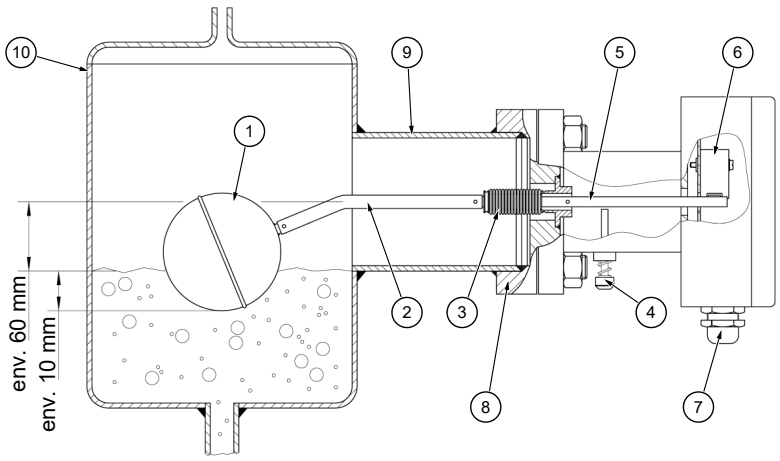


Fig. 1: Schéma de fonctionnement

1	Flotteur	2	Tige du flotteur
3	Soufflet en métal	4	Touche de contrôle
5	Levier d'activation	6	Micro-commutateur S1
7	Presse-étoupe	8	Bride et contre-bride
9	Raccord à souder	10	Récipient

3 Consignes relatives à la conception

Les limiteurs de niveau de remplissage sont conçus pour un mode de fonctionnement au taux de sollicitation faible (low demand mode) jusqu'au niveau SIL 2.

Dans une architecture multicanal et redondante, leur utilisation est possible sous forme de système partiel de sécurité jusqu'au niveau SIL 3 dans un mode de fonctionnement avec un taux de sollicitation faible ou élevé.

3.1 Schéma de raccordement pour applications SIL

Les contacts de commutation du limiteur de niveau de remplissage doivent alors être surveillés par un dispositif supérieur adapté et sécurisé conformément à la norme EN 61508 pour atteindre le niveau de couverture de diagnostic (DC) nécessaire.

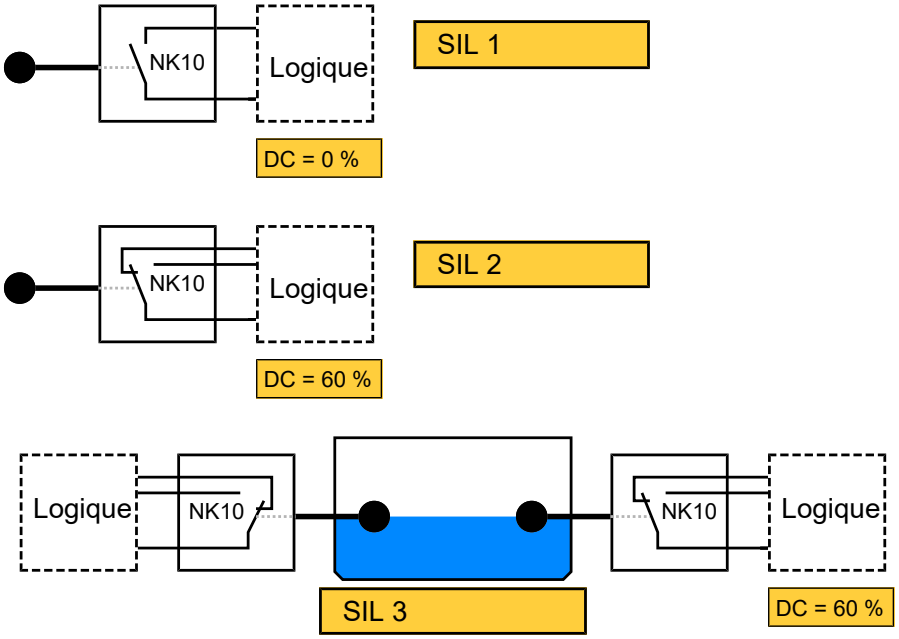


Fig. 2: Schéma de raccordement SIL

3.2 Maintenance et contrôles récurrents

Respectez également les informations de la notice d'utilisation.

Les valeurs PFD consignées dans la déclaration de conformité SIL sont valables pour l'intervalle de contrôle T1 = 1 an. Le contrôle du fonctionnement du limiteur de niveau de remplissage doit donc avoir lieu une fois par an pendant l'utilisation.

ATTENTION! Assurez la sécurité de l'installation et respectez les consignes relatives au fonctionnement.

L'appareil ne requiert aucune maintenance. Afin de garantir un fonctionnement fiable et une longue durée de vie de l'appareil, nous vous recommandons toutefois d'effectuer régulièrement les contrôles suivants :

- Contrôle du fonctionnement de la commutation en relation avec les composants en aval (au moyen de la touche de contrôle).
- Contrôle de l'étanchéité du raccordement par bride.
- Contrôle des raccordements électriques (assemblage par serrage des câbles).

Ce contrôle doit être effectué une fois par an ou plus souvent en fonction des consignes d'utilisation et doit être documenté par écrit.

Il convient d'adapter les cycles de contrôle exacts aux conditions d'exploitation et environnantes. En cas d'interaction de divers composants, il faut également respecter les notices d'utilisation de tous les autres appareils.

Tous les appareils défectueux ou présentant des vices doivent être renvoyés sans délai à notre service de réparation. Nous vous prions donc clarifier au préalable tous les renvois d'appareils avec notre service commercial. Pour renvoyer l’appareil, utilisez l’emballage d'origine ou un emballage de transport adapté.

3.3 Critères de sécurité

Le niveau SIL 1/2 ou SIL 3 est uniquement obtenu avec le limiteur de niveau de remplissage NK10 (qui fait office de capteur) lorsqu'il est combiné à un dispositif de sécurité supérieur (logique) au sens entendu par la norme EN 61508.

Enregistrement du signal Traitement du signal Commutation

- Le NK10 ne possède pas de système de diagnostic intégré. Si un diagnostic de la fonction de sécurité est nécessaire, celui-ci doit être effectué par des mesures externes comme partie du système de sécurité global. Les taux de défaillance indiqué pour DC = 60 % sont des valeurs indicatives liées à la logique d'évaluation et doivent être calculés pour chaque installation.
- Les taux de défaillance qui ont été calculés pour le Low Demand Mode peuvent également être utilisés pour calculer le PFH pour des applications en High Demand Mode jusqu'à un taux de sollicitation maximal de 12 fois par an. Ce taux de sollicitation peut entraîner de petites erreurs liées à l'usure.

$$PFH = \lambda_d$$

Type d’appareil	A
Mode de fonctionnement	LDM (Low Demand Mode)
Tolérance aux défaillances matérielles	HFT 0
Capacité systématique	SC 3
Intervalle de contrôle	T_1=1an
Durée d'utilisation	10 000 cycles de commutation ou 15 ans

Architecture 1oo1			
Facteur de couverture du diagnostic	DC	0	60
Taux d'erreur	λ_{du}	3,13 * 10^{-7} 1/h (313 FIT)	1,25 * 10^{-7} 1/h (125 FIT)
Taux de défaillance Low Demand Mode	PFD_{avg}	1,39 * 10^{-3}	5,50 * 10^{-4}
Taux de défaillance High Demand Mode	PFH	3,13 * 10^{-7} 1/h	1,25 * 10^{-7} 1/h

Architecture 1oo2			
Facteur de couverture du diagnostic	DC	0	60
Taux d'erreur	λ_{du}	3,13 * 10^{-7} 1/h (313 FIT)	1,25 * 10^{-7} 1/h (125 FIT)
Taux de défaillance Low Demand Mode	PFD_{avg}	1,41 * 10^{-4}	5,55 * 10^{-5}
Taux de défaillance High Demand Mode	PFH	3,20 * 10^{-8} 1/h	1,26 * 10^{-8} 1/h

4 Certificat SIL

Certificate

SIL/PL Capability

TÜVRheinland® CERTIFIED

www.tuv.com
ID 0600000000

Nr./No.: 968/V 1298.00/22

Prüfgegenstand **Product tested**	Füllstandsbegrenzer Level Limiter	**Zertifikats-inhaber** **Certificate holder**	Fischer Mess- und Regelungstechnik GmbH Bielefelder Str. 37a 32107 Bad Salzuflen Germany
Typbezeichnung **Type designation**	NK10 / NK10 H		
Prüfgrundlagen **Codes and standards**	IEC 61508 Parts 1-2 and 4-7:2010		
Bestimmungsgemäße Verwendung **Intended application**	Sicherheitsfunktion 1: Sicheres Schalten bei Erreichen des eingestellten Grenzwertes (Schalter S1) Sicherheitsfunktion 2: Sichere Vorwarnung bei Erreichen des eingestellten Grenzwertes (Schalter S2) - Option Die Füllstandsbegrenzer sind zur Verwendung in einem sicherheitsgerichteten System bis SIL 2 geeignet. Unter Berücksichtigung der mindestens erforderlichen Hardware-Fehlertoleranz von HFT = 1 können die Armaturen in redundanter Ausführung auch bis SIL 3 eingesetzt werden. Safety function 1: safe switching when the set limit value is reached (switch S1) Safety function 2: safe pre-warning when the set limit value is reached (switch S2) - option. The level limiter are suitable for use in a safety instrumented system up to SIL 2. Under consideration of the minimum required hardware fault tolerance HFT = 1 the valves may be used in a redundant architecture up to SIL 3.		
Besondere Bedingungen **Specific requirements**	Die Hinweise in der zugehörigen Installations- und Betriebsanleitung sowie des Sicherheitshandbuchs sind zu beachten. The instructions of the associated Installation, Operating and Safety Manual shall be considered.		

Zusammenfassung der Testergebnisse siehe Seite 2 des Zertifikates.
Summary of test results see page 2 of this certificate.

Der Ausstellung dieses Zertifikates liegt eine Evaluierung entsprechend dem Zertifizierungsprogramm CERT FSP1 V1.0:2017 in der aktuellen Version zugrunde, deren Ergebnisse im Bericht Nr. 968/V 1298.00/22 vom 08.08.2022 dokumentiert sind. Dieses Zertifikat ist nur gültig für Erzeugnisse, die mit dem Prüfgegenstand übereinstimmen.

The issue of this certificate is based upon an evaluation in accordance with the Certification Program CERT FSP1 V1.0:2017 in its actual version, whose results are documented in Report No. 968/V 1298.00/22 dated 2022-08-08. This certificate is valid only for products, which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit

Köln, 2022-08-11

Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. (FH) Wolf Rückwart

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

www.fs-products.com
www.tuv.com

DAkkS Deutsche Akkreditierungsstelle D-ZE-11052-02-01

TÜVRheinland®
Precisely Right.

Fig. 3: 968_V_1298_00_22_de_en_el_Page 1

968/V 1298.00/22 - page 2

TÜVRheinland®
Precisely Right.

Holder: Fischer Mess- und Regeltechnik GmbH
Bielefelder Straße 37a
D-32107 Bad Salzuflen
Germany

Product tested: **Level indicator / level limiter**
NK10 / NK10 H

Results of Assessment

Route of Assessment		2_H / 1_S
Type of Sub-system		Type A
Mode of Operation		Low Demand Mode
Hardware Fault Tolerance	HFT	0
Systematic Capability		**SC 3**

Safe switching when the set limit value is reached (switch S1)

Dangerous Failure Rate	λ_D	3.13 E-07 / h	**313 FIT**
Average Probability of Failure on Demand 1oo1	$PFD_{avg}(T_1)$	1.39 E-03	
Average Probability of Failure on Demand 1oo2	$PFD_{avg}(T_1)$	1.41 E-04	

Safe prewarning when the set limit value is reached (switch S2) - option

Dangerous Failure Rate	λ_D	3.13 E-07 / h	**313 FIT**
Average Probability of Failure on Demand 1oo1	$PFD_{avg}(T_1)$	1.39 E-03	
Average Probability of Failure on Demand 1oo2	$PFD_{avg}(T_1)$	1.41 E-04	

Assumptions for the calculations above: DC = 0 %, T_1 = 1 year, MRT = 72 h, β_{1oo2} = 10 %

High Demand Mode
In the opinion of the testing laboratory, the failure rates determined for the low demand mode can also be used for high demand mode applications up to a maximum demand rate of n_{op} = 12 / a. No failures due to wear are to be expected.

Origin of failure rates
The stated failure rates for low demand are the result of an FMEDA with tailored failure rates for the design and manufacturing process.
Furthermore the results have been verified by qualification tests and field-feedback data.
Failure rates include failures that occur at a random point in time and are due to degradation mechanisms such as ageing.
The stated failure rates do not release the end-user from collecting and evaluating application-specific reliability data.

Periodic Tests and Maintenance
The given values require periodic tests and maintenance as described in the Safety Manual.
The operator is responsible for the consideration of specific external conditions (e.g. ensuring of required quality of media, max. temperature, time of impact), and adequate test cycles.

TP-4800; Rev. 5.0 TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany

Fig. 4: 968_V_1298_00_22_de_en_el_Page 1

5 Annexe

5.1 Glossaire

Abrév. (A-Z)	Définition
β	*(en)* **Common Cause Factor** *(fr)* Facteur bêta Facteur de proportionnalité entre le taux CCF (défaillance de cause commune) et le taux de défaillance dangereuse du canal individuel.
DC	*(en)* **Diagnostic Coverage Factor** *(fr)* Degré de couverture du diagnostic Le paramètre DC indique le rapport entre le nombre de toutes les erreurs dangereuses détectées (λ_{DD}) et le nombre total d'erreurs dangereuses (λ_D). $DC = \frac{\sum \text{erreur dangereuse détectée}}{\sum \text{erreur dangereuse globale}} = \frac{\sum \lambda_{DD}}{\sum \lambda_D}$
FIT	*(en)* **Failure in Time** *(fr)* Défaillances par durée Taux de défaillances dans l'intervalle de 10^9 heures. $1\ FIT = 1 \times 10^{-9} \frac{1}{h}$
FMEDA	*(en)* **Failure Mode Effect and Diagnostic Analysis** *(fr)* Analyse des modes de défaillance, de leurs effets et de leur criticité Procédé de détermination des causes des erreurs et de leur impact sur le système.
HDM	*(en)* **High Demand Mode** *(fr)* Mode de service avec niveau de sollicitation élevé Mode de service avec une sollicitation élevée ou constante de la fonction de sécurité. Le taux de sollicitation du système de sécurité est supérieur à un par an.
HFT	*(en)* **Hardware Fault Tolerance** *(fr)* Tolérance aux défaillances matérielles La tolérance aux défaillances matérielles indique combien d'erreurs dangereuses sont possible en raison de l'architecture sans que l'exécution de la fonction de sécurité ne soit entravée. • HFT = 0 Une erreur dangereuse entraîne la défaillance de la fonction de sécurité. • HFT = 1 Deux erreurs dangereuses entraînent la défaillance de la fonction de sécurité.

LDM	*(en)* **Low Demand Mode** *(fr)* Mode de service avec un faible niveau de sollicitation La fonction de sécurité n'est exécutée que sur sollicitation pour faire passer le système dans un état sécurisé précis. La fréquence de sollicitation n'est pas supérieure à un par an.
MooN	*(en)* **Architecture with M out of N channels** *(fr)* Architecture de système « M-parmi-N » Architecture de système MooN avec les variables M et N : Classification et description du système de sécurité en termes de redondance et de procédés de sélection appliqués. • N - Indique le nombre total des canaux redondants d'une architecture de sécurité ou d'un circuit de sécurité. • M – Détermine le nombre de canaux qui doivent fonctionner correctement pour exécuter la fonction de sécurité.
MTBF	*(en)* **Mean Time Between Failures** *(fr)* Temps de fonctionnement moyen entre défaillances Durée de service moyenne entre deux défaillances.
$MTTF_d$	*(en)* **Mean Time To Dangerous Failures** *(fr)* Temps moyen avant défaillance dangereuse Durée de service jusqu'à une erreur présentant un danger.
MRT	*(en)* **Mean Repair Time** *(fr)* Temps moyen de réparation Temps moyen requis pour réparer.
MTTR	*(en)* **Mean Time To Repair** *(fr)* Temps moyen avant la remise en service Durée moyenne entre l'apparition d'une défaillance et la remise en service du système.
PFD	*(en)* **Probability of Failure on Demand** *(fr)* Probabilité de défaillance sur sollicitation Probabilité d'une défaillance présentant un danger en cas de sollicitation de la fonction de sécurité pour un mode de service avec un faible taux de sollicitation (Low Demand).
PFH	*(en)* **Probability of a dangerous Failure per Hour** *(fr)* Probabilité d'une défaillance dangereuse par heure Fréquence d'une défaillance dangereuse de la fonction de sécurité pour un mode de service avec un taux de sollicitation élevé ou constant (High Demand).

PFS	*(en)* **Probability of Failure Spurious** *(fr)* Probabilité de fausse défaillance
	Fréquence d'une défaillance due à une fausse alarme qui entraîne un arrêt non intentionnel du processus par le système de sécurité. Plus la valeur est faible, plus le système est disponible.
SC	*(en)* **systematic capability** *(fr)* capacité systématique
	Mesure la confiance (exprimée sur une échelle allant de SC 1 à SC 4) dans le fait que l'intégrité de sécurité systématique d'un élément réponde aux exigences du SIL fixé en matière de fonction de sécurité définie pour l'élément lorsque l'élément est utilisé conformément au manuel de sécurité pour objets conformes et aux instructions fixées pour l'élément.
SFF	*(en)* **Safe Failure Fraction** *(fr)* Part des défaillances non dangereuses
	Elle est calculée à partir du rapport entre les erreurs non dangereuses + les erreurs diagnostiquées ou détectées et le taux de défaillance total du système.[(1)]
SIF	*(en)* **Safety Instrumented Function** *(fr)* Fonction instrumentée de sécurité
	La fonction instrumentée de sécurité (SIF) est une mesure de protection qui n'est activée qu'en cas de défaut et empêche ainsi tout dommage corporel, matériel et de l'environnement.
SIL	*(en)* **Safety Integrity Level** *(fr)* Niveau d'intégrité de sécurité
	Il s'agit d'un niveau discret (parmi quatre possibles) qui permet d'évaluer les exigences de fiabilité des fonctions de sécurité dans les systèmes de sécurité. SIL 4 est le niveau le plus haut de l'intégrité de sécurité et SIL 1 le niveau le plus bas. Chaque niveau correspond à une plage de probabilité pour la défaillance d'une fonction de sécurité.
SIS	*(en)* **Safety Instrumented System** *(fr)* Système instrumenté de sécurité
	Système instrumenté de sécurité pour l'exécution d'une ou de plusieurs fonctions de sécurité. Un tel système comprend au moins un capteur, une commande supérieure de sécurité et un acteur.
T_1	*(en)* **Proof Test Interval** *(fr)* Intervalle du test de contrôle
	Le système de sécurité doit toujours se trouver dans un état qui garantit l'intégrité de sécurité définie. Le test de contrôle doit être exécuté pour le confirmer. L'intervalle de contrôle indique à quelle fréquence un test de contrôle doit être effectué pour garantir la fonction de sécurité.

[(1)] En raison de l'absence de diagnostic et des quelques erreurs négligeables pour les composants mécaniques, cette méthode n'est pas pleinement applicable pour les soupapes, les entraînements et d'autres composants mécaniques. Il incombe donc à l'utilisateur final d'assurer une SFF correspondante par des mesures de diagnostic adaptées et une construction sûre.

5.2 Taux de défaillances

Il convient de distinguer les défaillances suivantes pour les taux de défaillance :

1. défaillances non dangereuses
2. défaillances dangereuses
3. Erreur sans impact

Les deux premiers types d'erreurs se divisent à nouveau entre les erreurs détectables et les erreurs non détectables.

Les erreurs sans impact et les défauts sûrs, qu'ils soient détectés ou non, n'ont pas d'influence sur la fonction de sécurité. En revanche, les défaillances dangereuses ont pour effet de faire passer le système dans un état dangereux. Le diagramme suivant vous fournit une vue d'ensemble.

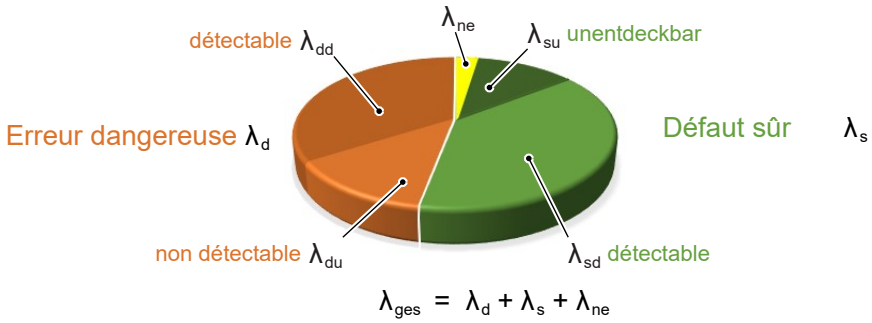


Fig. 5: Taux de défaillances

λ_d *(en)* **Dangerous failure rate**
(fr) Taux de défaillances dangereuses

λ_{dd} *(en)* **Dangerous detected failure rate**
(fr) Taux de défaillances dangereuses détectées

λ_{du} *(en)* **Dangerous undetected failure rate**
(fr) Taux de défaillances dangereuses non détectées

λ_s *(en)* **Safe failure rate**
(fr) Taux des défaillances non dangereuses

λ_{sd} *(en)* **Safe detected failure rate**
(fr) Taux des défaillances non dangereuses détectées

λ_{su} *(en)* **Safe undetected failure rate**
(fr) Taux des défaillances non dangereuses et non détectées

λ_{ne} *(en)* **No effect failure rate**
(fr) Taux de toutes les erreurs sans impact

5.3 Types d’appareil

Type A **Matériel d’exploitation simple**

Les appareils du type A sont des appareils « simples », le comportement de tous les composants utilisés en cas de défaillance et leur comportement dans des conditions de défaillance sont entièrement connus.

Il s’agit par exemple de relais, de résistances et de transistors, mais pas de composants complexes tels que des microprocesseurs.

Type B **Matériel d’exploitation complexe**

Les appareils du type B sont des appareils « complexes », le comportement de tous les composants utilisés en cas de défaillance et leur comportement dans des conditions de défaillance ne sont pas entièrement connus.

Ces appareils contiennent des composants électroniques tels que des micro-contrôleurs, des microprocesseurs ou des circuits intégrés propres à une application (ASIC). Il est difficile de définir complètement toutes les défaillances pour ces composants et notamment pour les fonctions pilotées par des logiciels.

5.4 Explication des pictogrammes

⚠ DANGER

Type et source du danger

Ce pictogramme signale une situation de danger **imminent entraînant** la mort ou des blessures corporelles très graves (niveau de danger le plus élevé).

1. Évitez un tel danger en respectant les dispositions en vigueur relatives à la sécurité.

⚠ AVERTISSEMENT

Type et source du danger

Ce pictogramme signale une situation de danger **potentiel pouvant entraîner** la mort ou des blessures corporelles graves (niveau de danger moyen).

1. Évitez un tel danger en respectant les dispositions en vigueur relatives à la sécurité.

⚠ ATTENTION

Type et source du danger

Ce pictogramme signale une situation de danger **potentiel pouvant entraîner** des blessures corporelles légères à moyennes, des dommages matériels et de l'environnement (niveau de danger faible).

1. Évitez un tel danger en respectant les dispositions en vigueur relatives à la sécurité.

AVIS

Remarque / Conseil

Ce pictogramme signale des remarques ou des conseils utiles pour un fonctionnement efficace et parfait de l'appareil.

Notes

Notes

FISCHER Mess- und Regeltechnik GmbH
Bielefelder Str. 37a
D-32107 Bad Salzuflen

Tel. +49 5222 974-0
Fax +49 5222 7170
www.fischermesstechnik.de
info@fischermesstechnik.de