

The Art of Measuring.



Français

P 32*00P0/1

Guide de sécurité SIL

PolyTrans® P32000P0/1*

ThermoTrans® P32100P0/1*

SensoTrans® P32200P0/1*

SensoTrans® P32300P0/1*

Table des matières

1	Champ d'application et normes.....	4
1.1	Abréviations.....	6
2	Descriptif de l'appareil et champ d'application.....	8
2.1	Fonction de sécurité.....	8
2.2	Définition de l'état sûr.....	8
3	Informations relatives à la programmation.....	9
3.1	Mode de fonctionnement à faible taux de demande.....	9
3.2	Mode de fonctionnement à taux de demande élevé	9
3.3	Types d'erreur.....	9
3.4	Intervalle d'essai de diagnostic.....	10
4	Montage et installation.....	11
5	Contrôles périodiques.....	13
5.1	Vérification du fonctionnement.....	13
6	Caractéristiques de sécurité.....	15
6.1	Suppositions.....	15
6.2	Caractéristiques spécifiques de sécurité.....	16
6.3	Exemple de calcul.....	17
7	Certificat.....	19

1 Champ d'application et normes

Ce guide de sécurité concerne les convertisseurs des séries PolyTrans® P32000P0/1*, ThermoTrans® P32100P0/1*, SensoTrans® P32200P0/1* et SensoTrans® P32300P0/1*.

Versions matérielles et logicielles valides :

- Numéros de série à partir de 1657362
- Logiciel de l'appareil à partir de la rév. 1.28 / 2.0

Les convertisseurs orientés sécurité de la série P32xxxP0/1* de Knick Elektronische Messgeräte GmbH & Co. KG sont certifiés SIL 2 (SIL 3 en cas de câblage redondant) par le TÜV, conformément à la norme EN 61508 :

TÜV Rheinland Industrie Service GmbH
Automation, Software und Informationstechnologie (ASI)
Am Grauen Stein
D - 51105 Cologne



N° du certificat et du rapport d'essai : 968/EZ 272.00/07

Les convertisseurs sont développés et contrôlés conformément aux normes suivantes :

- **EN 61508 : 2001**
Sécurité fonctionnelle des systèmes électriques/électroniques/programmables de sécurité
- **EN 61511 : 2004**
Sécurité fonctionnelle – Systèmes de sécurité pour l'industrie des processus
- **EN 61010-1 : 2001**
Contraintes de sécurité pour les appareils électriques de mesure, de commande, de régulation et de laboratoire
- **EN 61326-1 : 2006**
Appareils électriques de mesure, de commande, de régulation et de laboratoire – Exigences CEM
- **EN 61326-2-3 : 2006**
Appareils électriques de mesure, de commande, de régulation et de laboratoire – Exigences CEM – Partie 2-3 : Exigences particulières – Disposition de contrôle, conditions de fonctionnement et caractéristiques de puissance des convertisseurs avec traitement des signaux intégré ou amovible
- **IEC 61326-3-2 : 2006**
Appareils électriques de mesure, de commande, de régulation et de laboratoire – Exigences CEM – Partie 3-2 : Exigences d'immunité pour les appareils qui exécutent des fonctions de sécurité ou qui sont utilisés pour des fonctions de sécurité (sécurité fonctionnelle) – Applications industrielles dans des environnements électromagnétiques
- **EN 50178 : 1997**
Équipement électronique des installations à courant fort

1.1 Abréviations

Abréviation	Anglais	Français
SIL	Safety Integrity Level	L'un des quatre niveaux discrets correspondant à une plage de valeurs de l'intégrité de sécurité, sachant que le niveau 4 représente le degré le plus élevé de l'intégrité de sécurité et le niveau 1 le degré le plus faible
PFD	Probability of dangerous failure on demand	Indisponibilité de sécurité (voir CEI 60050-191) d'un système E/E/PE relatif à la sécurité pour exécuter la fonction de sécurité spécifiée lorsqu'une demande est effectuée par l'EUC ou le système de conduite ou de commande de l'EUC
PFD _G	Average probability of failure on demand for the group of voted channels	Probabilité moyenne d'une défaillance en cas de demande d'un groupe de canaux avec comparateur de sortie ou élément de décision à la majorité
PFH	Average frequency of a dangerous failure per hour	Fréquence moyenne d'une défaillance dangereuse d'un système E/E/PE relatif à la sécurité pour exécuter la fonction de sécurité spécifiée sur une période de temps donnée
PFH _G	Average frequency of dangerous failure for the group of voted channels	Fréquence moyenne d'une défaillance dangereuse pour un groupe de canaux avec comparateur de sortie ou élément de décision à la majorité
SFF	Safe failure fraction	Propriété d'un élément relatif à la sécurité qui est définie par le rapport entre le taux moyen des défaillances non dangereuses plus dangereuses détectées et le taux moyen des défaillances non dangereuses plus dangereuses
λ	Total failure rate (per hour) of a channel in a subsystem	Taux global de défaillance (par heure) d'un canal dans un sous-système
λ_D	Dangerous failure rate (per hour) of a channel in a subsystem, equal to 0.5 λ (assumes 50 % dangerous failures and 50 % safe failures)	Taux de défaillances dangereuses (par heure) du canal d'un sous-système, égal à 0,5 λ (en supposant une répartition des défaillances en 50 % dangereuses et 50 % sûres)
λ_{DU}	Undetected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the undetected dangerous failure rates within the channel of the subsystem)	Taux de défaillances dangereuses non détectées (par heure) du canal d'un sous-système. (La somme de tous les taux de défaillances dangereuses non détectées au sein du canal d'un sous-système.)
λ_{DD}	Detected dangerous failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected dangerous failure rates within the channel of the subsystem)	Taux de défaillances dangereuses détectées (par heure) du canal d'un sous-système. (La somme de tous les taux de défaillances dangereuses détectées au sein du canal d'un sous-système.)
λ_{SD}	Detected safe failure rate (per hour) of a channel in a subsystem (this is the sum of all the detected safe failure rates within the channel of the subsystem)	Taux de défaillances sûres détectées (par heure) du canal d'un sous-système. (La somme de tous les taux de défaillances sûres détectées au sein du canal d'un sous-système.)

Abbréviation	Anglais	Français
DC	Diagnostic coverage (expressed as a fraction in the equations and as a percentage elsewhere)	Degré de couverture du diagnostic (exprimé sous forme de fraction dans les équations, en pourcentage dans les autres cas)
β	The fraction of undetected failures that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)	Proportion de défaillances de cause commune non détectées (exprimée sous forme de fraction dans les équations, en pourcentage dans les autres cas)
β_D	Of those failures that are detected by the diagnostic tests, the fraction that have a common cause (expressed as a fraction in the equations and as a percentage elsewhere)	La proportion des défaillances de cause commune qui sont détectées par le test de diagnostic (exprimée sous forme de fraction dans les équations, en pourcentage dans les autres cas)
HFT	Hardware Fault Tolerance	Tolérance aux erreurs du matériel : Capacité d'une unité fonctionnelle à continuer à exécuter une fonction demandée en cas d'erreurs ou d'écarts
MTBF	Mean time between failures	Temps moyen entre deux défaillances
MTTR	Mean time to restoration (hour)	Durée moyenne jusqu'à la restauration (en heures)
MRT	Mean repair time (hour)	Durée moyenne de résolution (en heures)
FIT	Failure in time	1×10^{-9} erreurs par heure
T_1	Proof test interval (hour)	Intervalle du contre-essai (en heures)
T_2	Interval between demands (hour)	Intervalle entre les demandes (en heures)
Moon	M out of N channel architecture (for example 1oo2 is 1 out of 2 architecture, where either of the two channels can perform the safety function)	Architecture à canaux M sur N (par exemple, 1oo2 est une architecture avec canaux 1 sur 2, chacun des deux canaux pouvant exécuter la fonction de sécurité)
MoOND	M out of N channel architecture with Diagnostics	Architecture à canaux M sur N avec diagnostic
t_{CE}	Channel equivalent mean down time (hour) for 1oo1, 1oo2, 2oo2 and 2oo3 architectures (this is the combined down time for all the components in the channel of the subsystem)	Durée moyenne de défaillance d'un canal (en heures) pour architectures 1oo1, 1oo2, 2oo2 et 2oo3. (La durée de défaillance commune pour tous les composants dans un canal du sous-système.)
t_{GE}	Voted group equivalent mean down time (hour) for 1oo2 and 2oo3 architectures (this is the combined down time for all the channels in the voted group)	Durée moyenne de défaillance d'un groupe avec comparateur de sortie ou élément de décision à la majorité (en heures) pour architectures 1oo2 et 2oo3. (La durée de défaillance commune pour tous les canaux dans un groupe avec comparateur de sortie ou élément de décision à la majorité.)

2 Descriptif de l'appareil et champ d'application

2.1 Fonction de sécurité

Les convertisseurs transmettent les valeurs d'entrée dans un signal de sortie analogique normalisé de 0/4 à 20 mA ou de 0 à 5/10 V avec une isolation galvanique. La fonction de transmission peut être ajustée aux capteurs raccordés à l'entrée. Le signal de sortie analogique est retransmis à une unité logique (par ex. un API).

Dans une architecture monocanal (1oo1), les appareils peuvent être utilisés jusqu'à SIL 2. Dans une architecture multicanal redondante, ils peuvent être utilisés jusqu'à SIL 3. Les signaux de sortie des convertisseurs doivent être surveillés par un équipement approprié en amont (par ex. fonction de surveillance dans un API) et de manière orientée vers la sécurité comme un système 1oo2 au sens de la norme EN 61508 (cf. EN 61508-6, B 2.2.2).

2.2 Définition de l'état sûr

Type de signal de sortie	Etat sûr
0 – 20 mA	$\leq 3,6 \text{ mA} ; \geq 21 \text{ mA}$
4 – 20 mA	$\leq 3,6 \text{ mA} ; \geq 21 \text{ mA}$
0 – 10 V	$\leq 0,1 \text{ V} ; \geq 10,5 \text{ V}$
0 – 5 V	$\leq 0,1 \text{ V} ; \geq 5,25 \text{ V}$

3 Informations relatives à la programmation

3.1 Mode de fonctionnement à faible taux de demande

Les convertisseurs sont utilisés en mode de fonctionnement à faible taux de demande (low demand mode) lorsque le taux de demande auprès des convertisseurs ne dépasse pas une fois par an et ne représente pas plus du double de la fréquence du contre-essai (EN 61508-4, 3.5.12).

Le mode de fonctionnement à faible taux de demande peut aussi être utilisé lorsque le rapport entre le taux de test de diagnostic interne du convertisseur et le taux de demande dépasse la valeur 100 (EN 61508-2, 7.4.3.2.5).

La caractéristique correspondante est la valeur PFD. La valeur dépend de l'intervalle du contre-essai T_1 entre les tests de fonctionnement de la fonction de protection.

3.2 Mode de fonctionnement à taux de demande élevé

Si le « mode de fonctionnement à faible taux de demande » n'est pas approprié, utiliser le convertisseur comme un sous-système de sécurité en mode de fonctionnement à taux de demande élevé ou continu (high demand or continuous mode) (EN 61508-4, 3.5.12).

Le temps de tolérance aux erreurs du système général doit alors être supérieur à la somme des temps de réaction et/ou des intervalles de test de diagnostic de tous les composants de la chaîne de mesure de sécurité. La caractéristique correspondante est la valeur PFH.

3.3 Types d'erreur

Une défaillance non dangereuse (safe failure) n'entraîne pas le basculement du système de sécurité dans un état dangereux ou dans un état de dysfonctionnement. Le convertisseur bascule dans l'état sûr défini ou dans le mode de perturbation en cas de dépassement de la plage de mesure, par ex. 21 mA.

Une défaillance dangereuse non détectée (dangerous undetected failure) peut entraîner le basculement du système de sécurité dans un état dangereux ou dans un état de dysfonctionnement. Le convertisseur ne bascule pas dans l'état sûr défini ou dans le mode de perturbation.

3.4 Intervalle d'essai de diagnostic

Parallèlement aux fonctions de sécurité à proprement parler, des fonctions de diagnostic sont continuellement exécutées dans les convertisseurs afin de détecter tout comportement défaillant. L'intervalle d'essai de diagnostic représente la période pendant laquelle ces essais sont réalisés et répétés. Des erreurs de matériel fortuites sont détectées pendant cette période.

4 Montage et installation

Selon le modèle de convertisseur, les documentations suivantes doivent être jointes :

PolyTrans® P3200P0/1x	ThermoTrans® P32100P0/1x	SensoTrans® P32200P0/1x	SensoTrans® P32300P0/1x
Mode d'emploi TA-254.111-KNxxx	Mode d'emploi TA-254.113-KNxxx	Mode d'emploi TA-254.114-KNxxx	Mode d'emploi TA-254.115-KNxxx

Les consignes, les conditions générales et les valeurs limites indiquées dans les modes d'emploi doivent être respectées lors de l'installation et de l'utilisation des convertisseurs.

Les appareils pour lesquels un très haut degré de disponibilité est nécessaire doivent être affectés à la catégorie de surtension III. Avec la catégorie de surtension III et le degré de pollution 2, la tension de service maximale admissible est de 150 VCA/CC. Si la tension de service est > 150 VCA/CC, il est nécessaire de prendre des mesures adaptées de protection contre la surtension afin de s'assurer que la catégorie de surtension III est respectée.

Les câbles reliant le capteur situé sur le point de mesure au convertisseur doivent être disposés de manière à empêcher un court-circuit entre les fils et avec l'environnement des câbles.

Pour un type de signal de sortie configuré Courant (par ex. 4 ... 20 mA), la charge de sortie doit être $\geq 50 \Omega$.

Avant la mise en service et après chaque modification de la programmation, vérifier le fonctionnement conforme du convertisseur (cf. chapitre 5.1 « Vérification du fonctionnement »).

Si la programmation a été effectuée par le biais de l'interface IrDA[®], le convertisseur doit ensuite être placé en mode Read-Only. Dans ce mode de fonctionnement, les données peuvent uniquement être envoyées par le convertisseur via l'interface IrDA[®] (affichage des mesures, statistiques, ...).

Activer le mode Read-Only :

- Tous les commutateurs DIP = 0
- Tous les commutateurs rotatifs = 0

Une fois la programmation correctement effectuée, fixer les commutateurs à l'aide du film en polyimide autocollant fourni.

5 Contrôles périodiques

Le contre-essai permet de détecter d'éventuelles erreurs dangereuses non détectables par l'auto-diagnostic. Le bon fonctionnement du convertisseur doit donc être vérifié à des intervalles réguliers et appropriés.

C'est à l'utilisateur que revient la responsabilité de choisir le mode de contrôle et les intervalles de temps. Les intervalles de test sont entre autres déterminés lors du calcul de chaque circuit de sécurité d'une installation (valeurs PFD).

Le contrôle doit être réalisé de manière à démontrer le bon fonctionnement de la fonction de sécurité en interaction avec tous les composants.

5.1 Vérification du fonctionnement

Les valeurs PFD documentées dans le chapitre 6.x s'appliquent à l'intervalle du contre-essai $T_1 = 1$ an. Le bon fonctionnement du convertisseur doit être vérifié dans l'application. Pour cela, procéder comme suit :

- Activer le convertisseur avec la sortie ouverte (charge = ∞).
Vérifier les messages d'état et de diagnostic signalés par des LED :
 - Aucune erreur d'appareil ne doit être signalée (message d'erreur 10).
 - Pour le type de signal de sortie configuré Courant (par ex. 4 ... 20 mA), le message d'erreur 6 (erreur de sortie Charge) doit être signalé.
- Spécifier des valeurs de consigne pour le début et la fin de la plage de mesure, ainsi qu'une valeur moyenne (par ex. valeur 50 %). Vérifier que l'écart de mesure est compris dans les tolérances spécifiées.
- Vérifier que le basculement dans l'état sûr s'effectue correctement.
Pour le vérifier, privilégier la simulation d'une rupture de câble (entrée ouverte). La sortie commande alors à ≥ 21 mA (sorties de courant) ou $\geq 5,25$ V ou $\geq 10,5$ V (sorties de tension). Le message d'erreur « Sonde ouverte » est alors transmis (la LED rouge clignote 4 fois).

Le signal d'erreur est maintenu même si la cause de l'erreur a été résolue (message d'erreur auto-maintenu). Le message d'erreur est réinitialisé par un redémarrage (marche/arrêt de l'énergie auxiliaire ou via l'IrDA).

Si l'essai de fonctionnement s'avère négatif, le convertisseur doit être mis hors service et le processus doit être maintenu dans un état sûr par le biais d'autres mesures.

Le convertisseur lui-même ne nécessite pas d'entretien.

6 Caractéristiques de sécurité

6.1 Suppositions

- La communication par le biais de l'interface IrDA est exclusivement utilisée pour la configuration de l'appareil ou pour des fonctions de diagnostic, mais pas pour des opérations critiques de sécurité.
- Après la configuration (avec des commutateurs rotatifs/DIP ou l'interface IrDA), un contrôle de fonctionnement est réalisé afin de vérifier que la fonction de mesure exécutée est conforme aux préréglages.
- La durée de résolution (MRT) suivant un défaut de l'appareil ne dépasse pas 72 heures.
- La température moyenne considérée sur une longue période ne dépasse pas 55 °C.
- Les conditions ambiantes correspondent aux conditions moyennes d'un environnement industriel.
- Les spécifications du manuel utilisateur doivent être respectées.

6.2 Caractéristiques spécifiques de sécurité

Structure	1 canal (1oo1)
Catégorie	SIL 2 (logiciel SIL 3)
Type d'appareil	Type B
HFT	0
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
PFD_{SIL2}	$2,7 \cdot 10^{-4}$
PFH_{SIL2}	$4,8 \cdot 10^{-8}/h$
PFD_{SIL3}	$4,9 \cdot 10^{-6}$
PFH_{SIL3}	$8,5 \cdot 10^{-9}/h$
Intervalle d'essai de diagnostic	< 5 s
Temps de réaction aux erreurs en cas de dépassement positif ou négatif de la plage de mesure	< 2 s
Taux de défaillance :	
λ_s	759,2 FIT
λ_D	759,2 FIT
λ_{DU}	48,1 FIT
λ_{DD}	711,1 FIT

Remarque :

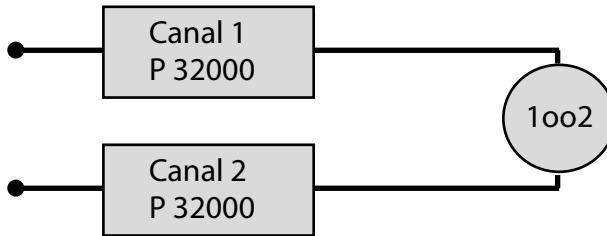
Le taux de défaillance des éléments électroniques augmente après une durée d'utilisation de 8 à 12 ans, ce qui entraîne une altération des valeurs PFD et PFH qui en sont dérivées (EN 61508-2, 7.4.7.4, remarque 3).

6.3 Exemple de calcul

L'hypothèse d'un système doublement redondant avec deux convertisseurs PolyTrans P32000 est utilisée à titre d'exemple de calcul concret avec PTC® Mathcad® sur la base de EN 61508: 2001 (système 1oo2).

L'intervalle du contre-essai T_1 est de 1 an (8760 h).

Afin que la fonction de sécurité soit correctement exécutée, les canaux doivent être reliés entre eux de manière à ce que l'un des canaux suffise au déclenchement de la fonction de sécurité. Dans un système 1oo2, cela provoque donc une défaillance dangereuse de la fonction de sécurité si les deux canaux sont simultanément défaillants.



$$\text{MTTR}:=72 \text{ hr}^1) \quad \text{MRT}:=72 \text{ hr} \quad \text{FIT}:=\frac{1}{10^9 \text{ hr}} \quad \beta:=0.02 \quad \beta_D:=0.01$$

$$T_1:=1 \cdot 8760 \text{ hr}$$

$$\lambda_{DU}:=48.1 \cdot \text{FIT} \quad \lambda_{DD}:=711.1 \cdot \text{FIT} \quad \lambda_D:=759.2 \cdot \text{FIT} \quad \lambda_S:=759.2 \cdot \text{FIT}$$

$$\frac{\lambda_{DU}}{\lambda_D} = 0.063 \quad \frac{\lambda_{DD}}{\lambda_D} = 0.937$$

$$t_{CE}:=\frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_1}{2} + \text{MRT} \right] + \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR} = [349.5] \text{ hr}$$

$$t_{GE}:=\frac{\lambda_{DU}}{\lambda_D} \cdot \left[\frac{T_1}{3} + \text{MRT} \right] + \frac{\lambda_{DD}}{\lambda_D} \cdot \text{MTTR} = [257] \text{ hr}$$

$$\text{PFD}:=2((1-\beta_D) \lambda_{DD} + (1-\beta) \lambda_{DU})^2 \cdot t_{CE} \cdot t_{GE} + \beta_D \cdot \lambda_{DD} \cdot \text{MTTR} + \beta \cdot \lambda_{DU} \cdot \left(\frac{T_1}{2} + \text{MRT} \right)$$

$$\text{PFD}=4.896 \cdot 10^{-6}$$

$$\text{PFH}:=2((1-\beta_D) \lambda_{DD} + (1-\beta) \lambda_{DU})^2 \cdot t_{CE} + \beta_D \cdot \lambda_{DD} + \beta \cdot \lambda_{DU} = [8.467 \cdot 10^{-9}] \frac{1}{\text{hr}}$$

¹⁾ Mathcad® utilise comme unité pour les heures hr.

Les valeurs suivantes sont obtenues pour ce système :

Structure	2 canaux (1oo2)
Catégorie	SIL 3
Architecture	Type B
HFT	1
SFF	97 %
DC	94 %
β	2 %
β_D	1 %
MTTR	72 h
t_{CE}	349,5 h
t_{GE}	67,5 h
$PFD_{G,1oo2}$	$4,9 \cdot 10^{-6}$
$PFH_{G,1oo2}$	$8,5 \cdot 10^{-9}/h$



ZERTIFIKAT
CERTIFICATE

Nr./No. 968/EZ 272.00/07

Prüfgegenstand Product tested	Messumformer-Reihe P32000	Zertifikatsinhaber Holder of the certificate	Knick Elektronische Messgeräte GmbH & Co. KG Beuckestrasse 22 14163 Berlin
Typbezeichnung Type designation	PolyTrans® P 32000 P0/1* SensoTrans® R P 32300 P0/1* SensoTrans® DMS P 32200 P0/1* ThermoTrans® P 32100 P0/1*	Verwendungszweck Intended application	Einsatz als Teil von Schutzeinrichtungen zur Überwachung sicherheitsrelevanter Signale (Temperatur, Widerstand, Potentiometer, Spannung, ...)
Prüfgrundlagen Codes and standards forming the basis of testing	EN 61508:2001 EN 61511:2004 EN 61010-1:2001 EN 61326-1:2006 IEC 61326-3-2:2006 EN 50178:1997		
Prüfungsergebnis Test results	Die Messumformer-Reihe P32000 mit den oben genannten Typen erfüllt die gestellten Anforderungen der EN 61508 für SIL 2 bzw. SIL 3 im redundanten Betrieb und können in Schutzeinrichtungen zur Überwachung von sicherheitsrelevanten Prozessgrößen eingesetzt werden.		
Besondere Bedingungen Specific requirements	Die Sicherheitshinweise im Sicherheitshandbuch und in den Gebrauchsanleitungen der Messumformer sind zu berücksichtigen.		



Der Prüfbericht-Nr.: 968/EZ 272.00/07 vom 12.10.2007 ist Bestandteil dieses Zertifikates.
Der Inhaber eines für den Prüfgegenstand gültigen Genehmigungs-Ausweises ist berechtigt, die mit dem Prüfgegenstand übereinstimmenden Erzeugnisse mit dem abgebildeten Prüfzeichen zu versehen.

The test report-no.: 968/EZ 272.00/07 dated 12.10.2007 is an integral part of this certificate.
The holder of a valid licence certificate for the product tested is authorized to affix the test mark shown opposite to products, which are identical with the product tested.

TÜV Rheinland Industrie Service GmbH
Geschäftsfeld ASI
Automation, Software und Informationstechnologie
Am Grauen Stein, 51105 Köln
Postfach 91 09 51, 51101 Köln

12.10.2007

Datum/Date

Firmenstempel/Company Seal

Dipl.-Ing. Klaus Kemp

Knick
Elektronische Messgeräte
GmbH & Co. KG

Beuckestr. 22 • 14163 Berlin
Germany

Phone: +49 30 80191-0

Fax: +49 30 80191-200

info@knick.de

www.knick-international.com

Copyright 2018 • Sous réserve de modifications

Version : 1.1

Dernière mise à jour de ce manuel le 10/04/2018

Les documents actuels peuvent être téléchargés sur
le site, sous le produit correspondant.



094230

20180410

TS-254.111-KNF02