



► Identification and Access Management – I.A.M.

PILZ
THE SPIRIT OF SAFETY

De la gestion des accès à la sécurisation de la maintenance ainsi que la protection des données et des réseaux, en passant par la sélection du mode de fonctionnement en toute sécurité, découvrez un système réunissant sécurité et sûreté !



► Identification and Access Management – I.A.M.



Plus d'informations sur la Gestion des Identités et des Accès

Pour une protection complète de vos collaborateurs et une sécurisation optimale de vos machines, vous avez besoin d'un concept de sécurité global tenant compte à la fois **de la sécurité et de la sûreté**. Car aujourd'hui plus que jamais, il est impossible de garantir une sécurité optimale sans prendre en compte la sûreté.

La gamme de Gestion des Identités et des Accès vous propose des produits et des solutions personnalisées conçus pour une grande variété de tâches liées aux défis de **la protection des collaborateurs, la responsabilité civile, l'optimisation de la productivité et la protection de vos données**.



Responsabilité civile

Pour ce qui est de la sécurité de leurs collaborateurs, la responsabilité des entrepreneurs et des supérieurs hiérarchiques peut être engagée en fonction de ce qu'ils ont fait ou omis de faire ! Par conséquent, il est essentiel de prendre des mesures appropriées et de s'assurer régulièrement de leur efficacité. Par exemple, les collaborateurs doivent être choisis en fonction des tâches qui leur sont confiées, habilités et équipés des aides requises. En plus des mesures organisationnelles, des solutions techniques, comme la gestion des accès avec le PITreader, peuvent être utilisées. Ainsi, il est possible d'octroyer des autorisations individuelles pour des machines ou des process spécifiques à tout moment avec une traçabilité parfaite.



Protection des collaborateurs

Il est indispensable d'organiser le travail de façon à éviter les risques pour la santé physique et psychique. Par conséquent, les niveaux de risque présents sur les différentes machines et la manière dont les (accès aux) machines doivent être sécurisé(e)s sont à contrôler au moyen d'une évaluation des risques. En plus des autorisations d'accès adéquates au niveau des protecteurs mobiles et de l'habilitation correspondante du personnel, l'utilisation de modes de fonctionnement est un moyen approprié. La sélection du mode de fonctionnement peut être mise en œuvre en toute sécurité à l'aide des produits PITmode, et garantit que chaque collaborateur peut uniquement effectuer les tâches pour lesquelles il est habilité.



Préservation de la productivité

Toutes les réflexions autour de la sécurité ne doivent toutefois pas compromettre la productivité. Les arrêts des machines – avec, dans le pire des cas, des personnes blessées ou des dommages causés aux machines – surviennent souvent à la suite d'une fraude, d'une mauvaise utilisation ou de l'absence de contrôle (des accès). Avec des responsabilités clairement attribuées, des autorisations d'accès adaptées et l'enregistrement des tâches effectuées, vous pouvez prévenir les erreurs et garantir la transparence. Le PITreader et ses fonctions de gestion des accès offrent à cet égard une solution parfaite pour le maintien de la productivité de vos installations.



Protection des données

La protection des données et la sécurité des réseaux font également l'objet d'une attention croissante. La sécurité est désormais inconcevable sans la sûreté, tant elles sont indissociables l'une de l'autre. La future directive Machines, qui entrera en vigueur au sein de l'UE en 2027, en tiendra également compte. Aujourd'hui déjà, il convient de sécuriser vos données, votre savoir-faire et vos processus d'exploitation contre les accès non autorisés. Des produits intelligents, comme le pare-feu industriel SecurityBridge ou l'interface USB commutable PIT ou USB, assurent une sécurité contre les attaques provenant de l'extérieur comme de l'intérieur.

► Exemples d'applications de Identification and Access Management

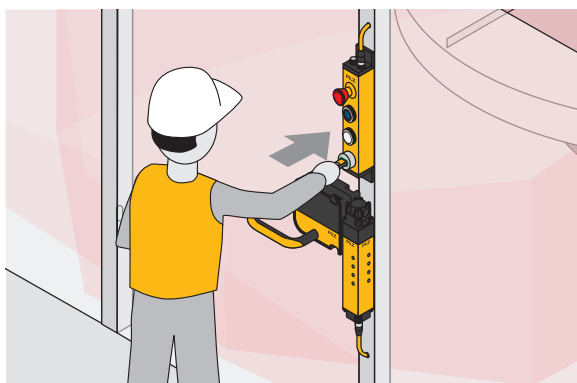
Découvrez des exemples d'applications concrètes et apprenez comment vous pouvez garantir la sécurité et la sûreté à l'aide d'un même système. Les possibilités s'étendent de l'authentification simple à la sélection du mode de fonctionnement en toute sécurité, la sécurisation de la maintenance ainsi que la protection des données et des réseaux, en passant par les autorisations d'accès complexes et la gestion des accès.



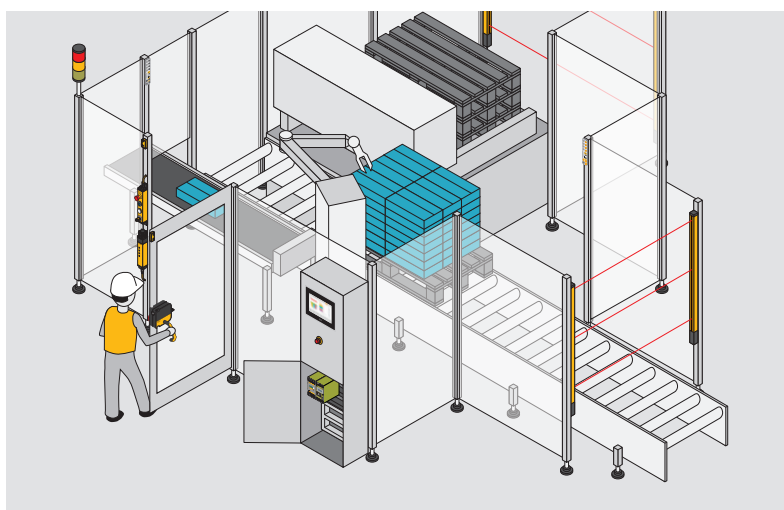
Plus d'informations sur les exemples d'applications

Autorisations et gestion des accès

Un accès sélectif aux machines dangereuses par le biais d'une authentification des utilisateurs permet de protéger vos employés contre les blessures, et vos machines contre une utilisation inappropriée et des dommages. Avec le système d'autorisations d'accès PITreader, il est possible de résoudre de nombreuses problématiques concernant les autorisations d'accès. Les possibilités vont de la simple validation pour remplacer le mot de passe à une matrice complexe d'autorisations hiérarchiques et des codages spécifiques à l'entreprise pour une protection supplémentaire contre la fraude, en passant par l'authentification pour certaines fonctions de parties de machines.



Pour la sécurité des protecteurs mobiles, le système d'autorisations d'accès PITreader offre un aspect de sécurité supplémentaire. Il permet ainsi de ne débloquent l'interverrouillage d'un protecteur mobile qu'une fois l'authentification effectuée. Cela vaut également pour les unités de commande telles que la boîte à boutons-poussoirs PITgatebox. Avec le PITreader intégré, il s'agit de la solution idéale pour l'authentification et la commande dans un seul appareil, qui garantit que seuls les collaborateurs autorisés peuvent exécuter des commandes sur l'installation.



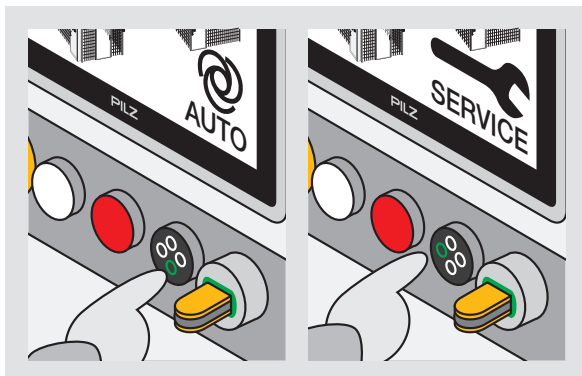
Sécurité des protecteurs mobiles avec authentification par PITreader sur les installations dangereuses.



► Exemples d'applications de Gestion des Identités et

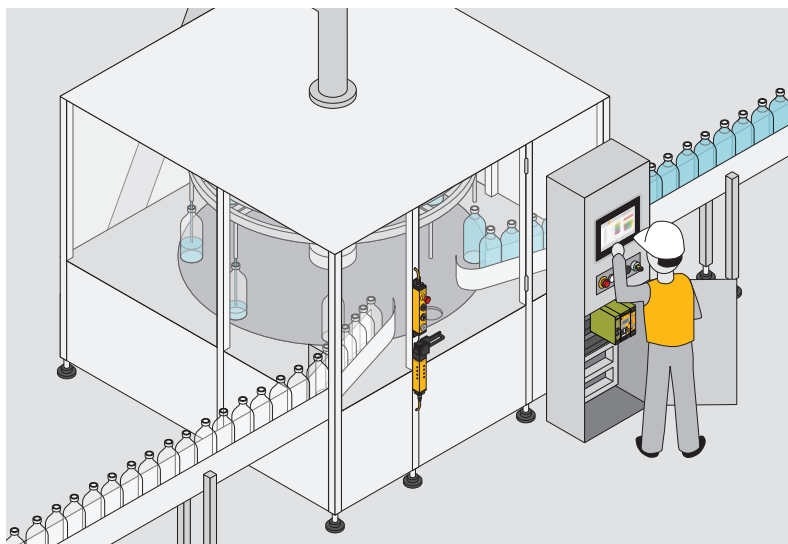


Plus d'informations sur les exemples d'applications



Sélection du mode de fonctionnement en toute sécurité

La sélection du mode de fonctionnement fait partie intégrante de la sécurité fonctionnelle lorsqu'une commutation entre différents niveaux ou différentes fonctions de sécurité est requise. C'est souvent le cas lorsqu'un changement d'outils est à l'ordre du jour ou qu'une machine nécessite de nouveaux réglages. En fonction du mode de fonctionnement sélectionné, un ou plusieurs dispositifs de sécurité, tels que les protecteurs mobiles ou les poignées d'assentiment, sont activés ou désactivés. Cela entraîne une augmentation des risques d'endommagement de l'installation et de blessures pour le personnel, qu'il convient donc de réduire autant que possible. Pour exclure au mieux toute utilisation inappropriée et toute fraude, l'accès à la sélection du mode de fonctionnement doit être réservé à des collaborateurs suffisamment qualifiés et être conçu de manière aussi simple et conviviale que possible pour l'utilisateur.



Commutation fonctionnelle en toute sécurité du mode de fonctionnement par saisie tactile sur PITmode flex visu.

Outre la commutation fonctionnelle en toute sécurité du mode de fonctionnement par autosurveillance jusqu'à PL d cat. 3 selon l'EN ISO 13849-1 ou SIL CL 2 selon l'EN 62061, le système de sélection du mode de fonctionnement et des autorisations d'accès PITmode permet également le réglage des droits d'accès, ce qui en fait la solution parfaite pour vos machines. Avec ses clés électroniques, il offre nettement plus de sécurité que les clés classiques. En effet, ces dernières sont trop souvent insérées dans les machines, offrant aussi peu de sécurité qu'une protection basée sur un mot de passe, qui finit bien souvent par être connu de tous.

Protection des données et sécurité des réseaux

L'importance de la protection des données et de la sécurité des réseaux dans l'environnement des installations industrielles ne cesse de croître. Si vos données, votre savoir-faire et vos processus d'exploitation ne sont pas suffisamment protégés contre les accès non autorisés et la fraude, ce qui permet à une personne malveillante de s'introduire dans votre système de commande depuis l'extérieur, la meilleure protection des protecteurs mobiles ne servira à rien.

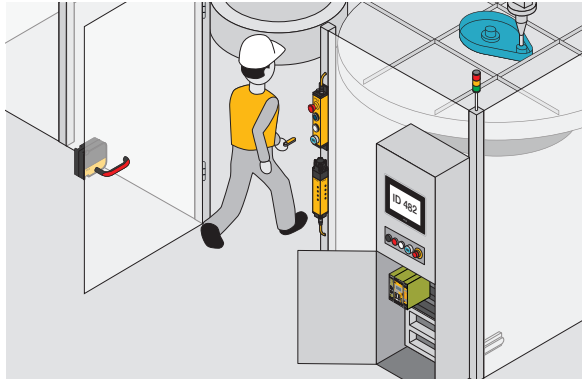
Le pare-feu industriel SecurityBridge surveille le flux de données entre le PC et le système de commande, garantissant ainsi une protection contre les menaces provenant de l'« extérieur », telles que les cyberattaques ou la fraude. En ce qui concerne les dangers venant de l'« intérieur », qu'ils soient causés par l'inattention ou la malveillance, la protection est assurée par l'interface USB activable PIT ou USB. Associé au PITreader, le port USB n'est activé que pour les personnes autorisées et ne permet qu'à ces dernières d'utiliser des appareils USB.

des Accès

Sécurisation de la maintenance « Key in pocket »

Protégez votre personnel des risques associés aux opérations de maintenance ! Utilisez la solution « Key in pocket » de Pilz pour empêcher tout redémarrage non planifié des machines tant que des personnes se trouvent dans la zone dangereuse. En comparaison avec les systèmes Lockout Tagout (LOTO) habituels, la sécurisation de la maintenance est mise en œuvre sur un plan purement électronique par le biais de clés RFID contenant les autorisations adéquates, ce qui rend superflus les dispositifs de verrouillage mécanique et les panneaux d'avertissement.

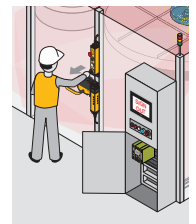
Pour accéder à l'installation, un ou plusieurs utilisateurs s'authentifient avec leurs clés à transpondeur personnelles sur le PITreader au niveau des protecteurs mobiles. Les identifiants de sûreté des utilisateurs sont alors sauvegardés dans une liste sécurisée dans le système de commande (PNOZmulti 2 ou PSS 4000) de Pilz. La machine peut ensuite être arrêtée et il est possible d'y accéder sans danger. Pendant ce temps, le transpondeur est conservé par le collaborateur. Pour remettre l'installation en service, toutes les personnes doivent se déconnecter avec leur transpondeur personnel après avoir quitté l'installation. Cela permet de supprimer la liste sécurisée et de débloquer la machine. En ce qui concerne les installations sans visibilité, le « contrôle de point aveugle » selon l'EN ISO 13849-1 5.2.2 entre également en ligne de compte. Un contrôle visuel de l'installation est alors exigé dans les parties difficilement visibles.



Connexion – saisie dans la liste sécurisée du système de commande Pilz.

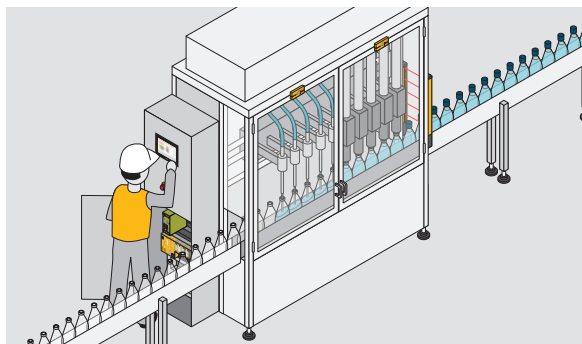


Intervention sur la machine – l'utilisateur a la « key » sur lui.



Déconnexion – suppression de la saisie dans la liste sécurisée du système de commande Pilz.

Étapes du processus de sécurisation de la maintenance « Key in pocket ».



Autorisation de l'interface USB PIT ou USB avec authentification par PITreader.

► Vue d'ensemble des produits PITreader et PITmode



Plus d'informations sur le PITreader et le PITmode

Avec la « Gestion des Identités et des Accès », nous vous proposons une vaste gamme de produits, de solutions et de logiciels issus d'un même fournisseur pour la mise en œuvre de tâches de sécurité et de sûreté.

Autorisations d'accès

PITreader et PITreader S

Avec le **système d'autorisations d'accès PITreader**, vous pouvez mettre en œuvre les tâches les plus diverses en ce qui concerne les autorisations des accès aux machines et aux installations. Elles s'étendent de la simple validation à une matrice d'autorisations complexe et à des codages spécifiques à l'entreprise, en passant par l'authentification. Les clés à transpondeur RFID sont disponibles dans une variante libre d'affectation ou avec des autorisations préparamétrées. Bien entendu, des logiciels adaptés sont disponibles pour la programmation simple des PITreader et des clés à transpondeur. Par ailleurs, le **PITreader S** permet d'intégrer le standard OPC UA. D'une part, cela augmente la sécurité de la communication entre le serveur et le client. D'autre part, le PITreader S étend les possibilités de raccordement sur des systèmes d'autres fabricants qui utilisent également l'OPC UA.



PITreader (S) card

Le **système d'autorisations d'accès PITreader(S) card** propose les mêmes fonctions que les variantes précédemment décrites. Avec le PITreader card et le PITreader sticker cependant, les transpondeurs RFID sont disponibles au format cartes ou jetons autocollants. Le PITreader card présente une zone transparente qui permet de voir l'affichage des états par LED sur le PITreader, même lorsque la carte est en place. Si vous disposez déjà de cartes compatibles RFID dans votre entreprise, vous pouvez également les utiliser pour l'authentification, ou encore employer les fameuses PITreader keys.

Boîte à boutons-poussoirs PITgatebox avec PITreader

Pour une protection optimale des protecteurs mobiles par une authentification, le PITreader S est également proposé dans la boîte à boutons-poussoirs PITgatebox. L'unité de commande avec système d'autorisations d'accès garantit que seuls les collaborateurs autorisés ont accès à l'installation et peuvent exécuter des commandes telles que l'activation, l'arrêt ou l'acquiescement de la machine.



Système de sélection du mode de fonctionnement et autorisations d'accès

PITmode fusion

Le **PITmode fusion** est le modèle modulaire du système de sélection du mode de fonctionnement, employé lors de l'utilisation d'un système de commande de sécurité issu d'un fournisseur tiers. Le système se compose de l'unité de lecture PITreader et de l'unité de contrôle (Safe Evaluation Unit – SEU), qui analyse le mode de fonctionnement sélectionné et commute avec une sécurité fonctionnelle. Cette sélection peut s'effectuer via des boutons-poussoirs existants ou l'élément de commande PIT oe 4S. Les fonctions du PITreader concernant les autorisations d'accès peuvent également être utilisées dans leur intégralité.



PITmode flex

Le **PITmode flex** est la solution pour tous ceux qui utilisent le micro automate configurable PNOZmulti 2 ou le système d'automatismes PSS 4000. Là encore, le PITreader est employé en tant qu'unité de lecture. L'analyse en toute sécurité du mode de fonctionnement est effectuée par un bloc logiciel déjà intégré au PNOZmulti 2 et au PSS 4000. Ainsi, aucune unité de contrôle séparée n'est nécessaire. La sélection du mode de fonctionnement peut être effectuée via l'élément de commande PIT oe 4S ou n'importe quel bouton-poussoir.

PITmode flex visu

Bien que le **PITmode flex visu** propose fondamentalement les mêmes fonctions que le PITmode flex, il se distingue néanmoins par la manière dont le mode de fonctionnement est sélectionné. Au lieu de se faire à l'aide d'un bouton-poussoir, cette sélection s'effectue par commande tactile sur un écran PMLvisu avec le PASvisu.



► Vue d'ensemble des produits et solutions PITmode



Plus d'informations sur le PITreader et le PITmode

Vue d'ensemble du système de sélection du mode de fonctionnement et des autorisations d'accès PITmode

	PITmode 3.xx	PITmode fusion	PITmode flex
Composants de la solution			
Application	► Système d'autorisations d'accès ► Sélection du mode de fonctionnement en toute sécurité jusqu'à PL d	► Système d'autorisations d'accès ► Sélection du mode de fonctionnement en toute sécurité jusqu'à PL d	► Système d'autorisations d'accès ► Sélection du mode de fonctionnement en toute sécurité jusqu'à PL d
Type	Compact	Modulaire avec boutons-poussoirs	Intégré et flexible avec boutons-poussoirs
Fonction principale	Sélection du mode de fonctionnement avec : ► 5 modes de fonctionnement ► 1 zone de travail	Sélection du mode de fonctionnement avec : ► 5 modes de fonctionnement ► 1 zone de travail	Sélection du mode de fonctionnement avec : ► 8 modes de fonctionnement ► 10 zones de travail
Utilisation	Utilisation avec des systèmes de commande FS de Pilz ou d'une autre marque pour la sélection du mode de fonctionnement et des autorisations d'accès	Utilisation avec des systèmes de commande FS de Pilz ou d'une autre marque pour la sélection du mode de fonctionnement et des autorisations d'accès	Utilisation avec des systèmes de commande FS de Pilz pour les autorisations d'accès et la sélection du mode de fonctionnement
Unité de contrôle de sécurité	Intégrée	En tant que composants SEU autonomes	Bloc logiciel intégré au système de commande FS de Pilz (PNOZ m B1 et PSSu PLC)
Saisie via	2 ou 4 boutons-poussoirs intégrés	► PIT oe 4S ► Bouton-poussoir tiers	► PIT oe 4S ► Bouton-poussoir tiers

Logiciel pour le PITreader

PITreader Webserver

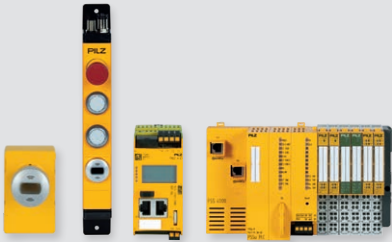
Le Webserver intégré permet de programmer facilement les clés à transpondeur du PITreader keys avec les données utilisateur et les autorisations ainsi que tous les autres paramètres importants du PITreader directement sur l'appareil. Cela permet d'effectuer rapidement la mise en service du PITreader, la configuration des interfaces et, le cas échéant, la liaison avec le serveur OPC UA.



PIT Transponder Manager (PTM)

Gérez rapidement et facilement le PITreader keys avec les paramètres utilisateur, les listes de blocage et vos données utilisateur grâce à l'interface graphique du PIT Transponder Manager. En quelques étapes, vous pouvez octroyer des autorisations d'utilisateur individuelles grâce à des modèles préconfigurés. Pour ce faire, vous pouvez créer les utilisateurs un par un ou les intégrer via la fonction d'importation. Profitez de la possibilité de lire les informations directement dans la base de données intégrée.

et PITreader

PITmode flex visu	PITreader autonome	Key in pocket
		
▶ Système d'autorisations d'accès ▶ Sélection du mode de fonctionnement en toute sécurité jusqu'à PL d	▶ Système d'autorisations d'accès	▶ Système d'autorisations d'accès ▶ Sécurisation de la maintenance « Key in pocket »
Intégré et flexible avec Visu	Compact	Compact
Sélection du mode de fonctionnement avec : ▶ 8 modes de fonctionnement ▶ 10 zones de travail	Sûreté pour les autorisations d'accès pour IHM, sécurisation des processus et des protecteurs mobiles	Sécurisation de la maintenance avec protection contre le redémarrage non autorisé
Utilisation avec des systèmes de commande FS de Pilz pour les autorisations d'accès et la sélection du mode de fonctionnement	Couplage à des systèmes API et IHM	Utilisation avec des systèmes de commande FS de Pilz pour la sécurisation de la maintenance
Bloc logiciel intégré au système de commande FS de Pilz (PNOZ m B1 et PSSu PLC)	-	-
Tuile de saisie tactile dans le PASvisu	-	Boutons-poussoirs



Système d'authentification des utilisateurs (User Authentication Service – UAS)

Le système d'authentification des utilisateurs (UAS) relie le système d'autorisations d'accès PITreader au système de gestion des données d'accès et des autorisations PIT Transponder Manager (PTM) en toute sécurité via HTTPS. Le système d'organisation gère toutes les autorisations et les analyse par le biais d'une base de données centrale d'autorisations pour tous les utilisateurs de clés à transpondeur. Cette base de données est alimentée par l'importation du PTM. L'UAS diffuse des fonctions telles qu'une liste de blocage à tous les PITreader mis en réseau. Par ailleurs, des informations de diagnostic complètes sont disponibles de manière centralisée.

► Support technique

Pilz vous propose une assistance technique 24 heures sur 24.

Amérique

Brésil

+55 11 97569-2804

Canada

+1 888 315 7459

Mexique

+52 55 5572 1300

USA (appel gratuit)

+1 877-PILZUSA (745-9872)

Asie

Chine

+86 400-088-3566

Corée du sud

+82 31 778 3300

Japon

+81 45 471-2281

Australie et Océanie

Australie

+61 3 95600621

Nouvelle-Zélande

+64 9 6345350

Europe

Allemagne

+49 711 3409-444

Autriche

+43 1 7986263-444

Belgique, Luxembourg

+32 9 3217570

Espagne

+34 938497433

France

+33 3 88104003

Irlande

+353 21 4804983

Italie, Malte

+39 0362 1826711

Pays-Bas

+31 347 320477

Royaume-Uni

+44 1536 462203

Scandinavie

+45 74436332

Suisse

+41 62 88979-32

Turquie

+90 216 5775552

Pour joindre notre hotline internationale, composez le :

+49 711 3409-222

support@pilz.com

Pilz développe des produits qui protègent l'environnement grâce à l'utilisation de matériaux écologiques et de techniques à faible consommation d'énergie. Notre production est effectuée dans des bâtiments de conception écologique qui respectent l'environnement et avec une faible consommation d'énergie. Pilz favorise ainsi le développement durable en vous offrant des produits avec efficacité énergétique et des solutions écologiques.



Fourni par :



Nous sommes représentés à l'échelle internationale. Pour plus de renseignements, consultez notre site Internet www.pilz.com ou prenez contact avec notre maison mère.

Maison mère : Pilz GmbH & Co. KG, Felix-Wankel-Straße 2, 73760 Ostfildern, Allemagne
Téléphone : +49 711 3409-0, Télécopie : +49 711 3409-133, E-mail : info@pilz.com, Internet : www.pilz.com

Imprimé à 100 % sur du papier recyclé dans le respect de l'environnement.

PILZ
THE SPIRIT OF SAFETY

12-3-fr-3-004, 2023-04 Printed in Germany
© Pilz GmbH & Co. KG, 2023

CECE®, CHRE®, CMSE®, InduraNET p®, Leansafe®, Master of Safety®, PAS4000®, PAScale®, PASconfig®, Pilz®, PTT®, PLID®, PMCPromote®, PMCTendo®, PMD®, PMJ®, PNOZ®, PRET®, PRCM®, PRIMO®, PRM®, PRM p®, PSEN®, PSS®, SafetyBUS p®, SafetyNET p®, THE SPIRIT OF SAFETY® sont, dans certains pays, des marques déposées de Pilz GmbH & Co. KG. Nous vous signalons que les caractéristiques des produits peuvent diverger des indications fournies dans ce document en fonction de la mise à l'impression et de l'étendue de la présentation. Nous déclinons toute responsabilité quant à la validité, l'exactitude et l'intégralité des informations fournies dans les textes et les images. Si vous avez des questions, veuillez prendre contact avec notre assistance technique.