Informations d’ordre général

Pilz GmbH & Co. KG
Felix-Wankel-Straße 2
73760 Ostfildern,
Allemagne
Allemagne/Germany
www.pilz.com

Les solutions d’amélioration se concentrent sur l’accès pour garantir la sécurité et la sûreté industrielle des machines

Une sécurité globale grâce à la gestion personnalisée des autorisations

Ostfildern, février 2023 – **Dans tous les endroits où il est nécessaire de protéger des objets de valeur, nous installons des portes, des serrures et des clés afin de limiter l’accès. Cela vaut également pour notre bien le plus précieux : notre sécurité sous toutes ses formes. En environnement industriel, il convient de protéger d’une part les personnes (sécurité) et d’autre part les machines et les données sensibles (sûreté industrielle). Une sécurité défaillante peut avoir diverses conséquences, d’une fausse manœuvre à un accident en passant par une cyberattaque majeure. Une gestion complète des identités et des accès qui régit clairement les autorisations en la matière contribue à un concept de sécurité global et à des processus efficaces.**

Dans l’environnement de production, les protecteurs mobiles qui indiquent clairement aux opérateurs la présence d’une zone sensible et la nécessité de faire preuve de prudence font partie du quotidien. Une interface homme-machine (Human Machine Interface ou HMI) ou une clé est requise pour accéder au processus situé derrière cette barrière de sécurité. Mais que se passe-t-il si la personne n’est pas qualifiée ou autorisée et s’expose à un danger ou en fait courir à d’autres ? De plus, une personne mal intentionnée peut être à l’origine d’une fraude affectant le processus, directement depuis la machine ou via un accès à distance. En matière d’autorisation d’accès, sécurité et sûreté industrielle sont étroitement liées. En outre, la sûreté industrielle garantit l’intégrité de la sécurité au niveau de la machine. Elle protège par exemple les machines ou les installations contre les accès non autorisés depuis l’extérieur, ainsi que les données sensibles des processus et des machines contre une falsification, une perte ou un accès non autorisé au niveau interne. Cela

inclut aussi bien les attaques délibérées que les incidents involontaires liés à la sûreté.

La sécurité et la sûreté industrielle vont de pair

Pour les exploitants de machines et d'installations, il est nécessaire d'attribuer les tâches et les autorisations de manière claire, et donc d'établir une gestion des identités et des accès. Cela implique non seulement de mettre en place des mesures organisationnelles telles que des directives de travail ou des contrôles réguliers des procédures, mais aussi d'intégrer des solutions de sécurité adaptées dans l'environnement de production. Lorsque ces mesures ne sont pas respectées, les personnes responsables au sein d'une entreprise peuvent être poursuivies à titre personnel en cas d'accident ou d'arrêt de production. Jusqu'ici, ces solutions de sûreté reposaient sur le volontariat et, dans de nombreux endroits, aucune intervention n'était jugée nécessaire. Toutefois, entretemps, les législateurs ont reconnu que la sécurité et la sûreté sont interdépendantes. C'est pourquoi la nouvelle directive Machines impose des mesures de sûreté obligatoires.

Les modes de fonctionnement renforcent la sécurité.

De plus, diverses normes C prescrivent que les différents modes de fonctionnement doivent aussi inclure des fonctions de sécurité correspondantes. Il peut s'agir par exemple du mode automatique, de l'intervention manuelle dans des conditions limitées ou du mode maintenance. La norme EN ISO 16090-1 pour les centres d'usinage et les machines spéciales impose obligatoirement au moins deux de ces modes de fonctionnement afin de garantir la sécurité fonctionnelle. Il est important de s'assurer qu'un seul mode de fonctionnement à la fois soit sélectionné et actif, et que celui-ci soit clairement indiqué.

Interdiction de l’accès anonyme

Mais comment décider qui a accès aux différents modes de fonctionnement et est autorisé à modifier ces derniers ? Pour cela, il faut définir les différents groupes de personnes qui peuvent accéder à la machine, tels que le personnel d’exploitation, de nettoyage ou de maintenance. Ensuite, les collaborateurs sont affectés à ces groupes en fonction de leur tâche ou de leur qualification. Selon la taille de l’entreprise, les autorisations ou les droits d’accès peuvent être octroyés à différents groupes d’utilisateurs ou, par exemple, à un type de machine utilisé dans toute l’entreprise. À l’issue d’une appréciation du risque, les experts en sécurité évaluent et analyse le risque lié à l’accès anonyme pour chaque danger. Enfin, des mesures de réduction du risque conformes à l’état de l’art et tenant compte des normes harmonisées sont mises en place.

La convivialité empêche la fraude

Lors de la mise en œuvre des mesures, il est important de garantir la facilité de prise en main et la convivialité pour les utilisateurs de l’entreprise afin d’exclure la fraude. Pour les fabricants de machines, cette règle s’applique dès le processus de développement. Les systèmes de commande intuitifs et conviviaux empêchent la mise en place de mesures de contournement de la sécurité ou les utilisations incorrectes des machines. De plus, un système de sécurité bien pensé contribue à des processus efficaces sans temps d’arrêt inutiles. C’est précisément cette problématique du « contournement des dispositifs de protection » qui constitue un point central de la norme EN ISO 14119. Cette dernière définit des principes de conception et de sélection des systèmes pour protecteurs mobiles et propose ainsi une aide concrète sur la manière d’éviter la fraude.

Solutions de sécurité personnalisées

Afin qu'une ouverture volontaire ou involontaire des portes d'accès ne présente pas de danger, celles-ci sont sécurisées à l'aide d'un système de sécurité pour protecteurs mobiles. En matière de sécurité, la protection de l'opérateur vis-à-vis des mouvements dangereux de la machine figure au centre des priorités. Selon qu'il s'agit d'une machine autonome ou d'installations complexes en réseau, une solution de sécurité sur mesure est nécessaire. Si les machines présentent une inertie dangereuse, l'interverrouillage joue un rôle important. Si les protecteurs sont franchissables, un système de déblocage à des fins d'évacuation s'impose.

Sécurisation sur mesure des protecteurs mobiles

Un système modulaire pour protecteurs mobiles tel que le PSENmlock de Pilz combine dans un même système la surveillance en toute sécurité des protecteurs mobiles et l'interverrouillage en toute sécurité. Il intègre en outre des fonctions de sécurité telles que l'arrêt d'urgence, le déblocage à des fins d'évacuation et un anti-redémarrage mécanique. Il offre la flexibilité et l'intelligence décentralisée nécessaires pour sécuriser de nombreuses applications. Une solution personnalisée associe des capteurs, un système de déblocage à des fins d'évacuation, des poignées de porte, ainsi qu'une boîte de commande à boutons-poussoirs. En fonction de l'application, les utilisateurs définissent ainsi leur solution personnalisée pour protecteurs mobiles. Afin de satisfaire aux exigences de sûreté industrielle, les accès et les autorisations sont désormais pris en compte.

Un seul système pour la sécurité et la sûreté industrielle

En pratique, la protection contre l'accès non autorisé peut être obtenue à l'aide d'un système de sélection du mode de fonctionnement et des autorisations d'accès. Ce dernier associe

sécurité et sûreté industrielle : la sélection du mode de fonctionnement et la gestion des autorisations d'accès à la machine. Les appareils de la gamme PITmode de Pilz constituent une solution de ce type permettant de basculer entre les modes de fonctionnement définis et la gestion des autorisations d'accès. L'utilisation est intuitive : chaque utilisateur reçoit son transpondeur codé individuel permettant une authentification utilisateur claire afin d'éviter toute fraude.

Gestion individuelle des accès et des modes de fonctionnement

Afin de personnaliser le concept de sécurité, le PITmode est proposé dans différentes versions. En tant qu'appareil compact tout-en-un, le PITmode inclut les boutons-poussoirs pour la sélection du mode de fonctionnement ainsi qu'une unité de contrôle, ce qui permet une installation peu encombrante. Le système modulaire PITmode fusion, pour sa part, est constitué de l'unité de lecture PITreader avec technologie RFID et Webserver intégré, ainsi que d'une unité de contrôle de sécurité Safe Evaluation Unit (SEU). Le PITmode flex est une autre variante : le PITreader est alors utilisé avec un système de commande de Pilz et un bloc logiciel pour l'analyse sécurisée. Son architecture modulaire permet l'intégration des autorisations d'accès et de la sélection du mode de fonctionnement à la conception des pupitres de commande existants. Les boutons-poussoirs existants peuvent être utilisés pour la sélection du mode de fonctionnement, ce qui simplifie l'utilisation. L'identification à l'aide du transpondeur est réalisée par l'unité de lecture PITreader. Le PITmode et le PITmode fusion offrent la sécurité fonctionnelle pour la sélection du mode de fonctionnement et les autorisations d'accès jusqu'à PL d.

Authentification simplifiée, même à distance

Pour sélectionner le mode de fonctionnement, l'utilisateur insère directement son transpondeur dans le PITmode et actionne une touche configurée pour le mode de fonctionnement ou la touche correspondante sur une HMI. Si l'autorisation a été accordée, l'utilisateur peut accéder au processus. Le même principe s'applique lorsqu'un agent de maintenance souhaite accéder à une machine à distance : la maintenance à distance ne peut pas commencer tant qu'une personne sur site n'a pas validé l'autorisation correspondante dans le système. Une fois la maintenance terminée, cet accès est refermé avant la remise en route de la machine. Cela permet d'éviter toute fraude par une personne non autorisée ou de laisser un port ouvert par inadvertance après les travaux de maintenance. Les exploitants renforcent ainsi la sûreté industrielle en pilotant l'attribution des autorisations et donc l'accès au processus.

Une solution complète pour la gestion des accès

Quand seule la gestion des accès est requise, le PITreader peut être utilisé en tant qu'appareil autonome ou en association avec un système de commande de Pilz en tant que système d'autorisations d'accès. En association avec le micro automate configurable de sécurité PNOZmulti 2, l'administrateur configure les autorisations d'accès aux machines et aux installations par simple glisser-déplacer à partir du logiciel de configuration PNOZmulti Configurator associé. Celles-ci sont ensuite transférées sur les clés à transpondeur RFID via l'unité de lecture PITreader. Grâce à l'intégration du standard OPC UA, la variante PITreader S peut être mise en place indépendamment d'un système de commande de Pilz, quelle que soit la marque du fabricant. Comme cela a déjà été

évoqué, les appareils PITmode peuvent être facilement intégrés aux écrans de commande existants.

Clé, carte ou jeton autocollant : à vous de choisir

La variante PITreader card unit offre davantage de flexibilité aux exploitants et aux utilisateurs : les cartes et jetons autocollants compatibles RFID peuvent être utilisés avec ou à la place d'une clé à transpondeur RFID. Si l'entreprise utilise déjà des cartes compatibles RFID, celles-ci peuvent également être employées avec le PITreader card unit : les utilisateurs n'ont ainsi besoin que d'une seule carte pour assurer plusieurs fonctions différentes. Fondamentalement, l'avantage des transpondeurs RFID – qu'ils utilisent une clé, une carte ou un jeton autocollant – tient au fait que plusieurs fonctions sont regroupées sur un seul transpondeur, créant ainsi un porte-clés mécanique. Cette configuration est confortable pour l'utilisateur, car il ne porte qu'un seul support d'identification sur lui. Les administrateurs, pour leur part, gagnent du temps sur la gestion et la maintenance des clés.

Un plus en matière de sûreté

Les aspects liés à la sûreté sont également pris en compte en ce qui concerne l'authentification des utilisateurs, la qualification et la protection des accès. Si un accident ou un incident de sûreté se produit sur la machine malgré toutes les mesures de sécurité mises en place, la lecture du transpondeur RFID permet de savoir qui a procédé à quelle modification. Lorsque cette fonction optionnelle est souhaitée, le système de commande enregistre également la durée d'accès dans le journal d'audit interne infalsifiable par l'intermédiaire de l'authentification.

La clé réside dans une administration rigoureuse

Pour garantir la sécurité et la sûreté industrielle sur l'ensemble du cycle de vie de l'application, les administrateurs consacrent beaucoup d'attention à la gestion des autorisations. Pour simplifier l'administration, des logiciels de Pilz adaptés prennent en charge l'organisation des utilisateurs et des transpondeurs. Ainsi, une petite clé RFID peut renfermer des matrices d'autorisations complexes ou des exigences régies au niveau de l'entreprise. Avec le PITreader Webserver intégré, les administrateurs programment les transpondeurs RFID associés au PITmode ou au PITreader et enregistrent dessus les données utilisateur et les autorisations. Tous les réglages importants sont effectués directement sur l'unité de lecture, ce qui accélère la mise en service, y compris la configuration des interfaces.

Limitation de l'accès aux interfaces

Les possibilités de gestion des identités et des accès couvrent également l'activation de ports USB industriels spécifiques, l'un des principaux points d'intrusion en cas d'incident de sûreté. Pour cela, le système d'autorisations d'accès PITreader est associé à un élément de commande comme le PIT oe USB qui dispose d'une interface maître USB 2.0 activable. Cette solution permet d'importer des programmes, d'extraire des données et de raccorder un clavier ou une souris de manière infraudable. En effet, l'activation de l'interface s'effectue exclusivement par le biais de l'autorisation correspondante et protège ainsi le flux de données de fabrication. En association avec un pare-feu industriel tel que le SecurityBridge de Pilz qui contrôle la communication de données au sein d'un réseau d'automatismes industriel, les machines peuvent être protégées contre les accès non autorisés et la fraude.

Sécurité et sûreté des machines existantes

Lorsque des machines existantes doivent être modernisées ou qu'une nécessité d'intervention sur ces dernières a été identifiée à la suite d'une évaluation du risque, le système d'autorisations d'accès PITreader peut facilement être installé en deuxième monte pour la mise en conformité : sur les sorties normées pour les commutateurs à clé d'un diamètre de 22,5 mm, l'appareil peut être monté directement. En association avec un système de commande de Pilz, il est possible de configurer directement la fonction de sécurité souhaitée. Si un système de commande tiers est utilisé, le PITmode fusion est installé afin d'intégrer le contrôle des autorisations d'accès et la sélection du mode de fonctionnement. En fonction du support pour transpondeur envisagé, il est possible d'utiliser les cartes à clé RFID présentes dans l'entreprise pour l'authentification.

Conclusion

Pour protéger notre bien le plus précieux, à savoir notre sécurité, il est nécessaire d'élaborer des solutions d'amélioration globales et de les mettre régulièrement à jour. Un système de gestion des identités et des accès qui régit clairement les autorisations et les accès au sein d'une entreprise en est une composante importante. La solution est un concept regroupant les mesures et prescriptions organisationnelles ainsi que les fonctions de sécurité appropriées. Pour cela, un système d'autorisations d'accès tel que le PITreader représente le bloc matériel idéal. Il peut être complété par des extensions logicielles pour l'organisation des utilisateurs et des transpondeurs. D'autres composants (système pour protecteurs mobiles, système de commande, logiciels et fonctions telles que la sélection du mode de fonctionnement) viennent compléter la solution afin de bénéficier d'un concept de sécurité et de sûreté

industrielle global. La prise en main est simple pour l’utilisateur grâce à sa clé individuelle.

Caractères : 14 675

Illustrations

Illustration 1 :
F_Press_IAM_Man_using_PITreader_Key_cold1.jpg (© Pilz GmbH & Co. KG)

Légende : Une gestion des identités et des accès complète régit l’accès à l’application et garantit ainsi l’intégrité des fonctions et mesures de sécurité – sécurité et sûreté industrielle incluses.

Illustration 2 :
F_Press_PITmode_fusion_402251_PIT_oe_4023311_P1_B_8_2_cold_2020_01 (Pilz GmbH & Co. KG)

Légende : Le PITmode fusion de Pilz est un système de sélection du mode de fonctionnement et des autorisations d'accès à conception modulaire qui réunit les fonctions de sécurité et de sûreté industrielle au sein d'un même système.

Illustration 3 :
F_Press_PITreader_S_card_unit_402321_and_PITreader_card_ye_g_402330_P1_B8_2_cold.jpg (Pilz GmbH & Co. KG)

Légende : Avec les cartes PITreader card et les jetons autocollants PITreader sticker comptables RFID, le système d'autorisations d'accès PITreader card unit de Pilz propose de nouveaux formats pour la mise en œuvre d'un système d'autorisations d'accès efficace.

Illustration 4 :

F_Press_PITreader_Webserver.jpg (© Pilz GmbH & Co. KG)

Légende : Les clés à transpondeur RFID sont analysées et configurées dans le PITreader. L'octroi des autorisations d'accès et des modes de fonctionnement s'effectue simplement via le Webserver associé.

Illustration 5 :
F_Press_Group_7_Modular_safety_gate_system_with_diagnostic_and_evaluation_P1_B8_2_cold_v0.jpg (© Pilz GmbH & Co. KG)

Légende : L'association flexible du système pour protecteurs mobiles PSENmlock, de l'ensemble poignée de porte adapté (en haut à gauche), de la boîte à boutons-poussoirs PITgatebox avec système d'autorisations d'accès intégré PITreader (en haut à droite), ainsi que du micro automate configurable de sécurité PNOZmulti 2 (en bas à droite) et de la solution de diagnostic Safety

Device Diagnostics (en bas à gauche) offre une solution complète pour protecteurs mobiles avec autorisations d'accès.

Encadré : Sécurisation numérique de la maintenance « clés en poche »

En plus de la gestion des autorisations d'accès proprement dite, le PITreader peut être utilisé avec un système de commande de Pilz tel que le micro automate configurable PNOZmulti 2 ou le système d'automatismes PSS 4000 pour la sécurisation numérique et efficace de la maintenance « clés en poche ». Grâce à elle, la machine ne redémarre pas pendant les opérations de maintenance et les personnes non autorisées n'y ont pas accès. En pratique, le système « clés en poche » fonctionne comme suit : un ou plusieurs utilisateurs autorisés à effectuer les travaux de maintenance s'authentifient sur l'installation. Après une authentification réussie, un identifiant de sûreté personnalisé est enregistré pour l'utilisateur sur une liste sécurisée dans le système de commande de Pilz. La machine peut alors être arrêtée, le protecteur mobile ouvert et l'utilisateur peut accéder à la machine. Pendant ce temps, les clés RFID restent « dans la poche de pantalon » de chaque utilisateur. Lorsque la maintenance est terminée et que toutes les personnes ont quitté la zone dangereuse, elles se déconnectent. Les identifiants de sûreté sont supprimés de la liste sécurisée du système de commande de Pilz et la machine peut être redémarrée. Contrairement à une sécurisation de la maintenance à l'aide de clés mécaniques, il est possible d'accéder à l'installation et de la quitter au niveau de n'importe quel protecteur mobile. Ainsi, la solution « Key-in-pocket » offre au personnel davantage de flexibilité et lui permet de gagner du temps lors de la maintenance. La sécurisation

numérique de la maintenance est spécialement conçue pour les machines comportant des zones dangereuses protégées par des enceintes de sécurité. L'exploitant sait à tout moment qui a accès à quelle tâche et peut également octroyer des autorisations temporaires.

1 578 caractères

Illustration de l'encadré Clés en poche :
F_Press_Group_PIT_Key_in_pocket_solutions_P1_B8_2_cold.jpg (© Pilz GmbH & Co. KG)

Légende : La sécurisation de la maintenance « Key-in-pocket » est composée du système d'autorisations d'accès PITreader, de la boîte à boutons-poussoirs PITgatebox et d'un système de commande de Pilz tel que le micro automate configurable PNOZmulti 2 ou le système d'automatismes PSS 4000.

Encadré : Octroi et gestion des autorisations

Lorsqu'un système d'autorisations d'accès est installé dans l'entreprise, la maintenance et la gestion régulières des autorisations et des données utilisateur sont essentielles pour garantir un niveau de sécurité élevé. Pour cela, Pilz met à disposition le logiciel PIT Transponder Manager (PTM) : via une

interface graphique, l’administrateur gère les réglages utilisateur, les listes de blocage et les données utilisateur. Des modèles préconfigurés et une fonction d’importation permettent l’écriture des autorisations utilisateur personnelles sur les transpondeurs RFID en seulement quelques étapes.

Si plusieurs PITmode ou PITreader sont utilisés dans une entreprise, ils peuvent être coordonnés avec le logiciel PIT User Authentication Service (UAS) de Pilz. Celui-ci permet de relier les systèmes de gestion, tels que le PTM ou un autre logiciel de gestion des utilisateurs, au PITreader. Le PIT UAS dispose d’une base de données d’autorisations centralisée pour les utilisateurs et permet ainsi l’importation et l’attribution des données issues du PTM à tous les PITreader. Les administrateurs peuvent consulter l’état de l’ensemble des PITreader ainsi qu’une liste de diagnostics. De cette manière, ils conservent une vue d’ensemble rapide même en cas d’utilisation de plusieurs appareils.

1 218 caractères

Illustration de l’encadré Gestion des utilisateurs :
((image à venir)).jpg (© Pilz GmbH & Co. KG)

Légende : Si plusieurs unités de lecture PITreader

sont utilisées dans une entreprise, elles peuvent être coordonnées avec le logiciel User Authentication Service (UAS).

Groupe Pilz

Le groupe Pilz est un fournisseur mondial de produits, de systèmes et de prestations de services pour les techniques d'automatismes. L'entreprise familiale dont le siège se trouve à Ostfildern (Allemagne) emploie environ 2 500 personnes. Avec 42 filiales et succursales, Pilz fournit dans le monde la sécurité pour les hommes, les machines et l'environnement.
Leader technologique, elle propose des solutions complètes pour les automatismes, qui englobent les capteurs, les systèmes de contrôle-commande et le Motion Control, y compris des systèmes pour la communication industrielle, le diagnostic et la visualisation. Une offre internationale de prestations de services, comprenant les conseils, l'ingénierie et les formations, complète la gamme. Au-delà de la construction de machines et d'installations, les solutions de Pilz sont utilisées dans de nombreux secteurs d'activités, comme l'intralogistique, le ferroviaire ou le domaine de la robotique.

www.pilz.com

Interlocuteurs pour la presse :

Martin Kurth

Presse d'entreprise et presse spécialisée
Tél. : +49 711 3409-158
m.kurth@pilz.de

Sabine Karrer

Presse spécialisée et presse d'entreprise
Tél. : +49 711 3409-7009
s.skaletz-karrer@pilz.de

Jenny Skarman

Presse spécialisée

Tél. : +49 711 3409-1067
j.skarman@pilz.de

Sabrina Schilling

Presse spécialisée

Tél. : +49 711 3409-7147
s.schilling@pilz.de

Hansjörg Sperling-Wohlgemuth
Gestion des congrès et des conférences
Tél. : +49 711 3409-239
h.sperling@pilz.de