



► Cybersécurité industrielle au moyen de zones

PILZ
THE SPIRIT OF SAFETY

Plus de sécurité et d'efficacité grâce à la séparation claire
entre les fonctions standard et les fonctions de sécurité



► Cybersécurité industrielle au moyen de zones et conduits

Protection des machines contre la corruption

Outre les systèmes informatiques (IT), les machines du domaine de la technologie opérationnelle doivent elles aussi être protégées de manière fiable contre les cyberattaques et les fraudes. À cet égard, la règle suivante s'applique : La sécurité des machines est toujours la priorité absolue et ne doit en aucun cas être compromise par des accès non autorisés. En Europe, cette exigence devient obligatoire en vertu du Règlement machines de l'UE : comment protéger efficacement les fonctions et les systèmes de commande dédiés à la sécurité ?

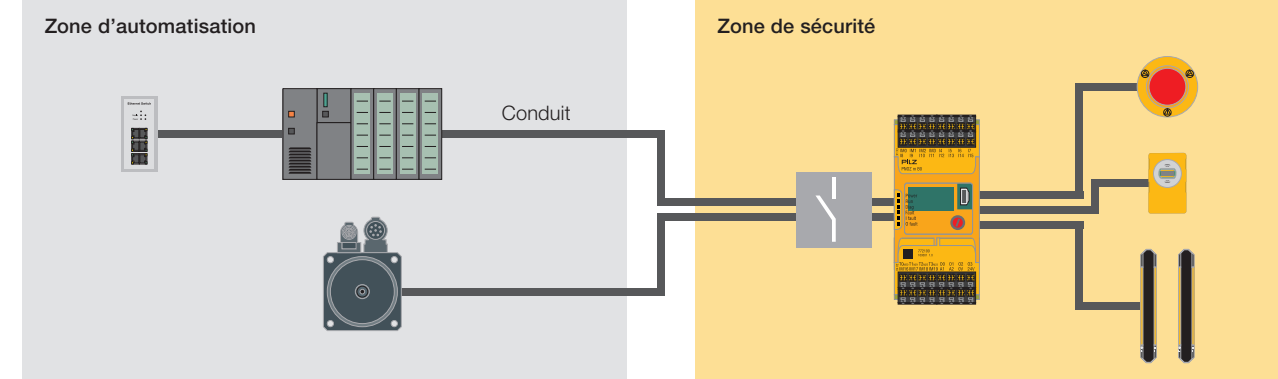
Des structures claires pour une sécurité maximale

Une approche qui a fait ses preuves consiste à séparer systématiquement les fonctions de sécurité en une zone distincte dotée d'un niveau de sécurité défini. Les connexions sécurisées (conduits) assurent une communication sécurisée entre les zones et réduisent les risques au minimum. Ainsi, les zones et conduits permettent de mettre en place une architecture claire et axée sur la sécurité pour les machines et installations.

Quel est le rôle des zones et des conduits ?

- Une évaluation plus claire des risques : Les zones permettent une analyse claire et précise, conformément à la norme EN ISO 12100.
- Mesures de sécurité ciblées : Chaque zone se voit attribuer un niveau de sécurité adapté, pour une protection efficace là où elle est vraiment nécessaire.
- Moins de points vulnérables : Les connexions sécurisées (conduits) garantissent la sécurité des communications et réduisent les cyberrisques.

IACS (Industrial Automation and Control Systems)



Séparation du système de commande de sécurité en une zone distincte avec un niveau de sécurité accru

Vos avantages :

- + une structure de sécurité claire grâce à la séparation des zones critiques pour la sécurité et des zones non critiques
- + une meilleure planification des mesures de sécurité, de maintenance et d'extension
- + une disponibilité accrue des machines grâce à une maintenance ciblée des zones
- + une cybersécurité efficace : Les niveaux de sécurité parfaitement adaptés par zone protègent les réseaux et les données
- + évolutivité aisée pour l'ajout de modules ou de machines supplémentaires
- + une documentation transparente garantissant la conformité CE



Info pratique : Cybersécurité industrielle pour réduire les risques

Découvrez comment les solutions de cybersécurité industrielle réduisent les risques liés à la sécurité des machines : www.pilz.com/security



► Bon à savoir

Avec les solutions de Pilz, telles que les gammes de relais de sécurité PNOZ, vous misez sur la sécurité : ceux-ci ne présentent aucune vulnérabilité sur le réseau et renforcent ainsi la cybersécurité industrielle de votre zone de sécurité !



Pour en savoir plus :
www.pilz.com/pnoz



Bonnes pratiques concernant les zones et les conduits :

- EN IEC 62443-3-2 : Segmentation du réseau en zones, séparation des systèmes de commande dédiés à la sécurité
- EN 50742 : Sécurité des machines – Protection contre la corruption au moyen de niveaux de sécurité dédiés à la sécurité
- TRBS 1115-1 : Obligations des exploitants de machines – La cybersécurité dans le cadre de l'évaluation des risques, protection de la sécurité par l'analyse des menaces
- MITRE ATT&CK : Séparation des systèmes de sécurité des réseaux d'exploitation

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, E-mail : info@pilz.com, Internet : www.pilz.com

PILZ
THE SPIRIT OF SAFETY