Règles de sécurité

Sécurisation de Saia PCD®

Les produits Saia PCD® fonctionnent en réseau, si bien que leurs paramètres de sécurité doivent être configurés correctement afin de réduire les risques liés à un accès non autorisé. Pour obtenir des informations d'ordre général sur la sécurisation des produits SBC, reportez-vous à la fiche d'information « Bonnes pratiques de sécurité générales pour les produits IP de SBC ». En plus des mesures indiquées dans la fiche d'information « Bonnes pratiques de sécurité générales pour les produits IP de SBC », suivez aussi les conseils donnés dans les sections suivantes. Adopter les règles de bonne pratique habituelles en matière d'installation et de sécurité permet de réduire le risque d'attaque informatique malveillante par un informaticien doué et équipé.

Liste de contrôle de sécurité

- ☐ Tous les projets Saia PG5® liés, y compris toutes les librairies qui en dépendent, sont inclus dans le plan de restauration après sinistre.
- ☐ L'accès physique à Saia PCD® est restreint.
- ☐ L'accès physique aux réseaux connectés à Saia PCD® est restreint.
- ☐ Tous les automates PCD de SBC sont exploités avec la dernière version disponible du firmware.
- ☐ Le réseau Ethernet est sécurisé, voir « Planification et sécurité du réseau ».
- ☐ Tous les services, ports et canaux de communication non utilisés sont désactivés.
- ☐ Les noms d'utilisateur ne peuvent pas être déduits et les mots de passe employés sont complexes.
- ☐ Les utilisateurs de Saia PCD® disposent uniquement des privilèges minimum requis.

Développement d'un programme de sécurité

Reportez-vous à la fiche d'information « Bonnes pratiques de sécurité générales pour les produits IP de SBC ».

Planification d'une restauration après sinistre

Au cours du développement du plan de restauration après sinistre, veillez à inclure tous les fichiers et toutes les librairies du projet Saia PG5® concerné nécessaires à la restauration du projet.

Considérations physiques et environnementales

Saia PCD® doit être installé dans un environnement fermé à clé, comme un local technique sécurisé ou une armoire verrouillée. Remarque : Veillez à ce que l'emplacement soit ventilé correctement.

Mises à jour de sécurité et packs de maintenance

Assurez-vous que la dernière version du firmware est installée sur tous les appareils Saia PCD®, notamment dans les systèmes avec accès à Internet.

Antivirus

Ne s'applique pas à Saia PCD®.

Planification et sécurité des réseaux

Réseau Ethernet

Il est recommandé de séparer le réseau Ethernet utilisé par Saia PCD® du réseau utilisé normalement dans les bureaux à l'aide d'un entrefer ou d'un réseau privé virtuel (VPN).
L'accès physique à l'infrastructure du réseau Ethernet doit être restreint. Vous devez aussi vous assurer que l'installation est conforme à la politique informatique de votre entreprise.
Les appareils Saia PCD® ne doivent pas être connectés directement à Internet. Ils doivent être déployés en toute sécurité derrière un pare-feu ou sur un réseau privé virtuel protégé par des mots de passe complexes ainsi que par des protocoles de sécurité Internet afin de minimiser le risque d'accès non autorisé.

Réseau MS/TP

L'accès physique à l'infrastructure du réseau MS/TP doit être restreint.

Réseau RS-485

L'accès physique à l'infrastructure du réseau RS-485 doit être restreint.

Réseau Profi-S-Bus

L'accès physique à l'infrastructure du réseau Profi-S-Bus doit être restreint.

Réseau CAN

L'accès physique à l'infrastructure du réseau CAN doit être restreint.

USB

L'accès physique au port USB des appareils Saia PCD® doit être restreint.

RS-232 (PGU)

L'accès physique au port RS-232 (PGU) des appareils Saia PCD® doit être restreint.

Bus E/S

L'accès physique au bus E/S des appareils Saia PCD® doit être restreint.

Port d'extension E/S

L'accès physique au port d'extension E/S des appareils Saia PCD® doit être restreint.

Services

Désactivez tous les services que vous n'utilisez pas. Cela permet de réduire la surface d'attaque et peut augmenter la performance du système Saia PCD®.

Serveur Web
Certains systèmes Saia PCD® fournissent un serveur Web HTTP susceptible d'écouter sur deux ports TCP. Il est recommandé de désactiver les deux ports d'écoute. Si un serveur Web est indispensable, assurez-vous dans ce cas que ce dernier est protégé par un mot de passe complexe et que des règles de pare-feu sont mises en place pour interdire tout accès indésirable. Notez qu'il est possible d'accéder au système de fichiers de Saia PCD® en utilisant le protocole HTTP et des données d'accès FTP. Si le serveur HTTP est activé, assurez-vous que les noms d'utilisateurs FTP ne peuvent pas être déduits et que les mots de passe correspondants sont complexes.

Serveur FTP
Certains systèmes Saia PCD® disposent d'un serveur de fichiers FTP. Il est recommandé de le désactiver. Si un serveur FTP est indispensable, assurez-vous alors qu'il est protégé à l'aide de noms d'utilisateurs impossibles à déduire et de mots de passe complexes.

BACnet IP
En raison de la nature non sécurisée du protocole BACnet, les systèmes Saia PCD® qui prennent en charge une fonctionnalité BACnet IP NE DOIVENT JAMAIS être connectés à Internet. Le système de sécurité des produits Saia PCD® ne les protège pas en écriture via BACnet. L'accès physique à l'infrastructure du réseau BACnet IP doit être restreint. Si les communications BACnet IP ne sont pas utilisées, désactivez la configuration du réseau BACnet IP dans le Configurateur d'appareils Saia PG5.

Serveur SNMP
Certains systèmes Saia PCD® disposent d'un serveur SNMP. L'accès au serveur SNMP ne requiert aucune authentification. Il est recommandé de désactiver le serveur SNMP. Si vous devez utiliser un serveur SNMP, alors le système Saia PCD® NE DOIT JAMAIS être connecté à Internet. De plus, la configuration SNMP dans le Configurateur d'appareils Saia PG5 doit être réalisée de sorte à n'autoriser qu'un accès limité.

Filtrage IP
Saia PCD® vous permet d'établir une liste blanche et une liste noire d'adresses IP visant à autoriser ou interdire l'accès au système. Il est recommandé d'activer ce service afin de fournir une couche de sécurité supplémentaire.

Environnements virtuels
Ne s'applique pas à Saia PCD®.

Sécurisation des appareils sans fil
Si vous utilisez un réseau sans fil, vous devez le sécuriser conformément à la politique informatique de votre entreprise.

Surveillance du système
Ne s'applique pas à Saia PCD®.

Domaines Windows
Ne s'applique pas à Saia PCD®.

Bonnes pratiques de sécurité générales pour les produits IP de SBC

Les directives suivantes vous sont données afin de réduire les risques existants. Les besoins exacts de chaque site doivent être évalués au cas par cas. Pour la grande majorité des installations, la mise en œuvre de tous les niveaux de sécurité décrits ci-dessous permet de sécuriser le système de manière plus que satisfaisante. En général, il suffit d'intégrer les quatre premiers éléments faisant référence aux réseaux locaux pour répondre aux besoins de la plupart des installations d'un réseau de contrôleur domotique.

Réseaux locaux (LAN) intégrant des composants de la société Saia-Burgess Controls AG
Assurez-vous que la politique des mots de passe permettant aux utilisateurs d'accéder à tous les services est appropriée aux systèmes en suivant ces directives non exhaustives :
- Utilisation de mots de passe complexes
- Changement de mot de passe cyclique recommandé
- Identifiants et mots de passe uniques pour chaque utilisateur du système
- Règles de divulgation des mots de passe

Évitez tout accès non autorisé aux équipements du réseau utilisés en lien avec des systèmes fournis par Saia-Burgess Controls AG. Quel que soit le système, évitez tout accès physique au réseau et aux équipement afin de réduire le risque d'interférences non autorisées. Les bonnes pratiques de sécurité concernant les installations informatiques demandent que les salles de serveurs, panneaux de brassage et équipements informatiques soient installés dans des locaux fermés à clé. Les équipements Saia PCD® doivent être installés dans des armoires de contrôle verrouillées, elles-mêmes situées dans des locaux techniques sécurisés.

Quelques mesures à prendre lors de la mise en service de certains éléments :
- Saia PCD® : assurez-vous que l'appareil est protégé par un mot de passe. Veillez à ce que les niveaux utilisateurs appropriés soient affectés aux utilisateurs du site.
- Visi.Plus : assurez-vous que le système est protégé par un mot de passe. Veillez à ce que les niveaux utilisateurs appropriés soient affectés aux utilisateurs du site, de l'administrateur à l'utilisateur standard. Les bonnes pratiques demandent généralement de n'attribuer aucun droit d'accès au compte utilisateur invité.

Adoptez une politique de mise à jour adaptée à l'infrastructure installée sur le site comme élément d'un contrat de niveau de service. Cette politique doit notamment comprendre la mise à jour de la dernière version des composants suivants du système :
- le firmware des régulateurs, RIO, HMI, etc.
- les logiciels superviseurs tels que le logiciel Visi.Plus
- les systèmes d'exploitation des ordinateurs et serveurs
- l'infrastructure du réseau et tous les systèmes d'accès à distance

Configurez séparément les réseaux informatiques destinés aux systèmes de contrôleurs domotiques et le réseau informatique de l'entreprise du client. Pour cela, configurez des réseaux locaux virtuels (VLAN) au sein de l'infrastructure informatique du client ou installez une infrastructure réseau séparée par un entrefer dédiée aux systèmes de contrôleur domotique.
Après la mise en service du système, limitez le trafic IP sur le réseau du contrôleur domotique (à l'aide de listes d'accès par exemple) aux types de protocoles requis pour une exploitation normale (S-Bus, BACnet...).
Vous trouverez de plus amples informations sur le trafic des communications en fonctionnement normal dans la documentation du produit.
Quand un superviseur de système centralisé sert d'interface à Saia PCD® (ex. Visi.Plus) et si le système ne demande pas d'accès direct à chaque serveur Web, alors l'infrastructure réseau doit être configurée de sorte à limiter l'accès au serveur Web.

Des réseaux locaux virtuels dynamiques avec attribution d'adresses MAC peuvent fournir une protection contre des connexions non autorisées d'un appareil au système et réduire ainsi le risque associé aux informations de surveillance individuelle sur le réseau.

Accès à distance aux systèmes IP de contrôle des bâtiments
- Si vous voulez accéder à des systèmes Saia PCD® à distance, utilisez la technologie VPN (réseau privé virtuel) pour réduire le risque d'interception des données et protéger les appareils de contrôle contre une exposition directe à Internet.
- Le produit SBC.Connectivity est une solution de connectivité gérée qui facilite les communications mobiles telles que le GPRS, la 3G, etc., ainsi que les communications filaires pour ce connecter à distance à Saia PCD®. Ce service offre un réseau sécurisé qui fournit un accès VPN simple aux appareils.

Les clients qui adoptent les règles de bonne pratique habituelles en matière d'installation et de sécurité réduisent le risque d'attaque informatique malveillante par un informaticien doué et équipé. Vous trouverez de plus amples informations dans la documentation spécifique au produit.

Saia-Burgess Controls AG
Bahnhofstrasse 18 | 3280 Morat | Suisse | www.saia-pcd.com
T +41 26 580 30 00 | F +41 26 580 34 99
support@saia-pcd.com | www.sbc-support.com

Représentants internationaux & distributeurs SBC :
www.saia-pcd.com/contact
PP26-620 11/2015 FRA01