La connectivité Internet augmente le risque de violation de la sécurité, mais cette connectivité est une exigence obligatoire pour de nombreux projets d'automatisation, ce qui rend les procédures de cyberprotection absolument cruciales.

Connexion Cloud, accès à distance, mise à jour de logiciels, sauvegarde des données et contrôle à distance pour la maintenance : le besoin de connectivité externe crée de nouveaux défis dans le domaine de la sécurité de l'information, car il augmente l'exposition potentielle aux risques. La responsabilité de prévenir les atteintes à la sécurité incombe au personnel des opérations et du contrôle, qui programme et connecte les automates à un réseau externe.

Unitronics offre une variété de solutions et d'outils qui peuvent être utilisés pour atténuer les risques et prévenir les atteintes à la sécurité.

Ce document détaille les principaux outils et recommandations destinés renforcer le niveau de cyberprotection des projets d'automatisation et des machines équipés des automates de la série UniStream® d'Unitronics.

1. Fondamentaux au niveau de l'équipement

a. **Restez informé** via pl-systems.fr. Unitronics développe et améliore ses produits tout au long de leur cycle de vie. Notre site Web contient les versions les plus récentes des logiciels et des systèmes d'exploitation, qui peuvent inclure des évolutions en matière de cyberprotection.

b. Rapport de mise à jour : ces documents peuvent contenir des informations de sécurité relatives à une version spécifique. **Unitronics recommande de mettre à jour les automates vers la version 1.32 et ultérieure.**

c. **Autorisations d'accès et mots de passe**

- Contrôlez rigoureusement les autorisations d'accès aux automates et aux équipements associés.
- Modifiez les mots de passe par défaut de l'API et stockez-les conformément aux meilleures pratiques. Changer le mot de passe par défaut et en définir un nouveau empêchera tout accès non autorisé à l'automate via UniLogic.

d. Les produits UniStream prennent en charge plusieurs niveaux de sécurité et de protection. Le développeur et l'utilisateur doivent mettre en œuvre les fonctionnalités suivantes conformément aux exigences du système :

- Définissez les mots de passe pour VNC via la gestion du serveur VNC.
- Définissez les autorisations pour UniApps via la gestion des mots de passe.
- Définissez les utilisateurs et les autorisations pour les écrans utilisateur via le contrôle d'accès utilisateur.
- Définissez les utilisateurs et les autorisations pour les écrans du serveur Web.
  Pour les systèmes où le téléchargement de l'application utilisateur s'effectue à l'aide d'une clé USB ou d'une carte SD, veillez à définir les différents mots de passe à l'emplacement prévu.

2. Niveau réseau

Communication sécurisée

a. Contrôleur en tant que client Internet : Si l'automate doit communiquer avec des composants ou des serveurs sur Internet, assurez-vous qu'il agit en tant que client, initiant ainsi la communication.

b. Connexion des équipements d'automatisation à Internet :

- Assurez-vous que tous les équipements sont positionnés derrière un pare-feu, sans aucune règle permettant l'exposition du réseau local (LAN) à des connexions depuis le réseau étendu (WAN), que ce soit via un routeur cellulaire ou un réseau câblé.
- Vérifiez l'absence de paramètres de transfert de port exposant directement l'équipement au réseau public.
  Pour une mise en œuvre rapide et efficace de la protection réseau, l'utilisation des produits UCR est recommandée. La série de routeurs industriels d'Unitronics intègre un pare-feu ainsi qu'une fonctionnalité VPN.

3. Solution complète

Connexion sécurisée - UniCloud

La plateforme UniCloud IIoT d'Unitronics permet une connexion sécurisée sans nécessiter d'adresses IP Internet fixes ou publiques. Aucune expertise préalable en cybersécurité ou en informatique n'est requise pour la mise en œuvre. La plateforme intègre plusieurs couches de chiffrement avancé et de protection, constituant ainsi une solution complète et sécurisée. Elle permet de restreindre l'accès en fonction du niveau d'autorisation et de suivre les connexions réelles de manière efficace.