AYI NEDJIMI Consultants

Sécuriser automates PLC et RTU en production industrielle

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide de sécurisation des automates PLC et RTU en production : durcissement firmware, contrôle d'accès, détection de modification et bonnes pratiques.

Résumé exécutif

Les automates programmables (PLC) et les unités terminales distantes (RTU) constituent les composants les plus critiques et simultanément les plus vulnérables des systèmes de contrôle industriels car ils assurent le lien direct entre le monde numérique et les processus physiques. Ce guide détaille les stratégies de sécurisation applicables en environnement de production active : durcissement des configurations par défaut et élimination des mots de passe constructeur, gestion granulaire des accès physiques et logiques aux automates, surveillance continue de l'intégrité des programmes chargés dans les PLC, gestion rigoureuse des firmwares avec qualification préalable des correctifs, et mesures compensatoires structurées pour les automates legacy ne supportant aucune fonction de sécurité native mais toujours en service opérationnel actif dans les installations industrielles les plus critiques du patrimoine industriel national.

Les automates programmables industriels transforment les instructions logiques en actions physiques : ouverture de vannes, régulation de température, contrôle de vitesse de moteurs, séquencement de processus chimiques. Leur compromission donne à l'attaquant un contrôle direct sur le monde physique, avec des conséquences potentiellement catastrophiques allant de la destruction d'équipements à la mise en danger de vies humaines. Pourtant, ces dispositifs critiques fonctionnent souvent avec des firmwares obsolètes, des mots de passe constructeur par défaut jamais modifiés, des services réseau superflus activés et une absence totale de mécanismes de détection de modification. La sécurisation des PLC et RTU en environnement de production représente un défi technique majeur, car toute intervention doit préserver la disponibilité du processus industriel et la sûreté de fonctionnement. Les attaques documentées contre ces dispositifs, de Stuxnet ciblant les S7-300 de Siemens au malware Triton visant les contrôleurs de sécurité Triconex de Schneider Electric, démontrent que les groupes de menaces avancés maîtrisent parfaitement les techniques d'exploitation des automates industriels et exploitent systématiquement les faiblesses de sécurité au niveau le plus bas de l'architecture de contrôle.

Durcissement des configurations automates

Le **durcissement des PLC** commence par l'élimination des configurations par défaut. Chaque automate livré en usine dispose de mots de passe par défaut documentés publiquement : « password » pour Allen-Bradley, des mots de passe vides pour certains Siemens, des PIN

numériques triviaux pour Schneider Electric. La première action consiste à modifier ces identifiants avec des mots de passe robustes et à activer les mécanismes de protection d'accès lorsqu'ils existent.

Les *modes de protection* des automates modernes offrent plusieurs niveaux de restriction. Siemens S7-1500 propose quatre niveaux de protection (aucun, lecture seule, lecture/écriture avec HMI, protection complète). Allen-Bradley ControlLogix/CompactLogix supporte le verrouillage de programme avec mot de passe. Ces modes doivent être activés au niveau le plus restrictif compatible avec les besoins opérationnels. En production, le mode « run » protégé, interdisant les modifications de programme sans authentification et arrêt manuel, constitue la configuration minimale recommandée par les guides de sécurisation de l'ANSSI pour les systèmes industriels.

La désactivation des **services réseau non nécessaires** réduit la surface d'attaque. Les serveurs web intégrés aux automates modernes, utiles pendant la mise en service, doivent être désactivés en production. Les services FTP, Telnet, SNMP et les ports de diagnostic distants constituent autant de vecteurs d'attaque exploitables. Un inventaire exhaustif des services activés sur chaque automate, suivi de la désactivation systématique des services non requis, forme la base du durcissement. Cette démarche s'inscrit dans la stratégie globale de segmentation réseau et Zero Trust appliquée aux environnements industriels.

L'attaque Stuxnet a démontré que la modification du programme d'un automate Siemens S7-300 pouvait être réalisée de manière invisible pour les opérateurs. Le malware remplaçait les blocs de code OB1 et OB35 par des versions malveillantes modifiant la vitesse des variateurs de fréquence des centrifugeuses, tout en interceptant les requêtes de lecture pour renvoyer des valeurs normales aux systèmes de supervision. L'absence de mécanisme d'intégrité sur les anciens S7-300 rendait cette manipulation indétectable sans analyse forensique approfondie du contenu de la mémoire de l'automate.

Comment surveiller l'intégrité des programmes automates ?

La surveillance de l'intégrité des programmes constitue la défense la plus efficace contre les attaques type Stuxnet. La technique de base consiste à extraire périodiquement le programme de l'automate et à comparer son empreinte cryptographique (hash SHA-256) avec une référence validée. Toute modification non autorisée déclenche une alerte immédiate. Les solutions commerciales comme **Claroty CTD** et Nozomi Networks Guardian automatisent cette surveillance en interrogeant régulièrement les automates via leurs protocoles natifs pour détecter les changements de programme, de configuration et de firmware.

Les automates de dernière génération intègrent des *fonctions d'intégrité natives*. Siemens S7-1500 supporte la vérification d'intégrité du firmware par signature numérique et la détection de modification du programme chargé. Rockwell Automation ControlLogix 5580 propose le Change Detection pour alerter sur les modifications de programme non planifiées. Schneider Electric Modicon M580 intègre des mécanismes de Secure Boot vérifiant l'intégrité du firmware au démarrage. Pour les automates legacy ne disposant d'aucune de ces fonctions, la

surveillance réseau passive détectant les commandes de programmation (Modbus fonction 8, S7comm Write Var) en dehors des fenêtres de maintenance planifiées constitue la mesure compensatoire principale.

Pourquoi la gestion des firmwares PLC est critique ?

Les **firmwares des automates** contiennent des vulnérabilités régulièrement publiées par les constructeurs et les organismes comme ICS-CERT. L'exploitation de ces vulnérabilités peut permettre l'exécution de code arbitraire, le contournement de l'authentification ou le déni de service de l'automate. Pourtant, la mise à jour des firmwares en environnement OT reste l'un des processus les plus complexes et les plus redoutés par les équipes d'exploitation.

La mise à jour d'un firmware PLC nécessite généralement un arrêt de l'automate, donc du processus industriel qu'il pilote. Les fenêtres de maintenance, parfois espacées de plusieurs mois voire d'années dans l'industrie continue, sont les seules opportunités pour appliquer ces mises à jour. Le processus doit inclure un test préalable sur un automate de spare ou un simulateur, une sauvegarde complète du programme et de la configuration, une procédure de rollback documentée et un plan de continuité en cas d'échec de la mise à jour. La mise en place d'une stratégie de gestion des logs et rétention permet de tracer chaque intervention sur les automates.

Constructeur	Gamme	Protection programme	Secure Boot	Détection changement
Siemens	S7-1500	4 niveaux + chiffrement	Oui	Oui (natif)
Siemens	S7-300/400	Mot de passe basique	Non	Non
Rockwell	ControlLogix 5580	Mot de passe + CIP Security	Oui	Change Detection
Schneider	Modicon M580	Application Protection	Oui	Oui
Schneider	Modicon M340	Mot de passe basique	Non	Non

Mon avis : La gestion des firmwares PLC devrait suivre le même niveau de rigueur que le patch management IT, mais avec des cycles adaptés aux contraintes de production. L'excuse du « on ne peut pas arrêter la production » ne tient plus face aux risques démontrés par Triton et Stuxnet. Les organisations doivent négocier des fenêtres de maintenance dédiées à la cybersécurité dans leur planning de production, au même titre que la maintenance préventive des équipements mécaniques.

Quelles mesures pour les automates legacy sans sécurité native ?

Les automates anciens (Siemens S7-300, Allen-Bradley SLC 500, Schneider Premium/Quantum) ne supportent aucune fonction de sécurité native : pas d'authentification robuste, pas de chiffrement, pas de détection de modification. Ces dispositifs, encore massivement déployés dans l'industrie avec des durées de vie dépassant 20 ans, nécessitent des **mesures compensatoires** rigoureuses pour atteindre un niveau de sécurité acceptable.

La première mesure est l'*isolation réseau maximale* : chaque automate legacy doit être placé dans un micro-segment réseau avec un contrôle d'accès strict au niveau du commutateur industriel. Seuls les dispositifs explicitement autorisés (serveur SCADA principal, poste d'ingénierie dédié) peuvent communiquer avec l'automate. La deuxième mesure est la surveillance continue du trafic réseau à destination de l'automate : toute commande de programmation, tout accès depuis une source non autorisée, toute communication sur un port inhabituel doit déclencher une alerte. L'approche de détection engineering fournit les méthodologies pour créer ces règles de surveillance spécifiques.

La troisième mesure est le contrôle d'accès physique renforcé : les armoires contenant les automates legacy doivent être verrouillées avec un contrôle d'accès traçable (badge, clé unique, journal des accès). Un accès physique à un automate sans protection logicielle signifie un contrôle total et immédiat. La quatrième mesure consiste à maintenir des sauvegardes régulières et vérifiées des programmes automates, permettant une restauration rapide en cas de compromission détectée.

Disposez-vous d'un inventaire à jour de tous vos automates avec leur version de firmware et la date de dernière mise à jour de sécurité ?

Faut-il migrer vers des automates certifiés IEC 62443 ?

La migration vers des automates certifiés **IEC 62443-4-2** offre des garanties de sécurité natives impossibles à reproduire par des mesures compensatoires sur des dispositifs legacy. Les automates certifiés intègrent le Secure Boot, le chiffrement des communications, l'authentification forte des accès de programmation, la détection d'intégrité du programme et la journalisation des événements de sécurité. Le surcoût à l'achat, typiquement 15 à 30% par rapport à un modèle non certifié, est largement compensé par la réduction des mesures compensatoires nécessaires et la simplicité d'atteinte du Security Level cible défini par la norme NIS 2.

La migration doit s'inscrire dans une stratégie pluriannuelle alignée sur les cycles de renouvellement naturels des automates. Remplacer un automate fonctionnel uniquement pour des raisons de cybersécurité est rarement justifiable économiquement, sauf pour les systèmes les plus critiques. L'approche recommandée consiste à spécifier systématiquement des automates certifiés IEC 62443 pour tout nouveau projet et tout remplacement, tout en renforçant les mesures compensatoires sur le parc legacy existant selon une priorisation basée sur la criticité du processus piloté et l'exposition réseau de chaque automate.

Comment sécuriser les accès de maintenance distante aux automates ?

La maintenance distante des automates constitue un vecteur d'attaque majeur qui nécessite des contrôles stricts. Les accès VPN directs vers les automates, encore pratiqués par de nombreux intégrateurs et constructeurs pour le support technique, exposent les dispositifs les plus critiques à des compromissions via les postes de travail des intervenants externes. L'architecture de maintenance distante sécurisée repose sur des **jump hosts durcis** positionnés dans la DMZ industrielle, avec authentification multifacteur, enregistrement vidéo des sessions et limitation temporelle des accès.

Les solutions de type *Privileged Access Management* (PAM) adaptées aux environnements OT, comme celles proposées par Wallix ou CyberArk, gèrent le cycle de vie complet des accès de maintenance : demande justifiée, approbation par le responsable OT, ouverture d'un créneau limité, supervision en temps réel de la session et clôture automatique. Chaque commande envoyée à l'automate pendant la session de maintenance est journalisée et peut être rejouée en cas d'investigation forensique. Les équipes de SOC reçoivent des alertes sur les sessions de maintenance active pour garantir une surveillance renforcée pendant ces périodes d'exposition accrue.

Sources et références : CISA ICS · ANSSI

Quelles bonnes pratiques pour la sauvegarde des programmes automates ?

La **sauvegarde régulière des programmes automates** constitue la dernière ligne de défense contre une compromission ou une corruption du code. Chaque version de programme validée en production doit être archivée avec son contexte : date de mise en service, modifications apportées, responsable de la validation et empreinte cryptographique SHA-256. Les outils de gestion de version comme PLC Version Control ou CODESYS Automation Server automatisent la capture périodique et la comparaison des programmes, alertant sur toute modification détectée entre deux captures.

Les sauvegardes doivent être stockées en dehors du réseau OT, idéalement sur un support déconnecté et dans un coffre physique sécurisé. La capacité de restauration doit être testée régulièrement lors des fenêtres de maintenance : télécharger une sauvegarde sur un automate de spare et vérifier le fonctionnement correct du programme constitue le test de restauration minimal. Les organisations les plus matures maintiennent un automate de spare pré-configuré pour chaque modèle critique, permettant un remplacement rapide en cas de compromission avérée d'un automate en production, en cohérence avec les pratiques de réponse aux incidents industriels.

À retenir : La sécurisation des PLC et RTU repose sur quatre piliers : le durcissement des configurations (mots de passe, services, modes de protection), la surveillance de l'intégrité des programmes, la gestion rigoureuse des firmwares avec des fenêtres de maintenance planifiées,

et des mesures compensatoires robustes pour le parc legacy. La migration progressive vers des automates certifiés IEC 62443-4-2 constitue l'investissement le plus structurant pour la sécurité OT à long terme.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr