Industrie 4.0 – comment assurer la cyber sécurité d'une nouvelle machine dès la conception ?

02 juin 2017, 02:00

Véronique Dossogne

Pour que l'Internet Industriel des Objets (IIoT)/Industrie 4.0 soit réalisé avec succès, il convient de prendre en compte les aspects de fiabilité et de cyber sécurité des opérations dès la conception de machines et systèmes connectés. Dans ce but, VDMA (Verband Deutscher Maschinen- und Anlagenbau) a développé un ensemble d'exigences de sécurité minimales pour les futures machines et usines.

La cyber sécurité est une question importante pour les usines intelligentes à partir du moment où le réseau inclut des systèmes IT connectés par Internet. En outre, une des idées fondatrices d'Industrie 4.0 est d'intégrer les chaînes d'approvisionnement dans la totalité des implantations et entreprises. Néanmoins, mettre sa production sur réseau crée des cibles potentielles pour l'espionnage. Le problème, c'est qu'il existe des recommandations et normes pour la sécurité IT classique, mais pas pour la protection des données des machines. VDMA a publié des directives, « Industrie 4.0 Security Guidelines : recommendations for actions », qui inclut des astuces fondamentales pour les fabricants et intégrateurs de machines.

La cyber sécurité dès la conception

La cyber sécurité, c'est la protection des systèmes IT. Si ces systèmes sont connectés via une intégration d'Industrie 4.0, les fabricants tout comme les opérateurs doivent réfléchir à la sécurisation à tout moment de cette connectivité entre entreprises. L'objectif de la sécurité Industrie 4.0 est de s'assurer la cyber sécurité des futures machines et usines tout au long de leur cycle de vie, plutôt que devoir comme aujoud'hui rajouter les fonctions sécuritaires par la suite.

L'intégration de la « sécurité dès la conception » signifie que cette fonction doit devenir une composante des futurs systèmes et usines, établissant ainsi la « sécurité en tant que fonction ». Ces directives fournissent l'opportunité de cibler des aspects spécifiques et de les examiner en autonomie. L'accent est mis sur la perspective des fabricants et des intégrateurs.

Recommandations

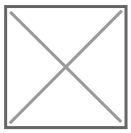
Vous trouverez dans ce document les recommandations fondamentales d'actions et les exigences minimales de mesures protectives permettant un niveau de protection de base des machines. Chaque recommandation est assignée à une fonction produit correspondante ; ainsi il suffit d'identifier les mesures de protection pertinentes pour la machine et ses fonctions respectives. Ce compromis représente une amélioration importante de la sécurité pour les entreprises qui

s’orientent vers Industrie 4.0.

Les fonctions produits sont également accompagnées de recommandations d’actions (voir la figure 2) afin d’indiquer le moment où une recommandation d’action devient une exigence minimale sur l’échelle de un à cinq d’Industrie 4.0, en d’autres mots, le moment où il convient de mettre en place une mesure protective fonctionnelle. « La boîte à outils VDMA Industrie 4.0 – Produits » (voir figure 1 ci-dessous) est alors utilisée comme échelle.



(Source : Industrie 4.0 Security Guidelines : recommendations for actions
Figure 1 : VDMA Industrie 4.0 – Toolbox-Products. Classes fonctionnelles d’une machine. Une échelle de fonctionnalité Industrie 4.0 de 1 à 5 est utilisée pour les classes A to F. Les entrées dans la colonne de gauche se réfèrent à une machine de production classique, la colonne de droite correspond à la vision intégrale d’Industrie 4.0



(Source : Industrie 4.0 Security Guidelines : recommendations for actions
Figure 2 : Exemple de recommandation d’action. Ce graphique montre que la recommandation devient une exigence minimale dès que le produit a, au minimum, une interface fieldbus ou un système de stockage de données pour l’échange d’informations.

Ces directives proposent 85 recommandations classées en 17 principes.

Les principes généraux à appliquer à tout dispositif IoT (perspective des fabricants) sont les suivants :

- Mise en place de mécanismes de mise à jour (si nécessaire)
- Documentation des interfaces et transmissions de données
- Utilisation de protocoles sécurisés
- Sécurisation de la maintenance à distance
- Consolidation des composants et logiciels
- Mise en place de fonctions d’authentification
- Utilisation de cryptographie
- Formation des développeurs de produits sur la cyber sécurité dès la conception
- Tests de cyber sécurité sur les produits et les implémentations

Les recommandations listées présentent un niveau de protection basique pour une petite ou moyenne entreprise qui s’oriente vers Industrie 4.0. Si les premières étapes ont déjà été mises en place et que la machine doit être conçue à l’avenir avec une fonctionnalité Industrie 4.0 complète, il est utile de consulter la documentation complémentaire.

Ci-dessous, quelques sources d’information importantes pouvant aider à établir une protection sécurisée.

En anglais

- VdS Quick Check Security

- Platform Industrie 4.0 Guidelines IT security in Industrie 4.0 : first steps towards secure production
- Platform Industrie 4.0 Guidelines IT security in Industrie 4.0 : action fields for operator
- BSI ICS Security Compendium
- ICS-CERT newsletter, reports and recommendations for action
- ISO/IEC 27000 series on information security
- IEC 62443 Industrial communication networks - Network and system security
- ISO/IEC 15408-1 Evaluation criteria for IT security
- NAMUR worksheet NE 153
- NAMUR worksheet NE 115

En allemand

- Light and Right Security ICS (LARS ICS)

Avec le soutien du Service Public Fédéral Économie, Sirris a mis en place l'Antenne-Normes Industrie 4.0, un service créé pour informer les entreprises belges - essentiellement les PME - des différentes normes existantes et en préparation. Faites-nous connaitre vos centres d'intérêts ou vos préoccupations sur ce vaste sujet qu'est le paysage des normes pour l'Industrie 4.0

Auteurs



Véronique Dossogne