Détecter les cyber-intrusions dans les réseaux de communication de poste

Comment améliorer la sécurité des sous-stations CEI 61850

Introduction

Plusieurs couches sont nécessaires pour garantir la cybersécurité des postes. La cryptographie permet d'authentifier les appareils mais ne permet pas pour autant de prévenir toute attaque. Les pare-feu et « air gaps » peuvent être contournés via les tunnels d'accès à distance existants, ou via les ordinateurs de maintenance directement reliés aux IED ou au réseau de communication (station bus) du poste. C'est pourquoi des mesures sont nécessaires pour détecter les menaces dans le poste afin de permettre une réponse rapide et de minimiser les conséquences.

Ce livre blanc décrit les exigences en matière de sécurité des postes CEI 61850 ainsi que les différentes approches permettant de détecter les menaces dans ces réseaux. Une approche spécialement développée pour les réseaux „station bus" et „process bus" CEI 61850 y est également décrite.

Les vecteurs d'attaque d'un poste

Nous allons définir une cyber-attaque sur un poste comme un événement lors duquel un ennemi modifie, dégrade ou désactive un service sur au moins un appareil de protection, d'automatisme ou de contrôle-commande au sein du poste. En regardant la figure 1, une sous-station typique peut être attaquée par tous les chemins marqués en rouge. Le vecteur d'attaque le plus fréquemment utilisé est la connexion de l'informatique d'entreprise (1), qui a été exploitée en Ukraine 2016 : attaque d'une sous-station. Cette connexion peut être permanente, pour la connexion aux serveurs de l'informatique d'entreprise, ou temporaire pour la maintenance à distance. Un attaquant pourrait également entrer par la connexion du centre de contrôle (2) - quel que soit le protocole SCADA utilisé.

Un autre point d'entrée concerne les PC d'ingénierie (3) branchés à l'équipement du poste. Lorsqu'un technicien de protection connecte son PC à un relais afin de modifier les paramètres (de protection), un logiciel malveillant sur le PC peut à son tour installer un logiciel malveillant sur le relais, comme avec les PLC dans la cyber-attaque de Stuxnet. Les ordinateurs portables utilisés pour tester le système CEI 61850 sont souvent directement connectés au réseau de communication (station bus) du poste, ce qui représente également une autre façon d'infecter les IED (4).

C'est pourquoi de nouveaux outils de test CEI 61850 sont disponibles, offrant une séparation cybersécurisée entre le PC de test et le réseau du poste. Il reste enfin l'appareil de test lui-même (5) comme point d'entrée potentiel. Pour cette raison, il est important que les fournisseurs d'équipements de test investissent dans le renforcement de leurs appareils afin de s'assurer que ce point d'entrée ne puisse pas être exploitable.

Le stockage des paramètres (3a) et des documents de test (4a) sont également une source potentielle d'attaque. Ce serveur de stockage fait donc également partie du périmètre critique. Par conséquent, il peut s'avérer judicieux d'introduire une solution de gestion des données séparée, isolée et protégée.

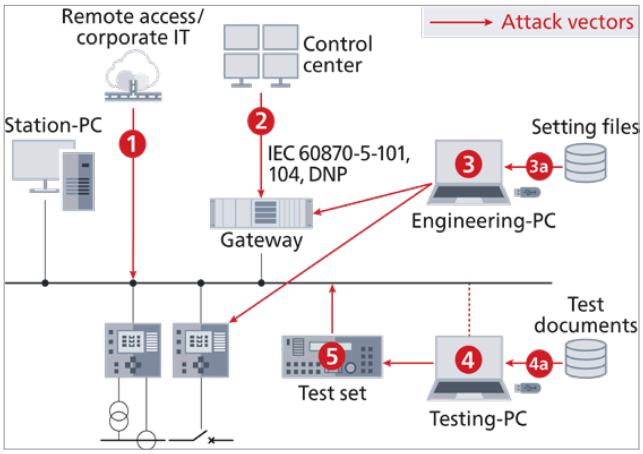

Figure 1 : Les vecteurs d'attaque d'un poste

Sécurité et CEI 61850

Une question fréquente relative à la cybersécurité dans les postes CEI 61850 est la suivante : « Que se passe-t-il si un agresseur injecte un GOOSE de déclenchement dans le réseau de communication du poste. Comment peut-on l'empêcher ? » Pour cela, nous ne devons pas nous concentrer sur l'agresseur disposant d'un accès physique au réseau du poste. Cette situation est également possible via d'autres mesures : un PC d'ingénierie ou de test infecté relié au réseau du poste, voire un IED infecté peuvent injecter des GOOSE. Dans ce contexte, les numéros d'état et de séquence („status number" et „sequence number") du message GOOSE sont assez souvent présentés comme des « mécanismes de sécurité ».

Néanmoins, de telles mesures devraient simplement s'appeler des « mécanismes de sécurité » car tout agresseur peut superviser le numéro d'état et de séquence actuel et injecter les valeurs adaptées. L'adresse MAC source du paquet GOOSE peut aussi être facilement imitée par l'agresseur. L'IED recevant le GOOSE n'a pas d'autre option

que de réagir au premier GOOSE reçu avec l'adresse MAC source et le numéro de séquence/état corrects. Il en va de même, bien entendu, avec le comptage d'échantillons dans les valeurs échantillonnées (Sampled Values). La seule vraie mesure permettant d'empêcher de telles attaques par injection consiste à s'assurer de l'authenticité et de l'intégrité du message à l'aide de codes d'authentification à la fin du message GOOSE, tel qu'indiqué par la norme CEI 62351-6. Avec cette mesure, l'IED émetteur est clairement identifié et il devient impossible de manipuler le contenu du message GOOSE. Vous noterez qu'il n'est pas nécessaire de crypter le message pour profiter de ces fonctions. Pour fournir et gérer ces clés d'authentification pour chaque IED, une infrastructure de gestion des clés est nécessaire à l'intérieur du poste. C'est la raison pour laquelle de tels mécanismes de sécurité GOOSE ne sont pas encore très utilisés pour le moment – mais cela va changer. Il en va de même avec les messages MMS et le contrôle d'accès basé sur le rôle.

Cryptage

Nous n'avons pas parlé du cryptage, bien qu'il soit souvent considéré comme la solution miracle en matière de sécurité. La norme CEI 62351 fournit également un cryptage pour GOOSE et MMS. Cependant, dans l'environnement du poste, seules quelques applications sont concernées par la confidentialité des messages. Si les messages ne peuvent pas être piratés (intégrité) et que l'émetteur peut être identifié (authentification) – ce qui est possible à l'aide de l'authentification dans GOOSE et MMS, les messages n'ont pas besoin d'être cryptés. Un exemple de cryptage nécessaire est si des GOOSE routables (R-GOOSE) sont transmis via un circuit de communication non crypté. Le cryptage fournit uniquement une charge supplémentaire pour les processeurs des IED, augmente le temps de transmission GOOSE et entrave les scénarios de test, sans pour autant offrir, dans la plupart des cas, de sécurité supplémentaire par rapport aux codes d'authentification. Le cryptage complique également l'analyse ultérieure des enregistrements du trafic et empêche les approches de surveillance telles que celles décrites ci-après.

Une défense approfondie

La plupart des postes CEI 61850 construits jusqu'à présent n'ont pas implémenté la norme CEI 62351. Même dans les postes où des GOOSE et MMS avec codes d'authentification sont appliqués, les appareils infectés dans le réseau pourraient encore infecter d'autres appareils ou affecter la disponibilité en perturbant le système de communication. C'est pourquoi la plupart des cadres de sécurité recommandent d'utiliser des « systèmes de détection d'intrusion » (IDS), un terme bien connu issu des systèmes informatiques classiques, afin de détecter les menaces et activités malveillantes sur le réseau. De tels IDS, tels que le StationGuard d'OMICRON, sont à l'heure actuelle de plus en plus utilisés dans le domaine des systèmes électriques.

Exigences en matière de détection pour les IDS dans les postes

Dans un poste CEI 61850, un IDS serait connecté comme illustré à la Figure 2. Des ports miroirs sur tous les switches applicables transmettent une copie de l'ensemble du trafic du réseau à l'IDS. L'IDS inspecte tout le trafic réseau communiqué par ces switches. Pour pouvoir analyser le trafic le plus important entre la passerelle et les IED, l'IDS doit, au minimum, être connecté au switch situé à côté de la passerelle et à tous les autres points d'entrée critiques dans le réseau. Les switches des différentes travées n'ont généralement pas besoin d'être couverts car le plus souvent seul le trafic en multidiffusion (GOOSE, Sampled Values) en découle. Pour s'assurer que l'ensemble du trafic en monodiffusion dans toutes les branches du réseau est analysé, il est essentiel que tous les switches soient reflétés dans l'IDS, ce qui n'est pas toujours possible si des switch intégrés dans les IED sont utilisés.

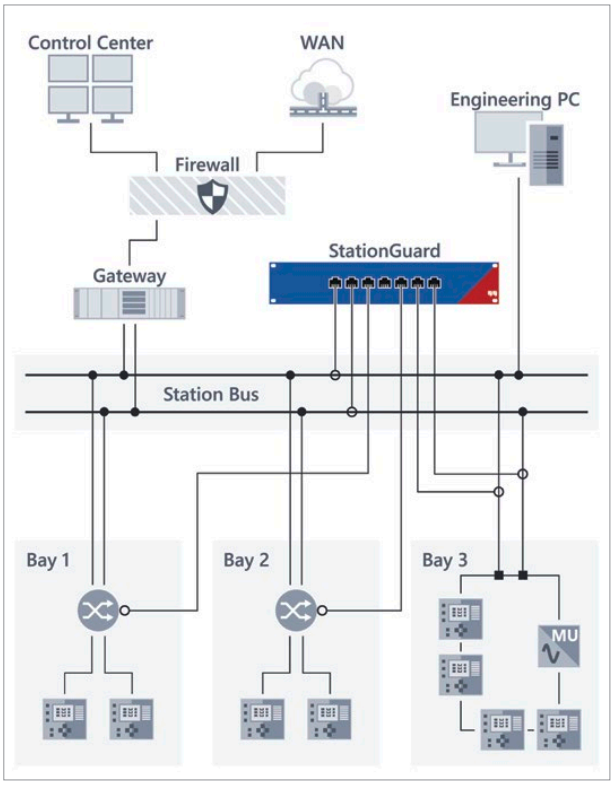

Figure 2 : Structure d'un poste avec IDS connecté

Cependant, les IDS des systèmes informatiques classiques ne sont pas adaptés à l'environnement du poste. Tandis que la sécurité informatique classique s'intéresse à des serveurs hautes performances avec des millions de connexions simultanément, la sécurité informatique des postes traite d'appareils aux ressources limitées, de systèmes d'exploitation personnalisés, de demandes en temps réel et de protocoles de redondance spécialisés. Par exemple, une attaque de type « refus de service » sur un service de communication d'IED ne nécessite souvent que 10 connexions, c'est-à-dire 10 paquets Ethernet, pour arriver à ses fins. Parce que les scénarios de « refus de service » n'étaient tout simplement pas pris en compte auparavant, lorsque ces appareils et protocoles ont été développés. En outre, on ne connaît qu'un petit nombre de cyber-attaques sur les postes, mais même la première occurrence d'une attaque peut avoir des conséquences dramatiques. Ainsi, un IDS de poste doit pouvoir détecter les attaques sans savoir au préalable à quoi elles ressemblent, et c'est exactement ce que le StationGuard d'OMICRON fait. C'est une approche très différente de celle d'un antivirus, qui recherche les virus dont il connaît la signature.

Des systèmes basés sur l'apprentissage

Pour pouvoir détecter des attaques inconnues, de nombreux fournisseurs utilisent une approche « basée sur l'apprentissage ». De tels systèmes étudient la fréquence et la datation de certains marqueurs de protocole pour tenter d'apprendre le comportement habituel du système. Une fois la phase d'apprentissage terminée, une alarme sera émise si l'un des marqueurs sort considérablement de la plage attendue. Cela a pour effet le déclenchement de fausses alarmes pour tout ce qui ne s'est pas produit pendant la phase d'apprentissage, tels que les événements de protection, les actions de manoeuvres ou d'automatismes peu courantes, ou les tests et la maintenance de routine. Comme ces systèmes ne comprennent pas la sémantique des protocoles, les messages d'alarme sont exprimés sous forme de jargon technique du protocole. Ainsi, les alarmes ne peuvent être examinées que par un technicien expérimenté en langage CEI 61850 et habitué à la sécurité des réseaux informatiques. Le technicien étudiant l'alarme doit également connaître la situation opérationnelle pour juger si certains événements de protocole CEI 61850 correspondent à un comportement valide. Par conséquent, de nombreuses fausses alarmes se produisent pour chaque poste, nécessitant toutes l'intervention de personnel hautement qualifié. Ainsi, des alarmes sont souvent ignorées ou écartées sans être étudiées, et l'IDS finit par être mis hors tension.

Figure 3 : StationGuard importe le fichier SCL (System Configuration Language) du poste afin de créer un modèle de système complet

L'approche

Pour les postes CEI 61850, l'ensemble du système d'automatisation, avec tous les appareils, modèles de données et schémas de communication, est décrit dans un format normalisé appelé SCL. Normalement, les fichiers de description de configuration du système (SCD) contiennent aussi des informations sur les appareillages primaires et pour un nombre croissant de postes, le schéma unifilaire est également présent. Ces informations permettent d'utiliser une approche différente pour détecter les intrusions. Le système de surveillance peut créer un modèle de système complet du réseau électrique et du système d'automatisation et comparer chaque paquet sur le réseau au modèle de système sous tension. Même les variables contenues dans les messages communiqués (GOOSE, MMS, SV) peuvent être comparés aux attentes dérivées du modèle de système. Ce processus est possible sans phase d'apprentissage, simplement avec une configuration à partir du SCL. Cette approche est mise en œuvre par le nouveau système de surveillance de la sécurité fonctionnelle StationGuard d'OMICRON.

La surveillance de la sécurité fonctionnelle

En substance, une surveillance fonctionnelle très détaillée est produite pour détecter les cyber-menaces dans le réseau. En raison du niveau détaillé de la vérification, non seulement les menaces de cybersécurité comme les paquets mal formés et actions de contrôle non autorisées sont détectées, mais également les pertes de communication, les problèmes de synchronisation horaire, et par conséquent aussi (certaines) défaillances de l'équipement. Si le schéma unifilaire est connu du système, et que des valeurs de mesures peuvent être observées dans la communication MMS (voire via des Sampled Values), les

possibilités de vérification sont infinies.

Par exemple, pour les GOOSE uniquement, il existe 35 codes d'alarmes d'évènements pouvant mal se passer. Cela va de simples écarts de numéros d'état/séquence (tel qu'expliqué ci-dessus) à des problèmes plus complexes, tels que des délais de transmission trop longs. Ces derniers sont détectés en mesurant précisément la différence entre l'horodatage de l'heure d'entrée dans le message et l'heure d'arrivée dans StationGuard. Si ce délai de transmission du réseau dépasse largement 3 ms pour un GOOSE de « protection » (selon la norme CEI 61850-5), cela indique un problème dans le réseau ou dans la synchronisation horaire.

Qu'en est-il pour la communication MMS ? À partir du modèle de système (extrait du SCL), on sait quels nœuds logiques contrôlent quels appareillages primaires. On peut ainsi distinguer les actions correctes/incorrectes et critiques/non critiques. La manoeuvre d'un disjoncteur et la commutation du mode de test CEI 61850 utilisent la même séquence dans le protocole MMS (Select-Before-Operate), mais l'effet dans le poste est assez différent. Ainsi, si le PC de test de la Figure 1 active le mode de test sur un relais, il peut s'agir d'une action légitime pendant la maintenance, mais il n'est très certainement pas légitime que le PC de test manoeuvre un disjoncteur. Nous étudierons cet exemple plus en détail par la suite.

Développé avec des techniciens PAC

Les recherches sur cette approche ont débuté en 2011. Les produits dérivés de ce concept, la supervision fonctionnelle 24 h/24 et 7 j/7 des SV, GOOSE et de la synchronisation horaire PTP sont disponibles dans un appareil d'analyse hybride mis sur le marché depuis 2015 (le DANEO 400 d'OMICRON). De plus, les retours de nombreux autres compagnies d'électricité du monde entier ainsi que certaines installations de validation de principe ont été intégrés à notre développement.

En 2018, l'une des premières installations de validation de principe a été mise en œuvre dans une sous-station de 110 kV de l'entreprise suisse de production et de distribution d'électricité et fonctionne depuis cette date. La Figure 4 montre l'installation dans une nouvelle sous-station en 2019. Dans ce montage, l'ensemble du trafic du switch « central » a été reflété dans StationGuard. Cela garantit que toute la communication depuis la passerelle ainsi que vers et depuis tous les IED est visible. Comme les connexions de maintenance à distance entrent également par ce switch, tout ce trafic peut également être inspecté par StationGuard. Puisque la communication GOOSE est en multidiffusion, et parce que la configuration du réseau le permet, tous les GOOSE des IED des travées du poste sont également visibles dans StationGuard.

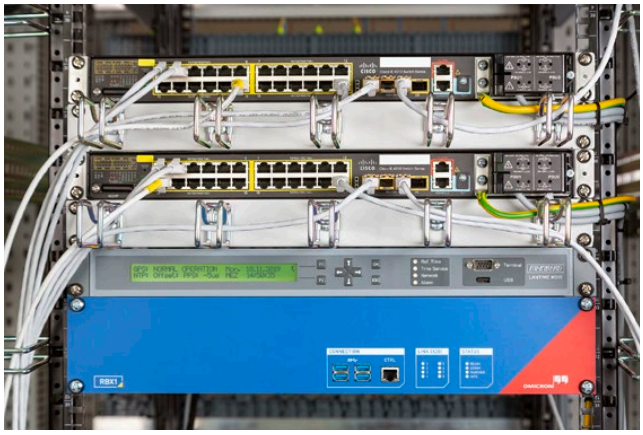

Figure 4 : StationGuard installé dans une nouvelle sous-station de 110kV, 2019

Affichage des alertes

Outre la suppression des fausses alarmes, il est également essentiel que les messages d'alarme délivrés soient compréhensibles par les techniciens en charge de l'exploitation des fonctions de protection, d'automatisation et réseau au sein du poste. Cela permet des temps de réaction plus rapides car souvent, ces alarmes sont déclenchées par des

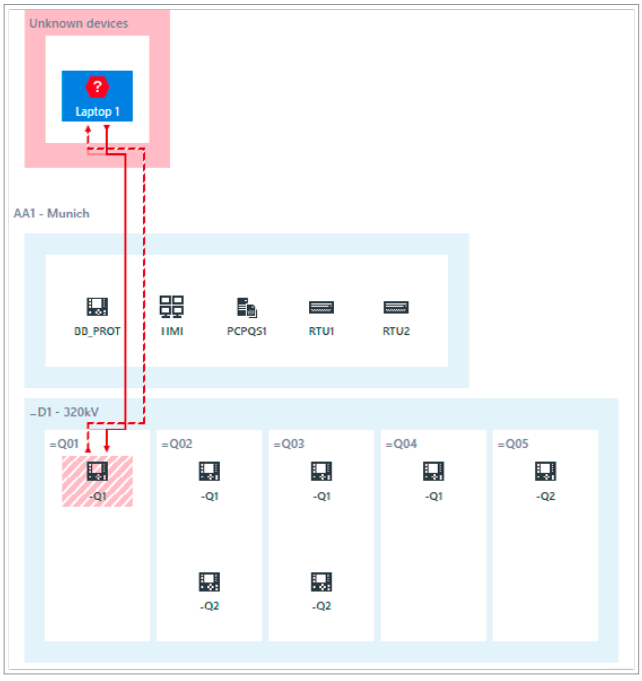

Figure 5 : Affichage graphique des alertes IDS à la place de simples listes des événements

techniciens travaillant dans le poste (ou à partir d'activités distantes). En outre, cela permet aux techniciens de sécurité et PAC de collaborer lors du traçage d'événements dans un poste.

La Figure 5 illustre une capture d'écran de l'affichage d'alarme graphique : l'alarme est illustrée sous forme de flèche allant du participant actif (Ordinateur portable 1) réalisant l'action interdite, jusqu'à la « victime » de l'action – un contrôleur de tranche dans la travée Q01.

La Figure 6 indique des détails sur cette alarme – un disjoncteur a été actionné (à l'aide d'une séquence de commande MMS), ce qui n'est pas autorisé pour un PC inconnu. En outre, cet ordinateur portable est également connecté via un protocole du fabricant et télécharge des fichiers par MMS. Les détails du message ont révélé des informations supplémentaires, telles que le nom du fichier téléchargé.

Figure 6 : Détails de la Figure 5 : portable inconnu tentant une manoeuvre non autorisée du disjoncteur

Inventaire des éléments

Tous les appareils qui communiquent sur le réseau sont détectés et affichés. Pour chaque appareil détecté, les informations provenant du trafic réseau capturé sont agrégées avec les informations provenant de la SCL. Cela permet d'afficher le fournisseur, le modèle et la version du microprogramme lorsqu'ils sont disponibles. La figure 7 montre les informations agrégées pour un cyber élément, y compris la description et le nom de l'équipement à partir du fichier SCD du projet.

Configuration

Comme nous l'avons déjà indiqué, aucune phase d'apprentissage n'est nécessaire. La détection débute dès la mise sous tension de l'appareil et ne peut pas être désactivée – pour des raisons de sécurité. Tant que le fichier SCD du poste ne sera pas chargé, tous les IED seront détectés et présentés comme des appareils inconnus. Une fois le fichier SCD chargé, les IED seront indiqués comme des appareils connus et la structure du poste sera assemblée en schéma « zéro filaire », tel qu'introduit avec StationScout. Les configurations peuvent également être préparées au bureau, puis installées sur site l'une après l'autre avec une mise en service rapide. Si tous les IED n'ont pas été créés dans un seul fichier (cela peut arriver), les IED additionnels peuvent aussi être importés un à un. Une fois l'importation terminée, l'utilisateur peut ajouter des rôles tels que « PC de test », « PC d'ingénierie », etc. aux appareils inconnus restants.

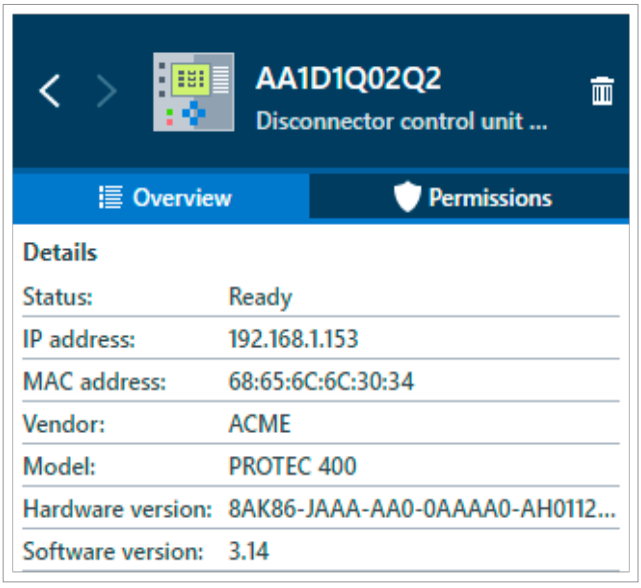

Figure 7 : Informations sur les actifs combinées du trafic réseau et du SCL

Que se passe-t-il en cas d'alarme ?

Il est important de noter que StationGuard est purement passif ; si une action n'est « pas autorisée », il déclenchera une alarme. Cette alarme peut être communiquée à la passerelle/au RTU et au centre de téléconduite ou à un système séparé collectant les alertes de sécurité – connu sous le nom de système de gestion des informations et des événements de sécurité (SIEM) utilisant le protocole Syslog. StationGuard ne réagit ou n'interfère pas activement avec le poste. Mais il permet une réaction rapide, par exemple l'isolement de l'appareil en question du réseau avant que tout dommage ne survienne. En fonction de la variante matérielle choisie, des sorties binaires définissables par l'utilisateur sont disponibles pour être branchées directement au RTU. Dans ce cas, la signalisation d'alarme s'effectue sans communication réseau et les alarmes

peuvent être intégrées dans la liste des signaux SCADA normaux comme tout autre signal câblé du poste.

Figure 8 : Vue de face de la variante 19" RBX1 de StationGuard

La cybersécurité de l'IDS lui-même

Comme les films de série B nous l'ont appris, les voleurs s'attaquent toujours au système anti-intrusion en premier lieu. Alors qu'en est-il de la sécurité de ce système d'alarme ? Un aspect important est qu'un matériel sécurisé autonome est utilisé plutôt qu'une machine virtuelle. Les deux variantes de StationGuard, la variante mobile (MBX1) et celle de 19" pour une installation permanente (RBX1), ont le même renforcement de plate-forme.

Toutes deux disposent d'une puce de cryptoprocesseur sécurisée conforme à la norme ISO/CEI 11889. Cela garantit que les clés cryptographiques ne sont pas stockées dans la mémoire flash mais dans une puce séparée protégée contre le piratage. En installant les certificats OMICRON sur cette puce pendant la production, une chaîne de démarrage mesurée et sécurisée est créée. Ainsi, chaque étape du processus de démarrage du firmware vérifie les signatures du module ou du pilote suivant à charger. Cela garantit que seul le logiciel signé par OMICRON peut être exécuté. Le stockage des appareils est crypté avec une clé unique propre à ce matériel, protégée à l'intérieur de la cryptopuce. Comme personne (y compris OMICRON) ne connaît cette clé, toutes les données de l'appareil seront perdues lors du remplacement ou de la réparation du matériel. De nombreux autres mécanismes s'assurent que les processus sur l'appareil ne peuvent pas être attaqués ou détournés, de sorte que l'approche de « défense approfondie » est également appliquée en profondeur dans le logiciel exécuté sur l'appareil.

Résumé

Les postes offrent des vecteurs potentiels aux cyber-attaques. Si un agresseur est capable d'influencer un ou plusieurs postes, les conséquences pour le réseau peuvent être dramatiques. C'est pourquoi des mesures de cybersécurité efficaces doivent être mises en place non seulement dans les centres de téléconduite, mais également dans les postes. Pour les postes CEI 61850, l'approche disponible en matière de détection d'intrusion produit quelques fausses alarmes et nécessite des faibles besoins de configuration grâce à la puissance du SCL. StationGuard détecte non seulement les menaces de sécurité, mais également les problèmes fonctionnels de la communication CEI 61850 et les IED – ce qui est utile dans les phases de tests de réception en usine et sur site. Il affiche les événements détectés dans le langage des techniciens de protection, d'automatisation et de contrôle-commande et offre ainsi l'avantage de permettre aux techniciens PAC et de sécurité de travailler ensemble à la résolution des problèmes.

Figure 9 : Vue de la face arrière de la variante 19" RBX1 de StationGuard

De plus amples informations sont disponibles à l'adresse : www.omicronenergy.com/stationguard