Nouvelle approche en matière de détection des cyber-intrusions dans les postes CEI 61850

Andreas Klien, OMICRON electronics GmbH, Klaus, Autriche
andreas.klien@omicronenergy.com

1 Résumé

Plusieurs couches sont nécessaires pour garantir la cybersécurité des postes. Les techniques cryptographiques permettent d'authentifier les appareils mais elles ne permettent pas 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 du poste. C'est pourquoi des mesures sont nécessaires pour détecter les attaques afin de permettre une réponse rapide et de minimiser les conséquences.
À cette fin, des systèmes de détection d'intrusion (IDS) sont utilisés dans les réseaux informatiques depuis plusieurs années. Comme on ne connaît qu'un petit nombre de cyber-attaques sur les postes, et que même la première occurrence d'une attaque peut avoir des conséquences dramatiques, les IDS doivent être en mesure de détecter les attaques sans connaître au préalable leurs signatures.
D'autres approches s'efforcent de détecter les attaques inconnues à l'aide d'une approche d'« apprentissage », en apprenant la fréquence de certains marqueurs de protocole. Ainsi, des événements rares mais légitimes déclenchent de nombreuses fausses alarmes.
Cet article présente une nouvelle approche de détection des intrusions dans les postes, utilisant un modèle du système d'automatisation CEI 61850 et le réseau pour différencier activités légitimes et malveillantes. Comme toutes les communications sont vérifiées, non seulement les intrusions de sécurité sont détectées, mais également les erreurs de communication et les défaillances des équipements. La configuration est automatiquement récupérée du fichier SCD CEI 61850 et aucune phase d'apprentissage n'est donc nécessaire.
Après avoir présenté les exigences logicielles et matérielles des IDS des postes, cette approche – appliquée dans le StationGuard d'OMICRON – est décrite en détail. L'article conclut avec un exemple pratique de mise en service.

2 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 une fonction sur au moins un équipement de protection, d'automatisme ou de commande au sein du poste. La Figure 1 montre tous les chemins marqués d'un chiffre par lesquels un poste peut être attaqué. Un agresseur peut pénétrer par la connexion du poste de commande (1), comme ça a été le cas dans l'une des cyber-attaques en Ukraine, où le firmware de passerelle a été modifié (entraînant leur destruction). Un autre point d'entrée concerne les PC d'ingénierie (2) 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 CPL dans la cyber-attaque de Stuxnet. Les ordinateurs portables utilisés pour tester le système CEI 61850 sont souvent directement connectés sur le réseau du poste, ce qui représente également une autre façon d'infecter les IED (3). 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 (4) comme chemin d'entrée possible. 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 chemin d'entrée ne puisse pas être exploitable.
Le stockage des paramètres (2a) et les documents de test (3a) 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.

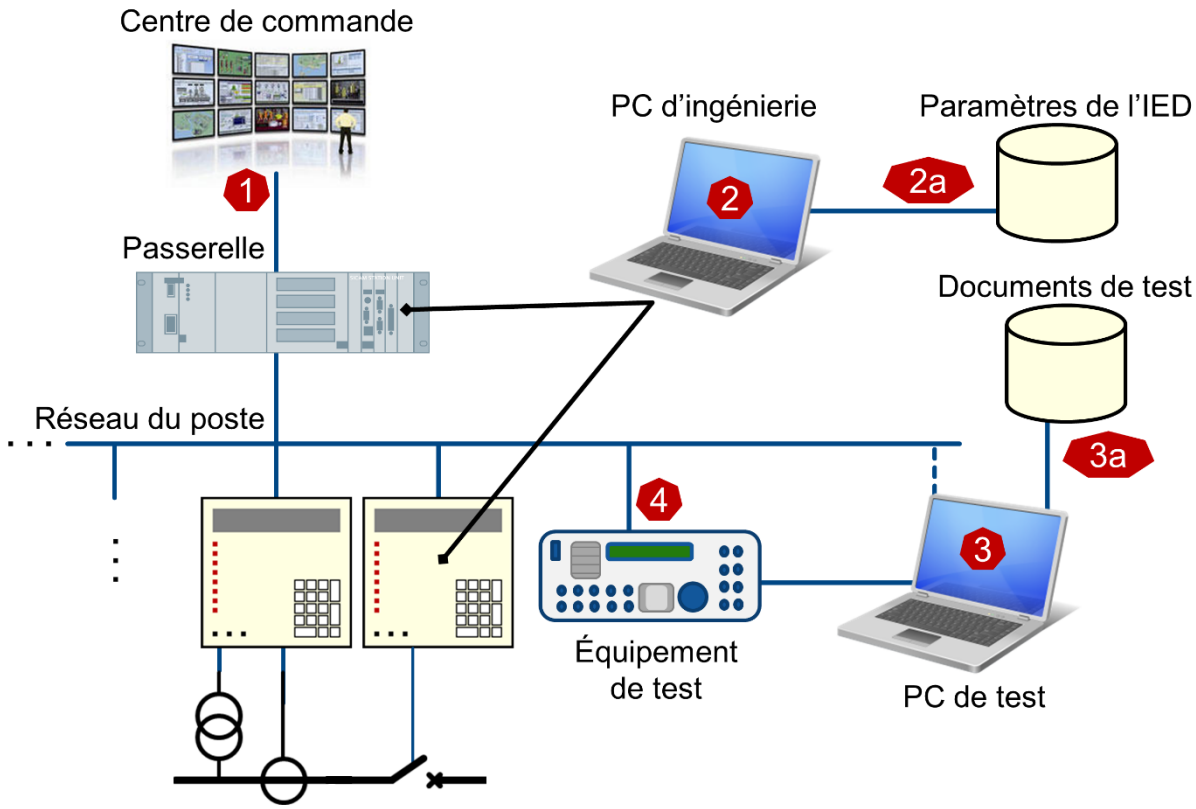

Figure 1 Vecteurs d'attaque d'un poste

3 La sécurité dans les postes 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 sur le réseau du poste. Comment peut-on l'empêcher ? »* Pour cela, nous ne devons pas nous concentrer sur le cas où l'agresseur dispose 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 du message GOOSE sont assez souvent présentés comme des « mécanismes de sécurité » GOOSE. Néanmoins, en 2019, de telles mesures devraient simplement s'appeler des « mécanismes de sécurité » car tout ennemi peut écouter 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'échantillon dans les valeurs échantillonnées. 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 d'envoi 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 le contrôle d'accès MMS et 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 chemin de communication non crypté. Le cryptage fournit uniquement une charge de processeur supplémentaire sur les IED, réduit 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 sur 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 issu des systèmes informatiques classiques, afin de détecter les menaces et activités malveillantes sur le réseau. De tels systèmes de détection d'intrusion sont à l'heure actuelle de plus en plus utilisés dans le domaine des réseaux électriques.

4 Les exigences en matière de détection d'intrusion dans les postes

Dans un poste CEI 61850, un système de détection d'intrusion serait connecté comme illustré en Figure 2. Des ports miroirs sur tous les switch applicables transmettent une copie de l'ensemble du trafic du réseau à l'IDS. L'IDS inspecte tout le trafic réseau communiqué par ces switch. 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 sur le réseau. Les switch au niveau des travées n'ont généralement pas besoin d'être couverts car le plus souvent seul le trafic en multidiffusion (GOOSE, Sampled Values) en provient. Pour s'assurer que l'ensemble du trafic en monodiffusion dans toutes les branches du réseau est analysé, il est nécessaire que tous les switch soient reflétés dans l'IDS, ce qui n'est pas toujours possible si des puces de switch intégrées dans les IED sont utilisées.

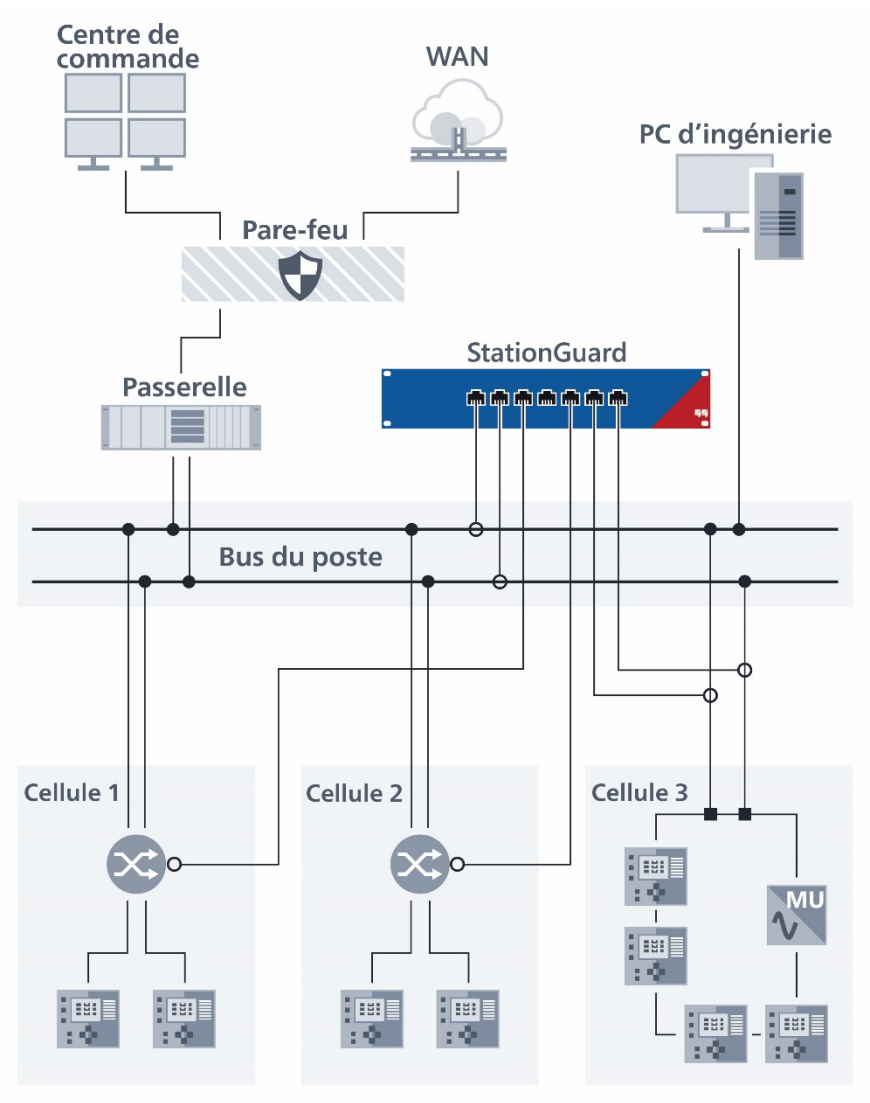

Figure 2 Comment l'IDS peut être connecté au réseau du poste

Cependant, les systèmes de détection d'intrusion 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 « 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, 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. C'est une approche très différente de celle d'un antivirus, qui recherche les virus dont il connaît la signature.

5 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 durée 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 durée de l'apprentissage, tels que des déclenchements de protection, des manœuvres manuelles ou automatiques d'équipements peu courantes, ou des tests et opérations de maintenance. Comme ces systèmes ne comprennent pas la sémantique des protocoles, les messages d'alarme sont exprimés en termes de détails de protocole techniques. Ainsi, les alarmes ne peuvent être examinées que par un technicien qualifié en détails de protocole CEI 61850 et habitué à la sécurité du réseau informatique. 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 service.

6 L'approche de StationGuard

Pour les postes CEI 61850, l'ensemble du système de contrôle commande, avec tous les équipements, 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 équipements 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 du système de contrôle commande numérique et du poste et comparer chaque paquet sur le réseau au modèle de système en service. 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.

La surveillance de la sécurité fonctionnelle

En substance, une surveillance fonctionnelle très détaillée est produite pour détecter les cyber-menaces sur 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 pannes de communication, les problèmes de synchronisation temporelle, 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 GOOSE uniquement, il existe 35 codes d'alarmes de cas de défaillance. Cela va de simples pointes de tension 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 sur le réseau ou dans la synchronisation temporelle.
Qu'en est-il pour la communication MMS ? À partir du modèle de système (extrait du SCL), on sait quels nœuds logiques contrôlent quels équipements primaires. On peut ainsi distinguer les actions correctes/incorrectes et critiques/non critiques. La manœuvre 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 actionne un disjoncteur. Nous étudierons cet exemple plus en détail par la suite.

Développé avec destechniciens PAC

Les recherches sur cette approche ont débuté en 2011. Les sous-produits de ce concept, supervision fonctionnelle 24 h/24 et 7 j/7 des SV, GOOSE et de la synchronisation temporelle PTP, sont disponibles dans un appareil d'analyse hybride (DANEO 400 d'OMICRON) depuis 2015. C'est ainsi que nous avons

été approchés par l'exploitant suisse de production et de distribution CKW. Nous connaissions bien les inconvénients des systèmes IDS disponibles sur le marché et nous cherchions une solution plus adaptée aux postes et plus conviviale pour les techniciens de protection, automatisme et contrôle (PAC). Cela a conduit à une coopération entre les techniciens PAC de CKW et l'équipe de développement de notre solution. J'étais curieux de savoir comment ils planifiaient la détection d'intrusion dans le cadre de la conception de la cybersécurité de leur futur poste. Entre-temps, les retours de nombreuses autres régies 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 un poste 110 kV de CKW et fonctionne depuis cette date. La Figure 3 montre l'installation utilisant la plate-forme matérielle mobile MBX1 au bas de l'image. Dans ce montage, l'ensemble du trafic du switch principal a été reflété dans StationGuard. Cela garantit que toute la communication depuis la passerelle et 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 sur les travées du poste sont également visibles dans StationGuard.

Figure 3 Installation dans un poste de 110 kV de CKW à l'aide de la variante de plate-forme mobile de StationGuard

Affichage des alertes

Au-delà de 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 protections, et du contrôle commande du poste. Cela permet des temps de réaction plus rapides car souvent, ces alarmes sont déclenchées par des 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 4 illustre une capture d'écran de l'affichage d'alarme graphique : l'alarme est illustrée sous forme de flèche allant du participant actif (PC de test) réalisant l'action interdite, jusqu'à la « victime » de l'action – un contrôleur de travée dans la cellule Q01. La Figure 5 indique des détails sur cette alarme –

un disjoncteur a été manœuvré (à l'aide d'une séquence de commande MMS), ce qui n'est pas autorisé pour un PC de test.

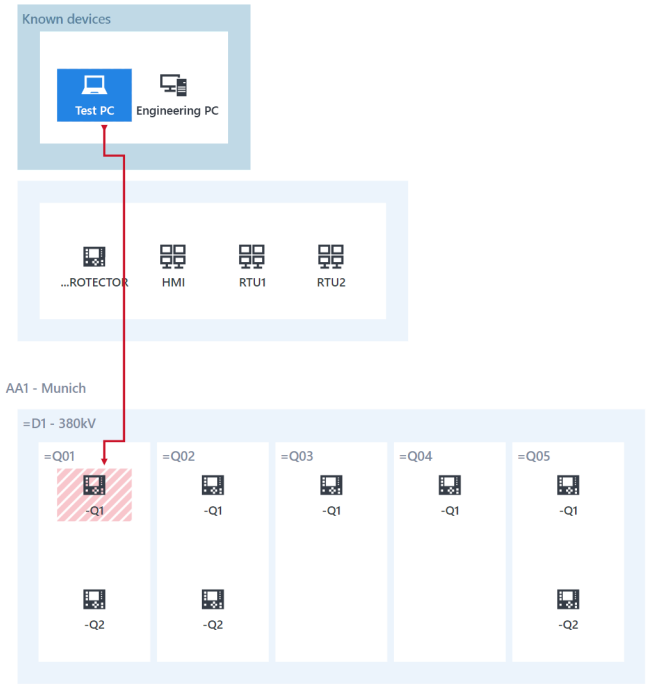

Figure 4 Affichage d'alarme graphique à la place de la liste des événements

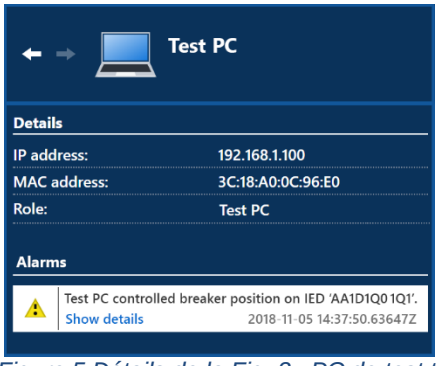

Figure 5 Détails de la Fig. 3 : PC de test tentant une commande non autorisée du disjoncteur

Mode de maintenance

Pour éviter les fausses alarmes, les tests de routine et les conditions de maintenance doivent être inclus dans le modèle du poste et de son contrôle commande. Cela signifie que l'équipement de test et d'ingénierie, y compris l'équipement de test de protection, peut être introduit dans le système. La Figure 6 montre que la maintenance a été activée pour la cellule Q01. Le PC de test de l'exemple ci-dessus peut maintenant en faire plus qu'avant. Il n'y aura pas d'alarme si le PC de test contrôle le test CEI 61850 ou le mode de simulation de l'IED Q1 dans cette travée. Cependant, la même alarme qu'avant sera activée si le PC de test manœuvre un disjoncteur dans cette travée , car les actions critiques telles que celle-ci ne sont pas autorisées pour un PC de test. Bien entendu, si les politiques de l'entreprise autorisent de telles actions, ces règles peuvent être modifiées.

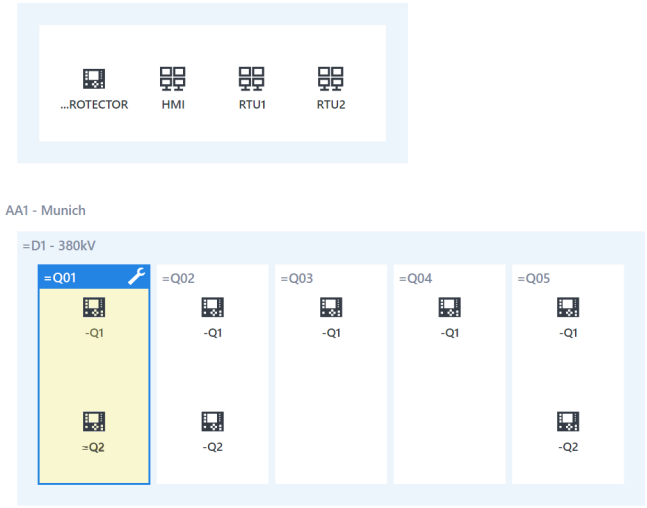

Figure 6 Mode de maintenance activé pour la cellule Q01

Configuration

Comme nous l'avons déjà indiqué, aucune phase d'apprentissage n'est nécessaire. La détection débute dès la mise en service 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 équipements inconnus. Une fois le fichier SCD chargé, les IED seront indiqués comme des équipements connus et la structure du poste sera assemblée en schéma « de communication simplifié », 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.

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 commande ou à un système séparé collectant les alertes de sécurité – connu sous le nom de système de gestion des incidents de sécurité (SIEM). StationGuard ne réagit ou n'interfère pas activement avec le poste. 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.

7 La cybersécurité de StationGuard

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. Tous ces mécanismes seront traités plus en détail dans un autre article.

8 Conclusion

Les postes offrent des vecteurs d'attaque 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 commande, mais également dans les postes. Pour les postes CEI 61850, l'approche disponible en matière de détection d'intrusion produit quelques fausses alarmes et la configuration de l'environnement est encore simple en raison de la puissance du SCL. Ce système détecte non seulement les menaces de sécurité, mais également les problèmes fonctionnels de la communication CEI 61850 entre les IED – ce qui est utile dans les phases de tests de réception en usine et sur site. Les systèmes de détection d'intrusion qui affichent les événements détectés dans le langage des techniciens de protection, d'automatisme et de contrôle ont l'avantage de permettre aux techniciens PAC et de sécurité de travailler ensemble à la résolution des problèmes.

OMICRON est une société internationale qui développe et commercialise des solutions innovantes de test et de diagnostic pour l'industrie électrique. Les produits OMICRON offrent aux utilisateurs une fiabilité extrême dans l'évaluation de leurs équipements primaires et secondaires. Des services dans le domaine du conseil, de la mise en service, du test, du diagnostic et de la formation viennent compléter l'offre OMICRON.

Des clients dans plus de 160 pays bénéficient déjà de la capacité d'OMICRON à mettre en œuvre les technologies les plus innovantes dans des produits d'une qualité irréprochable. Les centres de support implantés sur tous les continents leur offrent en outre une expertise et une assistance de tout premier plan. Tout ceci, associé à un réseau solide de partenaires commerciaux a contribué à faire de notre société un leader sur son marché dans l'industrie électrique.

Pour un complément d'information, une documentation supplémentaire et les coordonnées précises de nos agences dans le monde entier, veuillez visiter notre site Internet.

www.omicronenergy.com