CONCEPTION ET MISE EN SERVICE D'UNE ARCHITECTURE SECURISEE DE RESEAU DE POSTES

Andreas Klien[1], Yann Gosteli[2], Stefan Mattmann[3]

[1]OMICRON electronics GmbH, Klaus, Autriche (andreas.klien@omicronenergy.com)
[2]Centralschweizer Kraftwerke (CKW) AG, Lucerne, Suisse (yann.gosteli@ckw.ch)
[3]Centralschweizer Kraftwerke (CKW) AG, Lucerne, Suisse (stefan.mattmann@ckw.ch)

Mots clés : CYBERSÉCURITÉ, CEI 61850, DÉTECTION D'INTRUSION, AUTOMATISATION DE POSTE

Résumé

Les auditeurs des gestionnaires de réseau électrique et de la cybersécurité considèrent de plus en plus le centre de téléconduite comme un vecteur d'attaque critique et les postes comme des points d'entrée potentiels pour les cyber-attaques. Les processus, la manière dont la mise en service des systèmes de protection et de contrôle est réalisée et la manière dont l'accès à la maintenance à distance est mis en œuvre sont des facteurs de risque importants. Par conséquent, l'architecture du système de protection et de contrôle doit être revue du point de vue de la sécurité. Pour ce faire, l'entreprise suisse de production et de distribution d'électricité Centralschweizer Kraftwerke AG (CKW) a lancé en 2016/2017 un projet visant à développer une nouvelle architecture de référence pour ses systèmes secondaires. Leur conception se concentre à ces vecteurs d'attaque par des contre-mesures, tout en offrant un équilibre raisonnable entre maintenance et sécurité. Cette conception comprend plusieurs niveaux de sécurité contenant plusieurs couches de pare-feu. En outre, un système de détection d'intrusion (IDS) est appliqué. Le choix d'un IDS approprié pour les postes s'est avéré difficile, car de nombreux systèmes ne prennent pas en charge les exigences des réseaux de postes. Cet article commence par une énumération des principaux vecteurs d'attaque des postes, suivie d'une description de l'architecture de sécurité mise en œuvre pour la première fois dans un nouveau projet de poste 110 kV par CKW. Il conclut avec les expériences de choix d'un IDS adapté aux postes et les leçons tirées des tests de réception en usine de ce projet.

1. Introduction

1.1. Vecteurs d'attaque de postes

Dans le reste de cet article, nous allons supposer qu'une cyber-attaque sur un poste est un événement lors duquel un pirate modifie, dégrade ou désactive un service sur au moins un appareil de protection, d'automatisme ou de contrôle-commande au sein du poste. Pour y parvenir, un pirate peut utiliser l'un des chemins d'attaque représentés à la Figure 1 [1].

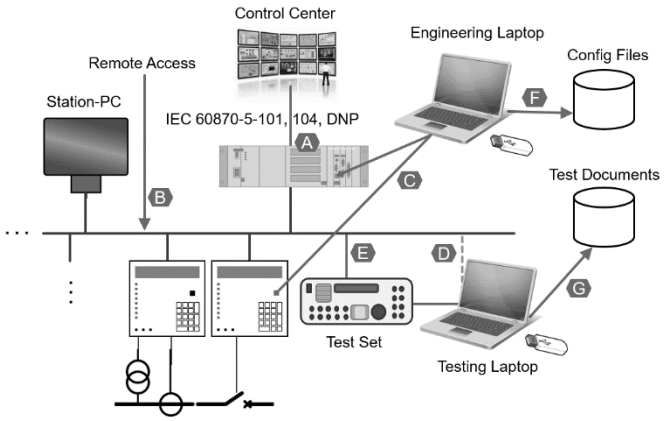

Figure 1 Vecteurs d'attaque sur des postes [1]

Un pirate peut pénétrer par la connexion du centre de téléconduite (**A**), comme ça a été le cas lors de la première cyber-attaque sur le réseau électrique en Ukraine, où le firmware de passerelles a été modifié (entraînant leur destruction) [2], ou par une connexion d'accès à distance (**B**), comme lors de la deuxième cyber-attaque en Ukraine en 2016 [3] et lors de la cyber-attaque « TRITON » sur des PLC d'infrastructures critiques [4].

Un autre point d'entrée concerne les PC d'ingénierie (**C**), branchés directement à l'équipement du poste ou au réseau 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 lors de la célèbre cyber-attaque de « Stuxnet » en 2010 [5].

Les ordinateurs portables utilisés pour tester le système CEI 61850 (**D**) sont souvent directement connectés au réseau de communication du poste, ce qui représente également une autre façon d'infecter

les équipements électroniques intelligents (IED). 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 (**E**) comme point 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 point d'entrée ne soit pas intéressant à exploiter.
L'emplacement de stockage des paramètres (**F**) et les documents de test (**G**) sont également une source potentielle de contamination. Leur serveur ou emplacement de stockage appartient donc également au périmètre critique et ne doit pas être situé dans la zone informatique du bureau. Par conséquent, il peut s'avérer judicieux d'introduire une solution de gestion des données séparée, isolée et protégée.

2. Proposition de nouvelle architecture de poste

2.1. Cybersécurité des OT à la pointe de la technologie

L'association suisse de l'industrie électrique VSE a créé un groupe de travail sur la sécurité des technologies opérationnelles (OT), qui a ensuite publié un document de recommandations de l'industrie : « Handbook on Basic Protection of Operational Technology in Power Systems » (Manuel de protection de base pour les technologies opérationnelles dans les systèmes électriques). Ce manuel fait référence au « Cyber Security Framework for Critical Infrastructure » (Cadre de cybersécurité pour les infrastructures critiques) du National Institute of Standards (NIST) [7], qui est sans cesse adapté et amélioré, la dernière version ayant été mise à jour en 2018. Le cadre du NIST est basé sur l'hypothèse qu'il n'existe jamais de protection totale contre les cyber-attaques. Avec suffisamment de connaissances et d'efforts, toutes les mesures de sécurité peuvent être violées. Sur cette base, le cadre du NIST recommande un processus composé de ces cinq étapes : « Identifier », « Protéger », « Détecter », « Réagir », « Récupérer ». La première étape est donc l'identification des vecteurs d'attaque (Identifier), comme présenté dans la section précédente de cet article. Ensuite, des contre-mesures peuvent être mises en œuvre à l'étape suivante (Protéger). Si un pirate peut encore franchir ces barrières, l'attaque doit être détectée (Détecter) et, au mieux, faire l'objet d'une action immédiate (Réagir) afin de rétablir un état normal le plus rapidement possible (Récupérer). Grâce aux enseignements tirés lors des étapes « Détecter » et « Réagir », de nouveaux vecteurs d'attaque peuvent être identifiés, de nouvelles contre-mesures peuvent être mises en œuvre et donc le processus se répète.

Les recommandations de l'industrie suisse mettent l'accent sur l'interaction des personnes, de la technologie et des processus au sein de l'organisation. Par exemple, la surveillance continue ou la détection d'intrusion (Détecter) n'a de sens que si l'on répond de manière appropriée aux messages d'alarme. Ainsi, les messages d'alarme doivent être compréhensibles pour toutes les personnes impliquées dans le processus de réponse : techniciens OT et spécialistes de la sécurité informatique. Dans le cas contraire, le processus de réponse devient inefficace. De plus, si l'IDS délivre trop de fausses alarmes, toutes les alarmes seront finalement ignorées.

2.2. Initiatives de cybersécurité des OT chez CKW [6]

Ces dernières années, la sécurité des OT, en particulier des systèmes de contrôle et de protection, a pris de plus en plus d'importance chez CKW. Cela est dû aux recommandations de l'industrie en Suisse mentionnées précédemment, mais surtout aux évaluations de la sécurité des OT réalisées par CKW ces dernières années. Ces évaluations ont révélé des points faibles tant au niveau des réseaux que de la technologie de contrôle des postes utilisée dans les postes. Par exemple, des transitions de zones dangereuses et certaines méthodes critiques d'accès à distance sur les ordinateurs de contrôle des postes ont été détectées. En outre, il n'a pas été possible d'évaluer si une attaque avait actuellement lieu dans le réseau du poste ou s'il existait des activités suspectes sur le réseau qui pourraient indiquer une attaque imminente.
D'après ces conclusions, CKW s'est fixé pour objectif d'éliminer les points faibles essentiels et de renforcer les exigences relatives à l'architecture de ses futurs postes. Ces conclusions ont donc été intégrées dans la nouvelle norme de conception de postes de CKW.

En plus de travailler sur cette norme de conception, CKW a pu s'impliquer dans le groupe de travail suisse pour le manuel de sécurité des OT mentionné. Sur la base de cet échange d'informations, CKW a systématiquement intégré les conclusions du groupe de travail dans ses propres normes de conception.

En 2016/2017, une équipe de projet de CKW a commencé à planifier le nouveau poste « US Rothenburg », qui sera mis en service en 2020. Dans ce projet, la nouvelle norme d'architecture sécurisée de CKW a été appliquée et les dernières recommandations du manuel de sécurité des OT suisse ont été suivies. Pour pouvoir mettre en œuvre ces mesures de sécurité élaborées, l'entreprise CKW a décidé de mettre en œuvre l'architecture du réseau et la configuration des switchs elle-même.

2.3. Conception du réseau

Dans la conception du réseau du poste US Rothenburg, des obstacles ont été construits dans chaque zone pour rendre une attaque aussi difficile que possible. La Figure 2 illustre le réseau du poste US Rothenburg.

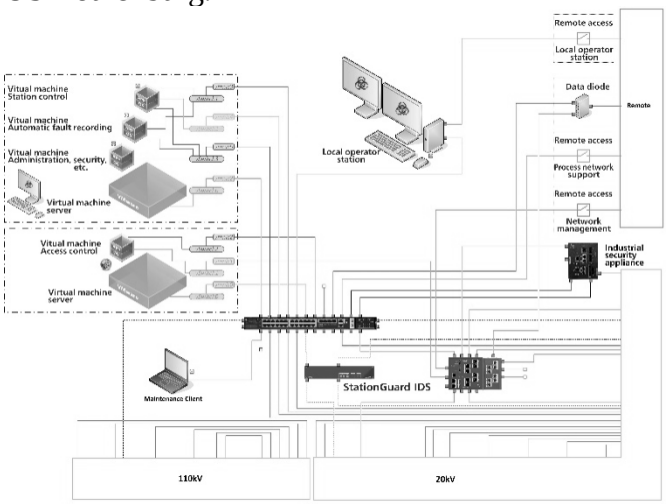

Figure 2 Architecture du réseau du poste US Rothenburg [6]

Dans cette architecture, tous les vecteurs d'attaque décrits à la section 1.1 de cet article sont traités en utilisant toute une série de mesures de sécurité. Les connexions à distance du site ont été traitées avec la plus haute priorité. Ces connexions à distance sont sécurisées par des pares-feux et des tunnels, mais également désactivées par défaut. Les connexions pour l'accès à distance ne sont activées que lorsque cela est nécessaire. Cela signifie que plusieurs personnes sont impliquées pour permettre l'accès à distance, comme dans un processus d'authentification à deux facteurs.

La communication entre le système SCADA (Supervisory Control and Data Acquisition) et le centre de téléconduite s'effectue au moyen du protocole série CEI 60870-5-101. Tous les accès aux équipements du poste à des fins de maintenance se font exclusivement par l'intermédiaire de postes de travail spéciaux, qui sont sécurisés de manière appropriée. Ces postes de travail sont virtualisés et se trouvent dans un emplacement central. Cet accès à distance à des fins de maintenance doit également être activé à distance.

Le système SCADA, le système d'oscilloperturbographie et les serveurs du système de sécurité sont virtualisés et exploités sur une machine hôte située localement dans le poste. Même le poste IHM local n'accède à ces systèmes qu'à l'aide d'un bureau distant par l'intermédiaire d'un pare-feu local supplémentaire. Le contrôle d'accès basé sur le rôle est utilisé. Cela signifie qu'il n'y a pas un mot de passe par équipement, mais un mot de passe par utilisateur. L'avantage est qu'un technicien peut utiliser son propre mot de passe dans tous les postes. Si un employé quitte l'entreprise, son utilisateur peut facilement être supprimé, aucun mot de passe ne doit être modifié. Cette gestion des utilisateurs est mise en œuvre à l'aide d'un serveur Active Directory (AD) central et d'un serveur RADIUS local dans le poste. Les utilisateurs doivent se connecter à l'aide de l'AD qui leur attribue les autorisations nécessaires. Si nécessaire, l'accès à l'AD central peut être activé à partir d'un emplacement central. En outre, les utilisateurs doivent se connecter à chaque IED avec un nom d'utilisateur et un mot de passe individuels. De ce fait, les IED utilisent le serveur RADIUS local pour vérifier l'authentification de l'utilisateur et du mot de passe et pour récupérer les autorisations attribuées à cet utilisateur. Cela s'applique aussi bien à l'accès aux appareils équipés d'outils d'ingénierie qu'à l'utilisation en face avant de l'IED. Aucun mot de passe standard n'est utilisé.

Tous les PC connectés au réseau du poste sont renforcés. Cela se fait, entre autres, en configurant le pare-feu Windows conformément à la matrice de communication du poste et, selon le rôle de ce client, en bloquant les fonctions des systèmes d'exploitation qui ne sont pas nécessaires.

Comme mesure de sécurité supplémentaire, le contrôle d'accès au réseau est mis en œuvre par le biais d'un contournement d'authentification MAC, ce qui signifie que seuls les équipements enregistrés peuvent se connecter au switch réseau.
En cas de dysfonctionnement, le switch doit également reconnaître et accepter les équipements de réserve du stock. Dans les switchs réseau du poste et le pare-feu, les listes de contrôle d'accès sont configurées de manière à imposer quel équipement est autorisé à communiquer avec quel autre participant au réseau, y compris le protocole utilisé et le port du switch.
Le réseau de communication du poste et le réseau de configuration et de maintenance sont logiquement (VLAN) et physiquement séparés. Cela signifie que, sur chaque IED, la communication CEI 61850 MMS et GOOSE fonctionne sur une interface réseau différente de l'accès à la maintenance. En outre, l'ensemble du réseau de communication du poste est segmenté, ce qui permet, entre autres, de séparer les segments suivants via un pare-feu :

- 110 kV (GOOSE et MMS)
- 20 kV (GOOSE et MMS)
- IHM locale
- Passerelle du protocole
- Systèmes auxiliaires
- Réseaux de maintenance pour les IED et les clients
- Réseau de gestion, VM, RADIUS

La communication entre le poste et les zones de réseau de niveau supérieur est en outre sécurisée par une diode de données. Cette diode garantit que seules les sessions de communication sortantes peuvent être initiées et fournit un autre niveau de sécurité.
Un système de détection d'intrusion (IDS) surveille l'ensemble du trafic réseau dans le système en utilisant une approche de liste blanche, c'est-à-dire que tout trafic inconnu, qui ne figure pas sur la liste blanche, crée par défaut une alarme. L'IDS signale l'alarme au centre de téléconduite par l'intermédiaire du RTU et à un centre d'exploitation de sécurité par le biais de protocoles spécialisés pour l'enregistrement des alarmes.

3. Détection d'intrusion

L'architecture de sécurité de CKW est basée sur l'établissement de segments de réseau, chacun étant séparé par le pare-feu. La configuration du pare-feu spécifie exactement quels protocoles peuvent être utilisés pour la communication entre les segments. Toutefois, les protocoles autorisés par le pare-feu, tels que MMS/GOOSE utilisé dans la norme CEI 61850, et les protocoles d'ingénierie propres aux fournisseurs peuvent également être utilisés pour attaquer les équipements et les infecter. Dans de tels scénarios, CKW voulait être en mesure de détecter les activités non autorisées à un stade précoce. À cet effet, il a été décidé qu'un IDS serait utilisé dans l'architecture de référence de CKW.
Pour pouvoir analyser le trafic le plus critique, c'est-à-dire la communication entre la passerelle et les IED, au moins tout le trafic de la passerelle devrait être reflété dans l'IDS. Les switchs des cellules n'ont généralement pas besoin d'être couverts car le plus souvent seul le trafic en multidiffusion tel que GOOSE ou Sampled Values en découle. Pour s'assurer que l'ensemble du trafic en monodiffusion dans toutes les branches du réseau est également analysé, il est recommandé que tous les switchs soient reflétés dans l'IDS.
Dans l'architecture de CKW, l'IDS est connecté à des ports miroirs sur tous les switchs réseau. Cela signifie que l'IDS analyse le trafic sur le réseau de communication du poste ainsi que le trafic entrant à distance avant et après avoir passé les pares-feux.

3.1. Exigences pour les IDS de postes

Le choix d'un IDS adapté aux postes s'est avéré difficile. Il était important que l'IDS puisse être facilement utilisé par les techniciens de protection, de contrôle-commande et de réseau responsables de tous les IED et de l'équipement de réseau. Pour prendre en charge le processus de réponse aux alarmes, il doit être facilement possible d'associer les alarmes de l'IDS aux événements du poste et aux journaux d'événements dans l'IHM. Par conséquent, l'IDS doit permettre des vues spécifiques pour les postes au lieu d'utiliser uniquement la terminologie de la sécurité informatique.
Jusqu'à récemment, il n'existait que deux approches principales pour l'IDS : l'approche basée sur la signature et l'approche « basée sur l'apprentissage ».
L'approche basée sur la signature fonctionne avec une liste noire comme un antivirus classique pour PC. Il recherche des modèles de virus et de logiciels malveillants connus. Le problème est qu'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. Un IDS de poste doit pouvoir détecter les attaques sans savoir au préalable à quoi elles ressemblent.
Par conséquent, un plus grand nombre d'IDS utilisent une approche « basée sur l'apprentissage ». L'IDS examine les paramètres génériques de différents protocoles pour connaître les valeurs moyennes et la fréquence de chaque paramètre.
Ensuite, en fonctionnement normal, une alarme est déclenchée chaque fois que la communication réseau s'écarte sensiblement de la moyenne observée. Par conséquent, de fausses alarmes sont déclenchées pour tous les événements qui ne se sont pas produits pendant la phase d'apprentissage. Cela inclut, par exemple, les déclenchements et les manœuvres d'exploitation, ou les tests de protection de routine. Comme le système ne connaît pas la signification des télégrammes sur le réseau, les messages d'alarme font référence aux paramètres génériques du protocole, comme « Échec réponse-écriture-confirmation MMS ». Il en résulte un nombre élevé de fausses alarmes, chacune d'entre elles devant être vérifiée par des spécialistes en informatique et des spécialistes de la norme CEI 61850. Un tel effort dans le processus de réponse n'était pas acceptable pour CKW.

3.2. Utilisation de l'approche IDS

Pour les postes CEI 61850, l'ensemble du système de contrôle-commande, avec tous les IED, modèles de données et schémas de communication, est décrit dans un format normalisé appelé SCL. Ces informations permettent d'utiliser une approche différente pour détecter les intrusions. Le système de surveillance peut créer un modèle de système du système de contrôle-commande numérique et comparer chaque paquet sur le réseau à son modèle. Même les variables contenues dans les messages communiqués (GOOSE, MMS, SV) peuvent être comparées aux attentes dérivées du modèle de système. Ce modèle de système comprend donc une liste blanche, car tous les paquets ne correspondant pas au modèle de système déclencheront une alarme. CKW a sélectionné un IDS basé sur cette approche (OMICRON StationGuard).
Cette approche permet de détecter les menaces de cybersécurité comme les paquets mal formés et actions de contrôle MMS interdites, mais aussi les pannes de communication, les problèmes de synchronisation horaire, et par conséquent aussi certaines défaillances de l'équipement.
En utilisant la section du poste dans le fichier SCL, un schéma général du poste peut être créé automatiquement, et les alarmes peuvent être représentées dans ce schéma. Un tel affichage peut aider à identifier si une action qui a déclenché une alarme a été effectuée intentionnellement : par exemple, l'événement peut avoir été causé par un technicien lors d'une opération de test, ou il peut correspondre à une activité malveillante d'un PC de test infecté.

Au moment de la rédaction de cet article, les tests de réception en usine (FAT) du poste US Rothenburg étaient terminés et sa mise en service était en cours. Concernant les FAT, il a fallu terminer quasiment toute la configuration du réseau pour pouvoir tester si la conception fonctionne. Nous avons également appris que l'IDS a besoin d'une assistance pour l'acheminement effectué par les multiples niveaux de pare-feu. De multiples duplications du trafic avant et après les pares-feux pourraient brouiller l'affichage de l'IDS. Toutefois, l'IDS sélectionné prend correctement en charge ce scénario. En outre, la création de la matrice de communication pour la configuration du pare-feu représente un effort considérable, car elle doit être réalisée manuellement. Comme l'IDS dispose déjà d'une liste blanche de SCL, ce processus pourrait également être automatisé à l'avenir.

4. Conclusion et perspectives

Si un pirate est capable d'influencer un ou plusieurs postes, les conséquences pour le réseau peuvent être dramatiques. Les postes offrent plusieurs vecteurs d'attaque où le pare-feu peut être contourné. L'architecture sécurisée de réseau de postes de CKW fournit de nombreuses contre-mesures aux vecteurs d'attaque identifiés dans cet article. Les mesures de sécurité assurent un niveau élevé de sécurité tout en permettant des procédures de maintenance et d'ingénierie efficaces grâce à l'accès à distance. Cette architecture repose sur la détection des intrusions au cœur du réseau. Pour les postes CEI 61850, une approche IDS utilisant le SCL pour établir automatiquement une liste blanche de tout le trafic réseau autorisé est disponible. Cela permet également d'afficher les événements détectés dans

le langage des techniciens de protection, d'automatisation et de commande afin qu'ils puissent collaborer avec les techniciens de sécurité informatique pour déterminer efficacement la cause des événements.

C'est dans la nature de la cybersécurité que chaque conception puisse être améliorée. Parmi les améliorations, on peut citer par exemple le contrôle d'accès au réseau basé sur des certificats selon la norme 802.1X [8] au lieu de l'approche MAC actuellement utilisée. Toutefois, pour cela, un plus grand nombre d'IED doivent prendre en charge la norme 802.1X, ce qui n'est pas le cas actuellement. Des articles complémentaires devraient rassembler les conclusions de la mise en service de ce projet et documenter les résultats des futures évaluations de sécurité et des tests de pénétration effectués sur ce poste.

5. Références

[1] Klien, A. : « New approach for detecting cyber intrusions in IEC 61850 substations », PAC World Conference Europe, Glasgow, 2019

[2] « Analysis of the Cyber Attack on the Ukrainian Power Grid », SANS, E-ISAC, https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf, accédé en novembre 2019

[3] « WIN32/INDUSTROYER - A new threat for industrial control systems », https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, accédé en novembre 2019

[4] « Threat Research - Attackers Deploy New ICS Attack Framework "TRITON" and Cause Operational Disruption to Critical Infrastructure », https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, accédé en novembre 2019

[5] D. Kushner : « The Real Story of Stuxnet
How Kaspersky Lab tracked down the malware that stymied Iran's nuclear-fuel enrichment program », IEEE Spectrum, février 2013

[6] Gosteli, Y., Klien A. : « Sichere Stationsleittechnik – Neue Cyber Security Architektur mit Intrusion Detection in der US Rothenburg », bulletin.ch, 2019, 6, p. 50-52

[7] NIST : « Framework for improving critical infrastructure cybersecurity », version 1.1, National Institute of Standards and Technology, avril 2018

[8] IEEE : « 802.1X-2010 - IEEE Standard for Local and metropolitan area networks--Port-Based Network Access Control », International Standard, février 2010

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