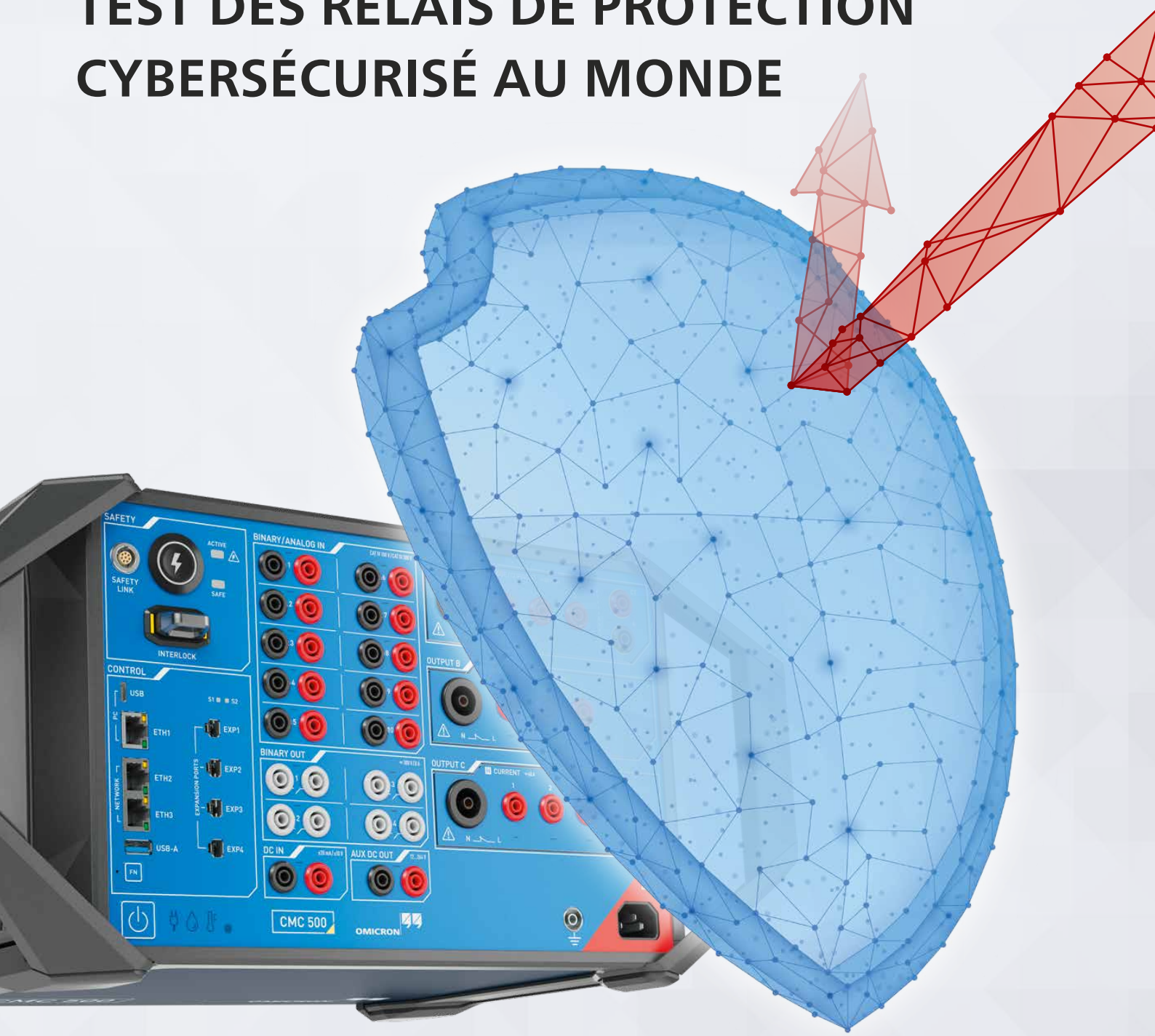
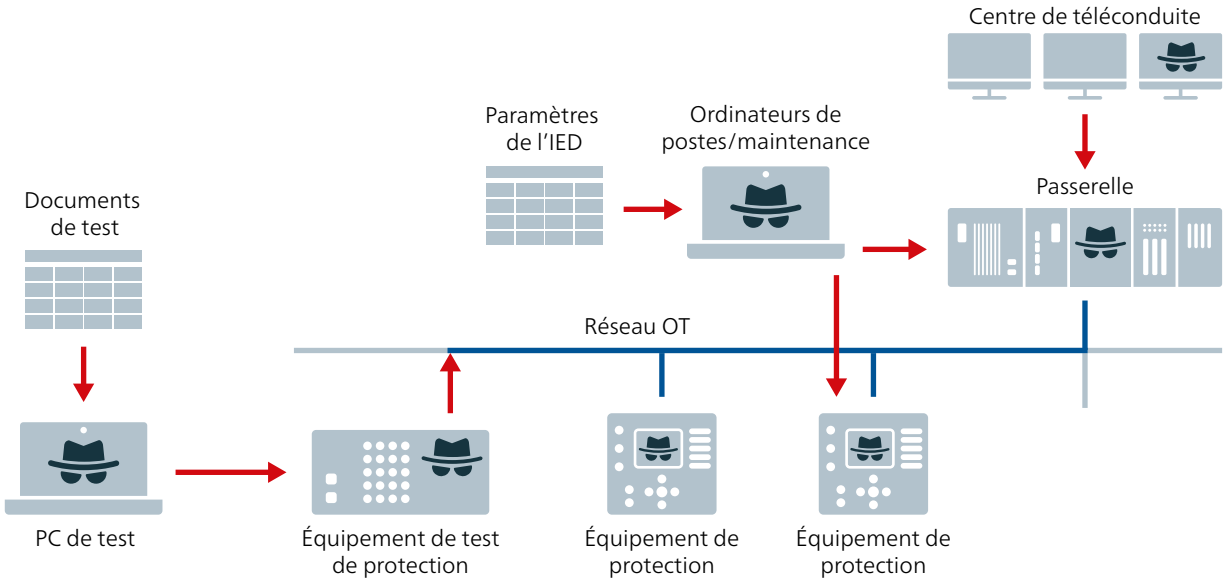
CMC 500

LE PREMIER ÉQUIPEMENT DE TEST DES RELAIS DE PROTECTION CYBERSÉCURISÉ AU MONDE





En cas de protection insuffisante, les pirates disposent de plusieurs possibilités pour accéder au bus de station des infrastructures critiques.

Une protection efficace des postes contre les cyberattaques nécessite une approche holistique. Les équipements de test des relais de protection cybersécurisés sont un élément essentiel de toute stratégie de sécurité. Découvrez pourquoi et comment nous avons établi une nouvelle norme en matière de cybersécurité pour les tests de protection.

Les cyberattaques sur les infrastructures critiques ne relèvent plus de la fiction. De nombreux incidents concrets en témoignent, notamment l'attaque en Ukraine en 2016 où des assaillants ont exploité la connexion vers un centre de téléconduite. Depuis, diverses réglementations imposent des exigences strictes pour protéger les infrastructures critiques. Par exemple, la directive NIS2 (sécurité des réseaux et de l'information) définit le cadre pour l'amélioration de la cybersécurité dans l'UE.

Une analyse approfondie des menaces, identifiant un maximum de vulnérabilités et de vecteurs d'attaque, est essentielle pour sécuriser les postes électriques. Une étude menée par le Ponemon Institute a révélé que 100 % des attaques examinées exploitaient des vulnérabilités connues. La diversité des vecteurs d'attaque rend la tâche complexe pour les compagnies d'électricité. En voici quelques exemples :

- Connexion avec le centre de téléconduite et les canaux de maintenance à distance
- Ordinateurs de postes et de maintenance
- Fichiers de firmware et de réglages des équipements de protection eux-mêmes
- Équipements de test utilisés dans les postes

Malgré une sensibilisation accrue aux cybermenaces, les solutions adaptées manquent toujours.

Dans le domaine des tests de protection, les équipements de test des relais de protection et les ordinateurs portables de test constituent eux-mêmes des vecteurs ▸

« Affirmer qu'un produit est cybersécurisé dès la conception implique bien plus que des mesures de protection matérielles et logicielles. ***L'analyse des vecteurs d'attaque potentiels est une démarche globale, englobant l'ensemble de l'entreprise et ses processus. »***

d'attaque. Un équipement de test sécurisé permet de traiter ces deux risques simultanément. Jusqu'à présent, il n'existait aucune solution sur le marché. C'est pourquoi nous avons conçu le CMC 500.

Les équipements de test comme vecteurs d'attaque

Pour répondre à cette problématique, nous avons conçu le CMC 500, le premier équipement de test des relais de protection renforcé contre les cyberattaques. Mais quelles mesures ont été nécessaires ? Et que signifie réellement cybersécurisé ? À l'instar d'une analyse des menaces appliquée aux infrastructures critiques, la première étape a été d'identifier les potentiels vecteurs d'attaque des équipements de test et de les traiter progressivement. Notre expertise avec StationGuard, notre système de détection d'intrusion (IDS) conçu pour le secteur de l'énergie, s'est révélée précieuse. Une approche globale a guidé le développement du CMC 500 pour une cybersécurité maximale. Cela impliquait des mesures au niveau des processus, de la production, des logiciels et du matériel. Ces mesures combinées ont permis de mettre en œuvre une véritable cybersécurité dès la conception.

Sécurité du matériel de test

Sur le plan matériel, le CMC 500 est doté d'un module de plate-forme fiable (TPM 2.0) conforme à la norme ISO/CEI 11889. Ce cryptoprocesseur constitue la base de plusieurs mesures de sécurité, en permettant le stockage sécurisé de clés et de certificats. Ainsi, toutes les communications sont chiffrées de manière fiable, et chaque équipement de test peut être identifié de façon unique, comme une empreinte digitale. Ceci permet de prévenir les attaques par interception / usurpation. De plus, la fonctionnalité de sécurisation et de mesure du démarrage garantit l'authenticité du firmware à chaque démarrage et empêche l'appareil de démarrer en cas d'échec de vérification. Un mot de passe peut également être défini pour renforcer la protection des communications.

Sécurité du logiciel de test

Un matériel sécurisé ne peut être pleinement efficace sans un logiciel de test adapté. C'est pourquoi nous avons appliqué une approche stricte à son développement. Nous nous sommes basés sur le processus Secure Software Development Life Cycle (SSDLC). Cette méthodologie, déjà utilisée pour StationGuard, garantit des normes de qualité élevées et une sécurisation du code, tout en offrant une gestion rigoureuse et la divulgation des vulnérabilités potentielles. Nous misons sur la transparence pour assurer la cybersécurité de nos produits.

Pour en savoir plus sur notre gestion des vulnérabilités, consultez la page omicronenergy.com/product-security.

Sécurité de la production et des réparations

Nous ne nous appuyons pas uniquement sur des fournisseurs et partenaires de confiance pour la production et la réparation. Les étapes les plus critiques sont réalisées en interne. Seuls quelques employés autorisés peuvent configurer les certificats

et clés des CMC 500. Ce processus structuré et sans interruption empêche toute manipulation durant son exécution. Grâce à un module de sécurité matérielle, nos applications logicielles développées en interne garantissent que les clés cryptographiques ne peuvent pas être volées. Toute tentative d'accès physique non autorisé entraîne la destruction de la clé. Enfin, comme dernière touche à nos mesures de protection complètes, ces modules sont stockés dans une salle de serveur hautement sécurisée.

Sécurité des processus au sein de l'entreprise

Qu'il s'agisse de développement matériel ou logiciel, de la production ou des réparations, les collaborateurs restent un élément central des processus de sécurité. Sensibiliser et former nos équipes à la sécurité informatique et des données est essentiel pour compliquer la tâche des cybercriminels. Nos employés participent régulièrement à des simulations de phishing en interne et des audits ISO/CEI 27001 afin de démontrer et renforcer leurs compétences en matière de cybersécurité.

Une nouvelle référence en matière de cybersécurité

Affirmer qu'un produit est cybersécurisé dès la conception implique bien plus que des mesures de protection matérielles et logicielles. L'analyse des vecteurs d'attaque potentiels est une démarche globale, englobant l'ensemble de l'entreprise et ses processus. C'est cette approche que nous avons adoptée pour le CMC 500. De plus, nous accompagnons nos produits tout au long de leur cycle de vie, avec un programme de gestion des vulnérabilités dédié. C'est ainsi que nous avons créé une solution unique sur le marché pour protéger les équipements de test des vecteurs d'attaque : le CMC 500, le premier équipement de test des relais de protection cybersécurisé.

Découvrez le nouveau CMC 500 !

omicron.energy/new-cmc

« Le cryptoprocesseur constitue la base de plusieurs mesures de sécurité, *en permettant le stockage sécurisé de clés et de certificats. »*