AYI NEDJIMI Consultants

Sécurité systèmes de contrôle énergie et utilities OT

Catégorie : Sécurité Industrielle OT/ICS Lecture : 8 min Publié le : 12/03/2026 Auteur : Ayi NEDJIMI

Guide sécurité des systèmes de contrôle pour le secteur énergie et utilities : SCADA électrique, smart grid, IEC 61850 et protection infrastructures.

Résumé exécutif

Les systèmes de contrôle du secteur de l'énergie et des utilities figurent parmi les cibles prioritaires des cyberattaques étatiques en raison de leur potentiel de disruption massive affectant l'ensemble de l'économie et de la population. Ce guide analyse les spécificités de sécurité des systèmes SCADA électriques distribuées sur des centaines de sous-stations, des réseaux smart grid intégrant des millions de compteurs intelligents, des protocoles IEC 61850 et IEC 60870-5-104 dépourvus de sécurité native, et des systèmes de distribution d'eau et de gaz confrontés à des menaces croissantes. Les recommandations couvrent la protection des sous-stations contre les attaques type Industroyer, la sécurisation des compteurs intelligents face aux attaques de masse, et la résilience opérationnelle face aux scénarios d'attaque documentés contre les infrastructures énergétiques ukrainiennes et américaines.

Le secteur de l'énergie constitue la cible privilégiée des groupes de cyberattaque étatiques pour son potentiel de disruption massive et son effet de cascade sur l'ensemble de l'économie. Les attaques contre le réseau électrique ukrainien en 2015 et 2016, les tentatives d'intrusion documentées contre des centrales nucléaires américaines, et les capacités du malware PIPEDREAM/INCONTROLLER ciblant les systèmes de contrôle industriels de multiples secteurs démontrent une menace active et persistante contre les infrastructures énergétiques. Les systèmes de contrôle de ce secteur présentent des caractéristiques uniques qui complexifient leur sécurisation : une architecture géographiquement distribuée sur des centaines voire des milliers de sites distants, des protocoles spécifiques comme IEC 61850 pour les sous-stations et IEC 60870-5-104 pour la téléconduite, des exigences de temps réel incompatibles avec certaines mesures de sécurité, et une interconnexion croissante via les smart grids et les énergies renouvelables distribuées qui élargissent considérablement la surface d'attaque. La protection de ces systèmes vitaux exige une expertise sectorielle pointue combinant la connaissance des réseaux électriques, des protocoles de téléconduite et des menaces cyber spécifiques au secteur énergétique.

Architecture SCADA des réseaux électriques et surfaces d'attaque

L'architecture SCADA des **réseaux de transport et de distribution électrique** se structure autour de centres de conduite (centres de dispatching) supervisés par des opérateurs 24/7, connectés à des centaines de sous-stations via des réseaux de télécommunication dédiés ou partagés. Chaque sous-station contient des dispositifs électroniques intelligents (IED) communiquant en IEC 61850 au sein de la sous-station, et en IEC 60870-5-104 (ou DNP3 en Amérique du Nord) vers le centre de conduite.

La surface d'attaque de cette architecture est considérable. Les liaisons de téléconduite, historiquement sur des réseaux série dédiés, migrent vers des réseaux IP partagés parfois avec des communications corporate. Les sous-stations distantes, physiquement accessibles dans des zones rurales, présentent des risques d'intrusion physique. Les *passerelles de protocole* convertissant les communications IEC 61850 internes en IEC 104 vers le centre de conduite constituent des points de pivot exploitables. La modernisation vers les smart grids ajoute des millions de points d'entrée via les compteurs intelligents et les systèmes de gestion de la demande. L'approche de segmentation réseau et Zero Trust doit s'adapter à cette architecture distribuée massive du secteur énergétique.

L'attaque du 17 décembre 2016 contre le réseau électrique ukrainien a utilisé le malware Industroyer/CrashOverride, premier malware spécifiquement conçu pour attaquer les réseaux électriques via les protocoles IEC 61850, IEC 104 et OPC DA. Le malware a envoyé des commandes d'ouverture de disjoncteurs via le protocole IEC 104 à la sous-station de transmission de Pivnichna près de Kiev, causant une coupure de courant d'environ une heure. L'attaque incluait un composant de sabotage ciblant les protections de distance des lignes électriques, qui aurait pu causer des dommages physiques aux équipements en cas de remise sous tension non contrôlée.

Comment sécuriser les protocoles IEC 61850 et IEC 104 ?

Le protocole **IEC 61850**, standard des communications au sein des sous-stations électriques, transporte des messages GOOSE (Generic Object Oriented Substation Events) critiques pour la protection des équipements haute tension. Ces messages, diffusés en multicast sur le réseau Ethernet de la sous-station, ne disposent d'aucun mécanisme d'authentification natif dans leur version originale. Un attaquant ayant accès au réseau de la sous-station peut injecter des messages GOOSE falsifiés pour déclencher ou inhiber des protections, avec des conséquences potentiellement destructrices sur les équipements électriques.

L'extension **IEC 62351** ajoute des mécanismes de sécurité aux protocoles de communication électriques. Pour IEC 61850 GOOSE, l'IEC 62351-6 propose l'authentification par signature HMAC des messages. Pour IEC 104, l'IEC 62351-3 spécifie l'utilisation de TLS pour le chiffrement et l'authentification mutuelle. Le déploiement de ces extensions reste toutefois limité par la compatibilité des IED existants et la complexité de gestion des certificats dans des sous-stations

distantes. Les mesures compensatoires incluent la segmentation réseau stricte au sein des sous-stations, la surveillance du trafic GOOSE par des sondes spécialisées comme Nozomi Networks, et le contrôle d'accès physique renforcé aux armoires réseau des sous-stations.

Protocole énergie	Usage	Sécurité native	Extension sécurité	Déploiement
IEC 61850 GOOSE	Protection sous-station	Aucune	IEC 62351-6 (HMAC)	Émergent
IEC 61850 MMS	Supervision sous-station	Aucune	IEC 62351-4 (TLS)	Limité
IEC 60870-5-104	Téléconduite	Aucune	IEC 62351-3 (TLS)	En progression
DNP3	Téléconduite (US)	SA v5 (opt.)	SA v5 (HMAC)	Marginal
ICCP/TASE.2	Inter-centre conduite	Aucune	IEC 62351-4	Variable

Pourquoi les smart grids élargissent la surface d'attaque ?

Les **smart grids** (réseaux électriques intelligents) intègrent des technologies de communication bidirectionnelle à tous les niveaux du réseau électrique, des centrales de production aux compteurs des consommateurs. Les compteurs communicants (Linky en France, avec 35 millions d'unités déployées), les concentrateurs de données, les systèmes de gestion de la demande et les interfaces avec les énergies renouvelables distribuées créent des millions de points d'entrée potentiels dans le système électrique.

Le protocole *DLMS/COSEM*, standard de communication des compteurs intelligents, supporte le chiffrement et l'authentification mais les implémentations varient en robustesse. La compromission massive de compteurs intelligents pourrait permettre des attaques de type « demand-side attack » : la manipulation simultanée de la charge de millions de compteurs (activation/désactivation coordonnée de relais de charge) pourrait déstabiliser le réseau électrique sans toucher aux systèmes SCADA de production et de transport. Cette menace, théorisée dans des publications académiques et prise au sérieux par les opérateurs, nécessite des contrôles de sécurité à l'échelle du parc de compteurs, intégrés dans la stratégie globale de SOC et supervision du réseau.

Mon avis : La course au smart grid a souvent priorisé la fonctionnalité et le déploiement rapide sur la sécurité. Les programmes de compteurs intelligents, déployés en millions d'unités avec des cycles de vie de 20 ans, créent une dette de sécurité massive qui devra être gérée pendant des décennies. Les prochains déploiements doivent impérativement intégrer la sécurité dès la conception, avec des mécanismes de mise à jour sécurisée à distance et une authentification robuste de chaque compteur.

Comment protéger les systèmes de distribution d'eau et de gaz ?

Les systèmes de distribution d'eau et de gaz partagent de nombreuses caractéristiques avec les réseaux électriques : architecture géographiquement distribuée, sites distants peu surveillés, protocoles de téléconduite similaires (Modbus, DNP3, IEC 104). Les stations de pompage, les

stations de traitement des eaux, les postes de détente gaz et les stockages constituent des cibles dont la compromission menace directement la santé publique et la sécurité des personnes.

L'incident de la **station de traitement d'eau d'Oldsmar** (Floride, 2021), où un attaquant a tenté de multiplier par 100 la concentration de soude caustique via un accès TeamViewer non sécurisé, illustre la vulnérabilité de ces infrastructures. La multiplicité des accès distants non maîtrisés (TeamViewer, AnyDesk, VNC) pour la maintenance des systèmes SCADA par des sous-traitants constitue le vecteur d'attaque le plus fréquent dans le secteur de l'eau. La sécurisation passe par la centralisation des accès distants via des solutions de gestion d'accès privilégiés et l'élimination de tout outil d'accès distant non autorisé sur les systèmes OT.

Vos sous-traitants de maintenance utilisent-ils des accès distants sécurisés et supervisés ou des outils grand public comme TeamViewer pour se connecter à vos systèmes SCADA ?

Quelles exigences réglementaires pour la sécurité des systèmes énergie ?

Le secteur de l'énergie fait l'objet d'exigences réglementaires renforcées. En Europe, la directive **NIS 2** classe les opérateurs d'énergie comme entités essentielles soumises aux obligations les plus strictes en matière de cybersécurité, incluant la notification des incidents dans les 24 heures et la mise en œuvre de mesures techniques proportionnées aux risques. En France, les arrêtés sectoriels ANSSI pour les OIV du secteur énergie imposent des mesures spécifiques : segmentation des réseaux, détection des incidents, cartographie des systèmes d'information d'importance vitale (SIIV).

En Amérique du Nord, les standards *NERC CIP* (North American Electric Reliability Corporation Critical Infrastructure Protection) définissent des exigences de cybersécurité obligatoires pour les opérateurs du réseau électrique interconnecté. NERC CIP couvre la gestion des actifs cyber (CIP-002), les périmètres de sécurité électronique (CIP-005), la gestion des changements de configuration (CIP-010) et la protection des communications (CIP-012). La conformité à ces standards fait l'objet d'audits réguliers avec des sanctions financières significatives en cas de non-conformité. L'alignement avec la directive NIS 2 structure cette mise en conformité pour les opérateurs européens.

Comment renforcer la résilience opérationnelle du secteur énergie ?

La résilience opérationnelle face aux cyberattaques repose sur la capacité à maintenir la fourniture du service essentiel même en cas de compromission partielle des systèmes de contrôle. Les opérateurs électriques doivent maintenir une capacité de **conduite manuelle** locale sur chaque sous-station, permettant aux opérateurs de terrain de contrôler les disjoncteurs et les transformateurs sans dépendre du système SCADA central potentiellement compromis. Cette capacité, héritée de l'époque pré-numérique, est essentielle et doit être régulièrement testée lors d'exercices dédiés impliquant les équipes de conduite de terrain.

Le *plan de continuité d'activité* spécifique aux cyberattaques OT du secteur énergie intègre des scénarios de dégradation progressive : perte de la supervision SCADA avec maintien de la conduite locale, perte de la téléconduite avec basculement en îlotage des zones de distribution, compromission des protections nécessitant un délestage de sécurité. Chaque scénario est documenté avec les procédures associées, les critères de déclenchement et les responsabilités. Les exercices sectoriels coordonnés par les autorités nationales (exercice Cyber Europe de l'ENISA, exercices NERC GridEx aux États-Unis) testent la résilience collective du secteur face à des cyberattaques simultanées contre plusieurs opérateurs, conformément aux principes de disaster recovery et continuité d'activité adaptés aux infrastructures critiques du secteur énergétique.

Sources et références : CISA ICS · ANSSI

Faut-il centraliser ou distribuer la sécurité OT des réseaux énergie ?

L'architecture de sécurité des grands opérateurs énergétiques fait face à un **dilemme structurel** entre centralisation et distribution. La centralisation au sein d'un SOC unique pour l'ensemble des sites offre une vision globale, des corrélations inter-sites et une mutualisation des compétences rares en cybersécurité OT. La distribution, avec des capacités de détection et de réponse autonomes sur chaque site, garantit une résilience face aux pertes de connectivité et une connaissance fine du contexte local.

Le modèle optimal combine un **SOC central OT** pour la corrélation, la threat intelligence et la coordination, avec des sondes de détection locales sur chaque site et des procédures de réponse autonomes activables en cas de perte de communication avec le SOC central. Cette architecture hiérarchique, directement inspirée du modèle de conduite des réseaux électriques (dispatching national, régional, local), s'appuie sur les technologies de détection de Claroty et de surveillance réseau OT capables de fonctionner en mode autonome tout en remontant les alertes vers une plateforme centrale lorsque la connectivité est disponible. L'intégration dans le SOC convergent IT/OT permet une supervision unifiée de l'ensemble du périmètre technologique de l'opérateur énergétique.

À retenir : La sécurité des systèmes de contrôle du secteur énergie et utilities nécessite une approche sectorielle intégrant la connaissance des protocoles spécifiques (IEC 61850, IEC 104, DLMS/COSEM), la gestion d'une architecture massivement distribuée, et la conformité aux réglementations sectorielles (NIS 2, NERC CIP). Les attaques documentées contre les réseaux électriques ukrainiens démontrent la réalité de la menace et l'urgence de renforcer les défenses.

Les opérateurs énergétiques doivent également sécuriser les interconnexions avec les producteurs d'énergie renouvelable distribués. Les parcs éoliens, les installations photovoltaïques et les systèmes de stockage par batteries connectés au réseau de distribution via des passerelles de communication représentent autant de points d'entrée potentiels dans l'infrastructure du gestionnaire de réseau. Les exigences de cybersécurité pour le raccordement de nouvelles installations de production distribuée doivent être formalisées dans les codes de

réseau et vérifiées lors de la mise en service, garantissant que chaque nouvelle source de production respecte les standards minimaux de sécurité définis par l'opérateur de réseau pour la protection de l'ensemble de l'infrastructure électrique interconnectée.

Ayi NEDJIMI Consultants — Expert cybersécurité offensive & intelligence artificielle

ayinedjimi-consultants.fr · ayi@ayinedjimi-consultants.fr

© 2026 — Reproduction interdite sans autorisation.