Cybersécurité des infrastructures de distribution d'électricité

www.kaspersky.fr/enterprise-security/industrial

#truecybersecurity

Cybersécurité des infrastructures de distribution d'électricité

Un système électrique moderne est une installation technique complexe, unique en termes d'échelle et d'importance pour la vie des gens. Compte tenu des caractéristiques physiques de l'énergie électrique et de la rapidité qui caractérise les processus électriques, le contrôle du fonctionnement des centrales est une tâche complexe d'un point de vue à la fois organisationnel et technique. C'est pourquoi les appareils conçus pour l'automatisation et la protection d'urgence des équipements électriques ont fait leur apparition en même temps que l'émergence du secteur de l'énergie. Les exigences liées à ces appareils, leur conception et leurs fonctionnalités ont évolué en même temps que les systèmes électriques qu'ils protègent, en réponse à une demande croissante des consommateurs.

Aujourd'hui, le système de protection, d'automatisation et de contrôle (SPAC) est un ensemble complexe de systèmes d'information interconnectés recouvrant tous les aspects du fonctionnement des centrages électriques. Le développement rapide des technologies informatiques et de communication a entraîné la modification des systèmes de protection et d'automatisation des composants électriques. En outre, les nouvelles fonctionnalités de contrôle intégrées aux systèmes modernes de protection et d'automatisation ont pour effet de modifier les principes de construction des réseaux d'alimentation électrique.

Améliorer la qualité du contrôle sera l'une des tâches principales du développement électrique à l'avenir, tout comme la transition vers les systèmes de réseaux intelligents. Par conséquent, les systèmes de contrôle jouent un rôle essentiel dans la production, le transport et la distribution d'électricité.

Aujourd'hui, les SPAC sont fortement intégrés et utilisent des technologies de communication basées sur des normes internationales ouvertes telles qu'IEC 60870, IEC 61850 et IEC 61970. L'intégration de sous-systèmes distincts a renforcé les capacités des systèmes de protection et de contrôle, ce qui les a rendus plus intelligents et efficaces à utiliser. En outre, les normes communes ont considérablement réduit le coût de l'intégration et fourni un niveau plus élevé de fiabilité fonctionnelle.

Un système moderne de contrôle et de protection des centrales électriques comprend différents types de sous-systèmes d'information tels que :

- les appliances matérielles et logicielles pour le contrôle automatique de la répartition ;
- le contrôle automatique de la maintenance des modes d'exploitation des systèmes électriques ;
- les systèmes de protection ;
- les systèmes de protection d'urgence automatiques ;
- les systèmes de contrôle des processus ;
- les systèmes de compteurs électriques automatiques ;
- les systèmes de contrôle qualité de l'électricité.

Vulnérabilité des SPAC des centrales électriques lorsqu'ils sont confrontés à des menaces de sécurité informatique

Le niveau élevé d'ouverture et d'intégration des systèmes électriques, ainsi que l'omniprésence de l'informatique et des technologies Internet dans la vie de tous les jours a fait émerger de nouveaux défis pour le secteur électrique. Les systèmes de contrôle et de protection modernes et automatisés des centrales électriques sont des systèmes informatiques distribués intégrés, qui communiquent par le biais de protocoles ouverts. Dans ces systèmes, la cybersécurité n'est pas prioritaire car ils ont été construits comme des solutions isolées. Cependant, pour les systèmes de contrôle modernes qui sont intégrés globalement et connectés avec les services d'entreprise, les risques de cybersécurité sont très élevés.

La norme IEC 62351 « Power systems management and associated information exchange – Data and communications security » (Gestion des systèmes électriques et échanges d'informations connexes - Sécurité des données et des communications) souligne les questions suivantes concernant la sécurité des informations dans les centrales électriques et les causes des failles :

Des communications ouvertes

Lignes de communication ouvertes et non protégées entre les différents composants des systèmes de protection et de contrôle ainsi qu'entre les différentes infrastructures électriques :

- **Absence de vérification d'identité.**
  Absence d'authentification ou faible niveau d'authentification des agents interagissant sur ces systèmes : par exemple, un appareil de réseau aléatoire sur le réseau technologique peut envoyer des commandes de contrôle incorrectes ou malveillantes à un système de haut niveau qui, en retour, peut provoquer l'exécution d'actions invalides par un opérateur de répartition.
- **Normes ouvertes et transmission des données ouvertes.**
  Les protocoles de transmission des données utilisés sont basés sur des normes publiquement disponibles, ouvertes et bien documentées. La mise en œuvre des protocoles et de leur code source, ainsi que les outils d'analyse et d'émulation, sont gratuits et publiquement disponibles. Les données transmises sur ces réseaux sont généralement ouvertes à la capture, la lecture, la modification et la relecture, ce qui simplifie l'accès et l'exécution des menaces par des intrus potentiels.
- **Haut niveau des communications du réseau.**
  Les niveaux élevés de communication entre les protocoles IEC 60807-5-10x et IEC 61850 MMS sont un aspect normal de leur fonctionnement. Mais ces communications ouvertes peuvent également faciliter de simples attaques par déni de service sur les appareils d'infrastructures technologiques (par exemple le système de contrôle des processus du centre de répartition ou les terminaux de protection) par le biais de l'envoi massif de paquets de données invalides.
- **Connexions aux réseaux publics.**
  Les réseaux technologiques et d'entreprise d'une centrale industrielle moderne peuvent comporter des interconnexions multiples à presque tous les niveaux de la hiérarchie du système de contrôle, ce qui augmente le risque d'accès externe non autorisé aux équipements technologiques.

Manque de sensibilisation à la cybersécurité parmi les employés

Un nombre limité de personnels techniques assure la maintenance de nombreux appareils qui sont souvent répartis sur un territoire et fonctionnent sans suivi permanent. Le personnel sur site manque souvent de connaissances, même basiques, en matière de cybersécurité :

- **Accès à distance privilégié à partir d'un réseau non fiable.**
  Pour des raisons pratiques ou pour assurer une maintenance simplifiée, les personnels techniques activent souvent le mode plein accès aux équipements de la centrale distants. Cet accès est souvent organisé de manière non officielle et non sécurisée, par exemple à partir de stations de travail d'entreprise ayant accès à Internet.
- **Absence de protection par mot de passe et de politiques de contrôle utilisateur.**
  Le fait qu'un nombre limité de personnels assure la maintenance de nombreux appareils complique l'élaboration et le maintien de politiques d'accès aux appareils, notamment les politiques de contrôle des utilisateurs et de protection par mot de passe. Ainsi, les appareils technologiques sont souvent exploités avec des mots de passe par défaut, ce qui simplifie l'accès non autorisé.
- **Logiciels obsolètes.**
  Les logiciels IED ne sont quasiment jamais mis à jour au cours de leur cycle de vie sur un dispositif technologique. Les bogues logiciels connus ne sont pas éliminés sauf s'ils affectent directement les processus technologiques.
- **Maintenance réalisée à partir de stations de travail non fiables.**
  Les stations de travail portables (ordinateurs portables) utilisées pour la maintenance des infrastructures technologiques sont souvent utilisées également comme des stations de travail d'entreprise traditionnelles, des équipements de tests logiciels, voire à des fins personnelles.
- **Absence de configuration et de contrôle réguliers des logiciels.**
  Les vérifications logicielles et la configuration des appareils sont réalisées de manière manuelle et irrégulière, souvent moins d'une fois par an.

Les exigences de sécurité ne sont pas respectées

Les exigences en matière de sécurité des informations sont rarement prises en compte dans la conception des appareils ou des logiciels et dans les processus de développement des infrastructures technologiques.

- **Faible résistance au piratage.**
  Habituellement, les développeurs ne tiennent pas compte de la vulnérabilité de leur code à des attaques ciblées ou à des actions illégitimes sur l'infrastructure technologique et ses composants. Par conséquent, la résistance des appareils au piratage est généralement faible.

- **Paramètres de sécurité du réseau invalides ou insuffisants.**
  Les paramètres invalides de segmentation du réseau et de contrôle de l'accès entre les segments du réseau au sein du réseau technologique, ainsi que l'absence de solutions de conception du réseau spécifiques dans les projets de mise en œuvre des SPAC, représentent un problème typique. Par conséquent, la qualité de la configuration des infrastructures du réseau dépend généralement des compétences et qualifications de l'équipe d'installation.
- **Absence de protection des données lorsqu'elles sont transmises sur des canaux ouverts.**
  Il existe un manque ou une absence de moyens sécurisés de transfert des données sur les lignes de communication ouvertes.
- **Absence de contrôle de l'accès basé sur les rôles.**
  L'absence de contrôle de l'accès basé sur les rôles peut entraîner des autorisations d'accès illégitimes, où les utilisateurs accèdent aux appareils sans que cela soit justifié par leurs missions officielles.
- **Absence de solutions de contrôle du démarrage des applications.**
  L'absence de solutions compatibles permettant de protéger les systèmes informatiques d'un démarrage non autorisé des applications a souvent pour effet de laisser les systèmes sans protection contre le lancement de logiciels non autorisés dans des environnements industriels. Les outils standards de contrôle du démarrage des applications sont souvent incompatibles ou inefficaces concernant les systèmes industriels (incompatibilité avec les logiciels technologiques, ressources insuffisantes sur des systèmes technologiques spécifiques, etc.).
- **Absence ou lacunes de l'outil d'enregistrement des événements de sécurité.**
  Il n'existe pas d'outils d'enregistrement des événements de cybersécurité et de suivi spécifiques, ou leurs fonctionnalités sont insuffisantes pour permettre d'interpréter correctement une situation.

Complexité du contrôle de l'accès par les sous-traitants

Le recours à des sous-traitants pour certains types de travaux de maintenance est courant. Par conséquent, il est fondamental de leur fournir uniquement un accès provisoire à une gamme limitée d'équipements qui n'ont pas d'influence sur les autres composants du système. Il est essentiel d'annuler l'accès une fois les travaux terminés.

Longue durée de vie des composants vulnérables

La durée de vie des appareils et des systèmes de protection et de contrôle est de 20 à 30 ans ; les systèmes non sécurisés installés aujourd'hui ne seront remplacés que dans deux décennies environ. Généralement, la mise à niveau partielle est extrêmement difficile étant donné que les solutions sécurisées (par exemple celles qui utilisent le chiffrement) sont souvent incompatibles avec les solutions standards vulnérables.

En plus des problèmes techniques visés ci-dessus, il existe également d'importants problèmes organisationnels. Tout d'abord, l'absence de lignes directrices définissant les mesures à mettre en œuvre lorsque des activités suspectes sont détectées au sein des systèmes automatisés. Deuxièmement, le manque de documents et de pratiques dans le cadre des enquêtes menées sur les perturbations des environnements technologiques, notamment les influences malveillantes sur les systèmes de contrôle à travers les technologies informatiques. Par exemple, du fait de leur ancienneté, certains documents de référence relatifs aux enquêtes et à la classification des perturbations technologiques ne considèrent même pas les incidents de cybersécurité comme une cause potentielle de dysfonctionnement. Si un tel incident a lieu, ses causes réelles ne seront pas révélées. De fait, les mesures qui s'imposent ne seront pas mises en œuvre et l'incident pourra se produire à nouveau.

Les exemples ci-dessus prouvent qu'il existe plusieurs problèmes systémiques :

- Les systèmes électriques modernes de protection et de contrôle des équipements électriques ne sont pas des systèmes isolés et fermés.
- Les systèmes de protection, d'automatisation et de contrôle ne comportent pas de fonctionnalités de cybersécurité intégrées suffisantes.
- D'un point de vue organisationnel et technique, la détection des influences négatives est extrêmement difficile dans la situation actuelle.
- Il n'existe pas d'orientations claires sur les interventions à mettre en œuvre lorsque des attaques sont détectées.

Solutions techniques pour la prévention, la détection et l'atténuation des menaces de cybersécurité

La norme IEC 62351 « Power systems management and associated information exchange - Data and communications security » (Gestion des systèmes électriques et échanges d'informations connexes - Sécurité des données et des communications) décrit en détail les outils disponibles pour assurer la sécurité des informations complexes dans les centrales électriques. Cependant, la plupart des solutions proposées peuvent uniquement être mises en œuvre moyennant le remplacement complet des appareils d'automatisation car elles nécessitent des modifications du format et de la procédure du protocole de communication.

Même si, dans ces circonstances, la mise en œuvre complète de la norme IEC 62351 semble représenter une perspective lointaine, une partie des exigences qu'elle énonce peut être satisfaite et appliquée aux systèmes modernes.

Kaspersky Industrial CyberSecurity (KICS) est une solution globale pour les infrastructures industrielles qui répond à ces critères.

Cette solution comporte deux composantes :

- KICS for Nodes – une composante de protection des terminaux du réseau industriel (comme les stations d'ingénierie, les stations des opérateurs, les serveurs SCADA).
- KICS for Networks – une composante de suivi du réseau industriel avec une vérification de l'intégrité du réseau et des capacités approfondies d'inspection du protocole d'application (IEC 60870-5-104, IEC 61850, etc. pour les infrastructures électriques).

KICS for Nodes

KICS for Nodes est un produit spécialisé destiné aux systèmes industriels. En tant qu'application logicielle sur ordinateur, il est conçu pour protéger les stations de travail des infrastructures technologiques contre les menaces de sécurité informatique (serveurs technologiques, stations de travail d'ingénierie et stations de travail d'opérateurs exécutant le système d'exploitation Windows).

Fonctionnalités principales de la solution :

- Établissement de listes blanches (contrôle du démarrage des applications) – bloque et empêche le démarrage de toutes les applications qui ne sont pas spécifiquement autorisées. Le composant de protection offre un mode de test pour permettre une installation et un débogage simples au stade du déploiement.

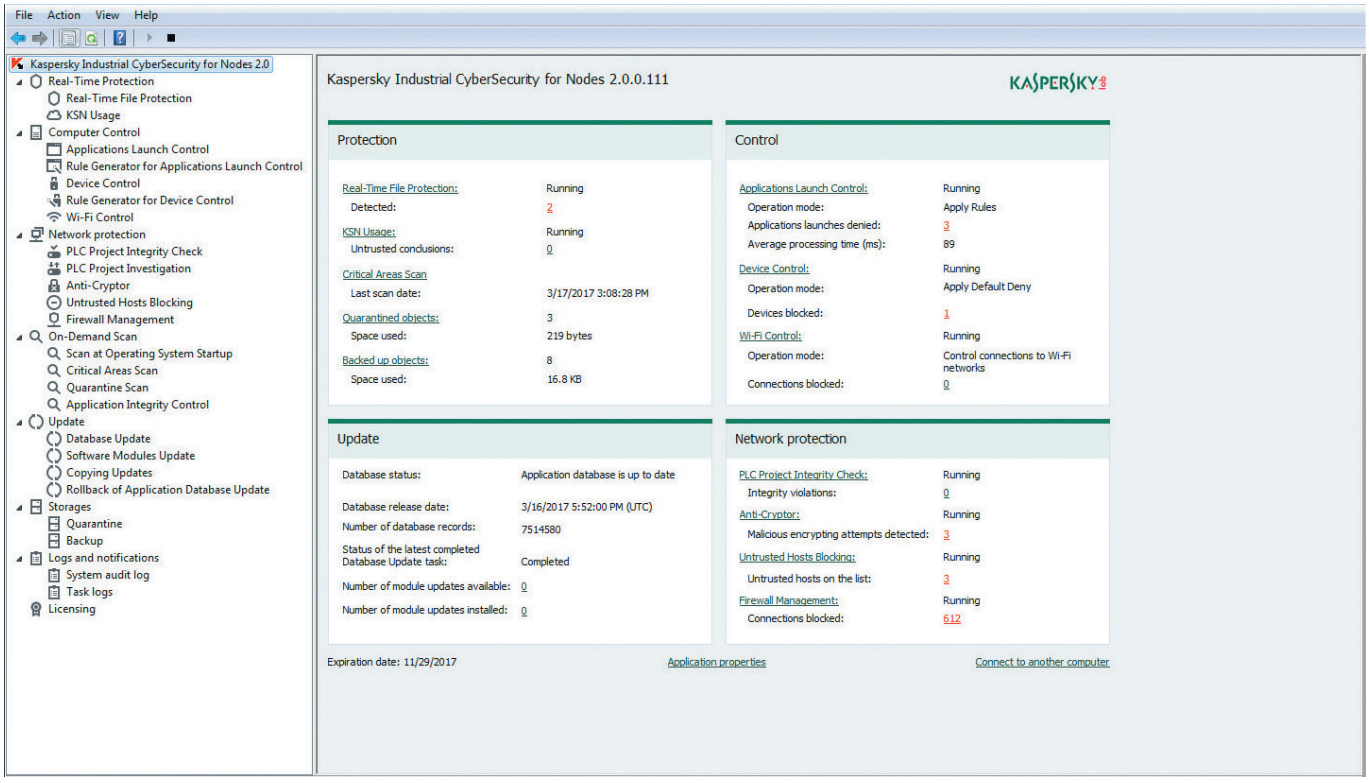

Image n°1. Interface locale KICS for Nodes

- Contrôle des appareils – permet aux administrateurs de définir et d'identifier les appareils pouvant être connectés afin de protéger les hôtes industriels. Cette technologie offre des opportunités de protection des systèmes industriels contre les connexions d'appareils non autorisées. Cette technologie propose des masques pour simplifier l'administration et permettre l'exploitation d'appareils en masse.
- Détection de logiciels malveillants (notamment les virus) – conjugue des méthodes de protection à base de signatures et des solutions heuristiques pour protéger les stations de travail Windows contre les menaces connues, inconnues et complexes.
- Pare-feu de réseau – fournit des fonctionnalités permettant de limiter les connexions réseau aux hôtes industriels. Prévention des intrusions – fournit des fonctionnalités permettant de suivre et de bloquer les activités de réseau suspectes sur les hôtes industriels.

KICS for Nodes peut être géré de manière centralisée après son intégration dans un système de contrôle des infrastructures de sécurité basé sur le Kaspersky Security Center, ce qui permet de bénéficier des fonctionnalités suivantes :

- Gestion centralisée et contrôle de la politique de sécurité – cette fonctionnalité permet de configurer des paramètres de sécurité à la fois pour des appareils individuels et pour des groupes.
- Mise à jour centralisée des bases de données d'antivirus sur les nœuds de réseau protégés (même si le réseau technologique n'est pas connecté à Internet) – ceci aide à assurer un haut niveau de sécurité du fait de la mise à jour des agents de sécurité à partir d'un serveur de contrôle simple au sein du réseau technologique. Les mises à jour peuvent être téléchargées directement sur Internet vers le serveur de contrôle à partir d'un nœud de retransmission (installé sur le réseau informatique ou DMZ), ou transférées au serveur de contrôle par un administrateur par le biais d'une clé USB.
- Test des nouvelles mises à jour avant la distribution – permet de vérifier la compatibilité des mises à jour avec les logiciels industriels avant leur distribution sur des hôtes industriels.
- Modèle basé sur des rôles pour la gestion distincte des politiques et des actions avec l'agent de sécurité – empêche les changements de politiques de sécurité sur le serveur de contrôle et les changements de paramètres des solutions de terminaux, ou la désactivation de la protection.
- La collecte centralisée des événements de sécurité des terminaux permet l'analyse exhaustive des données de sécurité des informations sur la base des événements enregistrés, tout en identifiant la cause exacte des incidents et en facilitant la planification des mesures d'atténuation.

Il convient de souligner que l'exploitation de KICS for Nodes se base sur des approches qui, par défaut, n'ont pas d'impact sur les processus technologiques.

KICS for Networks

KICS for Networks est une solution logicielle spécialisée de surveillance des réseaux industriels. Cette solution est capable d'identifier les anomalies et d'enregistrer les événements d'information importants à partir du trafic réseau industriel sans entraver les processus technologiques.

Les fonctionnalités principales de la solution sont les suivantes :

1. Surveillance de l'intégrité du réseau :
- Mode d'autoformation qui permet la détection et l'enregistrement de tous les nœuds LAN disponibles et des communications entre eux – ces données peuvent être utilisées comme point de référence et pour le suivi des modifications.
- Détection et enregistrement basé sur les adresses IP et MAC de nouveaux appareils réseau connectés aux segments contrôlés du réseau technologique.
- Détection et enregistrement de nouvelles communications réseau entre les nœuds, basés sur les attributs suivants : adresse du nœud de l'expéditeur, adresse du nœud du destinataire, protocole du réseau, port, nombre de connexions autorisées, etc.

2. Deep packet inspection (inspection approfondie des paquets d'information) :
- Examen, analyse et enregistrement des messages importants des protocoles technologiques en fonction de la configuration :
  - Détection des commandes de gestion des appareils (par exemple, basculement Marche/Arrêt) par le biais des protocoles du réseau industriel (IEC 61850, IEC 60870-5-104).
  - Détection des commandes permettant de modifier les paramètres de fonctionnement du système de contrôle et de protection (par exemple, commutation groupée à un point fixé) par le biais des protocoles du réseau industriel (IEC 61850, IEC 60870-5-104).
  - Détection des tentatives de paramétrisation et contrôle IED avec des logiciels de service par le biais de segments de réseau contrôlés.
- Surveillance générale des messages de télémesure.

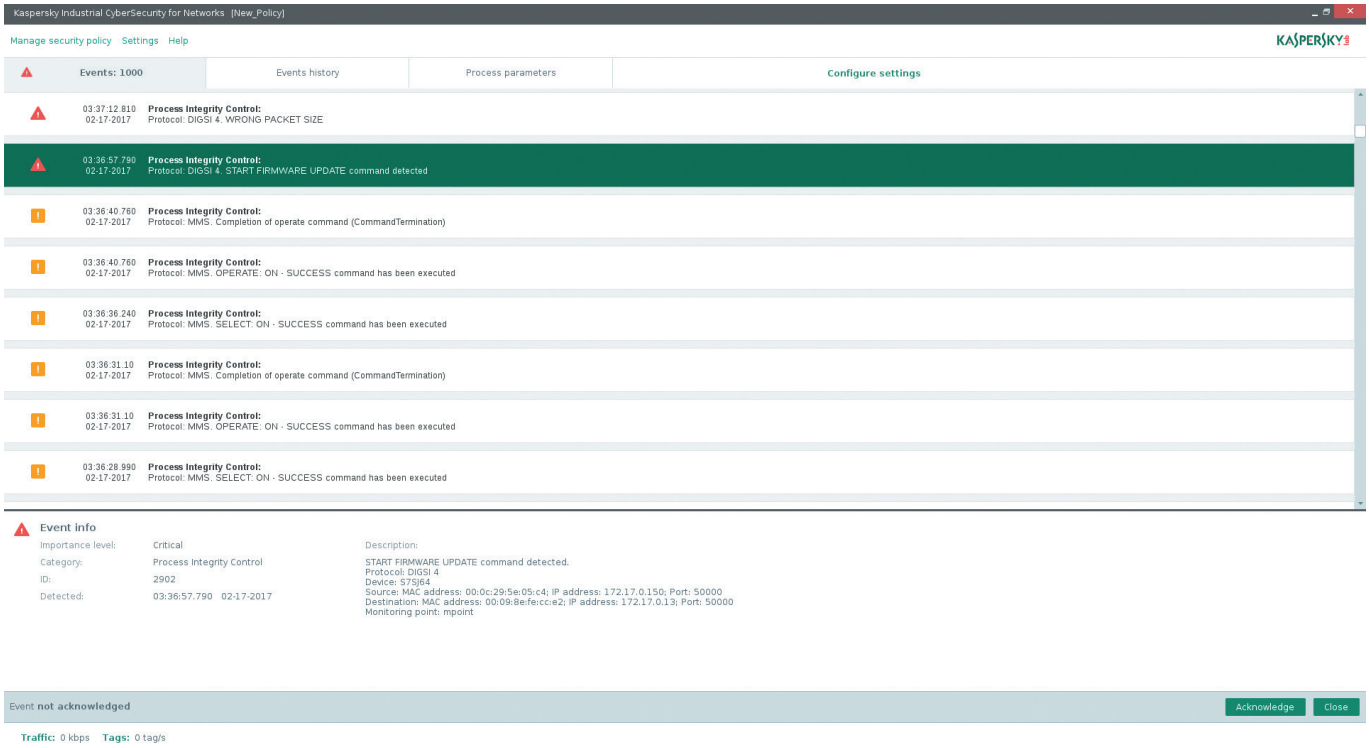

Image n°2. Interface locale KICS for Networks

3. Stockage des événements :

- Le système KICS for Networks permet de stocker les événements détectés dans une base de données interne sécurisée.
- Les informations sont limitées par période de stockage et taille de fichier archivé. L'exemple figurant à l'image n°3 (ci-dessous) illustre un scénario potentiel de déploiement de KICS for Networks et de KICS for Nodes.

KICS for Nodes et KICS for Networks : exemple de déploiement dans une sous-station électrique moderne

Un système de contrôle et de protection comprend deux segments LAN de topologie en anneau. Le premier segment de la sous-station électrique est le bus de poste (en vertu de la norme IEC 61850), qui permet les communications entre les IED. En outre, le bus de poste, les contrôleurs de sous-station et les passerelles de télémesure sont utilisés pour l'interaction informationnelle avec des niveaux plus élevés de contrôle des répartitions. Le segment LAN fournit un accès aux équipements du système de contrôle et de protection au moyen de logiciels d'ingénierie. L'accès au service peut être fourni à la fois localement et à distance. L'accès au service local est fourni à l'aide d'un ordinateur portable connecté directement aux IED ou au LAN du bus de poste. L'accès au service peut également être assuré à partir d'une station de travail à distance. Les communications rapides entre les nœuds du réseau au cours d'un fonctionnement stable sont conformes au protocole IEC 61850 MMS. Les communications de service concernant le paramétrage des appareils du système de contrôle et de protection sont fournies en vertu des protocoles d'application internes du fabricant d'équipements.

Le segment de LAN physique du bus est un réseau en anneau, formé par deux commutateurs connectés. Tous les appareils sont connectés aux commutateurs en tant que « double attached nodes » (DAN, nœuds doublement reliés). Par conséquent, il n'existe pas, sur le segment, de point de défaillance unique qui fournisse un niveau plus élevé de fiabilité du réseau. Les IED sont équipés de commutateurs intégrés et combinés en chaînes. Les extrémités des chaînes sont connectées aux commutateurs de réseau en anneau ; par conséquent, le trafic entre les appareils d'une chaîne n'est pas transmis par le biais des commutateurs réseau en anneau. Le contrôle réseau par topologie en anneau est exécuté à l'aide du RSTP. Le commutateur réseau est inclus pour fournir un accès de service à distance au réseau industriel par le biais d'un VPN.

Le second segment (segment de réseau opérateur) est également représenté par une topologie de réseau en anneau conçue pour les stations de travail des opérateurs et pour l'interaction entre les serveurs des systèmes de contrôle des processus.

Les interactions avec le Centre de contrôle du réseau et l'Opérateur système sont fournies directement par un contrôleur de sous-station connecté au système d'automatisation (voir l'image n°3). L'échange s'opère à travers le protocole IEC 60870-5-104.

L'installation de KICS for Networks est nécessaire dans chacun des segments de réseau sélectionnés, afin de fournir une surveillance complète des infrastructures de réseau technologique. Par conséquent, trois serveurs KICS for Networks doivent être installés pour le diagramme visé : un pour le segment bus de poste, un pour le segment de réseau d'opérateur et un pour la ligne de communication vers les niveaux de contrôle plus élevés. Pour connecter les serveurs KICS for Networks à l'infrastructure, il est nécessaire de reconfigurer les équipements de commutation afin de transférer tout le trafic SPAN de chaque segment de réseau vers le serveur correspondant.

Le serveur KICS for Networks est connecté aux ports SPAN des commutateurs du réseau. Cette configuration permet de recevoir uniquement le trafic industriel, sans impact sur les processus technologiques. KICS for Networks traite le trafic industriel et détecte les événements suspects. Les données liées aux événements enregistrés sont chiffrées et stockées de manière sécurisée. En outre, les événements sont transmis par voie chiffrée vers le Kaspersky Security Center, ce qui permet de fournir aux spécialistes de la sécurité une liste définitive d'événements détectés.

Le logiciel KICS for Nodes doit être installé sur chaque hôte industriel afin de protéger les infrastructures informatiques exécutant le système d'exploitation Windows. KICS for Nodes transmet également les événements détectés au serveur Kaspersky Security Center. Les hôtes industriels doivent contenir une interface réseau supplémentaire pour se connecter au segment de réseau de contrôle.

Toutes les communications du réseau de contrôle sont chiffrées. En cas de panne du réseau de contrôle, les composants KICS for Networks et KICS for Nodes continueront de fonctionner en mode autonome. Les données recueillies seront transmises au Kaspersky Security Center lors de la restauration du fonctionnement du segment de réseau.

KICS permet l'intégration avec les systèmes SIEM. Kaspersky Security Center organise un canal chiffré dans le système SIEM et transfère les événements configurés dans le SIEM (HP ArcSite, IBM QRadar et autres à travers le format Syslog). Des notifications peuvent également être envoyées par e-mail et SMS.

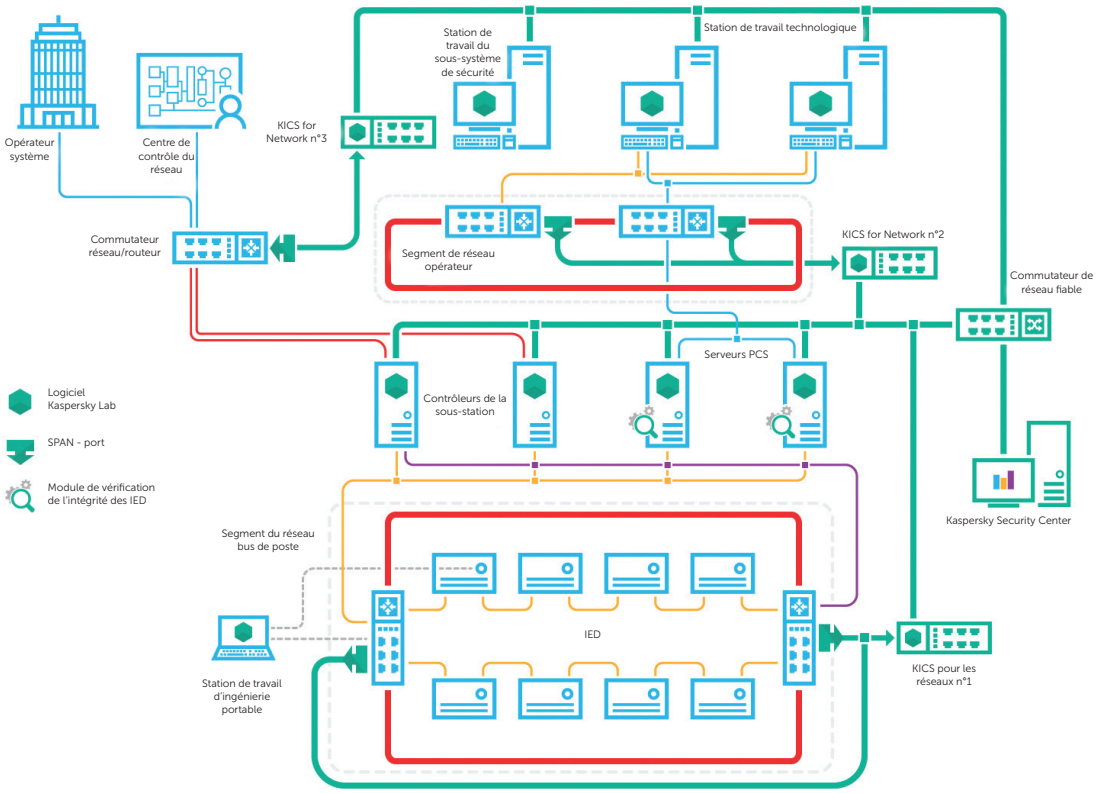

Image n°3 : Kaspersky Industrial CyberSecurity : déploiement des composants

Termes et définitions

AI – appareil informatique. Dispositif technique capable de traiter les données conformément à une logique de programme prédéfinie.

Cybersécurité industrielle – état de protection qui assure la disponibilité, l'intégrité et la confidentialité du processus technologique au niveau informatique/ des technologies opérationnelles.

IED – Intelligent Electronic Device (équipements électroniques intelligents). Dispositif informatique polyvalent, spécial et basé sur un microprocesseur ayant de larges capacités de communication numérique.

LAN – Local Area Network (réseau local). Réseau informatique couvrant un ensemble fixe d'unités de réseau connectées par le biais de médias gérés localement, regroupées selon le principe de l'emplacement dans un espace limité.

LCS – Langage de configuration de la sous-station*. Format de langage et de représentation spécifié par la norme IEC 61850-6 pour la configuration des appareils de sous-station électrique. Il contient des ressources de représentation d'un modèle d'informations relatif aux appareils, aux séries de données et aux services de communication. Basé sur le langage XML.

Réseau intelligent – Système électrique de nouvelle génération reposant sur un multi-agent qui organise et contrôle son fonctionnement et son développement afin d'utiliser toutes les ressources (naturelles, sociales, de production et humaines) de manière efficace. Ce système fournit une alimentation électrique sûre, de qualité et efficace pour les consommateurs grâce à l'interaction flexible de tous ses éléments (tous types de production, réseaux électriques et consommateurs confondus). Il est basé sur des technologies modernes et un système de contrôle hiérarchique intelligent et unifié.

SCP – Système de contrôle des processus. Système homme-machine basé sur les dispositifs d'automatisation industrielle et de télécommunication fournissant un contrôle des processus automatique et automatisé complet sur le site du dispositif contrôlé et permettant une exécution du contrôle à distance à partir d'un centre de répartition à distance.

SPAC – Système de protection, d'automatisation et de contrôle. Terme collectif désignant un complexe de systèmes de contrôle automatiques et automatisés à différentes fins, installés sur le dispositif.

SPAN – Switched Port Analyzer (analyseur de port commuté). Port de commutateur réseau utilisé pour collecter le trafic réseau mis en miroir à partir de ports sélectionnés du commutateur à des fins d'analyse.

SPCS – Système de Protection de Cybersécurité. Système automatique conçu pour fournir une cybersécurité au dispositif protégé.

Bus de poste – réseau informatique rapide et très fiable qui permet la transmission de données par le biais d'appareils intelligents mettant en œuvre des fonctionnalités de processus (au niveau cellulaire) ainsi que des complexes d'appareils, de matériels et de logiciels offrant des fonctionnalités générales de sous-station (au niveau de la sous-station), par exemple SCADA, passerelle télémécanique, etc. Dans certains cas, un bus de poste peut fournir des communications horizontales entre les appareils au niveau cellulaire. Pour empêcher les interférences électromagnétiques avec les systèmes de communication, les bus de postes sont souvent constitués d'un médium de transfert de données en fibre optique.

Système de protection – complexe d'IED conçu pour détecter et déconnecter rapidement les segments endommagés du système électrique contrôlé afin de garantir un fonctionnement stable du système.

Tout savoir sur la cybersécurité concernant les ICS :
https://ics-cert.kaspersky.com
Actualités des cybermenaces : **www.viruslist.fr**
Mini site Kaspersky Lab dédié à la sécurité industrielle :
https://ics.kaspersky.fr/

#truecybersecurity

www.kaspersky.fr

IIC MEMBER industrial internet CONSORTIUM

OPC FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ FINALIST ★ 2017

* « World Leading Internet Scientific and Technological Achievement Award » (prix du leader mondial en matière de réussite scientifique et technologique sur Internet) à la 3è World Internet Conference
** Prix spécial du China International Industry Fair (CIIF) 2016