Cybersécurité des sous-stations électriques IEC 61850

Stéphane Mocanu, Maëlle Kabir-Querrec, Jean-Marc Thiriet, Eric Savary

Cybersécurité des sous-stations électriques IEC 61850

Stéphane Mocanu[1], Maëlle Kabir-Querrec[1,2], Jean-Marc Thiriet[1], Eric Savary[2]

1) Gipsa-lab/Ense3/Grenoble-INP
2) Euro-System

Stephane.Mocanu@grenoble-inp.fr, Maelle.Kabir-Querrec@grenoble-inp.fr, Jean-Marc Thiriet@grenoble-inp.fr, Eric.Savary@euro-system.fr

Introduction

La notion de cybersécurité couvre divers aspects selon les menaces auxquelles l'on souhaite répondre :

- La confidentialité : empêcher la diffusion d'informations,
- L'intégrité : empêcher les modifications des configurations et contenus par des utilisateurs non autorisés,
- L'authentification : s'assurer que seules les entités (utilisateurs, services…) autorisées usent de leurs privilèges de lecture, d'actions…,
- La disponibilité / la non-répudiation : empêcher qu'une entité autorisée soit confrontée à un DoS (Denial of Service),
- La journalisation : enregistrement des événements pour analyse ultérieure.

Les vulnérabilités d'un système d'automation d'une sous-station électrique sont cependant différentes de celles auxquelles est confronté réseau d'entreprise traditionnel. Premaratne et al. [Premaratne_2008] distinguent deux objectifs principaux d'éventuels attaquants : perturber le service (compromet la disponibilité) et accéder aux informations confidentielles pour usage malveillant (faille dans la confidentialité).Toutefois d'autres types d'attaques peuvent être utilisés pour servir ces deux buts.

On peut souligner trois différences principales entre un réseau dédié à des opérations administratives ou d'ingénierie et un réseau industriel. Tout d'abord contrairement des ordinateurs conventionnels, les IEDs sont généralement des systèmes embarqués disposant de ressources computationnelles limitées. La seconde différence est la criticité temporelle : comme souligné dans l'édition 2011 du Guide Alstom pour la protection et l'automation des réseaux (Alstom Network Protection & Automation Guide), les applications industrielles reposent sur des opérations temps-réel avec des contraintes de temps très strictes. La dernière différence mais non la moindre concerne les protocoles de communication. Par exemple Modbus, DNP3 ou la pile de protocoles CEI-61850 sont des bus de terrain spécifiquement conçus pour des infrastructures et les IDS conventionnels ne gèrent pas ces protocoles.

Ainsi, les différences de technologies et d'usages rendent évidente la nécessité de techniques de détection d'intrusion dédiées aux systèmes d'automation des sous-stations.

Contexte

Forts de ce constat, le consortium formé d'Euro-System, bureau d'études et d'intégration dans l'Automatisme et l'Informatique Industrielle du bassin grenoblois, et du GIPSA-lab, laboratoire d'Automatique et de Traitement du Signal de Grenoble (Grenoble Image Parole Signal Automatique)

a décidé de démarrer une thèse sur le thème de la cybersécurité des systèmes de contrôle des postes électriques. Ces travaux de recherche s'inscrivent dans le cadre du standard international CEI-61850 normalisant les réseaux et systèmes de communication des sous-stations [CEI-61850]. L'un des objectifs de cette norme est de permettre l'interopérabilité, définie dans la partie introductive (CEI-61850 – 1) comme la capacité pour tous les IEDs du SAS "d'opérer sur le même réseau ou vecteur de communication en partageant données et commandes".

L'un des apports majeurs de ce standard est la définition d'un modèle de données orienté objet qui permet une décomposition fonctionnelle des services et une modélisation hiérarchisée de l'information. La figure ci-dessous permet de visualiser ce modèle.

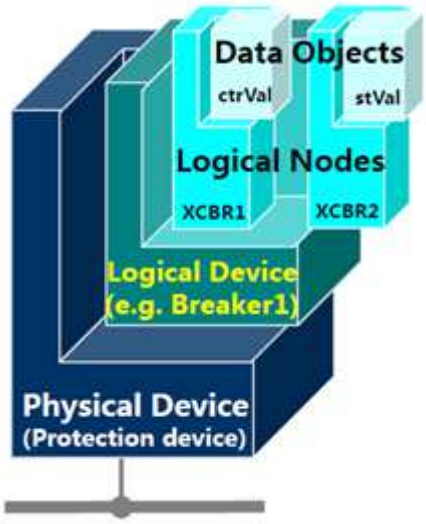

Fig. 1. Modélisation des données orientée objet définie par la norme CEI-61850

Une fonction est assimilée à un appareil virtuel, un Logical Device ou LD. Ce LD est lui-même décomposé en petites entités ou sous-fonctions, appelées nœuds logiques (Logical Nodes ou LN). Les LNs sont caractérisés par les données qu'ils manipulent, les méthodes qu'ils exécutent et les échanges qu'ils ont avec d'autres LNs. Un équipement réel, Physical Device, peut être constitué d'un ou plusieurs LDs.

L'autre contribution importante de cette norme est la spécification d'une pile de communication faisant appel à trois protocoles de communication. Le MMS (Manufacturing Message Specification) pour les échanges entre la supervision et la baie de contrôle, les GOOSE (Generic Object Oriented Substation Event) pour les communications entre IEDs, au sein de la baie donc, et les SMV (Sampled Measured Values) utilisés pour transmettre des grandeurs mesurées sur le procédé aux IEDs. Cette architecture de communication est illustrée dans la figure 2.

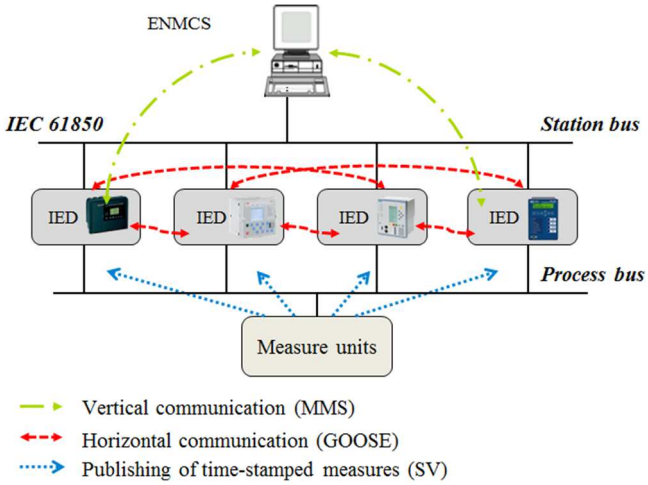

Fig. 2. Architecture de communication définie par la CEI-61850 (M. Nachar, Euro-System)

Les GOOSE et SMV ont des contraintes temps-réel spécifiques et sont donc mappées directement sur la couche liaison Ethernet du modèle OSI alors que MMS est basé sur TCP/IP.

Un IDS conforme à la norme CEI-61850

Un procédé industriel repose en général sur une topologie de réseau fixe des mécanismes connus spécifiques au domaine d'application. En particulier les mécanismes de communication sont bien définis et en général plus contraints que ceux de réseaux conventionnels tels qu'internet. On peut tirer avantage de cette connaissance pour concevoir un système de détection d'intrusion (IDS) ou d'anomalies sur mesure. C'est l'approche adoptée par Cheung et al. [Cheung_2007] : une étude approfondie des spécifications Modbus a permis d'énoncer des règles de comportement du système pour un IDS de règles.

L'IDS réseau pour SAS présenté dans [Hong_2014] identifie les messages multicast malveillants conformes à des signatures d'attaques connues. Ces règles ont été établies à partir des spécifications des protocoles GOOSE et SMV définies dans la norme CEI-61850.

Contrairement à Hong et al. [Hong_2014], nous voulons caractériser le comportement normal des systèmes et réseaux de communication d'une sous-station CEI-61850 et quantifier à quel point le système réel diverge de ce modèle. Cependant le choix fait dans cet article d'un IDS basé réseau semble le plus adapté pour gérer les messages multicast. Il suffira que l'équipement s'abonne à l'ensemble des GOOSE et SVM pour les parser.

Les communications MMS sont un autre problème puisqu'elles utilisent des adresses de destination précises. Elles sont utilisées à l'interface des niveaux de supervision et de baie. C'est pourquoi il a été proposé d'implémenter l'IDS directement dans la passerelle au point d'entrée du réseau de la baie [Premaratne_2010] ou d'utiliser un port miroir. L'autre argument en faveur de cette implémentation est la puissance computationnelle limitée des IEDs. L'expérimentation sur la plateforme dont le GIPSA-lab s'est dotée depuis l'automne 2014 (G-ICS, GreEn-ER Industrial Control systems Sandbox) nous aidera à répondre à cette question.

Quant au design de l'IDS lui-même, nous le voulons conforme au modèle orienté objet décrit précédemment. Cela afin de rendre possible une éventuelle future intégration de ce module de cybersécurité directement dans les IEDs comme une fonction à part entière. Notre fonction de cybersécurité doit donc être conçue en suivant la procédure donnée dans le standard : décrire d'abord la fonction et sa décomposition en LNs, puis décrire l'ensemble des LNs ainsi que les PICOMs échangés (Piece of Information for COMmunication, classe du modèle de données décrivant le transfert d'information entre LNs). La description détaillée des PICOMs achève la spécification de la fonction. Les procédures de spécifications sont données dans la partie 5 du standard.

La spécification de cette fonction de cybersécurité inclut les objets (fonctions, LNs, PICOMs) existants dans la norme et en propose de nouveaux quand nécessaire. Le travail en cours a pour objectif de proposer un modèle complet de LNs et PICOMs décrivant précisément la fonction de détection d'anomalies numériques CEI-61850.

Un autre objectif de ce travail de recherche est d'écrire un modèle du système basé sur la théorie des automates, ce qui pourra s'avérer utile pour l'estimation des performances et pour une future implémentation. De même il serait bon d'identifier les scenarios d'attaques et leurs conséquences, des méthodes inspirées de la sûreté de fonctionnement sont envisagées (Graphes d'attaque, méthodes d'analyse qualitative).

Glossaire

GOOSE	Generic Object Oriented Substation Event
IED	Intelligent Electronic Device
MMS	Manufacturing Message Specification
LD	Logical Device
LN	Logical Node
PICOM	Piece of Information for COMmunication
SAS	Substation Automation System
SMV	Sampled Measured Values

Références

Alstom Network Protection and Automation Guide, 2011

CEI 61850 Communication networks and systems in substations

Cheung S., Dutertre B., Fong M., Lindqvist U., Skinner K., Valdes A. (2007), Using model-based intrusion detection for scada networks, In Proceedings of the SCADA Security Scientific Symposium, Miami Beach, Florida, USA

Hong Junho, Liu Chen-Ching, Govindarasu M. (July 2014), Integrated Anomaly Detection for Cyber Security of the Substations, Smart Grid, IEEE Transactions on , vol.5, no.4, pp.1643,1653

Premaratne, U.; Samarabandu, J.; Sidhu, T.; Beresh, B.; Jian-Cheng Tan (Dec. 2008), Evidence Theory based Decision Fusion for Masquerade Detection in IEC61850 Automated Substations, Information and Automation for Sustainability, ICIAFS 2008, 4th International Conference on , pp.194,199