Future Generation Computer Systems 61 (2016) 128–136

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Challenges and research directions for heterogeneous cyber–physical system based on IEC 61850: Vulnerabilities, security requirements, and security architecture

Hyunguk Yoo, Taeshik Shon *

Department of Computer Engineering, Ajou University, Suwon, Republic of Korea

HIGHLIGHTS

- There are security concerns in the heterogeneous CPS environment based on IEC 61850.
- Two connections (IEC 61850-DNP3, IEC 61850-IEC 61970) are drawn from a case study.
- We classify the security vulnerabilities of the heterogeneous protocol environment.
- We present security requirements and architectures in the heterogeneous CPS environment.

ARTICLE INFO

Article history:
Received 4 March 2015
Received in revised form
7 August 2015
Accepted 16 September 2015
Available online 20 October 2015

Keywords:
IEC 61850
DNP3
IEC 61970
Cyber–physical system
Cybersecurity

ABSTRACT

IEC 61850, an international standard for communication networks, is becoming prevalent in the cyber–physical system (CPS) environment, especially with regard to the electrical grid. Recently, since cyber threats in the CPS environment have increased, security matters for individual protocols used in this environment are being discussed at length. However, there have not been many studies on the types of new security vulnerabilities and the security requirements that are required in a heterogeneous protocol environment based on IEC 61850. In this paper, we examine the electrical grid in Korea, and discuss security vulnerabilities, security requirements, and security architectures in such an environment.

1. Introduction

The IEC 61850 Edition 1 standard, which was published in 2005, was accepted by electric utilities around the world at a remarkably fast rate. This standard was originally developed for communications in substation automation systems. As IEC 61850 evolved, its areas of application were extended to hydropower systems, wind power systems, and distributed power systems. New sections of the standard were added for these extended areas, and the title of the standard was changed from "Communication Networks and Systems in Substations" to "Communication Networks and Systems for Power Utility Automation". Because the IEC 61850 standard has some advantages in terms of interoperability and long-term stability, it has been adopted as one of the core communication standards for the smart grid [1], which is a special example of a cyber–physical infrastructure. There is a growing need to harmonize the IEC 61850 system with other systems because the smart grid is a very complicated cyber–physical infrastructure of heterogeneous entities that interact with each other. For example, in the case of using IEC 61850 within a substation network, the IEC 61850 protocols need to be converted to the DNP3 protocol, which can be used for substation-to-control-center communication and vice versa. In addition, IEC 61850 must work harmoniously with other communication standards used in the control center, including IEC 61970, IEC 61968, and OPC UA. There is some ongoing standardization, including IEC 62361-102 and IEEE 1815.1 for heterogeneous CPSs based on IEC 61850. Recently, as cyber threats in the CPS environment have increased, security matters regarding the use of individual protocols in this environment are being discussed at length. However, there have not been many studies about the types of new security vulnerabilities and security requirements required in an environment where IEC 61850 and heterogeneous protocols are linked.

* Correspondence to: 206 Worldcup-ro, Yeongtong-gu, Department of Computer Engineering, Ajou University, Suwon, 443-749, Republic of Korea.
E-mail address: tsshon@ajou.ac.kr (T. Shon).

http://dx.doi.org/10.1016/j.future.2015.09.026
0167-739X/

Table 1
IEC 61850 standard parts for mapping to other protocols.

Parts	Description
80-1	Guideline for exchanging information from CDC-based data model using IEC 60870-5-101 or IEC 60870-5-104
80-2	Mapping DNP3 to IEC 61850 (future dual logo of IEEE 1815.1)
80-4	Mapping between DLMS/COSEM(IEC 62056) data models and IEC 61850 data models
80-5	Guideline for mapping information between IEC 61850 and IEC 61158-6 (Modbus)

In this paper, we look at security issues in the heterogeneous CPS environment based on IEC 61850 by examining the electrical grid in Korea, and we discuss security vulnerabilities, security requirements, and security architectures in such an environment. In Section 2, we examine the standardization of protocols that are closely related to IEC 61850-based CPSs. In Section 3, we derive some cases where IEC 61850 and heterogeneous protocols are linked from a case study of the electrical grid in Korea. In Section 4, we look at the security vulnerabilities of a heterogeneous protocol environment based on IEC 61850, and we present security requirements and security architectures. In Section 6, we discuss the suitability of the presented security architecture. Finally, we conclude this paper and suggest a direction for future studies.

2. Related communication standards for heterogeneous CPS based on IEC 61850

In this section, we briefly review the standardization requirements of IEC 61850 and other smart grid protocols that are closely related to the IEC 61850-based CPS.

2.1. IEC 61850

IEC TC 57 (Power Systems Management and Associated Information Exchange) published IEC 61850 Edition 1 in 2005. This initial version of IEC 61850 was limited to communication within a substation network. When IEC 61850-7-410, which defined the object model in the hydropower domain, was developed in 2007, the application range of that standard extended to the outside of the substation. Some of the extended parts of the standard cover methods of mapping with other protocols such as IEC 60870-5, DNP3, Modbus, and DLMS/COSEM (Table 1). The legacy communication protocols used in the industrial domain, such as IEC 60870-5, DNP3, and Modbus, were designed to operate over a low-bandwidth environment. Therefore, these protocols are relatively simple and are limited to providing the semantics of the messages. As modern cyber–physical systems become more complicated, the costs for system configuration and maintenance increase because the legacy industrial protocols cannot provide the meaning of each data point. By contrast, IEC 61850 is designed to support object-oriented information modeling and self-description [2]. These fundamental differences between IEC 61850 and other legacy protocols result in some problems in harmonizing the protocols and can cause security vulnerabilities, which are described in Section 4.

The IEC 61850 standard also has a long-term stability feature by splitting between its information model and communication protocols. At the time of writing, there are three communication protocols for conveying the IEC 61850 information model: MMS (over TCP/IP), GOOSE (over Ethernet), and SV (over Ethernet). MMS is used for most operational information that is not time critical, and GOOSE is used for time-critical information such as trip, interlock, and block. SV is used for the information of voltage and current sample.

The security aspects of IEC 61850 are specified in the IEC 62351 standard. For example, IEC 62351 Part 3 specifies how to secure TCP/IP-based protocols such as MMS through transport layer security (TLS) defined in RFC 5246, and Part 6 of the standard is being reworked for GOOSE/SV message integrity based upon the generation of a message authentication code.

2.2. DNP3

DNP3 is a legacy protocol that was developed in 1993 and standardized as IEEE 1815-2010 in 2010. It is still used widely in various CPS domains such as power grids, waterways, and railways in North America and Asia, although the IEC 61850 standard is becoming popular. In the case of an IEC 61850 substation as described in Section 3, DNP3 is a typical protocol for communication between the control center and substation. Therefore, to achieve interoperability, conversion between those two different protocols is inevitable in this environment. The Smart Grid Interoperability Panel singled out a study of the mapping method between DNP3 and IEC 61850 as Priority Action Plan 12, and instructed IEEE Working Group 14 to standardize the mapping method. The development of these standards is ongoing as IEEE P1815.1.

The security method for DNP3 messages is defined as, respectively, Secure Authentication Versions 2 and 5 in IEEE 1815-2010 and IEEE 1815-2012 (Table 2).

One of the most significantly changed parts in IEEE 1815-2012 is the reinforcement of the Secure Authentication that provides application layer functions to verify the source of the message and the message integrity. Secure Authentication Version 5 provides a new method to remotely change update keys by using symmetric or asymmetric cryptography [3]. Another newly added function, security statistics, can be used to record the number of occurrences of events related to DNP3 security in an outstation. These events include unexpected messages, authorization failures, and reply timeouts, which are reported through the objects of g121v1 (security statistic), g122v1 (security statistic change event), and g122v2 (security statistic change event with time).

2.3. IEC 61970

In 1993, the Electric Power Research Institute (EPRI) started the Control Center Application Program Interface (CCAPI) project to enhance the compatibility between various Energy Management System (EMS) applications. As a result of that project, EPRI developed the Common Information Model (CIM) [4], which provides a standardized method for describing common power-system objects with object-oriented relations for these objects. EPRI also developed the Generic Interface Definition (GID) [5], which provides a set of APIs to be used by software applications for accessing and exchanging CIM-based data. This work was published as the IEC 61970 standard in 2005. The IEC 61970 standard, which is used in control centers, has become another core standard of the smart grid, along with the IEC 61850 standard. The harmonization between IEC 61970 and IEC 61850 models is being developed by TC 57 Working Group 19 as the IEC 62361-102 standard because many applications require the integration of systems across these distinct environments. IEC 61970-502-8 is under development for the mapping of the CIM and OPC Unified Architecture (OPC UA), which is one of the core standards of the future smart grid. Meanwhile, XML security methods in IEC 62351-11 are being developed that can be applied to the XML format of the CIM.