

# EXPERIENCE FROM IMPLEMENTATION OF DATA AND COMMUNICATIONS SECURITY STANDARD (IEC 62351)

Wiwat Amornimit

*Information Technology Planning Department*

*Metropolitan Electricity Authority (MEA)*

*Bangkok, Thailand*

wiwat.pcd@mea.or.th

**Abstract**— In Metropolitan Electricity Authority (MEA), the focus has been almost exclusively on implementing MEA's power system infrastructure that can keep MEA's power system reliable. Until recently, MEA's Information Infrastructure that supports the monitoring and control of the power system has come to be critical to the reliability of MEA's power system.

Advances in SCADA systems have increased the interdependencies, enhancing MEA's power system operations but creating additional vulnerabilities. Such vulnerabilities and gaps in security must be addressed to adequately protect MEA's SCADA system. Securing the SCADA infrastructure is of critical importance to MEA, this specialized SCADA security includes protection against known and zero-day attacks, enabling MEA to more effectively meet the new security requirements specified in the emerging Data and Communications Security Standard (IEC 62351). The standard establishes the requirements needed to ensure the security of the electronic exchange of information needed to support the reliable operation of MEA power system.

MEA plays a major role in protecting the electric system by coordinating information exchange on SCADA security issues between the electricity utilities. The IEC 62351 standard currently under development proposes a mechanism for securing the DNP3 and IEC 60870-5-101 protocols now in use in MEA. To protect the SCADA system from physical and cyber attacks, MEA adopts and implements IEC 62351 security standard to secure both SCADA protocols.

This paper presents an overview of MEA's SCADA protocols and their possible cyber attacks. Summary of security requirements, threats, and security countermeasures from IEC 62351 security standard are described. The experiences gained from implementation of this security standard to protect MEA's SCADA system are discussed with practical information concerning the design and implementation of MEA's DMS project.

**Keywords:** SCADA/EMS, SCADA/DMS, SCADA Protocol, Data and Communications Security

## I. INTRODUCTION

In Metropolitan Electricity Authority (MEA), in the past the focus has been almost entirely on implementing power equipment that can keep MEA's power system more reliable. Until recently, communications and information flows have been considered of importance to MEA. Nevertheless, the Information Infrastructure such as SCADA/EMS and SCADA/DMS systems supporting the monitoring and control of MEA's transmission system and distribution system has

increasingly come to be critical to the reliability of MEA's power system.

As MEA's SCADA system relies increasingly on information to control the power system, the management of the power system infrastructure has become reliant on the information infrastructure. Therefore, the reliability of the power system is increasingly affected by any problems that the information infrastructure might suffer.

When MEA has become more and more dependent on the SCADA systems for day-to-day operations, communication protocols of the SCADA system, responsible for retrieving information from Remote Terminal Units (RTUs) and for sending control commands to the RTUs, are one of the most critical parts of MEA's power system control. These SCADA protocols have rarely integrated any security measures because they were very specialized and only operators are allowed to issue control commands from highly protected MEA's control centers. However, they are moving from simply legacy protocols to increasingly complex modern standard protocols. The standardized and well-documented protocols are more susceptible to hackers and actual terrorism to disrupt power system operations.

## II. SCADA STANDARD PROTOCOLS

For SCADA systems, four widely accepted international and industrial standard protocols are used in various countries. These protocols are

- IEC 60870-5 which is widely used for real-time data communication between SCADA systems and RTUs or Intelligent Electronic Devices (IEDs). It is used both in serial links (IEC 60870-5-101) and over networks (IEC 60870-5-104).
- DNP3 which was derived from IEC 60870-5 and is mainly used for real-time data communications between SCADA systems and RTUs or IEDs. It is used both in serial links and over networks (DNP3 over TCP/IP).
- IEC 60870-6 (TASE.2 or IEC 60870-6) which is primarily used for real-time data exchange between utility control centers.

- IEC 61850 which is used for real-time data communications between IEDs such as protective relays and meters within substations.

### III. IMPLEMENTATION OF SCADA STANDARD PROTOCOLS IN MEA

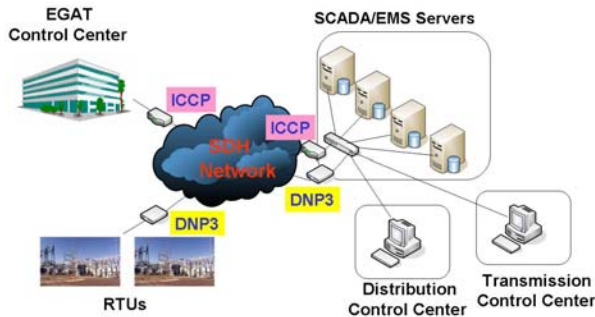


Fig. 1 MEA's SCADA/EMS Protocols

In MEA, for the existing SCADA/EMS system, two SCADA standard protocols are currently used for real-time data communications. These protocols are

- DNP3 which is used for real-time data communications between SCADA/EMS systems in both main and backup control centers and substation RTU in substations.
- IEC 60870-6 (TASE.2 or ICCP) which is used for real-time data exchanges between MEA's SCADA/EMS systems in both main and backup control centers and EGAT's SCADA/EMS system

The existing fiber optic cables and SDH switches are the main communication links between the SCADA/EMS system in both control centers and RTUs in substations and between MEA's SCADA/EMS and EGAT's SCADA/EMS.

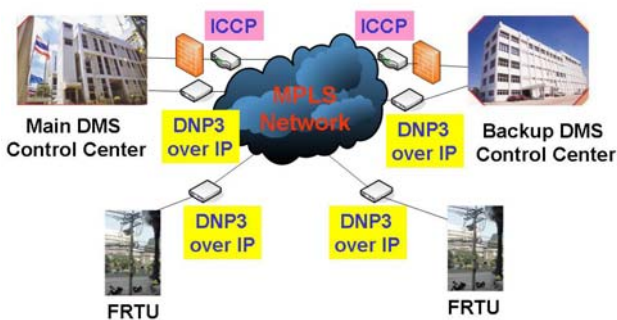


Fig. 2 MEA's upcoming SCADA/DMS Protocols

In the next two years, MEA plan to implement IEC 61850 protocol for real-time data communications between IEDs

within new substation. Furthermore, DNP3 will be used for real-time data communications between new SCADA/DMS systems in both main and backup control centers and feeder RTUs (FRTUs) installed on the electric poles. Concurrently, IEC 60870-6 (TASE.2 or ICCP) will be used for real-time data exchange between the existing SCADA/EMS and new SCADA/DMS systems.

The fiber optic and TETRA Digital Trunked Radio System (DTRS) will be used for main and backup data communications between the new SCADA/DMS systems in both control centers and FRTUs and fiber optic cables and MPLS switches will be used for data communications between both control centers and district control centers.

### IV. POSSIBLE CRITICAL THREATS TO MEA'S SCADA SYSTEMS

The existing MEA's SCADA/EMS systems are well-protected from security threats by isolation and firewalls. However, in the next two years, the requirements to integrate these systems with the new SCADA/DMS create possible threats. Furthermore, the uses of TETRA DTRS for data communications between the SCADA/DMS systems and FRTUs create additional vulnerabilities. Some of the common threats are less critical, while others are more critical. Although importance of specific threats can vary greatly depending upon the assets being secured, some of the more critical threats are:

- Blocked or delayed flow of information which could possibly disrupt SCADA operation
- Unauthorized changes to commands which could potentially damage, disable, or shutdown SCADA systems
- Inaccurate information sent to operator either disguise unauthorized changes or to cause the operators to initiate inappropriate actions

These unauthorized operations can cause power outages and potential loss of life.

### V. IEC 62351 DATA AND COMMUNICATION SECURITY STANDARD OVERVIEW

The IEC 62351 standard currently under development proposes a mechanism for securing the four most popular SCADA protocols now in use IEC 60870-5, DNP3, IEC 60870-6 (TASE.2 or ICCP), and IEC 61850. The details of IEC 62351 can be summarized as follows:

#### • IEC 62351-1: Introduction

This first part of the standard covers the background on security for power system operations, and introductory

information on the series of IEC 62351 security standards.

- **IEC 62351-2: Glossary of Terms**

This part will include the definition of terms and acronyms used in the IEC 62351 standards.

- **IEC 62351-3: Profiles Including TCP/IP**

IEC 62351-3 specifies security measures for IEC 60870-6 (TASE.2 or IEC 61850), IEC 61850, and IEC 60870-5-104. It uses TLS to meet the security requirement of authentication, confidentiality, and integrity. IEC 62351-3 protects against eavesdropping through TLS encryption, man-in-the-middle security risk through message authentication, spoofing through Security Certificates or Node Authentication, and replay through TLS encryption. However, IEC 62351-3 does not protect against denial of service.

- **IEC 62351-4: Security for Profiles that Include MMS**

IEC 62351-4 provides security for IEC 60870-6 (TASE.2 or IEC 61850) and IEC 61850. It works with TLS to configure and make use of its authentication: It also allows both secure and non-secure profiles to be used simultaneously, so that not all systems need to be upgraded with the security measures at the same time.

- **IEC 62351-5: Security for IEC 60870-5 and Derivatives (DNP3)**

IEC 62351-5 provides security for IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, and DNP3 (serial version) and for IEC 60870-5-104 and DNP3 (networked versions).

For IEC 60870-5-104 and DNP3 (networked versions), IEC 62351-5 utilizes authentication in addition to the security measures described in IEC 62351-3, which includes confidentiality and integrity provided by TLS encryption.

For IEC 60870-5-101, IEC 60870-5-102, IEC 60870-5-103, and DNP3 (serial version), IEC 62351-5 includes some authentication mechanisms which address spoofing, replay, modification, and some denial of service attacks. However, it does not address eavesdropping, traffic analysis, or repudiation that require encryption because the serial version is usually used with low bit rates communications media or with compute-constrained field equipment. TLS would be too compute-intensive and/or communications-intensive to use in these environments.

- **IEC 62351-6: Security for IEC 61850 Peer-to-Peer Profiles**

IEC 62351-6 provides authentication security measure for IEC 61850 Peer-to-Peer multicast datagrams (GOOSE, GSSE, and SMV) by using a mechanism that involves minimal compute requirements to digitally sign the messages.

## VI. SECURE DNP3 SPECIFICATION

New DNP3 specification (Secure DNP3), Volume 2, Supplement 1, "SECURE AUTHENTICATION", Version 1.00, Dated 3 February 2007, adds user and device authentication as well as data integrity protection to the DNP3 protocol. This specification is fundamentally based on IEC 62351-5 and is intended to be compliant with IEC 62351-5 specification. This specification addresses spoofing, modification, replay, eavesdropping, and non-repudiation security threats, as defined in IEC 62351 Part 2. While the DNP3 protocol specifies the data link, transport, and application layer, the Secure DNP3 only modifies the application layer and works the same whether it is serial or networked versions. However, there is a requirement that DNP3 over TCP/IP implement TLS encryption per the IEC 62351-3 specification.

## VII. IMPLEMENTING IEC 62351 IN MEA

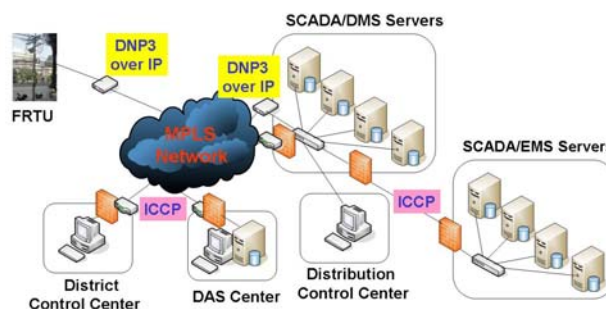


Fig. 3 MEA's upcoming SCADA/EMS/DMS Protocols

In MEA, the SCADA/EMS and SCADA/DMS systems are generally time-critical and delays are not acceptable for the delivery of measurements and control commands. These systems are designed to meet performance, reliability, safety, and flexibility. However, to prevent possible critical threats, MEA plan to implement the security measures specified in IEC 62351 for the following real-time data communications:

- For real-time data exchanges between MEA's SCADA/EMS system and EGAT's SCADA/EMS system and between MEA's SCADA/EMS system and MEA's SCADA/DMS system, Secure ICCP will be implemented according to IEC 62351-3 and IEC 62351-4. The requirement for the Secure ICCP is included in

the TOR of the SCADA/EMS migrating project and in the TOR of SCADA/DMS project. The security test and audit for the Secure ICCP is also specified in the TOR and will be performed during FAT and SAT. It is expected that the Secure ICCP will be implemented and finished in the next two years. The meeting between EGAT and MEA will be held to add the Secure ICCP in the bilateral agreement.

- For real-time data communications between SCADA/EMS systems and substation RTUs and between SCADA/DMS systems and feeder RTUs, Secure DNP3 will be implemented according to new DNP3 specification based on IEC 62351-5. However, to minimize performance impact on the communication link, only authentication at the application layer, not encryption or other security measures, is implemented to ensure end-to-end security. Moreover, only control commands from SCADA systems to RTUs are considered critical, requiring authentication. Furthermore, to enhance the security, the authentication of TETRA DTRS is also implemented. The requirement for the Secure DNP3 is specified in the TOR of the SCADA/EMS migrating project and in the TOR of SCADA/DMS project. The security test and audit for the Secure DNP3 is also specified in the TOR and will be performed during FAT and SAT. It is expected that the Secure DNP3 will be implemented and finished in the next two years.
- For real-time communications between IEDs within substation, the security measures specified in IEC 62351-3, IEC 62351-4, and IEC 62351-6 will be implemented for IEC 61850. The requirement to secure

IEC 61850 is specified in the TOR of the substation automation project.

## VIII. CONCLUSION

Securing the SCADA infrastructure is of critical importance to MEA. MEA adopts and implements IEC 62351 security standard to secure the DNP3 and ICCP protocols. However, to minimize performance impact on the communication link, only control commands from SCADA systems to RTUs are considered critical, requiring authentication. Therefore, authentication plays a major role to secure the SCADA/EMS and SCADA/DMS systems in MEA. During the procurement process, the requirement for security of the SCADA/EMS and SCADA/DMS systems is included in the TOR and the requirements for testing and auditing the security during FAT and SAT are also specified. In conclusion, for MEA's power system operations, authentication of control actions is far more important than "hiding" the data through encryption.

## REFERENCES

- [1] IEC 62351-1, Data and Communication Security – Part 1: Introduction and Overview.
- [2] IEC 62351-2, Data and Communication Security – Part 2: Glossary
- [3] IEC 62351-3, Data and Communication Security – Part 3: Profiles Including TCP/IP
- [4] IEC 62351-4, Data and Communication Security – Part 4: Profiles Including MMS
- [5] IEC 62351-4, Data and Communication Security – Part 5: Security for IEC 60870-5 and Derivatives
- [6] IEC 62351-4, Data and Communication Security – Part 6: Security for IEC 61850 Profiles
- [7] DNP3 Specification, Volume 2, Supplement 1, SECURE AUTHENTICATION, Version 1.00, 3 February 2007

## BIOGRAPHY



Wiwat Amornimit received his B.Eng. in Electrical Engineering from Chiangmai University, Thailand in 1982 and obtained his Master of Engineering Science in Electrical Engineering from University of New South Wales, Australia in 1992. He is currently an Electrical Engineer Level 10 in the Information Technology Planning Department, Metropolitan Electricity Authority (MEA). He has also worked as a Chairman of MEA's Industrial ICT Expert Group.