Network and System Management Object Modeling for Smart Grid Infrastructure

YooJin Kwon[1,3], Myung-Sup Kim[2], Yong Hun Lim[3], Jong In Lim[1]

1, Graduate School of Information Security
2, Department of Computer and Information Science
Korea University
{tmskim, jilim}@korea.ac.kr

3, Distribution Laboratory
Korea Electric Power Research Institute
Daejeon, Korea
{yjkwon, adsac}@kepco.co.kr

***Abstract*—Smart grid is an electricity network to monitor and control all its physical environments of electricity infrastructure in a fully automated way. As the importance of reliable energy utility infrastructure is growing, various security countermeasures to protect power system from security threats have been suggested, whereas there were less consideration on security by design, from the bottom system modeling level. Thus, this paper first highlights the international security standard on network and system management (NSM) requirements suggested from International Electronical Committee (IEC). Then this paper proposes significance of security by design, especially the security object modeling as the most important factor in smart grid environment. In our approach, we propose a common NSM objects for IEC-61850 protocol based substation automation environment. Finally, we present the setup procedures to implement and test NSM objects for IEC 61850-based digital substation in Korean environment.**

***Index Terms*—Network and system management (NSM), security object modeling, security management, IEC 62351-7**

I. INTRODUCTION

An increasing amount of technological advancements have motivated the development of a smart electric grid. Based on government driven projects, the smart grid in Korea expands the current capabilities of the grid's generation, transmission, and distribution systems with cutting-edge information technology, which consists of network and system infrastructures mingled up with traditional, physical power equipments. Distributed generation, renewable energy sources, micro-grid (MG), electric vehicles (EV), the demand response (DR) management of electricity, phasor measurement units (PMU), wide area measurement systems (WAMS), and advanced metering infrastructures (AMI) technology has been deployed in Jeju island test bed environment and completed the field test in 2013.

These recent smart grid environments focus now on security that provides an infrastructure capable of handling future requirements for reliability and assurance on network and systems. Numerous countries have acknowledged that cyber attacks have targeted their critical infrastructures while attackers use highly sophisticated attacks against utility infrastructure and systems. Thus, a comprehensive approach is required to utilize cyber–physical system (CPS) interactions to effectively manage the security concerns within the grid. Security requirement for smart grid is prioritized on availability, reliability and sustainability. Among these security requirements, availability refers to a system or component that is continuously operational for a desirably long length of time. In IEC 61850-based digital substation, availability of physical electric grid is the most critical factor due to serious blackout accident or security accident implications. Availability of time-critical service commands is also important. For instance, the delay constraint of the generic object oriented substation events (GOOSE) messages is 4 ms and response period for each measurement value of the manufacturing message specification (MMS) message is varied from 0.25 second to 2 seconds in IEC 61850. There has been much research to detect attacks on denial of service, packet forgery, packet replay, spoofing, and scanning attack, in general. However, no research has been found that implemented anomaly detection to countermeasure various attacks targeted for IEC 61850-based digital substation.

There have been many researches on security system in the smart grid environment. [1]-[2] Most security system research in the literature is mainly focused on intrusion detection systems, data encryption and security protocols, whereas there is no research investigated on security object modeling with our best knowledge in the IEC 61850 specific protocols or function commands. IEC 61850 protocol and function commands are used for standard communication between heterogeneous smart grid systems in Korea - in next generation SCADA system to control transmission, distribution, MG, EV, DR, PMU, WAMS and AMI environment. Moreover, current international standard on network and system management, IEC 62351-7, was developed in the absence of implementing the real network and system. A sophisticated object mapping to IEC 61850 requires additional analysis to ensure secure design in new system deployments.

In order to guarantee reliability and security in smart grid infrastructure, we setup a test-bed that replays the whole

TABLE 1 NSM classification based on its functionality

A. Communication Health (61)	*B. End system Health (30)*	*C. Intrusion Detection (45)*
1. Network configuration monitoring and control (12) 2. Network backup monitoring (10) 3. Network status monitoring (16) 4. Communication protocol monitoring (22)	5. End system monitoring (22) 6. End system security management (8)	7. Unauthorized access (5) 8. Resource exhaustion (9) 9. Buffer overflow (5) 10. Tempered/malformed PDU (5) 11. Physical access disruption (8) 12. Invalid network connection (6) 13. Coordinate attacks (7)

traffic of the digital substation in South Korean environment. By simulating these real traffic data, we propose security network and system management methodology leveraging an IEC 62351-7 international standard, and aim to get a high accuracy of attack detection ratio.

The contributions of our work are as follows. First, we classify the international security standard on network and system management requirements from IEC 62351-7 document. The standard document is written in complicated format and vocabulary terms, thus it needs to be refined in an intuitive table and summarization. As far as we know, this work is the first attempt to analyze the IEC 62351-7 document into an organized way. Second, we propose significance of security by design, especially security modeling as the most important factor to be setup in South Korean Smart grid environment. With our best knowledge, Korea has adopted one of the most advanced smart grid technologies in the world, strongly driven by the government. This work can be globally applicable for any other countries employing IEC 62351-7 in the smart grid. Third, NSM objects were newly implemented for IEC 61850-based digital substation in Korean environment, with proposed procedures to implement and test NSM objects as a case study.

II. IEC 62351-7 STANDARD FOR NETWORK AND SYSTEM MANAGEMENT

In International standard IEC 62351-7 [4], security through network and system management objects have been defined. Security capabilities can be improved by monitoring those objects continuously. According to five major network management functions, which are fault, configuration, accounting, performance and security, a power system equipment failure causes performance degradation that might affect the power system operation. Moreover, network configuration change could affect a single point of failure that results in a serious blackout accident in power system. Thus, power system nowadays is required to ensure security and reliability for power system operations according to standardized object models.

According to NSM security requirements suggested in IEC 62351-7 standard, there are 136 data object models for power system operation are defined. And object models are categorized into three top-level classes, 'Communication Health', 'End system Health' and 'Intrusion Detection'. Communication Health NSM objects is to monitor and control network and protocol level. End system Health NSM objects is to monitor and manage end system, which are mostly related to physical power equipment or facilities in the field. Intrusion detection NSM objects are to manage data related to intrusion detection system (IDS) logs and security system. These three classes can be more divided into 13 sub-classes as shown in Table I.

On the other point of view, there are different data object types defined for each NSM data objects as shown in Table 2- values, alarm, configuration setting, control, log, status, and setpoint. These data object types are described in the document vaguely. The detailed information is strongly needed to generate the actual value for each object and the test procedure to validate whether the information has been implemented correctly. But neither of them was depicted in the document, which has brought much confusion to IT system engineer and system administrators in the smart grid.

TABLE 2. DATA OBJECT CLASSIFICATION

Data object type classification	**description**	**Number of NSM objects**
Values	Status value when system operates normally	46
Alarm	Alarm message when status changed into abnormal	42
Configuration setting	Predefined network and equipment configuration	28
Control	Control signal	13
Log	Status change message	3
Status	Detection message on new equipment, node or route	3
Setpoint	Special value for parameter setting change	1

Thus, in this paper we propose the detailed definition and implementation on real NSM objects applicable for substation automation environment in South Korea. NSM objects with three top classes and 13 subclasses are analyzed in depth to be used in level 2 Switch and Security Information and Event Management (SIEM) system. Use case and case study are introduced for some objects which can be applicable for reliable and useful in the smart grid.

III. SECURITY-BY-DESIGN

The first step toward protecting the smart grid from security breaches involves risk analysis: The first cyber security risk is serious disruption to the electric grid, which the North American Electric Reliability Corporation (NERC) calls a critical national infrastructure. The NERC Critical Infrastructure Protection (CIP) guidelines [5] list security concerns that must be addressed. Another significant risk is loss of system availability, and the possibility of losing control of certain aspects of the grid.

After these basics, consequences of a grid failure must be considered. One possible consequence is process interruption. For example, manufacturing processes could be jeopardized, leading to damage of production equipment or the product being manufactured. Such forced outages could be detrimental to petrochemical refineries, pharmaceutical manufacturing, and other industries using continuous processes. Significant equipment damage can also occur in situations where electricity supplies important cooling or heating functions.

While news and media scenarios tend to dramatize wide-scale electricity black outs, another risk—asset misconfiguration—is more insidious. In this scenario, settings on equipment are changed, and normal operational protections are removed. For example, if a protective relay or a voltage tap is set to 130V instead of 120 for a residential area distribution line. Loss of data and confidentiality is the most subtle consequence—and is more applicable as we move to advanced metering infrastructure (AMI) and 15-minute interval meter reads, increasing the likelihood of misuses that can lead to an invasion of privacy for individual residents. Another risk factor follows from NERC CIP, which has now instituted substantial financial penalties resulting from violations of its regulations.

Another very serious risk involves employee safety. When considering protective measures, some utilities identify safety as their first priority and reliability as second. Personal injury to employees is a prime concern because typically two-thirds of the staff are field crews. While most utility line personnel are trained to always assume a line is energized, sudden presence of voltage due to a line being re-energized from an unauthorized source can still be a threat.

Lastly, there is the risk of loss of customer and public trust, particularly given how difficult it would be for a utility to deny awareness of the existence of cyber security threats. This would be more problematic for utilities in the jurisdiction of public utility commissions, since outages that utilities could have reasonably devices are also susceptible to denial-of-service attack by frequency jamming, or blocking received signals by wrapping the device in aluminum foil. Thus, one has to maintain the philosophy that the internal systems will eventually be exposed to attack. Reducing vulnerability of internal systems includes ensuring:

- Each application validates its input for reasonability before processing;
- Each application has a way of announcing an exception—whether it is a security intrusion or simply a failing Intelligent Electronic Device (IED) sending bad input.

It is for the security system to decide why the abnormal event occurred. Applications should not contain built-in weaknesses; however, any functional code of software may still contain security holes. Some of us are aware that certain vendors publish lists of security patches. On occasion, patterns can be observed in the descriptions of these weaknesses—problems that were effectively, but not intentionally, in the source code. A program may have passed its functional testing, but security issues may still exist. There are actually software products that can scan and analyze source code, somewhat as a compiler does, looking for potential problems with array indices, for example, buffer overflows, and other common conditions that may not have been checked. Beyond a locally written application having no detectable security flaws, there is the worrisome fact that a typical executable application, for example, executable file with .exe or .dll format, contains much code the programmer didn't write. Such code comes not from a source file, but from a multitude of pre-supplied libraries and linked-in objects.

Security provisioning can significantly affect system design, and therefore should be part of phase one in the design of any successful project. The re-design cost can be too high, not only in terms of delays and cost, but also in terms of public trust. At the time of this writing, smart grid projects funded through the American Recovery and Reinvestment Act (ARRA) have a fixed deployment time and a public "lessons learned" reporting requirement [6]. In the proposals, applicants are required to submit security and interoperability statements about the proposed project. These two requirements should help utilities understand best practices around smart grid security.

Once an incident occurs, the loss of trust makes a security retrofit, at any cost, less believable to the consumers. While security design should be in the first phase of a project, the time-worn phrase, "scope, schedule, and cost," can sometimes work against proper security design. Projects have schedules and cost, while hackers have no such constraints.

Therefore, long after the secure smart grid project is completed, cybercriminals may be working on new technologies to circumvent what has been done and acceptance tested. As a result, periodic security testing is required indefinitely and must be accounted for in ongoing operational cost. This is really no different from buying a substation and budgeting for annual maintenance expense.

The smart grid provides much more data about grid operations than the traditional grid. By using stream computing or complex event processing software, events on the grid may be categorized as operational, maintenance, or security. Correlating abnormal activity from all inputs then becomes part of the security detection methodology. There are several reasons why a series of secure devices might not achieve the desired end-to-end security: Problems with the interconnections, the communication link between each device,

the remote configuration and firmware upgrade process, secure application design.

It is therefore recommended that overall end-to-end security be an assigned responsibility on a project for the overall system integrator or another expert provider. As a result, smart grid security involves an architecture that includes security from the beginning, consists of more than just protective devices such as firewall, and engages processes as well as products. A simple perimeter defense is not sufficient; monitoring, both for events and physical actions, is required to bring the benefits of smart grid with minimal risk to this vital part of the infrastructure of power system.

IV. NSM Object Implementation

A. Implementation and test environment

In this research, we used Ubuntu operating system with SNMP agent. NetSNMP 5.6.1.1 was installed to implement SNMP, which is well-known open source library for network equipment monitoring. NetSNMP supports text-based snmpget, snmpset, snmptable commands.

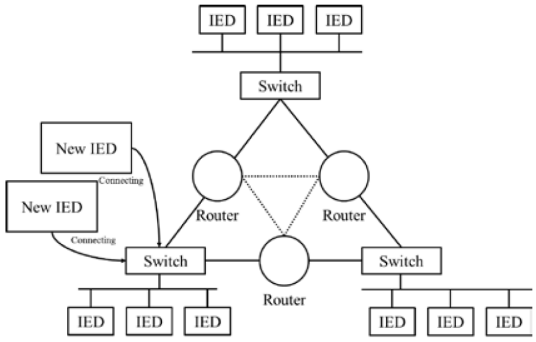

Figure 1. Experimental environment

B. Implementation steps

For the first step, 136 NSM objects were identified based on 2 level categories in Chapter 2. In the second step, NSM objects are then mapped into either service management information in IED equipment data attribute or network equipment- router, switch, passive IDS - data attributes in the substation automation environment. In the third step, NSM objects are combined to be implemented in specific security functionality. Network backup monitoring object and other related NSM objects have been combined, for example, to perform network backup monitoring functionality in the network device. In the last step, security agent and manager have been developed along with SNMP MIB file. *Security agent* is a subset of NetSNMP package by using daemon API communicating with SNMPD. *Security Manager* is managing trap message depending on trap rule definition.

C. L2 Switch monitoring object

- NodRs: rcDeviceCommReset

This object is to reset node through software capabilities.

- ConnFailTot: udpNoPorts, udpInErrors, tcpInErrs,tcpInErrs, tcpOutRsts

4 different NSM objects are bundled into one NSM objects to describe the total number of failures since the last reset.

D. Intrusion detection system monitoring object

- ConnCnt: tcpMaxConn

This object is to count on maximum number of connections of permitted.

- BufOvAlm : rcDeviceErrStackOverflow, rcDeviceErrHeapError

2 NSM objects are are bundled into one NSM objects to describe the alarm message on buffer overflow problem. TrfFrqAlm object is to alarm on exceeding traffic frequency setting with the following use case.

V. CONCLUSION

This paper proposes a new method of IDS where big data has been collected on smart grid. Major contributions of this research are summarized as follows:

- First, we classify the international security standard on network and system management requirements from IEC 62351-7 document into an organized way.
- Second, we propose significance of security by design, especially security modeling as the most important factor to be setup in South Korean Smart grid environment which can be globally applicable for any other countries employing IEC 62351-7 in the smart grid.
- Last, NSM objects were newly implemented for IEC 61850-based digital substation in Korean environment, with proposed procedures to implement and test NSM objects as a case study.

References

[1] Yan, Ye; Qian, Yi; Sharif, Hamid; Tipper, David, "A Survey on Cyber Security for Smart Grid Communications," *Communications Surveys & Tutorials, IEEE* , vol.14, no.4, pp.998-1010, Fourth Quarter 2012

[2] Komninos, N.; Philippou, E.; Pitsillides, A., "Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures," *Communications Surveys & Tutorials, IEEE* , vol.16, no.4, pp.1933,1954, Fourthquarter 2014

[3] Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, NIST, 2010.

[4] Network and system management (NSM) data object models, IEC 62351-7 TS Ed.2.0, 2013.

[5] NERC CIP guideline CIP-002-1 through CIP-009-1, available at http://www.nerc.com/fileUploads/File/Standards/Revised_Implementation_Plan_CIP-002-009.pdf

[6] Recovery Act, Department of Energy, US Government, available at http://energy.gov/oe/information-center/recovery-act