전력 IT 네트워크 보안 전망

김학만, 강동주
한국전기연구원

Prospection of Power IT networks

Hak-Man Kim, Dong-Joo Kang
KERI

Abstract - The importance of security is increased in power industry. Recently Power IT networks are attacked in cyber space and demage of attack become increased. For solving the problems, many research studies for network security enhancement are globally carried out in the world. In this paper, we introduce recent cyber attack cases, efforts for enhancing cyber safeness and put into perspective of potential security areas for power IT areas.

1. Introduction

Supplying electrical power is very important problem. Power system is composed of many systems and communication networks. Increment of cyber attack and terrorism threaten stable power supply. The interruption of power supply makes the daily life of people to endanger. Recently dangerous situations by cyber attack have been generated in the world. For that reason, various efforts for stable operation of power industry have been studied.

Recently, many communication networks of power industry such as SCADA (Supervisory Control and Data Acquisition), WAMS (Wide Area Measurement System), EMS (Energy Management Systems), DLC (Direct Load Control)system, SAS (Substation Automation System), Micro-grid system, SPID (Strategic Power Infrastructure Defense) and soon have been interconnected for more efficient operation. When networks are more interconnected, the danger against cyber attack and terrorism will be greater. For the reason, the huge interconnection network causes critical security problems against safe operation in the future.

In this paper, we introduce recent cyber attack cases, efforts for enhancing cyber safeness and put into perspective of potential security areas for power IT areas.

2. Cyber Security in Power IT

2.1 Cyber Attack

Power system has been exposed to cyber security problems with IT advancement and network growth. According to a DOE report released at 2005 year, the portion of energy industry takes almost 70% in main infrastructures being attacked in the States from 2002 to 2004 year. Fig. 1 shows statistics on cyber attacks happened on various industries.

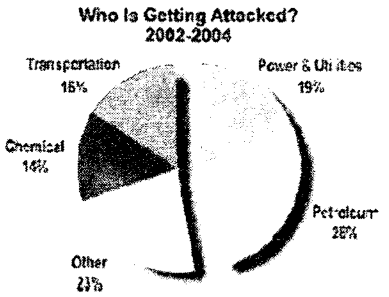

Exhibit 2.4 – Attacks on Industrial Control Systems

Source: Industrial Security Incident Database (Byres 2005)

Fig. 1 Cyber attacks on various industries [1]

The external attacks have been increased compared to internal attacks. We can check it out on Fig. 2 that external attacks are rapidly increasing recently.

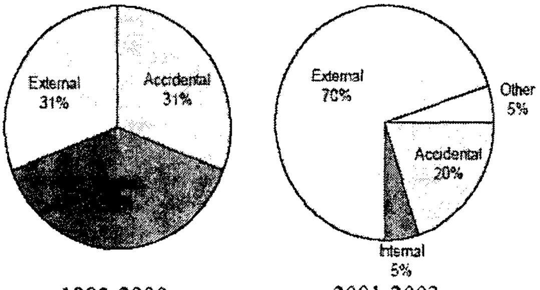

Fig. 2 Circular diagram on attack types [2]

The infrastructure is becoming the main target of terrorism, because the impact caused by attack is so huge. Cyber attacks could also cause the system fault like physical attack. A coordinated attack on major power plants or substations could trigger a cascading blackout with major social and economic impacts [2]. For example, computer hacker could destroy a substation transformer by sending the transformer overload signals, causing it to rapidly overheat and explode like doing it by a bomb or setting a fire [3].

Fig. 3 Substation under attack

According to [4], the following incidents illustrate the vulnerability of critical infrastructure systems:

An attack in 2001 on computer systems of CAL-ISO, California's primary electric power grid operator that apparently were not discovered for 17 days

An attack in 2003 by Vitek Boden on the SCADA system for the Maroochy Shire sewage control system in Queensland, Australia, that caused millions of gallons of sewage to be dumped into Maroochy waterways over a four-month period

An attack on the Ohio Davis-Besse nuclear power plant process computer - a 2003 Slammer worm attack - which disabled a nuclear safety monitoring system for over five hours

An attack in 2003 by the Sobig virus on CSX dispatching and signaling systems that disrupted freight and commuter rail service in Washington, D.C., Virginian and Maryland

2.2 Efforts for Enhancing Cyber Security

The use of IT within SCADA systems of critical infrastructures such as electric power, gas and oil transportation systems has made them exposed to cyber security problems and the have been targeted by cyber attacks and terrorism. According to [5] and [6], cyber risk of SCADA systems has been increased by the following:

Table 2. Activities for security - United States Case

Institute	Activites
DOE	- TSWG - Critical InfrastructureTestRange - National SCADA Test Bed
DHS	- NCS - NCSD Cyber Security Test Bed - I3P SCADA - Process Control System Forum
NERC	- Standards & Guidelines
AGA 12	- Standard
NIST	- Process Control Security Requirements Forum
NSF	- R&D Projects
FERC	- Projects
EPRI	- EIS Projects

2.3 Cyber Security in Power IT Network

Recently, many communication networks of power industry such as SCADA (Supervisory Control and Data Acquisition), WAMS (Wide Area Measurement System), EMS (Energy Management Systems), DLC (Direct Load Control)system, SAS (Substation Automation System), Micro-grid system, SPID (Strategic Power Infrastructure Defense) and soon have been interconnected for more efficient operation. When networks are more interconnected, the danger against cyber attack and terrorism will be greater. For the reason, the huge interconnection network causes critical security problems against safe operation in the future. Fig. 4 shows a example in Power IT network integration.

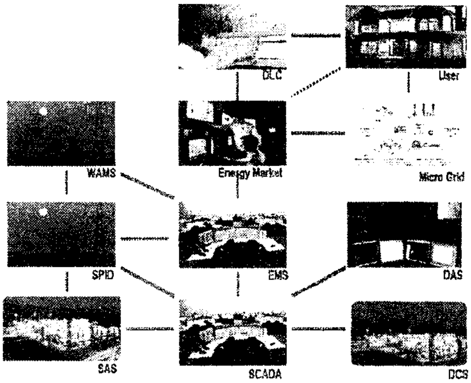

Fig. 4 Integration example of Power IT network

For enhancing Power IT network security, the following research efforts should be studied.

Access control
Firewalls and intrusion detection systems
Crytography and key management
OS security, etc.

3. Conclusions

The importance of security is increased in power industry. Recently Power IT networks are attacked in cyber space and demage of attack become increased. For solving the problems, many research studies for network security enhancement are globally carried out in the world.

Especially, Power IT networks become integrated for more efficient operation. For these situations, network security problems become more important.

In this paper, we introduce recent cyber attack cases, efforts for enhancing cyber safeness and put into perspective of potential security areas for power IT areas.

Reference

[1] Jack Eisenhauer, Paget Donnelly, Mark Ellis, Micheal O'Brien, Roadmap to Secure Control Systems in the Energy Sector, Energetics Incorporated, Colombia, Maryland, 2006

[2] Eric Byres, Justin Lowe, The Myths and Facts behind Cyber Security Risks for Industrial Control Systems, British Columbia Institute of Technology, PA Consulting Group

[3] John Douglas, Grid Security in the 21-th Century, EPRI Journal, 2005

[4] Ronald L. Krutz: Securing SCADA Systems, Wiley Publishing Inc., Indiana (2006)

[5] V.M. Igure, S.A. Laughter, R.D. Williams: "Security issues in SCADA networks", Computer&Society, Vol.25, pp. 498-506, 2006

[6] Thomas Kropp: "System Threats and Vulnerabilities - An EMS and SCADA Security System Overview", IEEE Power and Energy Magazine, pp.46-50, March, 2006