Research on the Integrated Security Supervision Technology of Cyber-Physical System in Substations

Chao SUN\textsuperscript{1,}\textsuperscript{*}, Zhen-yu TANG\textsuperscript{1} and De-he LIU\textsuperscript{1}

\textsuperscript{1}NR Electric Co., Ltd., 69 Suyuan Avenue, Nanjing 211102, China
*Corresponding author

Keywords: Smart grid, Security supervision, Cyber-physical system, Substation.

Abstract. International hacker organizations have made more effort to research on the penetration attack technologies for smart grid automation system, planned and implemented attacks to international power grid systems, and caused accidents. The author of this paper discusses the security challenges of cyber-physical system in substations from three perspectives: security threats, issues of security system in power grid and security requirements in substations, and introduces the integrated security supervision technical solution. It shows that to make substations more security, two part of missions must be accomplished by the integrated security supervision system. On the substation side, the system collects operation information, system log, and mirrored communication packets of devices, analyses devices and systems behaviour, assesses the local security situation. On the main station side, the system gathers security information from substations, distributes the security policy to substations, monitors and analyses the overall security situation with aggregate data. The solution has been deployed in several projects and achieved remarkable results.

Introduction

In recent years, according to the continuous development of smart grid and information technology, the power secondary system based on modern information and communication technology brings great changes of the basic structure of power infrastructure, and becomes an important technical guarantee for the safe, reliable, stable and economical operation of primary power system. The primary equipment of the power grid with the secondary system forms a complicated cyber-physical system. In this case, due to the extensive deployment and interconnection of the secondary system, the problems of secondary system of power grid, such as physical security, operational safety, and information security, are likely to affect the stability of the power system and the reliability of the power supply\cite{1} \cite{2}.

The security threats of the secondary system are increasing day by day. The foreign hacker organizations have strengthened the penetration and attack research on the cyber-physical system including the smart grid \cite{3}. Through the attack to the information system, the aim is to destroy the physical system, undermine social stability and impact on the national economy. Especially in recent years, hackers organized and implemented a number of attacks against international power grid, and caused some of power grid operation accidents \cite{4}. It is necessary to make more effort on the research of the integrated security protection of the cyber-physical system of smart grid. In the power grid, substation secondary system security protection has not yet reached the level of the master station system \cite{5} \cite{6}. By analysing the information security challenges of substation and the insufficiency of secondary security system in existing substations, this paper summarizes the current and future information security requirements of the secondary system in substations, and proposes the information security solution.
Challenges

Security Threats

The smart grid is a complex cyber-physical system, in which the secondary system of the substation is responsible for the monitoring and controlling of the power transmission and transformation equipment in the substation. The international hacker organization recognizes its importance and researches on attack means for the grid, especially the substation secondary system. Recently, more and more tools are developed by hackers for automation system penetration attack, such as Stuxnet, Flame, Havex, BlackEnergy and so on [7]. BlackEnergy was used by the hacker organizations as the carrier to penetrate the Ukrainian national power grid in 2015, which resulted in seven Ukrainian 110KV substations and 23 35KV substation failure, and blackout in a large area of Ukrainian Ivanov-Frankovsk region with half of the users affected. The path of the penetration attack is shown below:

![Diagram of the penetration attack](image)

**Figure 1. The path of the penetration attack.**

Attackers with phishing e-mail, firstly implanted of BlackEnergy into the office computer, which established a base in the office computer for horizontal penetration, and then spread virus to the SCADA host via the mobile media. After obtaining the control rule of the SCADA system, the virus stopped power supply of several lines by sending the control command. What’s more, the virus overwrote the MBR and some hard disk sectors, resulting in the unsuccessful restart of the SCADA system. Due to the loss of monitoring and control functions, the staff could only manually operate the primary equipment to restore of power supply, which slowing down the grid fault processing progress.

While attacking on the substation, the attacker made the customer service center lose efficacy by telephone DDoS attacks, hindering the customer service department to figure out the scope of power outages and the dispatch center to take emergency measures, Both actions together accomplished the attack damage to the power infrastructure.

Issues of Security System in Power Grid

According to the analysis of the above attack path, we can know that the attacker made use of vulnerabilities in Ukrainian power grid, such as imperfect physical isolation technology, lack of mobile media management and terminal protection measures to create the security event [8]. Chinese second power security system in the substation is relatively more perfect, but there are still some shortcomings:

1) Each component of the secondary security system does not interact with each other, and could not be integrated to determine the threat. Without relevance analysis of the alarm information of vertical encryption and firewall, the system cannot analyze the exact attack path.

2) The safety of the boundary of the security zone has been strengthened by the secondary
security system, but the security measures internal the security zone are relatively weak, such as server and workstation terminal security, debugging terminal management which accessing to the operating environment. There are some functional failure caused by improper maintenance, for example, updating malicious code or virus database not in time.

3) The security measures of substations are not as perfect as main stations. There are no IDS devices in substations, which could analyse possible security risks and attack behaviours via communication packages check. And if the substation copies the main station security measures, such as IDS, malicious code detection system and so on, the maintenance of these tools would be highly complex, and practice effect is difficult to guarantee.

4) The secondary security system cannot identify the power system-specific characteristics of the secondary system behaviours, resulting in misjudgement, which reducing the degree of maturity of the system, or on the other hand missing the real threat.

Security Requirements in Substations

To solve the information security issues in substations, the following aspects need to be considered:

1) The system can be interconnected with the existing substation secondary security device or system, thus improving the comprehensive judgment ability.

2) The system can fill in gaps of information security in the substation, adopt the targeted monitoring measures to the network communication and business behaviours of the substation, distinguish between the normal operation behaviour and the intrusion behaviour, which improving the system judgment accuracy.

3) The system is not only deployed in substations, but also need to be deployed in the main station side to meet the centralized monitoring requirements;

4) From the maintainable point of view, the system can reuse the graph and model of the secondary system in substations to reduce the maintenance workload. Simultaneously, the system can update the security policy to substations, thus improving the maintenance consistency and reducing the duplicate maintenance work load in substations.

Solution

System Architecture

There is secondary security equipment, including vertical encryption devices, firewalls, and positive and negative isolation devices, as well as the environmental monitoring system in substations. The integrated security supervision system of the substation needs to interconnect the above devices or systems, obtain the communication status information, configuration information, and the syslog of the ICT devices via the direct acquisition method, analyses the communication package via the bypass mirror method, in order to audit security behaviors and verify security baseline, achieve comprehensive analysis. The system architecture as shown below:
The system consists of two parts:

- The main station side system, deployed in regional and national dispatch centers, is responsible for communicating with security supervision devices in substations, gathering security information from substations, distributing the security policy to substations, monitoring the security situation of the secondary system in substations.

- The security supervision device is responsible for collecting operation information of substation network security equipment, communication packet, system log, monitoring devices and systems in substation, analysing the security situation, and verifying the configuration security baseline of the workstation or server.

- The data communication between the main station and the substation is via the non-real-time VPN of the dispatching data network, and adopting the IEC61850 protocol to implement graph, model, and data collection and configuration distribution.

The data flow diagram of the system is shown below:

Figure 2. The system architecture.

Figure 3. The data flow diagram.
The system consists of a master part in master station and a security supervision device in substations. The master part is deployed in the security zone II and the security zone III. The functions of data collection, configuration updating, and processing of the substation security and operation data are carried out in the security zone II. The modules deployed in the security zone III are responsible for statistical analysis, maintenance, report, alarm and package check. The data flow key points are as follows:

1) The security supervision device in substations collects operation information and configuration information of secondary devices, ICT devices and SCADA system through SYSLOG, SNMP, and SSH protocols, and obtains communication packages via bypass mirror.

2) For comprehensive supervision of secondary information security in the substations, the master system communicates with the security supervision device to get security events, illegal mobile terminal access records, device configuration verification result, and communication packages audit outcome.

3) OMS system provides secondary equipment account information to the master part.

4) The master system communicates with the higher-level master station via the VPN network in the security zone II, and exchanges KPI data.

5) The modules deployed in security zone II and III exchanges data through the positive and negative isolation devices, including the processed substation data from security zone II to III, such as baseline verification results, audit results, terminal management information, and package query results, and the configuration baseline data as well as security audit strategy from security zone III to II.

**Implementation Technologies in Substations**

The security supervision device is responsible for the collection of operating status, topology link relationships, system configuration, system logs and other information of the various secondary devices, ICT equipment and SCADA system in substations, and baseline verification and terminal access management. The data flow diagram of the substation is shown as the following figure:

![Data Flow Diagram of Substation](image)

Figure 4. The data flow diagram of the substation.

The security supervision device collects the operation information of ICT devices such as switches, firewalls, servers and workstations in the substation by the SNMP protocol, acquires the system logs of the vertical encryption devices, switches, firewalls, servers and workstations through the SYSLOG protocol, gets system configuration of firewalls, servers and workstations via SSH protocol. It also monitors secondary device operation and security status by the 61850 protocol or 103 protocol.

The security supervision device normalizes the collected logs and converts the log of different expressions into a unified description format, thus greatly improving the efficiency of log information.
processing and satisfying the complicated multi-dimensional statistical analysis. The device performs real-time, uninterrupted security event relation analysis of all normalized log streams through a predefined rule database and relation analysis engine. It supports regular expression rule and statistical function. For network traffic data, the device establishes periodic baseline and aperiodic baseline, judges the difference between actual flow characteristic information and baseline value by comparing analysis and loop analysis, identifies abnormal traffic attacks or violations. The device uses a self-learning and self-feedback mechanism for baseline generation and correction algorithm.

The security supervision device compares the collected device configuration information with the established baseline, identifies the system weak password, checks the virus database version of the anti-virus software, the system patch, the software installation record, and the software unloading record, monitors the network illegal connection to generate a list of differences compared with the baseline. Unauthenticated U disk or mobile hard disk access is automatically prohibited by the security supervision agent which deployed in the workstations or servers.

The security supervision device quickly processes the packages transmitted by the mirror port of the switch by the FPGA bus technology and analyzes the packages according to the preset rules, including broken links, port abnormal traffic, network storm, and package lost. At the same time, the package can be analyzed by the package feature extraction method and the abnormal business behaviors can be found.

Summary
The secondary system integrated security supervision technology of the substation covers the functions of substation security auditing, baseline verification and terminal management. The security supervision device supervises ICT devices, secondary security devices, secondary devices and SCADA system. It fills gaps in information security supervision in the substation, cooperates with the existing security device and system, and improves the comprehensive defence capability of the substation. The system based on the integrated security supervision technology of the substation has been deployed in several projects and has achieved remarkable results.

Acknowledgement
This research was supported by NR Electric Co., Ltd.

References


