Industry Solutions towards Cyber Security of Modern Switchyards/Grid and Distribution Systems

A K vishwakarma, Manager (O&M-EM), NTPC Korba

B K pandey, DGM(OS-Elect), Noida

Abstract: ***This paper discusses the practical challenge and issues with respect to cyber security of modern switchyards/SMART GRID for power utilities. Various cyber security standards are being emerged globally for compliance by all stakeholders related with power system. Power utilities cannot face unlimited budget towards the cyber security as the concept is premature in industries. The cost effective solutions for securing the modern electrical switchyards against cyber threat have been discussed. Many of these solutions can be implemented by the power utilities using available infrastructure with them, while costly solutions they can implement in phased manner.***

I. INTRODUCTION

Use of Industrial Automation and Control Systems are extensively increasing to manage power generation, transmission and distribution functions of the Grid. Apart from Industrial Control Systems, Information & Communication Technologies play a crucial role in improving reliability, availability, efficiency of the grid and making it "SMART" in meeting customers' modern age demands. Challenges in managing existing Grid infrastructure and ever growing demand for energy has led to several reforms and all stakeholders have started "Smart Grid" initiatives. At the same time, use of commercial IT equipment, open standards and protocols are exposing Electricity Grid to ever increasing risk of cyber-attacks. Recent Northern Power Grid Failure in India was suspected of cyber security breach. Power sector could be vulnerable to crippling cyber attacks on a scale that can have serious implications for national security and economy.

Presently all the power utilities, Transmission & Distribution agencies in modern power systems are using different form of electronic devices like Intelligent Electronic Devices (IEDs), Relays, SCADA etc and different communication means of communication for variety of purposes but there is no clear focus as far as cyber security of their infrastructure is concerned. Cost involved towards this is one of the major hurdles for not taking rigorous cyber security measures.

Also, Smart Grid will involve Distributed Generation (DG) that has a variable output and a variety of characteristics. The location where the Smart Grid is connected to the existing power system as well as DG is substation/modern switchyards. Therefore, the operation of such switchyards & related distribution network must be secured for reliable power supply and operation of power system. For example; in PV solar power integration, physical vulnerability might be the ability to easily access a circuit board in an inverter. Likewise, cyber vulnerability might be the ability to access and alter digital usage data in a smart meter associated with these systems. Although some vulnerability appears more serious than others, it will be the consequence value that will allow a utility to make important decisions about mitigation and design.

Distribution grid is a complex system. Data flow and consumption at lower levels directly relate to the larger grid and affect overall utility performance. Data movement throughout the system and back to a utility, for example, is subject to the security controls identified by standards and guidelines and applied by the utility.

II. SECURITY REQUIREMENTS

In general, Cyber security requirements for a modern grid /substations and distribution networks include three main security properties: confidentiality, integrity, and availability.

Confidentiality: Modern grid/ switchyards collect various type of data/information related to customers, grid equipments,

generators and other market participants. The collected data needs to be much secured.

Integrity of data, commands, and software: A huge amount of data is collected by sensors installed at various places within the grid/switchyards and action is taken according to this data. Unauthorized modification of data or insertion of garbage data would destabilize business and operational & maintenance activities.

Availability: Ensuring timely and reliable access to end use of information is of utmost importance in the modern grid/substations. Also, the system should be resilient to attack and not shutdown in the event of an intrusion. Blackouts need to be prevented under all circumstances.

III. SECURITY VULNERABILITIES

In evaluating the security threat to substations and distribution networks, it is to be kept in mind that numerous people have physical contact with various devices within the substation/SCADA systems. These individuals include employees, contractors, vendors, manufacturers, etc. Of particular concern is the fact that the typical substation environment can provide a means to compromise the entire architecture with the plant premises.

The following list provides some examples of possible security threats that may exist in modern switchyards:

- An authorized person is approached by an unauthorized person who offers financial reward for the point mapping, & password of the automation system
- Disgruntled employees or ex-employees who cause damage to satisfy a grudge
- Hobbyist intruders who gain pleasure from unauthorized access
- Software providers who, in attempting to protect their intellectual property rights, create vulnerabilities or threaten to disable the software in contractual disputes which may arise during construction or maintenance phase
- The vendor of the original system has left behind a backdoor which is unknown to the power utility
- Criminal activity directed against the power utility, its employees, customers, suppliers, or others
- Competing organizations searching for proprietary information of the power utility, its suppliers, or customers
- Injecting false information on price and meter data: An attacker can send packets to inject false information on current or future prices, or send wrong meter data to a utility company
- Malicious activities by enemy countries against any nation

It is also important to consider here that the inadvertent compromise of an IED (Intelligent Electronic Device)/Relays or automation system of modern switchyards by authorized personnel who do not intend to degrade or affect its performance, but through some action on their part, do also compromise the system. Examples include:

- The use of an outdated or incompatible configuration software version which results in a corruption of the substation device settings.
- Errors in entering settings/configuration data or errors in the engineering development of settings/configuration which compromise the performance of the system

In recent years, cyber attack has become increasingly sophisticated. Attacks have become automated, so that specialized expertise is not necessarily required to perform them. Many attackers install “root kits” on the victim systems which are usually designed to enable the intruder to re-enter the system at will, to prevent the system administrator from discovering the attack, and to destroy any remaining evidence of the attack when the intruder is finished.

III.A INTERNET VULNERABILITIES

There is a general misconception that a modern switchyards or distribution architecture must have an Internet connection, and then only cyber threat is possible. In fact, this is not true. For example, an inadvertent interconnection was made from a

third-party contractor who connected their computer to install a patch on an "isolated" relay or SCADA network of the power plant. The network became connected to the Internet because the third-party contractor's computer had a broadband Internet wireless card installed. As such, it is still possible to compromise the owner's system. Unfortunately, hackers tend to use an "island hopping" approach to infiltrate a network. They begin with firewall, web server, internal modem, etc. and use the compromised perimeter computer to launch a fresh attack on vulnerable devices on a "private" network.

III.B DIAL UP VULNERABILITIES

Many dial–up connections are used in modern power plants/substations. The dial-up connection of public address system allows any-point to any-point connections, just like the Internet. "Security through obscurity" is not a valid method to protect the resources that connect to the Public Switched Telephone Network (PSTN). Because the PSTN is an open network, an attacker does not need to take over any switchgear or computers at the phone company to perform an attack. This network is a low-effort, low-risk attack vector. Most dial-up modems provide little or no access control mechanism. Even when passwords provide electronic access control mechanisms, there are no intrusion detection mechanisms, or access logs which makes it more vulnerable.

III.C FIBER OPTIC VULNERABILITIES

Fiber optics is a common communications medium that many presume to be secure, but if a person can acquire physical access to the fiber, it is easy to compromise. Fiber optics is just as vulnerable to hackers as a wired or wireless network. Networking of relays and other devices is mostly done through fiber optic cabling for connecting remotely located IEDs. Since, the fiber optic cable route may not be under much surveillance, it is also vulnerable from cyber security point of view.

IV. CHALLENGES BEFORE POWER UTILITIES

Major challenges faced by power plants and T&D utilities towards cyber security are as follows:

- Older systems and equipments at the grid/distribution end will present a key difficulty in implementing cyber security solutions by power utilities. These were installed and designed without cyber security in mind and hence are often integrated with other systems through relatively unsecured modes (including retrofits) offering loopholes for cyber attack. In certain cases, compatibility issues may also be encountered during such integration.
- Enhancing security will result in even higher volumes of data due to the encryption and decryption. To avoid congestion, additional bandwidth will be required and consequently to maintain latency more sophisticated communication systems will also be required. There is trade-off between the level of security and available financial budget.
- Issues related to cyber security for substations and distribution systems etc, the risks and possible solutions are not fully understood by in integrated manned by various power utilities involved.

V. REMEDIAL MEASURES

As discussed in earlier section that utility has limited allocated budget. Also, many of the equipments which were installed earlier don't support security features. However, there are some cost effective measures which can be taken by power utilities to cater cyber threats.

V.1 TECHNICAL MEASURES

V.1.A Identification of all communication channels in switchyards/distribution systems

The first step to mitigate risks is to identify and visually inspect all communications paths via a network diagram and physical verification of the network. It is important to find out all interconnections between systems,

SCADA links, Energy Management Systems, engineering access, even maintenance. Visual inspection is required for wireless, Internet, telephone line, or dedicated fiber connections.

V.1.B PASSWORD MANAGEMENT

All security experts agree that strong password protection is still the best defense against electronic intrusion and other forms of unauthorized access. Regardless of what other authentication mechanisms are used, a good password will not only protect equipments/relays/IEDs against unauthorized settings but also it will safeguard the integrated system and will help in reliable operation of a substation or SCADA system or Energy Management System. It is extremely important to review and maintain the security of a system by using strong passwords in protective relays, controllers, and remote access points to SCADA systems or EMS systems.All the protection and networking engineers working in switchyards or maintaining distribution systems or any person involved with the above systems should be made aware to use strong passwords and routinely changing the same. Also, multilevel password authentication schemes in all IEDs and protective relays should be implemented (e.g. see Table I).

TABLE I: MULTILEVEL PASSWORD AUTHORISATION (Typical)

Access Level	Privileges	Authentication Requirements
Maintenance Engineer	View relay Settings	Level 1 Password
Manager-Maintenance	View and Change Relay Settings	Level 1 and Level 2 Passwords
Manager – Operation group	View relay setting, Breaker Control	Level 1 and Breaker Level Password

Level of authority should be provided by the utilities for their employees looking after operation and maintenance of the switchyard or distribution systems. An attacker must compromise two independent levels to have access of critical equipment (e.g. to open or close Circuit Breaker via remote access).

V.1.C ENABLING TIME OUT FEATURES

Features of time out system in Relays/SCADA equipments or communication devices in switchyard should be enabled wherever applicable such that it will temporarily lock out the communications port after predefined failed password login attempt. In addition, whenever the substation device locks out the remote communications port, it should also disconnect any current engineering access sessions by making the modem to hang up or by terminating the connection. This action will further enhance security.

V.1.D ENCRYPTION & AUTHENTICATION

capturing and dissecting Transmission Control Protocol/Internet Protocol (TCP/IP) frames over Ethernet is a relatively simple process using free tools available from the Internet. Network switches instead of hubs can be used by power utilities for mitigating the risk of Ethernet sniffing. Modern substation security should include the use of devices that secure byte-oriented data packets, such as those found on Modbus or DNP SCADA networks, with encryption and/or authentication algorithms. Authentication of the data packets ensures the data are from a trusted source and not modified in route. Encryption not only adds greater security but also provides privacy or confidentiality of the data.These security devices do not interfere with data flow on control and/or monitoring systems, but ensure confidentiality, authentication, and integrity of the transmitted data. The modern switchyards may achieve this over a LAN through tunneling the traffic through a

Virtual Private Network (VPN) based on Internet Protocol Security (IPsec) or Secure Sockets Layer (SSL).

C. SECURING DIAL-UP CONNECTION

To secure existing dial-up or remote engineering access, a serial encryption and authentication device can be used in line with the existing computer/modem/radio/fiber communications links in older switchyards. These types of devices provide data confidentiality and integrity, as well as prevent unauthorized access with session authentication.

D. SECURE TCP/IP LINKS

More computing platforms are finding their way into the modern grid/modern substations' automation system. A variety of special-purpose encryption and authentication devices for TCP/IP communications protocols provide confidentiality, integrity, and authentication services for utility communications. Depending upon the feature sets, these devices vary in cost and complexity of use. Power utilities can procure the system depending upon their risk assessment and allocated budget.

E. COMPARTMENTALIZATION OF INFORMATION

Power utilities should include a formal process of "need to know" and compartmentalization of information. It is very important to restrict access to system details only to those who need it. To do so, security management can be considered using access models such as discretionary access control (DAC) or mandatory access control (MAC). In DAC, the owner determines who can obtain and access data. In MAC, the policy and system defines who can access or modify information. In a MAC system, subjects and objects have sensitivity labels that specify a level of trust. In order to access an object, the subject must have a sensitivity level equal to or higher than the label of the object.

F. REGULAR MONITORING OF SECURITY STATUS

Switchyard engineers must view the log files regularly to identify suspicious activity. Many substation products and IEDs contain very effective monitoring and alarming technologies that will allow detecting and reacting to various malicious activities.

F.1 DEDICATED CONTACTS FOR ALARM

Modern substation IEDs can be configured for a dedicated alarm contact that will pulse in response to an event occurring. For example, whenever there is certain no of failed login attempts in IEDs or a user attains a level that may change the settings or a user saves a new settings configuration to the device, an alarm/annunciation will be generated as information for switchyard operation and maintenance personnel.

F.2 SEQUENCE OF EVENTS

In addition, power utilities can program devices to automatically send a time-stamped Sequence of Events (SOE) record in response to a change in the relay setting or so. They can also use SOEs to monitor changes in the internal logic bits in the device, including the alarm bit, the digital inputs, and the results of user-programmed logic equations. The event-reporting mechanism in modern devices is extremely flexible but not utilized fully by the power utilities at present. It is possible in modern IEDs of grid/substations such that logics can be configured to generate an SOE report for a wide variety of conditions as user desired.

F.3 MONITORING VIA STATION LAN/ SCADA LINKS

Controlling and monitoring the communications status points via the remote SCADA link or station LAN allows the ability to control and monitor engineering access permissions from unit control room. An HMI Communications Overview screen gives remote administrators the ability to grant engineering access to each serial or Ethernet connection independently for

security and safety. This prevents unauthorized connections and validates that a user is appropriately connected to an IED. Power utilities can use the same procedure to manage and monitor the EHV breakers.

F.4 AUTOMATED EVENT MESSAGING

Power utilities can use automated event messaging system that will send real-time alarm and event notification to the concerned substation maintenance personnel via a telephone call. The event messenger turns the contents of the text into a computer-generated voice message that will inform the recipient of the nature of the detected event. The substation event messenger receives a text message and automatically dials a pre-configured telephone number to notify the authorized recipient of the event or SOE report. Also, an Ethernet transceiver can be used which captures the message and sends it to a predefined email recipient or mail group.

V.2 ADMINISTRATIVE/POLICY MEASURES

VI. CONCLUSIONS

While protection and control engineers understand the power system and operational issues of energy transmission, they rarely understand the underlying communications technologies that allow data to be collected and accessed either locally or remotely.

Though one can never completely remove the possibility of attack, but can greatly reduce the probability of a successful attack and the severity of resulting effects by applying the suggestions outlined as above. These steps will greatly improve the overall security of communications to and from a modern grid/substations and related distribution systems.

To summarize, here are the general steps to secure a modern substation: i) Generate unique policy, standards and processes as per the need of organization. ii) Conduct a risk analysis based on qualitative and quantitative assessments. iii) Identify and map all communications pathways to and from the substation. iv) Use and manage strong passwords. v) Secure all access points to protect from attacks. vi) Practice “need to know” security and compartmentalize information. Vii) Monitor security status of critical electronic access points.

REFERENCES

1. Best practices for cyber security in the electric power sector, IBM Guide
2. “Cybersecurity as part of modern subsations”, Dwight Anderson &Garret Leischner, SEL Inc.
3. “A study of indian approach towrads cyber security”, M bandey& F.A. Mir , IEEE,2012
4. IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE Standard 1402-2000, 2000