Cyber Security - Security strategy for distribution management system and security architecture considerations

Timothy R. Vittor, Sukumara T
Distribution Automation
Electrification Products Medium Voltage
ABB Inc. - USA
Lake Mary, Florida USA
timothy.r.vittor@us.abb.com sukumara.t@us.abb.com

Sudarsan SD
Corporate Research
ABB GISL Ltd. - India,
Bengaluru, India
sudarsan.sd@in.abb.com

Janne Starck
Distribution Automation
ABB Oy – Finland
Vaasa, Finland
janne.starck@fi.abb.com

***Abstract*—We cover some practices and methods in creating effective cyber security architectures for substation and distribution automation systems and products which are robust enough to withstand cyber-attacks and resilient enough to recover in the event of security compromise and keeping device functional and executing its core functionality even during attack. This is achieved by a defense-in-depth strategy starting from product design, a dedicated security test center, secure system architecture, patch management and security audits. Understanding practices and processes help in handling cyber security in a holistic manner with an explicit focus on operational performance.**

***Index Terms*— Distribution System, Security Control, Cyber Security, Critical Power Infrastructure, Defense-in-Depth.**

I. INTRODUCTION

The recent cyber-attack on the power grid in Ukraine resulted in half the homes in Ivano-Frankivsk region with a population of 1.4 million being without electricity reportedly for 6 hours. Reports say on December 23, 2015, Kyivoblenergo utility company provided public updates to customers, indicating an unauthorized intrusion that disconnected 7 transmission substations (110 kV) and 23 (35 kV) distribution substations leading to an outage for more than 80,000 customers [4].

The attack was conducted mainly through distribution SCADA system computers along with a denial of service attack to the phone systems. Computers running the SCADA HMI software and related SCADA servers, mainly based on Windows operating system, were infected using booby-trapped macro functions and malwares embedded in Microsoft Office documents. The industrial control systems used to supply power to millions of people could be infected using such a simple social-engineering ploy of tricking the users to click on attachments. In this case, the utility operators resorted to turn the system to "Manual mode" of operation in order to restore the power system back into operation.

Also another suspected cyber security incident in Ukraine reported on 19th December 2016 and this time it's on a transmission level substation.

Cyber security once considered a non-issue has gained traction and become main stream as Information Technology (IT) networks get integrated with Operational Technology (OT) networks. This is highlighted by several cyber security incidents including the one mentioned above.

Concepts such as remote configuration/parameterization, monitoring, remote SCADA communication, remote diagnostics and firmware updates are becoming important requirements for relays and control systems. This leads to inherent requirements of integration of IT and OT networks. This in turn necessitates "Availability", "Integrity" and "Confidentiality" of information and data in Substation Automation systems and Distribution Automation networks.

While electric utility systems and processes having responsibility of creating and maintaining secure power system networks consistently provided some of the highest levels of reliability and security in the world by virtue of being isolated stand-alone networks that are often proprietary which limits interoperability. Performance based standards like NERC CIP, IEC 62443, ISO 27000, EU NIS Directive require utilities and end-users to implement a comprehensive security program and submit to regular compliance audits

which makes only power utilities and other end users to be NERC CIP compliant. Vendors can provide technical features that support the utilities or end-users to be NERC CIP compliant and support utilities and end-users to know how they can optimally secure their devices by adopting best practices and also build up awareness. The key challenge is in our ability to support end users in creating a converged IT-OT network without compromising on security aspects.

II. Challenges related to Security measures for distribution system

Internet of Things (IoT) coupled with integration of IT-OT networks is changing the landscape including utilities. Utilities are currently installing large numbers of modern relays in their substations, not only to replace legacy protective relays, but also for metering and equipment monitoring. These devices provide valuable information that can be put to use to improve reliability and reduce operating costs while throwing up new cyber security challenges.

At the outset, systems are becoming cyber-physical. Isolated physical access controlled systems can now be controlled using logical access from cyber-space. Sub-station and feeder equipment like protection, automation and control relays, and smart meters are being deployed with advanced communications networks which make them more vulnerable to cyber threats. Threat landscaping and identifying threat vectors is a key challenge to be dealt with to provide appropriate logical access control mechanisms.

Modern protection and control relays/sensors are the first level intelligent devices close to primary equipment, playing a critical role in substation protection, control and monitoring functionalities. Relays being at the bottom of the hierarchical communication network having first hand access to power system, not only play the role of protection which isolates the faulty section of subsystems from the rest of grid but also play an active role in post-fault power restoration and self-healing with the help of supported communication network. Yet these systems have limited resources and hence most vulnerable in a connected world. Especially the relays in the distribution systems unlike relays placed in secured network inside substations and generation plants. For example most of the recloser relays are installed on the poles near residential neighborhoods but exchanging data to with remote substation or distribution management systems (DMS).

Security standards applicable to such relays like NERC CIP, IEC 62351, and ISO 27000 etc. are still evolving. Gaps in these standards from cyber security perspective are being continuously understood and addressed. Even when identified issues are addressed, their adoption takes time.

Moving from controlled intranet to open IT-OT networks cannot always guarantee things like timely delivery, reliability, and access control. Even with no malicious intent, being not able to deliver payloads within time limits can bring down services. Malicious intent adds to the complication. Integration of IT-OT networks, at once changes the traditional prioritization between confidentiality, integrity & availability.

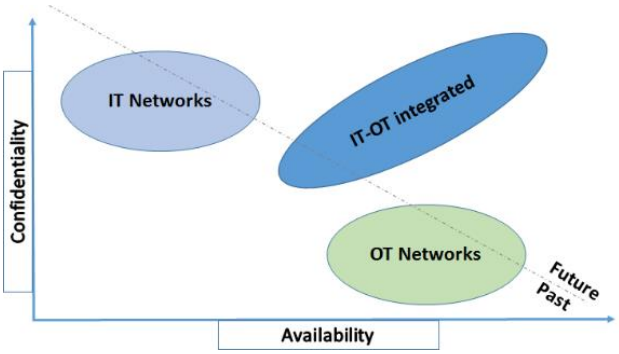

Figure 1: Confidentiality vs Availability prioritization in different networks

In fact, IT networks prioritize confidentiality over availability while in OT networks availability is paramount over confidentiality. Once integrated, we need mechanisms that support both confidentiality and availability in equal footing as shown in *figure 1*.

III. Stanadardization and its impact on power system

The cyber security standards for power system domain are continuously evolving. Many standardization activities are on-going and cyber security groups are set-up to strengthen security capabilities of critical power infrastructure, e.g., IEC 62351, NERC CIP regulations, IEEE 1686, National Institute of Standards and Technology (NIST) 7628 Guidelines for Smart Grid Cybersecurity, Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), ISO 27000, EU NIS Directive etc. Part of these standards define the cyber security capabilities to be adapted by relays in the substation and distribution systems. These standards also enable utilities effectively and consistently evaluate and benchmark cyber security capabilities of the system/ devices.

As per NERC CIP V6 the first step in any security program is the development of a security policy that forms the basis for any technical, procedural, or organizational security mechanism. Creating, communicating, and enforcing a security policy is a mandated management's responsibility. The next step is to build in processes to help establish and enforce the security policy which include a documented plan for employee hiring & separation, incident handling and disaster recovery.

Though NERC CIP (CIP-002) stresses on bulk electric system covering mostly transmission, sub-transmission, large control centers as high critical cyber assets to be protected for the reliable power system operation, many times a cyber-attack on connected distribution system would have cascading effect resulting massive impact on the power system reliability.

IV. Managing System Resources: Security Vs Performance

The core function of relays is executing protection and control algorithms, with other functions, e.g., SCADA communication, tool interface etc. being support ones.

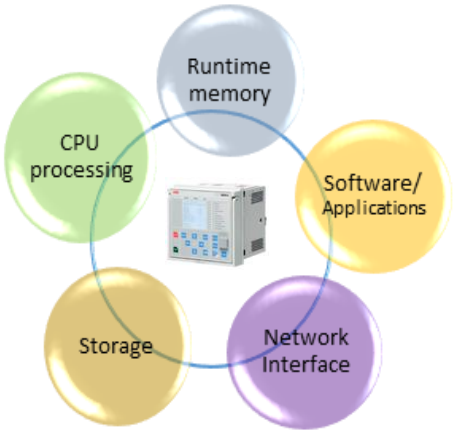

Figure 2: Constituents or resources of a typical Protection and Control relay architecture

Resource consumption by support functions like processing power and memory are concerns that should be addressed by appropriate architecture as in *figure 2* by assigning highest priority to protection modules. Hacking attempts like Denial of Service, fuzzing, eavesdropping, spoofing, man-in-the-middle, malformed packets sent through SCADA protocols etc. should not affect the core protection and control algorithm execution.

The relay architecture design needs to assign highest priority to its core protection functions to ensure that the relay is functional and is executing its core protection functionality during the attack period while other functions may recover at a later time.

Relay manufacturer need to test this behavior and its ability to maintain proper operation extensively through cyber security evaluation tests as part of device robustness test. These tests to be carried out preferably during product development life cycle and mandatorily before release. Observed vulnerabilities should be addressed appropriately.

Our experiences show that, the focus on vulnerability assessment or threat modeling and robustness testing done using a combination of proven commercial, open-source and proprietary security tools in a dedicated device security assurance center during product development and release cycles helps in creating robust device architecture.

V. Defense-in-depth Approach

Cyber security threats can be either Internal (insider with possible privileged access) or External, both capable of causing huge damage to the power system.

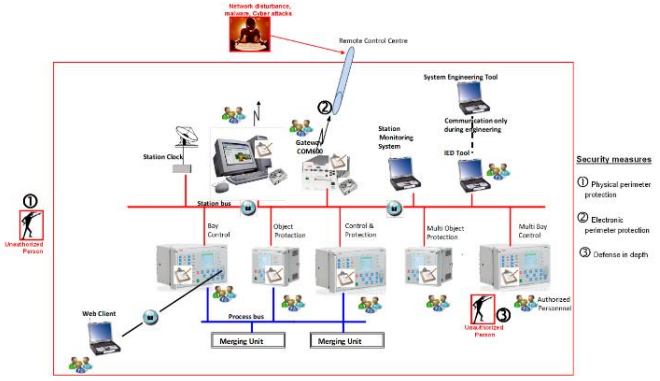

Figure 3: A typical substation automation setup with security mechanisms

The most important principle for any security architecture is defense-in-depth with several layers to avoid single point of failure. At the least, the most sensitive parts of the system are to be protected by multiple rings of defense as in the *figure 3* [1]. In addition to protection mechanisms, means of detecting attacks including both technical measures, such as intrusion detection systems, as well as procedural measures, such as review of log files or access rights are required.

VI. Security Control Measures for Power Distribution System

Cyber security architecture of a substation and devices in the sub-station or power distribution system should have following security considerations along with strong security polices as a part of defense-in-depth approach to support the overall security posture of the device/system: Physical Security, Access Management, Audit Trail, Network Separation, Communication Security, System Hardening, Application Security, Secure Storage.

A. Physical Security

Physical perimeter protection is a critical requirement in the line of defense for cyber security. NERC CIP-006 requires operational or procedural controls to restrict physical access definitions. Physical protection includes setting up physical boundaries, e.g. a fence, a closed control house, locked cabinets, or installing video cameras for monitoring purposes. A tight security management, with up-to-date asset registers, regular site surveys and audits can help identify rogue devices, personnel and give an early warning of intrusion attempts.

B. Access Management

An important security principle to follow is the principle of "least privileges". RBAC (Role based Access Control) principle needs to be adopted in providing right person with right privileges to operate/work on substation operation and control. No user or process should be able to do more in the system than what is needed for a given job and role. This principle helps prevent malicious attacks and accidents. Devices should enforce minimum password complexity and password protection mechanism.

NERC CIP (CIP-005) Electronic Perimeter Security requires monitoring and updation of access management credentials on continuous basis. The relay shall be able to detect and alert for the attempts at of or actual unauthorized accesses and provide access log for review.

C. Audit trail

Logs record events and enable monitoring of the operations. Protection and control relays in power transmission and distribution systems must have capability to record user activities associated with relay configuration, monitoring and control, as per NERC CIP (CIP-007), including failed login/logout, object access, configuration change, control operation like breaker closing and opening and administrative tasks. Also the EU NIS Directive is primarily focusing on the obligation for Critical Infrastructure to report cyber security incidents making security event logging particularly relevant. The audit trail can be used to:

- Review security-critical events
- Discover attempts to bypass security mechanisms
- Track usage of privileges by users
- Provide a deterrent against attempted attacks
- Perform forensic analysis

D. Network separation

Network should be divided into different zones depending on the criticality of the nodes within each zone. In a typical substation automation environment, separation could be based on bay and station level devices and computers depending on the size of the substation. Zones should be separated by appropriate security mechanisms.

The substation network must be separated from any external network. To authenticate accessing entities, the combination of a firewall with a VPN (virtual private network) gateway is a good option. A more secure architecture is to work with DMZ (demilitarized zone); a zone that serves as a proxy between external networks and the control system. The single electronic security perimeter required by NERC CIP will often not be enough and is a good example of why security for compliance sake is not sufficient. Security zones that separate systems based on their communication and protection needs minimizes security risks and provides defense-in-depth architecture.

E. Secure communications

Using Internet of Things (IoT) technology to retrieve the data and provide information for decision making through advanced analytics can help utilities in improving operation efficiency of power system network.

IoT based concepts like Microsoft's Azure, “ABB Ability”, support advanced analytics of data gathered through networked devices and sensors.

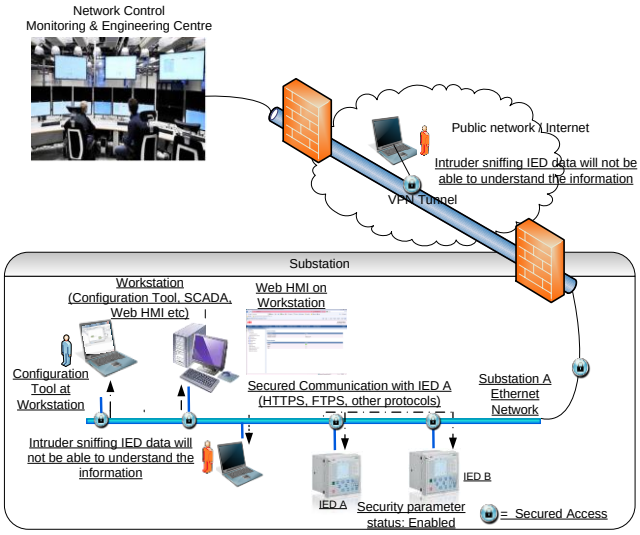

Figure 4: Secure communication through Public Network

E.g., IoT based “ABB Ability” concept is being used for monitoring 20,000 substation transformers and breakers in the network of American Electric Power with an Asset Health Center to analyze asset health, recommend maintenance actions and prioritize replacements [5]. Key factor here is to secure transfer of information or data to remote control and monitoring centers.

The main idea of secure communication is to create a secure channel over an unsecure network. This ensures protection from eavesdroppers and man-in-the-middle attacks by using appropriate cipher suites and trusted digital certificates. As in *figure 4*, for external connections, use of VPN is recommended for both operational, maintenance and engineering connections [2].

F. System hardening & Robustness

Relying on network separation and protected/secured communication is to be augmented by protecting each individual system component that includes system hardening. As in NERC CIP (CIP-007), every single device or computer within the substation must be hardened to minimize its attack surface. As in *figure 5*, hardening includes restricting applications, open ports and services to an absolute minimum with least privilege principle. This step is best done from vendors provided information on necessary ports or applications for normal operations, as well as security hardening guidelines for their products and systems.

Harden the system by removing or deactivating all unused processes, communication ports and services. It should be possible to open or close all physical ports dedicated for station bus communication in relay configuration. The relay manufacturer must mention in a cyber security deployment guideline or document, the IP ports which are opened by default as part of factory configuration and other ports available for configuration in order to set-up IP firewall for the station gateway.

Figure 5: General System hardening and robustness test process

System hardening is a continuous activity that starts from installation, commissioning, and during its life time. While system level vendors can at best provide some guidelines, it is the responsibility of the plant owner to decide security mechanisms and appropriate level of hardening. Services like finger printing and patch management as well as vulnerability assessment and penetration testing are key. Robustness of the communication protocol need to be tested. A robust implementation allows the device to recover from attacks. E.g., if a protocol is not implemented as per RFC, then the device may fail or restart when specific packet sequence is not followed. Robustness testing and analysis identifies such cases and forces the device manufacturer to fix these issues before offering it to the customer. While robustness may not be able to stop cyber-attacks due to lack of authentication and crypto mechanisms in the protocols themselves, it does ensure recovery post attack. This increases the availability of the device which is the primary need in OT environment.

G. Application Security

SCADA system in the substation includes relays, gateways and HMIs which use many custom and generic applications, databases etc. to receive, store and process the information for the decision making. Applications like web servers, event handlers, fault data recorders etc. communicate and exchange data with other parts of the system or with external programs or users. These applications must perform proper data validation before exchanging the information. Applications should use proper defenses to prevent any kind of cyber-attack or hacking to prevent or limit information leakage. Robustness analysis of the applications are as valid as the communication robustness analysis.

H. Security Storage & portable media

Securing sensitive data and operational information is necessary, and relevant files are to be encrypted. An alternative to this would be applying strict access control and generating alerts when this data is accessed.

Besides static connections between the substation and external networks there exists temporary, indirect connections, e.g., mobile devices connected to relay/computer, that are often overlooked when securing substation systems.

VII. PATCH MANAGEMENT AND HANDLING FIRMWARE UPDATES

Cyber security updates and software improvements drive relay manufacturers to release firmware updates occasionally if not regularly.

Firmware patch management is usually a cumbersome effort for the relay manufacturers as well as utilities. Relays are pure embedded devices with a life cycle of 20 years. Once in service on critical feeder or primary equipment, it's very difficult to obtain shutdown in order to update firmware at customer site/field. Also it's very important to retain or restore the customer's own customized configuration and protection settings after the completion of firmware update process.

For remote firmware update, prerequisite is that communication link must be secured. Updates on the relays installed on the fields may have to be done through dial-up connections over VPN links.

VIII. SECURITY CONSIDERATIONS FOR RELAYS CONNECTED VIA WIRELESS

In distribution automation, many times relays like recloser protection and feeder protection relays are outside in the field mounted on a pole or fitted in field marshalling boxes connected to main substation through wireless media. Only secure wireless communication with appropriate configuration is to be used as wireless traffic can be easily intercepted and manipulated by attackers.

Access points should be positioned and arranged such that the useful signal strength is limited as far as possible to within the physically secured perimeter, e.g. by use of directional antennas. Since wireless communication can be jammed, the overall system should be designed to react safely to loss of any wireless connection. In case of cyber-attacks relays still be able to perform its core protection functions and recovers back its communication capability as soon attack vectors diminished also the secure log events need to be generated to provide clue about the security breaching incidents.

IX. CONCLUSION

Cyber security environment is very dynamic. Relays and SCADA systems are key elements in the distributed power system network. In order to reap the benefits promised by the Smart Grid, continuous improvements are needed for these devices and systems to be secure.

The security architecture in the relays need to evolve continuously to keep power system network robust to handle cyber security threats effectively. We need to ensure that modern communications technology can continue to be used to retrieve the data provided by the thousands of relays in the power system network. It is always essential to do robustness analysis to ensure recovery from attacks and increase

availability. It is important to adapt secure product development practices including security assessment in order to create robust device architecture. The defense-in-depth principle demands protecting each individual system component in the power system network.

REFERENCES

[1] Markus Braendle, Steven A. Kunsman, "White paper Balancing the Demands of Reliability and Security Cyber Security for substation Automation, Protection and Control Systems", *Cyber Security ABB White Paper*.

[2] Sukumara T, Janne Starck,, Kishan SG, Harish G, Eashwar Kumar, , "Cyber Security – Secure Communication design for protection and control IEDs in sub-station", *in Proc. 2013 CIGRE D2 Colloquium, Mysore.*

[3] Sukumara T, Eashwar Kumar, Niko Lehtonen, Janne Starck, Fabrizio Commuzi, "Handling Cyber security updates for protection and control IEDs in substation during product's life cycle", *in Proc. 2015, CIRED 23rd International Conference on Electricity Distribution , Lyon, France, 15-18 June 2015*

[4] SANS ICS, *"Confirmation of a Coordinated Attack on the Ukrainian Power Grid"*, https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[5] ABB drives the Internet of Things and People, http://new.abb.com/docs/librariesprovider138/Hannover-Messe-2016/iotsp_positioing_en_1.pdf?sfvrsn=4