Practical Considerations for Security

Steven Hodder
GE Digital Energy, Multilin

1. Introduction

This paper has been prepared to outline some practical security strategies for protection & control engineers that can be adopted quickly and considerations when designing and implementing communications access to protection and control systems. The intention of this paper is not to provide a detailed explanation of NERC Critical Infrastructure Protection (CIP) standards, as this is discussed in several already-published works. Nor is the intent to provide a detailed treatise on the finer details in configuring the various facets of network security.

2. Drivers for Cyber Security

A number of world events in recent years has put critical infrastructure in the spotlight, and highlighted the need to adequately protect these systems from intentional and accidental interruption.

- The attacks on September 11th, 2001 changed the way North Americans viewed terrorism – the world became a very scary, dangerous place. A great deal of concern arose over the safety of key infrastructure in North America, including gas pipelines, transportation, water and electricity against similar terrorist attacks.
- The August 14th, 2003 Northeast blackout, along with several other high-profile outages, heightened awareness of the importance of the bulk electrical system, and provided a powerful illustration of the financial and societal impacts of a large-scale interruption of the electrical infrastructure.

The increased public and governmental concern over the safety, security and availability of critical infrastructure lead to the creation of a number of regulations regarding the identification, prioritization and protection of critical infrastructure .

3. What's all this "CIP" Stuff, Anyhow?

The North American Electric Reliability Corporation (NERC) has developed eight Critical Infrastructure Protection (CIP) standards (CIP-002 to CIP-009), covering the identification, protection, management, incident reporting and recovery for critical electronic systems for the bulk electrical system.

CIP-002	Critical Cyber Assets	Identification & enumeration of Critical Cyber Assets
CIP-003	Security Management Controls	Development of cyber security policy (incl. Auditing)
CIP-004	Personnel & Training	Background checks, regular training on security policy
CIP-005	Electronic Security	Electronic Security Perimeter & Access Controls
CIP-006	Physical Security	Physical Security Perimeter & Access Controls
CIP-007	Systems Security Management	Controls to Detect/Deter/Prevent Compromise
CIP-008	Incident Reporting	Incident Identification, Classification & Reporting
CIP-009	Recovery Plans	Restoration of Critical Cyber Assets once compromised

It is important to note that all of the above NERC standards are procedural in nature – they describe the 'What' and the 'Why', but they do not, other than in general terms, describe the 'How'. The end result is often

4. Cyber Security: Exactly What is it?

According to NERC CIP standards, so-called Critical Cyber Assets (CCAs) are defined as:

Critical Cyber Assets: any programmable electronic devices or communication networks that if damaged or otherwise made unavailable may impact the safe and reliable operation of the associated bulk electricity system.

The impact of this definition is fairly far-reaching in the world of Protection & Control. Effectively, this definition applies to protective relays and RTUs, local and remote HMI computers, and the communications infrastructure that connects them where remote access using routable protocols is used. The communications networks involved may include (but of course, not be limited to) local so-called Station Bus LANs as well as IEC 61850 Process Bus LANs where actively switched networks are involved.

So what exactly does this mean to the average Protection & Control engineer? What has changed to make the handling of P&C systems different from what was historically done? The principle answer to this question is simple: access.

Historically, electromechanical and static relays did not offer any digital communications interfaces and consequently there were

no means to access and modify these devices remotely. Any changes, including removing protection from service, required staff to be physically present within the station, standing directly in front of the device(s) involved. There was no operational (i.e. real-time values) or non-operational (i.e. historical, SOE, fault record) data within the protection devices so there was no driver to communicate with these relays.

With the introduction of digital relays, particularly more modern micro-processor based relays, there is an ever-increasing demand to provide communications access to these devices. Modern digital relays can provide real-time values and control for SCADA applications, non-operational data for fault and system disturbance analysis and the ability to interrogate (and potentially change) settings remotely via advanced communications protocols and interfaces. Therein lies the issue – remote access, if incorrectly provisioned and secured, may present a channel for malicious or unintentional disruptions to be caused on the power system.

Let us consider a very simple system as shown in Figure 1.

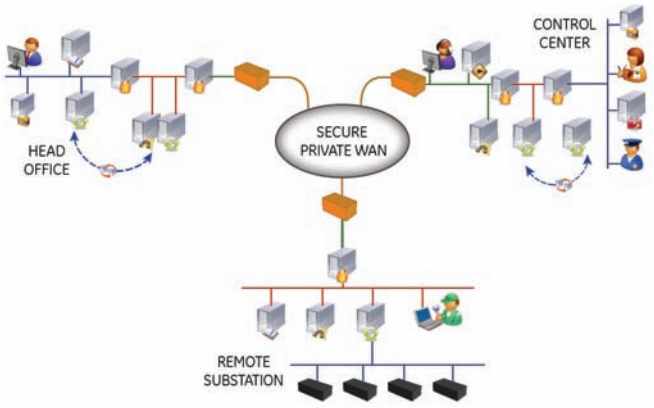

Figure 1.
Simple system with remote access

Here we have a single substation being accessed remotely from two separate locations: a Head Office location and a Control/ Operating center. Each location has different users each with different user requirements. Access is provided via a secure private LAN (such as SONET or VPN).

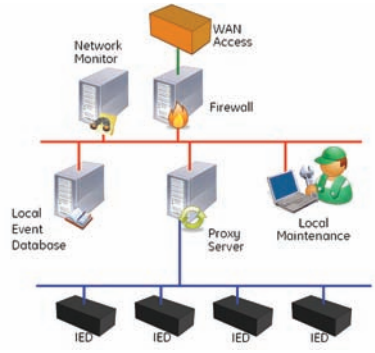

Figure 2.
Remote Substation

The Remote Substation consists of the following functions:

- A single point of access to the outside world (WAN Access), providing connections to external users. This WAN access may be channels within a SONET multiplexer or a VPN connection to an external network.
- A Firewall function that provides additional filtering of traffic between the external world and the secure network within the station.
- A Network Traffic Monitor, that examines network traffic generated locally and entering from the external network
- A Proxy Server, that mirrors the data generated and functions provided by the IEDs to the outside world to external users.
- A Local Event Server that automatically gathers events from all of the devices within the network, including relays and the Network Monitor, stores them locally and also provides for automated transfer to centralized event databases.

While these functions are shown as individual functions, often several may be merged into a single network appliance. For example, VPN access, firewall functions and network traffic monitoring may be involved into a single network appliance. Similarly, the event log and proxy server may be merged into a single device on the network.

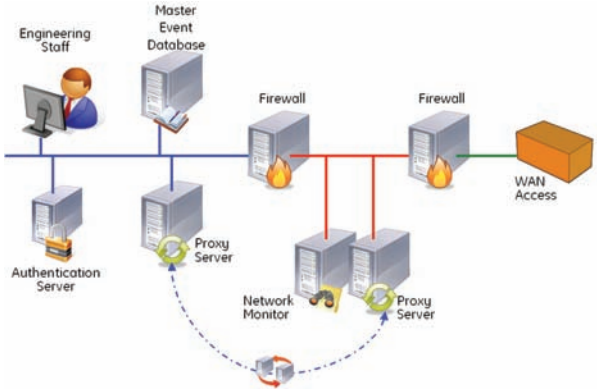

Figure 3.
Head Office

The Head Office system shares several functions with the Remote Substation, and adds several new functions.

- Two firewalls are set-up back-to-back, creating a specialized network known as a Demilitarized Zone (DMZ). This architecture is extremely common in the IT world where access is provided to common resources for both internal/ secure and external/insecure networks.
- Two proxy servers are provided, one within the DMZ and one residing on the office network. Data is mirrored on the proxy residing on the office network from the proxy residing in the DMZ and users on the office network access data on the local office network proxy only. Similarly, data is mirrored onto a Centralized Event Database for user access.
- The process of data mirroring is provided completely autonomously between the proxy servers (both at head office and at remote substations) with no human access required using Machine-to-Machine (M2M) transfer.

- A network monitor is provided within the DMZ to detect unauthorized traffic. If unexpected traffic on the DMZ is detected, then alarms/logs are generated. In general the only expected traffic on the DMZ will be:
  - M2M data coming from remote proxy servers destined for the DMZ proxy via the External Network firewall.
  - M2M data coming from DMZ proxy server destined for the office proxy and central event database via the Internal Network firewall.
  - Administrative traffic on the DMZ for configuration & monitoring of the network resources including the traffic monitor.
- A centralized Authentication Server allows users to prove their identity against the centralized user management database in order to gain access to the proxy and centralized event database.

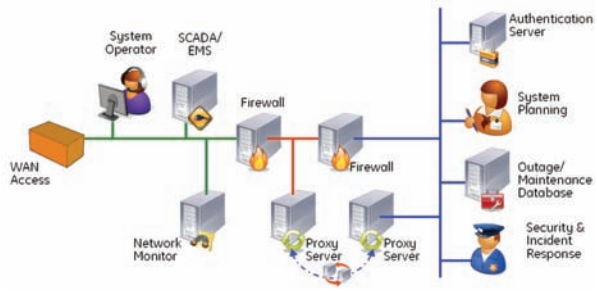

Figure 4.
Control Center

Finally, the control center again shares several functions with the Remote Substation and Head Office systems, with some new additions.

- The Primary Energy Management System (EMS) or SCADA system is provided in a dedicated, secured network connected to the secure WAN.
- Security and Incident Response, acting on incidents detected by the various network monitoring systems to detect and remediate unauthorized network access.

5. Cyber Security: Zones of Protection

Perhaps the best way to introduce cyber security is to provide an analogy to concepts that P&C engineers are already familiar with: zones of protection. In the power system, we provision protection for primary power system apparatus in zones encircling each power system element we wish to protect. Each zone is typically bound by measurement devices (current transformers) and there are isolators (circuit breakers) within the zone, typically just inside the measurement devices, to disconnect the primary apparatus from the rest of the power system in the event of a fault. So far, so good – but how does this relate to cyber security?

An analogy can be drawn between power system protection and the provisioning of zones of protection, and network system protection.

6. Defence-In-Depth

In the realm of cyber security, it is often common to refer to the concept of Defence-in-Depth, and perhaps the best way to describe this concept is to relate it back to the previous discussion on zones of protection.

We have within each network monitoring functions that monitor the flow of data from one system or device to another. These network monitors detect unusual network traffic patterns and generate signals in the event of illicit network access. These monitoring functions are often referred to as Intrusion Detection Systems (IDS) and are analogous to instrument transformers and protective relaying used to detect abnormal power system conditions.

The next step in the protection is to isolate devices or networks that are generating the illicit traffic based on signals from the IDS. The actions taken may include throttling down or turning off network ports, blocking access from specific addresses or forcing a reconfiguration of certain network resources to "hide" from external parties. These functions are commonly referred to as Intrusion Prevention Systems (IPS) and are analogous to the isolators (circuit breakers) in the power system used to isolate faulted portions of the power system to protect the remaining system.

If we take our overall simplified system shown in Figure 1, then consider the "zones of protection" shown in the following figures, beginning with the Remote Substation. There are a number of individual zones of protection for each location.

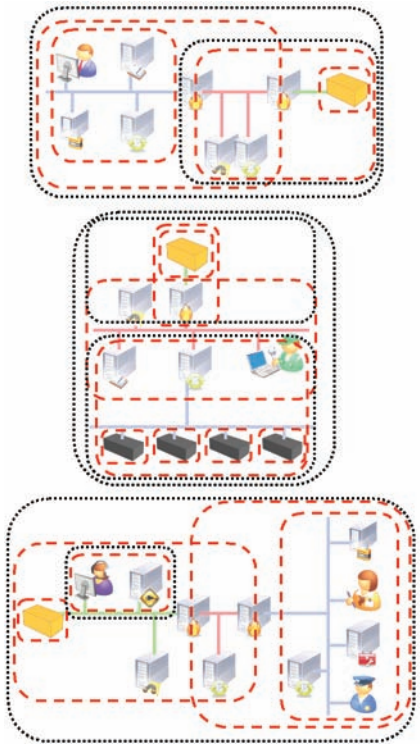

Figure 5.
Electronic Security Perimeters

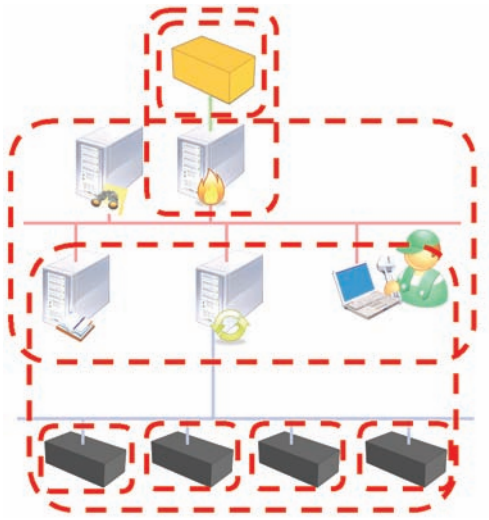

Figure 6.
Remote Substations ESPs

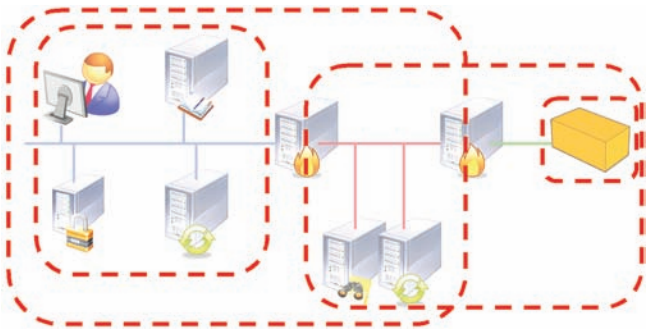

Figure 7.
Head Office ESPs

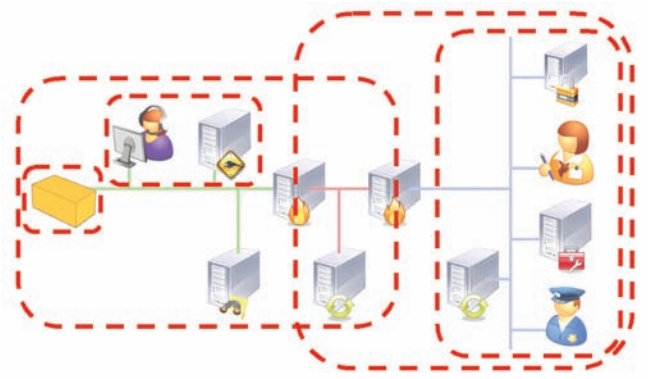

Figure 8.
Control Center ESPs

In each case, the system has overlapping "zones of electronic security", bounded by so-called Electronic Security Perimeters (ESPs). The concept of Defence-in-Depth refers to architectures that overlay several zones of protection. As can be seen, the overlapping of ESPs is very similar to the concept of overlapping zones of protection in protective relaying.

This Defence-in-Depth is an extremely key concept. Much like protective relaying, where occasionally blind spots exist, there are situations where complete security can not be provided within a single given device – however this does not mean that the device itself is unusable because it is insecure. It simply means that the electronic security "blind-spot" must be addressed by a higher-order network system.

In reality, it is advantageous in critical P&C systems to provide a significant portion of the security functionality in higher order network systems. Once commissioned, it is often impractical or risky to make changes to the in-service protective relaying. However, security is a very organic process that is constantly evolving. Users are frequently added or removed as staffing changes. New vulnerabilities are identified daily and fixes to address these vulnerabilities are released as frequently. Rather than making these continuous changes to critical P&C systems, these changes are made to higher order systems leaving P&C devices alone to perform their purpose.

7. Final Thoughts and Comments

This paper has presented some high-level concepts and discussions on the concepts of security in the context of P&C systems. It is not intended to be prescriptive to users, but rather raise issues for consideration and discussion when developing and providing security to comply with NERC CIP requirements.

Some final thoughts for consideration on the topic of security:

- The single largest threat to electricity infrastructure will likely be a direct physical attack on key generation and transmission assets. These assets are prime targets because:
    - They are large, easily identifiable targets that are typically located in remote areas (NIMBY principle) and in general, transmission stations are largely unmanned and poorly monitored (if monitored at all). This makes them ideal low-risk targets for malicious physical attacks.
    - The destruction and loss of key transmission infrastructure has an immediate and long-lasting impact on the bulk power system. Even if the fleet of generation remains completely in tact, insufficient transmission capacity will bottleneck or strand this generation capacity rendering it partially or completely unusable. Generation requires transmission infrastructure; electricity cannot be sent via courier.
    - Large power apparatus have extremely long lead times with very few vendors globally. This, coupled with the lack of common industry-wide specifications for key transmission assets like power transformers means there is a limited set of universal spares so that a physical attack will have an immediate, and long-lasting effect, on the power system.

- Secure remote access and security at the network layer is a well-understood issue within the general telecommunications industry at large. There exist a number of broadly accepted and thoroughly tested technology solutions for secure remote access, encryption, authentication, intrusion detection and prevention. Therefore, it is not advisable to "reinvent the wheel" when securing remote access, but rather judiciously apply existing best practices from the network communications industry.

- While adopting and implementing a solution, it is important to keep in mind the requirements of all users, not just one particular group. Different users will have different requirements and a security solution should not prevent legitimate users from having necessary access. Conversely, the business needs for remote access for each user group should be reviewed and justified – is direct remote access fundamentally required or can the data be provided by other means? Can data be mirrored securely to allow users to perform their necessary functions?

- To the maximum extent possible, critical protection, control and automation traffic should be carried over dedicated communication systems that are under direct administration of the controlling authority.

    - For example, within a generating station the control and automation network may be provisioned over a dedicated internal SONET network with user access only within the plant control room. While this may be an expensive option, it will also likely be the most secure method of providing access. In engineering, there is no such thing as a shortage, only a shortage at a price.

- Where connections between critical/secure and non-critical/less secure networks is made, multiple layers of security should be provided according to industry best practices.

    - De-Militarized Zones (DMZs)

    - Firewalls

    - Proxy Servers, including M2M (Machine-to-Machine) Proxies

- Advanced digital relays have a number of security features in the latest versions of firmware, including local and remote user passwords, remote user access supervision and security logging. It is recommended that users:

    - As part of CCA identification, include the specific version of relay firmware installed. Compare the firmware versions as-installed against the latest firmware version available, particularly with respect to new security features. Where needed, develop deployment plans to upgrade the firmware in those relays, starting with those CCAs that are designated as highly critical.

    - Enable and use existing security features within digital relays, particularly where these features have been disabled or left with default values:

        - Change passwords from defaults

        - Provide separate access passwords for local and remote access

        - Force the use of additional access controls for setting access

        - Provide routine auditing of changes to relay settings and commands executed through the relay. Where possible, invest in infrastructure to automate the collection, concatenation, reporting and archiving of security event data.

- Ensure that security-related alarms and events are communicated as part of a security monitoring system and included in the relay SOE record, and that the records for each relay SOE is downloaded automatically and mirrored in a central database to prevent loss of security event information.

    - Alarms should include excessive invalid password attempts made to the relay, local relay setting access granted, remote relay setting access granted.

        - Integrate alarms with outage and/or maintenance scheduling systems to detect if setting access is granted to a relay but no outage or work has been scheduled.

    - Develop expert algorithms to digest and analyze relay event data to look for patterns in events.

        - Crosschecking with maintenance scheduling and outage management systems/databases.

        - Crosschecking with standard network monitoring applications and logs (traffic pattern analysis, anomalous network traffic detection).

- There is no "magic bullet" for cyber security – security is as much an organizational/procedural activity as it is a single technology solution. The only way to provide true security is to implement Defence-in-Depth security.

8. References

[1] Homeland Security Presidential Directive/Hspd-7: Critical Infrastructure Identification, Prioiritization, and Protection.

[2] A Shortage of Engineers: A Novel. R. Grossbach. St. Martins Press 2001.