http:d2cigre.org

CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2015 Colloquium
October 15 to 16, 2015
Lima – PERU

D2-03_07

Building cyber resilience in EPUs IP networks

By

Lhoussain Lhassani*
Stedin
The Netherlands

SUMMARY

Almost every Electric Power Utility (EPU) is nowadays using modern networks based on Ethernet and IP (Internet Protocol). Those operational networks support different business needs. They are still growing and so are the needs. They connect different applications, locations and even external companies. Part of those needs concerns Operational Technology (OT), used to monitor and manage generation, transportation and distribution of electricity. The networks are meant for real time applications and are part of the critical infrastructures. We see at the same time serious growth in activities within the hack community. This means that EPUs has to deal continuously with new risks and to build a robust network and systems. In this paper we will describe an approach to the needed cyber security architecture to build a future proof resilient OT environment. It is based on best practices and is aligned with Operational Networks and related systems.

KEYWORDS

Security in Depth, IEC-62443/ISA99, Hardening, Whitelisting, Zoning, Access Control, AAA, Patch management, 'Militarized Zone', Disaster Recovery.

(*) Mail: Lhoussain.Lhassani@stedin.net

1. Introduction

Many EPUs are deploying new IP networks or expanding existing ones. Requirement of modern networks are becoming stringent, particularly when it comes to deliver continue and critical services. We will describe some best practices to enhance security of those services and reduce the risks by creating resilient networks.

2. Network services

Internet Protocol based networks are more and more used; native IP and sometimes on top of PDH/SDH.

These IP networks are growing vast and have to support more and more services as we can see on Figure 1.

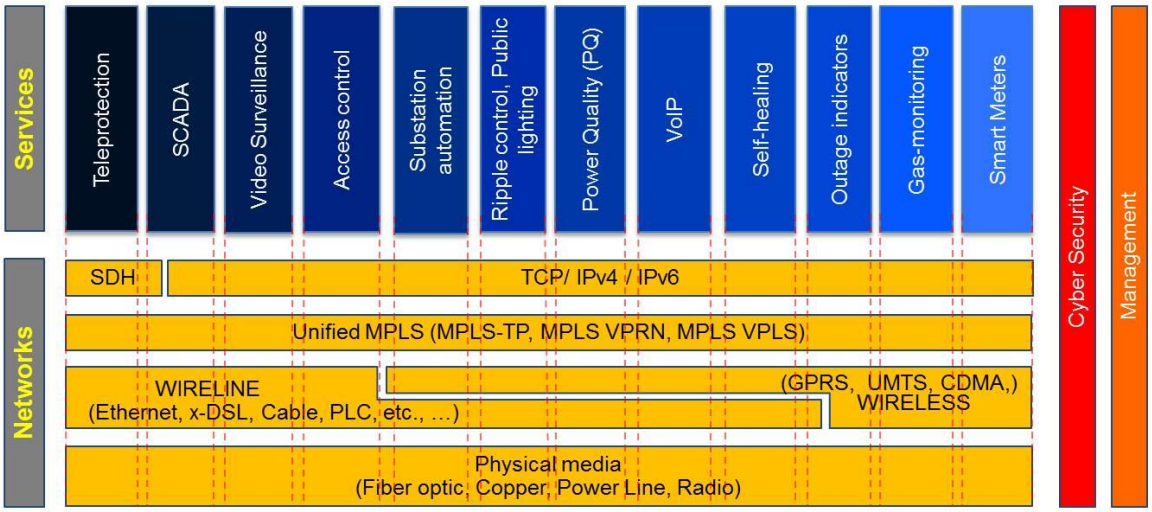

Figure 1: Examples of services and used media and protocols

Most of services are transported on the same IP network. Knowledge of the supported processes as well as an overview of the end to end communication are necessary to design, deploy and maintain those services, particularly in case of troubleshooting of a major incident.

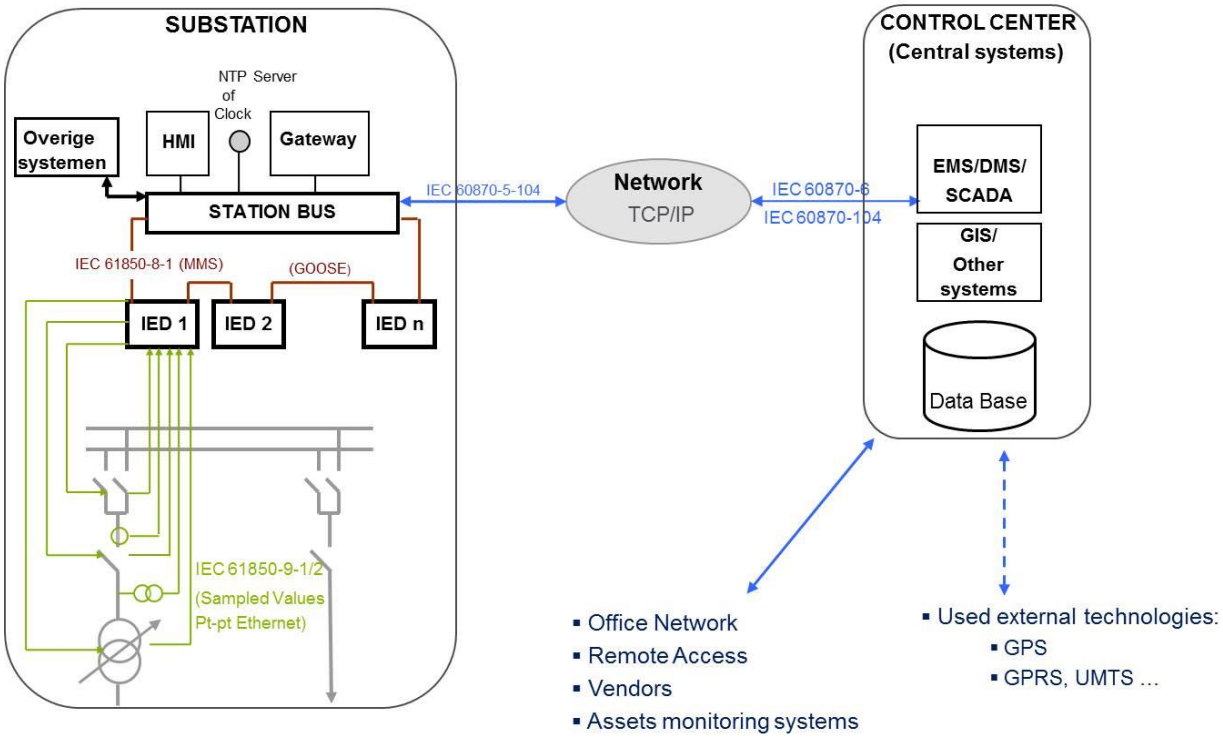

Figure 2: Topology of a simple SCADA – Substation network

3. Securing Network Services

Building resilience in the network or in some critical parts of it including the systems means building enough flexibility in the network infrastructure and systems. This to minimize the impact of possible major incidents and also to recover quickly.

Definition: *"Cyber resilience is the ability to minimize successful attacks and to recover quickly when breaches are suffered"*

3.1 Evolution in a hostile environment

In the past the networks were isolated from outside world. Nowadays we see many external connections.

- Office network
- Remote access for vendors and support staff
- Connections with other TSOs, DSOs …
- Mobile devices (Technical notebooks, tablets , Smartphones)
- USB devices, CDs, DVDs,..

Those connections can be a source of malware attack and their security has to be addressed.

3.2 Building redundancy

Depending on the ambition of the EPU and its budget, it is possible to deploy a redundant environment based on:

- Technology:
  - Interconnections: LAN/WAN
  - Systems
  - Location (datacenters)
  - Capacity

    - Protocols: Routing, Spanning Tree, PRP, MPLS
- Processes
    - Policies & Procedures
    - Disaster recovery
    - Recovery Strategy:
        - Safety
        - Minimizing the damages
        - Fast return to minimal operations
- Organization:
    - Skilled staff
    - Emergency communication (Digital, Voice)

3.3 Securing communication

The network communication has to be actively secured and monitored. The management processes has to be clearly defined and controlled. ITIL gives some good guidelines to their description and implementation. Aspects to take in account:

- Documentation and management processes
    - Network Inventory / Configuration database (CMDB)
    - Used applications
    - Network traffic / Used protocols
    - Logging/ Forensics
    - Base Line: What is normal
    - Network visibility: Monitoring (SIEM, Netflow …)
- Technology
    - How secure are your Tokens, firewall …
    - Use Data Diode / 'Hard wired' Firewalls
    - Encrypt network traffic
    - Encrypt media (USB and mobile devices)

4. Security Architecture

Security architecture receives more and more attention, particularly some industrial norms and guidelines such as IEC-62443, OLF-104 and 110.

Most companies use the IEC-2700 norm as a base for their office security policy. This norm has been extended to cover dedicated groups such as 27019 (Utilities) and the 27011 (Telecommunication).

The next sections will describe different methods to enhance resilience.

4.1 Zoning networks: IEC-62443/ISA-99

One of the most useful security concepts is to divide the network is small zones or compartments. Infection on one zone is limited to this zone. The rest is protected. This concept is based on the concepts of:

- Security zones: "Grouping of logical or physical assets that share common security requirements"
- Conduit: "A conduit is a path for the flow of data between two zones."

As described above, most EPUs have a network supporting many services and deployed widely. Besides that is getting complex. The approach of this norm suits such cases and offer the needed solution.

4.2 Security in Depth

Security in Depth introduces the concept of security in the form of different layers of security around what we want to protect (data, system or physical asset) A breach in one layer is protected by other layers of security. This is similar to physical security

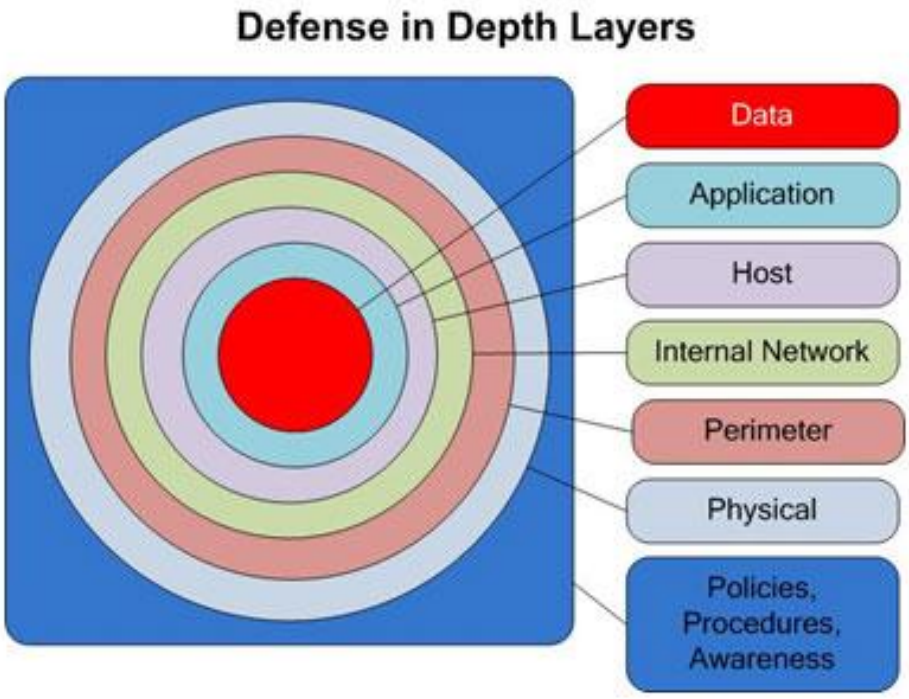

Figure 3: Security in Depth [Source: Microsoft.com]

4.3 Hardening

Most of the used OT devices (routers, switches, HMI, servers, etc.) has a multitude of unneeded ports or services. They have to be removed or explicitly disabled.

- Hardware: Physically disable unnecessary ports: Ethernet, USBs, serial ports …
- Software: Remove/disable:
  - All unnecessary services
  - Games, Media player, picture viewers, Web servers
  - NetBIOS, SMB …
- Check hardening after each upgrade or patch.

4.4 Patching

Several vulnerabilities are daily discovered and misused. OT systems are designed for their functionality and not always for security. That is the raison they are in general not so secure.

Discovered vulnerabilities get resolved by the use of a patches delivered by the vendor. They have to be implemented. This process is not well implemented within the most EPUs because of its possible impact. Besides that some systems have to remain up and running. There is not possibility to patch and test them. Nevertheless we have to find a way to deal with this requirement.

4.5 Whitelisting

The existing defense is based on blocking the unwanted: blacklisting. The method of whitelisting permits just what we want. This means we have to explicitly pre-define the needed programs for each group of users or devices such as HMIs, servers, notebooks etc. There are nowadays more and more tools to help deploying whitelisting.

4.6 Access Control

Access to all systems and data within OT has to be controlled. It is based on Authentication, Authorization & Accounting (AAA) and has to meet the following principles:

- Role-Based Access Controls
- Least Privilege
- Separation of Duties

4.7 Consider OT as 'Militarized Zone'

Most of the breaches are caused by human intervention, for example when clicking on a spam mail. To minimize those risks and to better secure our OT environment, we have to consider it as a 'Militarized Zone', a zone with very strict physical and logical rules. We have to define those rules, train our staff and invest in awareness.

5. Conclusion

Cyber Resilience is a balance between technology, organization and procedures such as a well-defined and tested Disaster and Disaster Recovery process and the necessary discipline. Besides the technology, we have to invest in awareness and knowledge.