Industrial Network Security

Securing Critical Infrastructure Network for Smart Grid, SCADA,
and Other Industrial Control Systems

2. About Industrial Networks

Attacks, Breaches and Incidents: Malware, Exploits and APT's

The focus of this book is how an attack might occour and subsequently how to best protect the Industrial Network and the connected ICS components against undesirable consequences that result from this action. Did the action result in some outcome—operational, health, safety or environment—that must be reported to a federal agency according to some regulatory legislation? Did it originate from another country? Was it a simple virus or a persistent rootkit? Could it be achieved with free tools available on the Internet, or did it require the resources of a state-backed cyber espionage group? Do such groups even exist?

Asset, Critical Asset, Cyber Asset, and Critical Cyber Assets

- *Asset:* Component that is used within an industrial control system.
  - Often physical (Workstation, server, network switch)
  - Also logical (Process graphic, database, logic program, firewall sule set or firmware)
  - In this book, any component of the network is called an asset
- *CCA:* Critical Cyber Asset: device that uses a routable protocol within a control center or is dial-up accessible. In version 5 of the standars, this change to take on a more holistic approach, taking into account BES (Bulk Electric Systems)

Security controls and Security countermeasures

These terms simply refer to methods of enforcing cybersecurity in order to reduce risk

Firewalls and IPS's

Basic firewalls may not be able to distinguish between what is a request and what is a response * *Deep Packet Inspection system* is a device that can decode network traffic and look at the contents or payload of that traffic. It is typically used by IDS's, IPS's, advanced firewalls and many other systems to detect signs of attacks. * Industrial Networks support high availability making most general IPS appliances less common on critical networks; IPS is more often applied at upper level networks where high availability (>99.99%) is not such a high priority.

Industrial Control System

- *An Industrial Control System (ICS)* is a broad class of automation systems used to provide control and monitoring functionality in manufacturing and industrial facilities. Aggregate of a variety of diferent system types
  - *Process Control Systems (PCS)*
  - *Distributed Control Systems (DCS)*
  - *Supervisory control and data acquisition (SCADA) systems*
  - *Safety instrumented systems (SIS)*
  - And many others

DCS or SCADA

Both systems are designed to monitor and to control manufacturing or industrial equipment.

ICS are often refered to in the media as SCADA, wich is both inaccurate and misleading. A SCADA system is a ICS, but not all ICS ara SCAADA.

Industrial Networks

The various assets that comprise a ICS are interconnected over an industrial Network.

Following Stuxnet, there has been a open source revision of the protocols that where in place. These protocols where found to have critical security bugs, wich instigated the critical industry sector to migrate to propietary protocols, often too cost-prohibitive for researches to procure and analyse.

Networks, Routeble Networks, and Nonroutable Networks

A *Nonroutable network* refers to those serial, bus and point-to-point comuniication links that utilize **Modbus/RTU**, DNP3, fieldbus and other networks.

A *Routable network* tipically means a network utilizing the protocol TCP/IP or UDP/IP although other protocols such as AppleTalk, DEVnet and others certainly apply.

In a industrial network, it is common that routable and nonroutable networks interconnect or overlap.

All networks and all devices should be considered potentially accessible and vulnerable.

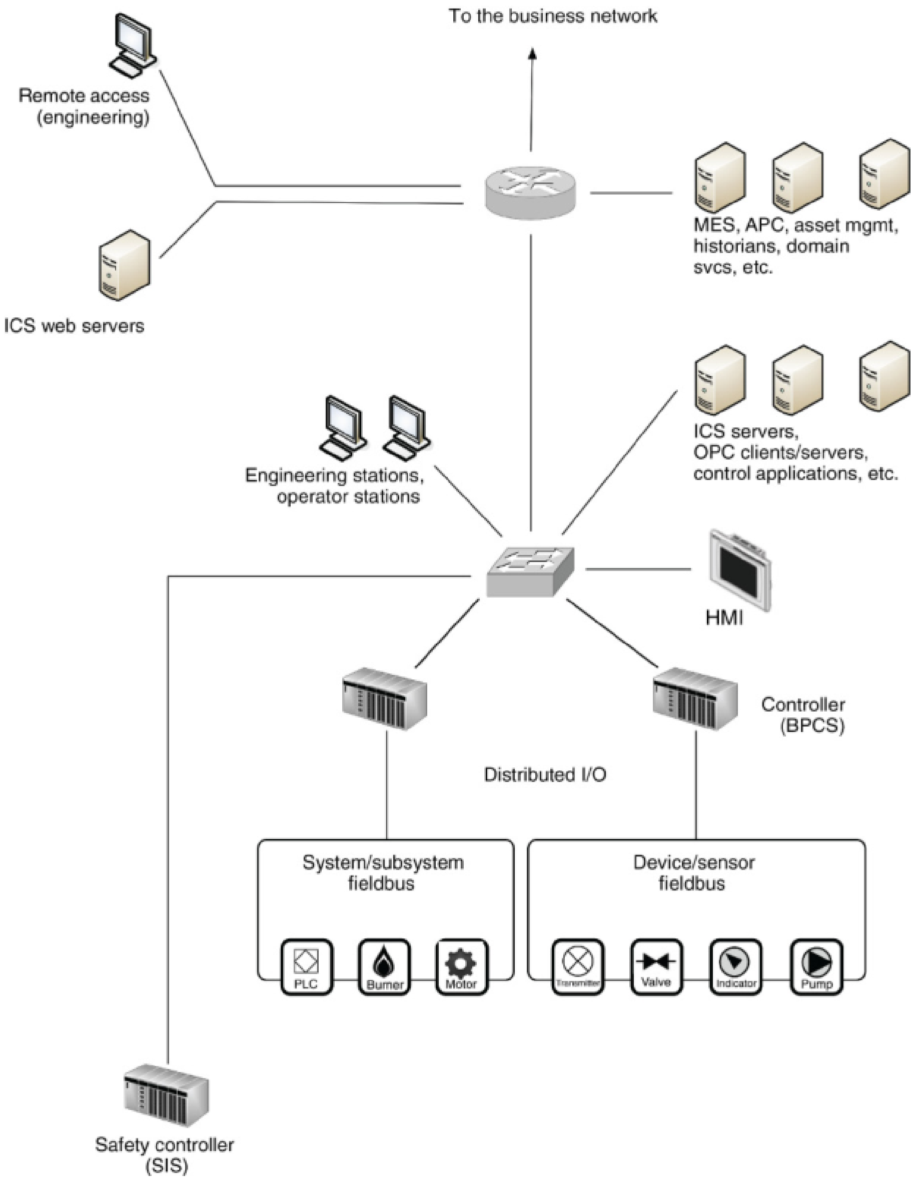


Figure 1: Sample network conectivity of an ICS

Enterprise or business networks

> Network of systems that provide the information infrastructure to the business. They can be suppliers that provide the raw material, customers, that recieve the finished product.

In the end, the business network and the industrial network interconnect to make up a single end-to-end network

It should be noted that there are several systems and services that exist in both networks, such as directory services, file servers and databases. These common services should not be shared, rather replicated, to minimize interconnectivity and reduce potential attack surfaces of both ICS and enterprise infrastructure.

Zones and enclaves

> Closed group of assets or a functional group of devices, services and applications that make up a larger system.

- *Zone:* A spetial network that has been created to expose a subset of resources to a larger, untrusted network.

While highly effective, there are times that they become inpractical, because of the complexity of controling a single device over a network. (Smart grids)

Network perimeters or electronic security perimeters

- *Perimeter:* The outermost boundary of any colsed group of assets (zone)
  - It is a logical point in wich implement cybersecurity controls.
  - Typically consist of Firewalls, IPS or similar network-based filters

Critical infrastructure

- *Industrial Networks:* are refered to as any network operating some sort of automated control system that communicates digitally over the network.
- *Critical Infrastructure:* is refering to the critical *systems and assets* used within a network computing infrastructire.

Utilities

Water, wastewater, gas, oil, electricity and communications are critical national infrastructures that rely heaviliy on industrial networks and automated control systems. They are also clear examples of industrial networks.

Nuclear facilities

High target for hackers, very secure and protected by law

Bulk electric

Defined as critical infrastructure under HSPD-7 and highly regulated in North America by NERC.

Smart Grid

Is a modernization of energy transmission, distribution, and consumption systems. It will be used as an example in this book, because, as it has become “smart”, the devices and components that make up the transmission, distribution, metering, and other components of the grid infrastructure have become sources of digital information, have been given distributed digital communication capability, and have been highly automated.

Chamical facilities

Unlike the Utility networks, they have to secure their intellectual property as much as they do their control systems and menufacturing operations.

Common Industrial Security Recommendations

1. Identify what systems need to be protected
2. Separating the systems logically into functional groups
3. Implementing a defense in depth strategy around each system or group
4. Controling access into and between each group
5. Monitoring activities that occour within and between groups
6. Limiting the actions that can be executed within and between groups

Identification of critical systems

The first step is determining what needs to be protected. Identifying the assets that need to be secured and their overall importance to the reliable operation of the overall Integrated System. When determining what needs to be protected, we have to map every existing device, and determine if it is a critical asset or not.

Network Segmentation / Isolation os Systems

Segmentation of assets into functional groups allows specific services to be tightly locked down and coltrolled, and is one of the easyest methods of reducing the attack surface that is exposed to potential threat actors.

Defense in depth

A defense in depth strategy should be implemented.

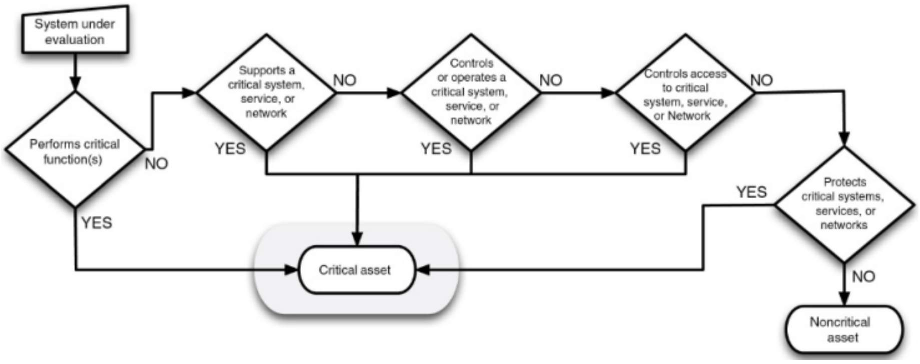

System under evaluation
Performs critical function(s)
YES
NO
Supports a critical system, service, or network
YES
NO
Controls or operates a critical system, service, or network
YES
NO
Controls access to critical system, service, or Network
YES
NO
Protects critical systems, services, or networks
YES
NO
Critical asset
Noncritical asset

Figure 2: Diagram to determine critical assets

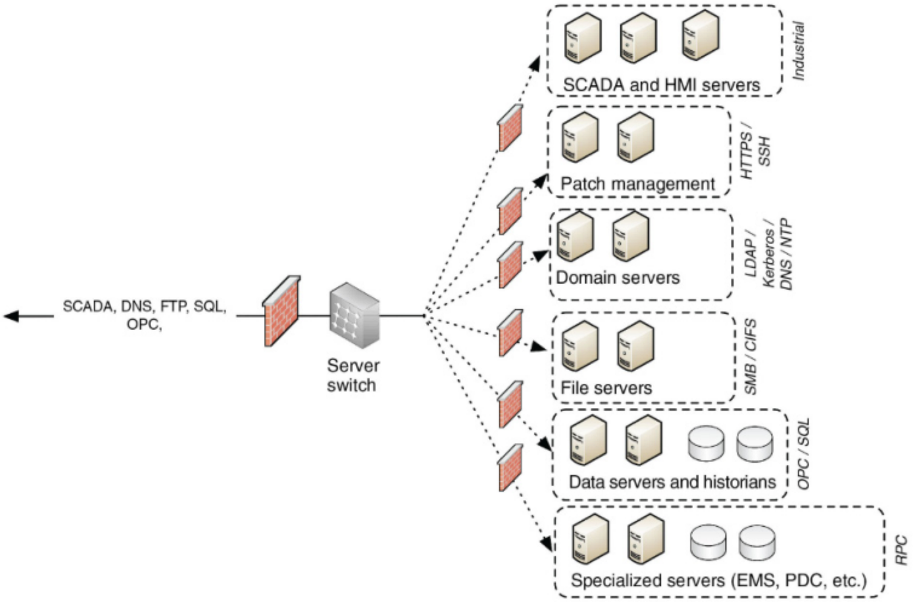


Figure 3: Funtional Groups - Done right

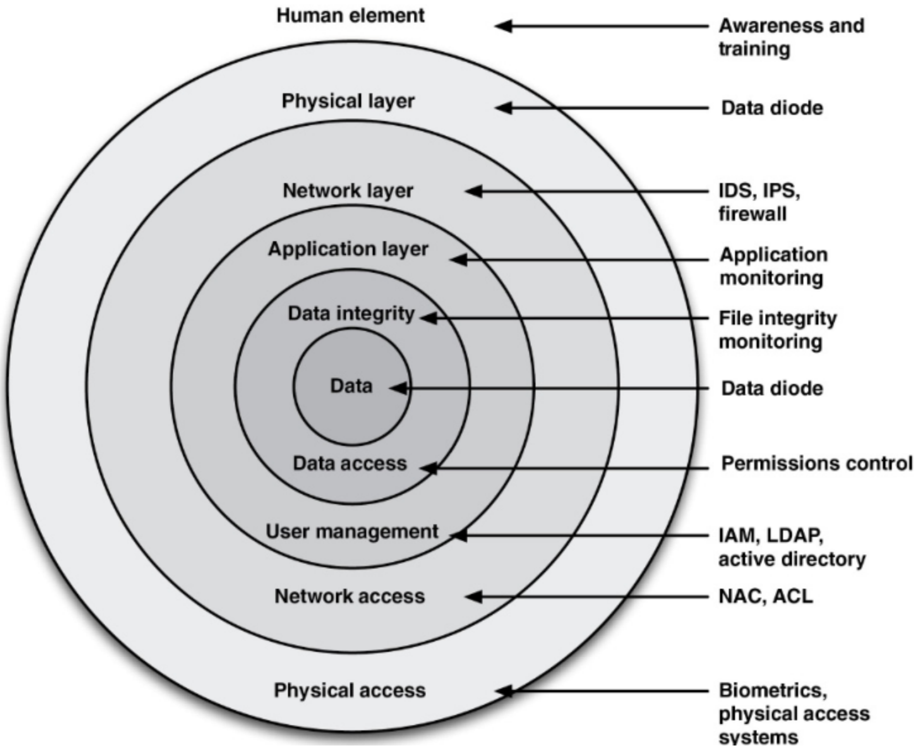


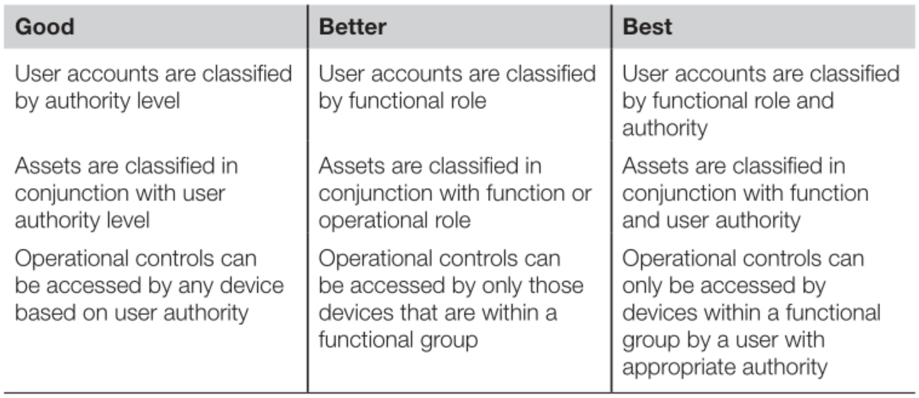
Figure 4: Defense in Depth

Access Control

Most dificult, but important aspects of cybersecurity. Considers 3 very important aspects of how a user interacts with resources.

- Identification
- Authentication
- Authorization

The successful implementation of access control is dificult because of the complexity of managing users and their roles and their mapping to specific devices and services that relate specifically to an employee's operational responsabilities.



Good	Better	Best
User accounts are classified by authority level	User accounts are classified by functional role	User accounts are classified by functional role and authority
Assets are classified in conjunction with user authority level	Assets are classified in conjunction with function or operational role	Assets are classified in conjunction with function and user authority
Operational controls can be accessed by any device based on user authority	Operational controls can be accessed by only those devices that are within a functional group	Operational controls can only be accessed by devices within a functional group by a user with appropriate authority

Figure 5: Access Control

The strengths of Access Control increases as a user's identity is treated with the aditional context of that user's roles and responsabilities within a functional group.

Advanced Industrial Security Recommendations

- *Security Monitoring:* Recognized method of providing situational awareness, Decide what has to be monitored
- *Policy Whitelisting:* A policy whitelist defines the behaviour that is acceptable. This is important in a ICS architecture, where an industrial protocol is able to exhibit specific behaviours, such as issuing commands, collecting data, or shuting down a system.
- *Application Whitelisting:* Defines the applications and files that are known to be good on a device and prevents any other application from executing.

Common Missperceptions About Industrial Network Security

- *Cyber security of industrial networks is not necessary:* There is no longer an air gap separating the ICS from any possible source of digital attack

- *Industrial security is an impossibility:* Even though devices in a ICS may not be patched, there are other measures to grant a intensive security
- *Cyber security is someone else's responsabilitie:* Cyber security is a end-to-end problem that requires a end-to-end solution
- *It is the same as a "regular" cyber security:* Industrial and business networks are diferent and require diferent security measures to adequately protect them.