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.

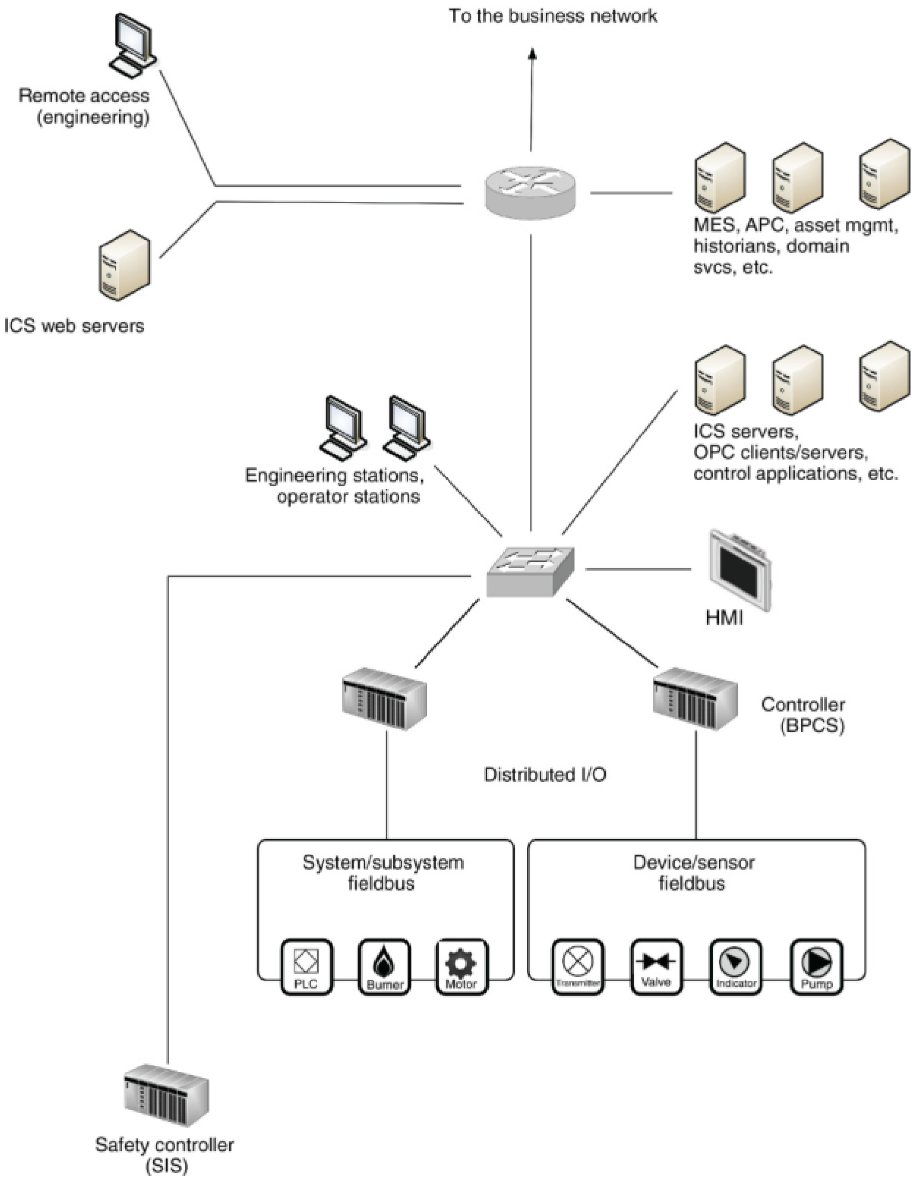

To the business network
Remote access (engineering)
ICS web servers
MES, APC, asset mgmt, historians, domain svcs, etc.
Engineering stations, operator stations
ICS servers, OPC clients/servers, control applications, etc.
HMI
Controller (BPCS)
Distributed I/O
System/subsystem fieldbus
PLC
Burner
Motor
Device/sensor fieldbus
Transmitter
Valve
Indicator
Pump
Safety controller (SIS)

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.

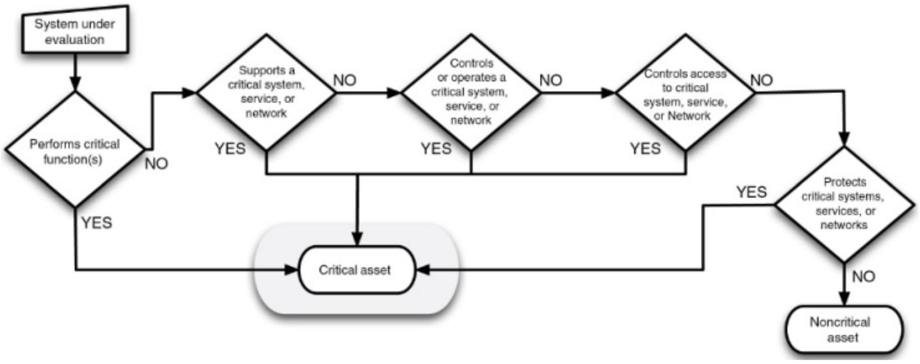

System under evaluation
Performs critical function(s)
NO
YES
Supports a critical system, service, or network
NO
YES
Controls or operates a critical system, service, or network
NO
YES
Controls access to critical system, service, or Network
NO
YES
Protects critical systems, services, or networks
YES
NO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

Figure 2: Diagram to determine critical assets

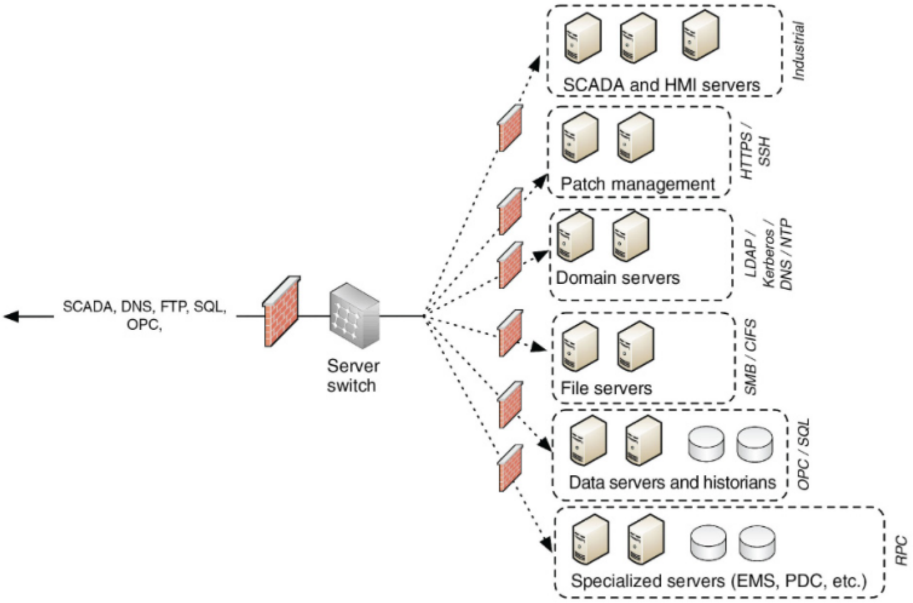


Figure 3: Funtional Groups - Done right

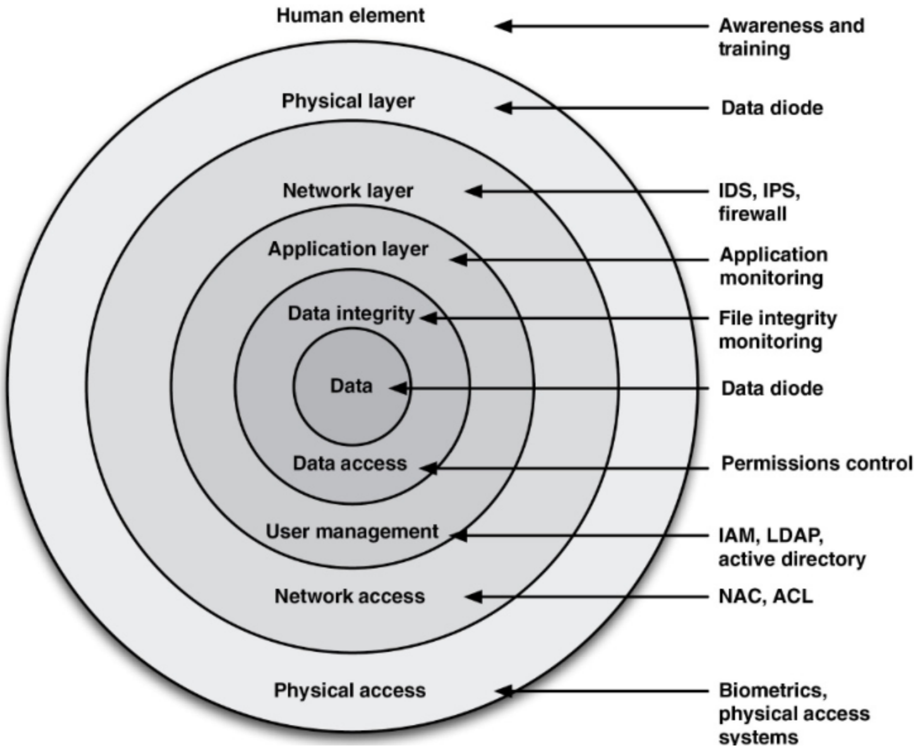


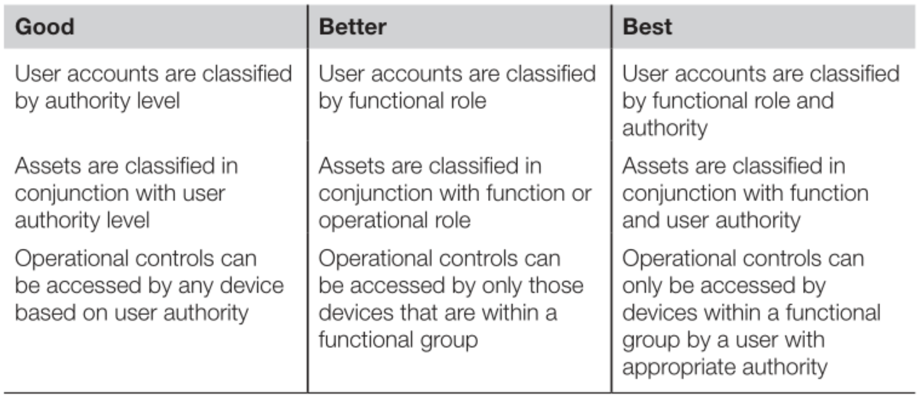
Figure 4: Defense in Depth

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.

3. Industrial Cyber Security History and Trends

Industrial Network systems differ from commercial network systems in that they are expected to operate for months or even years. This is due to the network's requirements of availability.

Importance of securing industrial networks

Before, physical security was a priority and there exists locked rooms and zones to prevent unauthorised people to enter the secure location. Dightal security wasn't a priority because the Industrial Network was air-gapped, but as more modern 'real-time' technology advanced, there needed to be a way of accessing air-tight restricted data, so it was broken.

The evolution of the cyber threat

- *Cyber Threat:* numerous definitions exist, but all have in common
- Unauthorized access to a system
- Loss of confidentielity, integrity or availability of the system, it's data or applications

The initial penetration of industrial systems is getting easyer through the evolution and deployment of increasingly complex and sophisticated malware.

The industrial systems at levels 2, 1 and 0 are being increasingly targeted.

The threats continue to evolve, learning from successful techniques from past malware while introducing new capabilities and complexity.

The industrial systems as they stand today simply don't stand a chance against a modern attack capability. Their primary line of defense remains the business networks that surround them and network-based defenses between each security level of the network.

Observations about the attacks

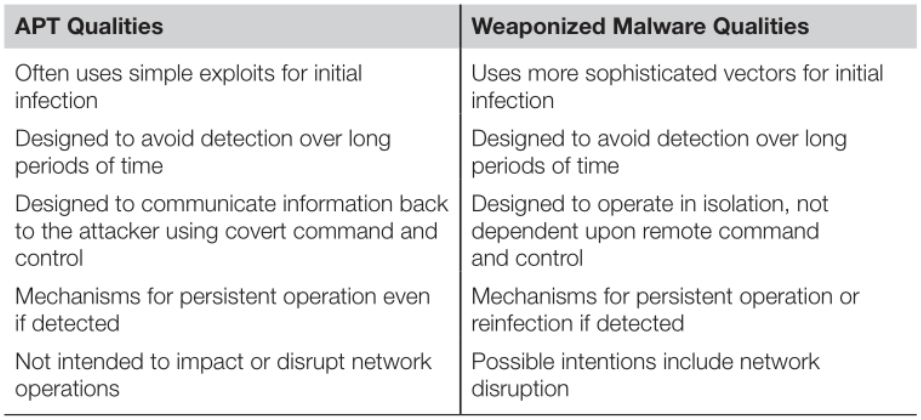
- Most attacks seem to be oportunistic
- Initial attacks, simpler exploits; Thwarted or discovered attacks, > sofisticated methods

- majority of cyberattacks -> Finantially motivated
- Malware samples increase at an alarming rate
- Majority of attacks originate externally and leverage weak or stolen credentials
- Majority of incidents affecting industrial systems are unintentional
- New malware code samples are increasingly more sophisticated
- Percentage of cyberattacks is high, but has been steadily decreasing
- Auto-run malware has been rising steadily
- Malware and Hacking-as-a-service has become more prevalent
- Remote access incidents have been steadily increasing
- Pretty straightworward:
  - Spear phishing
  - Watering hole
  - Database Injection

APT's and weaponized malware

Advanced Persistent Threats

Stuxnet is an example of an APT and Weaponized malware It replicated itself a number of times, and auto-removed itself from the system if it's host was no thte preconfigured target. It used 0-days to bypass IDS's and used Digital certificates (Stolen) to pretend it is a authorized program.



APT Qualities	Weaponized Malware Qualities
Often uses simple exploits for initial infection	Uses more sophisticated vectors for initial infection
Designed to avoid detection over long periods of time	Designed to avoid detection over long periods of time
Designed to communicate information back to the attacker using covert command and control	Designed to operate in isolation, not dependent upon remote command and control
Mechanisms for persistent operation even if detected	Mechanisms for persistent operation or reinfection if detected
Not intended to impact or disrupt network operations	Possible intentions include network disruption

Figure 6: Distinctions between Common APT and Weaponized Malware

Night Dragon

Discovered by McAfee, this weaponized malware targeted a series of Oil, Energy, and Petrochemical companies. The attack started with SQLi and pivoted it's way into internal network. They used Command and Control systems, and Remote Administration Toolkits, to recover sensitive information from the companie's executives. The goal of the attack, was to gain sensitive information. This is a form of cyber-espionage.

Stuxnet

Game-changer because it was the first targeted, weaponized cyber-attack against an industrial control system.

Advanced Persistent Threats and Cyber Warfare

Important diferences

- Cyber Warfare is higher in sofistication and in consequences, mostly due to available resources of the attacker and the ultimate goal of destruction versus profit.
- In many industrial networks, there is less profit available to a cyber-attacker than from others, and so it requires a diferent motive for attack (i.e. Socio-political)

Defending against modern cyber-threat

Advanced Persistent Diligence requires a strong **defense-in-depth** approach, to reduce the available attack surface for a attacker and to provide a broader perspective of threat activity for use in Incident Response, Analysis, Remediation, Restoration and investigation.

Now, traditional security measures are not enough and we have to use new technologies, such as:

- **Next-generation firewalls (NGFW)**
- **Unified Threat Management (UTM)**
- **ICS protocol aware IPS's**

Having situational awareness of what is attempting to connect to the system as well as what is going on within the system is the only way to start to regain control of the network and the system connected to it.

Insider Threats

> *Insider*: An individual who has approved access, priviledge, or knowledge of information systems, information services, and missions.

This definition can be expanded to the unique operational aspect of ICS to include a wide range of individuals:

- Employees with direct access to ICS components for operation
- Employees with highly priviledged access for administration and configuration
- Employees with direct access to ICS data

- Subcontractors with access to specific ICS components or subsystems for operation
- Services providers with access to specific ICS components or subsystems for support

Each of these individual can introduce unauthorised data to the system, wich is, in turn focused heavily on preventing outside attack

The Repository of Industrial Security Incidents (RISI) showed in 2013 that only 35% of incidents originated from outsiders. The reason is not a intentional will of causing harm to a system, but a result of unintentional or accidental actions directed on the overall security policies deployed within the architecture.

Hacktivism, Cyber Crime, Cyber Terrorism, and Cyber War

There are vulnerable industrial systems, and because these systems are vulnerable, anyone willing gto perform some research, download some freely available tools, and put forth some effort, can launch an attack. With a minimal knowledge of ICS, the likelyhood of a successfull attack with moderate consequences is significantly increased. The real question is one of motive and resources. The average person is not motivated enough, a hacktivist group is. The average person nay not have the resources to develop a 0-day exploit or execute spear-phishing campaigns, but now, all of these services, are available for hire. A fully weaponized attack on a critical infrastructure, no longer needs to be military, because it can be mercenary.

4. Industrial Control System and Operations

System Assets

We have to understand the type of devices that are connected to the network:

- Sensors, Actuators, Motor, Drives, Gauges
- Programmable Logic Controllers (PLC)
- Remote Terminal Units (RTU)
- Intelligent Electronic Device
- Human-Machine Interface
- Supervisory Workstation
- Data Historian
- And others

Programmable Logic Controller

- used to automate functions within manufacturing facilities.
- Typically hardened
- specialized for a specific use

- Custom OS, with as little overhead as possible
- Typically control real-time processes

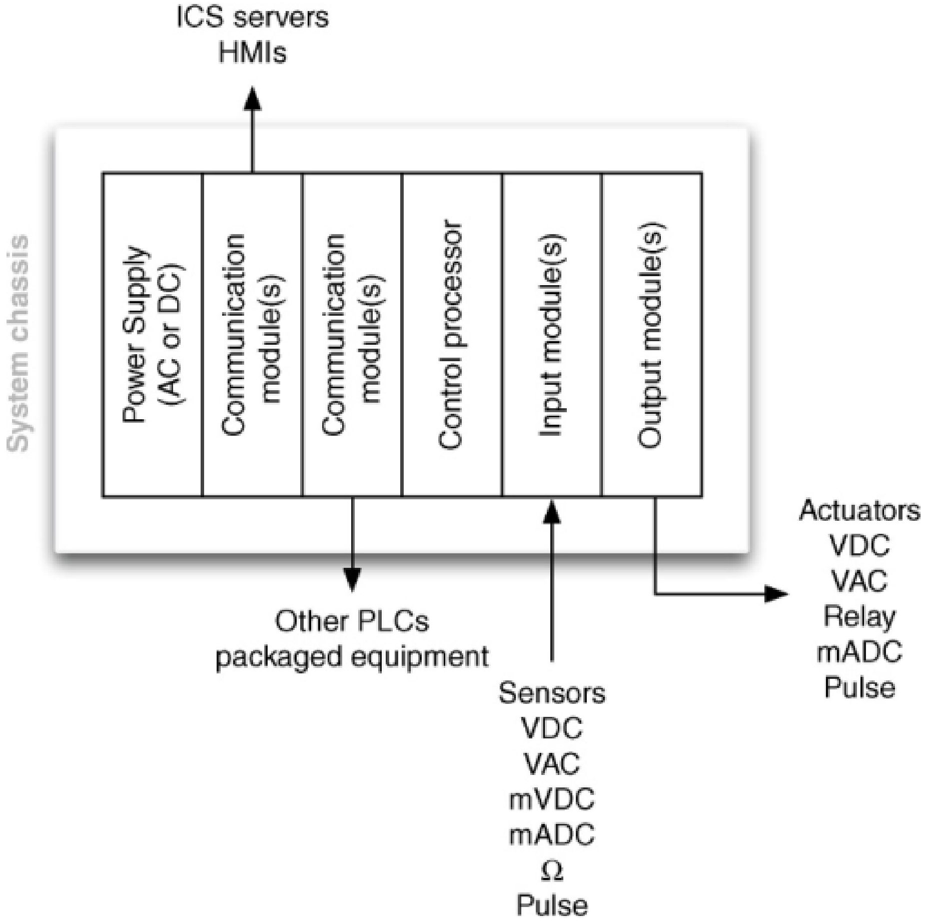


Figure 7: Contents of a typical PLC

Ladder Diagrams (LD) Is a simplistic programming language included with the IEC-61131-3 standard. Can be thought of as a set of connections between inputs (relay contacts) and outputs (relay coils) Ladder logic follows a relay function diagram. A path is traced from the left hand side, across “rungs” consisting of varius inputs. If a input relay is true, the path continues. If the path to the right side completes, the output coil will be set to true. Every step is tested in each scan

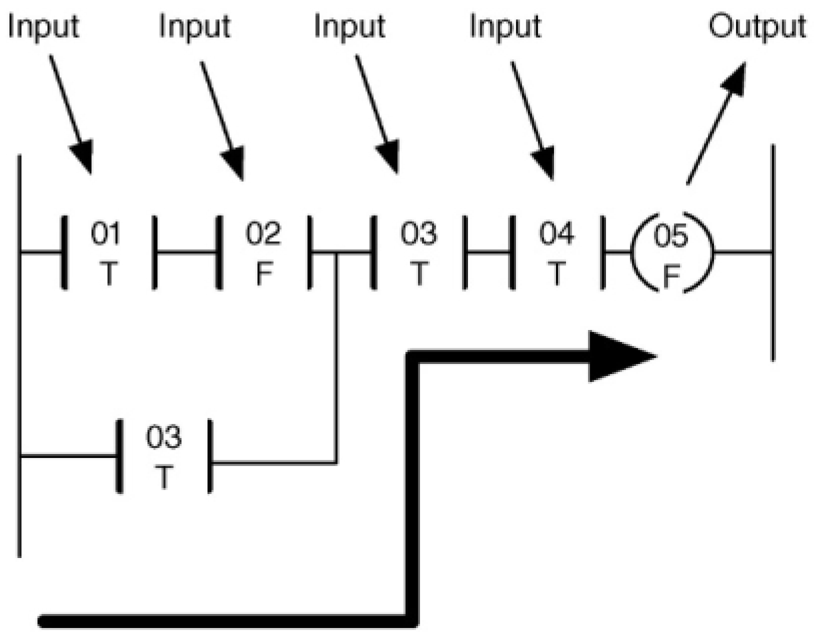


Figure 8: Example of a OR in a Ladder Diagram

Sequential Funtion Charts

Sequential Logic: Programming language used by PLC's and defined within the IEC-61131-3 standard

- Sequential Logic Differs from ladder logic in that each step is executed in isolation and progresses to the next step only upon completion.
- Very common in batch-oriented operations
- Can be uploaded the logic by direct serial or ethernet
- PLC's can hold the code and the compiled logic

Remote Terminal Unit

- Typically reside in a substation, along a pipeline or some other remote location
- Monitor field parameters and transmit the data back to the central monitoring station
- Commonly include a Modem, cellular data connection, radio or other wide area communication technology
- Typically stored in locations with no access to electricity and may be supplied with it by solar pannels
- Commonly placed outdoors, dubdued to extreme environmental conditions
- RTU's and PLC continue to overlap, to the point that a RCU can be

thought of as a remote PLC

Intelligent Electronic Devices

- Electric Utility Sector's take on RTU's.
- They manage electrical loads and provide local isolation when needed.
- They can also be installed in areas with high voltage and weather, such as a tower.

Human Machine Interface

- Used as an operator's means to interact with PLC's, RTU's and IED's.
- Replace manually activated switches, dials and controls used to sense and influence the process.
- Come in two predominant form-factors
  - Runs on Mordern OS and are capable of performing a variety of functions
  - Combine a Industrial Hardened computer, local touch pannel and is packaged to support door on direct pannel mounting. Typically use embeded OS and are programmed with a separate computer and assotiated engineering software.
- Used without password, because in a event of a emergency, using a password is unsafe.

Supervisory Workstations

- Collects information from assets used within a control system and presents that information for supervisory purposes.
- Is primary read-only
- Change parameters such as alarm limits for a process

Data Historian

- Specialized software that collects point values, alarm events, batch records, and systems and stores it in a purpose-built database.
- Data historized and stored within a historian is refered to as "tags" and can represent almost anything. (From airflow in a vent to acceptable loss margins)

Information used by both industrial operations and business management is often replicated across industrial and business networks. This represents a security risk, as a less secure network, such as a business network can provide access to a more secue zone.

Properly isolating and securing data historian components that connect with assets in les trusted networks within a semitrusted DMZ significantly help to minimize accesibility.

Business Information Consoles and Dashboards

Consist of the same data presented to a HMI or data historian system, but physically located elswhere, such as a executive office. The physical display in this case, is controled using a secure keyboard video mouse switching system (KVM) It can also be presented, using intermediary steps, to a website inside a company's intranet, or a excel sheet. Depending on the complexity of the BICAD's

System Operations

A typical industrial operation consists of several layers of programmed logic designed to manipulate mechanical controls in order to automate the operation. Each specific function is automated by what is com- monly referred to as a control loop. Multiple control loops are typically combined or stacked together to automate larger processes

Control Loops

One of the many automated processes that make up a Industrial Controller. The term loop, derives of the ladder-logic widely used in these systems. A closed loop is one in wich its output, affects its input. Closed loops provide automated control, open loops, provide manual control.

Control Processes

General term used to define larger automated processes within an industrial operation. One control process may be composed of one or more control loops. Each process is typically managed using a HMI, which is used to interact with the process.

Feedback loops

Feedback is generally provided directly from the HMI used to control a specific process.

Production Information Management

Once historized, the information can be further analyzed using tools, such as Statistical Process Control (SPC) / Statistical Quality Control (SQC), either directly from within the data historian or by using an external analysis tool, such as a spreadsheet. Historical data can be replayed at some point in the future to compare past and present plant operations.

Business Information Management

Operational monitoring and analysis provides valuable information that can be used by plant management to fine-tune operations, improve efficiencies, minimize costs, and maximize profits. This drives a need for replication of operational data into the business network. By placing an HMI outside of the ICS DMZ, any firewalls, IDS/IPS, and other security monitoring devices that are in place need to be configured to allow the communication of the HMI into and out of the ICS DMZ. This effectively reduces the strength of the security perimeter between the industrial and business networks to user authentication only.

Process Management

An HMI is used by an operator to obtain real-time information about the state of the process to determine whether manual intervention is required to manage the control process by adjusting an output (open loop) or modifying established set points (closed loop).

Safety Instrumented Systems

Safety instrumented systems (SIS) are deployed as part of a comprehensive risk management strategy utilizing layers of protection to prevent a manufacturing environment from reaching an unsafe operating condition. The Basic Process Control System is in charge of mantaining a discrete and continuous control of the process, but i case the process reaches extreme, unstable states, the Safety Instrumented System is deployed. This typically manages a automated shutdown of the process.

There are two risks originate within the SIS related to cyber incidents:

- The prevention of the SIS from properly performing its control functions can allow the plant to transition into a dangerous state that could result in catastrophic events.
- The SIS can also be used maliciously to cause unintentional equipment or plant shutdowns

In both cases, the need to isolate the SIS to the gratest extent is a reasonable approach to improving cybersecurity resilience. The systems have to be checked periodically to ensure they work. This is a good time to perform security operations such as SW updates and patching.

The smart grid

The smart grid is complex and highly interconnected. It is not the convergence of a few systems, but of many including customer information systems, billing systems or demand response systems. Most of these systems interconnect and intercommunicate with many others. The benefits of this allow for intelligent command and control of energy usage, distribution, and billing. The disadvantage of such a system is that the same end-to-end command and control pathways could be exploited to attack one, any, or all of the connected systems.

Network Architectures

The ICSs and operations discussed so far are typically limited to specific areas of a larger network design, which at a very high level consist of business networks, production networks, and control networks.

In reality, industrial networks consist of multiple networks, and they are rarely so easily and neatly organized.

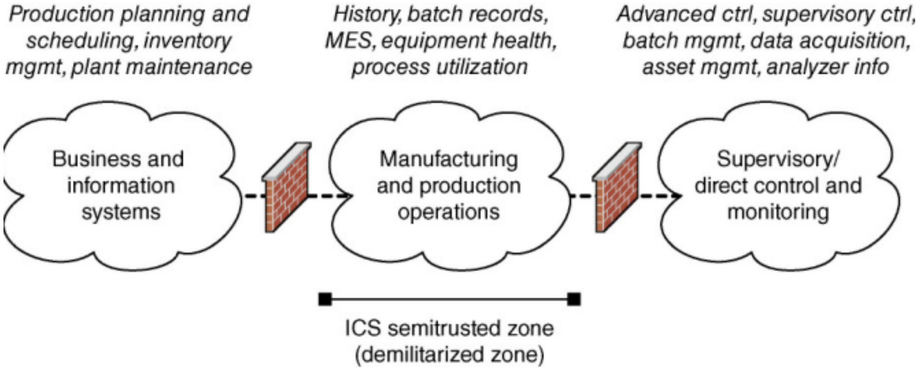

Production planning and scheduling, inventory mgmt, plant maintenance
History, batch records, MES, equipment health, process utilization
Advanced ctrl, supervisory ctrl, batch mgmt, data acquisition, asset mgmt, analyzer info
Business and information systems
Manufacturing and production operations
Supervisory/ direct control and monitoring
ICS semitrusted zone (demilitarized zone)

Figure 9: Funtional demarcation of industrial networks