
# Cybersecurity Essentials and Management for Energy Sector

## CSP001_C_E

PRESENTATION BY:
**DAVIDE FERRARIS**
UNIVERSITY OF MALAGA, SPAIN


# Acknowledgement


- *Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.*
- *Project Agreement no. 101083594*

# Topic-5: Secure Architecture Design and Implementation for Energy Systems

## Overview

- Design and implement secure network architectures for energy systems
- Secure network architecture in Energy Sector including SCADA systems, smart grids, and other critical energy assets
- Utilise network segmentation to isolate critical systems and reduce the impact of cyberattacks
- Configure firewalls and access control systems to protect energy networks and restrict unauthorised access
- Implement intrusion detection and prevention systems (IDS/IPS) to monitor and protect networks
- Employ VPNs for secure remote access to energy systems and sensitive data

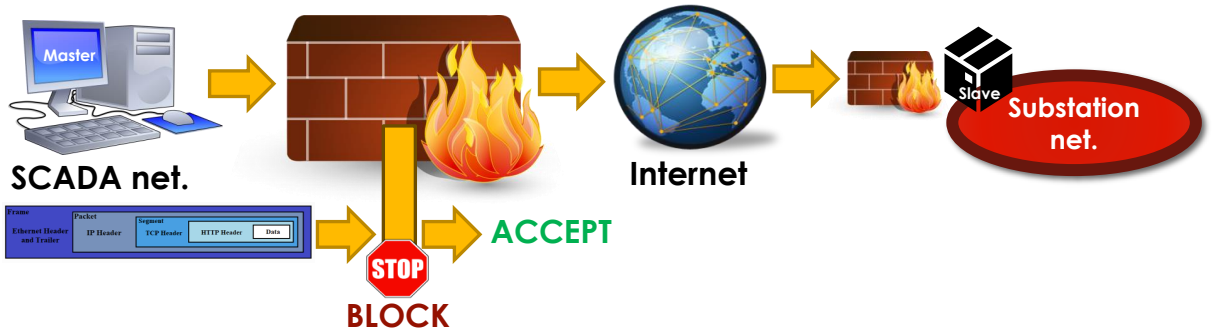
# Topic-5: Secure Architecture Design and Implementation for Energy Systems

## Overview

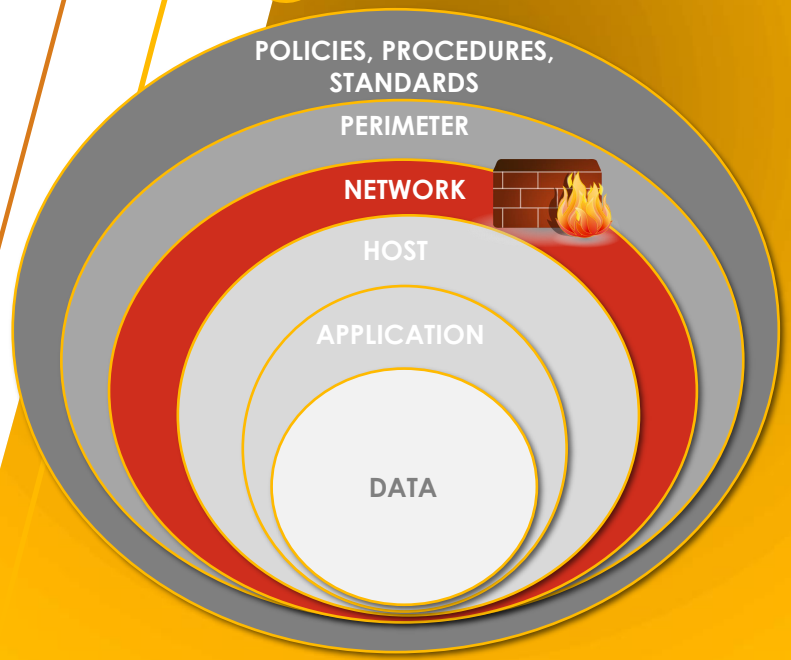
- Design and implement secure network architectures for energy systems
- Secure network architecture in Energy Sector including SCADA systems, smart grids, and other critical energy assets
- Utilise network segmentation to isolate critical systems and reduce the impact of cyberattacks
- **Configure firewalls and access control systems to protect energy networks and restrict unauthorised access**
- Implement intrusion detection and prevention systems (IDS/IPS) to monitor and protect networks
- Employ VPNs for secure remote access to energy systems and sensitive data

# Firewalls in energy control systems

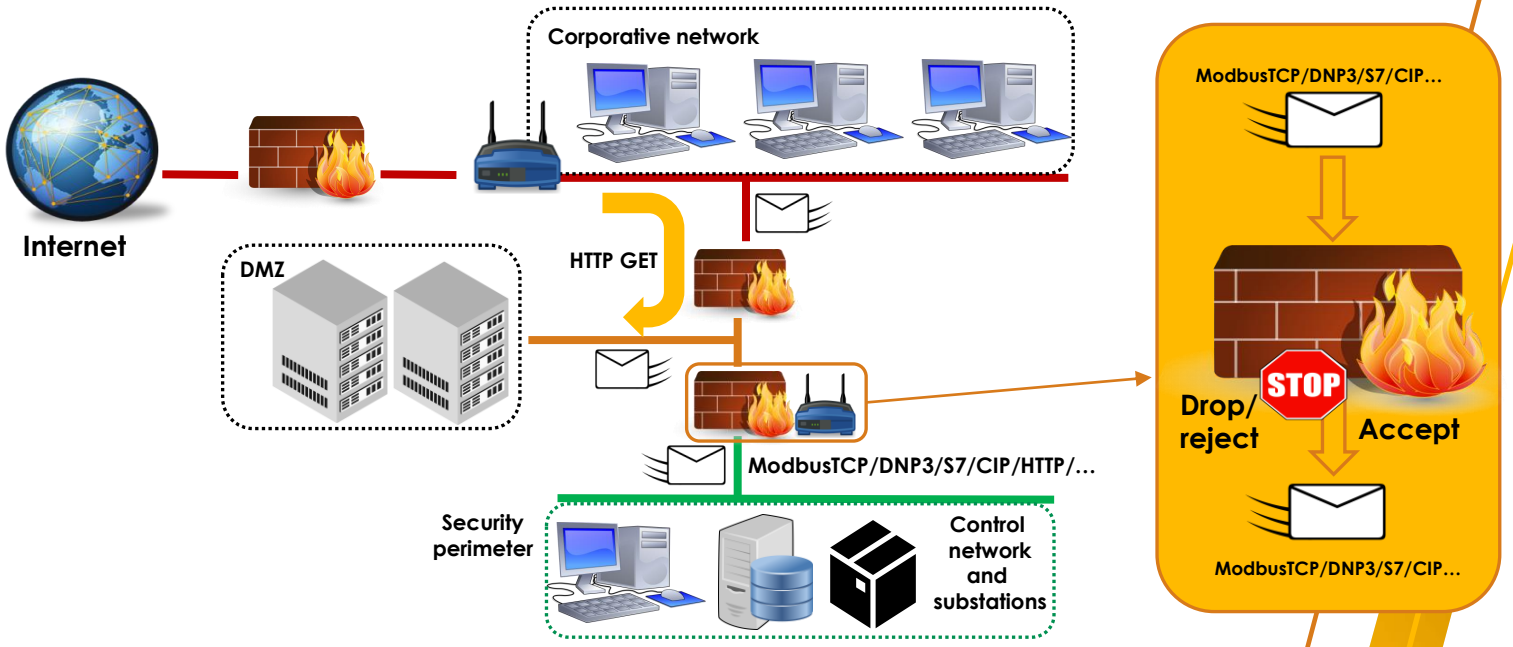
- A firewall is a **HW/SW component** of the system or network, whose purpose is to block unauthorised access, while allowing communication between authorised entities
  - E.g. block unauthorised connections to substations




- In power grids, firewalls are one of the main security elements, included as part of the first '**line of defence**' and of the network protection perimeter
  - They can be deployed on HMIs, SCADA servers, controllers (if applicable), gateways, routers or switches, and are mainly based on rules and actions for packet filtering



# Firewalls in energy control systems




- Firewalls have the ability to analyse and evaluate whether packets are suitable for their final delivery
  - E.g., whether the IP and/or MAC address is correct, the port is correct, the TCP/UPD/ICMP protocol is correct,...
- After this processing, the firewall (i) decides whether to accept or reject the final transfer of the packet to the destination, and (ii) must protect the security perimeter

# Four generations and evolution

- From their origins in the 1980s to the present day, firewalls have evolved into the fourth generation

1st generation: Packet filtering (packet filter)

2nd generation: Stateful firewalls (stateful inspection)

3rd generation: Application firewalls (application filtering)

4th generation: Next-Generation Firewall (NGFW)

# Four generations and evolution

- From their origins in the 1980s to the present day, firewalls have evolved into the fourth generation

**1st generation: Packet filtering (packet filter)**

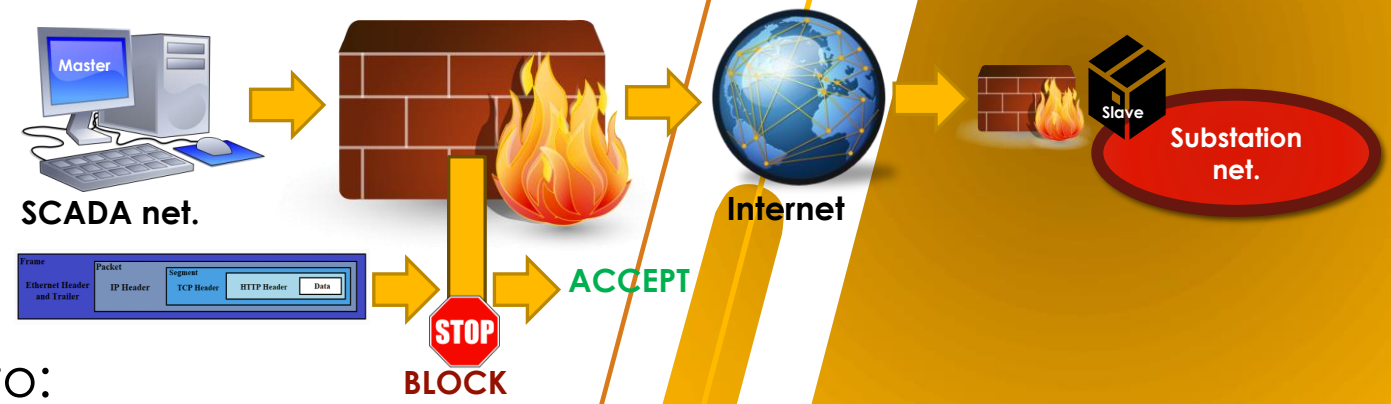
2nd generation: Stateful firewalls (stateful inspection)

3rd generation: Application firewalls (application filtering)

4th generation: Next-Generation Firewall (NGFW)

# 1st Generation: Packet filtering

- In 1988, the first packet filtering systems, known as "packet filtering" firewalls, emerge
- These systems are focused on providing an intensive inspection of packets, in terms of:
  - IP, MAC, protocols, ports
- If there is a match with any of the rules, the packet is:
  - Accepted
  - Blocked
- Firewall rules can be applied to:
  - Incoming traffic to the firewall
  - Outgoing traffic from the firewall to another network
  - Traffic forwarding to another firewall



# Four generations and evolution

- From their origins in the 1980s to the present day, firewalls have evolved into the fourth generation

1st generation: Packet filtering (packet filter)

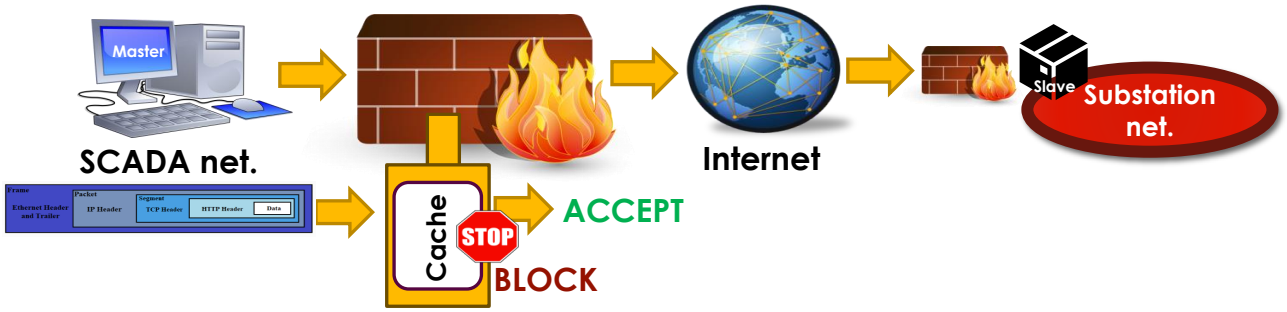
**2nd generation: Stateful firewalls (stateful inspection)**

3rd generation: Application firewalls (application filtering)

4th generation: Next-Generation Firewall (NGFW)

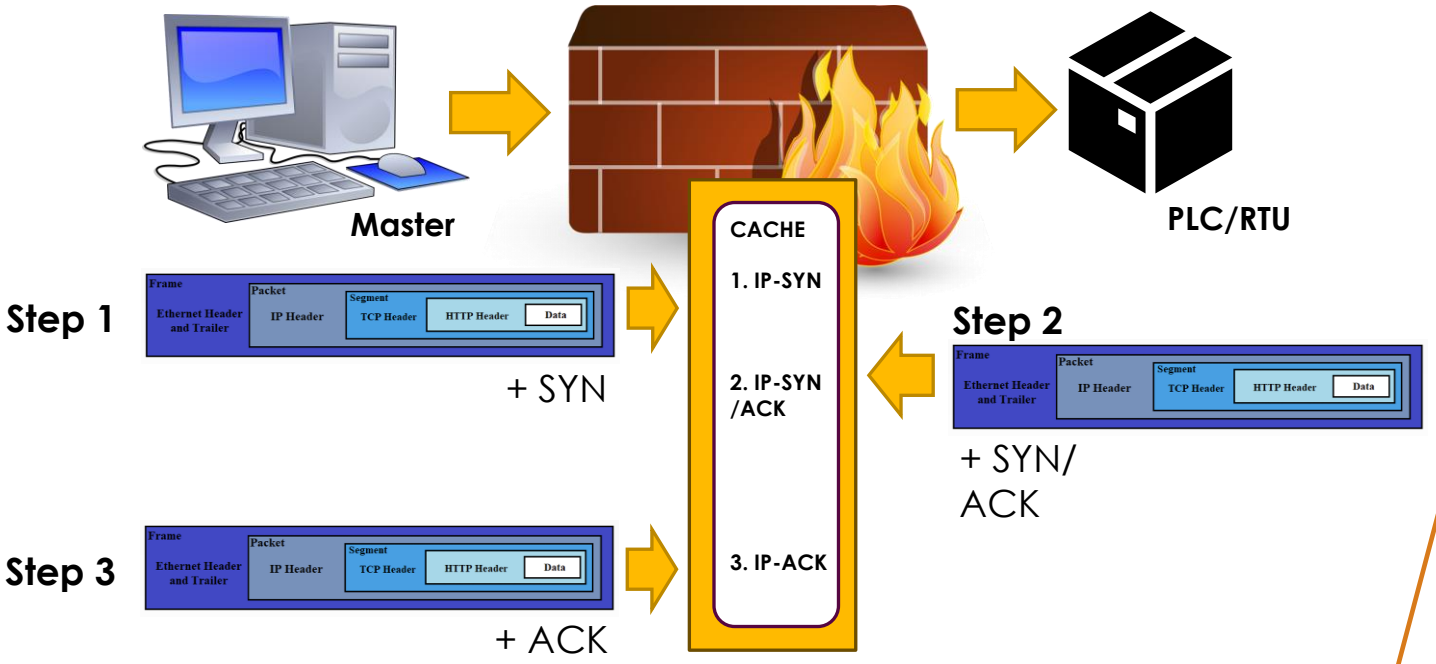
# 2nd Generation: Stateful firewalls

- This type of firewall inherits the features of the packet filtering system, but in addition it is able to record or "memorise" (through an internal cache) the previous statuses related to the received connections (e.g. SYN, SYN/ACK, ACK)
- This temporal register allows to:
  - Accept/drop the existence of new connections with specific statuses
  - Detect possible abuse of an existing connection
  - Detect irregularities in connections



# Example of its usefulness

- An example can be found in TCP 3-handshake connections, where it is necessary to control the SYN, ACK and SYN/ACK statuses



# Four generations and evolution

- From their origins in the 1980s to the present day, firewalls have evolved into the fourth generation

1st generation: Packet filtering (packet filter)

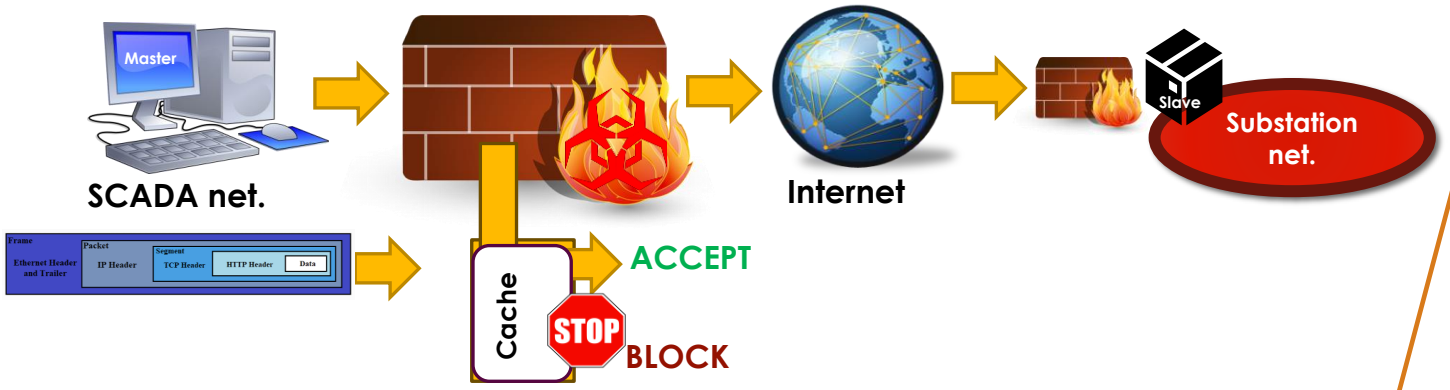
2nd generation: Stateful firewalls (stateful inspection)

**3rd generation: Application firewalls (application filtering)**

4th generation: Next-Generation Firewall (NGFW)

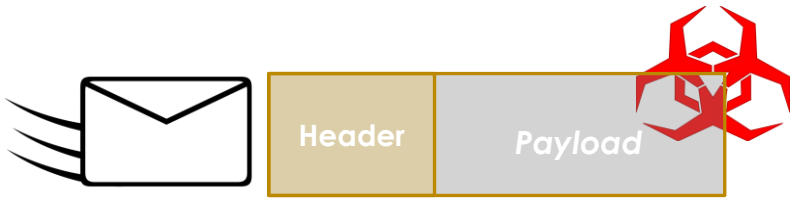
# 3rd Generation: Application firewalls

- This type of firewall adds new applications at the application level of the TCP/IP stack, such as:
  - "**Deep Packet Inspection**" (DPI) to detect irregularities or malware infection in packet contents
  - Intrusion detection and prevention systems
  - anti-malware
  - VPN
  - TLS
  - ...



# Deep Packet Inspection - DPI

- DPI is an advanced technique that consists of simply inspecting the "contents" of network packets to detect attack patterns or irregular conditions in packets
  - This feature arises because firewalls ONLY analyse the packet header (IP and TCP/UDP) WITHOUT looking at the payload (payload or message contents)
- Therefore, DPI aims to detect:
  - Irregular packet formats
  - Large/small packets
  - Infections in the payload
  - ....
- However, the usefulness of the DPI is limited
  - It only analyses certain conditions of the packet without exploring in detail the existence of attack vectors or patterns




# Four generations and evolution

- From their origins in the 1980s to the present day, firewalls have evolved into the fourth generation

1st generation: Packet filtering (packet filter)

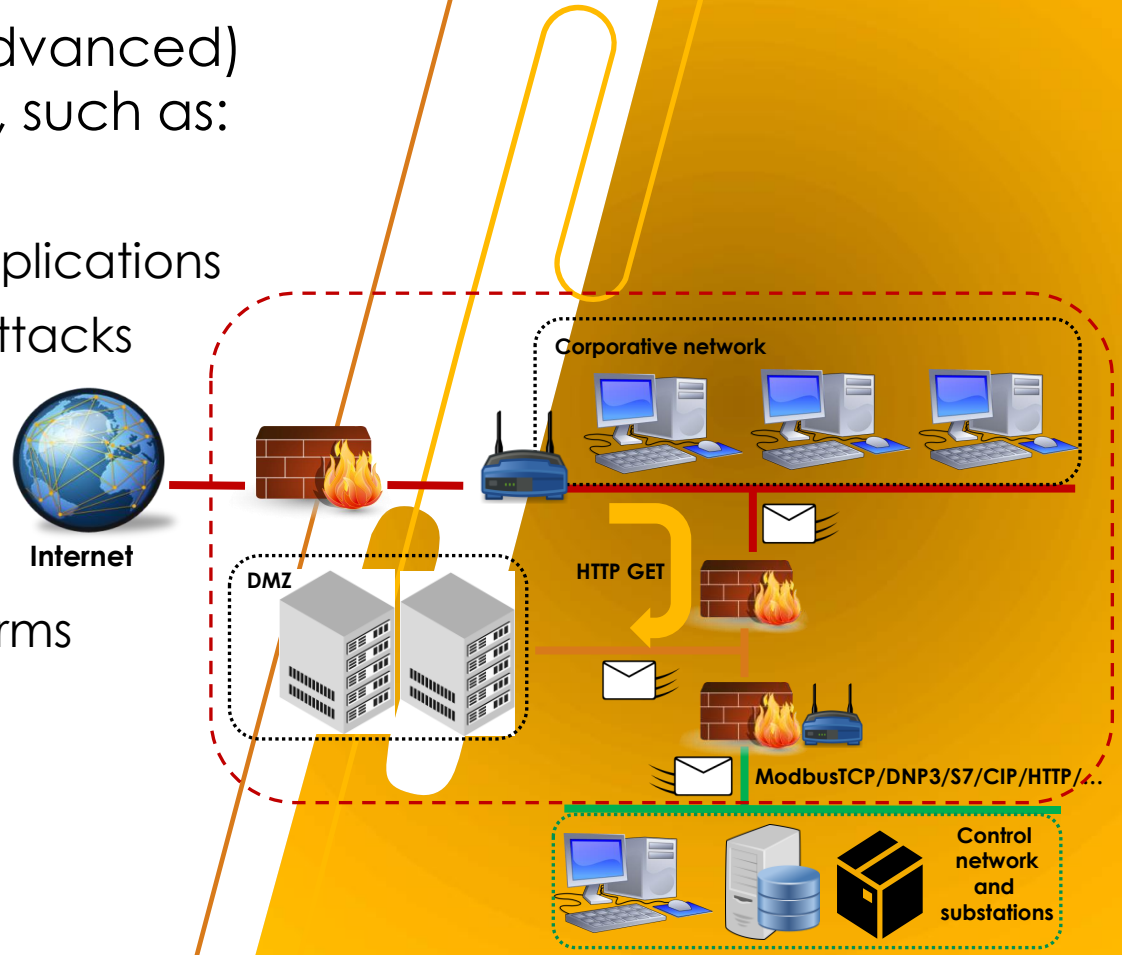
2nd generation: Stateful firewalls (stateful inspection)

3rd generation: Application firewalls (application filtering)

**4th generation: Next-Generation Firewall (NGFW)**

# 4th Generation: Next-Generation Firewall

- NGFW-based systems incorporate (more advanced) applications at the corporate network level, such as:
  - DPI
  - Management and monitoring of users and applications
  - Control of Advanced Persistent Threat (APT) attacks
  - Validation of applications
  - Data isolation
  - Protection of network systems in the cloud
  - Control and management from mobile platforms
  - etc.

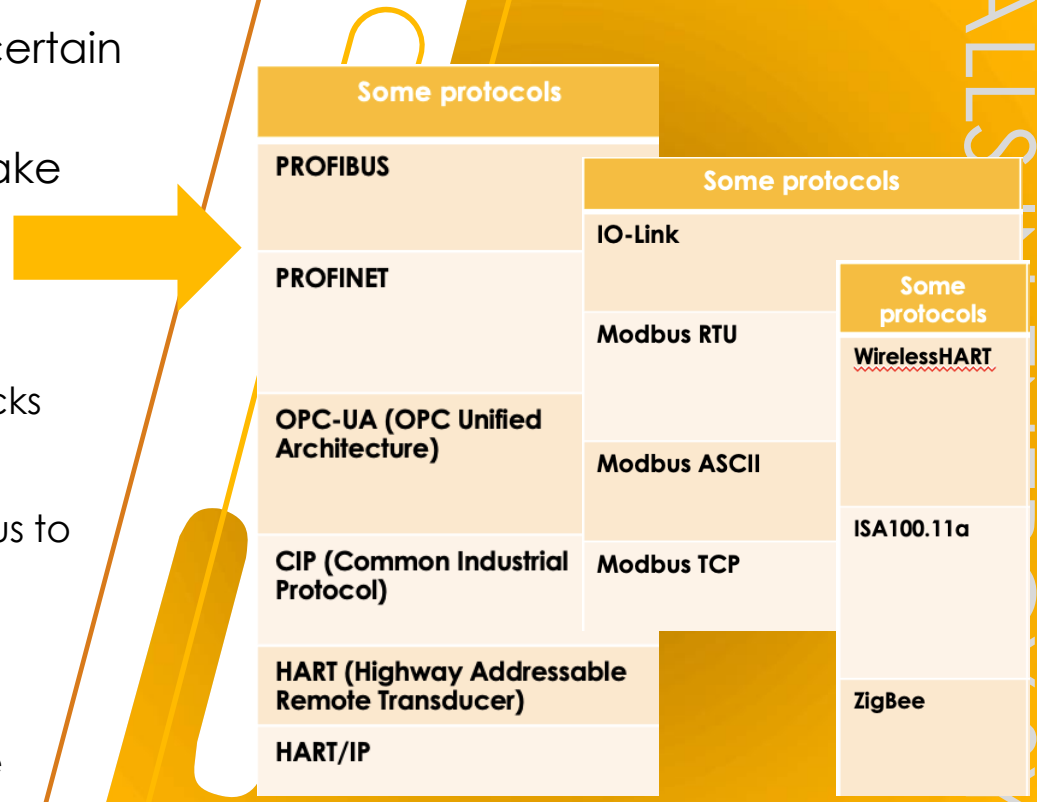


# Advantages of its use

- **Protect the most critical networks** (e.g., substations) against attacks from the Internet - by reducing the exposure of equipment to external networks through action rules
- Promote network **segmentation and isolation**
- Control **network traffic statuses**, generating alerts in the event of attacks or anomalies
- **Monitor suspicious activities** on the target network by analysing the network parameters and its resources, such as processes and connections
  - E.g. abuses to a specific IP of a network, abuses to certain ports, etc.

# Disadvantages of its use

- Firewall functionalities are subject to **pre-defined rules**, and to certain parameters such as IPs, ports or "protocol features"
- There are **too many industrial communication protocols** that make difficult to find a unified firewall capable of interpreting all the protocols – as already shown in the previous section !!
- **Any undefined condition by rules may be accepted**
  - If a port is open and not covered by filtering rules, it may lead to attacks
- The previous drawback leads to **constant updates**
  - And depending on the size of the network, firewall rules can be tedious to maintain
- The definition of **firewall rules is critical** for its proper usefulness
  - Most restrictive rules should be defined further down the list
  - Firewall rules are read as 'IF-THEN' - if the rule is not met, it jumps to the other rule, and if it is met, it executes the action and exits the firewall
- They do not ensure protection against **social engineering attacks or infections**, in applications or operating system processes



# Firewalls in HMIs and servers

- HMIs and servers in substations, control networks and enterprise networks are mainly based on traditional Operating Systems (OS) **Windows or Linux**
- What is more, many of the industrial components are very dependent on "*legacy OSs*"
  - According to Trend Micro in its report "*Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0*", remarks the prevalence of Windows XP (including 64-bit) whose support ended in 2014 !
    - This situation is due to the "*don't touch a working system*" mentality and the long replacement cycle of hardware and software equipment in industrial control systems
- It is essential to follow the "prohibitive" vision when defining firewall rules
  - Especially to limit unsecured HTTP, FTP or Telnet ports

Source: Trend Micro, Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0, https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf

# Firewalls in Windows 10/11

- Go to Windows 10/11 firewall:
  - 🔎: *Control Panel System and Security* > *Windows Firewall*
    - It will indicate the current status of the firewall Normally it is in "*Enabled*" mode
    - In "Applications and allowed features, it is possible to add new applications or services to the firewall list
  - 🔎: *Windows Firewall with Advanced Security console*, it is also possible to define rules or security policies
    - Select *Inbound Rules*, and then *Action* and *New Rule*
    - Establish the *New Inbound Rule* select *Custom,* and then select *Next*
    - Select the *software path*

Source: Configure rules with group policy, 2024. https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure

# Firewalls in Linux

- Linux incorporates in console, the **ufw** (uncomplicated firewall) firewall by default, running on the command line

| ufw commands |
| --- |
| Install and enable the ufw packages:<br>**$ sudo apt install -y ufw**<br>**$ sudo systemctl enable ufw**<br>**$ sudo systemctl restart ufw**<br>**$ yes \| sudo ufw enable** |
| Set the localisation of the configuration rules:<br>**$ ls /etc/ufw/applications.d/**<br>**$ sudo ufw app list** |
| Display the list of rules:<br>**$ sudo ufw status** |
| Add or delete rules<br>**$ sudo ufw allow/deny ([<puerto>/<protocolo>][<servicios>] [app <apps>])**<br>**$ sudo ufw delete allow/deny ([<puerto>/<protocolo>][<servicios>] [app <apps>])** |
| Reload firewall rules:<br>**$ sudo ufw reload** |
| Enable or disable logging (log is generated in */var/log/ufw.log*):<br>**$ sudo ufw logging on**<br>**$ sudo ufw logging off** |
| Reset firewall policies:<br>**$ sudo ufw reset** |

```
❯ sudo ufw status numbered

Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80                         DENY IN     Anywhere
[ 2] 80                         DENY OUT    Anywhere                   (out)
[ 3] 80 (v6)                    DENY IN     Anywhere (v6)
[ 4] 80 (v6)                    DENY OUT    Anywhere (v6)              (out)
```

Ports


COMMANDS

```
Commands:
 enable                          enables the firewall
 disable                         disables the firewall
 default ARG                     set default policy
 logging LEVEL                   set logging to LEVEL
 allow ARGS                      add allow rule
 deny ARGS                       add deny rule
 reject ARGS                     add reject rule
 limit ARGS                      add limit rule
 delete RULE|NUM                 delete RULE
 insert NUM RULE                 insert RULE at NUM
 prepend RULE                    prepend RULE
 route RULE                      add route RULE
 route delete RULE|NUM           delete route RULE
 route insert NUM RULE           insert route RULE at NUM
 reload                          reload firewall
 reset                           reset firewall
 status                          show firewall status
 status numbered                 show firewall status as numbered list of RULES
 status verbose                  show verbose firewall status
 show ARG                        show firewall report
 version                         display version information

Application profile commands:
 app list                        list application profiles
 app info PROFILE                show information on PROFILE
 app update PROFILE              update PROFILE
 app default ARG                 set default application policy
```

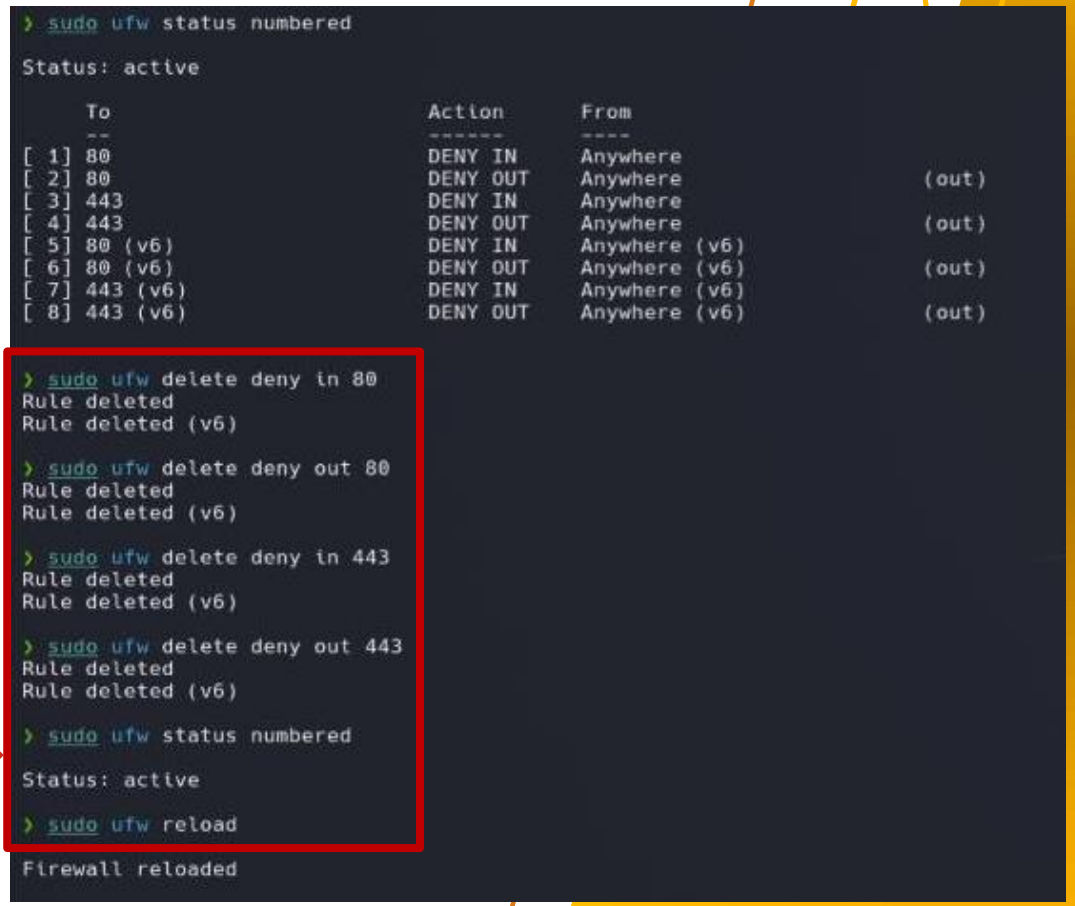
FIREWALLS IN OPERATING SYSTEMS

# Firewalls in Linux - Examples

- Block a specific address
  - **$ sudo ufw deny from 1.1.1.1**
- Block connections to a network interface
  - **$ sudo ufw deny in on eth0 from 15.15.15.51**
- Allow a connection type and service
  - **$ sudo ufw allow ssh**
  - **$ sudo ufw allow 22**
- Allow incoming connections from IP/subnet
  - **$ sudo ufw allow from 1.1.1.0/24 to any port 22**
- Allow incoming HTTP and HTTPS traffic
  - **$ sudo ufw allow http // sudo ufw allow 80**
  - **$ sudo ufw allow https // sudo ufw allow 443**
  - **$ sudo ufw allow proto tcp from any to any port 80,443**
- Allow traffic from an IP/subnet to a specific port
  - **$ sudo ufw allow from 1.1.1.0/24 to any port 3306**

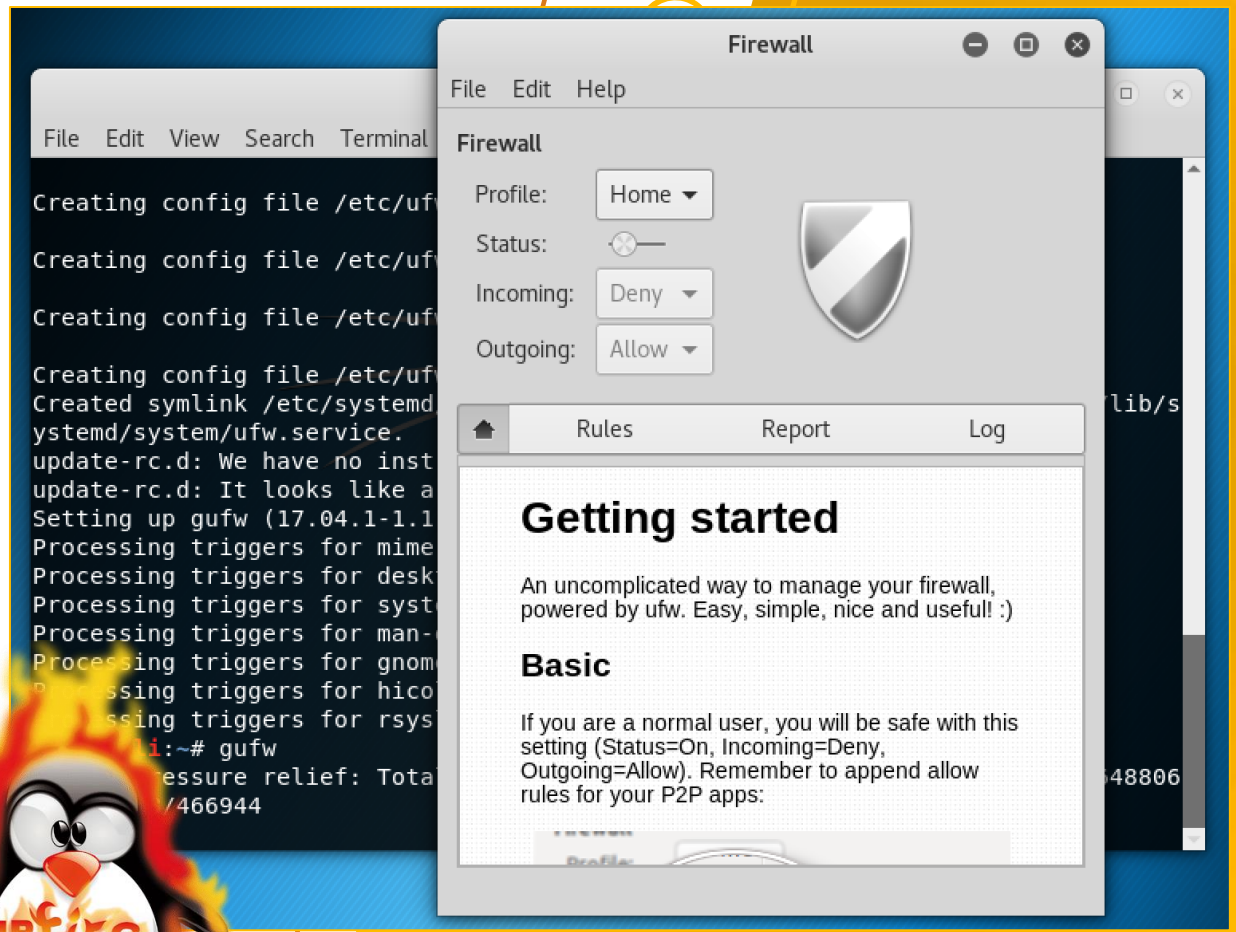
# Firewalls in Linux - Examples

- Deny an incoming port or service
  - **$ sudo ufw deny 25/tcp**
  - **$ sudo ufw deny 143/tcp**
  - **$ sudo ufw deny 993/tcp**
  - **$ sudo ufw deny 110/tcp**
  - **$ sudo ufw deny 995/tcp**
- Deny an outgoing port or service
  - **$ sudo ufw deny out 25/tcp**
  - **$ sudo ufw deny out 143/tcp**
- Deny an outgoing port or service
  - **$ sudo ufw deny out 25/tcp**
  - **$ sudo ufw deny out 143/tcp**
- Remove a particular policy
  - **$ sudo ufw delete deny in 443**
  - **$ sudo ufw status numbered**
  - **$ sudo ufw reload**



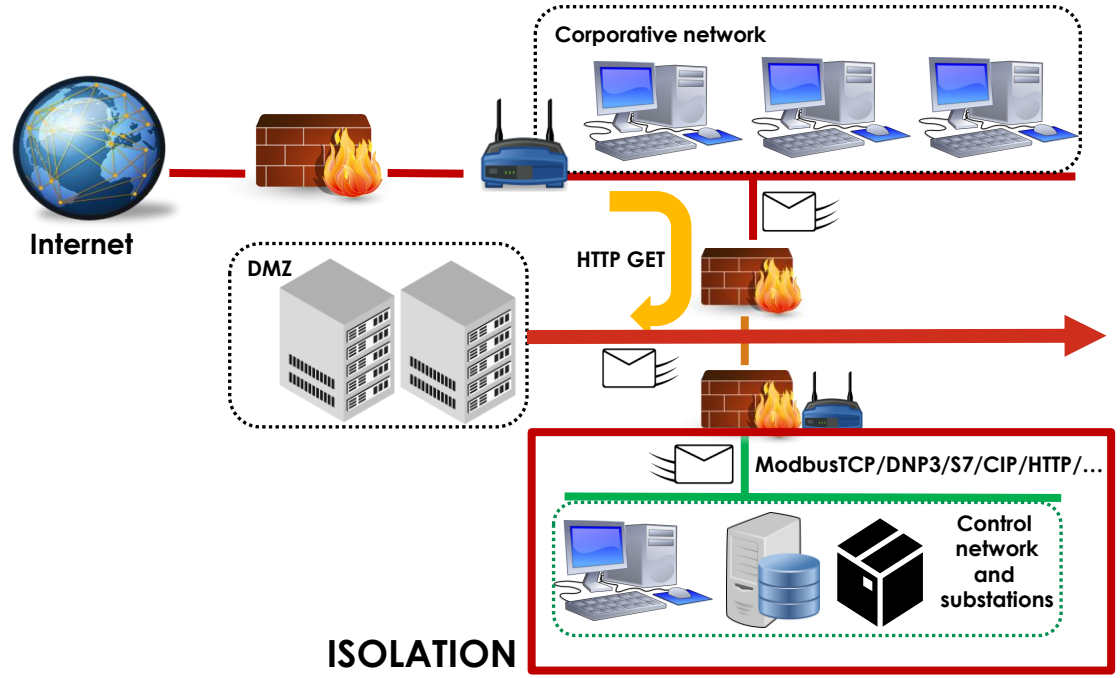
# Firewalls in Linux

- In Linux, it is also possible to use the ufw graphical interface, known as **gufw**
  - Install the ufw GUI interface:
    - **$ sudo apt install –y gufw**
  - Run the GUI under command line interface (CLI):
    - **$ sudo gufw**
- Nonethless, there are other many firewalls for Linux, such as:
  - IPfire
  - Smoothwall
  - IPCop
  - CSF,
  - …




# DMZ in energy control systems

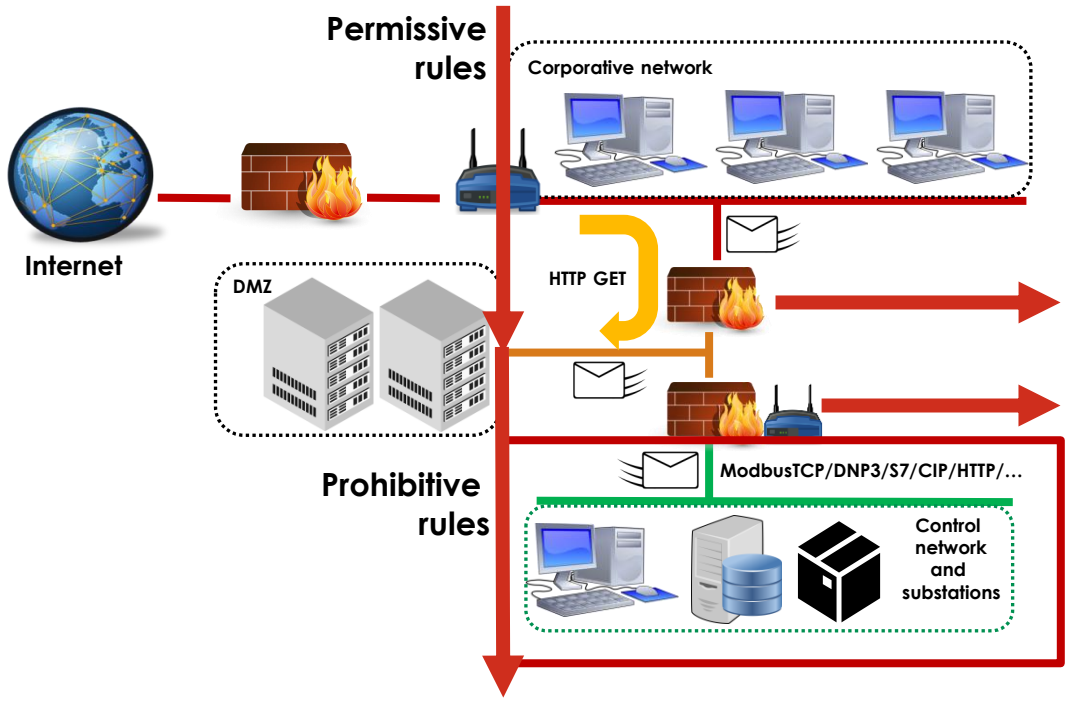
- Through firewall rules, it is possible to isolate control networks from queries to database servers, and from external networks
  - This prevention is through demilitarised zones (DMZ)




As these zones are part of the corporate network, it is necessary to "isolate" the control network from (i) the Internet and from (ii) the DMZ to avoid possible external penetrations from the DMZ

# DMZ in energy control systems

- Through firewall rules, it is possible to isolate control networks from queries to database servers, and from external networks
  - This prevention is through demilitarised zones (DMZ)




Therefore, the specific DMZ rules should be:

- **Permissive**: If connections are coming from the Internet to the DMZ network, or from the DMZ to the Internet
- **Prohibitive**: If connections are coming from the DMZ to the organisation's intranet network

# Access control in energy networks

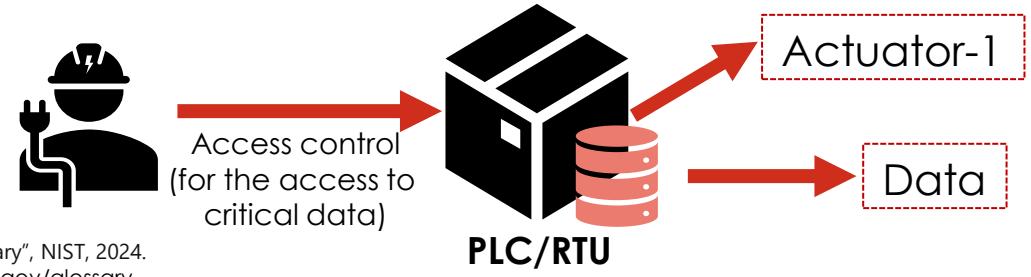
- The European Union Agency for Cybersecurity (ENISA) in "***Appropriate security measures for smart grids***" highlights access control as a priority measure for information systems security and their resources such as:
  - HMIs (including mobile devices), Operating Systems and applications
  - Workstations and servers, such as SCADA servers
  - Controllers, sensors, actuators
  - Databases and files
  - Network infrastructures or systems (e.g., cloud-edge, IIoT, digital twins, blockchain, …)
  - AI models, digital models, digital twins
  - Etc.
- The measures identified by ENISA are based on the ISO/IEC-27002 – ISO/IEC TR 27019, and the NISTIR-7628 for Smart Grids
  - Resulting in the measure: "**Logical access control**" (SM 9.3)
  - This is defined as "*The provider should enforce logical access to authorized entities on smart grid information systems and security perimeters*"

| ID | SM 9.3 |
|---|---|
| Measure | Logical access control. |
| Definition | The provider should enforce logical access to authorized entities on smart grid information systems and security perimeters. |
| Example | [From NERC CIP-003-4 - Requirement 5. Access Control] The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.<br>[From IEC 62443 - 4.3.3.7.2 Establish appropriate logical and physical permission methods to access IACS devices] The permission to access industrial automation and control system devices shall be logical (rules that grant or deny access to known users based on their roles). |

Source: ENISA, "Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation", 2012.
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

# Access control in energy networks

- To understand the "**access control**" concept, the National Institute of Standards and Technology (NIST) defines it as:
  - "*The process of **permitting or restricting access** to applications **at a granular level**, such as per-user, per-group, and per-resources*"
- The process involves two further actions:
  - **Authentication**: "*Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system*"
  - **Authorisation**: "*Access privileges granted to a user, program, or process or the act of granting those privileges*"
- This also means that human operators/users must first prove their identity and then verify their permissions to gain access to the requested resources




Source: CSRC, "Glossary", NIST, 2024.
URL: https://csrc.nist.gov/glossary

E.g., using the security credentials such as username/password, pin, smartcard, digital certificates, etc.

Note that authentication will be detailed in the next Topic, and here we will explore only the authorisation part

ACCESS CONTROL IN ENERGY SYSTEMS

# Authorization in energy networks

- To guarantee "access control", ENISA also adds in SM 9.3 some recommendations:

| Some recommendations related to authorization (local and remote) | To do this, it is necessary to: |
|---|---|
| • **Allowed methods of access control** are identified and documented<br>• Smart grid information system **enforces assigned authorizations for controlling access** to the smart grid information system **in accordance with organization-defined policy**<br>• User accounts **are granted with the most restrictive set of rights and privileges or access** needed for the performance of specified tasks | • Identify **authentication type and authorization schema**<br>• Have the list of **users and related access rights** |
| • The **main functions** of the system **are separated** through assigned access authorizations<br>• **Security functions are restricted** to the smallest number of users necessary to ensure the security of the environment | • List of **authorized users who can access to security functions** |

Source: ENISA, "Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation", 2012.
URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

# Authorization in energy networks

- To guarantee "access control", ENISA also adds in SM 9.3 some recommendations:

| Some recommendations related to authorization (local and remote) | To do this, it is necessary to: |
|---|---|
| • **Allowed methods of access control** are identified and documented<br>• Smart grid information system **enforces assigned authorizations for controlling access** to the smart grid information system **in accordance with organization-defined policy**<br>• User accounts **are granted with the most restrictive set of rights and privileges or access** needed for the performance of specified tasks | • Identify **authentication type and authorization schema**<br>• Have the list of **users and related access rights** |
| • The **main functions** of the system **are separated** through assigned access authorizations<br>• **Security functions are restricted** to the smallest number of users necessary to ensure the security of the environment | • List of **authorized users who can access to security functions** |

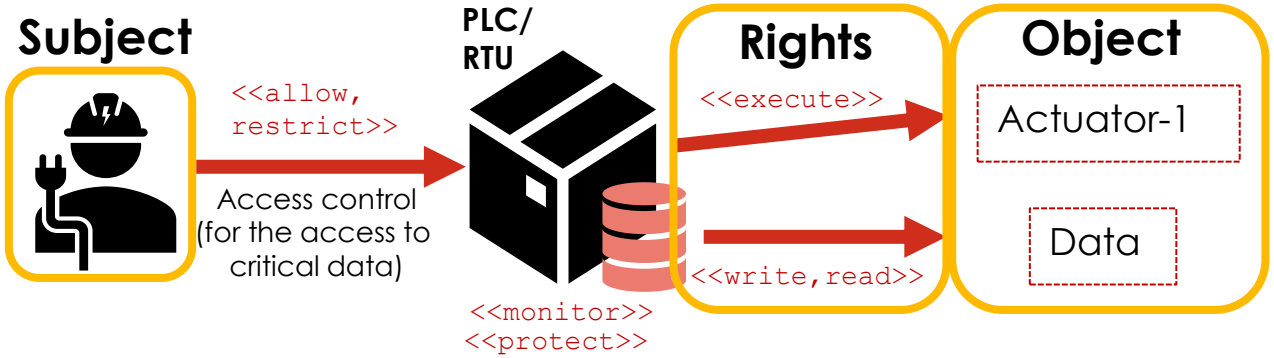
- Thus, it is necessary to identify the users, the objects to be protected, the methods and the rights to access the object

WHO – WHAT – HOW

Source: ENISA, "Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation", 2012. URL: https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

# Authorization in energy networks

- Indeed, when defining an access control policy, **methods or mechanisms** are needed to implement compliance with those security criteria that:
  - Allow, restrict
  - Monitor, protect
- The basic elements of an access control mechanism are:
  - **Object**: Resource to which access is controlled – e.g., PLC/RTU
  - **Subject**: Entity that potentially accesses the objects - Operator
  - **Access right**: Describes the way in which the subject could gain access the object: read, write, execute, delete, create, ...




ACCESS CONTROL IN ENERGY SYSTEMS

# Typical authorization mechanisms

- Access control mechanisms are mainly divided into several categories:

| DAC (Discretionary Access Control) | MAC (Mandatory Access Control) | RBAC (Role-based Access Control) | ABAC (Attribute-Based Access Control) |
|---|---|---|---|
| Based on the **requester identity and access rules** (which indicate which requesters are or are not allowed to do something) | Based on comparing **security labels** (indicating the criticality of the resources) **with security authorisations** indicating the security authorisations (stating which entities are allowed to access certain resources) | Based on the **role that each user has** within the system, **and rules** that remark which accesses are allowed to those who have a certain role | based on **attributes associated with the user** and, depending on the attribute, access to a system is allowed or not |

# Typical authorization mechanisms

- Access control mechanisms are mainly divided into several categories:

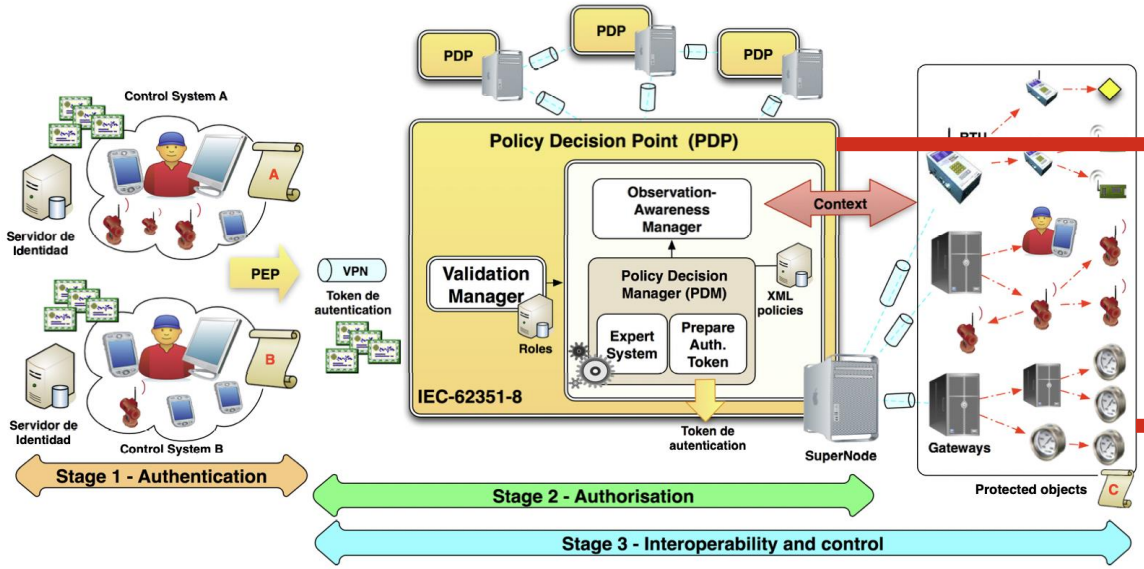
| DAC (Discretionary Access Control) | MAC (Mandatory Access Control) | RBAC (Role-based Access Control) | ABAC (Attribute-Based Access Control) |
|---|---|---|---|
| Based on the **requester identity and access rules** (which indicate which requesters are or are not allowed to do something) | Based on comparing **security labels** (indicating the criticality of the resources) **with security authorisations** indicating the security authorisations (stating which entities are allowed to access certain resources) | Based on the **role that each user has** within the system, **and rules** that remark which accesses are allowed to those who have a certain role | based on **attributes associated with the user** and, depending on the attribute, access to a system is allowed or not |

- These policies are not mutually exclusive
  - DAC + MAC; DAC + RBAC + ABAC; RBAC + ABAC; DAC + MAC + RBAC + ABAC …
- Due to the critical nature of the energy control systems, it is also important to store records of the accesses performed
  - This process will benefit **traceability and auditing** in the event of unwanted access to resources

**ACCOUNTABILITY**
Data traceability ➔ auditing

# Example (I) of an access control architecture for Smart Grid environments

- In C. Alcaraz *et al.*'s work, an access control architecture, which uses a set of terms such as "access control
  - **Policy Enforcement point (PEP)** at which the policy is applied
  - **Policy decision point (PDP)** at which the above mechanisms are implemented such as RBAC (roles extracted from IEC 62351-8) + ABAC (contextual states of the substations)




IEC 62351

| Roles | Rights associated with IEC-62351-8 roles | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | View | Read | Dataset | Reporting | Fileread | Filewrite | Filemgnt | Control | Config | Settinggroup | Security |
| Viewer[a] | ✓ | | | ✓ | | | | | | | |
| Operator[b] | ✓ | ✓ | | ✓ | | | | ✓ | | | |
| Engineer[c] | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | | ✓ | | |
| Installer[d] | ✓ | ✓ | | ✓ | | ✓ | | | ✓ | | |
| SECADM[e] | ✓ | ✓ | ✓ | | | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| SECAUD[f] | ✓ | ✓ | | ✓ | ✓ | | | | | | |
| RBACMNT[g] | ✓ | ✓ | | | | | ✓ | | ✓ | ✓ | |

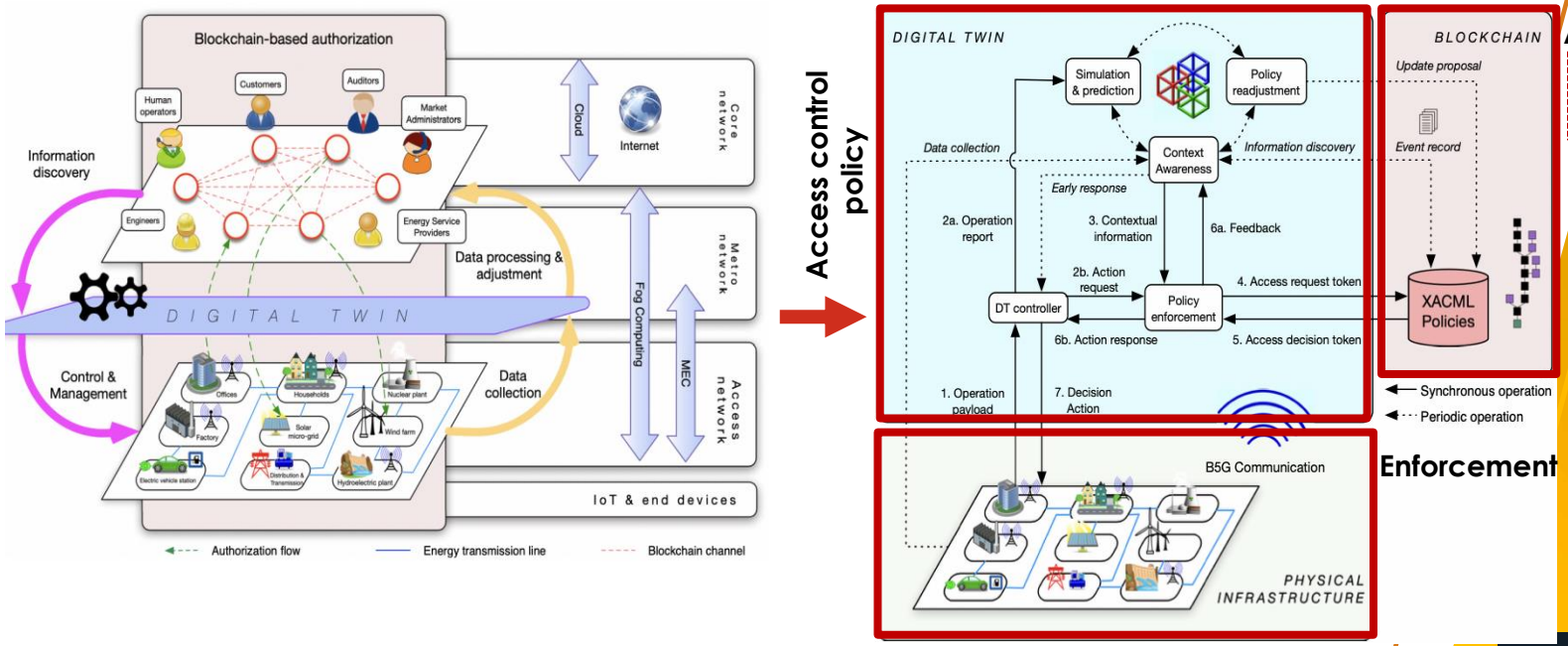
Depending on the status of each substation, certain users with certain roles and permissions will be able to access

For example, in substations completely affected by an attack, only operators or engineers will be able to access, in order to mitigate the effect and return the system to a stable state

Source: C. Alcaraz, J. Lopez, and S. Wolthusen, "Policy Enforcement System for Secure Interoperable Control in Distributed Smart Grid Systems", Journal of Network and Computer Applications, vol. 59, pp. 301314, 2016.

# Example (II) of an access control architecture for Smart Grid environments

- In J. Lopez *et al.*'s work, another access control architecture, whose policies are updated by digital twins:
  - Simulation: Predict the best policy to be applied based on RBAC+ABAC
  - Blockchain: Maintain records related to attributes of user and context
  - 5G/6G + Cloud-edge: Facilitate the policy enforcement in real-time




**Accountability**

- Abuses by malicious or careless users
- Contextual states of substations, microgrids and DERs

**Enforcement**

Source: J. Lopez, J. E. Rubio, and C. Alcaraz, "Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid", IEEE Wireless Communications, vol. 28, pp. 48-55, 2021.

# Final remarks

- Energy systems and their control infrastructures should be based on the well-known **firewalls**
  - Thus, the concept of the technology and its evolution through, its four generations, has been introduced
  - Also, both advantages and disadvantages for control systems have been highlighted, emphasising the difficulty of managing multiple industrial communication protocols
  - Finally, operating system firewalls were introduced, as well as the concept of DMZ, very useful for those corporate environments that make public access to local servers, such as web servers, databases, repositories, etc.
- But, in addition, existing **access control models** must be considered:
  - There are many traditional mechanisms that can be applied (DAC, MAC, RBAC, ABAC), but also ways to combine them with the new technologies
  - Through the new technologies (digital twins, blockchain, 5G/6G and cloud-fog-edge), we could enrich the potential features of access control policies and their main functions
- Last but not least, it is always advisable to take into account the recommendations provided by existing standards and guidelines

# References and sources


1. T. Piens, K. Wens, Mastering Palo Alto Networks, Build, Configure, and Deploy Network Solutions for Your Infrastructure Using Features of PAN-OS, 2022
2. Trend Micro, Securing Smart Factories: Threats to Manufacturing Environments in the Era of Industry 4.0, URL: https://documents.trendmicro.com/assets/white_papers/wp-threats-to-manufacturing-environments-in-the-era-of-industry-4.pdf
3. Configure rules with group policy, 2024. URL: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/configure
4. Archlinux, "Uncomplicated Firewall", 2024 URL: https://wiki.archlinux.org/title/Uncomplicated_Firewall
5. Microsoft, Turn on your Windows Defender Firewall, URL: https://learn.microsoft.com/en-us/mem/intune/user-help/you-need-to-enable-defender-firewall-windows
6. ENISA, "Appropriate security measures for smart grids. Guidelines to assess the sophistication of security measures implementation", 2012. URL:https://www.enisa.europa.eu/publications/appropriate-security-measures-for-smart-grids

# References and sources


7. DeepL Translator for proofreading.
   URL: https://www.deepl.com/translator
8. CSRC, "Glossary", NIST, 2024.
   URL:https://csrc.nist.gov/glossary
9. Source: J. Lopez, J. E. Rubio, and C. Alcaraz, "Digital Twins for Intelligent Authorization in the B5G-enabled Smart Grid", IEEE Wireless Communications, vol. 28, pp. 48-55, 2021
10. C. Alcaraz, J. Lopez, and S. Wolthusen, "Policy Enforcement System for Secure Interoperable Control in Distributed Smart Grid Systems", Journal of Network and Computer Applications, vol. 59, pp. 301314, 2016

# Connect with CyberSecPro:
## How to register and other practical information

1. Website:
   www.cybersecpro-project.eu
2. X (Twitter):
   https://twitter.com/CyberSecPro_eu
3. LinkedIn:
   https://www.linkedin.com/company/cybersecpro-euproject/


# Thank you

If you have any questions, please do not hesitate to contact:


- Davide Ferraris
  Substitute Professor
  University of Malaga
  ferraris@uma.es