Cybersecurity Essentials and Management for Energy Sector

CSP001_C_E

PRESENTATION BY:
ANTONIO MUÑOZ
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

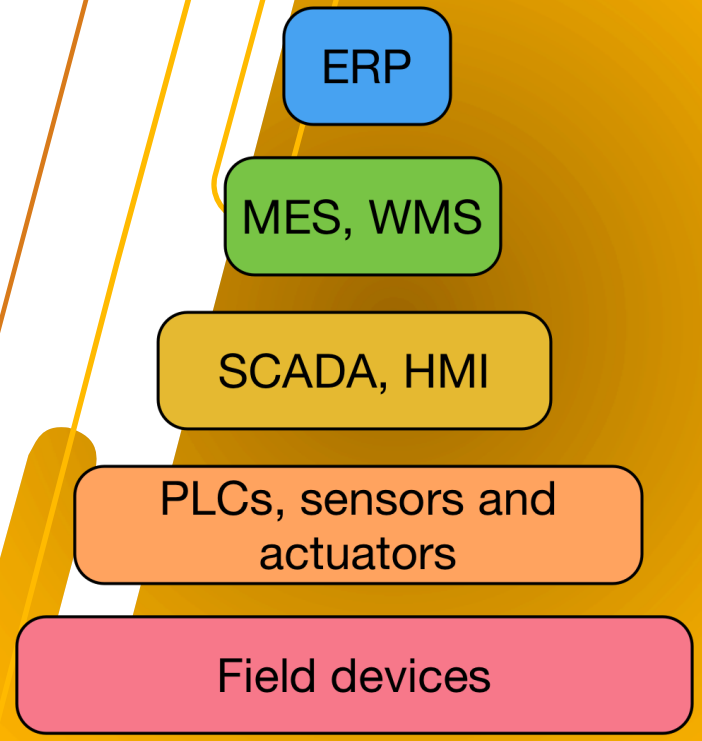
- **Design and implement secure network architectures for energy systems**
- Secure network architecture in Energy Sector including SCADA systems, smart grids, and other critical energy assets
- Utilise network segmentation to isolate critical systems and reduce the impact of cyberattacks
- Configure 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

Main networks in energy systems

- As noted in Topic 2, **Supervisory Control and Data Acquisition (SCADA) systems** are part of the monitoring process of energy systems
  - They are in charge of supervising statuses from the energy infrastructures, their operational processes and their components
  - Their main components are based on cyber-physical elements with the capability of:
    - Perceiving contextual statuses from the observed environment
    - Processing this information, and
    - Acting with the observed environment accordingly

Main networks in energy systems

- As noted in Topic 2, **Supervisory Control and Data Acquisition (SCADA) systems** are part of the monitoring process of energy systems
  - They are in charge of supervising statuses from the energy infrastructures, their operational processes and their components
  - Their main components are based on cyber-physical elements with the capability of:
    - Perceiving contextual statuses from the observed environment
    - Processing this information, and
    - Acting with the observed environment accordingly
- These systems normally follow **hierarchical structures** where:
  - Field devices connect with controllers
  - Controllers connect with SCADA servers and Human-Machine Interfaces (HMIs)
  - SCADA servers with Warehouse Management Systems (WMS)
  - WMS with Enterprise Resource Planning (ERP) servers

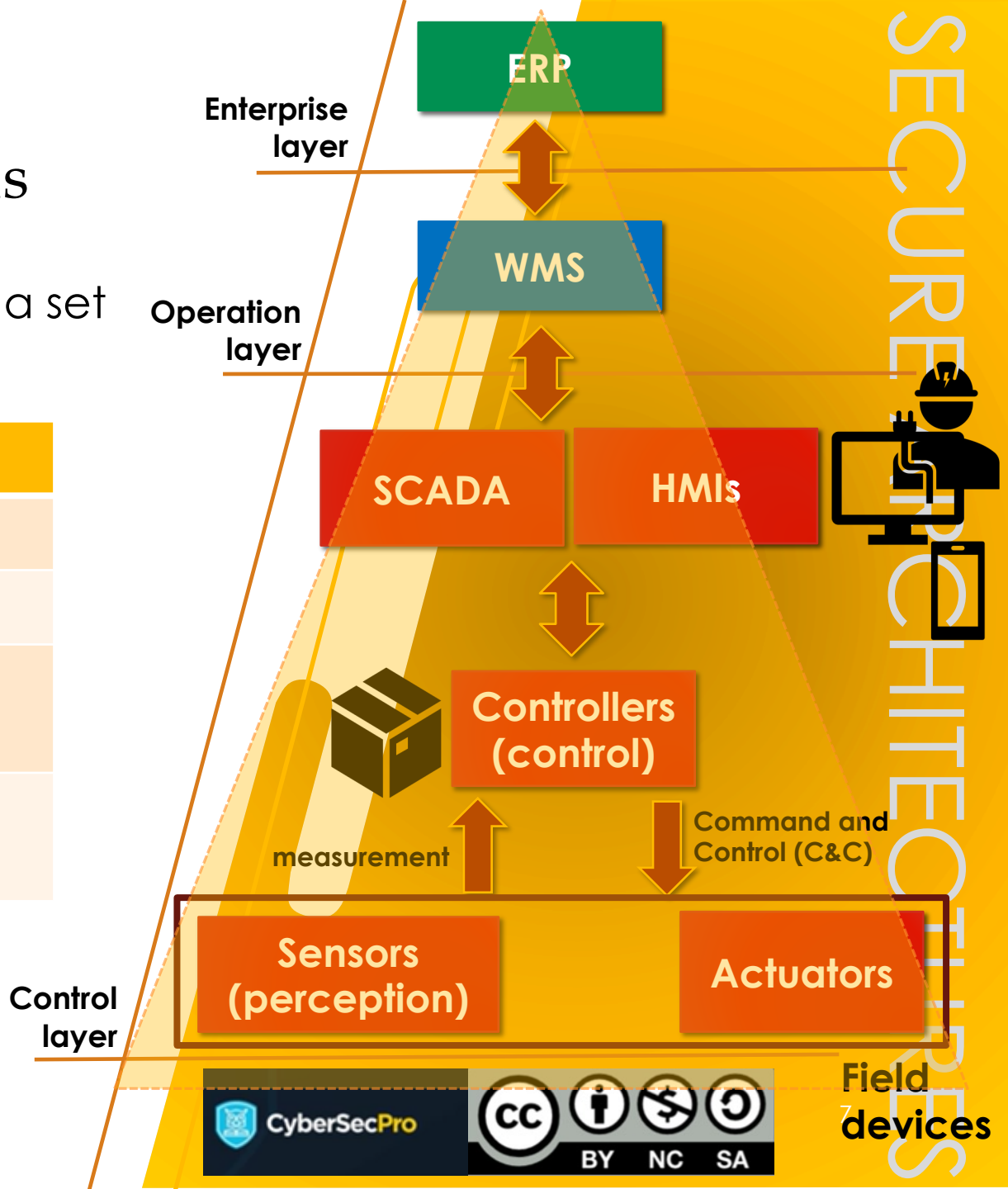


Traditional ISA-95 model

Main networks in energy systems

- This operational hierarchical is composed by a set of functional layers:

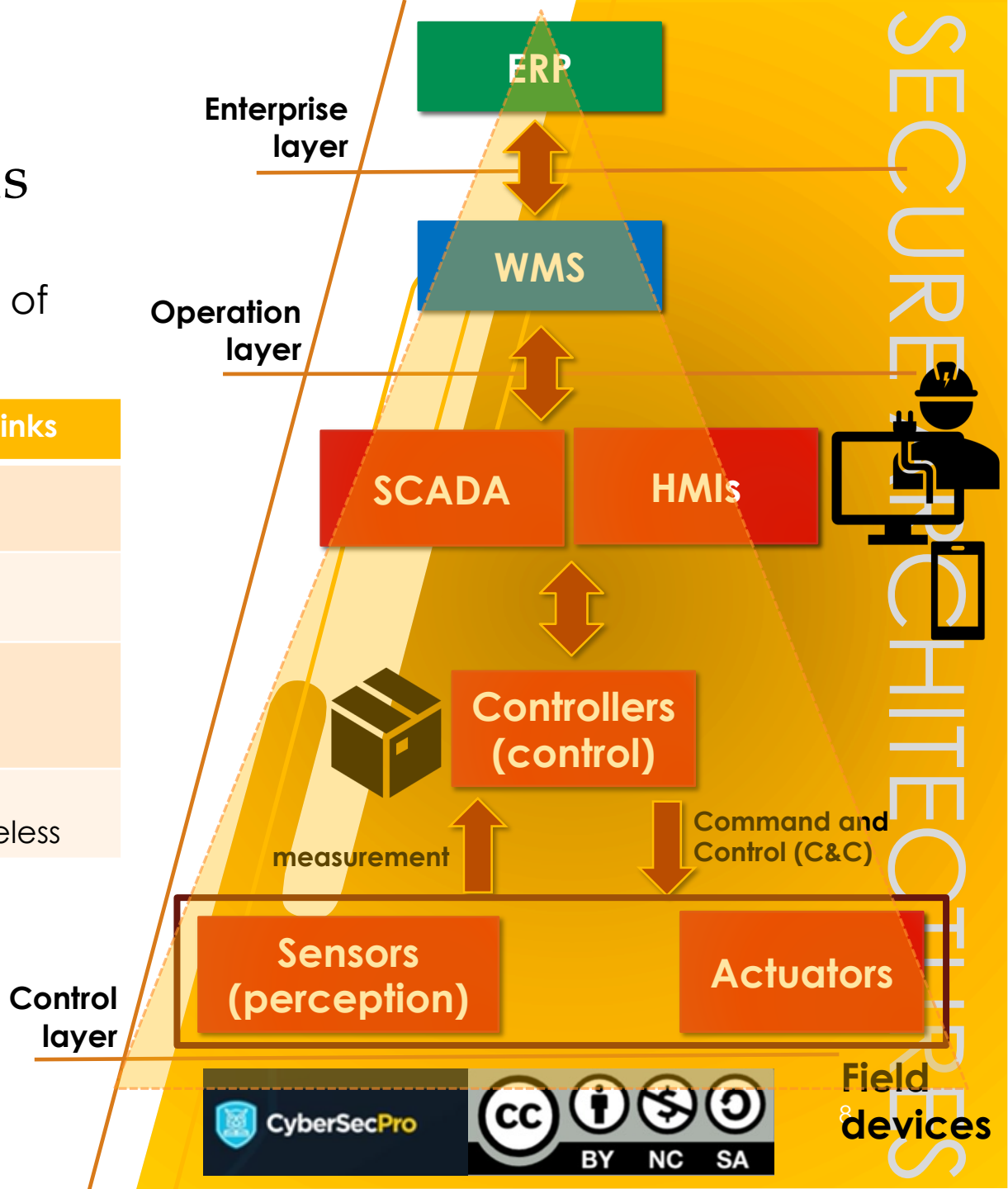
Functional layer	Components
Enterprise layer (ERP)	ERP servers
Operation layer (WMS)	WMS servers
Control layer	SCADA server, HMIs, controllers (PLCs/RTUs)
	Field devices (sensors, actuators)



Main networks in energy systems

- This operational hierarchical is composed by a set of functional layers:

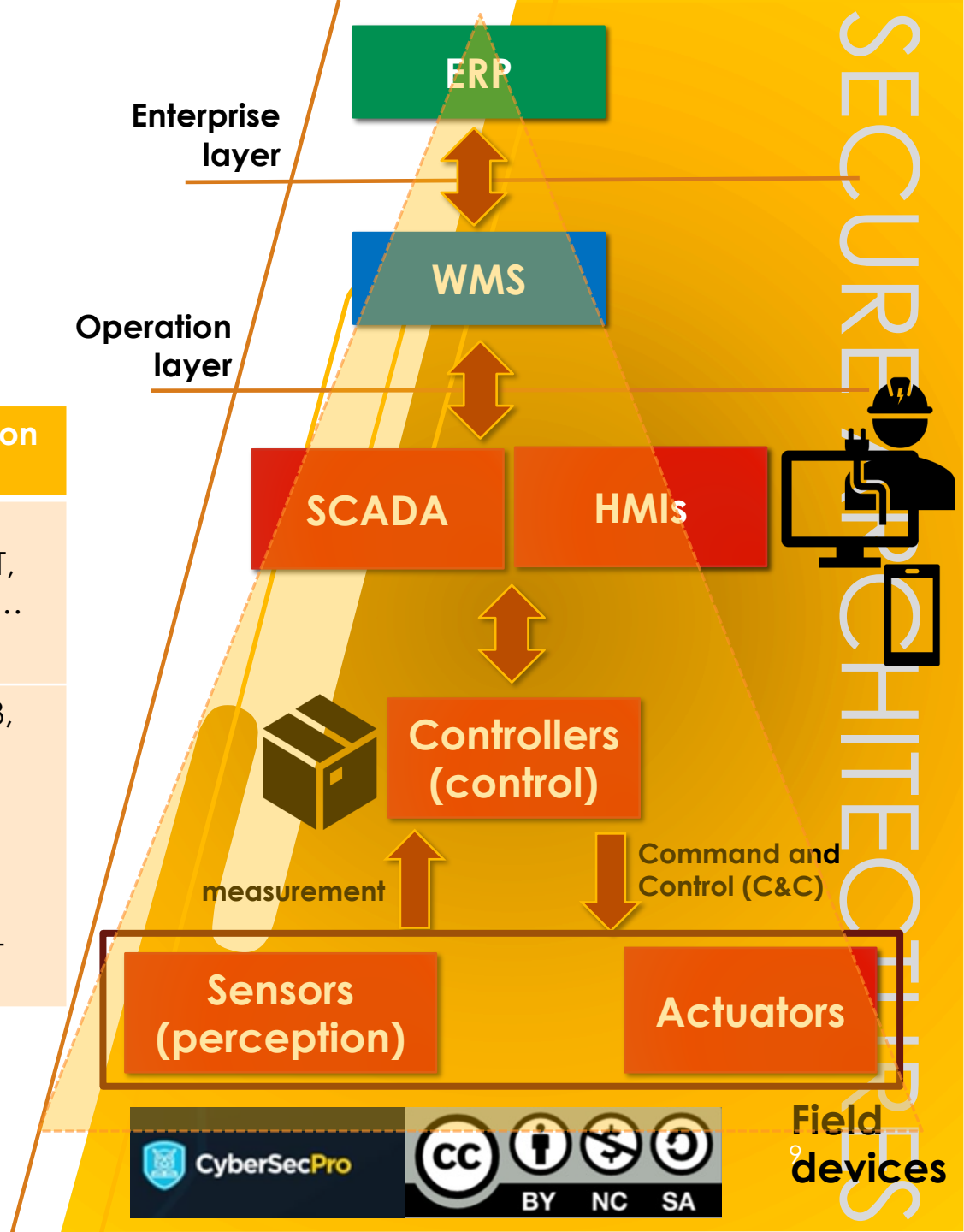
Functional layer	Components	Communication links
Enterprise layer (ERP)	ERP servers	Ethernet, wireless
Operation layer (WMS)	WMS servers	Ethernet, wireless
Control layer	SCADA server, HMIs, controllers (PLCs/RTUs)	Ethernet, wireless
	Field devices (sensors, actuators)	Ethernet, serial communication, wireless



Main networks in energy systems

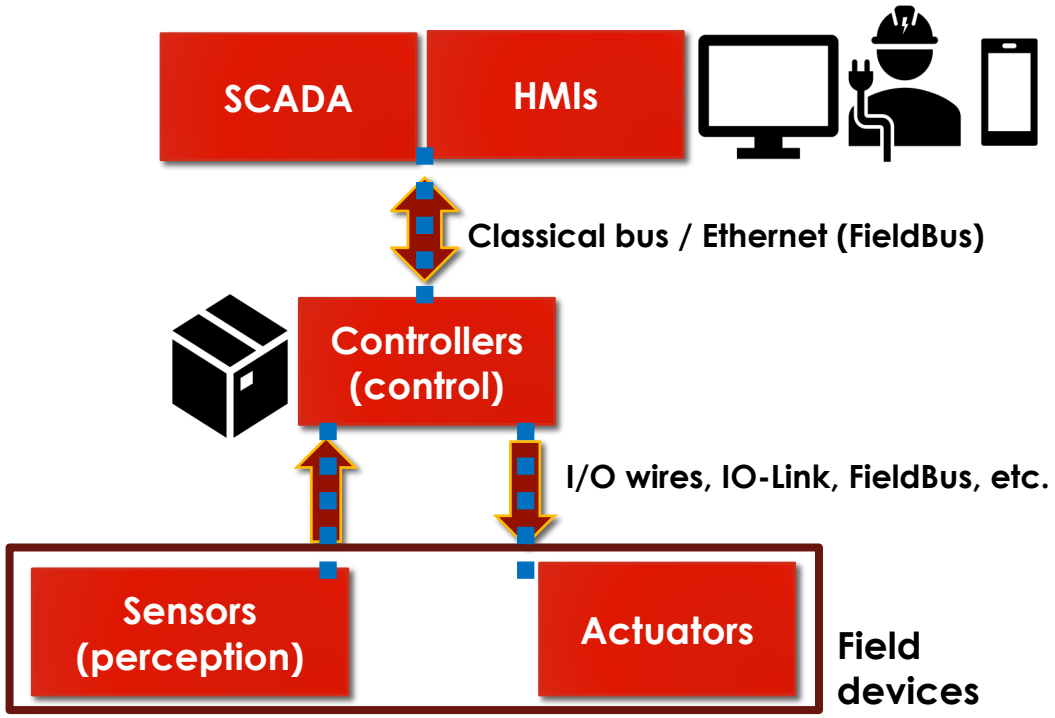
- This operational hierarchical is composed by a set of functional layers:

Functional layer	Components	Communication links	Communication protocols
Enterprise layer (ERP)	ERP servers	Ethernet, wireless	OPC-UA, Woopsa, MQTT, CoAP, AMQP,…
Operation layer (WMS)	WMS servers	Ethernet, wireless	
Control layer	SCADA server, HMIs, controllers (PLCs/RTUs)	Ethernet, wireless	OPC-UA, DNP3, Modbus RTU, ModbusTCP, EthernetIP, EthernetCAT, WirelessHART, ISA100.11a, IO-Link…
	Field devices (sensors, actuators)	Ethernet, serial communication, wireless	



Some comm. protocols and features

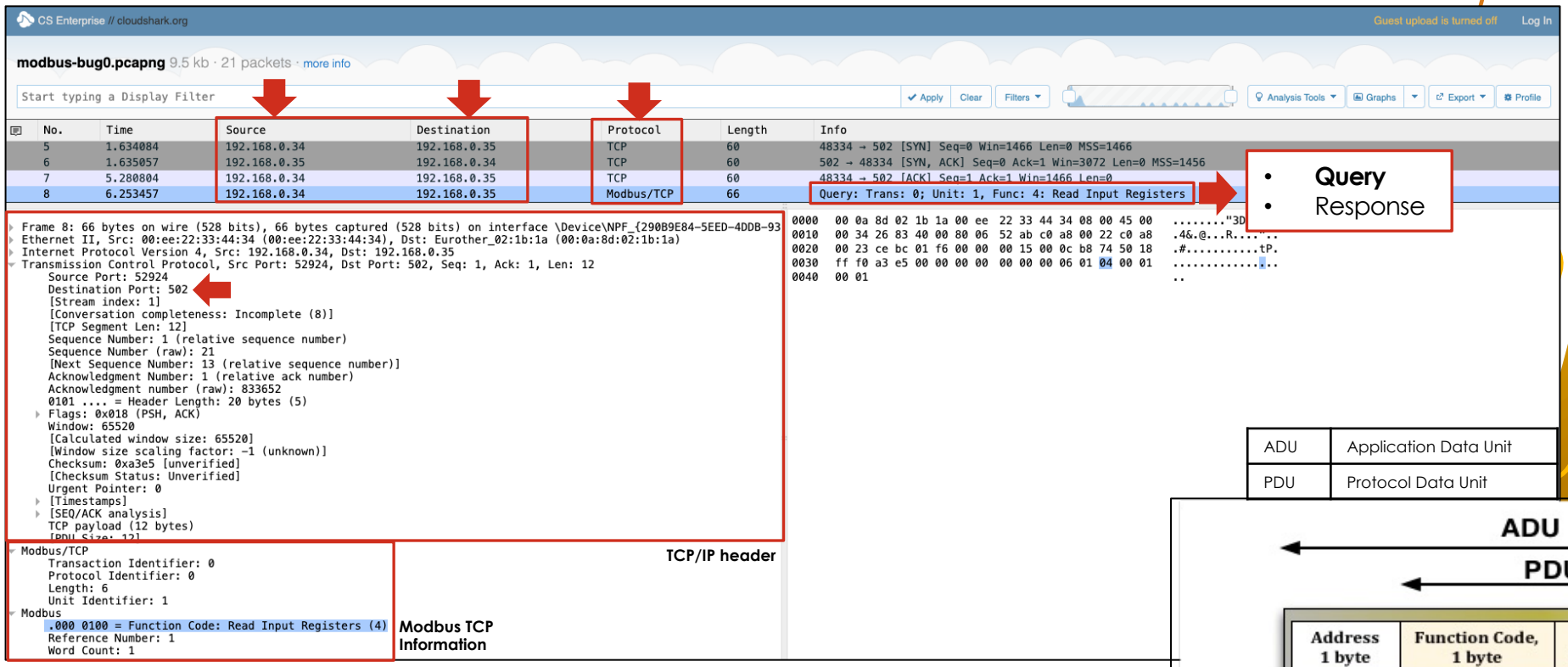
- **Control layer protocols** are composed of a set of CPS devices connected Peer-to-Peer (P2P) or through a comm. bus, following **master-slave connections**, where the master receive information from the slave at regular periods



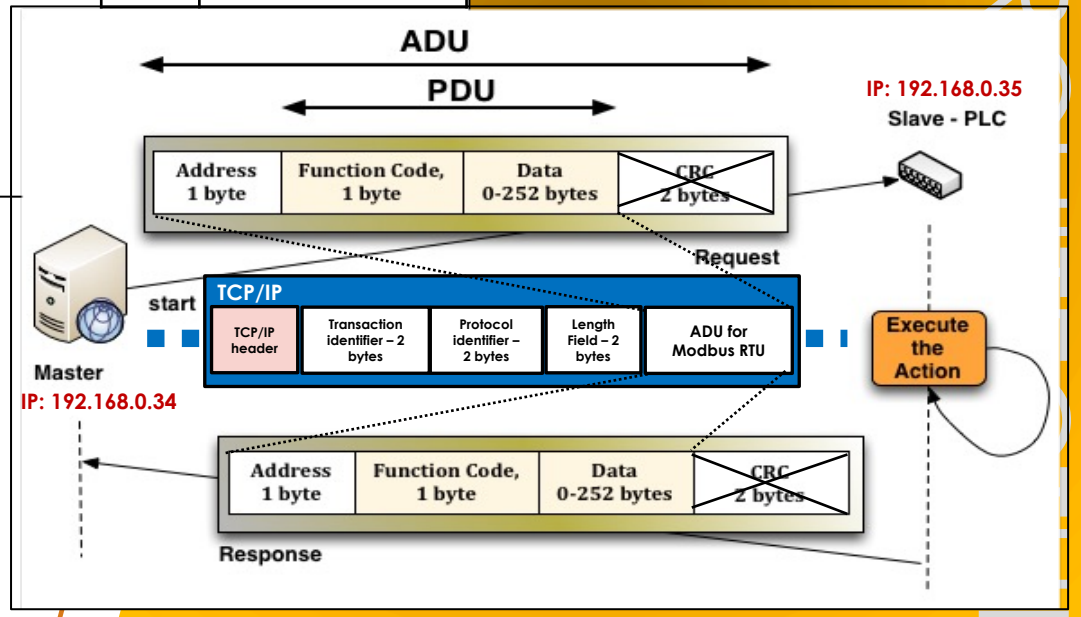
Some comm. protocols and features

- There is a relevant variety of **control layer protocols**, both open-source and proprietary

Some protocols	Communication	Features
IO-Link	• P2P connection	• Controllers and field devices • Management of states and units, offering **diagnosis**, configuration of interfaces, and management of events
Modbus RTU	• Master/slave • Serial comm.	• Controllers and field devices • Uses binary encoding, and adds **CRC (Cyclic Redundancy Check)** control
Modbus ASCII	• Master/slave • Serial comm.	• Controllers and field devices • Provides same goals as Modbus RTU, but applies ASCII characters for the communication
Modbus TCP	• Master/slave • TCP/IP comm.	• Encapsulates Modbus RTU over TCP/IP • **Does not provide confidentiality and authentication** mechanisms, and only verifies determined parts of the packets • **Lacks anti-replay mechanisms** to control DoS attacks • Does not include CRC because it is included by the TCP/IP layers

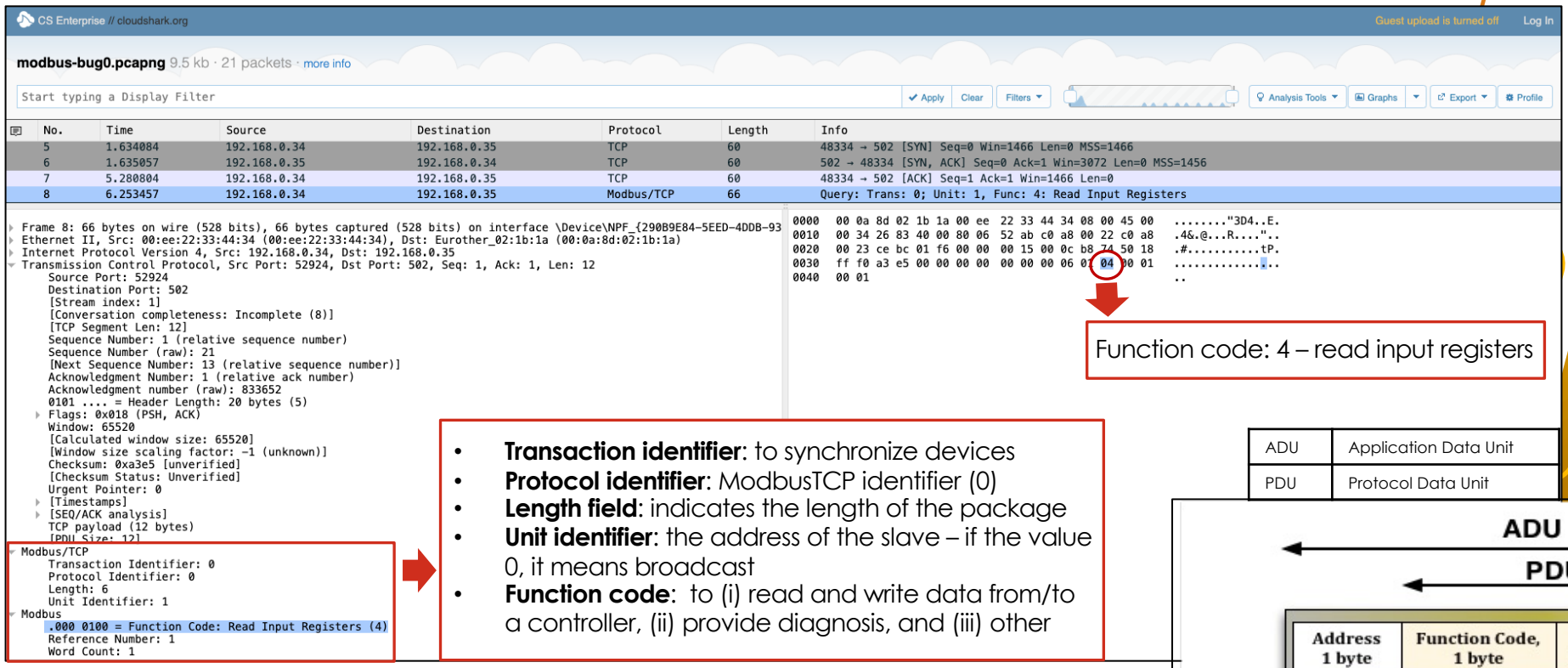


ADU	Application Data Unit
PDU	Protocol Data Unit



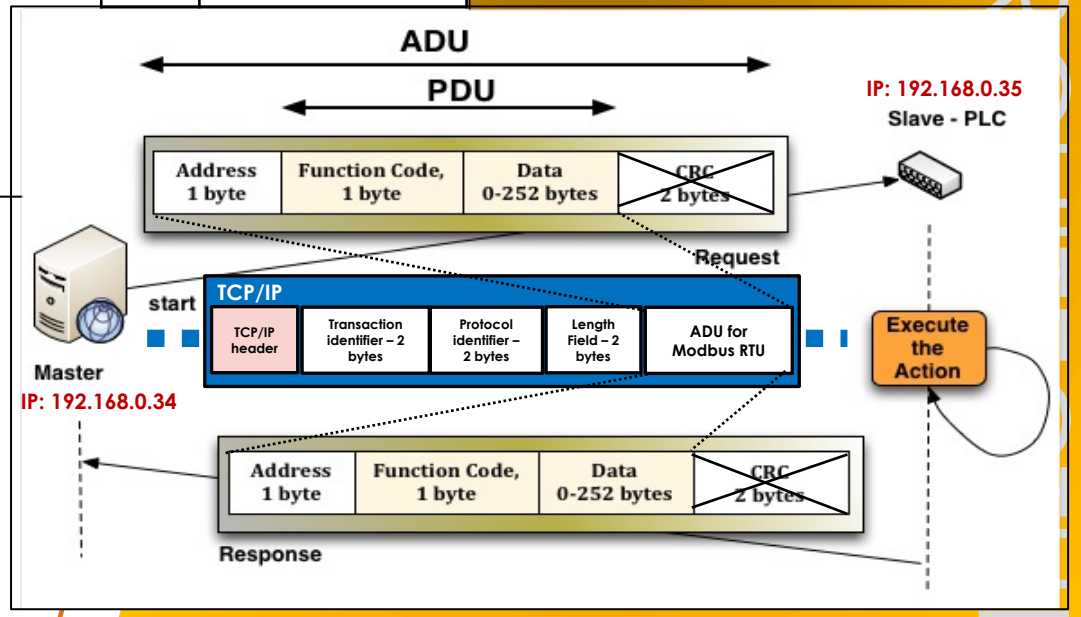
- **ModbusTCP**
  - 1 master can connect to 247 slaves with unique IDs
  - Clients and serves listen and receive data via port 502
  - The Modbus RTU packets are of 256 bytes: 1 byte for address, 1 byte for function code, 0-252 bytes for data and 2 bytes for CRC
  - However, the ModbusTCP ADU adds the MBAP (Modbus App. Protocol) with 7 bytes: 1 byte for Transaction Identifier, 2 bytes for Protocol Identifier, 2 bytes for Length Field and 1 byte for Address (the Unit Identifier == Address of 1 byte in PDU)

Figure source: CloudShark.org – modbus-bug0.pcapng
URL: https://www.cloudshark.org/captures/4b8f9f3579b3



- **Transaction identifier**: to synchronize devices
- **Protocol identifier**: ModbusTCP identifier (0)
- **Length field**: indicates the length of the package
- **Unit identifier**: the address of the slave – if the value 0, it means broadcast
- **Function code**: to (i) read and write data from/to a controller, (ii) provide diagnosis, and (iii) other

ADU	Application Data Unit
PDU	Protocol Data Unit



- **ModbusTCP**
  - 1 master can connect to 247 slaves with unique IDs
  - Clients and serves listen and receive data via port 502
  - The Modbus RTU packets are of 256 bytes: 1 byte for address, 1 byte for function code, 0-252 bytes for data and 2 bytes for CRC
  - However, the ModbusTCP ADU adds the MBAP (Modbus App. Protocol) with 7 bytes: 1 byte for Transaction Identifier, 2 bytes for Protocol Identifier, 2 bytes for Length Field and 1 byte for Address (the Unit Identifier == Address of 1 byte in PDU)

Figure source: CloudShark.org – modbus-bug0.pcapng
URL: https://www.cloudshark.org/captures/4b8f9f3579b3

Some comm. protocols and features

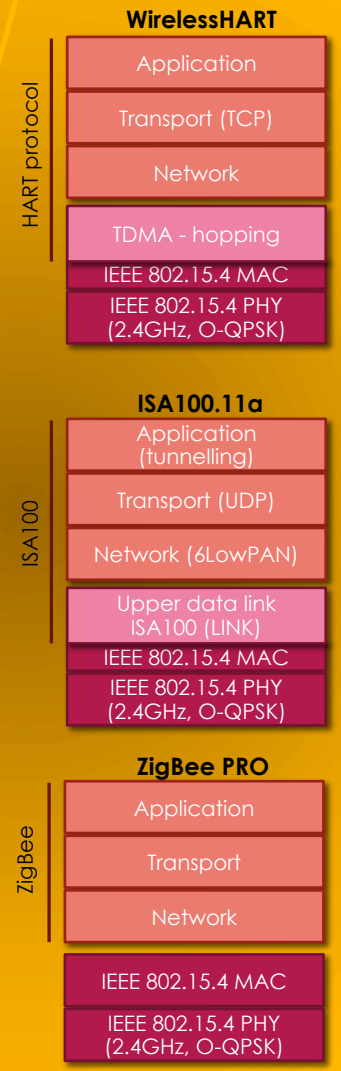
- There is a relevant variety of **control layer protocols**, both open-source and proprietary

Some protocols	Communication	Features
PROFIBUS	• Master/slave • Token-based comm. in multipoint busses	• Offers multiple control services: PROFIsafe with **integrity mechanisms** as support to the operational security, and PROFIdrive for **location-based interaction** with systems
PROFINET	• Works over Ethernet and TCP/IP	• Offers multiple control services: **Diagnosis, alerting,** configuration, maintenance, and synchronization • Extends the PROFIBUS profiles to add extra functionality, so a PROFINET network can control a PROFIBUS network through interfaces PROFINET IO or a proxy
OPC-UA (OPC Unified Architecture)	• Object-based comm., where each device is encapsuled on an object	• Uses data codification based on XML-RPC (XML over HTTP), and is based on two protocols: TCP/IP-based binary protocol for performance in real time, and SOAP-based protocol to manage the network through Web services • Offers service and device discovery, data exchange, **event management and alert**
CIP (Common Industrial Protocol)	• Object-based comm., where each device is encapsuled on an object • Ethernet/IP	• Offers multiple services: Control in real time, operational safety, power control, synchronization and prioritisation, **authentication via TLS/DTLS in Ethernet/IP, access control, integrity and confidentiality**, etc.
HART (Highway Addressable Remote Transducer)	• P2P connection and multipoint bus	• Controllers and field devices based on analogical communications • Data exchange (variables, states, parameters, data, units, configuration)
HART/IP	• Works over HART Ethernet and TCP/IP to encapsulate HART packets	• Enables the integration of a wirelessHART network into a HART network

Some comm. protocols and features

- There is a relevant variety of **control layer protocols**, both open-source and proprietary

Some protocols	Communication	Features
WirelessHART	• P2P comm. and mesh networks • Wireless comm. based on the IEEE **802.15.4** (low-rate wireless personal area networks (LR-WPANs)) • Command-oriented comm. based on the HART (TCP)	• Controllers/gateways and field devices • Offers services for **frequency hopping and blacklisting** methods, and **cryptography and authentication**
ISA100.11a	• P2P comm. and mesh networks • Wireless comm. based on the IEEE **802.15.4** (LR-WPANs) • Object-oriented comm. under UDP • Compatibility with 6LowPAN	• Controllers/gateways and field devices • Offers services for **frequency hopping and blacklisting** methods, and **cryptography and authentication**
ZigBee	• P2P comm. and mesh networks • Wireless comm. based on the IEEE **802.15.4** (LR-WPANs)	• Controllers/gateways and field devices • Offers services for **addressing schemes (stochastic, group), frequency agility**, and **cryptography and authentication**
ETC.	ETC.	ETC.



SECURE ARCHITECTURES

Some comm. protocols and features

- Also, there is a relevant variety of **enterprise and operation layer protocols**, working on different communication infrastructures
  - Cloud and edge-based architectures
  - RESTful-based/REST-based architectures such as CoAP
  - Publish/subscribe-based networks such as MQTT or AMQP

Some protocols	Features
CoAP (Constrained Application Protocol)	• Runs over UDP, so **depends on DTLS**
MQTT (Message Queue Telemetry Transport)	• Runs over TCP based on light headers to reduce energy consumption and bandwidth • **Authentication** is managed by brokers, and through username/password • **Does not provide encryption**, **so depends on TLS**
AMQP (Queuing Protocol Advanced Message)	• Runs over TCP and **depends on TLS** for security • Requires processing and memory to manage multiple queues (probably with duplicated information), so it is not recommended for constrained devices

TLS	Transport Layer Security, providing security on the Transport Layer and over TCP
DTLS	Datagram Transport Layer Security, offering the same security as TLS but over UDP

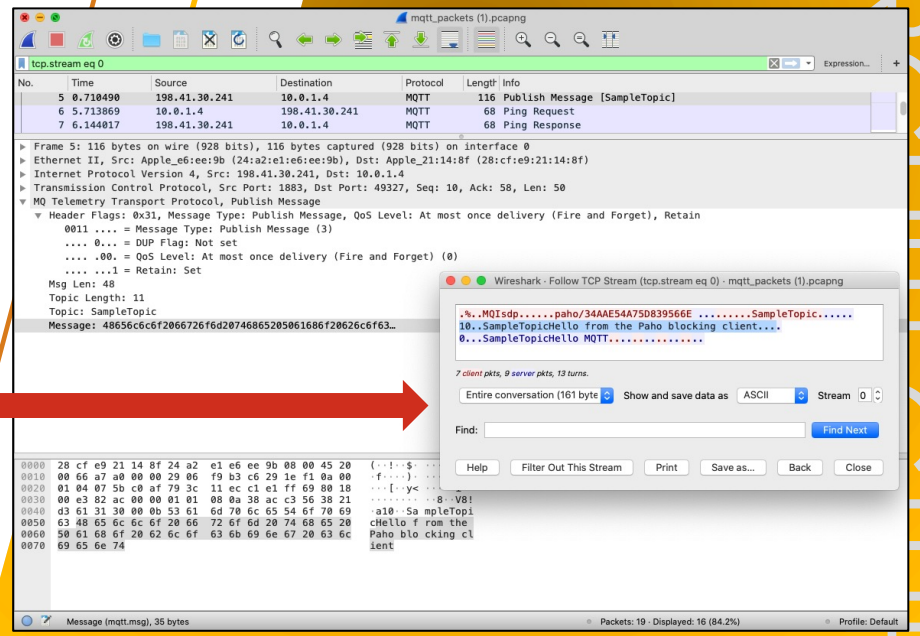
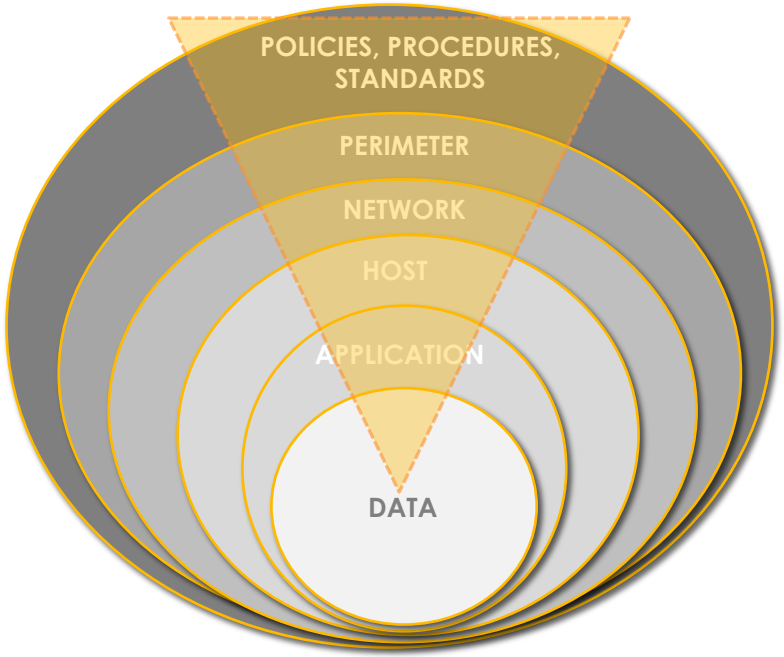


Figure source: Pradeesi, MQTT-Wireshark-Capture
URL: https://github.com/pradeesi/MQTT-Wireshark-Capture/blob/master/mqtt_packets.pcapng

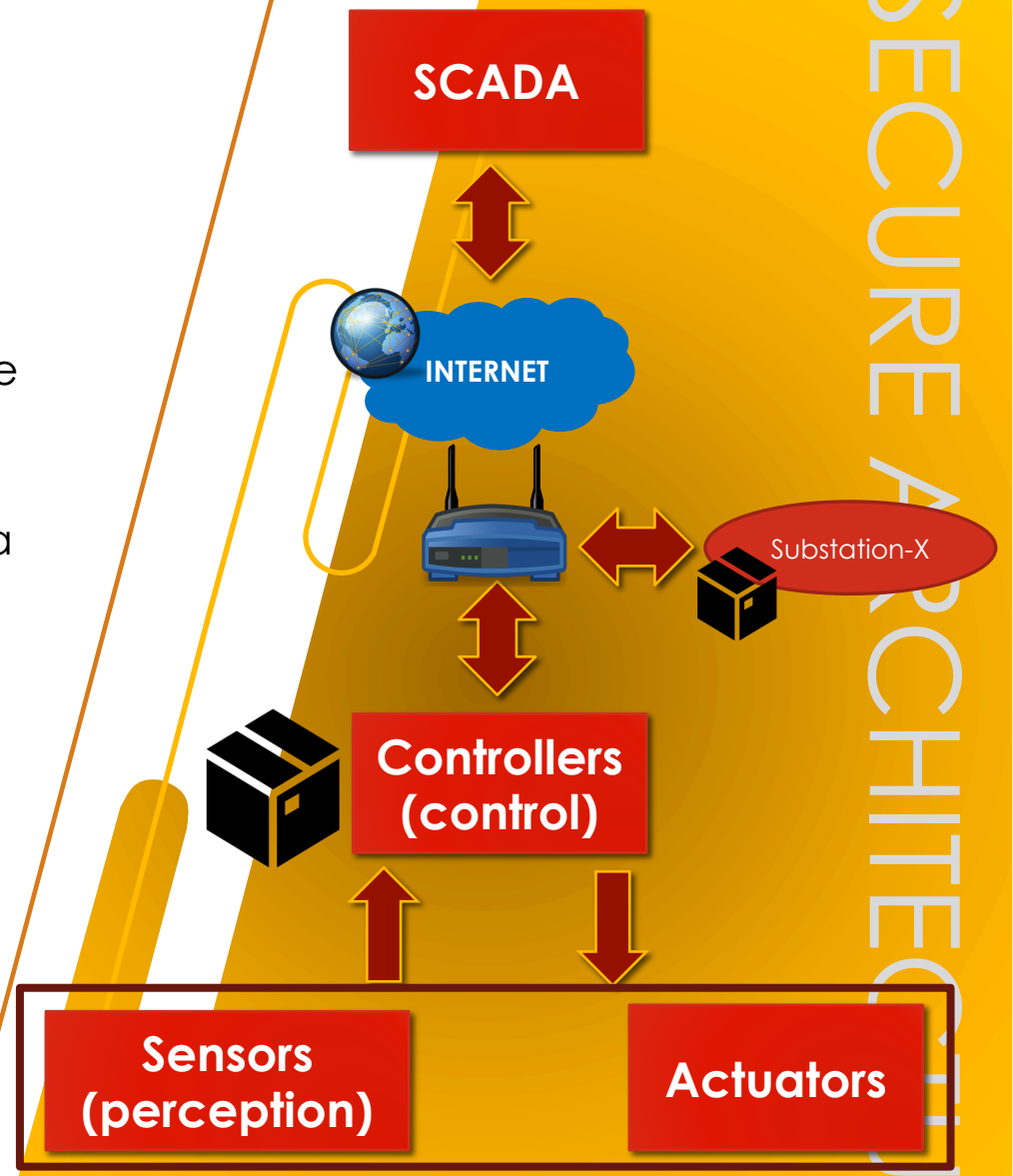
Secure architectures under security principles

- Therefore, there are many protocols that add security measures or rely heavily on external mechanisms, such as TLS/DTLS, for confidentiality, authentication and integrity
  - But even so, it is also necessary to consider other security measures following the good principle of "***defence in depth***"



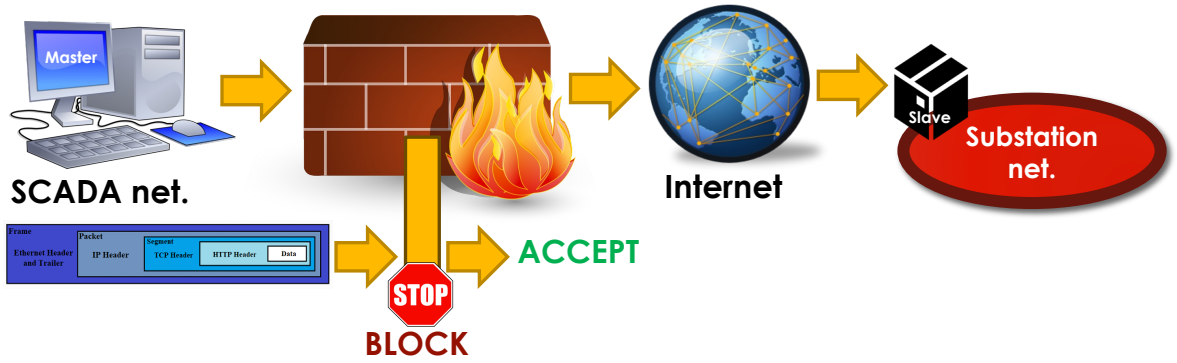
Secure architectures: At the network perimeter level

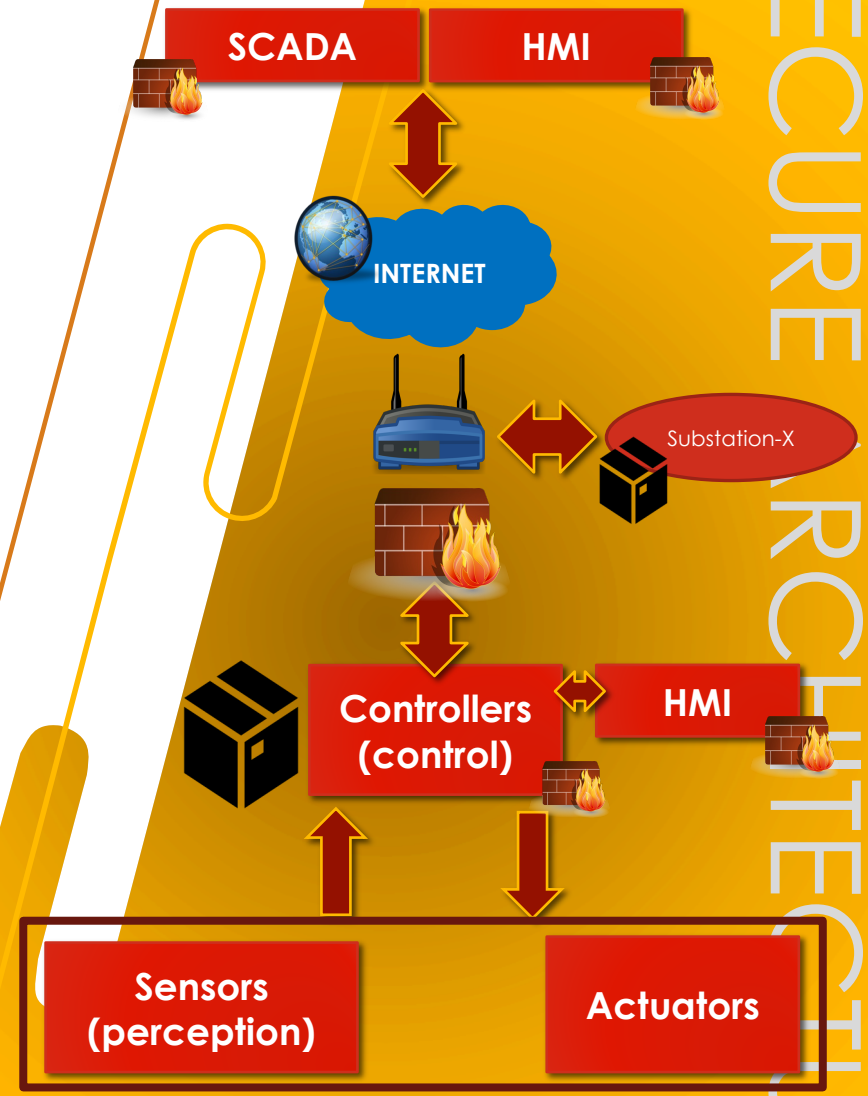
- **Router**:
  - A device capable of filtering network traffic and determining the next route of a packet
  - This filtering capability allows the system to establish connection and access policies, discarding incoming/outgoing packets to a network



Secure architectures: At the network perimeter level

- **Router**:
  - A device capable of filtering network traffic and determining the next route of a packet
  - This filtering capability allows the system to establish connection and access policies, discarding incoming/outgoing packets to a network
- **Firewall**:
  - A HW/SW component capable of filtering incoming/outgoing packets through a set of firewall rules
  - These rules establish which network traffic can (and cannot) access the system, such as substations or the SCADA network

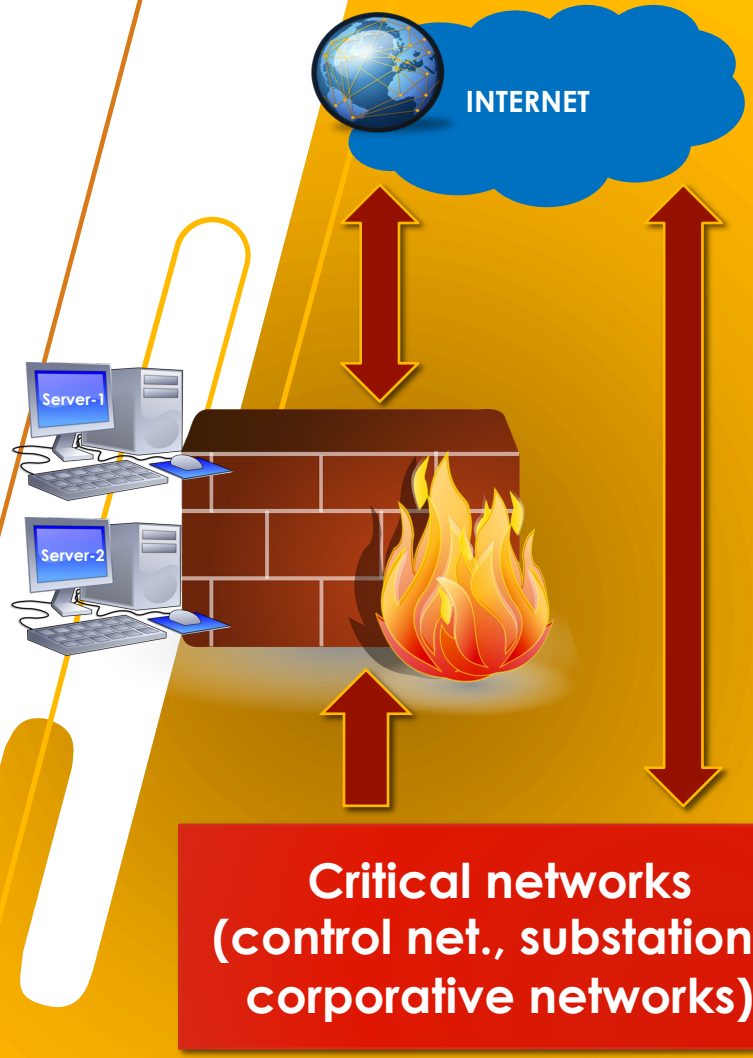




SECURE ARCHITECTURES

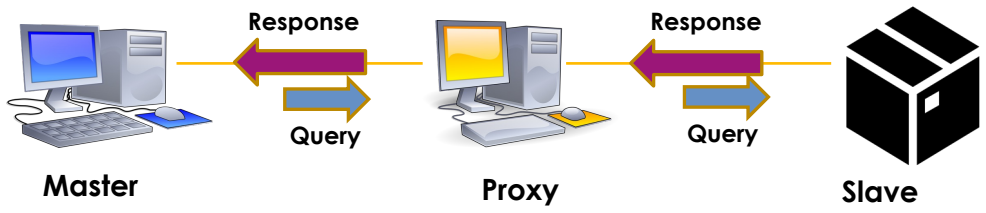
Secure architectures: At the network perimeter level

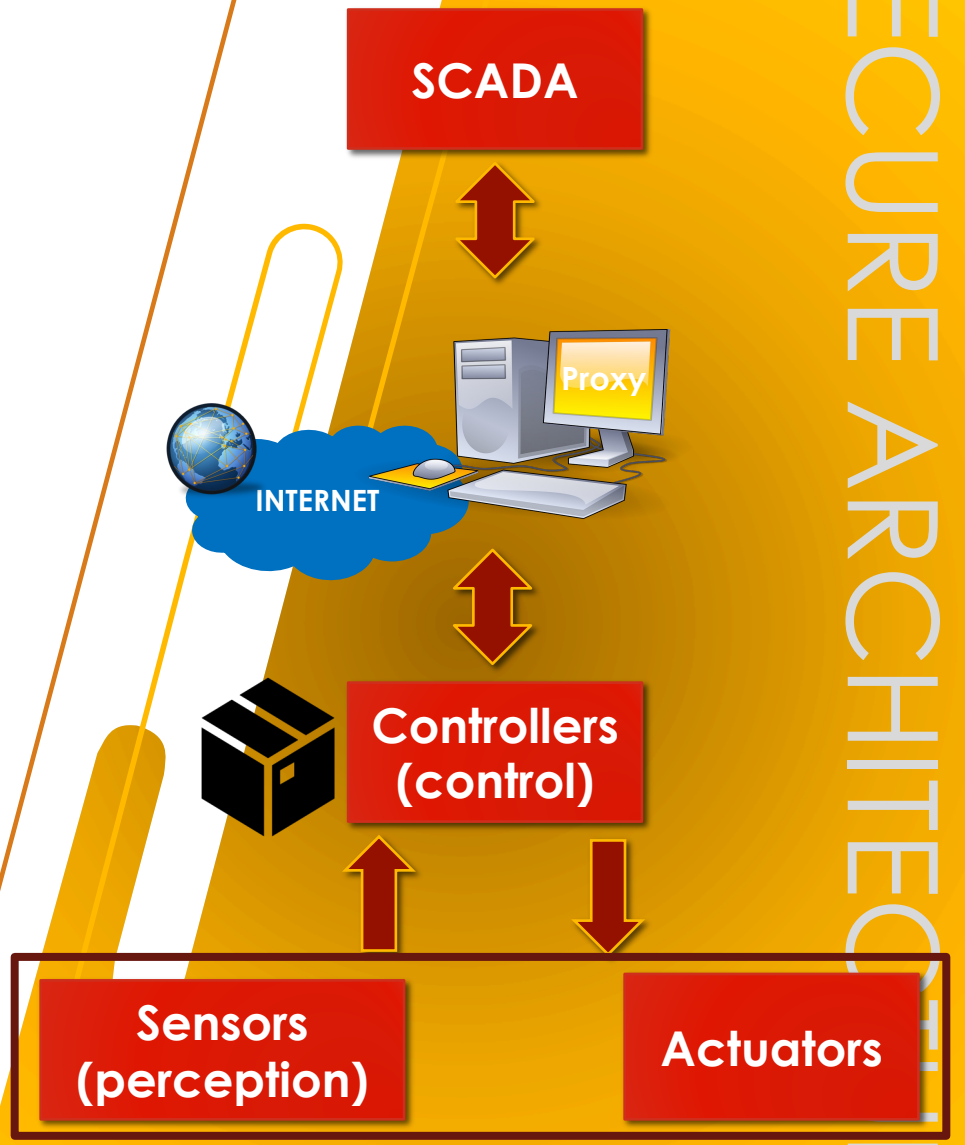
- **Router**:
  - A device capable of filtering network traffic and determining the next route of a packet
  - This filtering capability allows the system to establish connection and access policies, discarding incoming/outgoing packets to a network
- **Firewall**:
  - A HW/SW component capable of filtering incoming/outgoing packets through a set of firewall rules
  - These rules establish which network traffic can (and cannot) access the system, such as substations or the SCADA network
- **DMZ (Demilitarised Zone)**:
  - It creates subnets composed of servers that must be queried from external networks such as the Internet - *useful for corporative networks*
  - Therefore, DMZs are based on firewall rules that isolate the security network from other networks



Secure architectures: At the network perimeter level

- **Proxy**:
  - An intermediary device between a client node and a server (e.g. between a master and a slave), capable of adding additional security measures
    - E.g. hiding the IPs of nodes deployed in vulnerable networks, such as substations
  - This hiding process consists of replacing the IPs of the vulnerable nodes with the IP of the proxy:
    - All incoming traffic to a controller IP is protected through the Internet by using the IP of the proxy in the packets
    - All outgoing traffic from a controller IP to the master is protected by replacing this IP with the proxy IP
  - This type of protection subsequently avoids *passive traffic analysis* attacks

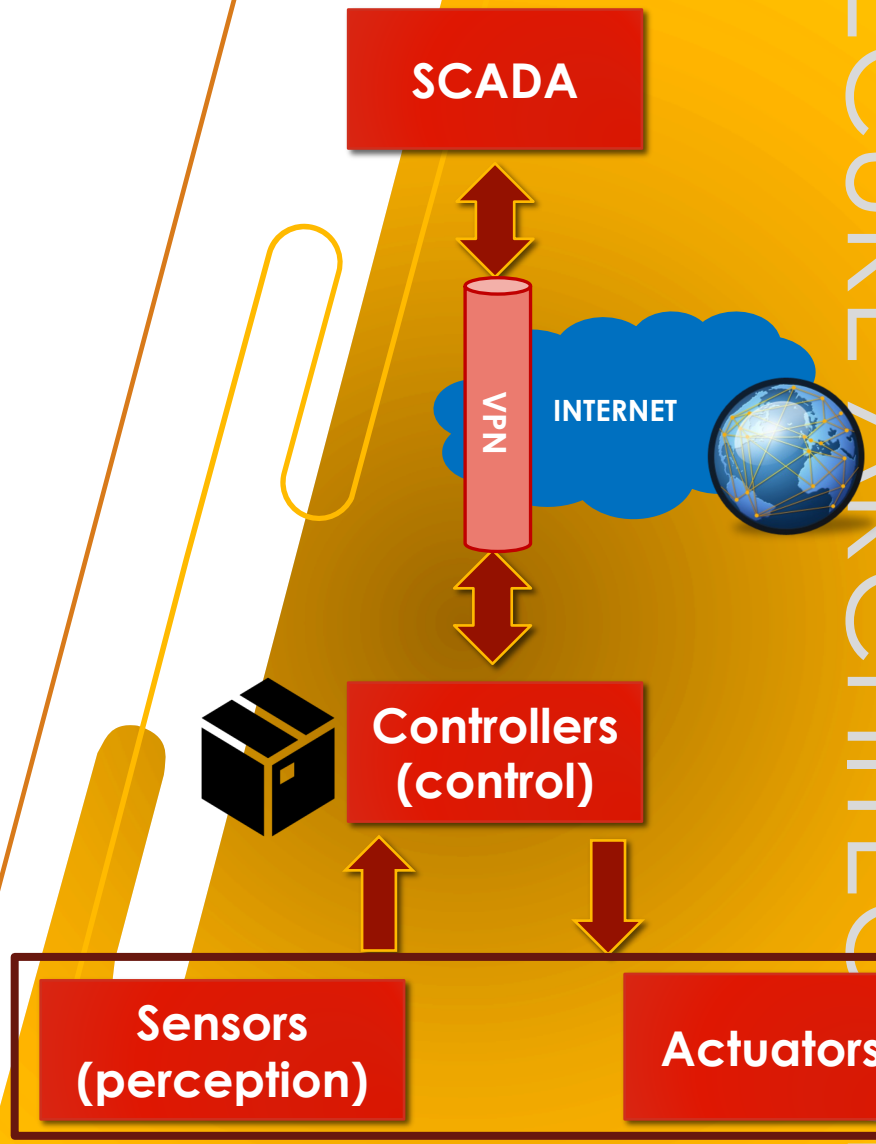




SECURE ARCHITECTURES

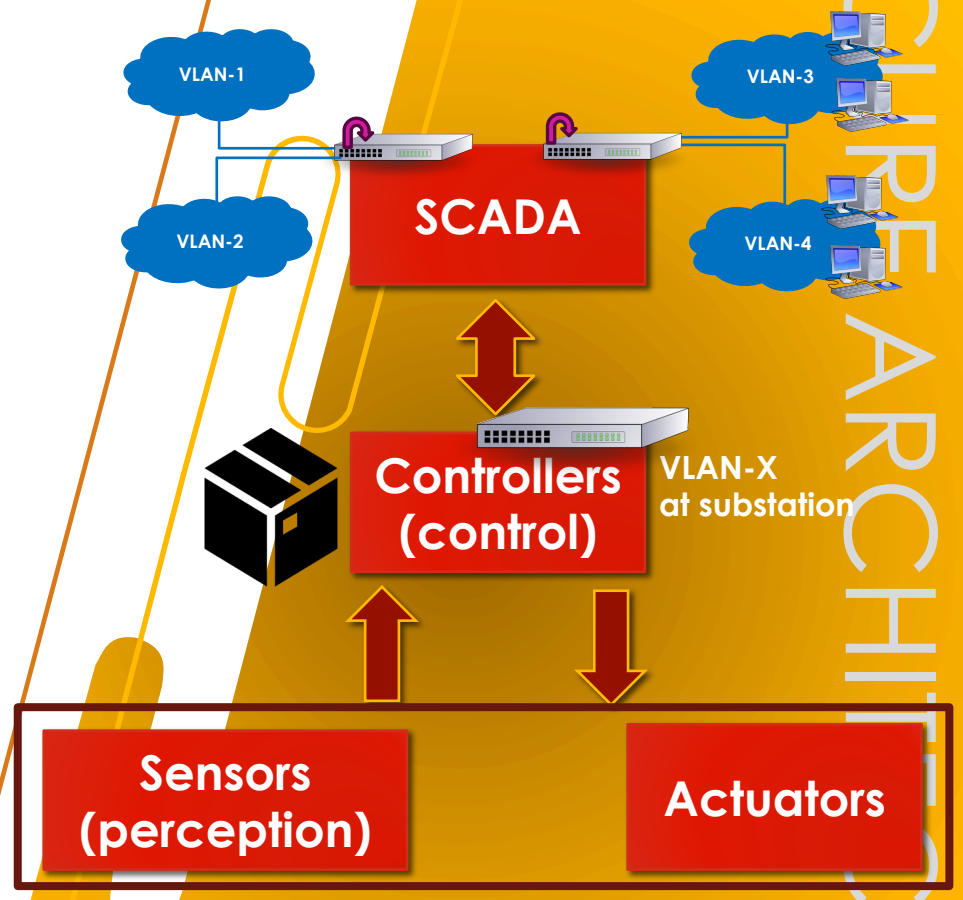
Secure architectures: At the network perimeter level

- **Virtual Private Network (VPN)**:
  - It corresponds to a P2P connection, whose communication channels are protected by the configuration of strong security measures (related to confidentiality, integrity and authentication)
  - These VPNs can be set up between different (control) devices, either between the master and the slave, between slaves, between routers, etc.
  - There are many types of VPNs supported by different security protocols, which will be detailed in the following sessions of this course



Secure architectures: At the network perimeter level

- **Virtual Private Network (VPN)**:
  - It corresponds to a P2P connection, whose communication channels are protected by configuring robust security measures (related to confidentiality, integrity and authentication)
  - These VPNs can be set up between different (control) devices, either between the master and the slave, between slaves, between routers, etc.
  - There are many types of VPNs supported by different security protocols, which will be detailed in the following sessions of this course
- **Virtual LAN (VLAN)**:
  - It corresponds to a "virtual" Local Area Network (LAN) whose connections are logically established in the switch/bridge
  - That is, a physical port of the switch/bridge is reserved for multiple logical connections, regardless of the location of the users
  - This "virtual" network enables:
    - Local connection of human operators, administrators or engineers to networks, and increases the connection capacities
    - Mobility of these operators in all or part of the system
    - Isolation of vulnerable sub-networks with respect to denial or service – more specifically to broadcast-based attacks

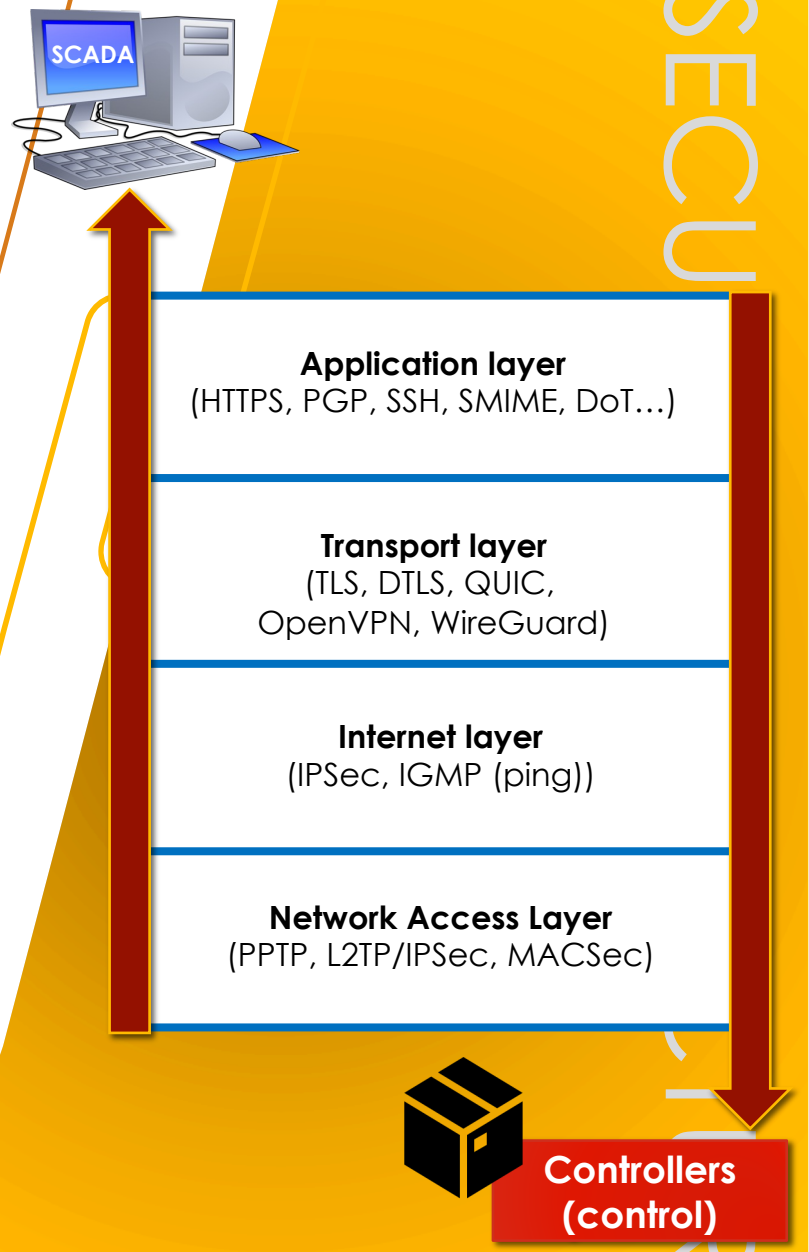


Secure architectures: At the network perimeter level

- **Intrusion Detection System (IDS)**:
  - System capable of collecting, analysing and alerting of anomalous or malicious activities
  - This detection capability can be based on a set of patterns or rules to deduce anomalous behaviour, or on advanced machine learning models
  - Moreover, there are different types of IDS, at network and host level, which we will detail throughout this course
- **Intrusion Prevention System (IPS)**:
  - It is an equivalent system to an IDS but with the ability to provide the same detection actions but adding response capabilities
  - Therefore, an IPS is able to detect and respond to anomalous events

Secure architectures: At the network service level

- Currently, the TCP/IP stack is based on a set of specific protocols, some originally developed for the stack, and others have been designed according to the needs, such as:
  - *Transport Layer Security (TLS)*
  - *Internet Protocol Security (IPSec)*
  - *Datagram Transport Layer Security (DTLS)*
  - *Quick UDP Internet Connections (QUICK)*
  - *Hypertext Transfer Protocol Secure (HTTPS)*
  - *Secure Shell (SSH)*
  - *Domain Name System (DNS) over TLS (DoT)*
  - *DNS over HTTPS (DoH)*
  - *Pretty Good Privacy (PGP)*
  - *Secure Multipurpose Internet Mail Extensions (SMIME)*
  - ...
- All these services are developed throughout the stack, providing different security measures



Secure architectures: At the standards level

- Many of these measures are considered by the current security standards for power systems, such as:
  - **IEC 62351**about "*Power Systems Management and Associated Information Exchange – Data and Communications Security*"
    - The standard covers various protection aspects to distributed energy networks, comprising: Security for IEC 60870 (for telecontrol equipment and systems), security for 61850 (at substations), data and communication security, role-based access control at substations,…
    - The measures range from the typical use of cryptography and authentication solutions to the application of security protocols (TLS), wireless communication and perimeter defence (VLANs and IDSs)
  - **ISA/IEC 62443** about "*Security for industrial automation and control systems*"
    - The standard establishes the security requirements, conditions and recommendations required to provide protection guarantees
    - This protection are also very varied, from the use of cryptography and authentication solutions to wireless security, network segmentation, access and management of resources, backups, accountability,…

Final remarks

- We have seen that control infrastructures typically follow a hierarchical structure, based on multiple industrial communication protocols
  - Many of these protocols, whether proprietary or open source, do not necessarily integrate strong security measures
  - It is therefore necessary to strengthen security by following the principles of "***defence in depth***"
- This defence must be done at different levels to achieve with the concept of "*defence in depth*":
  - At the network perimeter level
  - At the level of network services
  - At regulatory level, considering current security standards in power grids and substations

References and sources

1. CloudShark.org – modbus-bug0.pcapng, 2024
   URL: https://www.cloudshark.org/captures/4b8f9f3579b3
2. Vanimpe, "Introduction to Modbus TCP traffic", 2015
   URL: https://www.cloudshark.org/captures/4b8f9f3579b3
3. DeepL Translator for Proofreading:
   https://www.deepl.com/translator

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/

Co-funded by the European Union

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

Thank you

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

- Antonio Muñoz
  Associate Professor
  University of Malaga
  anto@uma.es