Network Protection for Energy Control Systems

CSP004_C_E

PRESENTATION BY:

- **CRISTINA ALCARAZ**
  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-1: Introduction to Energy Control Network Protection

Overview

- Introduction to the application scenario and the main security challenges in power control systems
- Taxonomy of threats and case studies
- Final remarks
- References and sources

Topic-1: Introduction to Energy Control Network Protection

Overview

- **Introduction to the application scenario and the main security challenges in power control systems**
- Taxonomy of threats and case studies
- Final remarks
- References and sources

Introduction to the energy sector

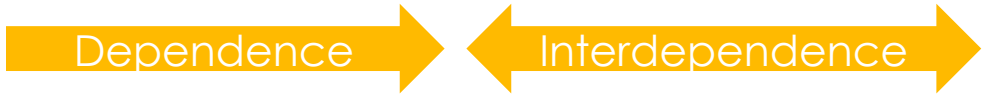
- The **energy sector** is the area in charge of producing, transporting and distributing energy to end users for its final consumption and welfare

- Diverse entities depend on the energy to operate properly:
  - Households to live comfortably
  - Offices to ensure business continuity and profitability
  - Critical infrastructures to provide essential services

Figure source: Vecteezy
URL:https://www.vecteezy.com/vector-art/7885798-flat-isometric-illustration-concept-solar-panel-industrial-city-view-on-smartphone

Introduction to the energy sector

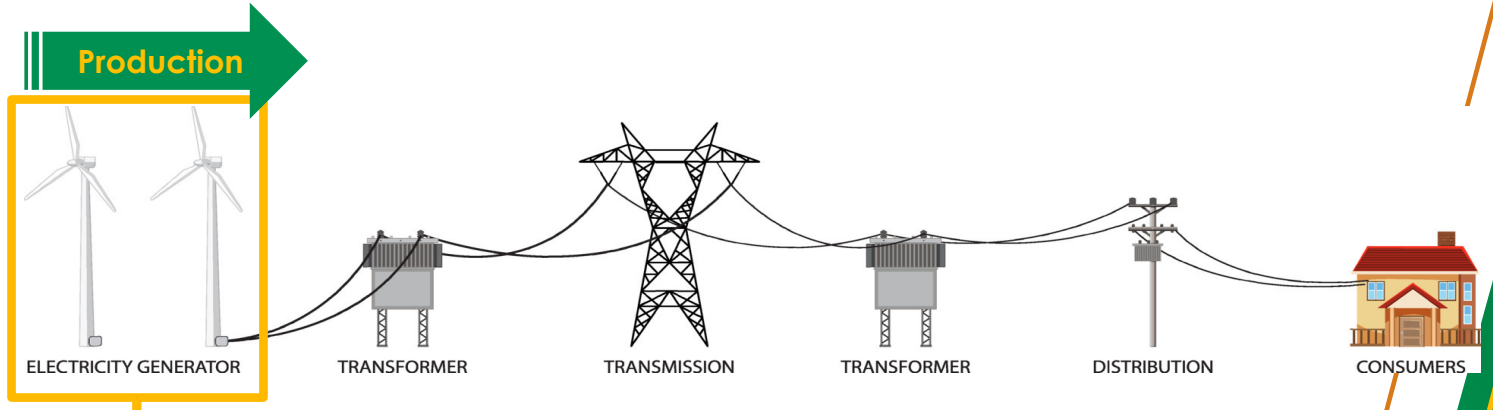
- This also means that **the energy sector and its infrastructures are** also considered **critical in nature**, and therefore:
  - Any shortfall in energy production or distribution may entail a serious impact on the provision of other essential services (e.g. healthcare, transportation, etc.) with a major impact on society, its well-being and economy
- In turn, this introduces the idea of "dependence" or "interdependence" between infrastructures,



- Without energy, it is not possible to:
  - Get progress in the Electrical Vehicle (EV) field and other related ones
  - Ensure the proper functioning of other systems and the use of electrical equipment to operate
  - Guarantee quality of life and comfort

Introduction to the energy sector

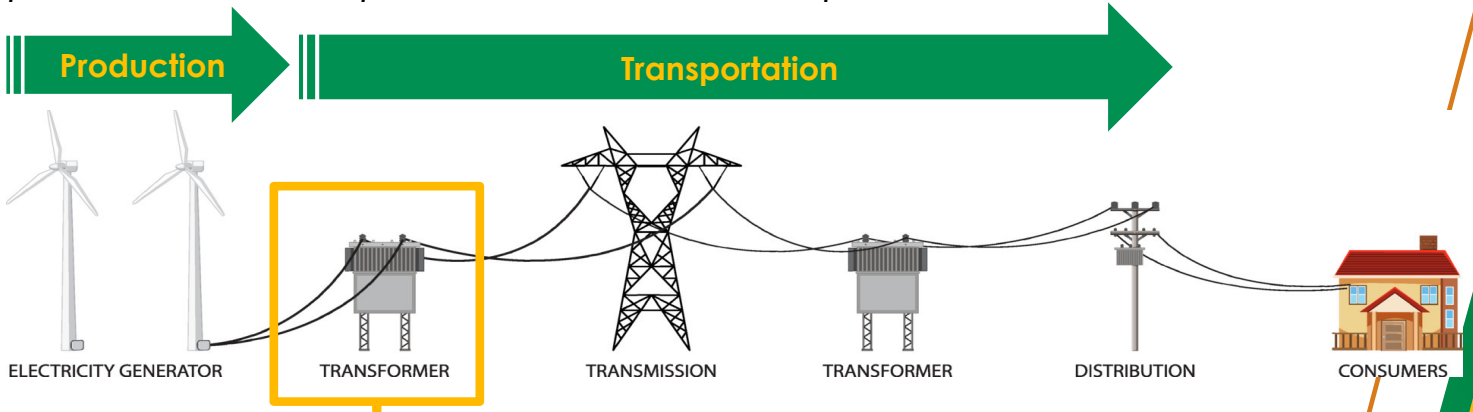
- Thus, 'energy' is considered as an **essential resource** for society, and the energy sources may be varied:
  - Coal, oil and gas, nuclear, and **electricity**
  - Note that this module will focus on electrical energy issues, but the concepts learned extend to all other related fields
- Power grid normally operate following the same functionality stages: *production, transportation and consumption*



Energy production incorporates mechanisms and components capable of generating large amounts of energy, with the additional capability to store and/or distribute it via pylons

Introduction to the energy sector

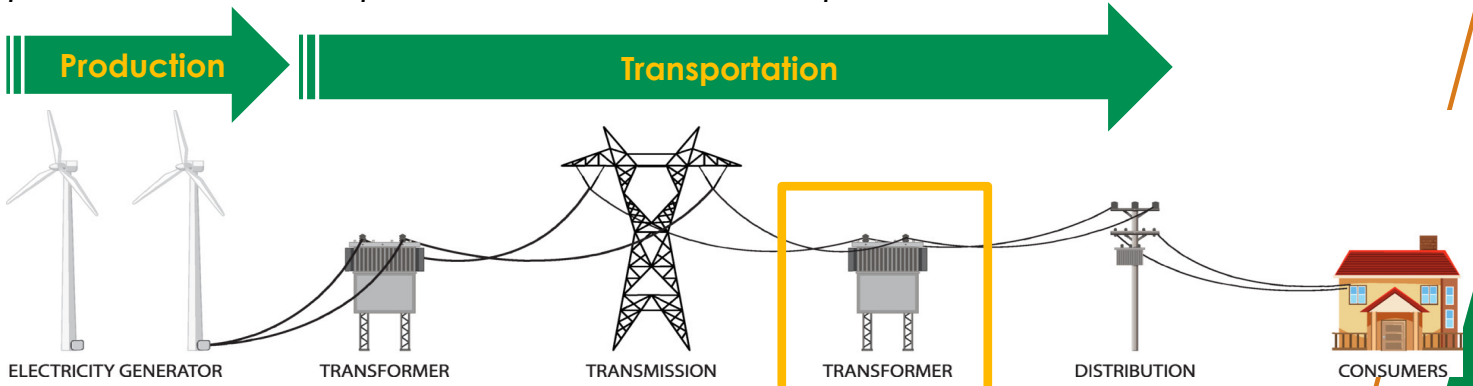
- Thus, 'energy' is considered as an **essential resource** for society, and the energy sources may be varied:
  - Coal, oil and gas, nuclear, and **electricity**
  - Note that this module will focus on electrical energy issues, but the concepts learned extend to all other related fields
- Power grid normally operate following the same functionality stages: *production, transportation and consumption*



Energy transmission aims to transport large quantities of electricity with high loads over long distances (via pylons), and they are mainly supported by storage and generation systems at substations

Introduction to the energy sector

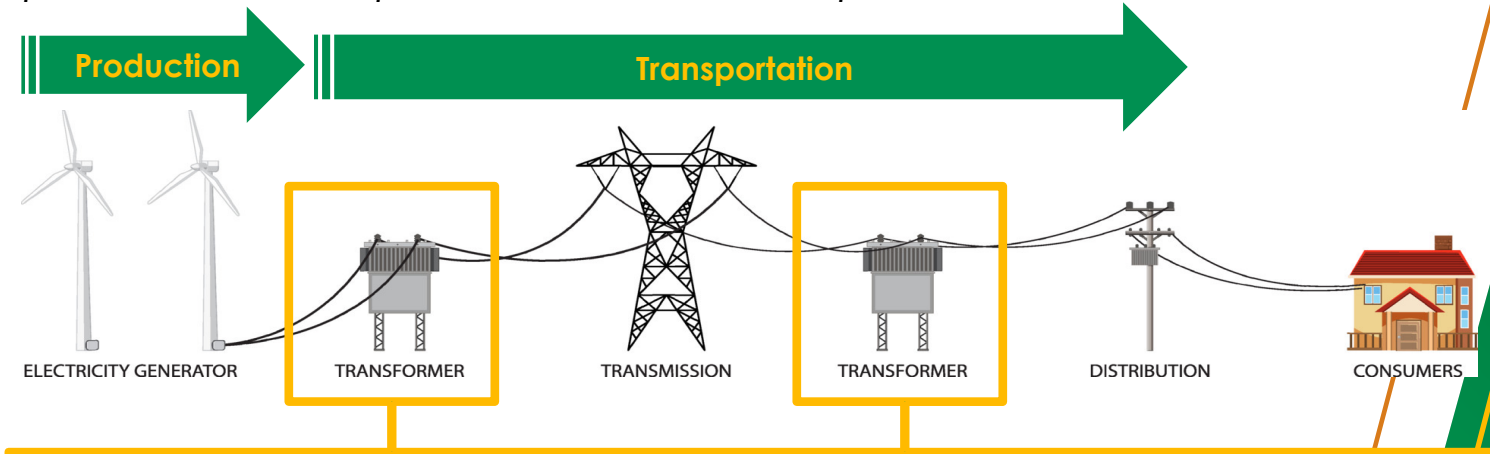
- Thus, 'energy' is considered as an **essential resource** for society, and the energy sources may be varied:
  - Coal, oil and gas, nuclear, and **electricity**
  - Note that this module will focus on electrical energy issues, but the concepts learned extend to all other related fields
- Power grid normally operate following the same functionality stages: *production, transportation and consumption*



Energy distribution consists of transporting electricity at an acceptable intensity for its final consumption, and probably with the support in storage and generation systems at substations located close to end users

Introduction to the energy sector

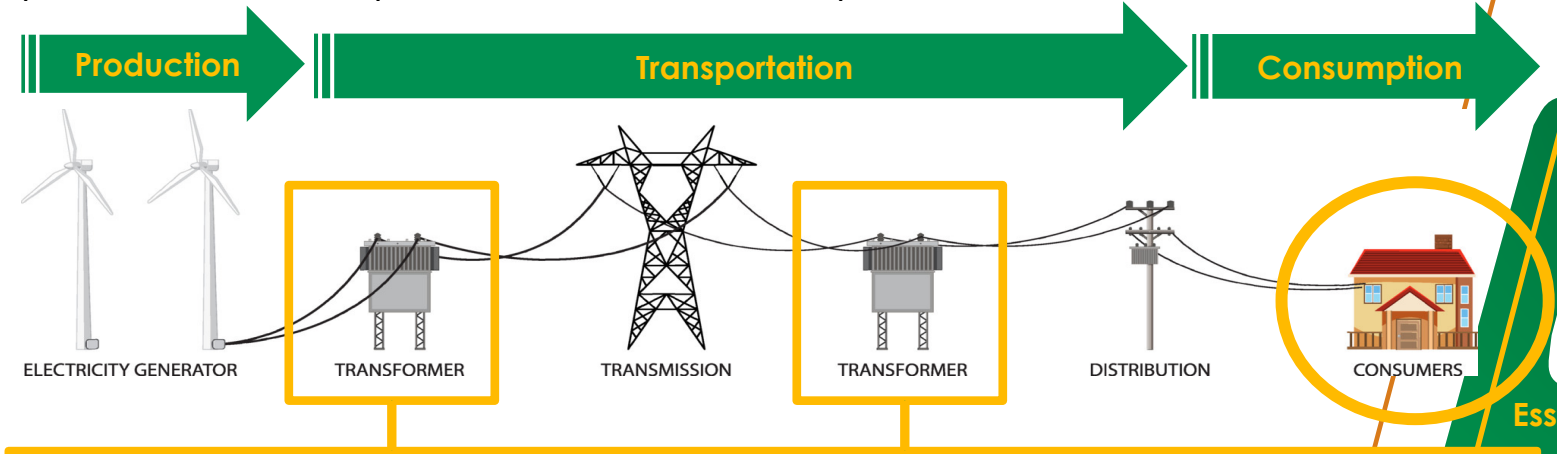
- Thus, 'energy' is considered as an **essential resource** for society, and the energy sources may be varied:
  - Coal, oil and gas, nuclear, and **electricity**
  - Note that this module will focus on electrical energy issues, but the concepts learned extend to all other related fields
- Power grid normally operate following the same functionality stages: *production, transportation and consumption*



Both the production of energy and its transformation for transport are carried out in **power substations**, which are: control sub-networks physically deployed around and near critical power components, whose control depends on cyber-physical elements such as sensors, actuators and controllers

Introduction to the energy sector

- Thus, 'energy' is considered as an **essential resource** for society, and the energy sources may be varied:
  - Coal, oil and gas, nuclear, and **electricity**
  - Note that this module will focus on electrical energy issues, but the concepts learned extend to all other related fields
- Power grid normally operate following the same functionality stages: *production, transportation and consumption*

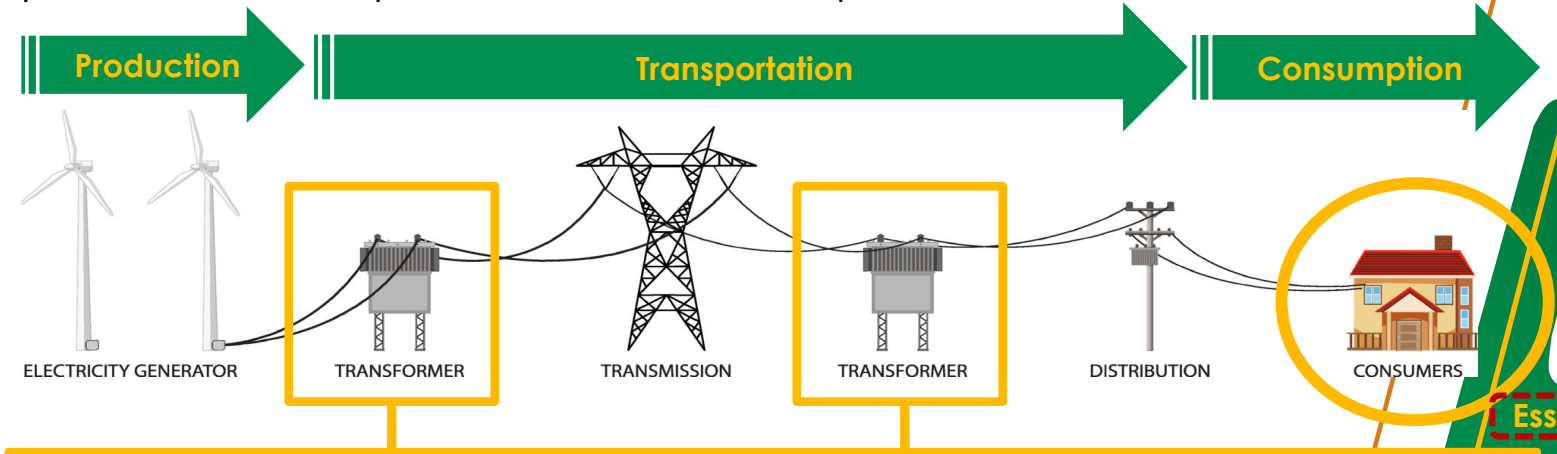


Essential for a comfortable life

Both the production of energy and its transformation for transport are carried out in **power substations**, which are: control sub-networks physically deployed around and near critical power components, whose control depends on cyber-physical elements such as sensors, actuators and controllers

Introduction to the energy sector

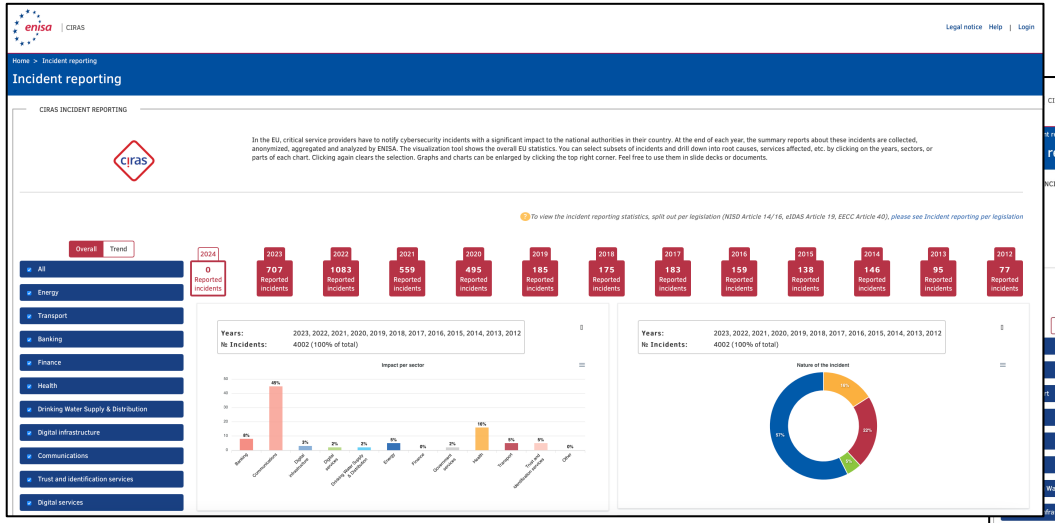
- Thus, 'energy' is considered as an **essential resource** for society, and the energy sources may be varied:
  - Coal, oil and gas, nuclear, and **electricity**
  - Note that this module will focus on electrical energy issues, but the concepts learned extend to all other related fields
- Power grid normally operate following the same functionality stages: *production, transportation and consumption*

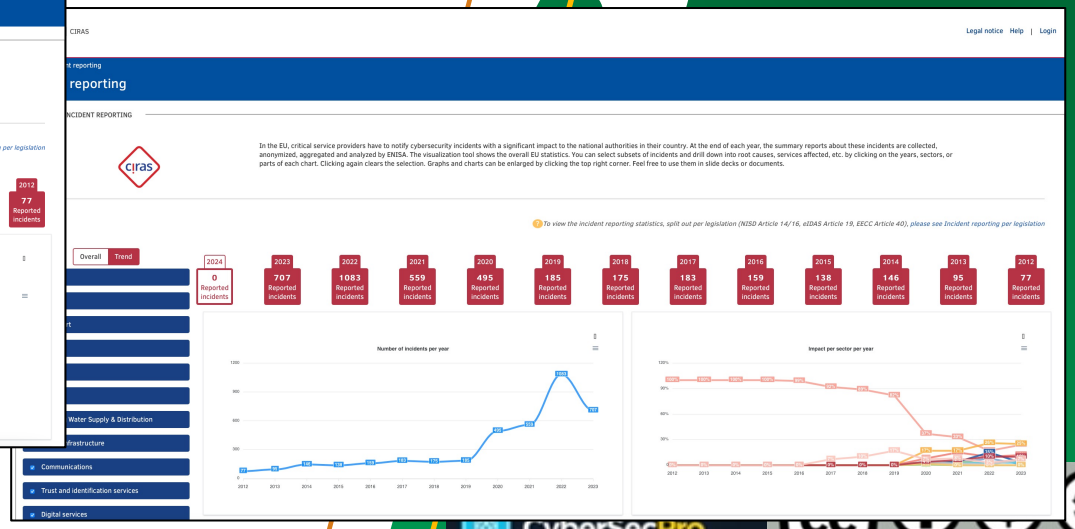


Both the production of energy and its transformation for transport are carried out in **power substations**, which are: control sub-networks physically deployed around and near critical power components, whose control depends on cyber-physical elements such as sensors, actuators and controllers

Introduction to the energy sector

- Indeed, attackers know the extent to which energy use is fundamental the correct functioning of society and its economy
- For that reason, the European Union Cybersecurity Agency (ENISA), though **CIRAS incident system**, annually updates and reports the cybersecurity incidents caused in European critical service providers, such as power systems

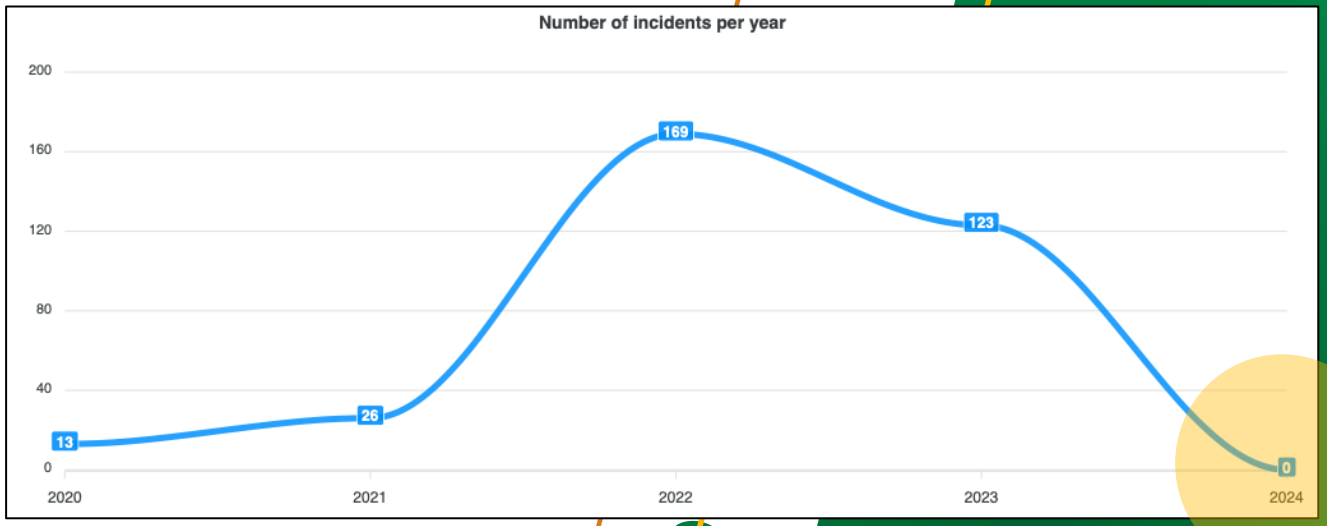


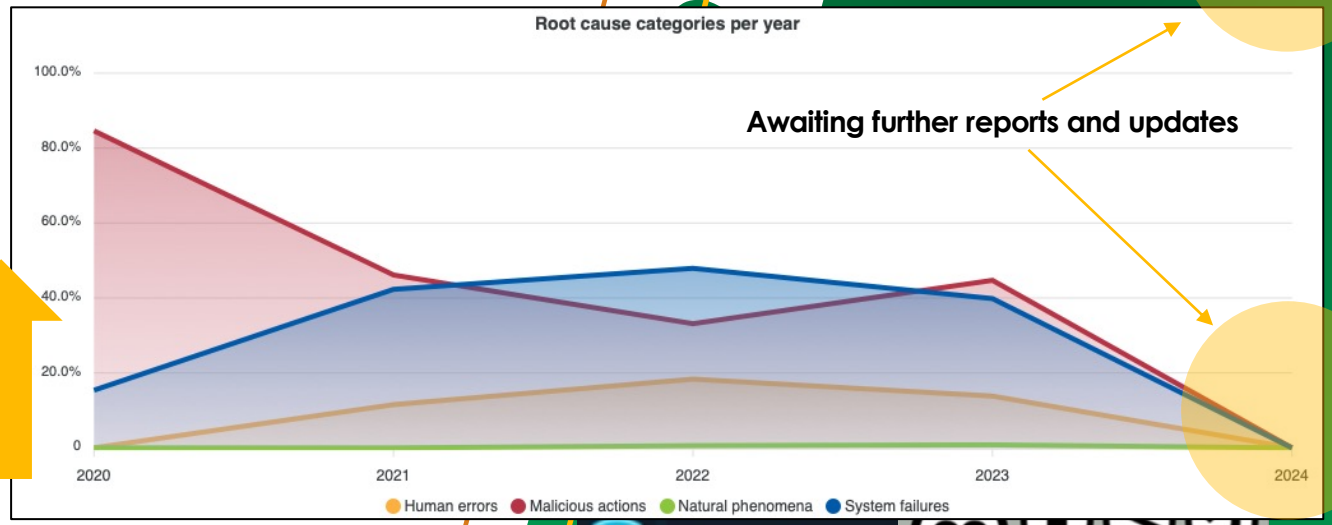


Source: ENISA, CIRAS, 2024
URL: https://ciras.enisa.europa.eu

Introduction to the energy sector

- ENISA CIRAS reports incidents in critical sectors and according to different perspectives, such as the number of incidents caused by:
  - Human errors
  - Malicious actions
  - Natural phenomena
  - Systems failures
- We also note that the threat tendency is high in the energy sector
  - Mainly caused by **malicious actions**, **system failures** that may lead to security breaches and **human factors**





Awaiting further reports and updates

Trend remains high, and vulnerabilities/failures are normally public available in repositories

Source: ENISA, CIRAS, 2024
URL: https://ciras.enisa.europa.eu

Introduction to the energy sector

- This trend may be due to the multiple changes taking place in the different strategic sectors, including energy, where **multiple information technologies and new paradigms** are being incorporated to facilitate:
  - Digital transformation and modernisation of systems and processes
  - Interoperability and decentralisation of services
  - The creation of autonomous and "smart" environments
- This conceptualisation of **smart in energy** means to:
  - Produce energy according to actual demand
  - Promote the use of renewable energy
  - Reduce emissions
  - Create more sustainable environments
  - Support the planet and avoid climate change
  - ...

Source: ENISA, CIRAS, 2024
URL: https://ciras.enisa.europa.eu

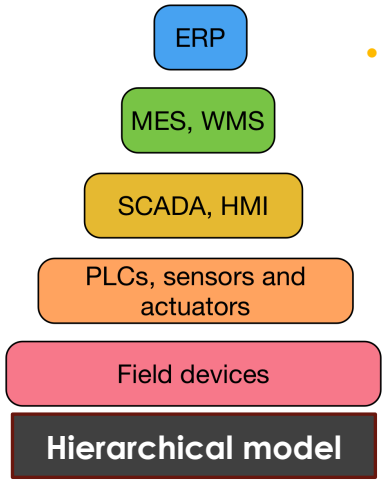
Introduction to the energy sector

- What is more, depending on the sector, **security and privacy issues** may also vary, mainly because each sector presents its own problems and threats
- In the energy sector, the impact could fall on:
  - **Physical resources**
    - Type: the grid or micro-grid, Distributed Energy resources (DERs), charging infrastructures, generators, transformers, pylons, etc.
    - Threats: cyber-attacks or sabotage
  - **Control resources**
    - Type: Supervisory Control and Data Acquisition (SCADA) systems, controllers, sensors, actuators, etc.
    - Threats: cyber-attacks against the monitoring and supervision of critical physical resources
  - **Data** belonging to users/organization:
    - Type: consumption data and control data
    - Threats: cyber-attacks on data privacy to corrupt the privacy of users or the reputation of the organisation

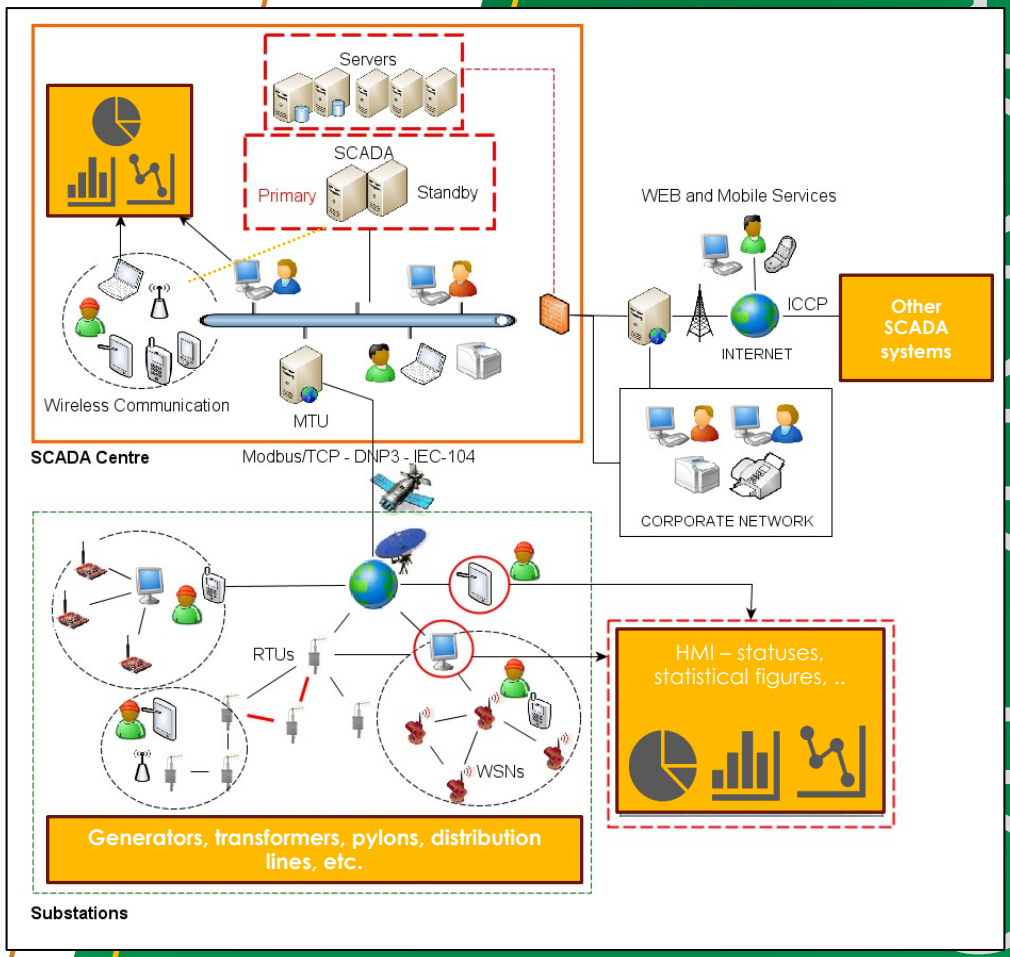
Our main focus of interest and object of study because control affects the management of physical resources and the management of data

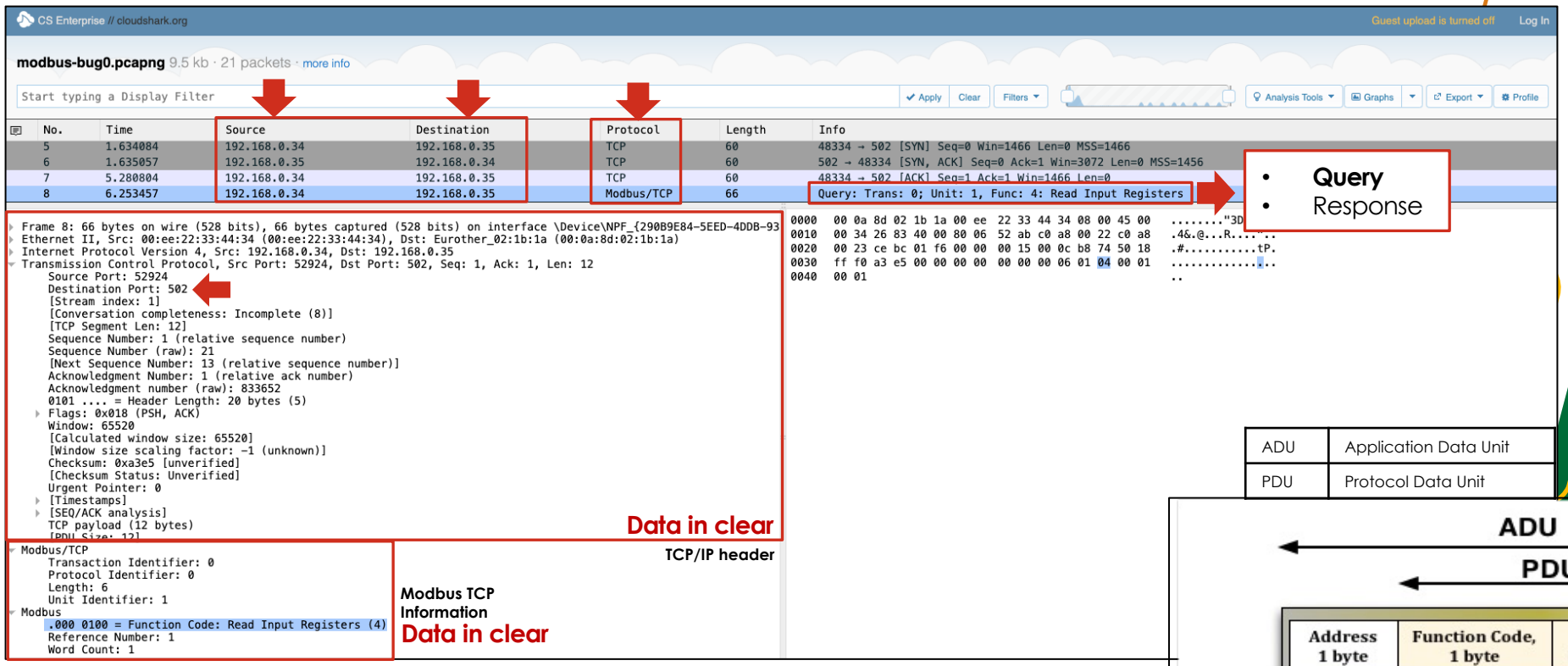
Traditional control architectures of critical energy systems

- In a SCADA system, there are three types of networks
  - **Corporative**: the business network
  - **SCADA centre**: the control network
  - **Substations**: control subnetworks, physically deployed around and close to CIs, and based on controllers, sensors, actuators, and other IoT devices
- The traditional architecture follows the ISA-95 model based on a **hierarchical structure**

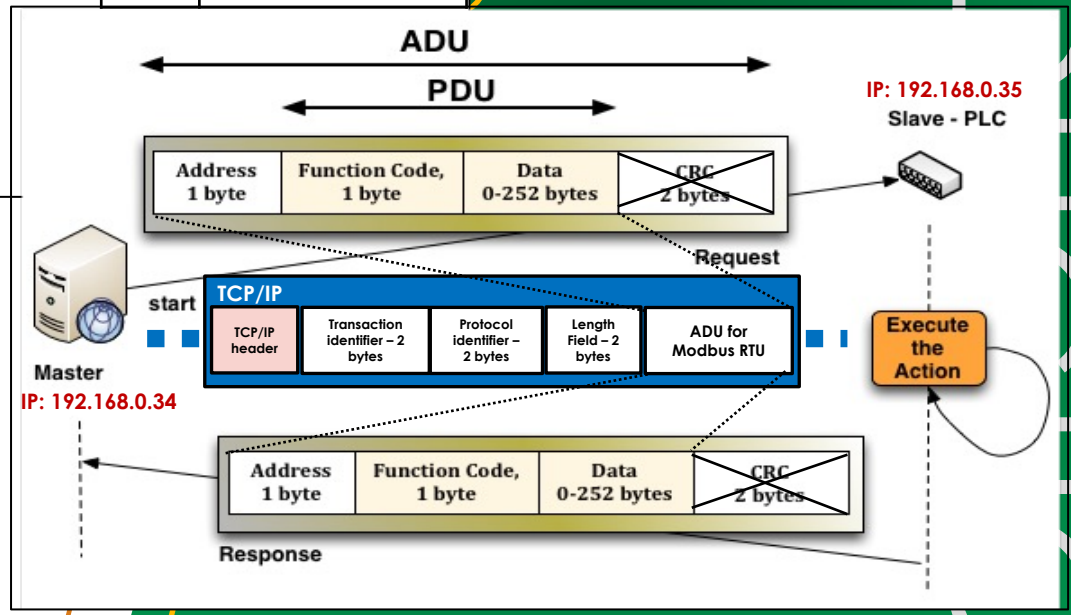


- The model is mainly based on:
  - Field devices: sensors, actuators
  - Controllers: Remote Terminal Units (RTUs) / Programmable Logic Controllers (PLCs)
  - Masters: SCADA servers
  - Human Machine Interfaces (HMIs)
  - **Multiple industrial communication protocols**: **ModbusTCP**, DNP3, IEC-104, EthernetIP, OPC-UA,…



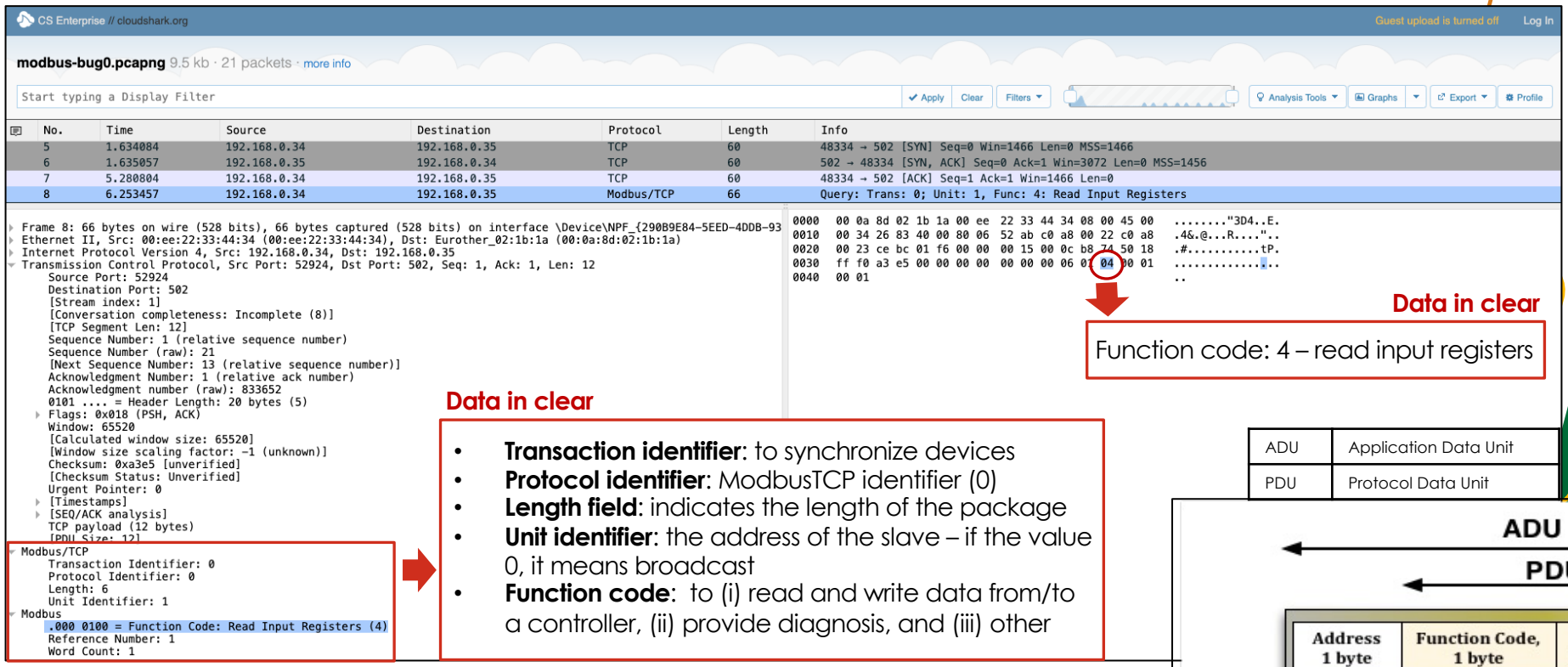


ADU	Application Data Unit
PDU	Protocol Data Unit



- **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)

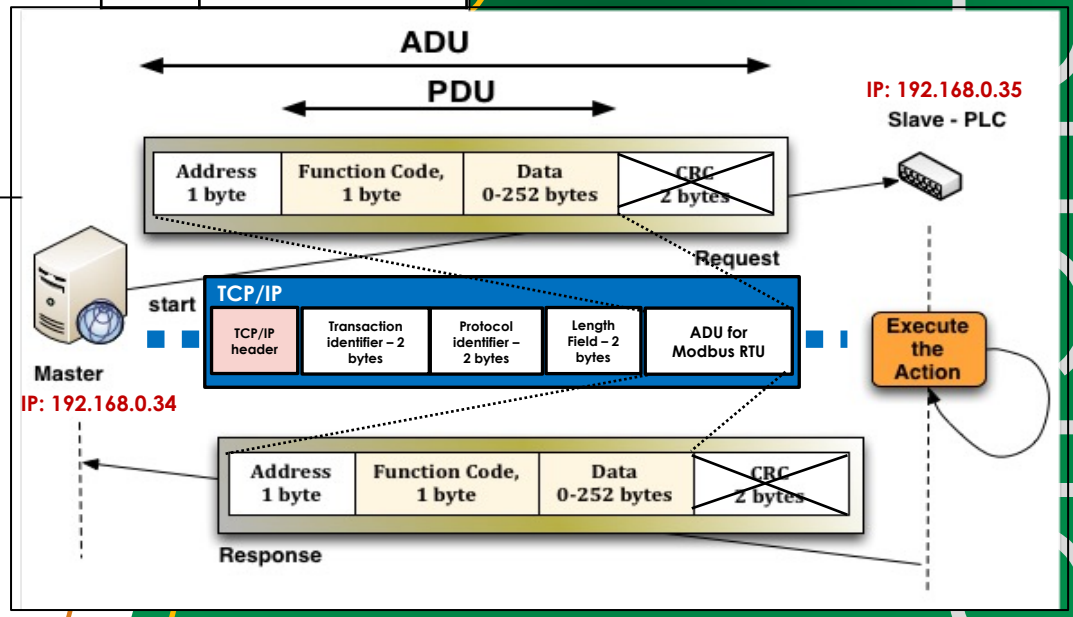
Figure source: CloudShark.org – modbus-bug0.pcapng
URL: https://www.cloudshark.org/captures/4b8f9f3579b3



Data in clear

- **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

Homework:
DoS Attack using HPING3

- **Objective**: to enhance your practical skills, it is crucial to engage in hands-on work. The aim of this exercise is to simulate real-world network interactions for transmitting data between a client and server using ModbusTCP and to provide an eavesdropping attack
- **Guidelines**: follow the steps below to set up a controlled, simulation-based lab environment using virtual machines (victims and an attacker). This setup will enable you to perform packet analysis on the target devices in a safe and isolated setting
  1. Use the GNS3 network simulator to create a topology with two nodes (victim machines) and a Kali Linux machine acting as the attacker
  2. Ensure you install these machines on your preferred virtual machine software and integrate them with the GNS3 server
- **Task**:
  - Install ***pyModbusTCP*** on your victim machines – virtual machines (local network)
  - Create a server-client example for data transmission
    - A useful example for creating a client-server demo can be found [1]
  - Simulate the transmission of ModbusTCP and use the Wireshark tool on the attacker machine
  - Analyse the communication between the victim machines and capture all data transmitted between them.

[1]: https://apmonitor.com/dde/index.php/Main/ModbusTransfer

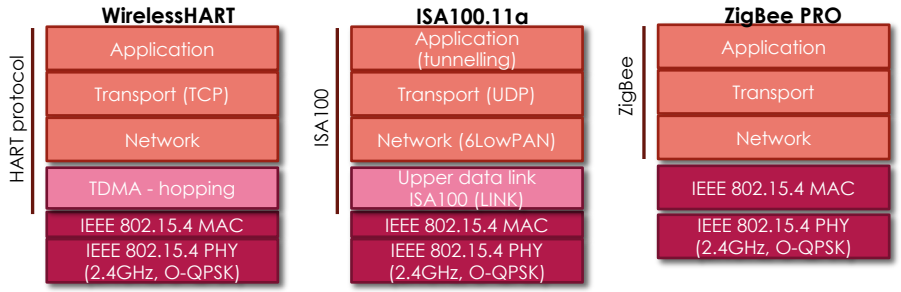
OPTIONAL PRACTICAL TASKS

Traditional control architectures of critical energy systems

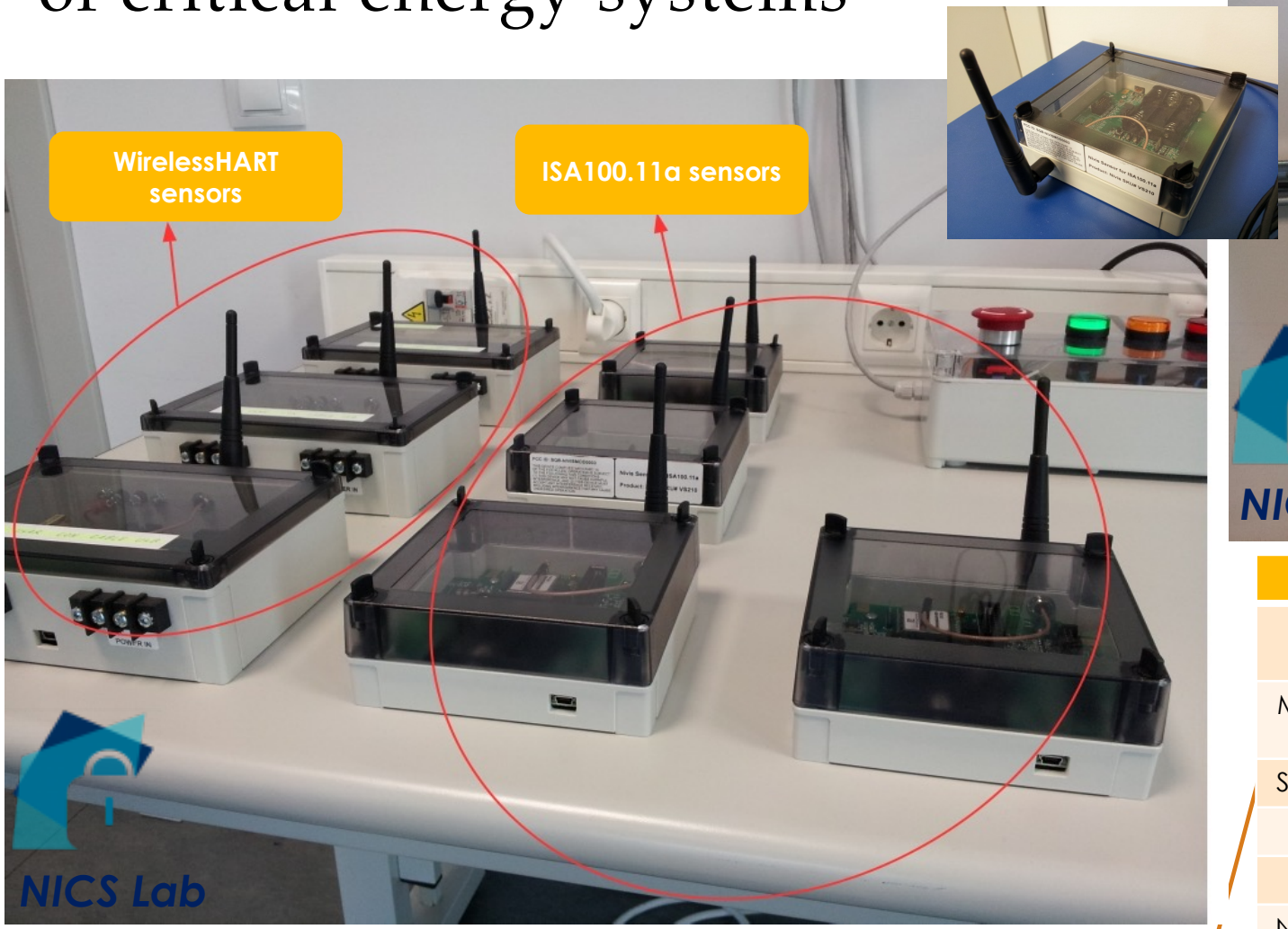
- As mentioned, there are many industrial protocols, such as:

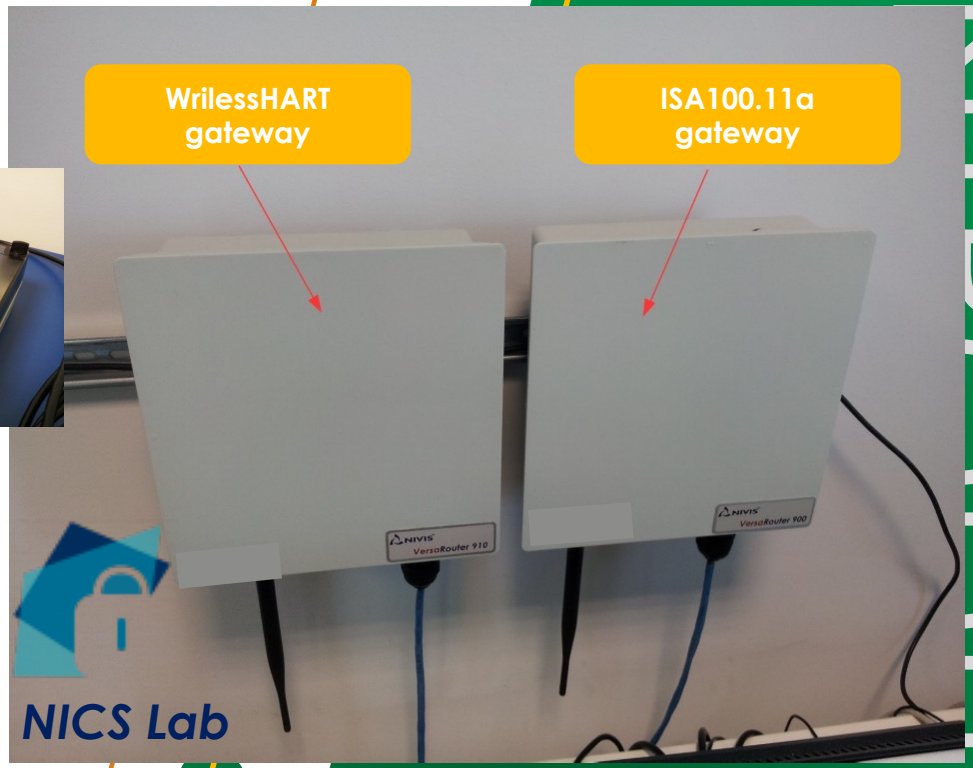
Some protocols	WIRED Communications
PROFIBUS	•Master/slave •Token-based comm. in multipoint busses
PROFINET	•Works over Ethernet and TCP/IP
OPC-UA (OPC Unified Architecture)	•Object-based comm., where each device is encapsuled on an object
CIP (Common Industrial Protocol)	•Object-based comm., where each device is encapsuled on an object •Ethernet/IP
HART (Highway Addressable Remote Transducer)	•P2P connection and multipoint bus
HART/IP	•Works over HART Ethernet and TCP/IP to encapsulate HART packets
Etc.	•… •…

Some protocols	WIRELESS Communications
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)
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
ZigBee	•P2P comm. and mesh networks •Wireless comm. based on the IEEE **802.15.4** (LR-WPANs)



Traditional control architectures of critical energy systems



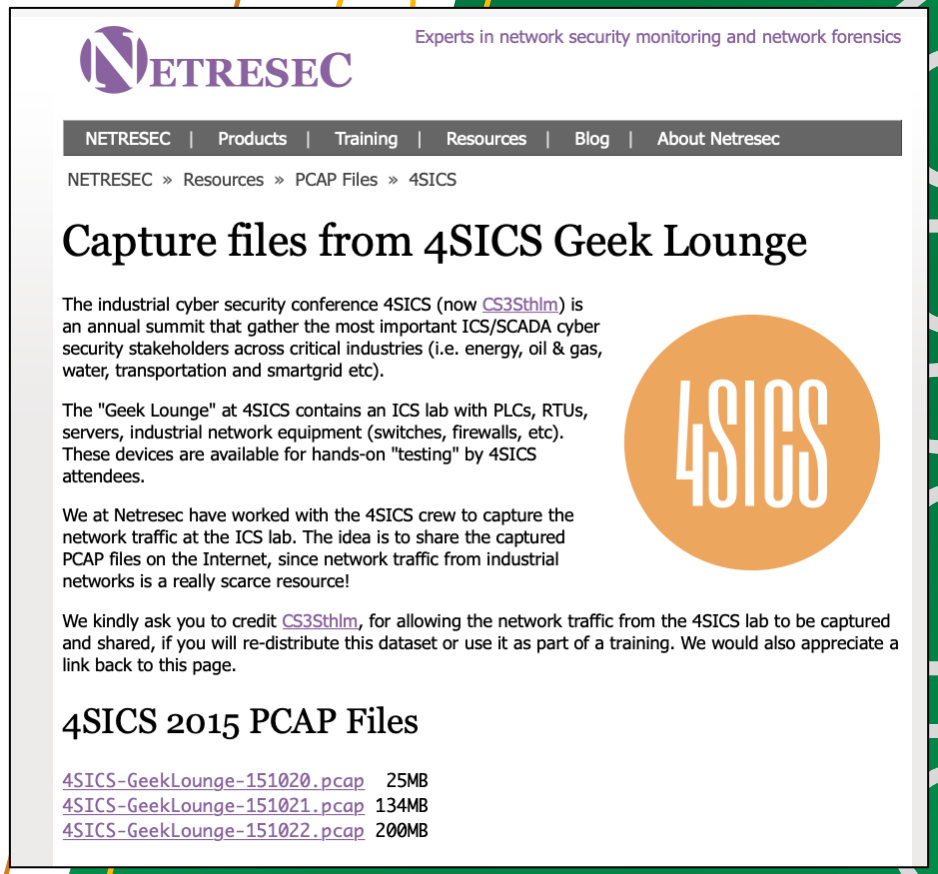


Features	WirelessHART	ISA100.11a	Zigbee
Mesh networks	Yes	Yes	Yes
Many-to-one networks	-	-	Yes
Star networks	-	Yes	Yes
Scalability	Yes	Yes	Yes
Security	Yes	Yes	Yes
Noise/interference control	Yes	Yes	Yes

Source: C. Alcaraz, J. Lopez, A Security Analysis for Wireless Sensor Mesh Networks in Highly Critical Systems, IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 40, no. 4, pp. 419-428, 2010, ISSN: 1094-6977.

Traditional control architectures of critical energy systems

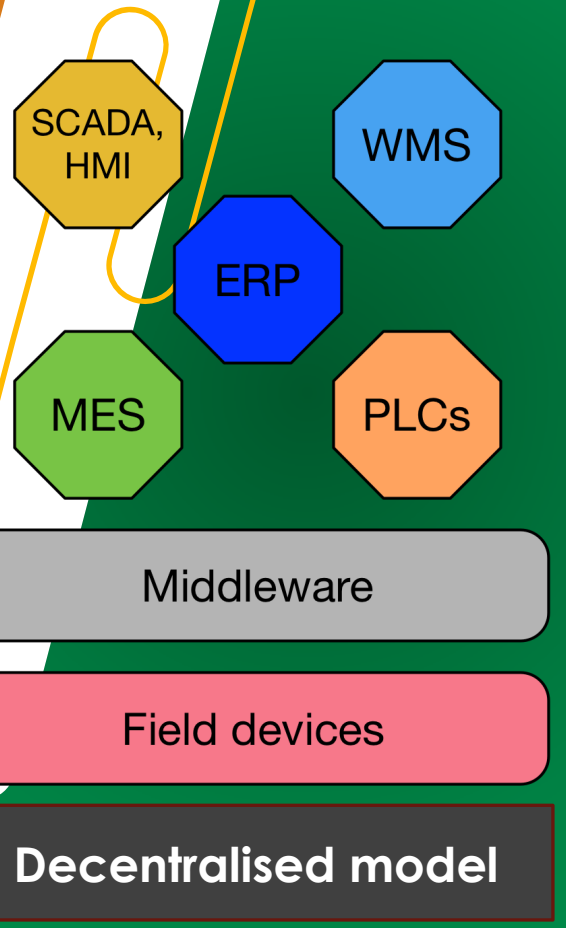
- Netresec also offers **4SICS Geek Lounge**, providing some files with captures of industrial traffic
  - URL: https://www.netresec.com/?page=PCAP4SICS
  - The captures are based on an Industrial Control System (ICS) Lab with PLCs, RTUs, servers and industrial network equipment - *all the information about the ICS Lab is found at the same website*
  - As requested, special acknowledgement goes to CS3Sthlm for allowing the community access to these captures
  - More SCADA/ICS network captures can also be found at: https://www.netresec.com/?page=PcapFiles
- With **Wireshark**, it is possible to analyse such captures
  - Wireshark a network dissector capable of understanding network packets and interpreting the various field of the packet



Source and figure source: Netresec, "Captures files from 4SICS Geek Lounge", 2024
URL: https://www.netresec.com/?page=PCAP4SICS
Source: CS3Sthtlm, 2014-2020, accessed in 2024.
URL: https://cs3sthlm.se

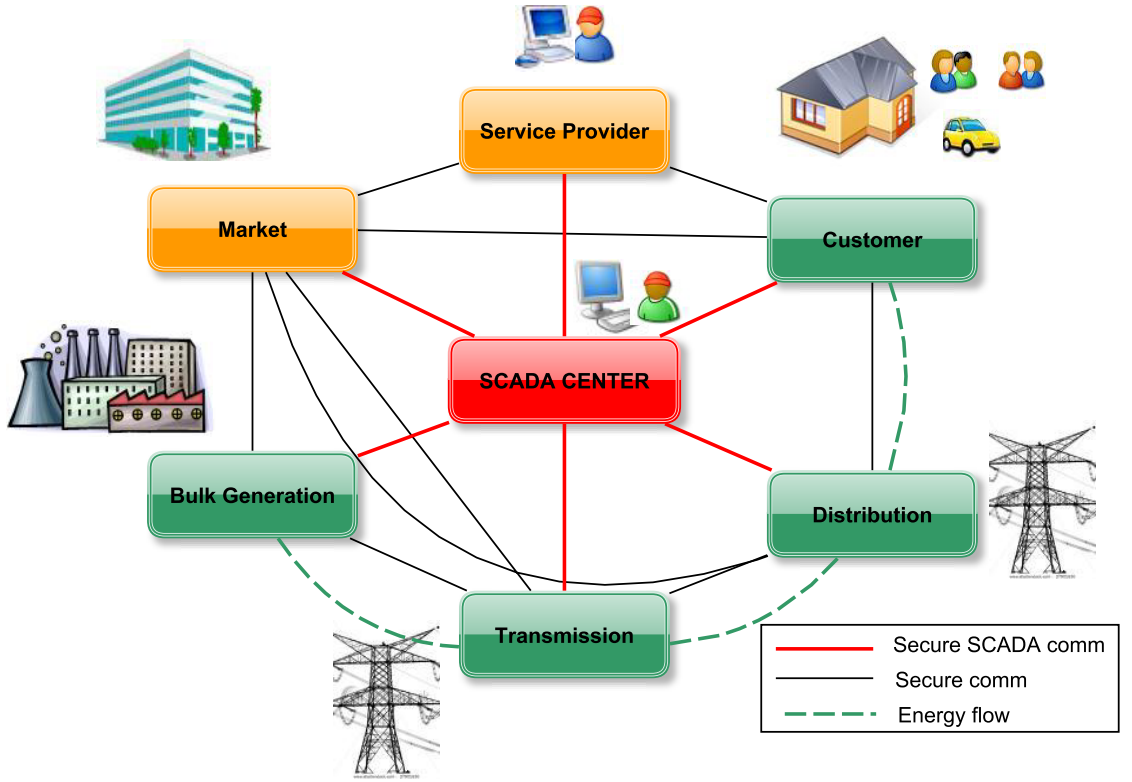
Modern control architectures of critical energy systems

- The previous hierarchical model (based on ISA-95 model) changes to accept now the inclusion of new technologies and paradigms in order to:
  - Modernise the operational processes
  - Digitalise, decentralise and customise processes and services
  - Control operations, processes and services from anywhere, at any time and in anyhow
- The idea is to create a new way of intelligently controlling the energy production and its distribution without wasting energy
  - Such that substations may be able to "*produce power according to the actual demand*" in a 'resilient' manner
- This evolution toward a new conceptualisation of "*smart ecosystem*" is what results in the power sector as **Smart Grid system**



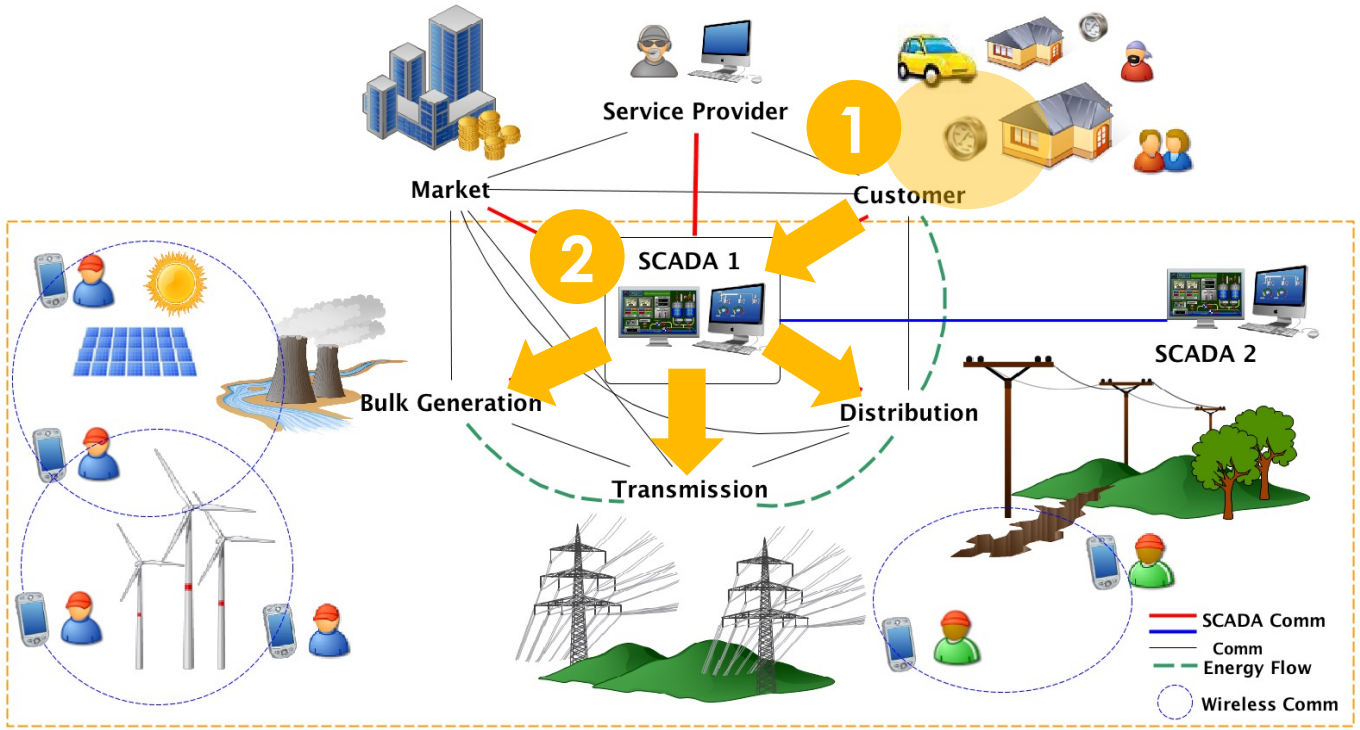
Towards the control of smart grids and microgrids

- The National Institute of Standards and Technology (NIST) provides a **conceptual mode Smart Grid** in which a set of entities cooperate to create collaborative and smart environments
- Therefore, a set of **stakeholders** arises:
  - Grid operators such as
    - Transmission System Operators (TSO)
    - Distribution System Operators (DSO)
  - Providers to facilitate the use of the energy
  - Billing entities
  - Market
  - Authorities or regulators to establish operation rules
  - Consumers / prosumers



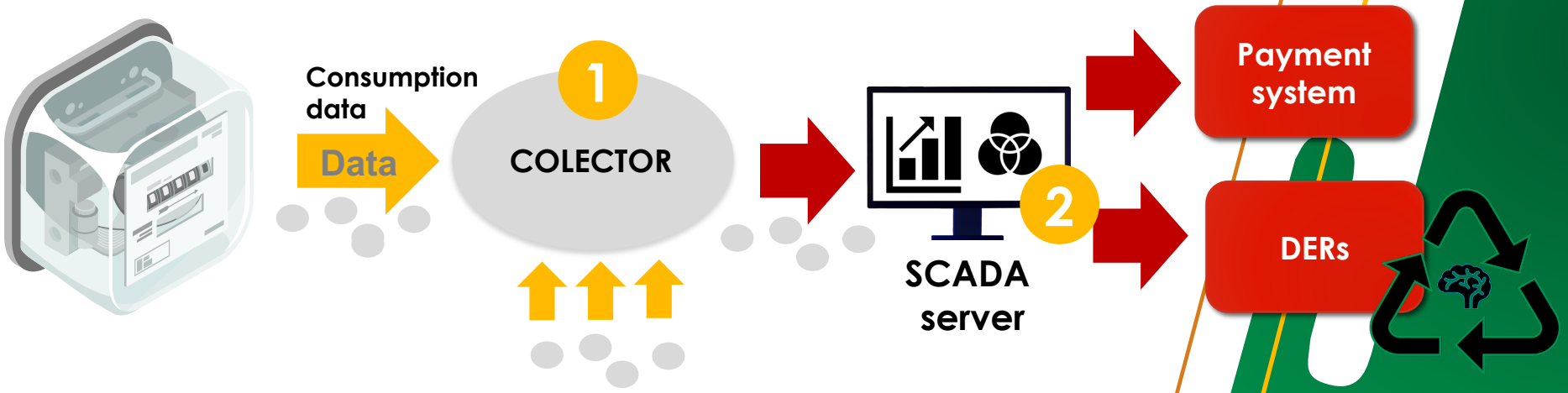
Towards the control of smart grids and microgrids

- However, to create "smart" ecosystems capable of producing power according to the actual demand, it is also required to:
  - Connect the control systems with the real world (the cities) through **smart meters**, which dynamically perceive actual consumption



Towards the control of smart grids and microgrids

- Therefore, smart meters can be seen as "sensors" for control domains, which are normally connected to collectors to transfer the consumption values, and enable
  - The control system to dynamically produce and distribute energy
  - The payment system to compute the final consumption value



- DERs are distributed energy resources deployed normally in microgrids, such as renewable systems, storage systems, or EVs batteries

Figure source: Vecteezy
URL:https://www.vecteezy.com

Towards the control of smart grids and microgrids

- Microgrids are small DER control sub-networks that allow users to control their own energy, with the ability to connect to the main grid (the Smart Grid)
- Thus, this type of deployment creates small "**operational islands**" with the objective of increasing "resilience" by reducing the impact of potential "**outages**"

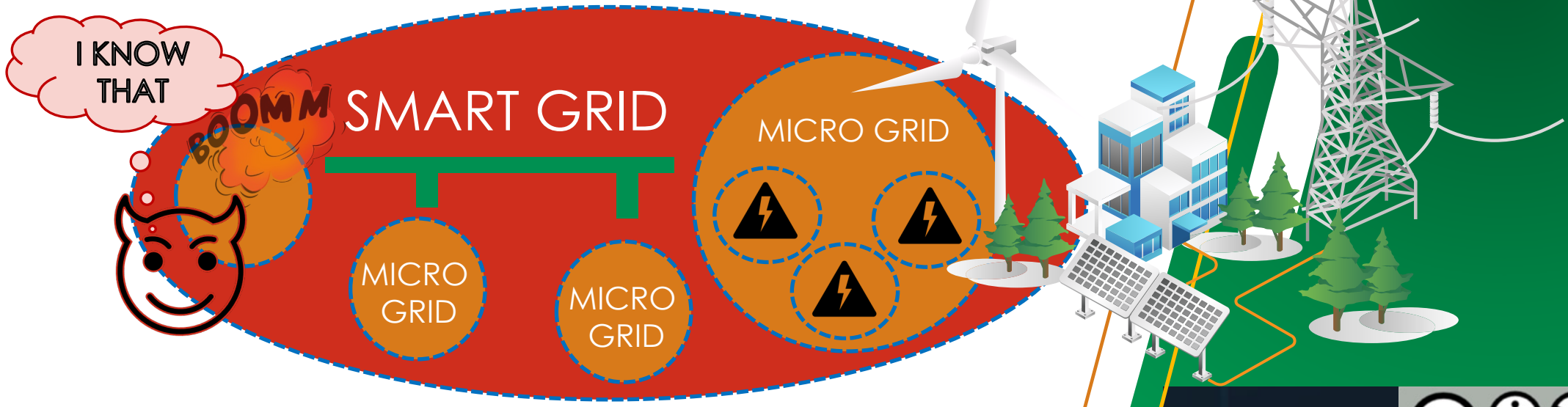
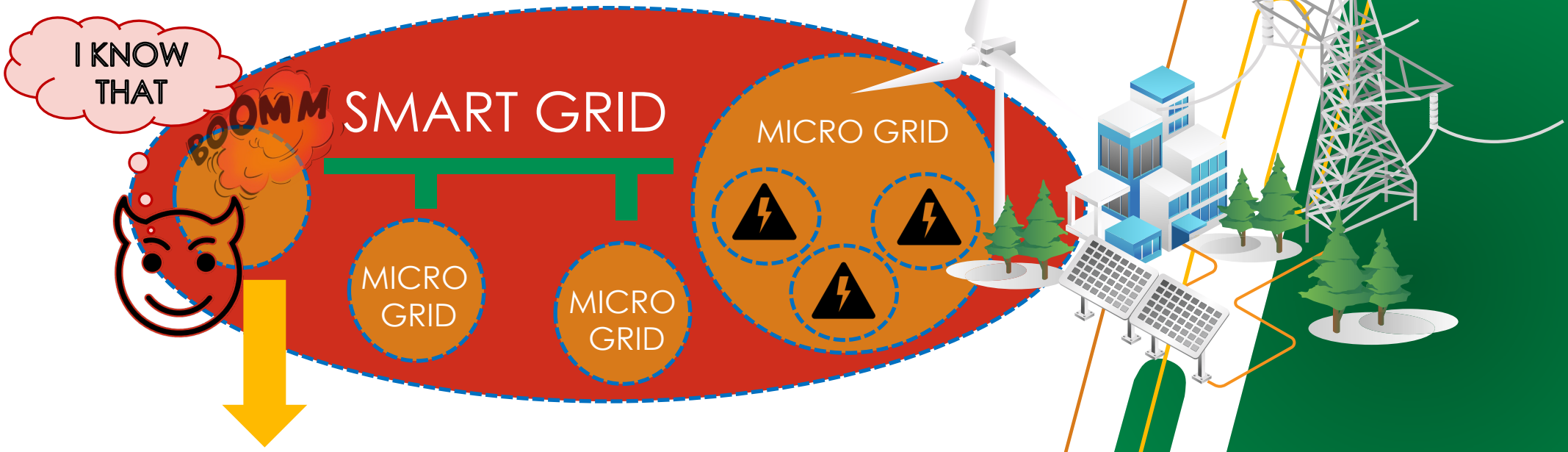


Figure source: Vecteezy
URL:https://www.vecteezy.com

Main challenges in power control networks



These types of threats and risks may come from:

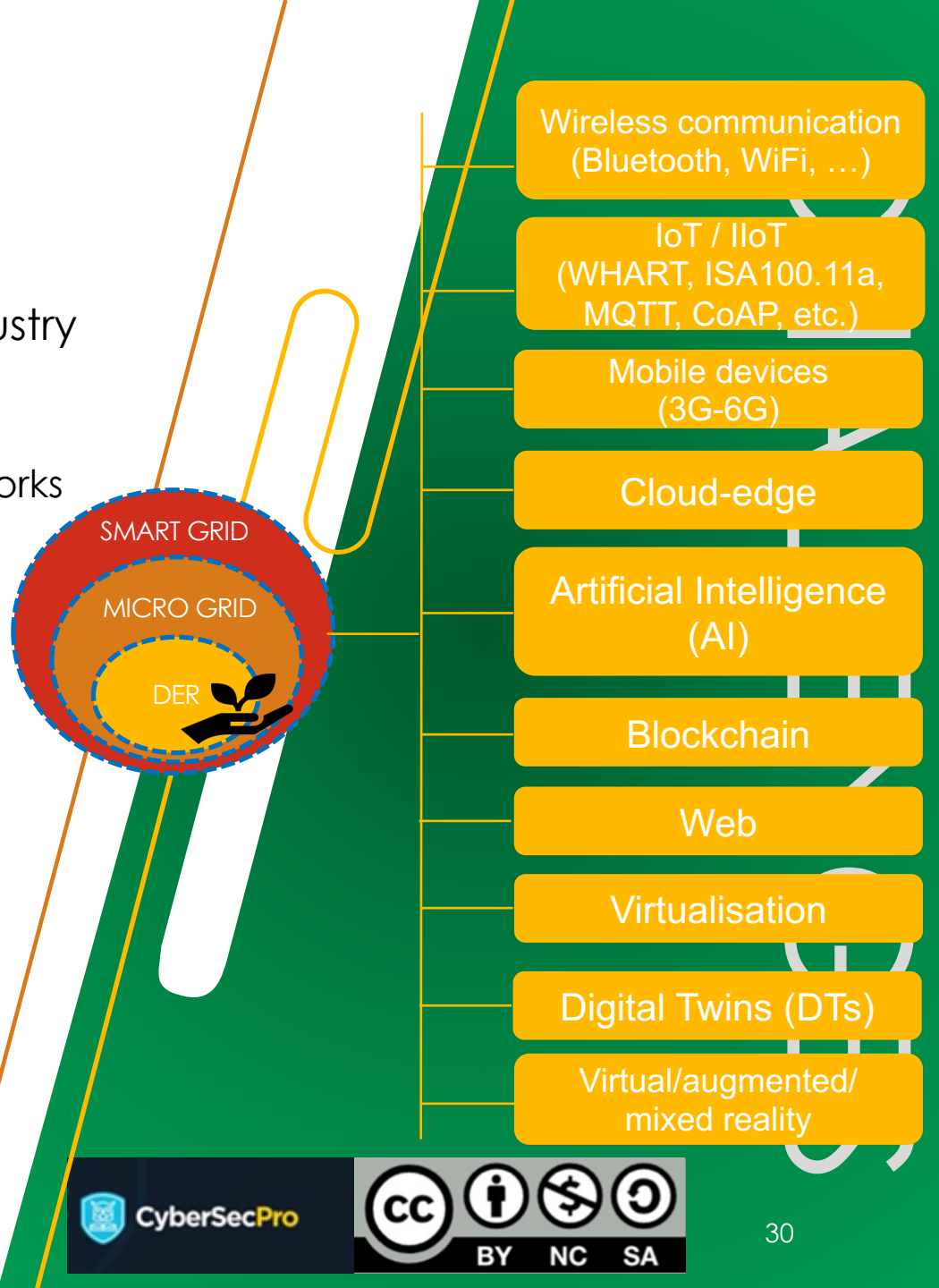
- Technological convergence
  - Information Technology (IT)/Operational Technology (OT)
- Complexity of the environment and their networks
  - Different types of communication networks - wired/wireless
- Inheritance of vulnerabilities
- Insecure legacy devices

Figure source: Vecteezy
URL:https://www.vecteezy.com

CHALLENGES

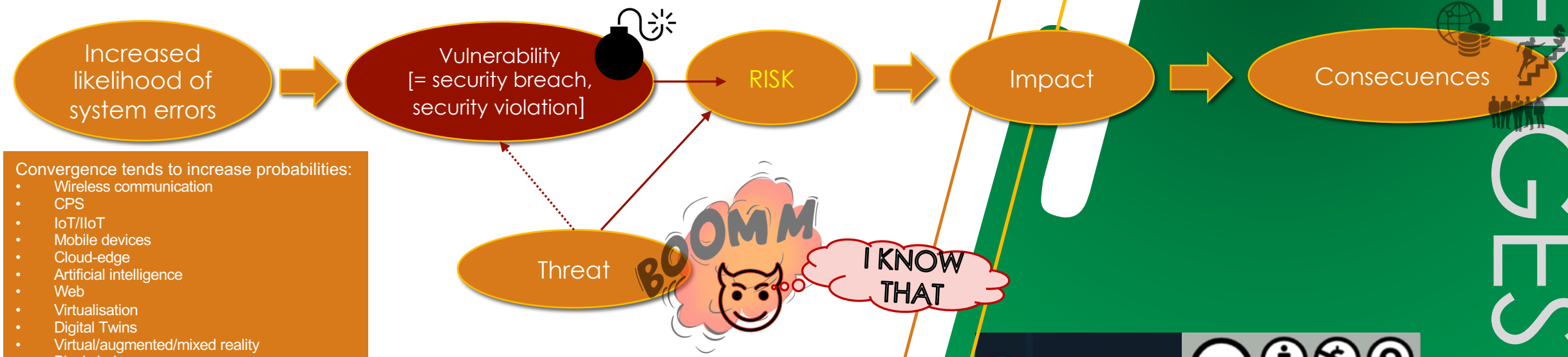
Technological convergence and complexity

- Multiple ITs emerge in the new conceptualisation of Industry 4.0/5.0, which applied to energy industry corresponds to **Energy 4.0/5.0**
  - These technologies could run on wireless and/or wired networks
  - Unfortunately, wireless communications bring threats:
    - Man-in-the-Middle
    - Eavesdropping
    - Spoofing
    - And a long etc.
- Most of these ITs must coexist with other existing ones
  - **OTs**: Controllers, sensors, smart meters, PMUs, HMIs, etc.
  - **Interconnection devices**: routers, switches, etc.
  - **Security devices**: firewalls, proxies, IDS/IPS, SIEMs, etc.
- RESULTING IN … **HETEROGENOUS AND COMPLEX CONTROL NETWORKS**



Inheritance of vulnerabilities and legacy devices

- According the NIST, a **vulnerability** can be defined as a "***weakness*** *in a system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat*"
  - ENISA also defines it as "*a* ***weakness*** *an adversary could take advantage of to compromise the confidentiality, availability, or integrity of a resource*"



Convergence tends to increase probabilities:
- Wireless communication
- CPS
- IoT/IIoT
- Mobile devices
- Cloud-edge
- Artificial intelligence
- Web
- Virtualisation
- Digital Twins
- Virtual/augmented/mixed reality
- Blockchain

CHALLENGES

Inheritance of vulnerabilities and legacy devices

- If we explore in detail some of the security features of some technologies, we might appreciate the following:

IIoT/IoT/CPS	Cloud-Edge	Artificial Intelligence	Blockchain	Digital Twins (DTs)	Virtual/augmented/mixed reality, attractive dashboards, ...
• HW/SW devices with limited resources to incorporate security measures • Security is therefore limited, and reliability mechanisms are lacking • Most devices still rely on batteries and wireless networks to function properly • …	• Limited control over data and actions of third parties • Threats may lead to privacy violations • Exposure of data if not adequately protected • …	• Risks of privacy issues due to the processing of large data volumes • Many AI models are accessible and public • Limited access control to models and training data • …	• Privacy risks due to data "sharing" • Data and device scalability • Necessary access control and security control mechanisms • …	• Limited control over data (e.g. DT models) and the intellectual property • Threats may lead to data privacy breaches • Violations of the integrity of the system itself if the DT is not properly protected against changes or falsifications • …	• Frequent parameter validation, filtering and sanitisation of input data • Necessary access control and least privilege • Protection of sensitive data and data integrity to avoid falsification or concealment of data (e.g. sensor measurements, statuses, etc.) • …

- In addition, many other security risks and vulnerabilities arising from legacy HW and SW components must be considered, such as:
  - CVE-2024-34244: "*libmodbus v3.1.10 is vulnerable to Buffer Overflow via the modbus_write_bits function*"- URL: https://nvd.nist.gov/vuln/detail/CVE-2024-34244
  - CVE-2024-25998: "*An unauthenticated remote attacker can perform a command injection in the OCPP Service with limited privileges due to improper input validation*" – OCPP is a very common common protocol for charging stations – URL: https://nvd.nist.gov/vuln/detail/CVE-2024-25998

Source: NIST, National Vulnerability Database (NVD), 2024
URL: https://www.netresec.com/?page=PCAP4SICS

What is public to enhance our security

- Most of the vulnerabilities are public through **Common Vulnerabilities and Exposures (CVEs)**, which explain the origin, the level of criticality and the affected resources
  - They are based on a unique identifier, **CVE-YYYYY-NNNN**, where **YYYYY** is the year and **NNNN** is the vulnerability number
- There are many repositories and websites reporting types of vulnerability and exposures, such as NIST NVD and MITRE CVE
- The publication procedure is simple and should be handled by any grid operator:

1. An entity must first discover the vulnerability and reports it to these organisations
2. A CVE-ID identifier associated with the vulnerability is requested
3. The characteristics associated with the vulnerability are specified (affected products, type of vulnerability, cause, impact, and at least one public reference)
4. Finally, the vulnerability is published

These types of reports and others to Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) are fundamental to avoid major impacts, and to promote **situational awareness** in related environments

CHALLENGES

Sources: NIST NVD: https://nvd.nist.gov/ and MITRE CVE: https://cve.mitre.org/

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 us:

- Cristina Alcaraz
  alcaraz@uma.es
- Abdelkader Shaaban
  abdelkader.shaaban@ait.ac.at