Cybersecurity Essentials and Management for Energy Sector

CSP001_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-2: Foundational Knowledge and Taxonomy of Energy Cybersecurity and Body of Knowledge

Overview

- Define energy cybersecurity and its significance in the energy domain
- Understand the various components of an energy cybersecurity ecosystem
- Classify cybersecurity threats and vulnerabilities specific to energy systems
- Overview of the Cybersecurity Body of Knowledge

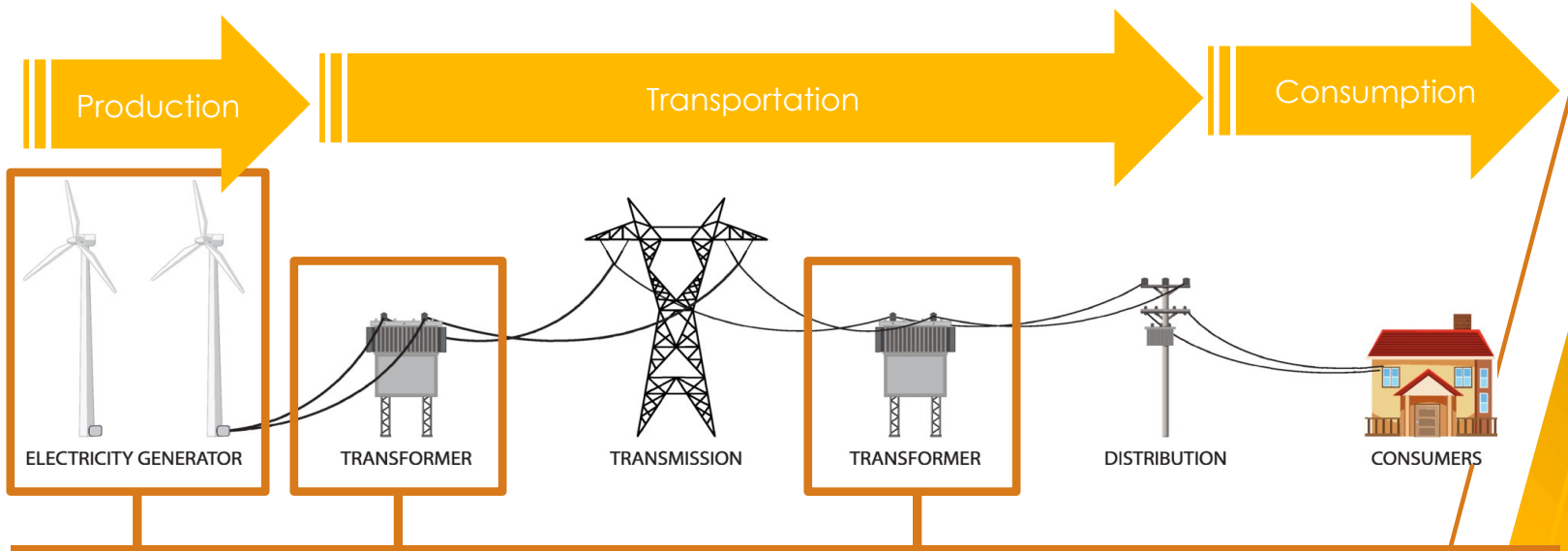
Topic-2: Foundational Knowledge and Taxonomy of Energy Cybersecurity and Body of Knowledge

Overview

- Define energy cybersecurity and its significance in the energy domain
- **Understand the various components of an energy cybersecurity ecosystem**
- Classify cybersecurity threats and vulnerabilities specific to energy systems
- Overview of the Cybersecurity Body of Knowledge

Typical operational stages of power systems

- Traditional electrical power systems usually follow systematic procedures,
  - where a set of industrial equipment and operational devices are configured to **produce and transport energy** to end-users



Both power production and its transformation for transport are carried out at energy substations: *physically subnets deployed around and close to CIs, and composed of control subnetworks with controllers, sensors, actuators, among other components*

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

Typical operational stages of power systems

- More specifically, three operational stages arise in power systems:
  - **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

Typical operational stages of power systems

- More specifically, three operational stages arise in power systems:
  - **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
  - **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

CLASSIC OPERATION

Typical operational stages of power systems

- More specifically, three operational stages arise in power systems:
  - **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
  - **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
  - **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

CLASSIC OPERATION

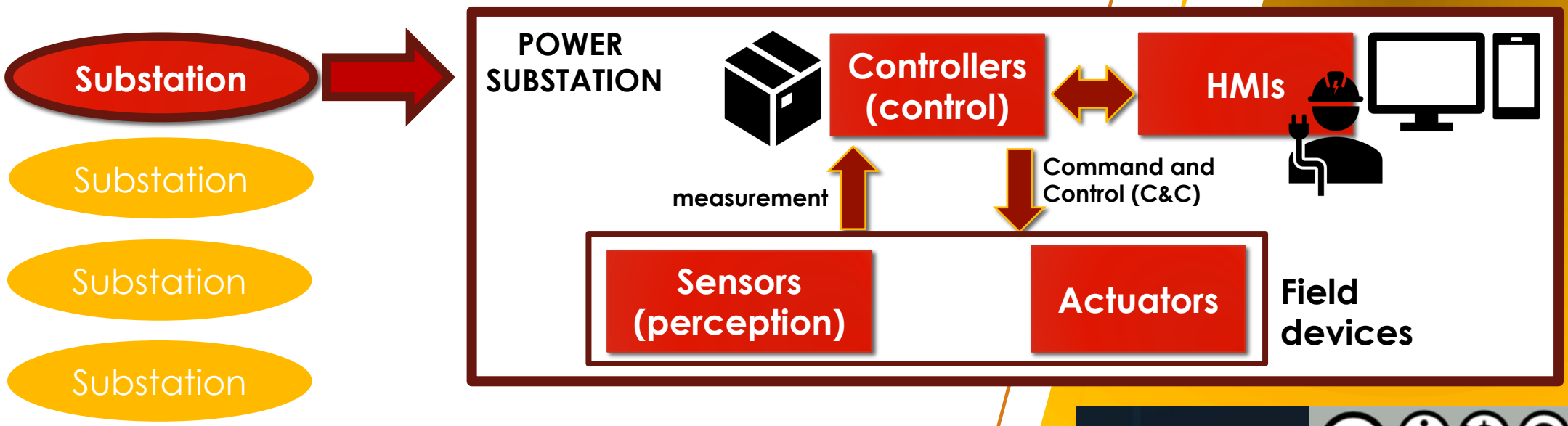
Typical operational stages of power systems

- Summarizing:
  - **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 – TO PRODUCE LARGE AMOUNTS OF POWER
  - **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 – TO INTENSIFY THE VOLUMEN FOR ITS TRANSPORT
  - **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 – TO REDUCE THE VOLUMEN FOR ITS CONSUMPTION

CLASSIC OPERATION

Typical operational technologies of power systems

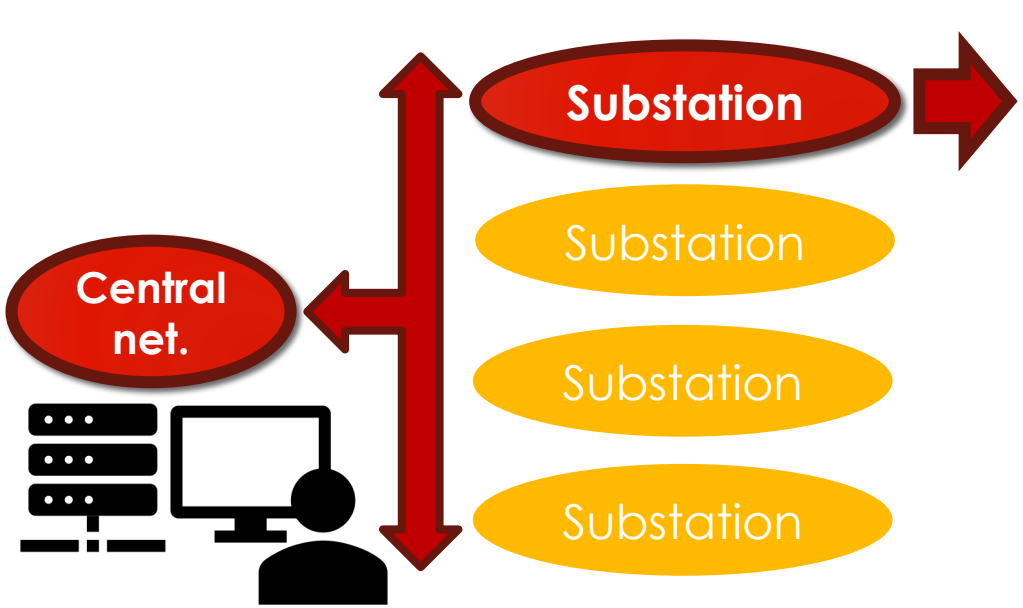
- Each substation is based on a set of Operational Technologies (OTs), such as:
  - **Field devices** such as sensors and actuators
  - **Controllers** such as Remote Terminal Units (RTUs) / Programmable Logic Controllers (PLCs) connected to field devices
  - **Human Machine Interfaces** (HMIs)

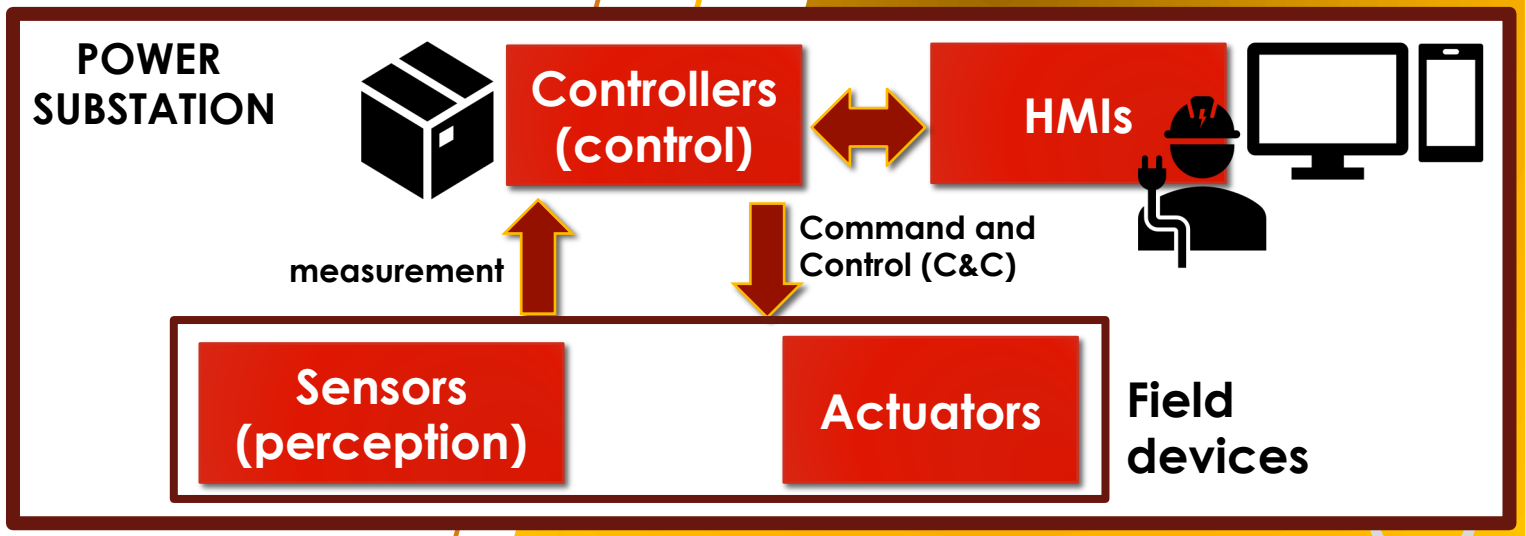


CLASSIC OPERATION

Typical operational technologies of power systems

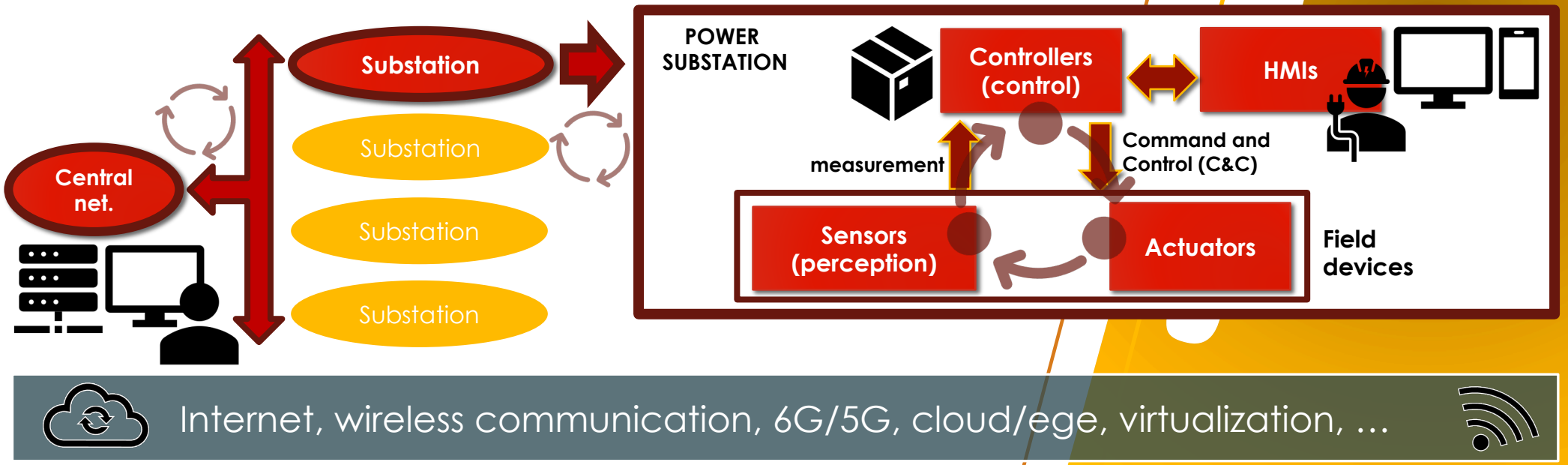
- Thus, through controllers human operators can have **a clear picture of the status of the entire system (or a subpart of it)** and control it locally or remotely
  - Human operators need to receive the information (dynamics / physical processes) from the context via sensors and controllers
  - Human operators needs to act with the context via controllers and actuators





Typical operational technologies of power systems

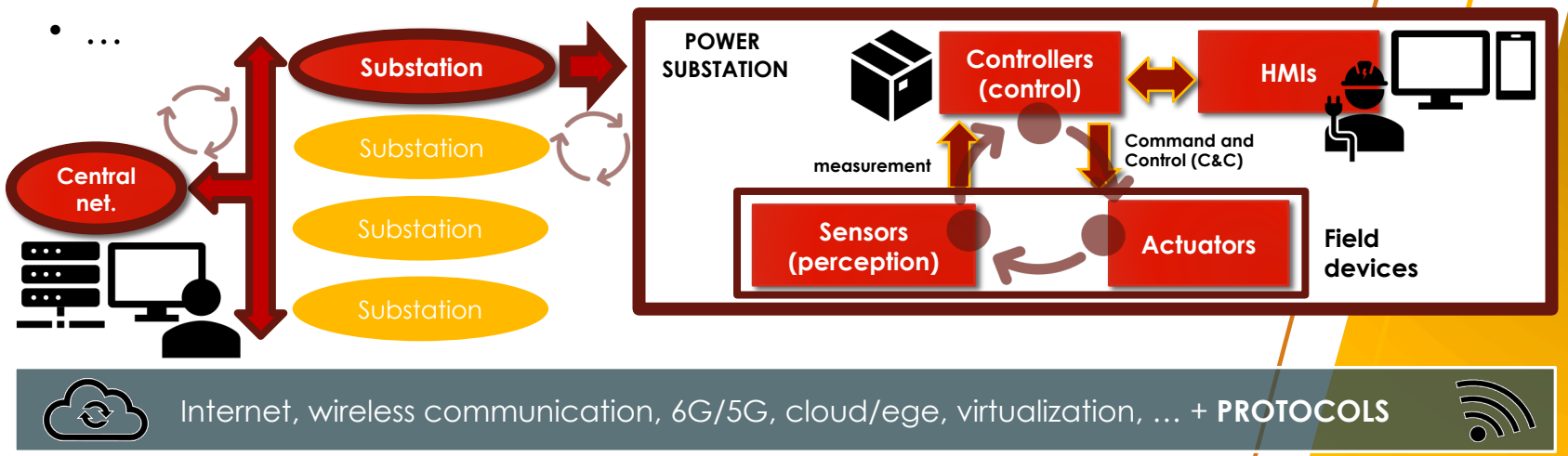
- In order to achieve this type of control, multiple types of **Information and Communication Technologies (ICTs)** emerge
  - Through ICTs human operators can (locally/remotely) monitor and control physical processes/devices deployed close to critical infrastructures, creating a sort of closed loop



CLASSIC OPERATION

Typical operational technologies of power systems

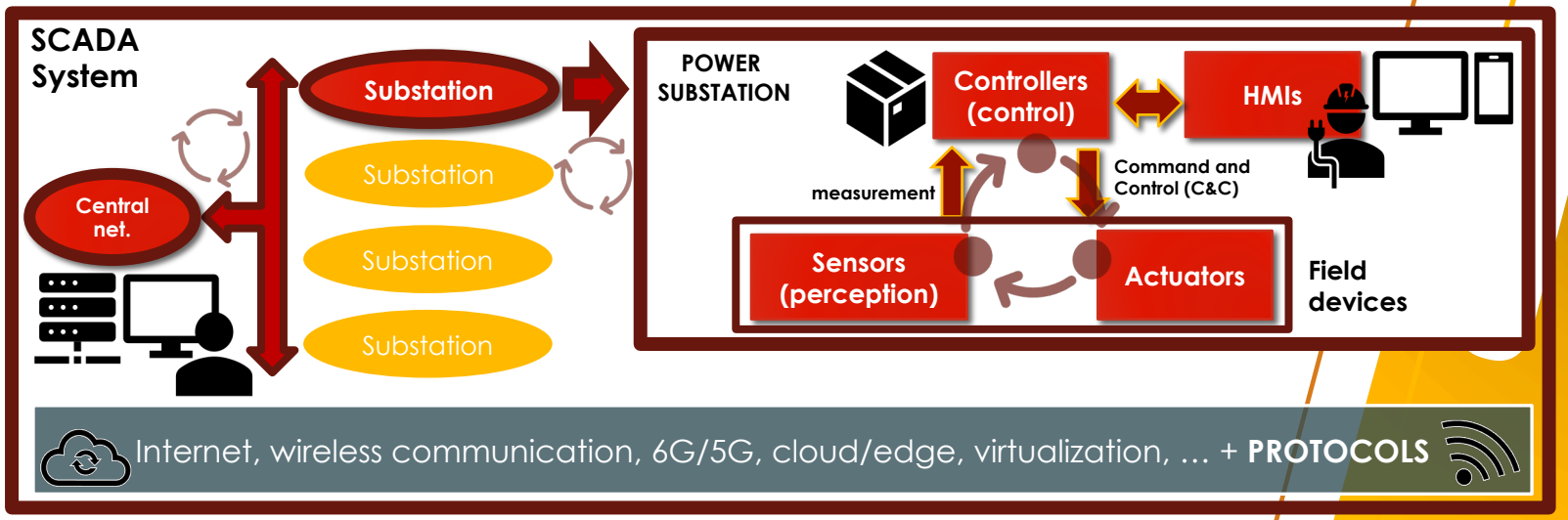
- Interconnection of systems and components can be carried out through:
  - Serial or TCP/IP communication
  - Gateway/backend servers
  - Cloud/edge infrastructures
  - Industrial comm. protocols: ModbusTCP, DNP3, IEC 104, S7, OPC UA,…
  - IoT comm. protocols : MQTT, CoAP, HTTPS,…
  - …



CLASSIC OPERATION

Typical operational technologies of power systems

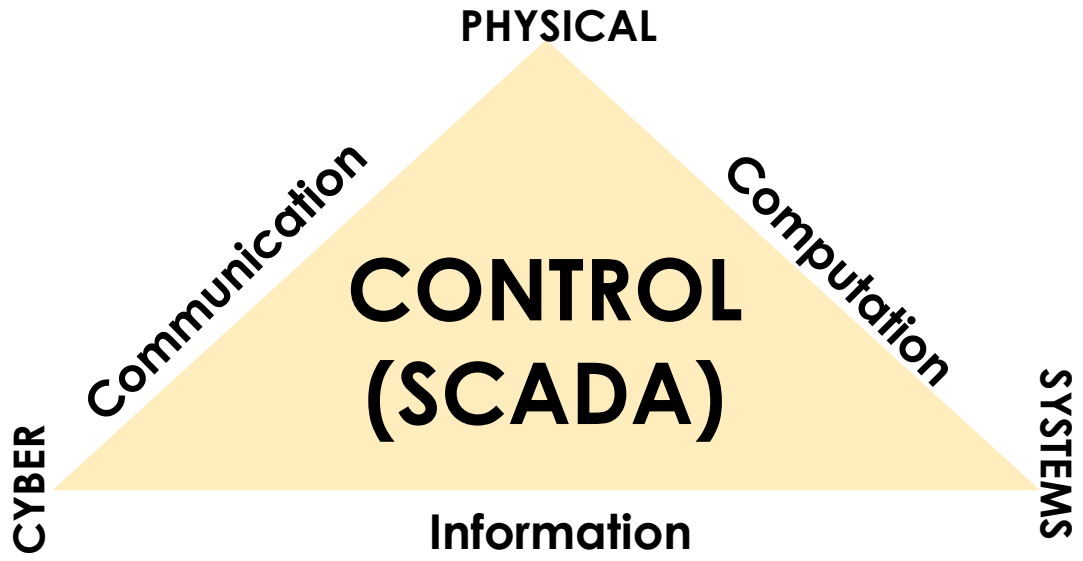
- The joining of these subnetworks is what results in the concept of **Supervisory Control and Data Acquisition (SCADA)** systems
- SCADA systems are networks capable of:
  - Processing large volumes of data from controllers or (I)IoT gateways
  - Analysing and changing the statuses of the observed environment via the controllers or (I)IoT gateways



CLASSIC OPERATION

New conceptualization of control in power systems

- Now, from a holistic perspective, we can introduce the well-known concept of "**Cyber-Physical System**" (CPS), which was introduced by Helen Gill of the U.S. National Science Foundation in 2006
  - She conceives the term of CPS as the way to combine and integrate computation with physical processes – but also communication

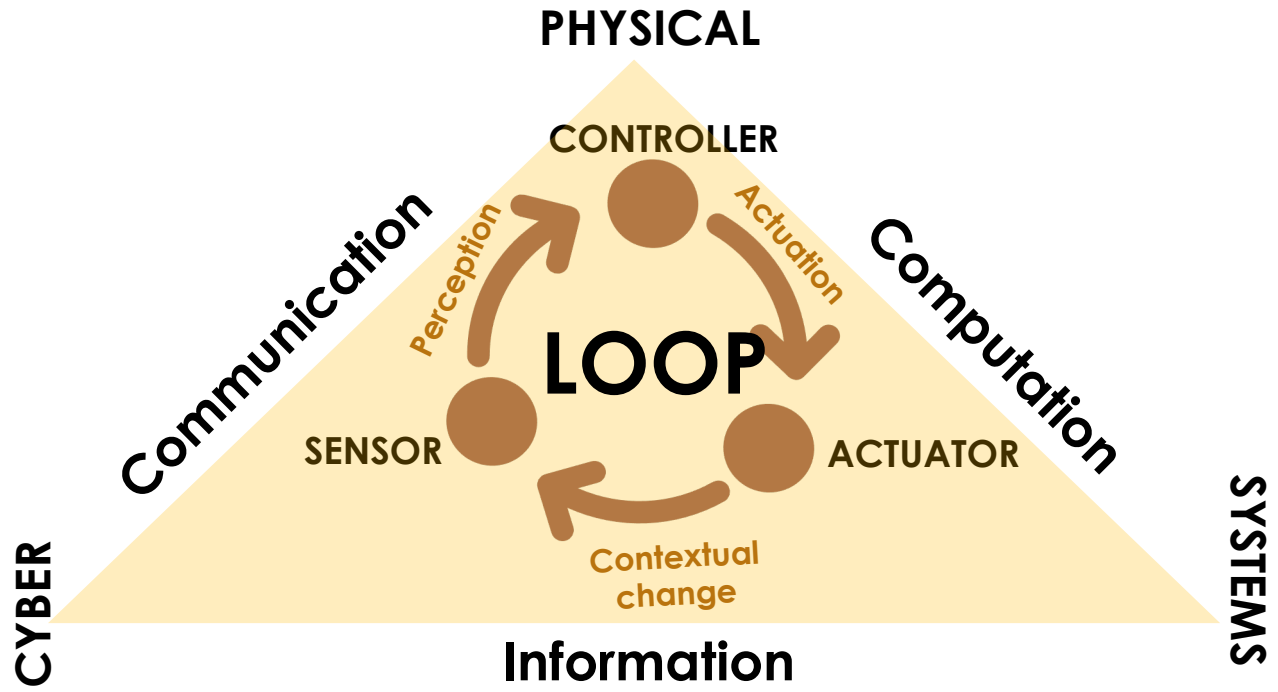


CPS can be understood as a **new discipline capable of capturing a set of theories, techniques and components of control** such as: embedded systems, real-time systems, hybrid systems (including IT), control theory, sensor networks, formal methods, among others

Source: S. A. Seshia, "Explorations in cyber-physical systems education", *Communications of the ACM*, *65*(5), 60-69, 2022

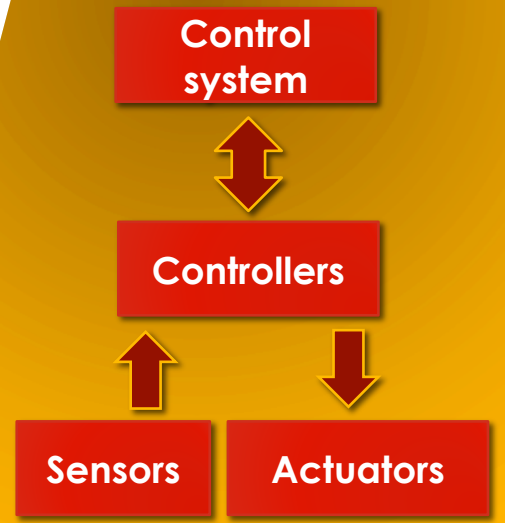
New conceptualization of control in power systems

- If we expand the main control elements in SCADA systems, we then obtain the follow structure:



What is more, each substation can be considered as CPS in nature

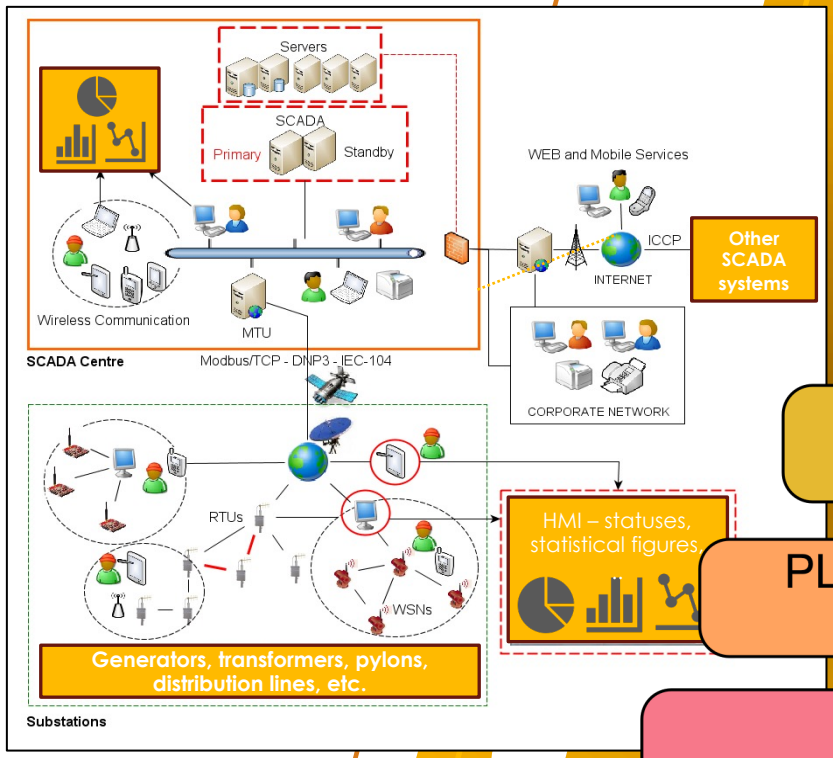
Thus, a CPS is a system capable of **embedding and orchestrating a set of computation and communication components** to process dynamics/physical processes of the "real-world" (and following a closed loop)



Source: S. A. Seshia, "Explorations in cyber-physical systems education", *Communications of the ACM*, *65*(5), 60-69, 2022

Typical control architectures

- In order to introduce the current control architectures, it is first necessary to go back to the traditional control systems
- Observing the figure, we can appreciate that SCADA systems are mainly composed of three main nets, following a rigorous **hierarchical architecture**:
  - Corporative networks
  - The control network
  - Substations
- The architecture follows the traditional ISA-95 model



CLASSIC OPERATION

ERP

MES, WMS

SCADA, HMI

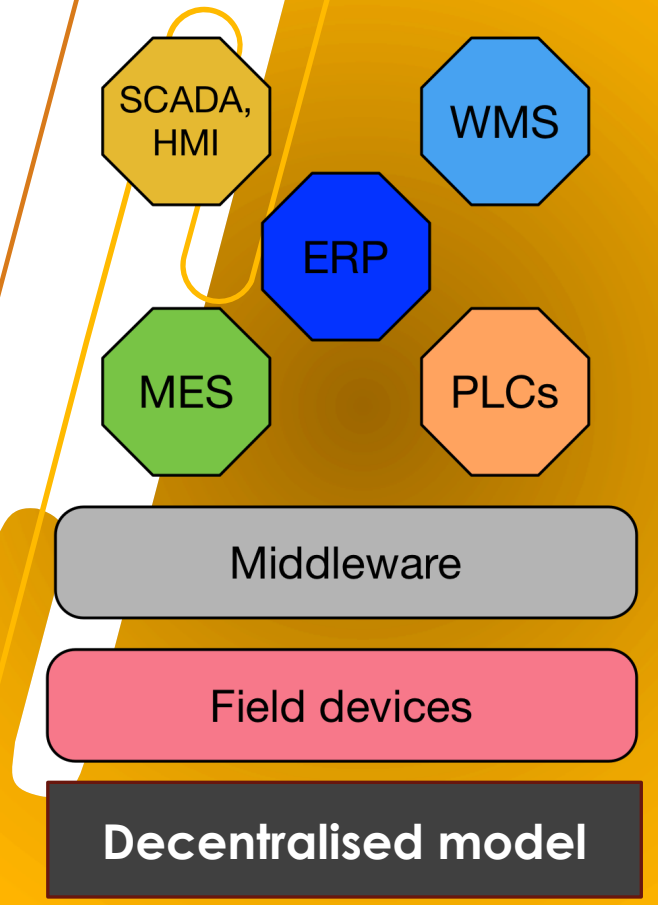
PLCs, sensors and actuators

Field devices

Hierarchical model

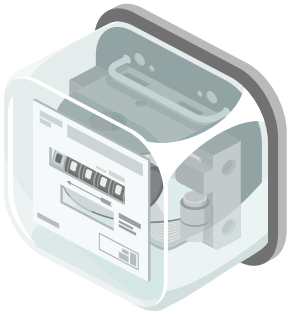
Modern control architectures

- However, this hierarchical conceptualisation is diluted with the current need 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 energy production and its distribution without energy waste
  - such that substations can be able to "*produce power according to the actual demand*"
- This evolution toward a new conceptualisation of "*smart ecosystem*" is what results in the power sector as: **Smart Grid system**



CLASSIC OPERATION

Modern control architectures

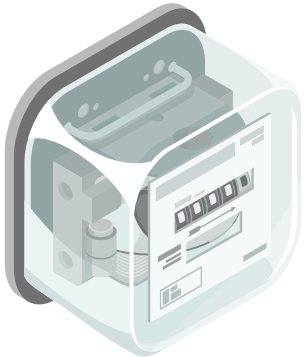


- To create a "smart" ecosystem capable of producing power according to the actual demand, it is required to:
  - Connect the control systems with the real world (the cities) through **smart meters**, which dynamically perceive actual consumption
  - Intensify the cooperation among stakeholders, as well the energy supply chain under regulatory frameworks
- Among the **stakeholders**, we highlight:
  - Grid operators such as:
    - Transmission System Operators (TSO)
    - Distribution System Operators (DSO)
  - Suppliers or providers to facilitate the use of the energy
  - Authorities or regulators to establish operation rules
  - Consumers / prosumers

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

Modern control architectures

- As previously mentioned, **smart meters** are essential operational components to dynamically perceive actual energy consumption in one or several areas
- Smart meters are normally connected to collectors to transfer the consumption values, and enable to
  - The control system to dynamically produce and distribute energy per area
  - The payment system to compute the final consumption value



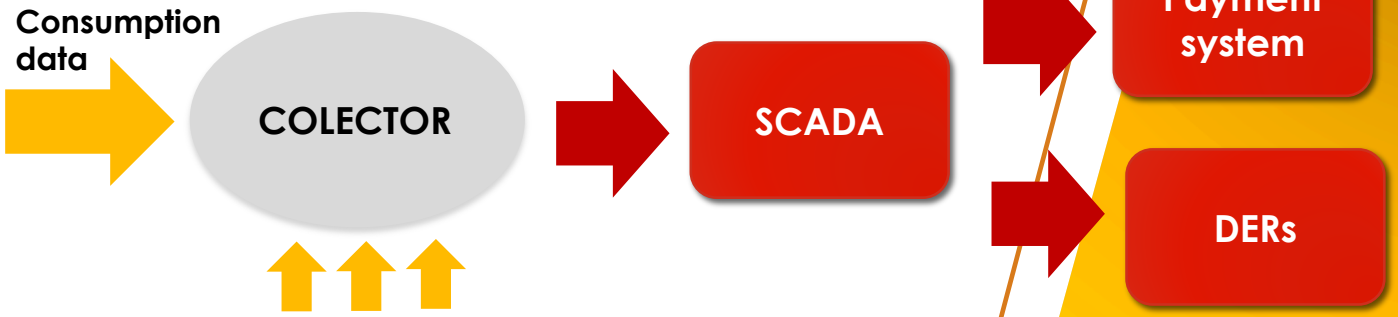
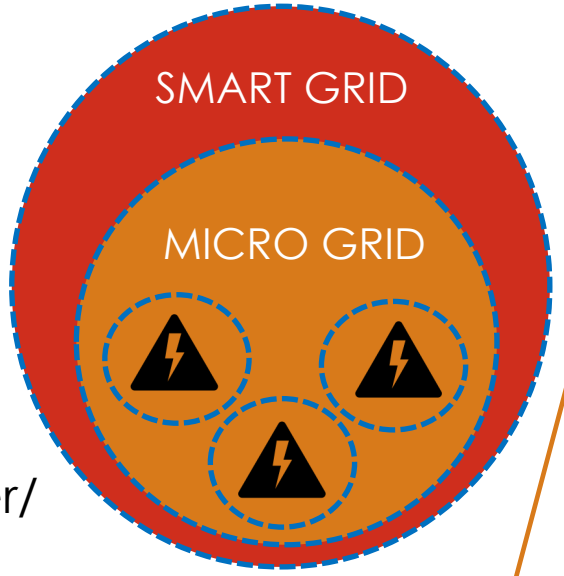


Figure source: Vecteezy
URL:https://www.vecteezy.com

From Smart Grids to Microgrids & DERs

- As part of the Smart Grid, **microgrid-based systems** emerge to produce energy in a "safe" way
- Microgrids correspond to mini-substations deployed close to the end user, whose main purpose is to:
  - Locally provide energy
  - Connect to the main grid to transfer/ receive energy



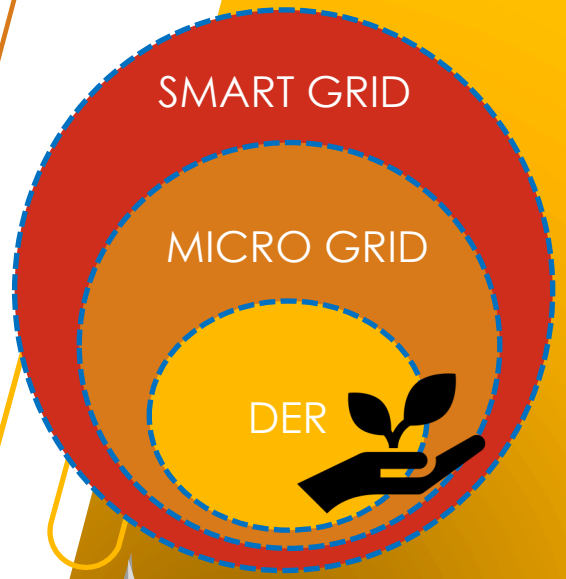
- This type of deployment creates "operational islands" with the objective of increasing:
  - "resilience" by reducing the impact of potential outages

CLASSIC OPERATION

From Smart Grids to Microgrids & DERs

- In the context of microgrids, we can also find
  - **Distributed Energy Resources** (DER)
    - Renewable systems such as solar panels or wind farms
    - Storage systems
    - Electrical vehicles (EVs) - EV batteries can revert energy to the grid if V2G exists
  - **Control systems**
  - **Smart meters**

Vehicle-to-Grid (V2G) is based on technologies that enable energy to be returned into the grid from the EV batteries

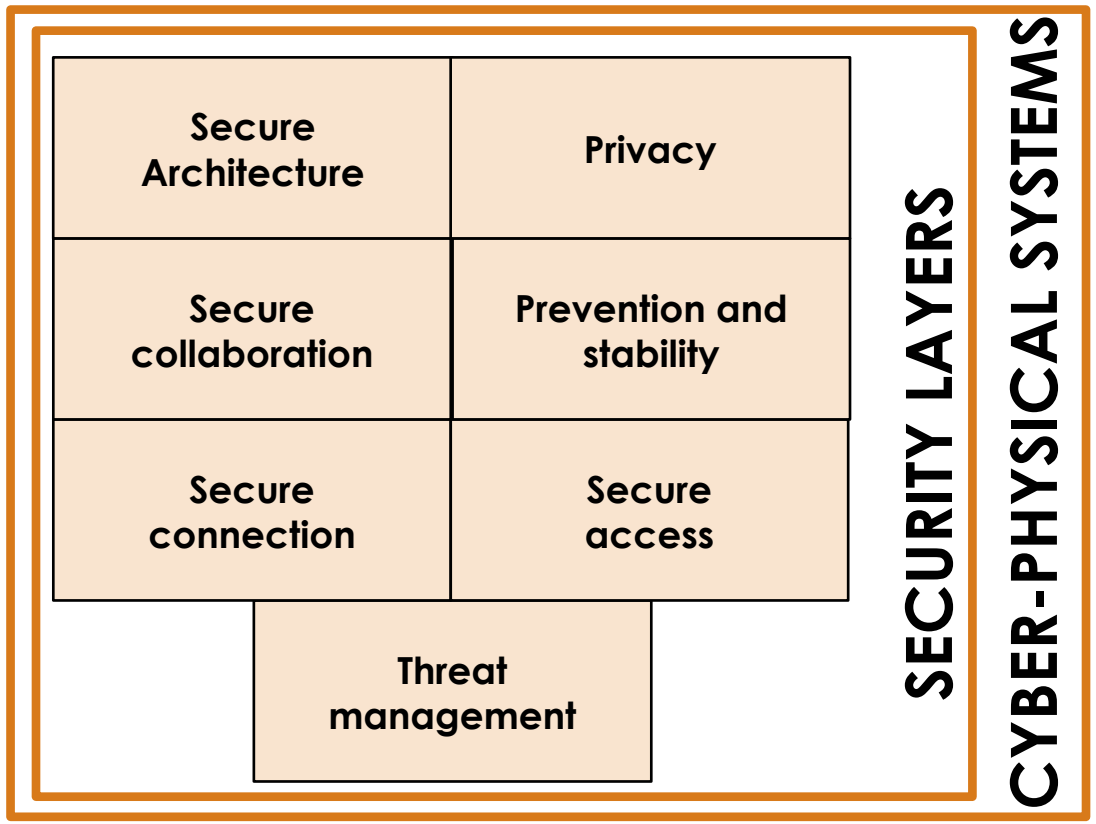


CLASSIC OPERATION

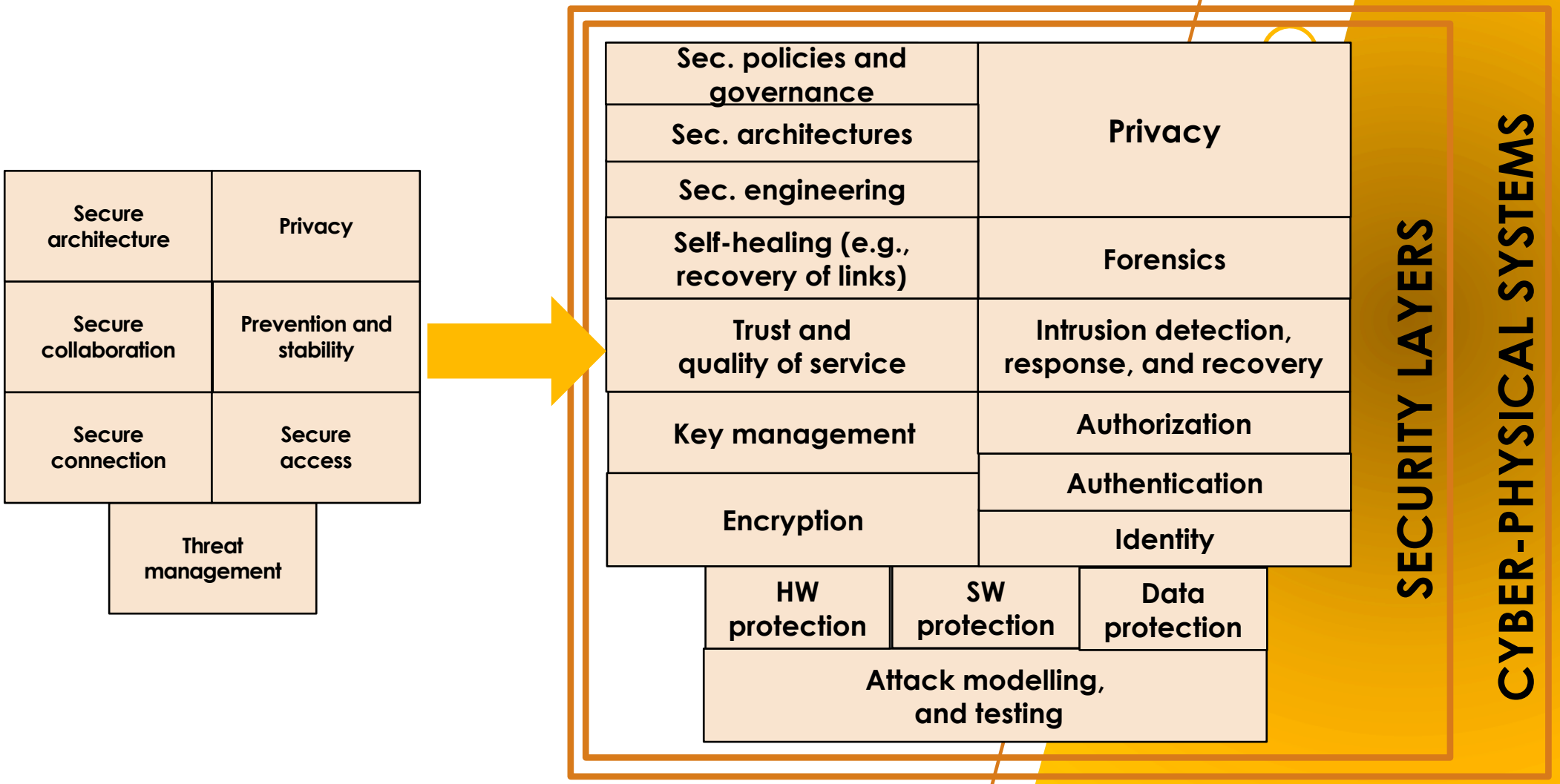
Figure source: Vecteezy
URL:https://www.vecteezy.com

Other relevant components in energy cybersecurity ecosystem

- Beyond the typical and modern operational components, it is also essential to consider other relevant elements related to cybersecurity and their protection layers



Other relevant components in energy cybersecurity ecosystem



Final remarks

- We have reviewed the functionality of both the conventional and modern power systems, and we have explored the main components of an energy cybersecurity ecosystem, such as:
  - Control substations and their main cyber-physical components that includes ICTs and protocols
  - SCADA systems
  - Smart Grid systems and microgrids
  - DERs
  - Smart meters
  - Stakeholders
- We have also introduced and linked the concept of CPS to power sector to handle the new terminologies, as well as cybersecurity components

References and sources

1. Some figures are attributed from Vecteezy,
   URL: https://www.vecteezy.com/ - thanks !
2. DeepL Translator for Proofreading:
   URL: https://www.deepl.com/translator
3. S. A. Seshia, "Explorations in cyber-physical systems education", Communications of the ACM, 65(5), 60-69, 2022

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

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:

- Cristina Alcaraz
  Associate Professor
  University of Malaga
  alcaraz@uma.es