

EC-Council

Internet of things

IOT


CCT

Certified Cybersecurity Technician

Module - 13

IoT and OT Security

This page is intentionally left blank.



Module Objectives

- 1 Understanding IoT and Why Organizations Opt for IoT-enabled Environments
- 2 Overview of IoT Application Areas and IoT Devices
- 3 Understanding the IoT Architecture and IoT Communication Models
- 4 Understanding the Security in IoT-Enabled Environments
- 5 Understanding OT and the Purdue Model
- 6 Overview of the Components of an ICS
- 7 Understanding the Security in OT-enabled Environments

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

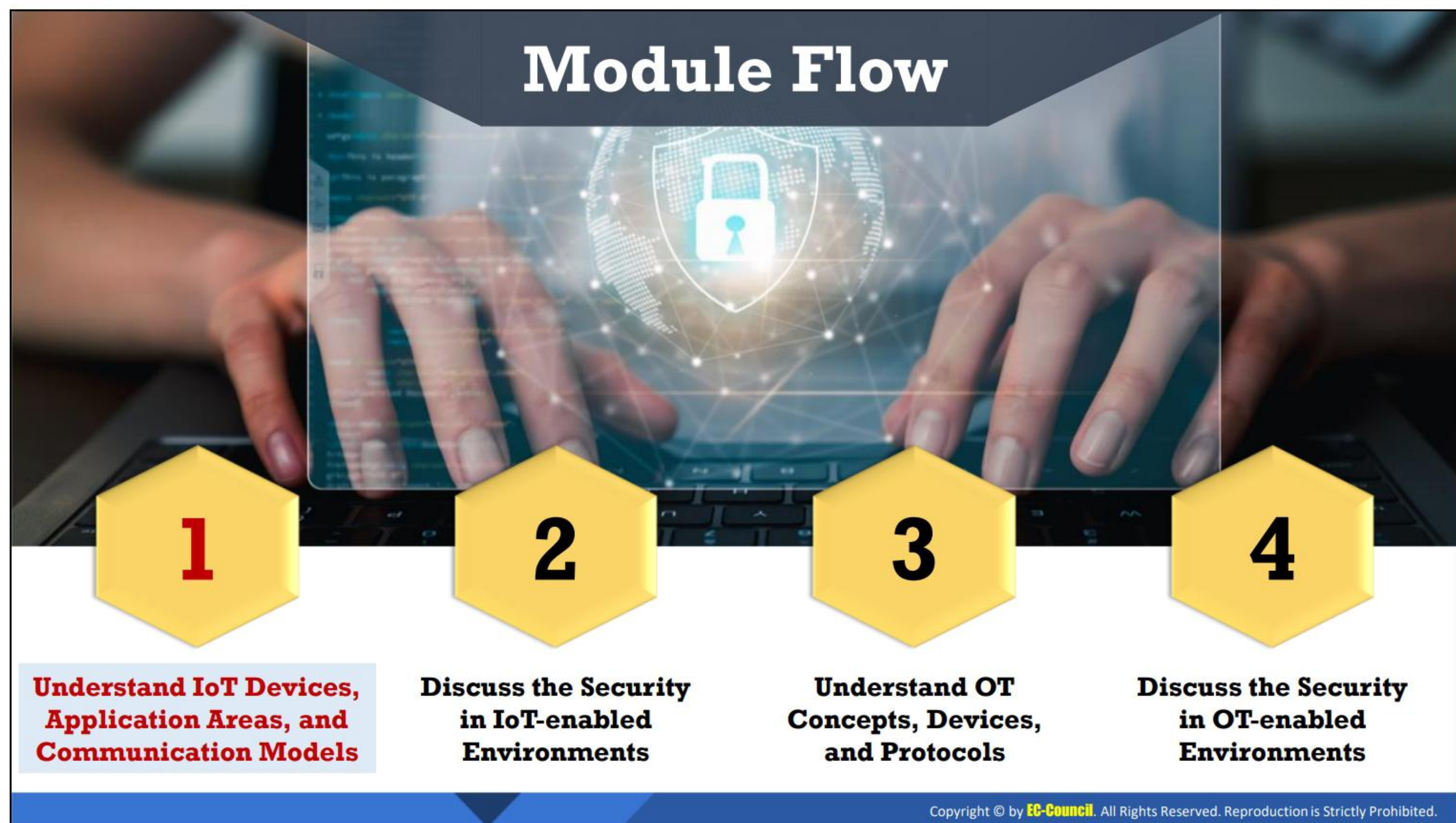
The Internet of Things (IoT) has evolved from the convergence of wireless technology, micro-electromechanical systems, micro-services, and the Internet. The IoT has introduced a range of new technologies with associated capabilities into our daily lives. As the IoT is an evolving technology, the immaturity of technologies and services provided by various vendors will have a broad impact on organizations, leading to complex security issues. IoT security is difficult to ensure as the devices use simple processors and stripped-down operating systems that may not support sophisticated security approaches. Organizations using these devices as part of their network need to protect both the devices and the information from attackers.

As industrial companies are digitizing their industrial facilities to enhance operational efficiency through Internet connectivity and remote data access, they need to increasingly focus on cybersecurity to mitigate new threats and safety issues arising from the convergence of operational technology and information technology (OT–IT). Organizations need to understand the landscape of cyber threats, industrial infrastructure, and business. Before implementing cybersecurity policies and controls, organizations need to identify and prioritize key risks and threats that will have the greatest impact on their business.

At the end of this module, you will be able to do the following:

- Understand IoT and why organizations opt for IoT-enabled environments
- Describe IoT application areas and IoT devices
- Describe the IoT architecture and IoT communication models
- Understand security in IoT-enabled environments
- Understand OT and the Purdue model

- Explain the components of an ICS
- Understand security in OT-enabled environments



Understand IoT Devices, Application Areas, and Communication Models

The objective of this section is to understand IoT devices and areas where IoT devices can be used in an enterprise.

What is IoT?

- ❑ Internet of Things (IoT), also known as **Internet of Everything** (IoE), refers to the network of devices having IP addresses and the capability to sense, collect, and send data using embedded sensors, communication hardware and processors
- ❑ In IoT, the term **thing** is used to refer to a device that is **implanted on natural, human-made, or machine-made** objects and has the functionality of **communicating over the network**

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

What is IoT?

The Internet of Things (IoT), also known as the Internet of Everything (IoE), refers to computing devices that are web-enabled and have the capability of sensing, collecting, and sending data using sensors, and the communication hardware and processors that are embedded within the device. In the IoT, a “thing” refers to a device that is implanted in a natural, human-made, or machine-made object and has the functionality of communicating over a network. The IoT utilizes existing emerging technology for sensing, networking, and robotics, therefore allowing the user to achieve deeper analysis, automation, and integration within a system.

With the increase in the networking capabilities of machines and everyday appliances used in different sectors like offices, homes, industry, transportation, buildings, and wearable devices, they open up a world of opportunities for the betterment of business and customer satisfaction. Some of the key features of the IoT are connectivity, sensors, artificial intelligence, small devices, and active engagement.

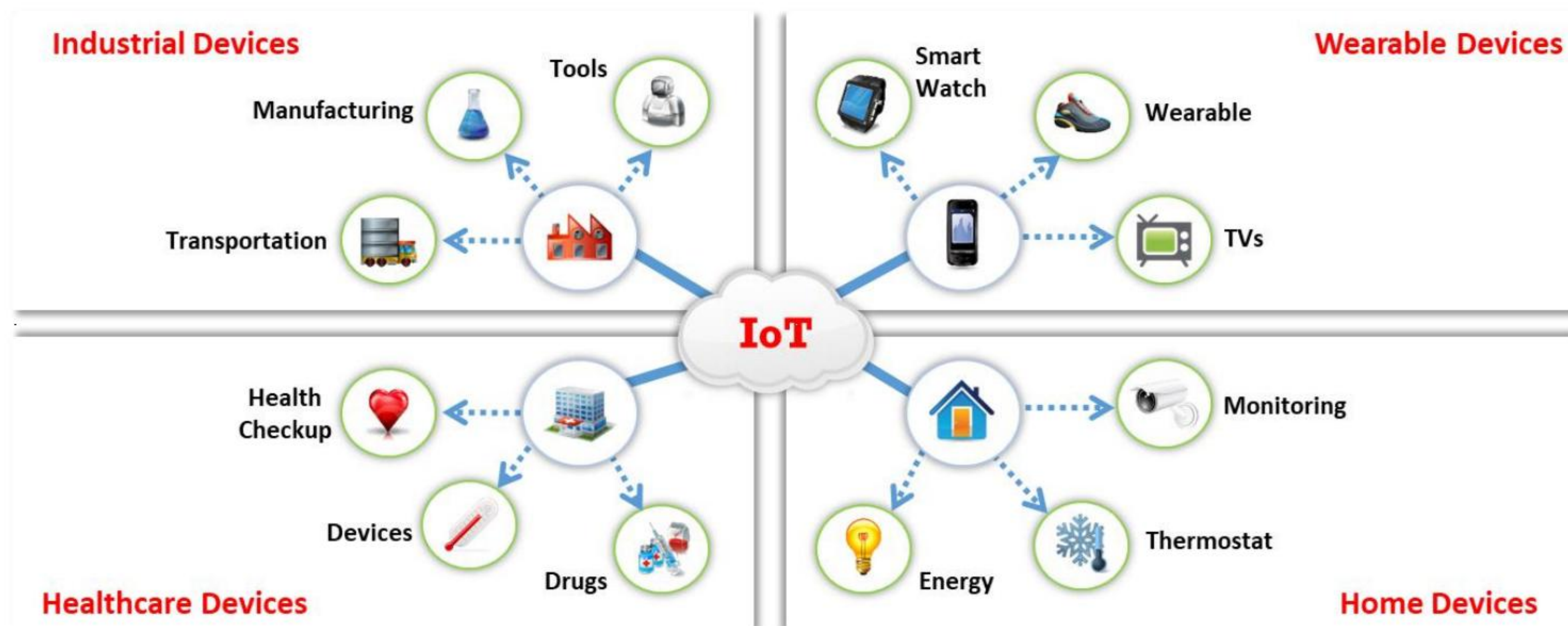
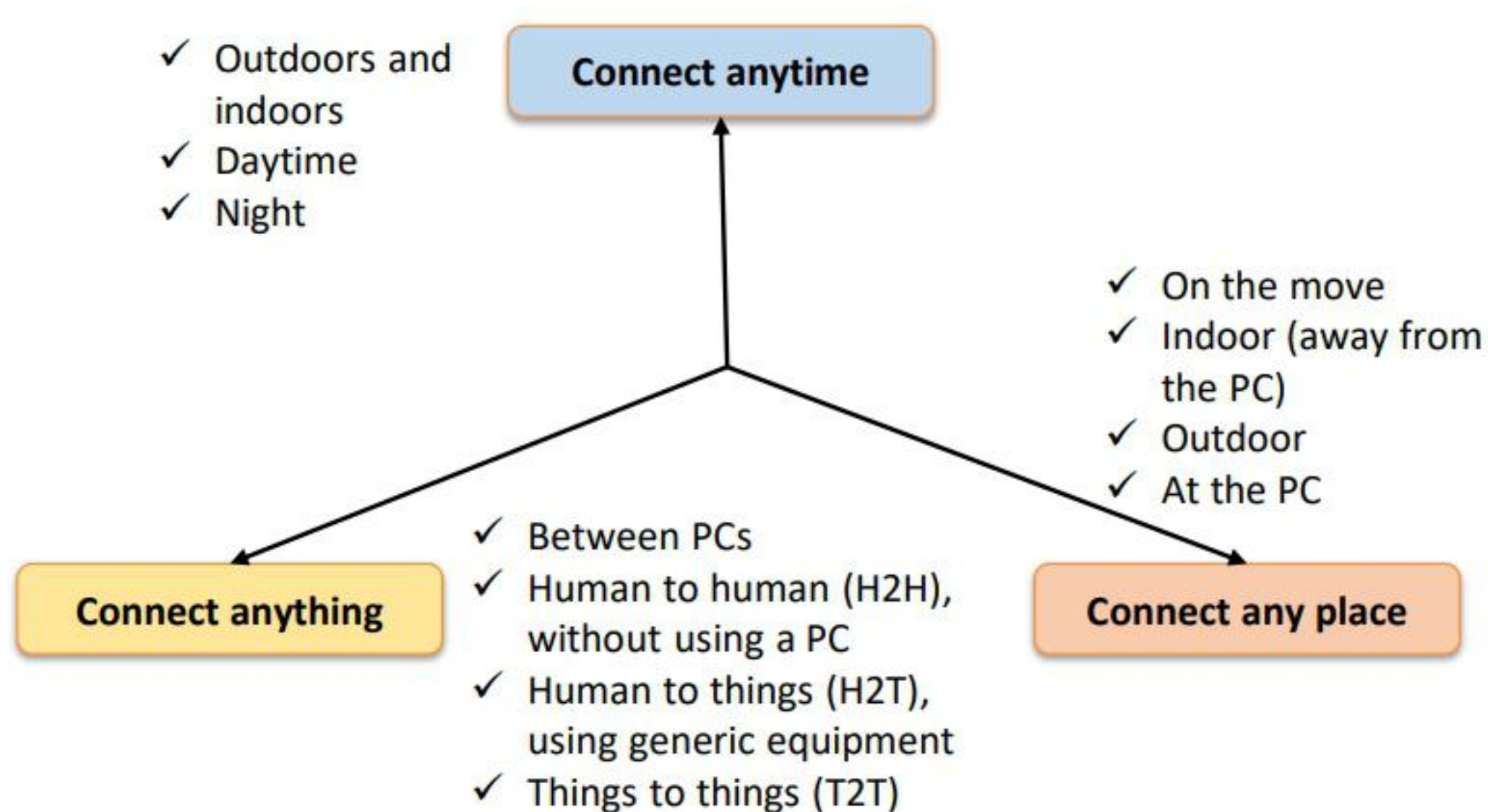


Figure 13.1: Illustration of IoT devices

Why Organizations are Opting for IoT-enabled Environments



IoT devices work on a **three-dimensional plane**, offering connectivity for anyone at anytime, for anything, and from any place



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Why Organizations are Opting for IoT-enabled Environments

Organizations are opting for IoT-enabled environments because IoT devices work on a three-dimensional plane and provide connectivity for anyone at any time, for anything, and from any place. IoT devices facilitate connection to various objects; examples include Human-to-Thing (H2T) interactions using generic equipment, Thing-to-Thing (T2T) interactions between PCs, and Human-to-Human (H2H) interactions without using a PC. The user can connect to IoT devices at any place regardless of whether they are on the move, indoor (away from PC), outdoor, or at the PC. The working mechanism of IoT devices on the three-dimensional plane allows the user to continuously monitor their business, resolve concerns instantly, increase the efficiency of the business, enhance the growth of the organization, increase security, etc.

Some key features of IoT are connectivity, sensors, artificial intelligence, small devices, and active engagement. IoT technology includes four primary systems: IoT devices, gateway systems, data storage systems based on the cloud, and remote control using mobile apps. These systems together enable communication between two endpoints. Discussed below are some of the important components of IoT technology that play an essential role in the working of an IoT device.

- **Sensing technology:** Sensors embedded in devices acquire a wide variety of information from the surroundings such as the temperature, gases, location, working of industrial machines, and health data of a patient.
- **IoT gateways:** Gateways are used to bridge the gap between an IoT device (internal network) and the end user (external network), thereby allowing them to connect and communicate with each other. The data collected by the sensors in IoT devices are collected and sent to the concerned user or cloud through the gateway.

- **Cloud server/data storage:** The collected data, after traveling through the gateway, arrives at the cloud, where it is stored and subjected to data analysis. The processed data is then transmitted to the user, who takes actions based on the information received.
- **Remote control using mobile apps:** The end user utilizes remote control devices such as mobile phones, tablets, and laptops installed with a mobile app to monitor, control, retrieve data from, and take actions on IoT devices from a remote location.

Example:

1. A smart security system is integrated with a gateway, which in turn helps connect the device to the Internet and cloud infrastructure.
2. The data storage in the cloud includes the information of every device connected to the network. The information includes the device IDs, the present status of the devices, who accessed the devices, and how many times they accessed the devices. It also includes information such as for how long the device was accessed the last time.
3. The connection with the cloud server is established through web services.
4. The user on the other side, who has the required app to access a device remotely on their mobile phone, interacts with the app and, in turn, with the device. Before accessing the device, they are asked to authenticate themselves. If the submitted credentials match those saved in the cloud, the user obtains access. Otherwise, access is denied, ensuring security. The cloud server identifies the device's ID and sends a request associated with that device using gateways.
5. If the security system recording footage senses any unusual activity, then it sends an alert to the cloud through the gateway, which matches the device's ID and the user associated with it. Finally, the end user receives an alert.

IoT Application Areas and Devices			
Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	HVAC, Transport, Fire & Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/Demand	Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	Infrastructure	Wiring, Network Access, Energy management	Digital Cameras, Power Systems, MID, e-Readers, Dishwashers, Desktop Computers, Washing Machines/Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Awareness & Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience & Entertainment	HVAC/Climate, Lighting, Appliance, Entertainment	
Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctor Office	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Trans Systems	Tolls, Traffic mgmt., Navigation	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices (Cont'd)			
Service Sectors	Application Groups	Locations	Devices
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/Processes	Petro-Chem, Hydro, Carbons, Food, Beverage	
	Converting/Discrete	Metals, Papers, Rubber/Plastic, Metalworking electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environ., Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	
	Public Infrastructure	Water, Treatment, Building, Environ. Equip. & Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

<http://www.beechamresearch.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Application Areas and Devices

IoT devices have a wide range of applications. They are used in almost every sector of society to assist in various ways to simplify routine work and personal tasks and, thus, improve the standard of living. IoT technology is included in smart homes and buildings, healthcare devices, industrial appliances, transportation, security devices, the retail sector, etc.

Some of the applications of IoT devices are as follows:

- Smart devices that are connected to the Internet, providing different services to end-users, include thermostats, lighting systems and security systems, and several other systems that reside in buildings.
- In the healthcare and life science sectors, devices include wearable devices, health monitoring devices such as implanted heart pacemakers, ECG, EKG, surgical equipment, telemedicine, etc.
- The Industrial Internet of Things (IIoT) is attracting growth through three approaches: increasing production to boost revenue, using intelligent technology that is entirely changing the way goods are made, and the creation of new hybrid business models.
- Similarly, use of IoT technology in the transportation sector follows the concept of vehicle-to-vehicle, vehicle-to-roadside, and vehicle-to-pedestrian communication, thus improving traffic conditions, navigation systems, and parking schemes.
- IoT in retail is mainly used in payments, advertisements, and tracking or monitoring products to protect them from theft and loss, thereby increasing revenue.
- In IT and networks, IoT devices mainly include various office machines such as printers, fax machines, and copiers as well as PBX monitoring systems; these serve to improve communication between endpoints and provide ease of sending data across long distances.

Source: <http://www.beechamresearch.com>

Service Sectors	Application Groups	Locations	Devices
Buildings	Commercial/ Institutional	Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums	Heating, Ventilation, and Air Conditioning (HVAC), Transport, Fire and Safety, Lighting, Security, Access, etc.
	Industrial	Process, Clean Room, Campus	
Energy	Supply/ Demand	Power Generation, Transport, and Distribution, Low Voltage, Power Quality, Energy Management	Turbines, Windmills, UPS, Batteries, Generators, Meters, Drills, Fuel Cells, etc.
	Alternative	Solar Wind, Co-generation, Electrochemical	
	Oil/Gas	Rigs, Derricks, Heads, Pumps, Pipelines	
Consumer and Home	Infrastructure	Wiring, Network Access, Energy Management	Digital Cameras, Power Systems, MID, e- Readers, Dishwashers, Desktop Computers, Washing Machines / Dryers, Meters, Lights, TVs, MP3 Devices, Games Consoles, Alarms, etc.
	Awareness and Safety	Security/Alerts, Fire Safety, Elderly, Children, Power Protection	
	Convenience and Entertainment	HVAC/Climate, Lighting, Appliances, Entertainment	

Healthcare and Life Science	Care	Hospital, ER, Mobile, POC, Clinic, Labs, Doctors' Offices	MRI Machines, PDAs, Implants, Surgical Equipment, Pumps, Monitors, Telemedicine, etc.
	In Vivo/Home	Implants, Home, Monitoring Systems	
	Research	Drug Discovery, Diagnostics, Labs	
Transportation	Non-Vehicular	Air, Rail, Marine	Vehicles, Lights, Ships, Planes, Signage, Tolls, etc.
	Vehicles	Consumer, Commercial, Construction, Off-Highway	
	Transport Systems	Tolls, Traffic Management, Navigation	
Industrial	Resource Automation	Mining, Irrigation, Agricultural, Woodland	Pumps, Valves, Vats, Conveyors, Fabrication, Assembly/Packaging, Vessels/Tanks, etc.
	Fluid/Processes	Petrochemicals, Hydro, Carbons, Food, Beverages	
	Converting/Discrete	Metals, Papers, Rubber/Plastic, Metalworking, Electronics, Assembly/Test	
	Distribution	Pipelines, Conveyance	
Retail	Specialty	Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events	POS Terminals, Tags, Cash Registers, Vending Machines, Signs, etc.
	Hospitality	Hotels Restaurants, Bars, Cafes, Clubs	
	Stores	Supermarkets, Shopping Centers, Single Site, Distribution, Centers	
Security / Public Safety	Surveillance	Radar/Satellite, Environment, Military Security, Unmanned, Fixed	Tanks, Fighter Jets, Battlefields, Jeeps, Cars, Ambulance, Homeland Security, Environment, Monitor, etc.
	Equipment	Weapons, Vehicles, Ships, Aircraft, Gear	
	Tracking	Human, Animal, Postal, Food, Health, Baggage	
	Public Infrastructure	Water, Treatment, Building, Environment, Equipment and Personnel, Police, Fire, Regulatory	
	Emergency Services	Ambulance, Police, Fire, Homeland Security	
IT and Networks	Public	Services, E-Commerce, Data Centers, Mobile Carriers, ISPs	Servers, Storage, PCs, Routers, Switches, PBXs, etc.
	Private Enterprise	IT/Data Center Office, Privacy Nets	

Table 13.1: IoT application areas and devices

IoT Technologies and Protocols

Short-range Wireless Communication

- ☐ Bluetooth Low Energy (BLE)
- ☐ Light-Fidelity (Li-Fi)
- ☐ Near Field Communication (NFC)
- ☐ QR Codes and Barcodes
- ☐ Radio Frequency Identification (RFID)
- ☐ Thread
- ☐ Wi-fi
- ☐ Wi-Fi Direct
- ☐ Z-wave
- ☐ ZigBee
- ☐ ANT

Medium-range Wireless Communication

- ☐ Ha-Low
- ☐ LTE-Advanced
- ☐ 6LoWPAN
- ☐ QUIC



Long-range Wireless Communication

- ☐ Low-power Wide-area Networking (LPWAN)
 - ☐ LoRaWAN
 - ☐ Sigfox
 - ☐ Neul
- ☐ Very Small Aperture Terminal (VSAT)
- ☐ Cellular
- ☐ MQTT
- ☐ NB-IoT

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Technologies and Protocols (Cont'd)

Wired Communication

- ☐ Ethernet
- ☐ Multimedia over Coax Alliance (MoCA)
- ☐ Power-line Communication (PLC)

IoT Operating Systems

- | | |
|--|---|
| <input type="checkbox"/> Windows 10 IoT | <input type="checkbox"/> ARM mbed OS |
| <input type="checkbox"/> Amazon FreeRTOS | <input type="checkbox"/> Zephyr |
| <input type="checkbox"/> Contiki | <input type="checkbox"/> Nucleus RTOS |
| <input type="checkbox"/> Fuchsia | <input type="checkbox"/> NuttX RTOS |
| <input type="checkbox"/> RIOT | <input type="checkbox"/> Integrity RTOS |
| <input type="checkbox"/> Ubuntu Core | |

IoT Application Protocols

- ☐ CoAP
- ☐ Edge
- ☐ LWM2M
- ☐ Physical Web
- ☐ XMPP
- ☐ Mithini/M3DA



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Technologies and Protocols

The IoT includes a wide range of new technologies and skills. The challenge in the IoT space is the immaturity of technologies with associated services, and that of the vendors providing them. This poses a key challenge for the organizations exploiting the IoT. For successful communication between two endpoints, IoT primarily implements standard and networking protocols.

The major communication technologies and protocols with respect to the range between a source and the destination are as follows:

Short-Range Wireless Communication

- **Bluetooth Low Energy (BLE):** BLE or Bluetooth Smart is a wireless personal area network. This technology is designed to be applied in various sectors such as healthcare, security, entertainment, and fitness.
- **Light-Fidelity (Li-Fi):** Li-Fi is like Wi-Fi with only two differences: the mode of communication and the speed. Li-Fi is a Visible Light Communications (VLC) system that uses common household light bulbs for data transfer at a very high speed of 224 Gbps.
- **Near-Field Communication (NFC):** NFC is a type of short-range communication that uses magnetic field induction to enable communication between two electronic devices. It is primarily used in contactless mobile payment, social networking, and the identification of documents or other products.
- **QR Codes and Barcodes:** These codes are machine-readable tags that contain information about the product or item to which they are attached. A quick response code, or QR code, is a two-dimensional code that stores product information and can be scanned using smartphones, whereas a barcode comes in both one-dimensional (1D) and two-dimensional (2D) forms of code.
- **Radio-Frequency Identification (RFID):** RFID stores data in tags that are read using electromagnetic fields. RFID is used in many sectors including industrial, offices, companies, automobiles, pharmaceuticals, livestock, and pets.
- **Thread:** A thread is an IPv6-based networking protocol for IoT devices. Its main purpose is home automation so that the devices can communicate with each other on local wireless networks.
- **Wi-Fi:** Wi-Fi is a technology that is widely used in wireless local area networking (LAN). At present, the most common Wi-Fi standard that is used in homes or companies is 802.11n, which offers a maximum speed of 600 Mbps and a range of approximately 50 m.
- **Wi-Fi Direct:** This is used for peer-to-peer communication without the need for a wireless access point. Wi-Fi direct devices start communication only after deciding which device will act as an access point.
- **Z-Wave:** Z-Wave is a low-power, short-range communication designed primarily for home automation. It provides a simple and reliable way to wirelessly monitor and control household devices like HVAC, thermostats, garages, home cinemas, etc.
- **Zig-Bee:** This is another short-range communication protocol based on the IEEE 203.15.4 standard. Zig-Bee is used in devices that transfer data infrequently at a low rate in a restricted area and within a range of 10–100 m.

- **ANT:** Adaptive Network Topology (ANT) is a multicast wireless sensor network technology mainly used for short-range communication between devices related to sports and fitness sensors.

Medium-Range Wireless Communication

- **HaLow:** This is another variant of the Wi-Fi standard; it provides an extended range, making it useful for communications in rural areas. It offers low data rates, thus reducing the power and cost of transmission.
- **LTE-Advanced:** LTE-Advanced is a standard for mobile communication that provides enhancement to LTE, focusing on providing higher capacity in terms of data rate, extended range, efficiency, and performance.
- **6LoWPAN:** IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) is an Internet protocol used for communication between smaller and low-power devices with limited processing capacity, such as various IoT devices.
- **QUIC:** Quick UDP Internet Connections (QUICs) are multiplexed connections between IoT devices over the User Datagram Protocol (UDP); they provide security equivalent to SSL/TLS.

Long-Range Wireless Communication

- **LPWAN:** Low Power Wide Area Networking (LPWAN) is a wireless telecommunication network, designed to provide long-range communications between two endpoints. Available LPWAN protocols and technologies include the following:
 - **LoRaWAN:** A Long Range Wide Area Network (LoRaWAN) is used to support applications such as mobile, industrial machine-to-machine, and secure two-way communications for IoT devices, smart cities, and healthcare applications.
 - **Sigfox:** This is used in devices that have short battery life and need to transfer a limited amount of data.
 - **Neul:** This is used in a tiny part of the TV white space spectrum to deliver high-quality, high-power, high-coverage, and low-cost networks.
- **Very Small Aperture Terminal (VSAT):** VSAT is a communication protocol that is used for data transfer using small dish antennas for both broadband and narrowband data.
- **Cellular:** Cellular is a type of communication protocol that is used for communication over a longer distance. It is used to send high-quality data but with the drawbacks of being expensive and having high power consumption.
- **MQTT:** Message Queuing Telemetry Transport (MQTT) is an ISO standard lightweight protocol used to transmit messages for long-range wireless communication. It helps in establishing connections to remote locations, for example via satellite links.
- **NB-IoT:** Narrowband IoT (NB-IoT) is a variant of LoRaWAN and Sigfox that uses more enhanced physical layer technology and the spectrum used for machine-to-machine communication.

Wired Communication

- **Ethernet:** Ethernet is the most commonly used type of network protocol today. It is a type of LAN (Local Area Network) that consists of a wired connection between computers in a small building, office, or campus.
- **Multimedia over Coax Alliance (MoCA):** MoCA is a type of network protocol that provides high-definition videos and related content to homes over existing coaxial cables.
- **Power-Line Communication (PLC):** This is a type of protocol that uses electrical wires to transmit power and data from one endpoint to another. PLC is required for applications in different areas such as home automation, industrial devices, and broadband over power lines (BPL).

IoT Operating Systems

IoT devices consist of both hardware and software components. Hardware components include end devices and gateways, whereas software components include operating systems. Due to an increase in the production of hardware components (gateways, sensor nodes, etc.), traditional IoT devices that previously used to run without an OS started adopting new OS implementations specifically programmed for IoT devices. These operating systems provide the devices with connectivity, usability, and interoperability.

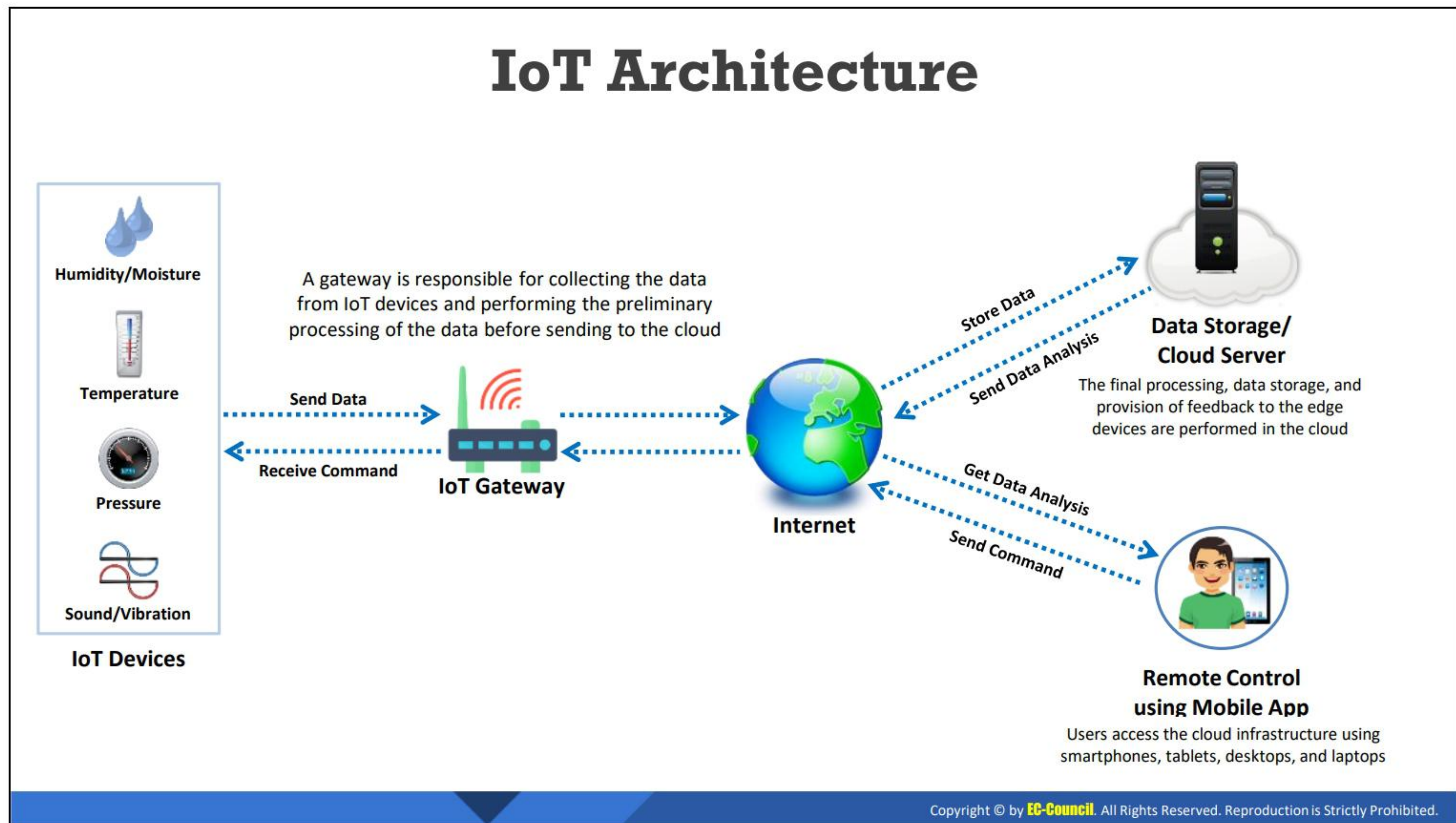
Given below are some of the operating systems used by IoT devices:

- **Windows 10 IoT:** This is a family of operating systems developed by Microsoft for embedded systems.
- **Amazon FreeRTOS:** This is a free open-source OS used in IoT microcontrollers that makes low-power, battery-operated edge devices easy to deploy, secure, connect, and manage.
- **Contiki:** This is used in low-power wireless devices such as street lighting, sound monitoring systems, etc.
- **Fuchsia:** This is an open-source OS developed by Google for various platforms, such as embedded systems, smartphones, tablets, etc.
- **RIOT:** This has fewer resource requirements and uses energy efficiently. It has the ability to run on embedded systems, actuator boards, sensors, etc.
- **Ubuntu Core:** Also known as Snappy, this is used in robots, drones, edge gateways, etc.
- **ARM mbed OS:** This is mostly used for low-powered devices such as wearable devices.
- **Zephyr:** This is used in low-power and resource-constrained devices.
- **Nucleus RTOS:** Primarily used in aerospace, medical, and industrial applications.
- **NuttX RTOS:** This is an open-source OS primarily developed to support 8-bit and 32-bit microcontrollers of embedded systems.

- **Integrity RTOS:** Primarily used in the aerospace or defense, industrial, automotive, and medical sectors.
- **Brillo:** This is an Android-based embedded OS used in low-end devices such as thermostats.
- **Apache Mynewt:** This supports devices that work on the BLE protocol.

IoT Application Protocols

- **CoAP:** Constrained Application Protocol (CoAP) is a web transfer protocol used to transfer messages between constrained nodes and IoT networks. This protocol is mainly used for machine-to-machine (M2M) applications such as building automation and smart energy.
- **Edge:** Edge computing helps the IoT environment to move computational processing to the edge of the network, allowing smart devices and gateways to perform tasks and services from the cloud end. Moving computational services to the edge of the network improves content caching, delivery, storage, and management of the IoT.
- **LWM2M:** Lightweight Machine-to-Machine (LWM2M) is an application-layer communication protocol used for application-level communication between IoT devices; it is used for IoT device management.
- **Physical Web:** Physical Web is a technology used to enable faster and seamless interaction with nearby IoT devices. It reveals the list of URLs being broadcast by nearby devices with BLE beacons.
- **XMPP:** eXtensible Messaging and Presence Protocol (XMPP) is an open technology for real-time communication used for IoT devices. This technology is used for developing interoperable devices, applications, and services for the IoT environment.
- **Mihini/M3DA:** Mihini/M3DA is a software used for communication between an M2M server and applications running on an embedded gateway. It allows IoT applications to exchange data and commands with an M2M server.



IoT Architecture

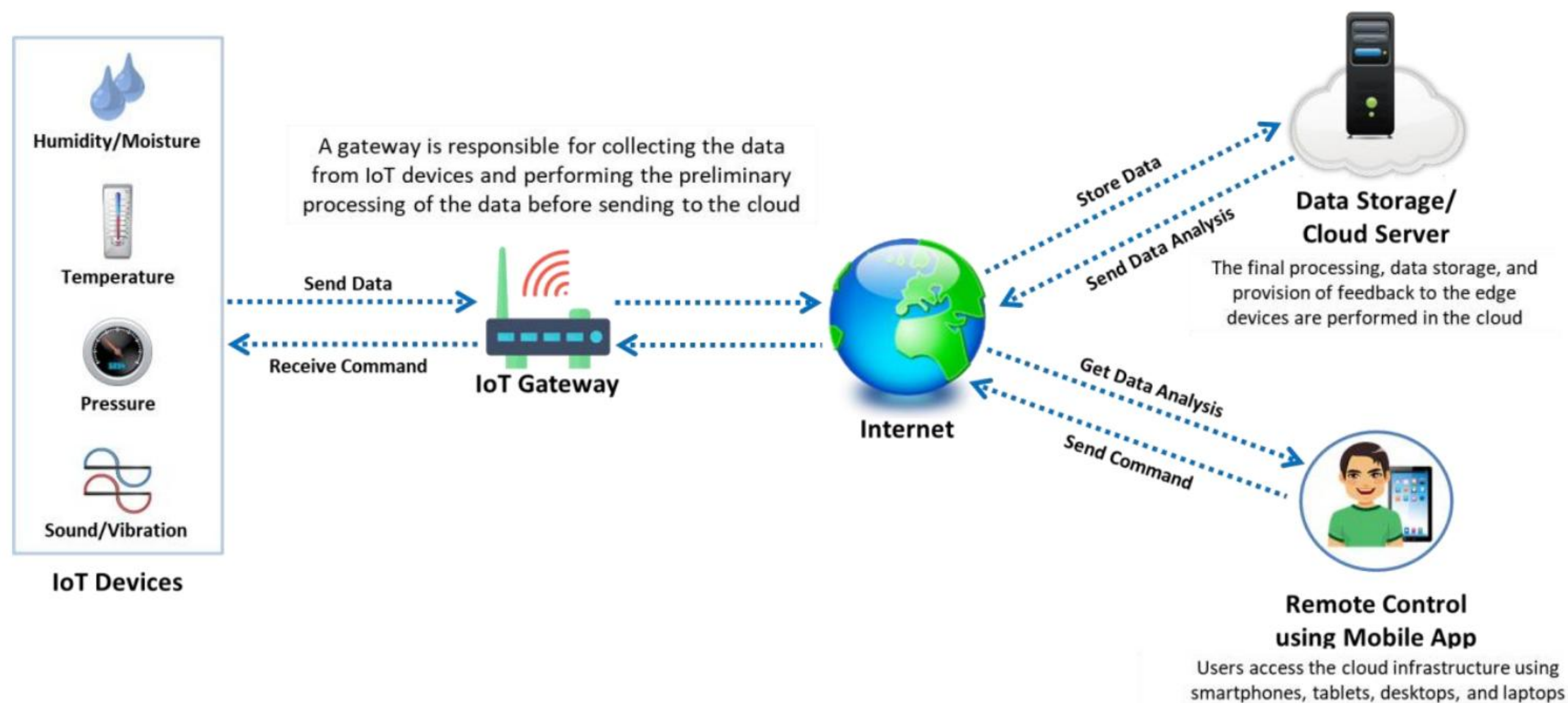


Figure 13.2: IoT Architecture

The IoT architecture includes several layers. These layers are designed in such a manner that they can meet the requirements of various sectors such as societies, industries, enterprises, and governments. The layers of the IoT architecture are connected to gather, save, and process data. The functions performed by various building blocks are as follows.

- **Gateways** are devices through which data are transmitted from things to the cloud and vice versa. They provide the following functions:
 - Pre-processing and filtering of data before transmitting them to the cloud, enabling lesser data volumes for detailed processing and storing

- Sending control commands from the cloud to things to let the things execute the commands using their actuators
- **Cloud gateways** have the following features:
 - Data compression
 - Securing data transfer between field gateways and cloud IoT servers
 - Ensuring compatibility with different protocols
 - Communicating with field gateways through various protocols based on the protocol supported by gateways
- **Streaming data processors** ensure that no data can be lost or corrupted by providing the following features:
 - Effective input data transition to a data lake
 - Application control
- **Data lakes** store the data produced by the connected devices in the natural format. If the data are required for meaningful insights, the data will be extracted from a data lake and loaded to a big data warehouse.
- **Big data warehouses** contain only cleaned, structured, and matched data. They can store the following:
 - Context information about the things and devices; examples include the locations of sensors
 - Commands sent by control applications to things
- **Data analytics** help data analysts find trends and obtain actionable insights by using the data in the big data warehouse. The analysis of the data in the form of schemas, diagrams, and infographics reveals the following:
 - Device performance
 - Inefficiencies of the IoT system and ways to enhance it

Moreover, manually found correlations and patterns further help create algorithms for control applications.

- **Machine learning** allows data analysts to create models for control applications. These models are updated regularly depending on the data in a big data warehouse. Examples include models for recognizing the patterns of an organization's employee behavior in terms of when they leave and return to the organization and adjusting the lights in the premises accordingly. After completing the phase of testing the applicability and efficiency of these models, they start to be used by control applications.
- **Control applications** send automatic commands and alerts to actuators. For example, if a pre-failure situation arises in an organization's equipment/devices, the sensors

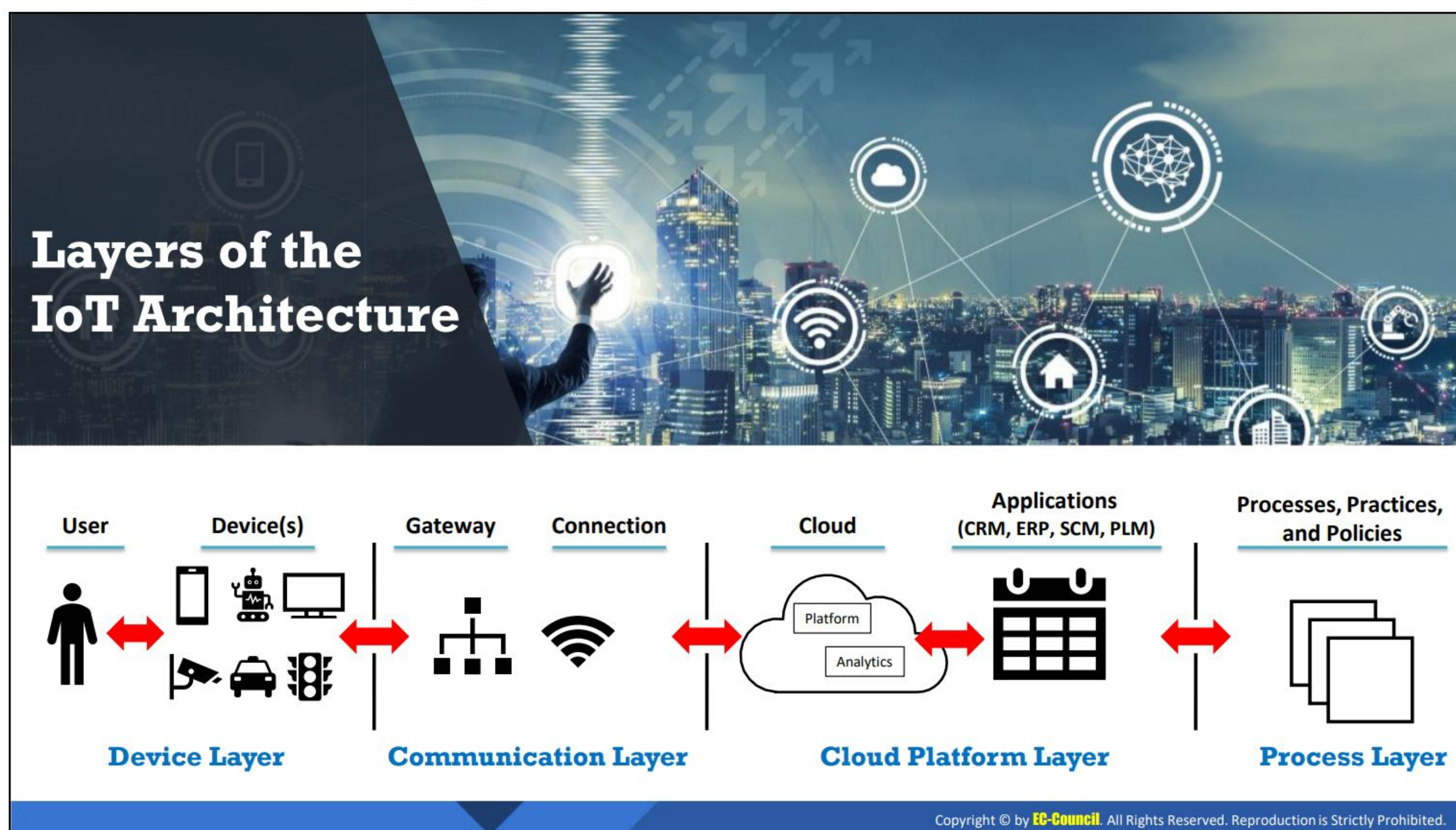
monitor the state of the devices, and the IoT system sends automatic notifications to system engineers.

The stored commands in a big data warehouse sent by control applications to actuators help in the following:

- Investigating problematic cases; for example, checking the connectivity, gateways, and actuators if the actuators fail to execute the commands sent by a control application
- Enhancing security by identifying security breaches (possible when detecting unusual or huge amounts of commands)

The control applications can be of the following two types:

- Rule-based control applications that operate based on the rules set by specialists
 - Machine-learning-based control applications that use models, which can be updated regularly with the data stored in a big data warehouse
- **User applications (web or mobile applications)** help change the behavior of the application controls. For example, if an IoT system performs certain actions poorly, user applications allow users to do the following:
- Connect to an IoT system
 - Monitor and control (by sending commands to control applications and setting options for automatic behavior) smart things while they are connected to a network of similar things.



Layers of the IoT Architecture

An IoT ecosystem is a combination of multiple IoT layers and comprises the components that allow organizations to connect to their IoT devices. Specifically, an ecosystem includes dashboards, remotes, gateways, analytics, networks, data storage, and security. The general architecture of an IoT ecosystem is different for different organizations. The ecosystem model that many organizations refer to when attempting to understand the IoT architecture includes the IoT layers.

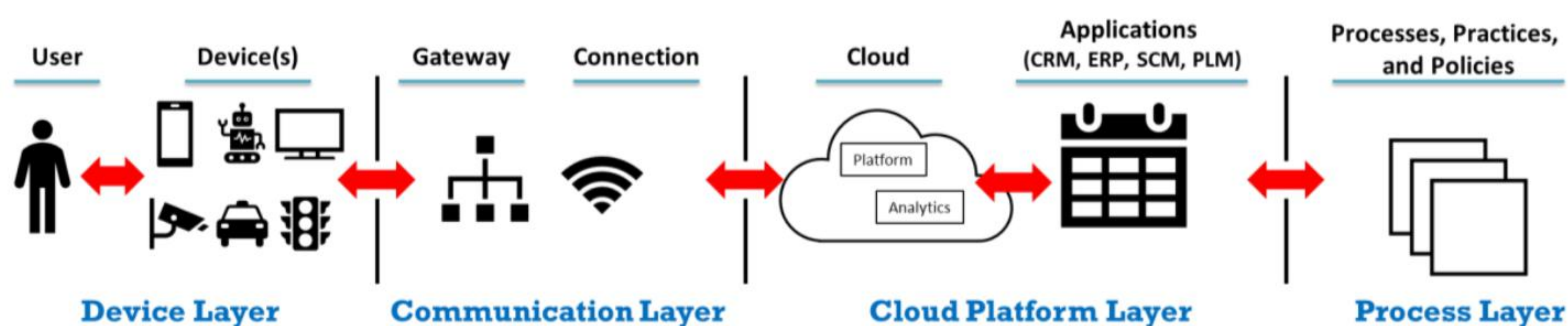


Figure 13.3: Layers of IoT Architecture

Layer 1: Device Layer

The device or thing layer of IoT includes the hardware that constitutes IoT devices. All the connected devices are the endpoint for an IoT ecosystem, and they acquire data based on a particular use case. The devices include the following:

- Sensors (temperature, gyroscope, pressure, light sensors, Global Positioning System (GPS), electrochemical, radio-frequency identification (RFID), etc.)
- Mobile devices (smartphones/tablets)
- Microcontroller units

- Networking gear
- Single-board computers

Layer 2: Communication Layer

The communication (connectivity/edge computing) layer includes the components of communication protocols and networks used for connectivity and edge computing. A use case is successfully executed with seamless connectivity between IoT devices.

- **Protocols:** For Internet-based IoT applications, a Transmission Control Protocol (TCP)/Internet Protocol (IP)-based architecture is used. Intranet-based IoT use cases utilize LAN, RF, Wi-Fi, Li-Fi, etc.
- **Gateway:** Gateways help manage traffic between IoT devices and connected networks. To maintain and monitor the traffic, the level-5 gateways are helpful.

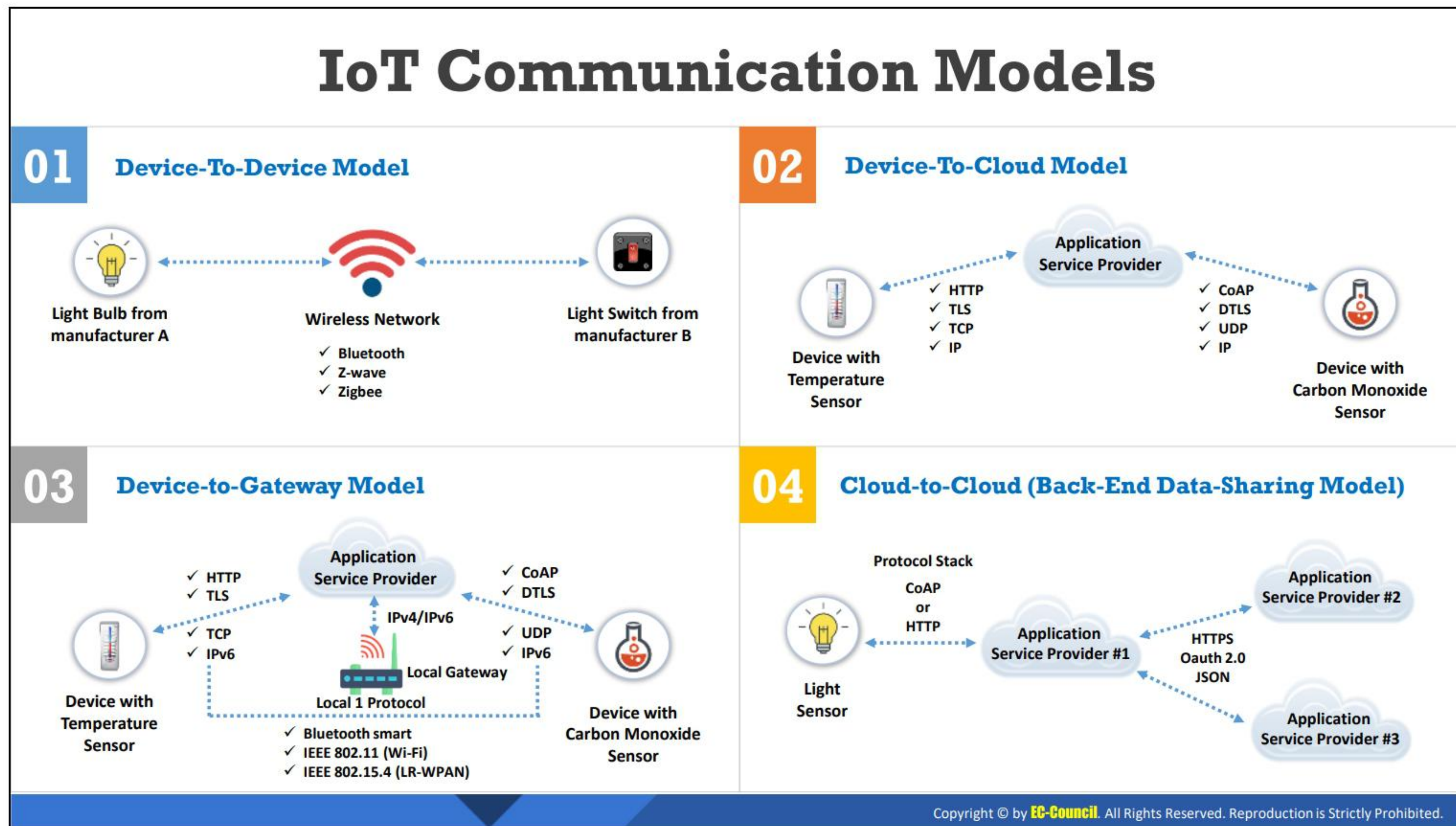
Layer 3: Cloud Layer

Servers hosted in the cloud accept, store, and process the sensor data received from IoT gateways. Many IoT solutions are integrated with cloud services. With a comprehensive set of integrated services and solutions, IoT cloud provides the required insights and perspectives for customers. It provides dashboards for monitoring, analyzing, and implementing proactive decisions.

Layer 4: Process Layer

The process layer gathers information and processes the received information. It includes the following:

- People
- Businesses
- Collaborations
- Decision making based on the information derived from policies and procedures of IoT computing



IoT Communication Models

IoT technology uses various technical communication models, each with its own characteristics. These models highlight the flexibility with which IoT devices can communicate with each other or with the client. Discussed below are four communication models and the key characteristics associated with each model:

■ Device-to-Device Communication Model

In this type of communication, inter-connected devices interact with each other through the Internet, but they predominantly use protocols such as ZigBee, Z-Wave or Bluetooth. Device-to-device communication is most commonly used in smart home devices such as thermostats, light bulbs, door locks, CCTV cameras, and fridges, which transfer small data packets to each other at a low data rate. This model is also popular in communication between wearable devices. For example, an ECG/EKG device attached to the body of a patient will be paired to his/her smartphone and will send him/her notifications during an emergency.



Figure 13.4: IoT device-to-device communication model

▪ Device-to-Cloud Communication Model

In this type of communication, devices communicate with the cloud directly, rather than directly communicating with the client to send or receive data or commands. It uses communication protocols such as Wi-Fi or Ethernet, and sometimes uses Cellular as well.

An example of Wi-Fi-based device-to-cloud communication is a CCTV camera that can be accessed on a smartphone from a remote location. In this scenario, the device (here, the CCTV camera) cannot directly communicate with the client; rather, it first sends data to the cloud, and then, if the client inputs the correct credentials, he/she is then allowed to access the cloud, which in turn allows him/her to access the device at his/her home.

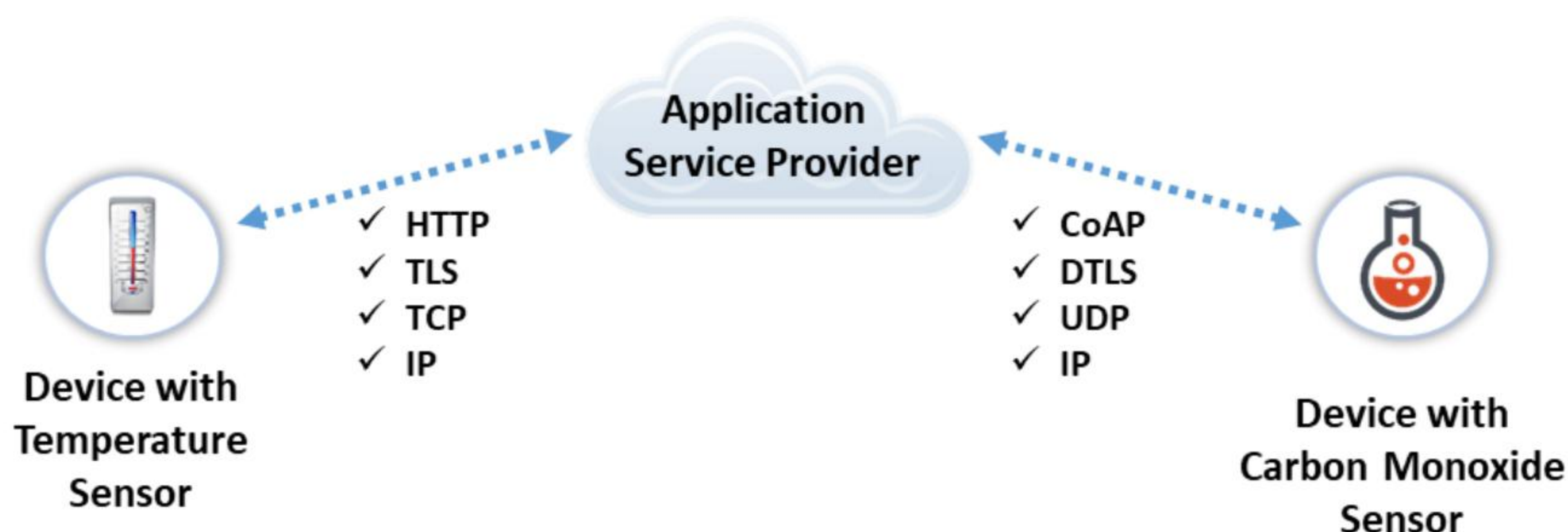


Figure 13.5: IoT device-to-cloud communication model

▪ Device-to-Gateway Communication Model

In the device-to-gateway communication model, the IoT device communicates with an intermediate device called a gateway, which in turn communicates with the cloud service. This gateway device could be a smartphone or a hub that is acting as an intermediate point, which also provides security features and data or protocol translation. The protocols generally used in this mode of communication are ZigBee and Z-Wave.

If the application layer gateway is a smartphone, then it might take the form of an app that interacts with the IoT device and with the cloud. This device might be a smart TV that connects to the cloud service through a mobile phone app.

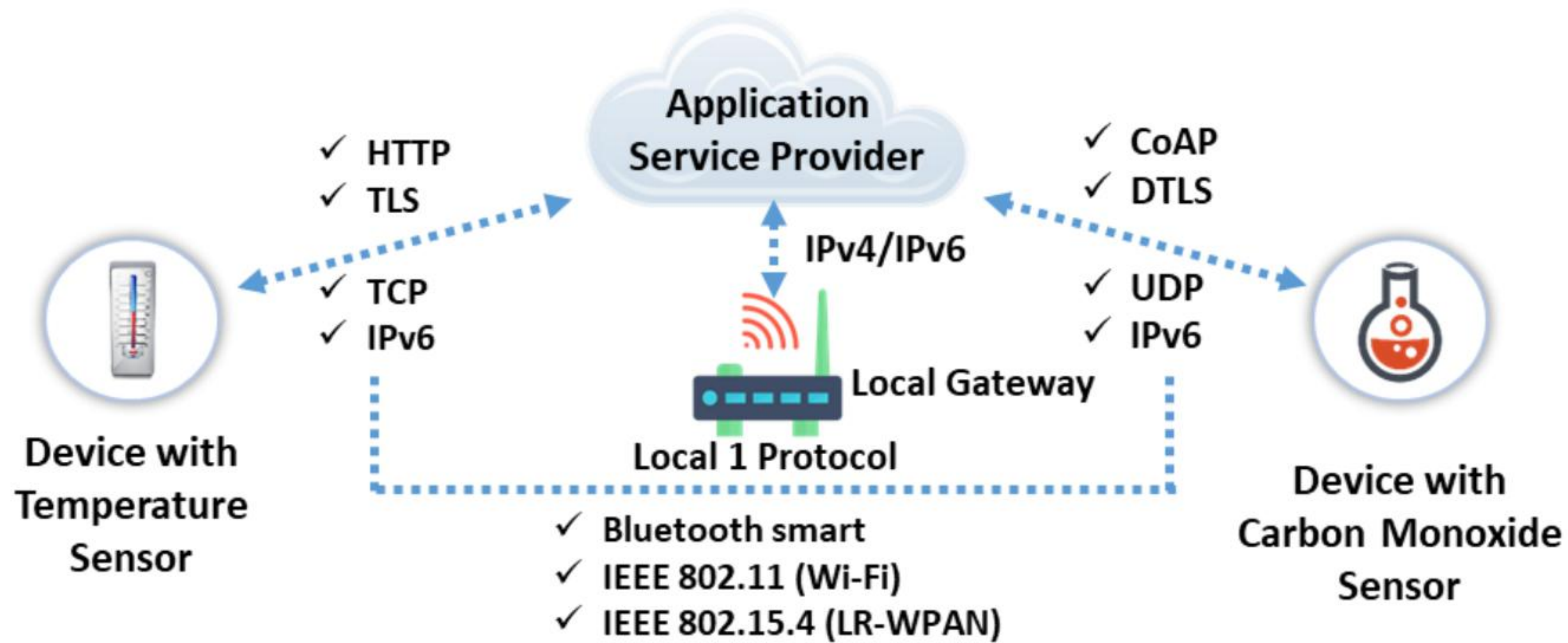


Figure 13.6: IoT device-to-gateway communication model

▪ Cloud-to-Cloud (Back-End Data-Sharing) Communication Model

This type of communication model extends the device-to-cloud communication type such that the data from the IoT devices can be accessed by authorized third parties. Here, devices upload their data onto the cloud, which is later accessed or analyzed by third parties. An example of this model would be an analyzer of the yearly or monthly energy consumption of a company. Later, the analysis can be used to reduce the company's expenditure on energy by following certain energy-harvesting or saving techniques.

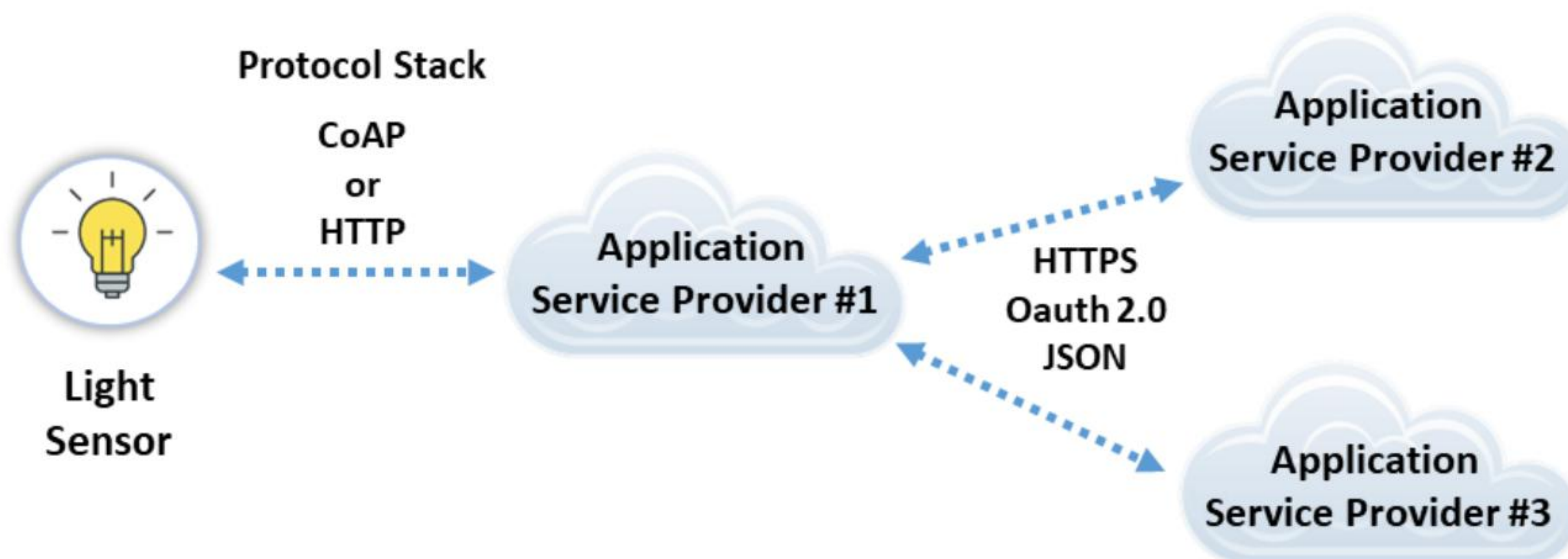
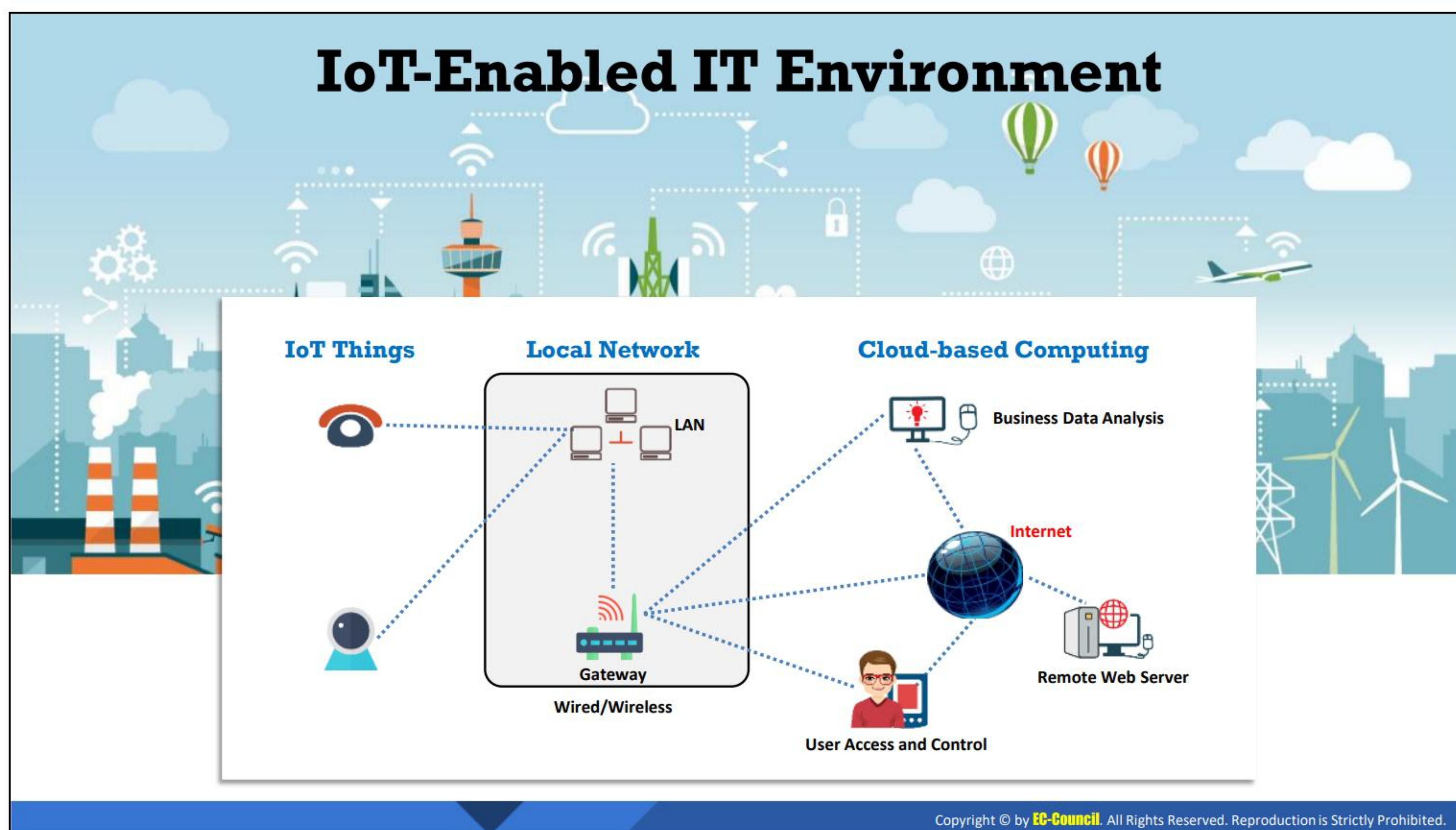







Figure 13.7: IoT back-end data-sharing model



IoT-Enabled IT Environment (Cont'd)

Features of an IoT-Enabled IT Environment

-  **Real-time monitoring** involves monitoring IoT assets, processing products, maintaining a flow, helping detect issues, and taking actions immediately
-  **Real-time analytics** involves analyzing IoT things and taking steps accordingly
-  **Multi-layer security** involves preventing unauthorized access to IoT things by using multi-factor authentication (MFA), Transport Layer Security (TLS), device identity management, etc.
-  **Data collection** involves the exchange of data between IoT-enabled organizations using different communication protocols
-  **Communication** among multiple devices involves configuring multiple devices to access IoT things even remotely at any time and from anywhere



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT-Enabled IT Environment

A typical IoT-enabled IT environment comprises devices/things that use a gateway for communicating over a network to access an organization's back-end servers running an IoT cloud platform. This IoT platform allows integrating the IoT information into the organization. The different tiers of an IoT-enabled IT environment are discussed below.

- **Things/Devices Tier**

The things/devices tier include smartphones, wearable devices, autonomous machines, and tags (RFID, NFC, QR codes) that can gather data using their embedded sensors, which can track key parameters related to the physical environment. Some examples for these parameters are air quality, humidity, light, and pressure. To transfer these telemetry data/command and control requests from IoT devices through a gateway to the cloud, protocols based on wired and wireless networking standards are used. Moreover, the command and control data are transferred from the cloud through the gateway to the devices. These devices can control the state of another device. For example, they can switch off faulty devices or raise an alarm about them. Thus, these IoT devices allow remote control.

- **Gateway/Control Tier**

The gateway/control tier focuses on communication, offload processing functions, and the driving of required actions. The gateway pre-processes the huge amount of data generated by sensors before sending it to the cloud tier; thus, it reduces the amount of unwanted data forwarded to the cloud tier. This process can reduce the costs of network transmission and allow the application of rules based on incoming data. The gateway can issue control information such as configuration changes to the devices while responding to the data tier's command and control requests such as authentication requests (bidirectional functioning). Moreover, the gateway acts as a proxy/edge device to legacy and low-power devices that cannot directly register and communicate with the IoT platform. In particular, the gateway can route commands received from the back-end to the respective device. All the new IoT devices, legacy devices, and edge devices form the IoT device layer.

A typical control tier facilitates efficient communication through a personal area network (PAN), a local area network (LAN), Bluetooth, Zigbee, Message Queuing Telemetry Transport (MQTT)/TCP, etc., and micro-computing (micro-multi core chips).

- **Communication/Data Center/Cloud IoT Platform/Cloud Tier**

The communication/data center/cloud IoT platform/cloud tier focuses on data computation to deliver insights and thereby generate business value. It acts as middleware by orchestrating the entire IoT workflow. It provides back-end business analytics to run event processes such as data analysis for creating and adapting business rules based on historical trends and then spreads business rules downstream. It needs to scale horizontally (for supporting an increasing number of IoT devices) and vertically (for addressing different IoT solutions). The cloud tier's key functions include the following:

- Event processing and analysis
- Data storage
- Message and connectivity routing
- Application integration and enablement

A typical cloud tier comprises software as a service (SaaS), business data analysis, user access controls, remote web servers, etc., and open/small operating systems (OSes) such as Linux.

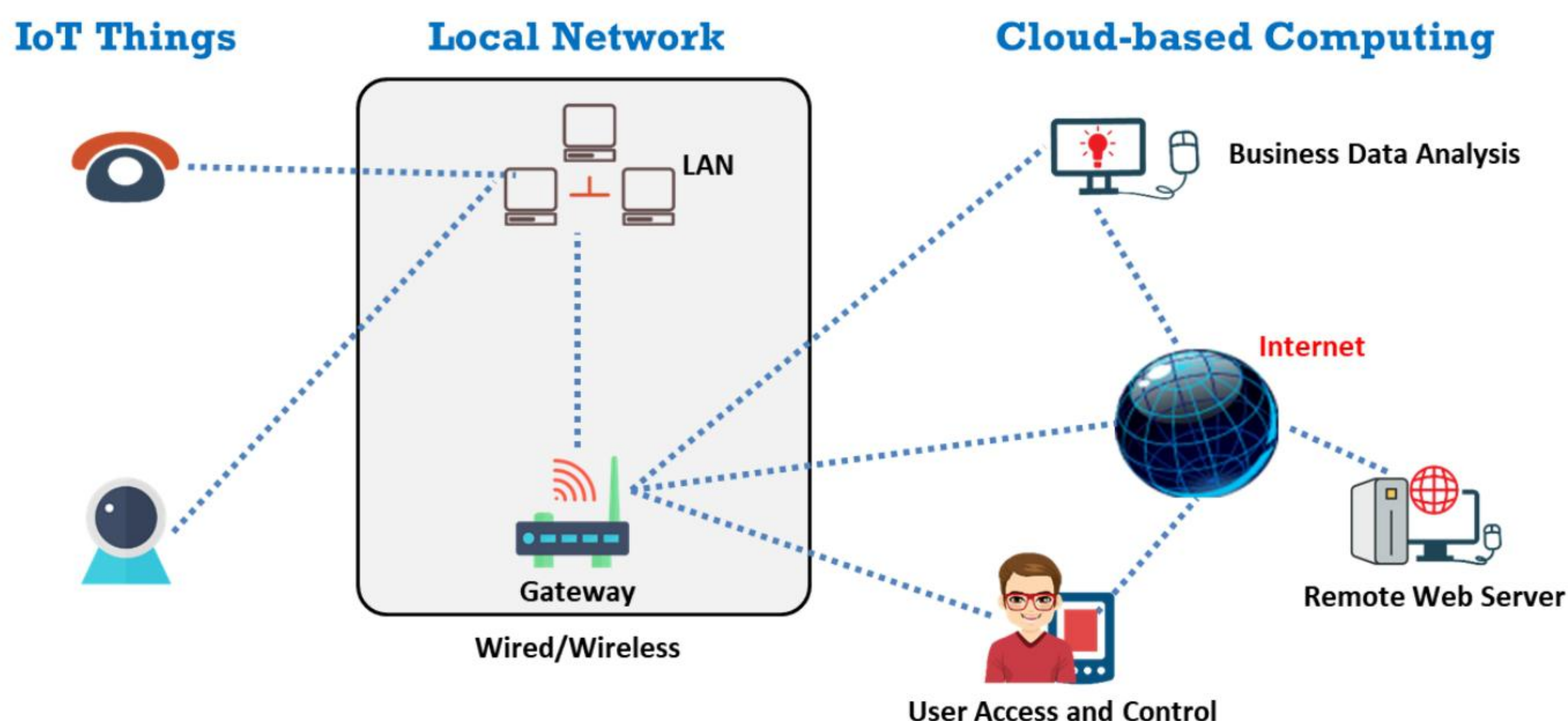


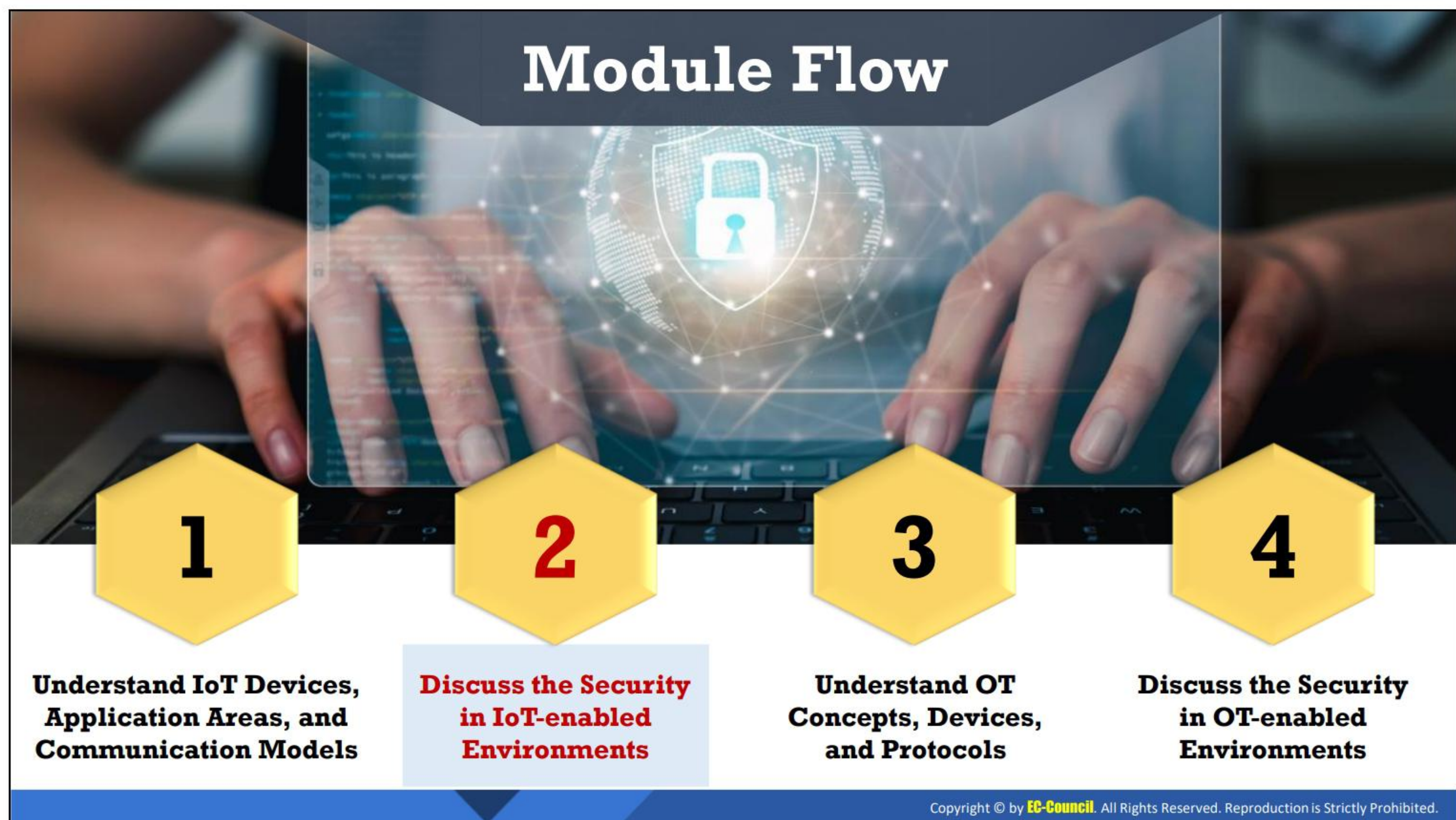
Figure 13.8: Schematic of an IoT-enabled environment

In the figure, the IoT things/devices layer communicates with a cloud gateway. Here, the gateway authenticates and authorizes the devices to participate in the workflow and thereby ensures secure communication between the devices and the centralized command center. Furthermore, the gateway can deal with different protocols and data formats. The devices and local gateways with different protocols (SOAP, REST, AMQP, etc.) register with the cloud gateway. Here, without considering the inbound protocol, the cloud gateway can provide a view of the device layer to the remaining IoT components.

Features of an IoT-Enabled IT Environment

The following features of IoT platforms help an IT environment reach its targets quickly:


- Real-time monitoring involves monitoring IoT assets, processing products, maintaining a flow, helping detect issues, and taking actions immediately.
- Real-time analytics involves analyzing IoT things and taking steps accordingly. For example, it provides graphs and real-time streaming analytics, allowing the business to overview its performance and production.
- Multi-layer security involves preventing unauthorized access to IoT things by using multi-factor authentication (MFA), Transport Layer Security (TLS), device identity management, etc.
- Data collection involves the exchange of data between IoT-enabled organizations using different communication protocols. These protocols should be lightweight and should provide low-network-bandwidth functionality.
- Communication among multiple devices involves configuring multiple devices to access IoT things even remotely at any time and from anywhere.







Discuss the Security in IoT-enabled Environments

The objective of this section is to explain the security principles in IoT-enabled environments.

Security in IoT-enabled Environments



-  With no or inadequate focus on IoT device security by manufacturers, security measures used to **harden** the IoT device are often insufficient
-  Therefore, organizations should focus on countering attack scenarios in IoT-enabled environments. Organizations should focus on securing network devices and routers in an IoT-enabled environment. This helps restrict the attacker from accessing other parts of the network and performing targeted attacks
-  The organization should use **multilayered** management. An overarching multilayered security plan and constant maintenance are necessary to effectively secure all these disparate IoT devices
-  Company-wide **collaboration** and **synchronization** are required to secure an IoT-enabled environment

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Security in IoT-enabled Environments

Because IoT devices are vastly different from each other, the security of devices relies on their type and model. With no or inadequate focus on IoT device security by manufacturers, security measures used for IoT devices often fall short. Therefore, an organization should focus on securing IoT devices and countering attack scenarios in IoT-enabled environments.

An organization can secure IoT devices by changing the default passwords, disabling unused features, updating firmware and applications, and using a legitimate application developed by a reliable vendor in the case of IoT devices that rely on third-party applications.




An adversary uses a compromised IoT device as an entry point to a network and performs a lateral movement attack. For example, a compromised smart printer can infect other systems and devices connected to the same network. A compromised router can spread malware to all the IoT devices connected to it. Therefore, organizations should focus on securing network devices and routers in an IoT-enabled environment.

To secure an IoT network and router, the user should map and monitor all the devices, apply network segmentation, ensure a secure network architecture, use routers with in-built firewalls, and disable unnecessary services such as Universal Plug and Play (UPnP). This helps in restricting the attacker from accessing other parts of the network and performing targeted attacks.

An organization should use multi-layered management. To secure all the different IoT devices, an overarching multi-layered security plan and constant maintenance are required. The organization should enforce security solutions that safeguard the IoT devices and detect malware at the endpoint level. It should also use security software that checks the network traffic between routers and connected devices to protect the IoT devices. Further, it should

utilize network appliances to monitor all the ports and network protocols for detecting advance threats and safeguard the IoT devices from targeted attacks. Company-wide collaboration and synchronization are required to secure an IoT-enabled environment.

IoT System Management

		
Device Management	User Management	Security Monitoring
<ul style="list-style-type: none">❑ Ensure secure data transmission to facilitate fine interaction between devices and to guarantee the proper functioning of devices in an IoT system	<ul style="list-style-type: none">❑ Provide control over the users who have access to an IoT system. User management includes identifying users, setting user roles and access levels, controlling access, etc.	<ul style="list-style-type: none">❑ To address security breaches at early stages and to prevent malicious attacks on an IoT system, perform the activities such as log and analyze commands sent by control applications to things, monitor and store all the actions of users, identify the patterns of malicious behavior, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT System Management

IoT system management involves the following.

- **Device management**

Ensure secure data transmission to facilitate fine interaction between devices and to guarantee the proper functioning of devices in an IoT system.

- **Identify the identity of devices** to ensure a trusted device with genuine software transmitting reliable data.
- **Configure devices and control them** as per the requirements of an IoT system. For example, provide IDs for devices.
- **Monitor and diagnose devices** to ensure the smooth and secure functioning of IoT devices.
- **Update software and maintain it** to add functionality, fix bugs, and address vulnerabilities.

- **User management**

Provide control over the users who have access to an IoT system. User management includes the following:

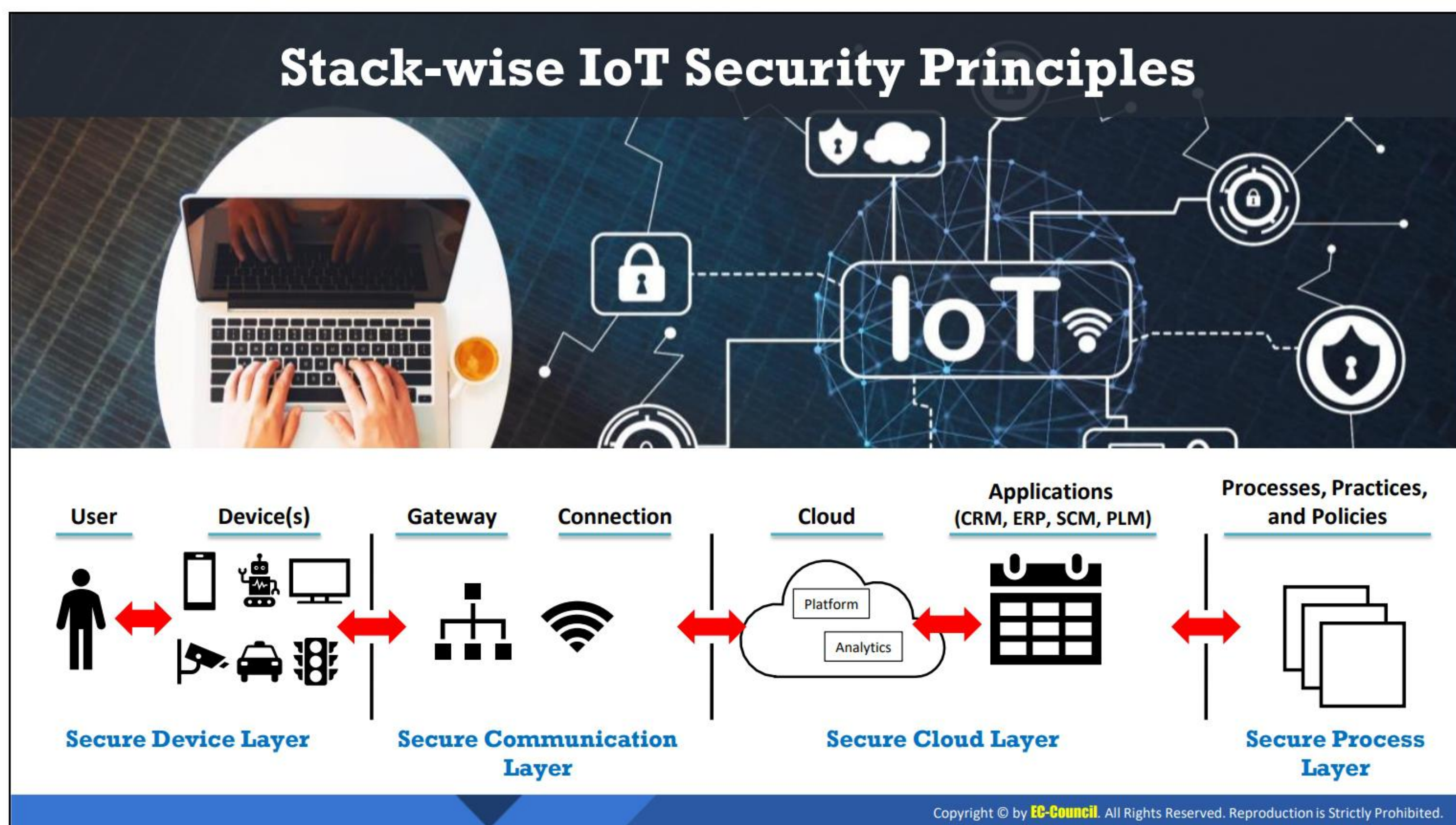
- Identify users.
- Set user roles (owners, guests, etc.).
- Set access levels for users.
- Control the access of a few users to specific information.

- Set user ownership.
- Add and remove users.
- Manage user settings.
- Allow permissions to perform certain operations within an IoT system (for example, controlling and recording user activities).

▪ **Security monitoring**

To address security breaches at early stages and to prevent malicious attacks on an IoT system, the following should be performed:

- Log and analyze commands sent by control applications to things.
- Monitor the actions of users.
- Store all actions in the cloud.
- Identify the patterns of malicious behavior.
- Store samples of malicious activity and compare them with the logs generated by the IoT system to avoid attacks and their impact.



Stack-wise IoT Security Principles

Several IoT devices are connected to the network and eventually to the cloud, which causes vulnerability to many threat vectors. To develop end-to-end (E2E) IoT solutions, the device, communication, cloud, and process layers should be secured. For this purpose, the following stack-wise IoT security principles should be implemented.

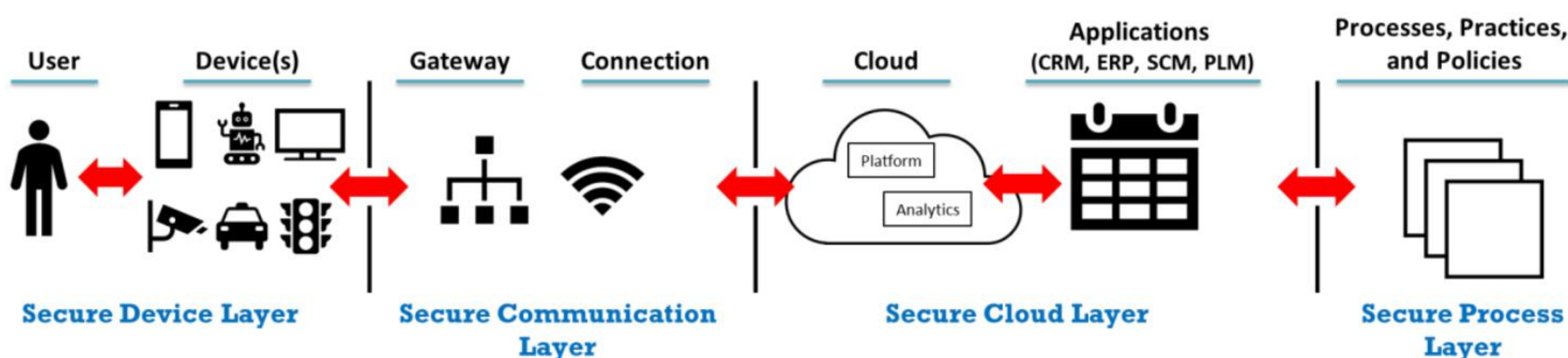


Figure 13.9: Stack-wise IoT security principles

IoT Security Principles on the Device Layer

- **Need for device intelligence to handle complex security tasks:** Most IoT devices communicate with services, the cloud, servers, etc., through the Internet or Wi-Fi. As these devices are powered by microprocessors, they are unable to handle the complexity of Internet connectivity and should not be utilized for front-line duty in IoT applications. Smart devices are secure and robust. They have embedded security features and can handle security, encryption, authentication, etc. Hence, smart devices should be used for front-line duty in IoT applications.
- **Security advantage of processing at the edge:** Smart IoT devices have an edge processing feature that processes data locally before sending the data to the cloud, thus

eliminating the need to forward a large quantity of data to the cloud. Edge processing enhances security by processing the data, packing the data into separate packets, and sending the data securely to the desired location. It allows users to keep sensitive information with them.

IoT Security Principles on the Communication Layer

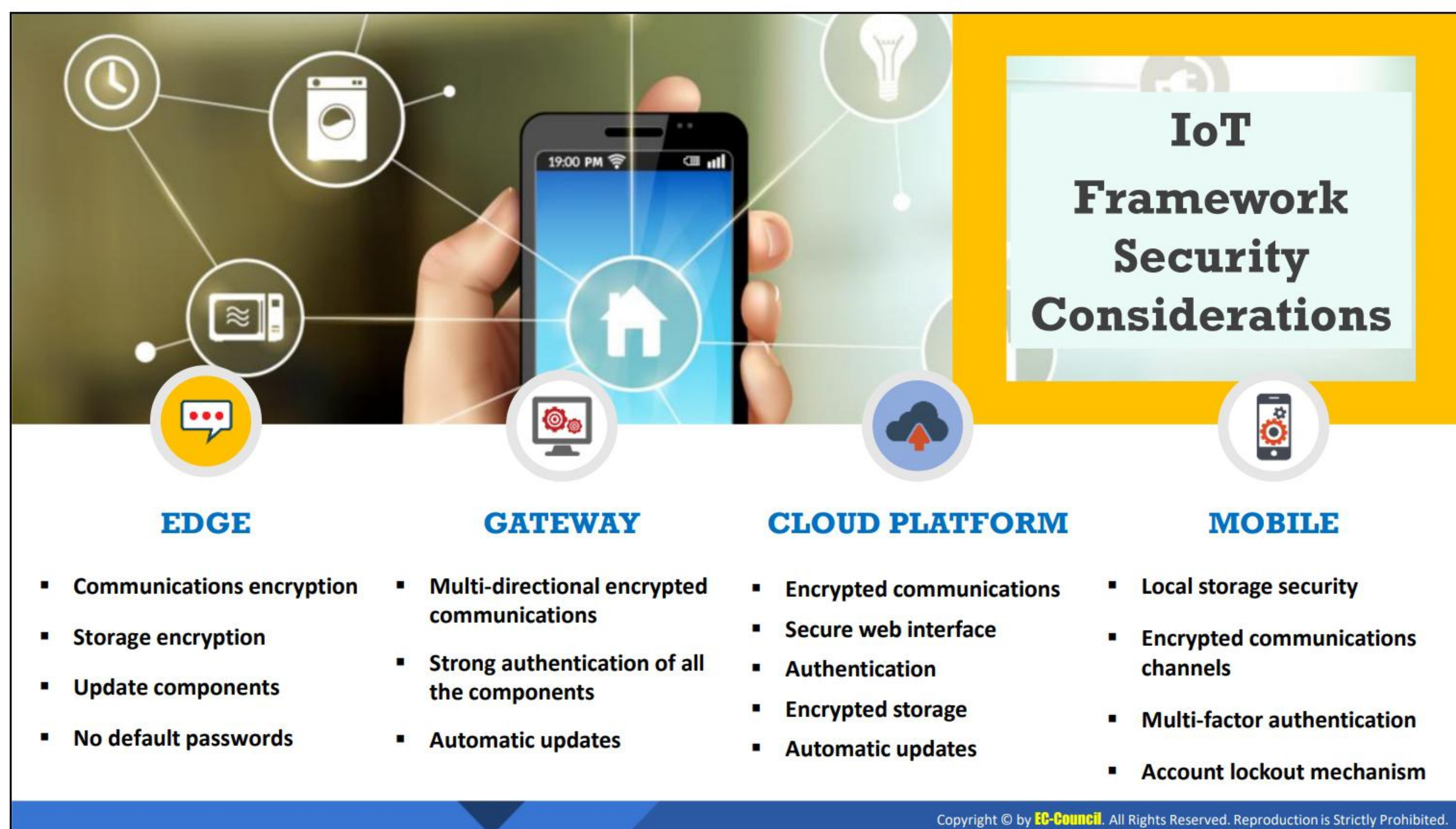
- **Initiate a connection to the cloud but not from the cloud:** Instead of connecting IoT devices with the Internet, they should be connected to the cloud. Incoming connections should be disallowed. Connection to the cloud establishes a bi-directional channel, through which the user can control the IoT device remotely.
- **Inherent security of a message:** All communications with IoT devices should be carefully handled. The user must enforce lightweight message-based protocols for IoT devices that consist of options for double encryption, filtering, queuing, etc. With proper labeling, the messages will be handled securely. For example, double encryption secures client data when the data pass through the message switch.

IoT Security Principle on the Cloud Layer

- **Identification, authentication, and encryption for machines, rather than humans:** Users access cloud services with a password. Occasionally, cloud services use two-factor authentication consisting of a password and a one-time password generator. For humans, passwords are the accepted method of authentication, but machines handle digital certificates while accessing cloud services. The system of digital certificates is used not only to authenticate transactions but also to encrypt the channel from the device to the cloud before the transaction. The cryptographic identification provided by the digital certificate cannot be achieved with a user ID and password.

IoT Security Principle on the Process Layer

- **Security of remote control and updates:** The remote control of an IoT device allows the user to perform remote diagnostics of the device, set new configurations, retrieve files, etc. The key to secure updates and remote control is to ensure that incoming connections to the device are disallowed; however, the device should establish a secure bi-directional connection with the cloud and utilize a message switch as a communication channel.



IoT Framework Security Considerations

To design secure and protected IoT devices, security issues should be properly considered. One of the most important considerations is the development of a secure IoT framework for building the device. Ideally, a framework should be designed in a way that provides default security, so that the developers do not have to consider it later.

Security evaluation criteria for the IoT framework are broken down into four parts. Each part has its own security-related concerns that are discussed in the evaluation criteria for each part. The security evaluation criteria for the IoT devices are discussed below:

▪ Edge

The edge is the main physical device in the IoT ecosystem that interacts with its surroundings and contains various components like sensors, actuators, operating systems, hardware and network, and communication capabilities. It is heterogeneous and can be deployed anywhere and in any condition. Therefore, an ideal framework for an edge would be such that it provides cross-platform components so that it can be deployed and work in any physical condition possible.

Other framework considerations for an edge would be proper communications and storage encryption, no default credentials, strong passwords, use of the latest up-to-date components, etc.

▪ Gateway

The gateway acts as the first step for an edge into the world of the Internet as it connects smart devices to cloud components. It is referred to as a communication aggregator that allows communication with a secure and trusted local network as well

as a secure connection with an untrusted public network. It also provides a layer of security to all the devices connected to it. The gateway serves as an aggregation point for the edge; therefore, it has a crucial security role in the ecosystem.

An ideal framework for the gateway should incorporate strong encryption techniques for secure communications between endpoints. In addition, the authentication mechanism for the edge components should be as strong as any other component in the framework. Wherever possible, the gateway should be designed in such a way that it authenticates multi-directionally to carry out trusted communication between the edge and the cloud. Automatic updates should also be provided to the device for countering vulnerabilities.

- **Cloud Platform**

In an IoT ecosystem, the cloud component is referred to as the central aggregation and data management point. Access to the cloud must be restricted. The cloud component is usually at higher risk, as it is the central point of data aggregation for most of the data in the ecosystem. It also includes a command and control (C2) component, which is a centralized computer that issues various commands for the distribution of extensions and updates.

A secure framework for the cloud component should include encrypted communications, strong authentication credentials, a secure web interface, encrypted storage, automatic updates, etc.

- **Mobile**

In an IoT ecosystem, the mobile interface plays an important part, particularly where the data needs to be collected and managed. Using mobile interfaces, users can access and interact with the edge in their home or workplace from miles away. Some mobile applications provide users with only limited data from specific edge devices, while others allow complete manipulation of the edge components. Proper attention should be given to the mobile interface, as they are prone to various cyber-attacks.

An ideal framework for the mobile interface should include a proper authentication mechanism for the user, an account lockout mechanism after a certain number of failed attempts, local storage security, encrypted communication channels, and security of data transmitted over the channel.

IoT Device Management

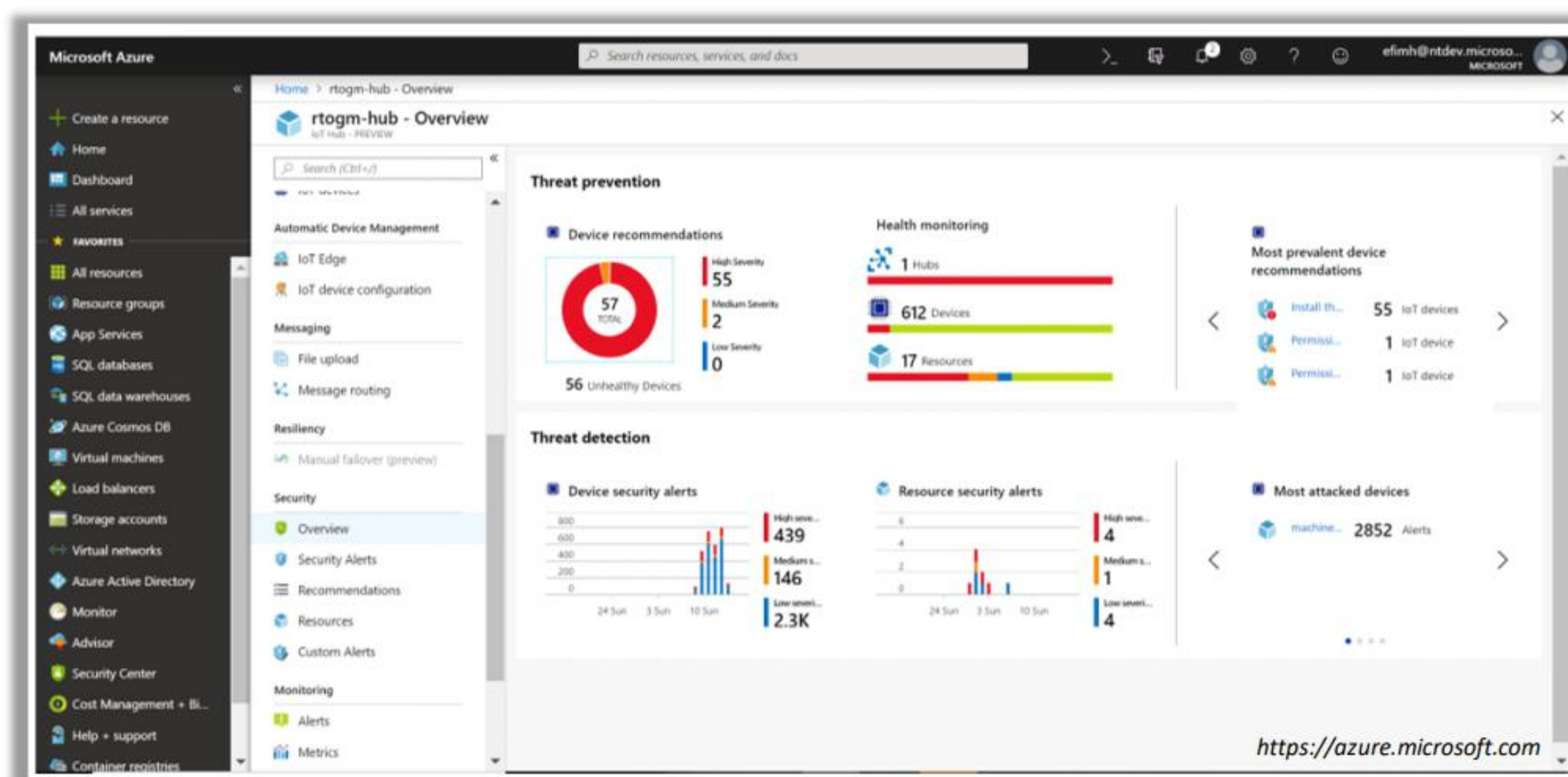
- ❑ IoT device management helps in supporting IoT solutions by using any software tools and processes and helps in **onboarding latest devices** securely and promptly



IoT Device Management Solutions

- Oracle IoT Asset Monitoring Cloud
<https://www.oracle.com>
- Predix
<https://www.ge.com>
- Cloud IoT Core
<https://cloud.google.com>
- IBM Watson IoT Platform
<https://www.ibm.com>
- AT&T IoT Connectivity Management
<https://www.business.att.com>

Azure IoT Central



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Device Management

IoT device management helps security professionals to track, monitor, and manage physical IoT devices from a remote location. Security professionals can use solutions such as Azure IoT Central, Oracle IoT Asset Monitoring Cloud, and Predix to perform IoT device management. These solutions allow security professionals to update the firmware remotely. Further, IoT device management helps in providing permissions and enhancing security capabilities to ensure protection against various vulnerabilities.

IoT device management can be very supportive in preventing IoT attacks as it can provide:

- Proper authentication, as only trusted and secure devices with proper credentials are enrolled
- Accurate configuration, controlling devices to ensure proper functionality and improved performance. It can also reset the factory settings during device decommissioning.
- Proper monitoring to detect flaws and diagnose operational issues and software bugs through program logs
- Secure maintenance of remote devices and frequent device updates with the latest security patches

IoT Device Management Solutions

IoT device management solutions are used by security professionals, IT admin, or IoT administrators for onboarding, organizing, monitoring, and managing IoT devices.

Discussed below are some IoT device management solutions:

- **Azure IoT Central**

Source: <https://azure.microsoft.com>

Azure IoT Central is a hosted, extensible software-as-a-service (SaaS) platform that simplifies the setup of IoT solutions. It helps to easily connect, monitor, and manage IoT assets at scale. Azure IoT Central can simplify the initial setup of an IoT solution and can reduce the management burden, operational costs, and overheads of a typical IoT project.

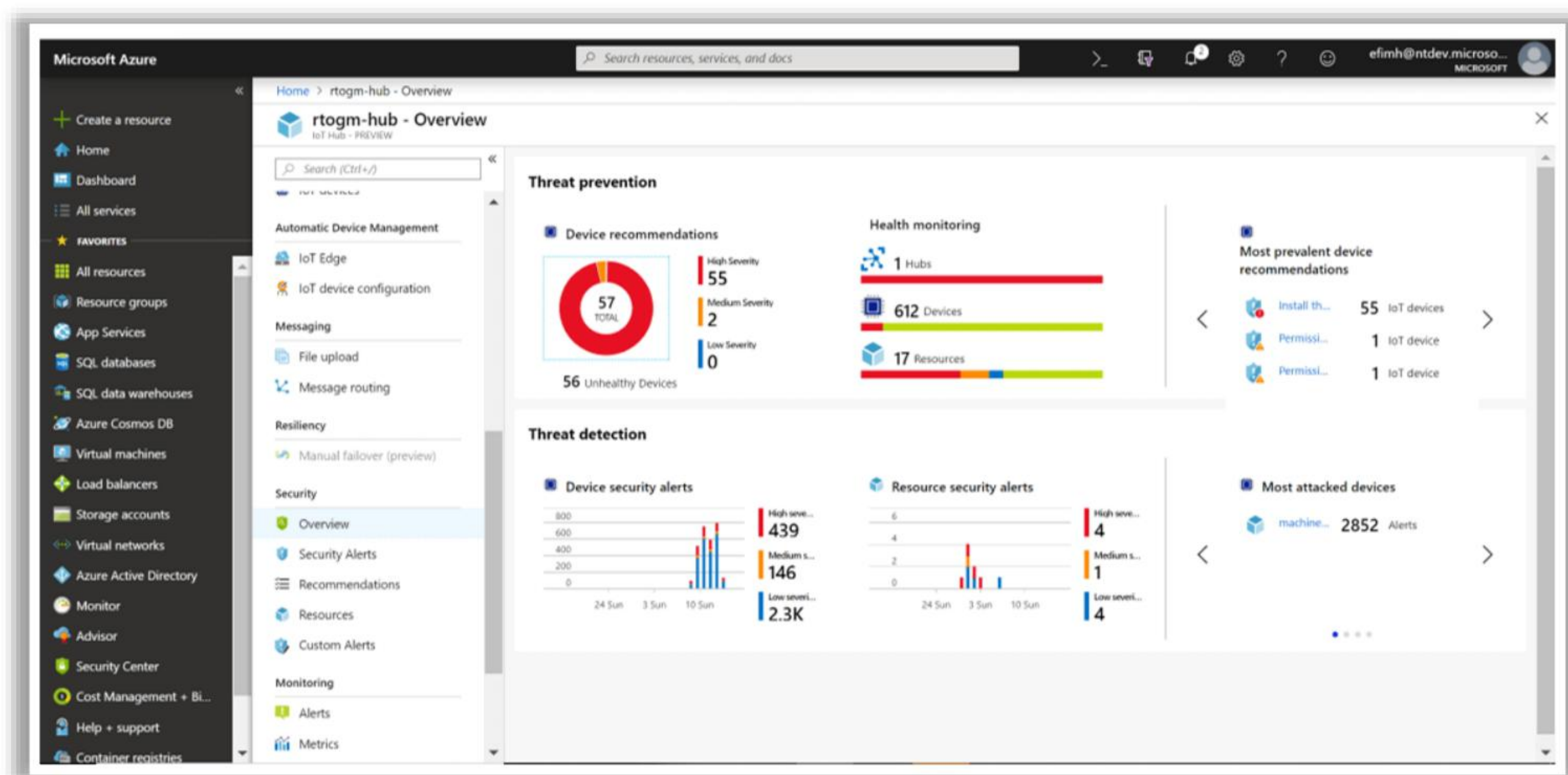
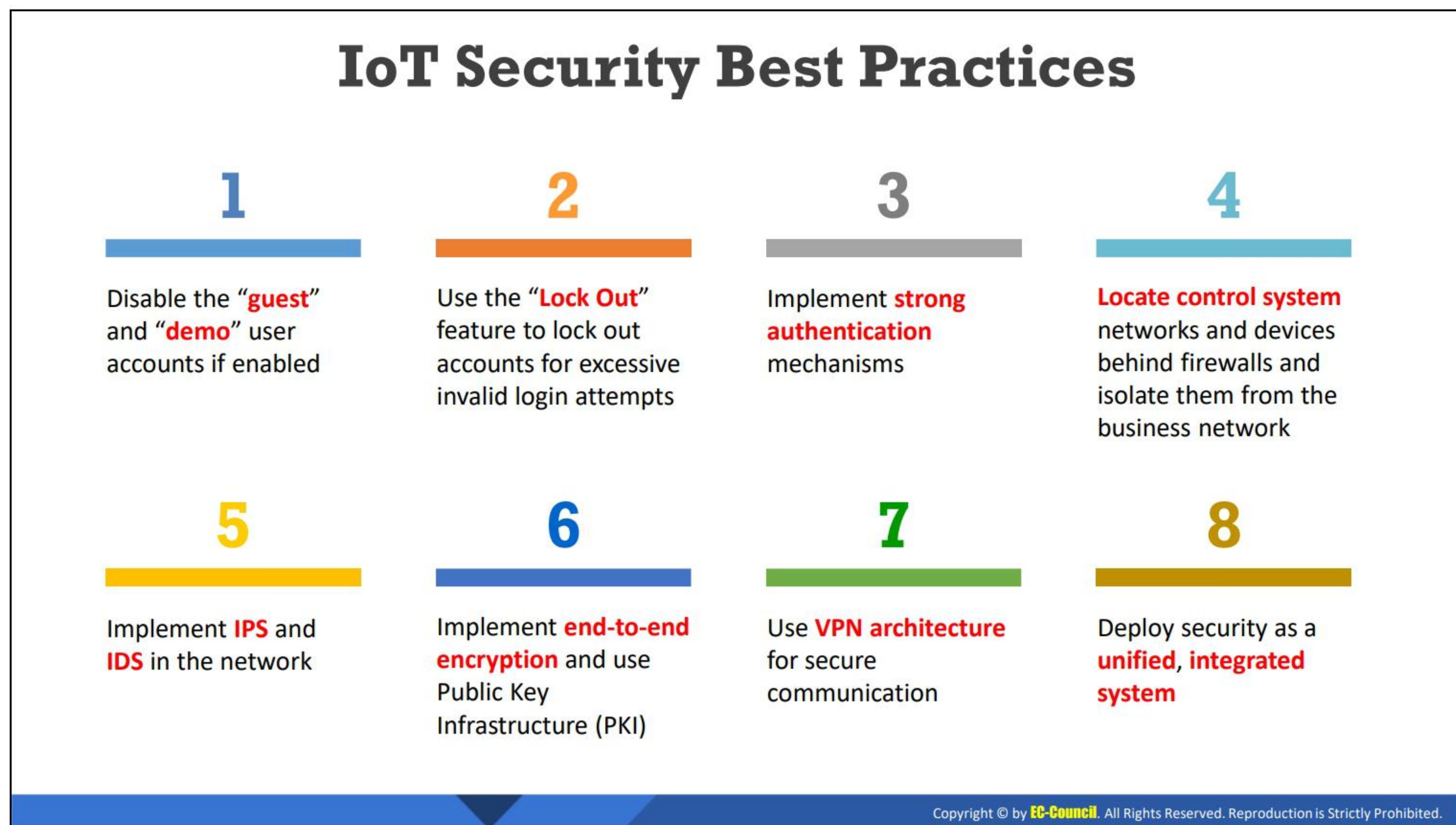


Figure 13.10: Screenshot of Azure IoT Central

Listed below are some of the additional solutions for IoT device management:

- Oracle IoT Asset Monitoring Cloud (<https://www.oracle.com>)
- Predix (<https://www.ge.com>)
- Cloud IoT Core (<https://cloud.google.com>)
- IBM Watson IoT Platform (<https://www.ibm.com>)
- AT&T IoT Connectivity Management (<https://www.business.att.com>)



IoT Security Best Practices

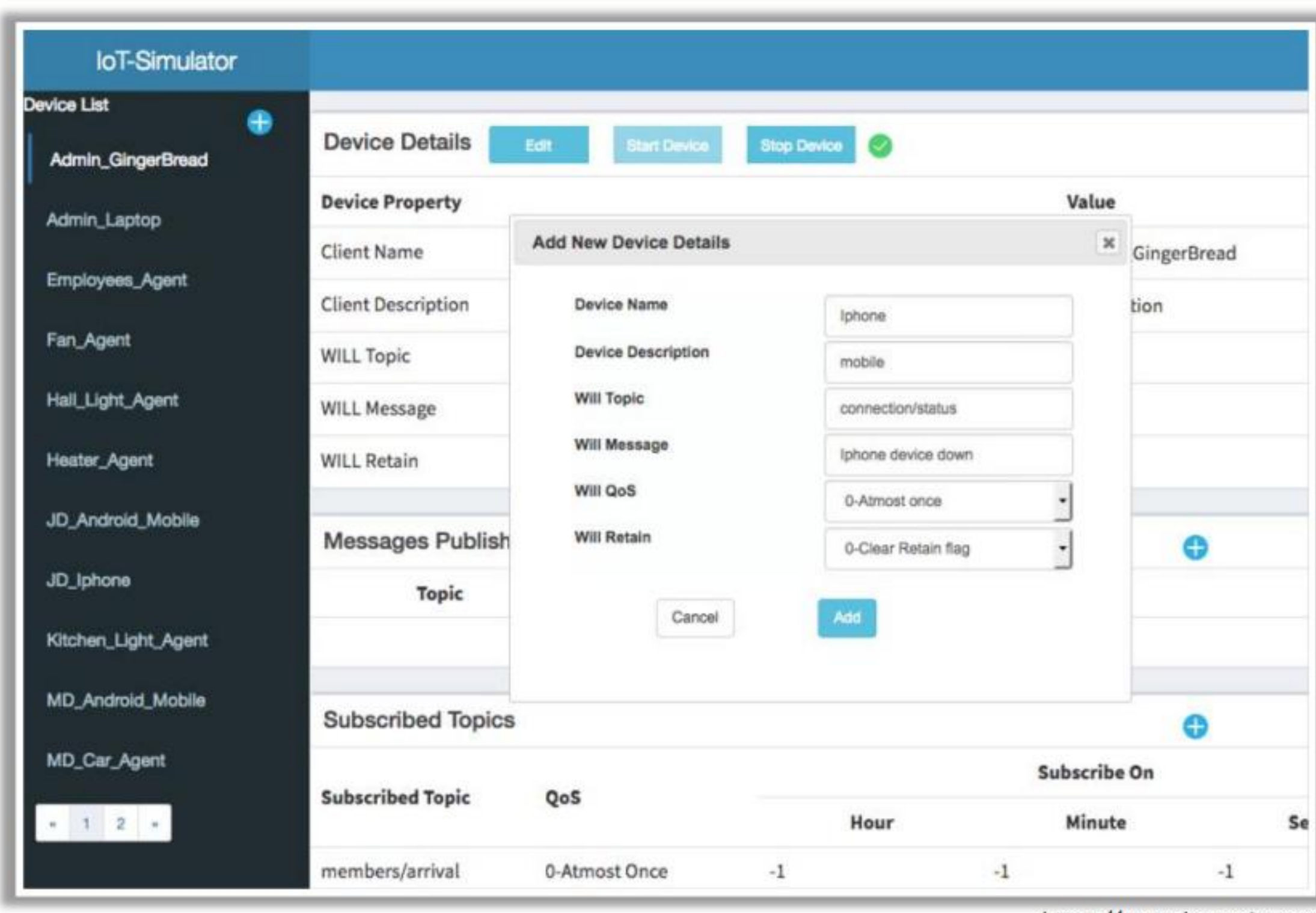
- Disable the "guest" and "demo" user accounts if enabled
- Use the "Lock Out" feature to lock out accounts for excessive invalid login attempts
- Implement a strong authentication mechanism
- Locate control system networks and devices behind firewalls, and isolate them from the business network
- Implement IPS and IDS in the network
- Implement end-to-end encryption and use public key infrastructure (PKI)
- Use VPN architecture for secure communication
- Deploy security as a unified, integrated system
- Allow only trusted IP addresses to access the device from the Internet
- Disable telnet (port 23)
- Disable the UPnP port on routers
- Protect the devices against physical tampering
- Patch vulnerabilities and update the device firmware regularly
- Monitor traffic on port 48101, as infected devices attempt to spread the malicious file using port 48101

- Position of mobile nodes should be verified with the aim of referring one physical node with one vehicle identity only, which means one vehicle cannot have two or more identities
- Data privacy should be implemented; therefore, the user's account or identity should be kept protected and hidden from other users
- Data authentication should be performed to confirm the identity of the original source node
- Maintain data confidentiality using symmetric key encryption
- Implement a strong password policy requiring a password at least 8–10 characters long with a combination of letters, numbers, and special characters
- Use CAPTCHA and account lockout policy methods to avoid brute-force attacks
- Use devices made by manufacturers with a track record of security awareness
- Isolate IoT devices on protected networks


IoT Security Tools

Bevywise IoT Simulator


Bevywise IoT Simulator is an intelligible simulation tool to simulate tens of thousands of **MQTT clients** in a single box




<https://www.bevywise.com>




SeaCat.io
<https://teskalabs.com>




DigiCert IoT Security Solutions
<https://www.digicert.com>



FortiNAC
<https://www.fortinet.com>



Darktrace
<https://www.darktrace.com>



Cisco IoT Threat Defense
<https://www.cisco.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

IoT Security Tools

The IoT is not the only range of devices connected to the Internet, but it is also a very complex, rapidly growing technology. To understand and analyze various risk factors, proper security solutions must be incorporated to protect the IoT devices. The use of IoT security tools helps organizations to significantly limit security vulnerabilities, thereby protecting the IoT devices and networks from different kinds of attacks.

- **Bevywise IoT Simulator**

Source: <https://www.bevywise.com>

Bevywise IoT Simulator is an intelligible simulation tool to simulate tens of thousands of MQTT clients in a single box. It can be used to develop, test, and demonstrate IoT servers and managers. IoT Simulator can be configured to send real-time messages within a range or from a random set of values based on the time and client. Further, it can simulate dynamic messages in two message formats, namely, TXT and JSON, like real-world IoT devices. For flexibly varying the data published in every sequence and to make the data in sync with the real device, IoT Simulator supports four types of dynamic values to be sent as a part of messages: system variable timestamp and client identifier, random, range, linear, and constant. IoT events can be configured with a predefined dataset by uploading a CSV file.

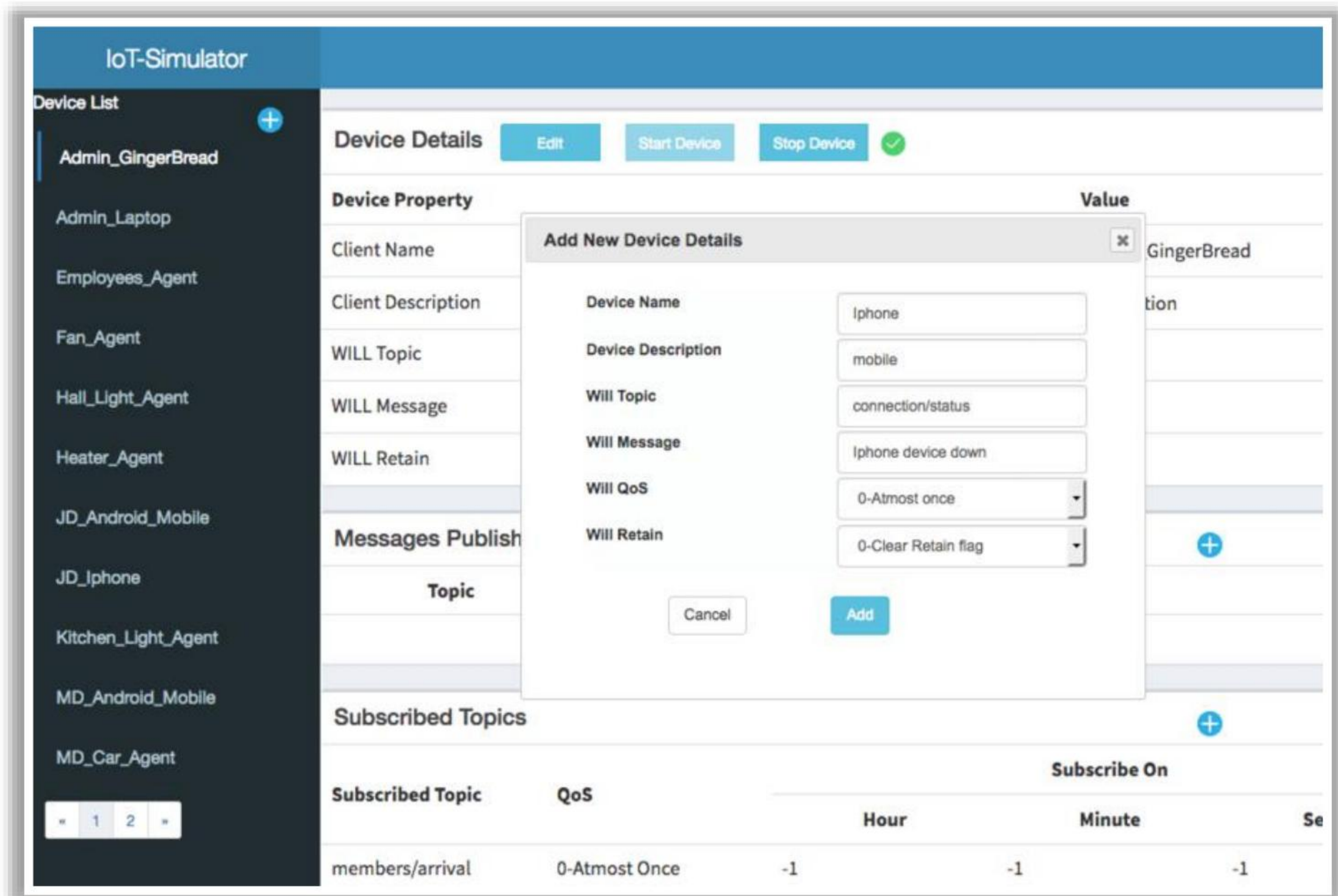
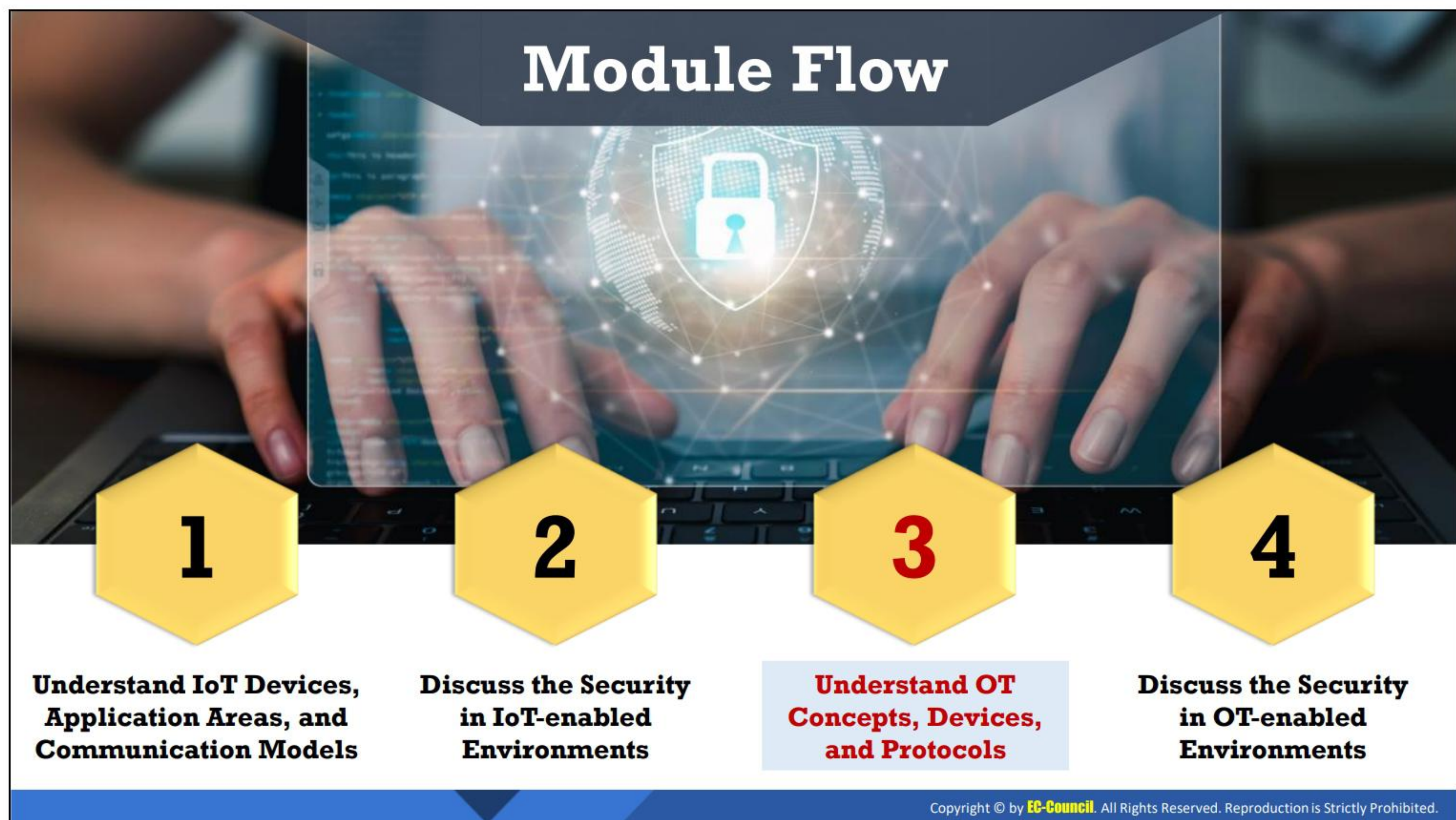


Figure 13.11: Screenshot of Bevywise IoT Simulator

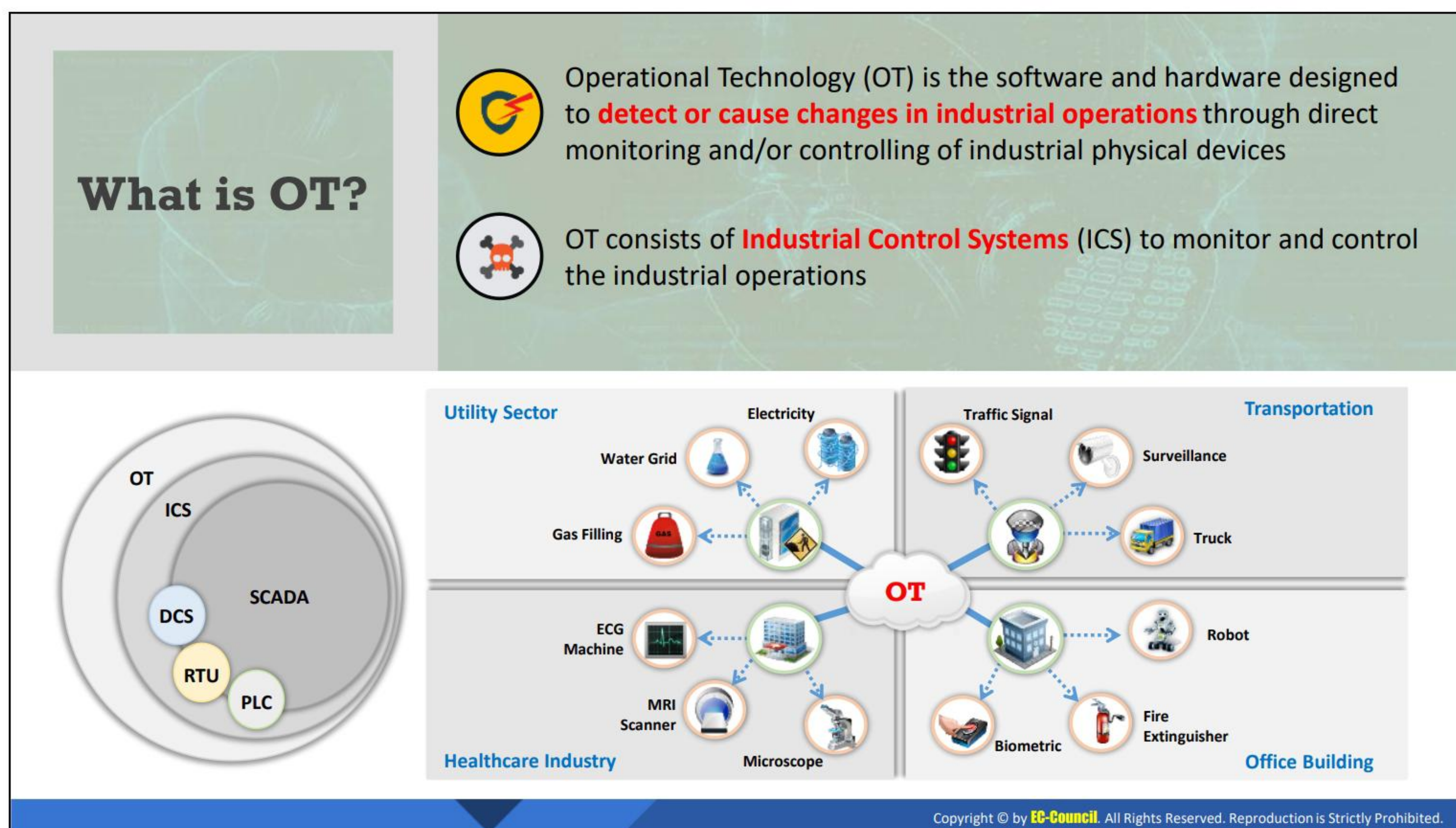
Listed below are some of the additional IoT security tools and solutions:

- SeaCat.io (<https://teskalabs.com>)
- DigiCert IoT Security Solutions (<https://www.digicert.com>)
- FortiNAC (<https://www.fortinet.com>)
- Darktrace (<https://www.darktrace.com>)
- Cisco IoT Threat Defense (<https://www.cisco.com>)



Understand OT Concepts, Devices, and Protocols

Operational technology (OT) plays a major role in today's modern society, as it drives a collection of devices designed to work together as an integrated or homogeneous system. For example, OT in telecommunications is used to transfer information from the electrical grid through wheeling power. The same telecommunications are also used for financial transactions between electrical producers and consumers. OT is a combination of hardware and software that is used to monitor, run, and control industrial process assets. This section discusses various important concepts related to OT.



What is OT?

OT is a combination of software and hardware designed to detect or cause changes in industrial operations through direct monitoring and/or controlling of industrial physical devices. These devices include switches, pumps, lights, sensors, surveillance cameras, elevators, robots, valves, and cooling and heating systems. Any system that analyzes and processes operational data (such as technical components, electronics, telecommunications, and computer systems) can be a part of OT.

OT systems are used in the manufacturing, mining, healthcare, building, transportation, oil and gas, defense, and utility sectors, as well as many other industries, to ensure the safety of physical devices and their operations in networks. This technology consists of Industrial Control Systems (ICSs), which include Supervisory Control and Data Acquisition (SCADA), Remote Terminal Units (RTU), Programmable Logic Controllers (PLC), Distributed Control Systems (DCSs), and many other dedicated network systems that help in monitoring and controlling industrial operations.

OT systems employ different approaches to design hardware and protocols that are unfamiliar with IT. Supporting older versions of software and hardware makes OT systems more vulnerable to cyber-attacks, as developing fixes or patches for them is very difficult.

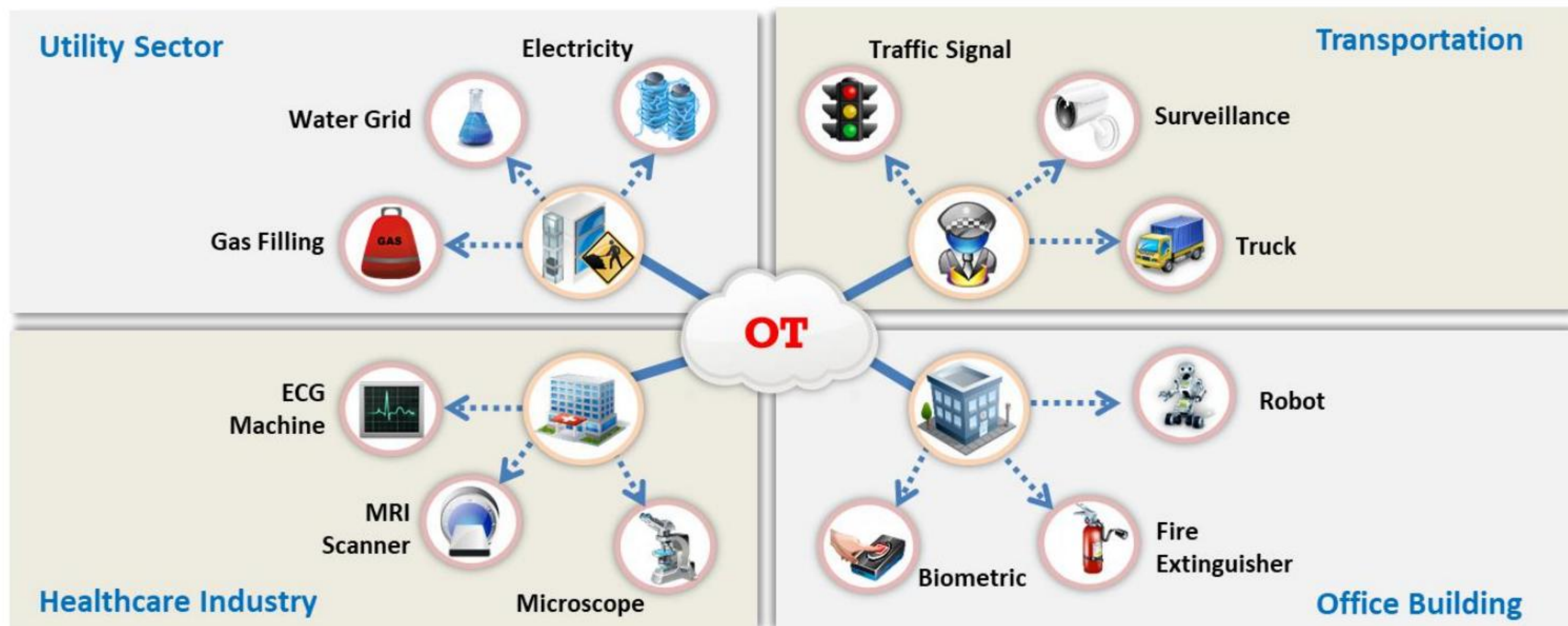


Figure 13.12: Devices connected to an OT network

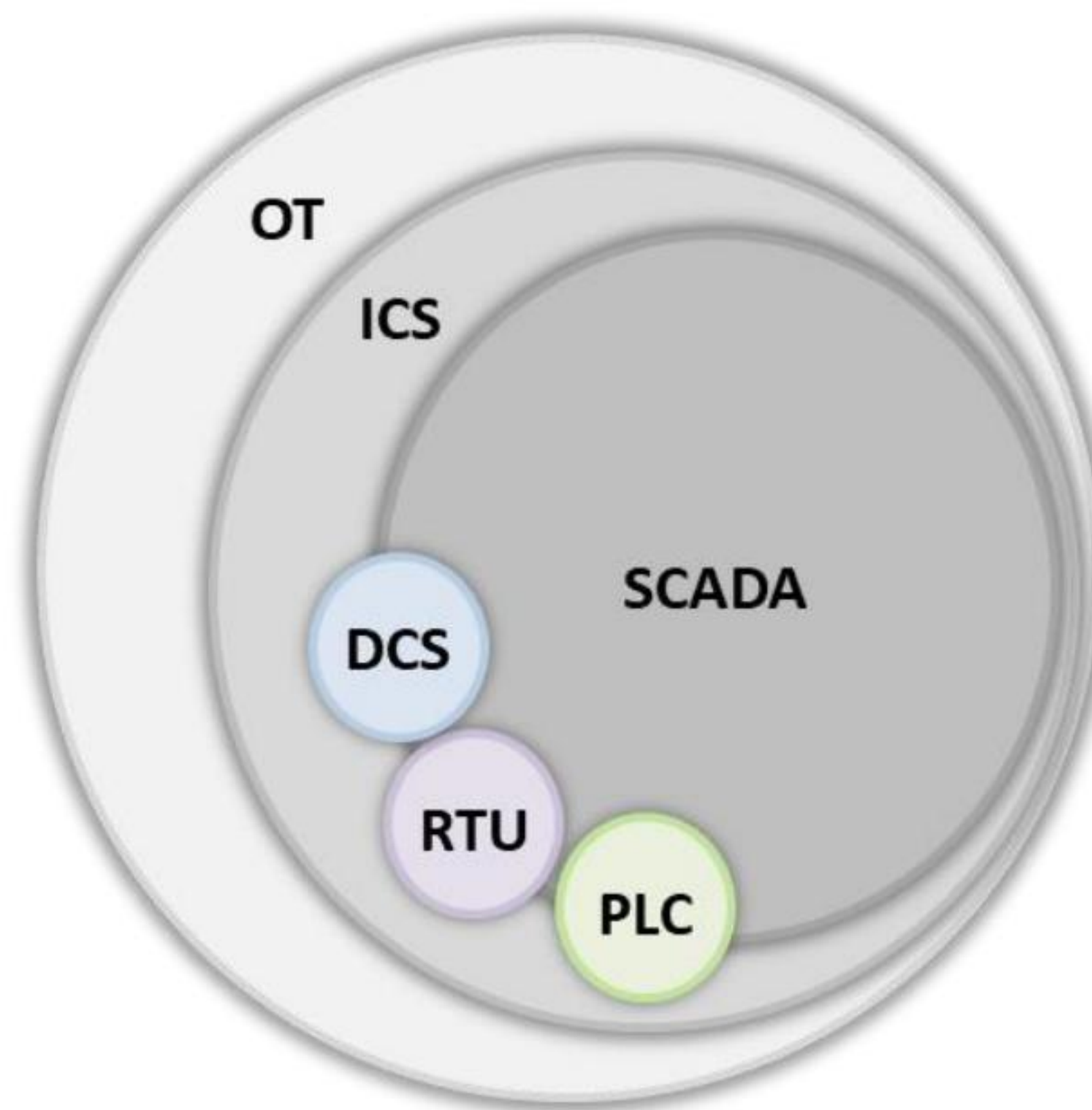


Figure 13.13: Components of OT

Essential Terminology



Assets

OT systems consist of **physical assets** such as sensors and actuators, servers, workstations, network devices, and PLCs, and logical assets such as flow graphics, program logic, databases, firmware, and firewall rules



Zones and Conduits

A **network segregation technique** used to isolate the networks and assets to impose and maintain strong access control mechanisms



Industrial Network

A network of **automated control systems** is known as an industrial network



Business Network

It comprises of a network of systems that offer **information infrastructure** to the business

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Essential Terminology (Cont'd)



Industrial Protocols

Protocols used for **serial communication** and communication over standard Ethernet. Ex: S7, CDA, CIP, Modbus, etc.



Network Perimeter

It is the outermost boundary of a network zone i.e. **closed group of assets**



Electronic Security Perimeter

It is referred to as the **boundary** between secure and insecure zones



Critical Infrastructure

A collection of **physical or logical systems** and assets that the failure or destruction of which will severely impact the security, safety, economy, or public health

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Essential Terminology

Discussed below are some of the most important and extensively used terms related to OT systems:

- **Assets**

Different components of OT are generally referred to as assets. Most OT systems, such as ICSs, comprise physical assets such as sensors and actuators, servers, workstations,

network devices, PLCs, etc. ICS systems also include logical assets that represent the workings and containment of physical assets, such as graphics representing process flow, program logic, database, firmware, or firewall rules.

- **Zones and Conduits**

Zones and conduits is a network segregation technique used to isolate networks and assets to impose and maintain strong access control mechanisms.

- **Industrial Network and Business Network**

OT generally comprises a collection of automated control systems. These systems are networked to achieve a business objective. A network comprising these systems is known as an industrial network. An enterprise or business network comprises a network of systems that offer an information infrastructure to the business. Businesses often need to establish communications between business networks and industrial networks.

- **Industrial Protocols**

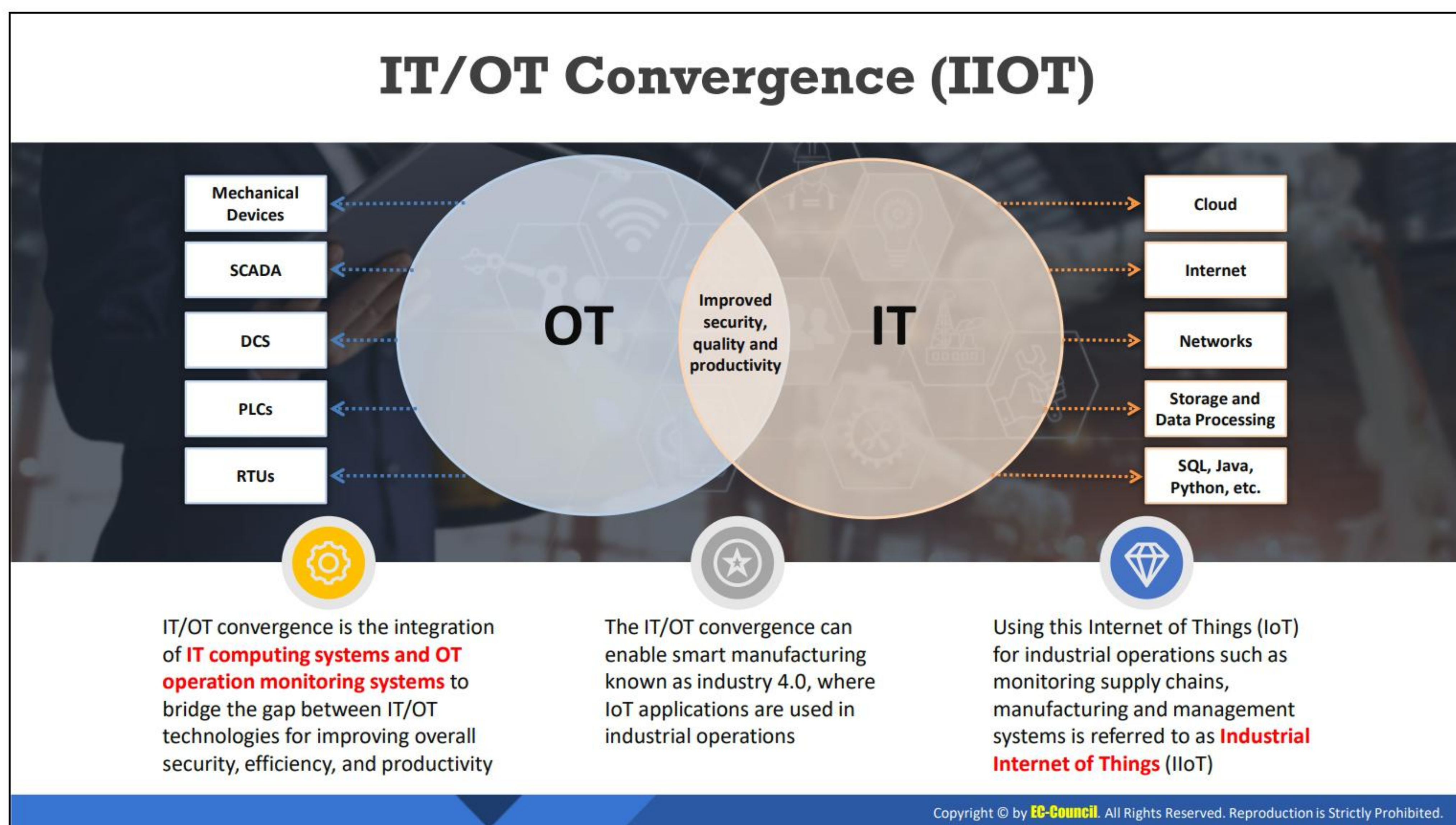
Most OT systems employ proprietary protocols (S7, CDA, SRTP, etc.) or non-proprietary protocols (Modbus, OPC, DNP3, CIP, etc.). These protocols are generally used for serial communication and can also be used for communication over standard Ethernet using Internet Protocol (IP) along with transport layer protocols TCP or UDP. As these protocols operate at the application layer, they are referred to as applications.

- **Network Perimeter/Electronic Security Perimeter**

The network perimeter is the outermost boundary of a network zone, i.e., a closed group of assets. It acts as a point of separation between the interior and exterior of a zone. Generally, cybersecurity controls are implemented at the network perimeter. An Electronic Security Perimeter refers to a boundary between secure and insecure zones.

- **Critical Infrastructure**

Critical infrastructure refers to a collection of physical or logical systems and assets, the failure or destruction of which will severely impact security, safety, the economy, or public health.



IT/OT Convergence (IIOT)

IT/OT convergence is the integration of IT (information technology) computing systems and OT operation monitoring systems. Bridging the gap between IT and OT can improve the overall business, producing faster and efficient results. IT/OT convergence is not just about combining technologies but also about teams and operations. IT and OT teams are traditionally separated and are found in their respective domains. For instance, IT teams monitor internal processes such as programming, updating systems, and safeguarding networks from cyber-attacks, whereas OT teams ensure overall maintenance and management, including that of employees and industrial equipment.

IT/OT teams are required to understand each other's operations and working structure. This does not mean switching IT engineers into field/plant engineers or vice versa; it is about building a bridge between them to co-operate with each other to improve security, efficiency, quality, and productivity.

Benefits of merging OT with IT

IT/OT convergence can enable smart manufacturing known as industry 4.0, in which IoT applications are used in industrial operations. Using the IoT for industrial operations such as monitoring supply-chain, manufacturing, and management systems is referred to as the Industrial Internet of Things (IIoT).

The following are some of the benefits of converging IT/OT:

- **Enhancing Decision Making:** Decision making can be enhanced by integrating OT data into business intelligence solutions.
- **Enhancing Automation:** Business flow and industrial control operations can be optimized by OT/IT merging; together they can improve the automation.

- **Expedite Business Output:** IT/OT convergence can organize or streamline development projects to accelerate business output.
- **Minimizing Expenses:** Reduces the technological and organizational overheads.
- **Mitigating Risks:** Merging these two fields can improve overall productivity, security, and reliability, as well as ensuring scalability.

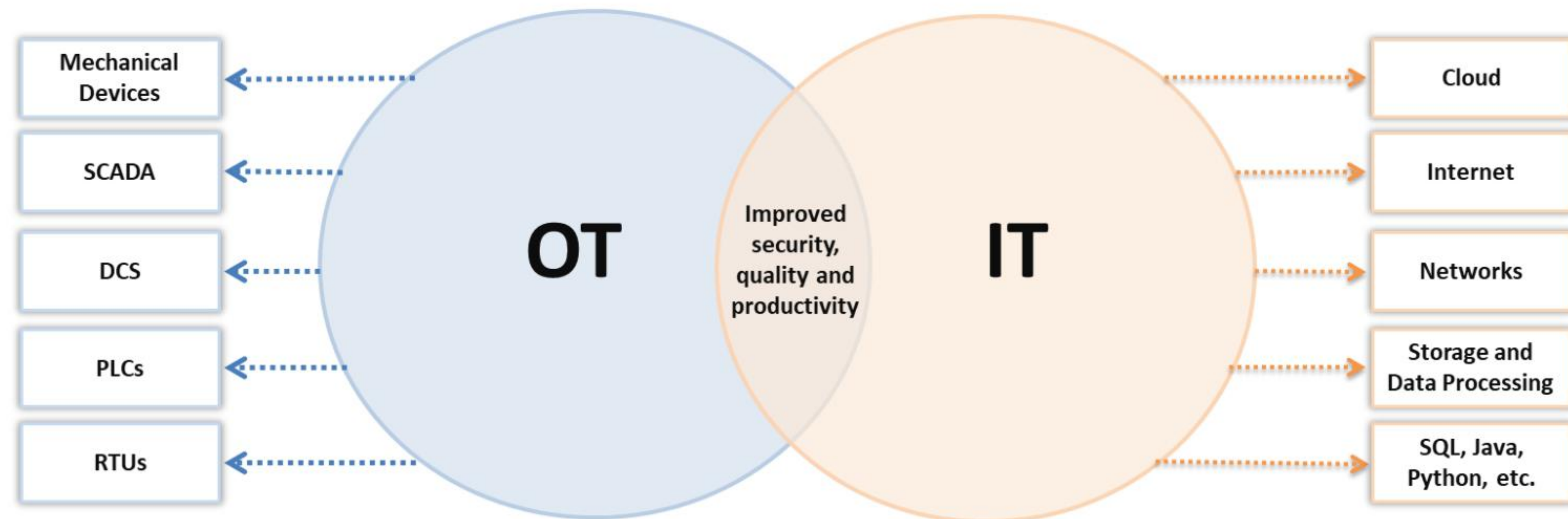


Figure 13.14: IT/OT convergence

The Purdue Model

- ❑ The Purdue model is derived from the **Purdue Enterprise Reference Architecture** (PERA) model, which is a widely used to describe internal connections and dependencies of important components in the ICS networks
- ❑ It consists of three zones

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

The Purdue Model

The Purdue model is derived from the Purdue Enterprise Reference Architecture (PERA) model, which is a widely used conceptual model that describes the internal connections and dependencies of important components in ICS networks. The Purdue model is also known as the Industrial Automation and Control System reference model.

The Purdue model consists of three zones: the manufacturing zone (OT) and enterprise zone (IT), separated by a demilitarized zone (DMZ), which is used to restrict direct communication between the OT and IT systems. The intention behind adding this extra layer is to confine the network or system compromises within this layer and provide uninterrupted production.

The three zones are further divided into several operational levels. Each zone, with associated levels, is described below:

IT Systems (Enterprise Zone)	Level 5	Enterprise Network
	Level 4	Business Logistics Systems
Industrial Demilitarized Zone (IDMZ)		
OT Systems (Manufacturing Zone)	Level 3	Operation Systems/Site Operations
	Level 2	Control Systems/Area Supervisory Controls
	Level 1	Basic Controls/Intelligent Devices
	Level 0	Physical Process

Figure 13.15: The Purdue model

- **Enterprise Zone (IT Systems)**

The enterprise security zone is a part of IT, in which supply-chain management and scheduling are performed using business systems such as SAP and ERP. It also locates the data centers, users, and cloud access. The enterprise zone consists of two levels.

- **Level 5 (Enterprise Network)**

This is a corporate level network where business operations such as B2B (business-to-business) and B2C (business-to-customer) services are performed. Internet connectivity and management can be handled at this level. The enterprise network systems also accumulate data from all the subsystems located at the individual plants to report the inventory and overall production status.

- **Level 4 (Business Logistics Systems)**

All the IT systems supporting the production process in the plant lie at this level. Managing schedules, planning, and other logistics of the manufacturing operations are performed here. Level 4 systems include application servers, file servers, database servers, supervising systems, email clients, etc.

- **Manufacturing Zone (OT Systems)**

All the devices, networks, control, and monitoring systems reside in this zone. The manufacturing zone consists of four levels.

- **Level 3 (Operational Systems/Site Operations)**

In this level, the production management, individual plant monitoring, and control functions are defined. Production workflows and output of the desired product are ensured at this level. Production management includes plant performance management systems, production scheduling, batch management, quality assurance, data historians, manufacturing execution/operation management systems (MES/MOMS), laboratories, and process optimization. Production details from lower levels are collected here and can then be transferred to higher levels or can be instructed by higher-level systems.

- **Level 2 (Control Systems/Area Supervisory Controls)**

Supervising, monitoring, and controlling the physical process is carried out at this level. The control systems can be DCSs, SCADA software, Human–Machine Interfaces (HMIs), real-time software, and other supervisory control systems such as engineering works and PLC line control.

- **Level 1 (Basic Controls/Intelligent Devices)**

Analyzation and alteration of the physical process can be done at this level. The operations in basic control include “start motors,” “open valves,” “move actuators,” etc. Level 1 systems include analyzers, process sensors, and other instrumentation systems such as Intelligent Electronic Devices (IEDs), PLCs, RTUs, Proportional Integral Derivative (PID) controllers, Equipment Under Control (EUC), and Variable

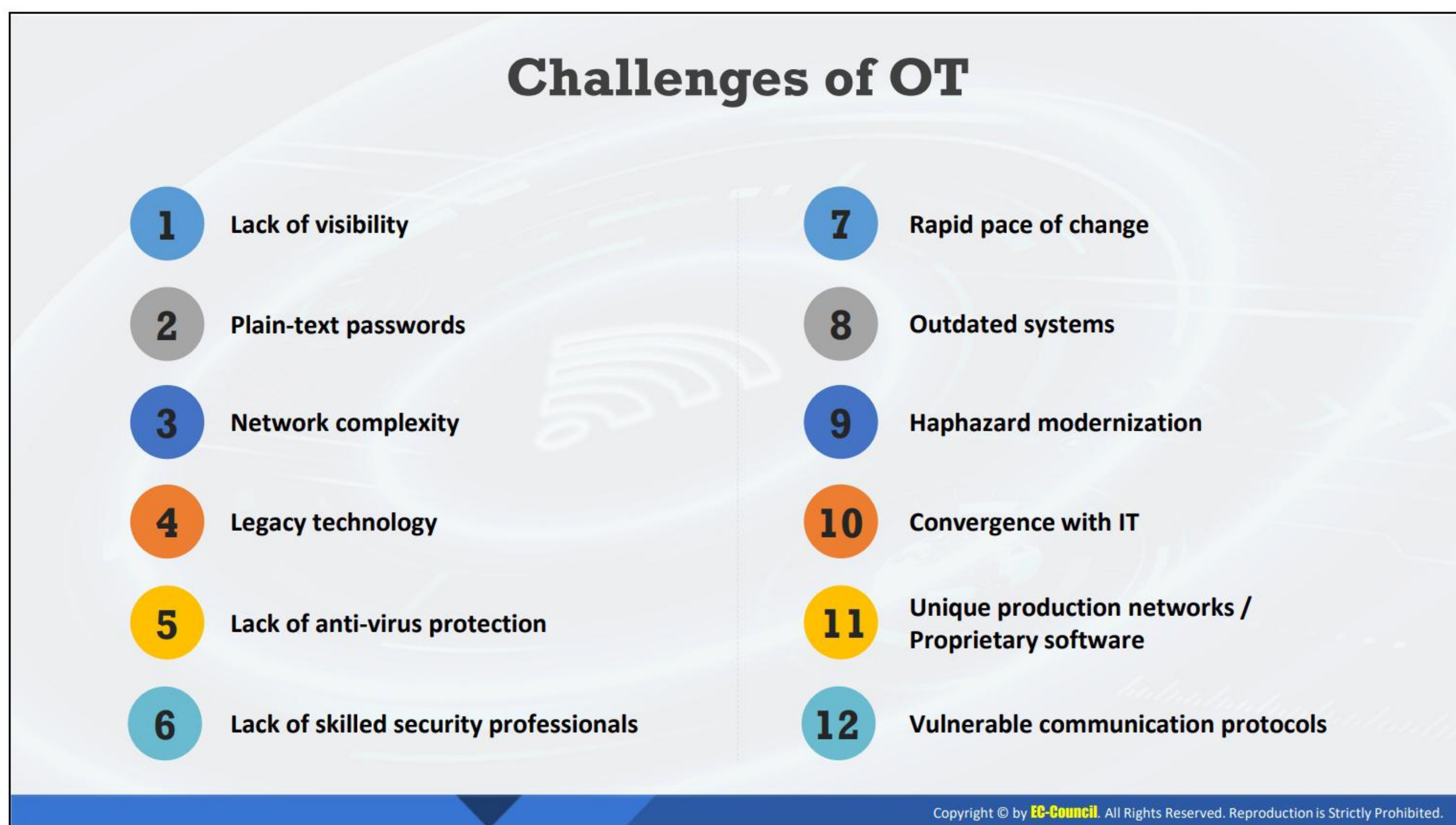
Frequency Drives (VFDs). PLC was used in level 2 with a supervisory functionality, but it is used as a control function in level 1.

- **Level 0 (Physical Process)**

In this level, the actual physical process is defined, and the product is manufactured. Higher levels control and monitor operations at this level; therefore, this layer is also referred to as Equipment Under Control (EUC). Level 0 systems include devices, sensors (e.g., speed, temperature, pressure), actuators, or other industrial equipment used to carry out the manufacturing or industrial operations. A minor error in any of the devices at this level can affect overall operations.

- **Industrial Demilitarized Zone (IDMZ)**

The demilitarized zone is a barrier between the manufacturing zone (OT systems) and enterprise zone (IT systems) that enables a secure network connection between the two systems. The zone is created to inspect overall architecture. If any errors or intrusions compromise the working systems, the IDMZ holds the error and allows production to be continued without interruption. IDMZ systems include Microsoft domain controllers, database replication servers, and proxy servers.



Challenges of OT

OT plays a vital role in several sectors of critical infrastructure, like power plants, water utilities, and healthcare. Absurdly, most OT systems run on old versions of software and use obsolete hardware, which makes them vulnerable to malicious exploits like phishing, spying, ransomware attacks, etc. These types of attacks can be devastating to products and services. To curb these vulnerabilities, the OT system must employ critical examination in key areas of vulnerability by using various security tools and tactics.

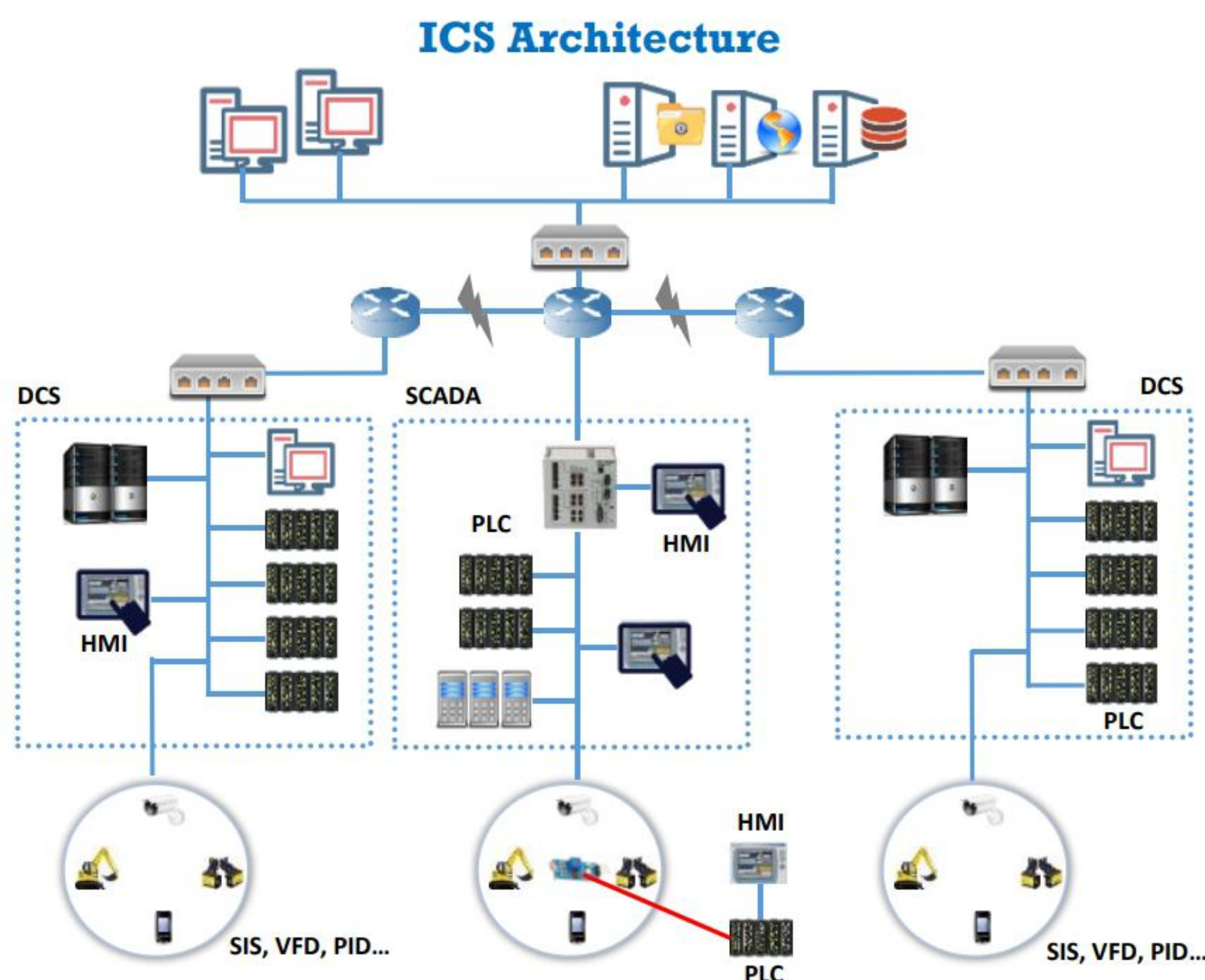
Discussed below are some of the challenges and risks to OT that makes it vulnerable to many threats:

- **Lack of visibility:** Broader cybersecurity visibility in the OT network achieves greater security and so one can rapidly respond to any potential threats. However, most organizations do not have clear cybersecurity visibility, making it difficult for the security teams to detect unusual behaviors and signatures.
- **Plain-text passwords:** Most industrial site networks use either weak or plain-text passwords. Plain-text passwords lead to weak authentication, which in turn leaves the systems vulnerable to various cyber-reconnaissance attacks.
- **Network complexity:** Most OT network environments are complex due to comprising numerous devices, each of which has different security needs and requirements.
- **Legacy technology:** OT systems generally use older technologies without appropriate security measures like encryption and password protection, leaving them vulnerable to various attacks. Applying modern security practices is also a challenge.

- **Lack of antivirus protection:** Industries using legacy technology and outdated systems are not provided with any antivirus protection, which can update signatures automatically, thus making them vulnerable to malware infections.
- **Lack of skilled security professionals:** The cybersecurity skills gap poses a great threat to organizations, as there is a lack of skilled security professionals to discover threats and implement new security controls and defenses in networks.
- **Rapid pace of change:** Maintaining the pace of change is the biggest challenge in the field of security, and slow digital transformation can also compromise OT systems.
- **Outdated systems:** Most OT devices, such as PLCs, use outdated firmware, making them vulnerable to many modern cyberattacks.
- **Haphazard modernization:** As the demand for OT grows, it must stay up to date with the latest technologies. However, due to the use of legacy components in OT system upgrading and patching, updating the system can take several years, which can adversely affect several operations.
- **Insecure connections:** OT systems communicate over public Wi-Fi and unencrypted Wi-Fi connections in the IT network for transferring control data, making them susceptible to man-in-the-middle attacks.
- **Usage of rogue devices:** Many industrial sites have unknown or rogue devices connected to their networks, which are vulnerable to various attacks.
- **Convergence with IT:** OT mostly connects with the corporate network; as a result, it is vulnerable to various malware attacks and malicious insiders. In addition, the OT systems are IT enabled, and the IT security team does not have much experience with the OT systems and protocols.
- **Organizational challenges:** Many organizations implement and maintain different security architectures that meet the needs of both IT and OT. This can create some flaws in security management, leaving ways for the attackers to intrude into the systems easily.
- **Unique production networks/proprietary software:** Industries follow unique hardware and software configurations that are dependent on industry standards and explicit operational demands. The use of proprietary software makes it difficult to update and patch firmware, as multiple vendors control it.
- **Vulnerable communication protocols:** OT uses communication protocols such as Modbus and Profinet for supervising, controlling, and connecting different mechanisms such as controllers, actuators, and sensors. These protocols lack in-built security features such as authentication, detection of flaws, or detection of abnormal behavior, making them vulnerable to various attacks.
- **Remote management protocols:** Industrial sites use remote management protocols such as RDP, VNC, and SSH. Once the attacker compromises and gains access to the OT network, he/she can perform further exploitation to understand and manipulate the configuration and working of the equipment.

Introduction to ICS

- ❑ ICS is often referred to as a collection of different types of **control systems** and their associated equipment such as systems, devices, networks, and controls used to operate and automate several industrial processes
- ❑ An ICS consists of several types of control systems like **SCADA**, **DCS**, **BPCS**, **SIS**, **HMI**, **PLCs**, **RTU**, **IED**, etc.
- ❑ ICS systems are extensively used in industries like electricity production and distribution, water supply and waste-water treatment, oil and natural gas supply, chemical and pharmaceutical production, pulp and paper, and food and beverages



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Introduction to ICS

The Industrial Control System (ICS) is an essential part of every industrial process and critical infrastructure found in industry. A typical ICS represents the information system that controls and supports all types of industrial processes, such as production, manufacturing, product handling, distribution, etc. An ICS often refers to a collection of different types of control systems and their associated equipment, such as systems, devices, networks, and controls used to operate and automate several industrial processes.

An ICS comprises several types of control systems, such as SCADA systems, DCSs, Basic Process Control Systems (BPCSs), Safety Instrumentation Systems (SISs), HMIs, PLCs, RTUs, and IEDs. This technology consists of various components, such as sensors, controllers, and actuators (mechanical, electrical, hydraulic, pneumatic, etc.), that act collectively to achieve an industrial objective.

The process is the part of an ICS system that is mainly responsible for producing the output. The control is the part of an ICS system that includes the instructions needed to obtain the desired output. This control part is either fully automated or may involve human intervention in the process loop. The operation of ICS systems can be configured in three modes, namely open loop, closed loop, and manual loop mode.

- **Open Loop:** The output of the system depends on the preconfigured settings.
- **Closed Loop:** The output always has an effect on the input to acquire the desired objective.
- **Manual Loop:** The system is totally under the control of humans.

The controller (control) of the ICS system is primarily responsible for maintaining compliance with the desired specifications. Generally, ICS systems include multiple control loops, HMIs, and tools used for remote maintenance and diagnostics. The remote management and diagnostics tools are built using various networking protocols. ICS systems are extensively used in industries such as electricity production and distribution, water supply and wastewater treatment, oil and natural gas supply, chemical and pharmaceutical production, pulp and paper, and food and beverages. In some industries, ICSs are even distributed physically across multiple locations and their processes may be dependent on each other. In such cases, communication protocols are extensively used for efficient communication between the distributed ICS systems.

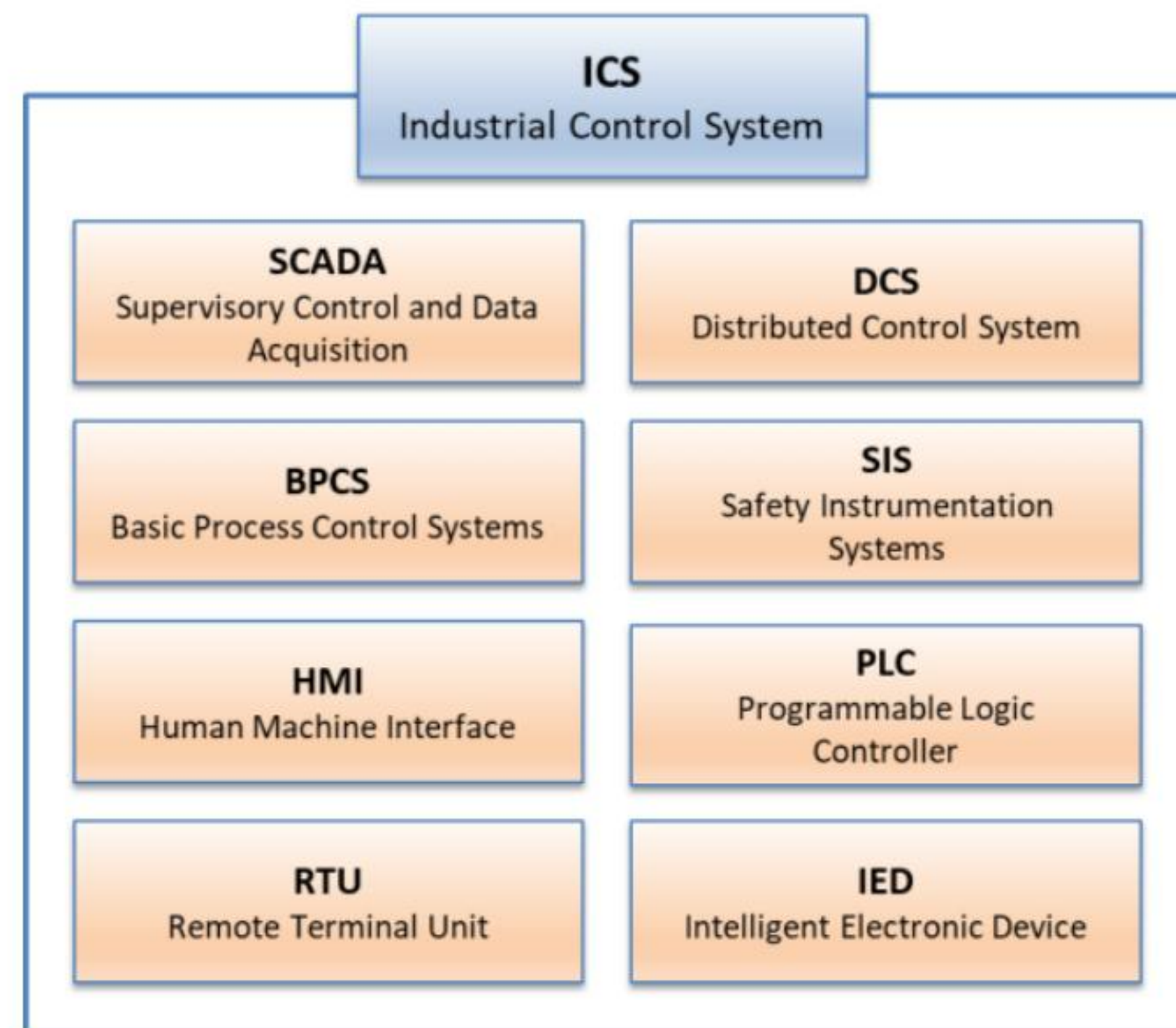


Figure 13.16: Components of an ICS

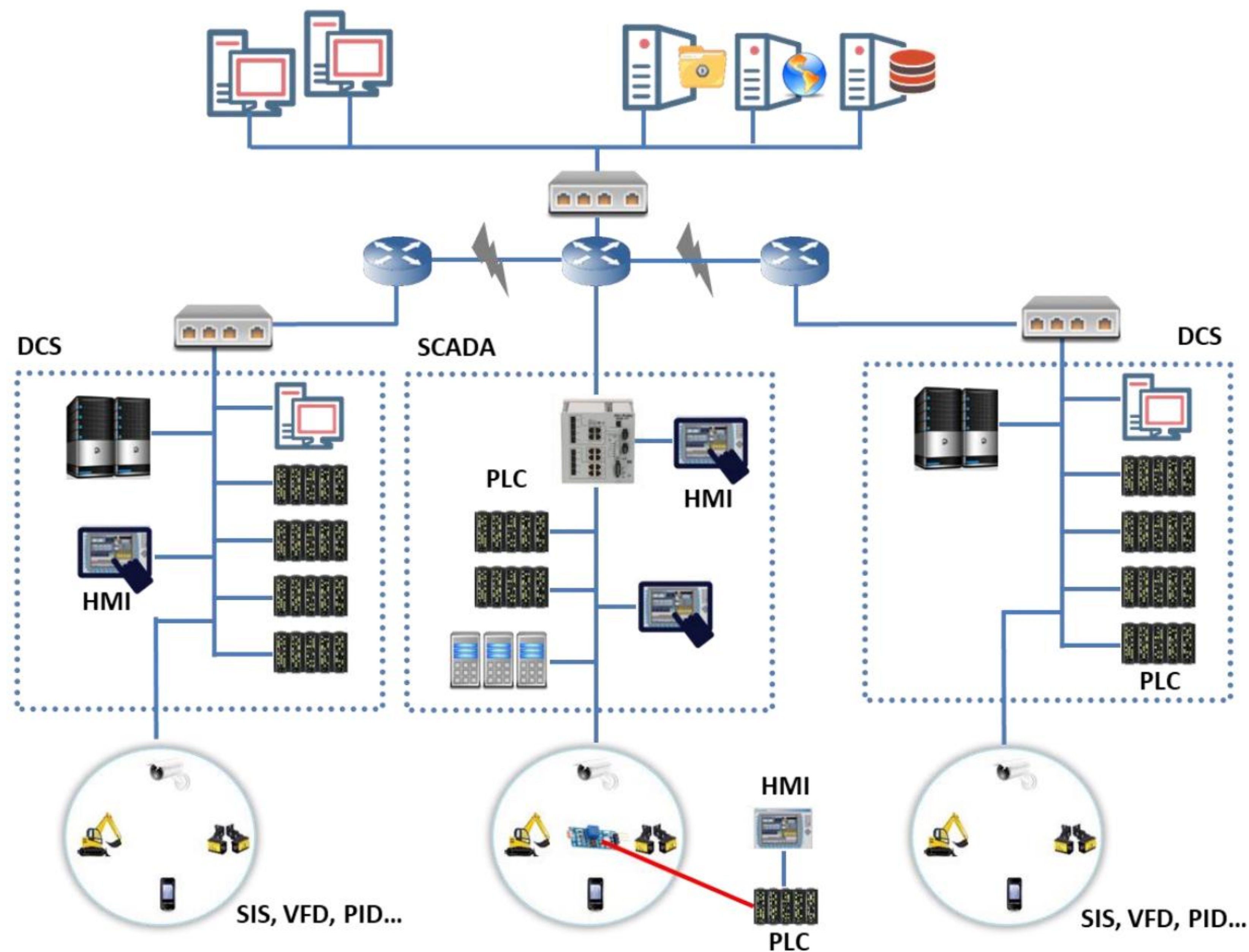
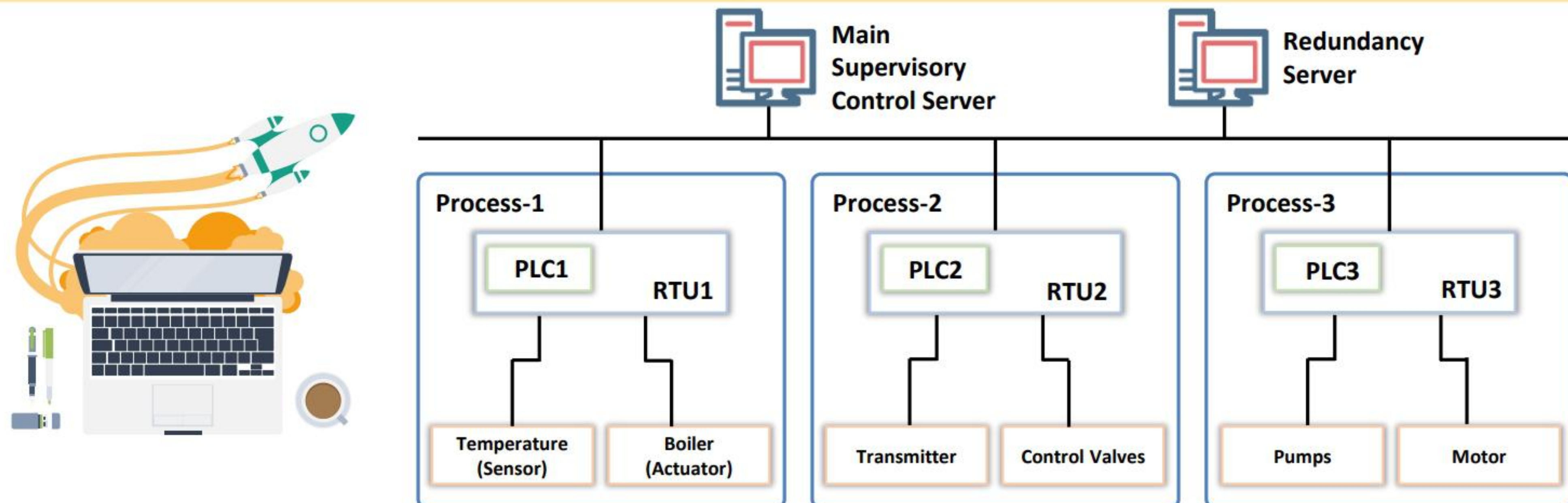


Figure 13.17: ICS architecture

Components of an ICS - Distributed Control System (DCS)

- ❑ DCS is a highly engineered and **large-scale control system** that is often used to perform industry specific tasks
- ❑ It contains a **centralized supervisory control** unit used to control multiple local controllers, thousands of I/O points, and various other field devices that are part of the overall production process
- ❑ It operates using a centralized supervisory control loop (SCADA, MTU, etc.) that connects a group of **localized controllers** (RTU/PLC) to execute the overall tasks required for the working of an entire production process



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

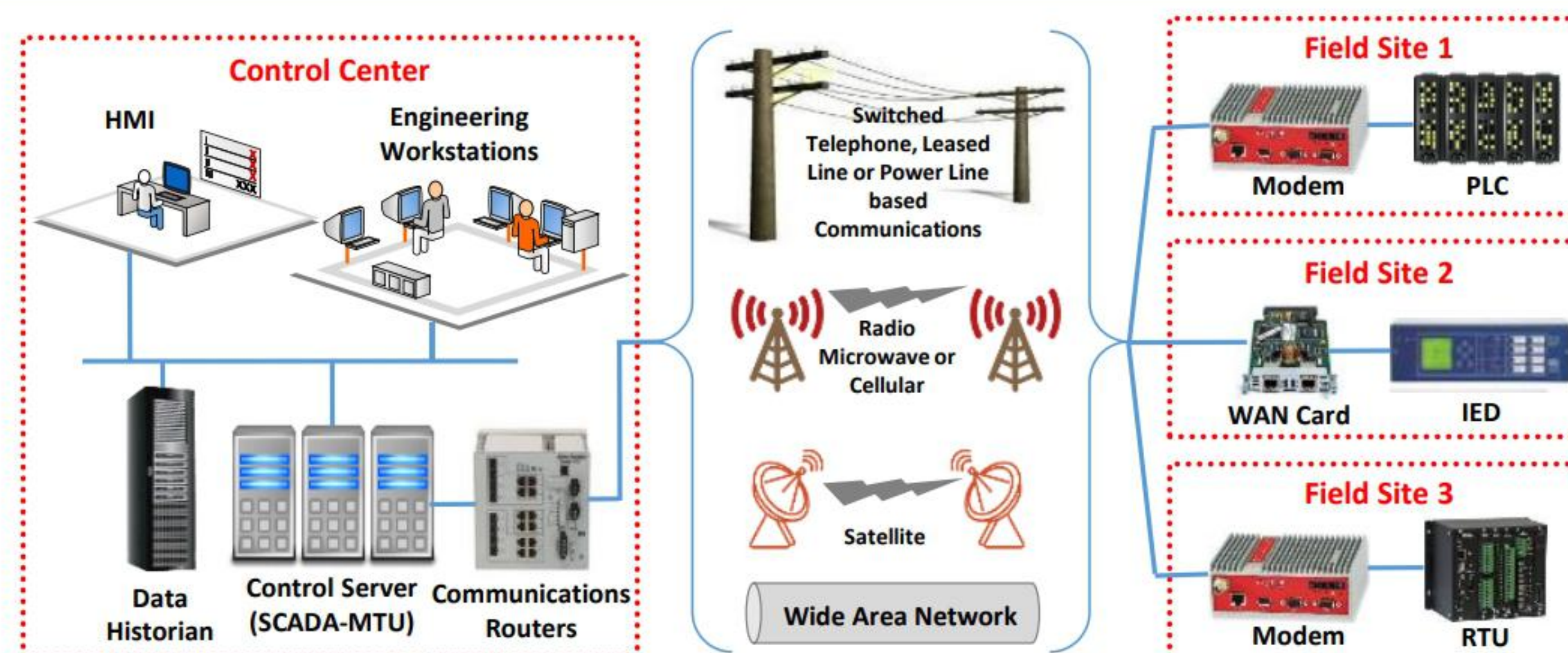
Components of an ICS - Supervisory Control and Data Acquisition (SCADA)



SCADA is a **centralized supervisory control system** that is used for controlling and monitoring industrial facilities and infrastructure



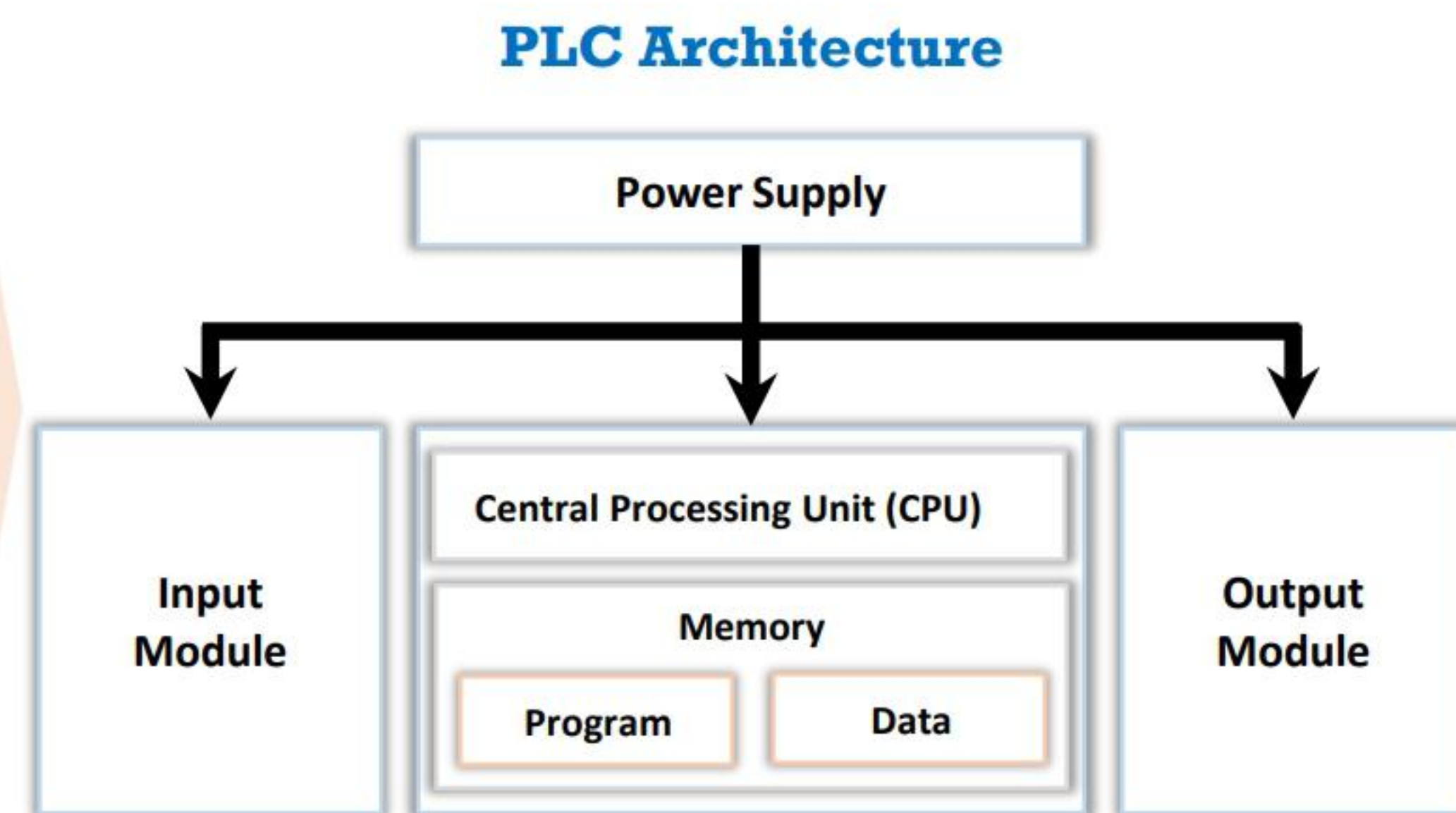
It provides **centralized controlling and monitoring** of multiple process inputs and outputs by integrating the data acquisition system with the data transmission system and Human Machine Interface (HMI) software



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Programmable Logic Controller (PLC)

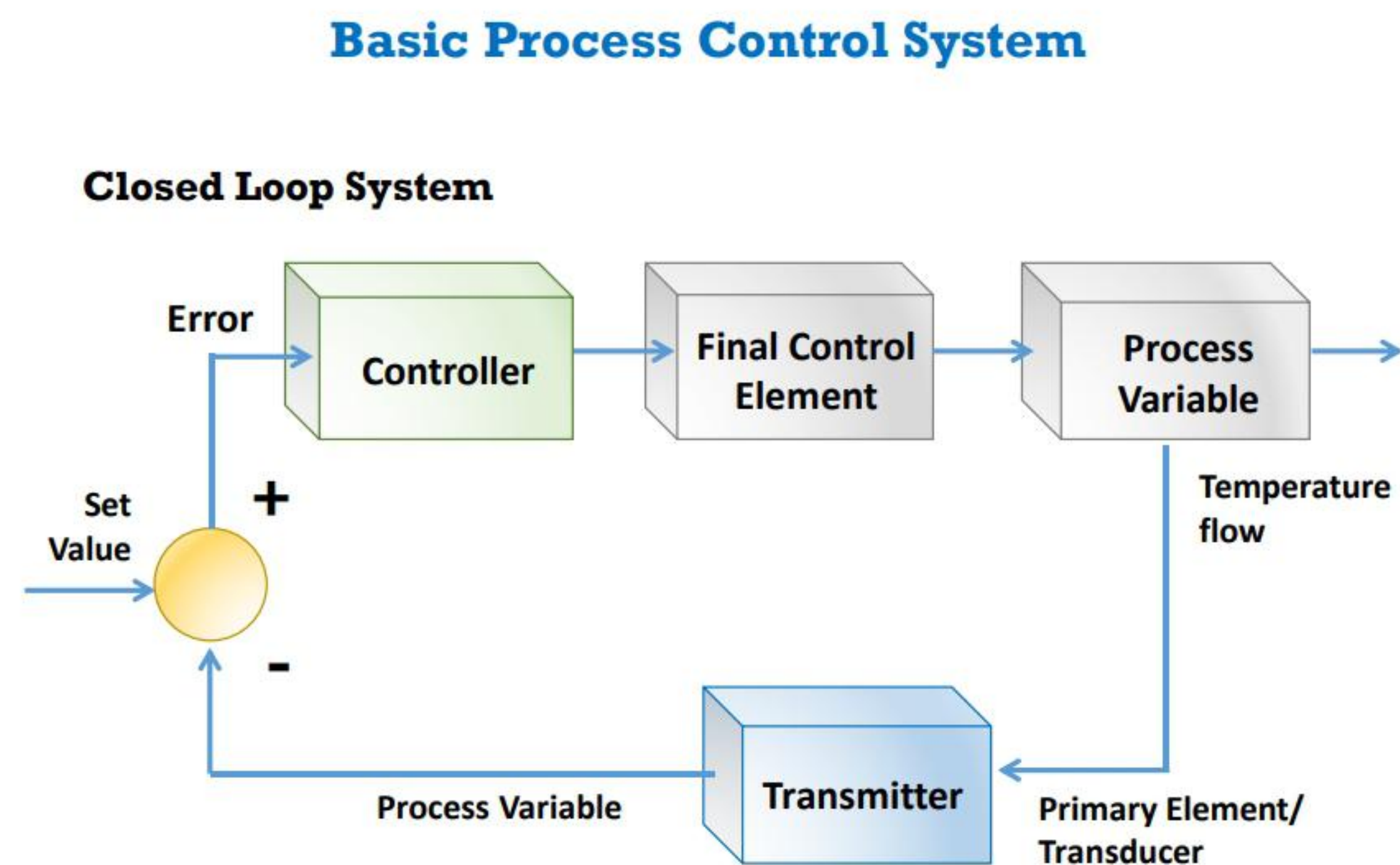
- ❑ A programmable logic controller (PLC) is a small **solid-state control computer** where instructions can be customized to perform a specific task
- ❑ PLC systems consists of three modules:
 - **CPU Module:** It comprises of a central processor and its memory component
 - **Power Supply Module:** It provides a necessary supply of power required for the CPU and I/O modules by converting the power from AC to DC
 - **I/O Modules:** These are used in connecting the sensors and actuators with the system for sensing and controlling the real-time values such as pressure, temperature, and flow
- ❑ PLCs are used in industries such as the steel industry, automobile industry, energy sector, chemical industry, glass industry, and paper industry



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Basic Process Control System (BPCS)

- ❑ A BPCS is responsible for **process control** and **monitoring** of the industrial infrastructure
- ❑ It is a system that **responds to input signals** from the process and associated equipment to generate output signals that cause the process and its associated equipment to operate based on an approved design control strategy
- ❑ A BPCS is applicable to all sorts of control loops like temperature control loops, batch control, pressure control loops, flow control loops, feedback and feed-forward control loops used in industries such as chemical, oil and gas, and food and beverages



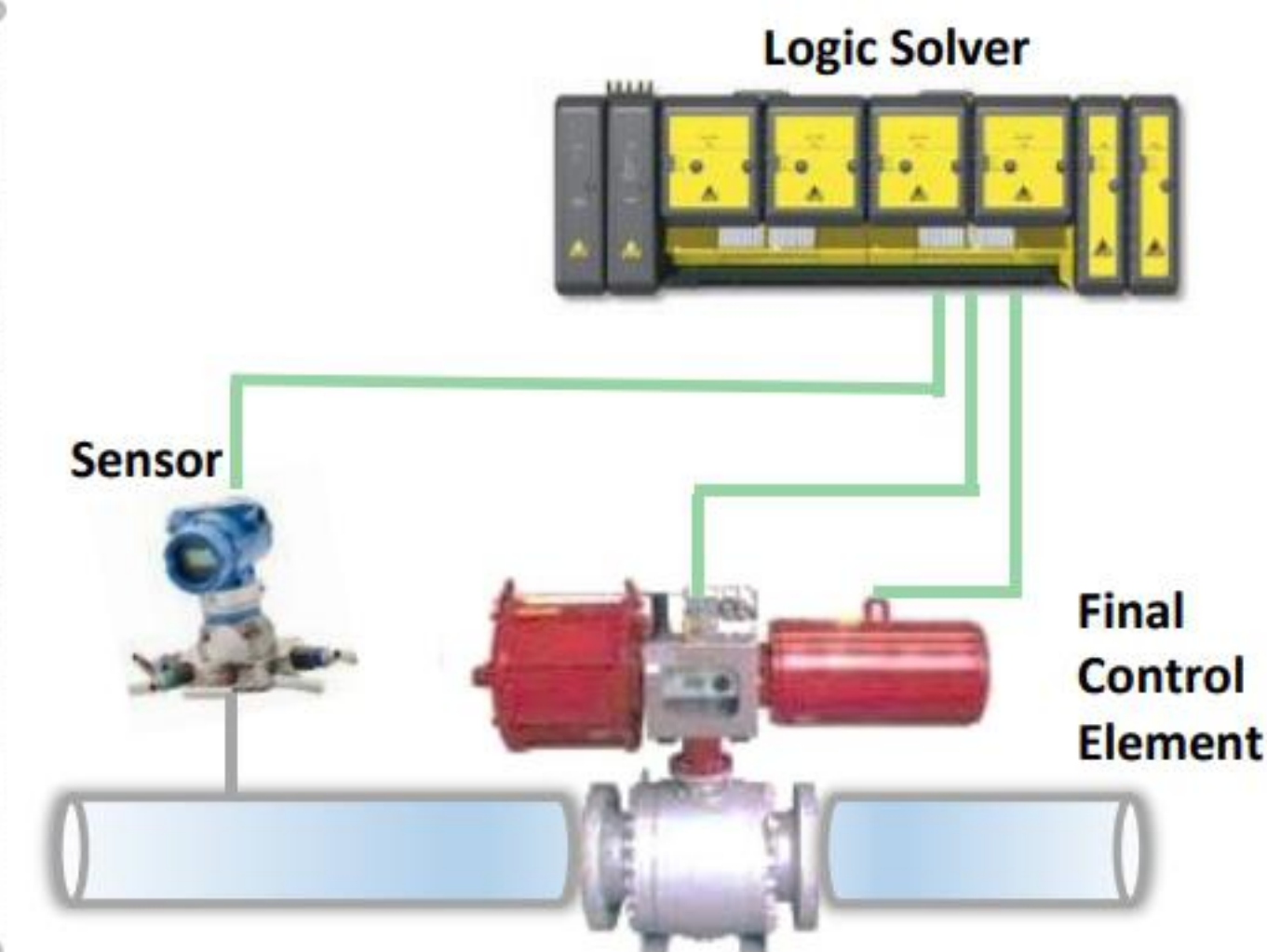
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS - Safety Instrumented Systems (SIS)



- ❑ An SIS is an automated control system designed to **safeguard the manufacturing environment** in case of any hazardous incident in the industry
- ❑ It is an essential component of a **risk management strategy** that uses layers of protection to prevent the operational boundaries of critical processes from reaching an unsafe operating condition

- ❑ An SIS system basically comprises of sensors, logic solvers and final control elements that maintain safe operation of processes by performing the following functions:
 - **Sensors collect information** to determine and measure the process parameters (temperature, pressure, etc.) to predict if the equipment is operating in a safe state or not
 - **Logic solvers act as controllers** that capture signals from the sensors and execute the pre-programmed actions to avoid risk by providing output to the final control elements
 - The **final control elements** implement the actions determined by the logic controller to bring the system to a safe state
- ❑ Typical examples of SIS systems are fire and gas systems, safety interlock systems, safety shutdown systems, etc.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Components of an ICS

An ICS is a broad class of command and control networks and systems that are required to control and monitor every industrial process. Each type of ICS works and functions differently based on the functionality and complexity of the control action.

ICSs can be classified into the following types of most commonly and widely used control systems:

▪ Distributed Control System (DCS)

A DCS is used to control production systems spread within the same geographical location. Such systems are primarily used for large, complex, and distributed processes that are carried out in industries such as chemical manufacturing and nuclear plants, oil refineries, water and sewage treatment plants, electric power generation plants, and automobile and pharmaceutical manufacturing. A DCS is generally a highly engineered and large-scale control system that is often used to perform an industry-specific task. It contains a centralized supervisory control unit used to control multiple local controllers, thousands of input/output (I/O) points, and various other field devices that are part of the overall production process.

To attain the process control, a DCS employs various feedback and feedforward loops along with key product conditions that are established as per the targeted set points. It operates using a centralized supervisory control loop, such as SCADA and MTU, that connects a group of localized controllers such as RTU/PLC to execute the overall tasks required for the working of an entire production process. A high level of redundancy is provided at every level, starting from the I/O of the controllers to the network level. This redundancy helps other processes to continue smoothly in case of any single processor

failure. The primary reason for choosing DCS systems in industry is the adaptability and flexibility that it provides in controlling distributed discrete field devices and their operating stations. Moreover, a DCS is scalable and hence can be arrayed either during initial installation as a large integrated system or as a modular system that can be integrated as per the requirements. DCSs are in a state of constant development as new technologies such as wireless systems and protocols, remote transmission, logging and data historian, and embedded web servers are being included over time.

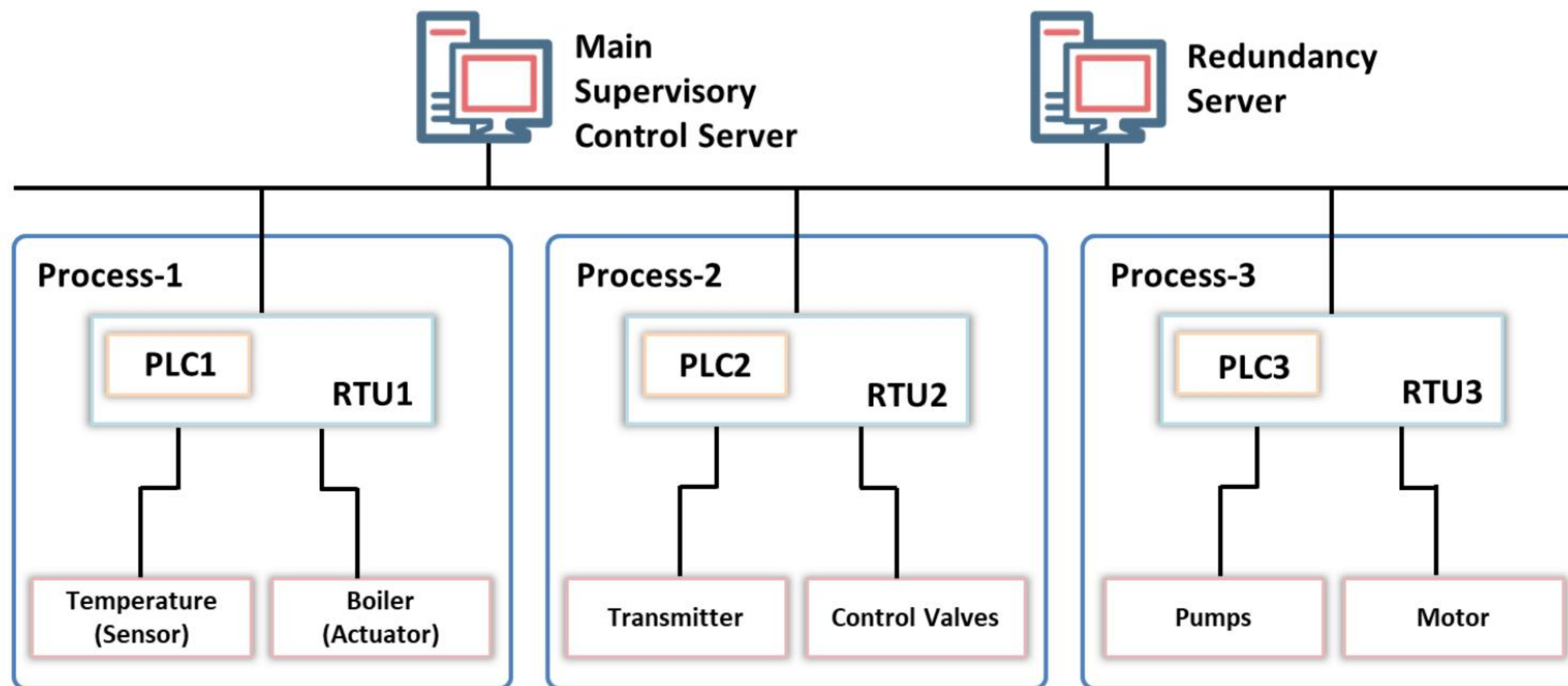


Figure 13.18: DCS architecture

▪ Supervisory Control and Data Acquisition (SCADA)

SCADA is a centralized supervisory control system that is used for controlling and monitoring industrial facilities and infrastructure. Many organizations incorporate SCADA systems for the automation of complex industrial processes, measuring trends in real time, and the detection and correction of problems. Generally, SCADA systems are distributed over a wide geographical area; as a result, various industries rely on SCADA systems for the transportation of oil and gas, wastewater treatment and management, pipeline operations, telecommunications, power grids, building automation, public transportation systems, etc.

The SCADA system is a centralized system that provides supervisory control and also enables real-time acquisition of data from dispersed assets used in industrial processes. It consists of hardware and software components that collect and send data to manage and control processes both locally and at remote locations. The collected data is stored in longtime storage devices such as a data historian to help the operators interpret the data and enable different setpoints. These setpoints help the system in efficiently responding to unusual actions, either by sending commands themselves or sending alerts to an operator.

SCADA systems provide centralized controlling and monitoring of multiple process inputs and outputs by integrating the data acquisition system with the data transmission system and HMI software. SCADA systems collect information from field devices and

transmit it to a central computer system. This information is displayed to the operator in a graphical or textual format, enabling the operator to control and monitor the entire SCADA system from a central location in real time.

The SCADA architecture consists of hardware such as a control server (SCADA-MTU) and communication devices (network cables, radio devices, telephone lines, cables, etc.) along with an array of field sites distributed geographically, consisting of PLCs, RTUs, etc., which are used to monitor and control the operation of industrial equipment. The information from the RTU is controlled and processed by the control server, and the field devices are controlled and monitored by the RTU or PLC. The SCADA software is programmed to inform the entire system regarding what should be monitored, when it should be monitored, and what the acceptable parameter ranges are, in addition to informing the system regarding the response that needs to be initiated when the parameter values exceed the set ranges. An IED may collect the data and transfer it to the control server directly, or a local RTU may instruct the IED to collect the data and send it to the control server. The IED includes a communication interface for monitoring and controlling various sensors and equipment. IEDs are either directly controlled by the control server or include local programming that enables them to act independently without the intervention of the control server. SCADA systems are fault-tolerant systems with redundant systems. This redundancy may not be sufficient to protect SCADA systems from malicious attacks.

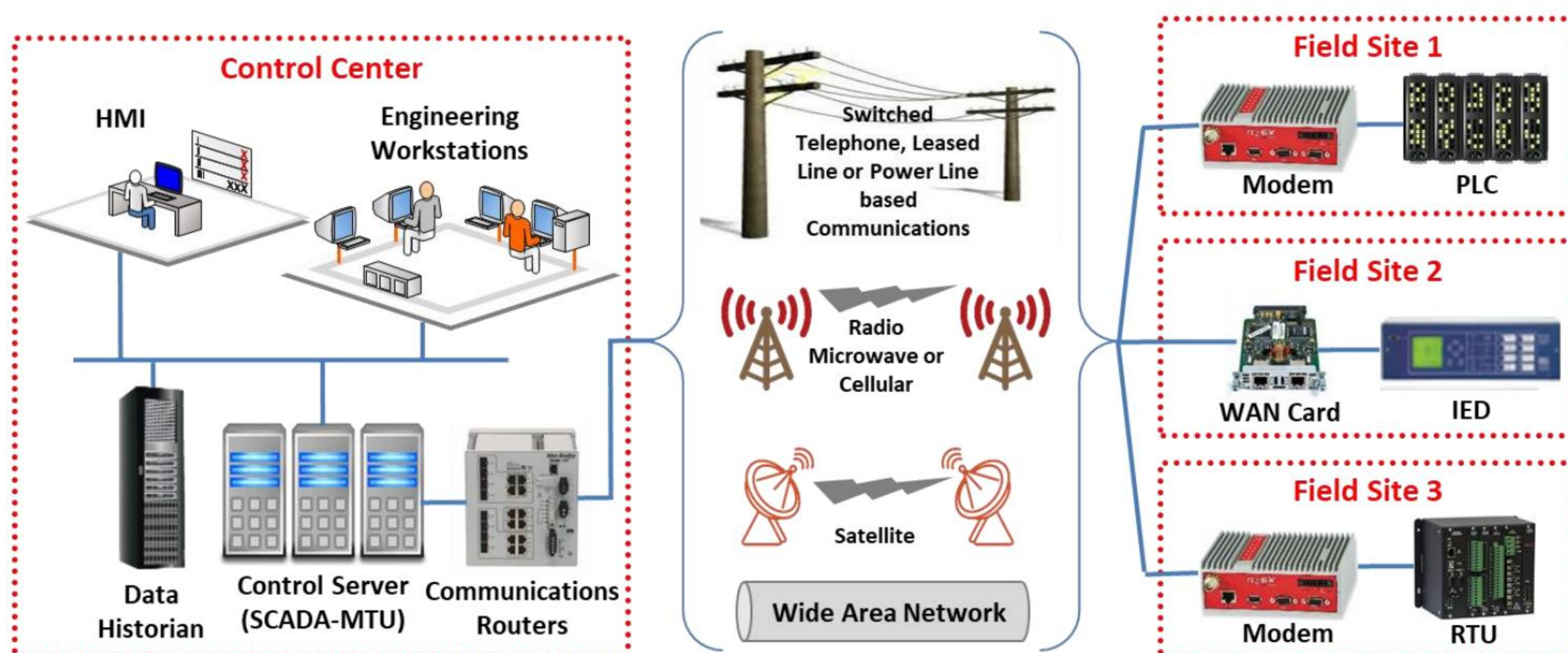


Figure 13.19: SCADA architecture

■ Programmable Logic Controller (PLC)

A PLC is a real-time digital computer used for industrial automation. PLCs are considered more than just digital computers in various industrial control systems due to their extraordinary features such as robust construction, ease of programming, sequential control, ease of hardware use, timers and counters, and reliable controlling capabilities. They are essentially built to survive severe industrial environments. The industries in which PLCs are used include the steel, automobile, energy, chemical, glass, paper, cement manufacturing industries.

The PLC is a small solid-state control computer for which instructions can be customized to perform a specific task. The stored instructions in PLCs can be used to perform specific functions such as logic, timing, counting, I/O control, communication, arithmetic, and file and data processing. The use of PLCs in industry has largely replaced drum sequencers, hard-wired relays, and timers.

PLCs perform continuous monitoring of input values produced by sensors and generate outputs needed for the operation of actuators.

A PLC system consists of three modules:

1. **CPU Module:** The CPU module comprises a central processor and its memory component. The processor is responsible for performing the required data computations and data processing by receiving inputs and producing corresponding outputs. The memory part consists of both RAM and ROM memories. RAM stores user-written programs, whereas ROM stores operating systems, drivers, and application programs. PLCs also include retentive memory that is used to preserve user programs and data when there is a breakage in power supply. This retentive memory helps in resuming the execution of the user program once the power supply returns. For this reason, PLCs generally do not use a monitor or keyboard for reprogramming the processor whenever the power fails.
2. **Power Supply Module:** The power supply module provides the necessary supply of power required for CPU and I/O modules by converting AC to DC. This module is essentially responsible for running the system. A 5 V DC output from the power supply module is used to run the computer circuitry of the PLC, whereas in some PLCs, a 24 V DC output from the power supply module is used to run sensors and actuators.
3. **I/O Modules:** The input and output modules of the PLC system are used in connecting the sensors and actuators with the system for sensing and controlling real-time values such as pressure, temperature, and flow.

There are different types of I/O modules. Some of the most important are discussed below:

- **Digital I/O Module:** Used for the connection of sensors and actuators that are digital in nature (only for switching ON and OFF). These modules work with multiple digital inputs and outputs and support both AC and DC voltages.
- **Analog I/O Module:** Used for the connection of sensors and actuators that provide analog electric signals. This module includes an analog-to-digital converter for converting analog data into digital data. The CPU module processes this digital data.
- **Communication I/O Module:** Used for exchanging information between a communication network and a CPU located at a remote distance.

The main purpose of a PLC is to make machinery and systems work automatically without human intervention. Therefore, a PLC is very important, as it is responsible for all the growth, manufacturing, production, etc.

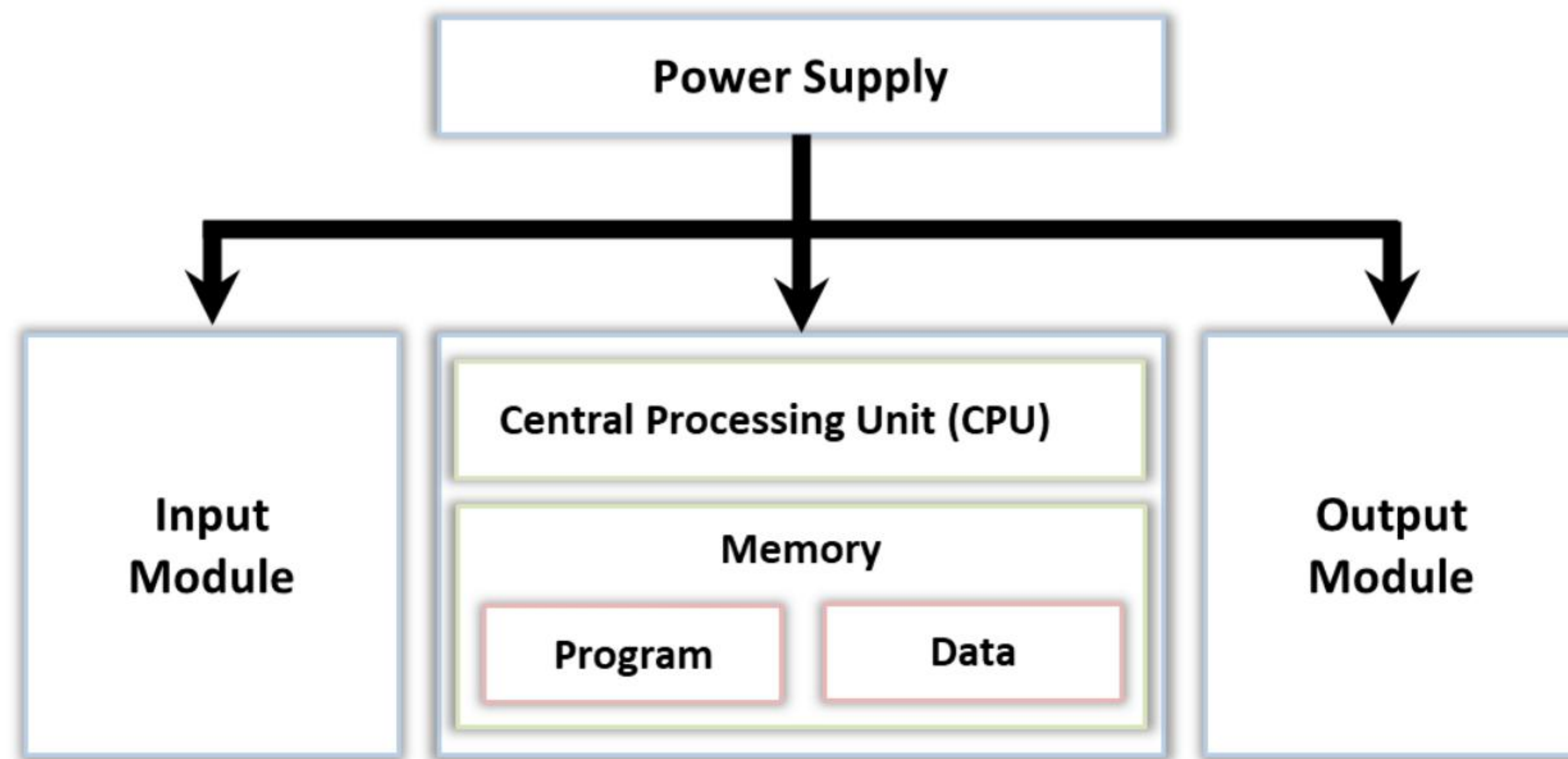


Figure 13.20: PLC architecture

▪ Basic Process Control System (BPCS)

A BPCS is responsible for performing process control and monitoring for industrial infrastructure. It is a system that responds to input signals from processes and associated equipment to generate output signals that allow the process and its associated equipment to operate based on an approved design control strategy. BPCS systems are dynamic in nature and are highly adaptable to changing process conditions. They are applicable to all sorts of control loops, including the temperature, batch, pressure, flow, feedback, and feedforward control loops used in industries such as the chemical, oil and gas, and food and beverages industries.

The use of BPCSs is crucial in industry as they act as the first layer of protection against any unsafe or hazardous condition to the equipment. BPCS systems are often used to push the performance limits to attain the desired performance. BPCSs differ from safety control systems in terms of security, as they lack diagnostic routines to identify any system flaws. However, they can meet a wide range of industrial challenges related to system operation and business monitoring could benefit from a well-designed control system.

Listed below are some of the important functions offered by BPCS:

- Offers trending and alarm/event logging facilities
- Provides an interface from which an operator can monitor and control a system using an operator console (HMI)
- Controls the processes that in turn optimize the plant operation to enhance the quality of the product
- Generates production data reports

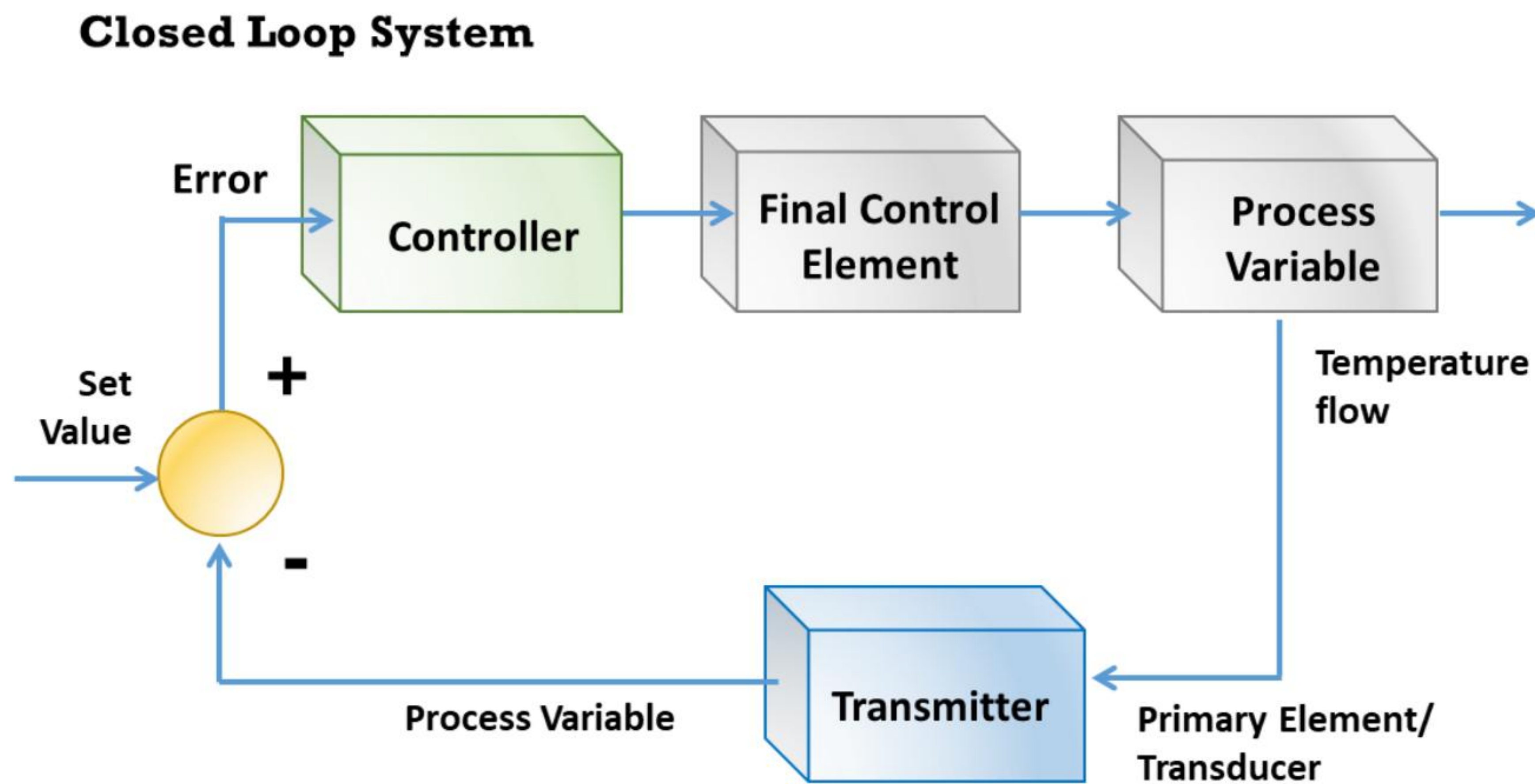


Figure 13.21: BPCS architecture

▪ Safety Instrumented Systems (SIS)

A safety instrumented systems (SIS) is an automated control system designed to safeguard the manufacturing environment in case of any hazardous incident in industry. They monitor and perform “specific control functions” to shut down the monitored system or bring it to a predefined safe state to reduce the adverse impacts of an incident. They function as an essential component of a risk management strategy that uses layers of protection to prevent the operational boundaries of the critical process from reaching an unsafe operating condition. Typical examples of SIS systems are fire and gas systems, safety interlock systems, safety shutdown systems, etc.

In industry, an SIS overrides the BPCS operationally and functions when BPCS does not operate a process within the normal operational parameters. For a given condition, if BPCS starts operating beyond normal operational limits, the SIS provides an automated control environment to detect and respond to the critical process. SIS either preserves the state or changes it to a safe state, i.e., equipment or process shutdown. Finally, the last layer of protection is applied where devices like relief valves, rupture disks, flare systems, etc. are used before the process enters the unsafe operating limits. The events generated and actions performed by the SIS system are illustrated in the diagram:

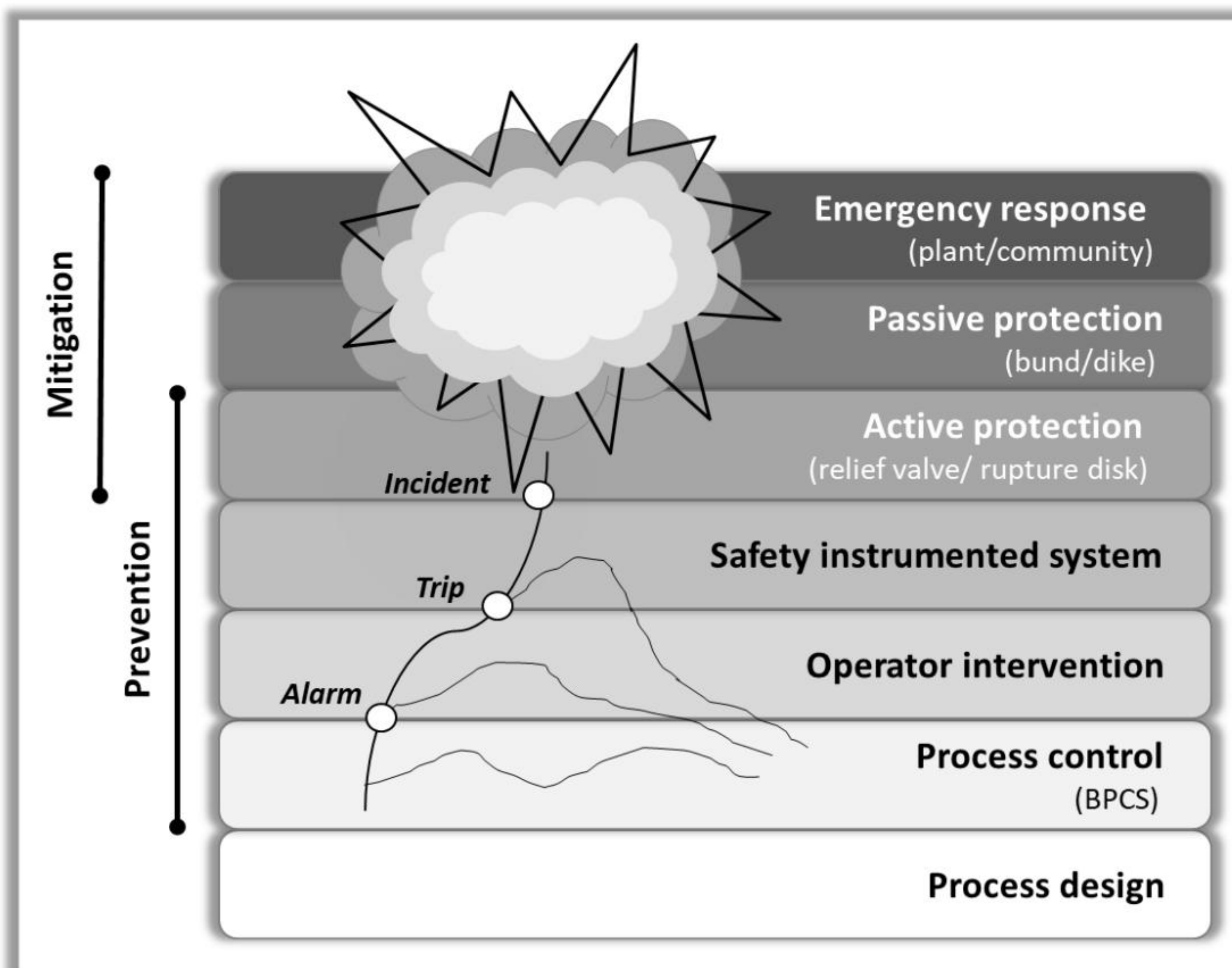


Figure 13.22: Layers of protection provided by SIS systems

The functional requirements of the work performed by SIS and how efficiently it should be carried out can be determined from Hazard and Operability Studies (HAZOP), Layers of Protection Analysis (LOPA), risk graphs, etc. The SIS system works independently from other control systems. It consists of sensors, logic solvers, and final control elements that maintain safe operation of the process by performing the following functions:

- **Field sensors** collect information to determine and measure process parameters such as temperature, pressure, flow, etc. to predict whether the equipment is operating in a safe state or not. Different types of sensor are available, such as pneumatic, electric switches, smart transmitters, etc.
- **Logic solvers** are helpful in deciding the necessary action to be taken based on the gathered information. They provide actions for both failsafe and fault-tolerant situations. They act as controllers that capture signals from the sensors and execute pre-programmed actions to avoid risk by providing output to the final control elements.
- **Final control elements** implement the actions determined by the logic controller to bring the system to a safe state. These elements generally comprise pneumatically activated on-off valves controlled by solenoid valves.

As no component in a system can be completely immune to failure, it is essential for industries to test SIS systems constantly. It is also important to conduct an assessment of its basic cybersecurity environment to ensure the smooth operations of the SIS. The main aim of assessing the working conditions of the SIS system is to guarantee safety and of the SIS so that it remains at its actual design levels.

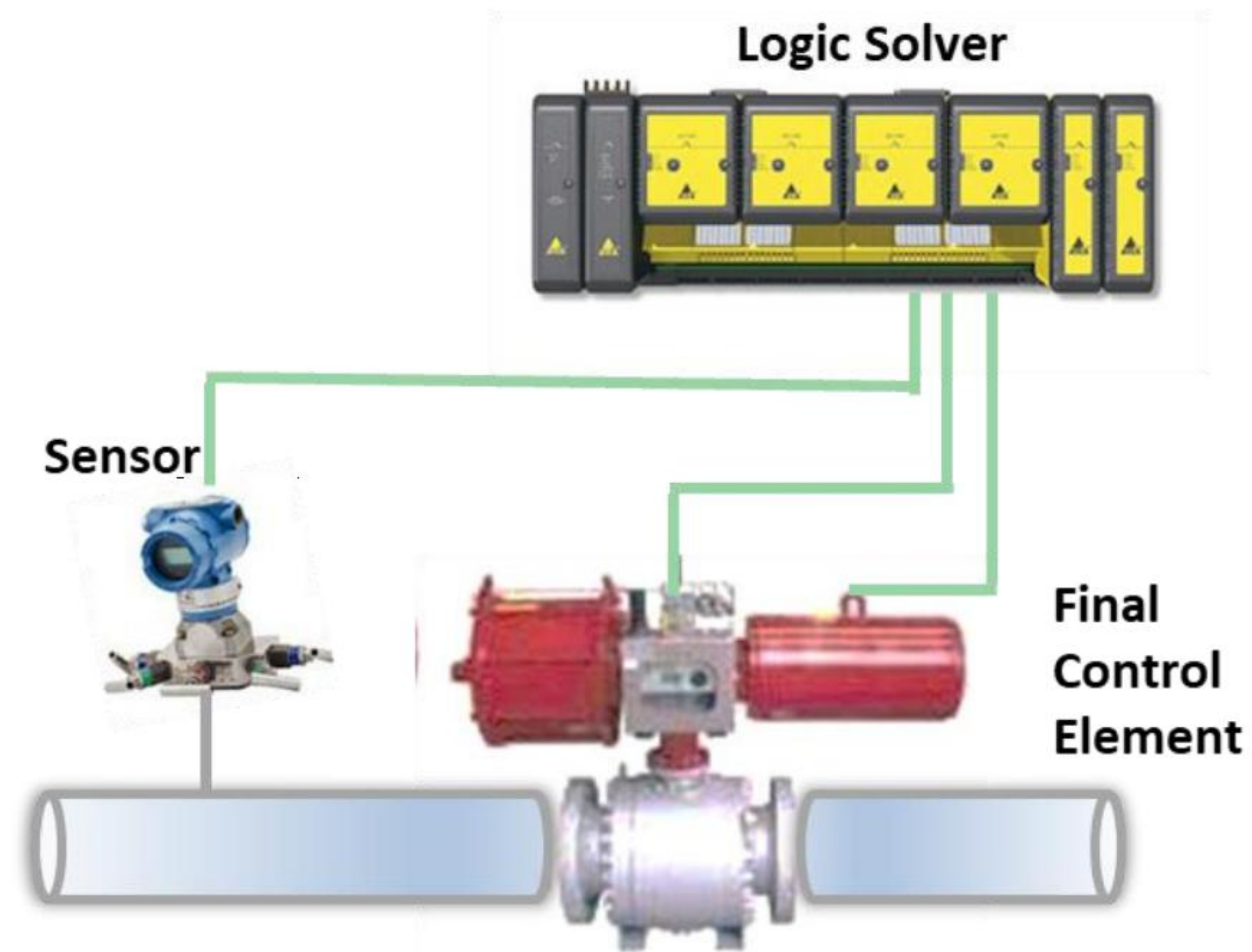
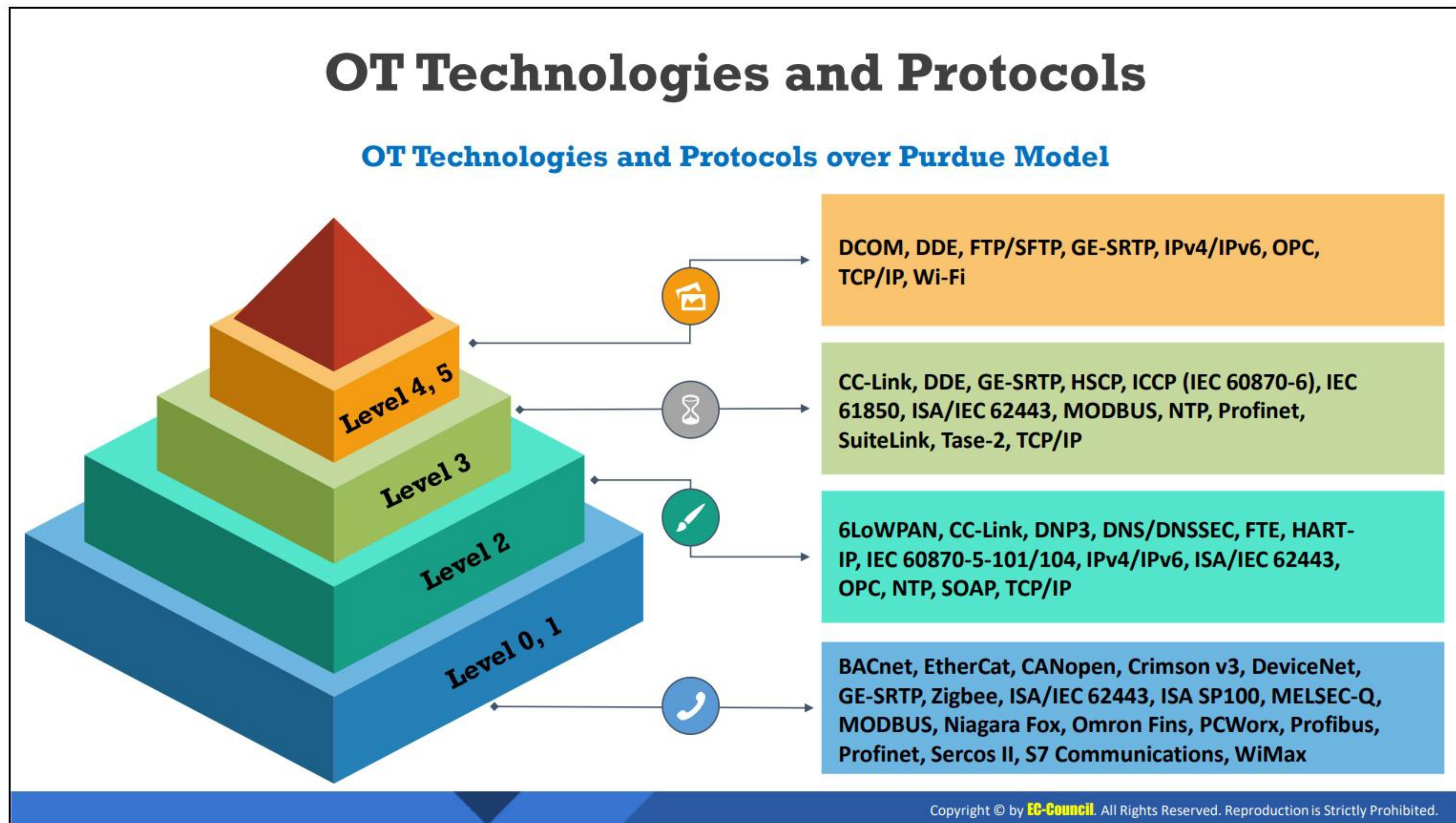


Figure 13.23: SIS architecture



OT Technologies and Protocols

Industrial network protocols constitute the real-time interconnectivity and information exchange between industrial systems and zones. These network protocols are deployed across the ICS network in any industry. To understand any industrial network, a security engineer needs to understand the protocols existing beneath the networks.

The key communication technologies and protocols of the OT network over the Purdue model defined by ISA-95 are as follows:

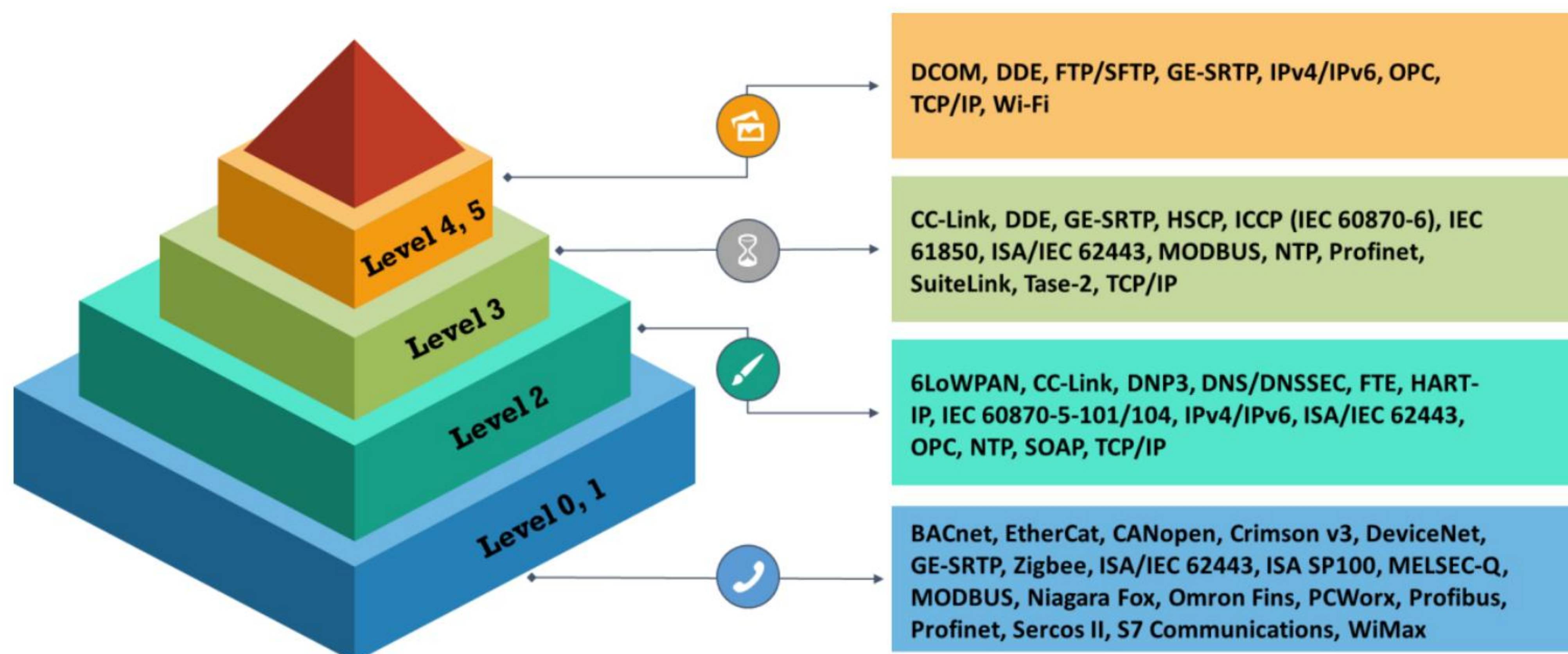


Figure 13.24: OT technologies and protocols over the Purdue model

Protocols used in Level 4 and 5

- **DCOM:** DCOM (Distributed Component Object Model) is Microsoft's proprietary software that enables software components to communicate directly over a network reliably and securely.
- **DDE:** DDE (Dynamic Data Exchange) is used for IPC (Inter-Process Communication).
- **FTP/SFTP:** FTP establishes a connection to the specific server or computer, and it is also used to download or transfer files. SFTP verifies the identity of the client, and once a secured connection is established information is exchanged.
- **GE-SRTP:** GE-SRTP (Service Request Transport Protocol), developed by GE Intelligent Platforms, is used to transfer data from PLCs, and runs on a selected number of GE PLCs that turn digital commands into physical actions.
- **IPv4/IPv6:** IPv4 is a connectionless protocol used in packet-switched networks. IPv6 is used for packet-switched internetworking, which provides end-to-end datagram transmission across multiple IP networks.
- **OPC:** OPC (Open Platform Communications) is a set of client/server protocols designed for the communication of real-time data between data acquisition devices like PLCs and interface devices like HMIs.
- **TCP/IP:** TCP/IP is a suite of communication protocols used for the interconnection of networking devices over the Internet.
- **Wi-Fi:** Wi-Fi is a technology that is widely used in wireless local area networking or LAN. The most common Wi-Fi standard used in homes or companies is 802.11n, which offers a maximum speed of 600 Mbps and a range of approximately 50 m.

Protocols used in Level 3

- **CC-Link:** A CC-Link (Control and Communications Link) is an open industrial network that enables devices from different manufacturers to communicate. It is used in machine, process control, and building automation.
- **HSCP:** Hybrid SCP (Secure Copy Protocol) is developed for transmitting larger file sizes at high speed on long-distance and wideband infrastructure.
- **ICCP (IEC 60870-6):** ICCP (Inter-Control Center Communications Protocol) (IEC 60870-6) provides a set of standards and protocols for covering ICS or SCADA communication in power system automation.
- **IEC 61850:** IEC 61850 is a common protocol that enables interoperability and communications between the IEDs at electrical substations.
- **ISA/IEC 62443:** ISA/IEC 62443 provides a flexible framework for addressing and mitigating current and future security vulnerabilities in industrial automation and control systems.
- **Modbus:** Modbus is a serial communication protocol that is used with PLCs and enables communication between many devices connected to the same network.

- **NTP:** NTP (Network Time Protocol) is a networking protocol that is used for clock synchronization between computer systems over packet-switched and variable-latency data networks.
- **Profinet:** Profinet is a communication protocol used to exchange data between controllers like PLCs and devices like RFID readers.
- **SuiteLink:** SuiteLink protocol is based on TCP/IP and runs as a service on Windows operating systems. It is mostly used in industrial applications that value time, quality, and high throughput.
- **Tase-2:** Tase-2, also referred to as IEC 60870-6, is an open communication protocol that enables the exchange of time-critical information between control systems through WAN and LAN.

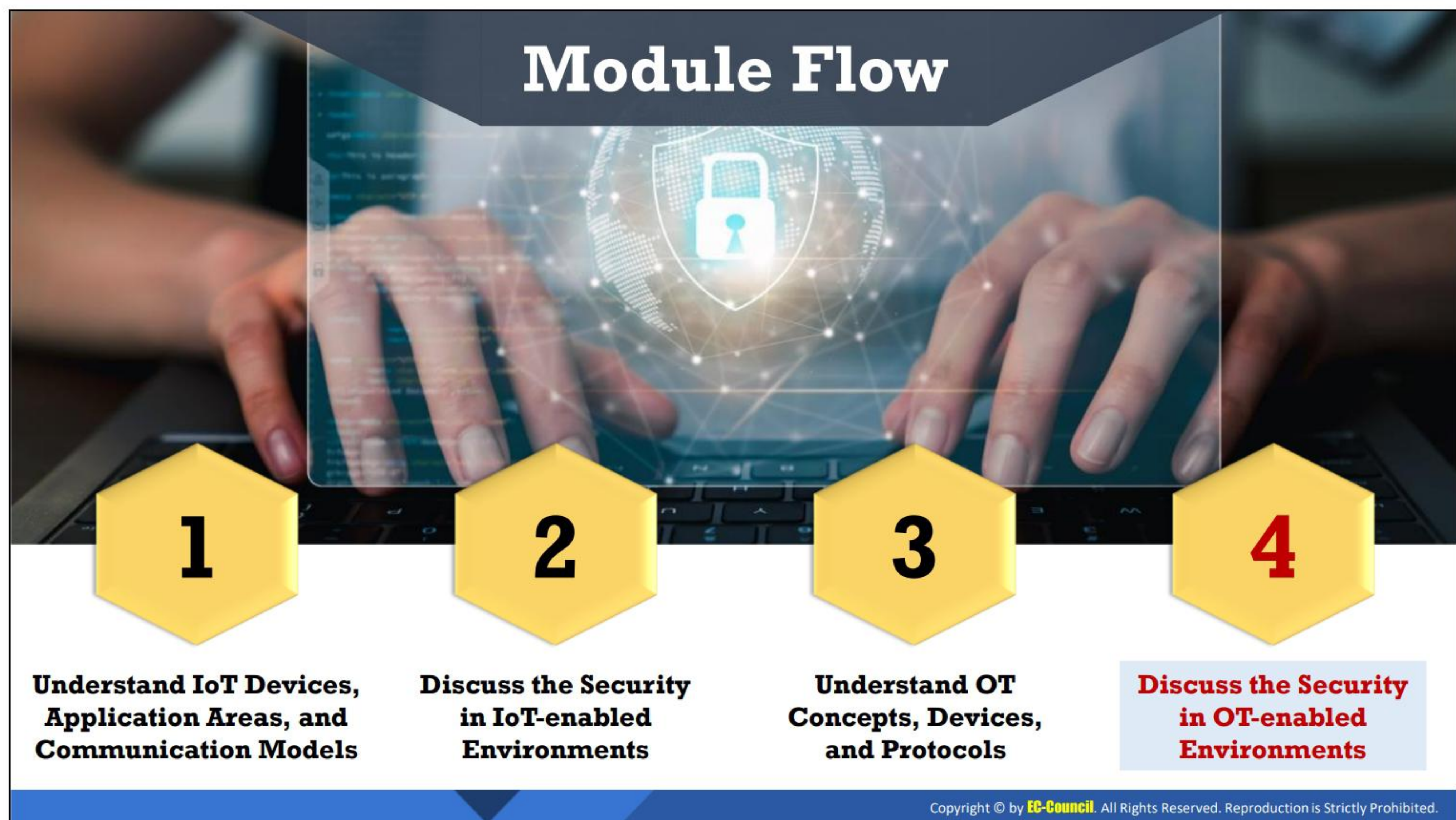
Protocols used in Level 2

- **6LoWPAN:** IPv6 over Low Power Personal Area Networks (6LoWPAN) is an Internet Protocol used for communication between smaller and low-power devices with limited processing capacity; it is mainly used for home and building automation.
- **DNP3:** DNP3 (Distributed Network Protocol 3) is a communication protocol used to interconnect components within process automation systems.
- **DNS/DNSSEC:** Domain Name System Security Extensions (DNSSEC) provide a way to authenticate DNS response data and can secure information provided by DNS.
- **FTE:** Fault Tolerant Ethernet (FTE) is designed to provide rapid network redundancy, and each node is connected twice to a single LAN through dual network interfaces.
- **HART-IP:** The HART-IP protocol is used to integrate WirelessHART gateways and HART multiplexers tightly and efficiently for sending and receiving digital information.
- **IEC 60870-5-101/104:** This is an extension of the IEC 101 protocol with some modifications in transport, network, link, and physical layer services. It enables communication between the control station and substation through the standard TCP/IP network.
- **SOAP:** SOAP (Simple Object Access Protocol) is a messaging protocol containing a stern set of rules that can administrate data transfer between client and server using the XML message format.

Protocols used in Level 0 and 1

- **BACnet:** BACnet (Building Automation and Control network) is a data communication protocol designed for building automation and control networks that implements standards such as ASHRAE, ANSI, and ISO 16484-5.
- **EtherCAT:** Ethernet for Control Automation Technology (EtherCAT) is an Ethernet-based fieldbus system that is appropriate for both hard and soft real-time computing necessities in automation technology.

- **CANopen:** CANopen is a high-level communication protocol based on the CAN (Controller Area Network) protocol. It is used for embedded networking applications like vehicle networks.
- **Crimson:** Crimson is the common programming platform used for a variety of Red Lion products such as G3 and G3 Kadet series HMIs, Data Station Plus, Modular Controller, and the Productivity Station.
- **DeviceNet:** DeviceNet is another variant of the Common Industrial Protocol (CIP) that is used in the automation industry for interconnecting control devices to exchange data.
- **Zigbee:** Zigbee is a short-range communication protocol that is based on IEEE 203.15.4 standard. Zigbee is used for devices that transfer data intermittently at a low data rate in a restricted area and within a range of 10–100 m.
- **ISA SP100:** ISA SP100 is a committee for establishing the industrial wireless standard ISA100. ISA100 is used for the industrial manufacturing environment and process automation industry.
- **MELSEC-Q:** MELSEC-Q provides an open and seamless network environment integrating different levels of automation networks such as CC-Link IE, high-speed, and large-capacity ethernet-based integrated open networks.
- **Niagara Fox:** Niagara Fox protocol is a building automation protocol used between the Niagara software systems developed by Tridium.
- **Omron Fins:** Omron Fins is used by PLC programs for transferring data and performing other services with remote PLC connected on an Ethernet network. It can also be used by remote devices such as FieldServer for transferring data.
- **PCWorx:** PCWorx is used in many ICS components, and they make a series of inline controllers (ILCs). These controllers allow the use of different ICS protocols and some common TCP/IP protocols.
- **Profibus:** Profibus is more complex than Modbus, and is designed and developed to address interoperability issues. It is employed in process automation and factory automation fields.
- **Sercos II:** The serial real-time communication system (Sercos II) comprises a digital drive interface appropriate for use in industrial machines. It is used in complex motion control applications with high specification designs.
- **S7 Communication:** S7 Communication is a Siemens proprietary protocol that runs between programmable logic controllers (PLCs) of the Siemens S7-300/400 family and is used in PLC programming and for accessing PLC data from SCADA.
- **WiMax:** Worldwide Interoperability for Microwave Access (WiMax) is based on the standard IEEE 802.16 and is envisioned for wireless metropolitan area networks. WiMax operates at frequencies between 2.5 GHz and 5.8 GHz with a transfer rate of 40 Mbps.



Discuss the Security in OT-enabled Environments

This section discusses various OT vulnerabilities and their solutions, security measures based on the Purdue model, international OT security organizations, OT security solutions, and tools. Following the security measures, organizations can implement proper security mechanisms to protect critical industrial infrastructure and associated IT systems from various cyber-attacks.

OT Vulnerabilities and Solutions

Vulnerability	Solutions
1. Publicly Accessible OT systems	<ul style="list-style-type: none"> Implement multi-factor authentication Use enterprise-grade firewall and remote access solution
2. Insecure Remote Connections	<ul style="list-style-type: none"> Use strong multifactor authentication mechanism and password policies Implement appropriate security patching practices
3. Missing Security Updates	<ul style="list-style-type: none"> Test applications in the sandbox environment before launching it live Employ a firewall and perform device hardening
4. Weak Passwords	<ul style="list-style-type: none"> Use separate username conventions for the corporate IT and OT networks Change default credentials at the installation time Perform security audits to meet compliance with secure password policies
5. Insecure Firewall Configuration	<ul style="list-style-type: none"> Implement secure firewall configuration Configure the access control list on the firewall

Vulnerability	Solutions
6. OT Systems Placed within the Corporate IT Network	<ul style="list-style-type: none"> Segregate the corporate IT and OT devices Establish a DMZ for all connections in the IT and OT systems
7. Insufficient Security for Corporate IT Network from OT Systems	<ul style="list-style-type: none"> Restrict access on the IT-OT network, based on the business need Establish a secure gateway between the two networks
8. Lack of Segmentation within OT Networks	<ul style="list-style-type: none"> State clear separation between critical and non-critical systems Implement zoning model that uses a defense-in-depth approach
9. Lack of Encryption and Authentication for Wireless OT Networks	<ul style="list-style-type: none"> Use strong wireless encryption protocols Use industry-standard cryptographic algorithms Conduct regular security audits
10. Unrestricted Outbound Internet Access from OT Networks	<ul style="list-style-type: none"> Conduct a formal risk assessment Monitor and segregate OT systems from external access Download security updates in a separate repository outside the OT network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Vulnerabilities and Solutions

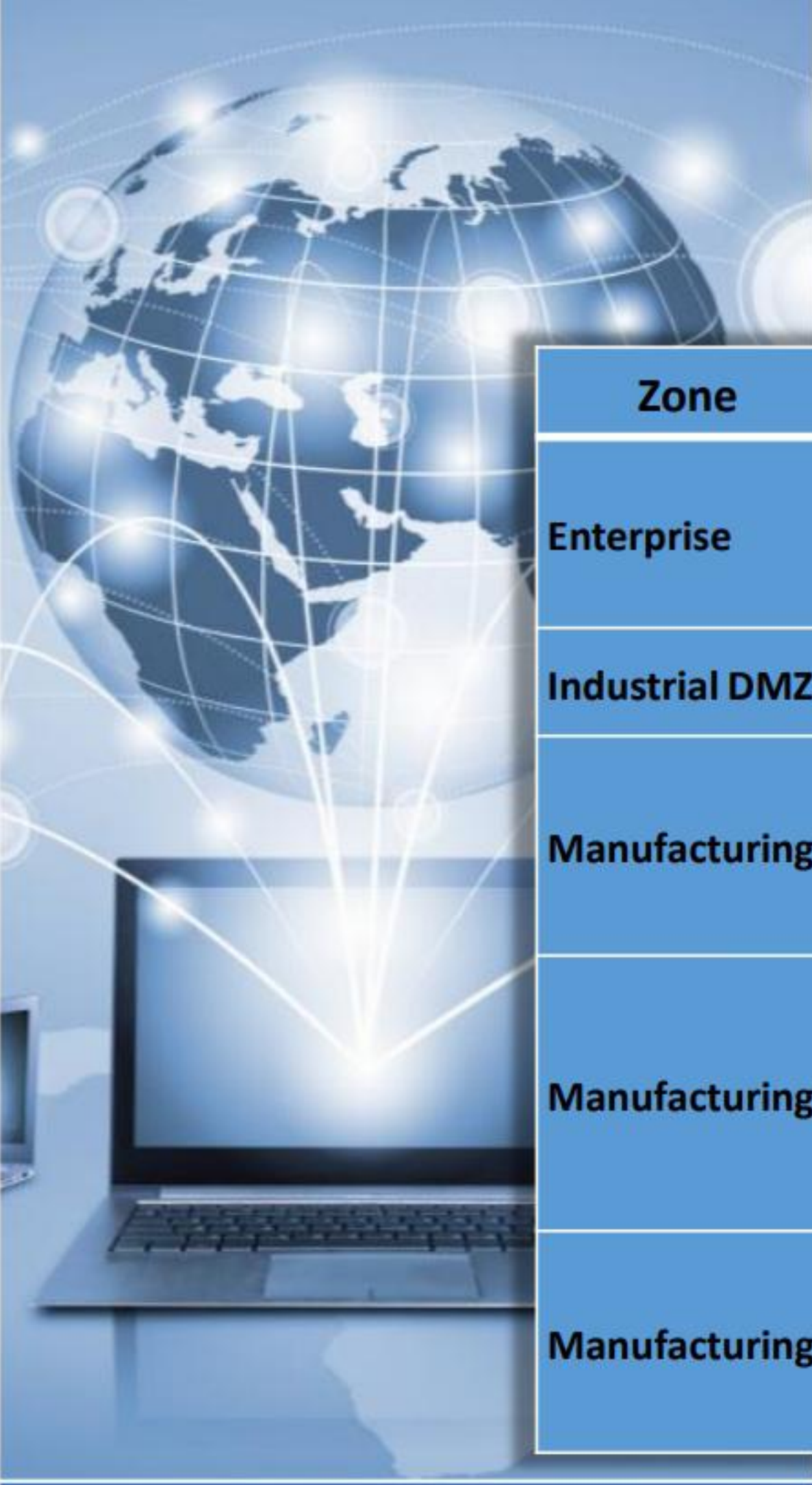
Vulnerabilities in industrial systems such as ICS/SCADA, PLC, and RTU pose a significant threat to the associated critical infrastructure. Organizations need to incorporate appropriate security controls and mechanisms to protect such systems from various cyber-attacks.

Discussed below are some of the most common OT vulnerabilities and solutions:

Vulnerability	Solutions
1. Publicly Accessible OT Systems	<ul style="list-style-type: none"> Implement multi-factor authentication Use enterprise-grade firewall and remote access solutions
2. Insecure Remote Connections	<ul style="list-style-type: none"> Use a strong multifactor authentication mechanism and robust password policies Implement appropriate security patching practices
3. Missing Security Updates	<ul style="list-style-type: none"> Test applications in a sandbox environment before launching them live Employ a firewall and perform device hardening
4. Weak Passwords	<ul style="list-style-type: none"> Use separate username conventions for the corporate IT and OT networks Change default credentials at time of installation Perform security audits to meet compliance with secure password policies for both IT and OT networks
5. Insecure Firewall Configuration	<ul style="list-style-type: none"> Implement secure firewall configuration Configure the access control lists on the firewall

6. OT Systems Placed within the Corporate IT Network	<ul style="list-style-type: none"> ▪ Segregate the corporate IT and OT devices ▪ Establish a DMZ (demilitarized zone) for all connections in the IT and OT systems ▪ Regularly monitor the DMZ
7. Insufficient Security for Corporate IT Network from OT Systems	<ul style="list-style-type: none"> ▪ Restrict access on the IT/OT network, based on the business need ▪ Establish a secure gateway between the OT and IT networks ▪ Perform regular risk assessment
8. Lack of Segmentation within OT Networks	<ul style="list-style-type: none"> ▪ State clear separation between critical and non-critical systems ▪ Implement a zoning model that uses a defense-in-depth approach
9. Lack of Encryption and Authentication for Wireless OT Networks	<ul style="list-style-type: none"> ▪ Use strong wireless encryption protocols ▪ Use industry-standard cryptographic algorithms ▪ Conduct regular security audits
10. Unrestricted Outbound Internet Access from OT Networks	<ul style="list-style-type: none"> ▪ Conduct a formal risk assessment ▪ Closely monitor and segregate OT systems from external access ▪ Download security updates in a separate repository outside the OT network

Table 13.2: OT vulnerabilities and solutions



How to Secure an IT/OT Environment

Security Controls based on Purdue Model

Zone	Purdue Level	Attack vector	Risks	Security Controls
Enterprise	5 & 4 (Enterprise network and Business Logistics Systems)	Spear phishing, Ransomware	Abusing infrastructure, access to the network	Firewalls, IPS, Anti-bot, URL filtering, SSL inspection, Antivirus
Industrial DMZ	3.5 (IDMZ)	DoS attacks	Malware injections, network infections	Anti-DoS solutions, IPS, Antibot, Application control
Manufacturing	3 (Operational Systems)	Ransomware, Bot infection, Unsecured USB ports	Altering industrial process, industrial spying, unpatched monitoring systems	Anti-bot, IPS, Sandboxing, Application control, Traffic encryption, Port protection
Manufacturing	2 & 1 (Control Systems & Basic Controls)	DoS exploitation, Unencrypted protocols, Default credentials, Application and OS vulnerabilities	Altering industrial process, industrial spying	IPS, Firewall, Communication encryption using IPsec, Security gateways, Use of authorized RTU and PLC commands
Manufacturing	0 (Physical process)	Physical security breach	Modifications or disruption in the physical process	Point to point communication, MAC authentication, additional security gateways at level 1 & 0

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

How to Secure an IT/OT Environment

IT/OT convergence is widely being adopted in industries such as traffic control systems, power plants, manufacturing companies, etc. These IT/OT systems are often targeted by the attackers to discover the underlying vulnerabilities and indulge in cyber-attacks. Based on the Purdue model, the IT/OT environment is divided into several levels, and each level is required to be secured with proper security measures.

The table below describes various attacks on different Purdue levels of an IT/OT environment, associated risks, and security controls to fortify the network against cyber-attacks:

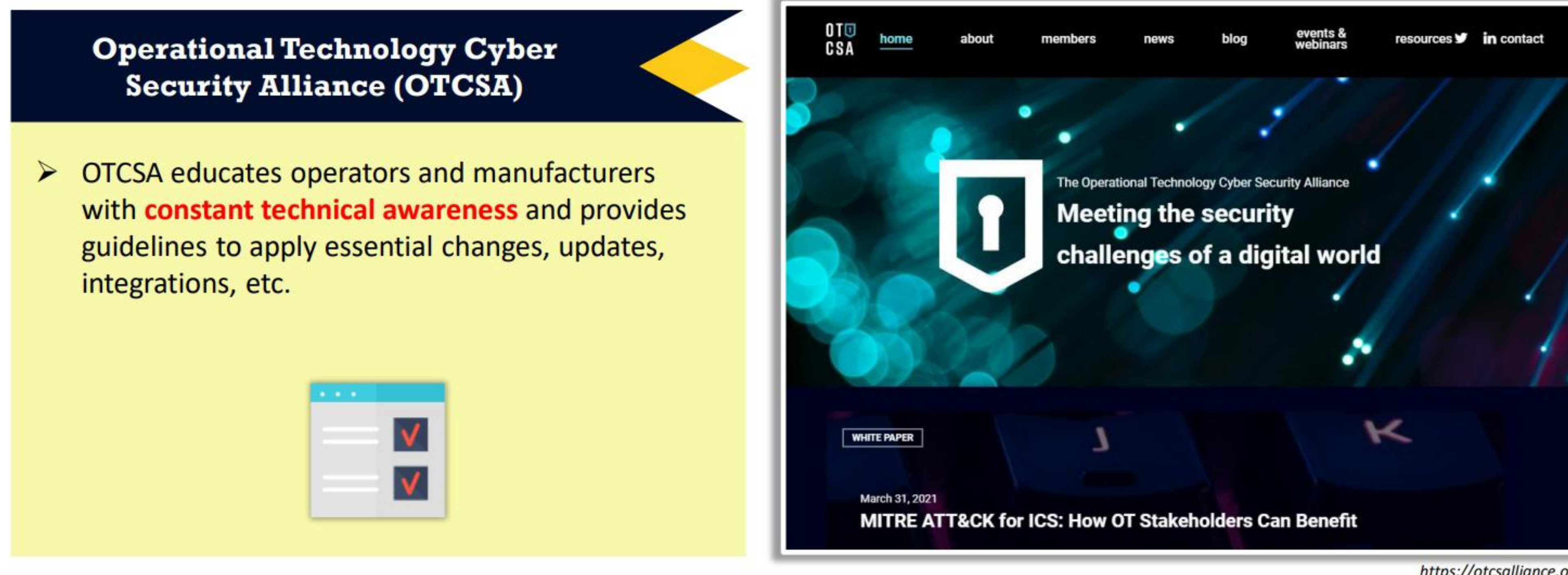
Zone	Purdue Level	Attack Vector	Risks	Security Controls
Enterprise	5 & 4 (Enterprise Network and Business Logistics Systems)	Spear phishing, Ransomware	Abusing infrastructure, Access to the network	Firewalls, IPS, Anti-bot, URL filtering, SSL inspection, Antivirus
Industrial DMZ	3.5 (IDMZ)	DoS attacks	Malware injections, Network infections	Anti-DoS solutions, IPS, Antibot, Application control
Manufacturing	3 (Operational Systems)	Ransomware, Bot infection, Unsecured USB ports	Altering industrial process, Industrial spying, Unpatched monitoring systems	Anti-bot, IPS, Sandboxing, Application control, Traffic encryption, Port protection

Manufacturing	2 & 1 (Control Systems and Basic Controls)	DoS exploitation, Unencrypted protocols, Default credentials, Application and OS vulnerabilities	Altering industrial process, Industrial spying	IPS, Firewall, Communication encryption using IPsec, Security gateways, Use of authorized RTU and PLC commands
Manufacturing	0 (Physical process)	Physical security breach	Modifications or disruption to the physical process	Point-to-point communication, MAC authentication, Additional security gateways at levels 1 and 0

Table 13.3: Attacks on different Purdue levels

International OT Security Organizations

- ❑ Global cybersecurity organizations such as **OTCSA** and **OT-ISAC** are committed to providing appropriate security policies and insights into improving the security resilience of critical infrastructures



Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

International OT Security Organizations

As OT is being widely spread and interconnected with IT, security researchers need to be more cautious and implement strong security policies to strengthen the OT networks. Some global cybersecurity organizations are committed to providing appropriate security policies and insights into improving the security resilience of critical infrastructures.

Listed below are a few international organizations that alert companies of threats and provide IT/OT solutions to protect the OT industries against cyber-attacks.

- **OTCSA**

Source: <https://otcsalliance.org>

The Operation Technology Cybersecurity Alliance (OTCSA) educates operators and manufacturers with constant technical awareness and provide guidelines to apply essential changes, updates, integrations, etc. The security team in OTCSA also provides support in understanding OT security challenges and solutions to safeguard the assets of the industry.

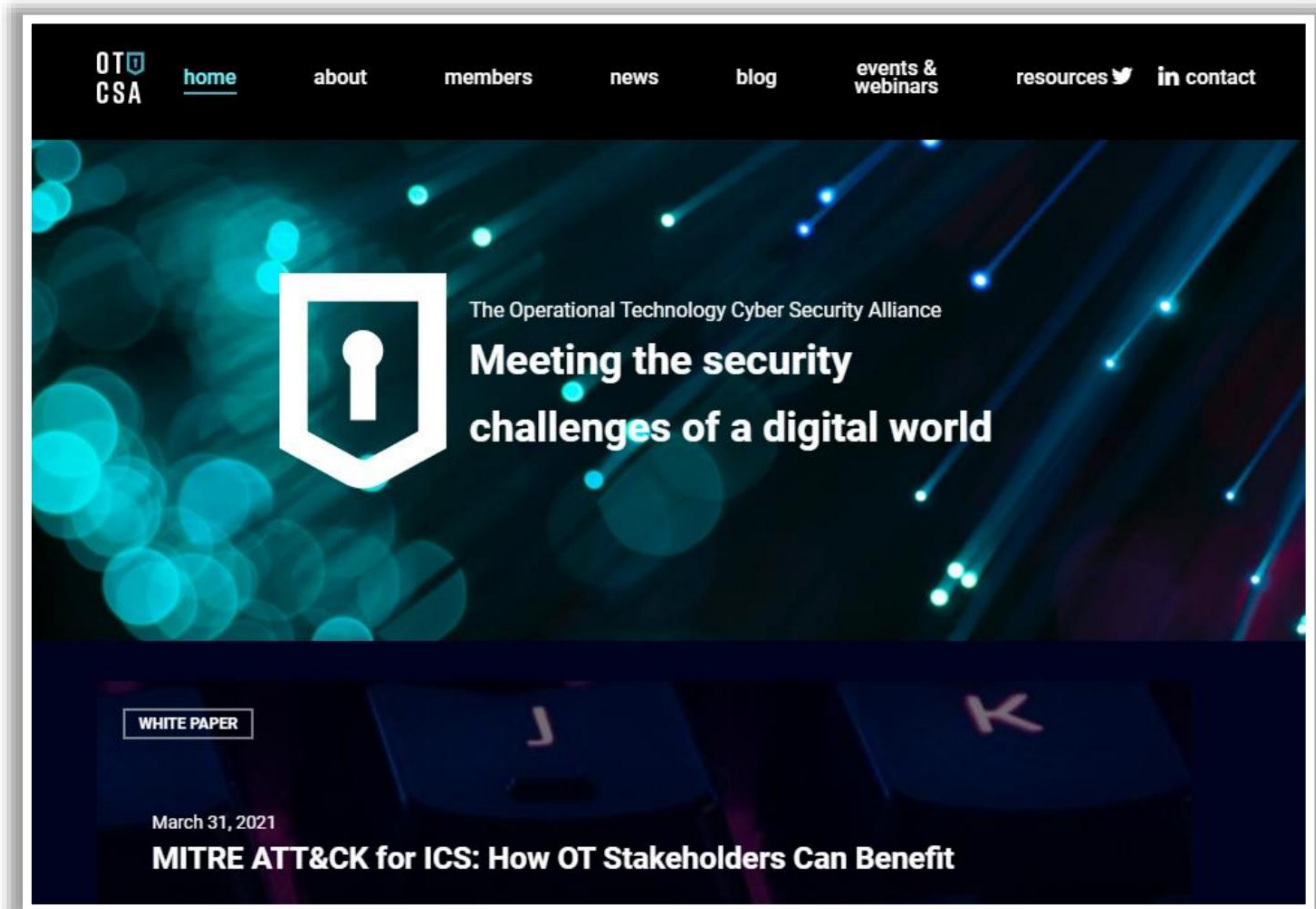


Figure 13.25: Screenshot of OTCSA






- **OT-ISAC**

Source: <https://www.otisac.org>

The Operational Technology Information Sharing and Analysis Center (OT-ISAC) is a core hub to share threat information among OT industries such as energy and water utility sectors. The organization offers various tools and techniques to exchange information securely between the OT/IT spectrum to protect industrial systems or networks against malicious intrusions. Being associated with various information sharing centers, the OT-ISAC obtains information regarding imminent threats and provides timely solutions to fortify the industrial systems of registered companies.



Figure 13.26: Screenshot of OT-ISAC

OT Security Solutions	
	Firewalls <ul style="list-style-type: none"> Firewalls are used in the network for monitoring and controlling the incoming and outgoing network traffic You can use firewall solutions such as SCADAWall, and Waterfall for securing the OT network
	Unified Identity and OT Access Management <ul style="list-style-type: none"> Access management helps industries to centralize certain operations like adding, securing, changing, and removing user access to the OT systems You can use tools such as OTaccess, and FireEye for identifying and managing access to industrial systems
	Asset Inventory and Device Authorization <ul style="list-style-type: none"> Asset inventory helps in connecting only authorized devices to the network and detect vulnerabilities in the devices You can use tools such as SCADAfence, and CyberLens for asset inventory and device authorization
	OT Network Monitoring and Anomaly Detection <ul style="list-style-type: none"> OT network monitoring employs machine learning algorithms for easy detection and identification of malicious behaviors You can use tools such as Claroty, and OT ThreatFeed for OT network monitoring and anomaly detection
	Decoys to Deceive Attackers <ul style="list-style-type: none"> Decoys are honeypots used in OT environments to lure attackers to reveal their presence and activities You can use decoy tools such as ThreatDefend, Conpot, and GasPot for protecting the network

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Security Solutions

The industrial and corporate sectors are rapidly digitizing their operational value chain, giving access to OT devices from a broader range of the Internet. The cost of managing security in the heavy industrial sectors is being largely overlooked, leading to several security challenges. Hence, it is considered safer for all the industrial sectors to invest in cybersecurity programs and solutions.

Cybersecurity professionals should deploy solutions by sensibly examining the recent cybersecurity challenges and requirements they face in the current trend that can be combined with suitable operational changes. Hence many incumbent OEM providers and start-ups have developed several recent tactics and technologies for protecting the OT environment.

As the heavy industries have a decentralized nature, the security solutions can be integrated into all technology-linked decisions across IT and OT. In addition, the second line of defense can be implemented by using Information Risk Management (IRM). Some industries also provide a third line of defense by implementing internal audit functions.

Some of the emerging technology solutions used by organizations to protect the OT environment are as follows:

▪ Firewalls

Firewalls are used in a network for monitoring and controlling the incoming and outgoing network traffic. Firewalls help in improving security controls by inspecting the traffic that traverses the gateway between the OT and IT networks. They can also help in identifying and blocking new threats. Thus, the attacker can be limited from traversing between the networks after compromising a system. It is also advisable to employ the critical assets and systems in a DMZ away from the SCADA systems.

Security professionals can use tools such as SCADAWall, Waterfall, and Palo Alto NGFW for protecting the network.

- **Unified Identity and OT Access Management**

Access management helps industries to centralize certain operations like adding, securing, changing, and removing user access to the OT systems. All this data is linked with the organization's identity-management system, which can provide strong authentication. The access management helps minimize the attack risk by providing the least privileges to superuser accounts. This helps the security personnel to trace the critical assets and helps in identifying the attack sources.

Security professionals can use tools such as OTaccess, FireEye, etc. for identifying and managing access to industrial systems.

- **Asset Inventory and Device Authorization**

Asset inventory helps in connecting only authorized devices to the OT network, and it can detect all the connected devices. It can also detect the vulnerabilities in the devices, which are categorized based on the device manufacturer, version, and type. These tools can also be used to identify faults in the connected devices in the network, and it can also enhance the efficiency of the device.

Security professionals can use tools such as SCADAfence, CyberLens, Guardian, and Dragos for asset inventory and device authorization.

- **OT Network Monitoring and Anomaly Detection**

OT network monitoring is used for constantly monitoring the systems in industrial networks. These monitoring tools help in tracking the traffic in a non-invasive way. These tools perform anomaly detection, which is the process of identifying any malicious or unexpected events. Most of these tools use machine-learning algorithms for easy detection and identification of malicious behaviors.


Security professionals can use tools such as Claroty and OT ThreatFeed for OT network monitoring and anomaly detection.

- **Decoys to Deceive Attackers**

Decoys are honeypots used in the OT environment that incorporate deception technology to automate the creation of traps or decoys to lure the attackers into revealing their presence and activities. This adds an extra layer of protection from attackers trying to penetrate the industrial network.

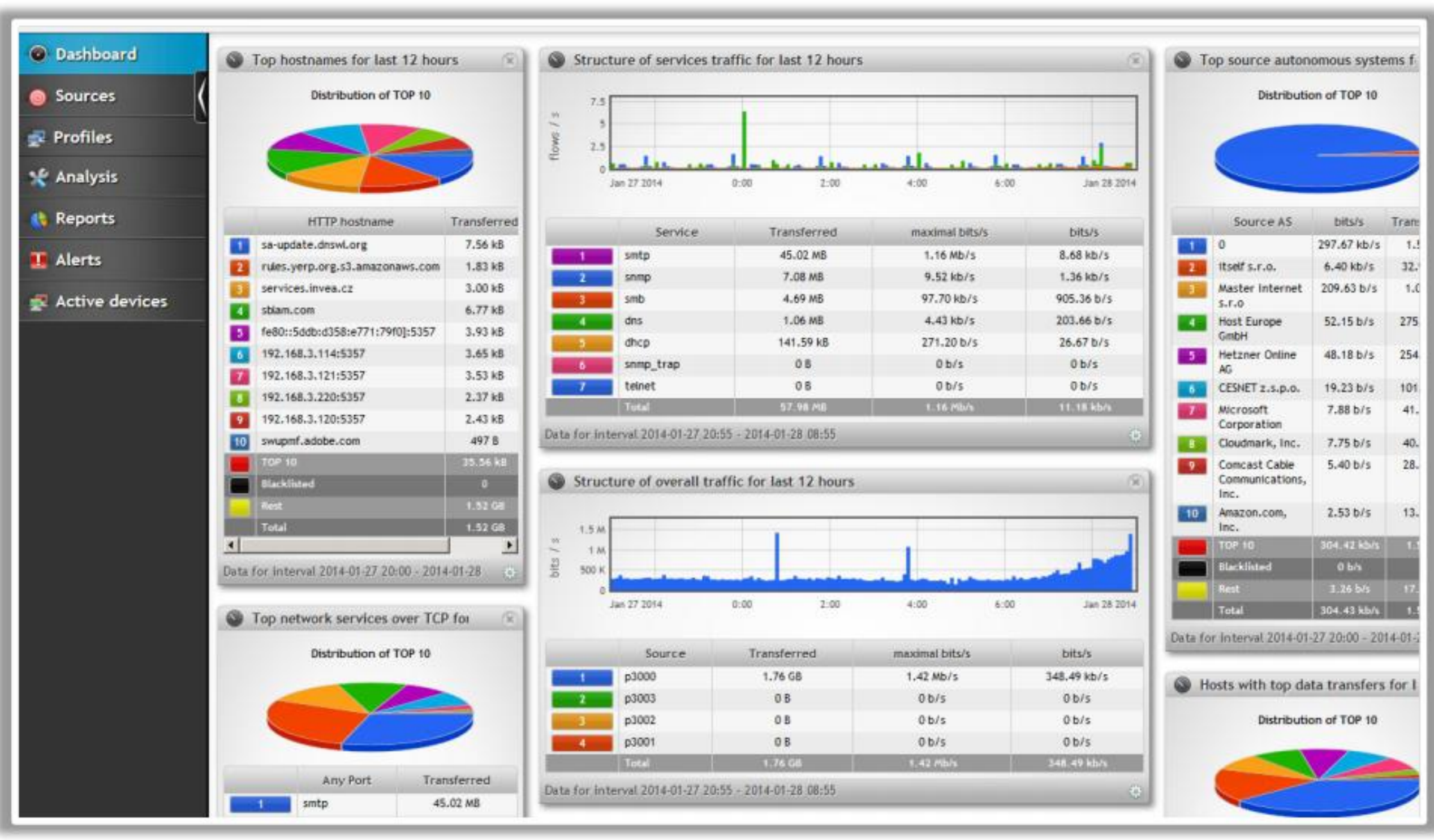
Security professionals can use tools such as ThreatDefend, Conpot, and GasPot to protect the network.

OT Security Tools




Flowmon


Flowmon empowers manufacturers and utility companies to **ensure the reliability** of their industrial networks to avoid downtime and disruption of service continuity




<https://www.flowmon.com>




tenable.ot
<https://www.tenable.com>




Forescout
<https://www.forescout.com>



PA-220R
<https://www.paloaltonetworks.com>



Fortinet ICS/SCADA solution
<https://www.fortinet.com>



Nozomi Networks Guardian
<https://www.nozominetworks.com>

Copyright © by **EC-Council**. All Rights Reserved. Reproduction is Strictly Prohibited.

OT Security Tools

Discussed below are various tools you can use to secure OT systems and networks:

- **Flowmon**

Source: <https://www.flowmon.com>

Flowmon empowers manufacturers and utility companies to ensure the reliability of their industrial networks confidently to avoid downtime and disruption of service continuity. This can be achieved by continuous monitoring and anomaly detection so that malfunctioning devices or security incidents, such as cyber espionage, zero-days, or malware, can be reported and remedied as quickly as possible.

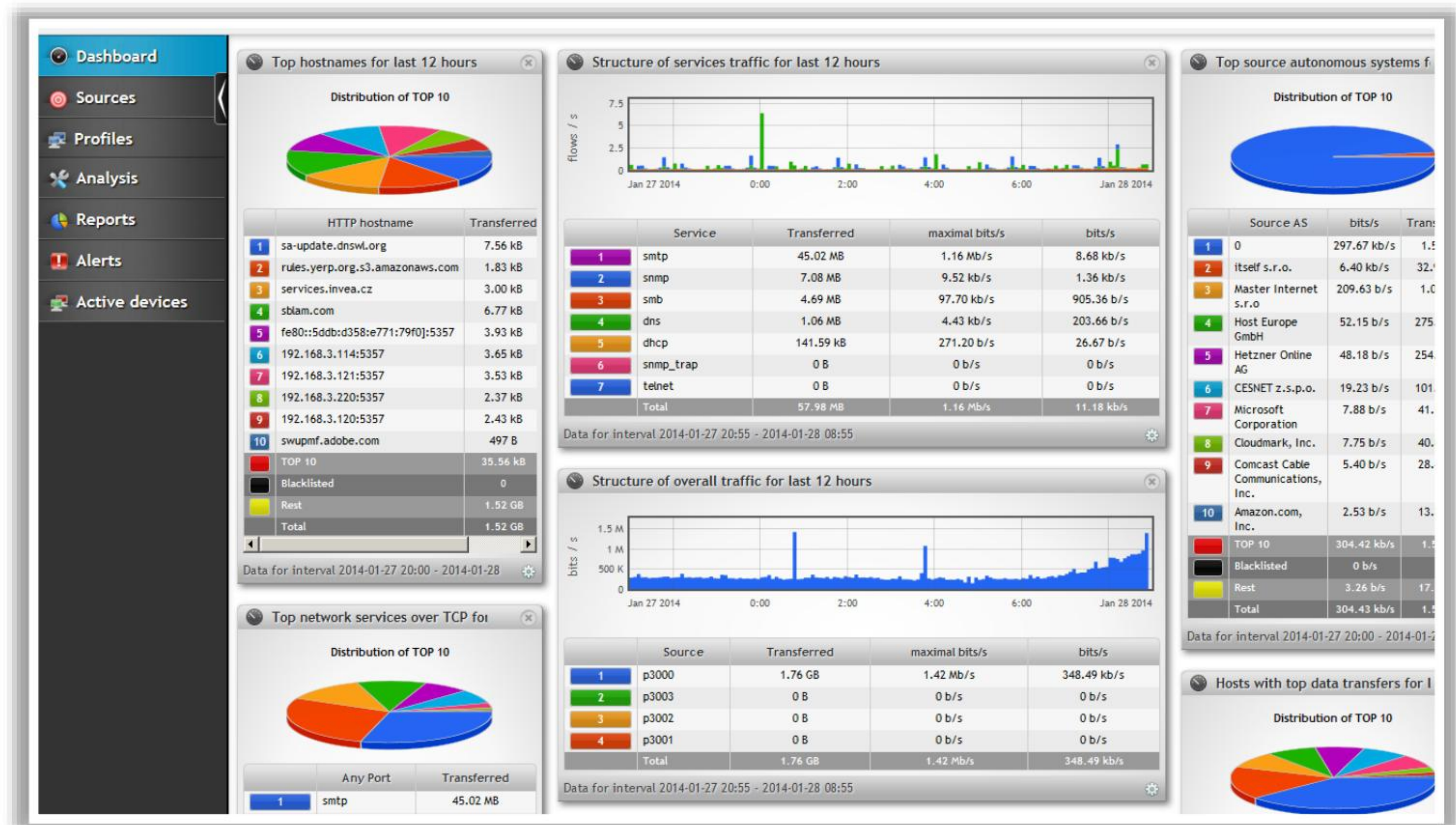


Figure 13.27: Screenshot of Flowmon

Listed below are some additional tools for securing an OT environment:

- tenable.ot (<https://www.tenable.com>)
- Forescout (<https://www.forescout.com>)
- PA-220R (<https://www.paloaltonetworks.com>)
- Fortinet ICS/SCADA solution (<https://www.fortinet.com>)
- Nozomi Networks Guardian™ (<https://www.nozominetworks.com>)

Module Summary

- 1 This module discussed IoT concepts and why organizations opt for IoT-enabled environments
- 2 It discussed IoT application areas and IoT devices
- 3 It also discussed the IoT architecture and IoT communication models
- 4 This module discussed the security in IoT-enabled environments
- 5 It also discussed OT concepts including the Purdue model and the components of an ICS
- 6 Finally, this module presented a detailed discussion on the security in OT-enabled environments
- 7 In the next module, we will discuss cryptography concepts in detail



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Summary

This module has discussed IoT concepts and why organizations opt for IoT-enabled environments. It has discussed IoT application areas and IoT devices as well as the IoT architecture and IoT communication models. This module also discussed security in IoT-enabled environments. Furthermore, it discussed OT concepts including the Purdue model and the components of an ICS. Finally, this module presented a detailed discussion on security in OT-enabled environments.

In the next module, we will discuss cryptography concepts in detail.