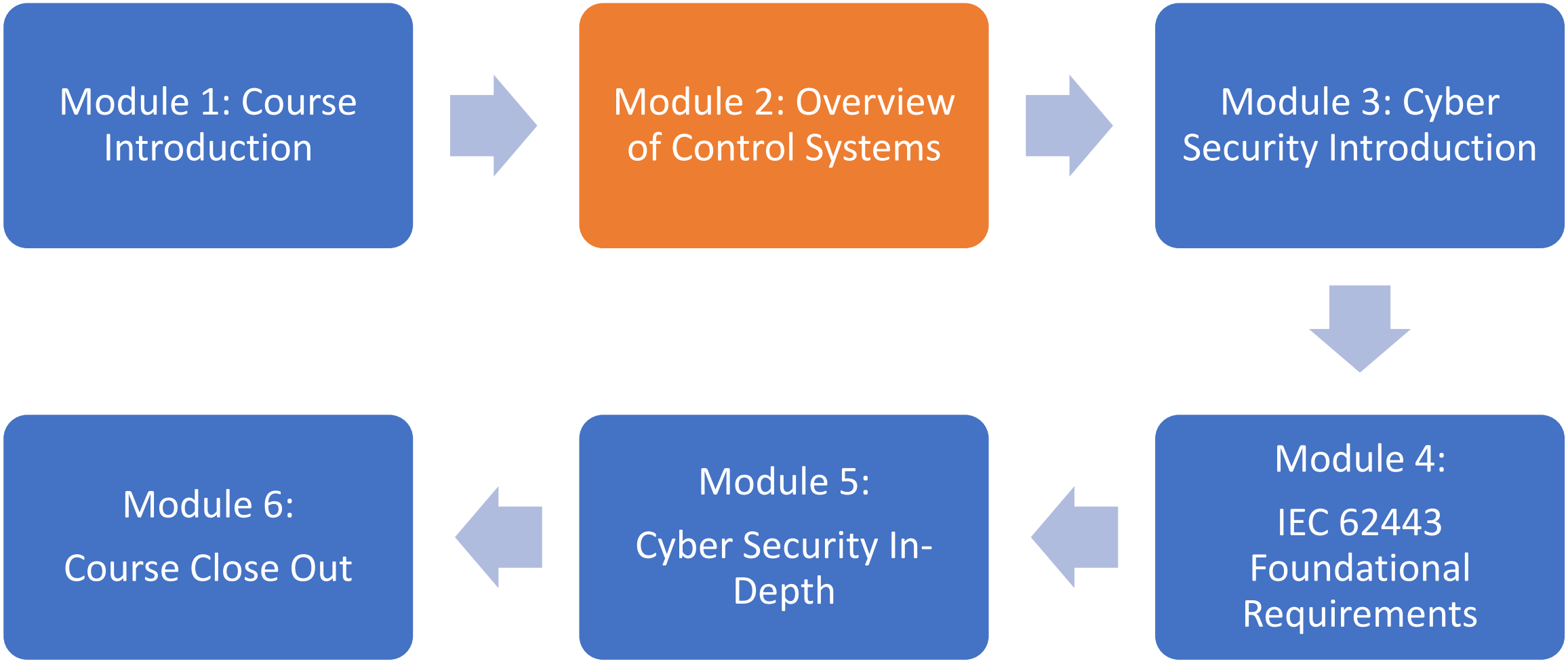
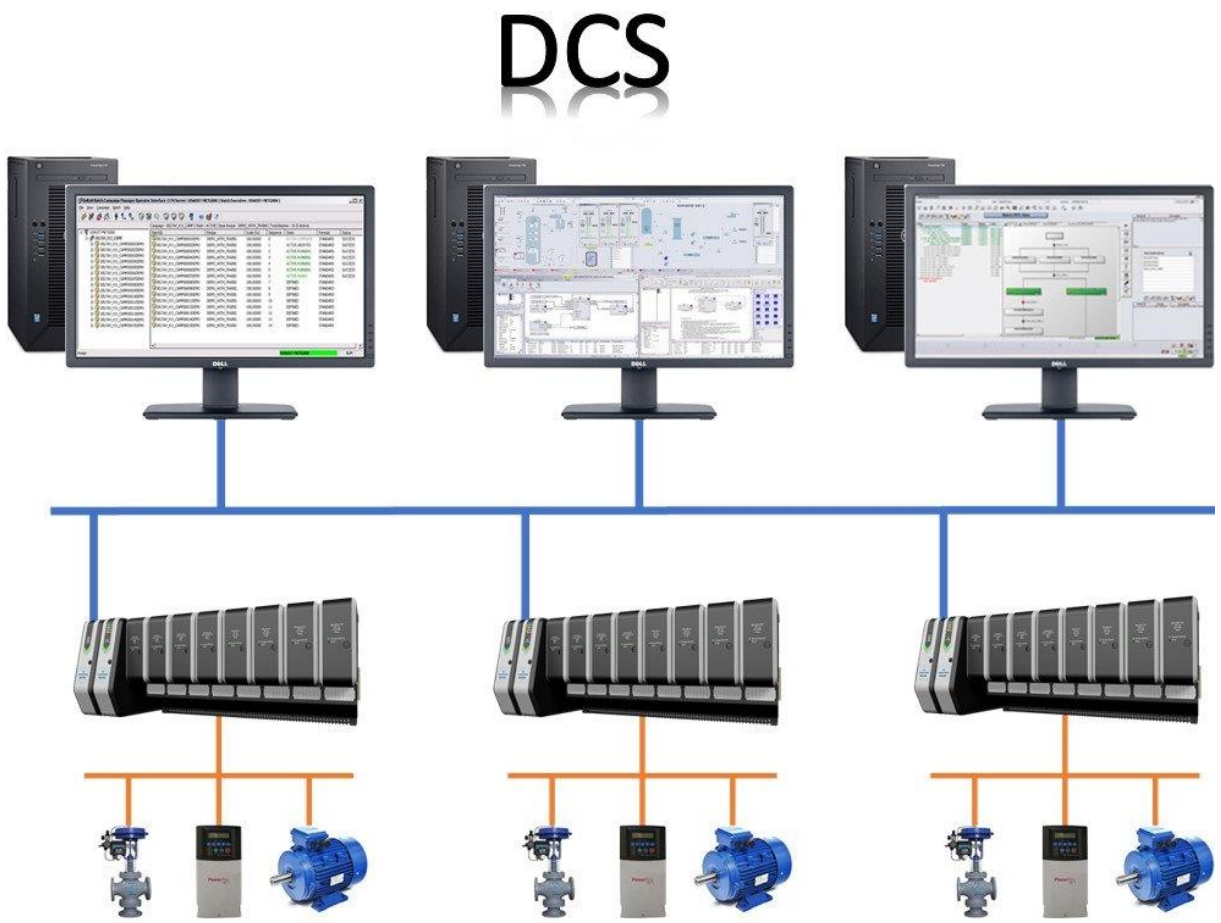
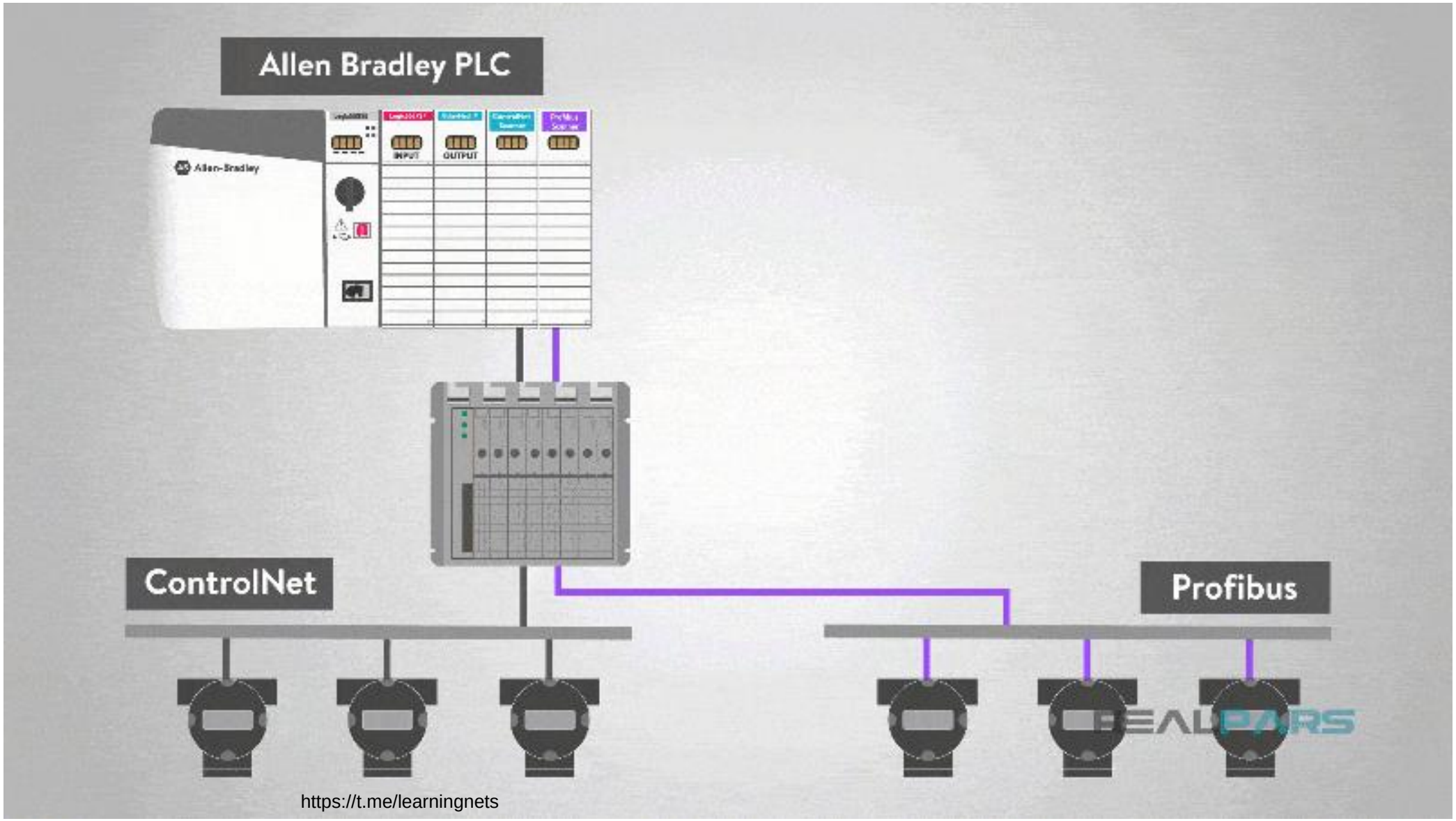


What is a or Distributed Control System (DCS)?

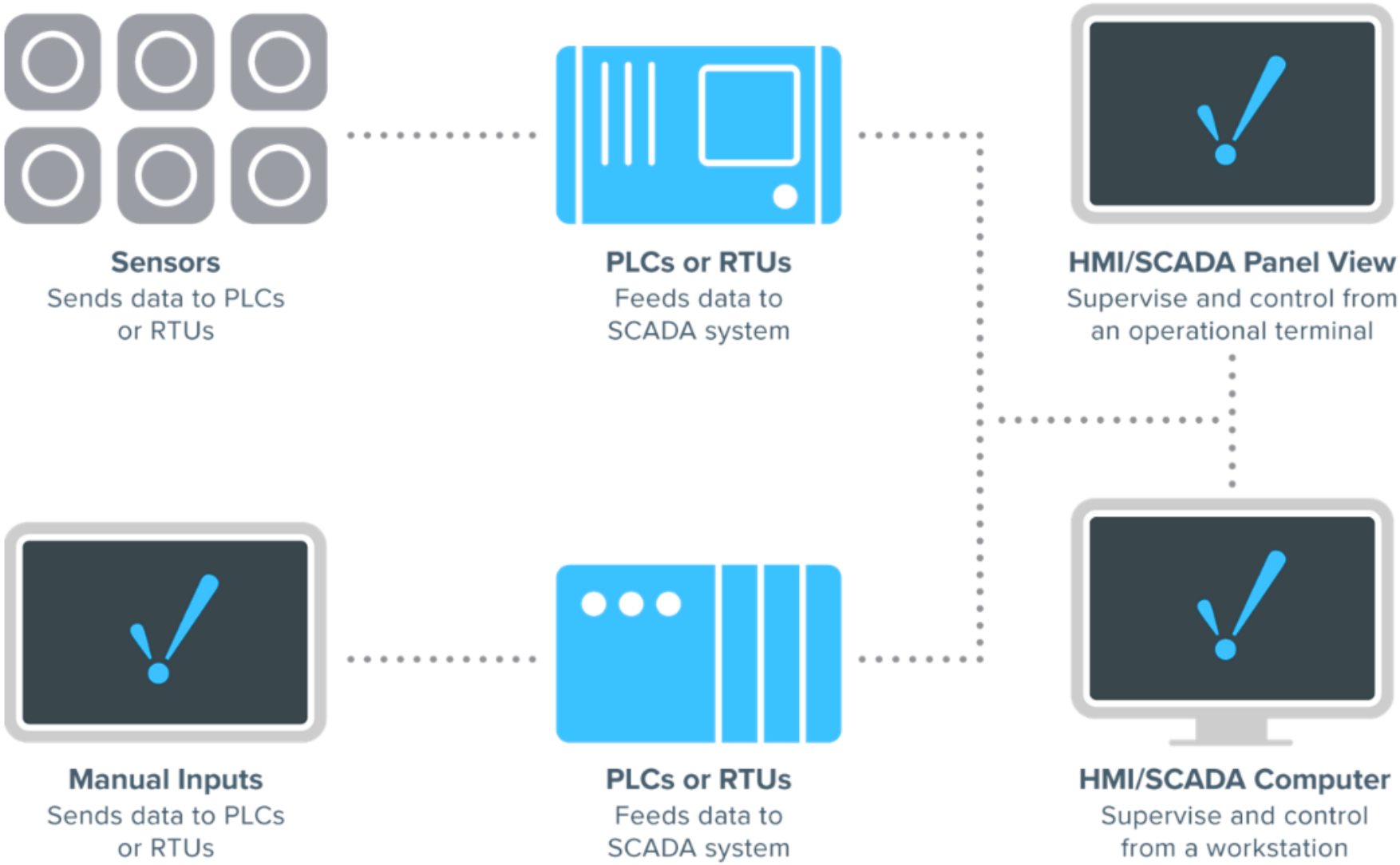


DCS refers to a control system where the control functions are distributed rather than centralized on a single controller or algorithm. This distributed nature allows for the placement of multiple controllers and automation systems across a large geographical area, which in turn enables centralized monitoring and control from a single console or operator workstation.

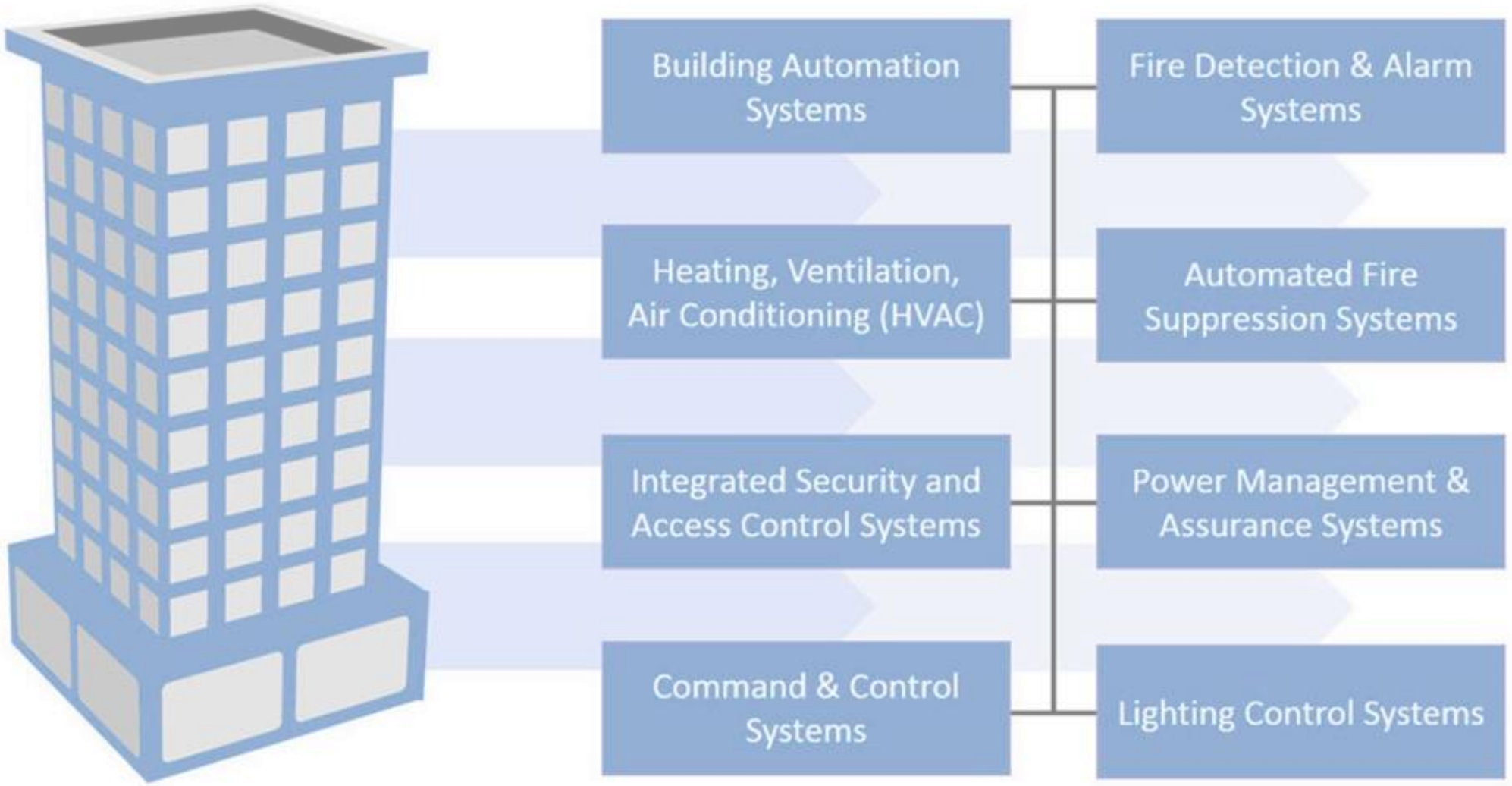
Programmable Logic Controllers



SCADA Explained

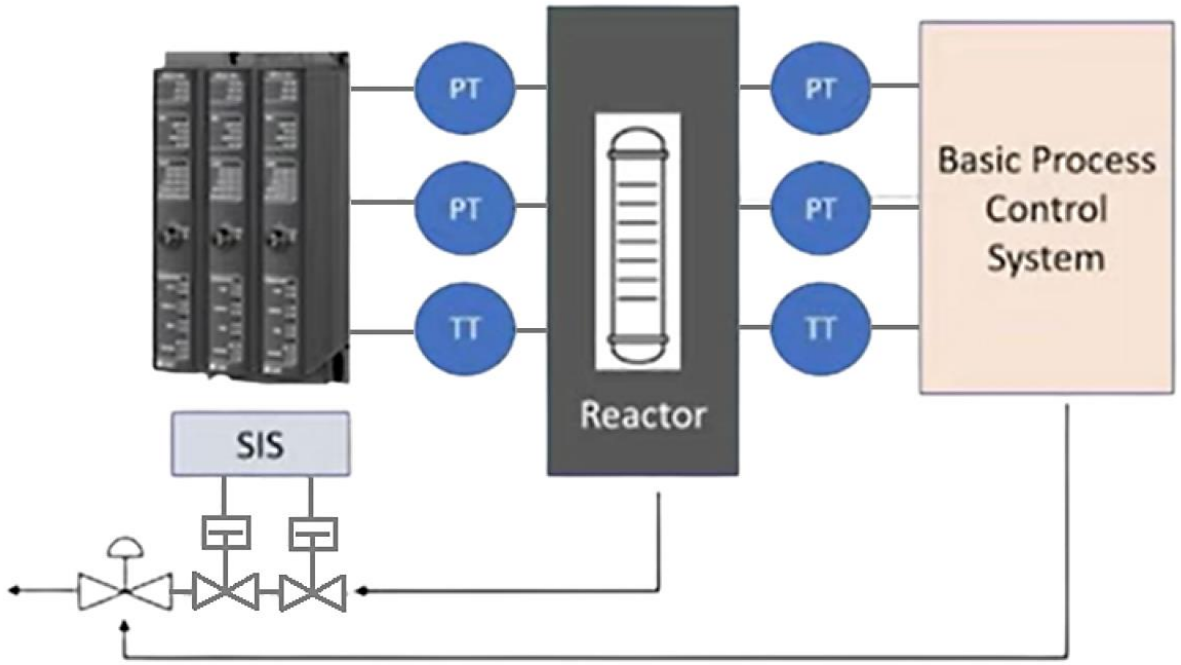


Building Automation and Control System Overview

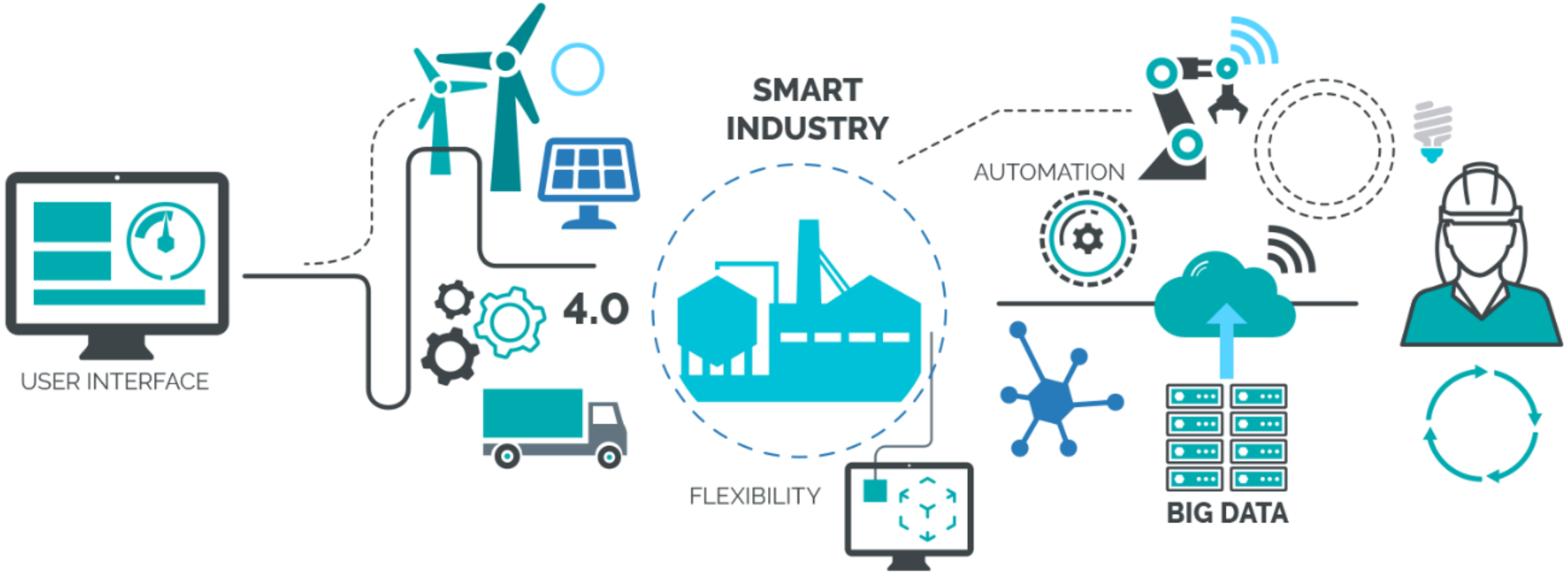


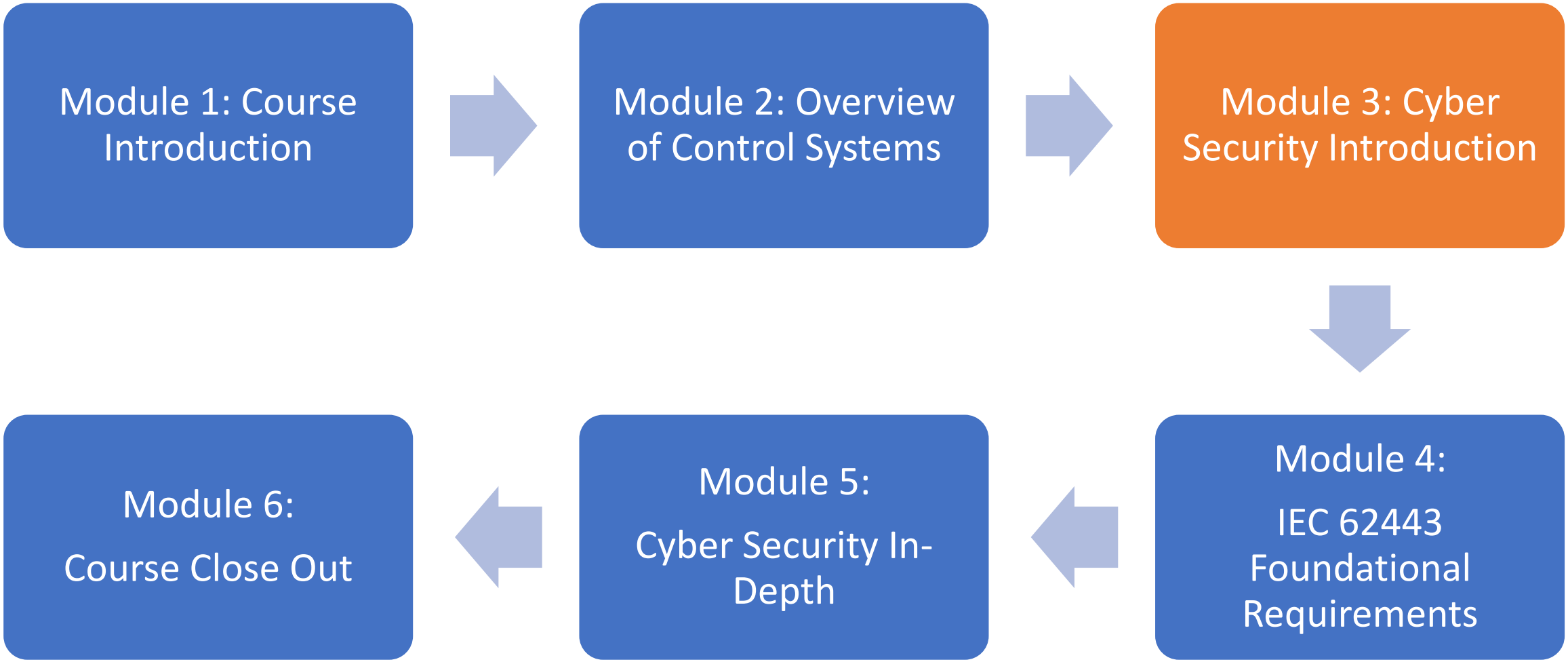
Safety Instrumented Systems (SIS) Overview

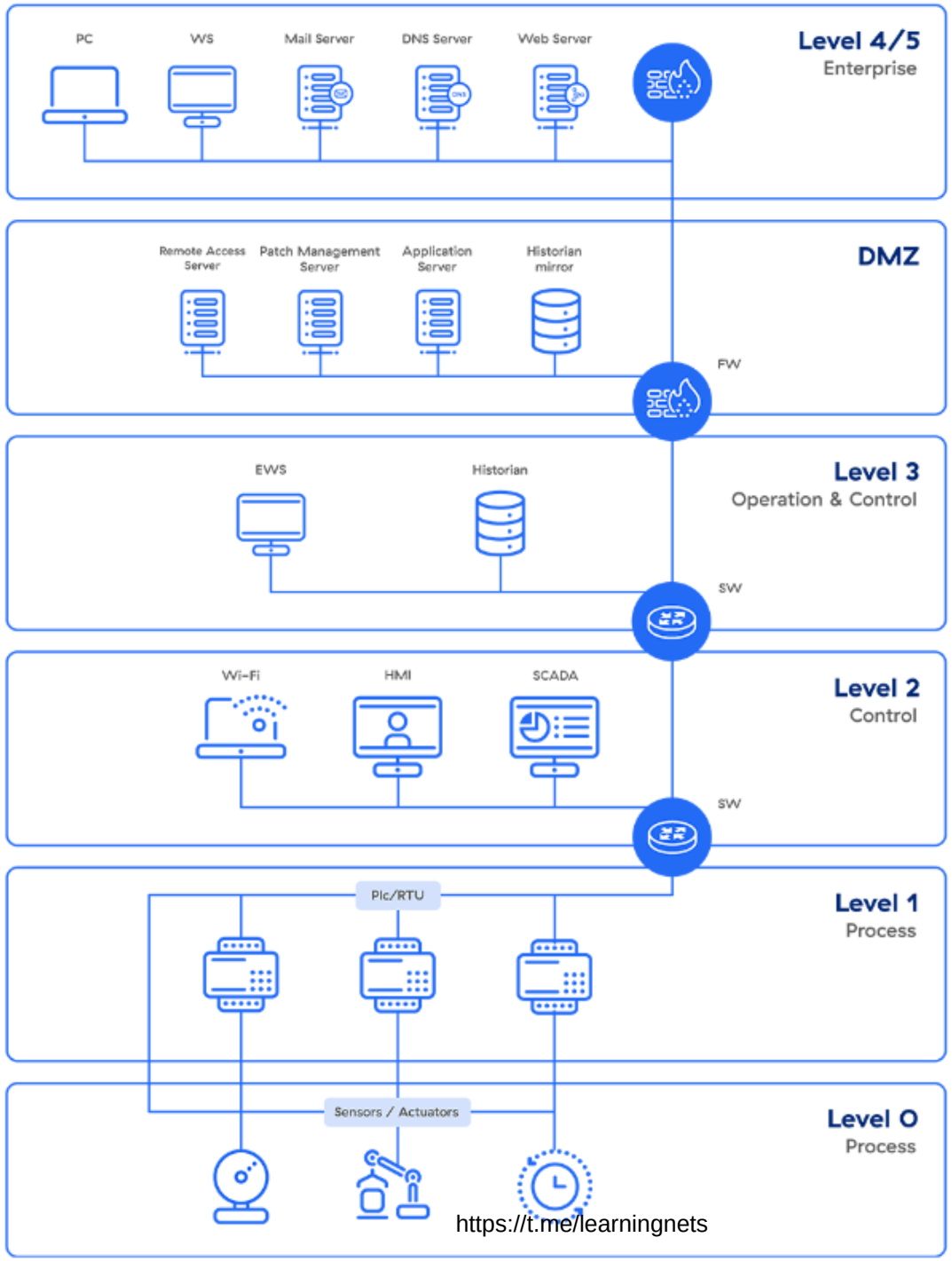
What is SIS? SIS stands for Safety Instrumented System. These systems are the unsung heroes of industrial safety, designed to reduce the likelihood or consequences of hazardous situations by bringing the system to a safe state when needed.



Industrial Internet of Things





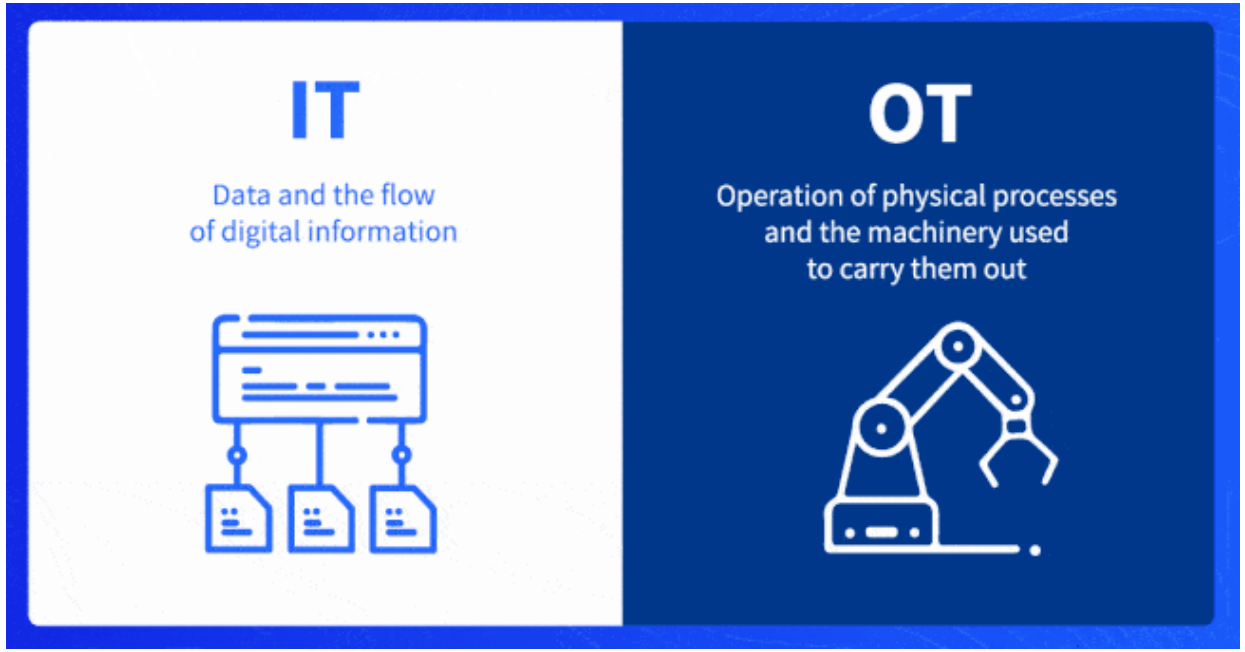


Purdue Model

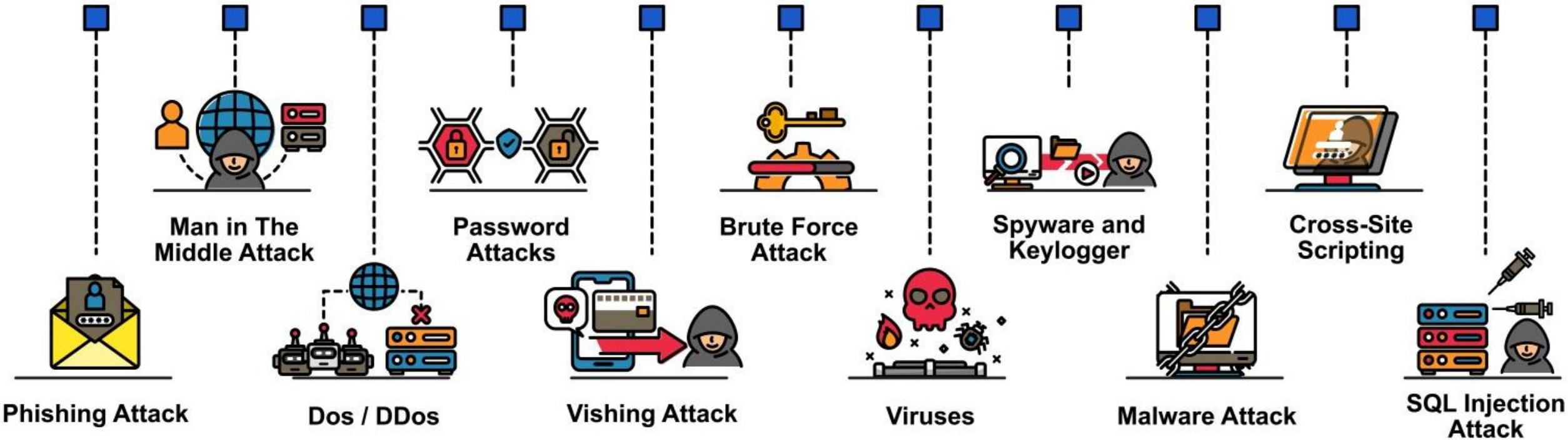
The Purdue model is a structural model for industrial control system (ICS) security that concerns segmentation of physical processes, sensors, supervisory controls, operations, and logistics.

Difference Between OT and IT Networks

Operational technology (OT) is the hardware and software that monitors and controls devices, processes, and infrastructure, and is used in industrial settings. IT combines technologies for networking, information processing, enterprise data centers, and cloud systems. OT devices control the physical world, while IT systems manage data and applications.



CYBER SECURITY ATTACKS



Anatomy of a Cyber Attack

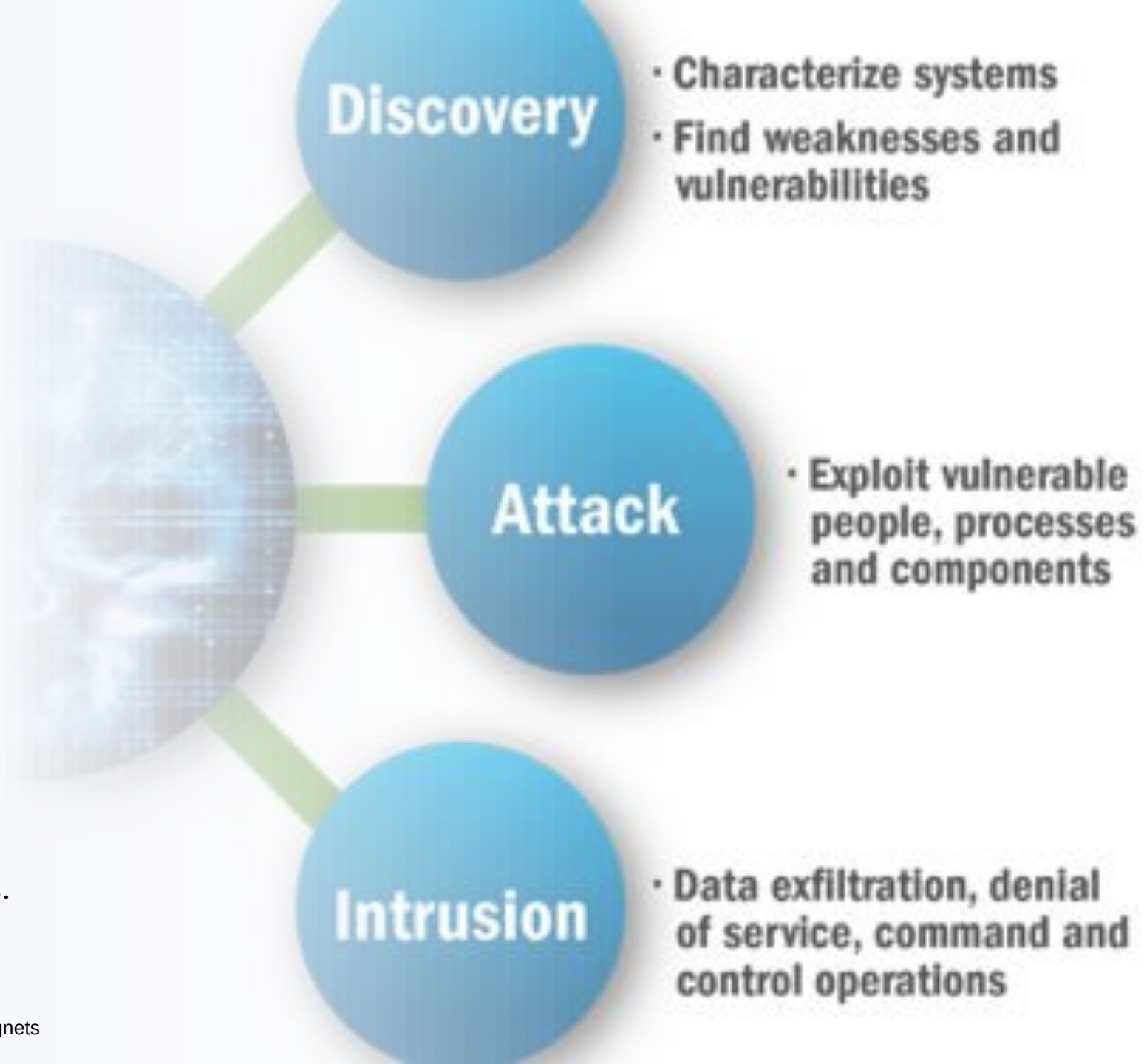
Understanding Cybersecurity:

Grasp cyber attack concept for comprehensive defence.

Know methods malicious actors use to exploit vulnerabilities.

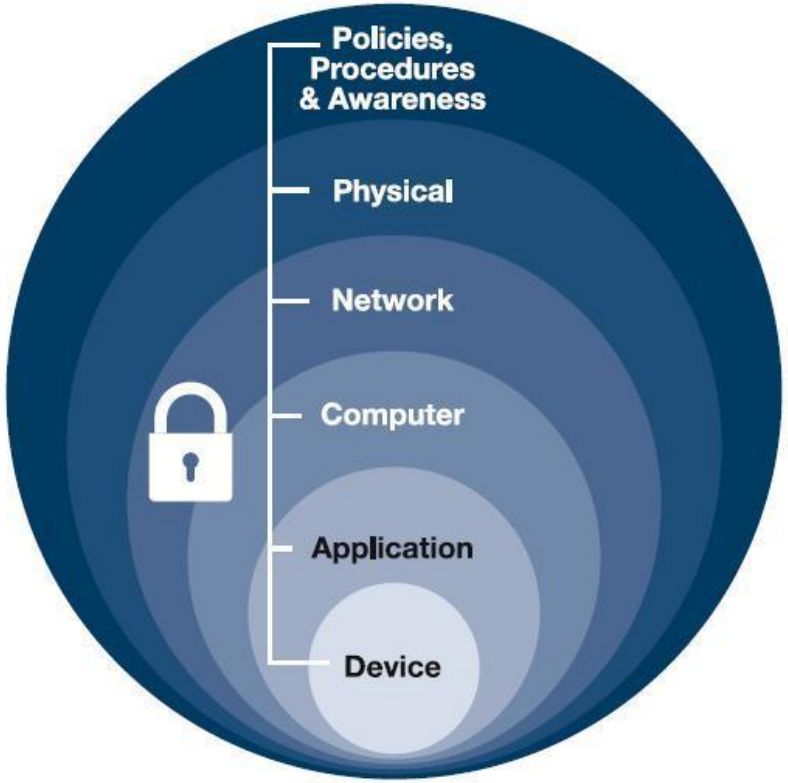
Similarity to techniques security pros use for testing.

Insight into approaches helps implement effective defense strategies.



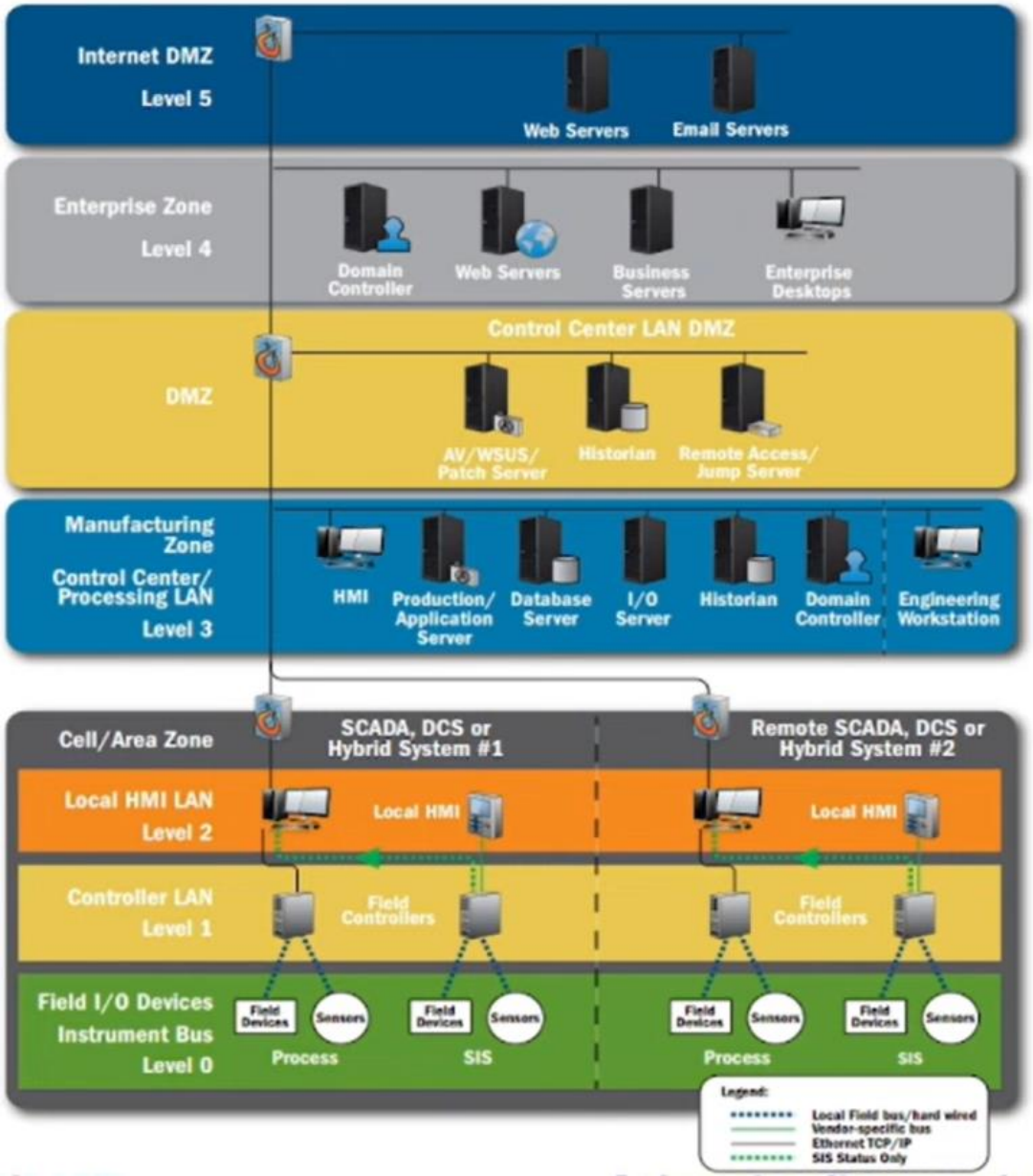
Defense in Depth

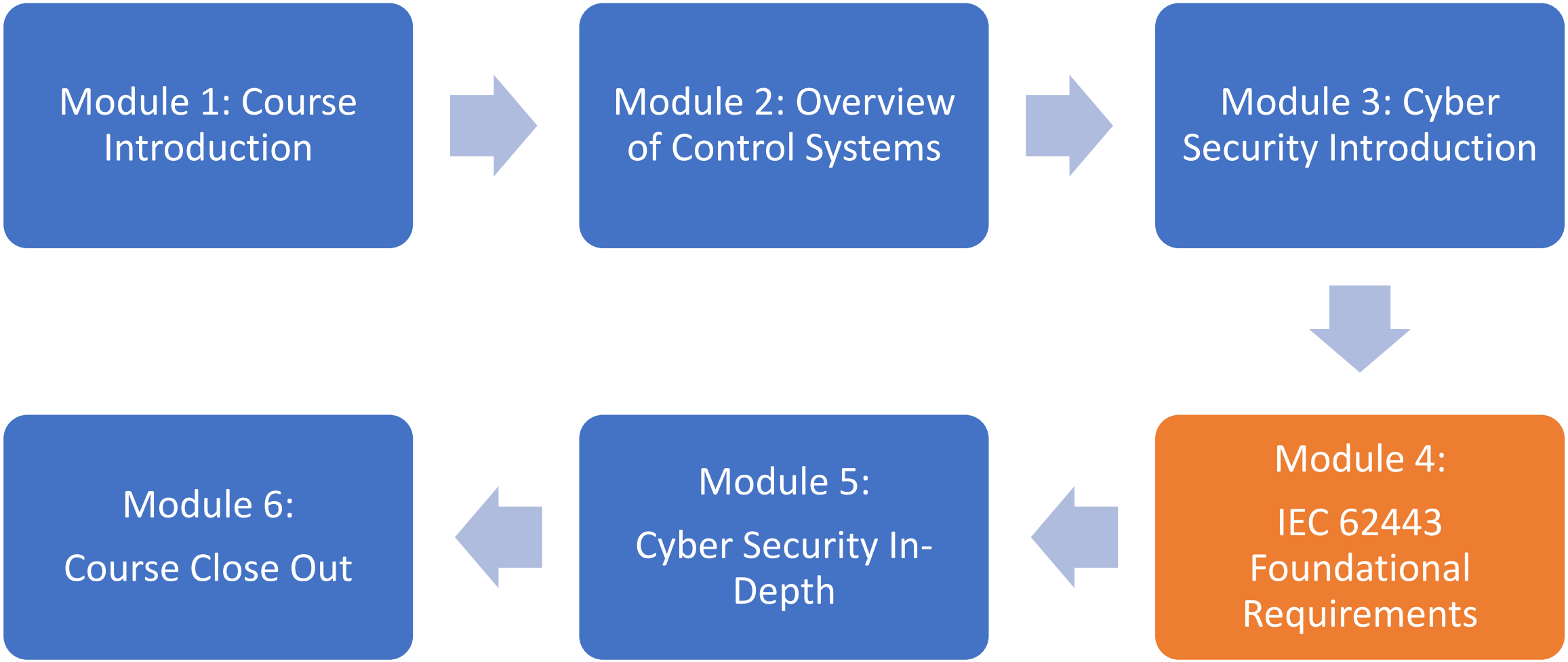
Defense in depth is a strategic approach that leverages multiple layers of security measures to protect an organization's assets.



Control system Architectures

- Heightened Reliance on Automation and Control Systems
- Insecure External Network Connectivity
- Utilization of Technologies with Known Vulnerabilities
- Absence of a Business Case for Cybersecurity
- Limited Security in Control System Technologies
- Inadequate Security in Communication Protocols
- Availability of Open Source Information





ICS Cyber Security Standards

BS EN61511 2017

Risk Assessment for Cybersecurity

Mitigating Strategies

ISA/IEC62443

Assess

Implement

Maintain a Defence in Depth Strategy

Foundational requirements contain methods encompassing People, Processes and Technology to attain required IACS Security Levels (SLs)

Defines requirements for Risk Assessing both existing IACS and new designs

Defines technical requirements for IACS security

FR 1-Access Control (AC)

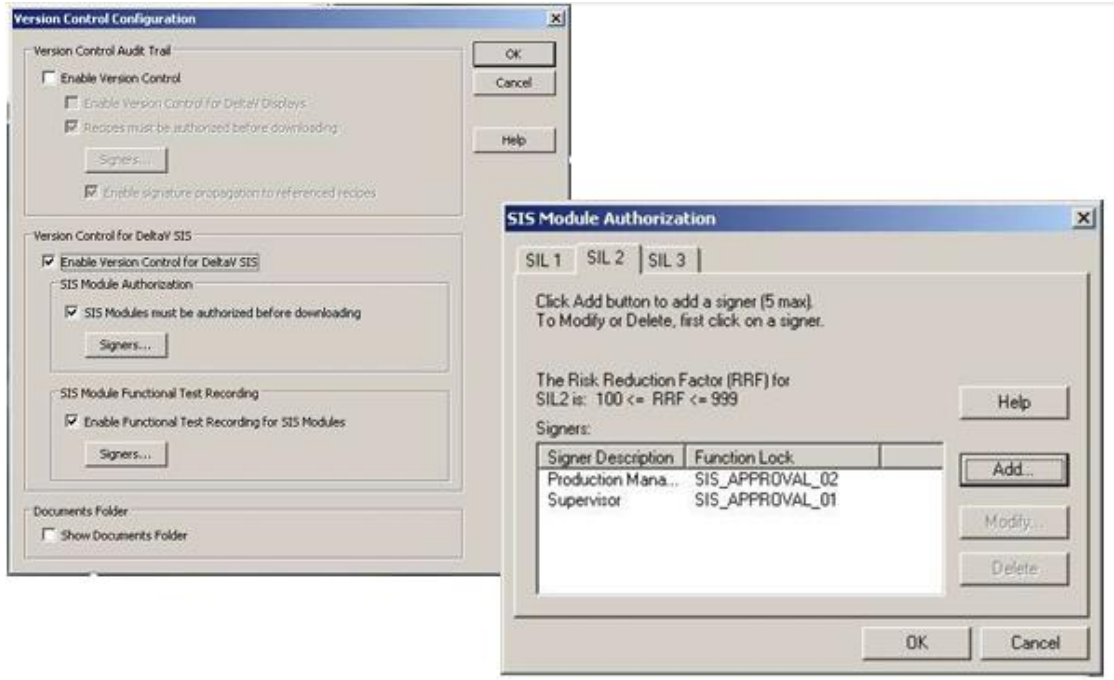
1.Access Control (AC)
2.Reliably Identify and Authenticate
3.All Users (Humans, Software Processes, and Devices)

FR 2-Use Control

1.Use Control (UC)
2.Enforce Assigned Privileges
3.Authenticated User (Human, Software Process, or Device)
4.Monitor the Use of Privileges

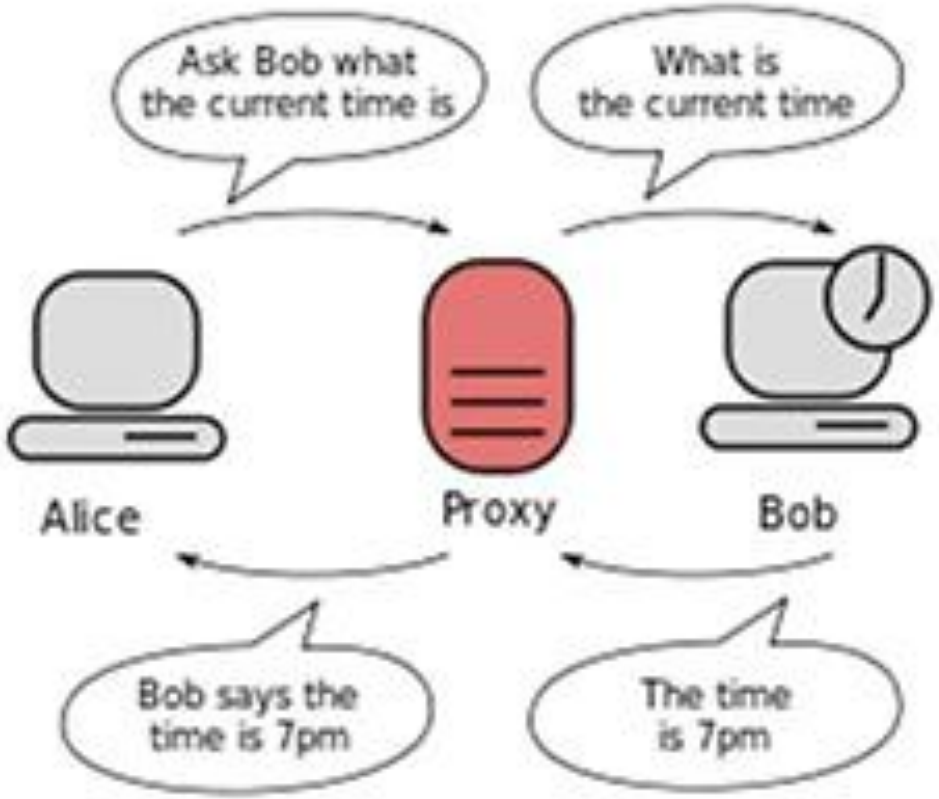
FR 3-System Integrity

1.System Integrity (SI)
2. Ensure the Integrity of the IACS
3. Prevent Unauthorized Manipulation



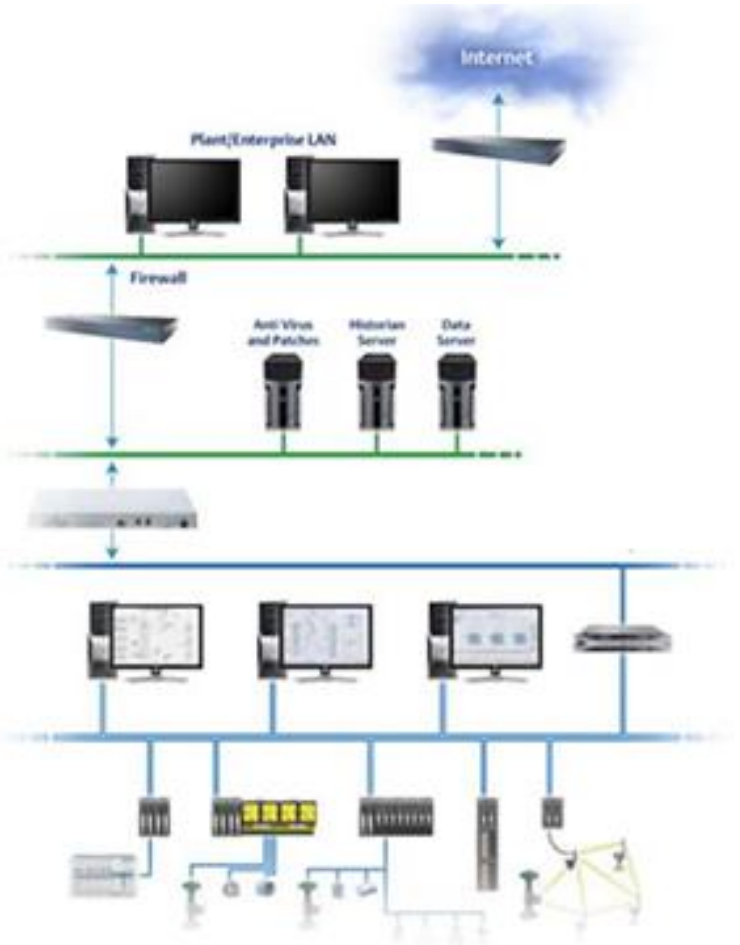
FR 4 -Data Confidentiality (DC)

1.Data Confidentiality (DC)
2.Ensure the Confidentiality of Information
3.On Communication Channels and in Data Repositories
4.Prevent Unauthorized Disclosure



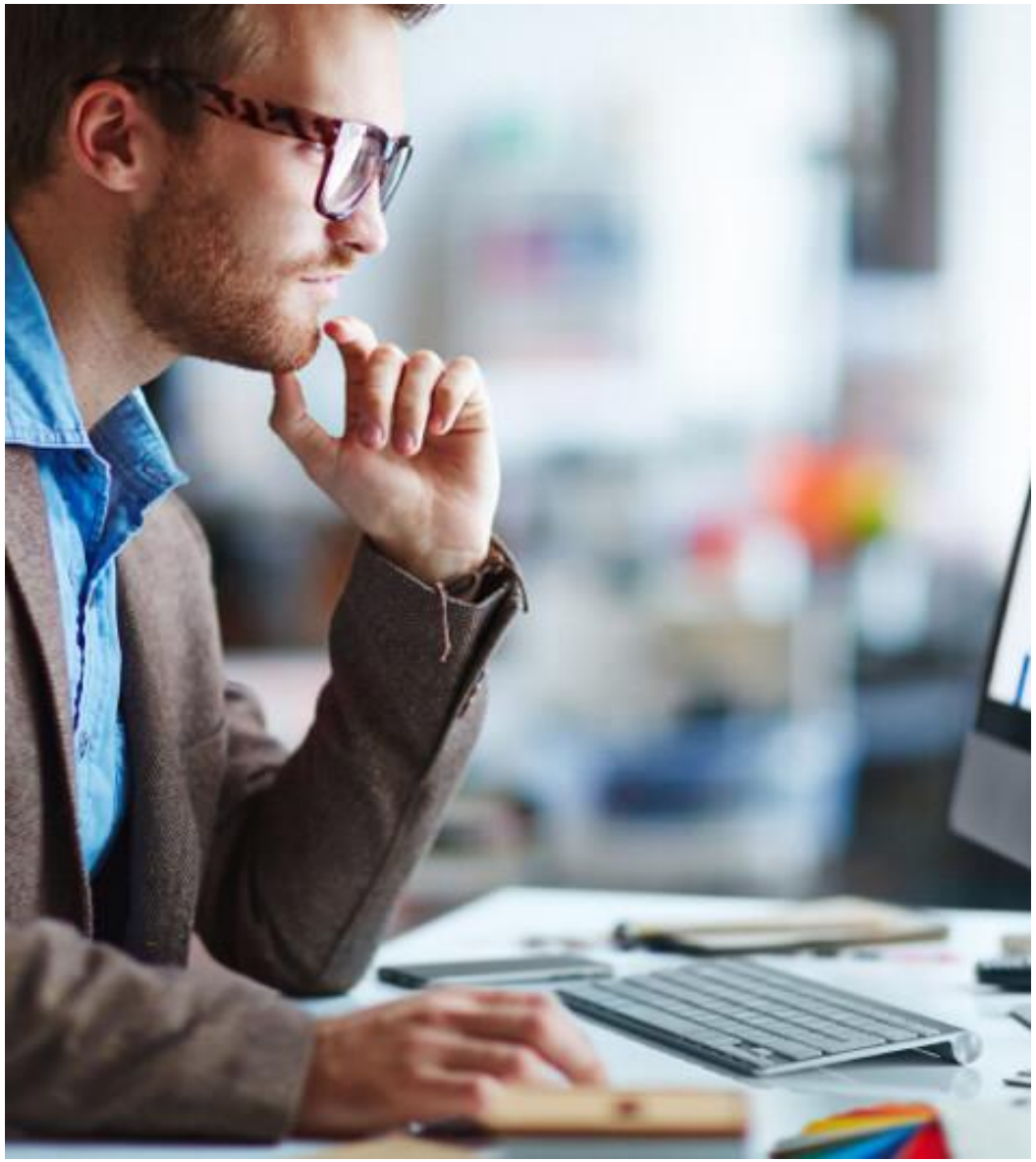
FR 5-Restrict Data Flow (RDF)

1.Restrict Data Flow (RDF)
2.Segment the Control System via Zones and Conduits
3.Limit Unnecessary Flow of Data



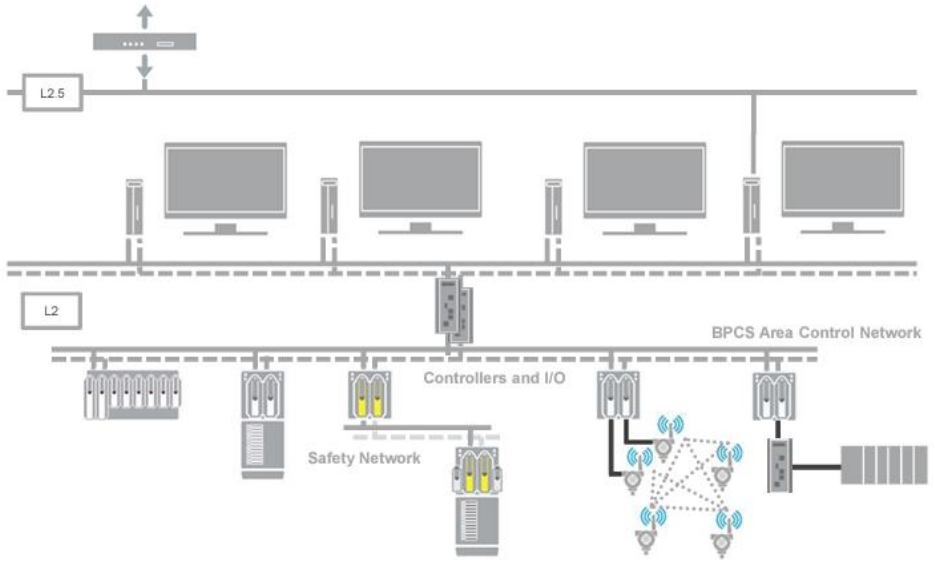
FR 6-Timely Response to Events (TRE)

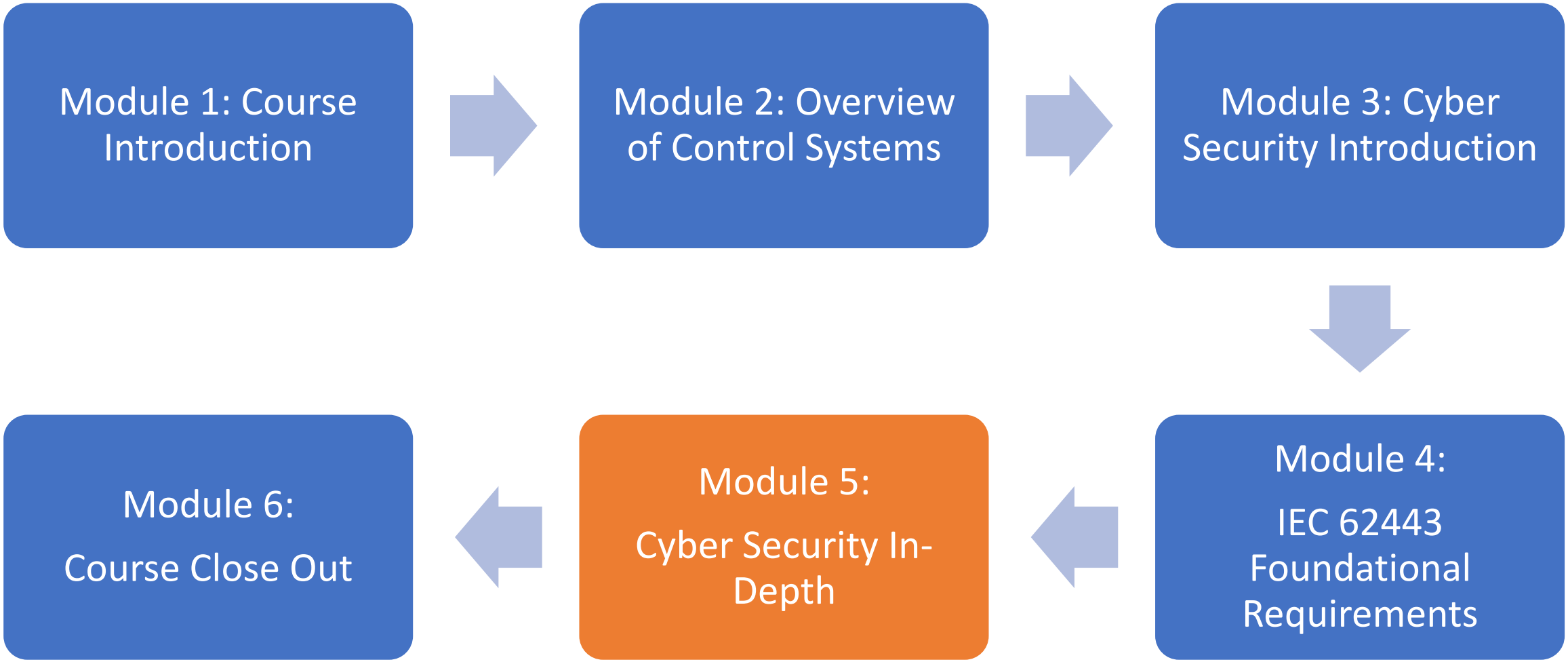
1.Timely Response to Events (TRE)
2.Respond to Security Violations
3.Notify the Proper Authority
4.Report Needed Evidence of the Violation
5.Take Timely Corrective Action



FR 7-Resource Availability (RA)

1.Resource Availability (RA)
2.Ensure the Availability of the Control System
3.Against the Degradation or Denial of Essential Services



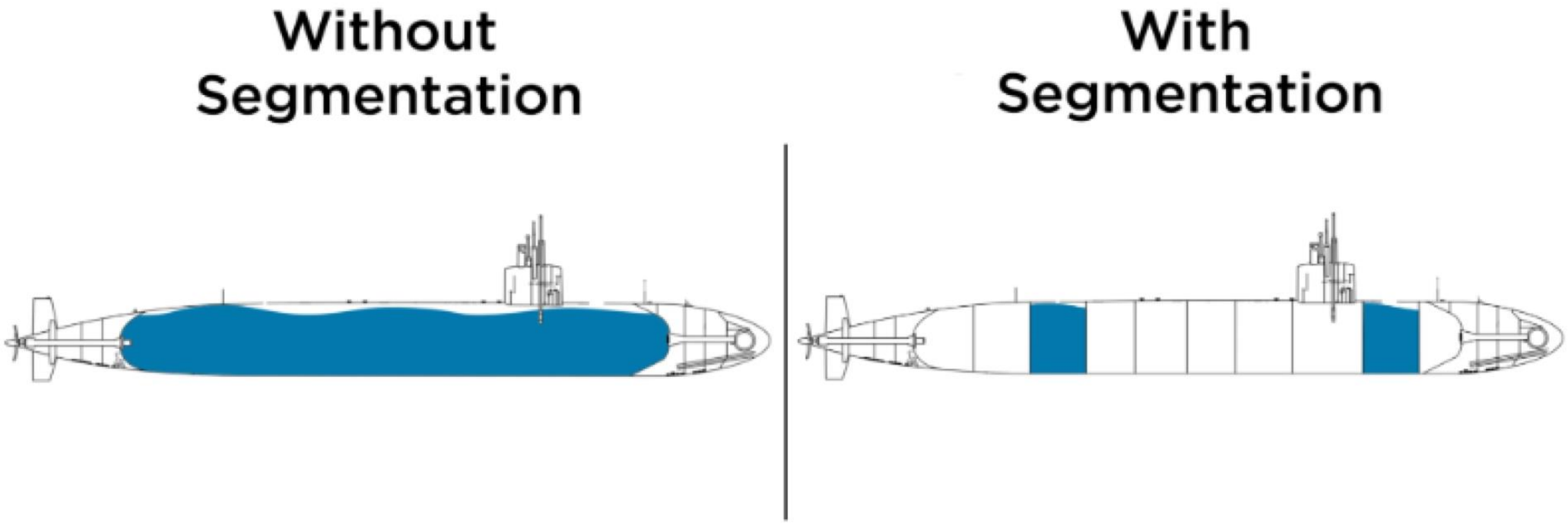


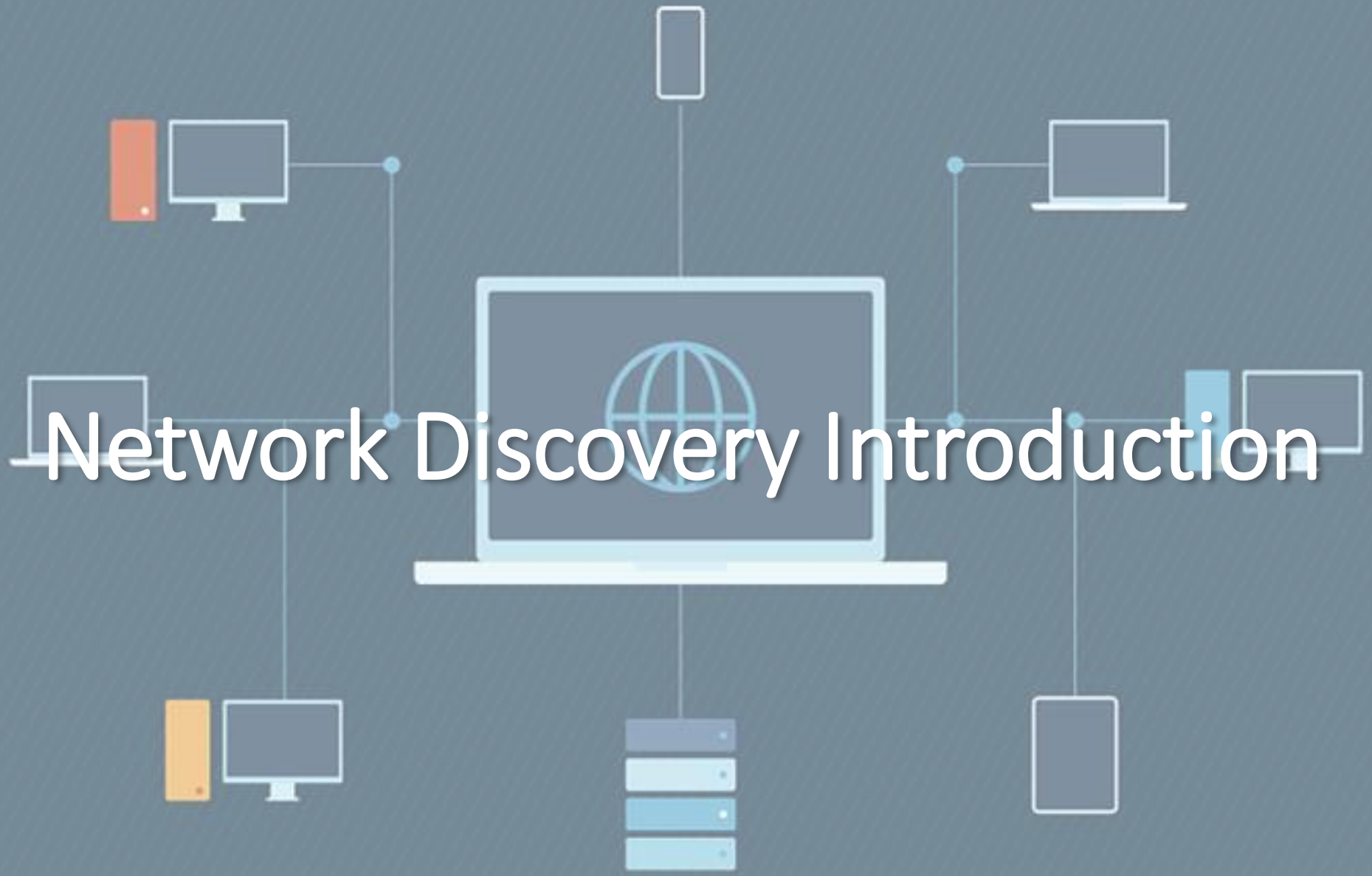
Asset Management: Strengthening Security

Asset Management: Strengthening Security

- Systematic identification and management of data, personal devices, systems, and facilities.
- Prioritization of assets based on significance for robust security.
- Encompasses diverse elements such as data, personal devices, systems, and facilities within the organization.

Network Segmentation

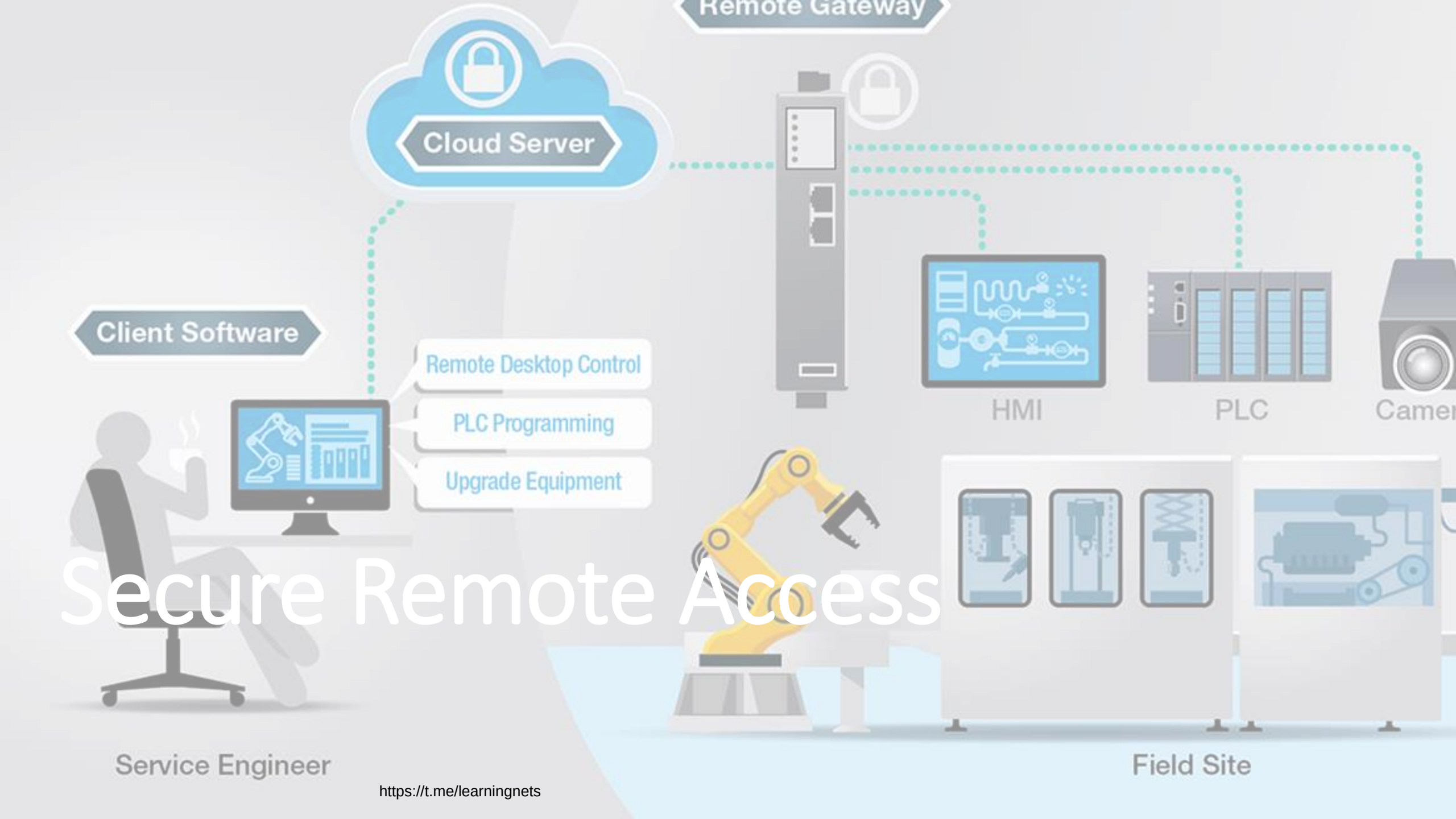




Network Discovery Introduction

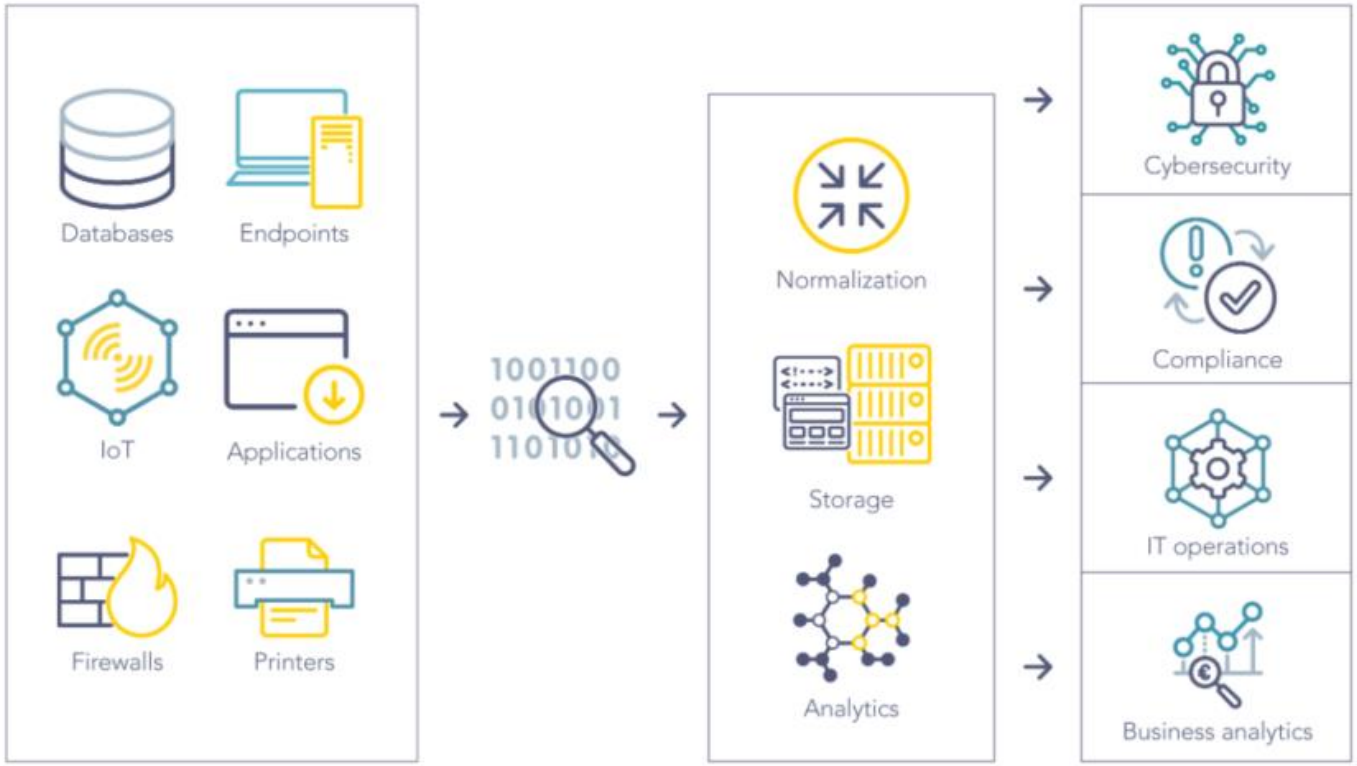
Intrusion Detection

An Intrusion Detection System (IDS) is a vital tool in cybersecurity. It detects unusual digital activity and raises alarms when necessary. Analysts then investigate and take actions, such as isolating compromised systems or blocking unauthorized access. In essence, an IDS plays a crucial role in safeguarding the digital realm.



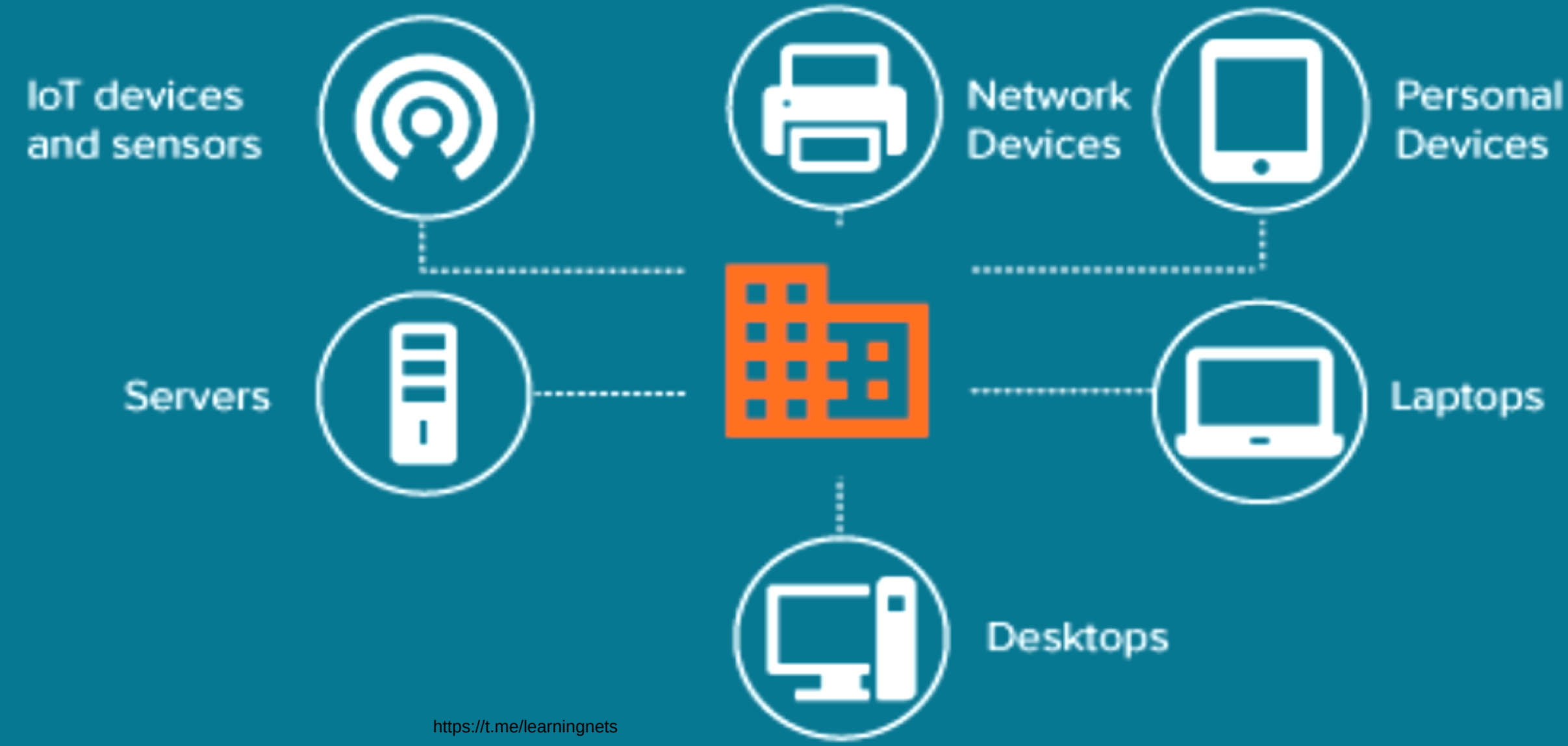
SIEM Introduction

SIEM software collects and aggregates log data generated throughout the entire IT infrastructure, from cloud systems and applications to network and security devices, such as firewalls and antivirus.



What is an endpoint?

Any device that accesses your corporate network.




https://t.me/learningnets