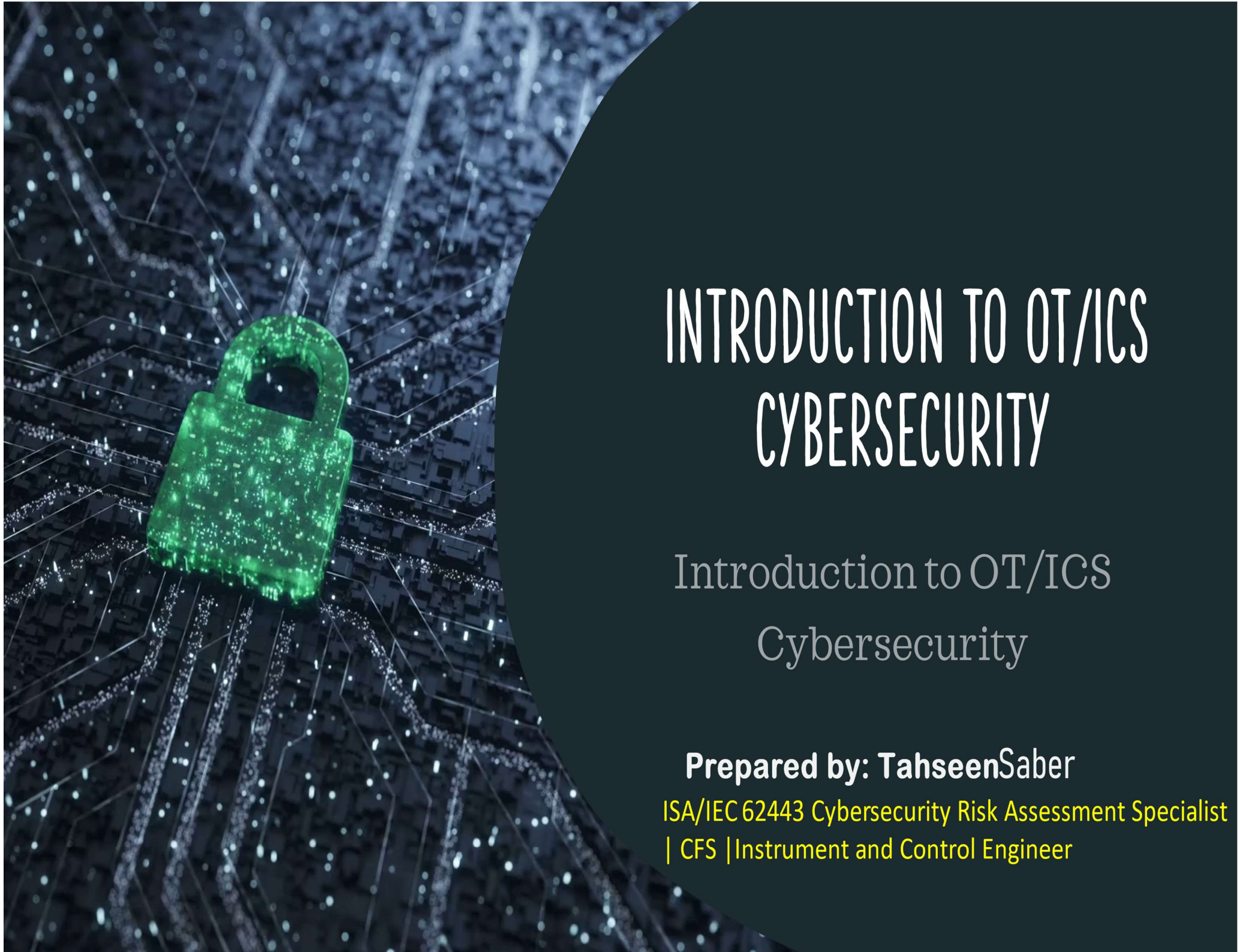
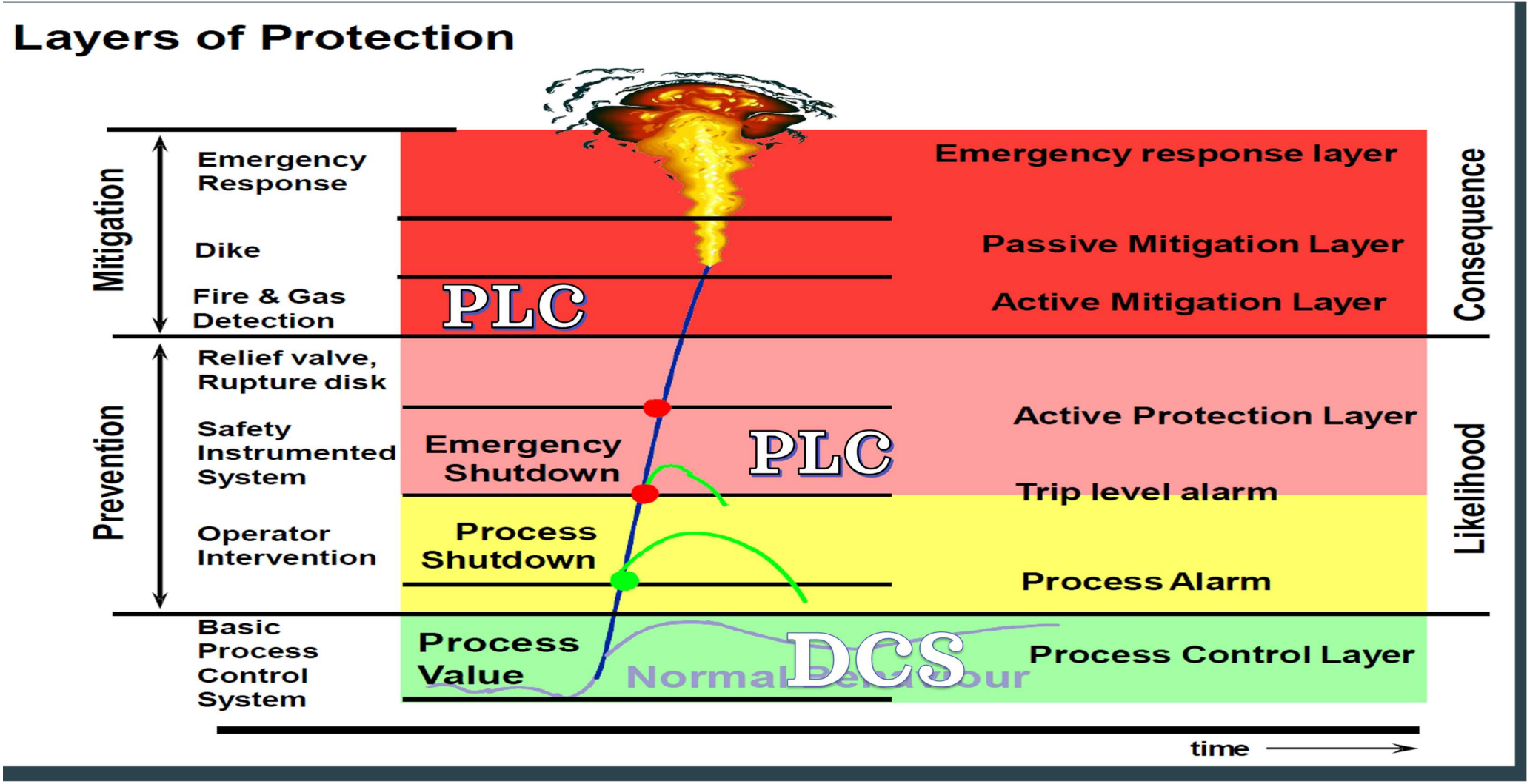


INTRODUCTION TO OT/ICS CYBERSECURITY

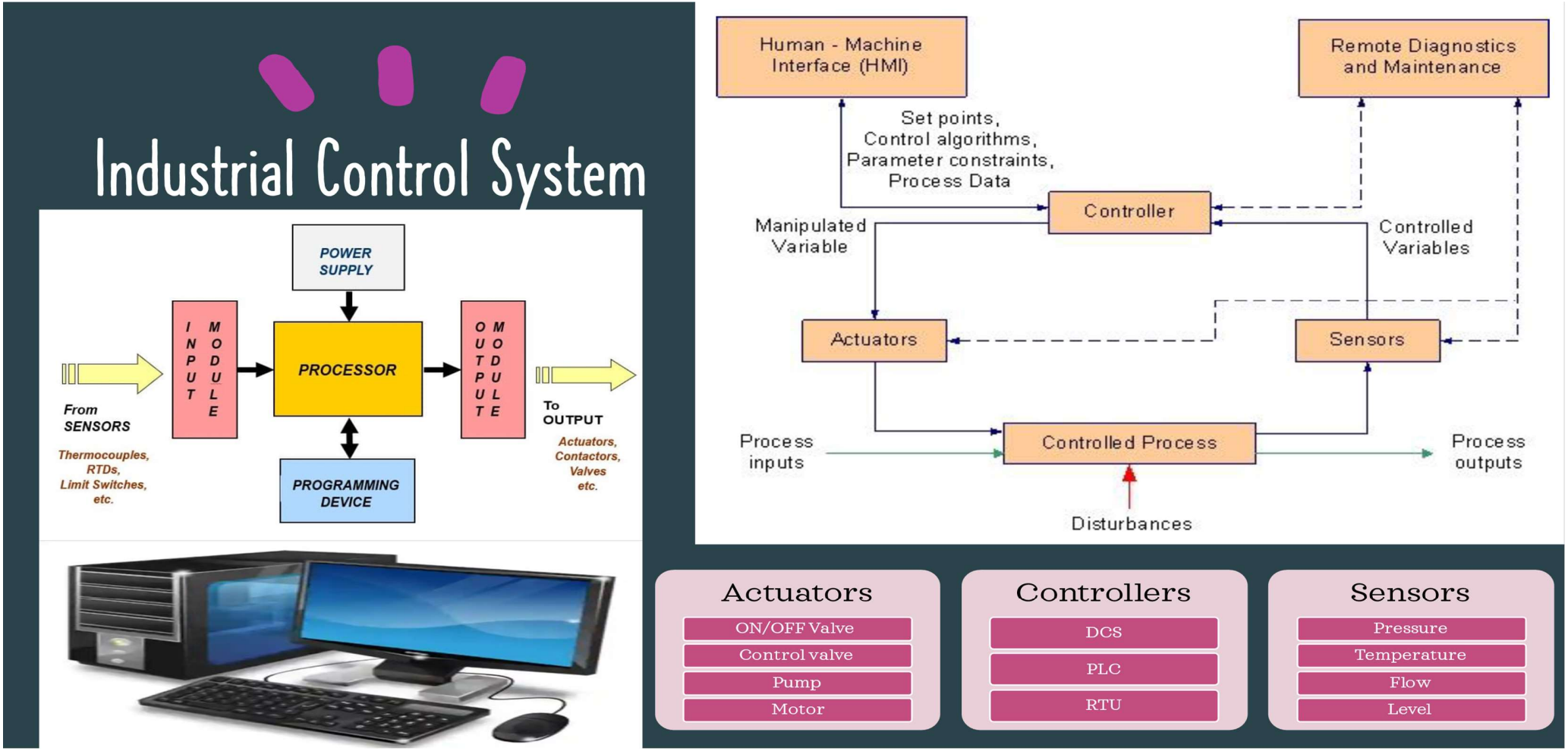
Introduction to OT/ICS Cybersecurity

Prepared by: TahseenSaber

ISA/IEC 62443 Cybersecurity Risk Assessment Specialist | CFS |Instrument and Control Engineer



- The independent protection layers **IPLs** are vital to keep plant operate smoothly and safely, and in case of any fire case will take appropriate mitigation controls to protect plant from catastrophic consequences such as explosions and fire.
- There are three **IPLs** that depends on cyber assets (**DCS**, **ESD** and **F&G** systems) which emphasis importance of such assets to protect plant so it is important to maintain availability and integrity for theses cyber assets and from this point OT cybersecurity became important.



Any control loop in the plant contains:

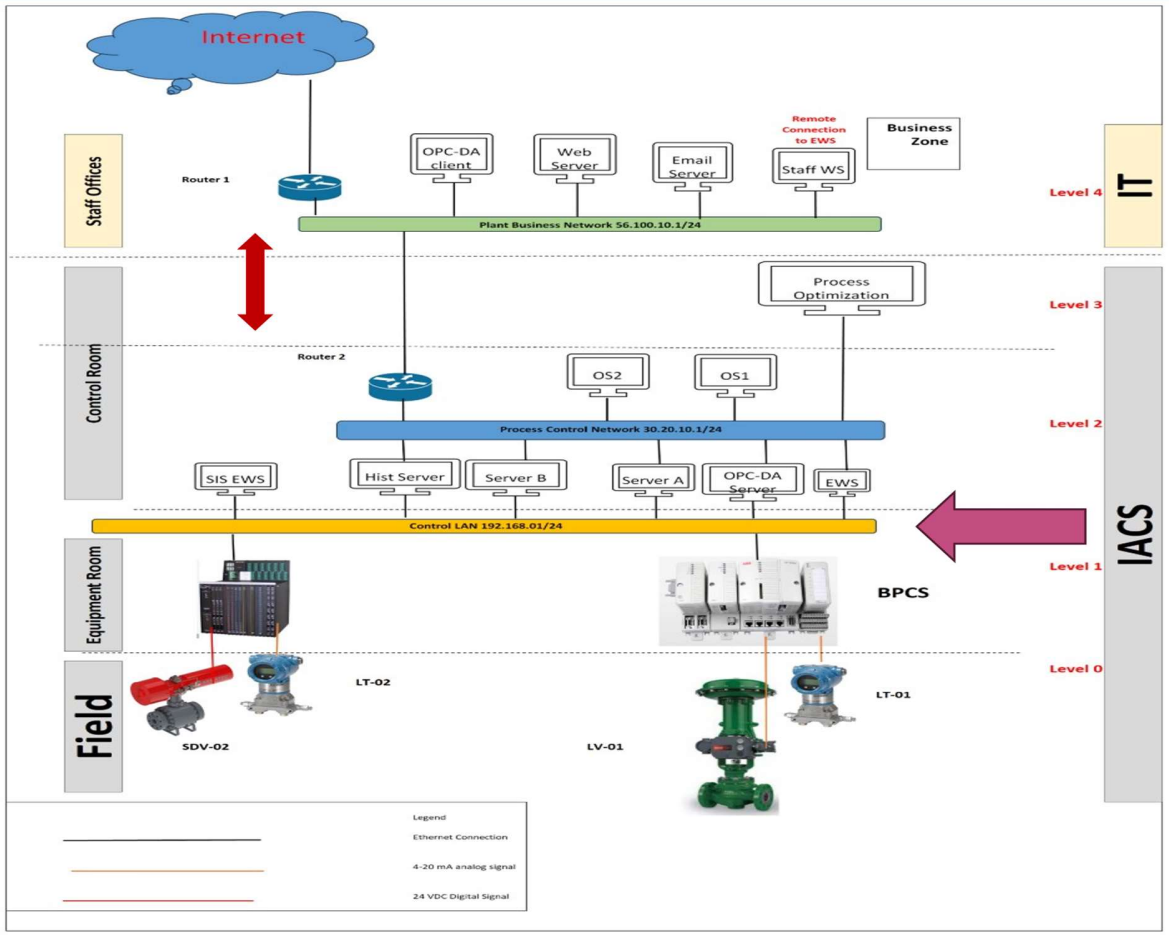
- Sensors to sense process parameters such as pressure, flow, level and temperature .
- Controllers such as **PLC** , **DCS** controllers , SCADA **RTU** , **VFD** ,etc. to control process parameters at required setpoints and to take actions according to implemented logic and control algorithms .
- Final control elements such as ON/Off valve, control valve, pump, motor, etc.

It is worthy mentioned that PLC and workstation are similar in components (Input , output and processor)

- Input for workstation is keyboard, output is screen and processor.
- Input to PLC is sensors, Out puts are finial control elements and processor.

LC is cyber asset like workstation but with different shape and different input and output methods.

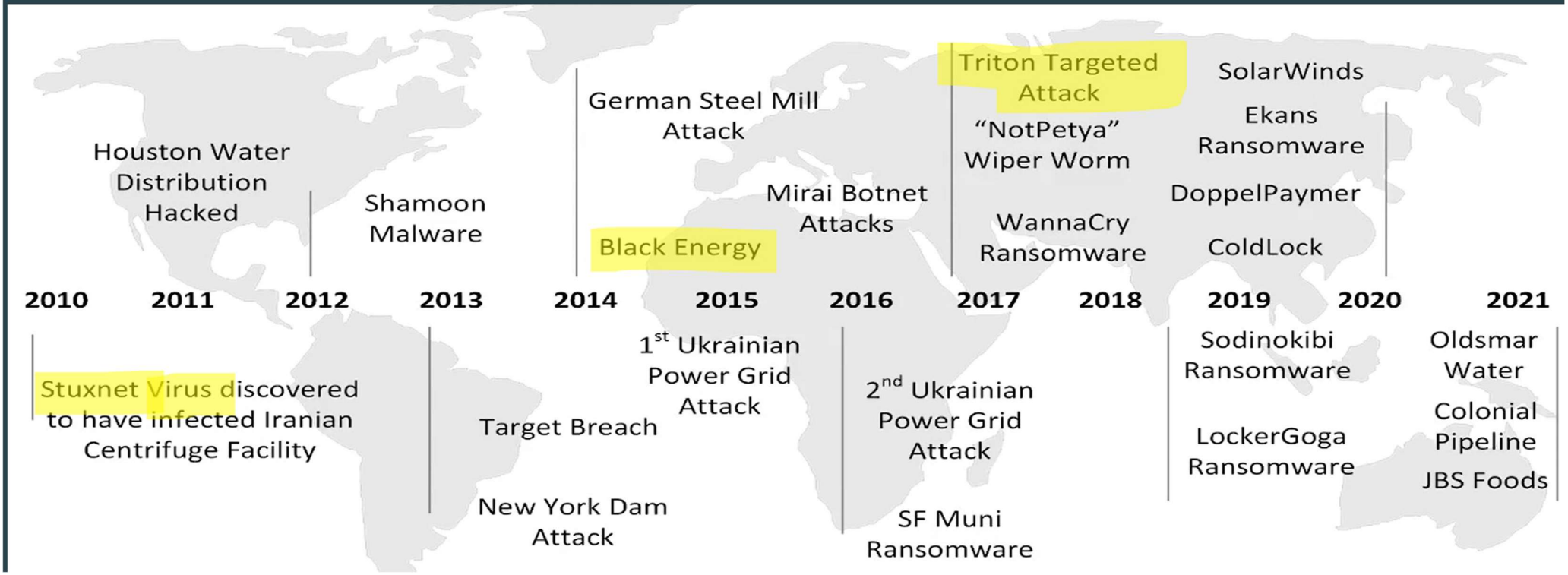
Industrial Control System architecture



The Industrial control system **ICS** infrastructures is like **IT** network structure contains same ethernet switches which used in IT networks which makes it vulnerable to the same **cyber threats** which threaten IT environment.

Isolation of **OT** and make it isolated **island** becomes impossible Due to rapid and spread **digitization** through transferring all process data for enterprise network which used in data analysis to help top management in decisions and enhance production optimization.

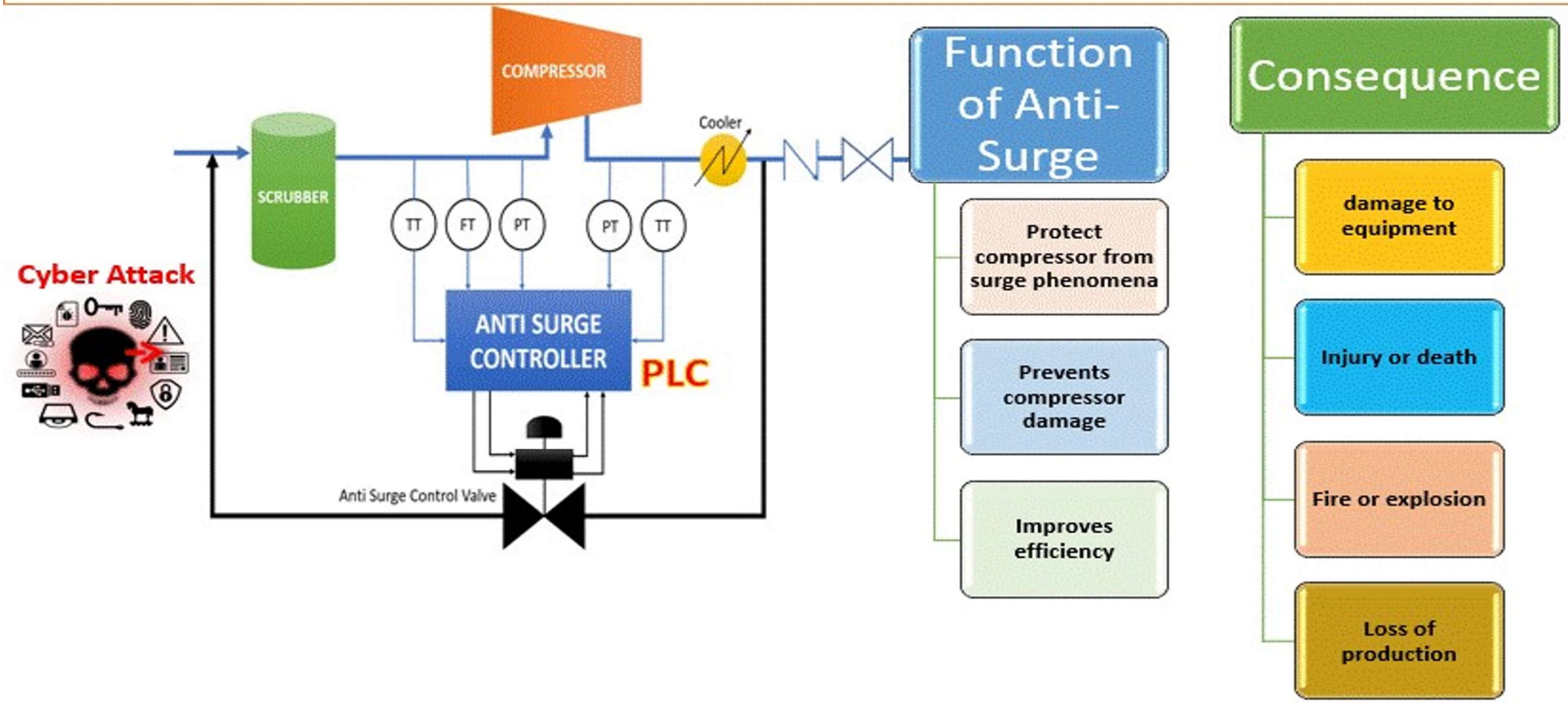
History of Cyber Incidents affected industrial control system



The History of cyber incident affected critical infrastructure all a lot such as:

- **Stuxnet** : is a malicious computer worm first uncovered in 2010 and is believed to be responsible for causing substantial damage to the nuclear program of Iran
- **Black Energy:** hackers using the Black Energy 3 malware remotely compromised information systems of three energy distribution companies in Ukraine and temporarily disrupted the electricity supply to consumers.
- **Triton Targeted Attack:** In August of 2017, TRITON malware was used to target and disrupt Safety Instrumented System (SIS) controllers within a Saudi petrochemical refinery.

Cyber attack effect on Anti-Surge Controller for Gas Compressor



- The **anti-surge** controller is one of the most critical control loops in a turbine or compressor. It is responsible for preventing the compressor from entering in surge, which can cause damage to the equipment.

- If a cyber attacker is able to successfully attack the anti-surge controller, they could change the parameters of the controller in a way that could lead compressor to surge.
- This could have **catastrophic** consequences, such as loss of production, damage to equipment, or even injury or death.

Trends in Control System Cybersecurity

Control systems use more commercial off the shelf (COTS) software and hardware

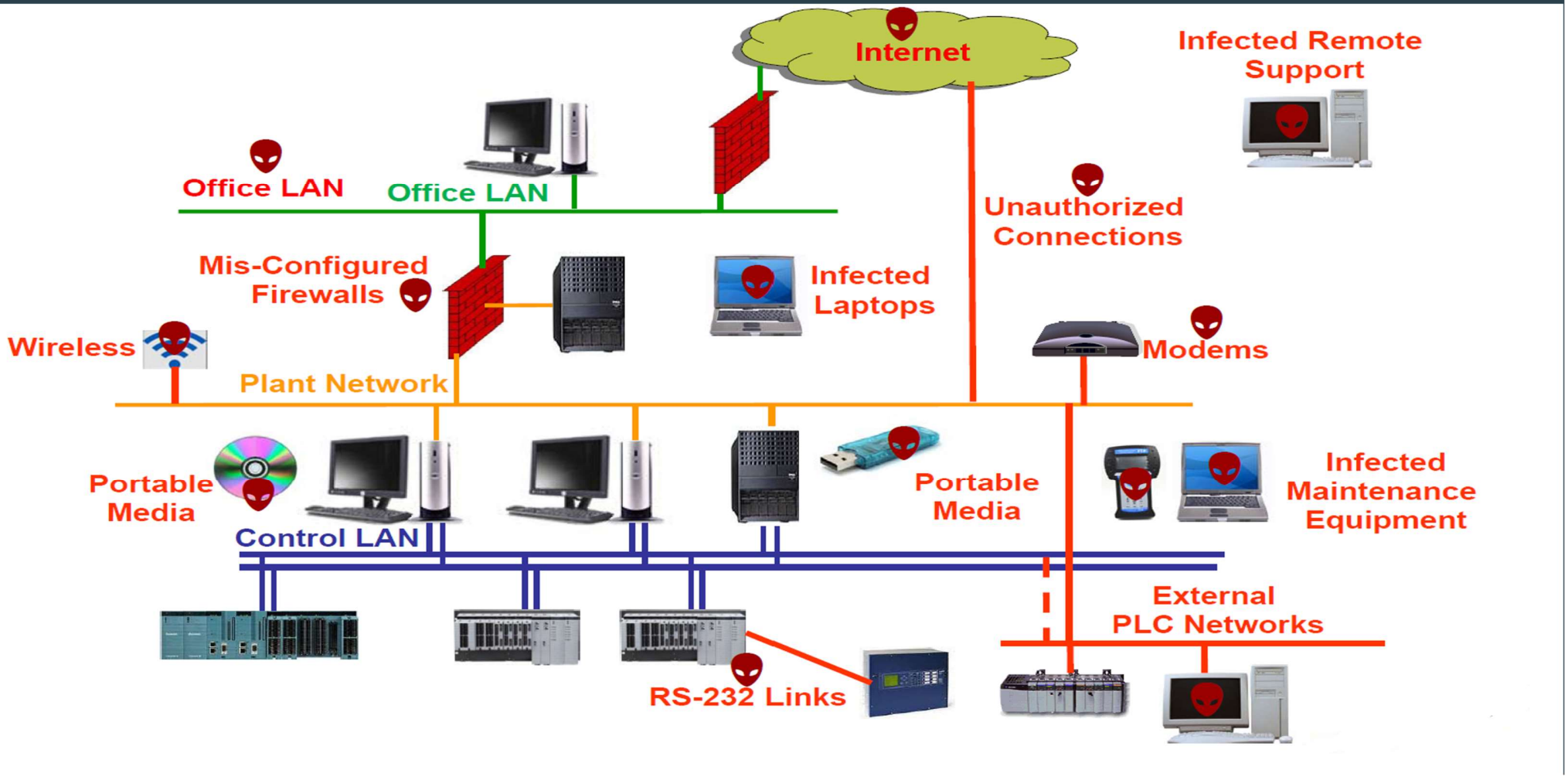
Common use of Internet Protocols (IP)

Increased use of remote monitoring and access

Businesses have reported more unauthorized attempts and marked increase in malicious code attacks and Isolation or network separation is difficult or impossible

Tools to automate attacks are commonlyavailable and Hacking become service you can buy , no need to be attacker to perform cyber attack

We Don't Connect to the Internet

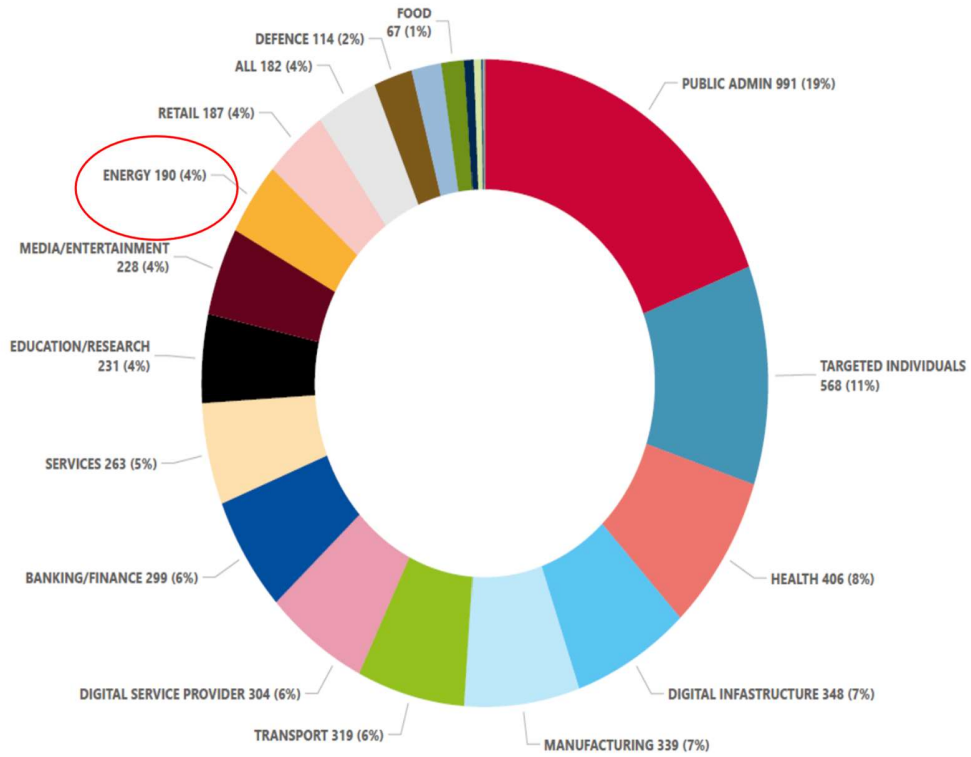


- Most of OT asset owners have concept that we are safe and away from cyber-attack but this not correct as, the industrial control system could be affected by infected **USB stick**, infected **engineering laptop**, infected remote connection and misconfigured **firewall** between OT and IT.

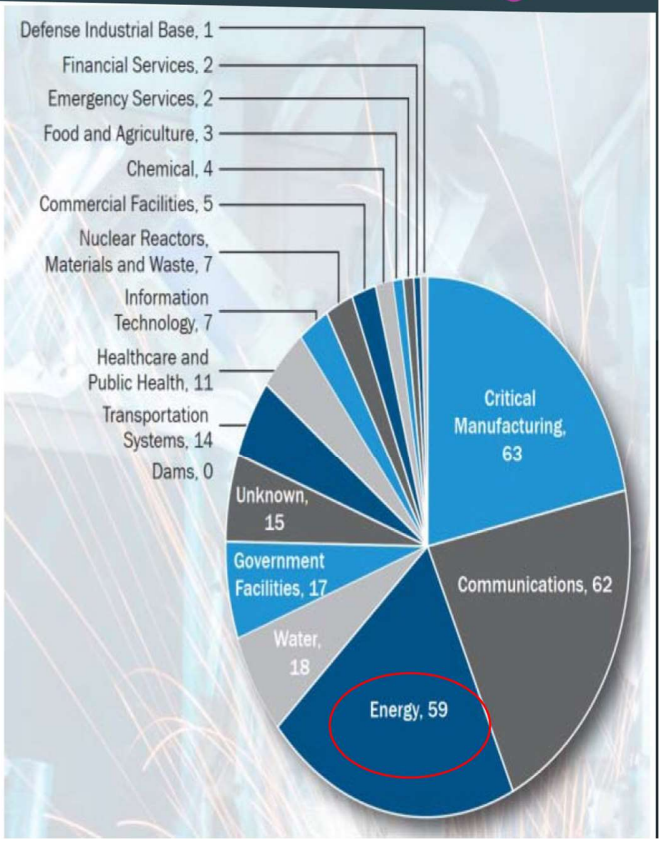
- **OT cybersecurity** concerned about maintaining availability and integrity of OT assets from human error of operation and maintenance teams not only **cybercriminal.**

Our Facility is Not a Target

Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)



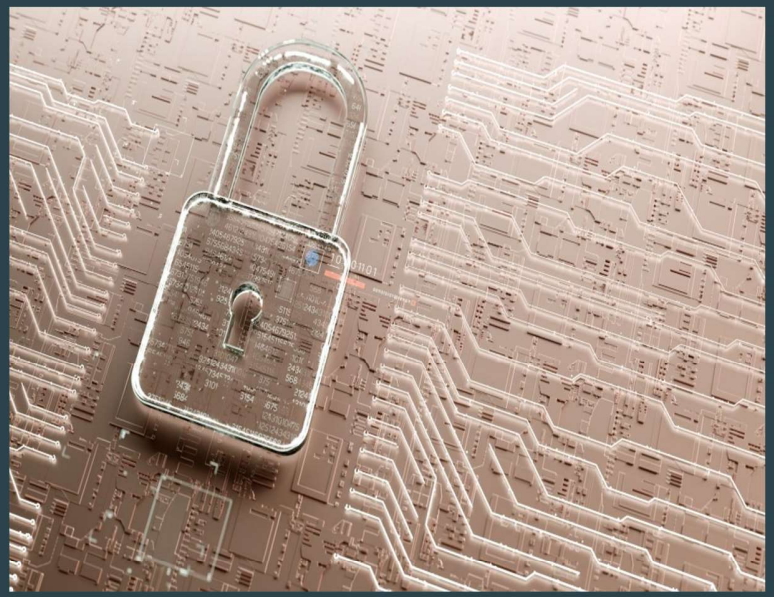
Incidents by sector
290 in 2016



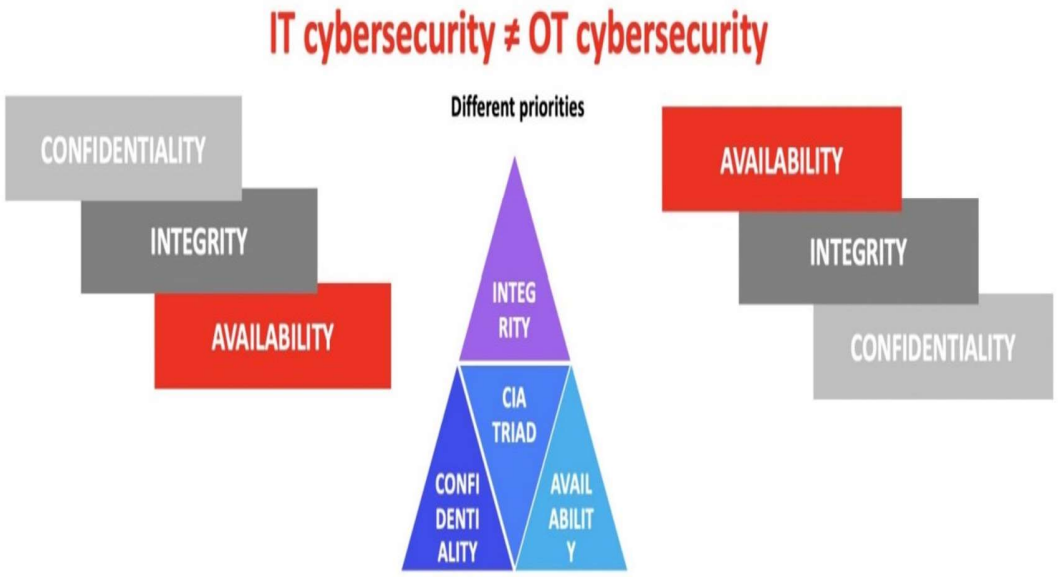
- **Cyber incident** targeted OT environment in different sectors increasing rapidly and for example cyber incident affected energy sector in las year was 190 in compared to 2016 was 59 cyber incidents.
- So **Asset owners** of critical infrastructure to take OT cybersecurity as priority to keep plants run smoothly and safely without production loss or incidents.

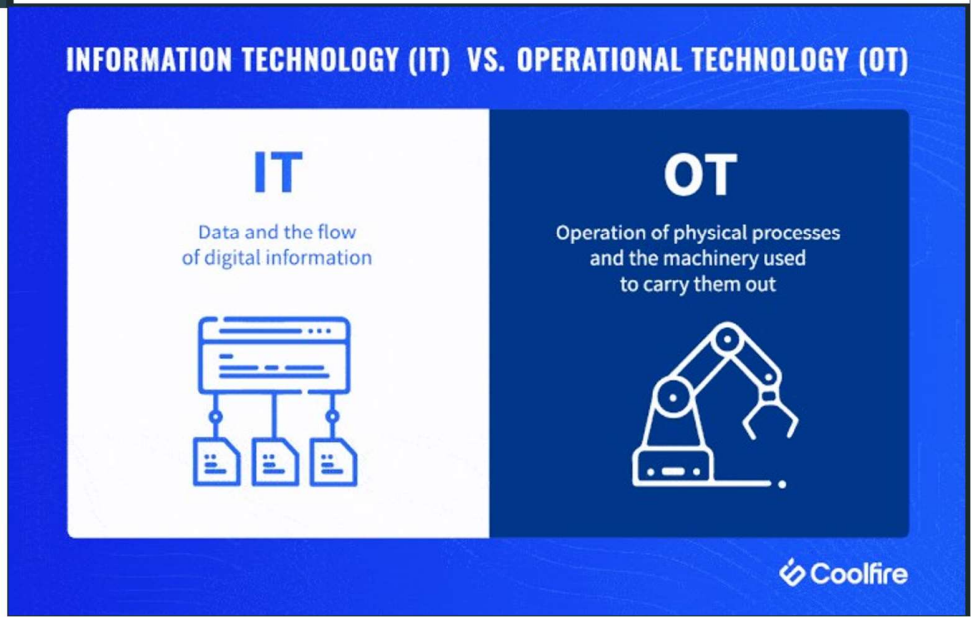
Could IT Cybersecuritysecure and protect industrial control system against cyberattack?

Answer :No



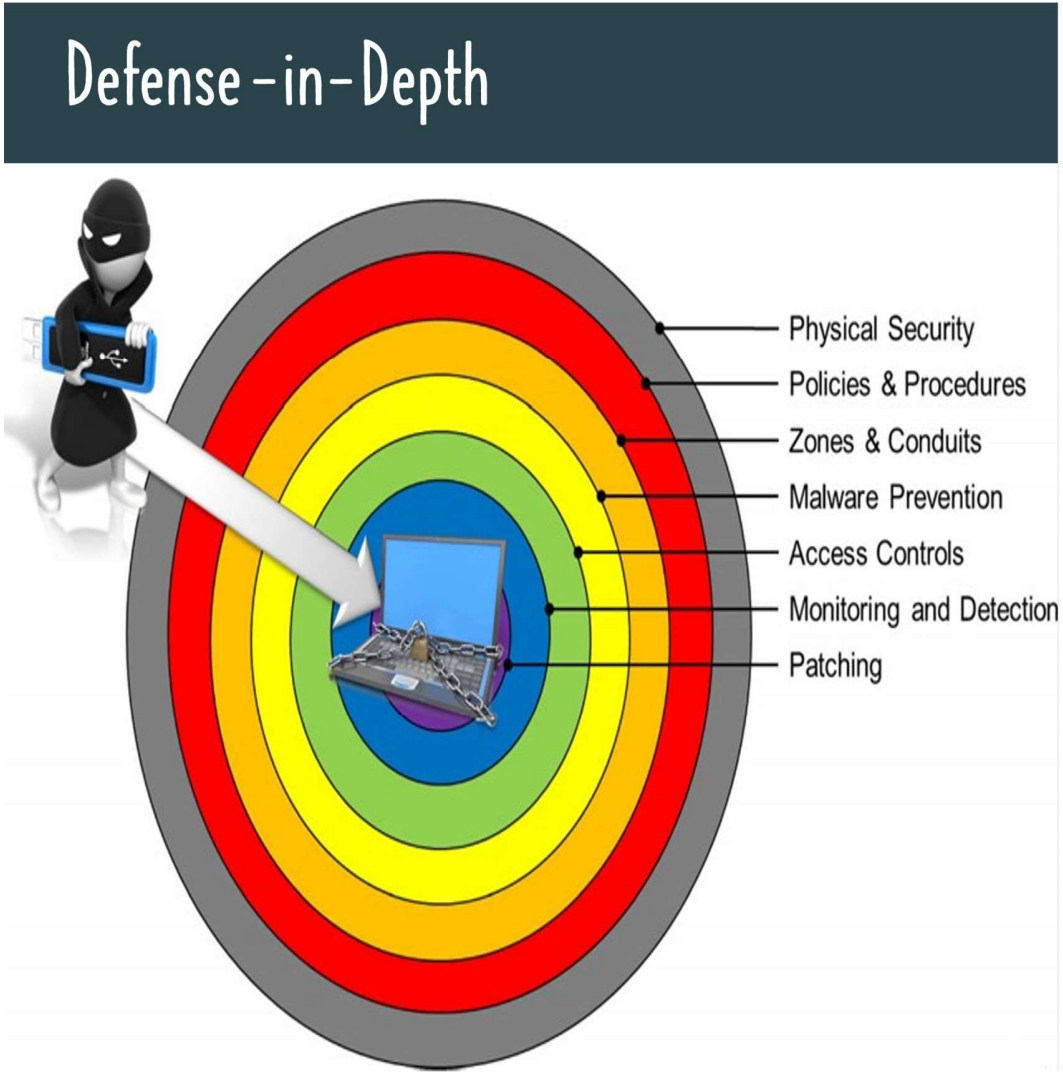
Difference Between Operation Technology OT and Information Technology IT

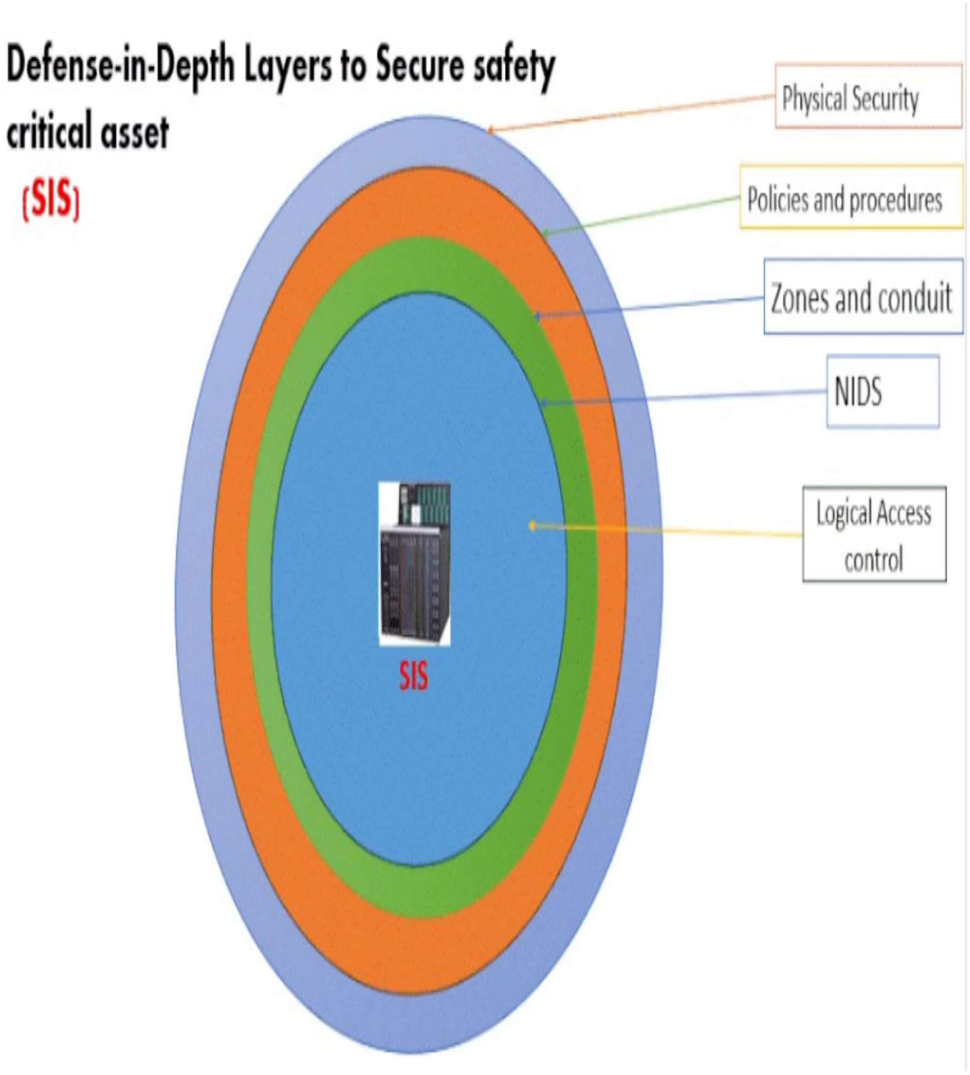




- The difference between OT and IT in priorities makes special Requirements to deal with OT cybersecurity to maintain its **availability** and **integrity** as OT deals with physical process.

- For example, in IT **patch management** is straightforward process, may be every month do it but in OT it required special precautions and permits to perform patch management for any controllers.
- Another example is in IT realm it is easy to **restart** workstation but in OT is not permitted.

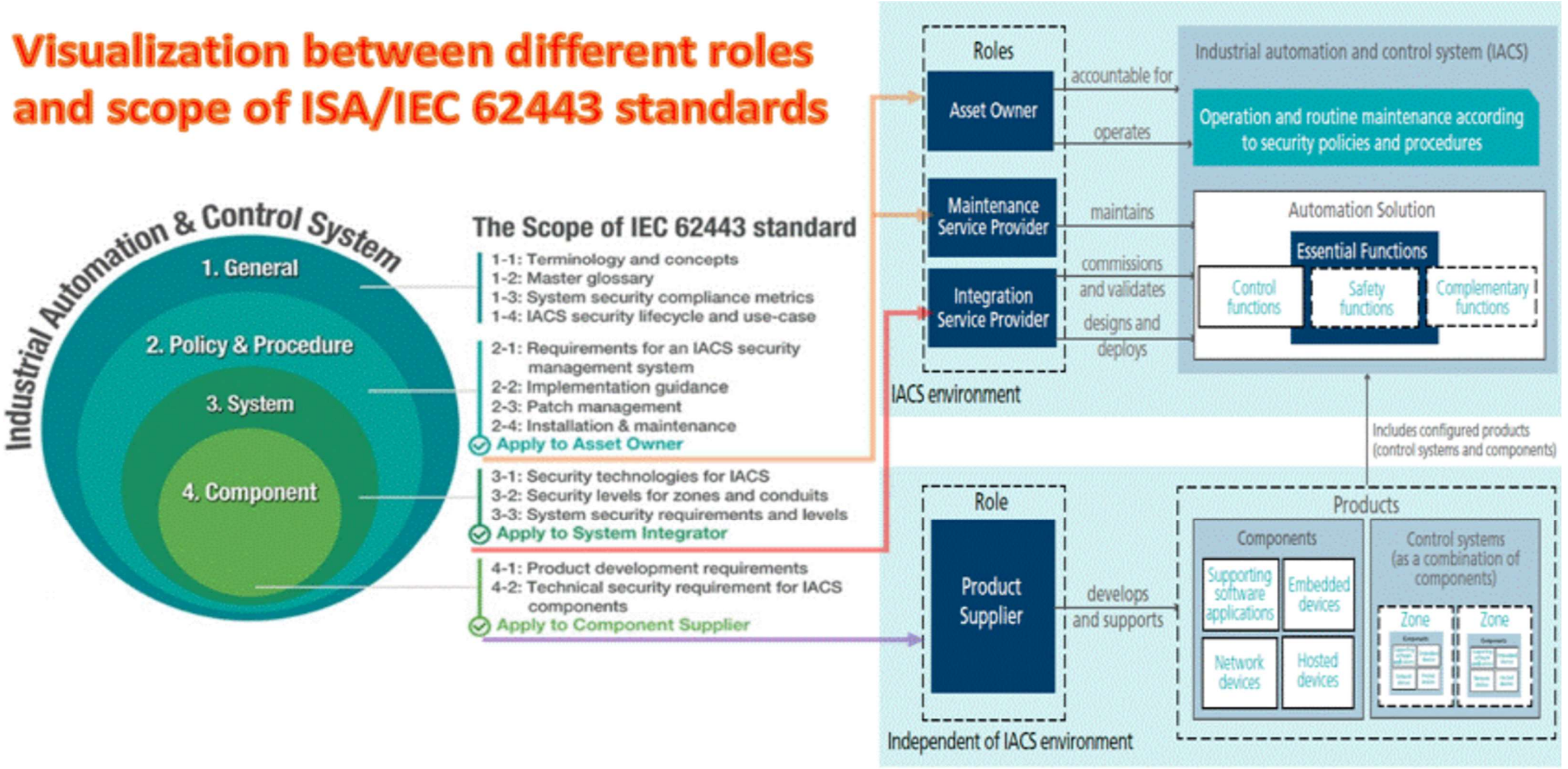




- Due to high risk which could results from high consequences in case of lost availability or integrity of industrial control system, So It is very important to protect industrial control system by applying multiple layers of defense.

- This is called a **defense-in-depth** (D-ID) strategy. It means that if one layer of security is breached, the subsequent layers will still be able to prevent the attack.
- The selection of these layers should be the result of an effective cyber risk assessment. This assessment should identify the specific threats and vulnerabilities to industrial control system and then select the most appropriate cybersecurity countermeasures to mitigate those cyber risks.

Visualization between different roles and scope of ISA/IEC 62443 standards



- **ISA/IEC 62443** standards are the most popular in OT cybersecurity contains 14 publications.
- It divides the cybersecurity topics by stakeholder category / roles including:
  - the operator,
  - the service providers (service providers for integration and for maintenance)
  - the component/system manufacturers.
- The different roles each follow a risk-based approach to prevent and manage security risks in their activities.
- **ISA/IEC 62443-2-1** "Security program requirements for IACS asset owners" is directed to asset owner to help in issue cyber security management system.