SIU Southern Illinois University
CARBONDALE

Department of Computer Science
Southern Illinois University Carbondale

CS 491/531
SECURITY IN CYBER-PHYSICAL SYSTEMS

Lecture 5: Industrial Networks

DR. ABDULLAH AYDEGER

LOCATION: ENGINEERING A 409F

EMAIL: AYDEGER@CS.SIU.EDU

Outline

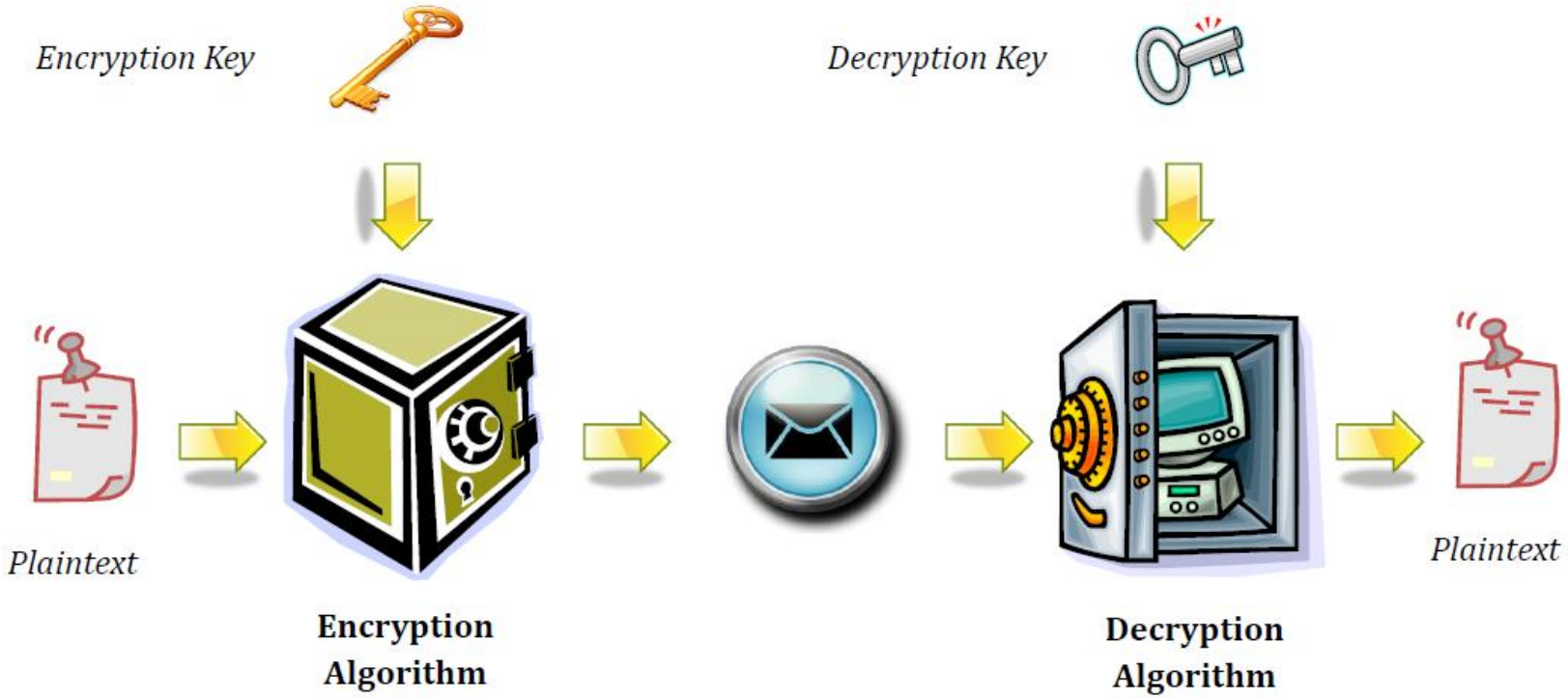
Naming in CPS

Abstract Models for CPS Domains

- Industrial Control Systems
- Smart Grid
- Medical
- Vehicles

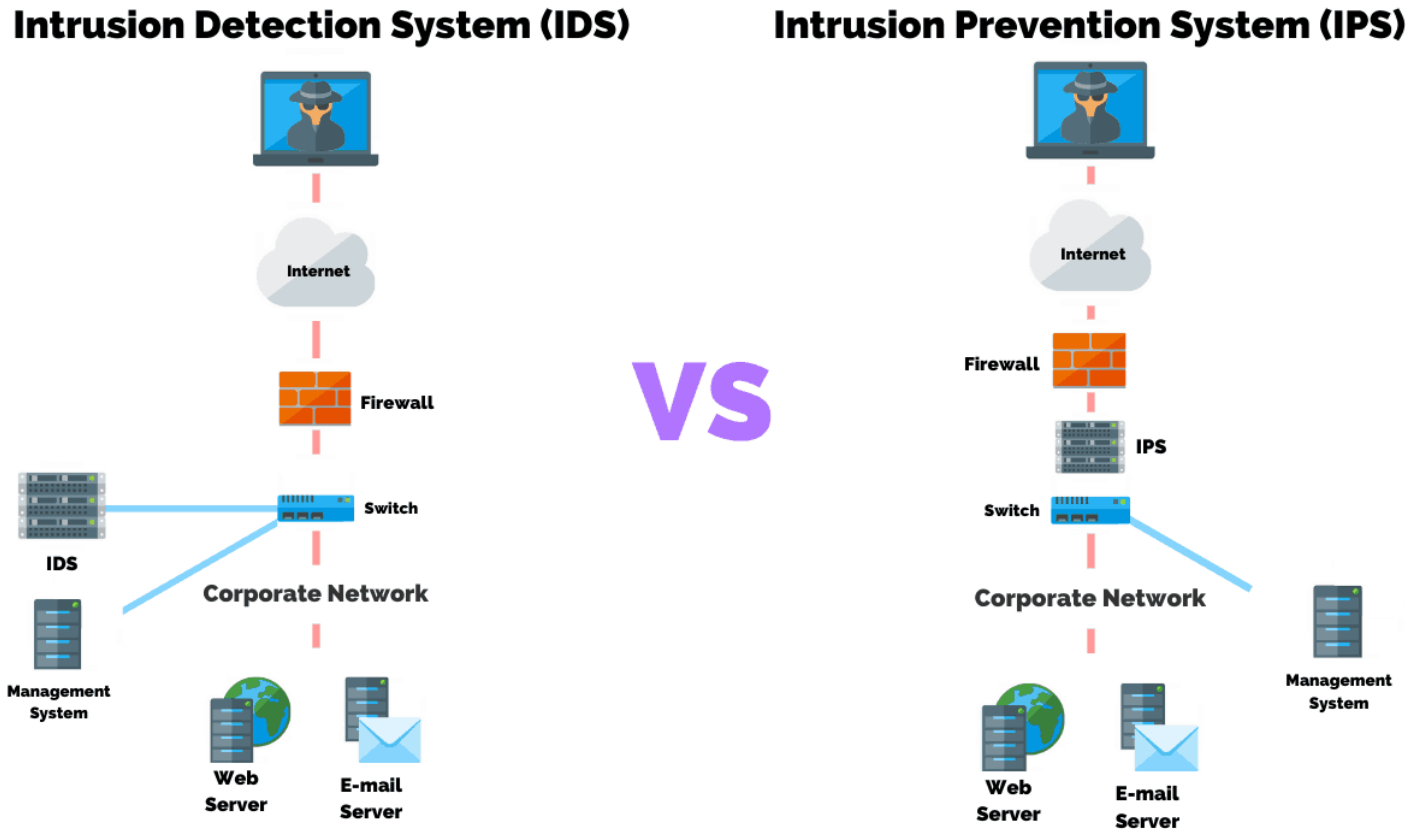
Recall: Cybersecurity Tools

Encryption: Symmetric and Asymmetric



Recall: Cybersecurity Tools

IPS vs IDS



Different naming in CPS

CPS can be called different names, depending on the application using them. For example:

- A very important and representative CPS is the Supervisory Control and Data Acquisition (SCADA) system, which is used in Critical Infrastructure (CI) such as the Smart Grid and **Industrial Control Systems (ICS)**
- Other examples have emerged in medical devices such as wearable and implantable medical devices
- In addition, a network of small control systems are embedded in modern cars to improve fuel efficiency, safety, and convenience

Industrial Control Systems (ICS)

Refers to control systems used to enhance the control, monitoring, and production in different industries such as the nuclear plants, water and sewage systems, and irrigation systems

Sometimes ICS is called *Supervisory Control and Data Acquisition* (SCADA) or *Distributed Control Systems* (DCS) => For consistency, we will use the term ICS

Different controllers with different capabilities collaborate to achieve numerous expected goals

- A popular controller is the *Programmable Logic Controller* (PLC), which is a microprocessor designed to operate continuously in hostile environments

Industrial Control Systems (ICS)

Field device is connected to the physical world through sensors and actuators

- Usually, it is equipped with wireless and wired communication capacity that is configured depending on the surrounding environments
- It can also be connected to PC systems in a control center that monitors and controls the operations

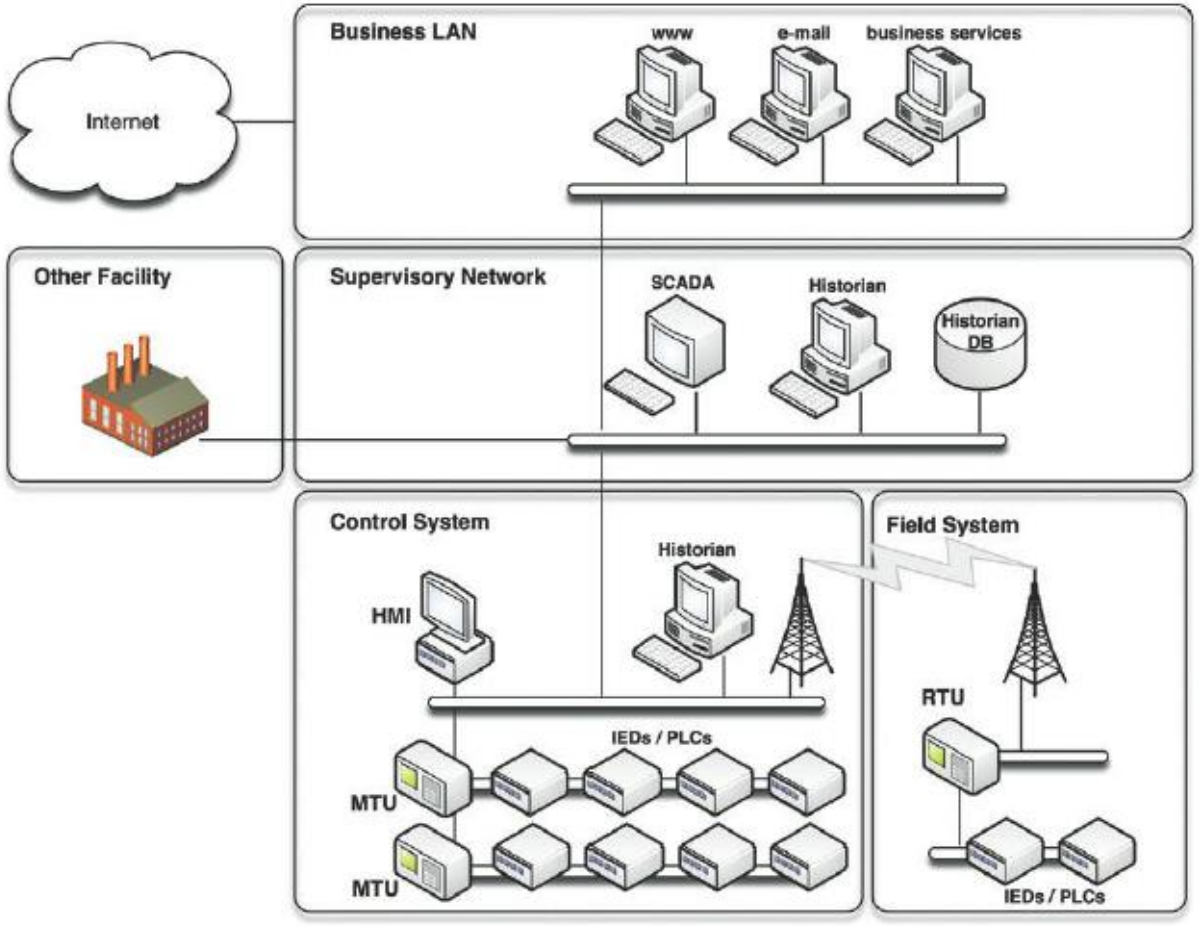
Industrial Networks

SCADA is just one specific piece of an industrial network, separate from the control systems themselves

- These control systems can be referred to as Industrial Control Systems (ICS), Distributed Control Systems (DCS), or Process Control Systems (PCS)

Each area has its own physical and logical security considerations, and each has its own policies and concerns

Sample Industrial Automated Control System Network



Critical Infrastructure

Utilities

Nuclear Facilities

Bulk Electric

Chemical Facilities

Smart Grid Systems

The smart grid is envisioned as the next generation of the power grid that has been used for decades for electricity generation, transmission, and distribution

The smart grid provides several benefits and advanced functionalities:

- At the national level, it provides enhanced emission control, global load balancing, smart generation, and energy savings
- At the local level, it allows home consumers better control over their energy use that would be beneficial economically and environmentally

Medical Devices

Integrating cyber and physical capabilities to deliver better health care services

- Medical devices with cyber capabilities that have physical impact on patients
  - Such devices are either implanted inside the patient's body, called Implantable Medical Devices (IMDs),
  - Or worn by patients, called wearable devices
    - Wearable devices communicate with each other or with other devices, such as a remote physician or smartphone

They are usually equipped with wireless capabilities to allow communication with other devices such as the programmer, which is needed for updating and reconfiguring the devices

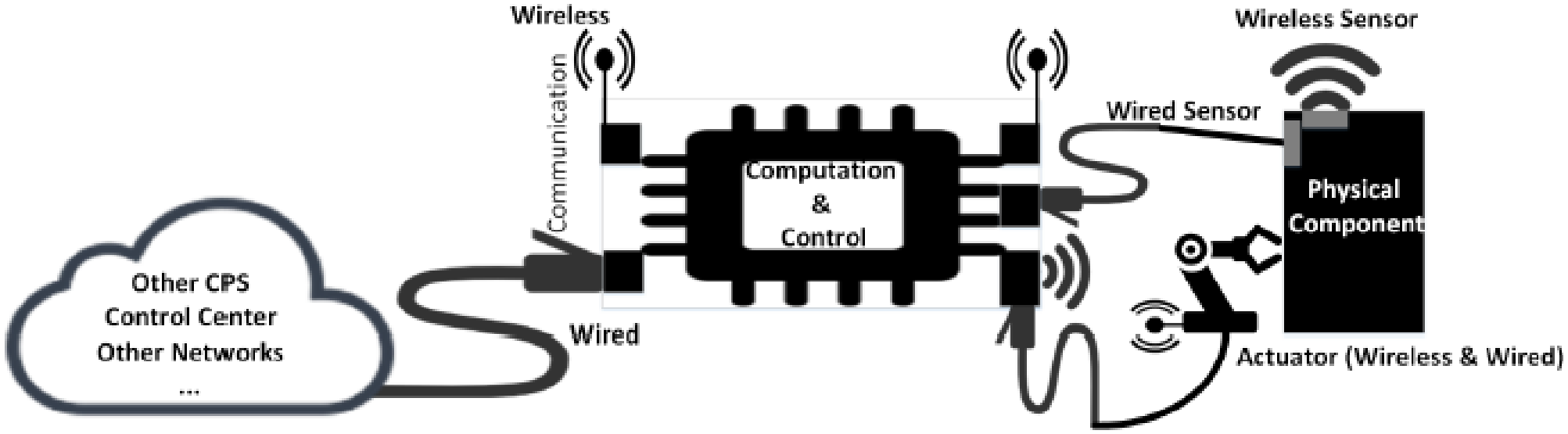
Smart cars/Modern vehicles

More environment-friendly, fuel-efficient, safe, and have enhanced entertainment and convenience features

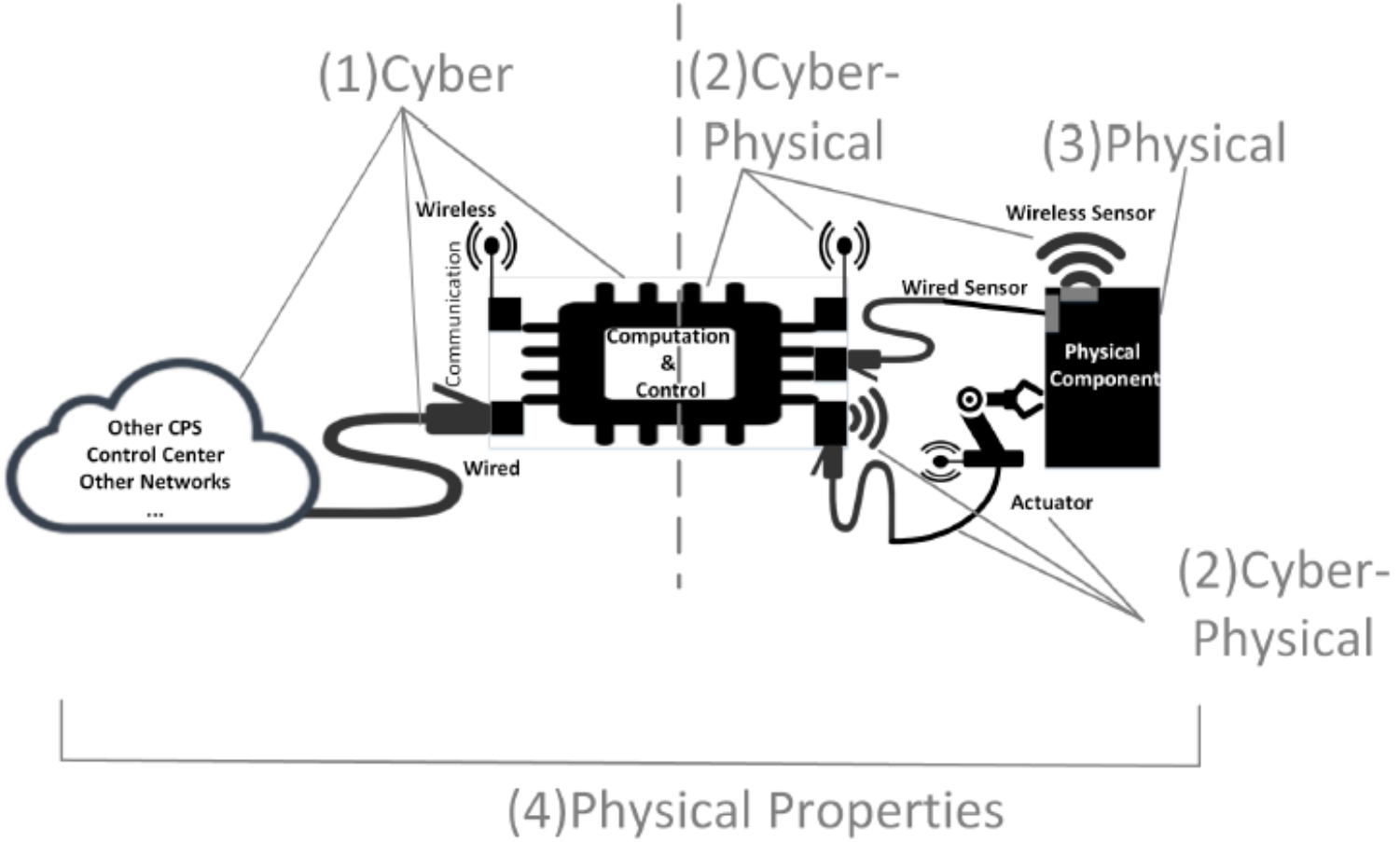
These advancements are made possible by the reliance on a range of 50 to 70 computers networked together, called Electronic Control Units (ECUs)

- ECUs are responsible for monitoring and controlling various functions such as engine emission control, brake control, entertainment (radio, multimedia players) and comfort features (cruise control)

CPS: Abstract Model

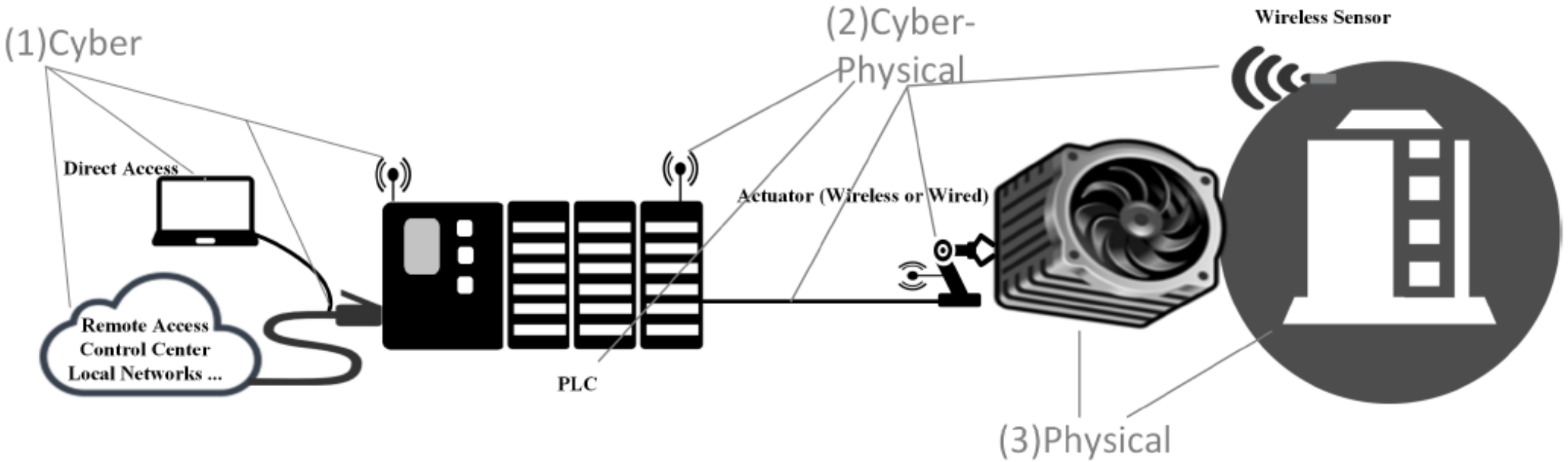


CPS: Abstract Model



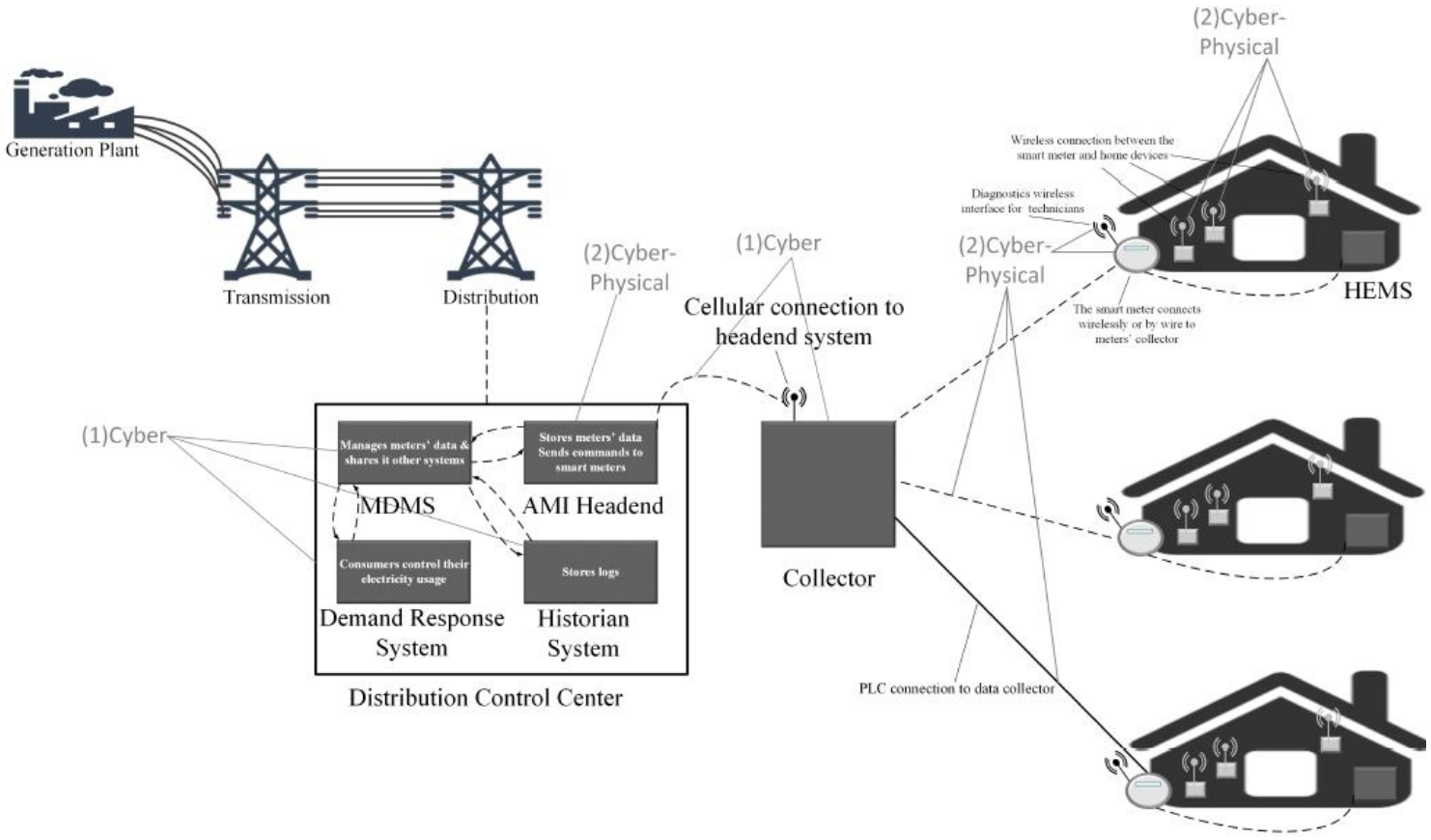
CPS aspects in ICS

CPS aspects in a Programmable Logic Controller (PLC) scenario, where it is used for controlling the temperature in a chemical plant

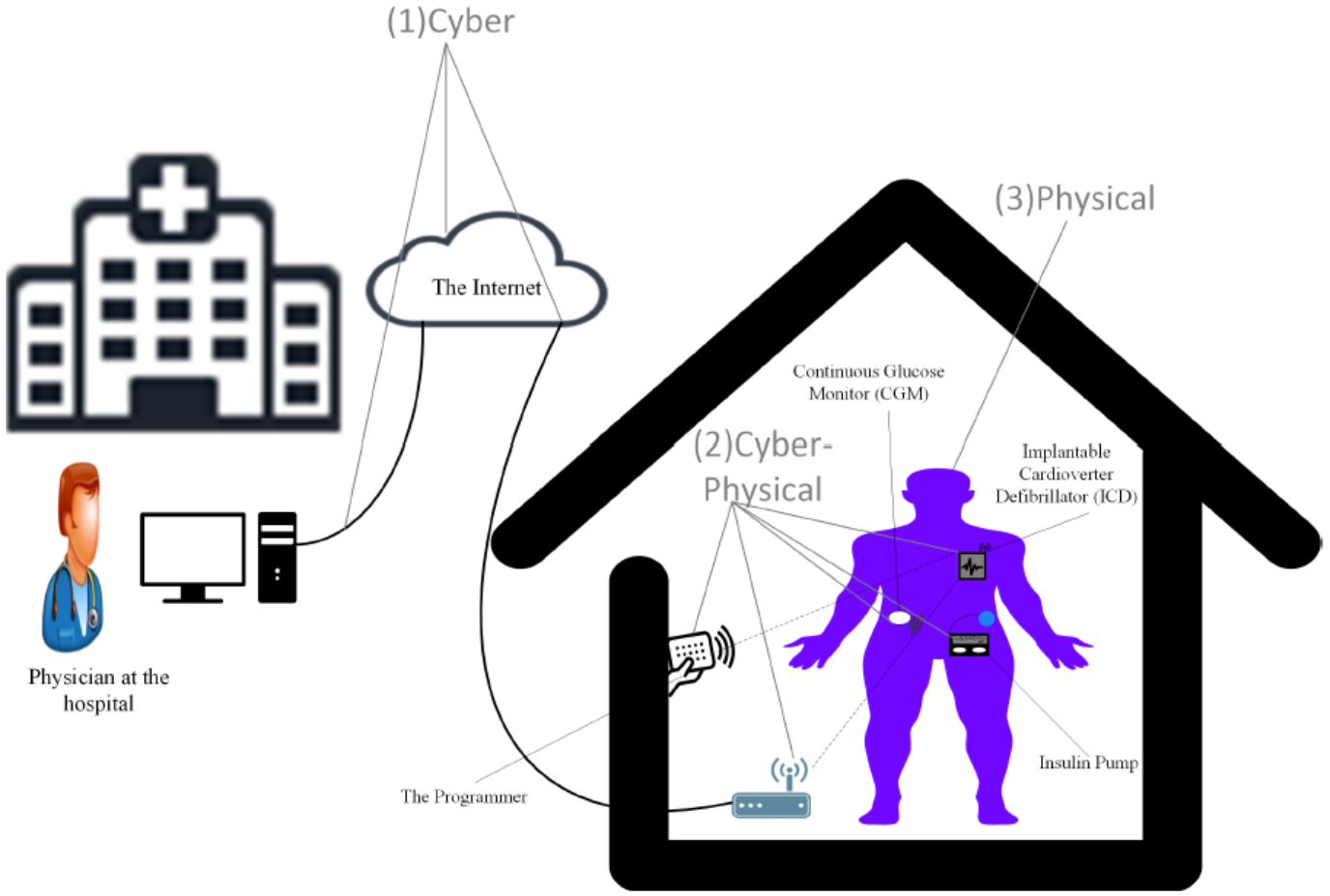


CPS aspects in the Smart Grid

A smart meter is attached to every house to provide utility companies with more accurate electricity consumption data and customers with convenient way to track their usage information



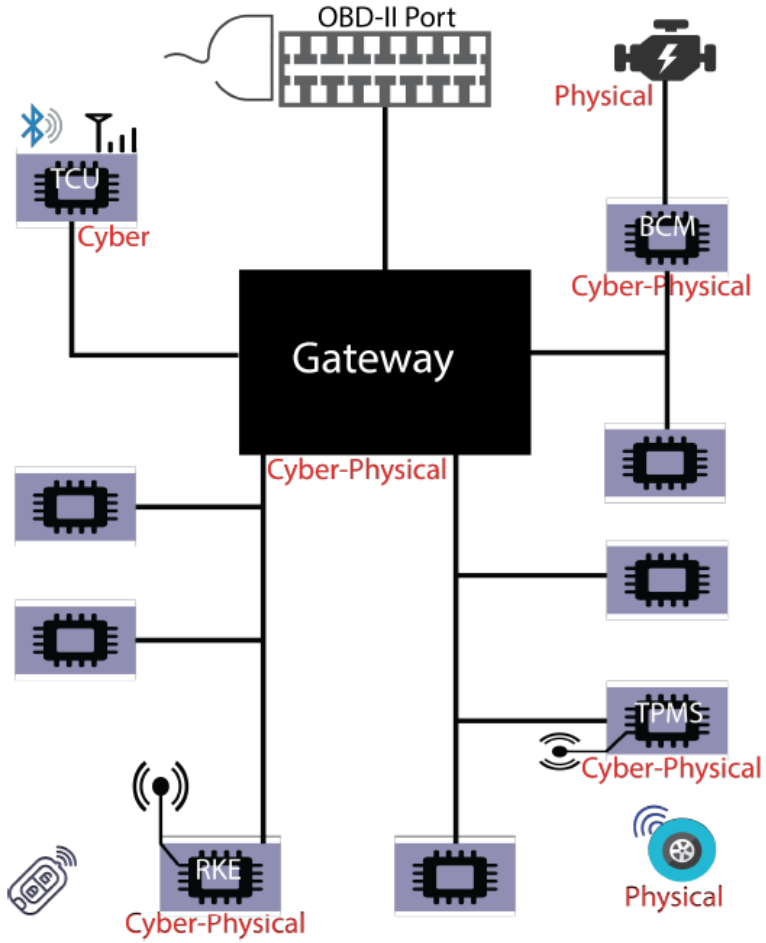
CPS aspects in medical devices



CPS aspects in smart cars

Controller Area Network (CAN) bus is important for two reasons:

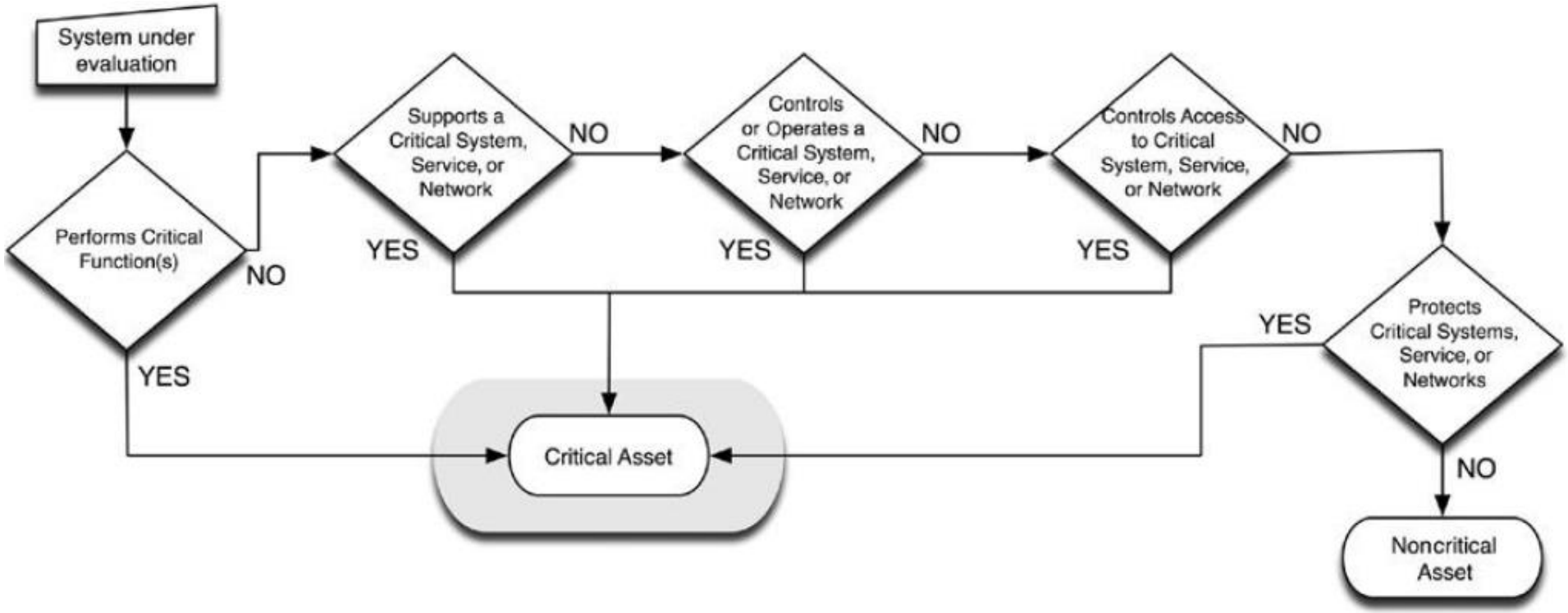
- Most security issues result from CAN-based networks
- It has been required to be deployed in all cars in the U.S. since 2008, thus it is in almost every car around us
  - Heard of OBD2?



Common Industrial Security Recommendations

Identification of Critical Systems

- Critical Assets
- Noncritical Assets

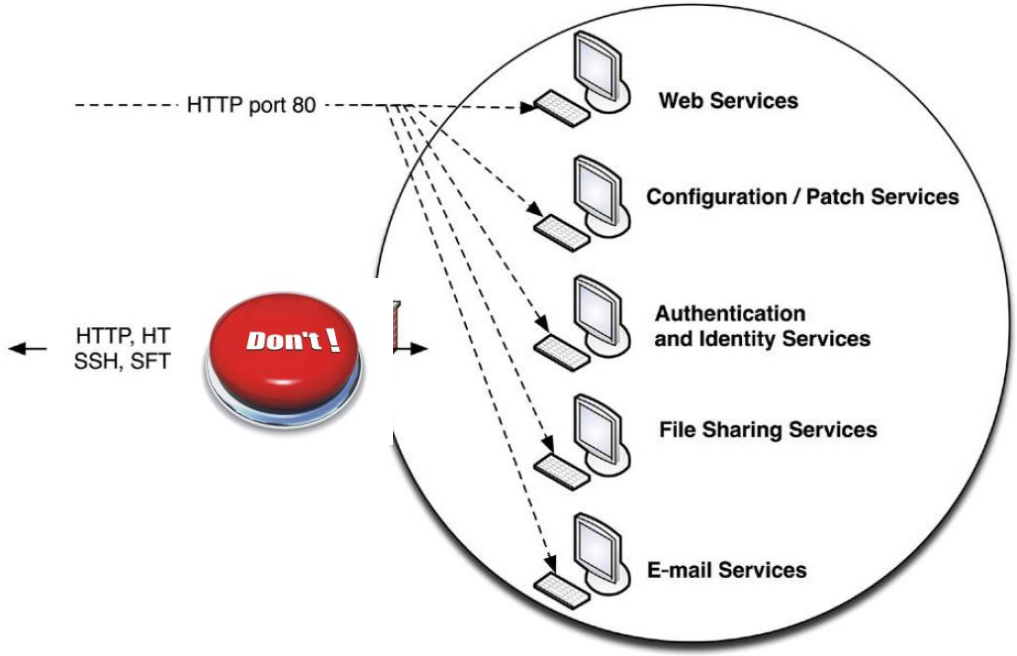


Common Industrial Security Recommendations

Network Segmentation/Isolation of Systems

The separation of assets into functional groups allows specific services to be tightly locked down and controlled;

- One of the easiest methods of reducing the attack surface that is exposed to attackers
- Simply by disallowing all unnecessary ports and services, we also eliminate all vulnerabilities—known or unknown—that could potentially allow an attacker to exploit those services



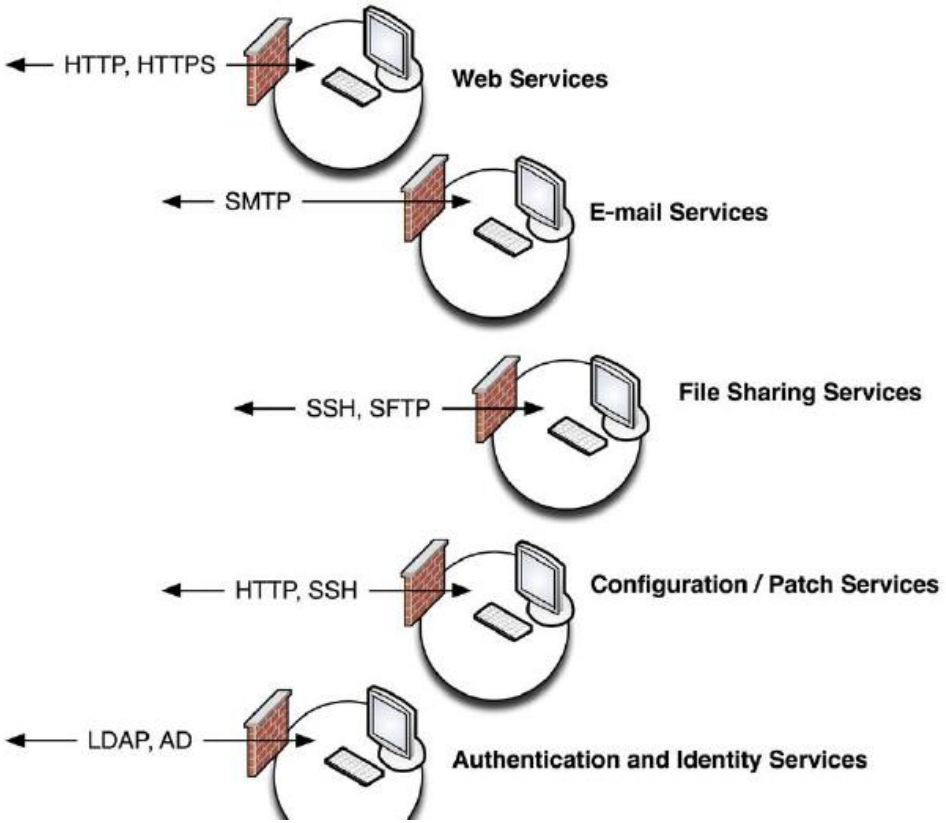
Placing All Services Behind a Common Defense Provides a **Broader** Attack Surface on All Systems

Common Industrial Security Recommendations

Network Segmentation/Isolation of Systems

If each specific service is grouped functionally and separated from all other services,

- All web servers are grouped together in one group, all e-mail services in another group, etc.
  - The firewall can be configured to disallow anything other than the desired service, preventing an e-mail server from being exposed to a threat that exploits a weakness in HTTP



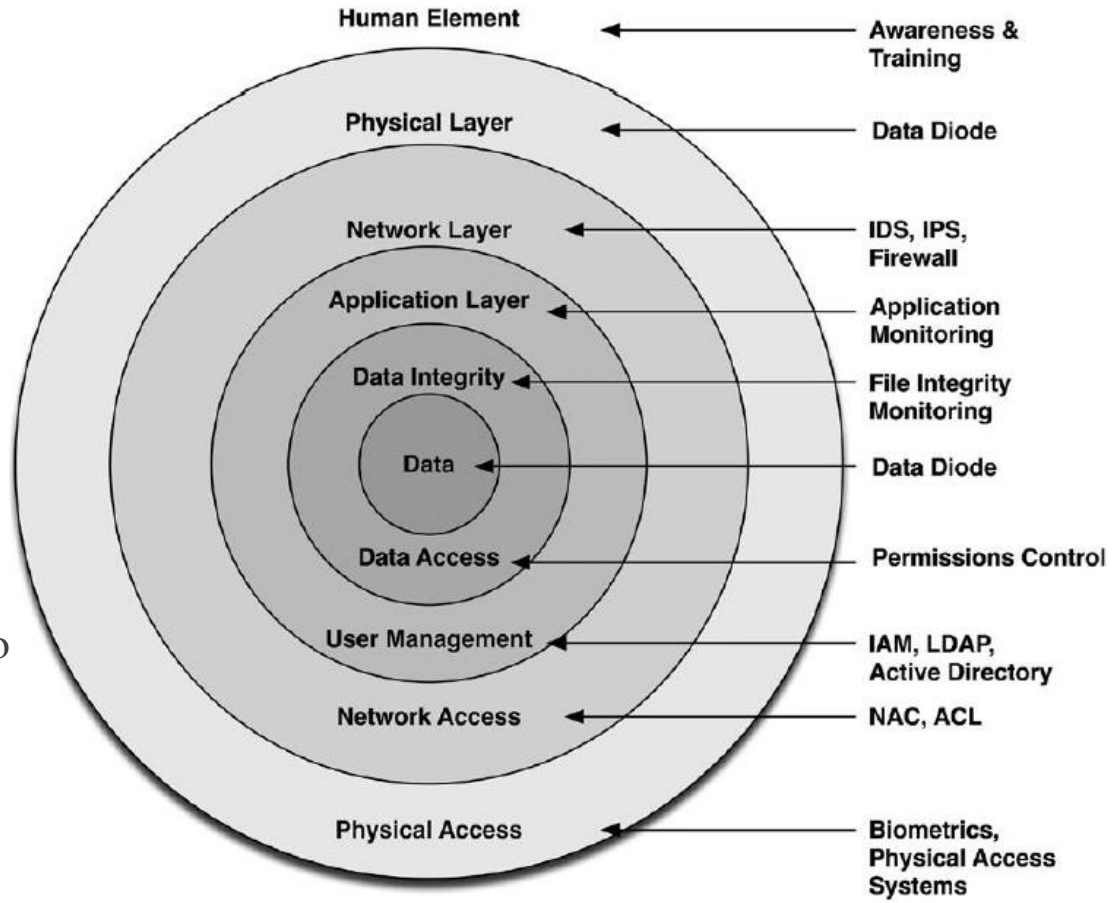
Separation into Functional Groups Reduces the Attack Surface to a Given System

Common Industrial Security Recommendations

Defense in Depth

Layered or tiered defensive strategy

- The layers of the networks
- Physical or Topological layers consisting of subnetworks and/or functional groups
- Policy layers, consisting of users, roles, and privileges
- Multiple layers of defense devices at any given demarcatio point (such as implementing a firewall and an IDS or IPS)



Common Industrial Security Recommendations

Access Control

By locking down services to specific users or groups of users, it becomes more difficult for an attacker to identify and exploit systems.

- The further we can lock down access, the more difficult an attack becomes

One example:

- Only allow a user to authenticate during that user's shift (user credentials combined with personnel management)

Common Industrial Security Recommendations

Access Control:

- The strength of access controls increases as a user's identity is treated with the additional context of that user's roles and responsibilities within a functional group

Good	Better	Best
User accounts are classified by authority level	User accounts are classified by functional role	User accounts are classified by functional role and authority
Assets are classified in conjunction with user authority level	Assets are classified in conjunction with function or operational role	Assets are classified in conjunction with function and user authority
Operational controls can be accessed by any device based on user authority	Operational controls can be accessed by only those devices that are within a functional group	Operational controls can only be accessed by devices within a functional group by a user with appropriate authority

Importance of Securing ICS

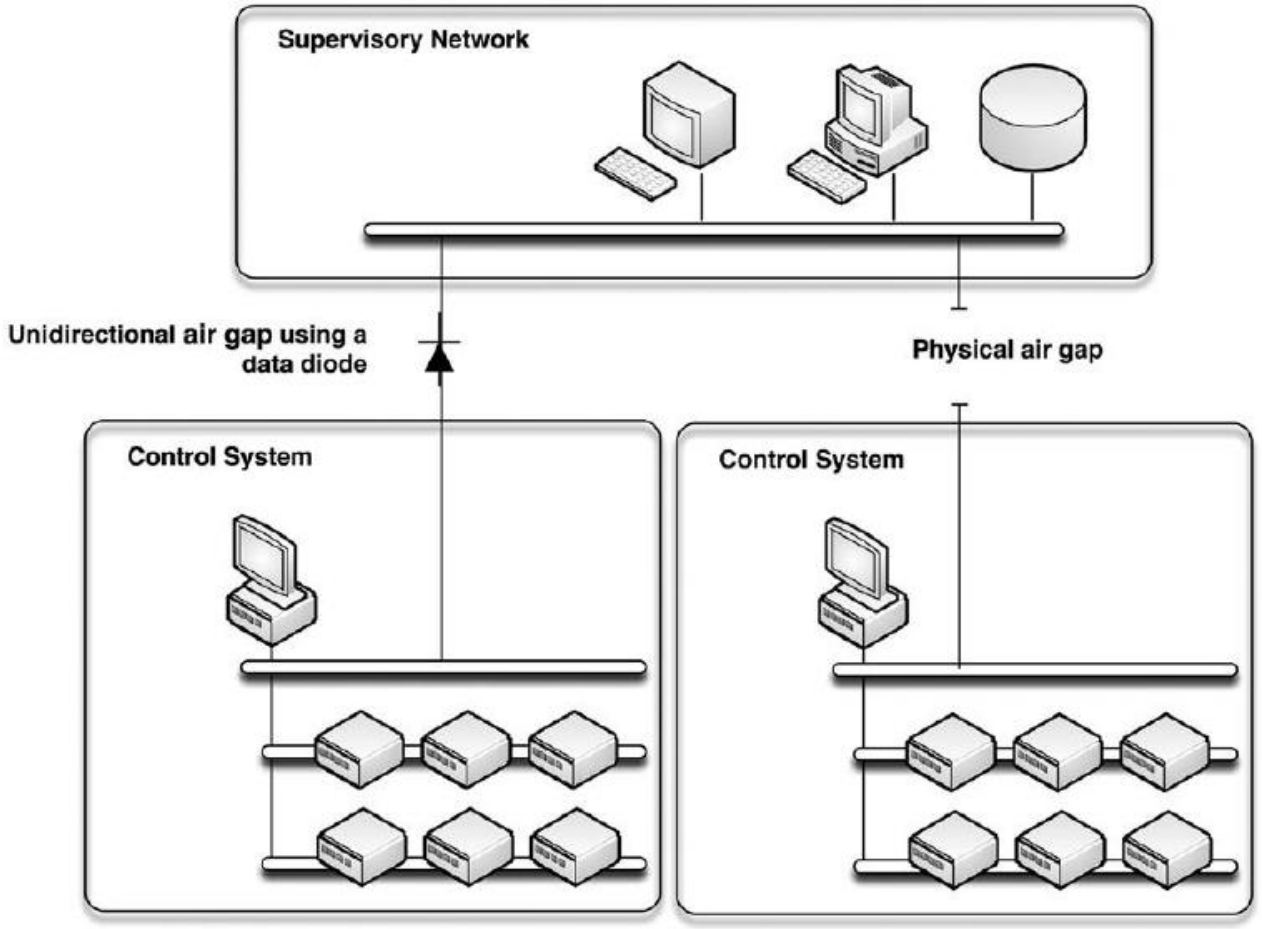
Many industrial systems are built using legacy devices

- In some cases running legacy protocols that have evolved to operate in Internet

Before the proliferation of Internet connectivity, web-based applications, and real-time business information systems, energy systems were built for reliability

- Physical security was always a concern, but information security was not a concern, because the control systems were air-gapped:
  - That is, physically separated with no common system (electronic or otherwise) crossing that gap

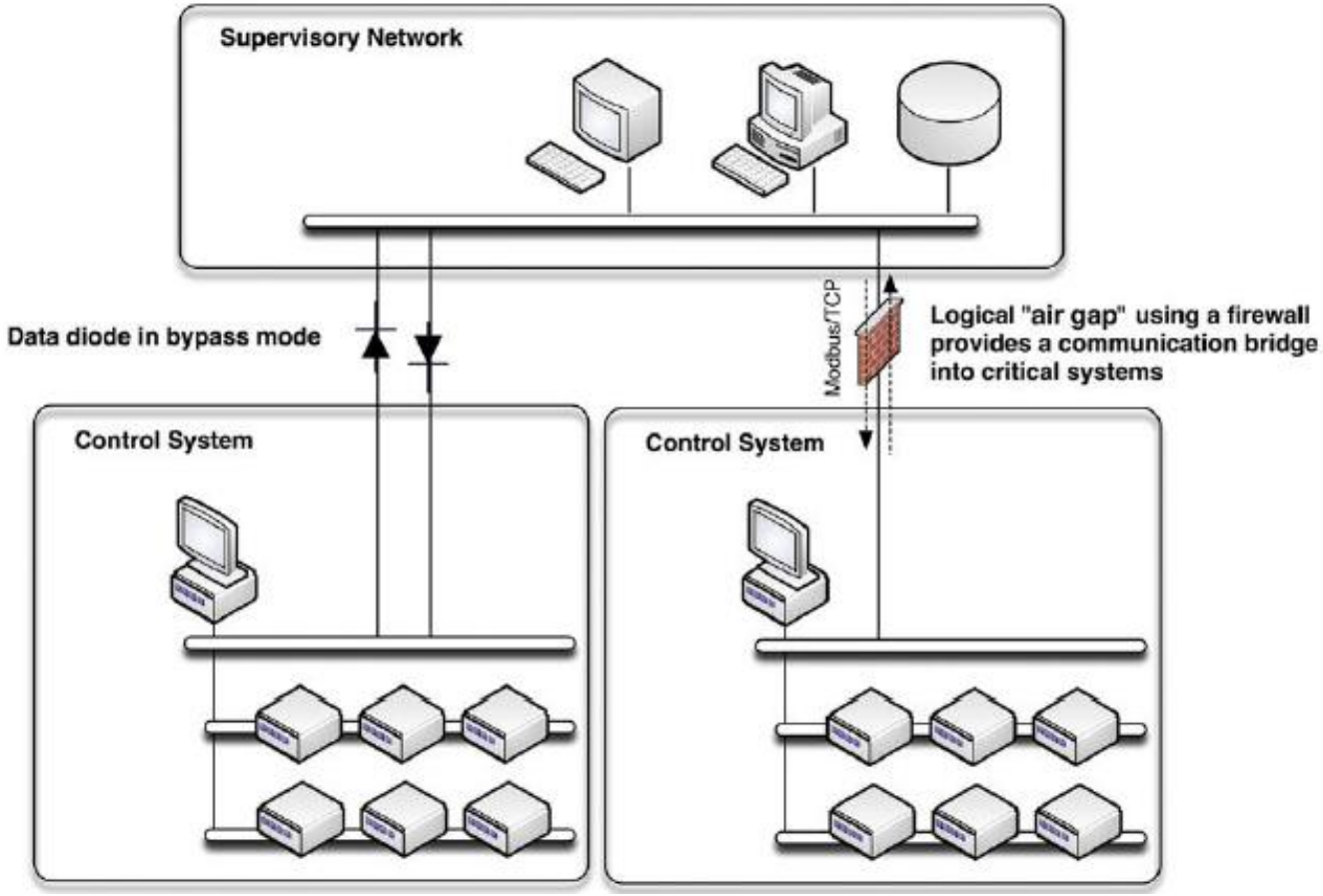
ICS Air Gap Separation



ICS: The Reality of the Air Gap

There is now a path into critical systems

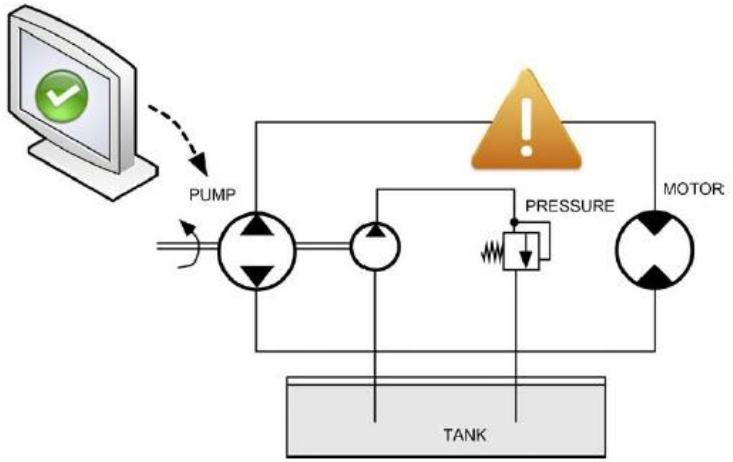
- Any path that exists can be found and exploited



Impact of ICS Incidents

Safety Controls

- To avoid catastrophic failures, most industrial networks employ automated safety systems
- Many of these safety controls employ the same messaging and control protocols used by the industrial control network's operational processes, and in some cases, such as certain fieldbus implementations, the safety systems are supported directly within the same communications protocols as the operational controls, on the same physical media



The Potential Impact of Successful Cyber Attacks

Incident Type	Potential Impact
Change in a system, operating system, or application configuration	Introduction of command and control channels into otherwise secure system Suppression of alarms and reports to hide malicious activity Alteration of expected behavior to **produce unwanted and unpredictable results**
Change in programmable logic in PLCs, RTUs, or other controllers	Damage to equipment and/or facilities Malfunction of the process (shutdown) Disabling control over a process
Misinformation reported to operators	Causing inappropriate actions in response to misinformation that could result in a change in programmable logic Hiding or obfuscating malicious activity, including the incident itself or injected code (i.e., a rootkit)

The Potential Impact of Successful Cyber Attacks

Incident Type	Potential Impact
Tampering with safety systems or other controls	Preventing expected operations, fail safes, and other safeguards with potentially damaging consequences
Malicious software (malware) infection	May initiate additional incident scenarios May impact production, or force assets to be taken offline for forensic analysis, cleaning, and/or replacement May open assets up to further attacks, information theft, alteration, or infection
Information theft	Sensitive information such as a recipe or chemical formula are stolen
Information alteration	Sensitive information such as a recipe or chemical formula is altered in order to adversely affect the manufactured product

Examples of Incidents

Will be in your **homework**: Provide CPS/ICS/Industrial Network incidents and give detailed explanation about it.