Critical Infrastructure Security

Lecture 4

Dr. Naveed Anwar Bhatti

Webpage: naveedanwarbhatti.github.io

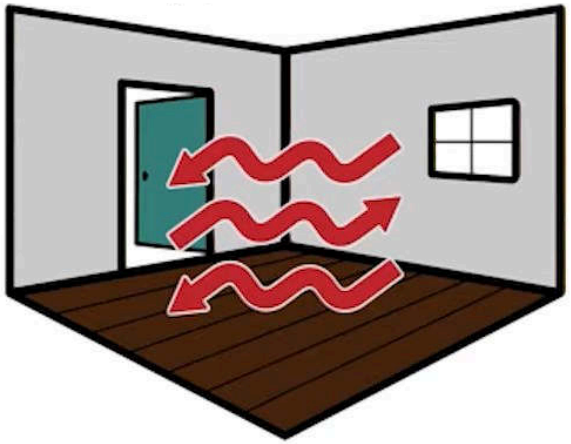
Background: Control Systems

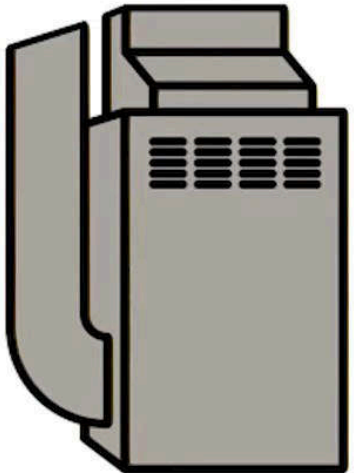
Control Systems

Control Systems

Sensor

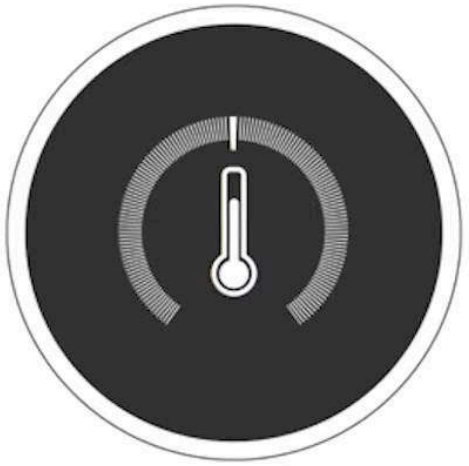
System





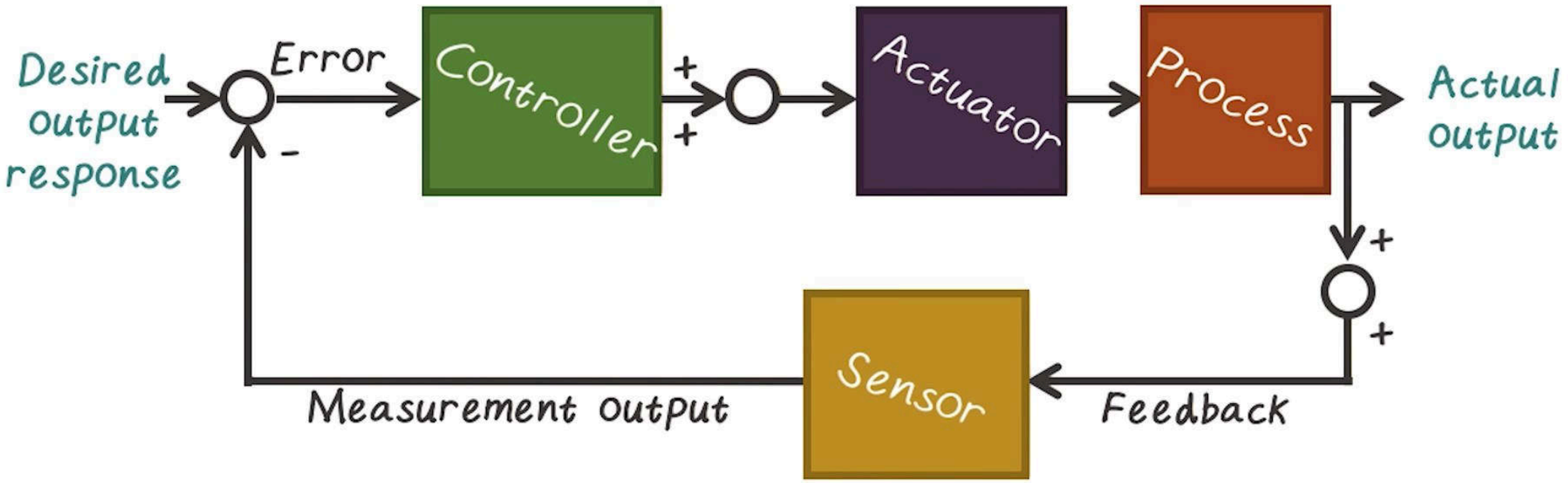
Actuator

Controller

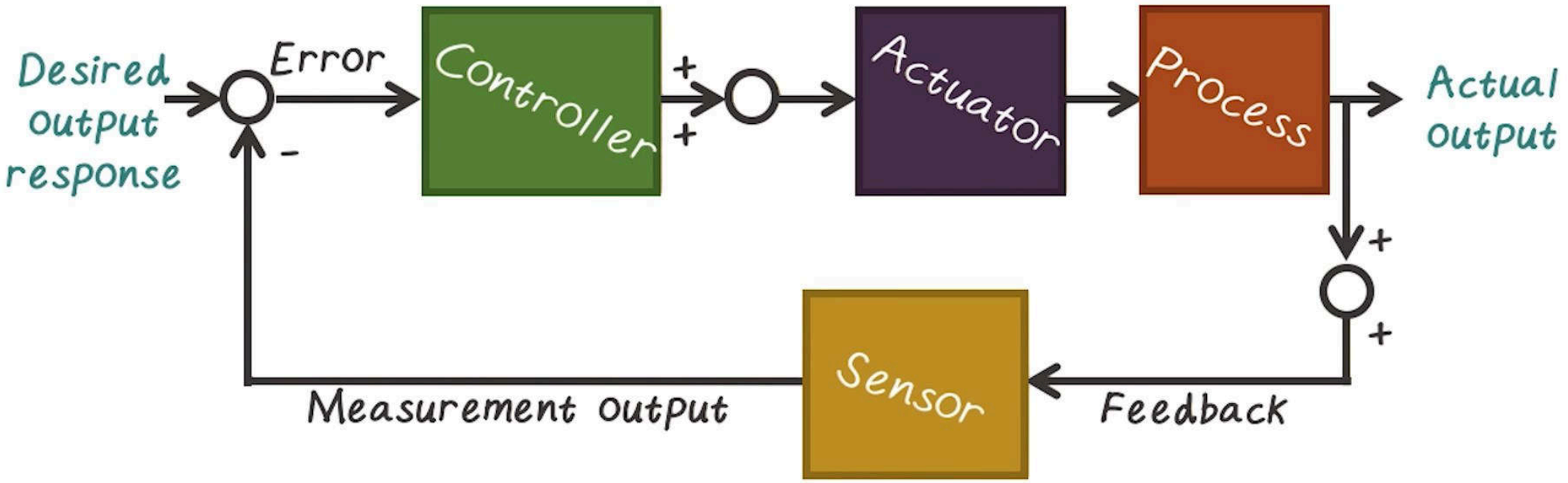


Control Systems: Open-loop

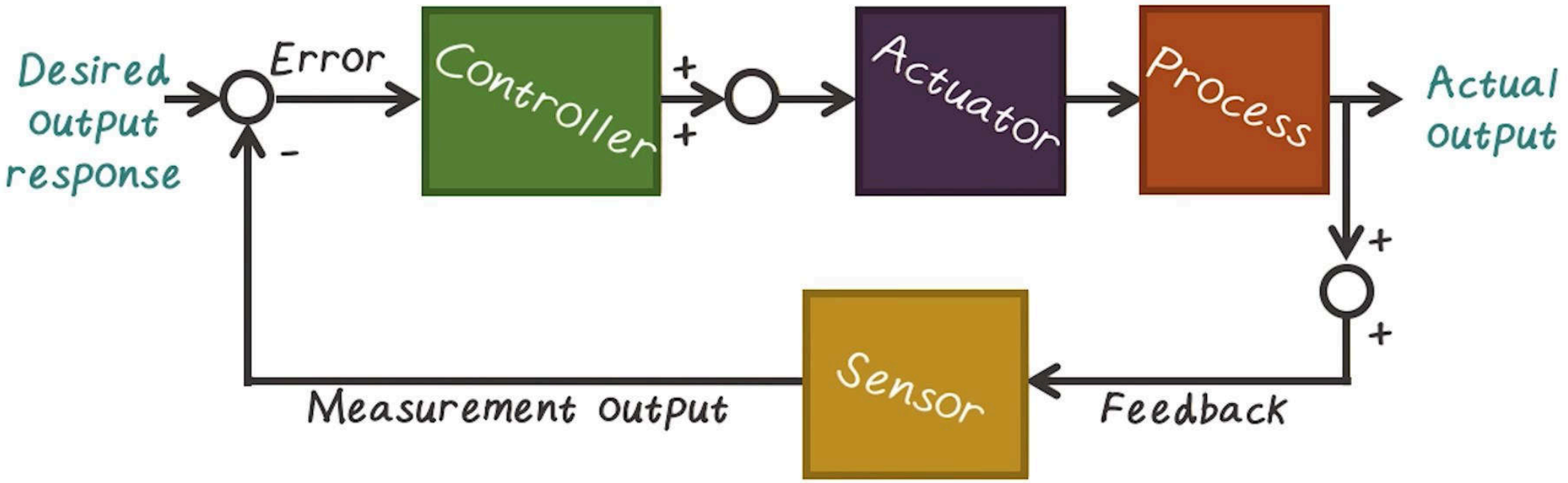
Control Systems: Closed-loop



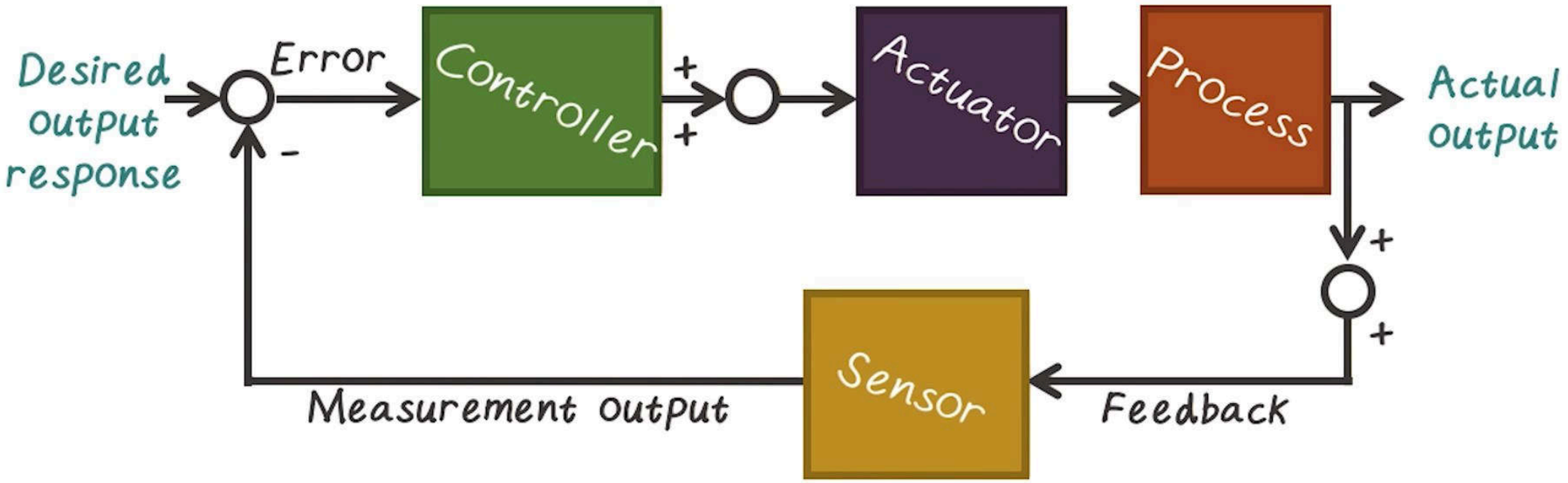
Control Systems: Closed-loop



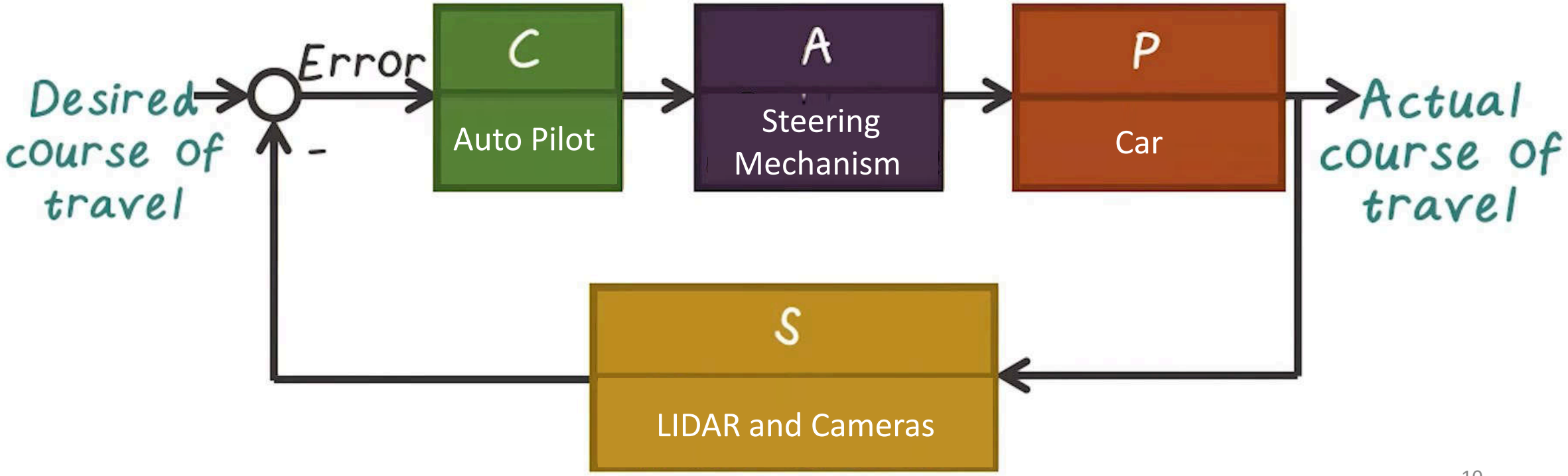
Control Systems: Closed-loop



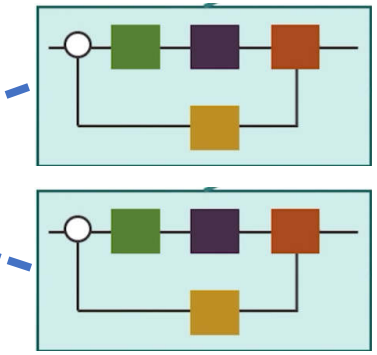
Control Systems: Closed-loop



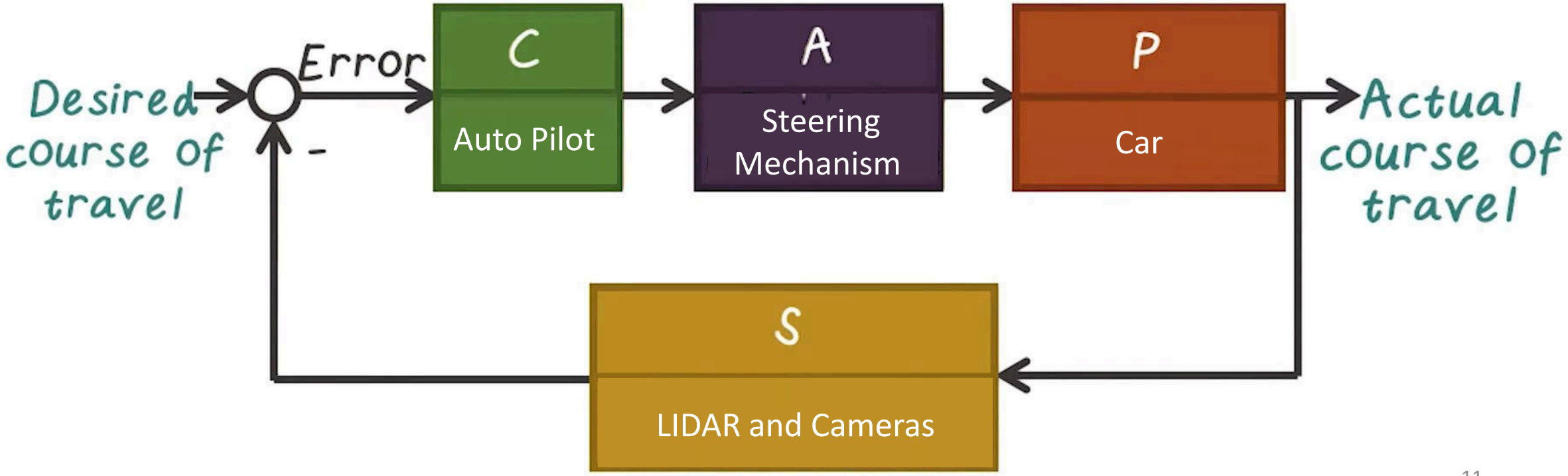
Control Systems: Closed-loop



Control Systems: Closed-loop



Control Processes



Threats to ICS

Moving towards **Critical Infrastructure Security**

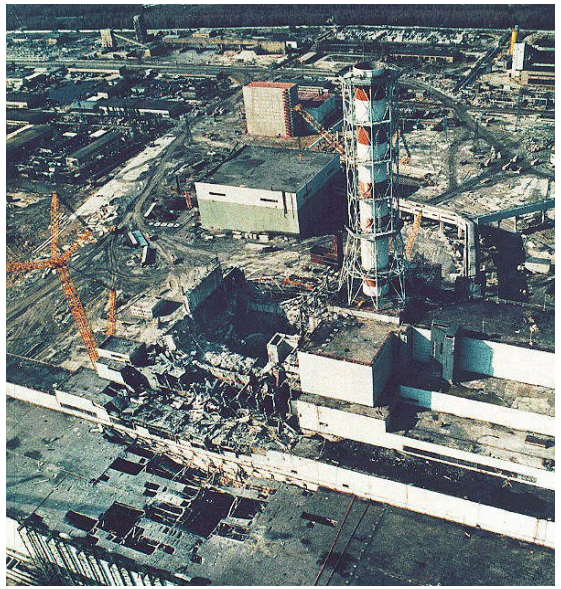
Threat

“A potential cause of an unwanted incident, which may result in harm to a system or organization”

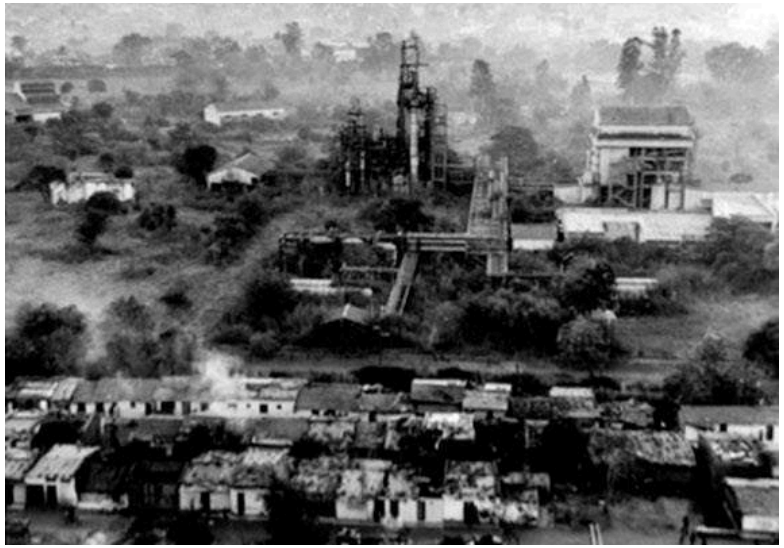
- ISO27000 2014

Background

- What types of threats were historically faced by ICS?
  - Malfunction
  - Mal-operation
  - Power failure
  - Material leakage



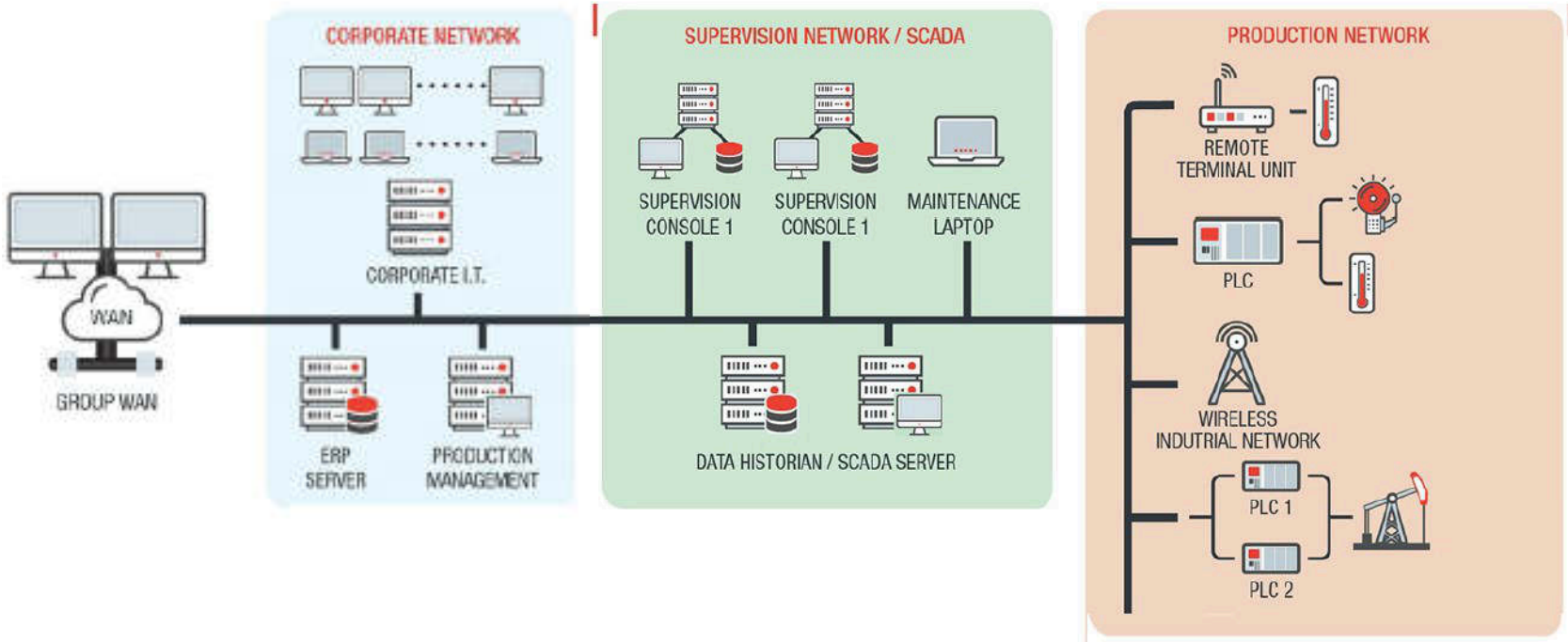
Chernobyl disaster 26 April 1986



Bhopal disaster, 3 December 1984

Background

- ‘Cyber’ security was never a concern for ICS. Reasons?
  - ICS were ‘specialized’
    - Hardware, software, communication
  - ICS were disconnected from outer world
  - ICS were just controlling processes no one would want to hack!

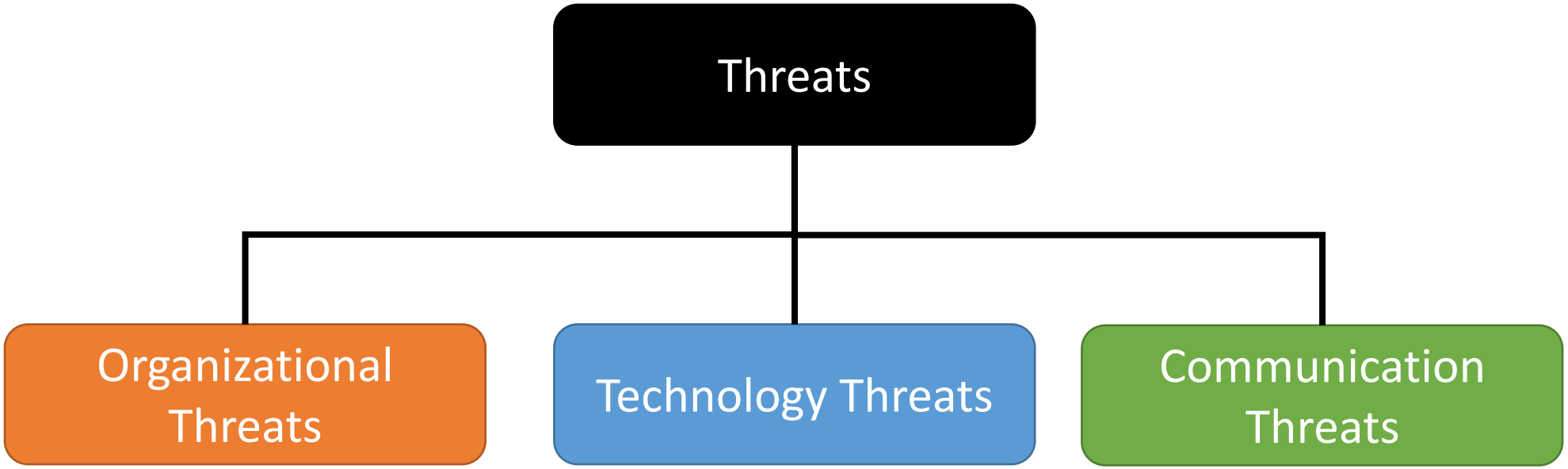


Background

- With the involvement of ICT in every aspect of life, ICS was bound to be affected
  - Proprietary replaced by COTS alternatives
  - ICS protocols is openly available
  - Industrial processes can be monitored and controlled from **smartphone!**

- Hackers have started taking interest in using their skills to disturb operations on a **mega scale!**
  - Disgruntled employees may also find an easy way to take revenge from the management…

Types of threats to ICS



Organizational threats

- Lack of understanding of cyber threats at all levels
- Executives only focus on achieving business objectives
  - Main parameters: production efficiency, reliability and safety
- Sole responsibility of cyber security is assigned to IT department
- No high level policy making, auditing or reporting mechanism in place
- Cultural differences between ICS and ICT departments

Organizational threats

- Depreciated systems with vulnerable, unpatched OS can still be found controlling important parameters in various application areas
- Strict implementation of ICT security standards may be a threat to the business objectives!
- Procurement of security products and services may involve initial and recurring costs which do not immediately promise a good ROI value
  - This factor may cause relaxation or complete removal of cyber security requirements

Architecture / technology threats

- Systems are not upgraded as frequently as applications
  - Same holds true for ICS
  - Legacy systems are not able to fully implement security features, e.g., encryption, offered by new applications

- Security features, e.g., passwords, are not utilized
  - Security configurations are often disabled by default
  - Setting of password was mentioned on Page 52 of a PLC manual!
  - The PLC was connected to the Internet without the password, and was easily accessible to hackers
  - The same model of PLC was used to control waste water pumps, swimming pools, heating systems, wind power generator, etc…

Architecture / technology threats

- New functionality in old package
  - Technical staff may just replace the old component with a new one without paying attention to technological changes that might make the use of the component insecure

- Old ICS protocols do not:
  - Protect messages
  - Protect against man-in-the-middle attacks
  - Describe the course of action in case of illogical node/data
    - Experiments showed that a vast number of ICS devices crash when an uncommon packets is received at their ports!

Network / communication threats

- The common threats related to **Internet and WiFi apply** to ICS…

- In addition, there are more:
  - Changing business environment requires operational data to be available remotely

  - **Short-range** wireless connectivity is commonly being used in ICS environment, and this can be hacked by attackers to gain access to the control and monitoring network

Network / communication threats

- Remote access to the ICS has also become a common requirement
  - Helps in update/ remote troubleshooting by vendors
  - Usually implemented using VPNs or remote desktops
  - May cause trouble if not properly managed
- Dependence of ICS systems on ICT systems may cause unexpected and undesired effects on processes
  - An upgrade or a simple reboot of an ICT system or network device my cause hours of shutdown
- Sharing of low-bandwidth connections among ICT and ICS channels
- Direct connection with the Internet!

Human Factors

- Lack of awareness
- Negligence/casualness
- Disgruntled employees

Operational threats

- Weak password protection
- Lack of proper change management process
- Same development and operational environments
- Patching
  - The “Don’t touch it if it’s working” mentality
- Same software component/library is used in various devices by multiple manufacturers
  - If a vulnerability is discovered in the component , it may take a long time by all manufactures to provide the patched product
- Malware protection not regularly updated
- Physical access to ICS by ICT people

Thanks a lot

If you are taking a Nap, **wake up**.....Lecture Over