Announcement

- Mini-project
  - Due: 16 April 23:59 (Sun)

- Take-home Exam 2
  - Due: 24 April 2023 23:59 (Mon)
  - Covers Week 7-12

- Quiz 6
  - Due 17 April 2023 23:59 (Mon)
  - Covers Week 11 and 12 lecture slides
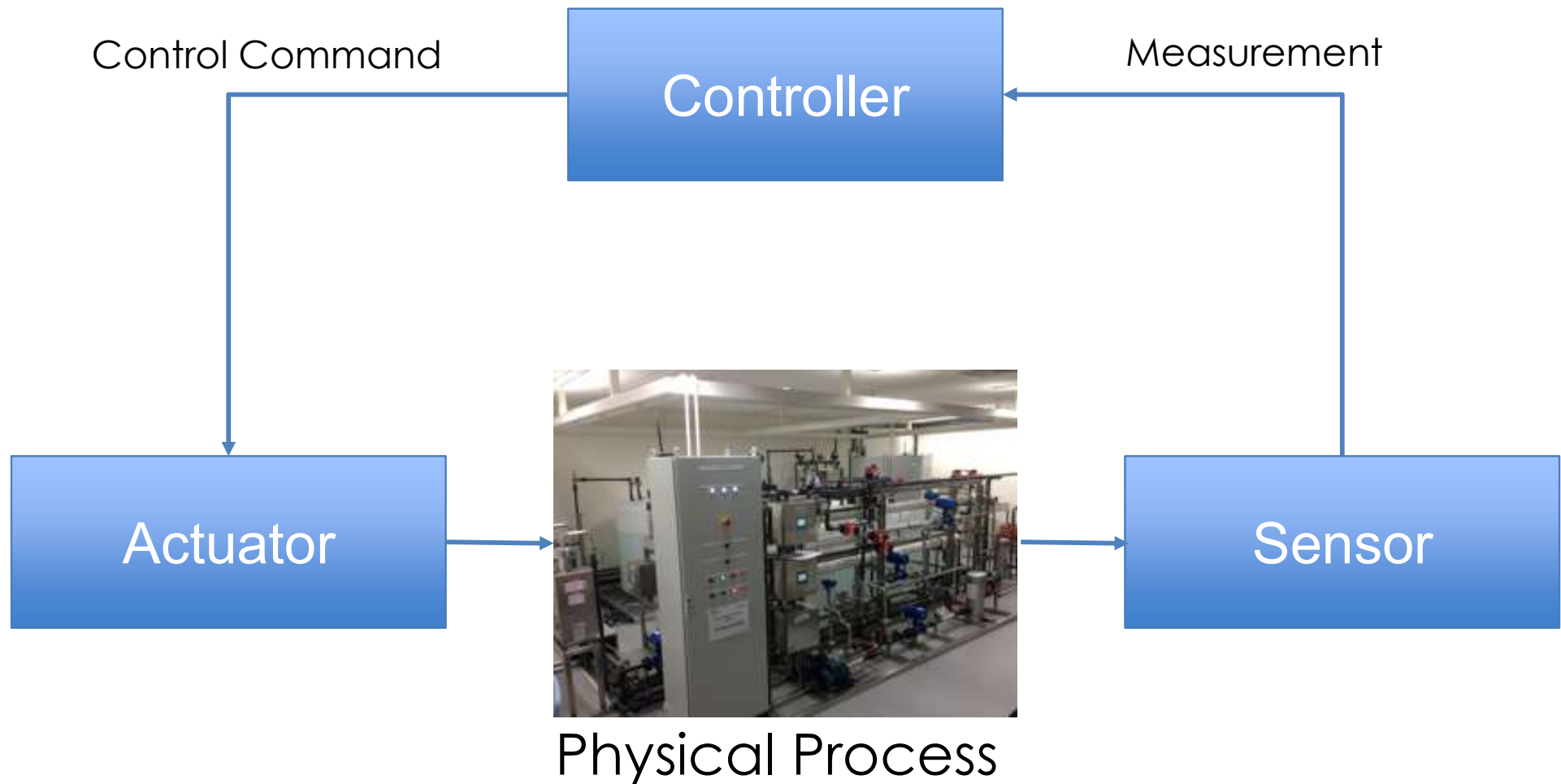
CS5321 Network Security
Week 9: CPS/ICS Security

Industrial Control Systems (ICS)

- Control and monitoring systems for industrial plants and critical infrastructure

- Include Supervisory Control and Data Acquisition (SCADA), sensors, actuators, controllers, and communication channels connecting them.

Control Loop of ICS

Control Command

Measurement

Controller

Actuator
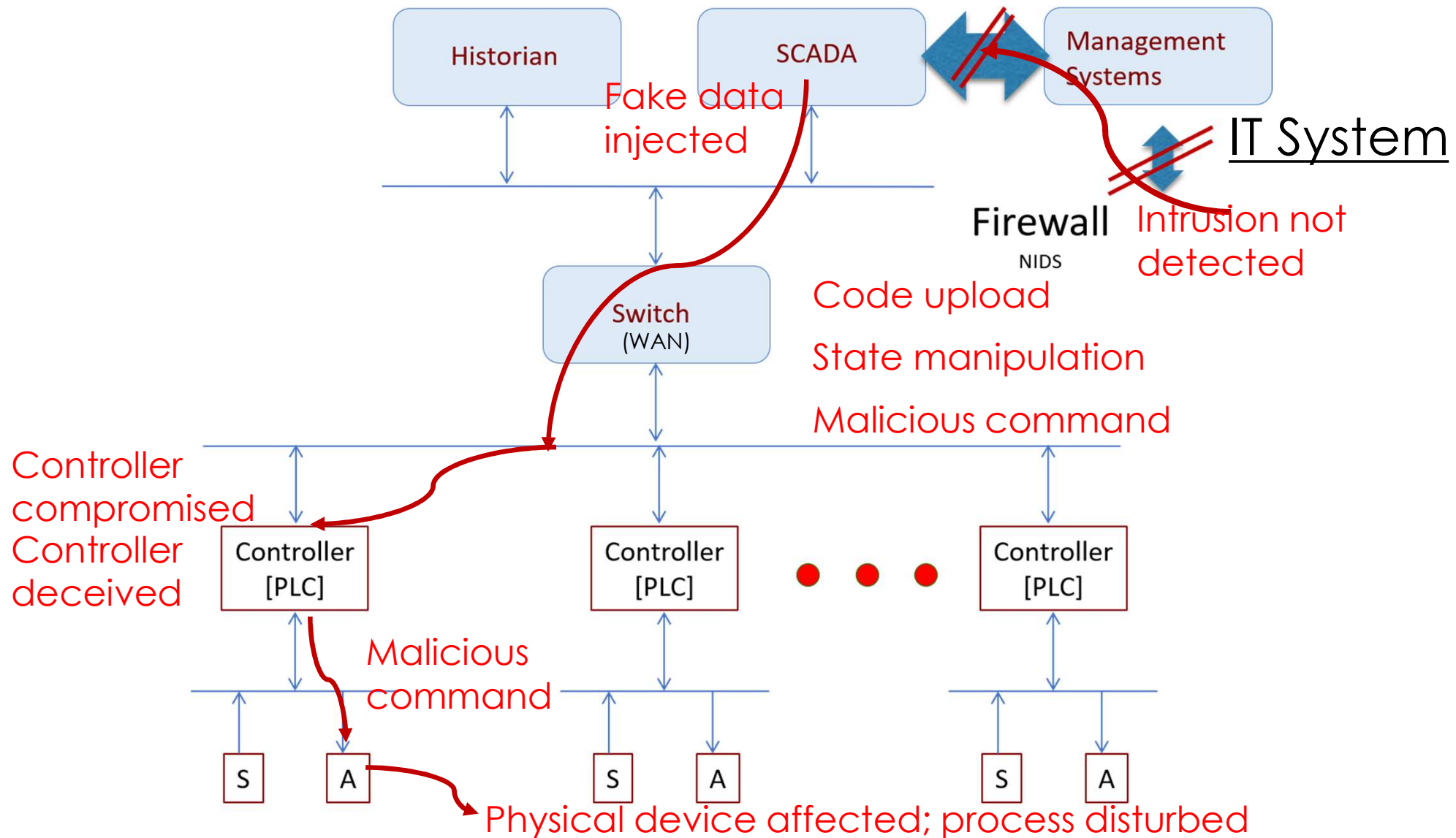

Sensor

Physical Process

Security by "Air Gap"

https://www.belden.com/blog/industrial-security/goodbye-air-gaps-hello-improved-ics-security

- **Isolation** from other systems or external network
- **Dedicated** communication infrastructure
- *All devices were trusted.*
- *Security was not part of protocol or system design.*

Attacks against Modernized ICS

ICS (OT) System

Historian

SCADA

Management Systems

Fake data injected

IT System

Firewall
NIDS

Intrusion not detected

Switch (WAN)

Code upload

State manipulation

Malicious command

Controller compromised
Controller deceived

Controller [PLC]

Controller [PLC]

Controller [PLC]

Malicious command

S A

S A

S A

Physical device affected; process disturbed

Cybersecurity vs CPS/ICS Security

- Cybersecurity
  - Confidentiality
  - Integrity
  - Availability

- Second-level latency requirement

- Frequently updated/upgraded
- Easy to patch

- Cause data breach, financial loss etc.

- CPS/ICS security
  - **Availability**
  - Integrity
  - Confidentiality

- **Real-time** availability

- Millisecond level latency requirement

- Long life time (Resource-constrained, legacy devices)
- Difficult to update/upgrade
- **Physical damage**, life-threatening situations