Industrial Control Systems

ARCHITECTURES & SECURITY ESSENTIALS

1 day training course

agentschap voor Innovatie
door Wetenschap en Technologie

howest
De Hogeschool West-Vlaanderen
Lid van de Associatie universiteit gent

KU LEUVEN

UNIVERSITEIT GENT

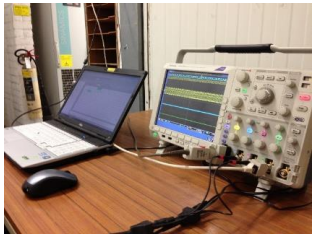
- **Tetra Industriële Security** (140354)
- **Tetra Verboten** (140318)

Energy and Automation: Who are we?

Energy and Automation,

Technology Campus Gent, KU Leuven

http://www.kuleuven.be/eena



Research topics automation:

- Industrial Data Communication
- Model based control on industrial controllers

Contact:

dr. Ing. Bart Huyck,	Project manager E&A	bart.huyck@kuleuven.be
Ing. Hendrik Derre,	Project employee	hendrik.derre@kuleuven.be

Course Outline

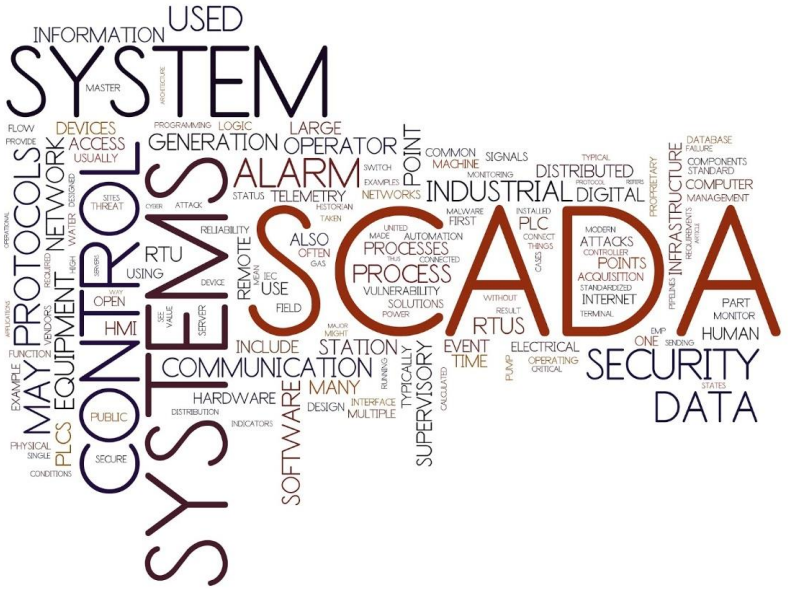
- **ICS OVERVIEW**
  - Terms & Definitions
  - Generic architectures
  - History of ICS
- **Hands on: Basic PLC Programming**
  - Creating a first Flowchart-based program
  - Creating visualisation
- **Commonly used ICS protocols**
  - Overview of ICS protocols
  - Security considerations for commonly used protocols
  - Hands-on: Wireshark captures
- **Introduction to ICS Security**
  - Basics of a ICS security penetration test
  - Red team Exercise & Demo's

Course Outline

- **ICS OVERVIEW**
  - Terms & Definitions
  - Generic architectures
  - History of ICS
- **Hands on: Basic PLC Programming**
  - Creating a first Flowchart-based program
  - Creating visualisation
- **Commonly used ICS protocols**
  - Overview of ICS protocols
  - Security considerations for commonly used protocols
  - Hands-on: Wireshark captures
- **Introduction to ICS Security**
  - Basics of a ICS security penetration test
  - Red team Excercise & Demo's

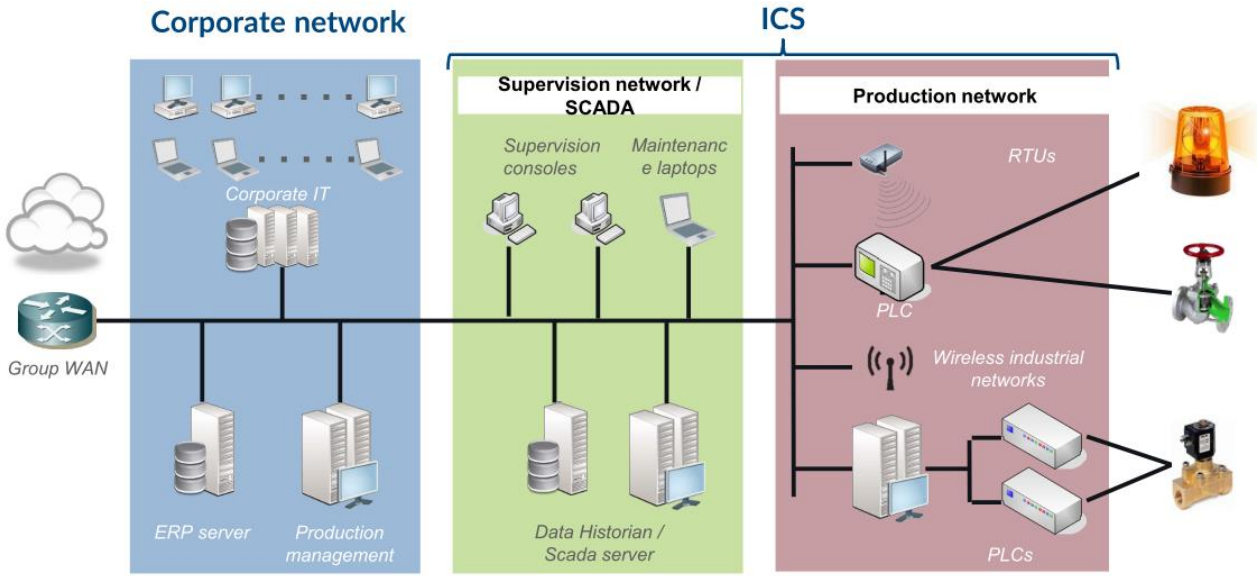
Industrial Control systems: General Overview

- **Terms & Definitions**
- Generic control systems architectures
- Abriviated history of automation



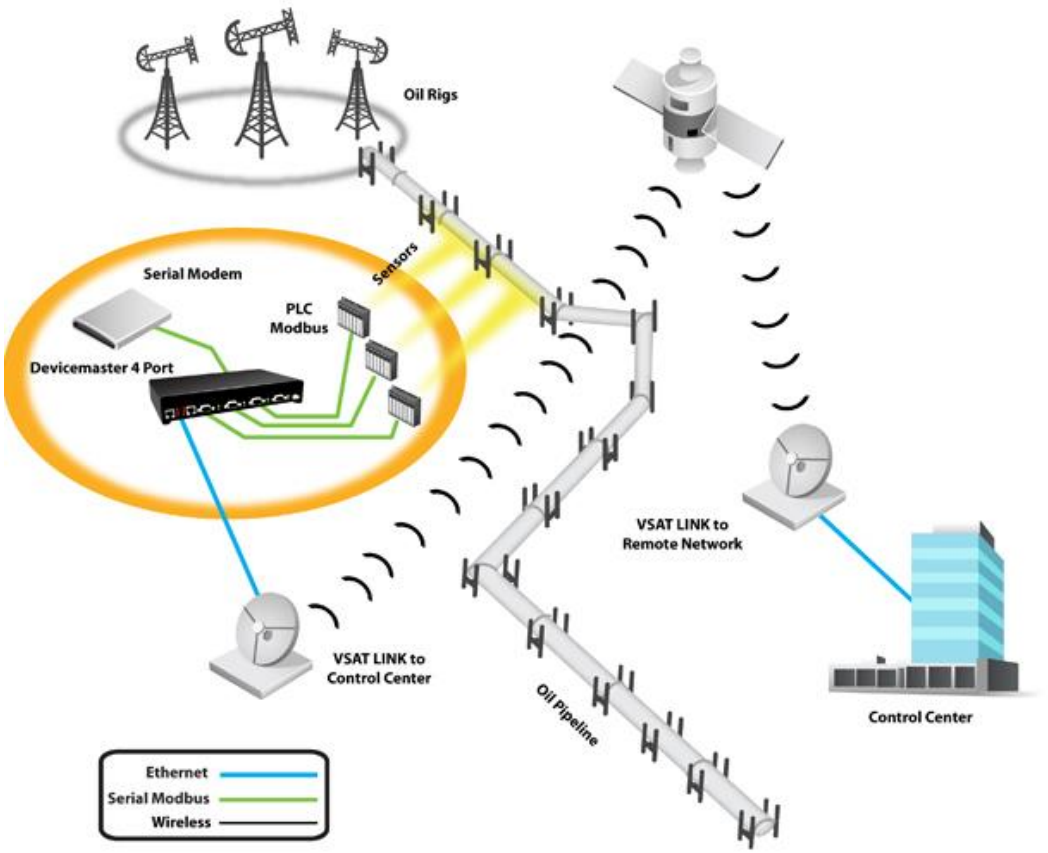
ICS: Industrial Control System

An ICS is an broad class of command and control networks and systems that are used to support all types of industrial processes. They include a **variety of system types** including supervisory control and data acquisition (**SCADA**) systems, distributed control systems (**DCS**) , process control systems (**PCS**), safety control systems (**SIS**) and other, often smaller control systems configurations such as programmable logic controllers (**PLC's**).



SCADA:
Supervisory Control and Data Acquisition

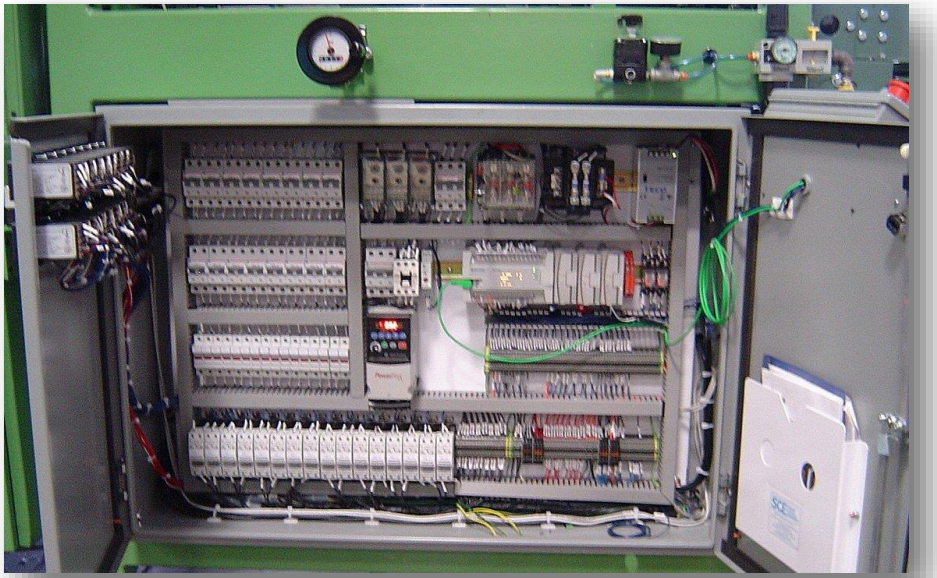
A generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (e.g., delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated.



DCS: Distributed Control System

An industrial control system deployed and controlled in a distributed manner, such that various distributed control systems or processes are controlled individually.

In a control system, refers to control achieved by intelligence that is distributed about the process to be controlled rather than by a centrally located single unit.



PLC: Programmable Logic Controller

A Solid-state control system that has a user-programmable memory for storing instructions for the purpose of implementing specific functions such as I/O control, logic, timing, counting, three mode (PID) control, communication, arithmetic, and data and file processing.

RTU: Remote Terminal Unit

A remote terminal unit is a device combining remote communication capabilities with programmable logic for the control of processes in remote locations.

IED: Intelligent Electronic Device

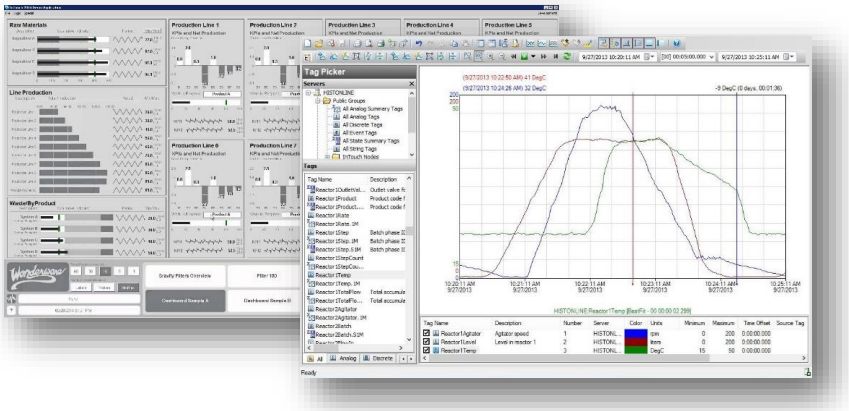
An intelligent electronic device is an electronic component (such as a regulator and circuit control) that has a microprocessor and is able to communicate, typically digitally using fieldbus, real-time Ethernet, or other industrial protocols.

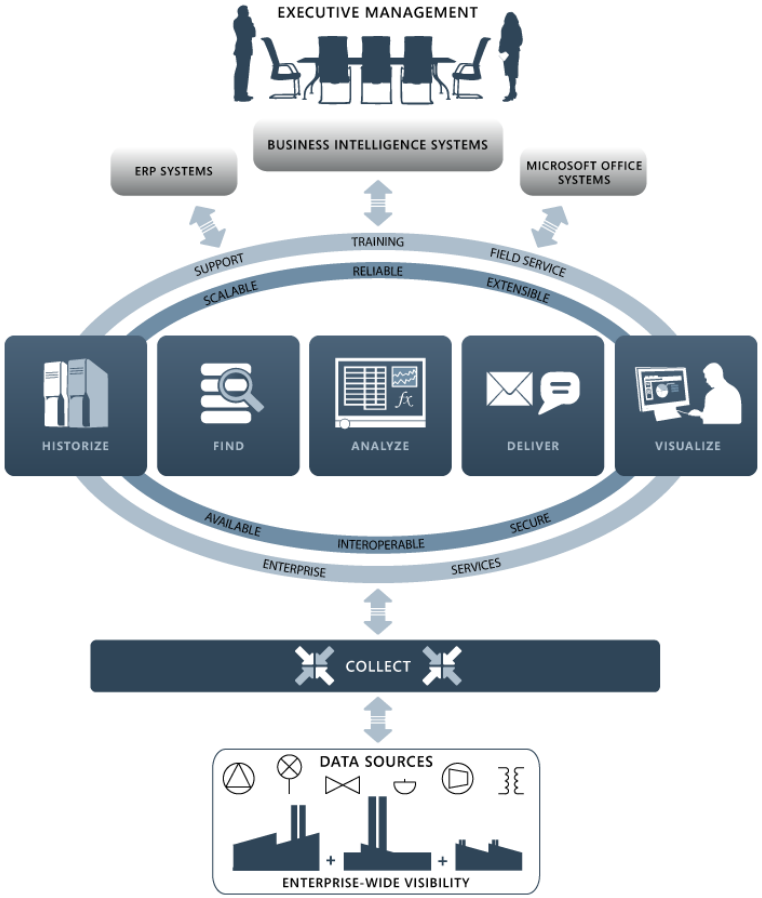
HMI: Human-Machine Interface

A human-machine interface is the user interface to the processes of an industrial control system. An HMI effectively translates the communication to and from PLCs, RTUs, and other industrial assets to a human-readable interface, which is used by control systems operators to manage and monitor processes. An HMI can range from a physical control panel with buttons to an industrial PC with a colour graphics display running dedicated HMI software.

Historian

A Historian is a software service which accumulates time-stamped data, boolean events, and boolean alarms in a database which can be queried or used to populate graphic trends in the HMI. This centralized database supports data analysis using statistical process control techniques.



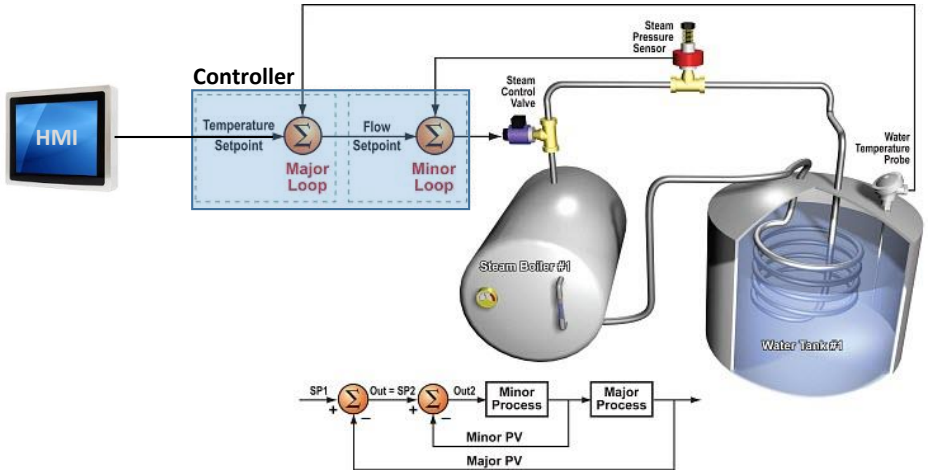


Control System

A System in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include SCADA, DCS, PLCs and other types of industrial control systems.

Control Loop *(automation view)*

A combination of field devices and control functions arranged so that a control variable is compared to a set point and returns to the process in the form of a manipulated variable (sensor-controller-actuator-feedback)

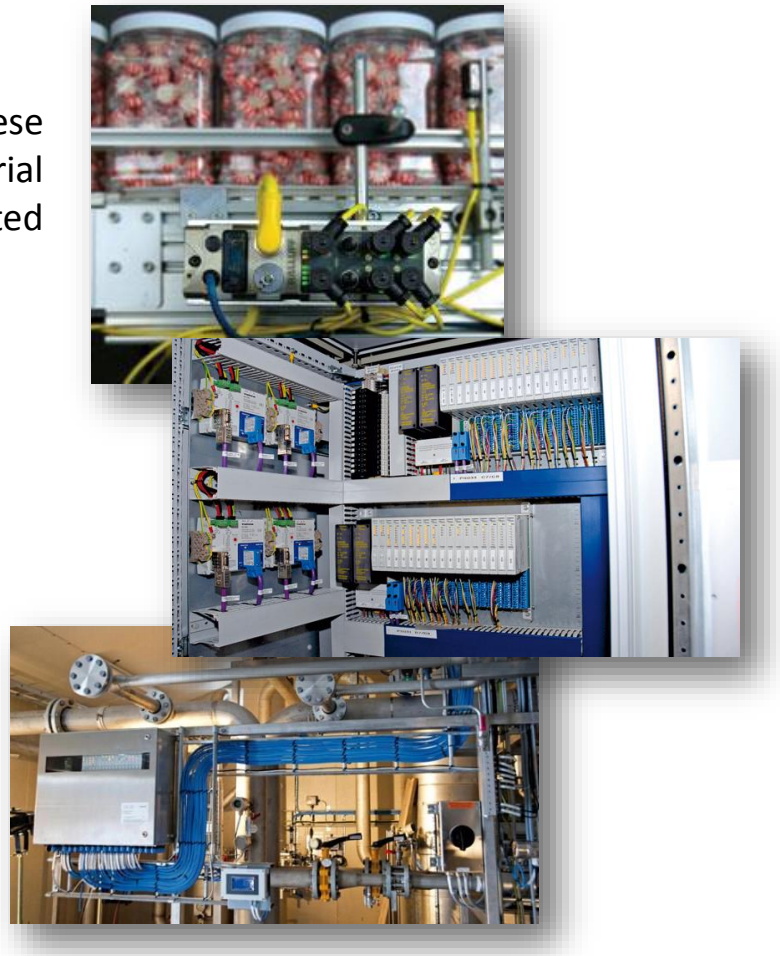


Field Device

Equipment that is connected to the field side of an ICS. These devices monitor and control physical processes in the industrial infrastructures. They may be installed inside cabinets or mounted directly onto the infrastructure.

Types of field devices include:

- RTUs,
- PLCs,
- Actuators & sensors,
- HMIs,
- Communication devices,
- …



Remote IO

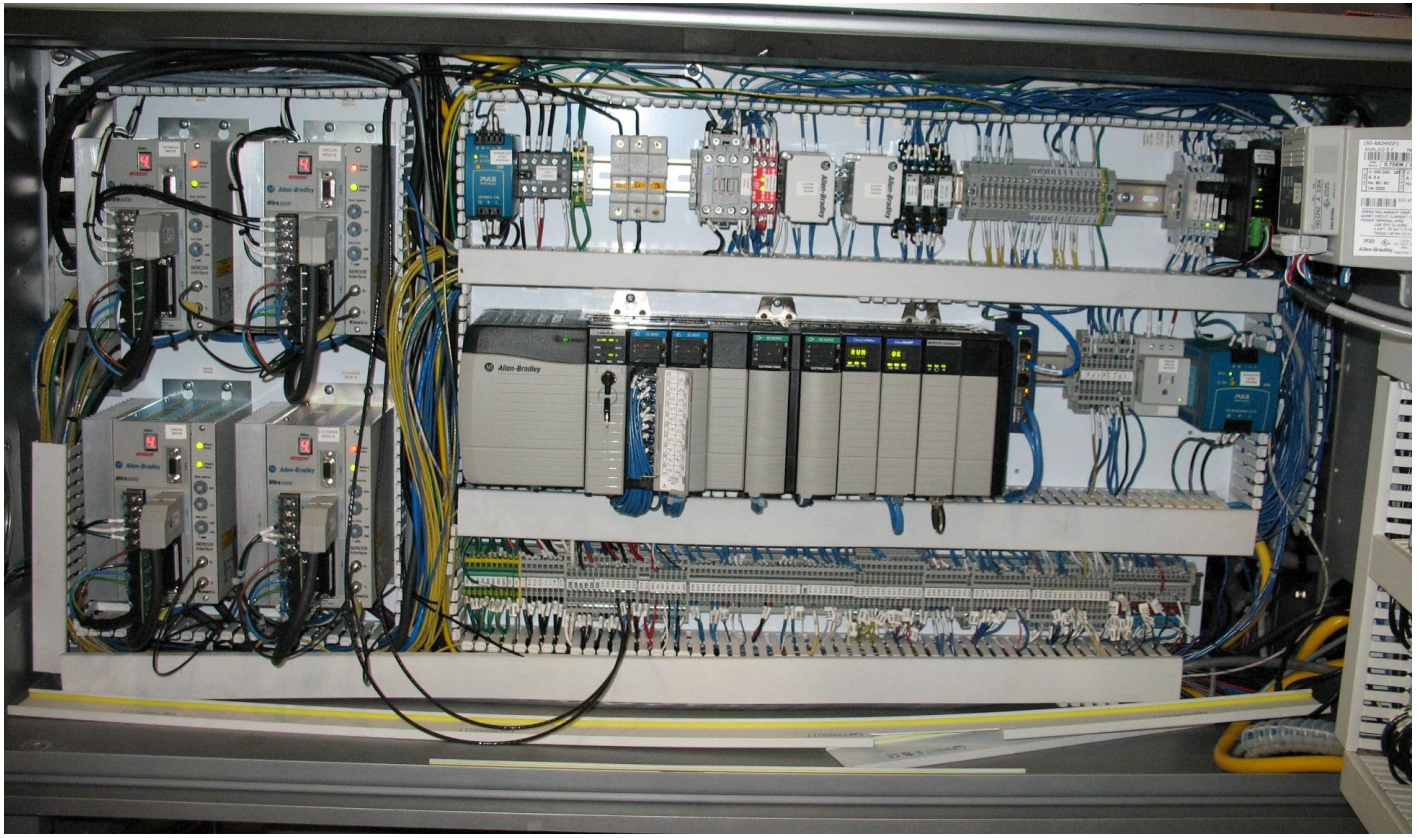
Inputs and outputs of the controller aren't located inside the controller itself (on the same backplane) but in a separate hardware component (often placed in the field). The remote IO communicates with the controller over fieldbus.

Field Bus

A Digital, serial, multi-drop, two-way data bus or communication path or link between low-level industrial field equipment such as sensors, transducers, actuators, local controllers, and even control room devices. Use of fieldbus technologies eliminates the need of point-to-point wiring between the controller and each device.

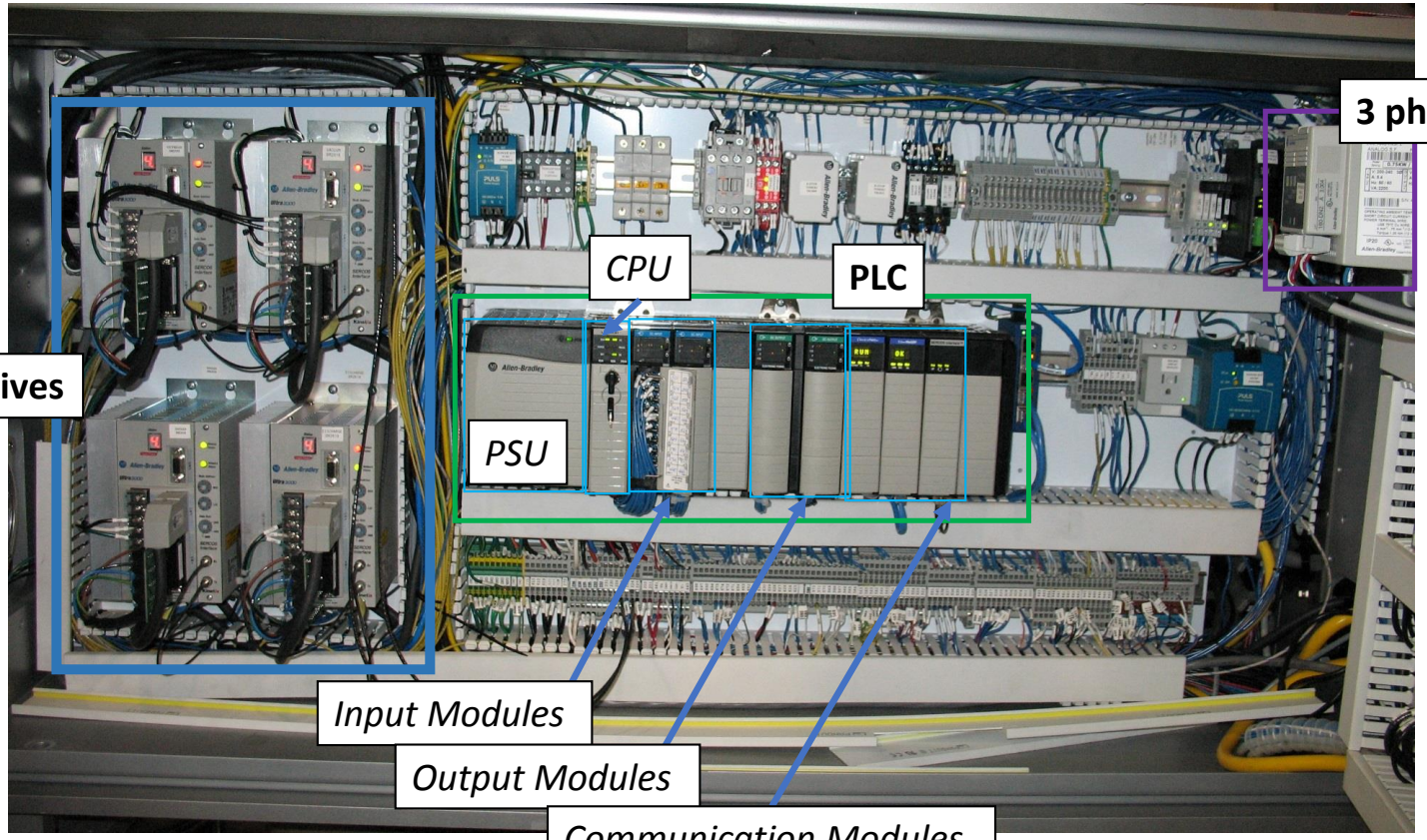
EtherNet/IP
EtherCAT Technology Group
Modbus
PROFINET
PROFIBUS
DeviceNet
CANopen

What's inside a control cabinet

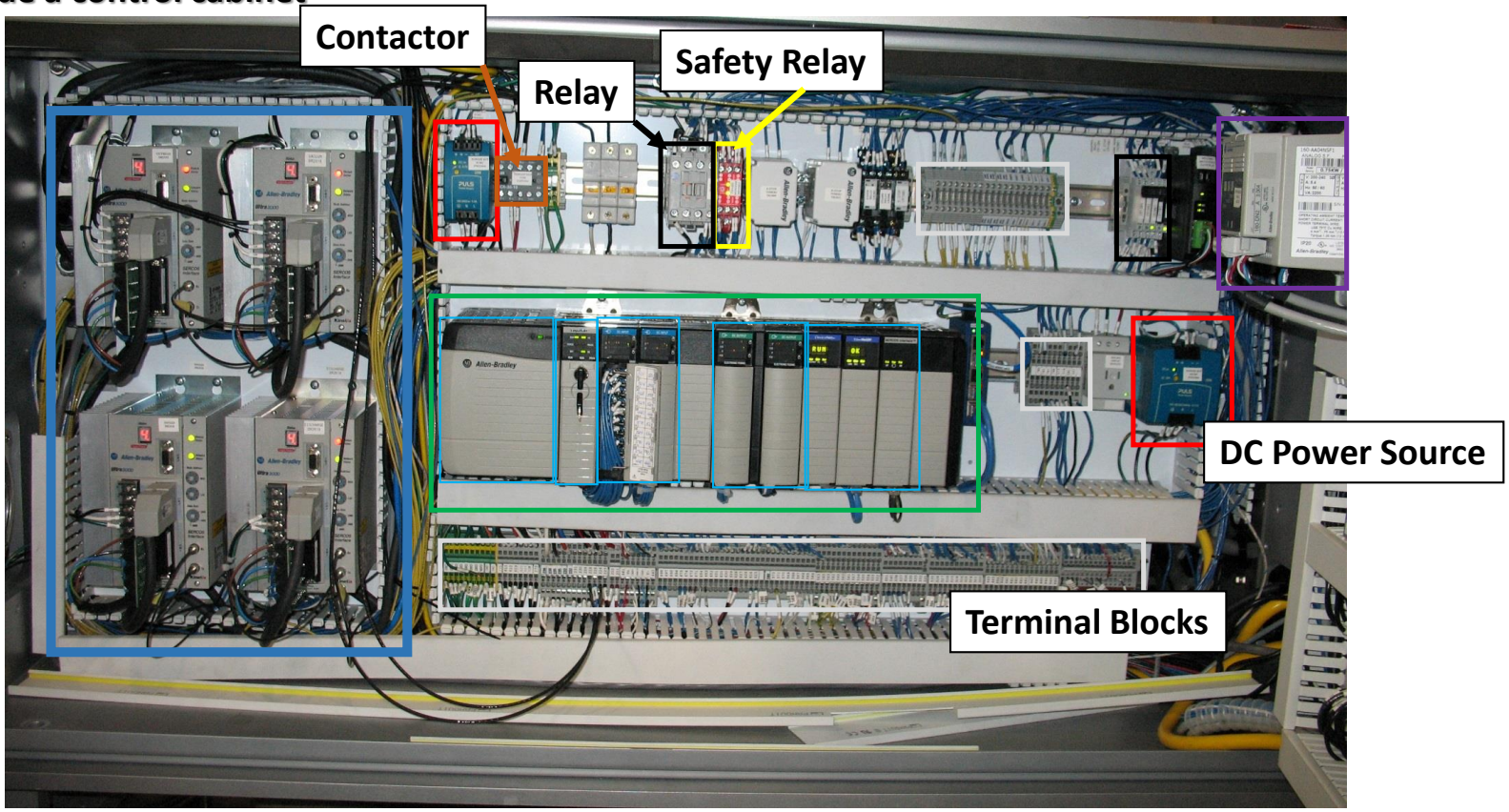


ICS Overview: Terms & Definitions

What's inside a control cabinet

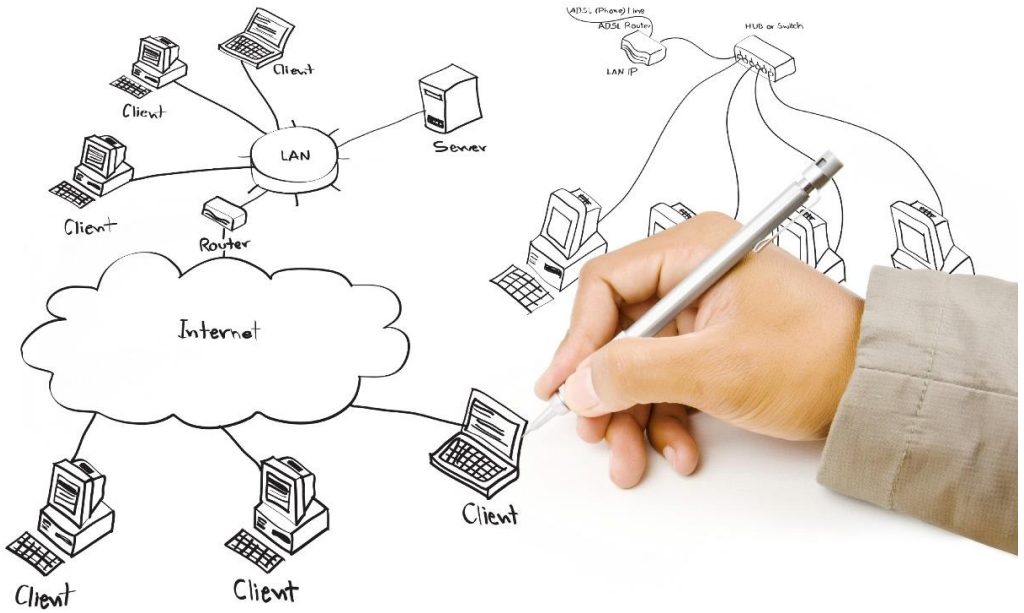


What's inside a control cabinet



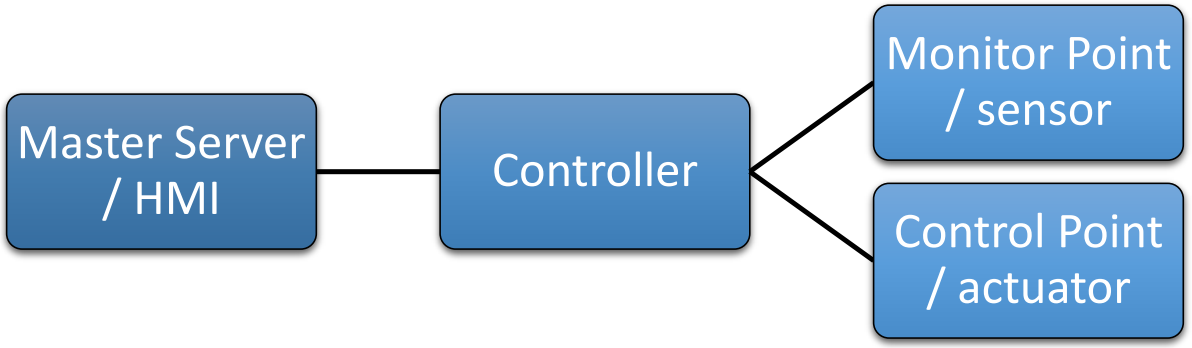
Industrial Control systems: General Overview

- Terms & Definitions
- **Generic control systems architectures**
- Abriviated history of automation



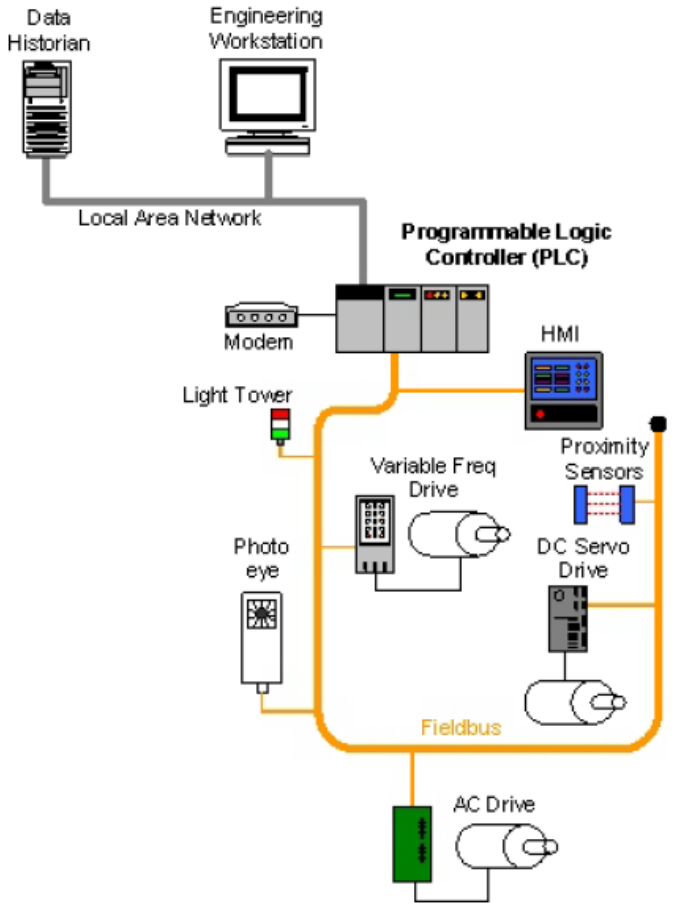
ICS Overview: Generic architectures

Basic Control System architecture: *Simplified model*



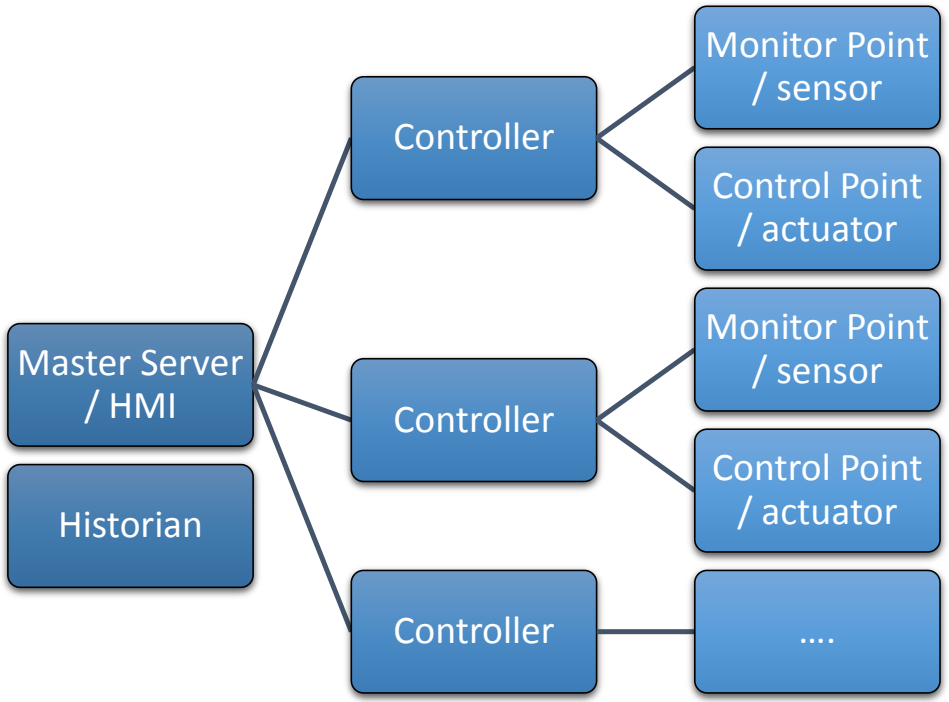
ICS Overview: Generic architectures

Basic Control System architecture: *Real world implementation*



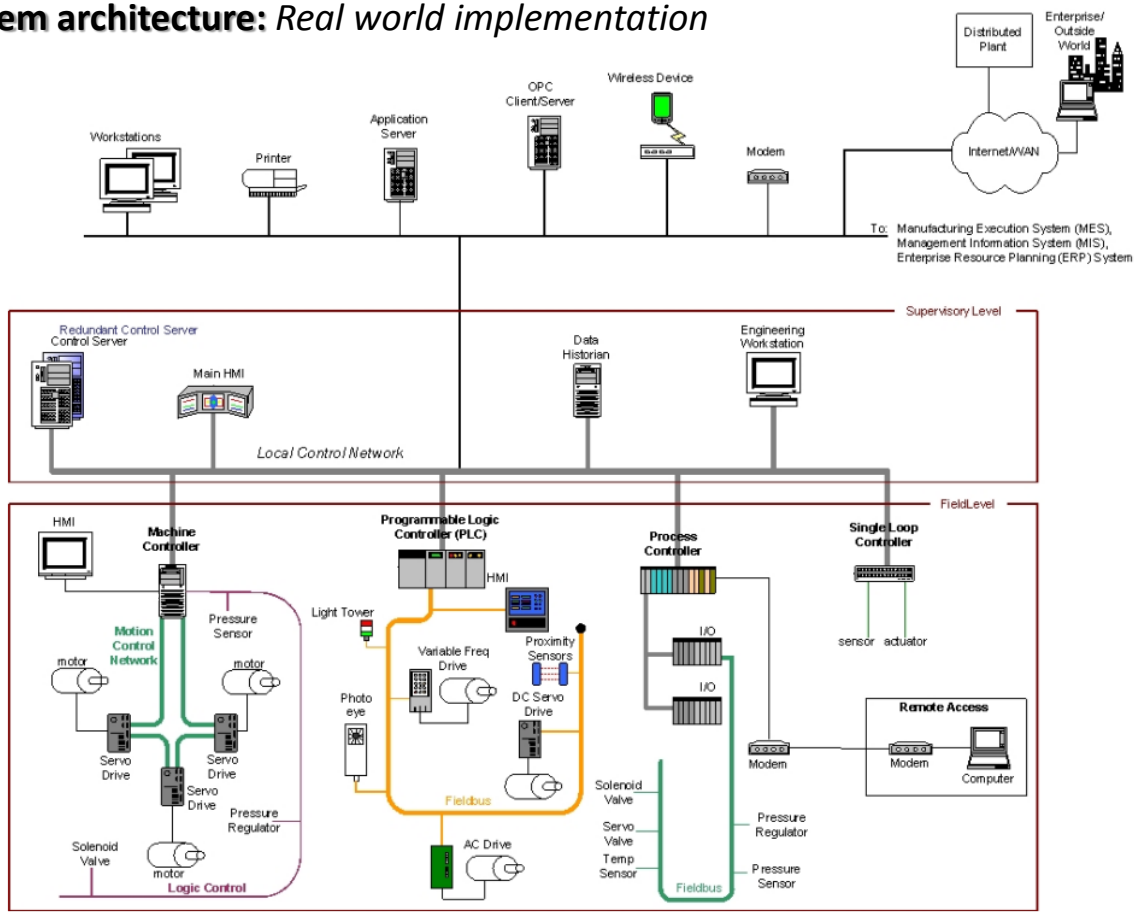
ICS Overview: Generic architectures

Distributed Control System architecture: *Simplified model*



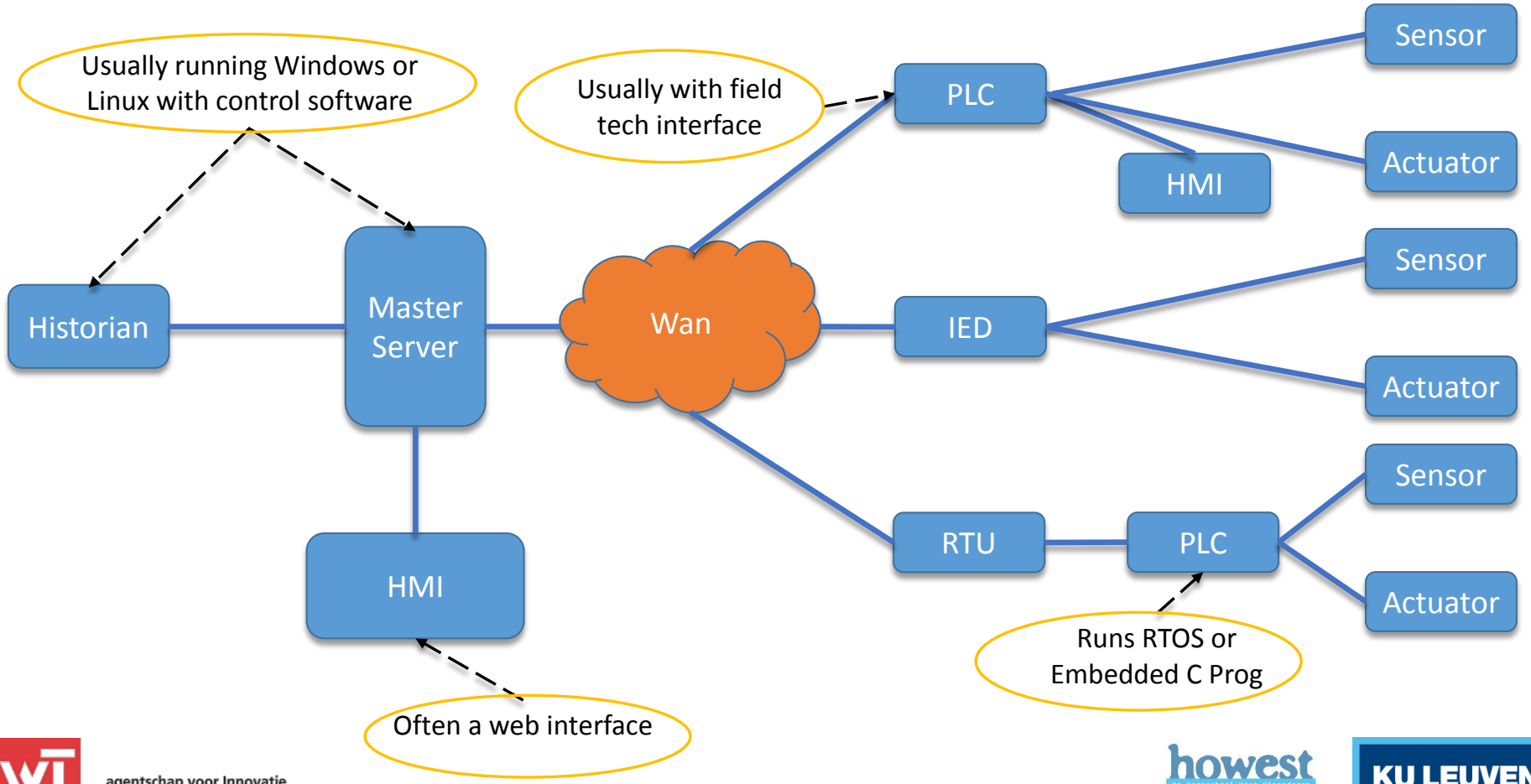
ICS Overview: Generic architectures

Distributed Control System architecture: *Real world implementation*



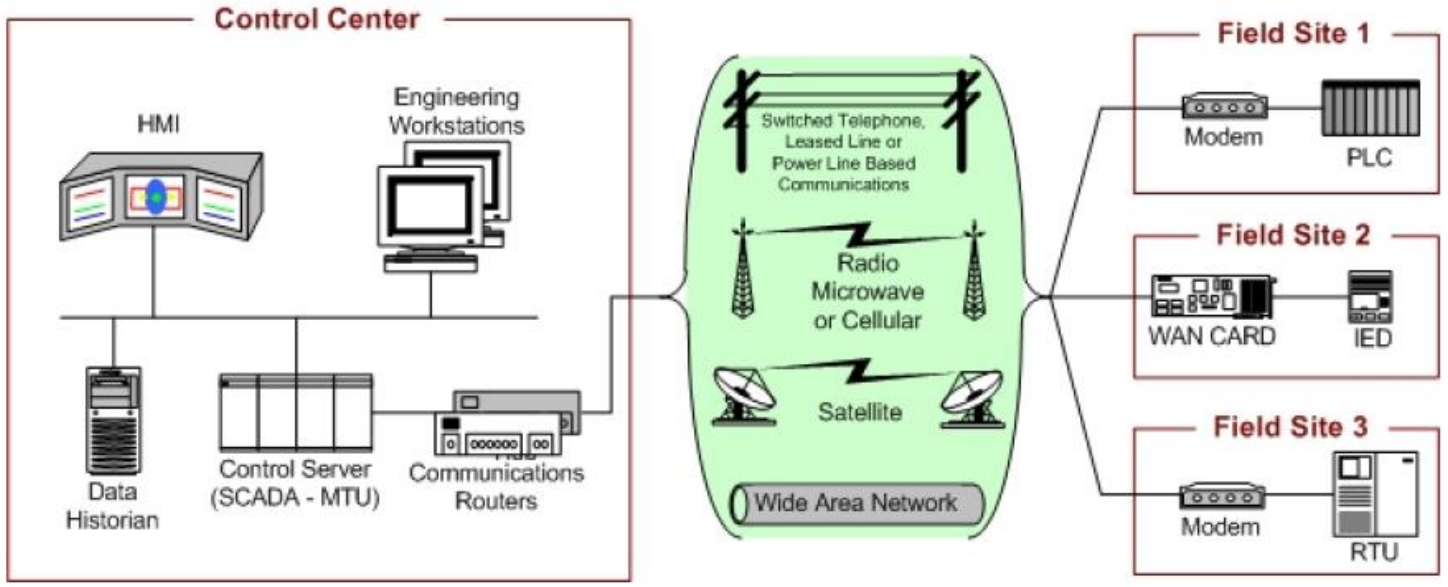
ICS Overview: Generic architectures

Generic SCADA architecture: *Simplified model*



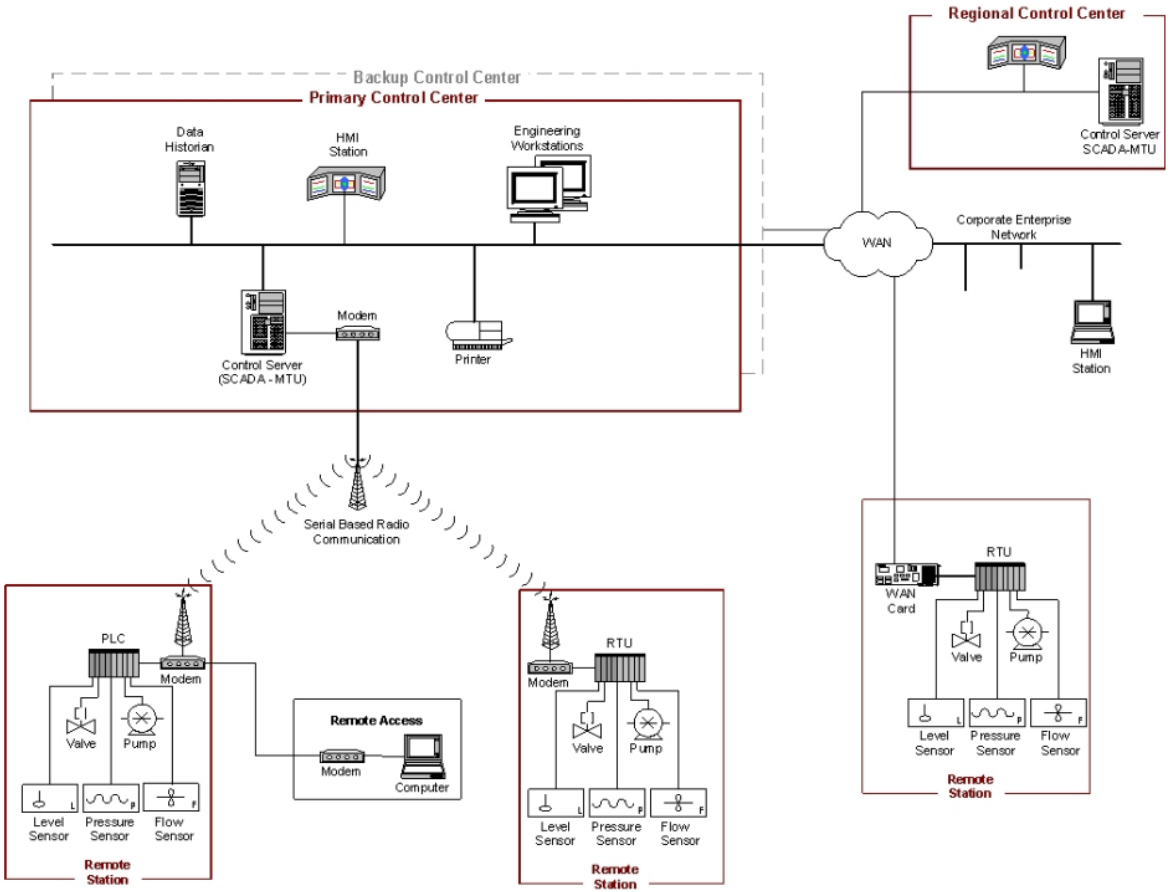
ICS Overview: Generic architectures

Generic SCADA architecture: *Real world implementation 1*



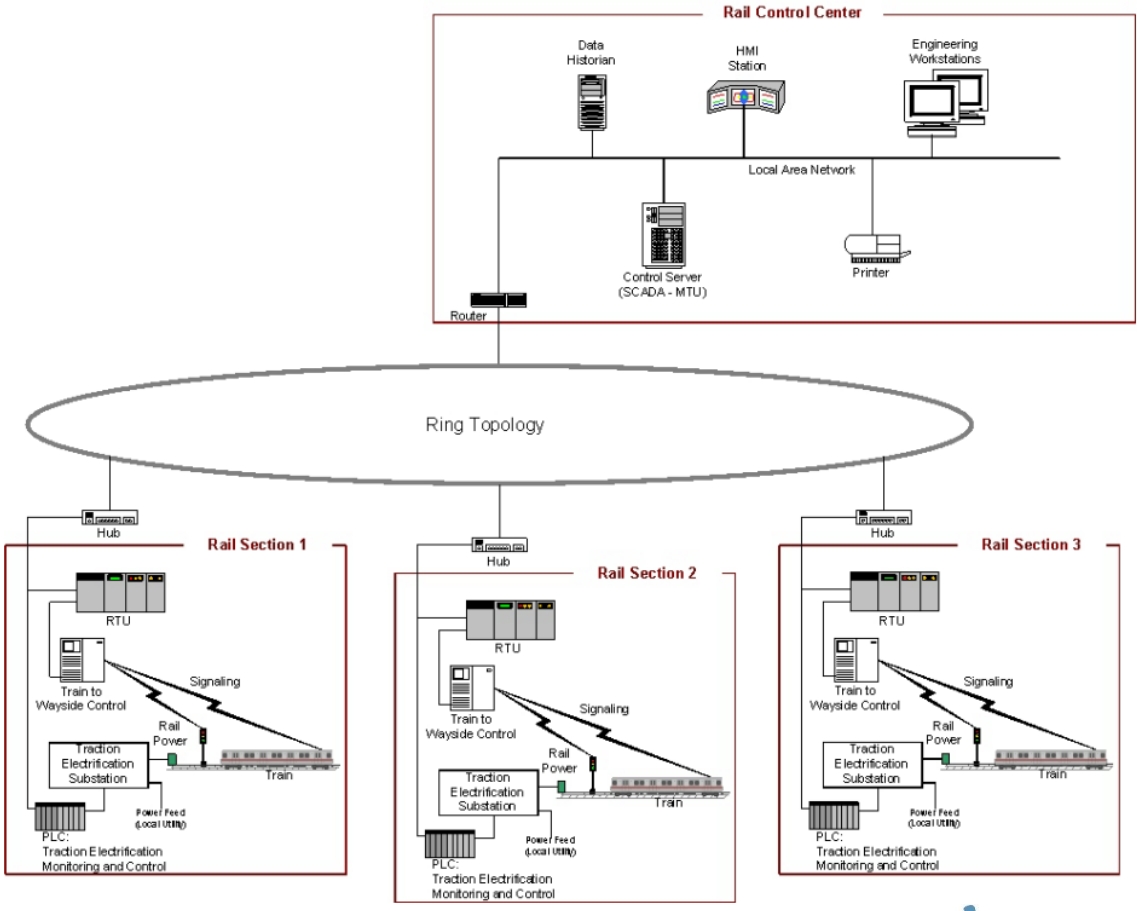
ICS Overview: Generic architectures

Generic SCADA architecture: *Real world implementation 2*



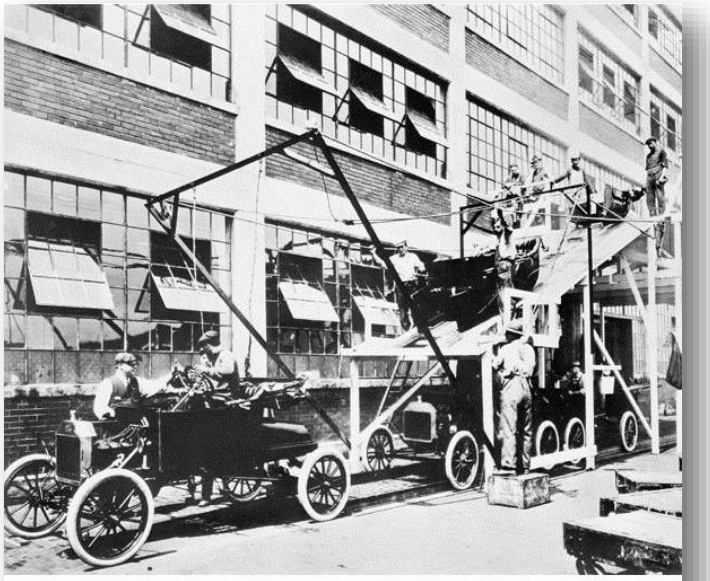
ICS Overview: Generic architectures

Generic SCADA architecture: *Real world implementation 3*



Industrial Control systems: General Overview

- Terms & Definitions
- Generic control systems architectures
- **Abriviated history of automation**



Ford assembly line 1913

ICS Overview: Abriviated history of automation

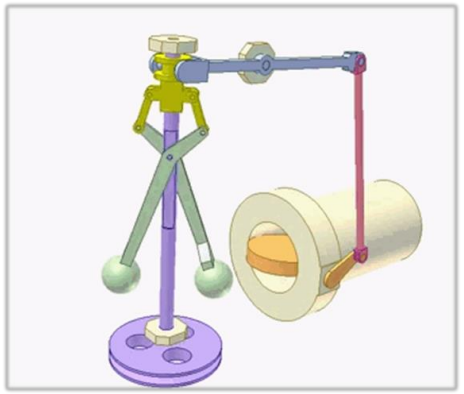
1700-1900 First Industrial Revolution

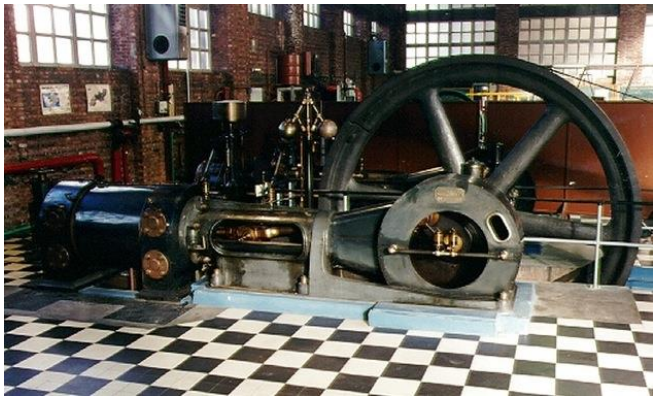
– Mechanical production powered by steam

1620: Cornelis Drebbel designed a feedback loop, or closed loop control system, to operate a furnace, effectively designing the first thermostat.

1745: Edmund Lee's tenting of sails on windmills

1788: James Watt's steam governor provided proportional control of the throttle





ICS Overview: Abriviated history of automation

1700-1900 First Industrial Revolution

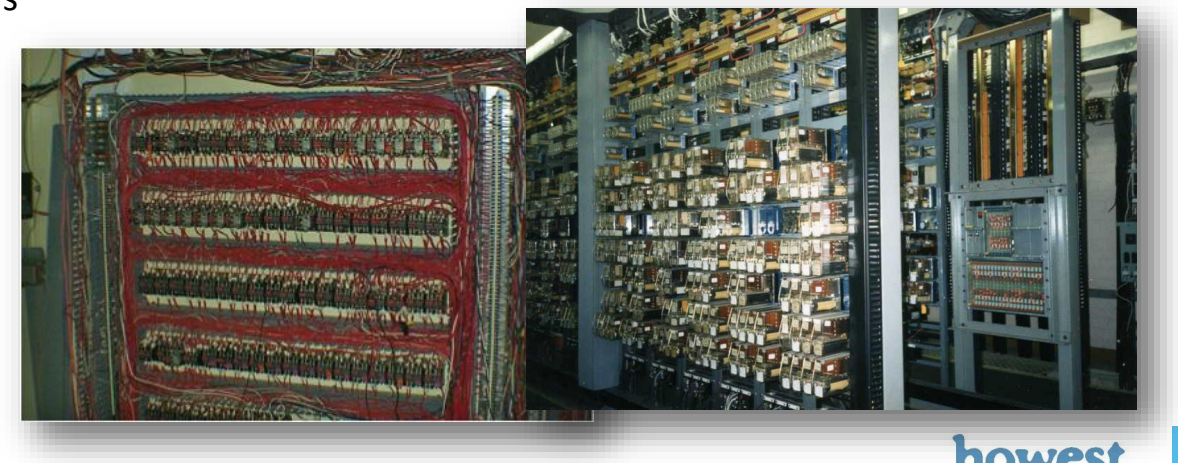
– Mechanical production powered by steam

1823-1883: William Siemens focusing on improving the Watt governor

1831-1879: James Clerk Maxwell published a now-famous paper entitled “On Governors” in 1868

1873: Jean Joseph Léon Farcot published a book on what he called “servo-motcur”

1900: Use of relays and control cabinets in remote rooms to turn things on/off by use of switches and monitor recorders



ICS Overview: Abriviated history of automation

1900-1970 Second Industrial Revolution

– Mass production powerd by electricity

1932: The concept of “negative feedback” was understood and was incorporated into new control theory concepts and design of control systems (Bell laboratories)

1950s: Machine tools were automated using Numerical Control (NC) using punched paper tape

1959: first use of distributed control throughout a large industrial plant

ICS Overview: Abriviated history of automation

1900-1970 Second Industrial Revolution

– Mass production powerd by electricity

1968: First design concept of a programmable controller by Richard (Dick) Moreley. The initial machine – which was never delivered – only had 125 words of memory and there were no considerations for speed.

1969: Modicon 084 the first programmable controller (PC) implemented. The name modicon stood for MOdular DIgital CONtroller.

ICS Overview: Abriviated history of automation

1970-2000 Third Industrial Revolution

– Automation of production by electronics

1971: Allen-Bradley designed and named the bulletin 1774 PLC and coned the term “Programmable Logic Controller (PLC)”

1973: Modbus introduced to allow PLCs to talk with one another

1976: Remote I/O is introduced

ICS Overview: Abriviated history of automation

1970-2000 Third Industrial Revolution

– Automation of production by electronics

1986: PLCs are linked to PCs

1990s: Fieldbus protocols to include ControlNet, DeviceNet, Profibus, Fieldbus Foundation,…

1992: Ethernet and TCP/IP connectivity for PLCs

2003: First controllers witch embedded web server