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

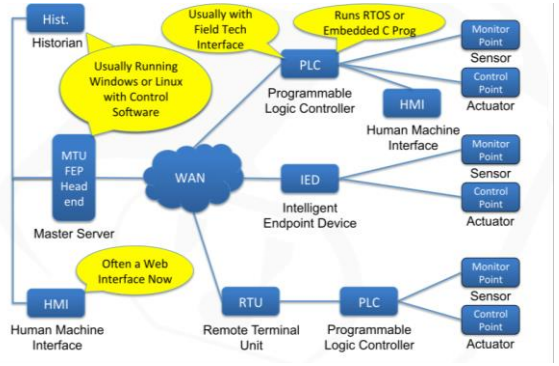
UNIVERSITEIT GENT

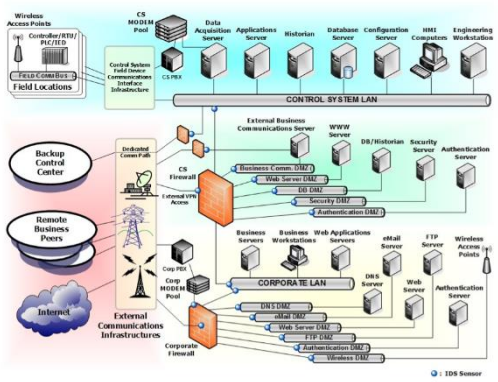
Course outline

- ICS OVERVIEW
  - Generic architectures
  - Terms & Definitions
  - 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

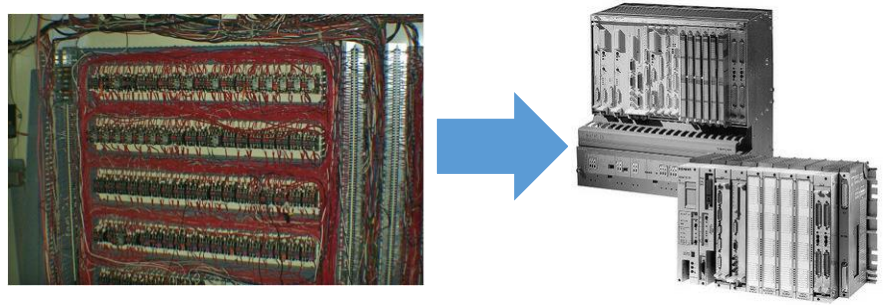
ICS OVERVIEW

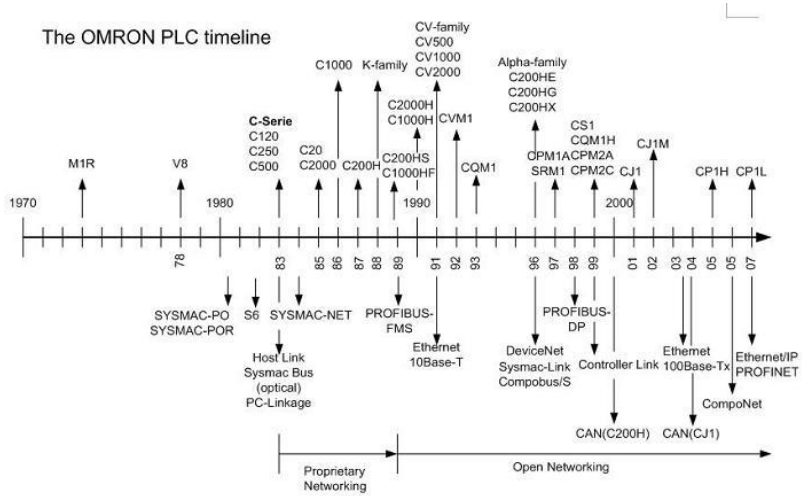
- Generic architectures





- ICS History



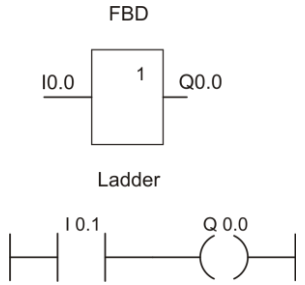


- Terms & Definitions

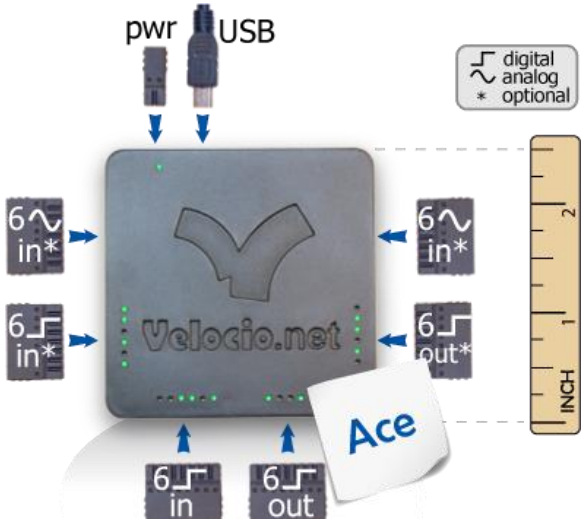
- Industrial Control Systems (ICS)
- Distributed Control Systems (DCS)
- Supervisory Control and Data Acquisition (SCADA)
- Programmable Logic Controllers (PLC)
- Remote Terminal Unit(RTU)
- Intelligent Electronic Device (IED)
- Control System
- Control Loop
- Control Center
- Control Network
- Field Device
- Field Bus
- Data Historian
- Human-Machine Interface (HMI)
- Real-Time
- …

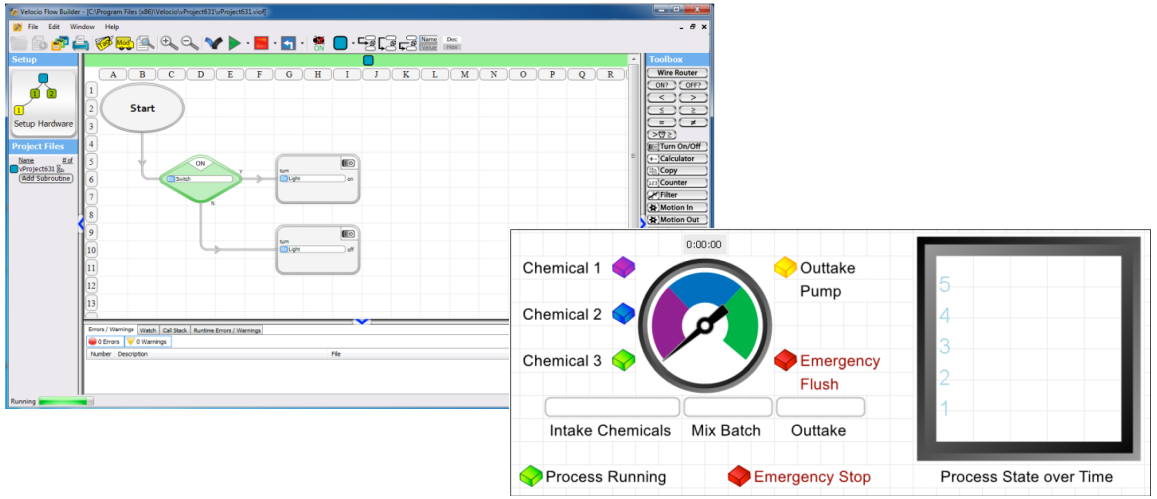
Hands-on: Basic PLC programming

- IEC 61131-3 Programming Languages
  - Ladder diagram (LD)
  - Sequential Function Charts (SFC)
  - Function Block Diagram (FBD)
  - Structured Text (ST)
  - Instruction List (IL)



- Creating a basic PLC program and visualisation





Commonly used ICS protocols

- Overview of commonly used ICS Protocols & Security considirations

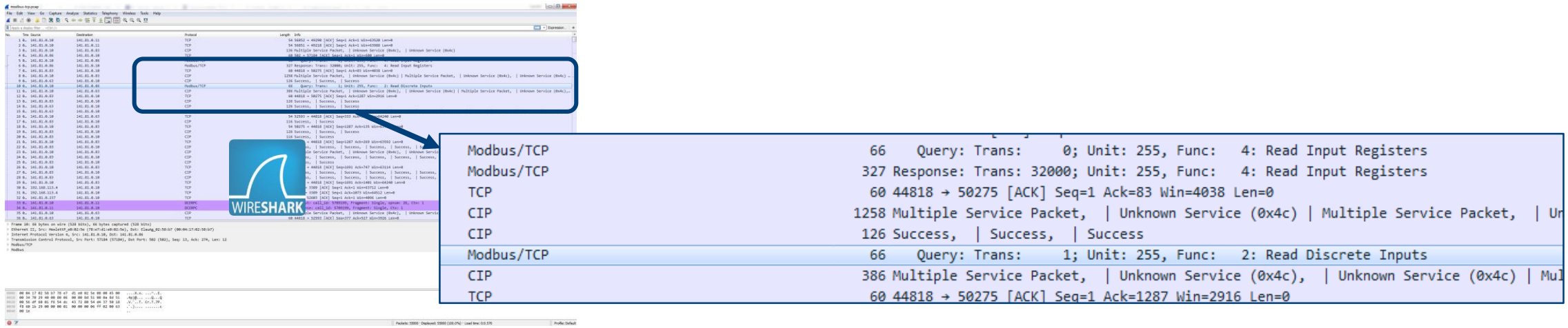
Universal ICS Protocols
- Modbus TCP: TCP/502
- OPC UA: TCP/4840
- OPC UA XML: TCP/80,TCP/443

Process Automation Specific Protocols
- EtherCAT: UDP/34980
- Ethernet/IP: TCP/44818, UDP/2222,44818
- FL--net: UDP/55000 to 55003
- Fieldbus HSE: TCP/1089--1091, UDP/1089--109
- HART--IP: TCP/5094,UDP/5094
- PROFINET: TCP/34962--34964, UDP/34962--34964

Building Automation Specific Protocols
- BACnet/IP: UDP/47808
- LonTalk: UDP/1628, UDP/1629
- Fox (Tridium/Niagara): TCP/1911

….

- Hands-on: Wireshark Captures (ICS protocols)



Introduction to ICS security

- Basics of an ICS penetration test
  - Attack Surfaces
  - Applied ICS Scanning
  - Tools & techniques
    - Nmap, Shodan, PLCScan, Scapy, Modbuspal, Metasploit, …

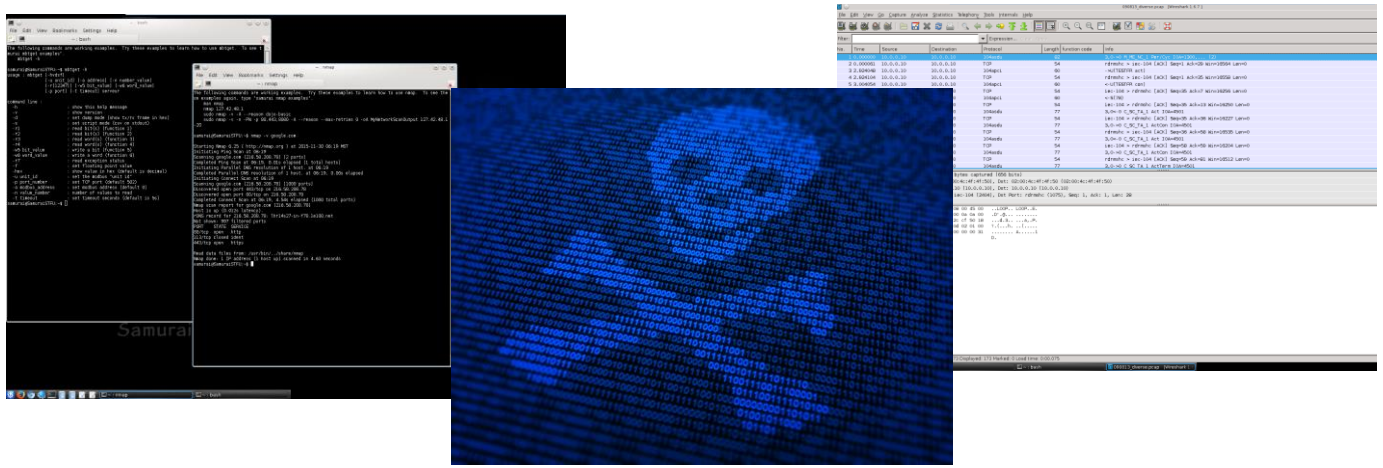
SHODAN Computer Search Engine

NMAP

metasploit®

Think like a hacker …

- Hands-on: Red team excercises & Demo's
  - Capturing and Fuzzing Modbus traffic to manipulate a procces



Summary

- What will you receive
  - Basic knowledge of how Industrial control systems function, their components and architectures
  - Learn why Industrial control systems are different from their IT counterparts
  - Basic understanding of how “hackers” can infiltrate control systems and manipulate them
  - Experience through hands-on sessions
- Who Should attend
  - IT (includes operational technology support)
  - IT security (includes operational technology security)
  - Engineering
- Prerequisites
  - Understanding of TCP/IP & Networking design/architectures
  - Laptop Required

"That concludes my prepared remarks.
I'll take questions that fit my prepared answers."