Introduction to ICS

Introduction to ICS

Tiberius Mihai

Advisor, IT Security

Stefan Minciu

Advisor IT Security

05.11.2021

$ whoami

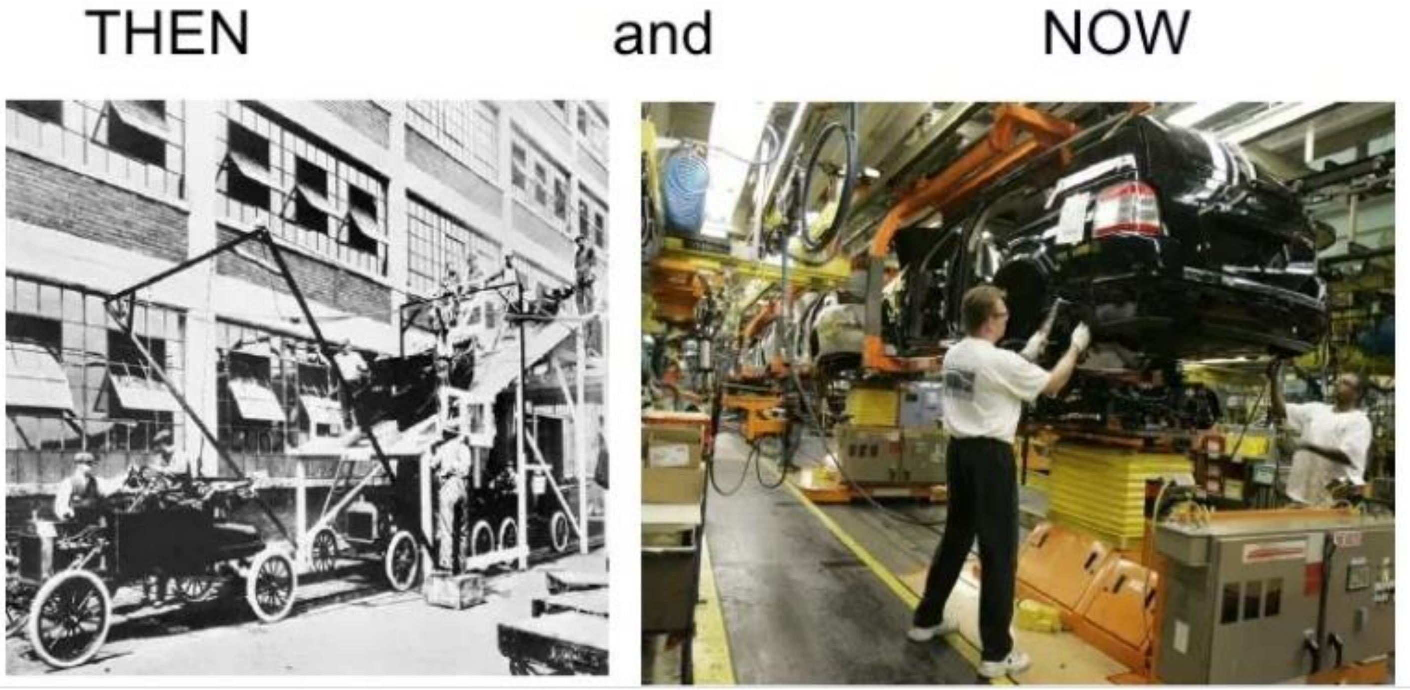
- Tiberius Mihai
- Advisor IT security
- 5 years in DCS development

- Minciu Stefan
- Advisor IT security
- Over six years as SCADA developer

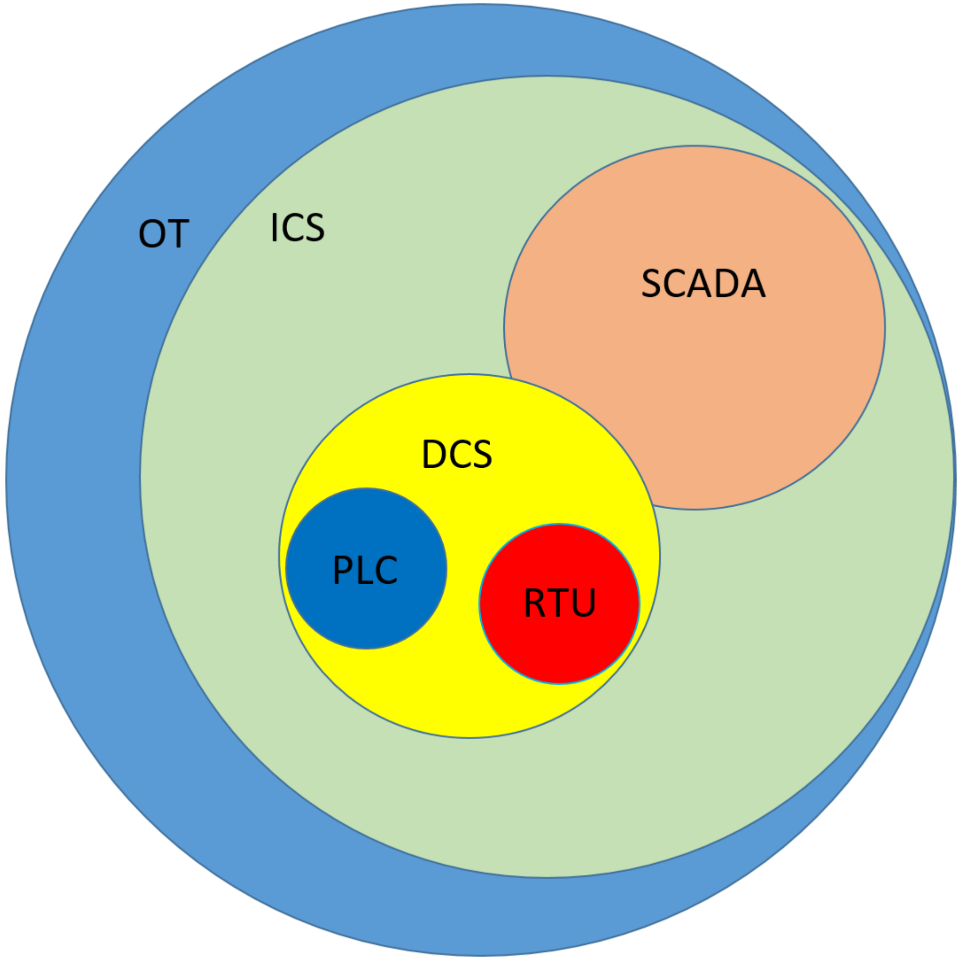
Summary

- Presentation purpose
- General information: ICS
- Field devices and Controllers
- Supervisory systems
- ICS cyber-kill chain
- Case study - Crashoverride
- ICS process simulation

Key Concepts in Industrial Environment



Key Concepts in Industrial Environment



Open loop

Closed loop

Manual mode

Control Systems

Control System

A device / set of devices that governs the behavior of other devices / systems

Examples:

- Home thermostat
- Access doors
- Elevators

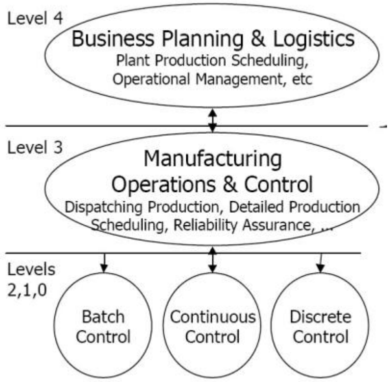
ICS

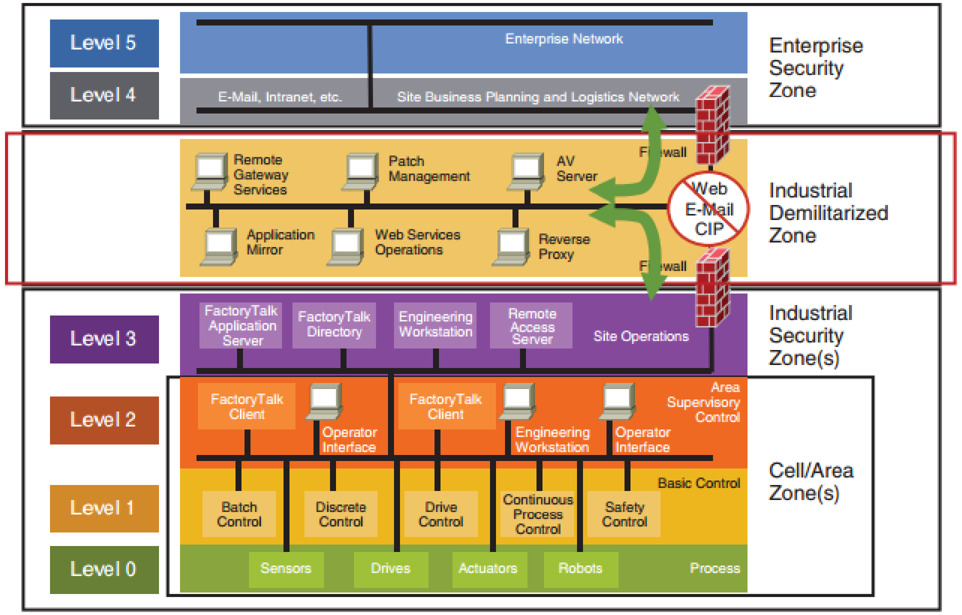
Large group of control systems

Exponentially more complex and dangerous

Purdue Architecture

- One of the most known architectures for ICS
- Created by a consortium – Purdue + Industry
- Each level has specific devices and applications associated





Purdue levels 0 and 1

Controllers

- **PLCs**
- **RTUs**
- **IEDs**

Field device

- **Sensors**
- **Actuators**

Field devices

- Two main categories of devices:
  - Sensors: pressure, temperature, humidity, vibration, etc.
  - Actuators: solenoids, valves, pumps, burners, etc.
- Communication can be done using:
  - Basic I/O: digital and analog signals
  - Smart I/O: using network protocols
- Time synchronization is critical









Programable logic controllers - PLCs

- Main component of the control process
- Physically hardened
- General purpose controller

Remote terminal units - RTUs

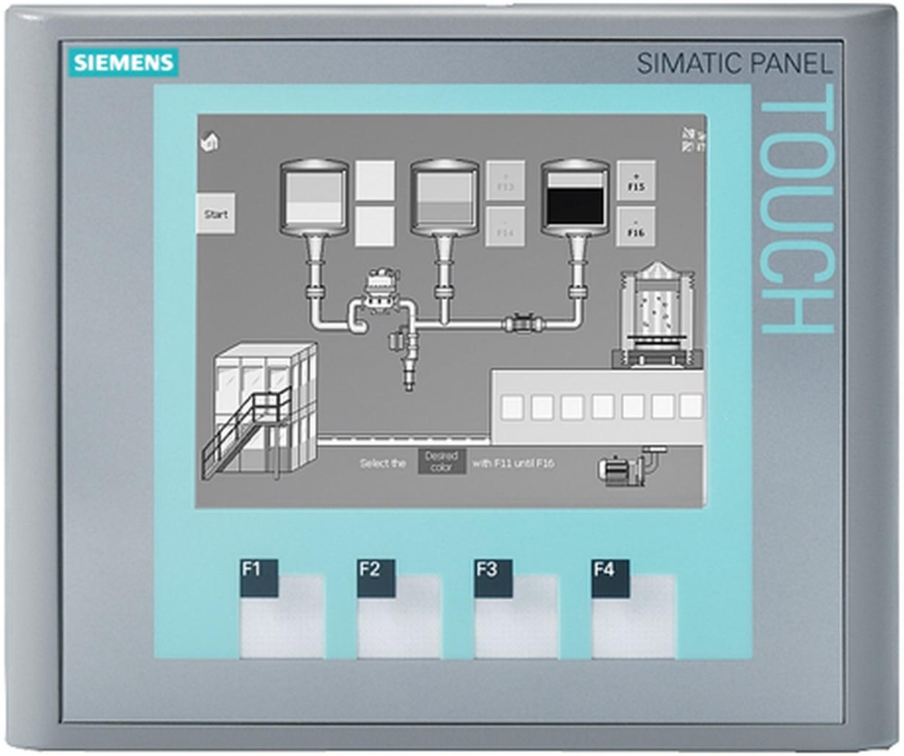
- Intermediate devices between the control systems and the supervisory level
- Used when control systems are spread over a large geographical area
- Usually used with WAN connections
- Can run simple programs

Inteligent electronic devices - IEDs

- Purpose built controller
- Device is self-contained
  - Limited functionality
  - Code cannot be extended
  - Microcontroller based

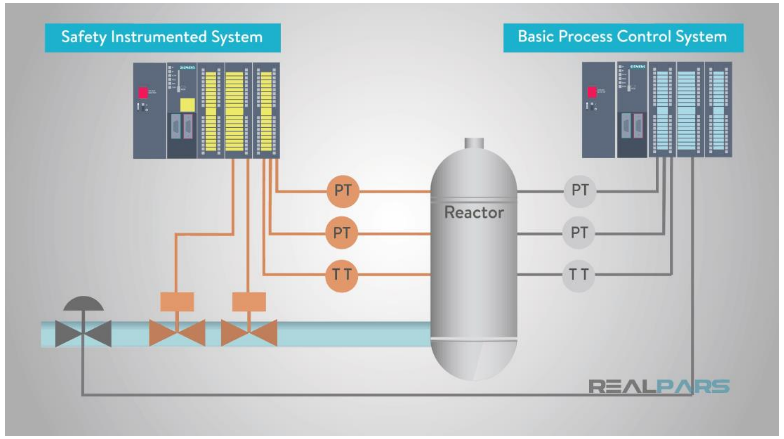
Human Machine Interfaces - HMIs

- Mainly used for process status visualization
- Contain inputs to control the process locally
- Embedded web servers allow visualization remotely



Safety Instrumented Systems - SIS

- Dedicated system for monitoring and controlling dangerous situations in the process
- Program logic is simpler than the control logic

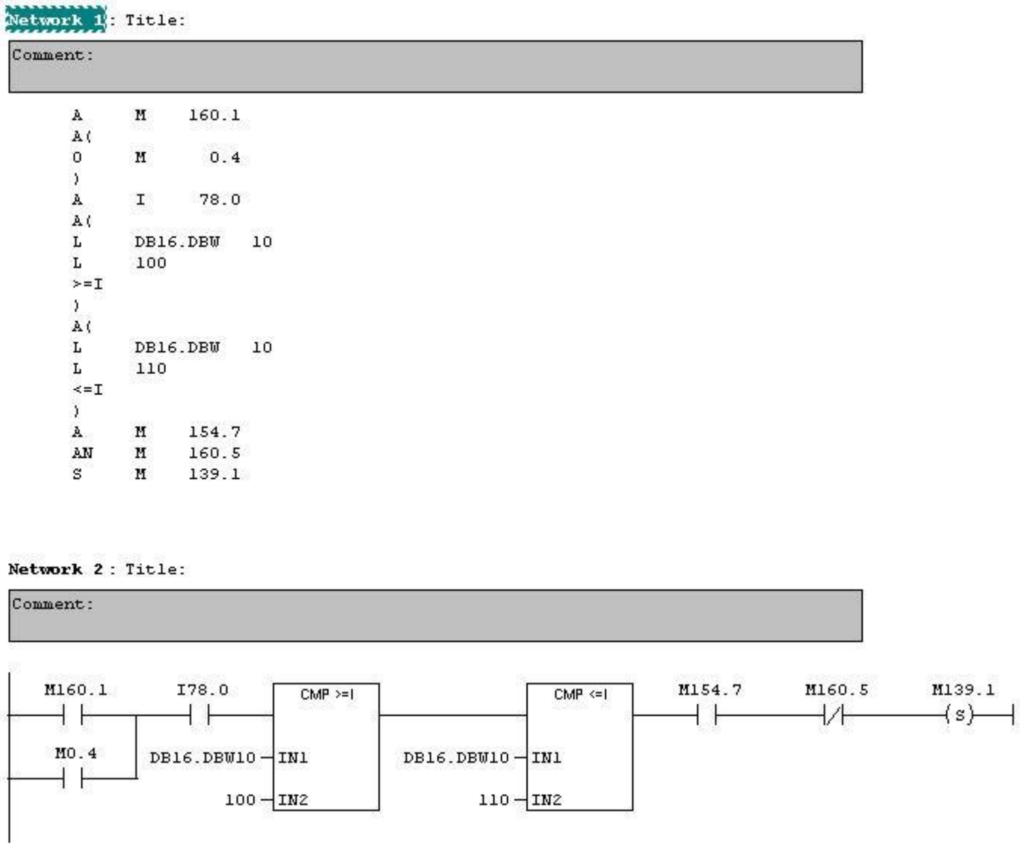


Controller programming

- Real time operating system
- Programmed for a specific task
- Standard IEC 61131-3 defines 5 standard languages:
  - Instruction List
  - Ladder Logic
  - Structured Text
  - Function Block
  - Sequential Function Chart

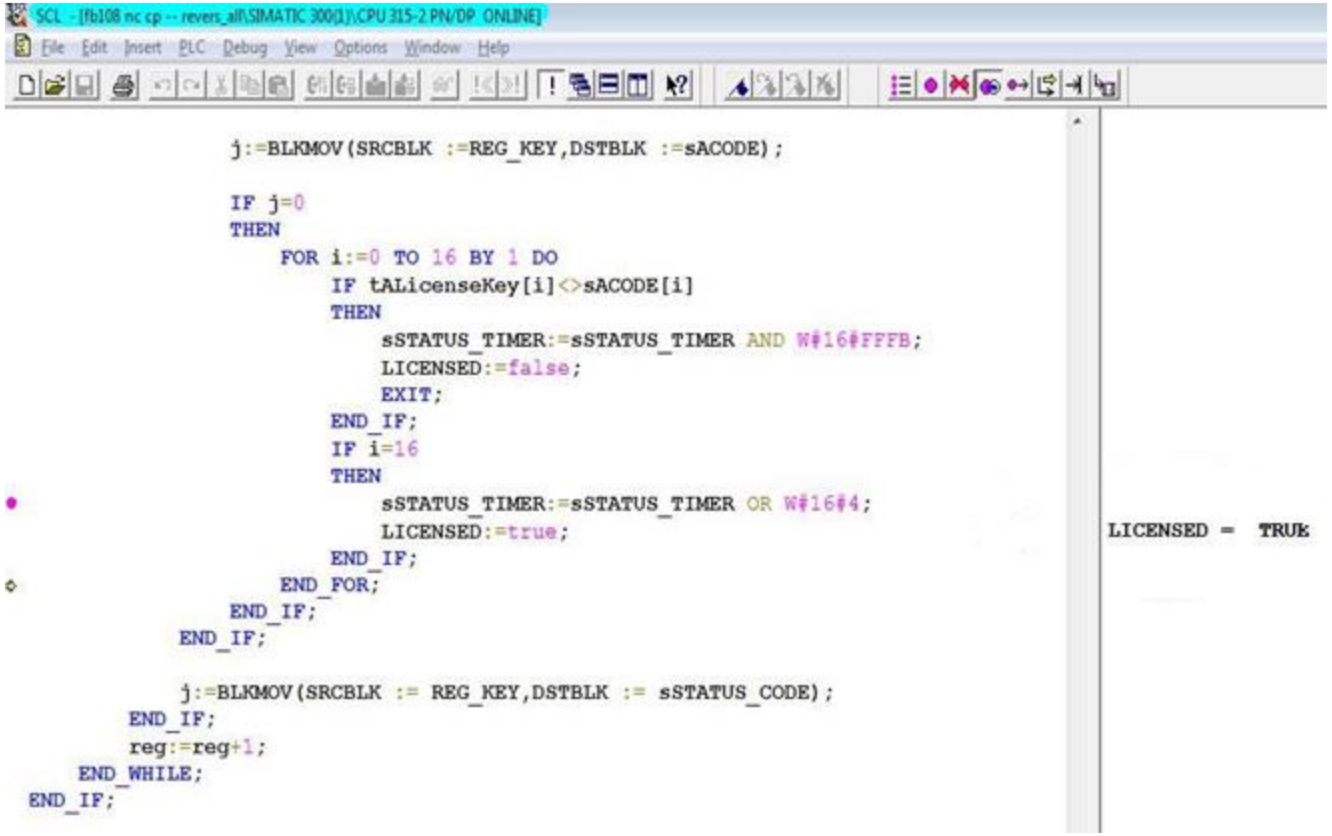
IL and LAD

- Instruction list – similar to assembler, popular especially in Europe
- Ladder diagram – derived from electrical diagrams, easy to read, easy to debug
- Disadvantages of this languages: difficult to implement complex functions, code is not compact



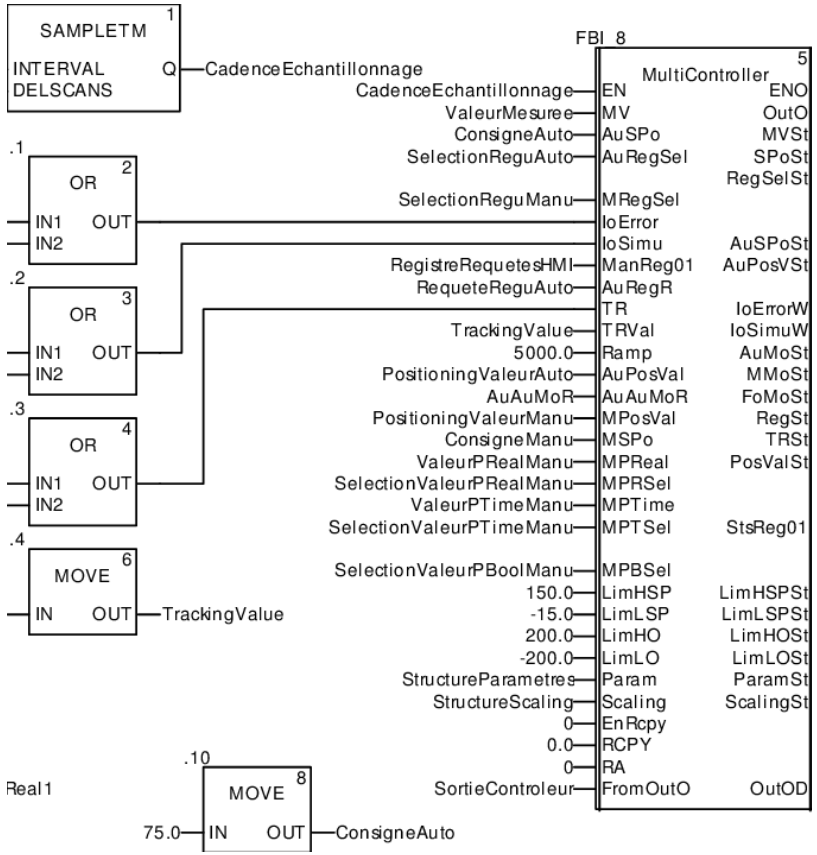
STL

- Similar to high level languages like C
- Suited for creating complex functions
- Can be hard to debug



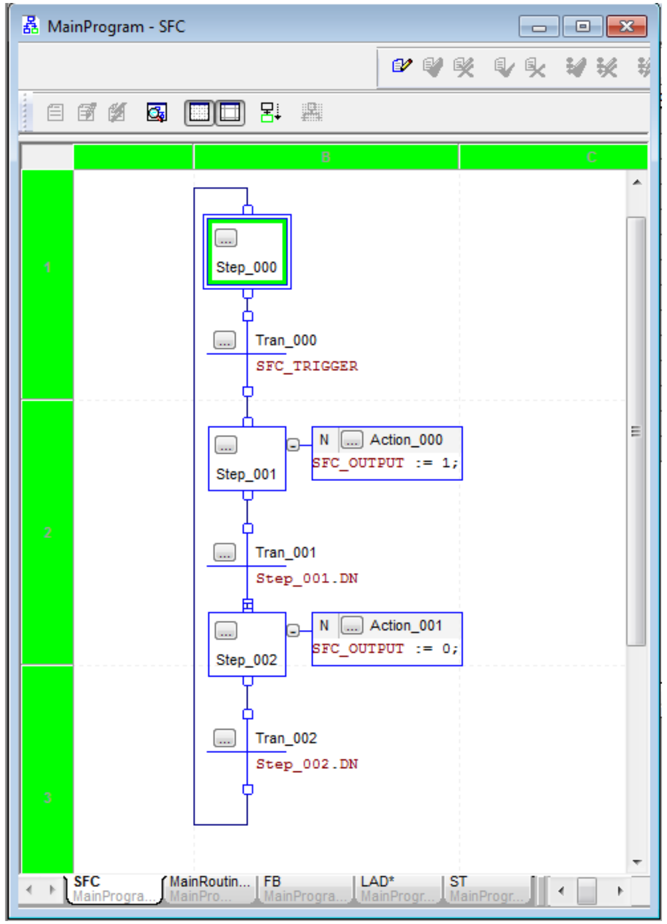
FBD

- A series of blocks with connected inputs and outputs
- Can be used for a high-level overview of the automation process

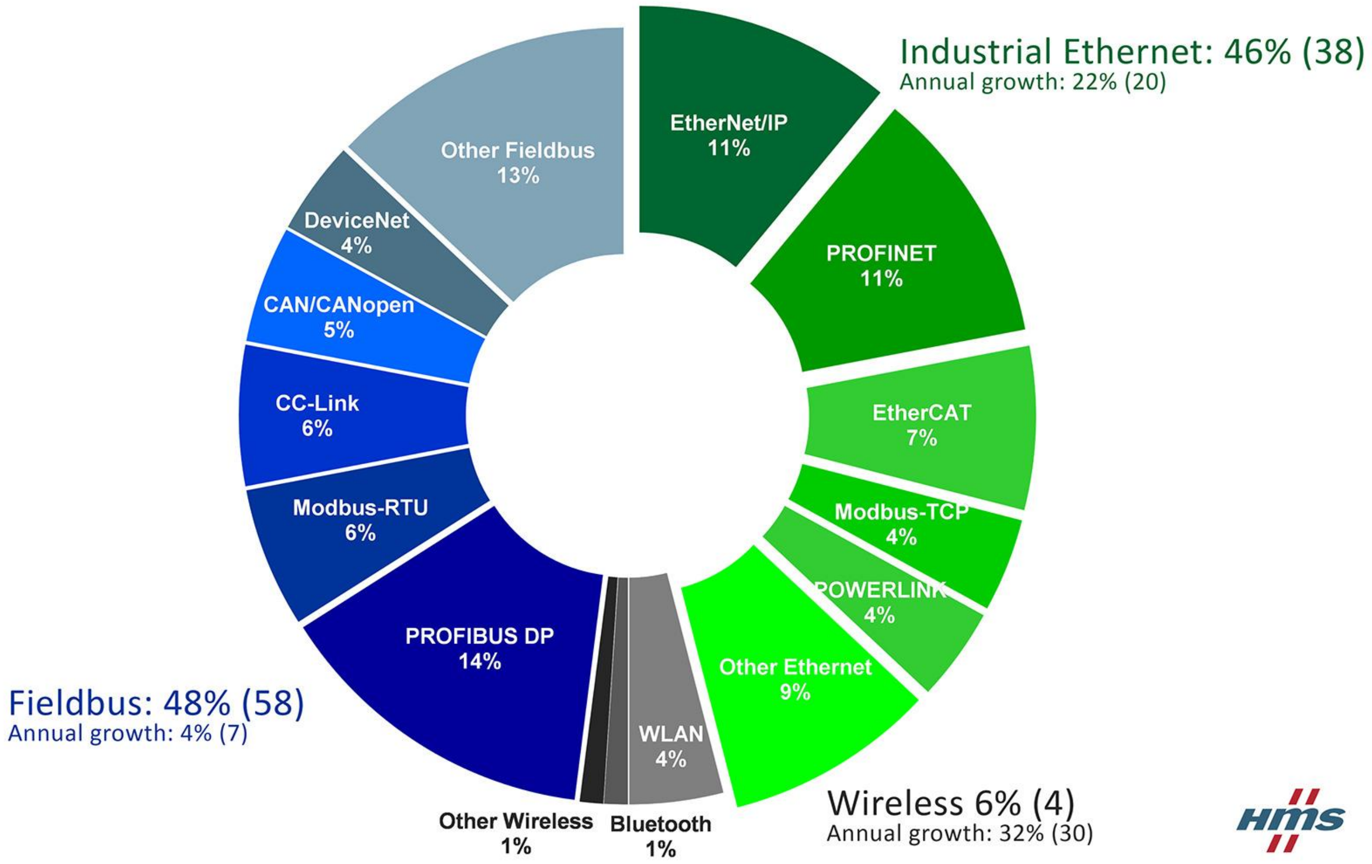


SFC

- A series of steps and transitions
- Can be used for the implementation of state machines in control sequences



Industrial communication protocols

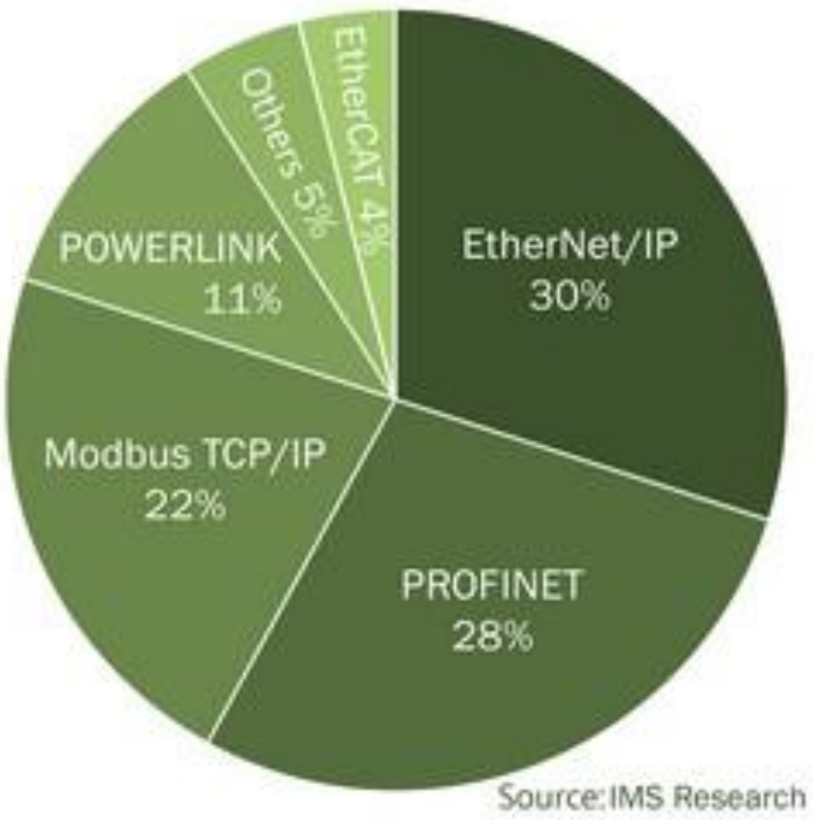


Protocol types

- Three main types:
  - Serial
  - Ethernet based
  - TCP/IP based
- Split into communication families
- Each family can have one or more implementation types

Comunication Profile Families			
Family	**Serial Bus Based**	**Ethernet Based**	**TCP/IP Based**
CPF 1	Fundation Fieldbus H1, H2	HSE	-
CPF 2	ControlNet, DeviceNet		EtherNet/IP
CPF 3	Profibus(DP, PA)	Profinet(RT,IRT)	Prifinet TCP/IP
CPF 4	P-NET	-	-
CPF 5	WorldFTP		-
CPF 6	Interbus	-	-
CPF 8	CC-Link	CC-Link IE	-
CPF 9	HART, WirelessHART	-	-
CPF 10	Yokogawa Vnet	-	Vnet/IP
CPF 11	-	Toshiba Tcnet RTE	Toshiba Tcnet
CPF 12	-	EtherCAT	EtherCAT UDP
CPF 13	-	Ethernet Powerlink	-
CPF 14	-	EPA	-
CPF 15	Modbus (RTU, ASCII)	-	Modbus TCP
CPF 16	Sercos I, Sercos II	Sercos III	-
CPF 19	Mechatrolink-II	Mechatrolink-III	-

Ethernet based protocols



Modbus TCP

- Developed by Modicon in 1979
- Widely accepted protocol
- Master – slave protocol:
  - Master polls the field devices
  - Field devices can’t initiate the communication
  - I/O divided between contacts/coils and registers
- Currently an open protocol managed by a foundation (2004)
- Security was not taken into consideration when developing the protocol

Profinet

- Ethernet implementation of Profibus(serial protocol)
- Has 3 different versions:
  - TCP/IP – transport of noncritical data(100ms)
  - RT(Real Time) – control systems 10ms
  - IRT(Isochronous Real Time) - high speed loops(1 ms)
- Device discovery via Profinet DCP
- Field devices have slot and sub-slot identifiers

Ethernet IP

- Ethernet implementation of DeviceNet (2001)
- Facilitates the use of Common Industrial Protocol
- Uses broadcast UDP for I/O data
- Data rates are defined by the engineer
- Newer versions of the protocol support unicast

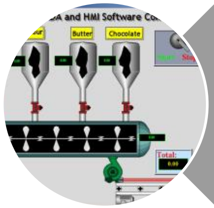
DNP3

- Primary used in the energy sector
- Master-slave protocol
  - Timestamped data
  - Unbalanced/balanced
- Cryptographic protection via TLS

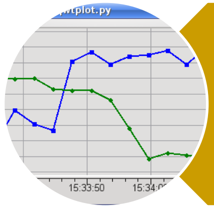
OPC / UPC UA

- ICS vendor neutral protocol
  - Provides a consolidated data view
  - Allows data collection and generating views
- Two variants OPC DA/UA
  - DA – supported only on Windows
  - UA - cross platform
- OPC UA provides a common framework to interface

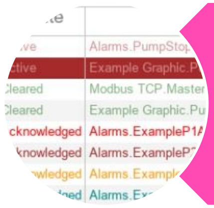
Basic components – L2



HMI



Historian



Alarms

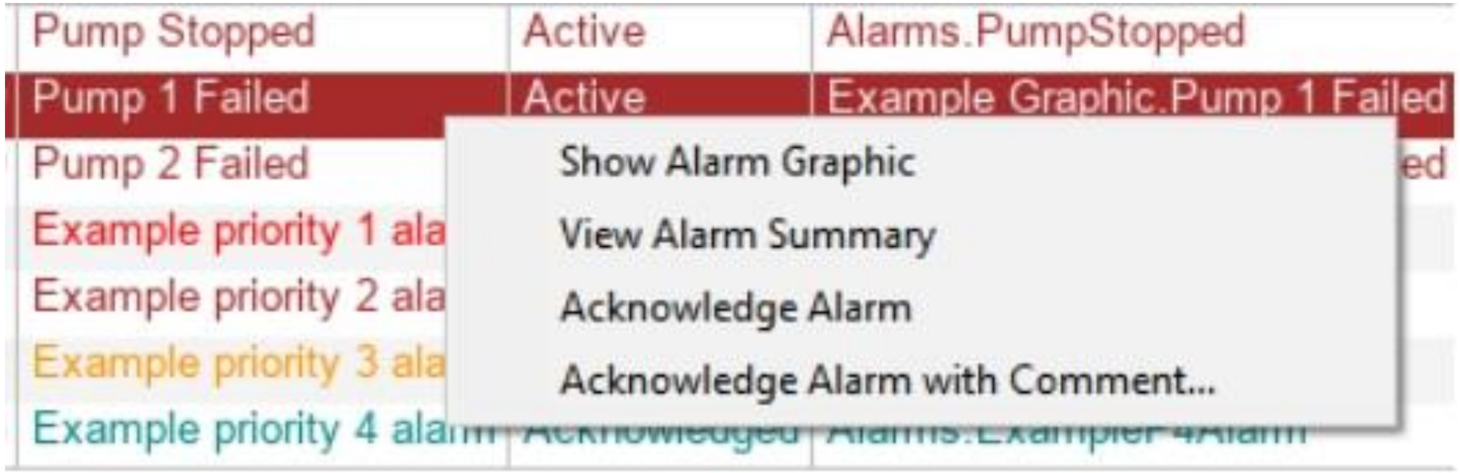
Human machine interface (HMI)

- Presents process data to human operator
- Typically a model diagram created by integrator
- Also displays alerts that require operator attention
- HMI may facilitate manual control of the process
- SCADA system can work without HMI

*slide source Sans Institute

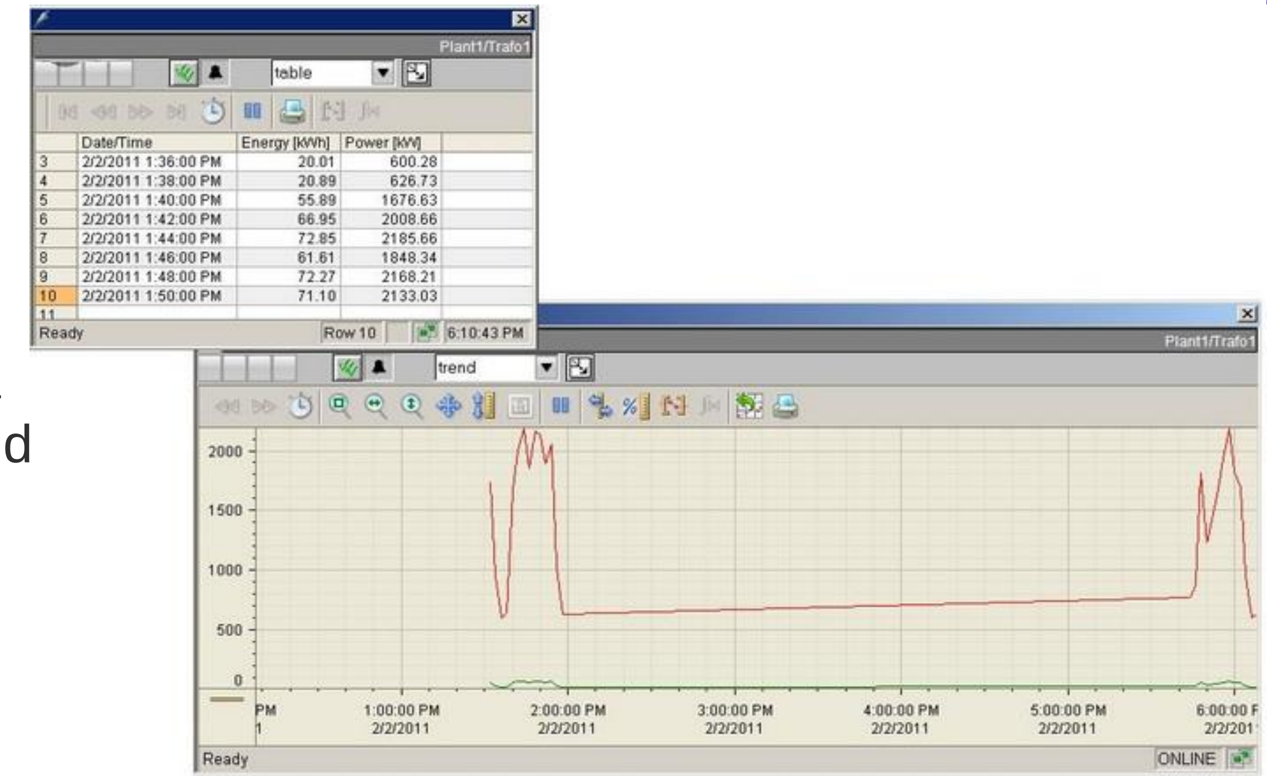
ALARMS

- An alarm informs operators of an abnormal event or condition
- Alarms may be visual, audible, or digital
- Annunciator panels aid in locating problem



Historians

- Data store for ICS process data
  - often is a relational database (SQL), but not always
  - contains event logs as well as time-series data
  - could have traditional GUIs, web interfaces, and API access
- Business needs access for its processes
  - should replicate master historian in ICS to a read-only slave historian for business
- Helps to create repots



OS compatibility

Windows :
1.Citect - Schneider
2.SIMATIC WinCC - Siemens
3.Visual Designer - Eaton
4.FactoryTalk View - Rockwell Automation
5.Cimplicity - General Electric Digital

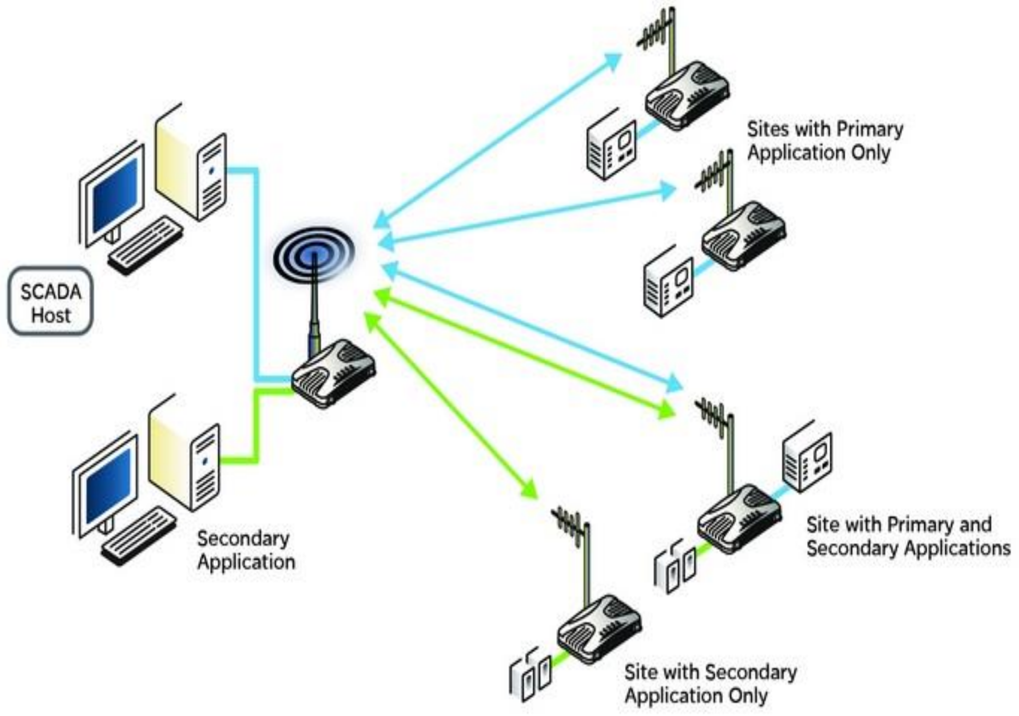
Linux, Unix and Windows:
1.Fast/Tools SCADA – Yokogawa

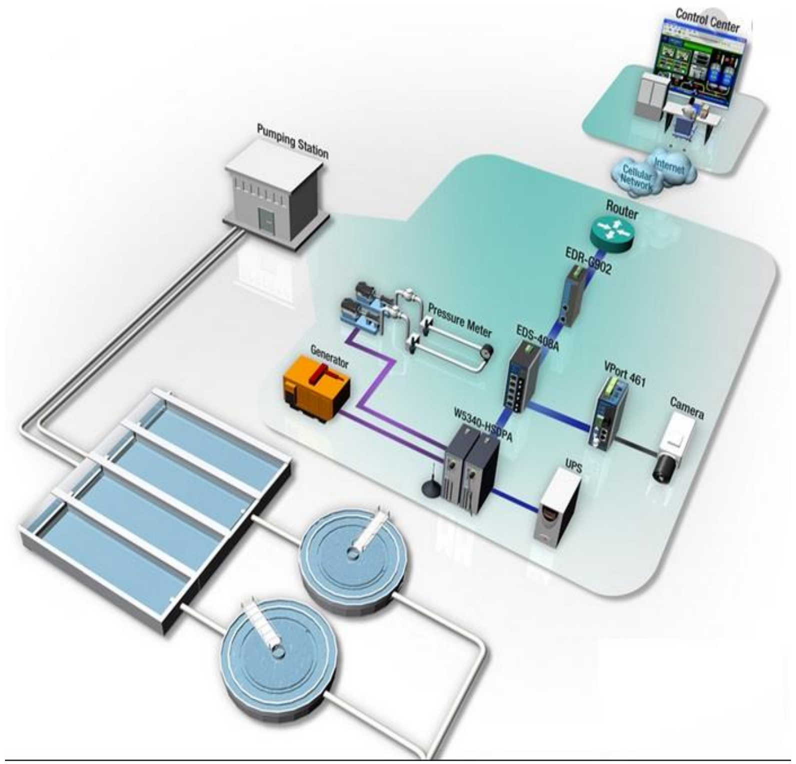
RTOS - real-time operating system
1. PLC / RTU
2. Embedded Systems

Windows, Linux and Mac OS:
1.MySCADA - MySCADA technologies
2.ScadaBR - MCA Sistemas

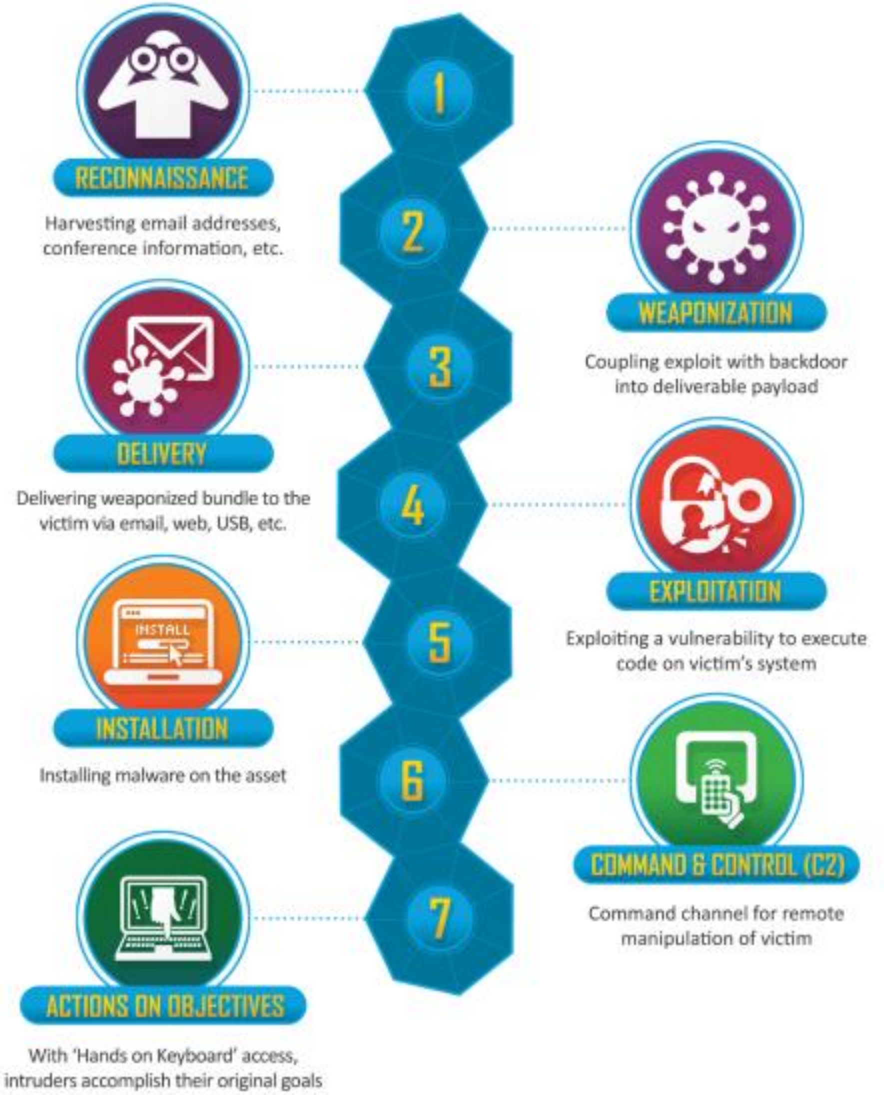
ICS system- Implementation examples

- **SCADA** - Supervisory control and data acquisition (*oil and gas pipelines, wind farms, water sector*)
- **DCS -** Distributed control systems (*oil refining, pharmaceuticals, food sector, petrochemical*)
- **BMS / EMS -** Building management system / Energy management system (*buildings, warehouse)*
- ***MES** – Manufacturing execution system (manufacturing, pharmaceutical, food sector, etc)*



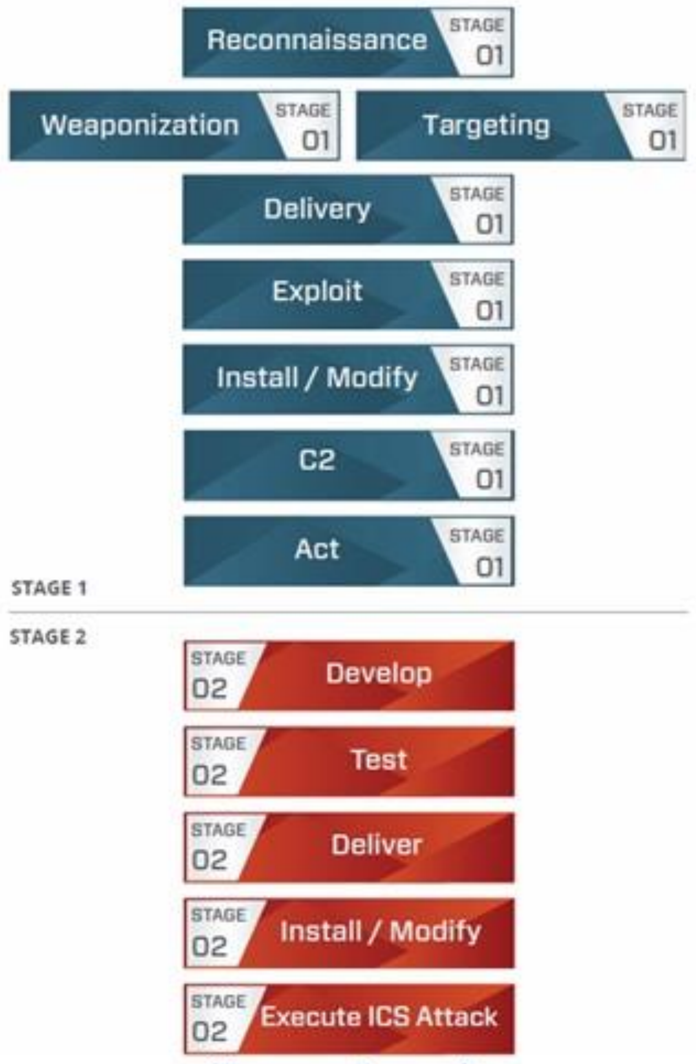


IT – Cyber Kill Chain Model



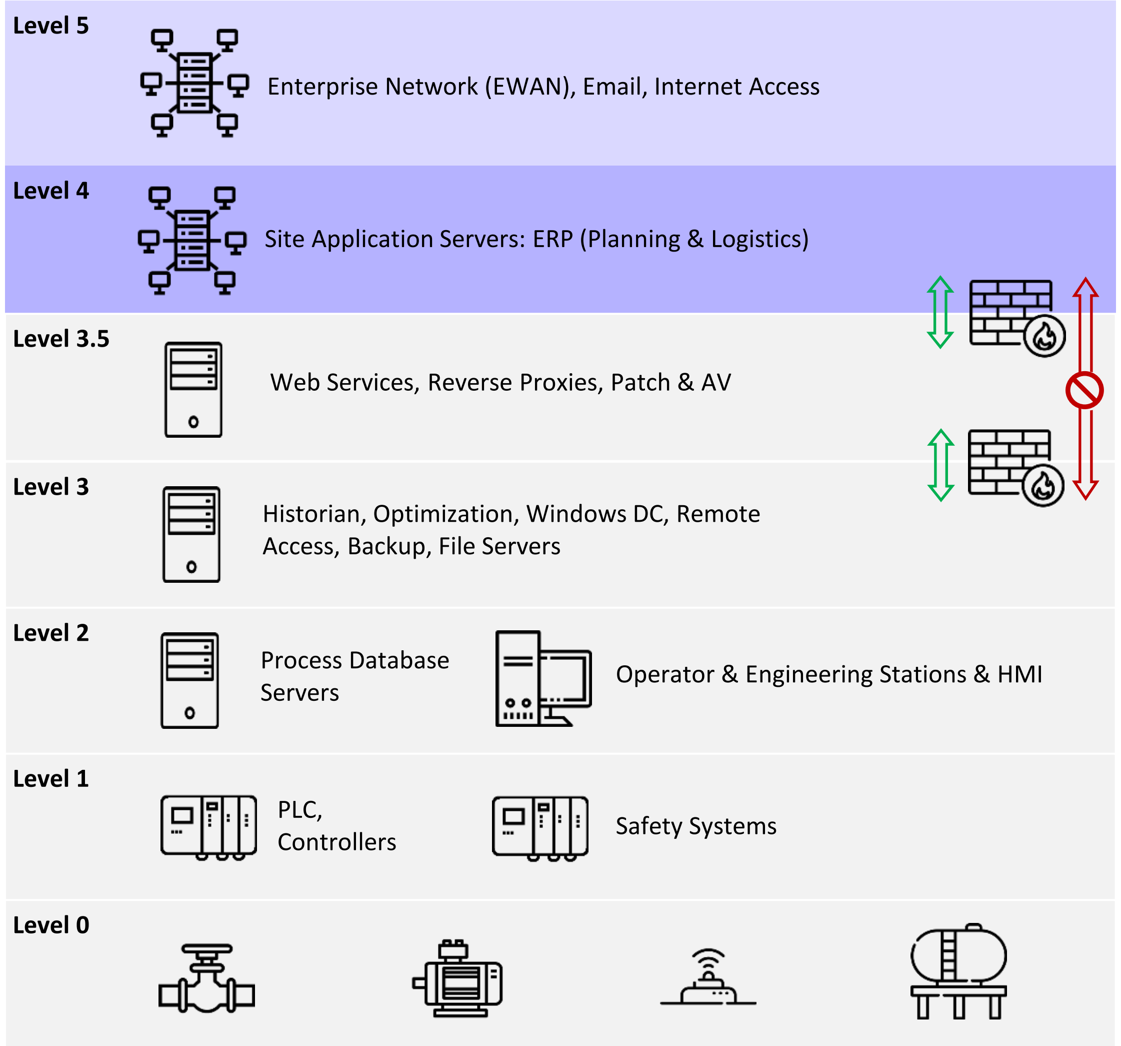
ICS – Cyber Kill Chain Model

- the cyber kill chain is a series of steps that trace stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The kill chain helps us understand and combat ransomware, security breaches, and advanced persistent attacks (APTs).



(Source: Dragos)

The attack surface – L4 & L5



- **Levels 5 & 4:** common Enterprise IT environment.

- Typical attacks:
  - Delivery with Phishing
  - Waterhole Attack
  - Vulnerable exposed services
  - Initial access and lateral movement with valid accounts

- Potential OT attack indicators:
  - Persistence
  - Lateral movement
  - Significant data collection (emails or files exfilled)

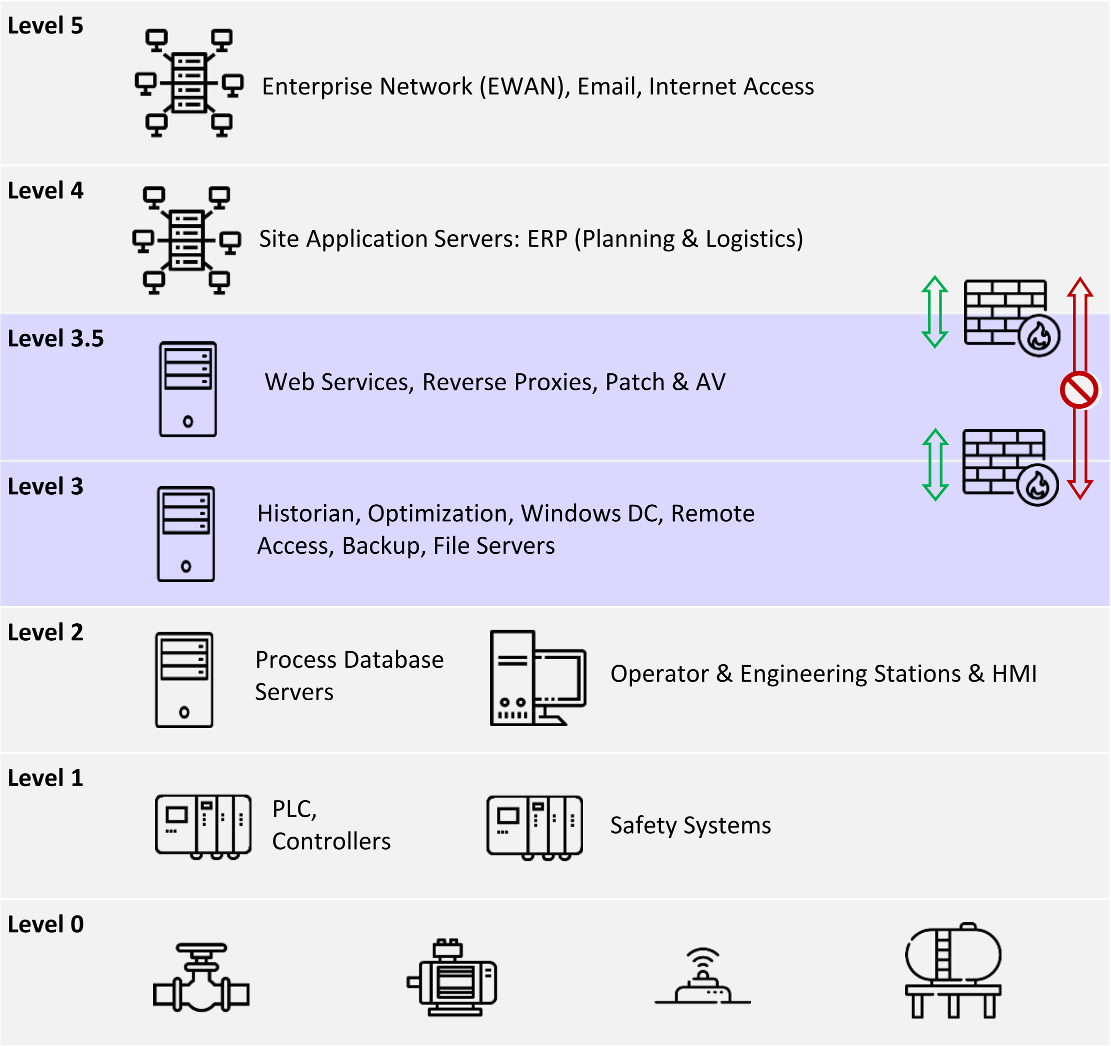
- Known Malware:
  - Havex (phishing attack vector)
  - BlackEnergy (spear phishing attack vector)

ICS malware – L4 & L5

- **Havex**
  - Remote access trojan used for espionage - discovered in 2013
    - modular malware allows various plugins/modules
      - OPC to conduct reconnaissance on industrial equipment on the target network.
  - delivered in numerous ways, including:
    - Phishing
    - Waterhole attack
    - Embedded in installer or firmware on vendor website
  - after infection a system, it connect back to one of hundreds C2 servers
  - target: infected more than 2470 victims (industries such as pharmaceuticals and energy)

- **BlackEnergy**
  - Used by cybercrime groups since 2007 for DDS service attacks
  - An advance actor took BE and upgraded it with new capabilities
    - zero-day exploit
    - SCADA exploit: SIMANTIC, CIMPLICITY and Advantech
  - Target: campaign across multiple years targeting Russian-based interests such as Ukraine, Poland, NATO

The attack surface – L3.5 & L3



© Leandros Maglaras, source: [Purdue Model for Control Hierarchy (researchgate.net)]()

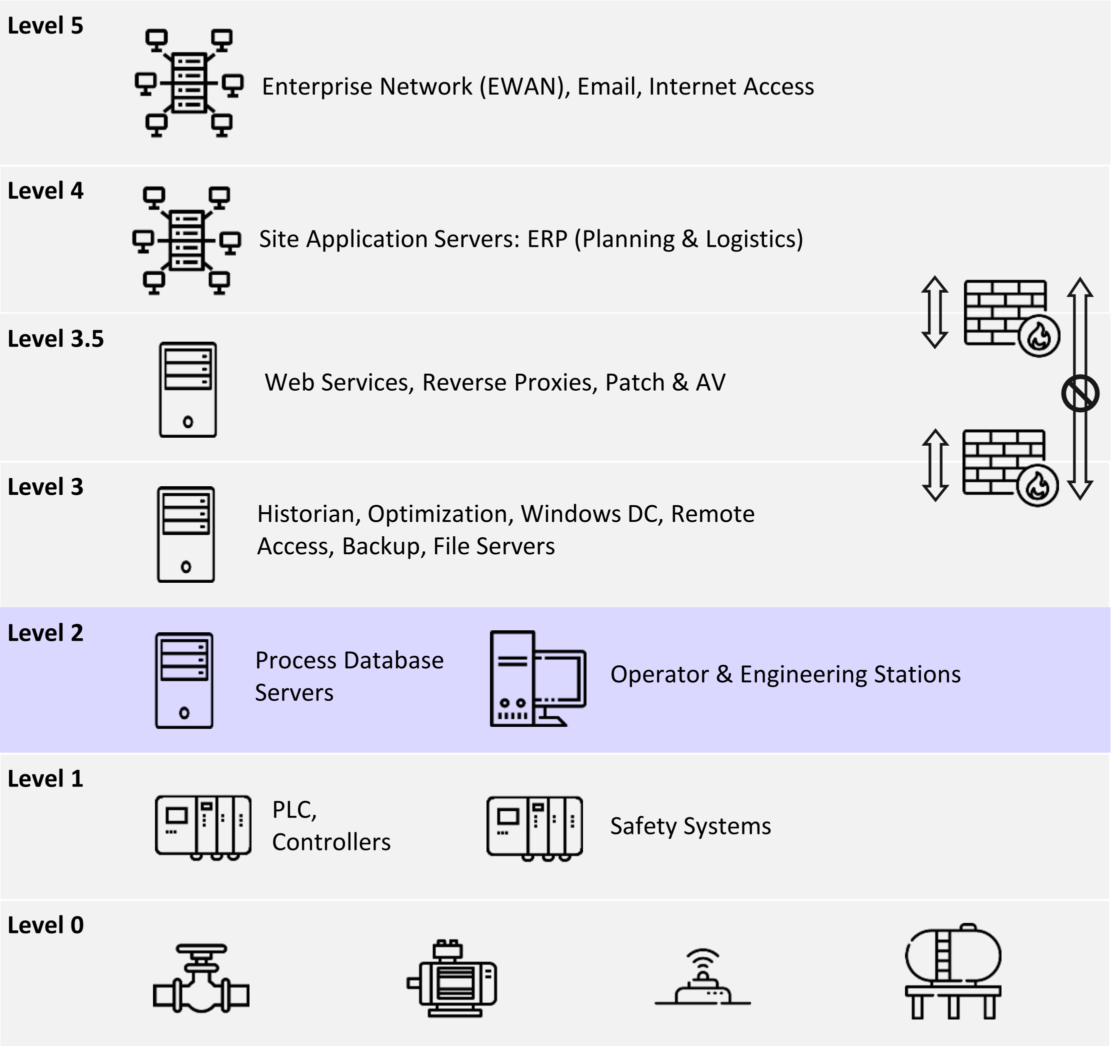
- **Level 3** – where high-level Applications are.
- **Level 3.5** or Plant DMZ.
  - Might be used to link to other plants.

- Typical attacks:
  - Lateral movement with valid accounts
  - Vulnerable exposed services
  - Discovery
  - Malware payloads
  - Improper configuration

- Potential OT attack indicators:
  - Any Malware detection
  - Any unknown outbound traffic

- Known Malware:
  - Havex (waterhole attack vector)
  - CRASHOVERRIDE (data historian provided access to OT)
  - Trisis/Tritron (it is known that a VPN provided access to OT)

The attack surface – L2



- **Level 2** – Supervisory network
  - This is where Operators (👷) work.

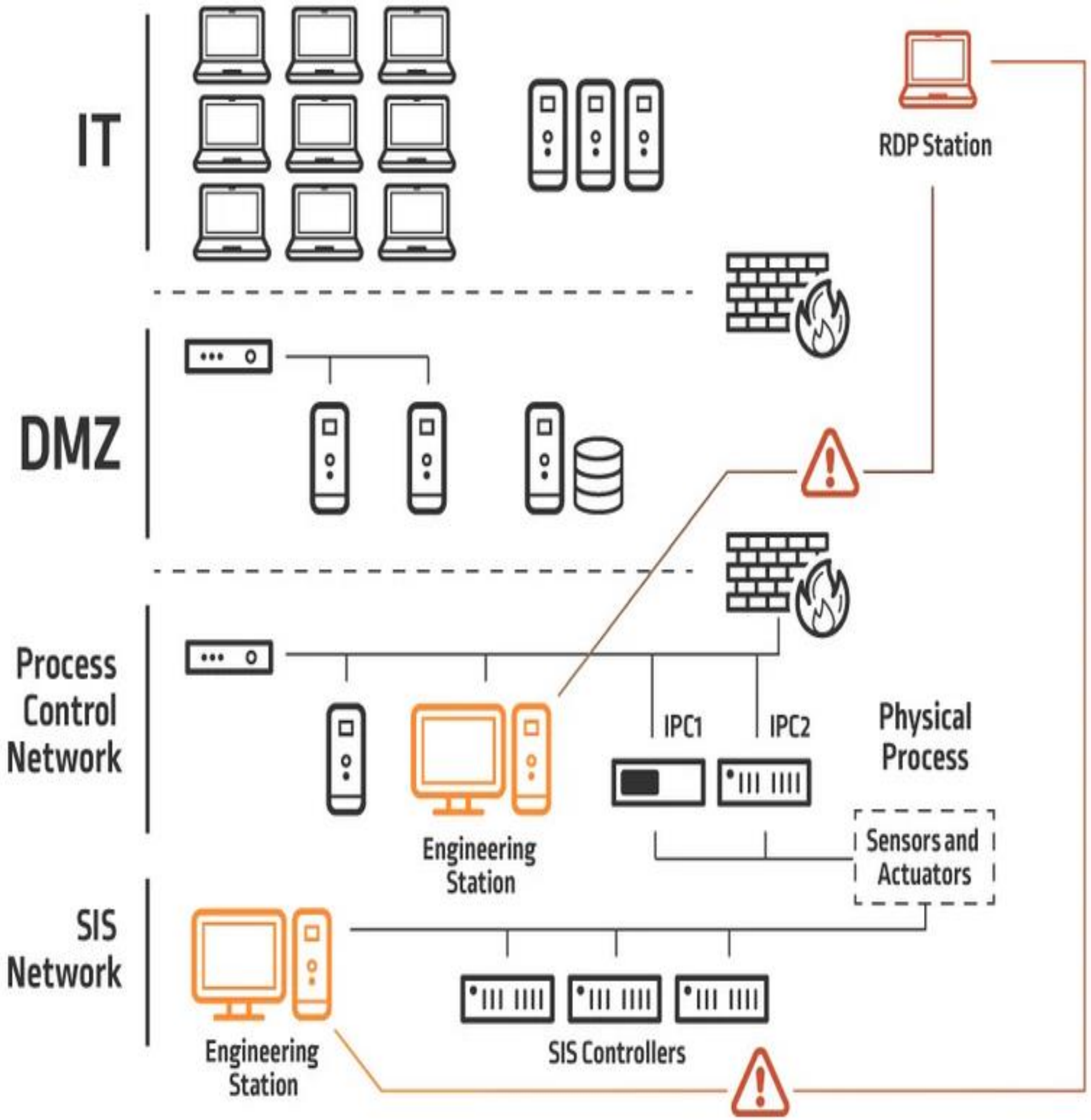
- Typical attacks:
  - Lateral movement with valid accounts
  - Remote access / Supply chain
  - Unauthorized operation
  - PLC program changes

- Potential OT attack indicators:
  - Unauthorized changes or access (programming)
  - System files integrity. Malware detection
  - Process Alerts baselining

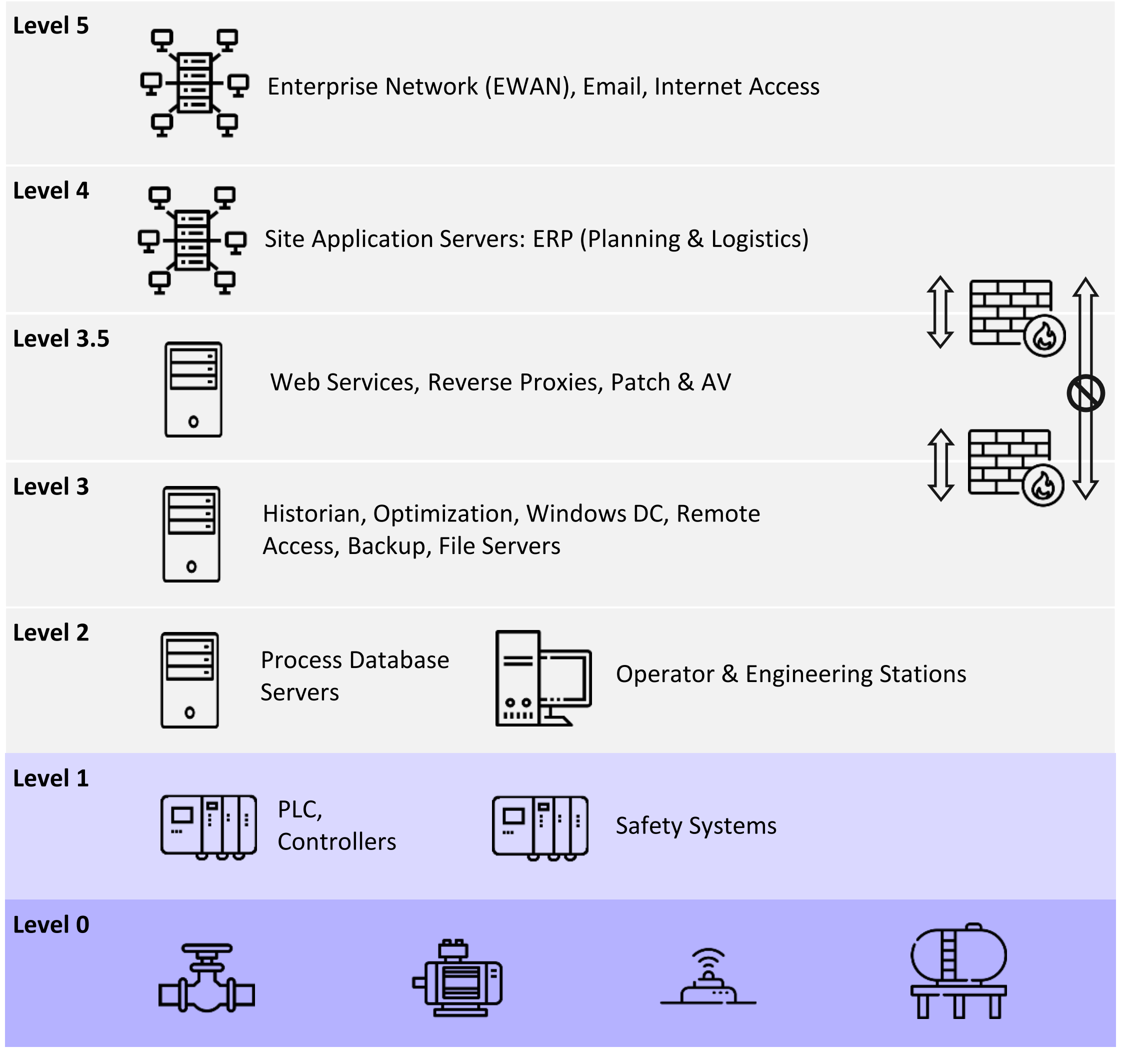
- Known Malware:
  - Havex (waterhole attack vector)
  - CRASHOVERRIDE (data historian provided access to OT)
  - Trisis/Tritron (it is known that a VPN provided access to OT)
  - Stuxnet (USB / Infected laptop)

ICS malware – L2

- **Trisis / Tritron**
  - Discovered on December 17, 2016
  - First to specifically target SIS
  - The attack caused a plant shut down in Saudi Arabia
  - The real impact was the potential for loss of human life
  - The adversary gained access to an Engineering Workstation connected to the SIS as early as 2015 and then developed TRISIS



The attack surface – L1 & L0



- **Level 1** – Controllers
  - Includes safety systems
- **Level 0** – Field devices
  - Can include wireless connections

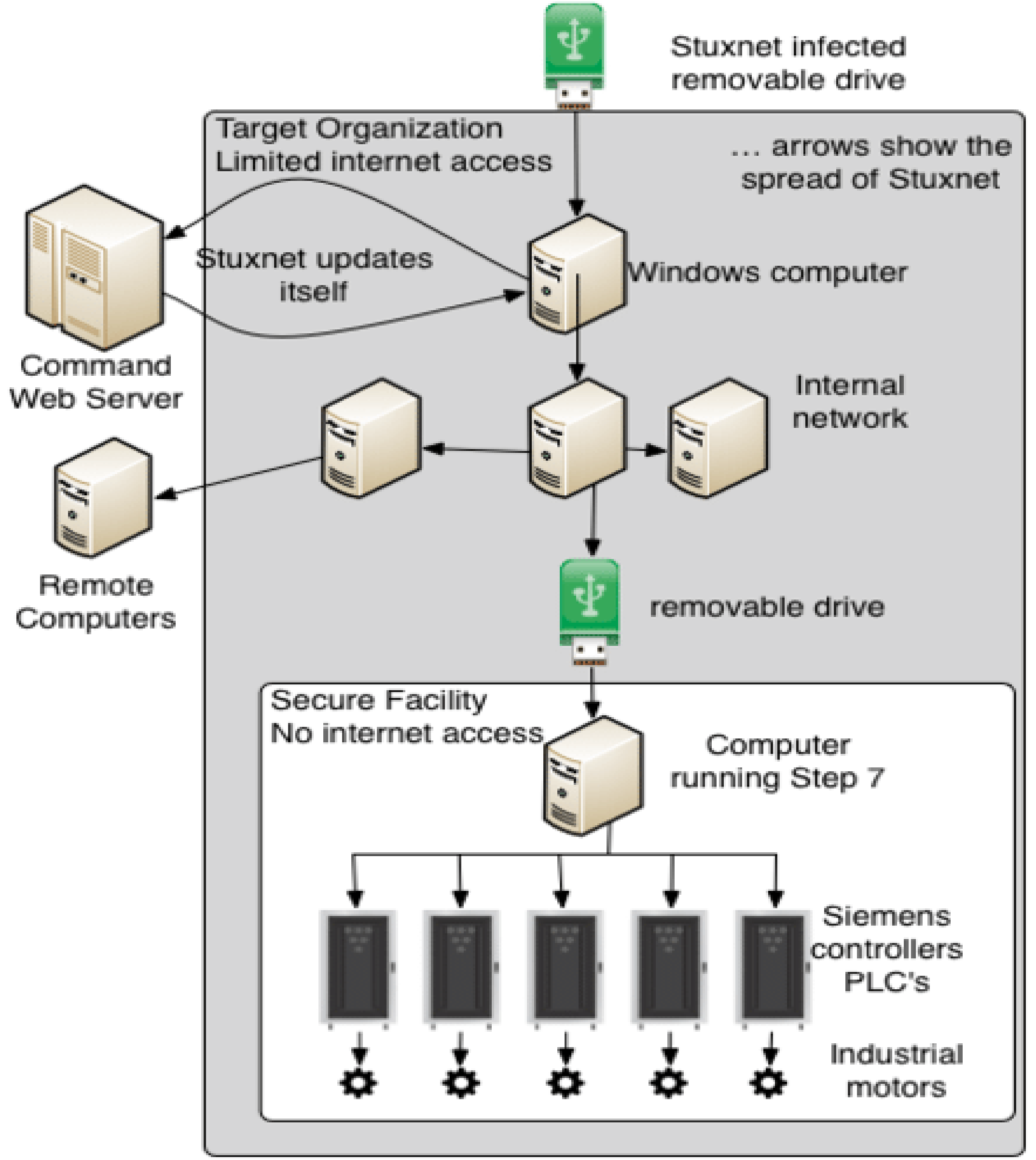
- Typical attacks:
  - Firmware rootkit
  - Change control / program logic
  - Deny access / service

- Potential OT attack indicators:
  - Traffic inspection and anomaly detection
  - Process Alerts baselining
  - Performance monitoring

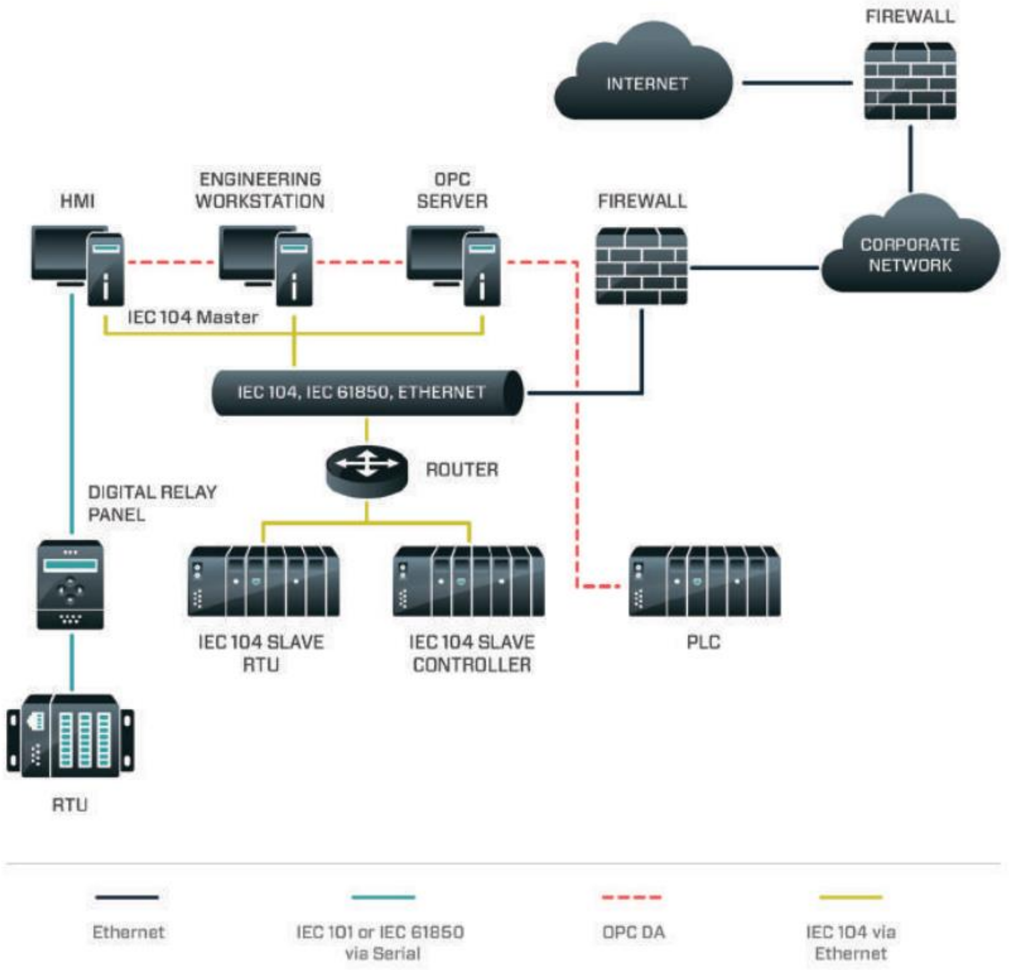
- Known Malware:
  - Stuxnet (USB / Infected laptop)
  - Trisis/Tritron

ICS malware – L1 & L0

- **Stuxnet**
  - Malicious computer worm first uncovered in 2010
  - Stuxnet targets supervisory control and data acquisition (SCADA) systems and is believed to be responsible for causing substantial damage to the nuclear program of Iran
  - Malware with four zero-days and an ICS-targeted payload
  - Bypassed air-gapped network through engineering laptop or USB



Crashoverride



Crashoverride

Phishing

- Most likely the initial access was done via phishing emails

Pivoting

- Attackers likely used credential dumping tools to obtain legitimate accounts
- Dual homed system was identified, and new accounts were created for additional access

Historian compromise

- Attackers compromised a historian due to its extensive connections into the ICS environment

Crashoverride

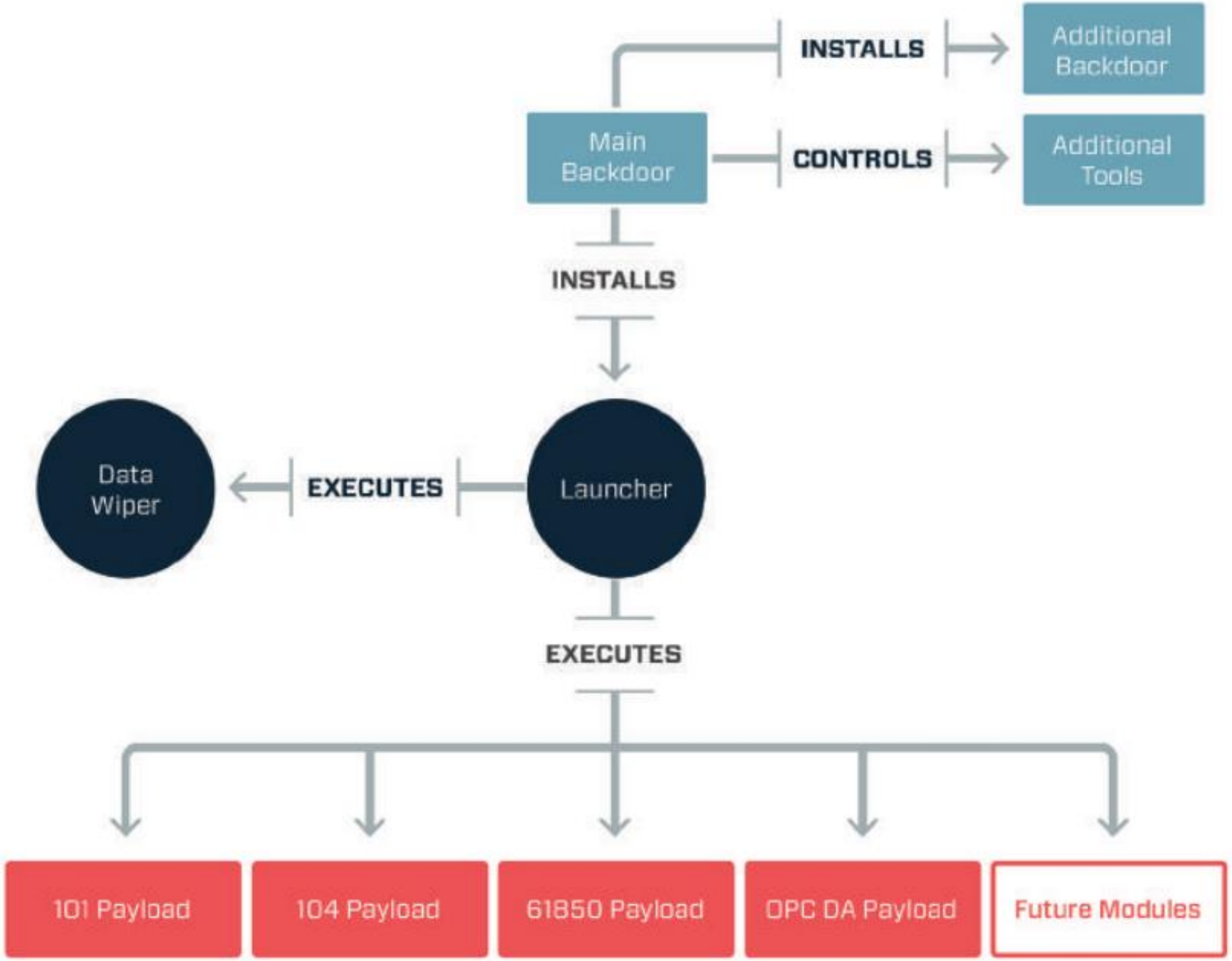
Pivoting in ICS
- Reconnaissance in ICS for systems of interest

Delivery
- Attackers deployed Crashoverride to the target systems
- Once copied Crashoverride is started as a system service

Execution
- Crashoverride has a modular approach with modules for IEC104, SIPROTEC DoS, DataWiper

Impact
- The impact was limited due to the attackers not controlling enough CB and failing to execute the DoS

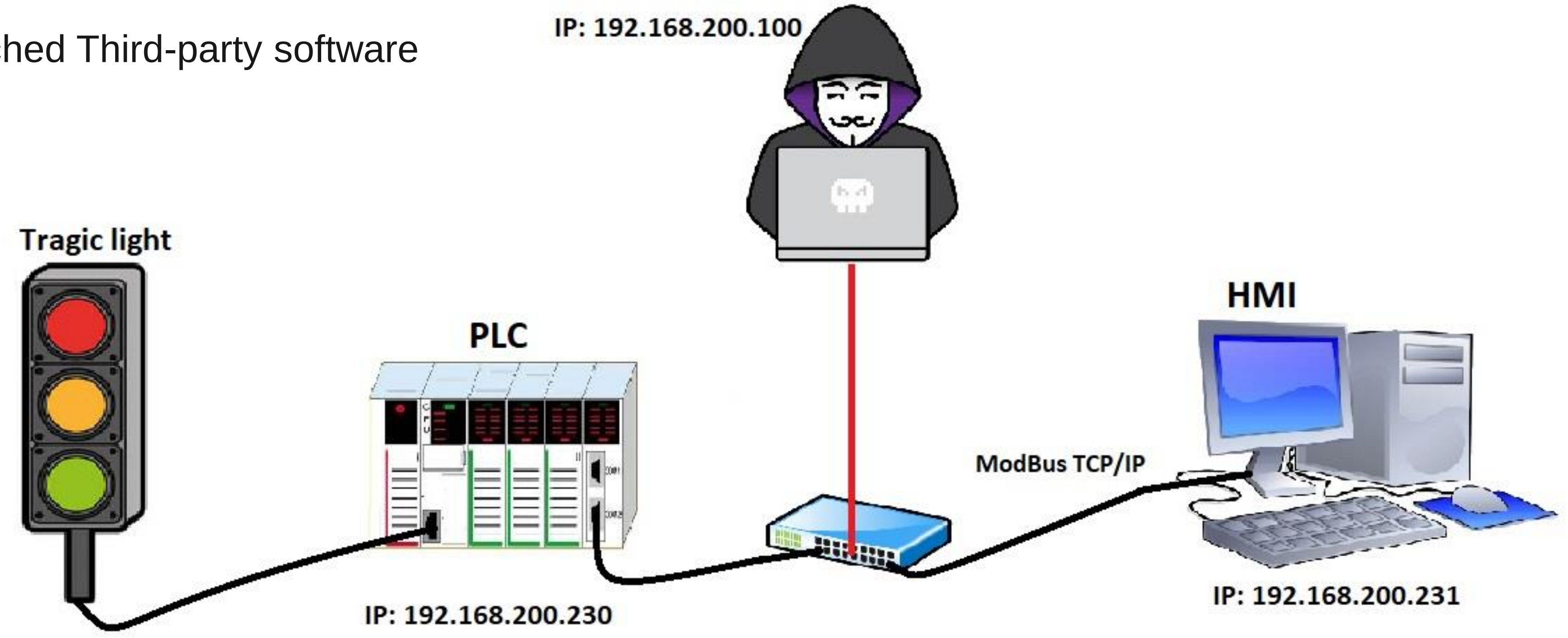
Crashoverride



ICS simulation overview

- SCADA system vulnerability:

- Weak protection of user credentials
- Open-Source Information Available
- Default Passwords
- Physical Access
- Unpatched Systems / Unpatched Third-party software
- Communication Protocols
- etc



Simulation Time