Pentesting ICS 101

By Arnaud SOULLIE

Who am I?

Arnaud soullié

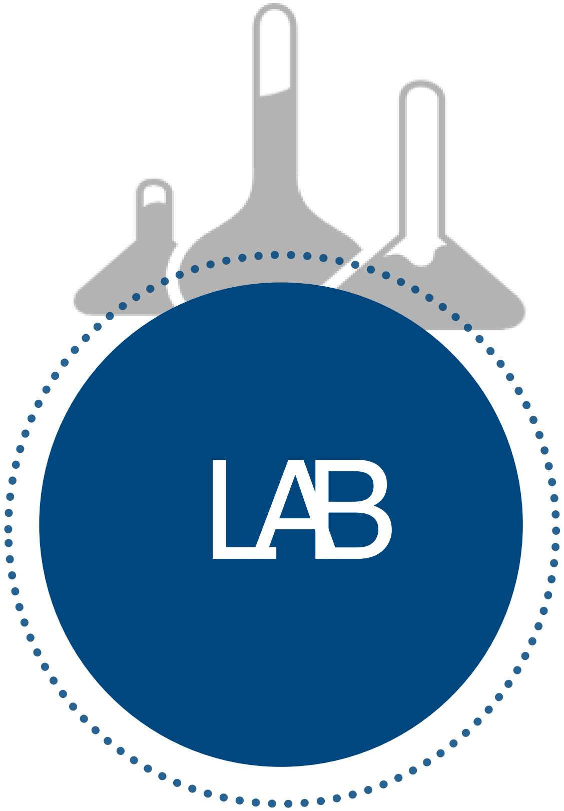
Senior security auditor

@arnaudsoullie

interests

- Windows Active Directory
  Can a Windows AD be secured ? JSSI 2014 (French, sorry)
- SCADA (BHEU14, HIP15, BruCon, BSLV15, DC24)
- Wine tasting / Motorbike riding
  (we're not going to talk about it today)
- Sorry for the French accent

WAVESTONE



LAB PREREQUISITE

WHAT'S IN THE LAB vm?

KALI LINUX

ADDITIONAL TOOLS

- MODBUSPAL
- MBTGET
- PLCSCAN
- SNAP7
- …

SCRIPTS

- PCAP SAMPLES
- SCRIPTS SKELETONS
- …

http://tinyurl.com/dc24-ics101

Agenda

DEFCON 24 ICS WORKSHOP

1. Introduction to ICS
2. WHAT'S wrong with ICS security ?

1h

3. Programming plcs HANDS-ON !
4. Pentesting PLCs HANDS-ON !

1h30

5. Capture the flag ! HANDS-ON !
6. Securing ics

1h30

ICS Introduction

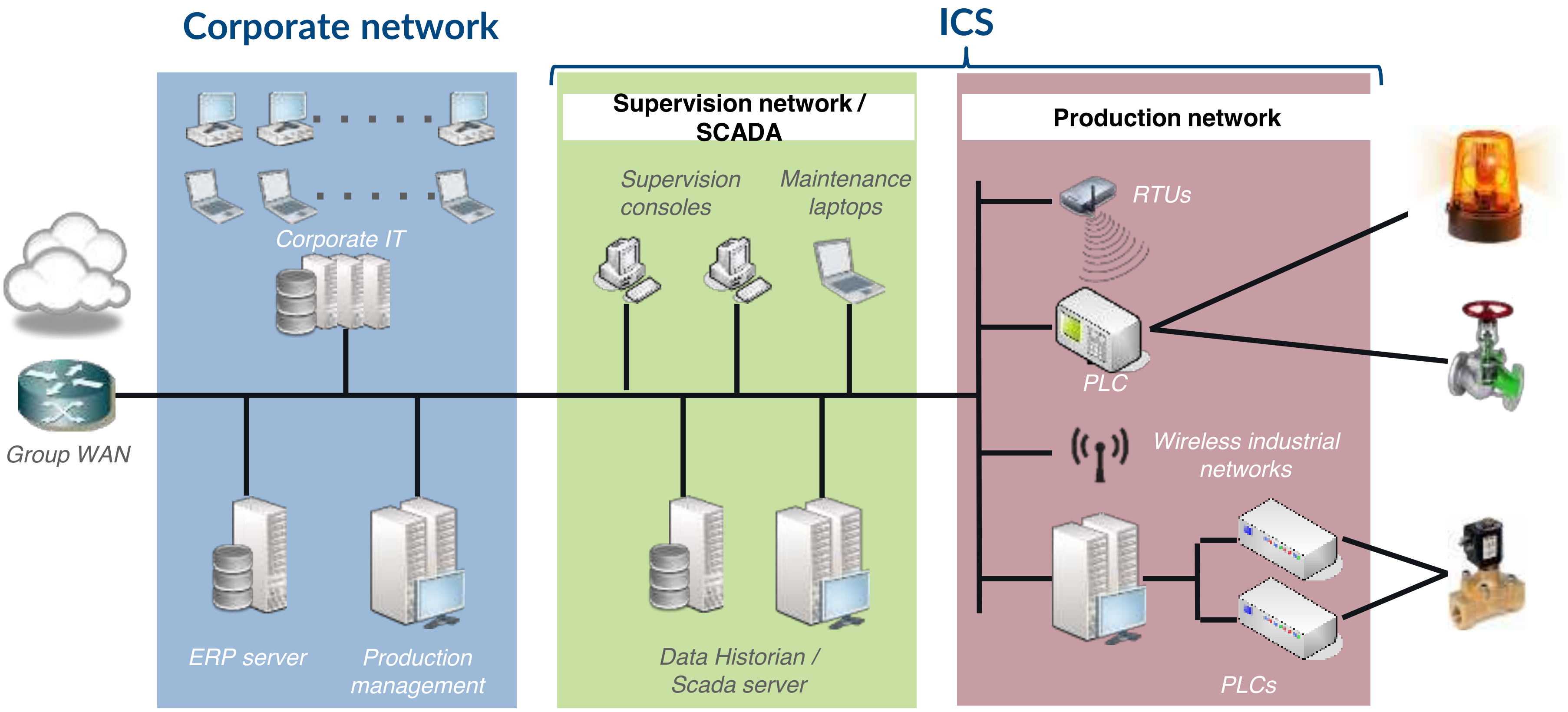
Where do we find Industrial Control Systems?

Manufacturing plants
Food

Power plants
Building automation systems (AC/HVAC/..)
Water treatment
Pharmaceutical manufacturing
Chemical plants

But also…swimming pools, building heating system, dams, etc.

What is an Industrial Control System (ICS)?



Corporate IS handle data

≠

ICS handle interfaces data with physical world (cyber-physical systems)

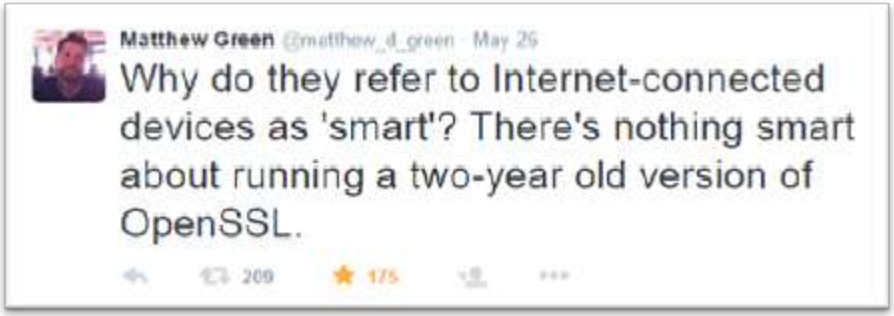
What about IoT/ smart stuff ?

Fit the definition of « cyber-physical » systems

http://weputachipinit.tumblr.com/

- Cardio-meter for your smartphone
- « Smart » electrical plugs

By the way, « smart » clearly isn't the right word



Matthew Green @matthew_d_green · May 26

Why do they refer to Internet-connected devices as 'smart'? There's nothing smart about running a two-year old version of OpenSSL.

BLACKSOCKS | Smarter Socks - Probably the smartest socks in the world

→ Not in the scope of this training

Evolution of ICS

- Started with electrical relays ➔ hard wired automation, no update possible
- Then moved to programmable electronics
- Then to IP-network enabled devices
- Now and future is more and more COTS

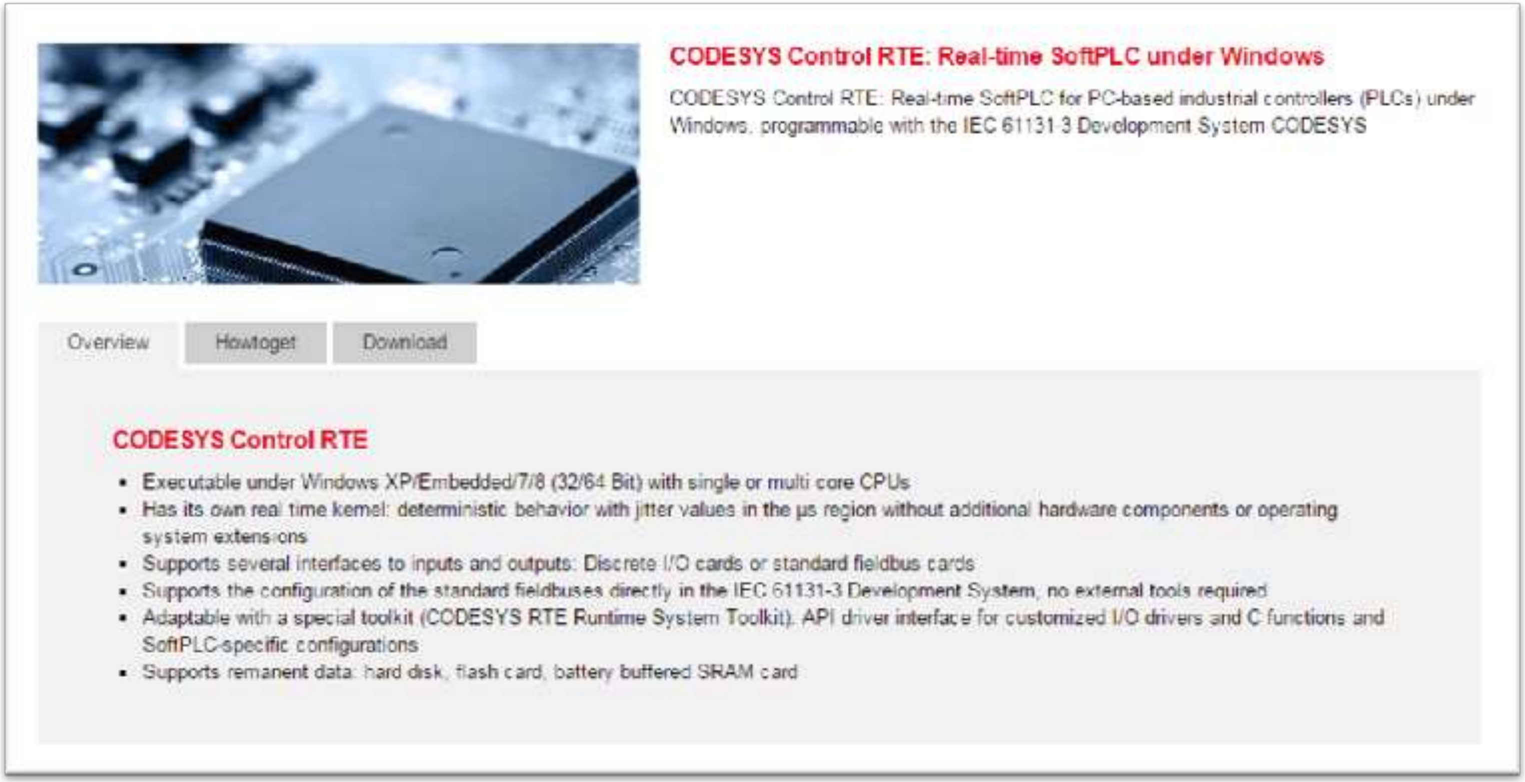
ICS evolution timeline

- From 1700s : Industrial revolution
- 1900s : use of relays to control remote systems
- 1950s : use of punch paper tape to control machines
- 1960s : use of distributed control to control a plant
- 1969 : First PLCs
- 1973 : Modbus invented
- 1986 : PLCs controled by PCs
- 1992 : TCP/IP for PLCs
- 2003 : web servers for PLCs
- ~2010s : Brace yourselves, AD is coming !
- Then what for the 10 next years ??

Future of ICS (well at least, current trends)

Now and future is more and more COTS

- Active Directory domains
- Soft-PLCs : CodeSYS under Windows computers

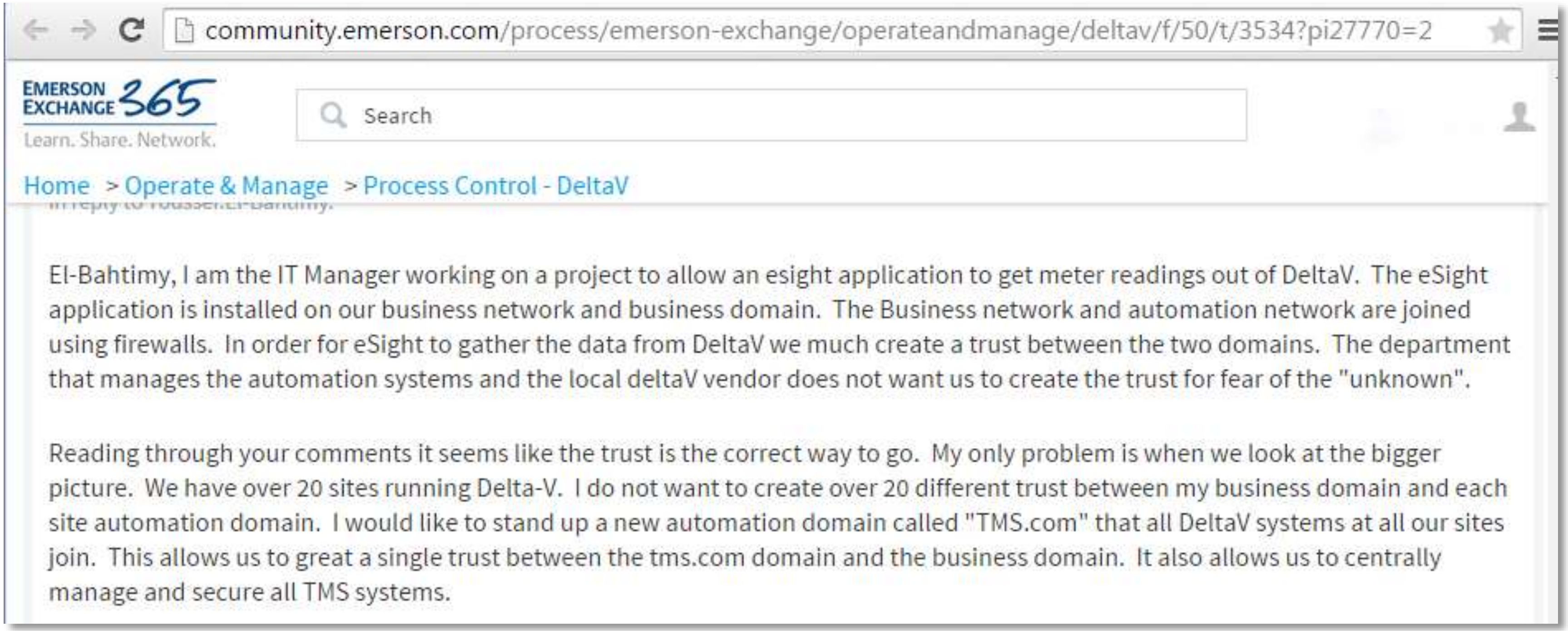


CODESYS Control RTE: Real-time SoftPLC under Windows

CODESYS Control RTE: Real-time SoftPLC for PC-based industrial controllers (PLCs) under Windows, programmable with the IEC 61131-3 Development System CODESYS

CODESYS Control RTE

- Executable under Windows XP/Embedded/7/8 (32/64 Bit) with single or multi core CPUs
- Has its own real time kernel: deterministic behavior with jitter values in the µs region without additional hardware components or operating system extensions
- Supports several interfaces to inputs and outputs: Discrete I/O cards or standard fieldbus cards
- Supports the configuration of the standard fieldbuses directly in the IEC 61131-3 Development System, no external tools required
- Adaptable with a special toolkit (CODESYS RTE Runtime System Toolkit). API driver interface for customized I/O drivers and C functions and SoftPLC-specific configurations
- Supports remanent data: hard disk, flash card, battery buffered SRAM card


community.emerson.com/process/emerson-exchange/operateandmanage/deltav/f/50/t/3534?pi27770=2
EMERSON EXCHANGE 365
Learn. Share. Network.
Search
Home > Operate & Manage > Process Control - DeltaV

El-Bahtimy, I am the IT Manager working on a project to allow an esight application to get meter readings out of DeltaV. The eSight application is installed on our business network and business domain. The Business network and automation network are joined using firewalls. In order for eSight to gather the data from DeltaV we much create a trust between the two domains. The department that manages the automation systems and the local deltaV vendor does not want us to create the trust for fear of the "unknown".

Reading through your comments it seems like the trust is the correct way to go. My only problem is when we look at the bigger picture. We have over 20 sites running Delta-V. I do not want to create over 20 different trust between my business domain and each site automation domain. I would like to stand up a new automation domain called "TMS.com" that all DeltaV systems at all our sites join. This allows us to great a single trust between the tms.com domain and the business domain. It also allows us to centrally manage and secure all TMS systems.

This is what happens when you star using too much IT in OT

A bit of vocabulary

ICS (*Industrial Control System*)

=

IACS (*Industrial Automation and Control Systems*)

~=

SCADA (*Supervisory Control And Data Acquisition*)

~=

DCS (Distributed Control System)

Nowadays, people tend to say “SCADA” for anything related to ICS

SCADA vs DCS

In theory …

- SCADA : event / data acquisition driven
- Used across several sites (even at the country scale)
- Can work even when offline
- Low response time

- DCS : process driven
- Limited to local process monitoring
- DCS works as standalone system
- Dedicated products by the vendors for specific industries / process

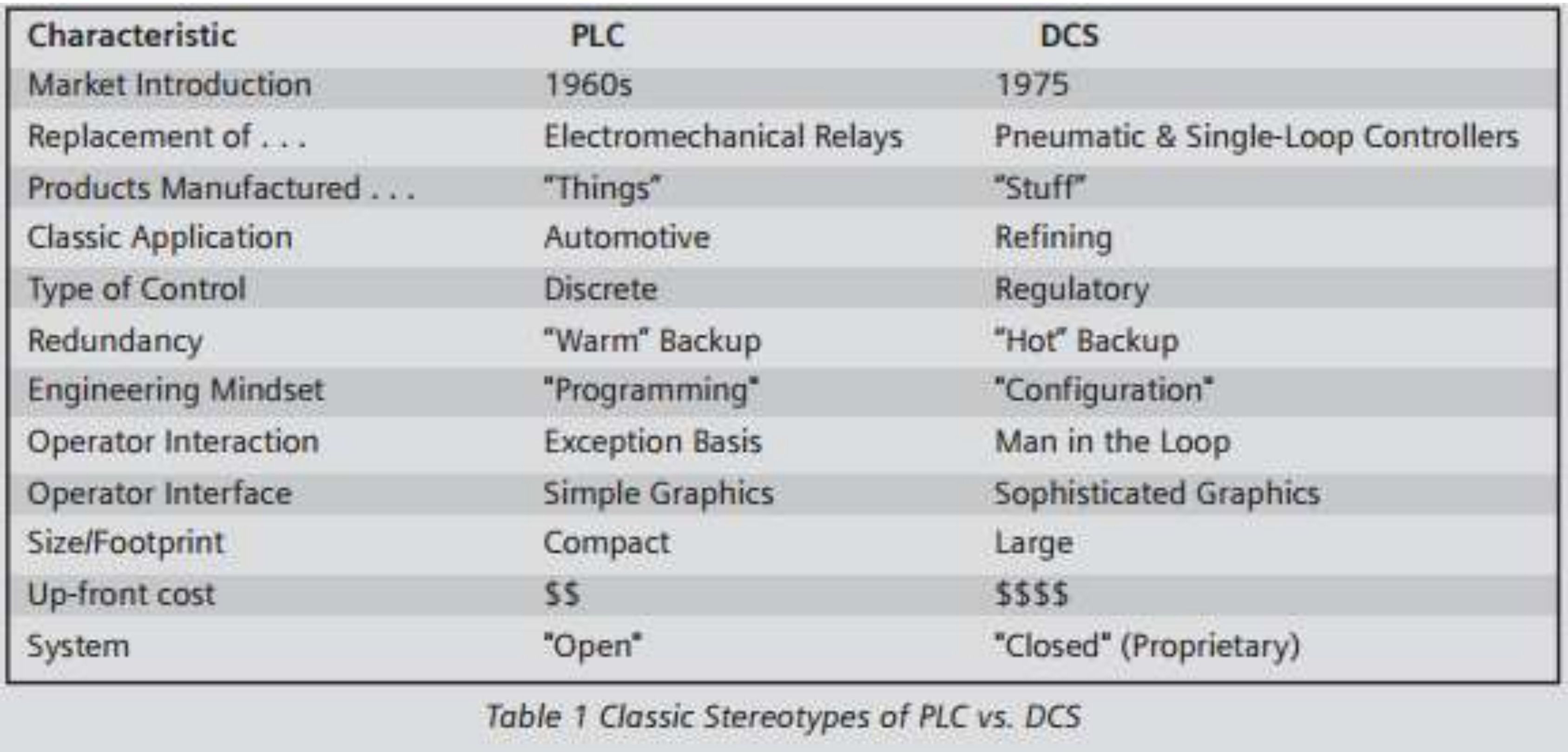
In reality …

In the real world,you’ll find some PLCs even when DCS is used

Today, SCADA manufacturer tend to have DCS functionnality, while DCS systems response time is lowering to be comparable to traditional SCADA response time

SCADA vs DCS

Siemens vision (1/3)



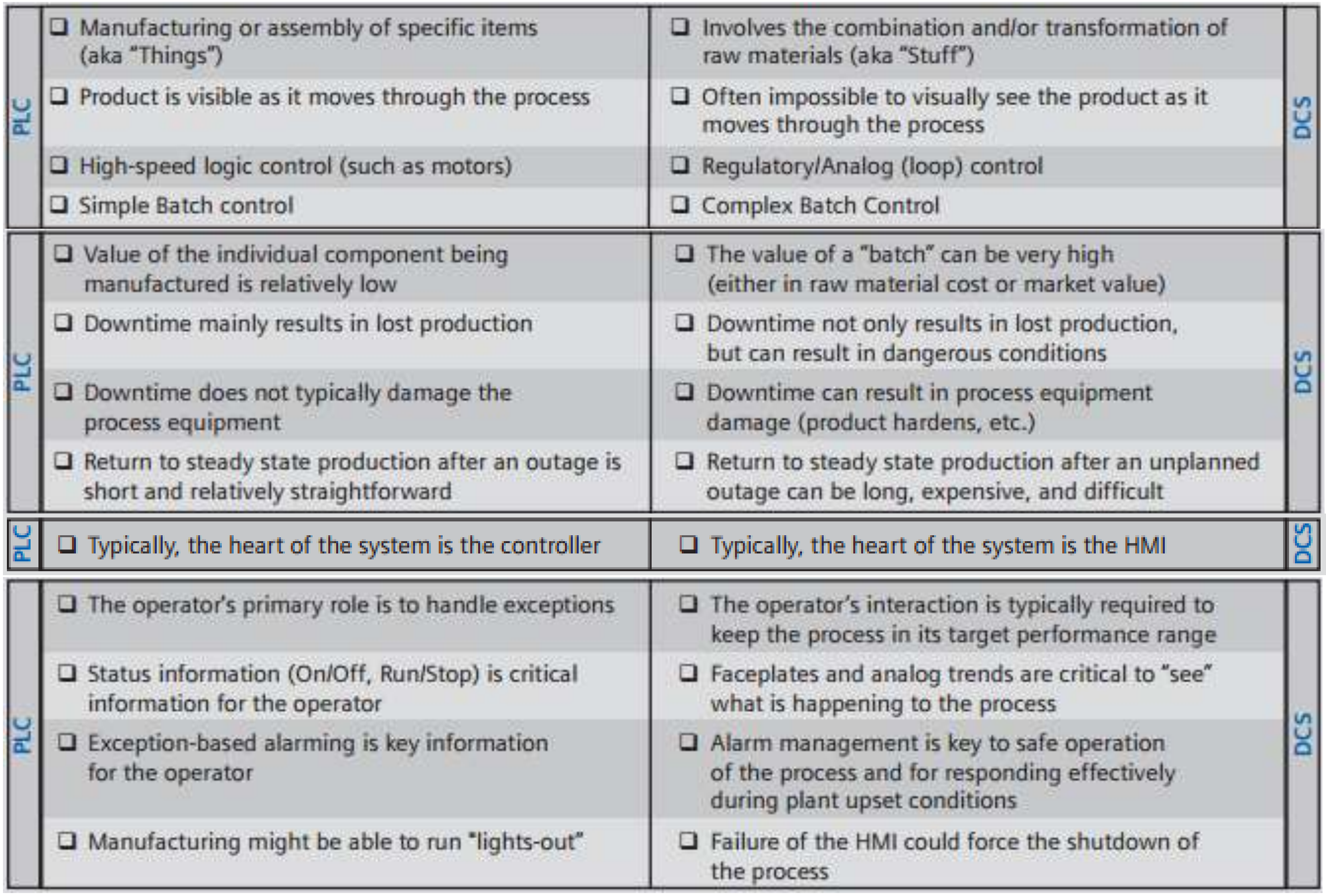
Characteristic	PLC	DCS
Market Introduction	1960s	1975
Replacement of . . .	Electromechanical Relays	Pneumatic & Single-Loop Controllers
Products Manufactured . . .	"Things"	"Stuff"
Classic Application	Automotive	Refining
Type of Control	Discrete	Regulatory
Redundancy	"Warm" Backup	"Hot" Backup
Engineering Mindset	"Programming"	"Configuration"
Operator Interaction	Exception Basis	Man in the Loop
Operator Interface	Simple Graphics	Sophisticated Graphics
Size/Footprint	Compact	Large
Up-front cost	$$	$$$$
System	"Open"	"Closed" (Proprietary)

Table 1 Classic Stereotypes of PLC vs. DCS

From « DCS or PLC? Seven Questions to Help You Select the Best Solution" http://w3.siemens.com/mcms/process-control-systems/SiteCollectionDocuments/efiles/pcs7/support/marktstudien/PLC_or_DCS.pdf

SCADA vs DCS

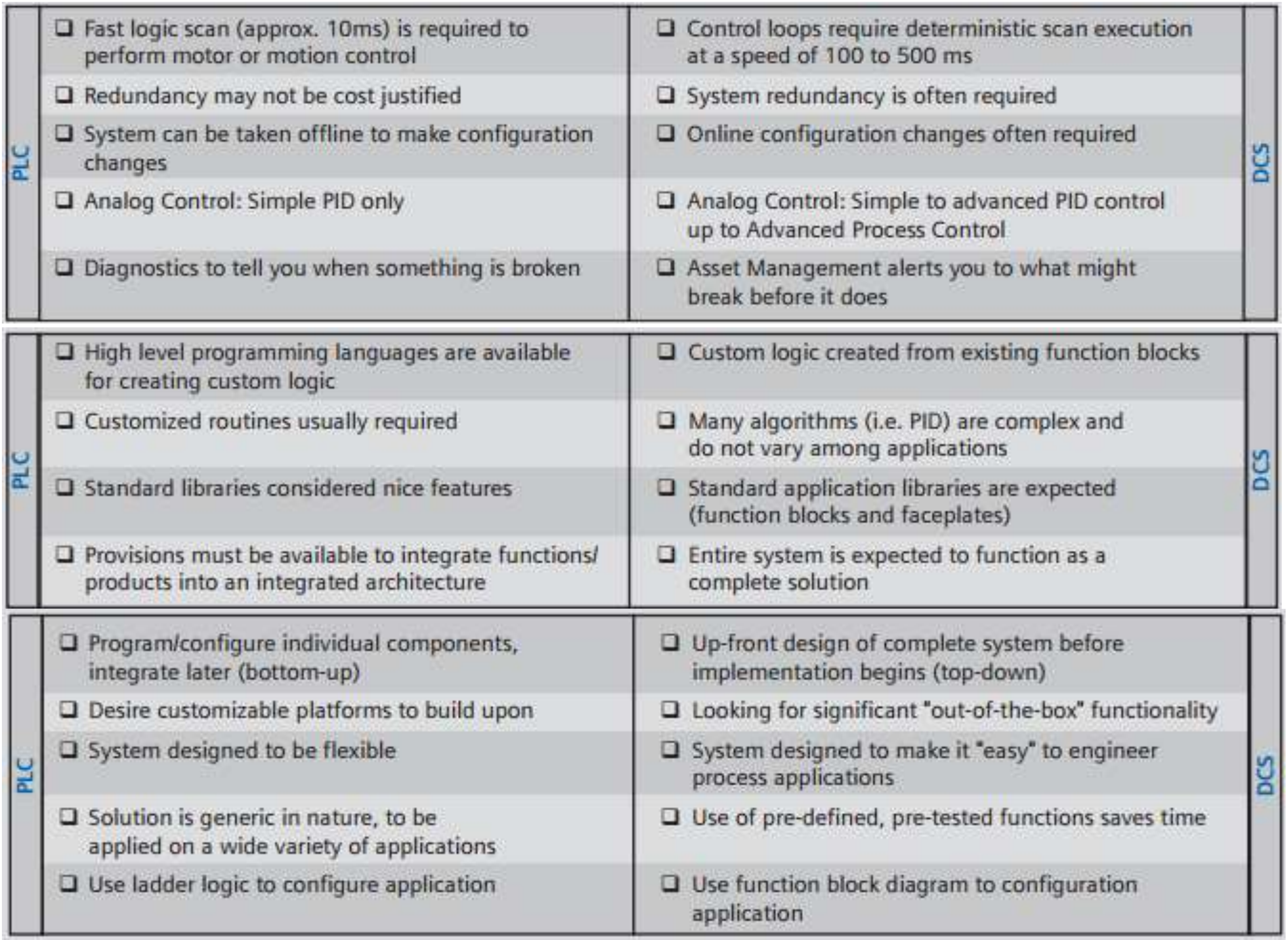
Siemens vision (2/3)



PLC	☐ Manufacturing or assembly of specific items (aka "Things")	☐ Involves the combination and/or transformation of raw materials (aka "Stuff")	DCS
	☐ Product is visible as it moves through the process	☐ Often impossible to visually see the product as it moves through the process	
	☐ High-speed logic control (such as motors)	☐ Regulatory/Analog (loop) control	
	☐ Simple Batch control	☐ Complex Batch Control	
PLC	☐ Value of the individual component being manufactured is relatively low	☐ The value of a "batch" can be very high (either in raw material cost or market value)	DCS
	☐ Downtime mainly results in lost production	☐ Downtime not only results in lost production, but can result in dangerous conditions	
	☐ Downtime does not typically damage the process equipment	☐ Downtime can result in process equipment damage (product hardens, etc.)	
	☐ Return to steady state production after an outage is short and relatively straightforward	☐ Return to steady state production after an unplanned outage can be long, expensive, and difficult	
PLC	☐ Typically, the heart of the system is the controller	☐ Typically, the heart of the system is the HMI	DCS
PLC	☐ The operator's primary role is to handle exceptions	☐ The operator's interaction is typically required to keep the process in its target performance range	DCS
	☐ Status information (On/Off, Run/Stop) is critical information for the operator	☐ Faceplates and analog trends are critical to "see" what is happening to the process	
	☐ Exception-based alarming is key information for the operator	☐ Alarm management is key to safe operation of the process and for responding effectively during plant upset conditions	
	☐ Manufacturing might be able to run "lights-out"	☐ Failure of the HMI could force the shutdown of the process	

SCADA vs DCS

Siemens vision (3/3)



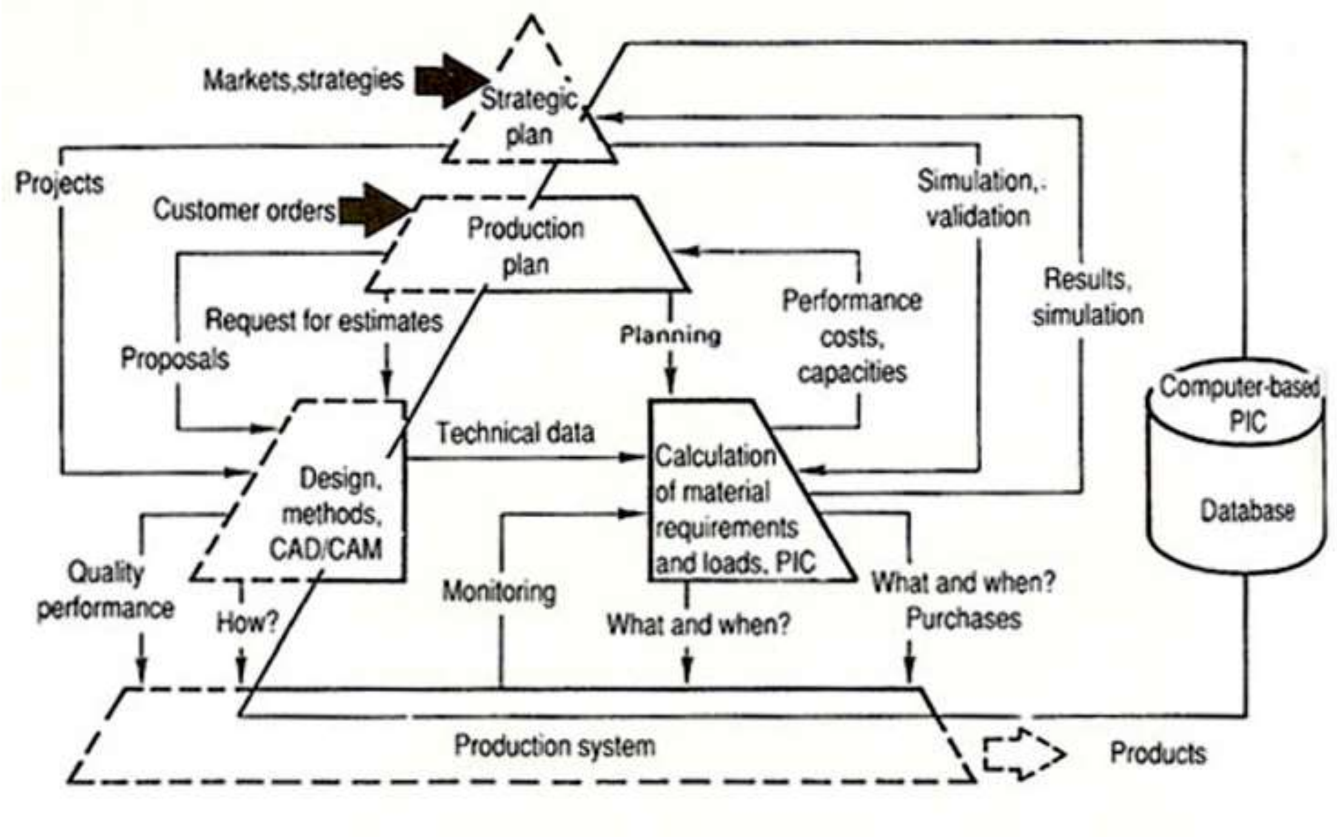
PLC	DCS
☐ Fast logic scan (approx. 10ms) is required to perform motor or motion control	☐ Control loops require deterministic scan execution at a speed of 100 to 500 ms
☐ Redundancy may not be cost justified	☐ System redundancy is often required
☐ System can be taken offline to make configuration changes	☐ Online configuration changes often required
☐ Analog Control: Simple PID only	☐ Analog Control: Simple to advanced PID control up to Advanced Process Control
☐ Diagnostics to tell you when something is broken	☐ Asset Management alerts you to what might break before it does
PLC	**DCS**
☐ High level programming languages are available for creating custom logic	☐ Custom logic created from existing function blocks
☐ Customized routines usually required	☐ Many algorithms (i.e. PID) are complex and do not vary among applications
☐ Standard libraries considered nice features	☐ Standard application libraries are expected (function blocks and faceplates)
☐ Provisions must be available to integrate functions/ products into an integrated architecture	☐ Entire system is expected to function as a complete solution
PLC	**DCS**
☐ Program/configure individual components, integrate later (bottom-up)	☐ Up-front design of complete system before implementation begins (top-down)
☐ Desire customizable platforms to build upon	☐ Looking for significant "out-of-the-box" functionality
☐ System designed to be flexible	☐ System designed to make it "easy" to engineer process applications
☐ Solution is generic in nature, to be applied on a wide variety of applications	☐ Use of pre-defined, pre-tested functions saves time
☐ Use ladder logic to configure application	☐ Use function block diagram to configuration application

ICS COMPONENTS

- **Sensors and actuators**: allow interaction with the physical world (pressure sensor, valves, motors, …)
- **Local HMI**: Human-Machine Interface, permits the supervision and control of a subprocess
- **PLC**: Programmable Logic Controller : manages the sensors and actuators
- **Supervision screen**: remote supervision of the industrial process
- **Data historian**: Records all the data from the production and Scada networks
- **RTU** : Remote Terminal Unit (standalone PLC)
- **IED** : Intelligent Electronic Device (smart sensor)

CIM pyramid

Computer Integrated Manufacturing



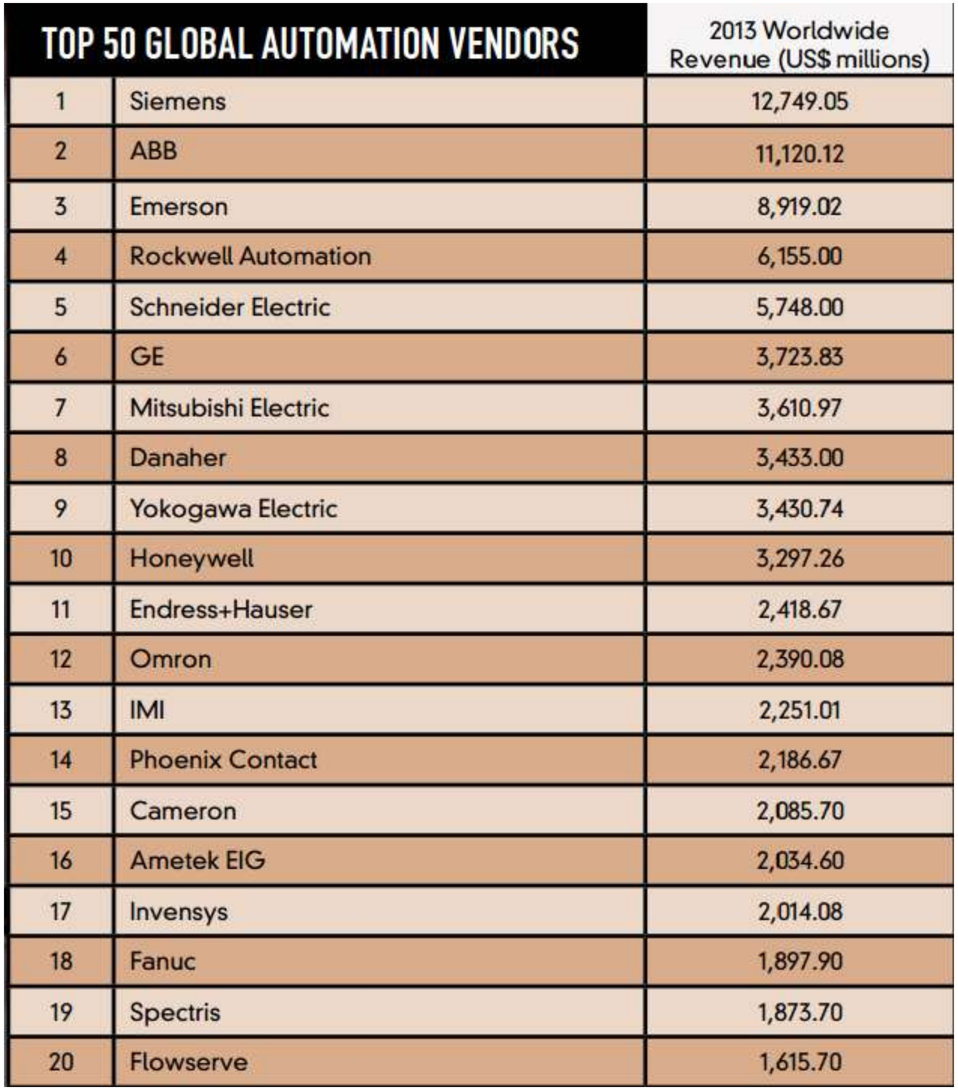
Level 3 : Orders and stock management, clients and accounting ➔ Handled by the ERP
Level 2 : Management of products : storage, moving, etc
Level 1 : Automation
Level 0 : Sensors and actuators

Industrial protocols

- At the beginning, specific protocols on specific physical layer (RS232, RS285, 4-20 current loop)
- Some protocols were adapted to TCP/IP, like Modbus, and other were developped to allow interoperability.

- Currently, the most used seem to be :
- HART / Wireless HART
- Profibus
- Modbus
- Profinet / S7
- DNP3
- For the field protocols (used by the PLCs, and some « intelligent » sensors/actuators)
- OPC for data echanged with the corporate network / Windows-based systems

ICS vendors



TOP 50 GLOBAL AUTOMATION VENDORS		2013 Worldwide Revenue (US$ millions)
1	Siemens	12,749.05
2	ABB	11,120.12
3	Emerson	8,919.02
4	Rockwell Automation	6,155.00
5	Schneider Electric	5,748.00
6	GE	3,723.83
7	Mitsubishi Electric	3,610.97
8	Danaher	3,433.00
9	Yokogawa Electric	3,430.74
10	Honeywell	3,297.26
11	Endress+Hauser	2,418.67
12	Omron	2,390.08
13	IMI	2,251.01
14	Phoenix Contact	2,186.67
15	Cameron	2,085.70
16	Ametek EIG	2,034.60
17	Invensys	2,014.08
18	Fanuc	1,897.90
19	Spectris	1,873.70
20	Flowserve	1,615.70

<u>Number of employees</u>

Siemens : 362 000
ABB : 150 000
Emerson : 115 000
Rockwell : 22 500
Schneider Electric : 152 000

Honeywell
OMRON
YOKOGAWA
SIEMENS
ABB
Rockwell Automation
Schneider Electric
PHOENIX CONTACT

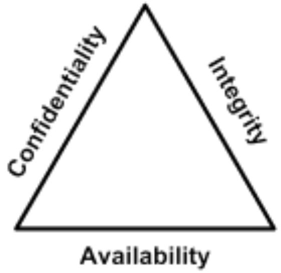
http://www.controlglobal.com/assets/00_images/2014/12/CG1412-Top50AutoVendors.pdf

IT vs OT

- The essential criteria for ICS security is availability, not confidentiality
- ICS were designed to be isolated, but today need to communicate with the outside world
- The use of COTS and standard protocols is relatively new
- Lifetime of components span over decades
- No security awareness

IT vs OT

IT



OT

Availability : My system is working correctly
Integrity : My system is working as expected

OT cares more about **safety**

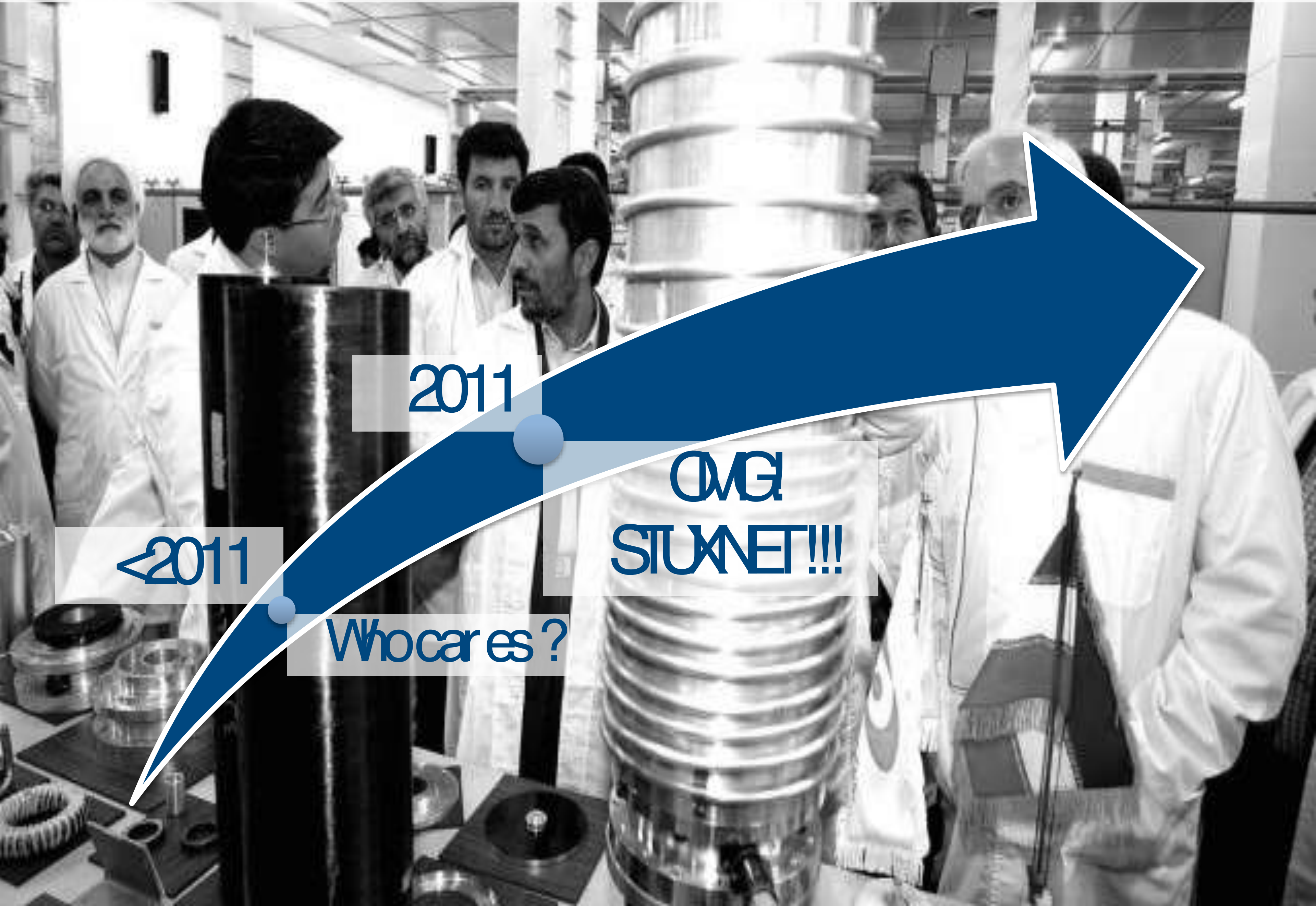
Applied regularly on standards systems	**Security patches**	Only recently provided by vendors. Applied once a year tops
Deployed on all Windows machines, centrally managed	**Antivirus**	Sowly starting to show up. Some vendors used to / stil forbid AV usage (lack of support if AV is installed) Not managed
Centralized, dedicated teams, standard operations and procedures	**System Administration**	Lack of local skills, heterogeneous environments, lots of different tools to use, vendor support is mandatory
Nominative accounts	**IAM**	Generic, shared accounts, no password policy
Service interuptions are OK, especially outside business hours	**Availability**	Real-time operations, downtime is unacceptable or very costly
Standard, TCP/IP protocols that include authentication and encryption	**Protocols**	Lot of vendor-specific protocol no security built in
No people endangered	**Impact**	Possible impact of people, environnent, industrial gear

SCADA SECURITY AWARENESS TIMELINE (SIMPLIFIED)

<2011

Who cares?

SCADA SECURITY AWARENESS TIMELINE (SIMPLIFIED)



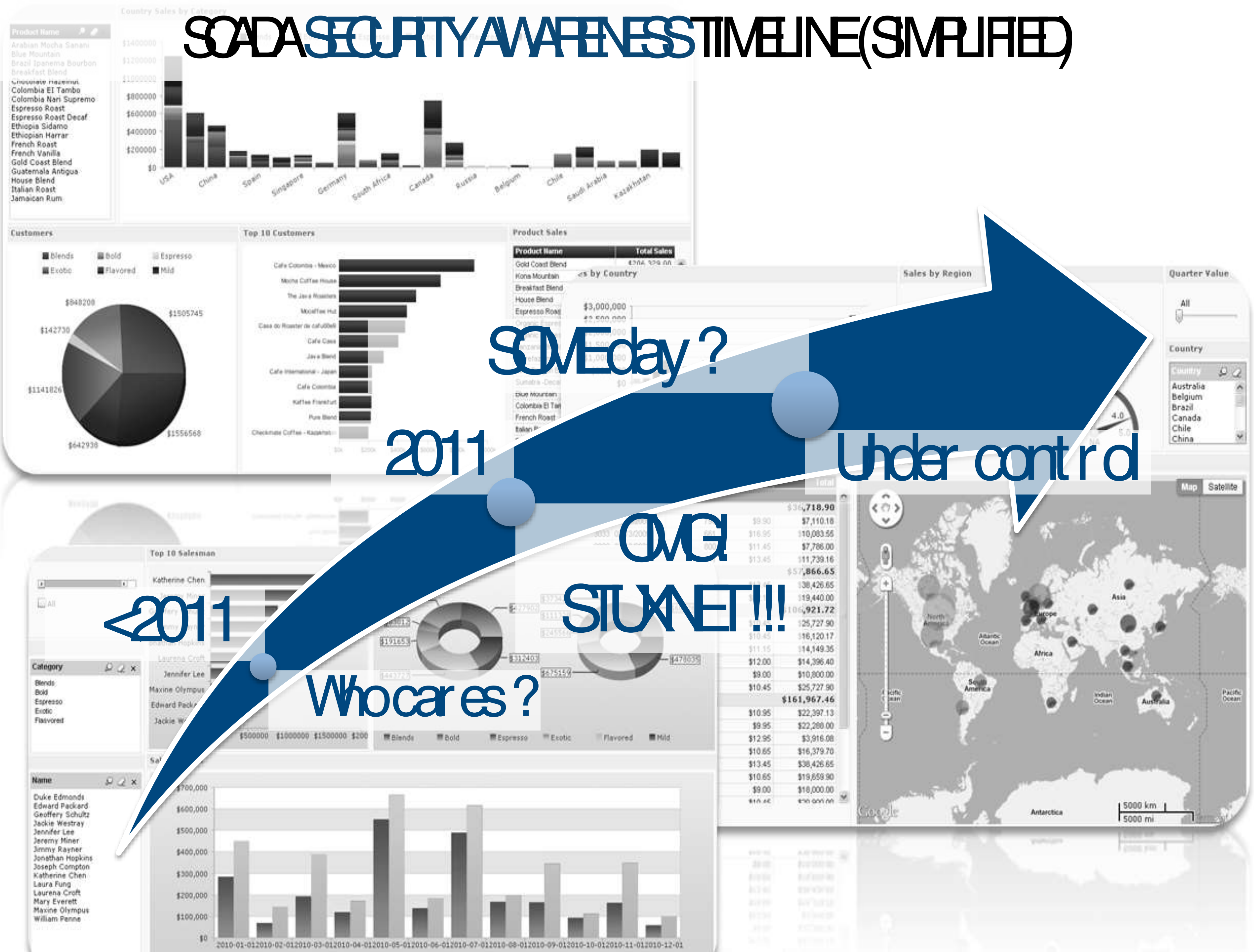
<2011

Who cares?

2011

OMG!
STUXNET!!!

SCADA SECURITY AWARENESS TIMELINE (SIMPLIFIED)



<2011

Who cares?

2011

OMG! STUXNET!!!

SOMEday?

Under control

ICS security awareness is growing

At the government level → Regulations

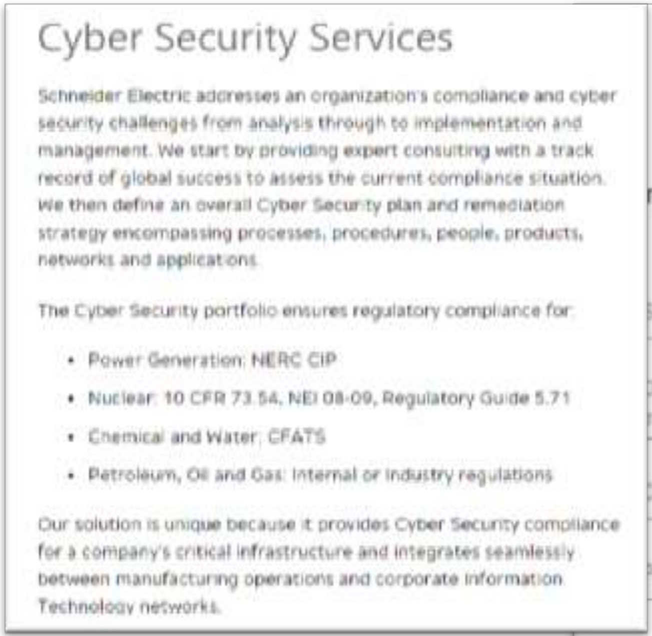
In industrial companies → policies

For the general audience → fear

Vendors Cyber-Security offer

Most ICS vendors have know understood the client’s worries about security and offer different kinds of dedicated products and/or services

That DOES NOT mean that vendors’ staff has the required knowledge and training about ICS security



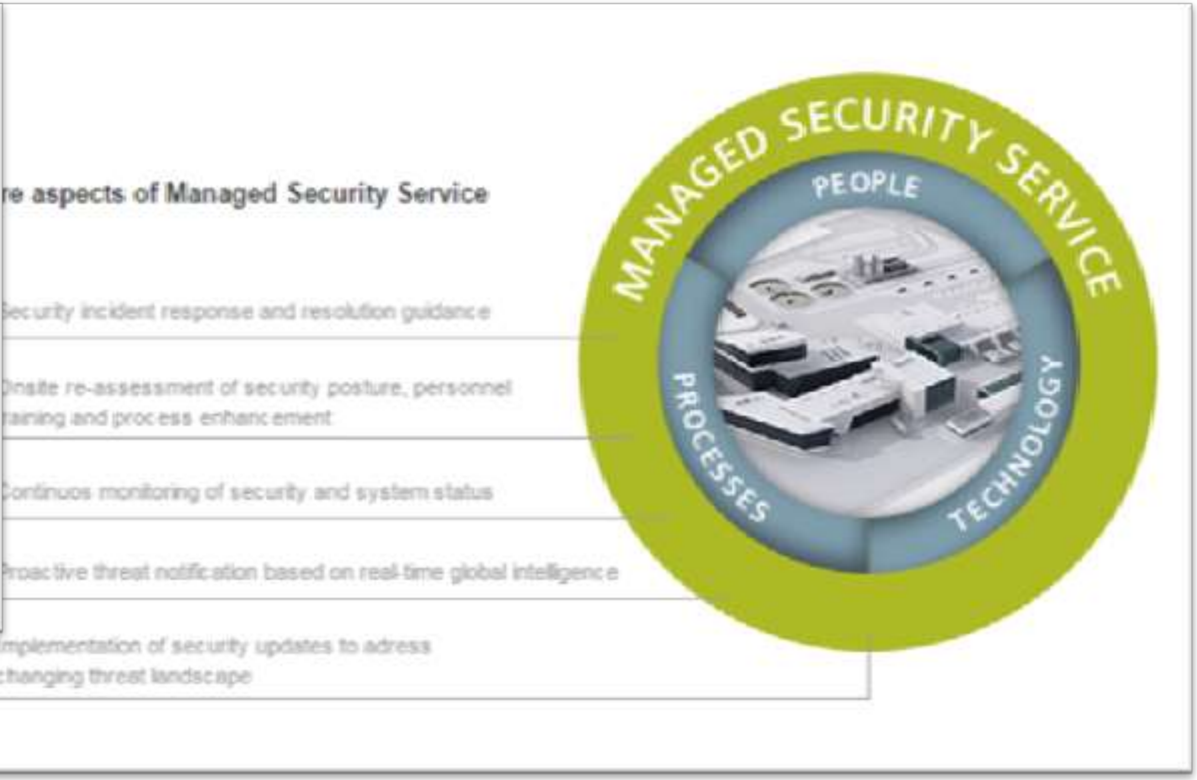
Cyber Security Services

Schneider Electric addresses an organization's compliance and cyber security challenges from analysis through to implementation and management. We start by providing expert consulting with a track record of global success to assess the current compliance situation. We then define an overall Cyber Security plan and remediation strategy encompassing processes, procedures, people, products, networks and applications.

The Cyber Security portfolio ensures regulatory compliance for:

- Power Generation: NERC CIP
- Nuclear: 10 CFR 73.54, NEI 08-09, Regulatory Guide 5.71
- Chemical and Water: CFATS
- Petroleum, Oil and Gas: Internal or industry regulations

Our solution is unique because it provides Cyber Security compliance for a company's critical infrastructure and integrates seamlessly between manufacturing operations and corporate information Technology networks.



re aspects of Managed Security Service

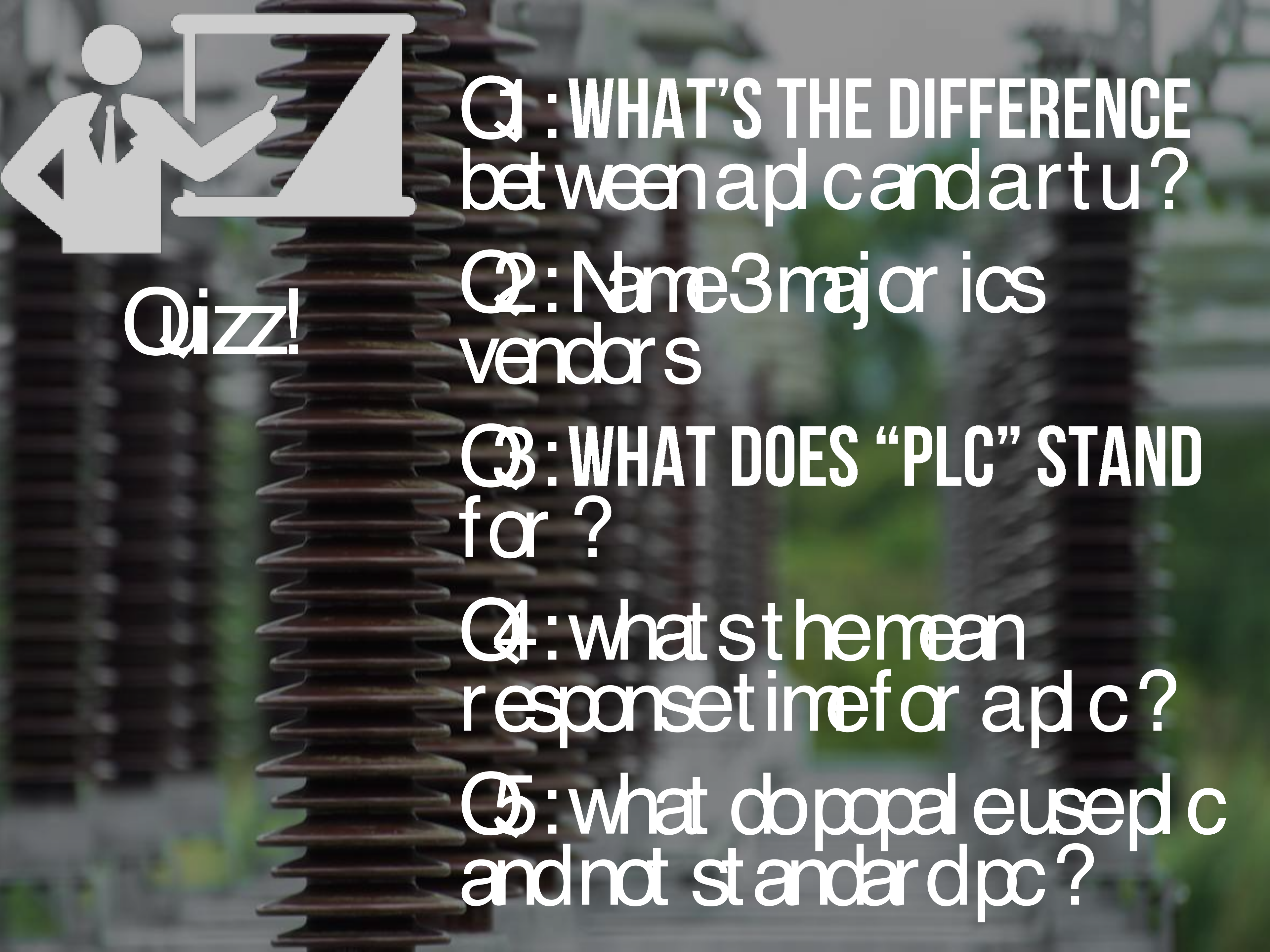
Security incident response and resolution guidance

Onsite re-assessment of security posture, personnel training and process enhancement

Continuos monitoring of security and system status

Proactive threat notification based on real-time global intelligence

Implementation of security updates to adress changing threat landscape



Quizz!

Q1: WHAT'S THE DIFFERENCE between a plc and a rtu?

Q2: Name 3 major ics vendors

Q3: WHAT DOES "PLC" STAND for?

Q4: whats the mean response time for a plc?

Q5: what do popale use plc and not standard pc?

Module 2: WHAT IS WRONG WITH CURRENT ICS security?

Organization & awareness

Network segmentation

Vulnerability management

security In protocols

third paRty management

security supervision

Organization & awareness

- ICS security does not have the same level of maturity as IT in general
- You will often face situation were nobody is in charge of ICS security
- Sometimes, there is even nobody in charge of IT (computers, switches)
- Someone is in charge of ICS safety, but not security
- ICS are often still out of the CISO perimeter

Awareness : misconceptions

- SAFETY != SECURITY
- Our ICS are not connected
- Proprietary protocols are safer
- I have an Antivirus, I am safe
- $BIG_VENDOR products are certainly secure
- The safety systems will prevent anything bad from happening

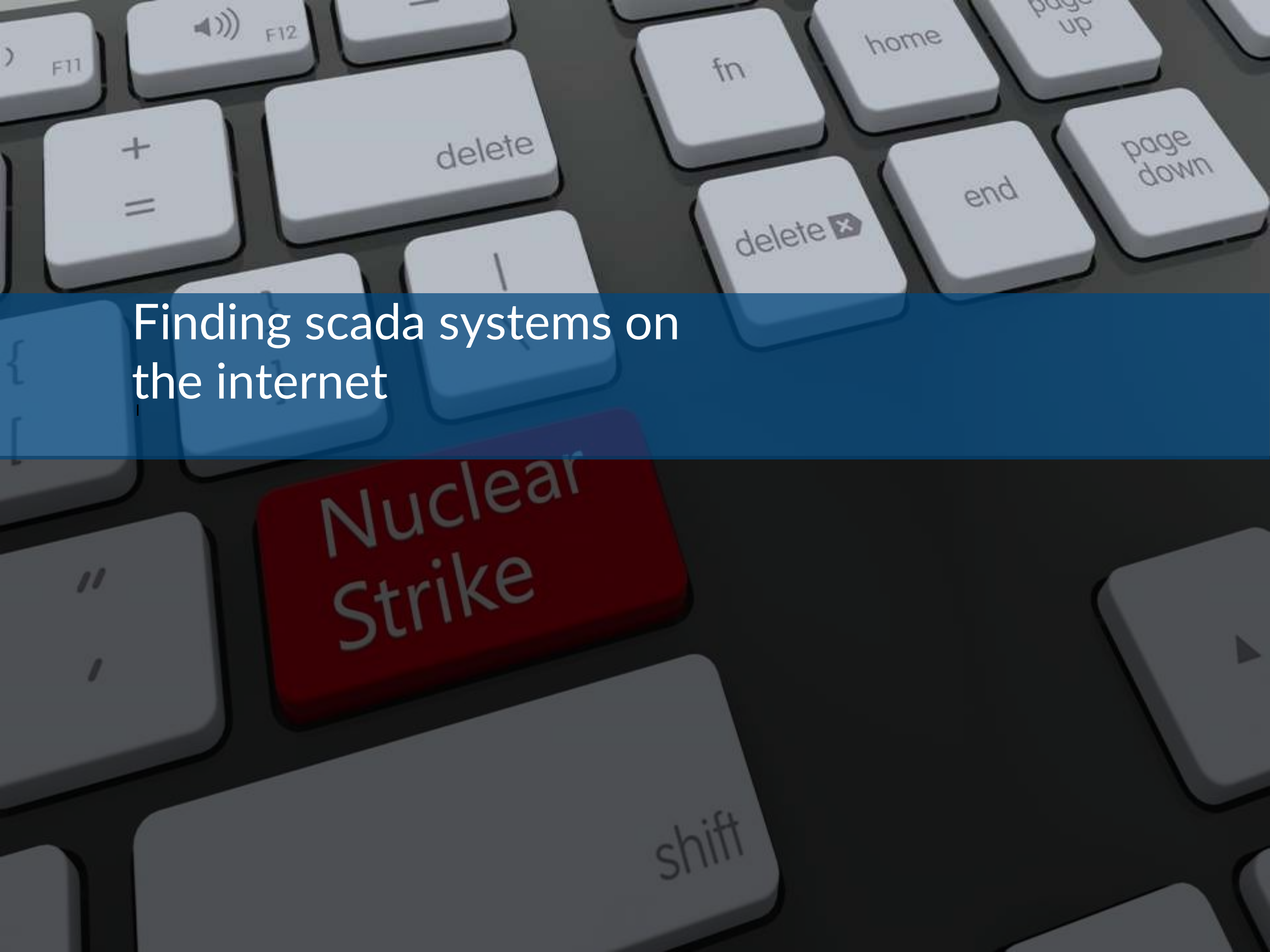
Network segmentation

- Mostly a fail
- Nothing is air-gapped, ever (well, almost)
- « *It is segmented because my laptop can't connect to both networks at the same time* »
- Often, poorly configured ACLs on routers
- Wide access to the ICS from the
- Port 80 allowed to everyone
- Spoiler alert : port 80 allows to do plenty of nasty things
- How good is your network segmentation if you directly copy files from the office network to the ICS network ?

Reconnaissance : exposure

- Exposure on the Internet : Shodan
- What's cool about Shodan is that it doesn't require any validation from the client (mostly free, but features like export are paid options)
- How do it work : Shodan scans the whole Internet at regular times and gives you access to the results
- YOU do not send a single packet to the client's infrastructures
- Can give you information about the type of technologies used
- Most of the time, client is not aware that systems are exposed to the Internet...

Finding scada systems on the internet



EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

- Shodan is a search engine dedicated to find devices exposed to the Internet
- It regularly scans the whole Internet IPV4 range (~4,3 billions IPs)
- Results are partially free (you have to pay to export the results)

What can you find?

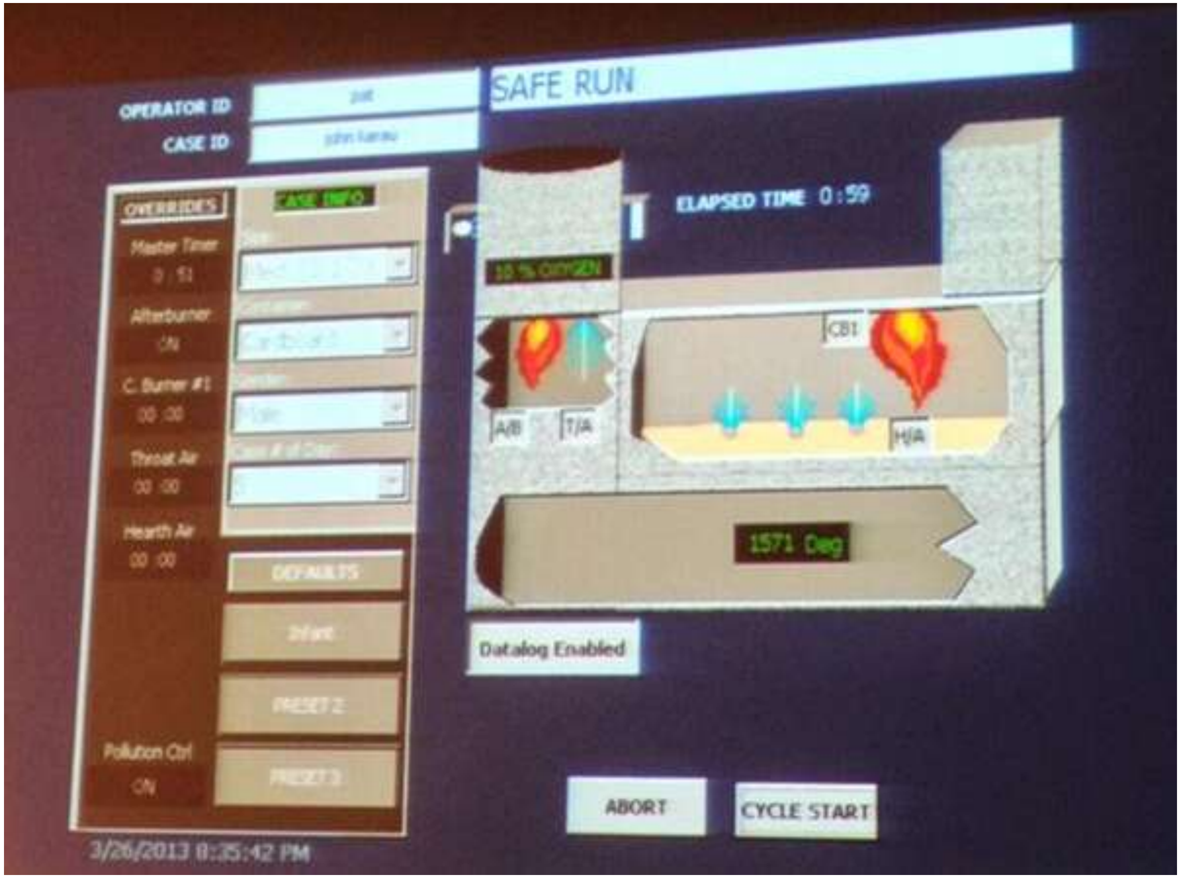
- All kinds of connected devices
  - PLCs
  - Webcams
  - Smart-things (fridge, TV, …)
- Things you can't even imagine…
- Example ICS report : https://www.shodan.io/report/l7VjfVKc

ALTERNATIVES?

- Scan the Internet yourself (Zmap, Massscan)
- Other online services/surveys

FUNNy things you can find on teh interwebs

It’s not just webcams.



SAFE RUN

ELAPSED TIME 0:59

Master Timer 0:51

Afterburner ON

C. Burner #1 00:00

Throat Air 00:00

Hearth Air 00:00

Pollution Ctrl ON

10 % OXYGEN

1571 Deg

Datalog Enabled

3/26/2013 8:35:42 PM

This is a crematorium. On the internet.

Vulnerability management : a hard topic

- ICS help industries make money. Most of the time, by producing something. The more « uptime » the ICS has, the more money you make. That is why a lot of ICS run 24/7
- Each production stop costs money, hence the difficulty to regularly apply security patches.
- Moreover, it is not unusual for ICS vendors to advise owner not to install AV software, in order to prevent false positives. Fortunately, this situation changes.

Vulnerability management

Also, not all plants have the luxury of having acceptance/test platform.

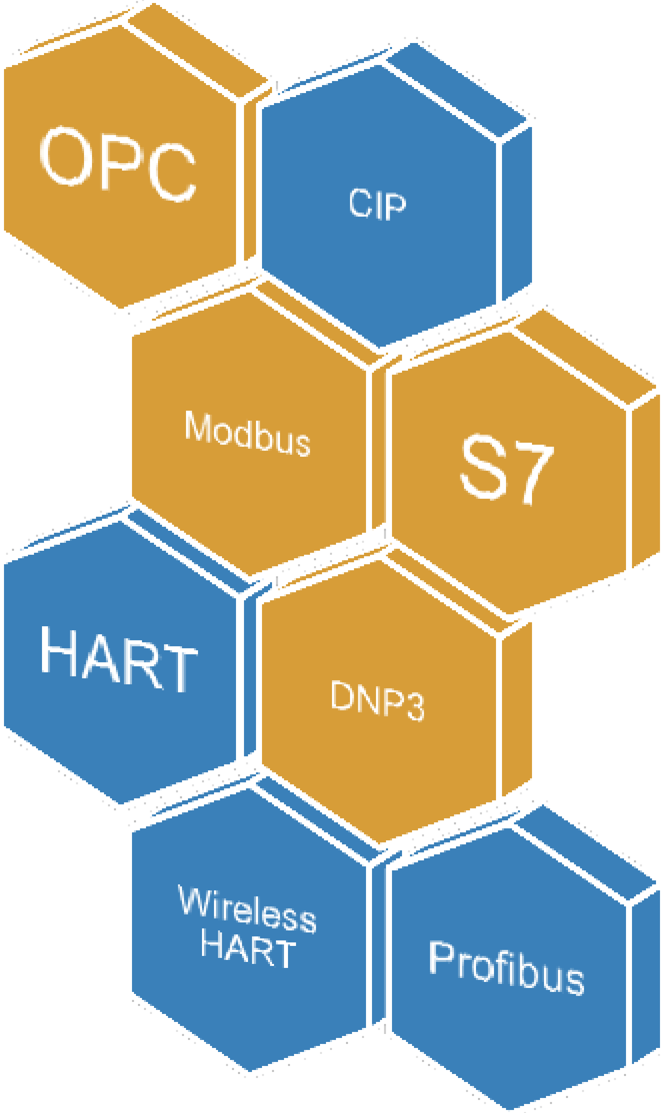
As ICS hardware is much more costly than VMs, sometimes security patches must be applied to production directly.

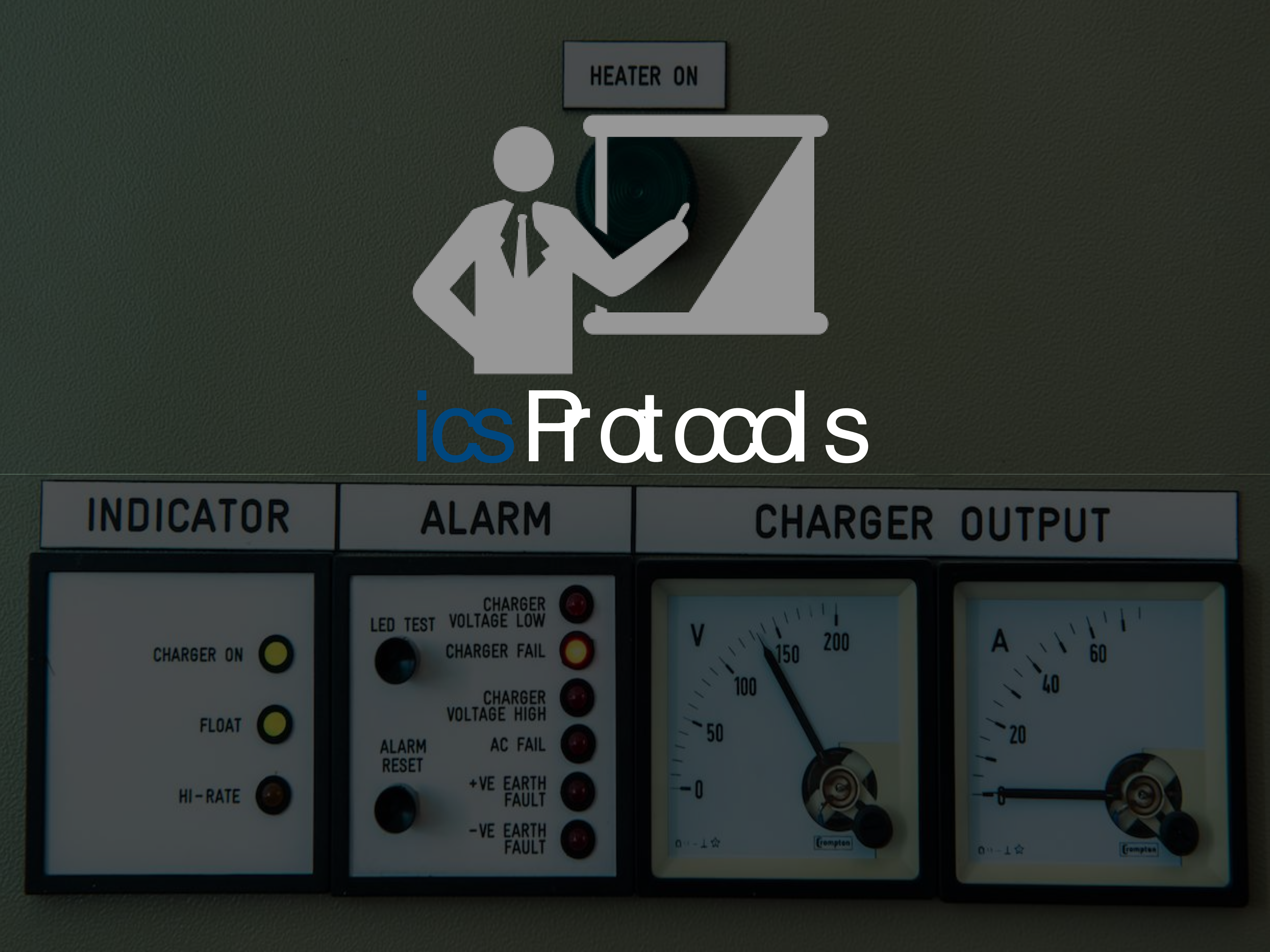
Security in protocols

ICS devices often use proprietary protocols, and there are also several standards.

That is why on a given plant/factory ICS, you are likely to find several protocols in use.

We will cover the most used ones.





icsProtocols

Modbus protocol

●○○○

- Serial communication protocol invented in 1979 by Schneider Electric
- Developed for industrial application
- Royalty-free
- Now one of the standards for industrial communications

How it works:

- Master / Slave protocol
- Master must regularly poll the slaves to get information
- Modbus addresses are 8 bits long, so only 247 slaves per master
- There is no object description: a request returns a value, without any context or unit

Security anyone?

- Clear-text
- No authentication

Modbus protocol

●●○○

- Modbus was originally made for serial communications
- However it is now often used over TCP

MODBUS/TCP FRAME FORMAT

Name	Length	Function
Transaction identifier	2	For synchronization between server & client
Protocol identifier	2	Zero for Modbus/TCP
Length field	2	Number of remaining bytes in this frame
Unit identifier	1	Slave address (255 if not used)
Function code	1	Function codes as in other variants
Data bytes or command	n	Data as response or commands

Modbus protocol

●●●○

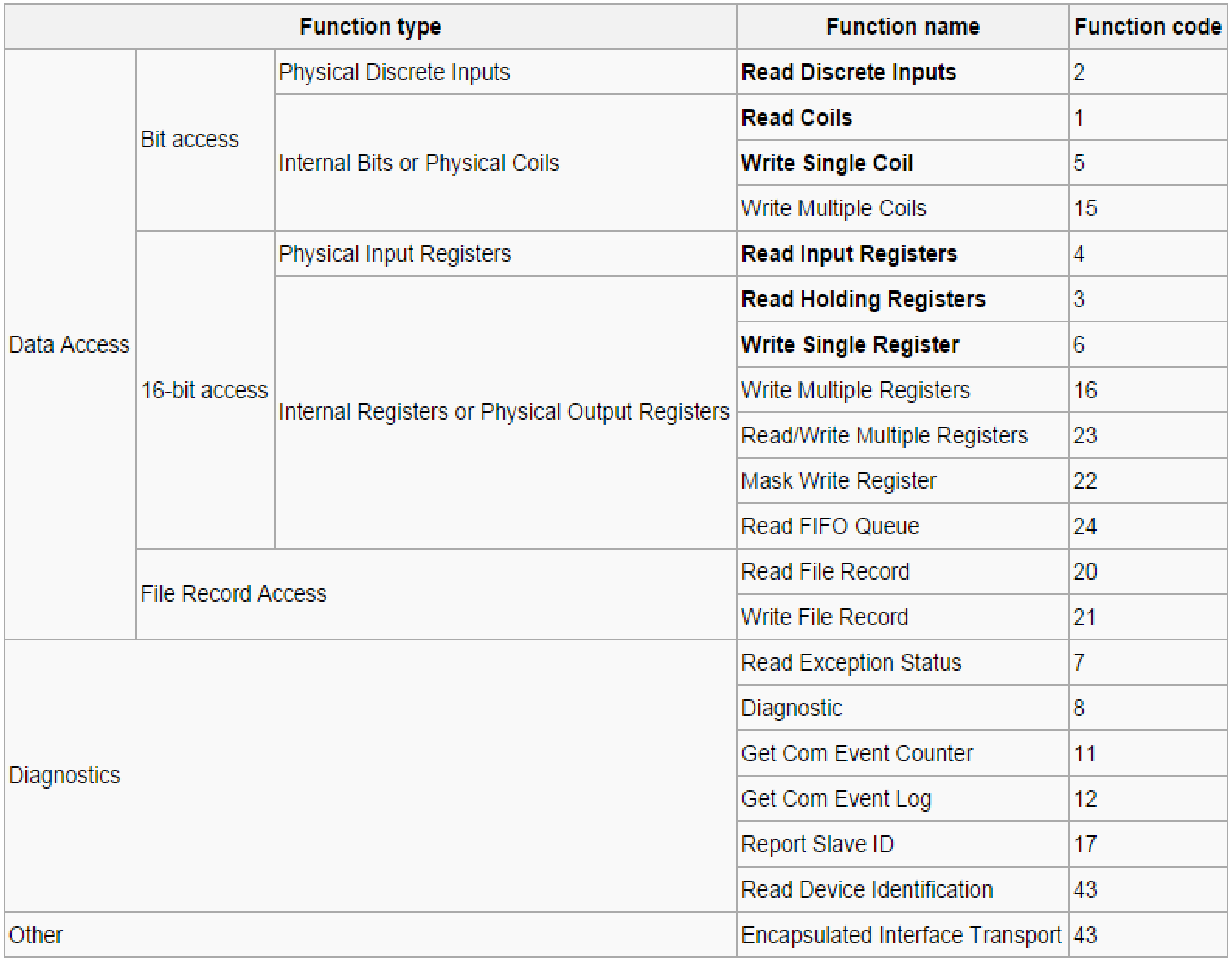
- The most common Modbus functions allow to read and write data from/to a PLC
- Other functions, such as file read and diagnostics functions also exist
- Undocumented Modbus function codes can also be used to perform specific actions

COMMONLY USED MODBUS function codes

Function name	Function code
Read coils	1
Write single coil	5
Read holding registers	3
Write single register	6
Write multiple registers	16
Read/Write multiple registers	23

Modbus protocol

ALL documented MODBUS function codes (from wikipedia)



Function type			Function name	Function code
Data Access	Bit access	Physical Discrete Inputs	**Read Discrete Inputs**	2
		Internal Bits or Physical Coils	**Read Coils**	1
			Write Single Coil	5
			Write Multiple Coils	15
	16-bit access	Physical Input Registers	**Read Input Registers**	4
		Internal Registers or Physical Output Registers	**Read Holding Registers**	3
			Write Single Register	6
			Write Multiple Registers	16
			Read/Write Multiple Registers	23
			Mask Write Register	22
			Read FIFO Queue	24
	File Record Access		Read File Record	20
			Write File Record	21
Diagnostics			Read Exception Status	7
			Diagnostic	8
			Get Com Event Counter	11
			Get Com Event Log	12
			Report Slave ID	17
			Read Device Identification	43
Other			Encapsulated Interface Transport	43

S7
protocol

- Proprietary protocol by Siemens
- TCP port 102
- Based on COTP (Connection-Oriented Transport Protocol, RFC905)
- A Wireshark dissector is available in the dev branch
- No security

- New version of the protocol available starting with version 4 and up of the PLC firmware : provides mutual authentication and communication encryption
- Security features analyzed by Quarkslab, see the talk from SSTIC https://www.sstic.org/2015/presentation/analyse_de_scurite_de_technologies_propritaires_scada/

DNP3 protocol

- Standard protocol, developped by GE in the 90’s
- Slave/Slave : Information can be share at the initiative of any device
- Layer 2 protocol (just top of physical layer), ported to TCP/IP
- Integrity is verified using CRC
- Data reporting communication : only send the data that has changed (simplified), or at the initiative of the PLC/RTU
- Used for smartgrids in the US
- Secure DNP3 introduced in 2007
    - Works on serial and TCP versions
    - Challenge/response to exchange a session key (using PSK)
    - Can be done at startup, every XX minutes, or only for sensitive actions (write requests for example)
    - There is also an aggressive mode, which can be exploited to perform replay attacks
    - Possible to use secure DNP3 over TLS

Profibus
protocol

●○○○

- Standard protocol
- Used for communication with field devices (sensors/actuators)
- Uses 4-20mA current loop

OPC
protocol

- Standard protocol
- Used to exchange data between ICS and Windows devices
- Works on TCP/IP
- Several variants:
    - *OPC-DA : Data access, used to gather data from the process control*
    - *OPC A&E : Alarm & Events*
    - *OPC HDA : Historical Data Access*
    - *OPC DX : Data Exchange, allow to exchange data between OPC servers*
    - *OPC Security*
    - *OPC XML-DA*
    - *OPC UA : Unified Architecture, aimed at replacing the others while using a more modern Service Oriented Architecture.*

- Provides authentication and encryption, probably the future of ICS protocols

#foreverdays

#foreverdays is a term coined by @reverseics
Very important concept when talking about ICS
The highest vulnerabilities are not patched.

So it is really worth considering the effort of patch management of ICS equipement when you know

ICS-CERT

INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT listed over **250 attacks** on ICS in 2013

- **59% of attacks** targeted the energy sector
- **79** attacks successfully compromised the target
- **57** attacks did not succeed in compromising the target
- **120** attacks were not identified/investigated

Quizz!

Q1: what are the security features of the modbus protocol?

Q2: which port is used for modbus? For s7?

Q3: what is opc mostly used for?

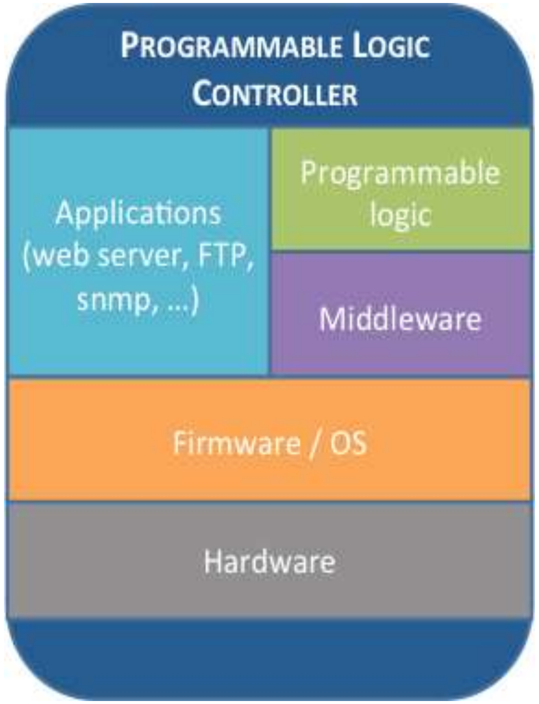
Q4: why are some plcs exposed to the internet?

Programming PLCs

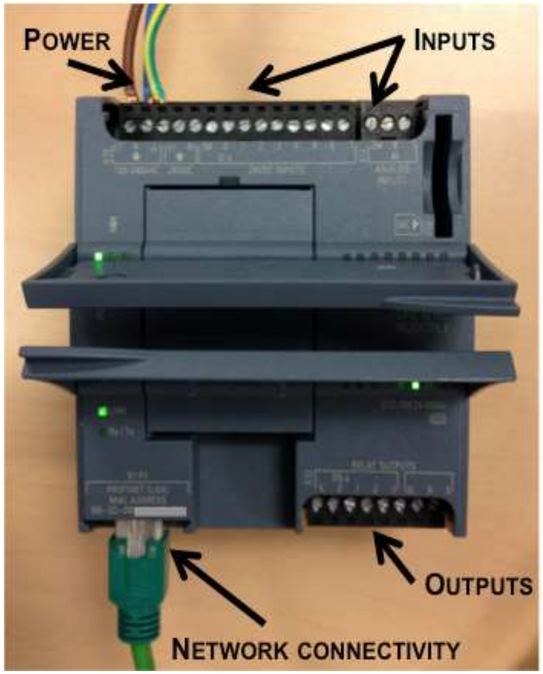
What is
A PLC?

- Real-time digital computer used for automation
- Replaces electrical relays
- Lots of analogue or digital inputs & outputs
- Rugged devices (immune to vibration, electrical noise, temperature, dust, …)

What's inside ?


PROGRAMMABLE LOGIC CONTROLLER
Applications (web server, FTP, snmp, …)
Programmable logic
Middleware
Firmware / OS
Hardware

Siemens S7-1200

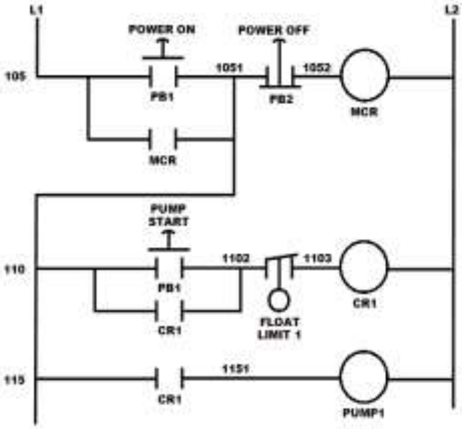


A few pics of PLCs

PLC programming

- "*Ladder Logic*" was the first programming language for PLC, as it mimics the real-life circuits
- IEC 61131-3 defines 5 programming languages for PLCs
  - **LD**: Ladder Diagram
  - **FBD**: Function Block Diagram
  - **ST**: Structured Text
  - **IL**: Instruction List
  - **SFC**: Sequential Function Chart

Ladder diagram example



Structured text example

```
(* simple state machine *)
TxtState :=
STATES[StateMachine];

CASE StateMachine OF
   1: ClosingValve();
ELSE
    ;; BadCase();
END_CASE;
```

Instruction list example

```
LD      Speed
        GT      1000
        JMPCN   VOLTS_OK
        LD      Volts
VOLTS_OK LD     1
        ST      %Q75
```

Programming with SoMachine

- SoMachine is the software provided by Schneider Electric to program the entry-level PLCs.
- PLCs used in big plants are usually programmed using Unity Pro, for which there is no free demo version.
- Fortunately, the way this software work is very much the same

Programming with SoMachine

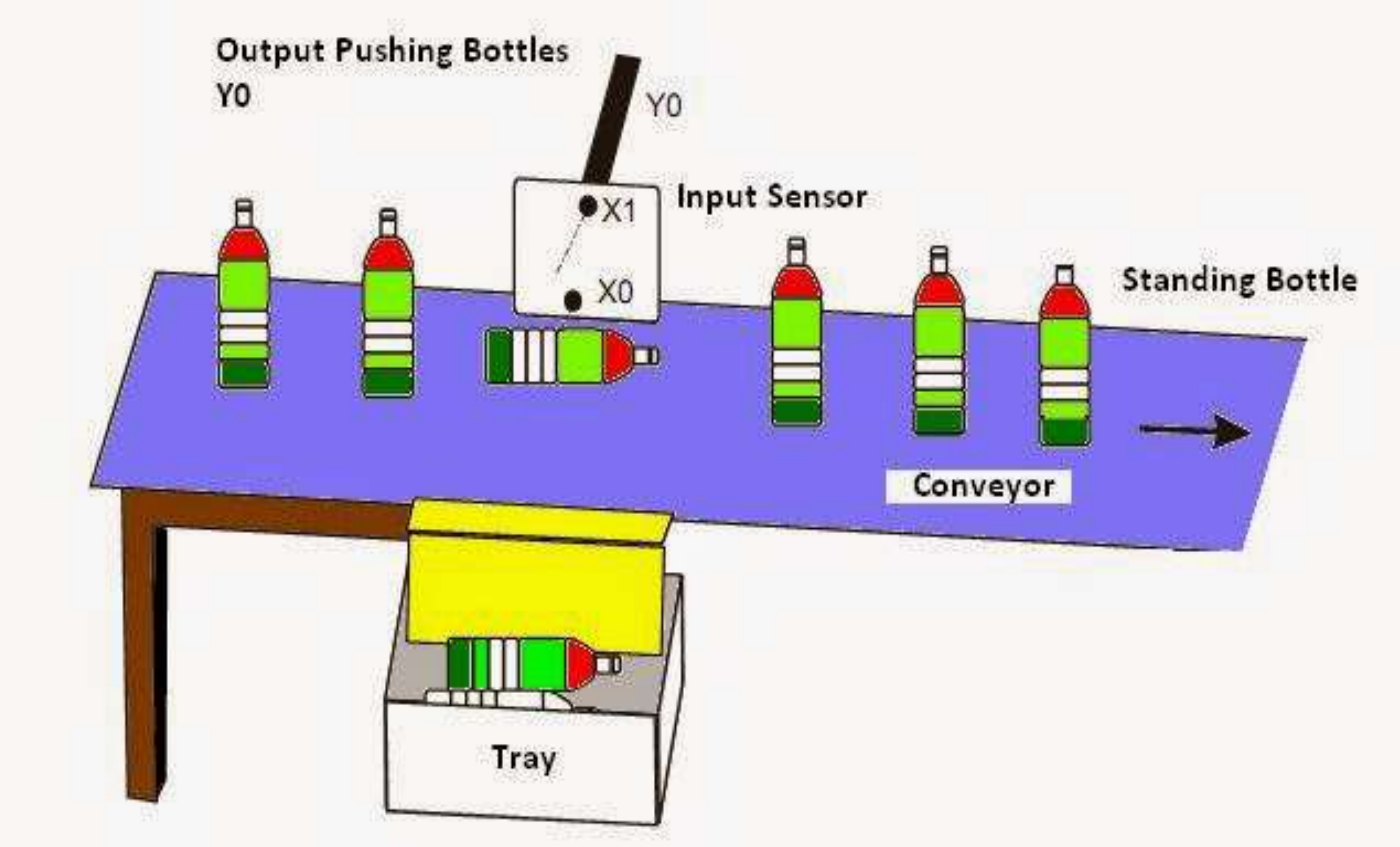
- SoMachine is the software provided by Schneider Electric to program the entry-level PLCs.
- PLCs used in big plants are usually programmed using Unity Pro, for which there is no free demo version.
- Fortunately, the way this software work is very much the same

PLC
Programming

- Create a project
- Define the hardware setup
- Create variables
- Define the program
- Test
- Debug
- Push to PLC
- START

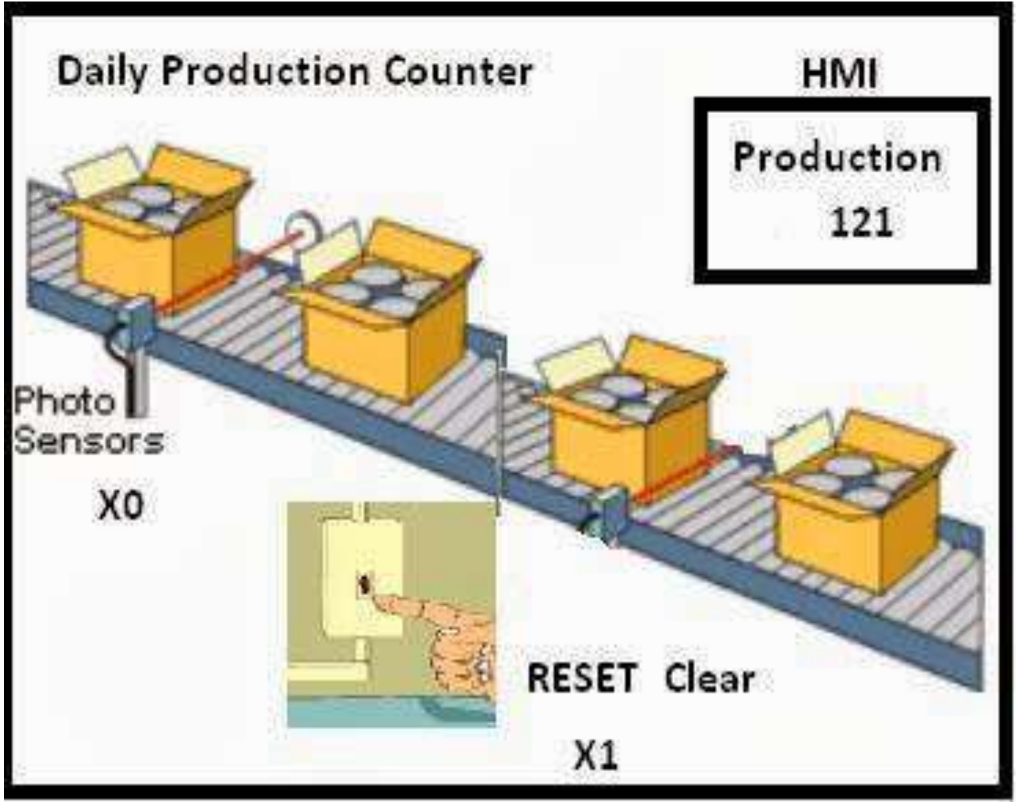
PLC
Programming

- Production line
- Flipped-over bottles must be put in the tray



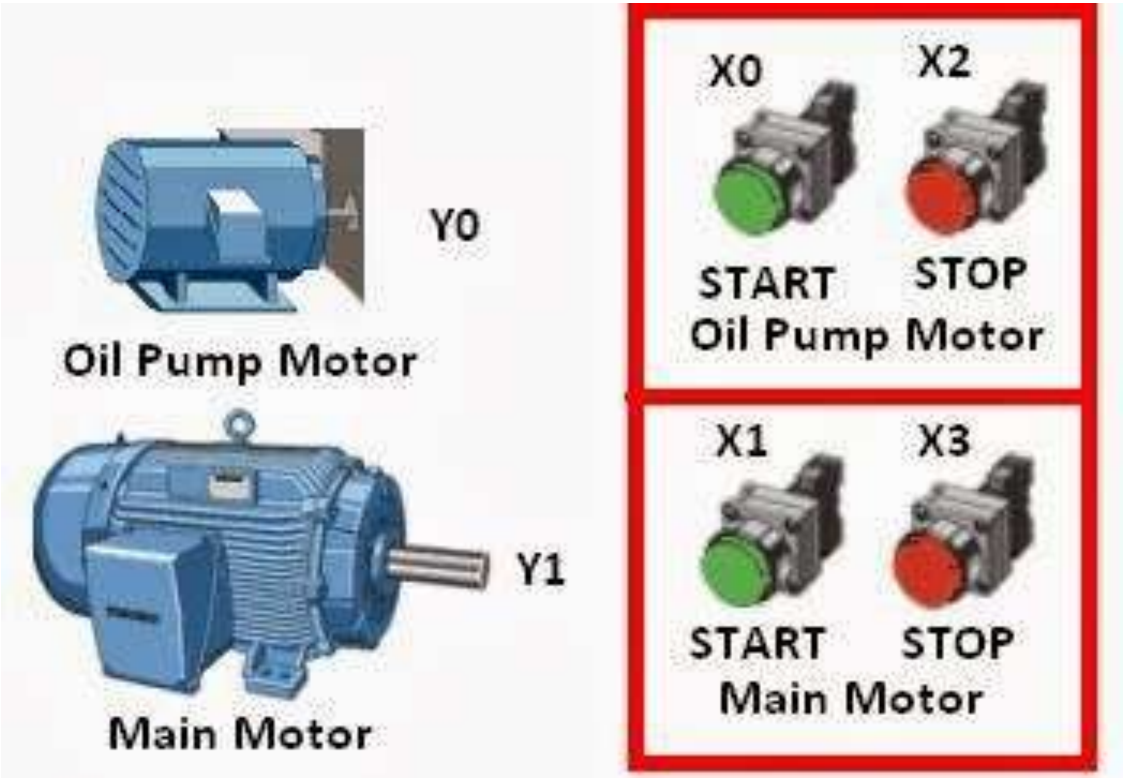
PLC
Programming

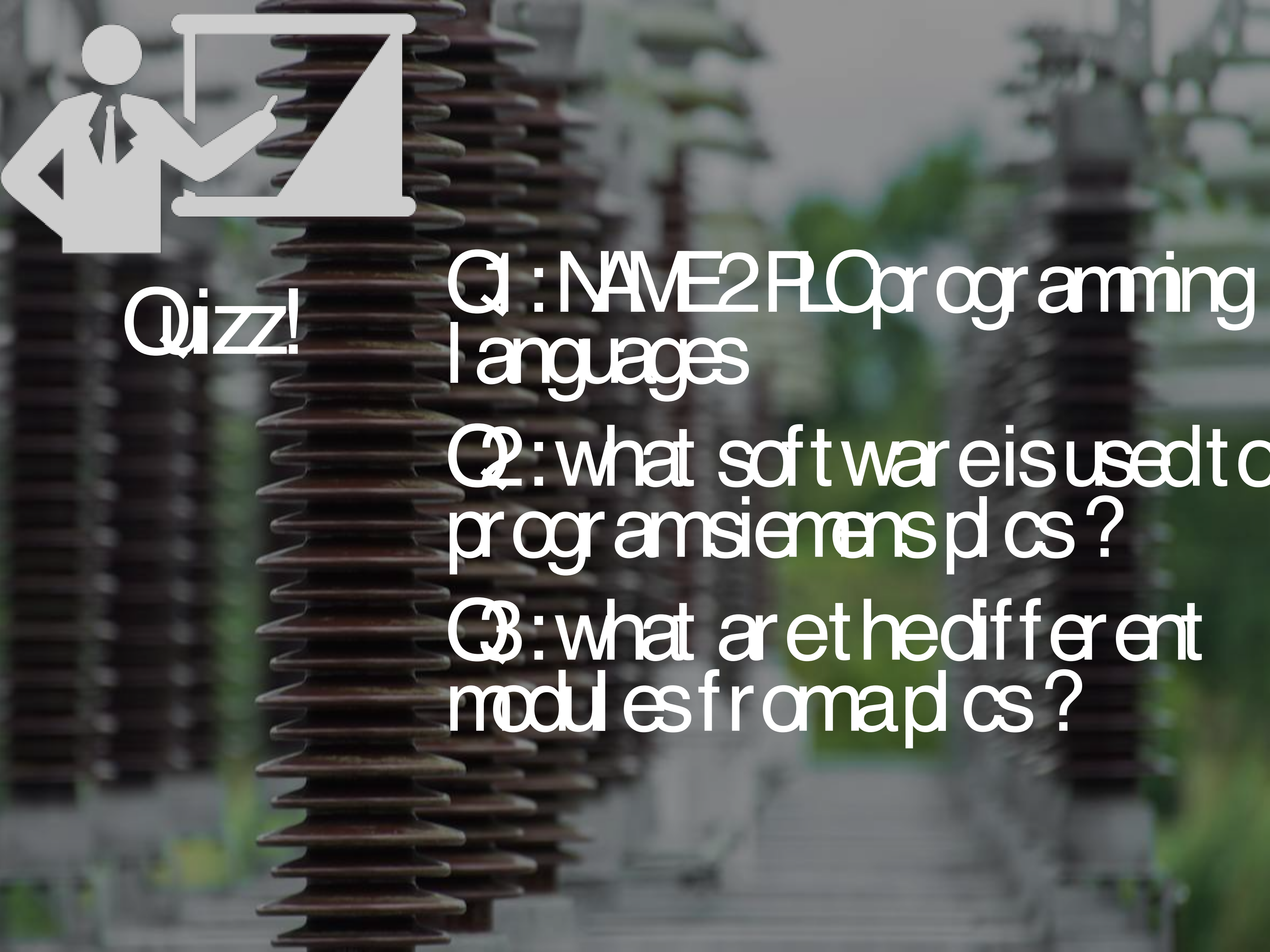
- Another production line
- Display indicates when 10 packages
- A button allows resetting the display



PLC
Programming

- The main motor must only start if the oil pump is running
- Motor must stop is X3 is pressed





Quizz!

Q1 : NAME 2 PLC programming languages

Q2 : what software is used to program siemens plcs ?

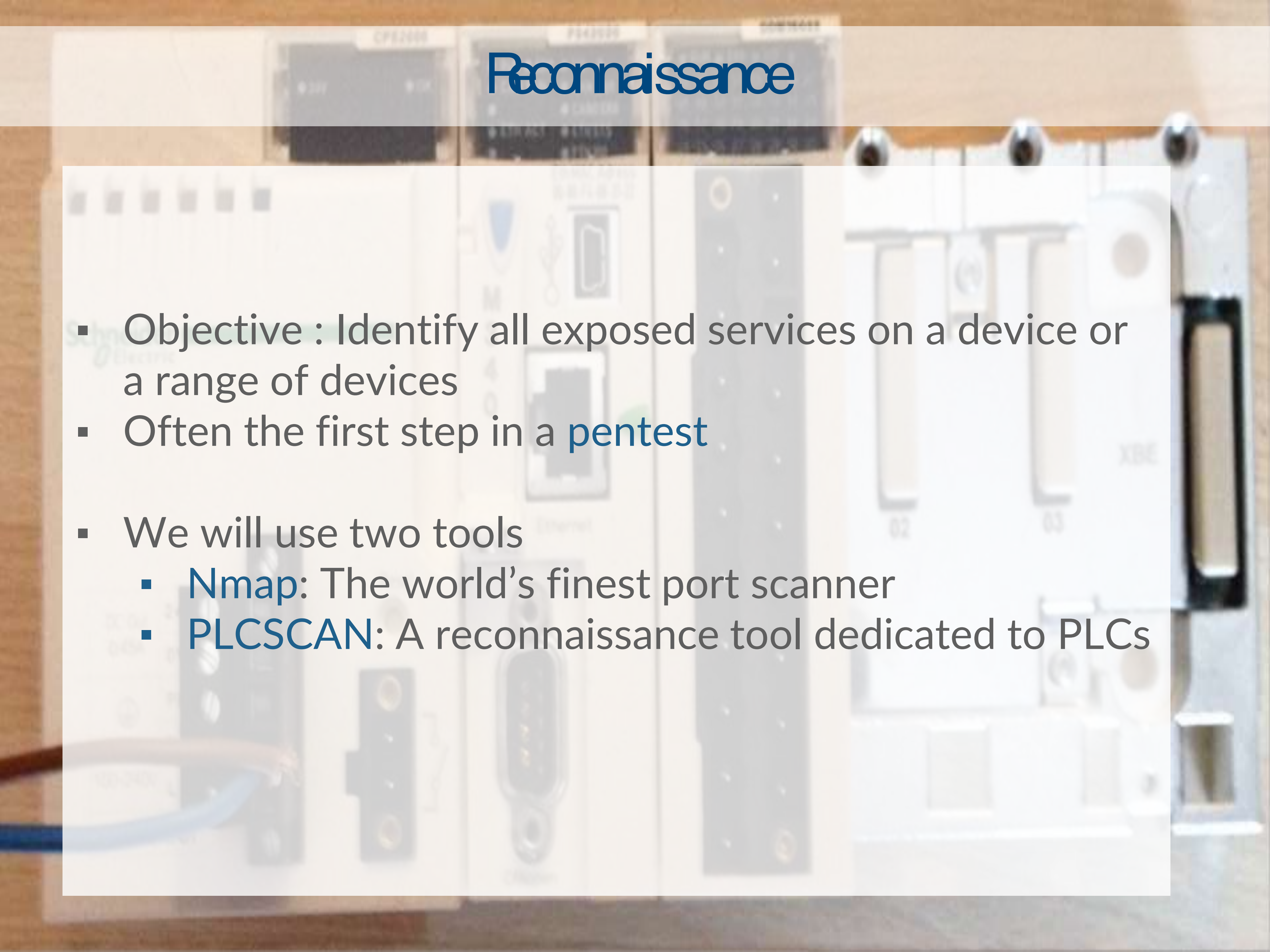
Q3 : what are the different modules from a plcs ?

WARNING
The following show features stunts
performed either by professionals or
under the supervision of professionals.
performed on this show.

Attacking plcs

Never do this
on LIVE production systems

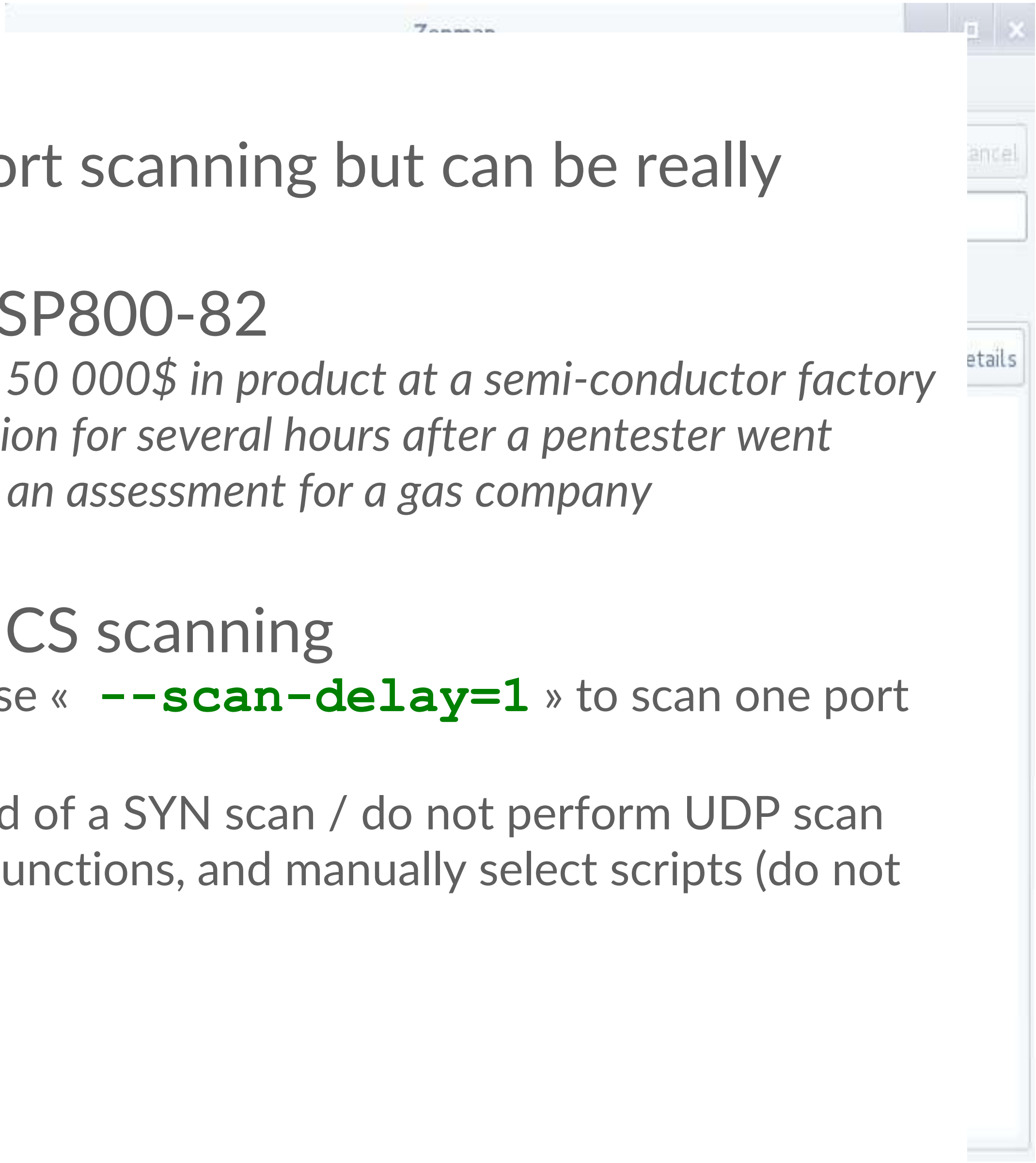
Reconnaissance



- Objective : Identify all exposed services on a device or a range of devices
- Often the first step in a pentest

- We will use two tools
  - Nmap: The world's finest port scanner
  - PLCSCAN: A reconnaissance tool dedicated to PLCs

Reconnaissance (Nmap)



- The de-facto tool for port scanning but can be really dangerous on ICS
- Two stories from NIST SP800-82
  - *A ping sweep broke for over 50 000$ in product at a semi-conductor factory*
  - *The blocking of gas distribution for several hours after a pentester went slightly off-perimeter during an assessment for a gas company*

- Nmap useful setup for ICS scanning
  - Reduce scanning speed! Use « **`--scan-delay=1`** » to scan one port at a time
  - Perform a TCP scan instead of a SYN scan / do not perform UDP scan
  - Do not use fingerprinting functions, and manually select scripts (do not use "**`–sC`**")

Reconnaissance (PLCSCAN)

Siemens PLC

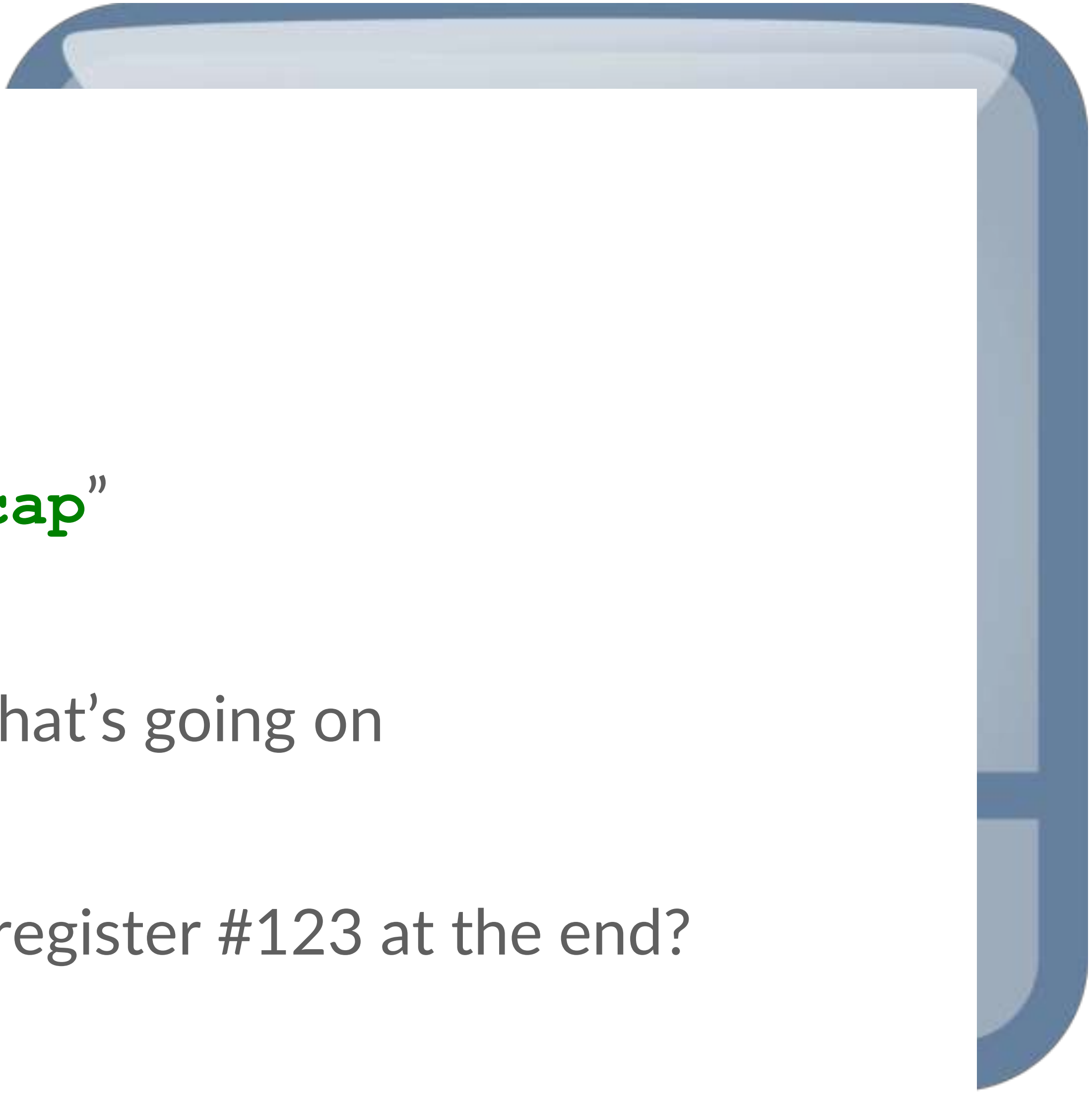
```
127.0.0.1:102
  Module
  Basic Hardwa
  Basic Firmwa
  Unknown (129
  Name of the
  Name of the
  Plant identi
  Copyright
  Serial numbe
  Module type
```

Modbus device

```
127.0.0.1:502
  Unit ID: 0
    Response e
    Device inf
  Unit ID: 255
    Response e
    Device: La
```

- https://code.google.com/p/plcscan/
  by SCADAStrangeLove (http://scadastrangelove.org/)
- Scans for ports `102` (Siemens) and `502` (Modbus) and tries to pull information about the PLC (modules, firmware version,…)
- Not exhaustive since not all PLCs use Modbus or are Siemens
- What if I told you there was another way… SNMP ?

Lab Session #1: Analyzing a Modbus communication with Wireshark

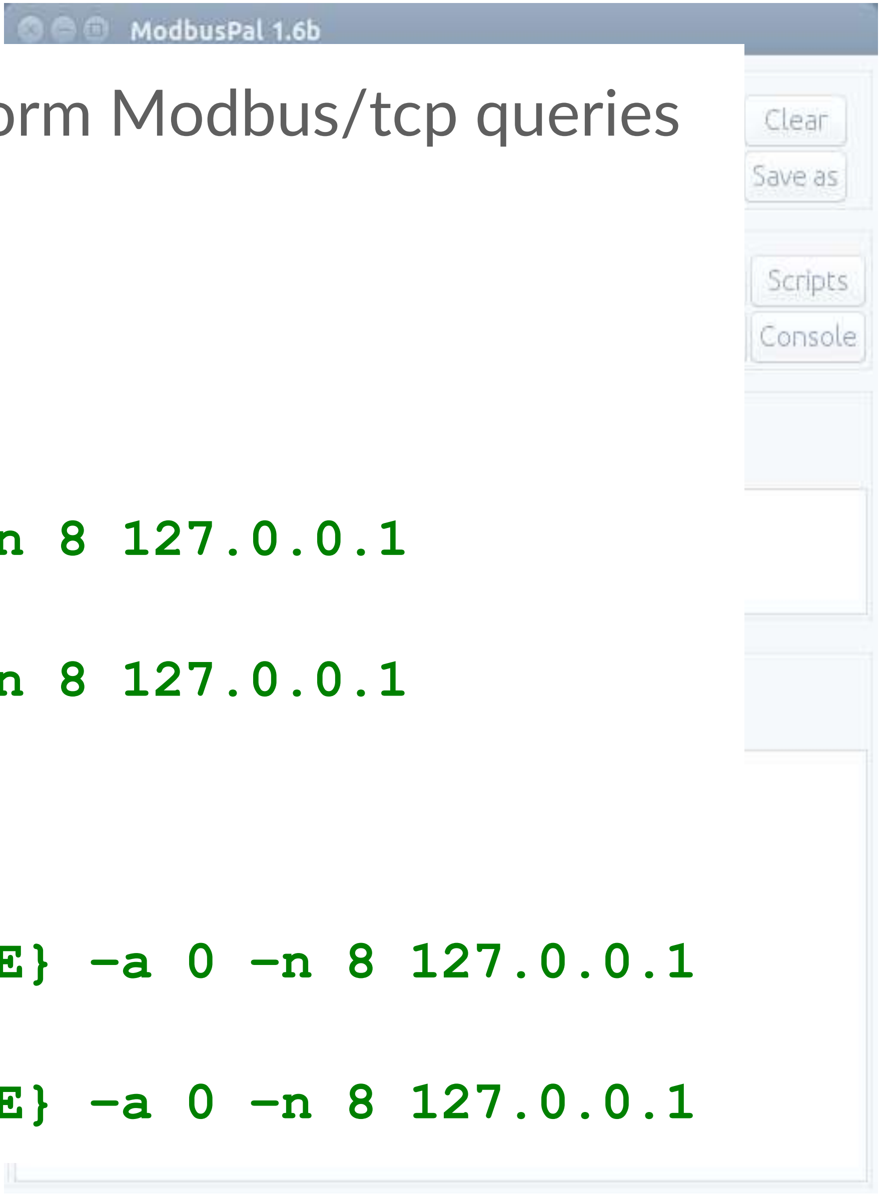


- Launch Wireshark
- Open “`modbus1.pcap`”
- Try to understand what’s going on
- What’s the value of register #123 at the end?

Lab session #2: ModbusPal

- Modbuspal is a modbus simulator
  `$ > java -jar ModbusPal.jar`
- Add a modbus slave
- Set some register values
- Query it with:
  - MBTGET Perl script
  - Metasploit module
- Analyze traffic with Wireshark

Lab session #2: ModbusPal + MBTGET



- Mbtget is a perl script to perform Modbus/tcp queries

```
$ > cd toolz
$ > ./mbtget -h
```

- Read requests
  - Coils (1 bit)

    ```
    $ > ./mbtget -r1 -a 0 -n 8 127.0.0.1
    ```

  - Words (8 bits)

    ```
    $ > ./mbtget -r3 -a 0 -n 8 127.0.0.1
    ```

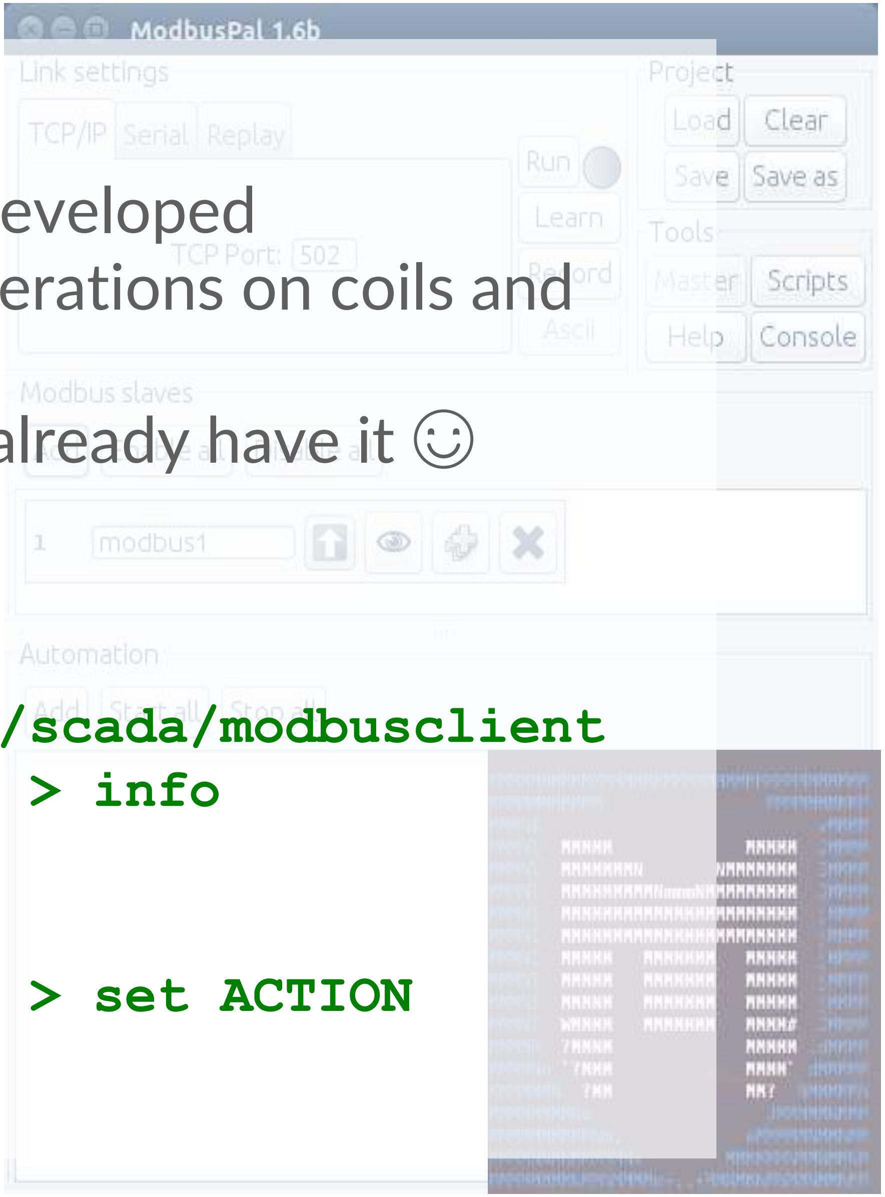
- Write requests
  - Coils (1 bit)

    ```
    $ > ./mbtget -w3 #{VALUE} -a 0 -n 8 127.0.0.1
    ```

  - Words (8 bits)

    ```
    $ > ./mbtget -w6 #{VALUE} -a 0 -n 8 127.0.0.1
    ```

Lab session #2: ModbusPal + METASPLOIT



- A simple modbus client that I developed
- Can perform read and write operations on coils and registers
- Included in msf's trunk so you already have it ☺

- Launch msf console

```
$ > msfconsole
msf > use auxiliary/scanner/scada/modbusclient
msf auxiliary(modbusclient) > info
```

- Play!

```
msf auxiliary(modbusclient) > set ACTION
```

Lab session #3 : S7 using Snap7

- Snap7 is an open-source library implementing Siemens S7 protocol
- Launch the demo server

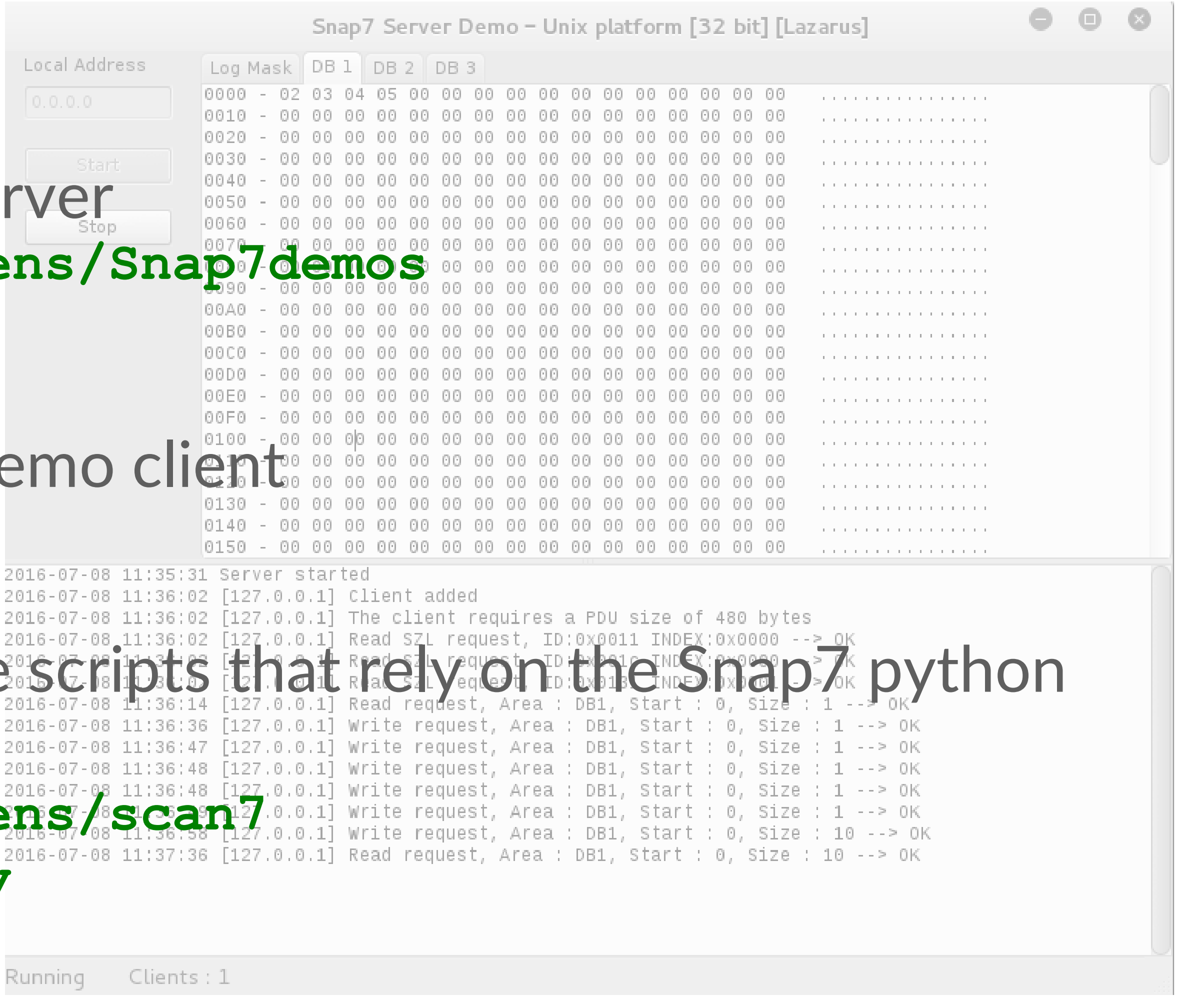
```
$ > cd toolz/siemens/Snap7demos
$ > ./serverdemo
```

- Query it using the demo client

```
$ > ./clientdemo
```

- You can also use the scripts that rely on the Snap7 python wrappers

```
$ > cd toolz/siemens/scan7
$ > python XXXX.py
```



```
0000 - 02 03 04 05 00 00 00 00 00 00 00 00 00 00 00 00    ................
0010 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0020 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0030 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0040 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0050 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0060 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0070 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0080 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0090 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00A0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00B0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00C0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00D0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00E0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
00F0 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0100 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0110 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0120 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0130 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0140 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
0150 - 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00    ................
```

```
2016-07-08 11:35:31 Server started
2016-07-08 11:36:02 [127.0.0.1] Client added
2016-07-08 11:36:02 [127.0.0.1] The client requires a PDU size of 480 bytes
2016-07-08 11:36:02 [127.0.0.1] Read SZL request, ID:0x0011 INDEX:0x0000 --> OK
2016-07-08 11:3[illegible] [127.0.0.1] Read SZL request, ID:0x001c INDEX:0x0000 --> OK
2016-07-08 11:3[illegible] [127.0.0.1] Read SZL request, ID:0x013[illegible] INDEX:0x000[illegible] --> OK
2016-07-08 11:36:14 [127.0.0.1] Read request, Area : DB1, Start : 0, Size : 1 --> OK
2016-07-08 11:36:36 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 1 --> OK
2016-07-08 11:36:47 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 1 --> OK
2016-07-08 11:36:48 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 1 --> OK
2016-07-08 11:36:48 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 1 --> OK
2016-07-08 11:3[illegible] [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 1 --> OK
2016-07-08 11:36:58 [127.0.0.1] Write request, Area : DB1, Start : 0, Size : 10 --> OK
2016-07-08 11:37:36 [127.0.0.1] Read request, Area : DB1, Start : 0, Size : 10 --> OK
```

Running Clients : 1

Attacking standard services

- Most PLCs have standard interfaces, such as HTTP and FTP
- Lets' say security was not the first thing in mind when introducing these features …

- On Schneider M340
  - FTP credentials are hardcoded sysdiag /factorycast@schneider
  - Allows you to retrieve the password file for the web UI

Lab session #4 : Attacking PLCs

- Unauthenticated actions on PLCs
  - Schneider “STOP/RUN”

    ```
    msf > use auxiliary/admin/scada/modicon_command
    ```

  - Schneider “Logic download/upload”

    ```
    msf > use auxiliary/admin/scada/modicon_stux_transfer
    ```

MSF’s module is not working properly on large programs.
I made some **unfinished** modifications on my Github : https://github.com/arnaudsoullie/metasploit-framework/blob/modicon_stux_transfer/modules/auxiliary/admin/scada/modicon_stux_transfer.rb
Also included in your VM as « modicon_stux_transfer_ASO »

Capture The Flag!

Your mission, should you choose to accept it, is to stop the train and capture the flag with the robot arm.

Hacking ICS?

IT'S ....

No crazy « hanging from the ceiling without sweating » stuff required !

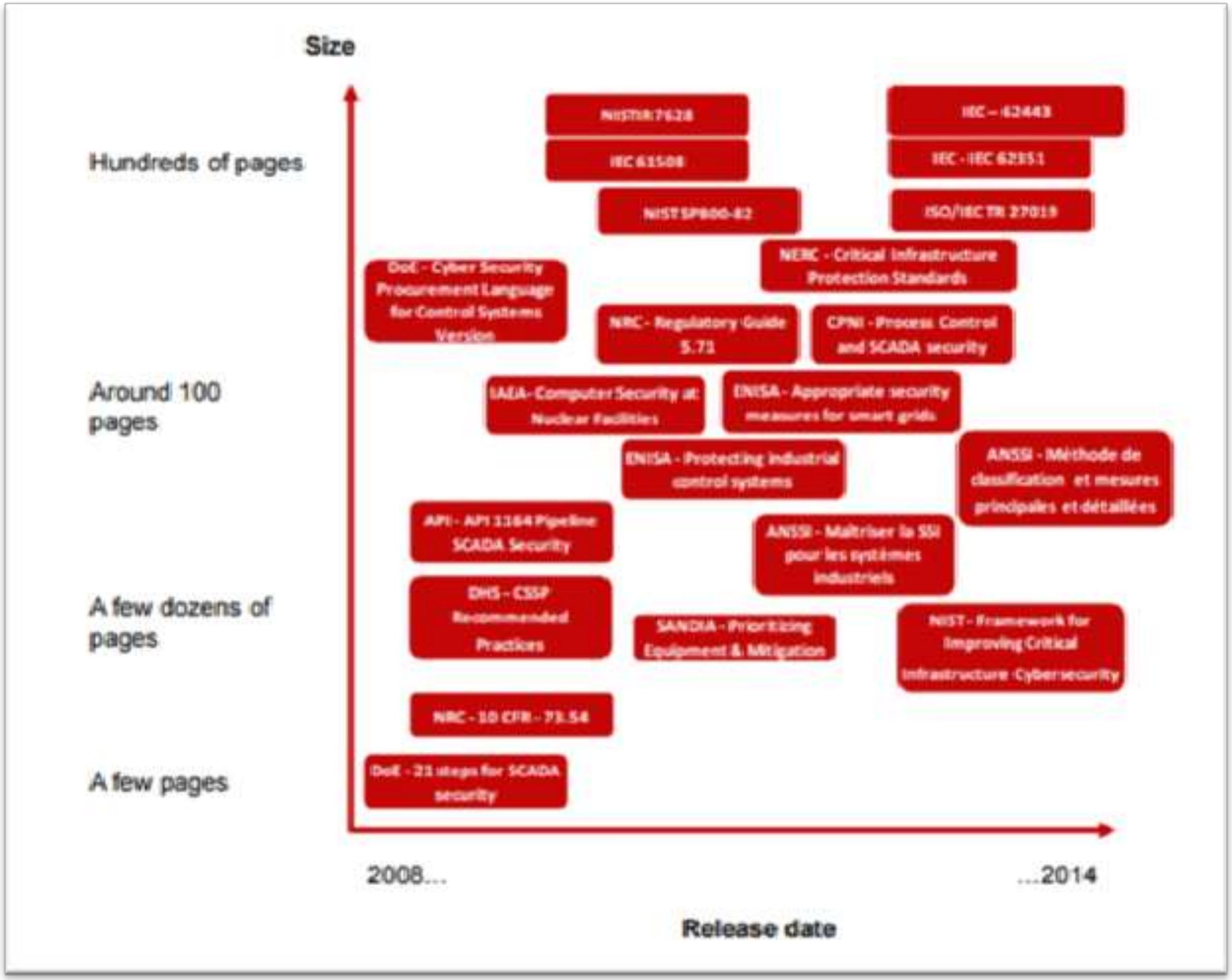
Securing ICS

- ICS security standards
    - Comparison
    - ANSSI
    - ISA99
    - 62443
- System hardening
- Network segmentation
    - Theory
    - Necessary evil : data exchange
    - Technical solutions : FW, DMZ, Data diodes
- Security monitoring
    - Why ?
    - How ?
    - Integration with process supervision ?

ICS security standards

There are quite a few !

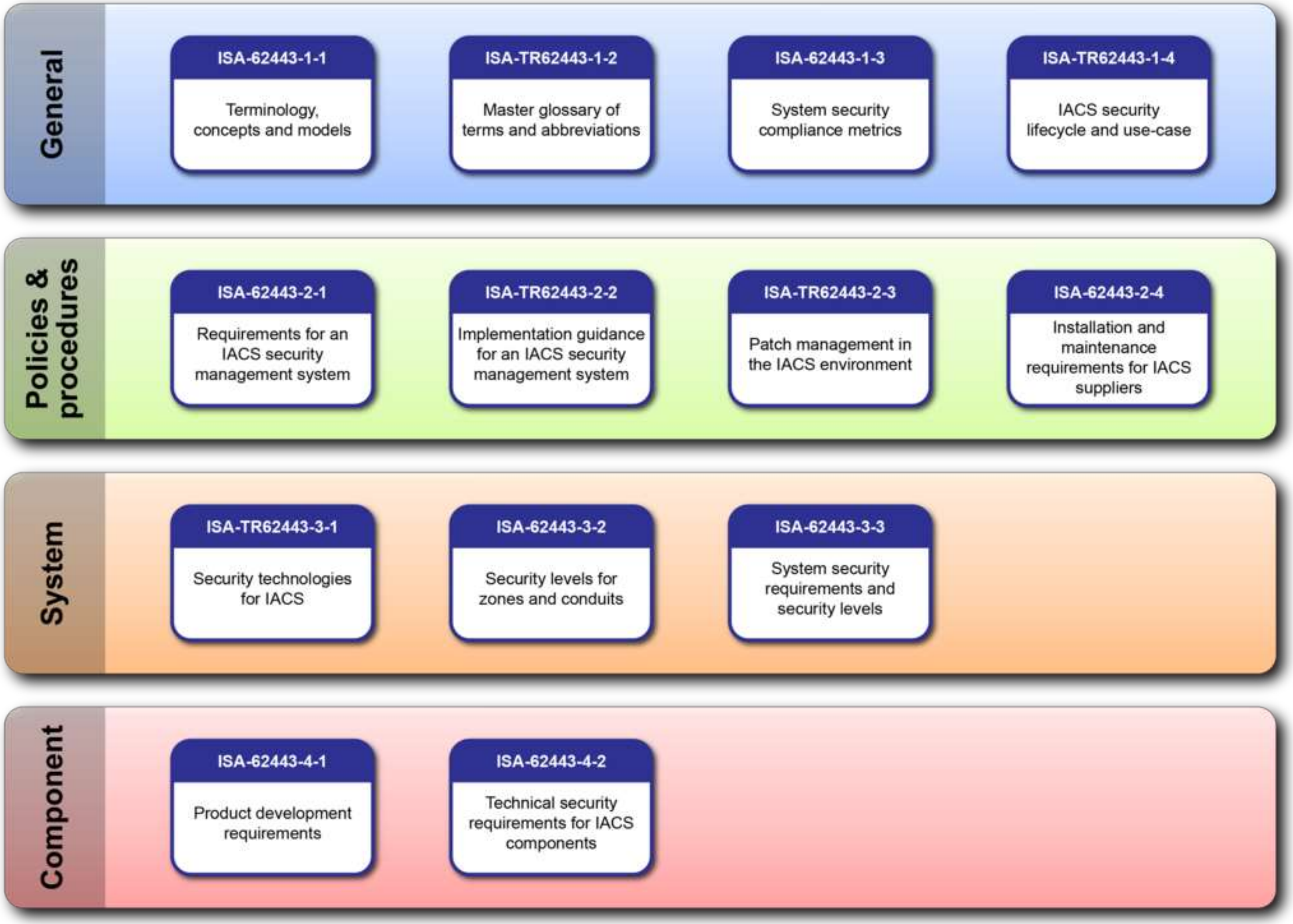
Let’s use a document published by the CLUSIF, a French information security association.



https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2014-Cyber-Security-of-Industrial-Control-Systems.pdf

ISA99 / IEC62443

ISA 99 is the old name, the document was initally created by the ISA (International Society for Automation)



General	**ISA-62443-1-1** Terminology, concepts and models	**ISA-TR62443-1-2** Master glossary of terms and abbreviations	**ISA-62443-1-3** System security compliance metrics	**ISA-TR62443-1-4** IACS security lifecycle and use-case
Policies & procedures	**ISA-62443-2-1** Requirements for an IACS security management system	**ISA-TR62443-2-2** Implementation guidance for an IACS security management system	**ISA-TR62443-2-3** Patch management in the IACS environment	**ISA-62443-2-4** Installation and maintenance requirements for IACS suppliers
System	**ISA-TR62443-3-1** Security technologies for IACS	**ISA-62443-3-2** Security levels for zones and conduits	**ISA-62443-3-3** System security requirements and security levels	
Component	**ISA-62443-4-1** Product development requirements	**ISA-62443-4-2** Technical security requirements for IACS components		

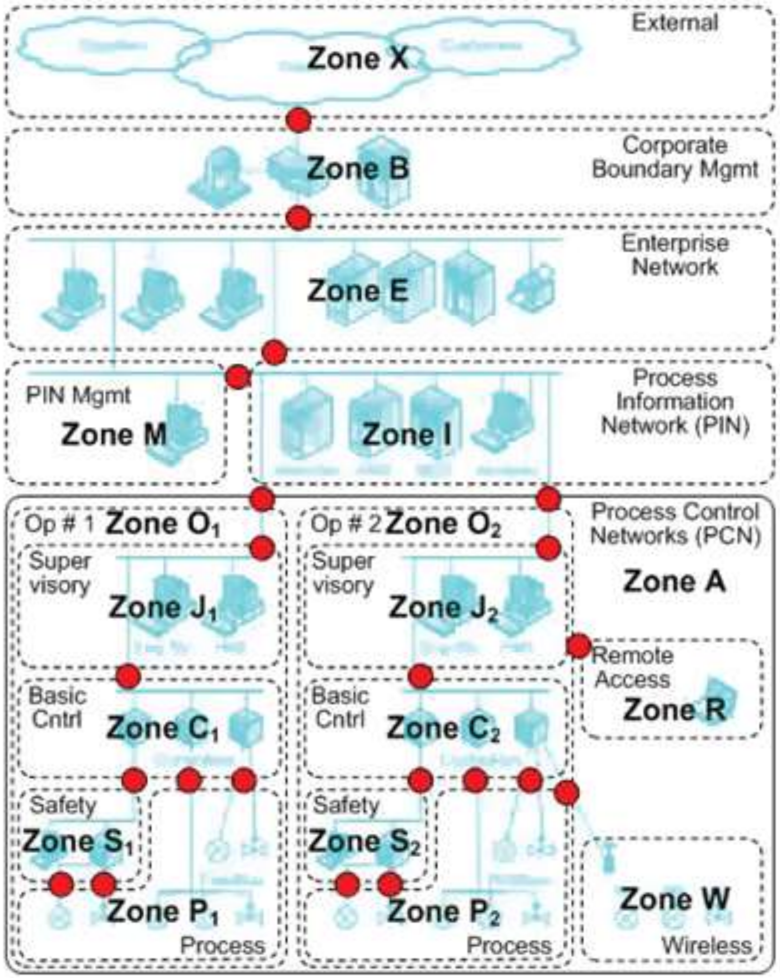
http://en.wikipedia.org/wiki/Cyber_security_standards#/media/File:ISA-62443_Standard_Series_2012.png

ISA99 / ISO62443

A few concepts :

- Security lifecycle : security must be integrated during each phase of a product development, use and end of life
- Zones and conduits : Instead of applying the same security level and security measures to all parts of the ICS, the ICS is segmented in zones, which have a homogeneous security level, and « conduits » are defined to exchange information between zones.
- Securiy levels : Define security levels in the same way as SIL (Safety Integrity Levels) [Note that there is no correlation whatsoever between security levels and safety levels]
- Target Security Levels
- Achieved Security Levels
- Capability Security Levels

Figure 3: Network zones and conduits



NIST SP 800-82

NIST = National Institute for Standards and Technology
Much more technical than the IEC 62443

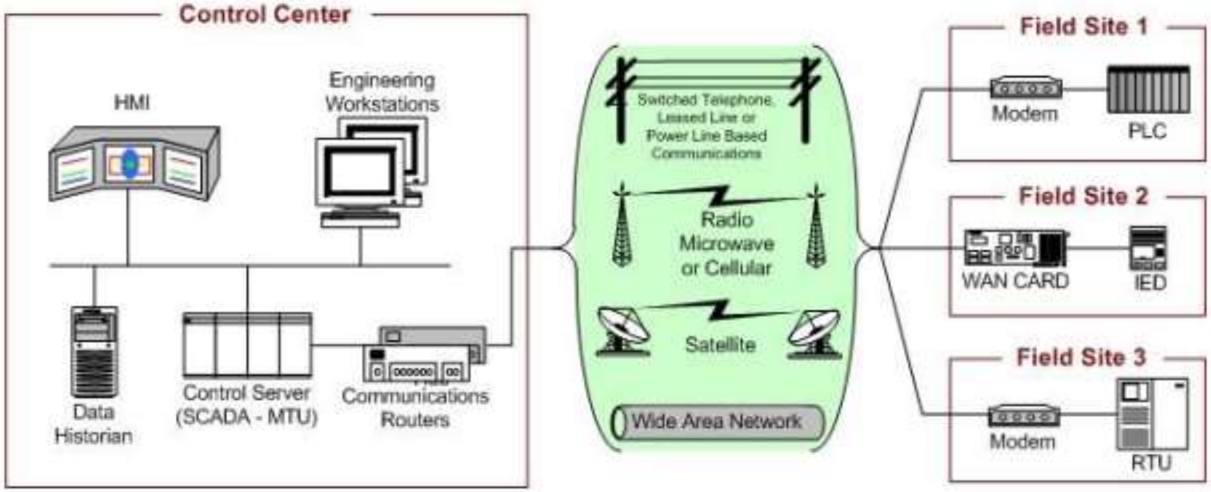


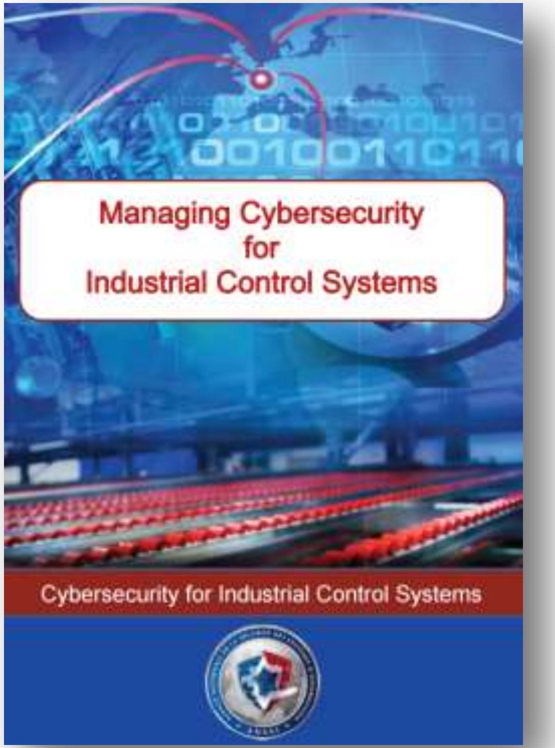
Figure 2-2. SCADA System General Layout

Old-school icon set ☺

French specific standards : The ANSSI

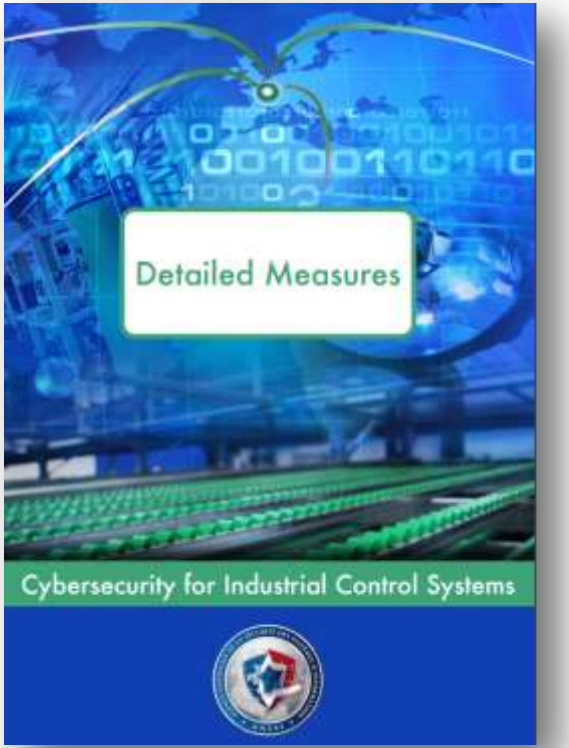
Really well done, ~~but only in French at the moment n~~ow in English !

http://www.ssi.gouv.fr/administration/guide/la-cybersecurite-des-systemes-industriels/



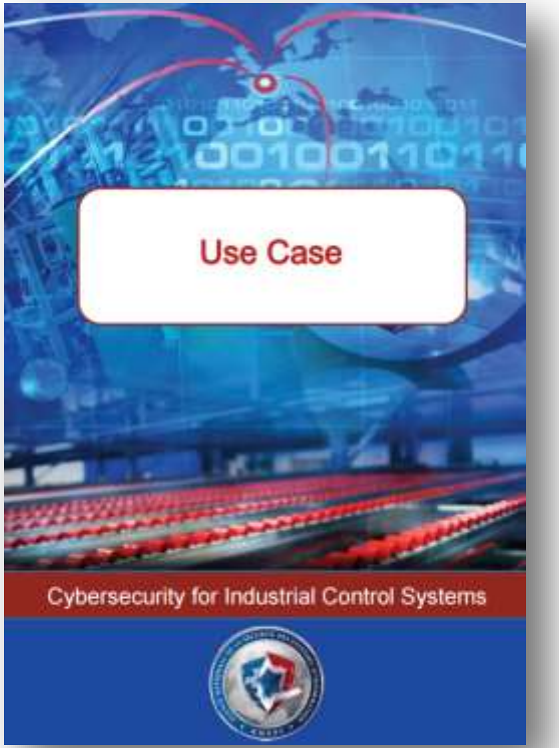
Managing Cybersecurity
for
Industrial Control Systems

Cybersecurity for Industrial Control Systems



Detailed Measures

Cybersecurity for Industrial Control Systems



Use Case

Cybersecurity for Industrial Control Systems

RIPE

Created by Langner Security
RIPE : Robust Ics Planning and Evaluation.

Rejects the idea of risk management (I am exagerating a bit), and focuses on security capabilities

Based on concepts from quality management, with 3 attributes:

- Verifiability
- Completeness
- Accuracy

Composed of 8 domains :

- System population Characteristics
- Network architecture
- Component Interaction
- Workforce Roles and Responsibilities
- Workforce Skills and Competence Development
- Procedural Guidance
- Deliberate Design and Configuration Change
- System acquisition

System hardening

We won't cover all the possible ways to harden a server configuration.
There are numerous quality resources on the topic, here are a few :

- DISA : http://iase.disa.mil/stigs/Pages/index.aspx
- CIS : https://benchmarks.cisecurity.org/downloads/
- …

However, here are the biggest topics

- Patching process
- Services
- Attack surface
- User accounts & permissions
- File permissions
- Network configuration
- Remote administration

System hardenning: whitelisting

- Since configuration and software do not change much in ICS, it is possible to go one step further in hardenning.
- You can use whitelisting technologies to prevent any unauthorized program from being executed.
- AppLocker from Microsoft allows you to do that, as well as some 3rd party tools, most of the time by AV companies (McAfee, Symantec, …)
- It is also possible to perform regular, automated configuration review to detect unauthorized changes
- Not to be forgotten : in case of vulnerability exploitation or if you have admin access, this could be bypassed

Network segmentation : why & how ?

- First question : why do we need to have network segmentation ?
  - Impacts of a compromise are higher on an ICS
  - We cannot afford to have attackers from the corporate network pivot to the ICS

- Second question : how to segregate the networks ?
  - Real question is : how to segregate while allowing some communications
  - Let’s take a look at NIST SP800-82

Network segmentation : Dual home

1st solution : Dual-homed workstations or servers (two network cards, one of the corporate network, one on the ICS network)

Network segmentation: Firewall

A firewall filters flows between corporate and ICS networks

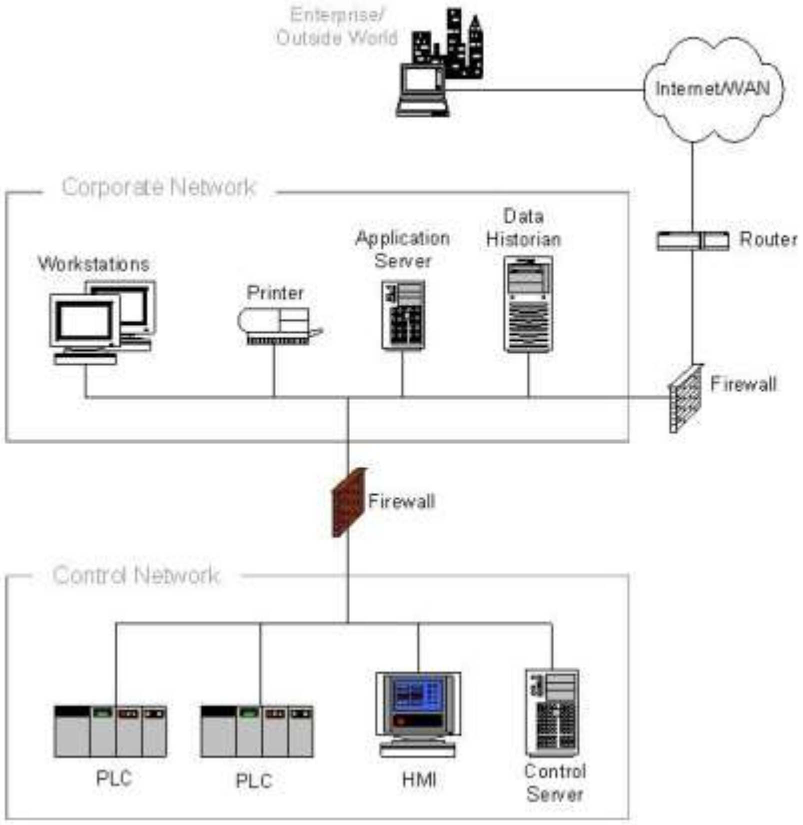


Figure 5-1. Firewall between Corporate Network and Control Network

For example, Data historian is allowed to query information from the control server in the ICS network.

If the Data Historian is compromised, attackers may then take control of the control server and thus modify the integrity of the process control

Network segmentation: Firewall + router

Same story

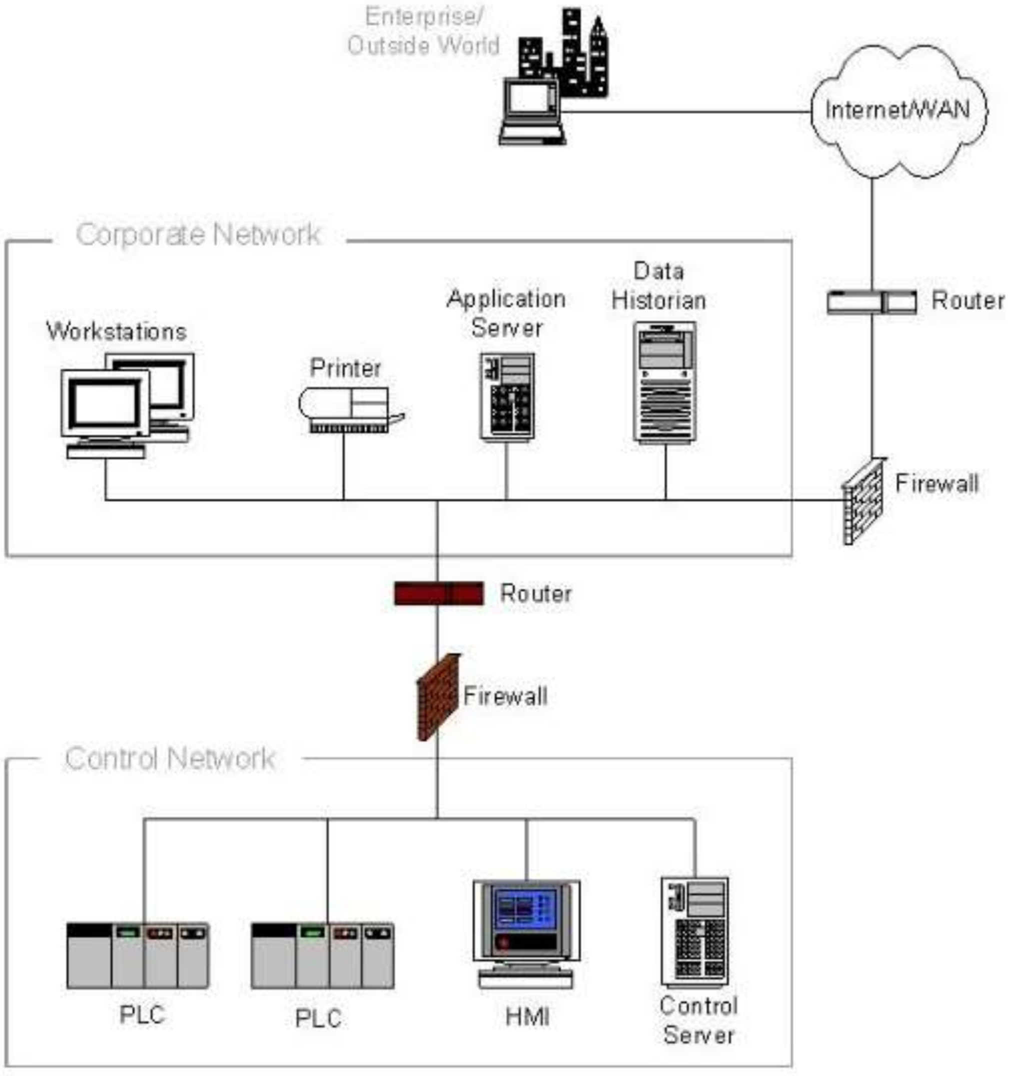


Figure 5-2. Firewall and Router between Corporate Network and Control Network

Network segmentation : DMZ

There is no direct network flow between corporate and ICS networks.

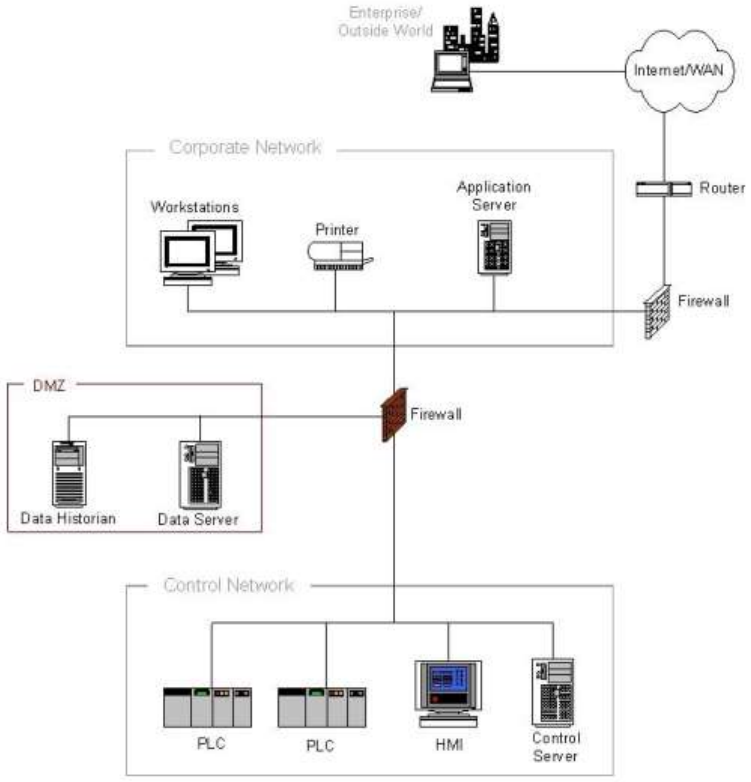


Figure 5-3. Firewall with DMZ between Corporate Network and Control Network

Corporate -> DMZ : ALLOW
ICS -> DMZ : ALLOW
ANY -> ANY : DENY

However, beware of client-side vulnerabilities

Network segmentation: DMZ with 2 firewalls

Quite the same as the previous one

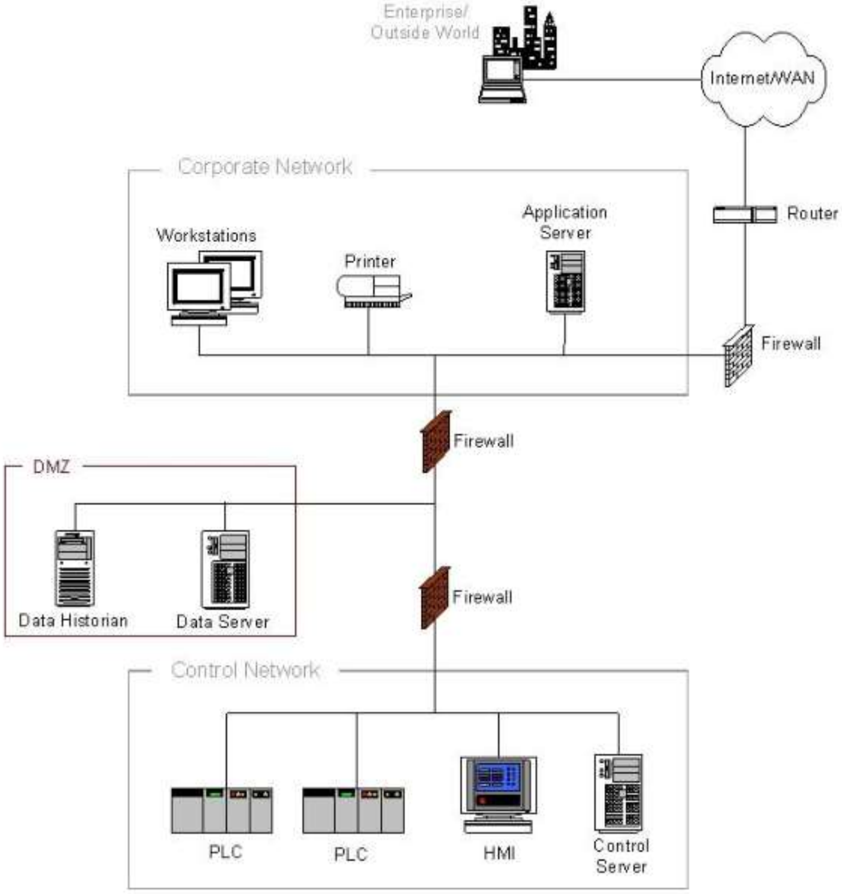


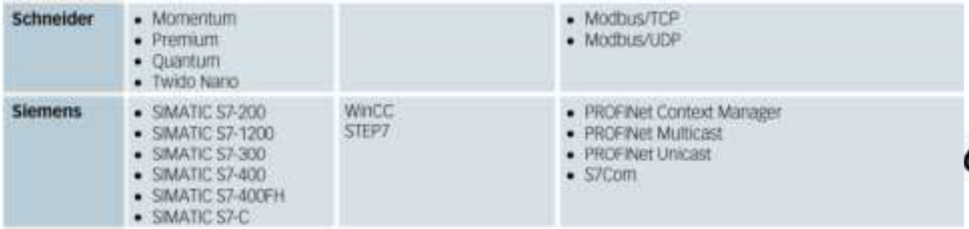
Figure 5-4. Paired Firewalls between Corporate Network and Control Network

Using 2 firewalls from different brands might prevent some attacks.

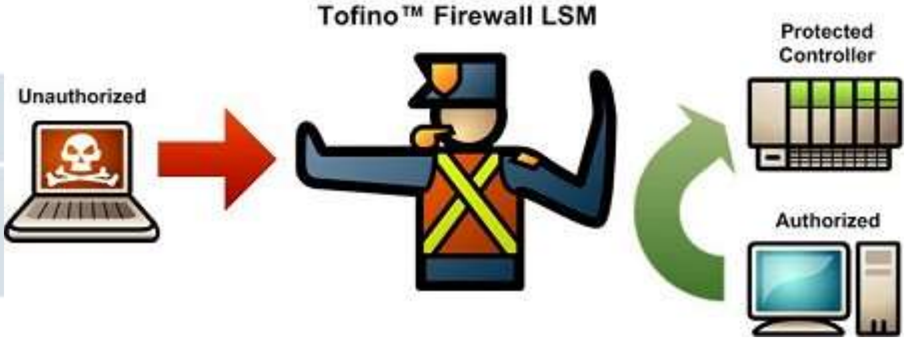
Also, easier to manage if you have one firewall team for corporate and one for ICS

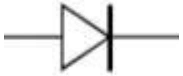
Network segmentation: DPI and IPS

- In order to provide a more context-specific filtering, it is possible to use DPI (*Deep Packet Analysis*) technology to allow or deny packets based on some protocol fields.
- Example: only authorize Modbus read requests, or deny Modbus 0x5a (90) function
- These features are available on most firewalls, but most of the time only « industrial » firewall will include the ability to inspect ICS specific protocols.
- You can also perform those operations with an IPS, but at the moment there are only a few ICS signatures



Schneider	• Momentum • Premium • Quantum • Twido Nano		• Modbus/TCP • Modbus/UDP
Siemens	• SIMATIC S7-200 • SIMATIC S7-1200 • SIMATIC S7-300 • SIMATIC S7-400 • SIMATIC S7-400FH • SIMATIC S7-C	WinCC STEP7	• PROFINet Context Manager • PROFINet Multicast • PROFINet Unicast • S7Com





Network segmentation : One-way gateways

- Not mentionned clearly in NIST SP800-82
- Offers the highest security level, but is also the most difficult to implement
- A data-diode is a network device based on a real diode, that transmits data only one-way.
- The fact that data cannot be transmitted in the other way is guaranteed by the laws of physics : hack that !
- Problem : since packets can only go one way, it is not possible to TCP protocol, as even the initial handshake (*SYN/SYN-ACK/ACK*) would fail. Only UDP-based protocols can be used.
- Consequence : you have to adapt the infrastructure to use a compliant protocol. That usually means that we need a gateway on each side of the diode

Check my project DYODE : *Do Your Own DiodE*
https://github.com/arnaudsoullie/dyode

Network segmentation: One-way gateways

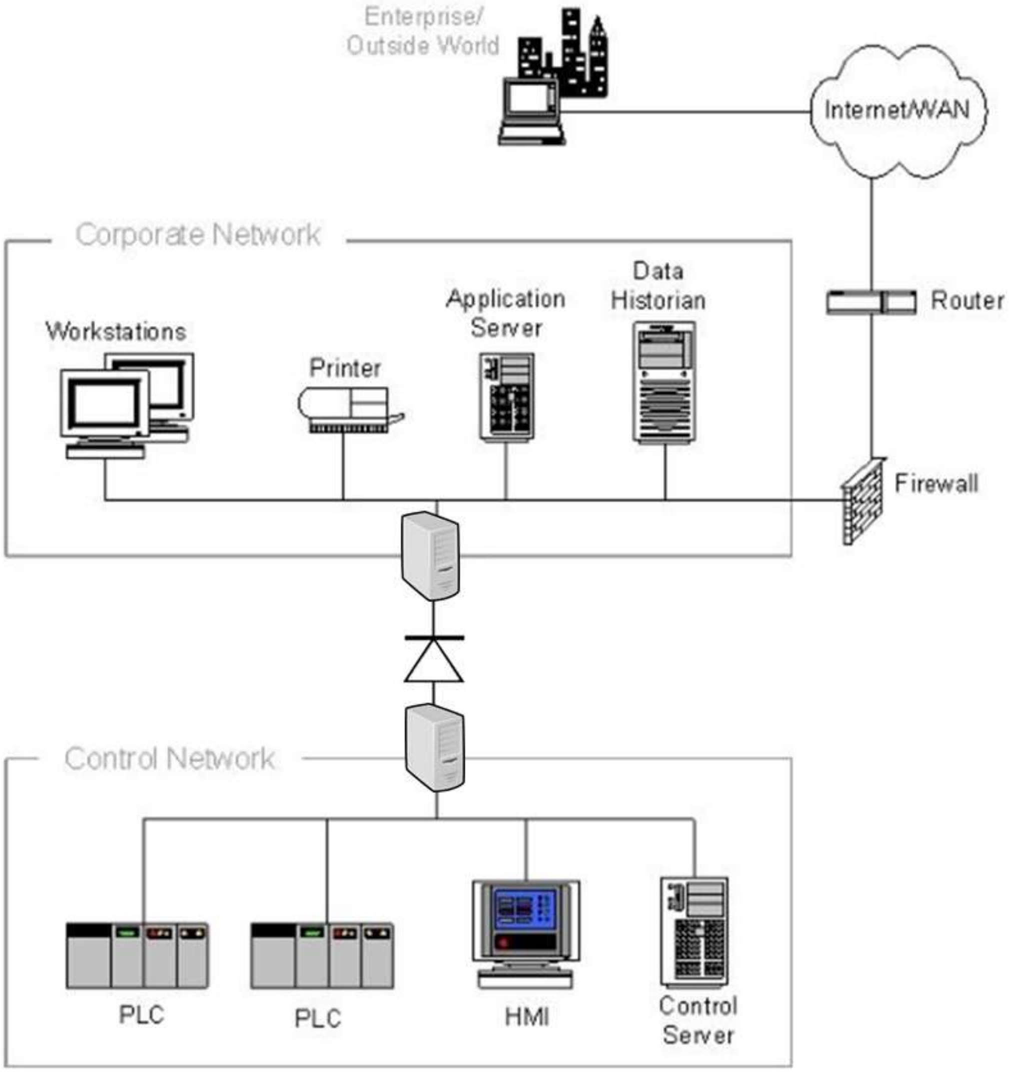


Figure 5-2. Firewall and Router between Corporate Network and Control Network

Network segmentation : One-way gateways without diodes

FPGAs

FPGA are Integrated Circuits that can be programmed. Once programmed, they are « burned » which means they cannot be reprogrammed.
Some gateways use this technology to perform network filtering.
It is « less » secure than a data diode since it is not physics-based and errors in FPGA code could allow data to go the other way around. However, it is probably an acceptable risk.

Software data-diode

PolyXene is a highly secure multi-security level operating system
It is based on several instances of Xen segregated by a micro-kernel
It is software-based but with a high security level.

Advantages of these solutions is that it can integrate all other security controls (protocol specific controls like read-only, etc..)

Network segmentation : Air gaps

Airgap is the notion of having no network connection between two networks. While this notion is important, it lacks the reality check that some form of data exchange is always necessary.
For example : update the servers, update the AV signatures, …

That is why it is necessary to also include laptops and USB drives into the picture, as they are often used to « brake » the airgap

Network segmentation : laptops

From what I’ve seen, most of the time people consider that there is an airgap if machines are not SIMULTANEOUSLY connected to the corporate network and the ICS networks.
That is a narrow view, as malware and pentesters can perform actions asynchroneously.

Example : Compromise of the coporate Active Directory, installation of a RAT on the PC from an operational, then program it to perform network reconnaissance on the ICS when it is connected, and send back the result to the C&C when the laptop is connected back to the corporate network.

Network segmentation : USB drives

When network segmentation is performed correctly, people tend to use USB keys to exchange data between corporate and ICS networks. The use of USB blocking « caps » is not really a solution, as :

- You do not really need the key to unlock it, I’ve seen a lot of people able to do it with a simple screwdriver
- You usually have to let at least 1 or 2 USB ports available for mouse and keyboard, so what is the point ?

What we need is a solution and process to exchange data between corporate and ICS

Importing data from corporate to ICS

Network-based

Plug a USB key or drop a file on a share on the corporate network and it will be analyzed and then available on a network share on the ICS network.

USB key based

Most solutions are based on AV : You plug the key, it is scanned, you unplug the key and go to the ICS. This can be flawed on several layers :

- If this workstation is connected, it can be comprised
- If you use the same AV as on the computer from which you took the files, what’s the point ?
- If you use the same USB key for corporate and ICS network you could be vulnerable to BadUSB (reprogramming the USB firmware).

Importing data from corporate to ICS

What should be the requirements ?

- Use different USB keys for corporate and ICS
  You could have a color code, and use AV / GPOs to filter the USB key authorized by manufacturer / serial number
- Be able to use several AV
- If something is detected an alert should be raised and treated

Wait a minute…what about how the file were retrieved in the first place ?
If you use a standard corporate laptop to connect to the ICS vendor, download the patch and then use your super-secure USB-checking solution, you are still vulnerable…

A dedicated PC, not managed by the Active Directory, should be used to download updates. It should have a dedicated proxy configuration that only allows it to connect to a whitelist of websites. Binaries signatures should be checked when provided.

Security monitoring

SCADA and DCS are ALL about monitoring; however, this doesn’t include security monitoring…

I strongly believe that security events should be treated as process events.

Example : an virus detection of one of the workstation should raise an alert not only locally, but also in the control room.

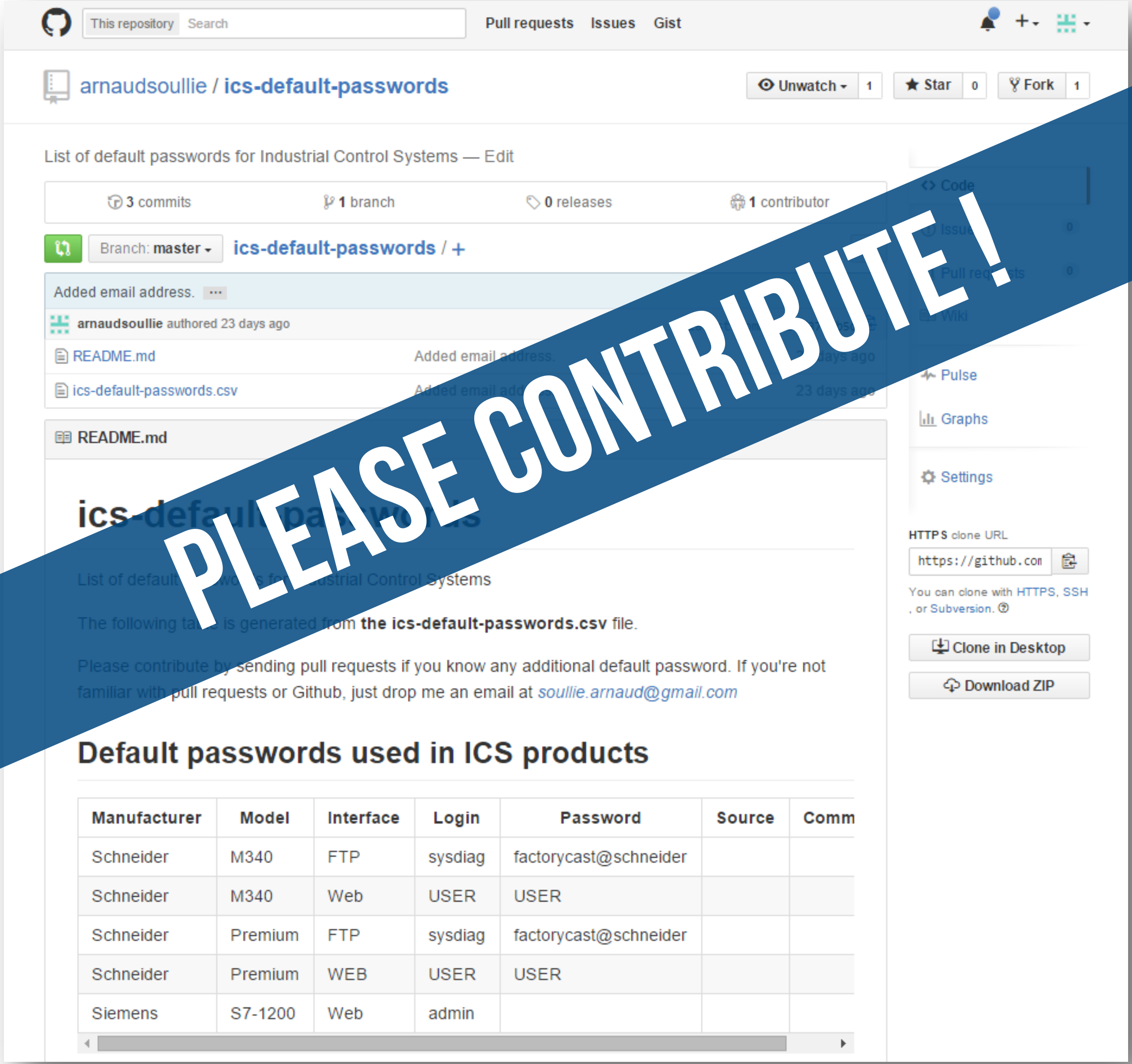
Moreover, we have to use the fact that ICS networks do not change that much over time, and consequently we can build a standard basis and act on any modification to it.

Network flows and application whitelisting should be achievable on an ICS network.

Do you have any question ?

Thanks for attending

PLEASE CONTRIBUTE !



arnaudsoullie / **ics-default-passwords**

List of default passwords for Industrial Control Systems — Edit

3 commits · 1 branch · 0 releases · 1 contributor

Branch: master · ics-default-passwords / +

Added email address. …

arnaudsoullie authored 23 days ago

README.md	Added email address.	23 days ago
ics-default-passwords.csv	Added email add	23 days ago

README.md

ics-default-passwords

List of default passwords for Industrial Control Systems

The following table is generated from **the ics-default-passwords.csv** file.

Please contribute by sending pull requests if you know any additional default password. If you're not familiar with pull requests or Github, just drop me an email at *soullie.arnaud@gmail.com*

Default passwords used in ICS products

Manufacturer	Model	Interface	Login	Password	Source	Comm
Schneider	M340	FTP	sysdiag	factorycast@schneider		
Schneider	M340	Web	USER	USER		
Schneider	Premium	FTP	sysdiag	factorycast@schneider		
Schneider	Premium	WEB	USER	USER		
Siemens	S7-1200	Web	admin			

https://github.com/arnaudsoullie/ics-default-passwords