black hat ARSENAL 2022

The Positive Way
WAVESTONE

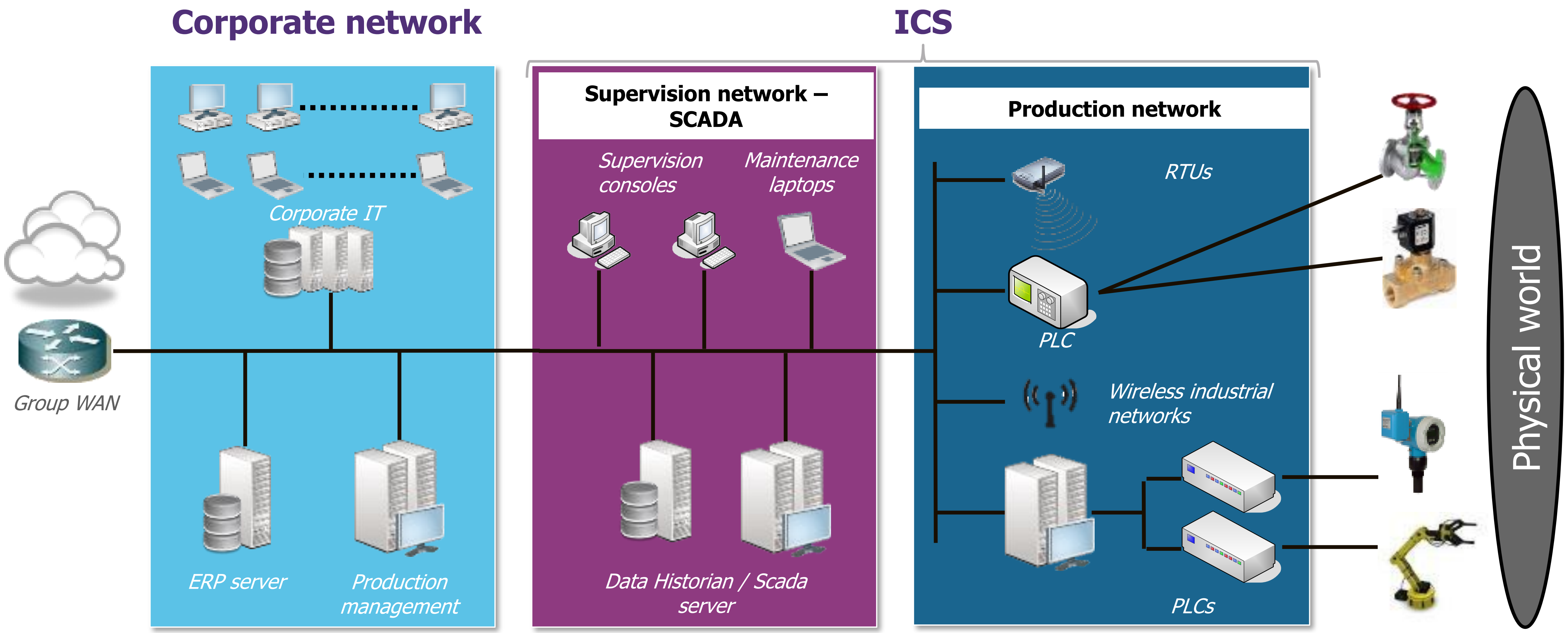
Capture the Train!

An introduction to Industrial Control systems

Arnaud Soullié
Paris office
@arnaudsoullie

Dhruv Sharan
London office

What is an Industrial Control System?



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

Modbus protocol

- Industrial protocol originally (1979) developed for serial bus (RS-485), later adapted to TCP/IP (port 502)
- **No authentication** / no encryption

  → *If you have network access, you can interact with the device*

- Several Modbus functions, mostly to **read/write data** from/to a PLC
- 2 types of data in Modbus : coils & registers
- Coils are 1-bit data (0 or 1)
- Registers are 16-bit data (0-65535)

Transaction identifier	**Protocol identifier**	**Length field**	**Slave address**	**Funtion code**	**Data**
					Variable structure depending on the function
2 bytes	2 bytes	2 bytes	1 byte	1 byte	N bytes

Our challenges for today

1. Identify devices on the network
2. Gather information about these devices
3. Use industrial protocols to take control of the robotic arm and capture the flag ☺

Step 1: Scanning

Scanning live ICS environments in dangerous
Legacy equipment sometimes doesn’t like a lot of packets and/or a lot of unclosed TCP connections.

A few general recommandations

```
nmap 192.168.0.1-100
```

Do a full TCP scan, not SYN scans

```
nmap -sT
```

Limit the use of scripts and fingerprinting

~~nmap -sV -O~~

Reduce the scan speed

```
nmap –T3 (not T5 ☺ )
nmap –scan-delay 100ms
nmap  --max-hostgroup 1
```

Step 2: Interacting with Modbus devices

Try to read and write some data to understand what's going on and to move the robotic arms!

Using python's pymodbus

```
pymodbus.console tcp --host IPADDR

> client.connect
```

```
> client.read_coils address 0 count 16 unit 1
> client.read_holding_registers address 0 count 16 unit
> client.write_register address 1  value 123 unit 1
> client.write_coil address 0 value 1 unit
```

black hat ARSENAL 2022

DECEMBER 7-8

EXCEL LONDON / UK

The Positive Way

WAVESTONE

Slides and code snippets at:

https://github.com/wavestone-cdt/bheu22-capture-the-train

Arnaud Soullié
Paris office
@arnaudsoullie

Dhruv Sharan
London office