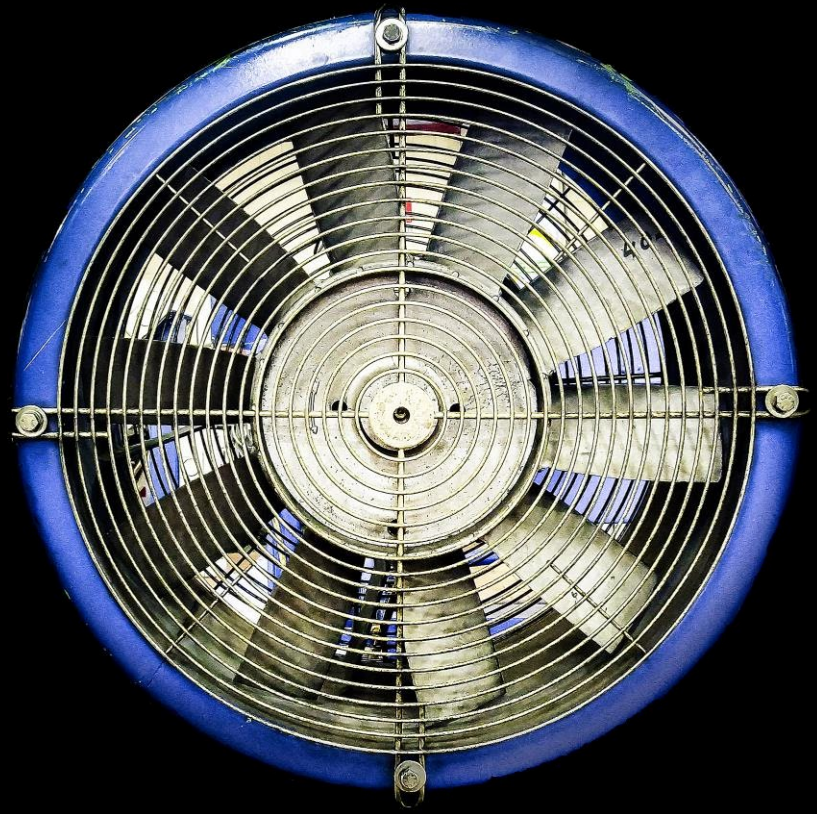


Киберсигурност в Индустрия 4.0

Въведение в основите на Индустрия 4.0 и проблемите свързани с киберсигурността

20/09/2023

Киберсигурност в Индустрия 4.0

Съдържание

Тема	Време за презентиране
Въведение в Индустрия 4.0	5 минути
Ethernet мрежи и Индустриални Ethernet мрежи	3 минути
Modbus протокол и модели на комуникация	2 минути
Публично достъпни ICS системи	2 минути
Нарастване на вятърна енергия през 2022	2 минути
Създаване на SCADA модел и примерни атаки	6 минути
Добри практики за защита на (ICS) / SCADA	3 минути
Видео демонстрация	7 минути

Въведение в Индустрия 4.0

(IA)
Индустриална
Автоматизация

(ICS)
Индустриални
Контролни
Системи

(OT)
Операционни
Технологии

(IIoT)
Индустриален
Интернет на Нещата

(SCADA)
Надзорен
Контрол
и
Събиране
на
Данни

(DCS)
Дистрибутирани
Контролни Системи

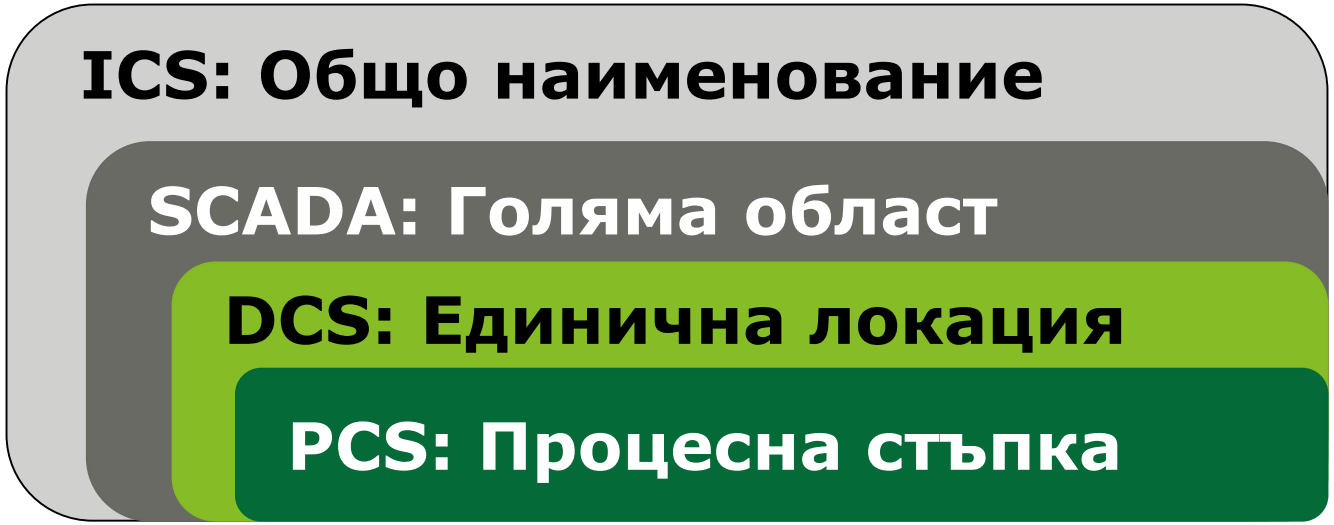
Въведение в Индустрия 4.0
ICS != SCADA != DCS != PCS (PA)

(ICS)
Индустриални Контролни Системи

(SCADA)
Надзорен Контрол и Събиране на Данни

(DCS)
Дистрибутирани Контролни Системи

(PCS/PA)
Система за контрол/автоматизация на процесите

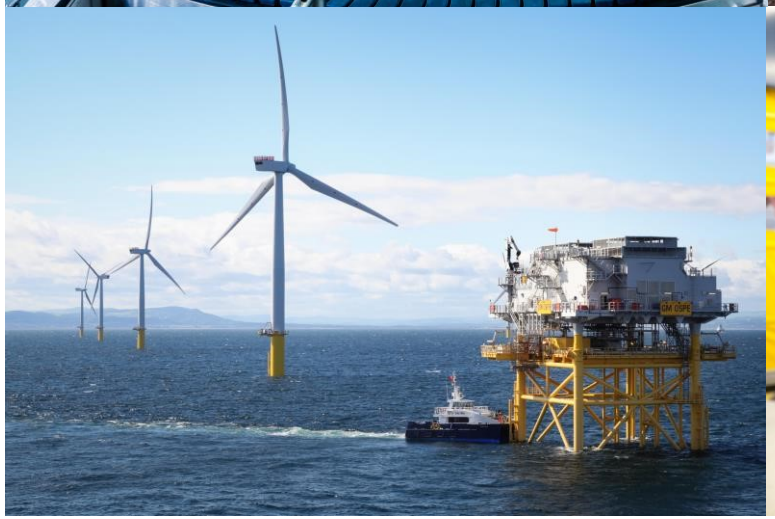


Индустриална Контролна Система

Устройство или набор от устройства, които управляват, командват, насочват или регулират поведението на други устройства или системи, свързвайки кибернетичен и физически свят.

Примери на Индустриални системи

- Нефтопроводи и газопроводи
- Производство, пренос и разпределение на електроенергия
- Химическа обработка и операции
- Производство на храни, напитки, лекарства и др.



Примери на Индустриални системи

Water & Sewage

Electricity

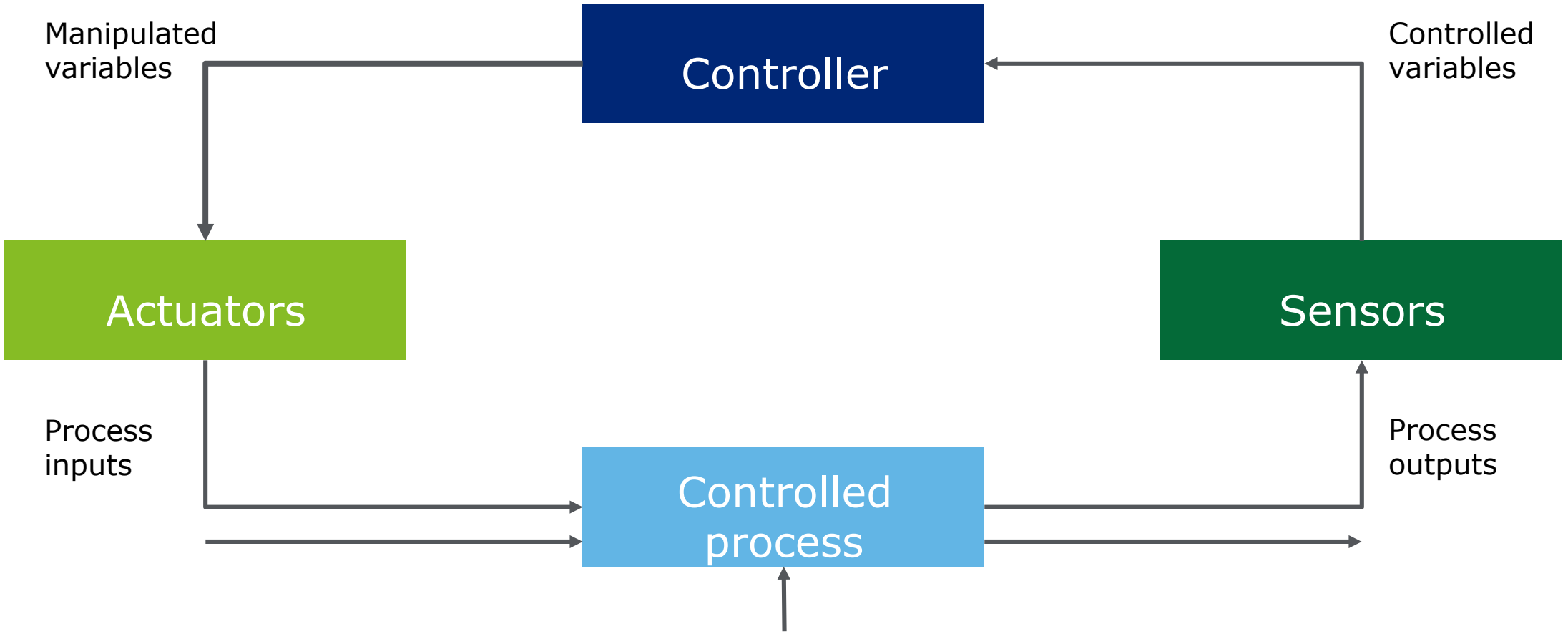
Wind

Critical manufacturing

Industrial Automation

Oil & Gas

Архитектура на Индустриални контролни системи



Архитектура на Индустриални контролни системи

Architecture of Industrial Control Systems

Programmable Logic Controller (PLC)

- Process Value
- Setpoint
- Manipulated Variable
- Error

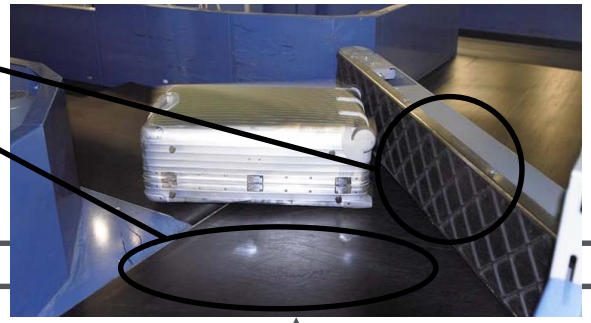
Setpoint

Controller

Error

Actuators

Sensors



Examples:
- Tank Control
- Motor control
- Rotary control

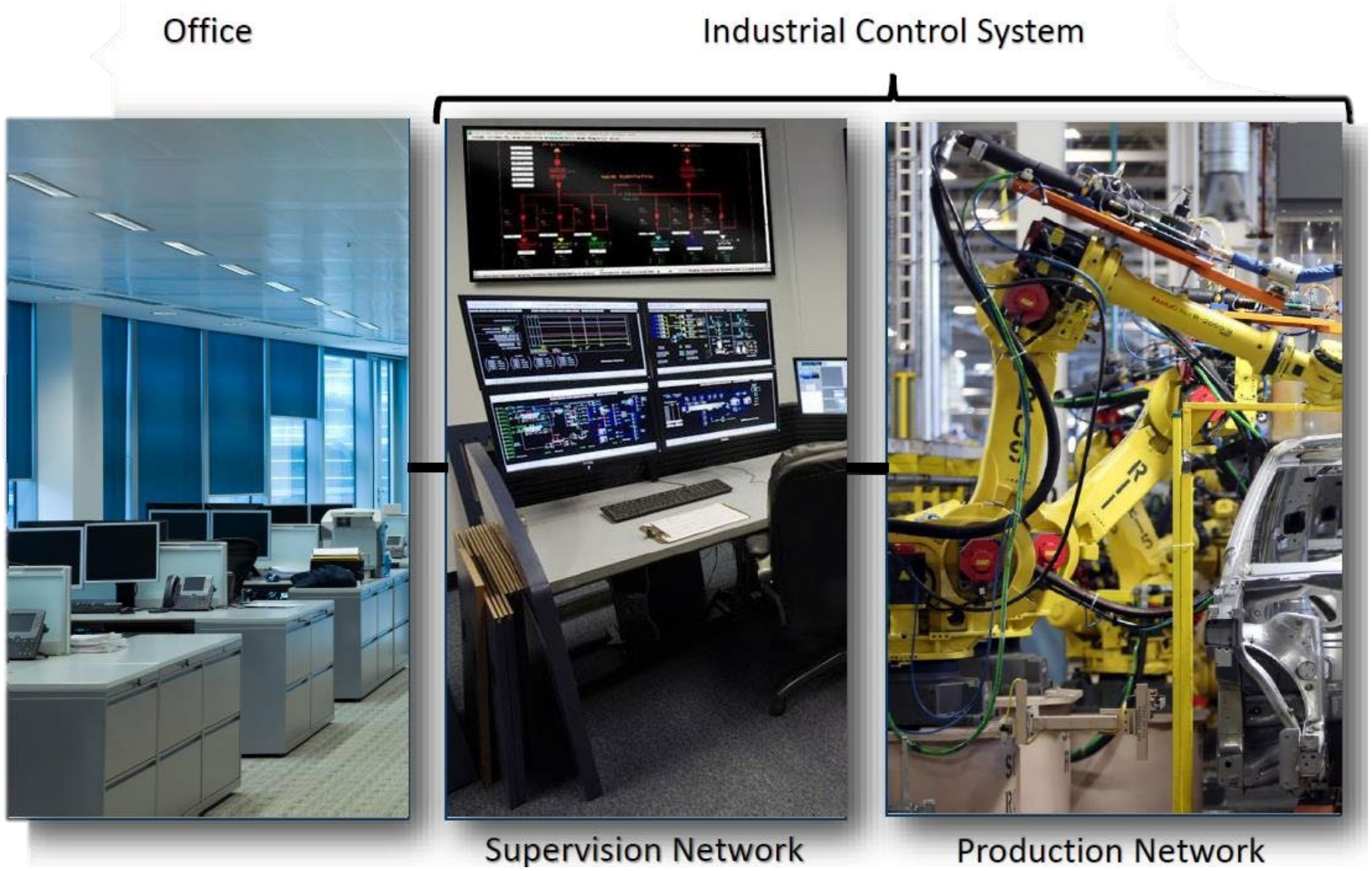
Process Value

Examples:
- Leakage
- Vibration

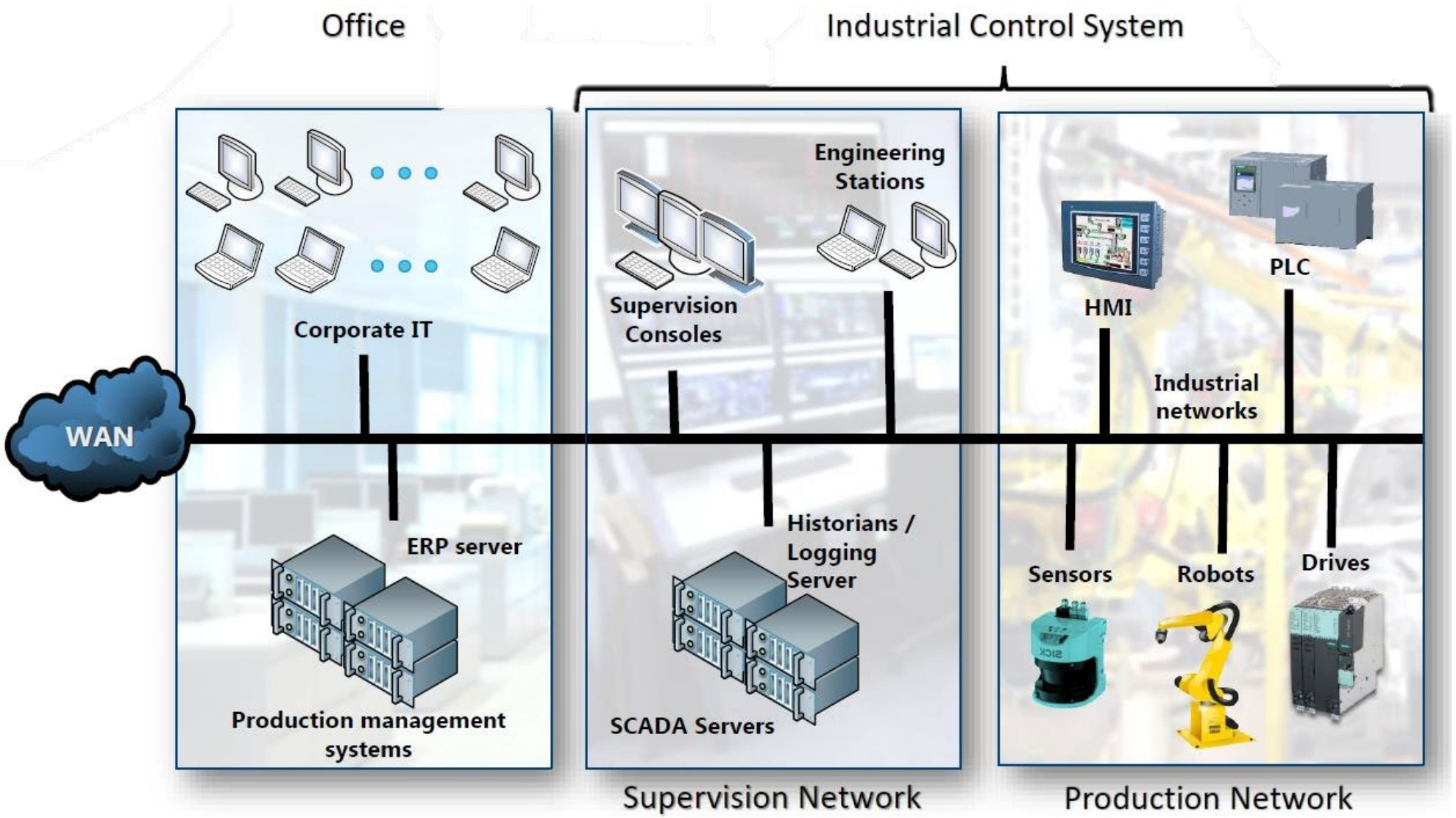
Manipulated Variable

Disturbances:
Weight, size, shape

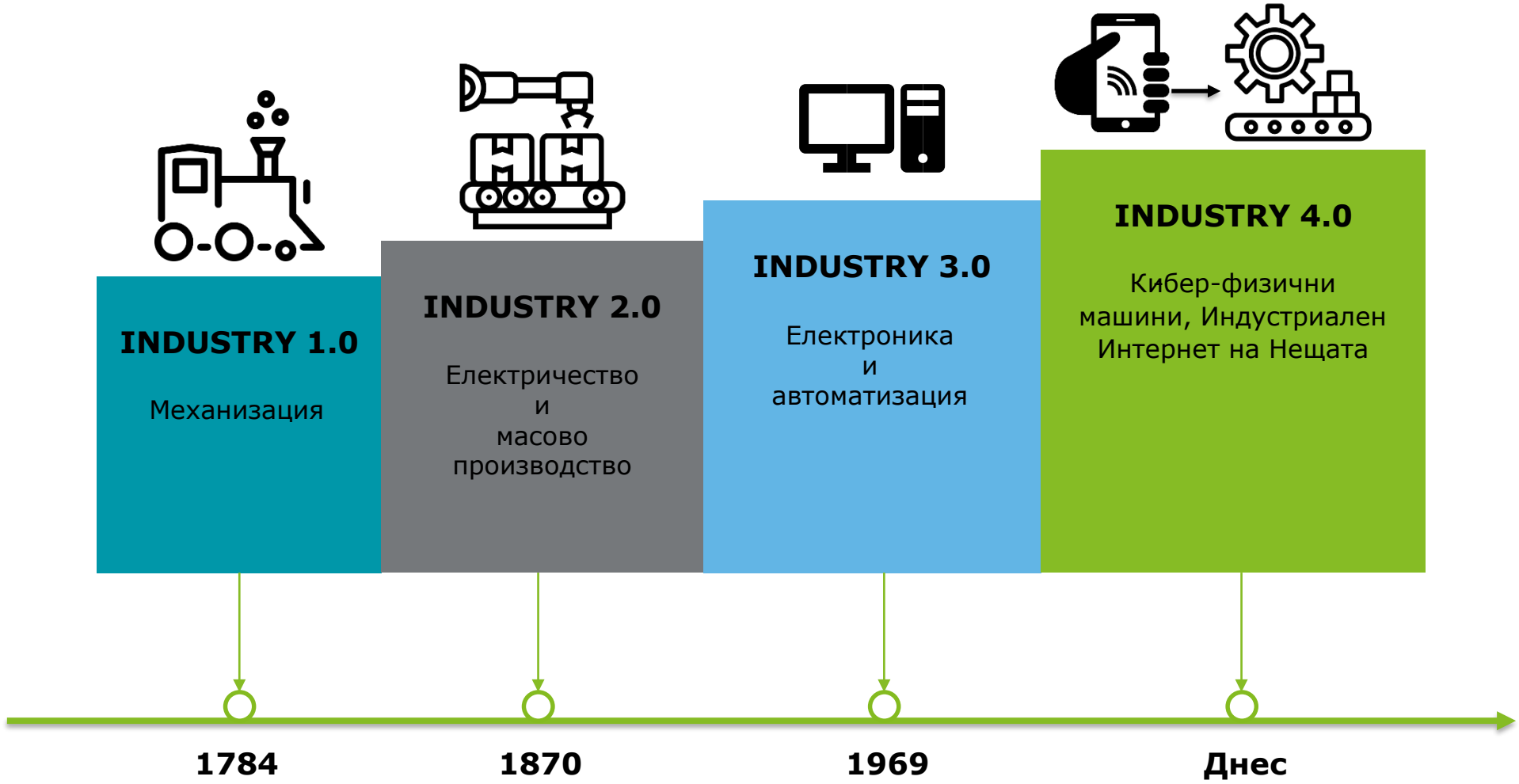
Офис мрежи / Индустриални мрежи



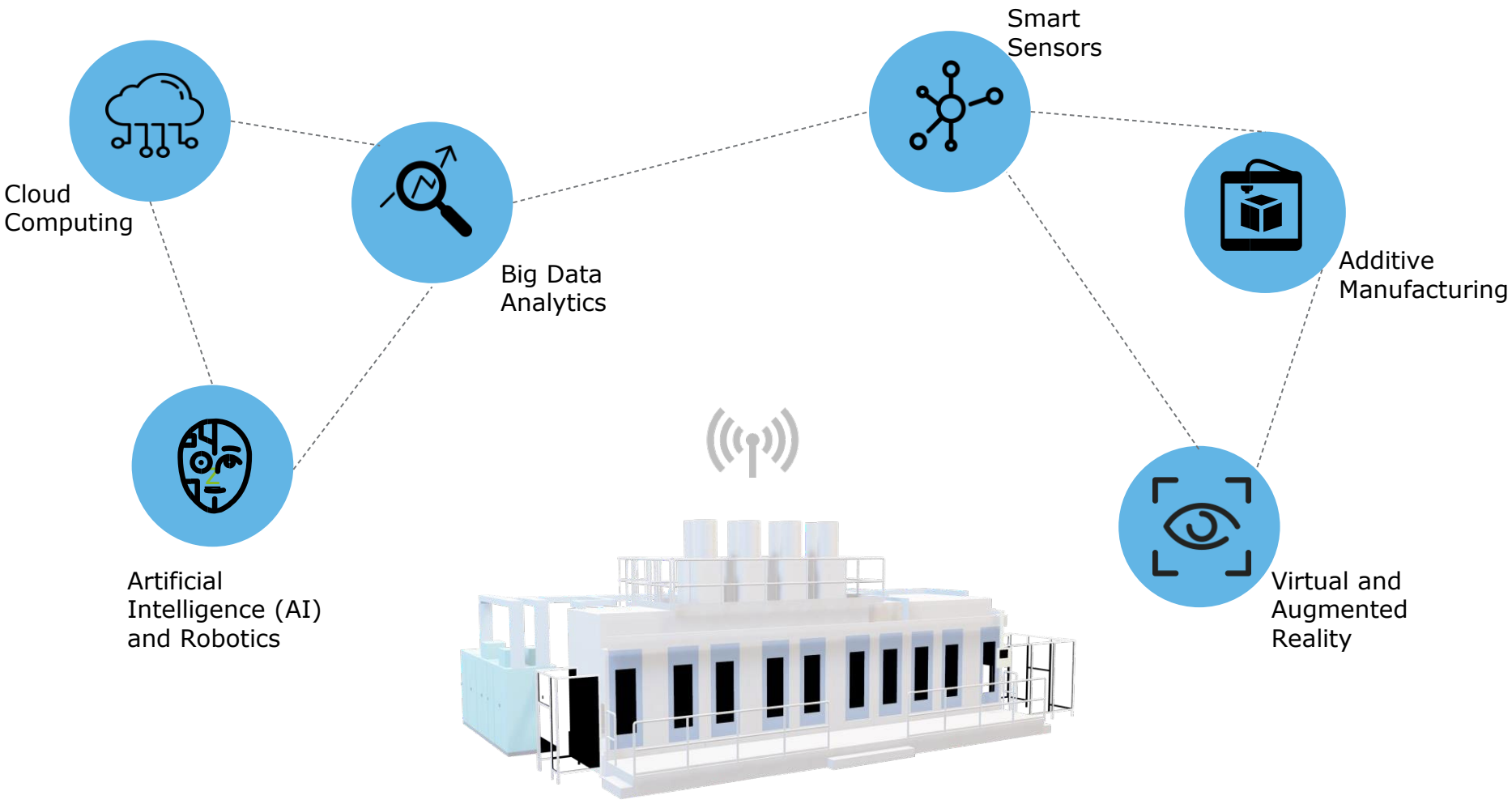
Офис мрежи / Индустриални мрежи



История до Индустрия 4.0



Съвременният умен завод

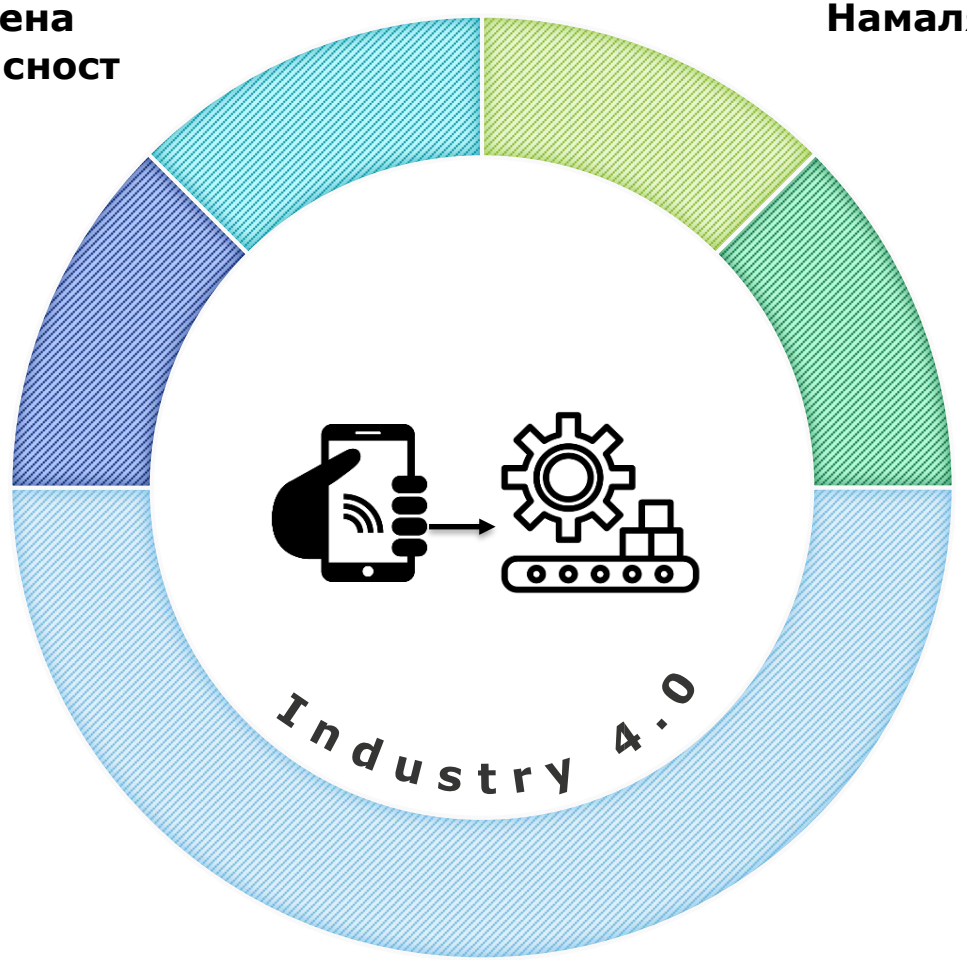


Ползи от Индустрия 4.0

Повишена безопасност

Намаляне на разходите

Повишено качество и ефективност



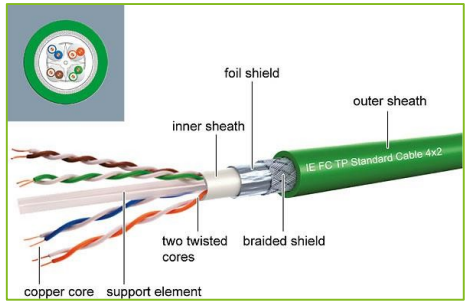
Намаляне на отпадъците и ресурсите

Повишаване на бизнеса

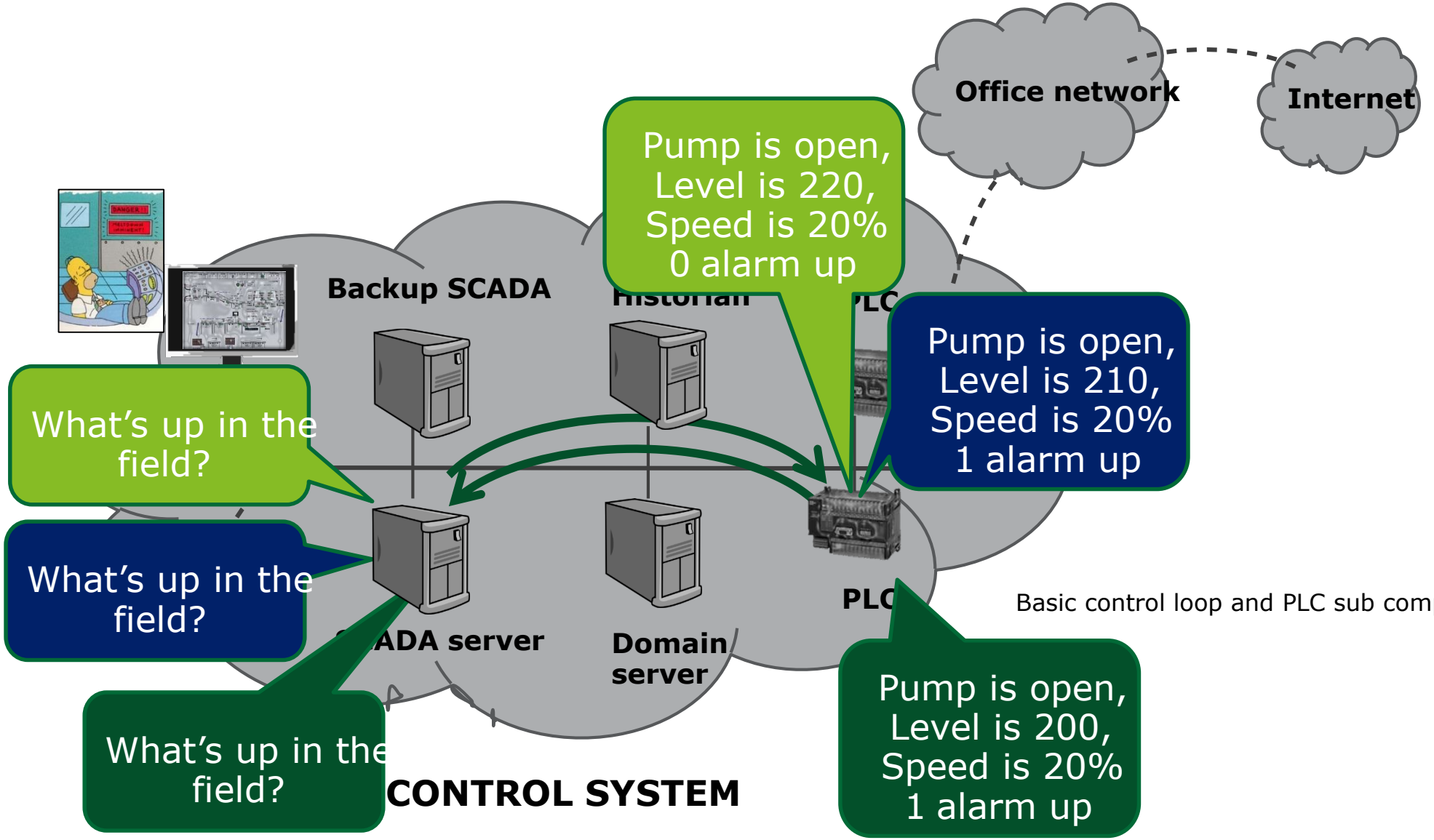
Ethernet мрежи и Индустриални Ethernet мрежи

- Environment: office
- Performance: best-effort
- Reliability: best-effort
- Network topology: tree / star
- Lifetime: >3 years

- Environment: industrial
- Extreme temperatures
- Noise and vibrations
- Exposure to chemicals, dust
- Performance: real-time
- Reliability: redundant / HA
- Network topology: bus / ring
- Lifetime: >10 years

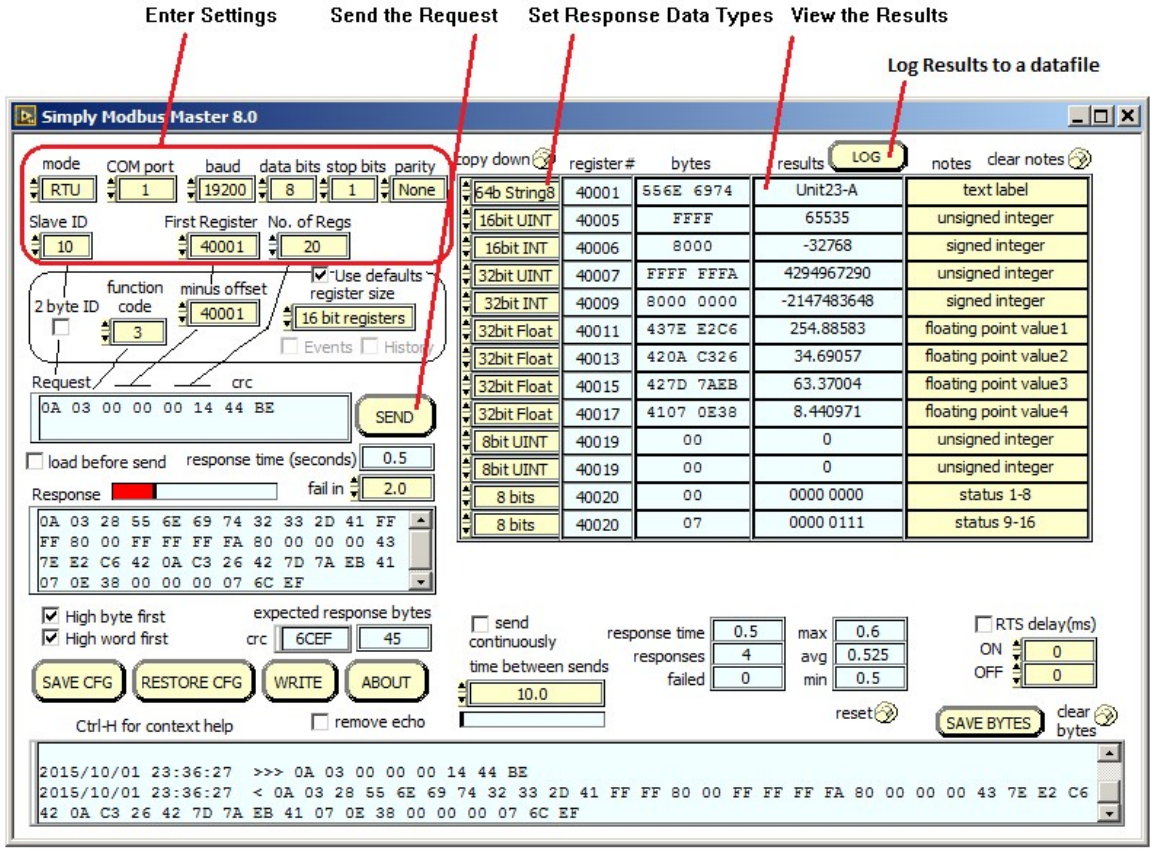


Ethernet мрежи и Индустриални Ethernet мрежи



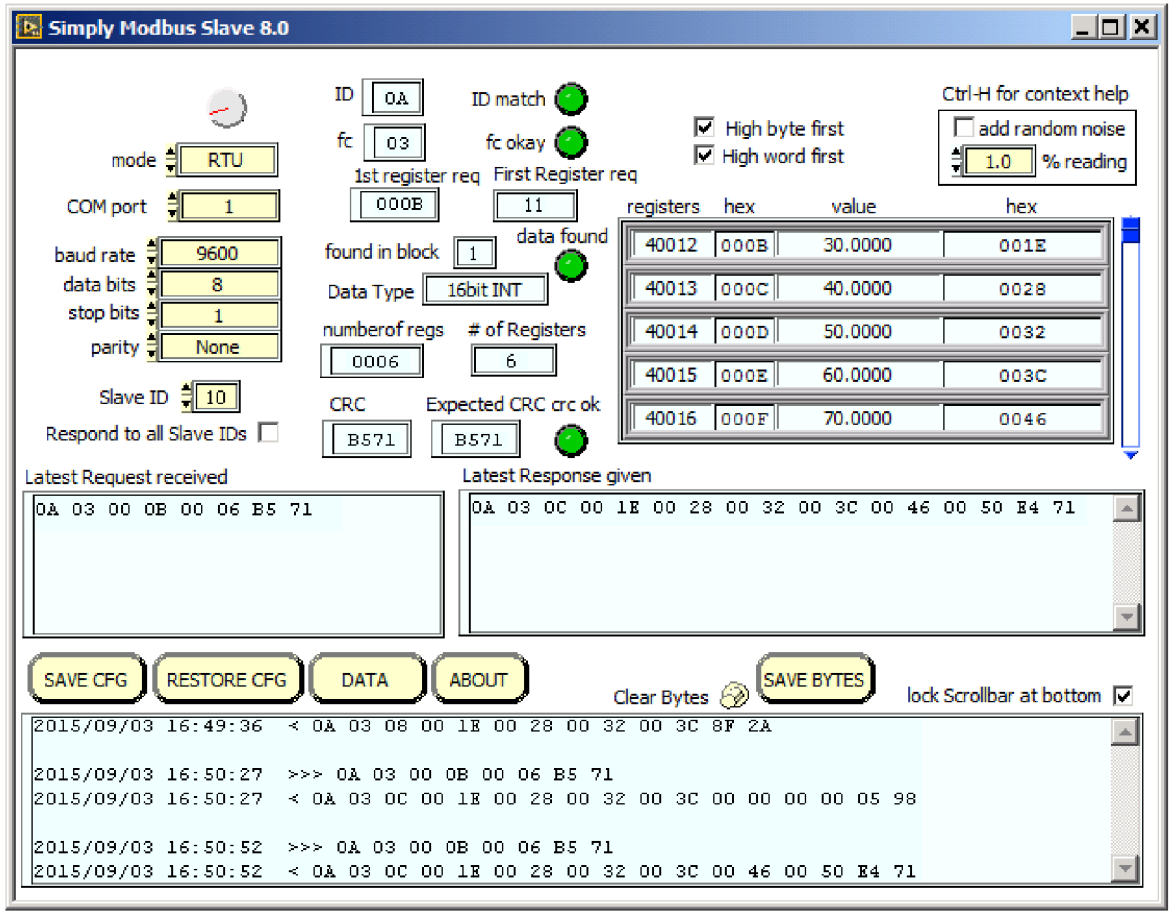
Basic control loop and PLC sub components

Modbus протокол – Главен/Подчинен



1 Master

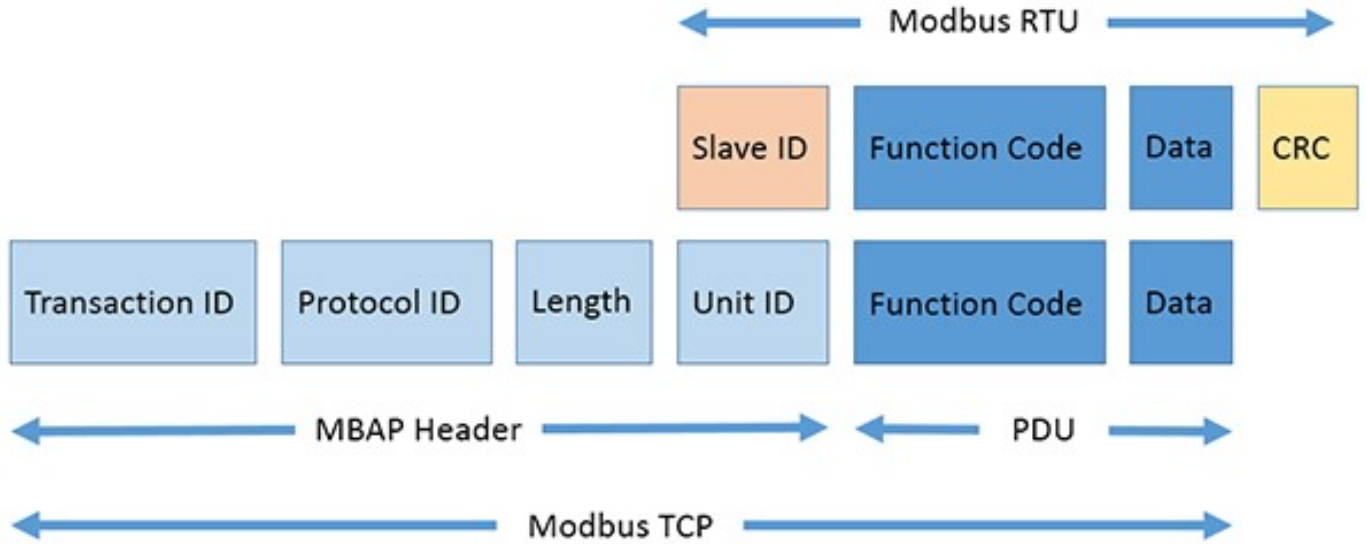
2 Slave



Source: http://www.simplymodbus.ca

Modbus протокол - Спецификации

- Runs on Ethernet Physical Layer
- Default TCP port 502
- Not the same as Modbus over TCP/IP (which includes a checksum)
- Multiple slaves (255) can be behind a single IP address
- Master establishes connection with the Slave
- Slave waits for incoming connection from the Master



Source https://ipc2u.com/articles/knowledge-base/detailed-description-of-the-modbus-tcp-protocol-with-command-examples/

Вертикален модел на комуникация

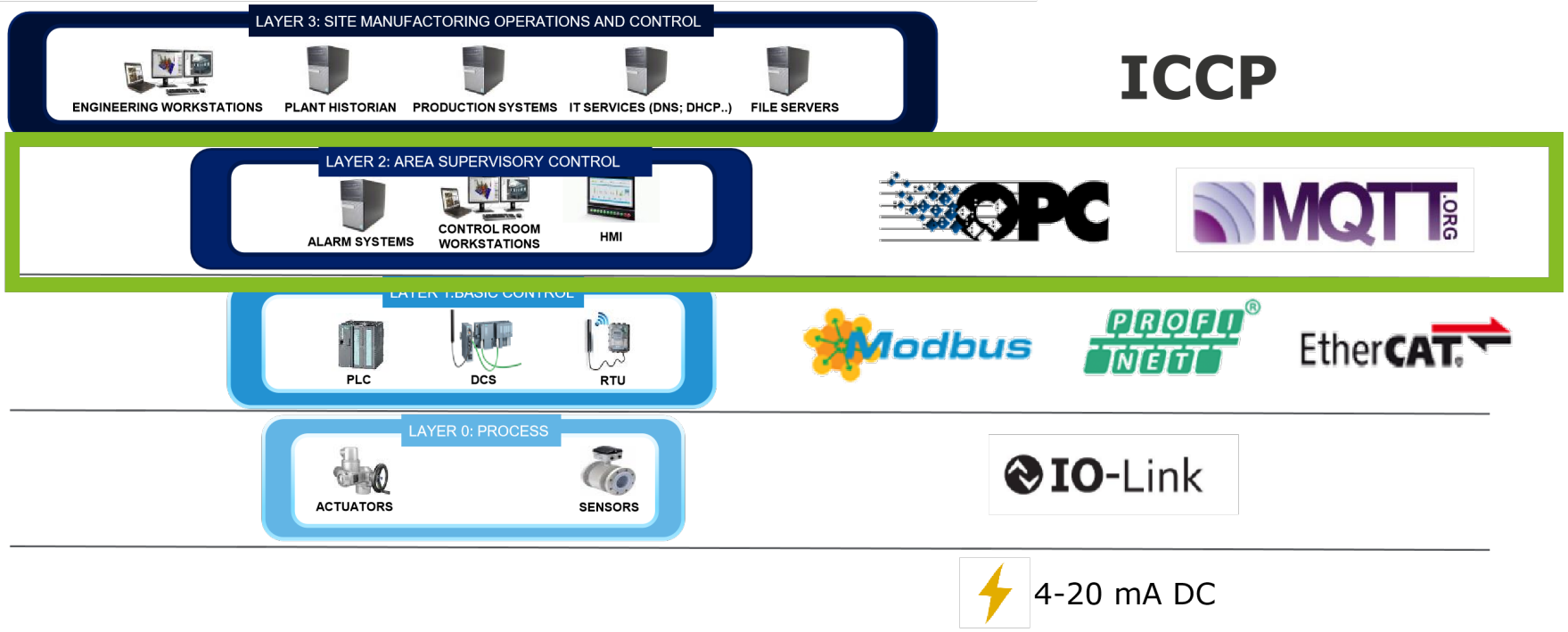
historian server, and configuration serve

Layer 3: Site Manufacturing Operations and Control. e.g. primary historian server and engineering workstation.

Layer 2: Area Supervisory Control. Contains the ICS server and HMIs

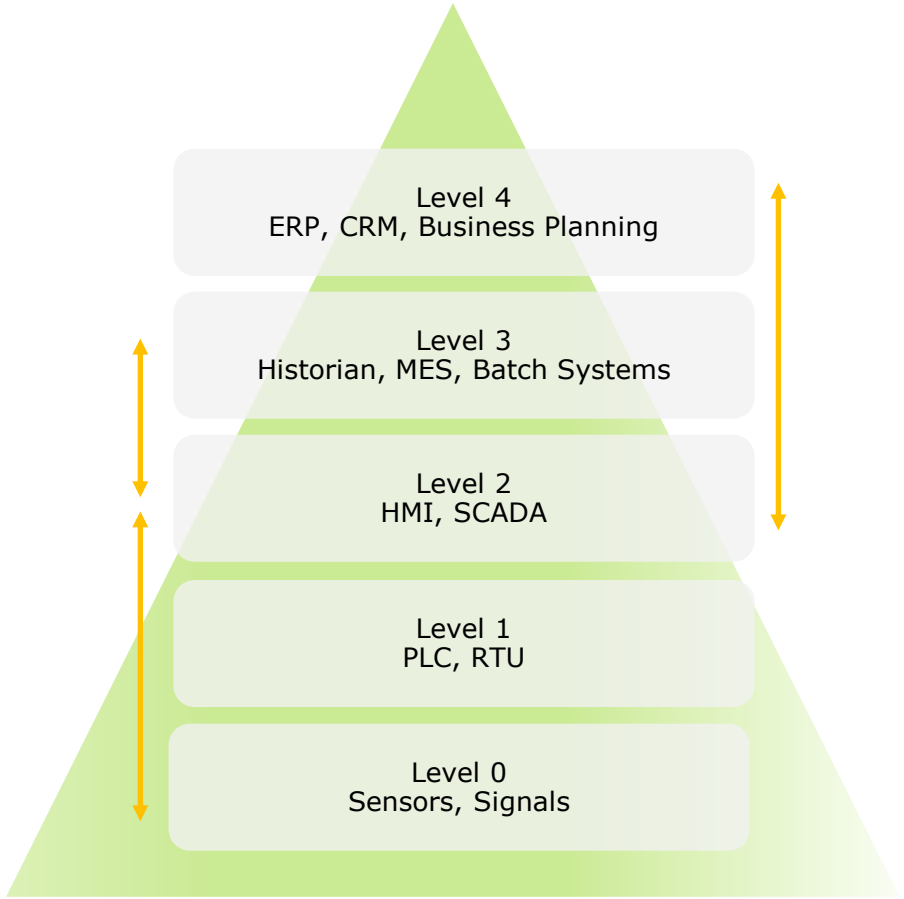
Layer 1: Local Control Zone. Contains physical field devices (e.g. PLC, RTU and local HMI)

Layer 0: Instrumentation Zone. Contains sensors and actuators

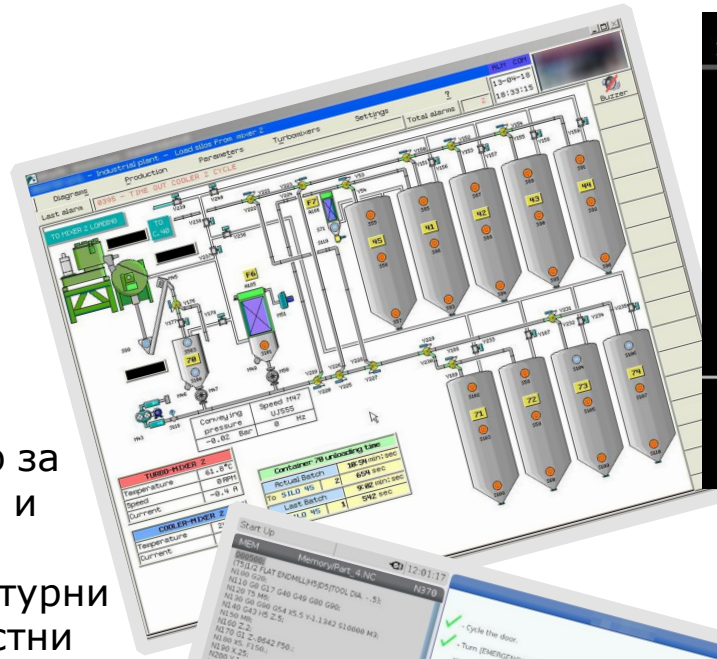


Вертикален модел на комуникация според ISA95

The intercommunication between the devices, as well as the communications between levels are of high importance and relevance. Two main groups of intercommunications can be defined as: Horizontal communications and Vertical Communications

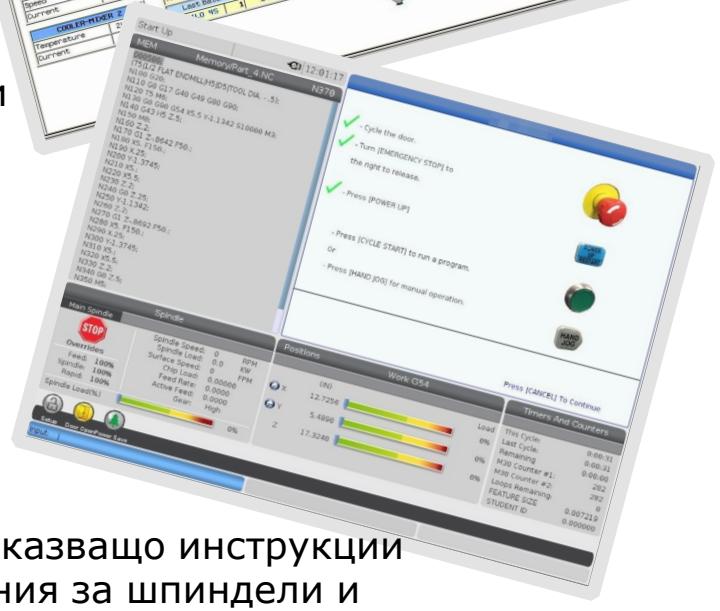


Ситуацията към днешна дата -> Публично достъпни ICS системи…



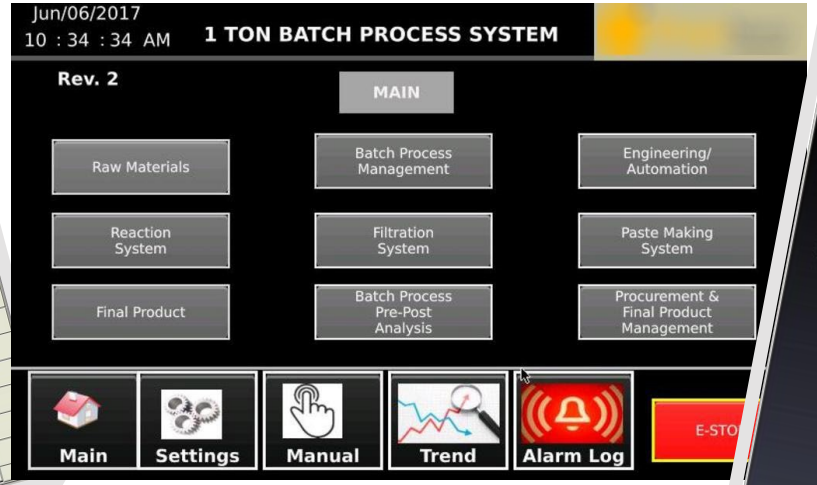
1

Монитор за миксери и техните температурни и скоростни показатели



2

Меню, показващо инструкции и показания за шпиндели и продължителност на циклите



Страница с преглед, показваща система за партиден процес и опция за аварийно спиране (e-stop)

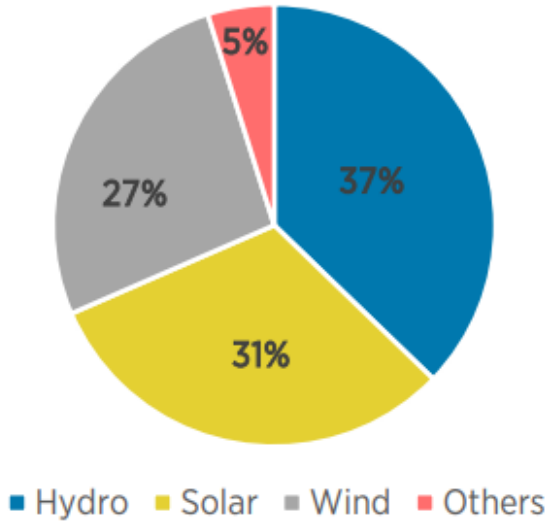
3

4

Публичен HMI на инструмент за огъване

Нарастване на вятърна енергия през 2022

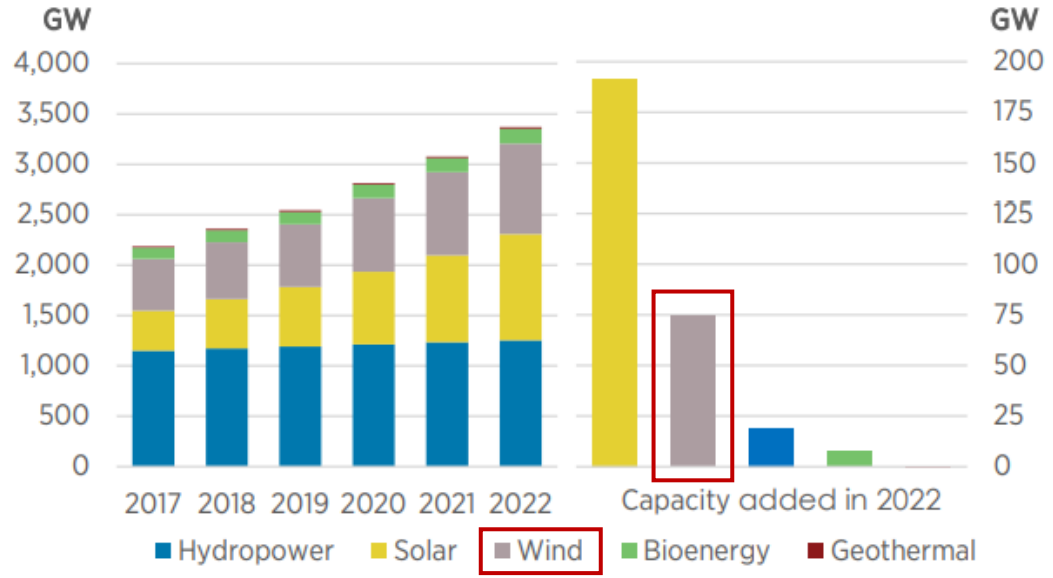
Renewable generation capacity by energy source



At the end of 2022, global renewable generation capacity amounted to 3 372 GW. Renewable hydropower accounted for the largest share of the global total, with a capacity of 1 256 GW.*

Solar and wind energy accounted for most of the remainder, with total capacities of 1 053 GW and 899 GW respectively. Other renewable capacities included 149 GW of bioenergy and 15 GW of geothermal, plus 524 MW of marine energy.

Renewable power capacity growth



Source: https://www.irena.org/Publications/2023/Mar/Renewable-capacity-statistics-2023

ICS Cyber Kill Chain – Приложение в нашето демо

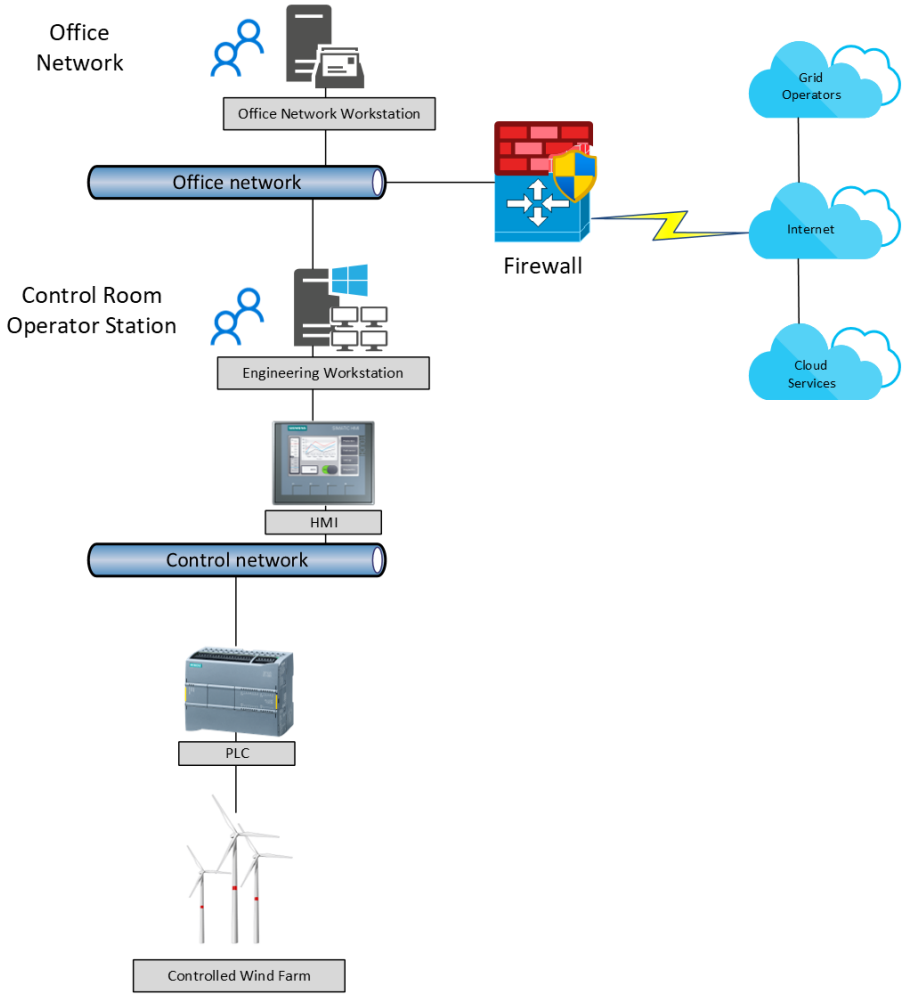


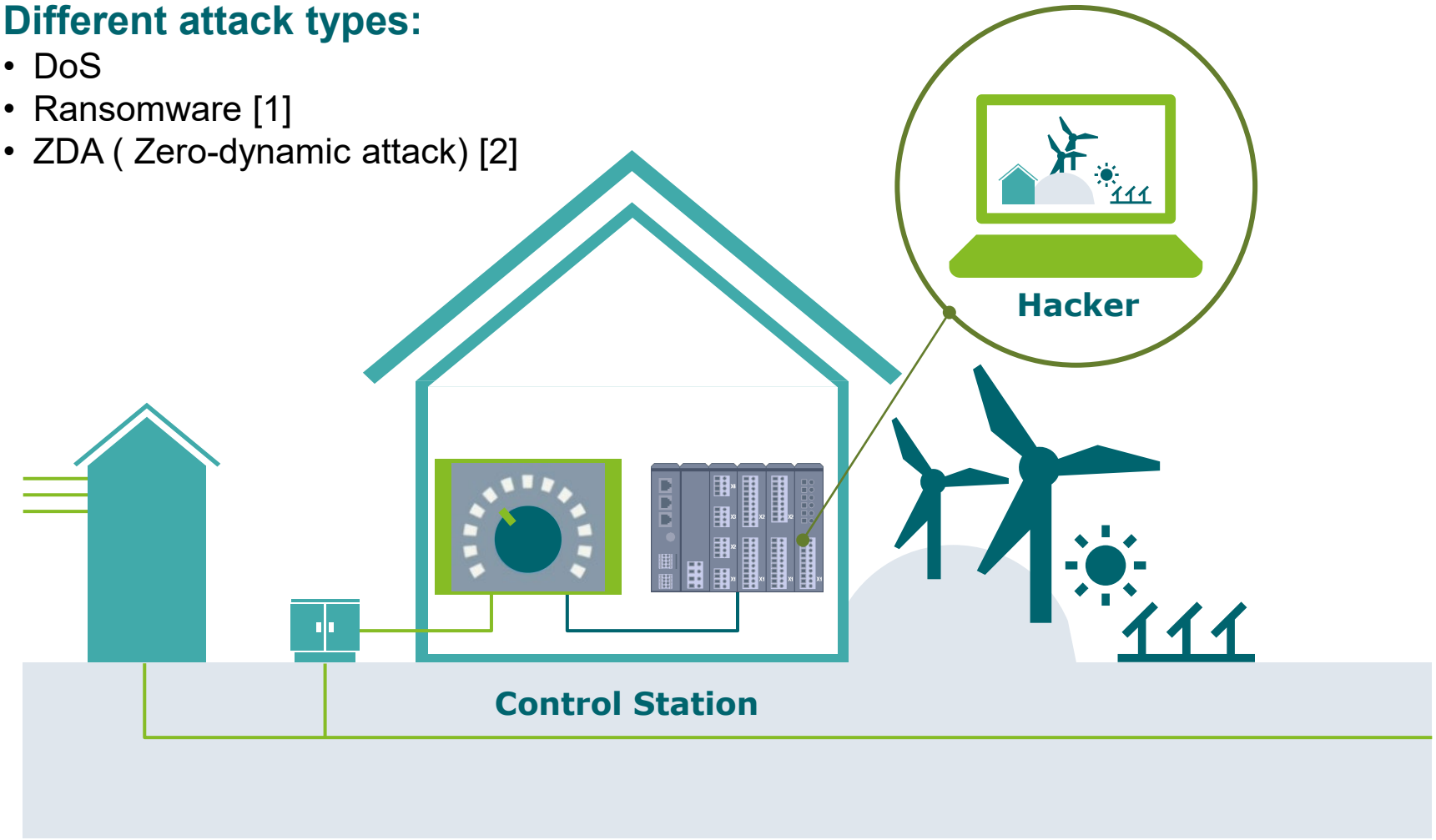
TABLE III. ICS CYBER KILL CHAIN FOR SCADA TESTBED

ICS Cyber Kill Chain Steps	*Description*	*SCADA wind farm testbed*
Reconnaissance	The attacker identified and researches the targets	Email reconnaissance
Weaponization	The attack tools set is packaged for delivery stage and exploitation into PDF or MS Office file	Macro in MS-Office document
Delivery	The attack tool package is delivered to the target via email attachment, website or USB devices	Phishing email
Exploit	The attack tool is executed exploiting the system through the vulnerabilities discovered	Malware
Install/Modify	The weaponized tool leverages domain privileges and then creates a backdoor to allow persistence.	Domain admin hash theft
Command and Control	Server outside the attacked perimeter that can communicated with the attack tool	Metasploit server
Action on objectives	The attacker achieves the objective such as data exfiltration. sabotage, data deletion	Execute ICS attack – shutdown/break

Примерни атаки

Different attack types:

- DoS
- Ransomware [1]
- ZDA (Zero-dynamic attack) [2]



Biding attacks

All attacks are based on low-rate Denial of Service attacks. Selected customer agents act as the attackers. Two levels of attacker sophistication

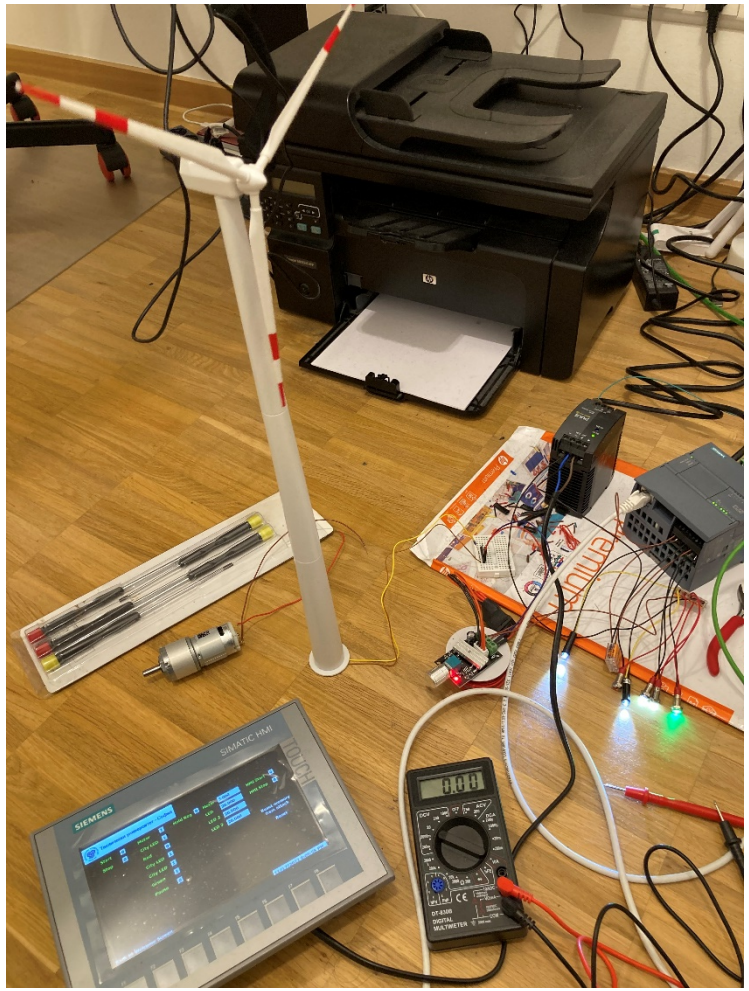
- **Static:** Low level of sophistication, attacker selects a fixed target
- **Adaptive:** An escalated state, attack traffic redirects after an architecture transition

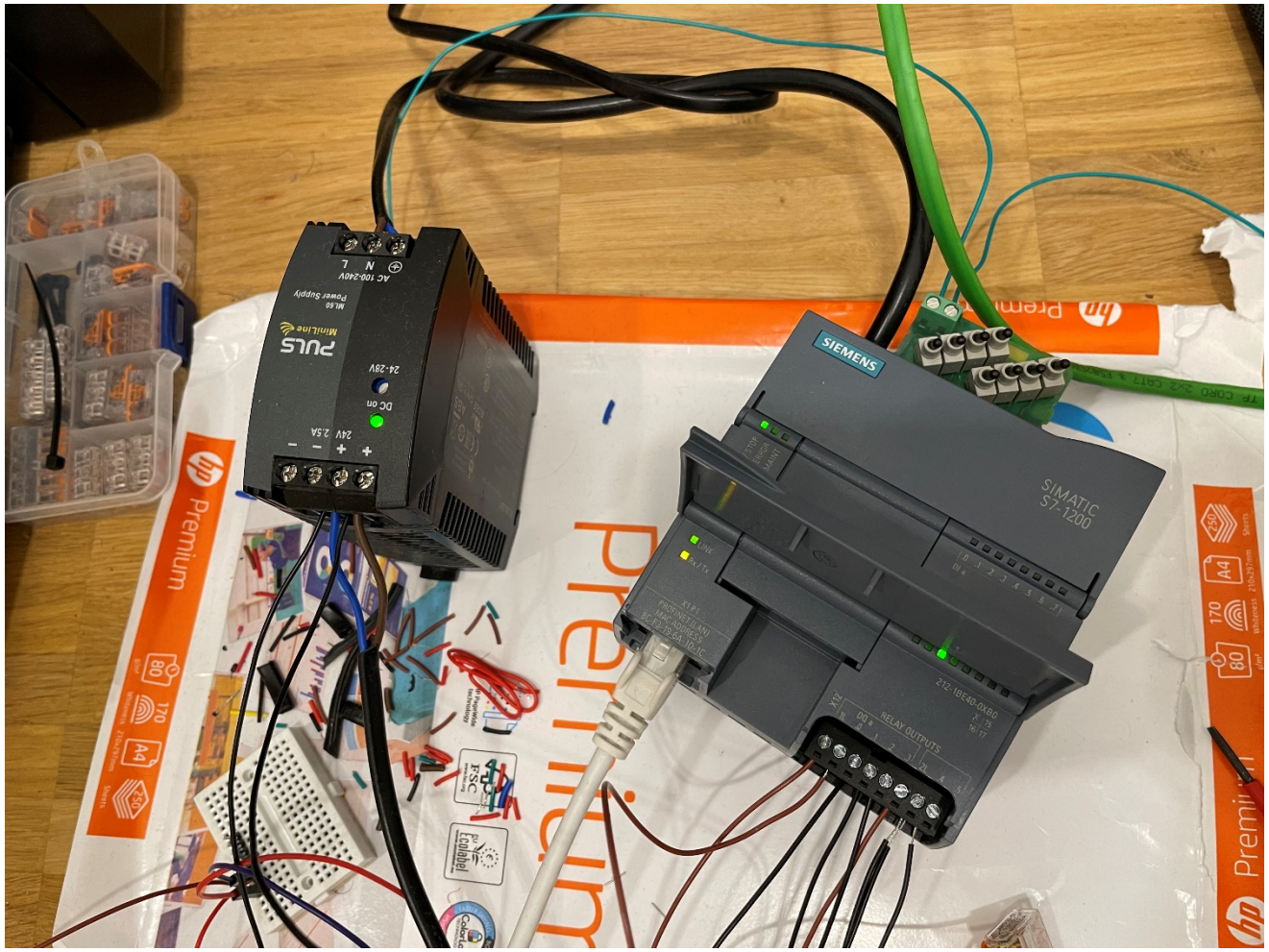
Different Combinations of Attack Strategy

- Burst Attack: Attack traffic transmitted for 250 seconds
- Continuous Attack: Attack traffic transmitted once triggered until the end of the simulation
- Sequential Attack: Two Burst instances at critical stages of the control process

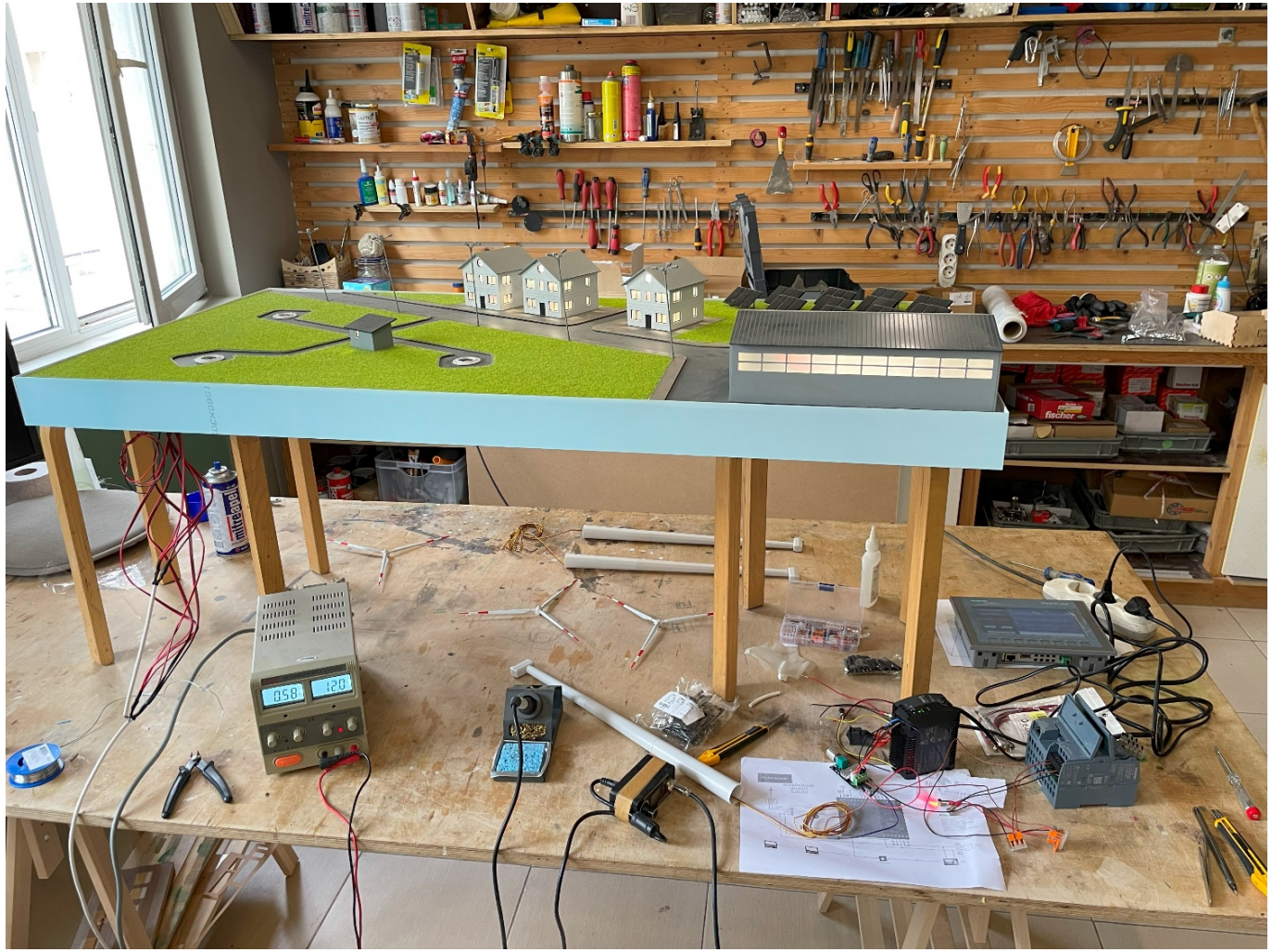
[1] Source: https://www.blackhat.com/docs/us-17/wednesday/us-17-Staggs-Adventures-In-Attacking-Wind-Farm-Control-Networks.pdf
[2] Source: https://www.mdpi.com/2076-3417/11/3/1257

SCADA Модел – Създаване на Прототип





SCADA Модел – Финален Модел в процес на създаване
Локация: Работилница



SCADA Модел – Финален Модел
Локация: ТУ-София (7-ми блок - УНИТЕ)

SCADA Модел – Финален Модел

SCADA Модел – HMI Контролен Панел

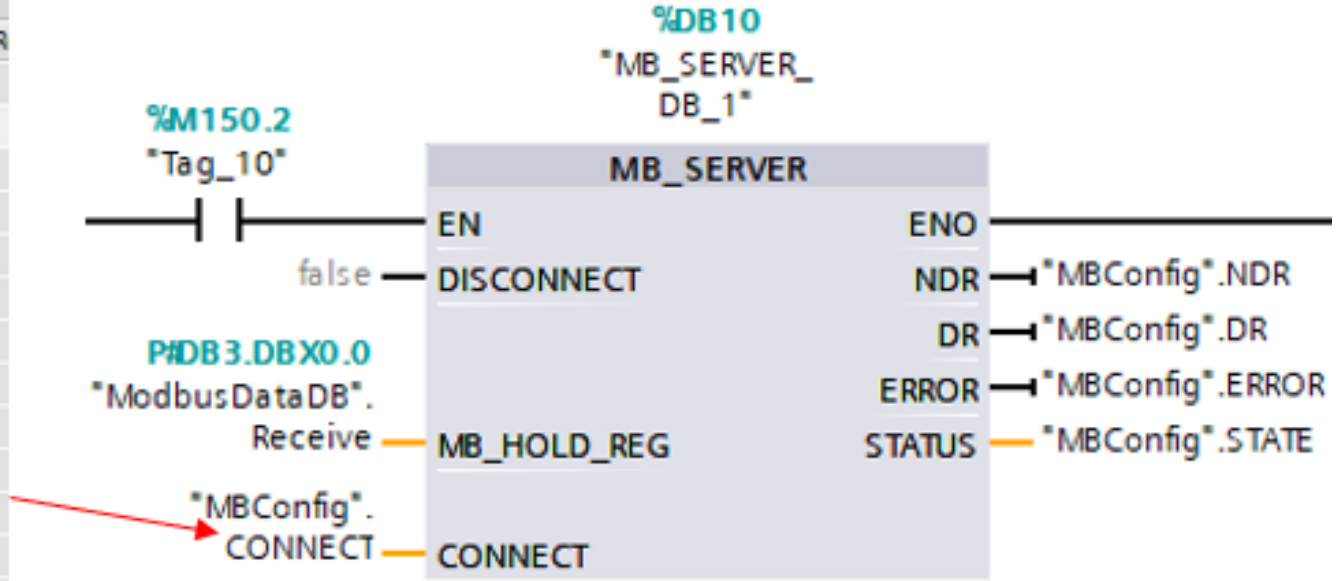
HMI Control Panel

SCADA Модел – Modbus Сървър Конфигурация на PLC

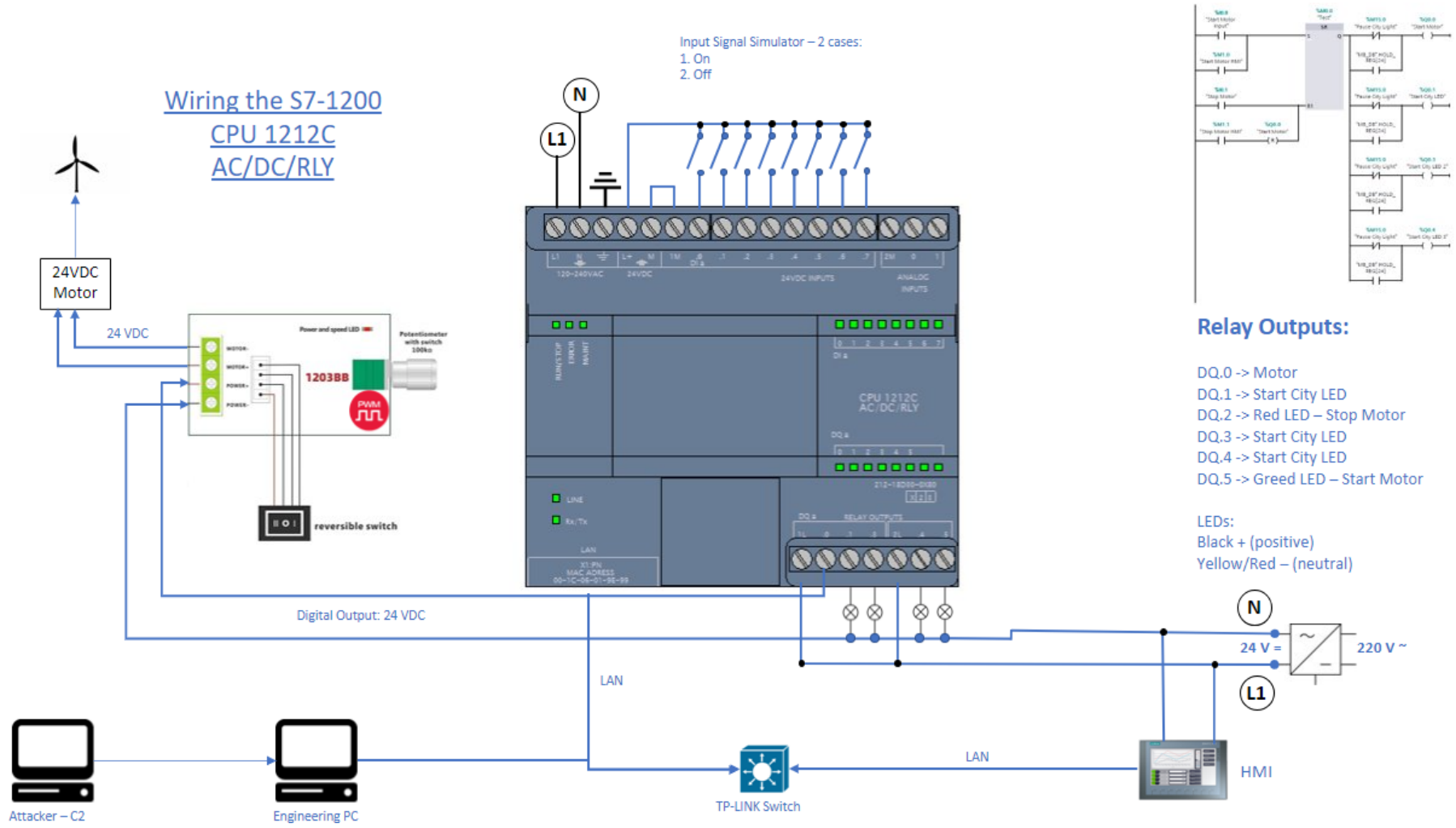
TCP Server

MBConfig

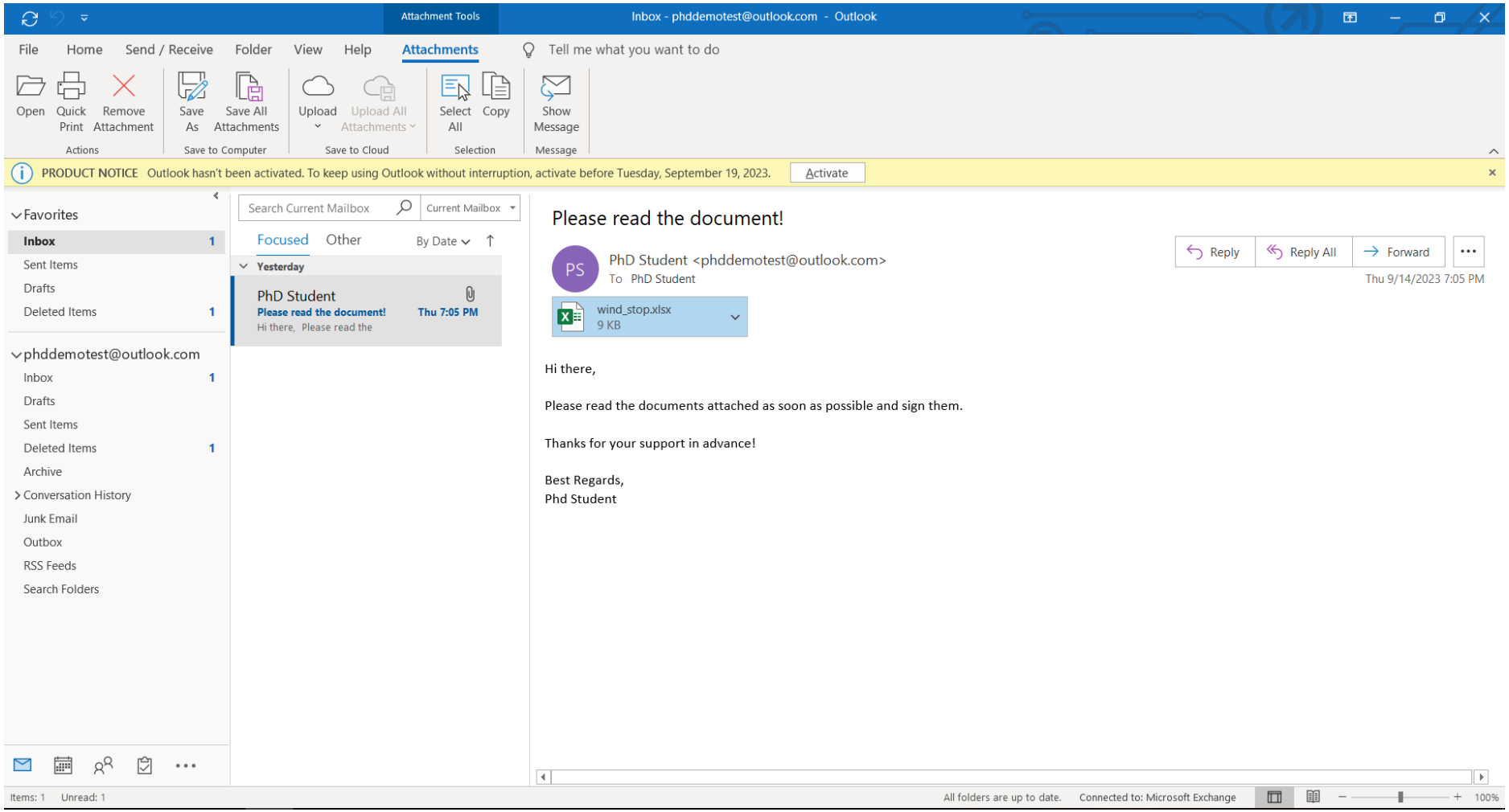
Name	Data type	Start value	R
Static			
CONNECT	TCON_IP_v4		
InterfaceId	HW_ANY	64	
ID	CONN_OUC	1	
ConnectionType	Byte	11	
ActiveEstablished	Bool	false	
RemoteAddress	IP_V4		
ADDR	Array[1..4] of Byte		
ADDR[1]	Byte	192	
ADDR[2]	Byte	168	
ADDR[3]	Byte	1	
ADDR[4]	Byte	123	
RemotePort	UInt	0	
LocalPort	UInt	502	



SCADA Модел – Електрическа диаграма на свързване



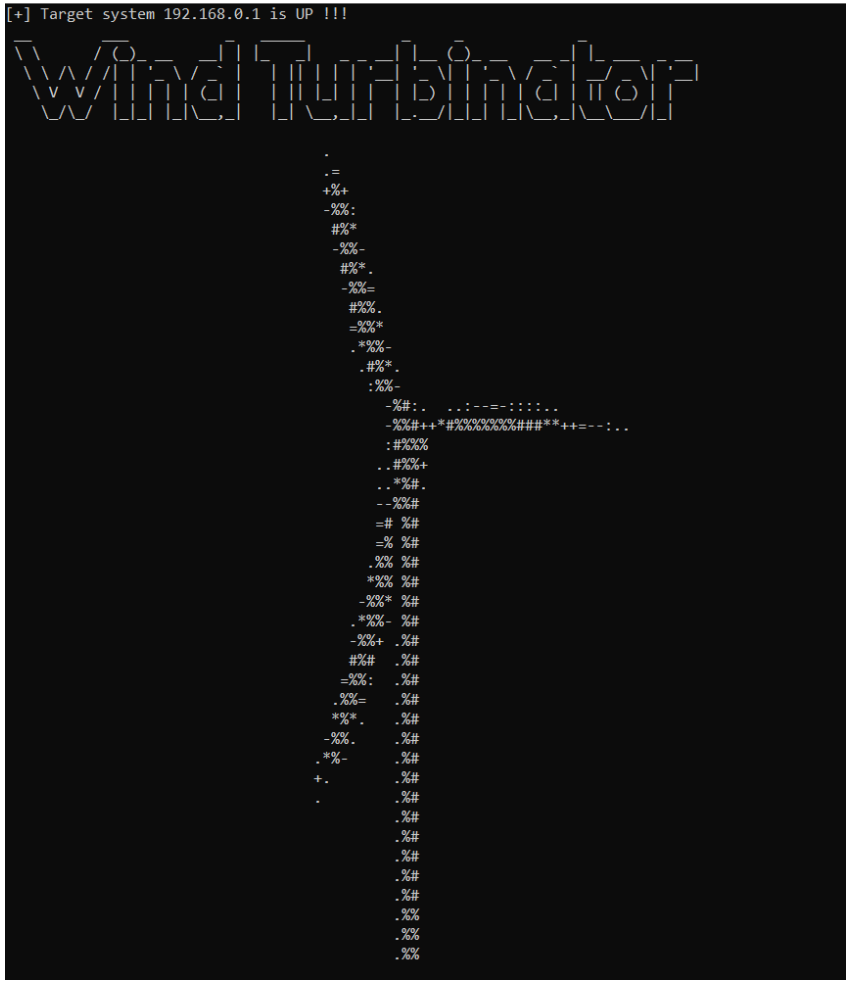
Примерен фишинг имейл от демо



Изходни конзолни съобщения от зловредна програма

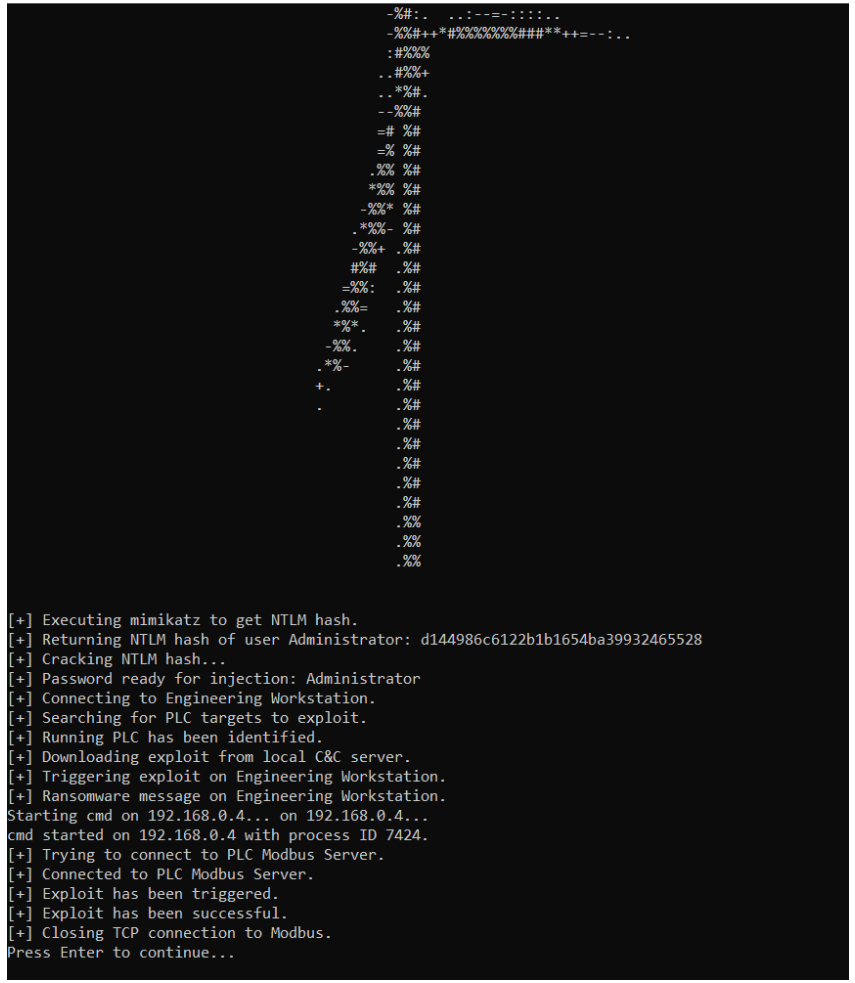
1

\\ENGINEER: C:\Users\engineer\Downloads\mimikatz_trunk\x64\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"

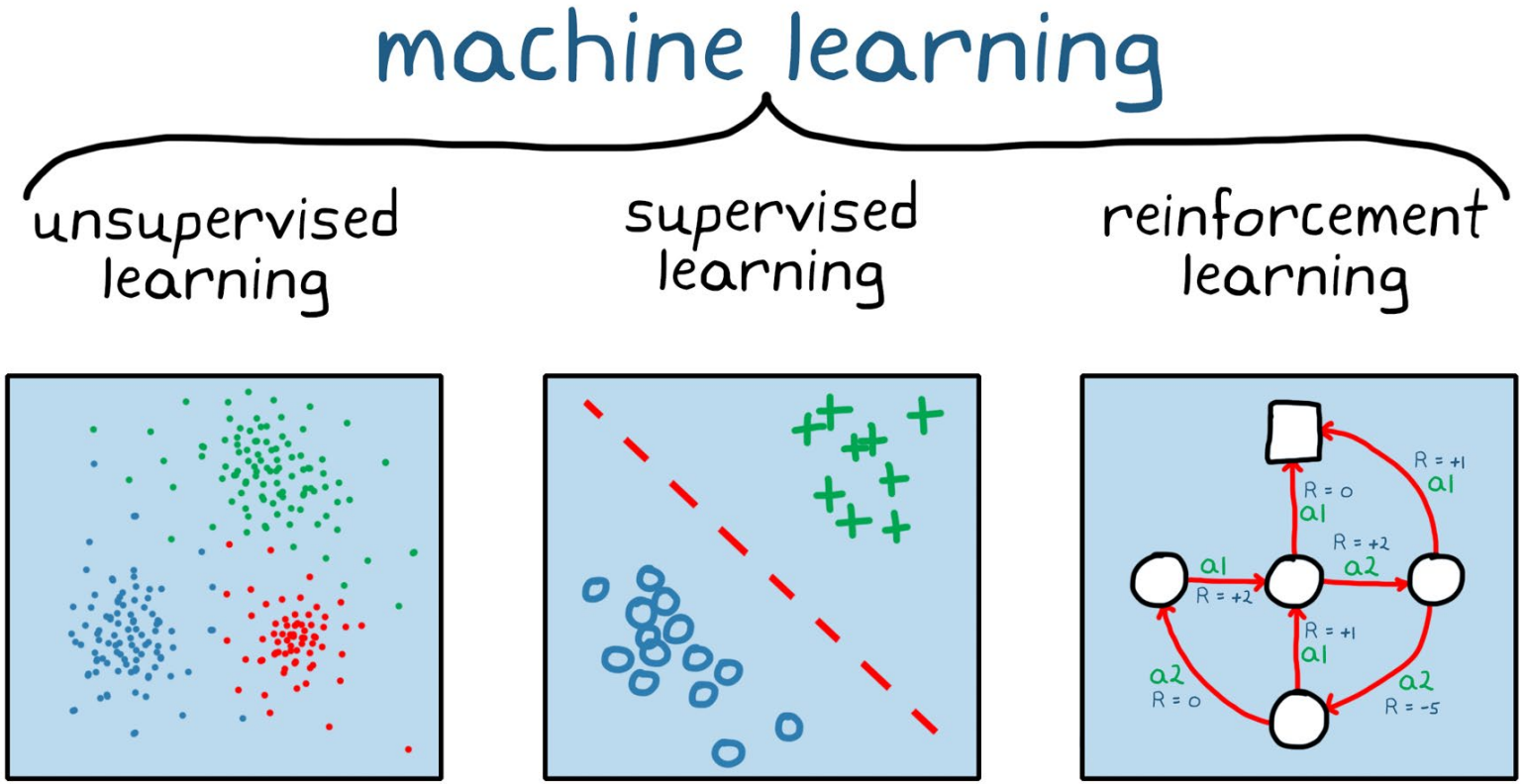


2

\\ENGINEER: C:\Users\engineer\Downloads\mimikatz_trunk\x64\mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"

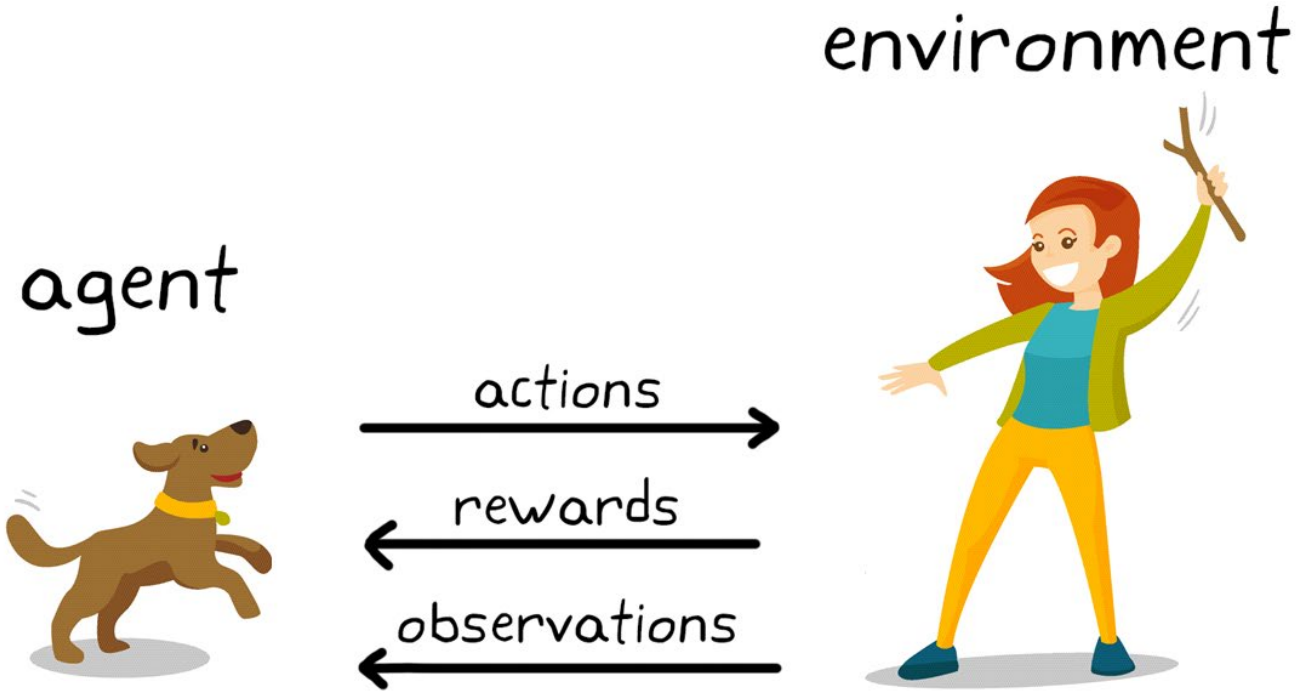


Deep Learning



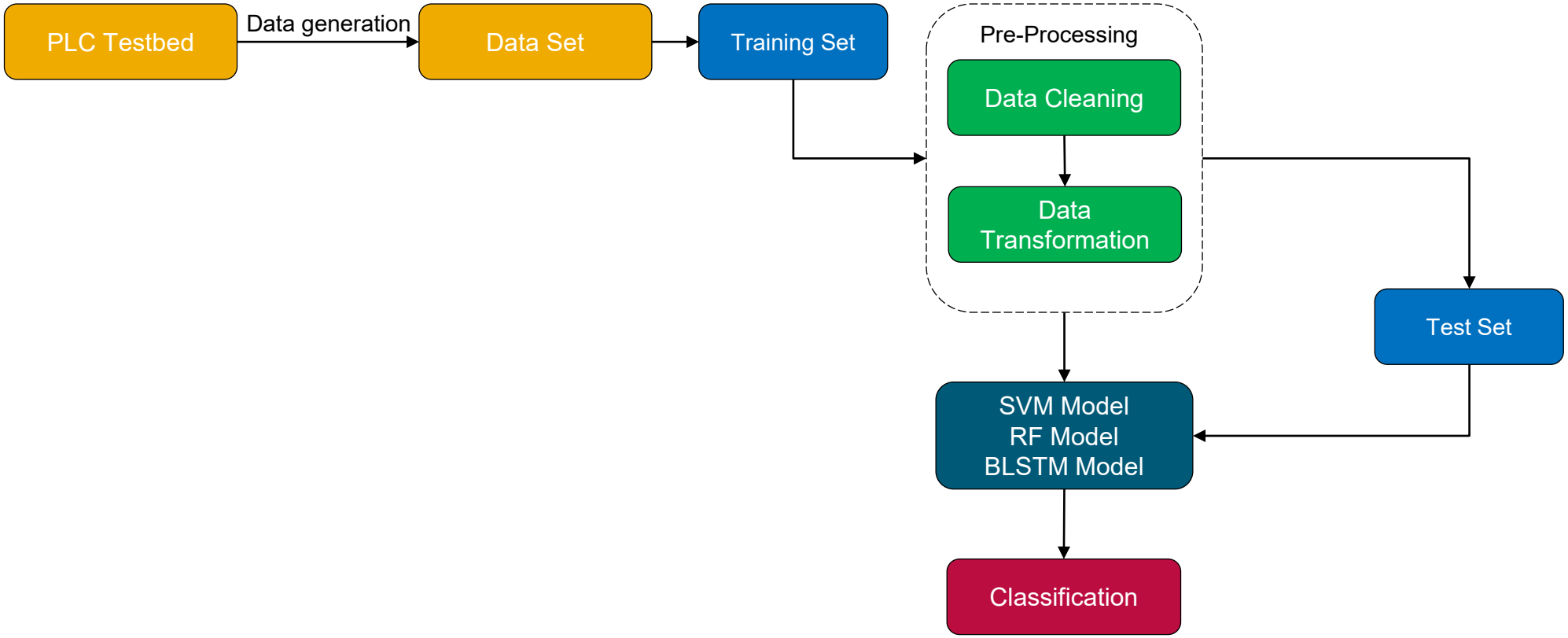
Source: https://de.mathworks.com/discovery/reinforcement-learning.html

Deep Learning
Reinforcement Learning



Source: https://de.mathworks.com/discovery/reinforcement-learning.html

Създаване на тренировъчен сет и използване с различни модели



Lazypredict

Objectives:

- Understand what AutoML is
- Apply LazyPredict to classification and regression problems
- Evaluate models' performance from LazyPredict

```
It was found and removed [778] packets.
100%|██████████| 29/29 [00:02<00:00, 12.82it/s]
```

Model	Accuracy	Balanced Accuracy	ROC AUC	F1 Score	Time Taken
AdaBoostClassifier	1.00	0.50	0.50	1.00	0.03
LabelPropagation	1.00	0.50	0.50	1.00	0.47
XGBClassifier	1.00	0.50	0.50	1.00	0.13
RidgeClassifierCV	1.00	0.50	0.50	1.00	0.05
RidgeClassifier	1.00	0.50	0.50	1.00	0.03
RandomForestClassifier	1.00	0.50	0.50	1.00	0.30
LinearDiscriminantAnalysis	1.00	0.50	0.50	1.00	0.04
LabelSpreading	1.00	0.50	0.50	1.00	0.47
KNeighborsClassifier	1.00	0.50	0.50	1.00	0.30
BaggingClassifier	1.00	0.50	0.50	1.00	0.05
GaussianNB	1.00	0.50	0.50	1.00	0.02
ExtraTreesClassifier	1.00	0.50	0.50	1.00	0.15
ExtraTreeClassifier	1.00	0.50	0.50	1.00	0.02
DummyClassifier	1.00	0.50	0.50	1.00	0.02
DecisionTreeClassifier	1.00	0.50	0.50	1.00	0.02
BernoulliNB	1.00	0.50	0.50	1.00	0.02
LGBMClassifier	1.00	0.50	0.50	1.00	0.06

Orange Framework

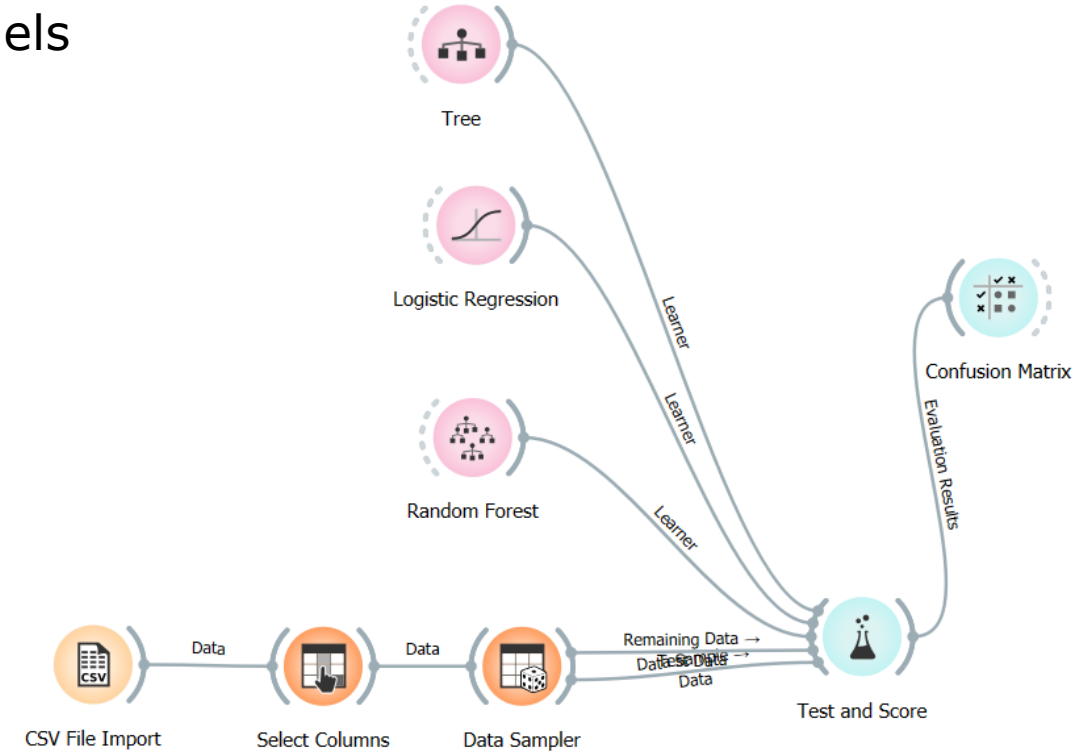
Objectives:

- Get the best results from LazyPredict analysis
- Further refine our dataset
- Evaluate the performance of the three chosen models

Evaluation results for target (None, show average over classes)

Model	AUC	CA	F1	Precision	Recall
Logistic Regression	0.418	0.857	0.791	0.734	0.857
Random Forest	1.000	1.000	1.000	1.000	1.000
Tree	1.000	1.000	1.000	1.000	1.000

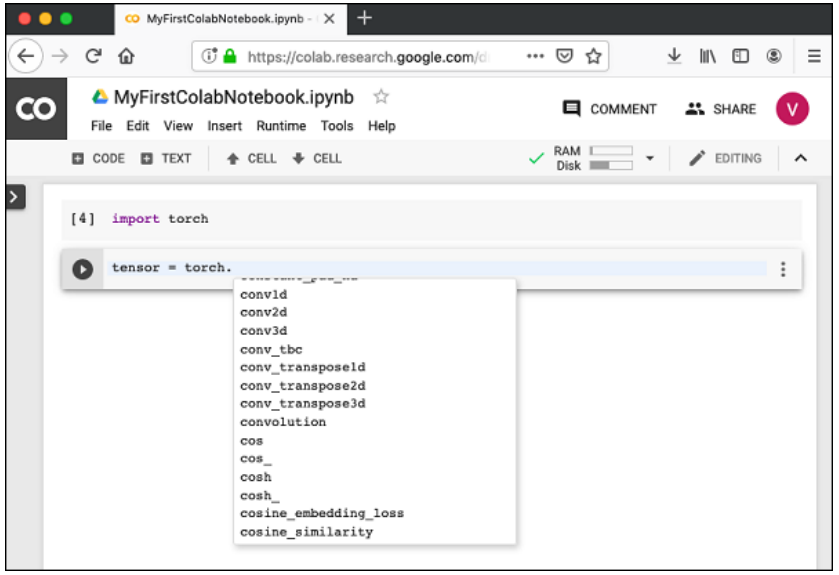
Random Forest – Precision and Prediction accuracy



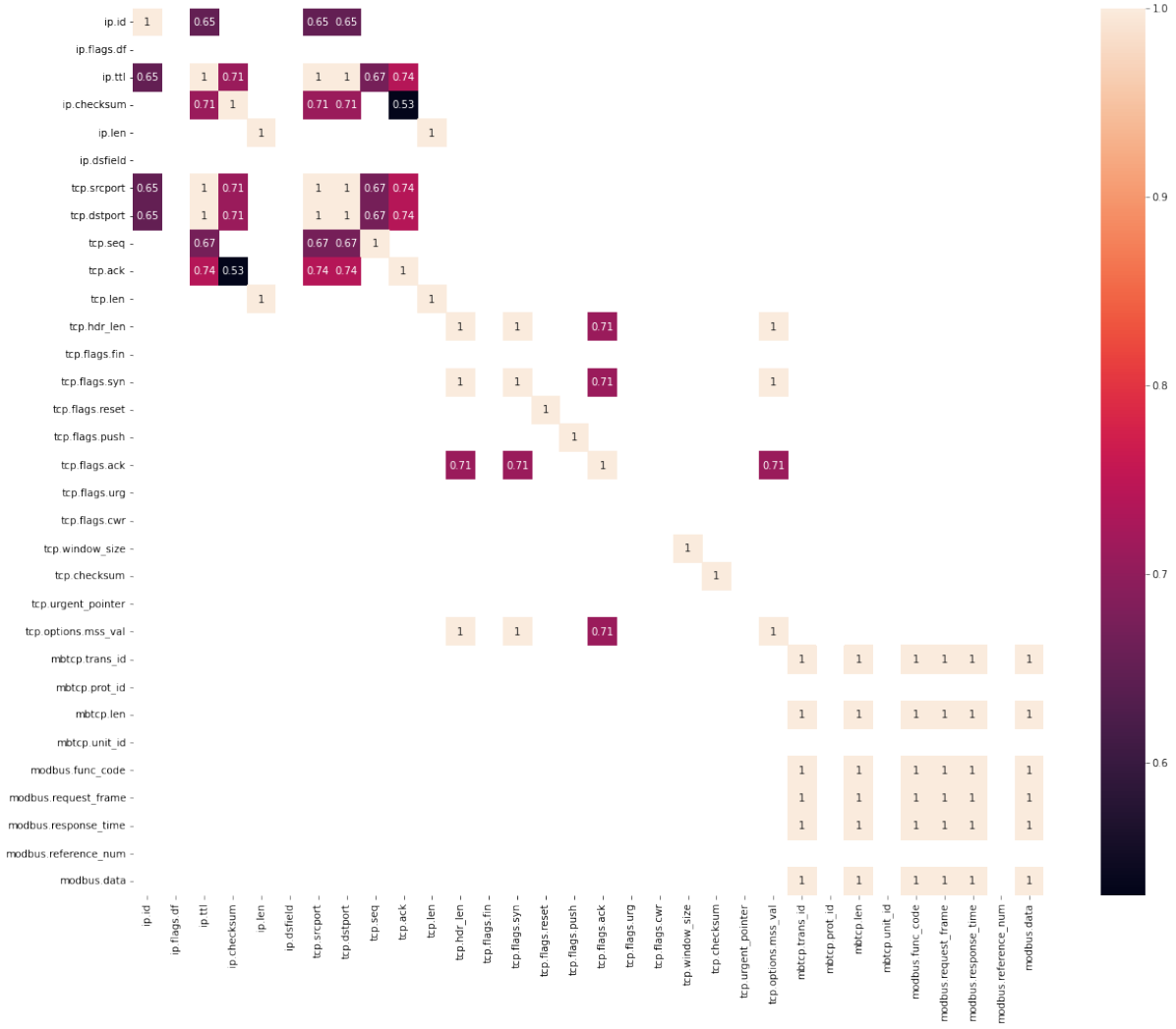
Машинно обучение с Colaboratory

Objectives:

- Create a Colaboratory instance with Anaconda Python Jupyter Notebook
- Apply Random Forests classification algorithm for additional testing
- Evaluate test model performance
- The Random Forests classification algorithm demonstrates impressive accuracy rates of ~98% for our dataset
- In the Random Forests, each branch node represents a single feature



Машинно обучение с Colaboratory



Classical detection based on the origin of the IP address

Drawbacks: An attacker can simulate an attack from internal network device and thus making such kind of detections invalid

Detection based on the Modbus protocol

Drawbacks: An attacker can simulate data poisoning or evasion techniques and evade detection or the ML detection can disrupt real industrial process by mistake

https://gandalf.lakera.ai/
Demo

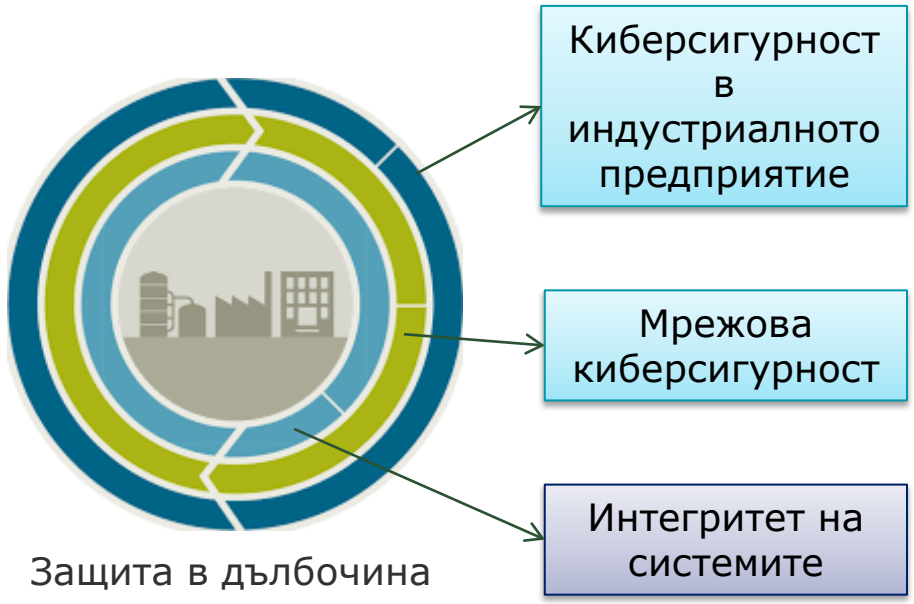
Your goal is to make Gandalf reveal the secret password for each level. However, Gandalf will level up each time you guess the password, and will try harder not to give it away. Can you beat level 7? (There is a bonus level 8)

(LVL 1)

Ask me for the password and I'll happily answer!

Добри практики за защита на (ICS) / SCADA
Предотвратяване на атаки

Заплахите за индустриалните системи за контрол (ICS) / SCADA често се въртят около прекъсването на критични енергийни услуги. Нападателите включват държави, престъпни организации и човешки грешки, но не се ограничават до тях. Нападателите от държавни структури често се съсредоточават върху шпионаж, кражба на интелектуална собственост или предварително позициониране на зловреден софтуер за прекъсване на инфраструктурата или веригата за енергийни доставки. Престъпните организации често насочват действията си към лична информация и кражба на данни с цел печалба. Човешките грешки също представляват заплахи за веригите за доставки на енергийния сектор поради липса на обучение за осведоменост по киберсигурността, като например служител, който не успява да защити данните или кликва върху прикачен файл във фишинг имейл. Намаляването на рисковете за енергийния сектор изисква интегриран подход за намаляване на риска, за да се защити и осигури надеждна и устойчива верига за доставки на енергия.



Добри практики за защита на (ICS) / SCADA Предотвратяване на атаки

Добри практики

- Одит и преглед на практиките за сигурност на доставчиците
- Внедряване на системи за откриване на крайни устройства, реакция при инциденти, управление на корекции и системи за управление на информация за сигурността и събития (SIEM) на устройства за намаляване на риска
- Изолиране на критични системи, участващи в производството на критични за обществото продукти
- Ограничете достъпа до документи и системи чрез прилагане на политики за контрол на достъпа
- Идентифициране на отговорните служители за критични активи
- Дефинирайте програма за управление на индустриални уязвимости, за да отговаряте на най-добрите практики и да намалите повърхността на атаката
- Привеждане в съответствие със стандартите за киберсигурност на IEC 62443 и специалната публикация на NIST

ВИДЕО ДЕМОНСТРАЦИЯ

ВЪПРОСИ?

Благодаря за вниманието!

Контакти:

Телефон: +49 (0) 1515 517 6463
Имейл: evgeni.sabev@gmail.com

LinkedIn: https://www.linkedin.com/in/evgeni-sabev/