Nebras

CyberSecurityExpert

OT Cybersecurity

Fundamentals

Nebras
CyberSecurityExpert

Introduction to OT

Introduction to OT Cybersecurity - Part 1

Contents

Process Logic Cycle

Sensors / Actuators

Safety Instrumented System

Tags

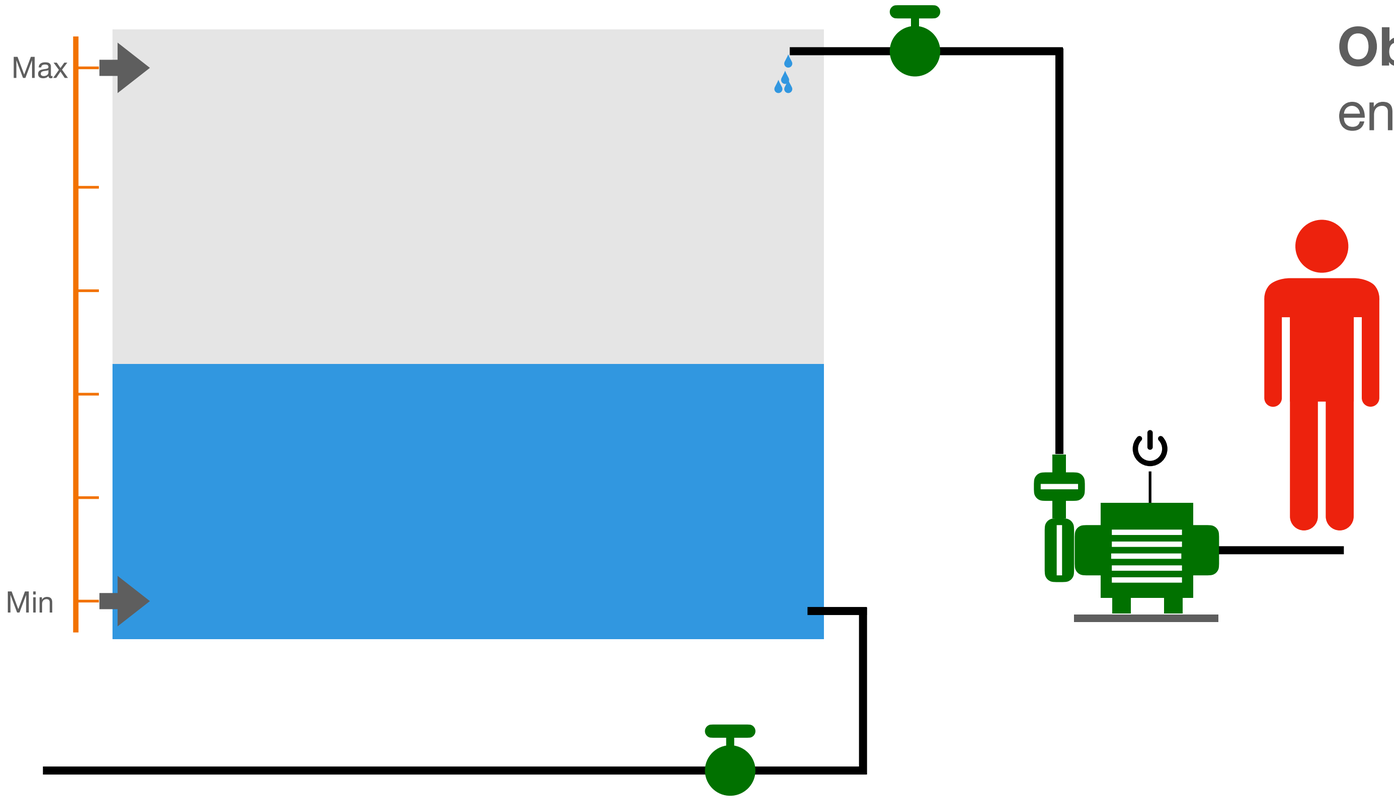
Data Historian

Maintenance

Nebras
CyberSecurityExpert

Plant Watering Example

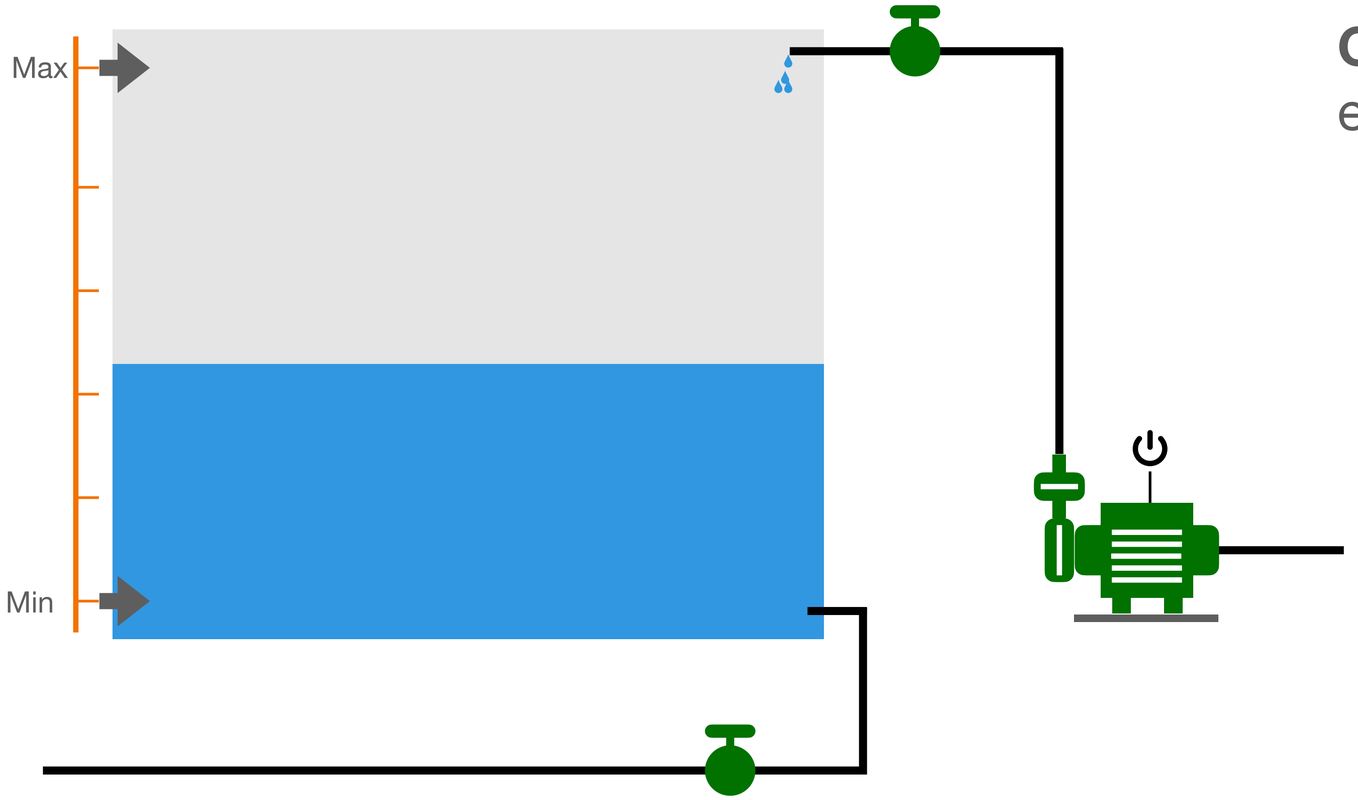
Nebras
CyberSecurityExpert



Objective: We need to have enough water supply.

Components:
- Water tank
- Water Pump
- Pipes
- Valves
- Level of water
- Power On/Off
- Water

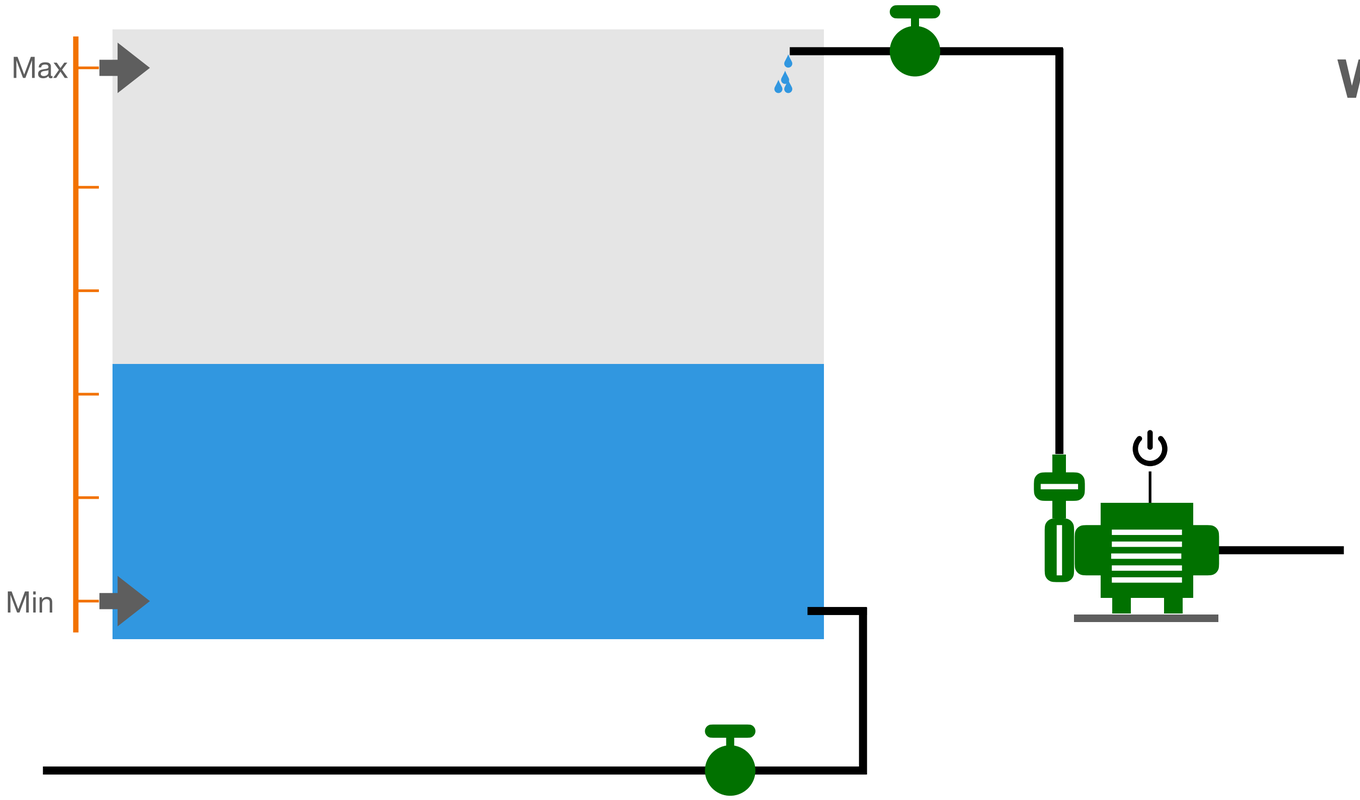
Nebras
CyberSecurityExpert



Objective: We need to have enough water supply.

Components:
- Water tank
- Water Pump
- Pipes
- Valves
- Level of water
- Power On/Off
- Water

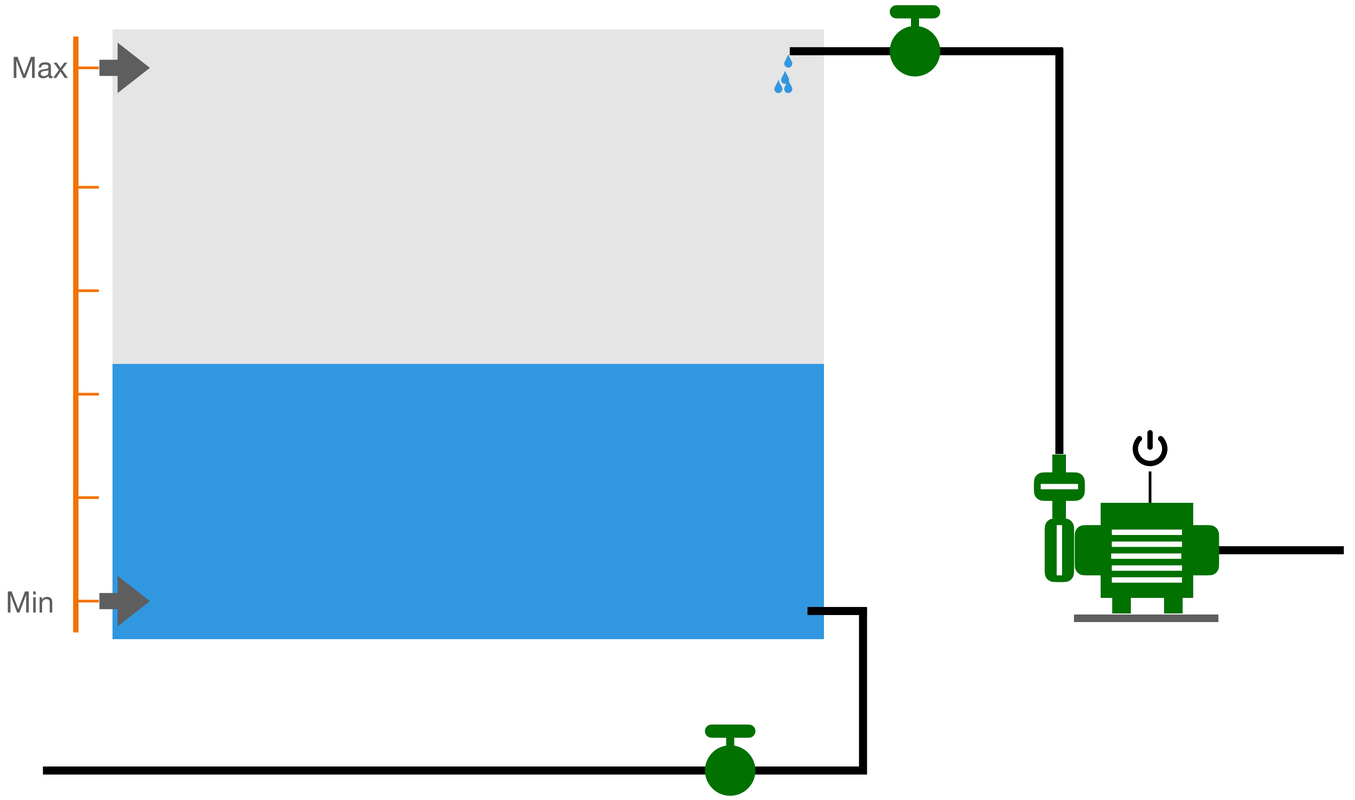
Nebras
CyberSecurityExpert



What can be automated?

Objective: less manual work!

Nebras
CyberSecurityExpert



Active components

- Water Pump
- Valves
- Level of water
- Power On/Off

Passive components

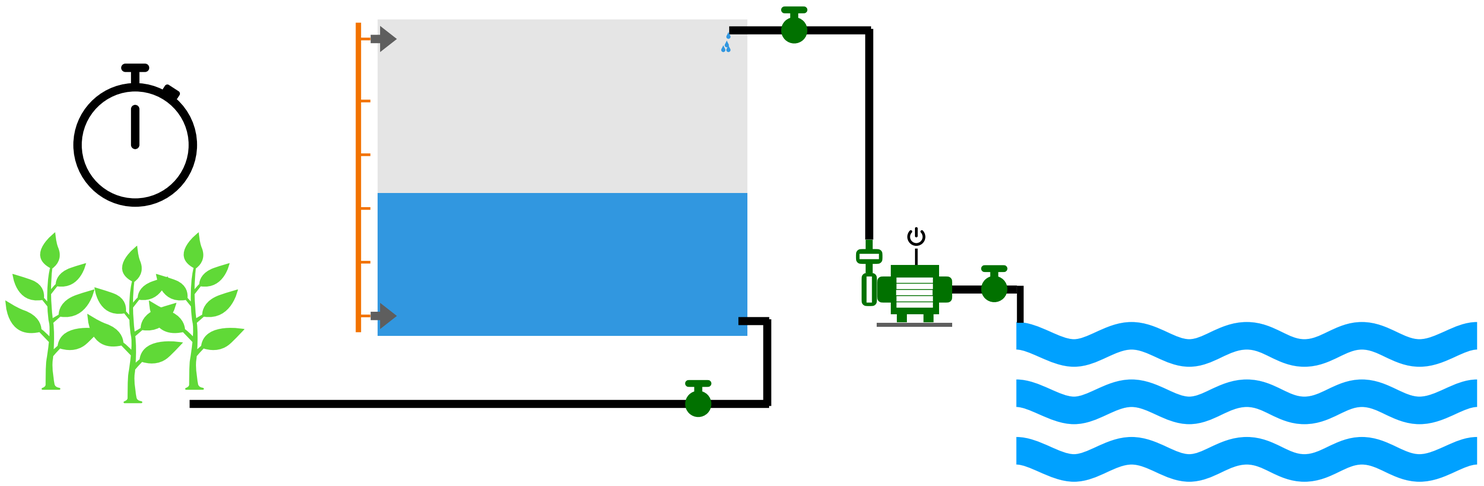
- Water
- Pipes
- Tank

Nebras
CyberSecurityExpert

Plant watering

Water Storage

Water Source

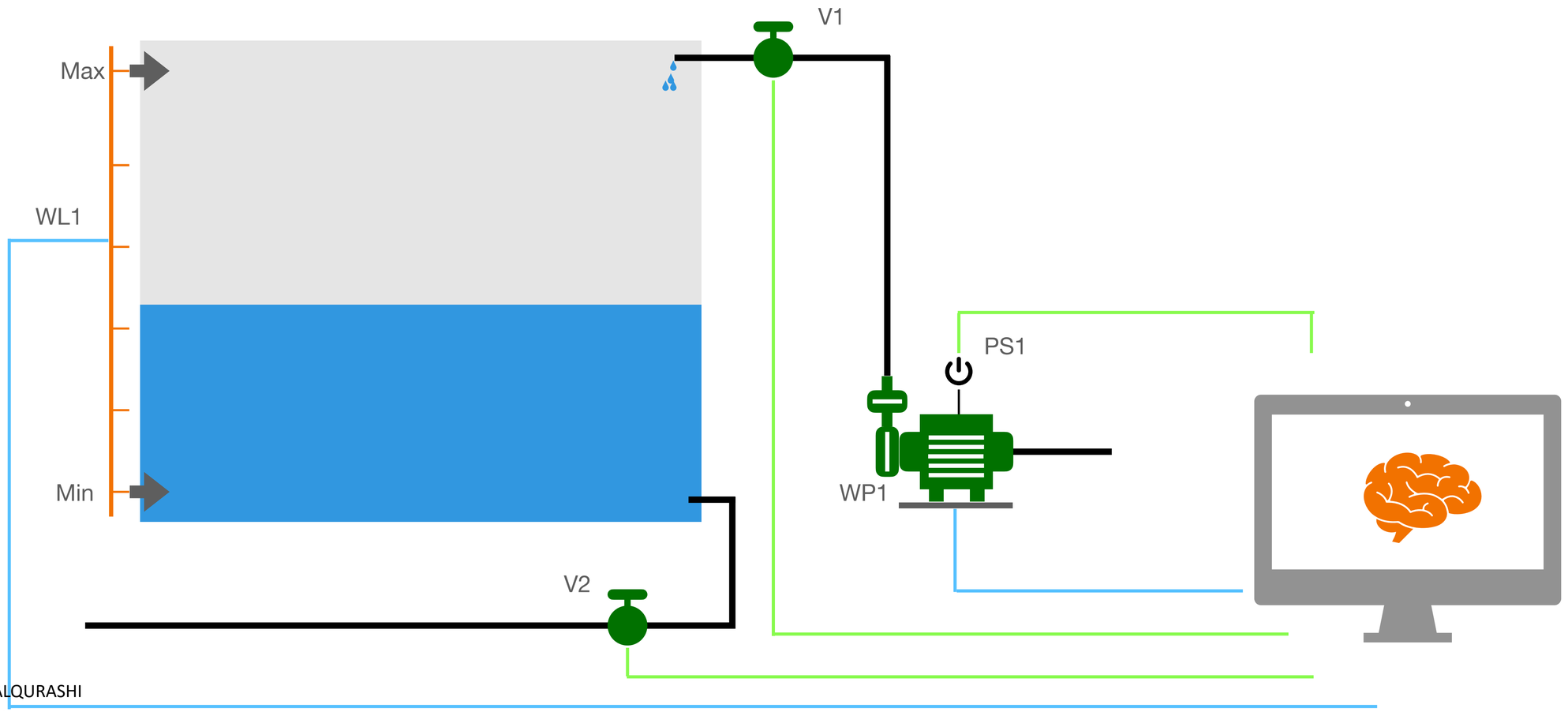


Larger scale

Larger scale
Nature of operation
Type of processes in use

Nebras
CyberSecurityExpert

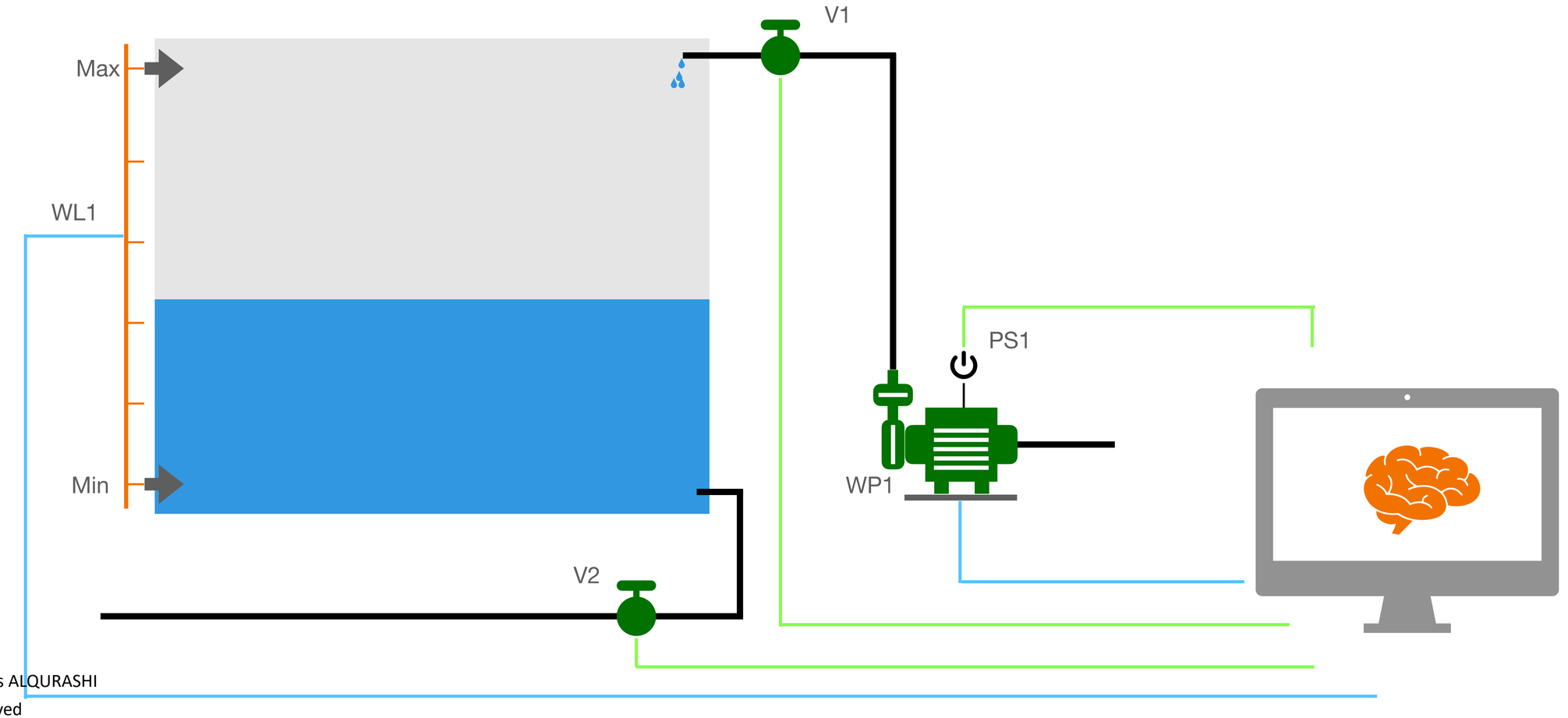
Connect the active components



Nebras
CyberSecurityExpert

Active components

Component	Type of data
V1	Open / Close
V2	Open / Close
WL1	Level of water
PS1	On / Off
WP1	On / Off



Nebras
CyberSecurityExpert

Data conversion and representation

Component	Type of data	Read / Write
V1	Open / Close	W
V2	Open / Close	W
WL1	Level of water	R
PS1	On / Off	W
WP1	On / Off	R

Data conversion and representation

Component	Type of data	Read / Write	Conversion	Example
V1	Open / Close	W	Binary	1
V2	Open / Close	W	Binary	0
WL1	Level of water	R	Scale	18279 -> 50%
PS1	On / Off	W	Binary	1
WP1	On / Off	R	Binary	0

Conversion Example

Sensor provides an analog value range from 200 - 1200
The logical control need to read the value and perform scale conversion
In our example:
0% is represented by analog 200
100% is represented by analog 1200
Based on this scale, when Sensor reads analog value of 700 it’s represented by 50%

Nebras
CyberSecurityExpert

Connections to I/O

Component	Type of data	Read / Write	Conversion	Example	Input / Output
V1	Open / Close	W	Binary	1	O
V2	Open / Close	W	Binary	0	O
WL1	Level of water	R	Scale	18279 -> 50%	I
PS1	On / Off	W	Binary	1	O
WP1	On / Off	R	Binary	0	I

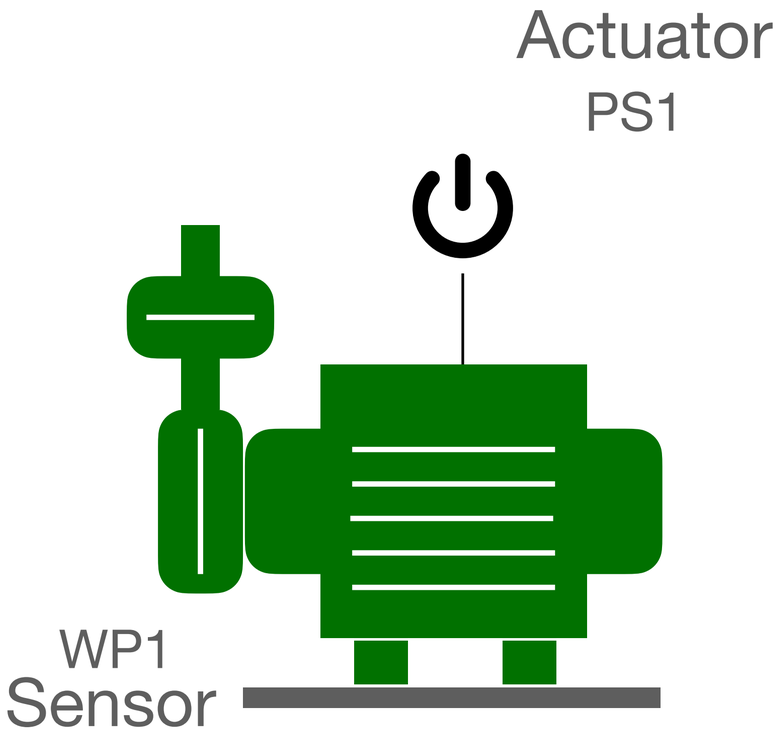
Nebras
CyberSecurityExpert

Field device Type

Component	Type of data	Read / Write	Conversion	Example	Input / Output	FD
V1	Open / Close	W	Binary (digital)	1	O	Actuator
V2	Open / Close	W	Binary (digital)	0	O	Actuator
WL1	Level of water	R	Scale (Analog)	18279 -> 50%	I	Sensor
PS1	On / Off	W	Binary (Digital)	1	O	Actuator
WP1	On / Off	R	Binary (Digital)	0	I	Sensor

Nebras
CyberSecurityExpert

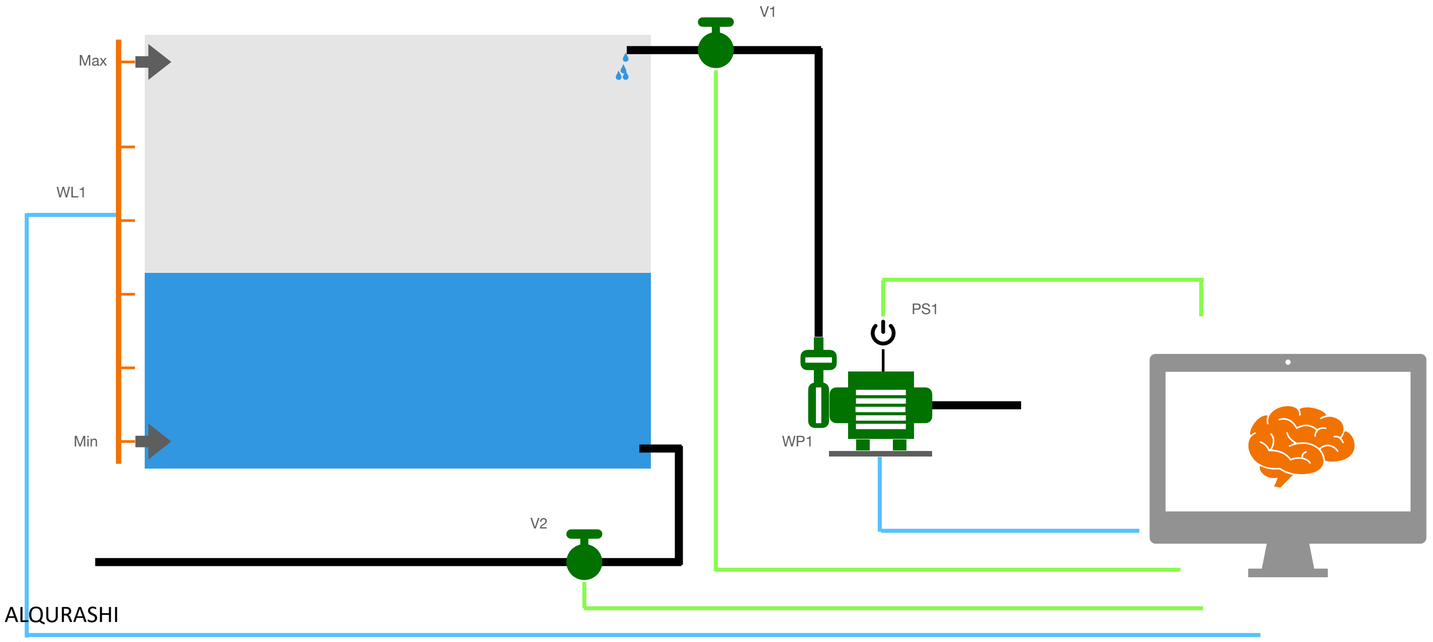
*** Note to avoid confusion**



Nebras
CyberSecurityExpert

The Logic

Read Water Level WL1



Nebras
CyberSecurityExpert

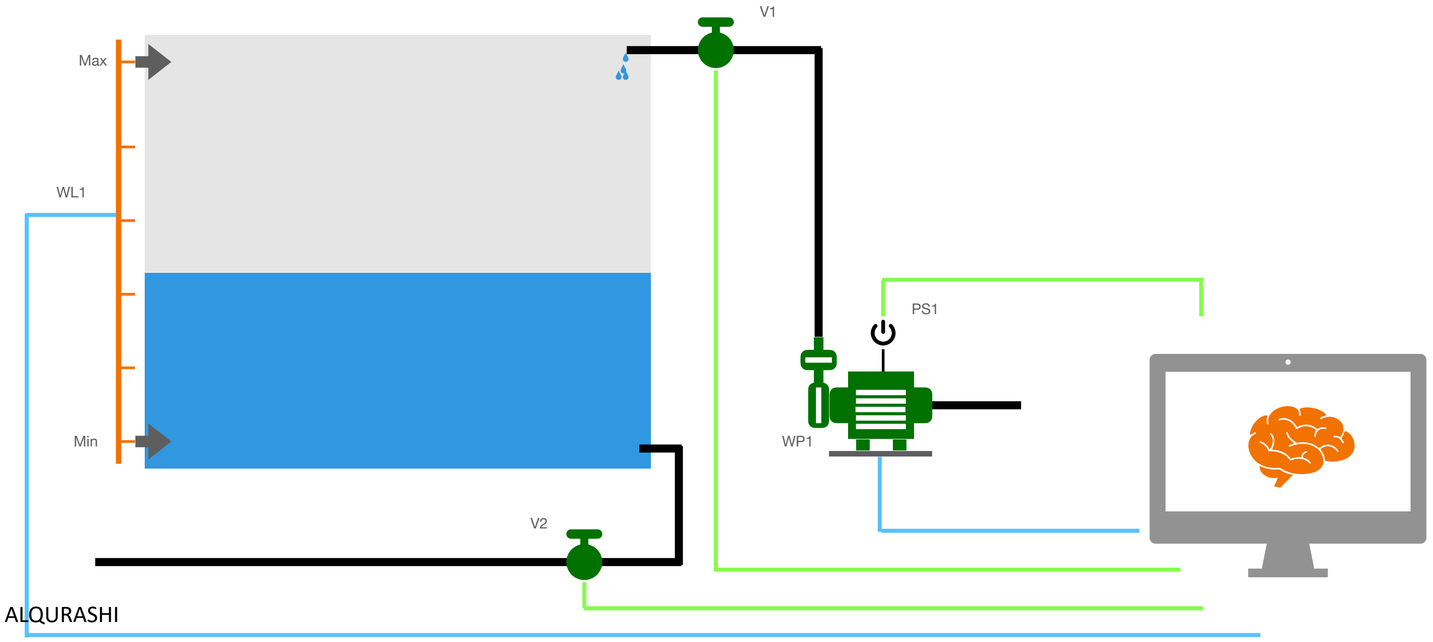
The Logic

Read Water Level WL1

WL1 <= 20%

WL1 > 20% & < 90%

WL1 >= 90%



Nebras
CyberSecurityExpert

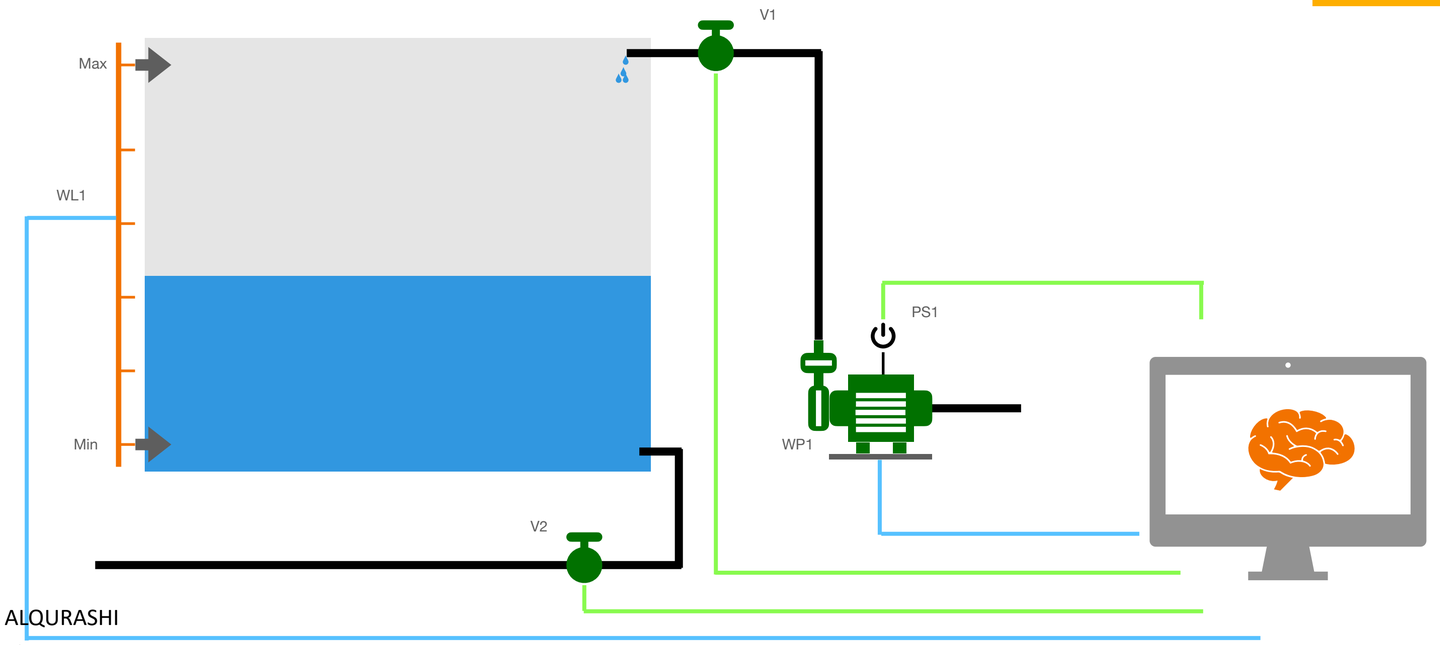
The Logic

Read Water Level WL1

WL1 <= 20% → Close Valve V2
Open Valve V1
Turn Power Switch PS1 ON

WL1 > 20% & < 90% → Open Valve V2
Open Valve V1
Turn Power Switch PS1 ON

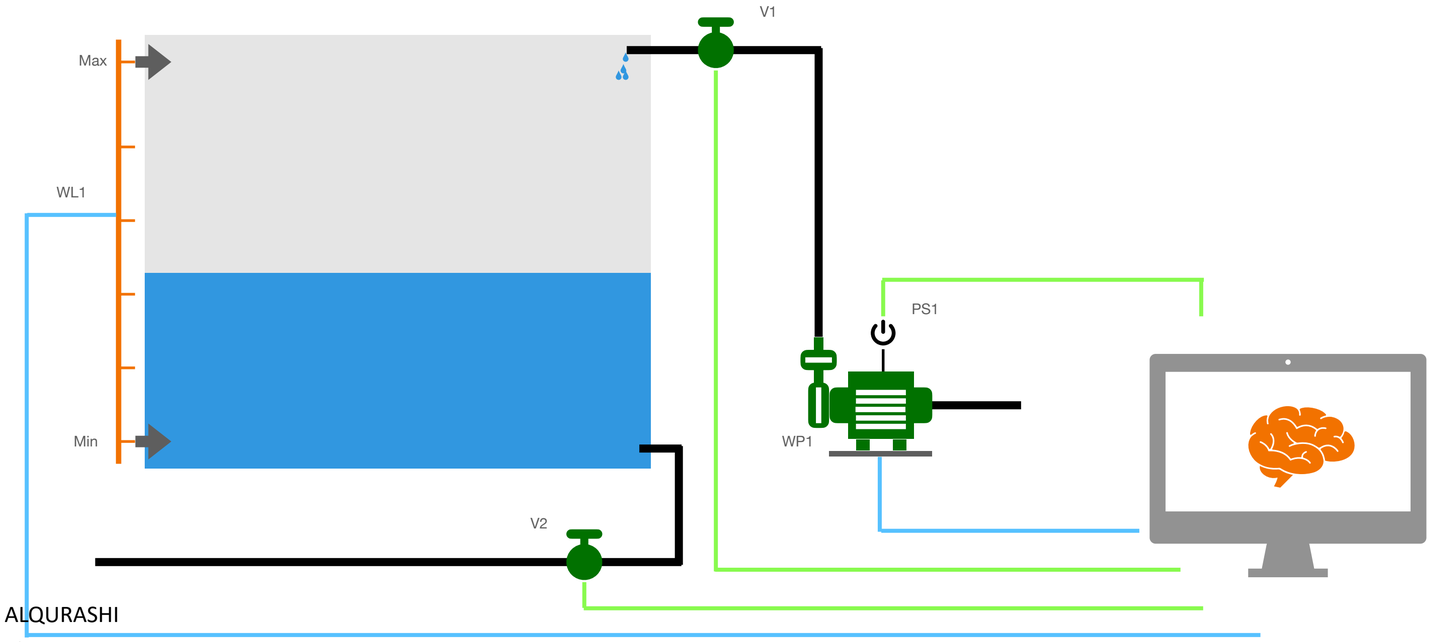
WL1 >= 90% → Open Valve V2
Turn Power Switch PS1 OFF
Close Valve V1



Nebras CyberSecurityExpert

Controller Logic Cycle

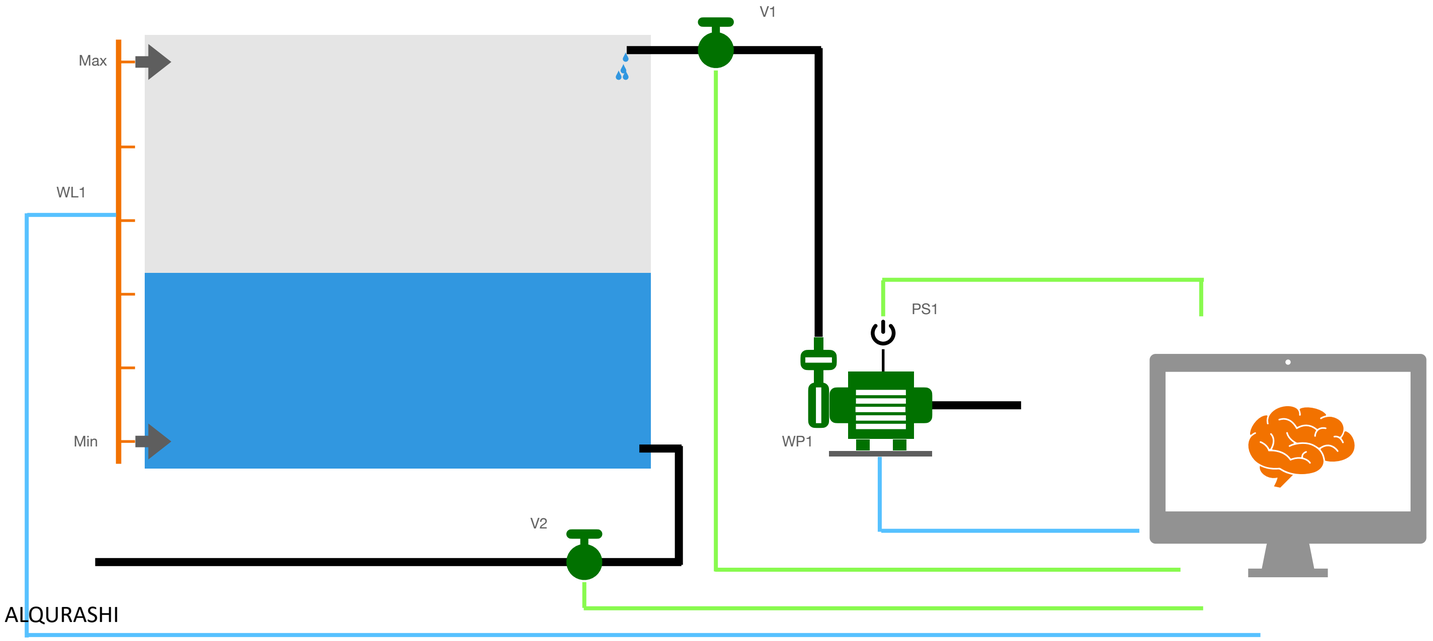
- The logic is designed in continuous cycle.
- A delay of time can be added before the beginning of next cycle.



Nebras
CyberSecurityExpert

Operation and Safety considerations

- We need to make sure not to turn ON Water Pump WP1 while Valve V1 is closed.
- We need to consider the order
- We need to make sure not to pump water to tank while it’s Full
- External Factors (Water Source check, Plant Watering Schedule)



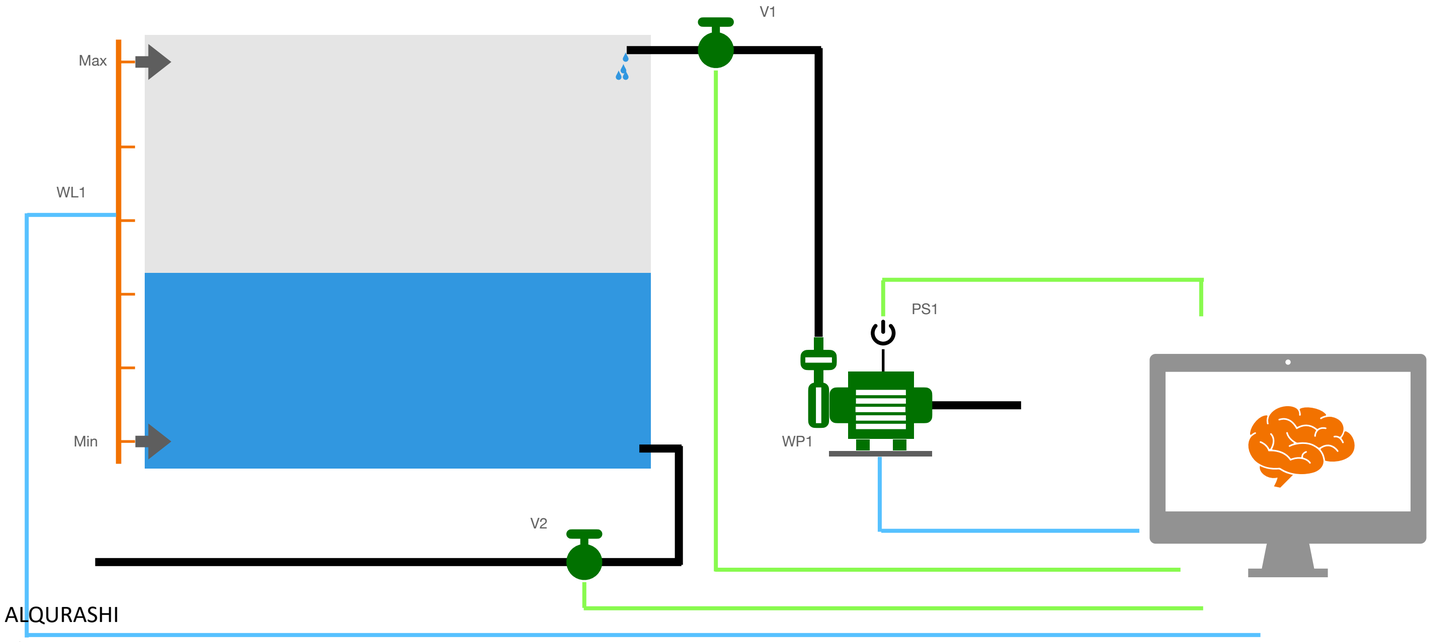
Nebras
CyberSecurityExpert

Monitoring

Water Level WL1
Water Pump WP1
Valves V1 & V2

Writing value

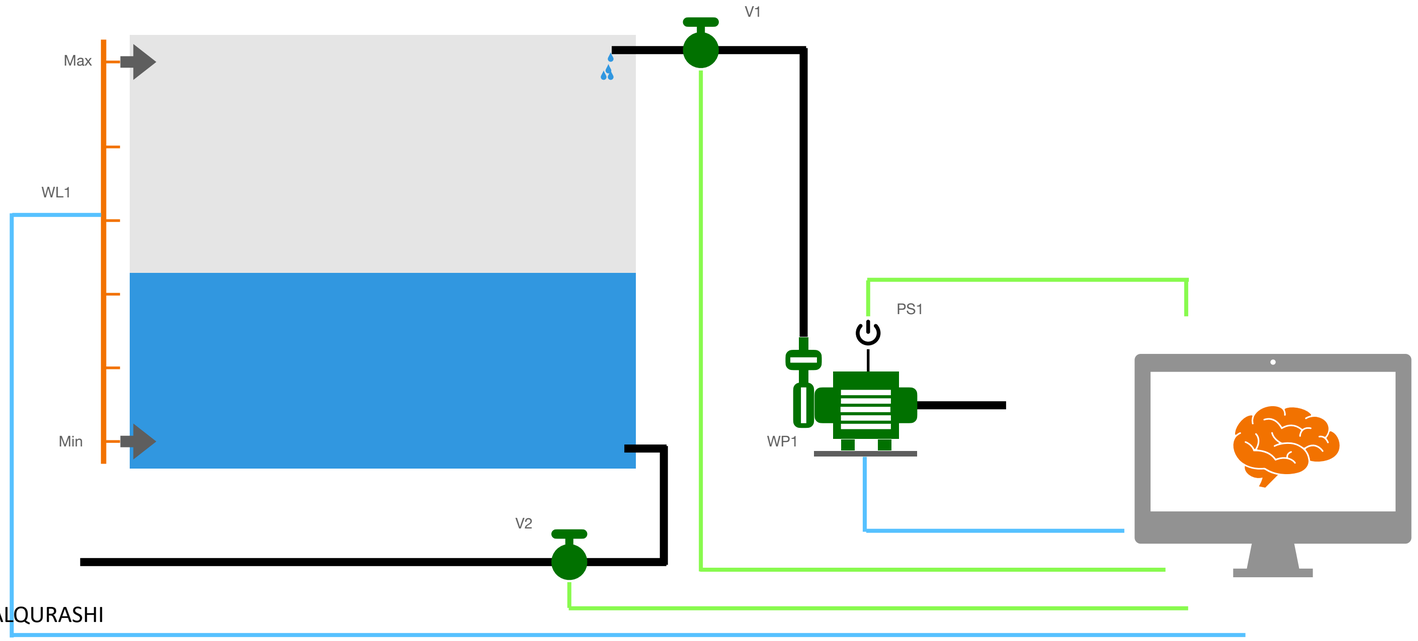
We could check the value of the output device then write new value if different as some devices are sensitive.



Nebras
CyberSecurityExpert

Maintenance

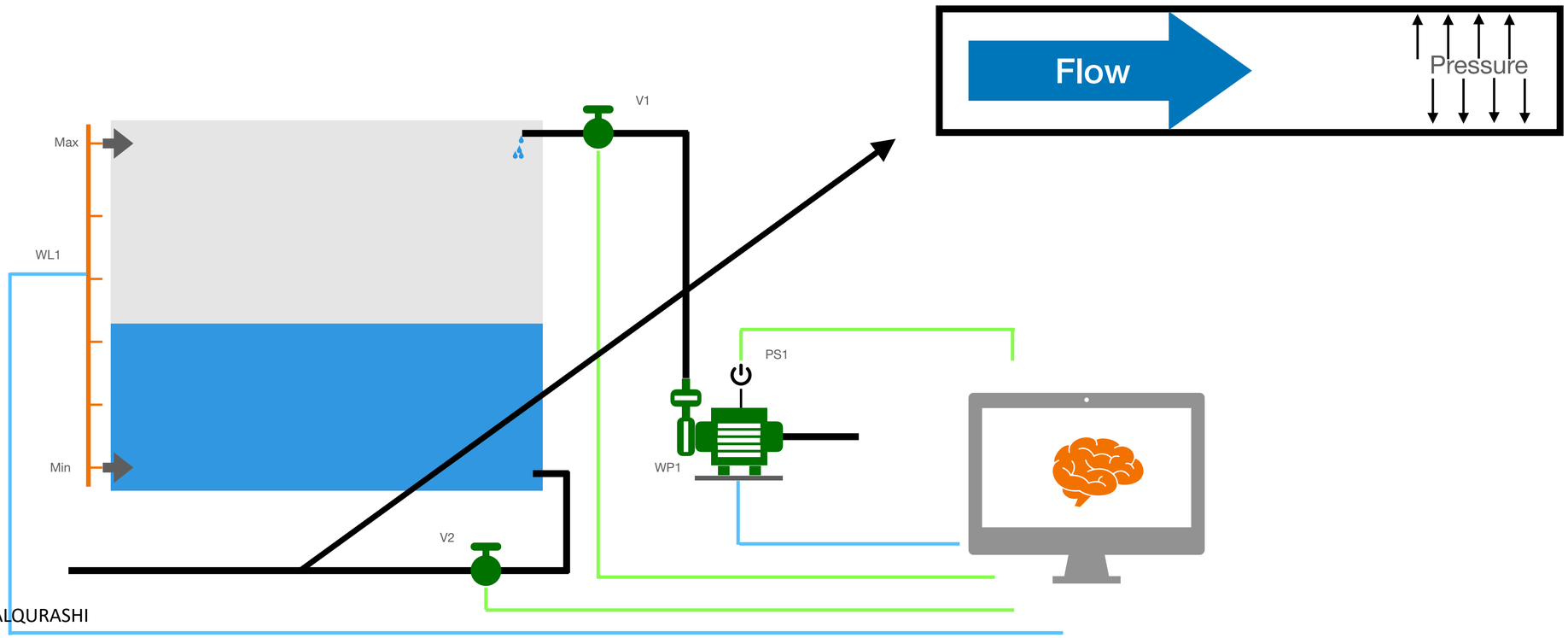
Further details can be obtained to help in maintaining the health and safety of the system.
- We can add more sensors to have better visibility of the health of components.
- Flow, Pressure, Temperature, up time, life cycle, ..etc
- How to determine water leak?



Nebras
CyberSecurityExpert

Maintenance

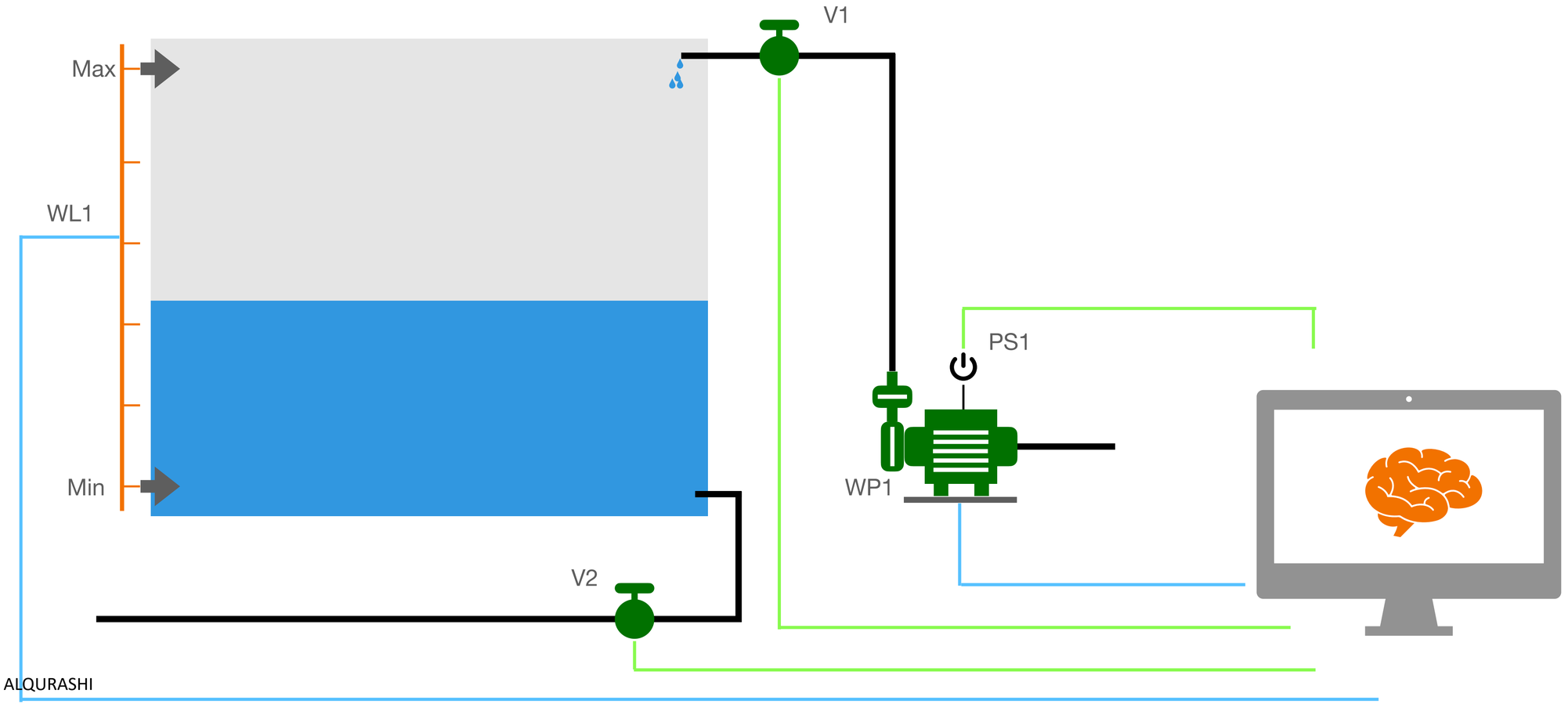
Further details can be obtained to help in maintaining the health and safety of the system.
- We can add more sensors to have better visibility of the health of components.
- Flow, Pressure, Temperature, up time, life cycle, ..etc
- How to determine water leak?



Nebras
CyberSecurityExpert

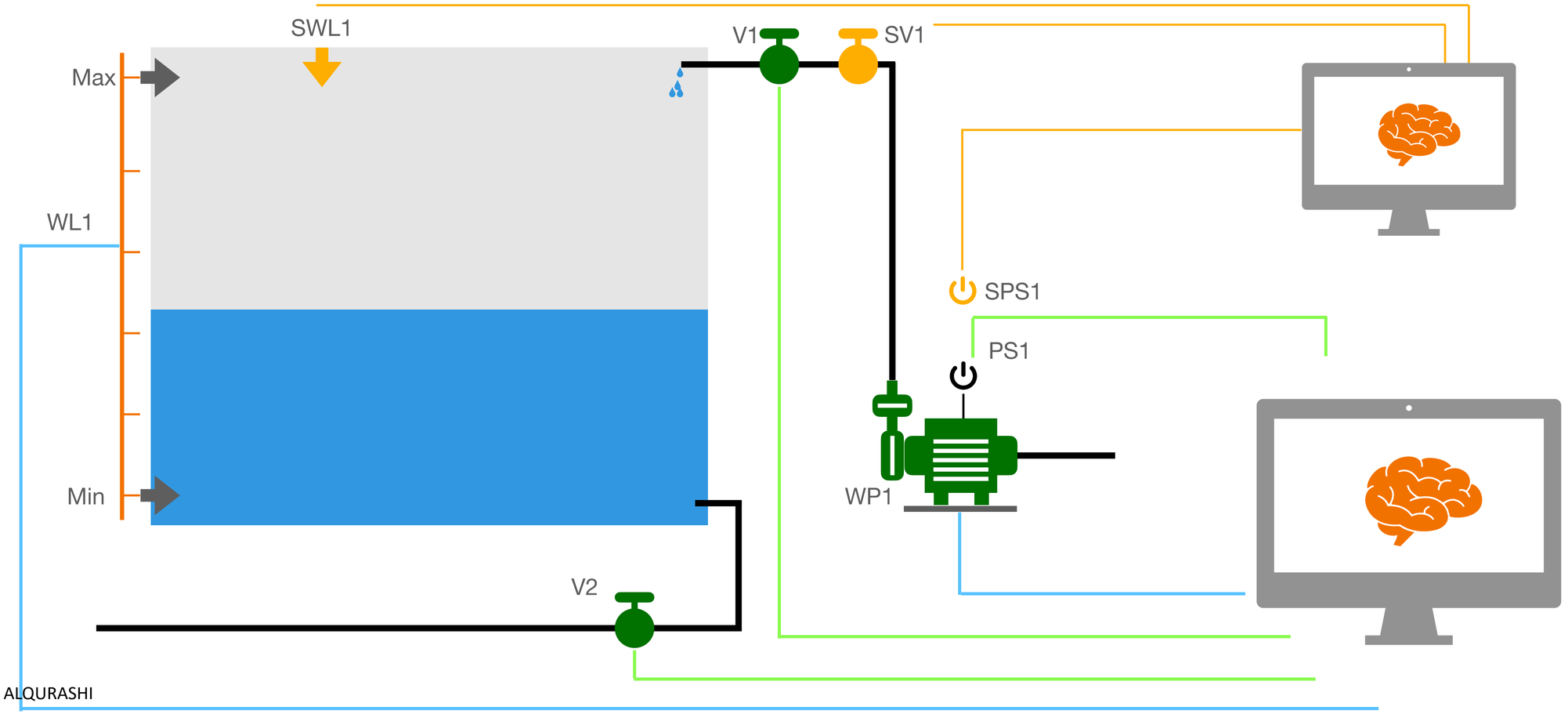
Safety Instrumented System SIS

We had Safety consideration all the way implementing the system and Logic.
SIS objective is to avoid failures in the system
Depending on the type of operation the loss could be in term of financial loss, reputation, and even loss of lives!
SIS is a redundant System, only concerned to avoid system failures and to maintain safety
Safety is the most important key factor in Operational Technology



Safety Instrumented System SIS

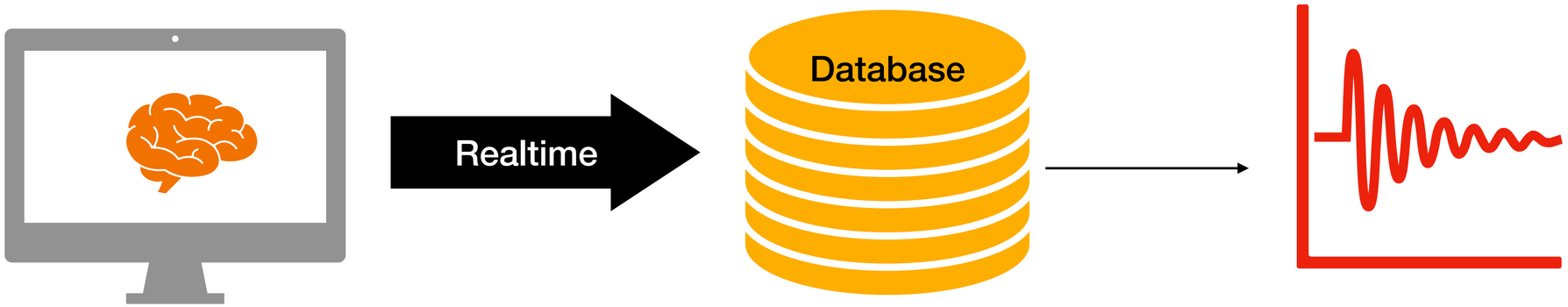
We had Safety consideration all the way implementing the system and Logic.
SIS objective is to avoid failures in the system
Depending on the type of operation the loss could be in term of financial loss, reputation, and even loss of lives!
SIS is redundant System, it's only concerned in avoiding system failures and to maintain safety
Safety is the most important key factor in Operational Technology



Nebras
CyberSecurityExpert

Data Historian

- Data is ingested in realtime from the operation.
- Ingested data will be aggregated into Database.
- Often called tags
- Continuously ingested in realtime each tag has timestamp.
- Ex: Timestamp / tag name / value
- Designed for fast ingestion without dropping any value.
- It’s different from IT Database.
- The data can be used later for analysis, maintenance, reports, ..etc



Nebras
CyberSecurityExpert

Quick summary

Process Logic Cycle

Sensors / Actuators

Safety Instrumented System

Tags

Data Historian

Maintenance

Nebras
CyberSecurityExpert