École Polytechnique Fédérale de Lausanne

Industrial Automation, CS-487

Course Project

Alexandre Nicolas LECHARTIER - 284529
David KWAKYE -269682
Wilhelm WIDLUND MELLERGÅRD - 361948
Defne CULHA - 353020
Héctor M. RAMIREZ C. - 358635

April 10, 2023

Table of content

Project description

This year project considers a paint production plant made of four mixing stations. As illustrated in Figure 1 below, each color mixing station is composed of 5 color tanks (cyan, magenta, yellow, black and white) and one mixing tank. Each color tank is controlled via an output valve, and the mixing tank can be emptied via a dedicated pump and output valve. Each tank has four sensors detecting the very low, low, high and very high levels of color as well as a flow meter and level sensor providing respectively the actual amount of paint leaving each tank and the remaining amount of paint left in a tank.

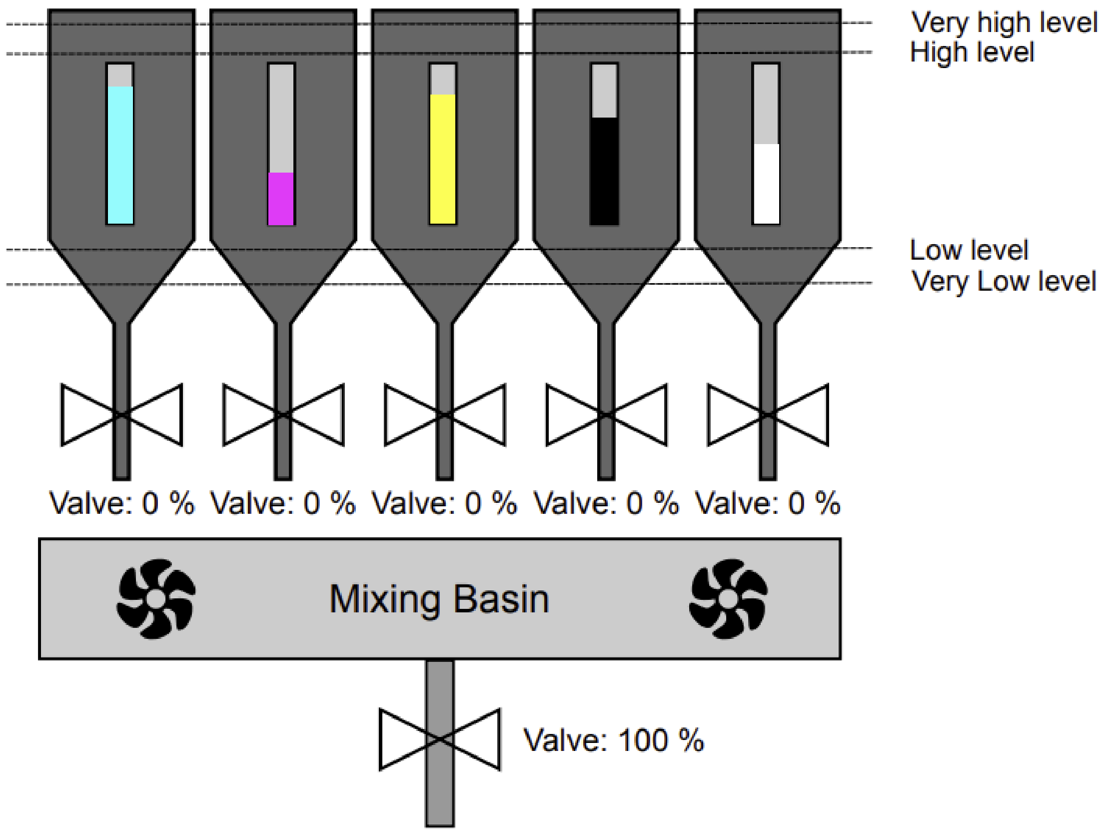

Figure 1: Schematic representation of one of the four color mixing stations

The goal of the project is to provide the monitoring and control infrastructure to operate such a plant by defining the automation architecture from the I/O cards to the SCADA system.

Work distribution

The various sub-tasks in the project are distributed among the group members according to the following table.

Table 1: Distribution of tasks among group members

Task	Group member
Report proofreading	All
Functional analysis (Part 1)	Alexandre LECHARTIER
Automation architecture (Part 2)	Héctor M. RAMIREZ C.
Supervision (Part 3)	David KWAKYE & Wilhelm WIDLUND MELLERGÅRD
Qualitative dependability analysis (Part 4)	Defne CULHA

1 Functional Analysis

The plant is composed of 4 mixing station. Thus, a mixing station is composed of 5 color tanks and a mixing tank. In the following is the lookup table for making correspond each color to a tank number used for convention:

Table 2: Table of used colors per tank number

Used color per tank number	
tank number	color in tank
tank 0	mixing
tank 1	cyan
tank 2	magenta
tank 3	yellow
tank 4	black
tank 5	white

For each mixing station, we use the same signals with the same naming convention, but we add the station number in front of the name. We define the high level signal of the mixing tank as being high_tank_0 for a mixing station. This means that for mixing station 1, we name the signal using this pattern X_high_tank_0, where X is the mixing station number.
For mixing station 1, we will have 1_high_tank_0.
For mixing station 2, we will have 2_high_tank_0.
For mixing station 3, we will have 3_high_tank_0.
For mixing station 4, we will have 4_high_tank_0.

Identify for the whole plant the following points:

- List of input signals (sensors) with their types and ranges

  Per tank, we need to be able to measure the level for this we use switch sensors (with floats) to measure discrete levels and time of flight sensors (with ultrasounds), to measure continuous levels. We also use electrical boards to measure the current drawn by the motors of the mixers. And a camera to measure the color in the tank. We also assume that the station is behind a fence and that when the operator enters the station, operation is resumed. This is to avoid any injury of the operator. Additionally, we only have a sensor for the level very high of the mixing tank, as we will need it to be sure of when the tank overflows.

Table 3: Table of input signals (sensors) with their types and ranges

List of input signals (sensors) with their types and ranges			
input signal	type	range	naming convention
tank very low level tank 1	discrete	0 or 1	very_low_tank_1
tank very low level tank 2	discrete	0 or 1	very_low_tank_2
tank very low level tank 3	discrete	0 or 1	very_low_tank_3
tank very low level tank 4	discrete	0 or 1	very_low_tank_4
tank very low level tank 5	discrete	0 or 1	very_low_tank_5
tank low level tank 1	discrete	0 or 1	low_tank_1
tank low level tank 2	discrete	0 or 1	low_tank_2
tank low level tank 3	discrete	0 or 1	low_tank_3
tank low level tank 4	discrete	0 or 1	low_tank_4
tank low level tank 5	discrete	0 or 1	low_tank_5
tank high level tank 1	discrete	0 or 1	high_tank_1
tank high level tank 2	discrete	0 or 1	high_tank_2
tank high level tank 3	discrete	0 or 1	high_tank_3
tank high level tank 4	discrete	0 or 1	high_tank_4
tank high level tank 5	discrete	0 or 1	high_tank_5
tank very high level tank 0	discrete	0 or 1	very_high_tank_0
tank very high level tank 1	discrete	0 or 1	very_high_tank_1
tank very high level tank 2	discrete	0 or 1	very_high_tank_2
tank very high level tank 3	discrete	0 or 1	very_high_tank_3
tank very high level tank 4	discrete	0 or 1	very_high_tank_4
tank very high level tank 5	discrete	0 or 1	very_high_tank_5
outflow tank 0	continuous	-100 to $100 m^2/s$	outflow_tank_0
outflow tank 1	continuous	-100 to $100 m^2/s$	outflow_tank_1
outflow tank 2	continuous	-100 to $100 m^2/s$	outflow_tank_2
outflow tank 3	continuous	-100 to $100 m^2/s$	outflow_tank_3
outflow tank 4	continuous	-100 to $100 m^2/s$	outflow_tank_4
outflow tank 5	continuous	-100 to $100 m^2/s$	outflow_tank_5
level tank 0	continuous	0 to 100%	level_tank_0
level tank 1	continuous	0 to 100%	level_tank_1
level tank 2	continuous	0 to 100%	level_tank_2
level tank 3	continuous	0 to 100%	level_tank_3
level tank 4	continuous	0 to 100%	level_tank_4
level tank 5	continuous	0 to 100%	level_tank_5
current drawn by mixer's motor 1	discrete	0 to 100%	mixer_current_1
current drawn by mixer's motor 2	discrete	0 to 100%	mixer_current_2
color in mixing tank	discrete	32 bit RGB	mixer_color
door open	discrete	o or 1	door_open

- List of output signals (actuators) with their types and ranges

  To be able to mix paint accurately, we need to be able to precisely control the output valves. When the new color is mixed, we may want to output all the paint as fast as possible. In this case, we use the pump with the fully opened valve.
  Also, depending on the process and the type of paint, we may want to modulate the mixing speed for better efficiency or faster production.

Table 4: Table of output signals (actuators) with their types and ranges

List of output signals (actuators) with their types and ranges			
input signal	type	range	naming convention
output valve tank 0	continuous	0 to 100%	output_valve_0
output valve tank 1	continuous	0 to 100%	output_valve_1
output valve tank 2	continuous	0 to 100%	output_valve_2
output valve tank 3	continuous	0 to 100%	output_valve_3
output valve tank 4	continuous	0 to 100%	output_valve_4
output valve tank 5	continuous	0 to 100%	output_valve_5
Emptying pump tank 0	discrete	0 to 100%	empyting_pump_0
mixing basin mixer speed	continuous	0 to 100%	tank_speed_0

- List of alarms to be displayed to the plant operators

Table 5: Table of alarms to be displayed to the plant operators

List of alarms to be displayed to the plant operators		
alarm	description	naming convention
very low tank 1 very low tank 2 very low tank 3 very low tank 4 very low tank 5	triggered when the tank level is under very low level marker	very_low_1 very_low_2 very_low_3 very_low_4 very_low_5
low tank 1 low tank 2 low tank 3 low tank 4 low tank 5	triggered when the tank level is under low level marker	low_1 low_2 low_3 low_4 low_5
very high tank 0	triggered when the tank level is over the very high marker	very_high_0
empty tank 0 empty tank 1 empty tank 2 empty tank 3 empty tank 4 empty tank 5	triggered when the tank is empty (use low level & tank level sensors)	empty_0 empty_1 empty_2 empty_3 empty_4 empty_5
emptying process tank 0 tank 1 tank 2 tank 3 tank 4 tank 5	triggered when the tank is being emptied (use valve command)	emptying_process_0 emptying_process_1 emptying_process_2 emptying_process_3 emptying_process_4 emptying_process_5
leak of tank 0 leak of tank 1 leak of tank 2 leak of tank 3 leak of tank 4 leak of tank 5	triggered when valve closed & level sensor measures level decreases over some time $24 \gtrapprox \Delta t \gtrapprox 1$ *hour* (use tank level sensor over time & valve command)	leak_0 leak_1 leak_2 leak_3 leak_4 leak_5

uncontrolled level stagnation of	triggered when valve command open & level not changing (use tank level sensor & valve command)	
tank 0		level_stagnation_out_0
tank 1		level_stagnation_out_1
tank 2		level_stagnation_out_2
tank 3		level_stagnation_out_3
tank 4		level_stagnation_out_4
tank 5		level_stagnation_out_5
uncontrolled input level stagnation of tank 0	triggered when tank 0 level rises & tank 1, 2, 3, 4 or 5 is leaking	
from tank 1		level_stagnation_in_01
from tank 2		level_stagnation_in_02
from tank 3		level_stagnation_in_03
from tank 4		level_stagnation_in_04
from tank 5		level_stagnation_in_05
measured level conflict	triggered when tank's measured levels are in conflict (obtained from range sensors & level sensors)	
of tank 0		level_conflict_0
of tank 1		level_conflict_1
of tank 2		level_conflict_2
of tank 3		level_conflict_3
of tank 4		level_conflict_4
of tank 5		level_conflict_5

Alarms need to be displayed to the operators, to indicate critical possible situations that may lead to a system failure. For this, we use alarms on low levels of color tanks, to inform that a refill may be needed soon, and a very high level for the mixing tank to inform that the tank may overflow.
If one of the color tanks is empty, we trigger an alarm. If the mixing tank is empty when emptying it, we also trigger an alarm. An alarm is triggered when we empty any tank.
We also measure the level when the tank is not used, if its measured value decreases over time while its valve is closed, we trigger an alarm. If we want to output the content of any tank, and it doesn't work, we trigger an alarm. This many happen if the valve is open, but the level does not decrease. A similar alarm is triggered if we want to output paint from one color tank, but mixing tank level is not changing, e.g. for an open valve of a color tank and no change measured on the range sensor.
Another alarm is triggered if the measured levels on the tanks do not overlap, e.g. we measure a very high level on tank 1, but the range sensor says it's full at 50% only.

- List of interlocks and their logic

  We want to ensure that no liquid is coming in the mixing tank while we empty the mixing tank, so we close the color tank's output valves.
  If we measure an overfull of the mixing tank, we will raise the alarm and stop the process.
  When we input color in the mixing tank, we want to ensure that the mixing tank output valve is closed.
  We assume that the mixing fence is secured by a fence to avoid operators to go in and injure themselves. When an operator is in it, a special protocol has to be followed to avoid injuries.
  In case of a too high leakage of any tank, the plant is shut down.
  When operating motors of the mixing palms, some unexpected incident may happen, such as having a palm stuck. This will lead to a motor in stalling state and may heat up the plant. To avoid any risk of fire, the current of the motor is measured. If the current is too high, the motor is stuck and the plant is shut down and needs emergency maintenance.

Table 6: Table of interlocks and their logic

List of interlocks and their logic		
Interlock	logic	naming convention
emptying tank 0	when the tank 0 is being emptied, close the tanks' 1, 2, 3, 4 & 5 valves	emptying_tank_0
max level tank 0	close tanks 1, 2, 3, 4 & 5 output valves, if tank 0 very high level is active and tank 0 level at 100%	max_level_tank_0
secure tank 0 operation	close tank 0 output valve, when output valves of tanks 1, 2, 3, 4 & 5	secure_operation_0
open fence operation	stop process when fence is open, until fence closed and start button is pressed	open_fence_process_stop
high leakage shut down	stop process, when tank output valve closed & big level decrease measured	high_leakage_process_stop
motor stall	stop process, when motor is stalling (motor uses too much current)	motor_stall_process_stop

Along with the signal identification, you will have to propose a naming convention to be used throughout the plant.

2 Automation Architecture

2.1 Hardware description

2.1.1 Assumptions

About e**xplosive atmospheres**: The assignment document does not specify whether the paint is oil-based or water-based, hence our assumption was that the paint is water based. Explosive hazard is not considered, this way we avoided dealing with explosive atmosphere, otherwise we would have to use specialized equipment for this application, based in an additional hazard analysis for this type of zones which is not covered in the course. Although some elements have an ATEX II 2G as a minimum, the **PLC has not special inputs and intrinsic-safe barriers were not considered**.
Pipe dimensions: 1" tubes in each tank.
Tank dimensions: 2 mts long max, no specification about with. The tanks are considered to be stainless steel.
Filling of mixing tank by flow control with proportional valves. No clean design directives as is not a food or pharmaceutical application. No safety PLC included.

2.1.2 Sensors (Inputs)

Figure 2: Point level sensor

Discrete point-level sensors: For this task, all sensors were considered to be the same type of sensor. All of them are **capacitive sensors**, that can be attached to the tanks with a special mounting. We were careful to verify that they could be used with liquid media. In this case the sensors work either with water-based liquids or oil-based liquids.
Number of pieces: 24
Name: LMC410, LMGCE-C12E-QSKG-1/US
Provider: IFM
Output: Discrete, PNP at 24V Connection: M12
Type of Mounting: G12 thread
Datasheet: LMC410 - Sensor for point level detection

Figure 3: Pressure level sensor

Continuous Level sensors: In this case a hydrostatic pressure senor was selected for the level. This would avoid some complications compared to other sensors, because we have not a specific assumption about the dimensions of the tank, a pressure sensor would be practical for measuring the level of each tank by using the **hydrostatic pressure.**
Number of pieces: 6
Name: PS307A

Provider: IFM
Output: Continuos, 4 . . . 20 [mA] Connection: Has cable
Type of Mounting: Suspended in fluid.
Datasheet: PS307A - Hydrostatic submersible pressure transmitter

Figure 4: Flow sensor

Continuous Flow sensors: The chosen principle of this sensor is the **calorimetry**. This is particularly useful and practical for this application, as it doesn't need a big mounting space and can work either with oil or water-based liquids. It allows us to not worry much about the specific conductivity, density, or viscosity of the paint.
Number of pieces: 6
Name: SA2000 SAR12XDBFRKG/US-100 Provider: IFM
Output: Continuous, 4 . . . 20 [mA]
Connection: M12
Type of Mounting: G12 thread
Datasheet: SA2000 - Flow sensor

2.1.3 Actuators (Outputs)

Ball valve with controller: For the actuator, a ball valve was chosen, as it allows to do flow control for liquid media. Although for flow control applications a butterfly valve is usually better, for small pipe diameters a ball valve is suitable. The whole actuator is provided as a single system with the vendor "FESTO". It was configured according to the application parameters discussed in the functional analysis.
The controller is a **CMSX** positioner from FESTO that has an embedded board that does the PID control. It is attached to the valve. It is actuated with pneumatic energy. The input is a 4-20 mA value from the PLC and the output is the position according to the input current.

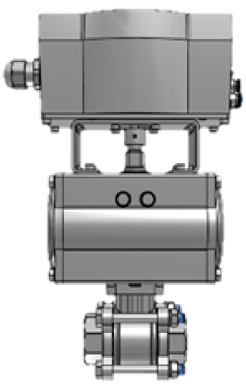

Figure 5: Flow sensor

The actuator has two parts, a 1" stainless steel ball valve, attached to a pneumatic actuator, that operates at 6 bar of air pressure. It is connected to the controller with a bridge. The details can be seen in the list attached to the datasheet.
Number of pieces: 6
Name: KVZB, C2653937
Provider: FESTO
Input: Continuous, 4 . . . 20 [mA] Output: ¼ spin according to input.
Pneumatic connection: 6mm tubing.
Electric connection: Cooper cable
Type of Mounting: G1 thread
Datasheets: Assembly KVZB

2.1.4 Control architecture

PLC: Communication protocol is not specified; therefore, the PLC was chosen to be flexible. The selected configuration of the PLC is Profi-Net which is the Siemens standard, nevertheless if there is the need to change to any other protocol this PLC can be configured with Ethernet IP, Ethercat or Modbus TCP, moreover it can also send data through OPC-UA, which will enable us to implement a SCADA system.

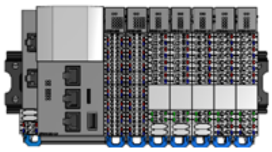

Figure 6: PLC: CPX-E

Number of pieces: 1
Name: CPXE
Provider: FESTO
Digital inputs: 2 modules with 16 DI
Analog Inputs: 3 modules with 4 AI
Analog Outputs: 2 modules with 4 AI
Protocol as slave: Profi Net
Protocol for SCADA: OPC-UA
Type of Mounting: DIN Rail for cabinet
Datasheet: CPX-E
Modules and configuration: 60E-CPN-2M3NI2NO - CPX-E parts

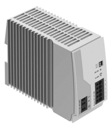

Figure 7: PLC: Power Supply CACN

Control power supply is dedicated to power the sensors, and control devices. Has enough Output current for the applicactions considered.
Number of pieces: 1
Name: CACN-3A-1-20-G2
Provider: FESTO
Input: 220V
Output: 24V - max 20 A
Datasheet: Power supply unit CACN

Figure 8: PLC: Power Supply CACN

AC Motor Control: Frequency variator from ABB. It enables to start the mixer's motor in a safe way, it also allows to regulate the speed if necessary to consume less power and save energy if the mixing doesn't need much power. As the motor is triphasic, so is the frequency variator, which was dimensioned based on the characteristics of the mixer's motor.
Number of pieces: 1
Name: ACS310-03X-07A4-2
Provider: ABB
Input power: 3/60/220V
Input control: 4 - 20 [mA] (other options are available, but for our application this is the one to be used).
Output: 3/xx/220V
Datasheet: ABB ACS310

Figure 9: Sensor cables

Cables for flow and point level sensors.
Number of pieces: 30
Name: EVC006 Vendor: IFM
Length: 10m
Connection: M12 socket and 4-wire end for PLC
Datasheet: EVC006 cable with socket

2.1.5 Control Architecture diagram

This is the architecture for a single tank and the mixing tank. The other 4 colour tanks have the same architecture but are omitted to simplify the diagram.

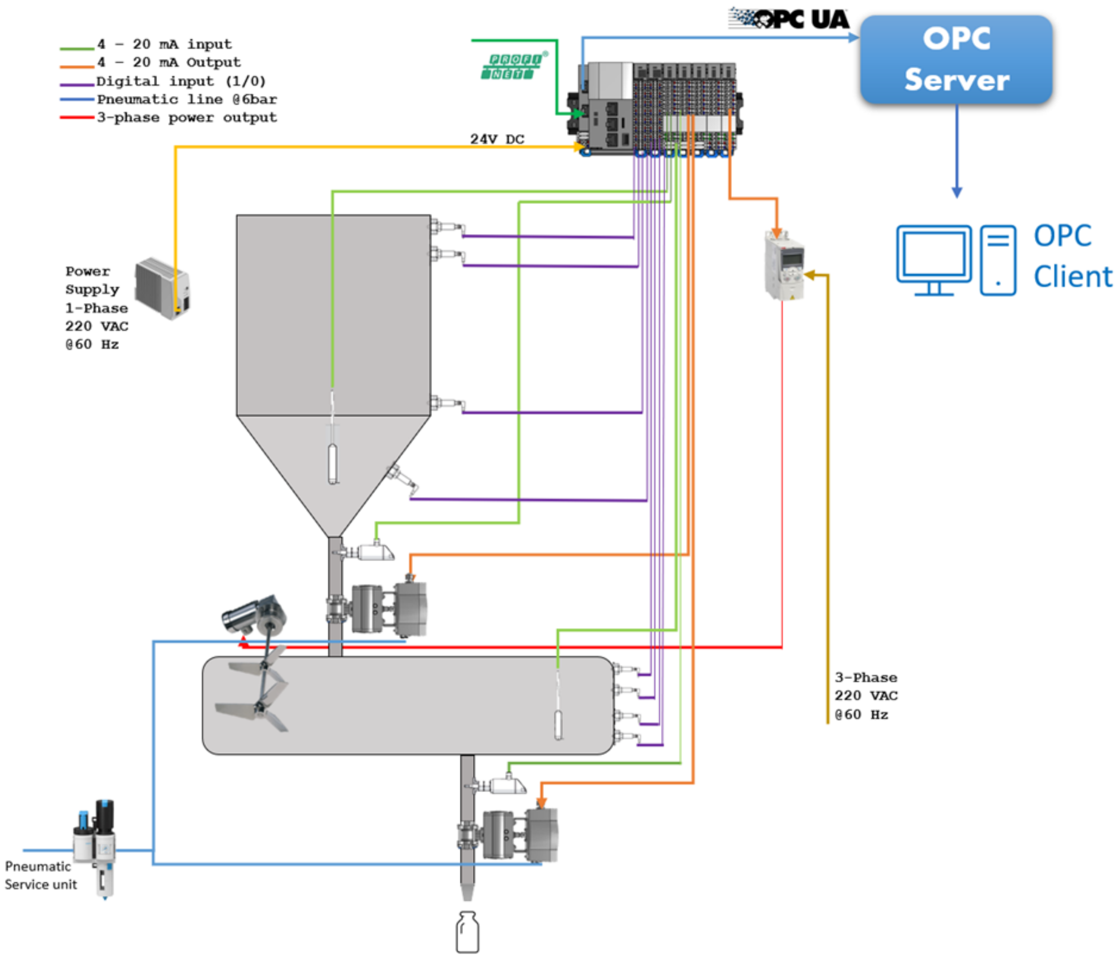

Figure 10: Caption

3 Supervision

3.1 Synoptic views

3.1.1

For our synoptic view, we chose to use a hierarchy with 3 stages. The first stage is the Process Area Overview. It displays the general state of the 4 mixing station. In these windows (drawn in figure 11) we have all the information to assess the current status of each mixing station. We know what the process is supposed to be, and we have a clear view of events and notifications. We chose to use color to help the viewer to see in one blink if something is wrong and require immediate attention. Once problems are noticed, The supervisor can click on the `Detailed view` button to get to the second level of the hierarchy, for each mixing station respectively.

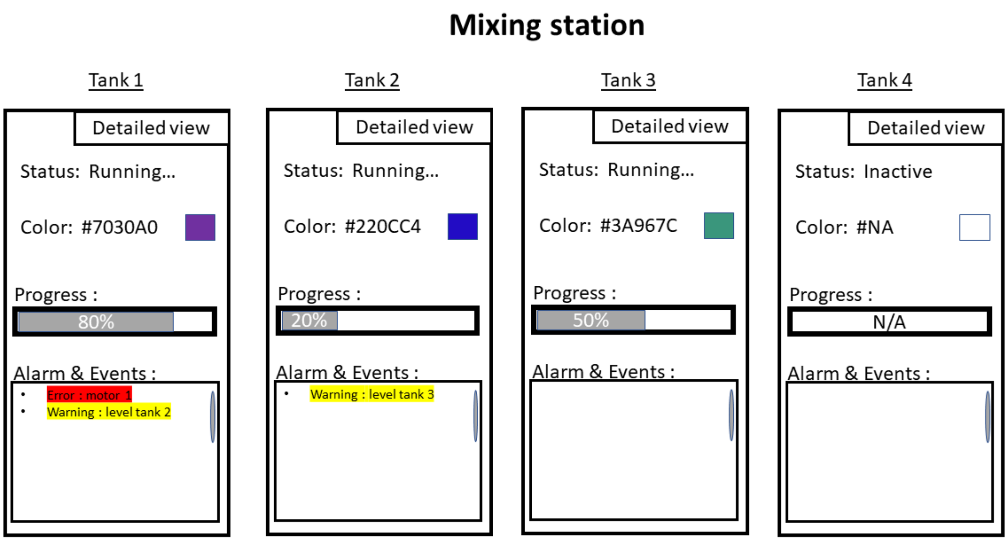

Figure 11: Process Area overview

The second Level is the Process Unit Control page (figure 12). This one contains information regarding each tank in a specific mixing station. The user can understand what could be happening with the current values of sensors on display. This layout allows anyone to see if the level of paint is still acceptable or if a pump doesn't function as expected. If time dependent information is needed, we can navigate to the third layer, with the `Detailed view` button.

The third layer (figure 13) contain graphs which show the evolution of values from the chosen tank over time. It could be useful if we need the history to know how quickly things have changed.

3.1.2

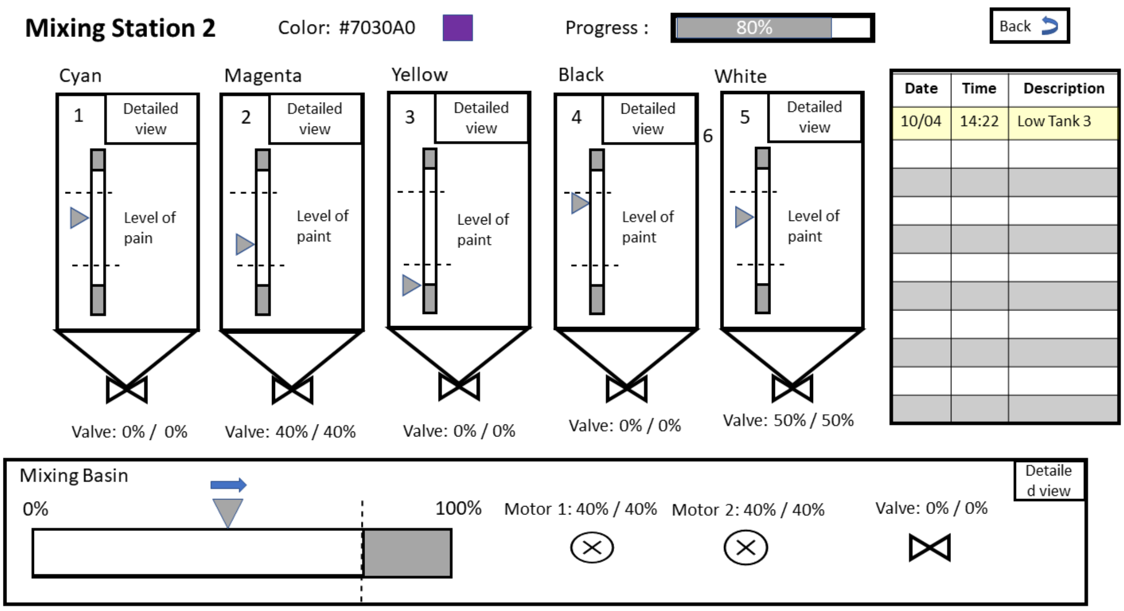

Figure 12: Process Unit control

Figure 13: Process Unit Detail

4 Qualitative Dependability Analysis

We will consider each component of the single mixing station system. The station is made up of 3 main parts: colour tanks, mixing tank and the control system. Colour tanks have output valves, sensor to detect flow, sensors to detect colour levels. Mixing tank has an output pump, sensors to detect detect flow, sensors to detect its level.

4.1 Fault Tree Analysis (FTA)

To perform FTA, following steps are followed.

4.1.1 Top-level events

First we identify the top-level event, which is the failure or event that we want to analyze. 3 top level events are identified in this case.

1. The mixing tank does not receive the correct colour of a paint mixture.
2. The mixing tank overflows.
3. The mixing tank doesn't receive enough paint as requested.

4.1.2 Intermediate and basic events

Next, we identify the potential causes or contributing factors that can lead to each primary event.

4.1.2.1 Incorrect colour

For top-level event 1 where the mixing tank does not receive the correct colour of a paint mixture, intermediate event scenarios could be identified as follows.

(a) Incorrect colour mixing ratios set in controller.

(b) Contaminated mixing tank or colour tanks.

(c) Less amount of paint flowing from one or more of the colour tanks.

(d) More amount of paint flowing from one or more of the colour tanks.

The intermediate events can be caused by basic events as follows.

(i) For 1a, it can be due to incorrect input from the control system, human error in setting the mixing ratios.

(ii) For 1b, it can be due to incorrect labelling of a paint colour, accidental mix of colour in a tank from the control system, human error in filling the tanks.

(iii) For 1c, it can be due to lack of materials, colour tank level sensor fails to detect correct level, inaccurate flow meter readings or scheduling mistake in filling the tanks.

(iv) For 1d, it can be due to colour tank level sensor fails to detect correct level, inaccurate flow meter readings or one of the output valves of the colour tanks fail to close.

4.1.2.2 Tank overflows

For scenario 2 (mixing tank overflows), intermediate events are identified as follows.

(a) Mixing tank level sensor fails to detect correct level.

(b) Mixing tank output valve fails to open.

(c) More amount of paint flowing from one or more of the colour tanks.

The intermediate events can be caused by basic events as follows.

(i) For 2a, it can be due to inaccurate flow meter readings or broken hardware.

(ii) For 2b, it can be due to clogging of the pump or inaccurate flow meter readings.

(iii) For 2c, it can be due to a hardware problem of the pump or inaccurate flow meter readings.

4.1.2.3 Not enough paint

For scenario 3 where there is not enough paint in the mixing tank as requested, intermediate events are identified as:

(a) Mixing tank output valve fails to close.

(b) One or more of the colour tank fails to pour colour.

The intermediate events can be caused by basic events as follows.

(i) For 3a, it can be due to mixing tank level sensor fails to detect correct level, a hardware problem of the pump or inaccurate flow meter readings.

(ii) For 3b, it can be due to it can be due to lack of materials, colour tank level sensor fails to detect correct level, a hardware problem or a clog at the valve or scheduling mistake when filling the tanks.

Now, we have identified the basic events which cause of the top undesired and severe events which could happen. These basic events can be further analyzed for their potential causes and consequences and appropriate measures can be taken to reduce the likelihood and impact of failures.

4.2 Failure Modes and Effects Analysis (FMEA)

We also perform FMEA. First we identify potential failure modes. These can be colour tanks and output valves failing to open or close, colour tank level sensor fails to detect correct level, mixing pump fails to work properly, mixing tank level sensor fails to detect correct level and most severely when the control system fails to operate. We analyse each of these now and calculate their Risk Priority Numbers (RPN).

4.2.1 Colour tanks

(a) **Failure mode:** Colour tanks' output valves failing to open or close
Severity: If the valve fails to open, the tank won't be able to dispense paint or if it failts to close, it will dispense more than required paint and might cause incorrect ratios and mixing tank overflowing. This will cause faulty products and may create a mess in the production plant. Severity score assigned as 8.
Occurrence: The valves are relatively reliable, but there is some risk of failure due to old or cheap hardware. Occurence score assigned as 4.
Detection: The failure of the valve would be immediately noticeable during the production process when a valve is not flowing. Detection score assigned as 8.
RPN: 8 x 4 x 8 = 256

(b) **Failure mode:** Colour tanks' level sensor fails to detect correct level.
Severity: If the sensor fails, it could result in incorrect amounts of paint being dispensed and cause wrong ratios in mixing tank which can then cause faulty products. Severity score assigned as 6.
Occurrence: The sensors can suffer from calibration issues. Occurence score assigned as 6.
Detection: Broken sensors can go a long way without getting noticed but it can be detected in control checks. Detection score assigned as 7.
RPN: 6 x 6 x 7 = 252

4.2.2 Mixing tank

(a) **Failure mode:** Mixing pump fails to work properly
Severity: If the pump fails, this will result in uneven production, unreliable quality and faulty products. Severity score assigned as 9.
Occurrence: The pumps are reliable. Occurence score assigned as 3.
Detection: The failure of the pump would be noticed immediately. Detection score assigned as 9.
RPN: 9 x 3 x 9 = 243

(b) **Failure mode:** Mixing tank level sensor fails to detect correct level
Severity: If the level sensor fails, it could result in incorrect mixing ratios, resulting in faulty products. Severity score assigned as 7.
Occurrence: Sensors can suffer from calibration problems. Occurence score assigned as 5.
Detection: Broken sensors can go a long way without getting noticed but it can be detected in control checks. Detection score assigned as 7.
RPN: 7 x 5 x 7 = 245

4.2.3 Control system

(a) **Failure mode:** Control system fails to operate
Severity: If the control system fails, it could result in everything getting shutdown for the worst case, and less severely it could cause incorrect mixing ratios and faulty products. This is one of the most severe things that can happen. Severity score assigned as 10.
Occurrence: The control system is reliable, but there is still some risk of failure due to human errors or some eletrical problems. Occurence score assigned as 2.
Detection: The failure of the control system would be noticed immediately. Detection score assigned as 9.
RPN: 10 x 2 x 9 = 180

Now that we have calculated RPN for each potential failure mode, to improve the reliability and robustness of the production plant, the focus would be to mitigate the risks of potential failure modes with the highest RPN. A RPN threshold could also be decided and every potential failure mode should have a RPN of lower than that threshold. For example, to lower RPN of failure mode which the colour tanks' output valves failing to open or close, higher quality valves could be used.