



École Polytechnique Fédérale de Lausanne

Group 8

Industrial automation project

ChocoMation Automation



Figure 1: AI-generated chocolate factory image

AMMANN Florian (347346) ,
MAIROLL Emanuel (404912) ,
MITRIC Marko (315718) ,
AKGÜN Muratcan (387714)

Professors :

M. Jean-Charles Tournier
M. Philipp Sommer

May 26th 2025

Contents

1	Introduction	4
	Introduction	4
2	Functional Analysis	5
	Functional Analysis	5
	2.1 Plant overview	5
	2.2 Piping and Instrumentation Diagram	6
	2.3 Component Selection and Reasoning	6
	2.4 Station Functionalities	8
3	Automation Architecture	11
	Automation Architecture	11
	3.1 PLC Configuration	11
	3.2 Communication Network	11
	3.3 Network Protocols	11
4	Supervision	12
	Supervision	12
	4.1 SCADA System Requirements	12
	4.2 Market Survey and Vendor Analysis	12
	4.3 Final Choice	14
	4.4 Synoptic Views	15
5	Qualitative Dependability Analysis	18
	Qualitative Dependability Analysis	18
	Summary of FMEA and Safety Controller Selection	18
	Summary of FTA	18

Conclusion	19
.0.1 Figures for Qualitative Dependability Analysis	20
.0.2 Pseudocode for the Automation	23

1 Introduction

Context

This project addresses the design, implementation, and supervision of an automated chocolate powder production plant. The factory produces chocolate powder through a series of processes. The steps of the production line are the raw material handling, their mixing, drying and milling, and finally packaging.

Goal

The primary goal of this project is to gain hands-on insight into the structure and integration of industrial automation systems. It aims to develop an understanding of how a production plant is automated from the field level (sensors and actuators) to the high-level supervision layer (SCADA). By replicating an industrial setting, the project intends to bridge theoretical knowledge with practical implementation and prepare us for real-world automation engineering challenges.

Overview

We began by performing a functional analysis of the plant, identifying all sensor inputs, actuator outputs, alarms, and interlocks for each unit in the process. Based on this, we developed the P&ID the plan and we defined the automation architecture, justifying the choice of PLCs, fieldbuses, and communication protocols. A market survey was then performed to select a SCADA platform that meets the plant's requirements. We developed a mock-up of the synoptic views used for supervising the overall process. Finally, we carried out a qualitative dependability analysis using Failure Modes and Effects Analysis (FMEA) and Fault Tree Analysis (FTA) to identify potential weaknesses and ensure system robustness.

2 Functional Analysis

2.1 Plant overview

At the beginning, Cocoa, milk powder and sugar are stocked in 3 different tanks, each equipped with a humidity and a level indicator. At the bottom of each tank, the outlet is a valve that feed into a pneumatic conveyor in charge of bringing raw materials to the mixing station.

This station is also equipped with a level sensor, as well as a temperature sensor and a controller to manage the heater alimentation. An additional current controller is connected to the motor of the mixer. After the mixing operation, a valve extracts the material, which goes into the rotary dryer.

For the rotary dryer, a current controller is in charge of the rotation speed, a humidity sensor keeps track of the drying process, and a temperature sensor and controller manage the dryer heat intensity.

After drying, the mixture goes to a milling station that will make it become powder again. This milling station is controlled with current, and a current sensor is in charge of torque measurement.

The finished chocolate powder is then stocked into a buffer tank equipped with a level sensor, before being sent to the packaging process.

The packaging process begins with a weighing stage. The chocolate powder is poured onto a plastic foil through a valve controlled by the weight sensor located under the foil. The packaging is stored on a roller equipped with a level sensor and an analyser for torn detection.

Once weighted it goes to the sealing and cutting station. Where the plastic foil is sealed by termosolder, a temperature controller is connected to the heating element and finally the sealed foil filled with chocolate powder is cut and goes to the plant output.

2.2 Piping and Instrumentation Diagram

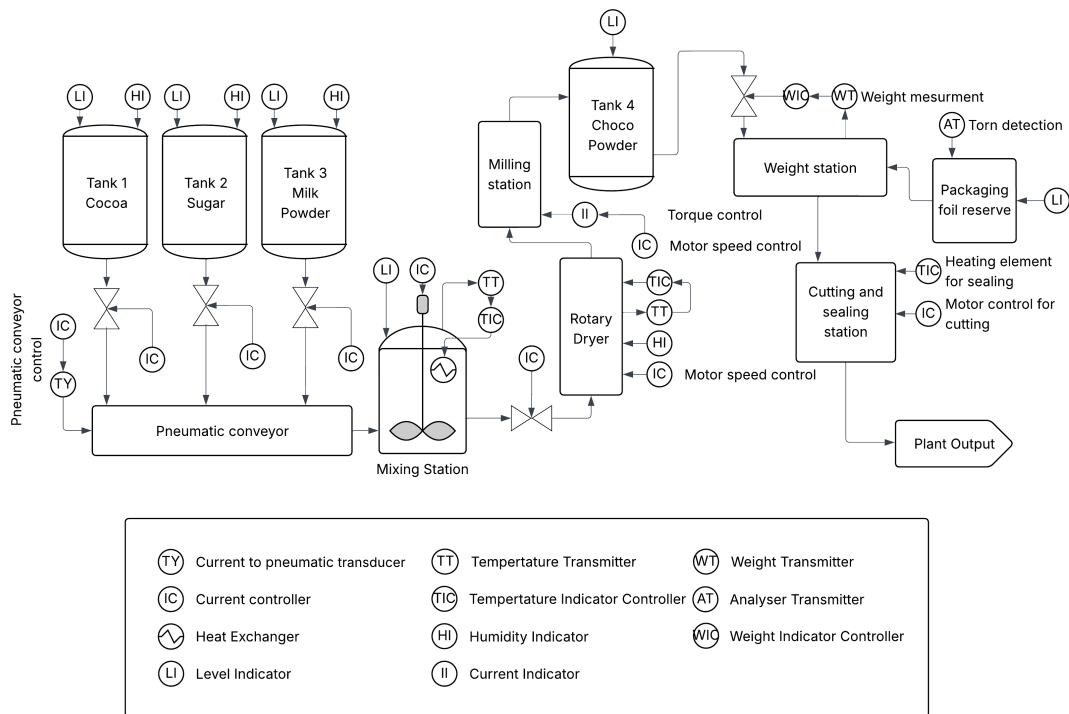


Figure 2: P&ID

2.3 Component Selection and Reasoning

Motors and Drives:

- **SINAMICS S120 + SIMOTICS T-1FW3 Torque Motors:** Selected for high-torque tasks in the mixing station, drying drum, and milling. These motors have precise torque and speed control, are reliable in continuous operation and are simple to integrate in the automation system via PROFINET.
- **SINAMICS S210 + SIMOTICS S-1FK2 Servo Motors:** Used in packaging for the precise cutting of bags. Chosen for high precision and accuracy, as well as the SIMATIC Motion Control functionality of the PLC.
- **Elmo Rietschle G-BH1 2BH1:** Driving the positive pressure pneumatic conveyor connecting storage and mixing. Switched with a simple 3RF2 relay for simplicity.

Actuators:

- **SIPART PS2 Valve Positioners:** Used at raw material handling, mixing, and packaging for fine control of material flows controllable with 4–20 mA analog signals, which allows precise dosing control gives and positional feedback to the PLC.

- **SIRIUS 3RF2 Solid State Relays (SSRs):** Used to control heating elements in mixing, drying, and packaging processes. Chosen for durability, the absence of mechanical wear, and ability to handle frequent switching cycles reliably. Also reused for switching the pneumatic conveyor, for simplicity.

Sensors:

- **SITRANS LR100/LR110 Radar Level Sensors:** Deployed in raw material storage, mixing vat and packaging. These sensors provide non-contact measurements which are important in dusty environments to prevent contamination and maintain hygiene. The LR110 variant monitoring the foil roll is specifically used for its higher precision of up to 2mm.
- **SITRANS TS500 Temperature Sensors:** Installed in mixing and drying to deliver precise temperature readings to ensure product quality and safety by alerting to abnormal conditions.
- **QFM2101 Humidity Sensors:** Used to monitor moisture content in storage silos and during drying, important for maintaining product quality and preventing spoilage or clumping.
- **Kistler 4503B Torque Sensor:** Integrated into milling equipment, allowing the system to detect and react quickly to jams or abnormal mechanical stresses, protecting the equipment.
- **SIWAREX WP231 + WL260 Load Cell:** Used in packaging for precise measuring of bag weight, which is critical for the consistency of the product.
- **SIRIUS 3RG7 Photoelectric Sensor:** Monitors packaging foil integrity and presence, immediately stopping packaging in case of foil tear or other issues.

Safety Components:

- **Cerberus OP921 Smoke and CO Detectors:** Installed for the early detection of fire hazards, which trigger quick automated responses.
- **Sintrol S203 Dust Sensors:** Continuously monitor dust concentrations to prevent from dust explosions.
- **SIRIUS ACT Emergency Stop Buttons:** For manual intervention to immediately shut down machinery
- **SIRIUS 8WD46 Alarm Beacon:** For clear audible/visual warnings during emergencies.
- **FOGTEC High-Pressure Water Mist System:** Automatically deployed fire suppression system, quickly extinguishing detected fires to minimize damage.

2.4 Station Functionalities

Raw Material Handling

Three vertical silos serve as raw material storage and are drained from a valve at the bottom, connecting to the next station using a pneumatic conveyor.

- **Inputs:**
 - **Level Sensors:** SITRANS LR100, 4–20 mA - Mounted on each silo top for continuous, non-contact measurement of powder level.
 - **Humidity Sensors:** QFM2101, 4–20 mA - Installed inside each silo to monitor the moisture of the internal air.
- **Outputs:**
 - **Outlet Valves:** SIPART PS2, 4–20 mA - Each silo outlet is fitted with a valve positioner, feeding into a pneumatic conveyor connected via a rotary airlock valve. The PLC sends an analog signal for valve adjustment and receives position feedback.
 - **Pneumatic Conveyor:** Elmo Rietschle G-BH1 2BH1 + SIRIUS 3RF2 - Pneumatic Conveyor blower connecting storage and mixing.
- **Alarms:**
 - **Low Material Level:** Issue **operational** warning, stop feed line.
 - **High Humidity:** Issue **quality** warning, flag for quality check.
- **Safety Interlocks:**
 - **Emergency Stop / Fire:** All outlet valves close immediately.

Mixing Station

A closed vat with an agitator and electrical heater to process the incoming material. The Vat is conveyor-fed from the top and drained from a valve at bottom.

- **Inputs:**
 - **Level Sensor:** SITRANS LR100, 4–20 mA - Monitors product level in the vat.
 - **Temperature Sensor:** SITRANS TS500, 4–20 mA - Records vat temperature.
- **Outputs:**
 - **Agitator Motor:** SINAMICS S120, PROFINET - PLC sets agitator speed via PROFINET.
 - **Heater (Relais):** SIRIUS 3RF2 SSR, digital - PLC controls the heater of the vessel through SSR.
 - **Discharge Valve:** Pneumatic, SIPART PS2, 4–20 mA - For product outflow.
- **Alarms:**

- **High Level:** Stop product inflow, Issue **operational** warning
- **Low Level:** Stop agitator, Issue **operational** warning.
- **High Temperature:** Disable heater, Issue **quality** warning.
- **Safety Interlocks:**
 - **Critical Temperature:** Triggers Emergency Stop procedure, activates fire suppression system.
 - **Emergency Stop / Fire:** Agitator and heater are disabled, discharge valve closes.

Drying and Milling

Consists of an open ended drying drum, directly feeding into the milling machine, grinding into a buffer tank. The milling machine is covered in such a way to **not** be considered a safety hazard for workers.

- **Inputs:**
 - **Drum Temperature:** SITRANS TS500, 4–20 mA - Measures drying air temperature.
 - **Exhaust Humidity:** QFM2101, 4–20 mA - Monitors process air moisture.
 - **Mill Torque:** Kistler 4503B, 4–20 mA - Detects mechanical load on mill.
- **Outputs:**
 - **Drum Motor:** SINAMICS S120, PROFINET - Controls drum rotation.
 - **Mill Motor:** SINAMICS S120, PROFINET - Drives milling unit.
 - **Dryer (Relais):** SIRIUS 3RF2 SSR, digital - Controls air heating.
- **Alarms:**
 - **Low Material:** Halt affected feed line, Issue **operational** warning.
 - **High Humidity:** Flag for quality check, Issue **quality** warning.
- **Safety Interlocks:**
 - **Critical Temperature:** Triggers Emergency Stop procedure, activates fire suppression system.
 - **Emergency Stop / Fire:** Disable motors and heater.

Packaging Station

The finished Cocoa Powder is packaged in thermally sealed plastic bags. The Station automates bag filling, sealing, and cutting the foil for the bag from a large continuous foil roll.

- **Inputs:**
 - **Bag Weight:** SIWAREX WP231 + WL260, PROFINET - Monitors powder weight in each bag.

- **Foil Roll Level:** SITRANS LR110, 4–20 mA - Measures foil supply left.
- **Foil Not Torn:** SIRIUS 3RG7, digital - Detects foil presence at sealing point.
- **Buffer Level:** SITRANS LR100, 4–20 mA - Checks buffer tank status.
- **Outputs:**
 - **Filling Valve:** Pneumatic, SIPART PS2, 4–20 mA - For dosing powder.
 - **Sealing Heater:** SIRIUS 3RF2 SSR, digital - Activates bag sealing.
 - **Cutting Servo:** SINAMICS S210, PROFINET - Operates bag cutter.
- **Alarms:**
 - **Buffer Overflow:** Stop inflow to buffer, Issue **operational** warning.
 - **Foil Low/Break:** Pause packaging, Issue **operational** warning.
- **Safety Interlocks:**
 - **Emergency Stop / Fire:** Filling valve closes, heater and cutter shut down.

Safety System

Monitors hazards in the manufacturing process and triggers process-wide safety procedures like an Emergency Stop.

- **Inputs:**
 - **Smoke/CO Detection:** Cerberus OP921 - Fire detection points at multiple and redundant locations.
 - **Dust Level:** Sintrol S203 - Monitors airborne dust at all machine exhausts, has to be redundant.
 - **Emergency Stop:** SIRIUS ACT - Hardwired E-stop buttons on all machines.
- **Outputs:**
 - **Alarms:** SIRIUS 8WD46 - Visual/audible signaling of emergencies.
 - **Fire Suppression:** FOGTEC - Water mist system to quickly estinguish fire.
 - **Process Shutdown:** PLC outputs disable all relevant drives and heaters.
- **Alarms / Interlocks:**
 - **Fire Detected:** Activates fire suppression system, Alarm and shutdown, (safety)
 - **Dust Hazard:** Alarm and shutdown, (safety)
 - **Emergency Stop:** Alarm and shutdown, (safety)

3 Automation Architecture

3.1 PLC Configuration

- **Main Controller – SIMATIC S7-1500:** Chosen for its modularity and the capacity to handle analog and digital signals required by the production line. It manages central processing tasks, sequential logic, and real-time control loops.
- **Redundant Safety Controllers – SIMATIC S7-1200 G2:** Two safety PLCs are installed as a redundant pair with hot failover. Safety functions such as emergency stop, fire, and dust detection are handled independently of the process PLC. In case one unit fails, the second controller takes over safety operations without interruption.

3.2 Communication Network

- **PROFINET Protocol:** Used for data exchange between PLCs, sensors, and actuators. Chosen for its compatibility with selected Siemens components, as well as for its reliability.
- **Network Topology:** A star topology is to be implemented with a central switch located in the control cabinet. Each operational station is connected individually, simplifying wiring as well as troubleshooting and maintenance.
- **Distributed Remote I/O:** Remote ET 200SP I/O racks are installed near each station to minimize cabling length and complexity. This approach simplifies installation and maintenance and reduces the likelihood of communication failures.

3.3 Network Protocols

- **OPC UA:** Used for standardized data exchange between PLCs, SCADA, and higher-level systems. Allows to easily integrate the system with supervisory control and data analytics.
- **Ethernet/IP, TCP/IP:** Backbone protocols for plant-wide communication on which OPC UA runs on.

4 Supervision

To effectively monitor and control the chocolate powder production plant, the SCADA system needs to provide real-time data, clear process visualization, alarm handling, and historical logging. Since the plant uses Siemens SIMATIC S7-1500 and S7-1200 PLCs, the system should be compatible with these controllers and support OPC UA. The setup is relatively small, with fewer than 50 I/O points, so the SCADA solution should be simple and well-suited to that scale.

4.1 SCADA System Requirements

- Less than 50 I/O signals (digital and analog)
- Native support for OPC UA and Ethernet
- Compatibility with Siemens SIMATIC controllers
- Real-time monitoring with synoptic views
- Alarm management and historical data logging
- Scalability and modularity for future expansion
- Affordable license availability is preferred
- Preference for web-based HMI access and secure remote monitoring

4.2 Market Survey and Vendor Analysis

Siemens WinCC Unified

- Licenses vary between CHF 800–2000 depending on the number of monitor clients.
- Native support for Siemens ET 200SP and S7-1200 via TIA Portal.
- Supports OPC UA and TCP/IP.
- Provides web-based HMI, integrated engineering, and scalable architecture.
- Widely available through Siemens and authorized distributors.

Ignition by Inductive Automation

- Base platform pricing starts at USD 1100 and depending on the additional modules, the price goes up. The Pro Package which includes the necessary functionalities, like alarm notifications and reporting, costs USD 23080.
- Supports Siemens PLCs via OPC UA; may require additional configuration.
- Supports OPC UA, MQTT, TCP/IP.
- Modular platform, web-based HMI, unlimited tags, and scripting capabilities.
- Downloadable with extensive documentation and support.

Open Automation Software (OAS)

- SCADA system starts at USD 1121; additional modules are priced separately.
- OPC UA support with Siemens PLC connection via OPC servers.
- Supports OPC UA, MTCConnect, RESTful API.
- Offers real-time data access, cloud integration, and mobile support.

COPA-DATA zenon

- Commercial licenses range from CHF 1500–4000 depending on configuration.
- Native Siemens PLCs and TIA Portal support.
- Supports OPC UA, MQTT, and Modbus.
- Provides energy data management, batch tracking, FDA compliance, and cybersecure HMI.

AVEVA System Platform

- Price information is available after contact with sales.
- Siemens integration via OPC UA or DA; but mainly for Schneider Electric software and hardware solutions, as it offers native integration for them.
- Supports OPC UA, Modbus, MQTT.
- Enterprise-level redundancy, predictive analytics, and advanced SCADA modeling.
- Widely used in industry, though potentially over-complex for smaller applications.

4.3 Final Choice

Siemens WinCC Unified stands out as the most suitable platform for our chocolate powder production plant for several reasons.

First, WinCC Unified supports natively the Siemens SIMATIC S7-1500 and S7-1200 PLCs already in use at the plant. As all automation and supervision systems will work within Siemens TIA Portal, it simplifies engineering, reduces development time and helps avoid possible integration problems.

Second, the platform fully supports the required industrial communication protocols, including OPC UA, and Ethernet. These protocols are essential for real-time data exchange, interoperability, and secure communication across the automation system.

Another major advantage is the modern web-based HMI that WinCC Unified provides. This feature enables flexible and secure remote access from any device with a browser, allowing operators and engineers to monitor and control the system from anywhere, improving operational responsiveness.

WinCC Unified also allows for scalable solutions. As the plant expands or new functionalities are needed, the system can grow accordingly, whether it's adding more I/O points, extending to new production areas, or incorporating more advanced control features.

From a financial perspective, WinCC Unified offers competitive licensing options, especially suitable for systems with fewer than 50 I/O signals. This makes it a cost-effective solution without compromising on performance or reliability.

Lastly, Siemens' global presence and long-standing reputation in industrial automation provide assurance of ongoing support, documentation, and updates, making WinCC Unified a future-proof investment.

In conclusion, Siemens WinCC Unified meets the current and foreseeable requirements of the project. It combines technical robustness, user-friendly design, integration flexibility, and reliable vendor support which makes it the optimal SCADA platform for our chocolate powder production plant.

4.4 Synoptic Views

The hierarchy of the different presented views is given in figure 3 :

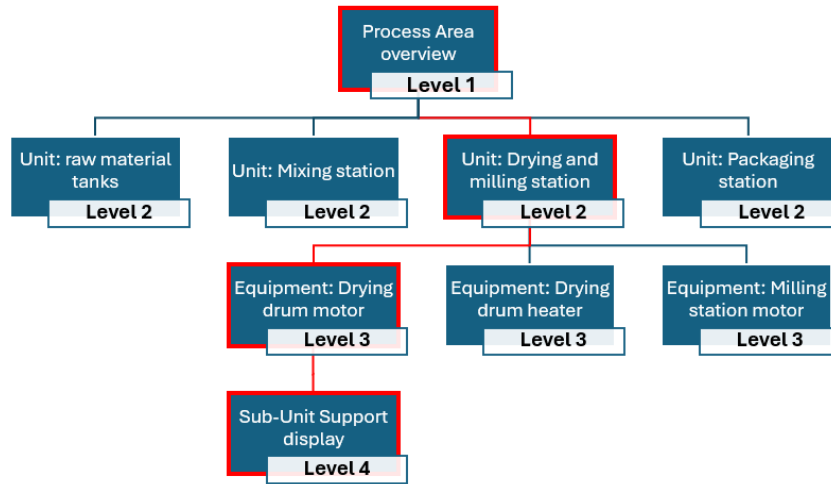


Figure 3: Synoptic view architecture

The views that we will present are marked in red in the above diagram.

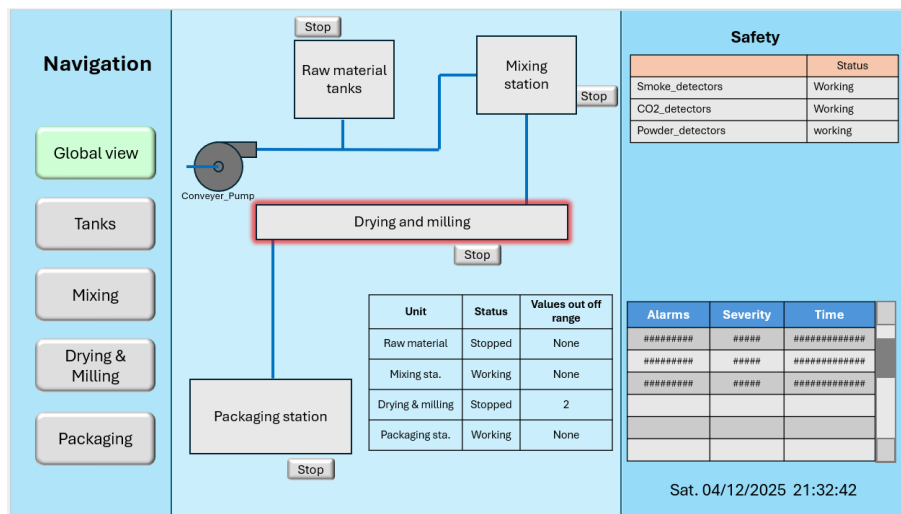


Figure 4: Synoptic view level 1

The screen is divided into 3 main areas. The left side is dedicated to navigation; the buttons allow to navigate across the different views and levels and get back to the global process overview. The middle part displays the global view of the plant with its subunits. A Stop button is located next to each block to interrupt the operations in case of emergency. A table summarizes the status (working/stopped) of the units and the number of sensor’s reading out of range. Finally, the right side show the safety informations and alarms. All the controlled devices (motors, actuators, heaters, etc.) are displayed in white (ON) or in dark grey (OFF)

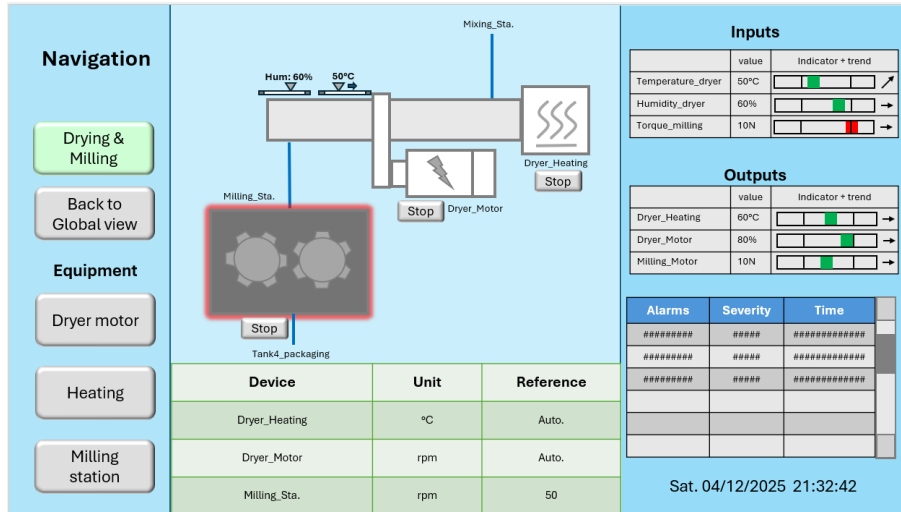


Figure 5: Synoptic view level 2

The Unit view gives a more detail about the input and output process value. The middle part zooms on the selected unit, the bottom now displays the current control parameters with the reference being either entered manually or set automatically. The right side now gives a better overview of the inputs and outputs of the Unit.

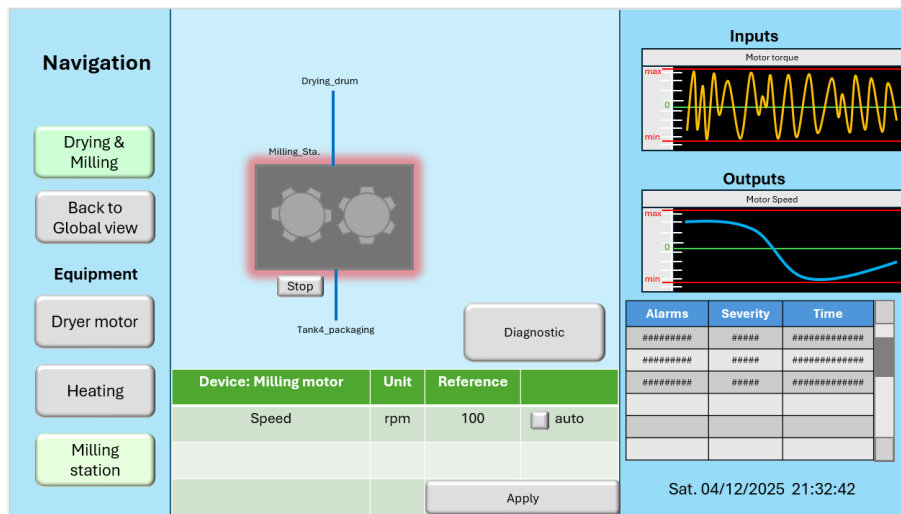


Figure 6: Synoptic view level 3

The Subunit view focuses on a specific equipment of the Unit. In the middle screen, the subunit is highlighted, and a table allows to change and apply control references. The right side displays the history of the different process values of the selected subunits, giving more insight than the previous view. To access the level 4 view, click on "diagnostic"

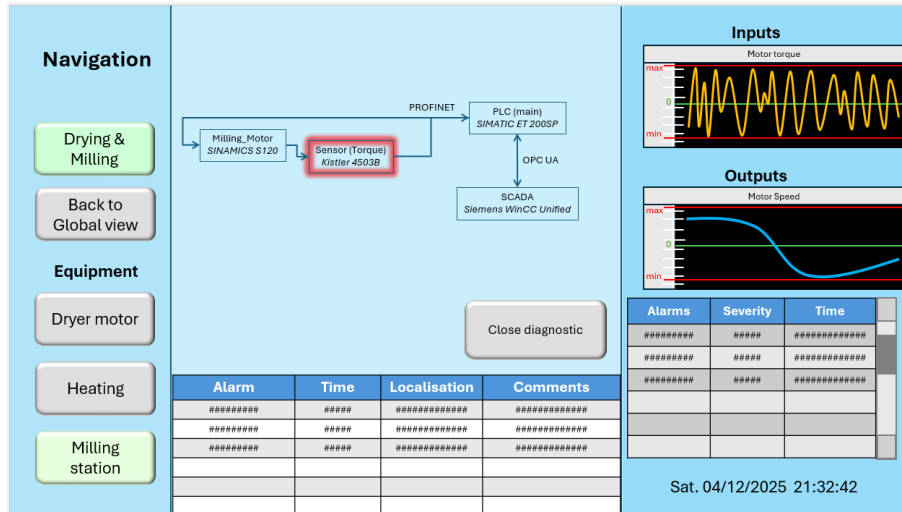


Figure 7: Synoptic view level 4

The diagnostic view displays the selected equipment and its connections the other elements up to the SCADA. The bottom of the window displays more information about the alarm and give comments to the operator about the diagnostic. To go back to the level 3 view, one should click the "close diagnostic" button.

5 Qualitative Dependability Analysis

Summary of FMEA and Safety Controller

We performed a Failure Modes and Effects Analysis (FMEA) for all main components. The analysis showed several fire risks due to heating elements, and identified the safety controller as the single most critical point of failure. To address this, we chose a redundant safety PLC setup to ensure that emergency shutdowns remain available if one controller fails. The full FMEA table can be found in the appendix.

Summary of FTA

We performed a Fault Tree Analysis, and the main hazards (named as "Fire, Explosion or Major Hazard") are triggered by different main scenarios: Fire Propagation from either the Mixing Station or Drum Dryer, a Material Spillage & Contamination or Explosion from Dust Ignition. Fire propagation from drum dryer can happen either by a fire started in mixing station or drum dryer. In each case, if a smoke detector fails at the same time, the fire will not be detected. The root causes of this risk can either be a heater stuck at ON position (PLC or relay fault), a temperature sensor failure or a safety relay/control failure.

Material spillage & contamination can happen due to a stuck valve at silo or buffer outlet along with the failure of mechanical overrides and level monitoring system. A valve failure can be happen because of the actuation failure or signal disconnection.

Explosion from dust ignition occurs when dust sensor fails to detect a hazard and an overheating element ignites dust. The sensor failure can happen due to a power loss or a blocked sensor. Overheating element can ignite dust because of an ongoing fire hazard. The full FTA tree can be found in the appendix.

As we can see from this analysis, smoke detector and dust level sensor are critical points of the design and have to be functioning permanently. That's why they have to be installed in redundant locations.

Conclusion

For us, designing the automation for the Chocolate Powder Factory has been a very insightful experience. Designing your own plant provides a practical perspective that you simply cannot get purely from lectures alone.

Looking at our plant, we think one of its strengths is the strong focus on safety, including multiple redundant safety systems. However, there is also definitely room for improvement in other areas. If we were to build this as a real plant, we would greatly benefit from the guidance of a process expert, particularly for refining processes such as drying and packaging.

It is also worth mentioning that the Siemens workshop was quite helpful for this project. It gave us initial hands-on exposure to many of the components used, including the PLC system, and provided some insight into how an automation engineer typically "thinks" about problems.

.0.1 Figures for Qualitative Dependability Analysis

Find the figures on the next page.
This page was intentionally left blank.

Table 1: FMEA Table for ChocoMation Automation (excerpt)

Component name/ID	Function	Failure mode	Failure cause	Failure effect (local)	Failure effect (global)	Failure detection	Other provision	Remark
Silo/Buffer Outlet Valve	Dosing material	Stuck open	Actuator jam, signal lost	Buffer overfills, spills	Flooding, material loss, contamination	Buffer level alarm, trend monitoring	Mechanical override	–
			SSR shorted, PLC fault	Overheating, possible boiler	Fire, dust explosion	Overtemp alarm, fire detector	Redundant temperature sensor, hardware safety relay	Fire hazard
Mixing Station Heater (SSR)	Heating	Stuck ON	SSR open	Product not heated	Poor product quality, batch loss	Low temp alarm, process check	–	–
			Relay stuck, control error	Overheated drum, possible ignition	Fire, explosion, system shutdown	Drum temp alarm, smoke detector	Redundant overtemp protection, fire-rated enclosure	Fire hazard
Drum Dryer Heater	Air heating	Stuck ON	Overload, object jam	Product flow interrupted, possible gear damage	Production halt, possible equipment damage	Motor current monitoring, torque sensor	Overload clutch, automatic shutdown	Safety stop, quality loss
			Servo fault, control loss	No cut, bags jam at exit	Production block, rework needed	Motor current monitoring, jam alarm	Servo redundancy or manual bypass	–
Packaging Cutting Servo	Cut/seal film	Fails to move	Feedback fail	Machine damage, injury risk	Equipment loss, personal hazard	End stop, E-stop, torque limit	Interlocked access door, dual-channel E-stop	Safety relevant
			Dirty lens, faulty wiring	Bags unsealed, powder loss	Product spillage, quality complaints	Foil tension/trend, presence sensor	Dual sensor or signal plausibility check	–
Load Cell (Packaging)	Measure weight	Signal lost/stuck	Cable break, overload	Under/overflow of bags	Out-of-spec product, complaints	PLC plausibility check, QC sampling	Cross-check by periodic sample weighing	Quality risk
			Power fail, SW bug	All process stops, loss of control	Process down, safety acts	Watchdog, comm. loss alarm	Manual override, fallback to safety PLC	–
Safety PLC	Emergency/fire logic	Fails to activate	HW/SW/config error	Emergency not handled	Fire/explosion, major loss	Heartbeat, test routines	Dual-channel safety PLC, separate power supply	Highest risk
			Soiled/failed unit	Fire undetected, spreads	Major plant/equipment loss, injury	Routine test, redundancy	Multiple detectors, automatic test	High risk
Fire Detector	Detect fire/smoke	Fails to detect	Blocked, power loss	No dust warning	Explosion risk	Periodic test, redundancy	Redundant dust sensors, regular cleaning	Explosion hazard

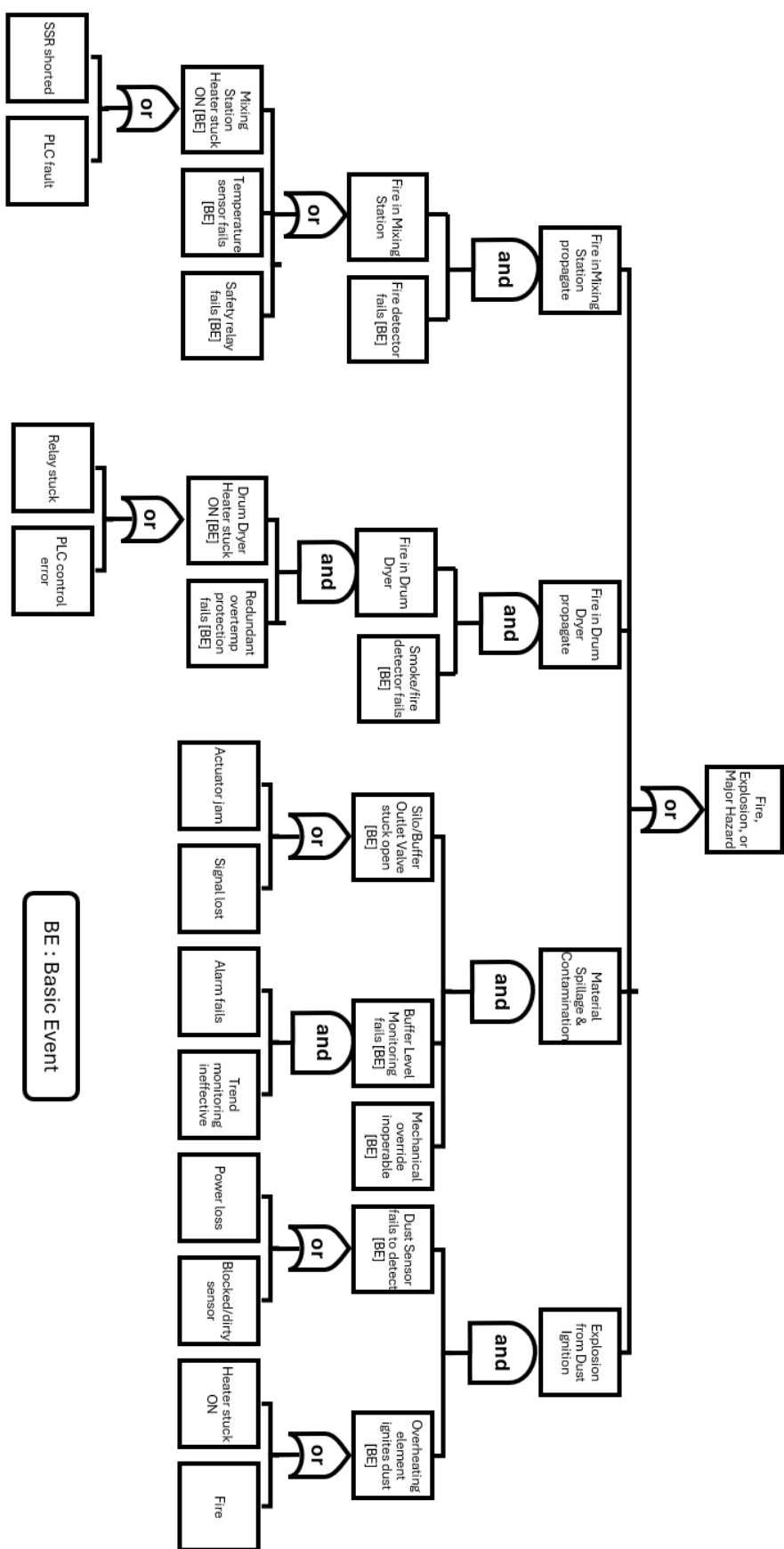


Figure 8: Fault tree analysis

.0.2 Pseudocode for the Automation

Raw Material Handling

Main Controller:

Listing 1: Raw Material Handling Main Controller

```

for tank in tanks:
    if tank.level < TANK_HEIGHT_10CM:
        stop_conveyors()
        trigger_alarm(f"Tank {tank} is out of material!", LEVEL.
            OPERATIONS_WARN)

    if tank.humidity > TANK_HUMIDITY_5_PCT:
        trigger_alarm(f"Tank {tank} has high humidity!", LEVEL.
            QUALITY_WARN)

```

Redundant Safety Controllers:

Listing 2: Raw Material Handling Safety Controller

```

if fire_detected() or estop.pressed():
    for valve in all_material_outlet_valves:
        valve.close()

```

Mixing Station

Main Controller:

Listing 3: Mixing Station Main Controller

```

if vat.temp >= TEMP_CRIT:    # Handled on safety controller
    pass
elif vat.temp >= TEMP_MAX:
    heater.off()
    trigger_alarm("Vat temperature high!", LEVEL.QUALITY_WARN)
elif vat.temp < TEMP_SET - TEMP_HYS:
    heater.full_on()
else:
    heater.set((TEMP_SET - vat.temp) * Kp)    # simple P-trim

if vat.level < LEVEL_MIN:
    agitator.off()
    trigger_alarm("Vat level low mixer stopped!", LEVEL.
        OPERATIONS_WARN)
else:
    agitator.on()

if vat.level > LEVEL_MAX:
    feed.off()
    trigger_alarm("Vat level high feed stopped!", LEVEL.
        OPERATIONS_WARN)

```

Redundant Safety Controllers:

Listing 4: Mixing Station Safety Controller

```

if vat.temp >= TEMP_CRIT:
    alarm_light.on()
    fire_extinguisher.on()
    shutdown_all_machinery()
    trigger_alarm("Vat temperature CRITICAL!", LEVEL.
        SAFETY_CRITICAL)

if fire_detected() or estop.pressed():
    alarm_light.on()
    fire_extinguisher.on()
    heater.off()
    agitator.off()
    discharge_valve.close()
    trigger_alarm("Emergency Stop / Fire in Mixing Station!", LEVEL.
        SAFETY_CRITICAL)

```

Drying and Milling

Main Controller:

Listing 5: Drying and Milling Main Controller

```

if drum.temp >= TEMP_CRIT:    # Handled on safety controller
    pass
elif drum.temp >= TEMP_MAX:
    dryer.off()
    trigger_alarm("Drum temperature high!", LEVEL.QUALITY_WARN)
elif drum.humidity > HUM_SET + HUM_HYS:
    dryer.full_on()
else:
    dryer.set((HUM_SET - drum.humidity) * Kd)

if mill.torque >= TORQUE_STUCK:
    drum_motor.off()
    mill_motor.off()
    trigger_alarm("Milling gears STUCK!", LEVEL.OPERATIONS_WARN)
else:
    drum_motor.set(DRUM_SPEED)
    mill_motor.set(MILL_SPEED)

```

Redundant Safety Controllers:

Listing 6: Drying and Milling Safety Controller

```

if drum.temp >= TEMP_CRIT:
    alarm_light.on()
    fire_extinguisher.on()
    shutdown_all_machinery()
    trigger_alarm("Drum temperature CRITICAL!", LEVEL.
        SAFETY_CRITICAL)

if fire_detected() or estop.pressed():
    alarm_light.on()
    dryer.off()

```

```

drum_motor.off()
mill_motor.off()
trigger_alarm("Emergency Stop / Fire in Drying & Milling!",
              LEVEL.SAFETY_CRITICAL)

```

Packaging

Main Controller:

Listing 7: Packaging Main Controller

```

# Packaging procedure
if (not foil.present) or (foil.left_cm <= FOIL_LOW_CM):
    filling_valve.close()
    heater.off()
    cutter.off()
    trigger_alarm("Packaging foil missing!", LEVEL.OPERATIONS_WARN)
    wait_until(foil.present and foil.left_cm > FOIL_LOW_CM)

wait_until(bag.present) # empty pouch in place
while bag.weight < FILL_TARGET_G:
    filling_valve.open()
filling_valve.close()

heater.on()
wait(SEAL_TIME_S)
heater.off()
cutter.on()
wait(CUT_TIME_S)
cutter.off()

if buffer.level > BUFFER_OVERFLOW_LVL:
    stop_inflow()
    trigger_alarm("Buffer Tank overflows!", LEVEL.OPERATIONS_WARN)

```

Redundant Safety Controllers:

Listing 8: Packaging Safety Controller

```

if fire_detected() or estop.pressed():
    filling_valve.close()
    heater.off()
    cutter.off()
    trigger_alarm("Emergency Stop / Fire in Packaging!", LEVEL.
                  SAFETY_CRITICAL)

```

Safety System

Redundant Safety Controllers:

Listing 9: Safety System Safety Controller

```

if smoke_co2.detected():
    alarm_light.on()
    fire_extinguisher.on()

```

```
    shutdown_all_machinery()
    trigger_alarm("Smoke detected!", LEVEL.SAFETY_CRITICAL)

if powder.level > DUST_15g_m3:
    alarm_light.on()
    shutdown_all_machinery()
    trigger_alarm("Powder explosion hazard!", LEVEL.SAFETY_CRITICAL
    )

if estop.pressed():
    alarm_light.on()
    shutdown_all_machinery()
    trigger_alarm("Emergency Stop pressed!", LEVEL.SAFETY_CRITICAL)
```