Critical Systems Lab - MESCC
Water Pumping Automated System

Ricardo Mendes 1201779

Arthur Gerbelli 1220201

ISEP, January 2024

Contents

1 Introduction

The current document, is the result of the work done during the first delivery of the CSLAB class.

The document is divided into three parts, each one of them focused on the evaluation topics: **requirements specification** documentation, **rationale for selected technology** and **list of physical sensor and/or actuator** used for the demo.

The system that we are modeling is a Water Pumping System (WPS) for two rainwater wells. These types of systems are essentially used to move water from a lower elevation to a higher one.

A Remote Status Station is also described in the document. Its main function is to give a level of observability of the WPS and to alert the *maintenance team* for a possible failure.

There is also an additional feature. The status of the system should also be visible through a web server.

2 Requirement Specification

2.1 Problem Domain

2.1.1 Stakeholder Needs

Based on the system's description and some clarifications during the classes, we identified the following Stakeholder needs:

SN-1 .1: The water in the WPS must be pumped from a lower level to a higher one.

.2: Every WPS is an independent system; they don't have influence on each other.

SN-2 .1: The status of each element of the wet well needs to be displayed in a Remote Status Station (RSS).

.2: The RSS must display the water level, the pump status, an alarme and a button to disable the alarm.

.3: The alarm must be ON when a problem in the system is identified.

SN-3 The status information must be accessible through a web page.

SN-1 is WPS specific, **SN-2** is RSS specific and **SN-3** is Web Server specific.

2.1.2 System Context

For a better understanding of the system, we developed an external view, and so, identified external entities that do not belong to the system but interact with it. The following diagram is the output of this analysis:

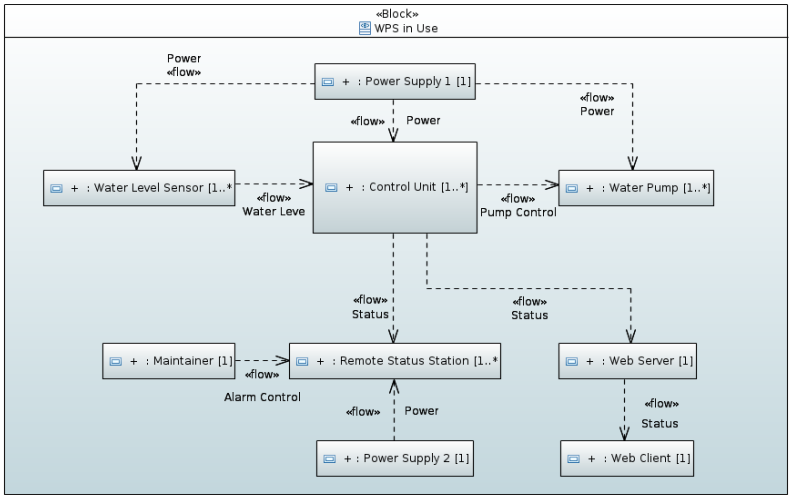

Figure 1: System Context

Although some elements represented in the diagram are part of the WPS (sensor, control unit, pump and RSS), we divide them into subsystems with their own responsibilities and interactions.

By decoupling the WPS responsibilities, we are simplifying it and turning the critical system requirements easier to grasp and model.

The main identified external entities are: **Power Supply**, **Maintenance Team** and **Web Client**.

Please notice the independent Power Supply for the Control Unit and the RSS as a way to deal with the critical requirements.

2.1.3 Use Cases

By analyzing the Stakeholder Needs, we can see that the main goal of the WPS is to control the water level inside the wet well. This goal can be captured in the model as the *"Control Water Level"* use case of the *Control Unit In Use* system context.

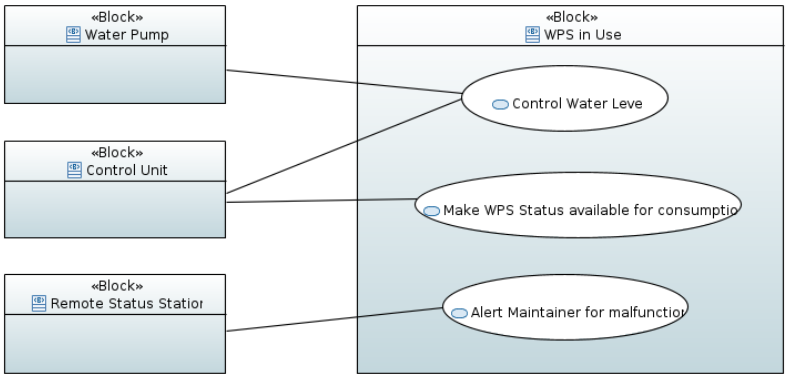

Figure 2: Use Case diagram

A closer look at the use case *"Control Water Level"* gave rise to the below activity

diagram. No alternative scenario was modeled.

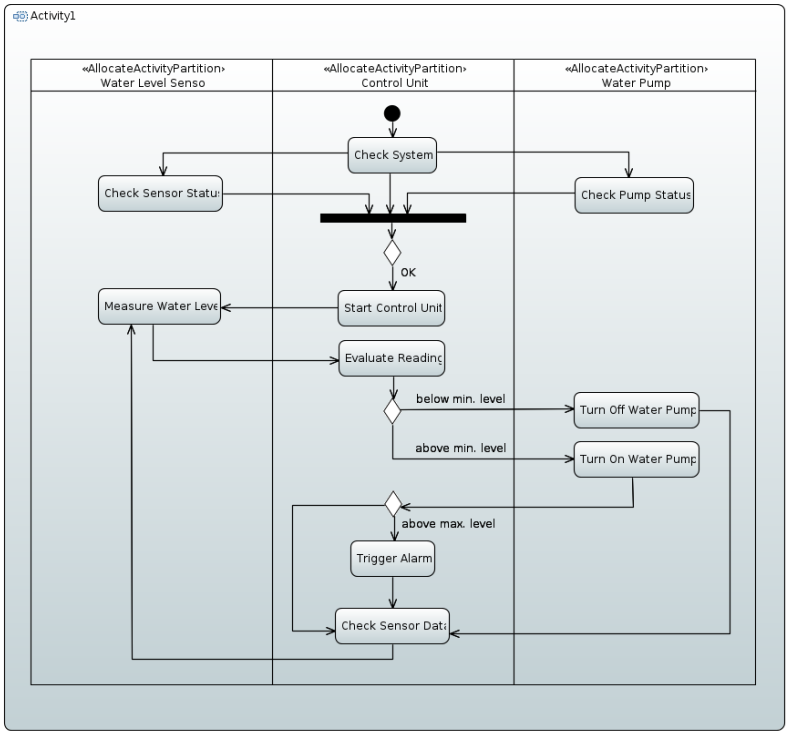

Figure 3: Use Case Activity diagram

2.1.4 Measure of Effectiveness

To be able to describe the performance of the system, some quantifiable characteristics of the WPS were identified:

- Energy Consumption in *kilowatts per hour*
- Wet Well Capacity in *cubic meters*;
- Water Inflow in *liters per second*;
- Water Outflow in *liters per second*.

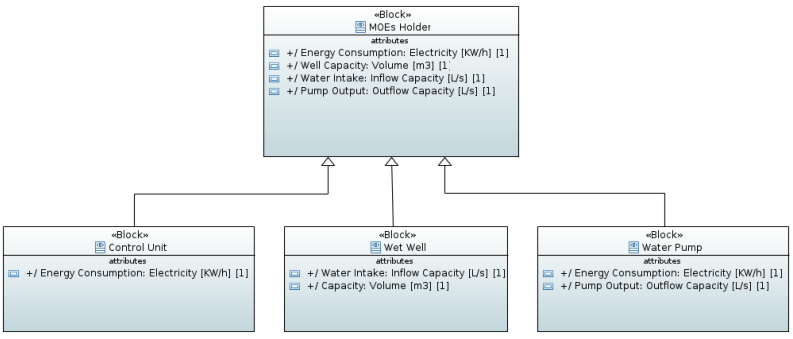

Figure 4: Measure of Effectiveness diagram

As illustrated, each characteristic can be related to a specific element of the WPS.

2.1.5 Functional Analysis

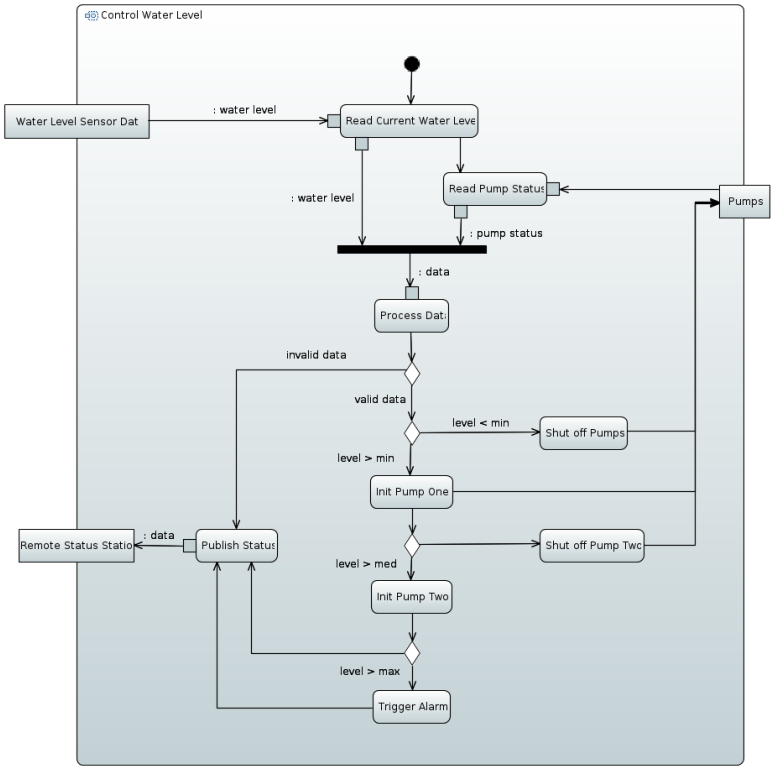

Figure 5: Functional Analysis diagram

2.1.6 Conceptual Subsystems

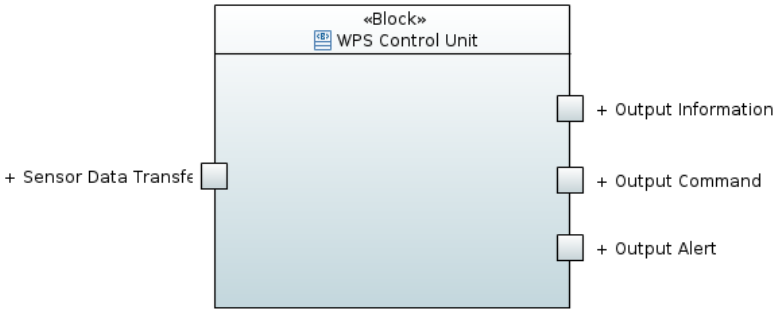

Figure 6: Conceptual Subsystem Communication diagram

2.1.7 Traceability to Stakeholder

2.2 Solution Domain

2.2.1 System Requirements

SR-1 **.1:** While the water level is above the minimum level, WPS shall have a pump working.

.2: When the water level is below minimum level, WPS shall have all pumps stopped.

.3: If the water level is above the maximum level, then the WPS shall trigger an alarm at the Remote Status Station (RSS).

.4: A second pump shall be turned on only when the water level is above 2/3 the maximum water level.

.5: When only one pump is available, the maximum water level shall be reduced to 2/3.

SR-2 s

The status of all WPS shall be displayed on all RSS.

.2: If the alarm is ON, the button in the RSS shall only disable it.

SR-3 The status of all WPS shall be visible on one web page.

2.2.2 System Structure

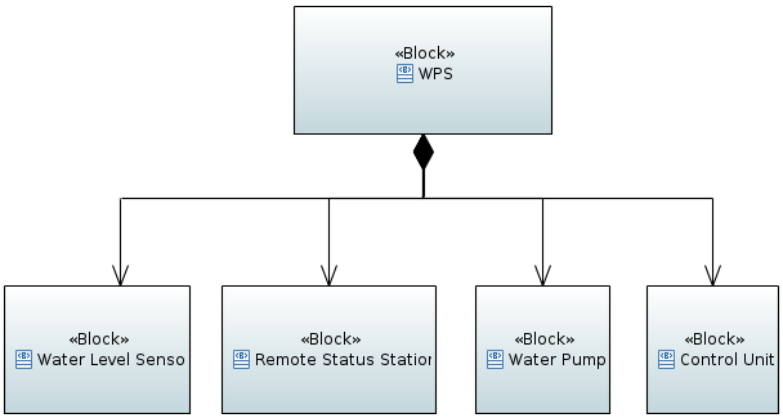

Figure 7: System Structure Diagram

2.2.3 System Behavior

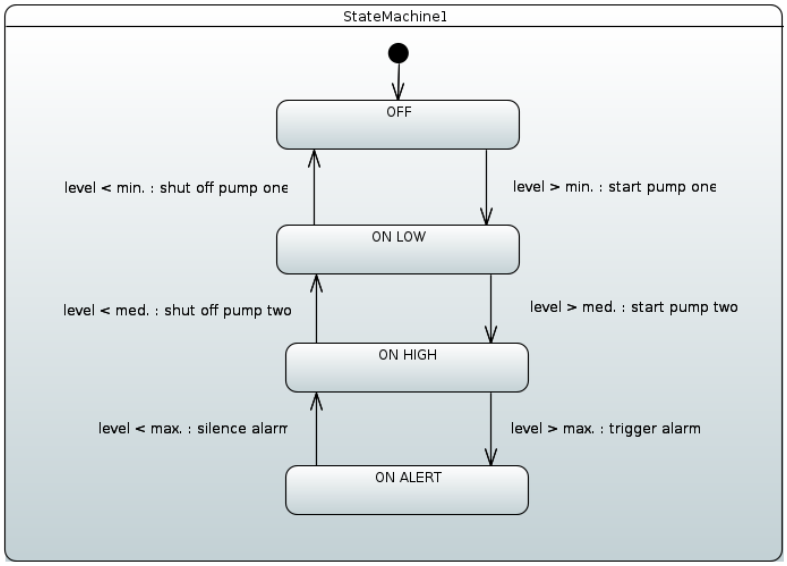

Figure 8: State Machine

2.3 Analysis of safety and reliability

H-1:
- **Description:** One of the pumps stops working.
- Cause: Mechanical problem.
- Effect: Lost of redundancy and reduction of system performance.
- **Mitigation:** Reduce the maximum water level to 2/3 and trigger alarm.

H-2:
- **Description:** The two level sensors give contradictory readings, i.e. one above max and one below min.
- Cause: Sensor malfunction, connection issues.
- Effect: Inapropriete system behavior.
- **Mitigation:** Choose a worst case or compare with the last reading to find the fault. Trigger alarm.

H-3:
- **Description:** Power shortage.
- Cause: Multiple causes
- Effect: Complete failure of the system.
- **Mitigation:** RSS with independente power supply and trigger alarm.

H-4:
- **Description:** Both pumps stopped working.
- Cause: Mechanical problem.
- Effect: Complete failure of the system.
- **Mitigation:** Trigger alarm.

H-5:
- **Description:** RSS are not getting information from WPS.
- Cause: Connection issues or Messagem broker stoped working.

- Effect: Wrong status readings.
- **Mitigation:** Trigger alarm or remove broker as single point of failure by using protocols like DDS.

H-6:
- **Description:** RSS stops working.
- Cause: Malfunction.
- Effect: Unknown WPS status.
- **Mitigation:** Have redundancy by having multiple RSS and each one displaying all statuses from all WPS.

H-7:
- **Description:** A pump doesn't turn OFF when the water level in bellow minimum.
- Cause: Mechanical problem.
- Effect: Pump overheating and complete failure.
- **Mitigation:** Trigger alarm.

3 Selected Technologies

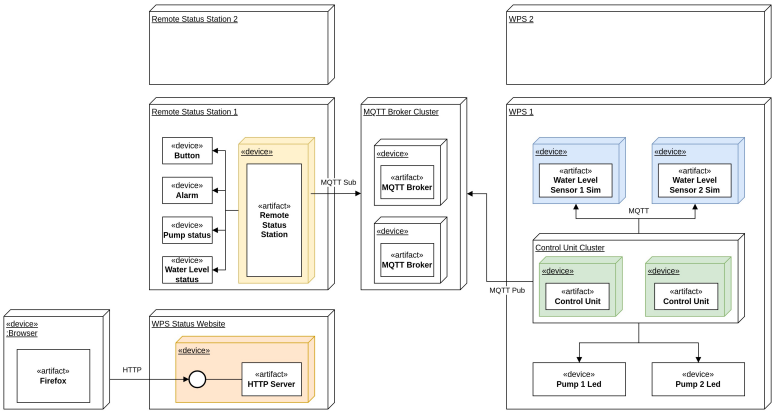

Figure 9: Deployment diagram

4 List of physical sensors/actuators

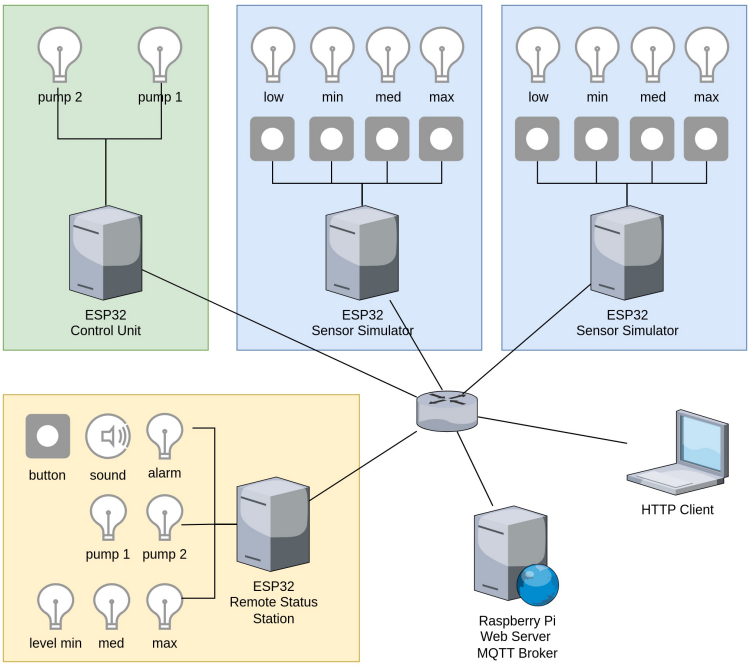

Figure 10: Network diagram