Critical Systems Lab - MESCC
Water Pumping Automated System

Ricardo Mendes 1201779

Arthur Gerbelli 1220201

ISEP, January 2024

Contents

1 Introduction

This document is a follow-up of the previous work.

It takes into account the feedback received during the last presentation and also the current objectives of the exercise.

2 Requirement Specification

2.1 Problem Domain

2.1.1 [UPDATE] Stakeholder Needs

Although not mentioned on the assignment, we choosed to add some changes to the Stakeholder Needs that are paramount to understand the next chapters.

- **SN-1.3** Every WPS will have two pumps and two water level sensors to achieve a certain level of redundancy and reliability on the system.
- **SN-1.4** To improve the systems performance, and given that we have one unused water pump, this pump should only be used when the water level is above medium.
- **SN-1.5** In case that only one water pump is operational, the max capacity of the WPS should be lower.

2.1.2 [UPDATE] System Context and Use Cases

During the previous analysis of the System's Context and Use Cases we want to split the WPS system as a whole. The main objective is to split responsabilities and so, simplifying the clarification of the requirements. Another output is the creation of two easy to grasp systems: on a simple system we can achieve a system with obviously no bugs, on a complex one we can only wich to achieve a system with no obvious bugs.

The update were made in the Use Case diagrams:

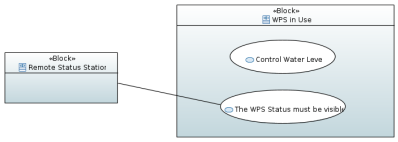

Figure 1: Use Case diagram - WPS

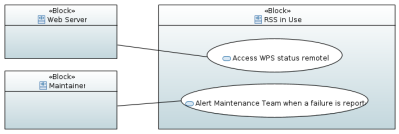

Figure 2: Use Case diagram - RSS

The activity diagram of the use case "Control Water Level", also shows that WPS can be seen as an independent system regarding the RSS.

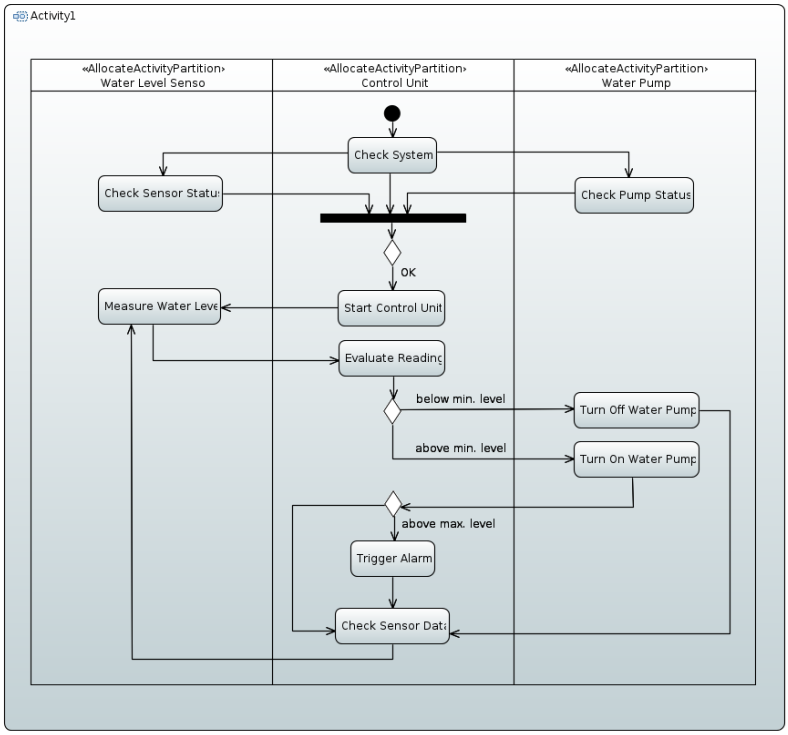

Figure 3: Control the Water Level inside the well

2.2 Solution Domain

Show traceability (system context and system subsystems)
Model the reality
Specify how sensor works

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 **.1:** 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 a web page.

2.2.2 System Structure

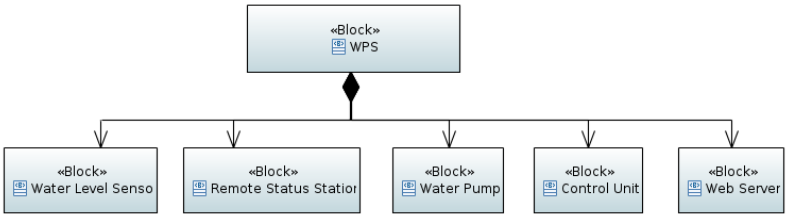

Figure 4: System Structure Diagram

2.3 Analysis of safety and reliability

Given that we are dealing with a critical system, the analysis of safety and reliability as bigger impact on the implementation of the solution.

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: Inappropriate system behavior.
- **Mitigation:** Choose a worst case or compare with the last reading to find the fault. Always trigger the 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: Unknown status of the system.
- **Mitigation:** Implement a cluter of MQTT Brokers or remove this single point of failure by adopting 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.

Most of the hazards listed could be handled as non-functional requirements. Because of that, a more detailed description of some of them is needed.

H-1 and **H-4** touches on the redundancy of the water pumps. Because having an unused water pump would mean a reduced performance of the system, we choose to use the two pumps even when the system is healthy. The second pump is only used when the water level is high. If, for some reason, one of the pumps is not working, the system will reduce the max capacity of the well and trigger an alarm to alert the maintenance team.

H-2 is interesting because introduces a problem that cannot be answered with a reliable voting system. If the reading of both sensor are too unequal, there must be a way to distinguish between the wrong and the correct data. There are three possible ways to deal with the issues: choose a master and a slave sensor, retain the previous input and compare it with the current one, or choose the worst case.

H-3 and **H-6** illustrates the importance of the RSS. During a localized power shortage on the well, the RSS should not be affected and so, still be able to alert the maintenance team. Having two RSS in the building also assures redundancy, specially if they have separated power supplies.

H-5 is sensible to a special limitation of having only one system dealing with the main communication. A single MQTT broker is also a single point of failure that could jeopardize the whole system. Having a cluster of brokers or using a middleware like DDS is a way to mitigate or even remove completely this risk.

3 Implementation

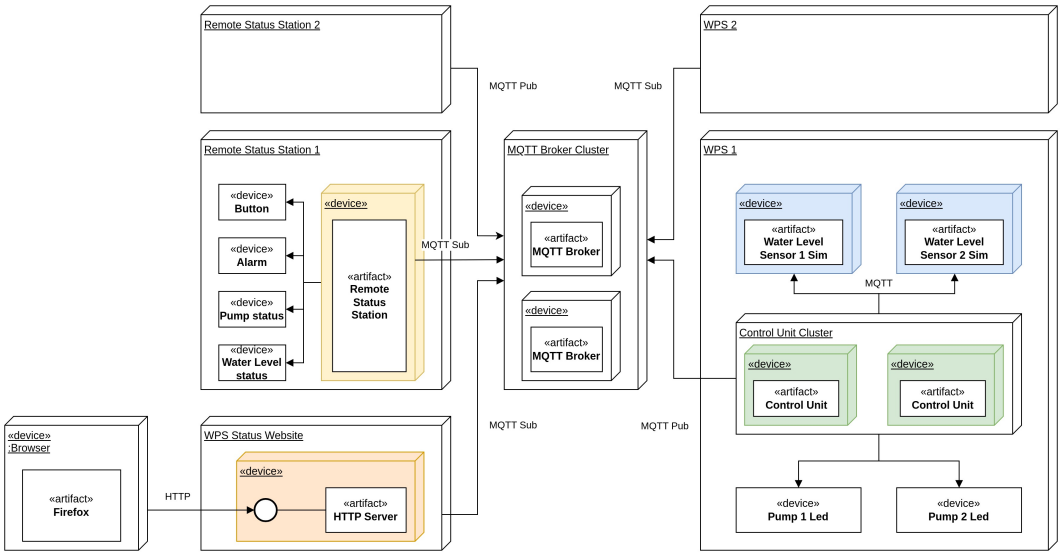

Figure 5: Deployment diagram

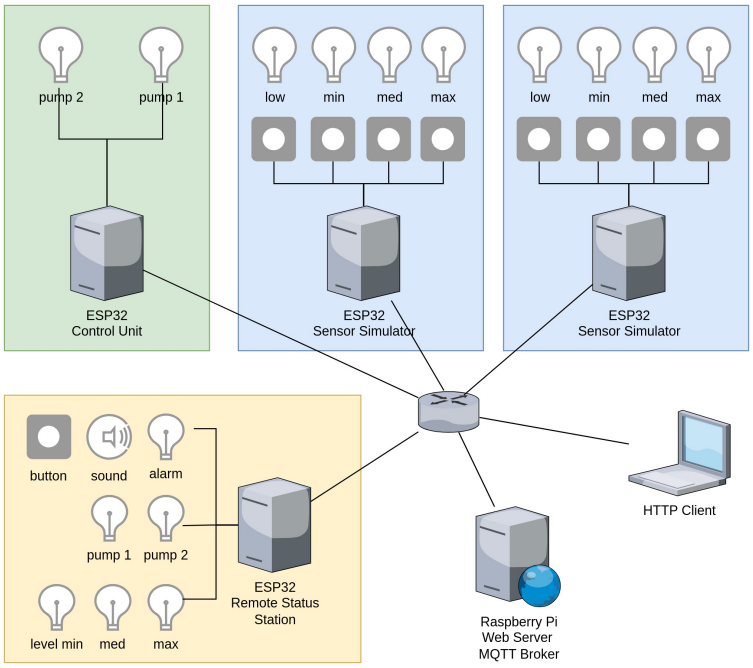

Figure 6: Network diagram