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 be used when the water level is above 2/3 of the well max capacity.
- **SN-1.5** In case that only one water pump is operational, the max capacity of the WPS should be lower.

SN-1.4 and SN-1.5 are the result of the stakeholder capacity to describe the system performance using the identified *Measure of Effectiveness*. The wet well capacity and the input flow can be greater if we use the second pump instead of leaving it on stand-by to be used during failure.

As described in the Stakeholder Needs, the second pump will work only if the water level is above 2/3 of the well capacity. In case that one of the pumps stops to be operational, an alarm will be triggered to alert the maintenance team, and the max water level will be reduced.

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:

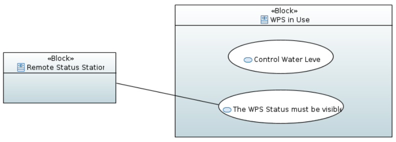

Figure 1: Use Case diagram - WPS

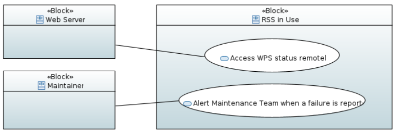
«Block»
Web Server
«Block»
RSS in Use
Access WPS status remotel
«Block»
Maintainer
Alert Maintenance Team when a failure is report

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. The interactions are between the sensors, the water pump and actuator and the control unit.

The most importante externality of the WPS -in this academic context- is give visibility to its internal status.

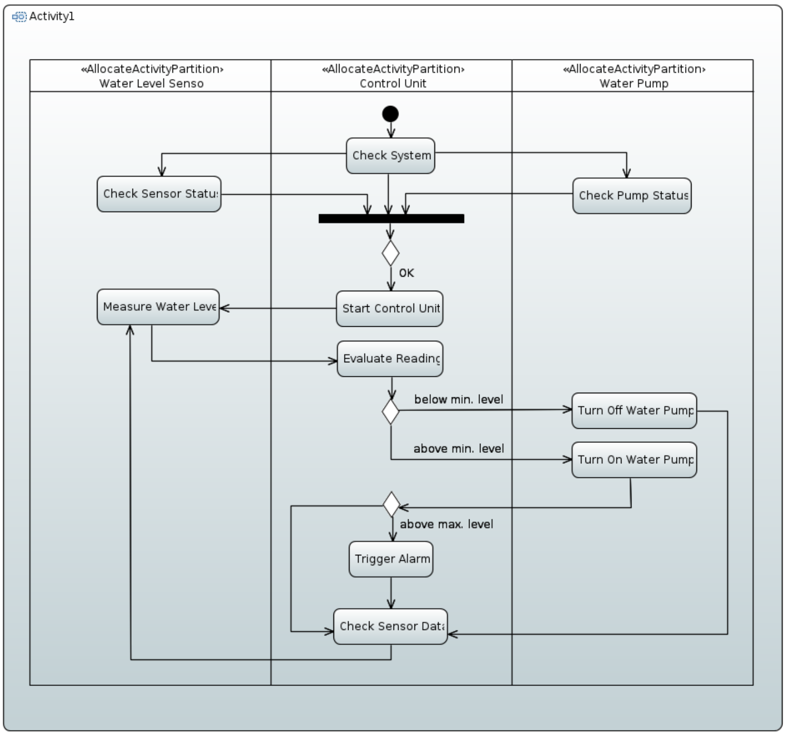

Figure 3: Control the Water Level inside the well

2.2 Solution Domain

Show traceability (system context and system subsystems)

Model the reality

Specify how sensor works

2.2.1 Hazard Analysis

Given the critical nature of the system, we reintroduced here an updated analysis if its hazards. This list maps directly to the Stakeholder Need SN-1.3 but goes a little bit further.

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:** Both pumps stopped working.

- Cause: Mechanical problem.
- Effect: Complete failure of the system.
- **Mitigation:** Trigger alarm.

H-3:

- **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.

H-4:

- **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:** 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. Tirgger the alarm if the system in unable to achieve a consensus.

H-5:

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

H-6:

- **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-7:

- **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-8:

- **Description:** Control Unit stops working.
- Cause: Malfunction, bug.
- Effect: Total failure of the system.
- **Mitigation:** Have redundancy by having a cluster of nodes running the Control Unit. If the number of nodes is 3 we can implement a voting system and run the same process with the same input in parallell. This would improve the system fault tolerance.

The main output of this analysis is the update of the System Requirements.

2.2.2 System Requirements

!!!!!!!!!!!!! Change color of new requirements !!!!!!!!!!!!!!!!!!!!! !!!!!!!!!!!!! Update Traceability !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

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.

.6: If the readings of the sensor are uneven to a level of 20cm, the system should choose the worst case scenario, following the table below:

		sensor #1			
		0	**1**	**2**	**3**
sensor #2	**0**	0	0	0	3
	1	0	1	1	3
	2	0	1	2	3
	3	3	3	3	3

0 = below min; **1** = above min; **2** = above med; **3** = above max.

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.

.3: The RSS shall have an independent power supply from the WPS.

.4: The alarm on the RSS shall have an independent power supply from the RSS itself and from the WPS.

SR-3 .1: The status of all WPS shall be visible on a web page.

SR-4 .1: To improve the whole system's reliability and availability, a cluster of MQTT brokers should be deployed.

2.2.3 System Structure

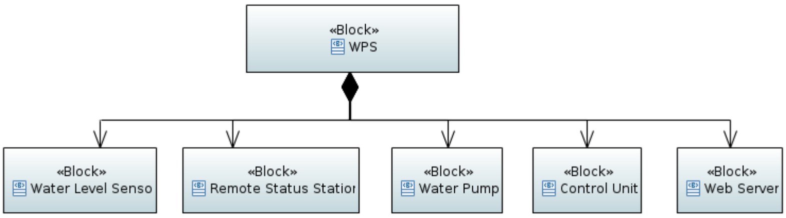

Figure 4: System Structure Diagram

3 Implementation

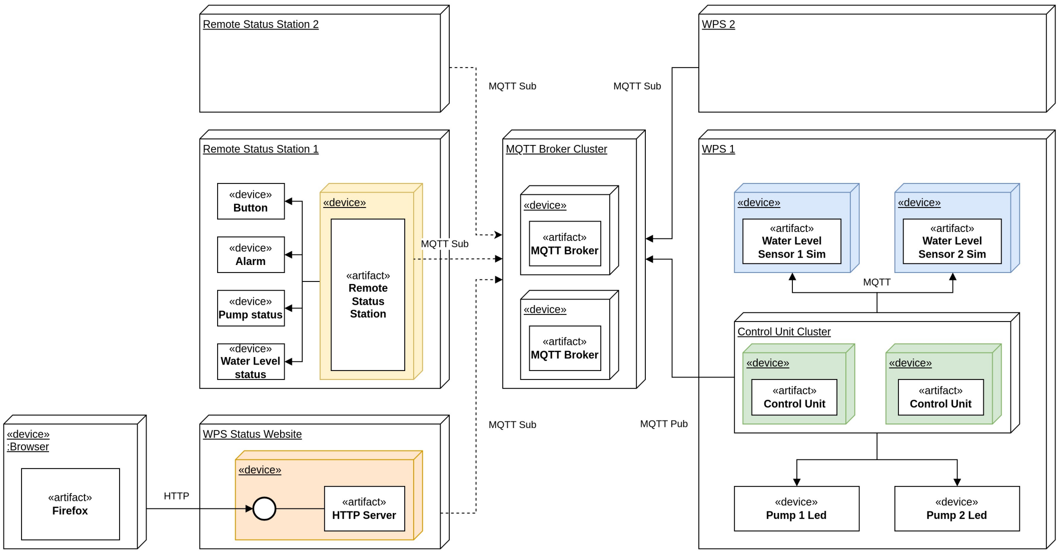

Figure 5: Deployment diagram

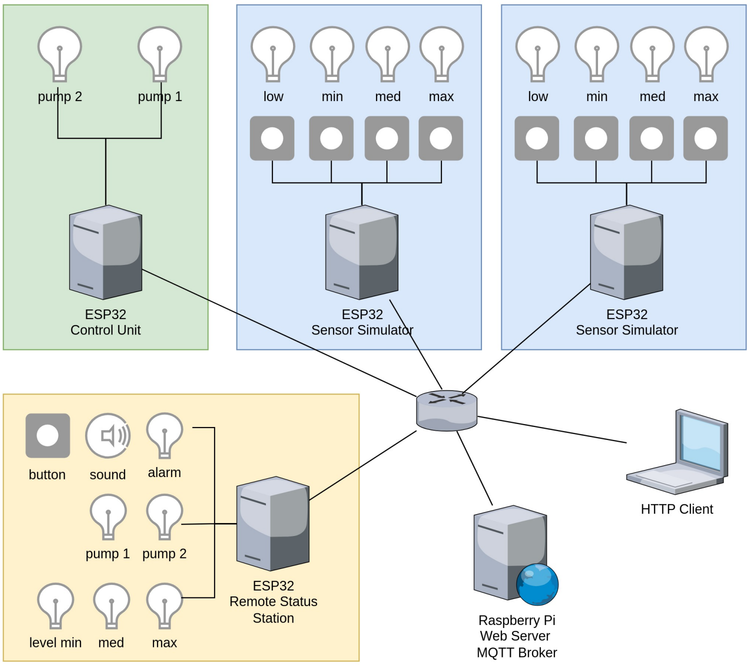

Figure 6: Network diagram