Critical Systems Lab - MESCC
Water Pumping Automated System

Ricardo Mendes 1201779

Arthur Gerbelli 1220201

ISEP, January 2024

Contents

1 Introduction

2 Requirement Specification

2.1 Problem Domain

2.1.1 Stakeholder Needs

SN-1 .1: The water in the wet well must be pumped to a higher level.

.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.

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

2.1.2 System Context

2.1.3 Use Cases and 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.

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

SR-2 The status of all WPS shall be displayed on all RSS.

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

2.1.4 Measure of Effectiveness

2.1.5 Functional Analysis

2.1.6 Conceptual Subsystems

2.1.7 Traceability to Stakeholder

2.2 Solution Domain

2.2.1 System Structure

2.2.2 System Behavior

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.
- Effect: Wrong status readings.
- **Mitigation:** Trigger alarm.

H-6:
- **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

4 List of physical sensors/actuators