ELE3305

Design Report

Student Name: Kate Bowater

Student Number: U1019160

Due Date: 8 April 2024

# Executive Summary

Table of Contents

[Executive Summary 2](#_Toc162088283)

[Application Scenario 2](#_Toc162088284)

[Specifications 5](#_Toc162088285)

[Overview of System 5](#_Toc162088286)

[Data Encoding/Scaling 5](#_Toc162088287)

[ICT security risks 6](#_Toc162088288)

[Conceptualisation 6](#_Toc162088289)

[References 6](#_Toc162088290)

# Application Scenario

Aquaponics is defined as a closed system where fish and plants survive and grow together by providing each other with nutrients. In this system, rather than filtering out waste from the tanks, the waste from fish is consumed by bacteria and converted into nitrates which plants use for nourishment [1] [2]. The thriving plants then release oxygen into the water which circulates back to the fish. In this system, the delicate balance of water pH, temperature and oxygen levels are vital for a happy ecosystem [3], and so requires constant monitoring to ensure fish and plants are obtaining adequate nutrients and not stressed out.

Implementing automated monitoring and maintenance to the aquaponics system using Internet of Things (IoT) will take the strain off the owner of the aquaponics system to ensure all these elements are measured and addressed in a timely manner, reducing the risk of plant and fish illness or death caused by lack of supervision [1] [4].

# Specifications

## Sensors

The details of the sensors required to monitor the aquaponics system include the following:

Table 1: Sensor information

|  |  |  |  |
| --- | --- | --- | --- |
| **What is Measured** | **Ideal Range** | **Units** | **Recommended Sensor** |
| Dissolved Oxygen (DO) | 5-8 | mg/L | Atlas DO probe |
| pH | 6.5-8 | - | DFROBOT-SKU:SEN0169 |
| Water Temperature | 18-30 | °C | DFROBOT-DS18B20 |

## Control

To control the aforementioned factors of the tanks, a PLC program can provide automation of required equipment. For dissolved oxygen, an air pump will add more O2 to the water and turn off when the required level is reached.

The water temperature is controlled using a heater to increase the temperature, and when the water temperature is too high then a water pump will activate to increase flow through the tank to cause temperature to decrease.

The pH level is a complex factor closely tied to oxygen and temperature levels. It is assumed in a well-balanced system that the pH level will be self-maintained and should not fall outside the ideal range, but if it does it requires direct intervention from the user due to complex associations to other variables, so only an alert will be sent to the user.

These actions are all outlined in Table 2 below. If any values outside of the ideal range mentioned in Table 1 are detected, the PLC will activate to maintain balance of the aquaponics system. It should be noted that the provided actions are not exclusive (as temperature, DO and pH can directly affect each other), but are the only ones provided to maintain simplicity for the conceptual design of the system.

Table 2: Control of sensor readings

|  |  |  |
| --- | --- | --- |
| **Sensor** | **Problem** | **Required Action** |
| DO | < 5 mg/L | Turn on air pump |
| > 8 mg/L | Turn off air pump |
| pH | < 6.5 | Notify user |
| > 8 | Notify user |
| Water Temp | < 18 °C | Turn on heating system |
| > 30 °C | Turn on water pump |

## Power Supply

For the system to run over Internet of Things (IoT) the software can be implemented on a small device such as Raspberry Pi. This can be connected to a small power supply either via mains or utilise solar. It could also incorporate battery back up to ensure upkeep of the tanks in the event of power loss. The simplicity of this aquaponics system can then be scaled up to meet larger demands including aquariums and farming [2].

# Overview of System

\*\*\*

Documentation of the existing system including an overview of the relevant protocols used in the context of the project and an evaluation of why they are appropriate for the application or why other protocols would be more suitable.

\*\*\*

## Network

The information obtained from the sensors in Table 1 are sent via LoRaWAN (long range wide area network) to The Things Network (TTN). A message broker, in this case Mosquitto, uses MQTT protocol to take these messages as subscriptions. MQTT is appropriate for this situation because of the simple, small amounts of data being sent from the tank’s sensors which do not require large headers or bandwidth. HTTP is another protocol that could have been used for this scenario, but MQTT is low cost, reliable in unstable connections, and provides scalability unlike HTTP which requires more resources to run [6]. The request-response model of HTTP is also a disadvantage compared to MQTT which can send messages without direct authentication to the nodes.

Using TTN, the message broker then sends the message through a local network to the subscribed nodes: Node-Red, OpenPLC, and a web-based human machine interface (HMI). Figure 1 shows an overview of the network and connected devices.

The protocol to connect the sensors and devices to OpenPLC is Modbus TCP/IP. Using TCP/IP allows the data to be carried over ethernet as it is already a widely used protocol and provides compatibility with preexisting ethernet infrastructure [10]. As the data being transferred is only small, Modbus is also suitable for this application due to its limited packet transfer size of 260 bytes [11].

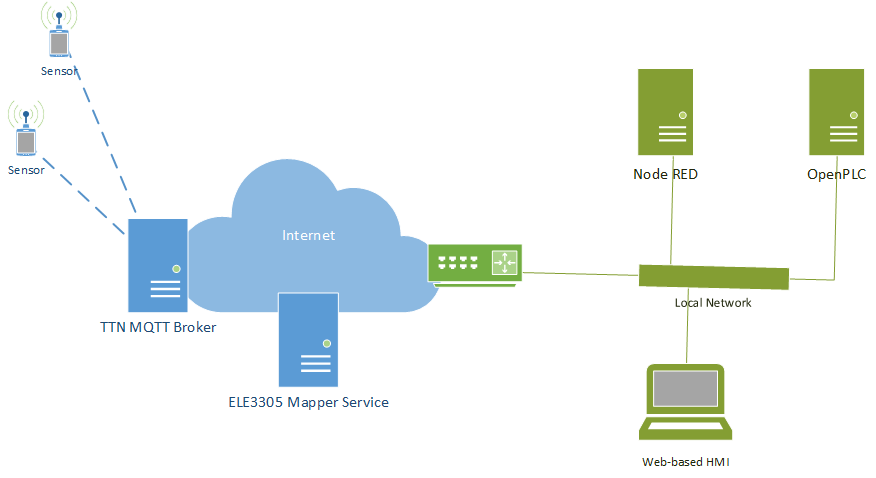


Figure 1: Network layout for aquaponics system

## Node-Red

Node-Red is used to implement the IoT network. This creates flows for the decoding and scaling of the received information before forwarding to OpenPLC and HMI. This also provides the interface for the user to interact with the system where they can view alerts and controls, as mentioned below under HMI.

Use of Node-Red is appropriate as it is easy to set up with visual nodes for flow creation. This means other technicians can easily access and interpret the layout to make changes for the user if needed. Connection to other nodes on the IoT network is also easy to manage using the flows, and the built-in UI dashboard is a necessary feature for the user and is conveniently provided in Node-Red’s features.

## OpenPLC

OpenPLC is used to implement the logic that will provide automated control to the aquaponics system, as laid out in Table 2 under specifications. The circuit is created and uploaded to the OpenPLC software which is connected to Node-Red to be implemented in the flows.

The actions in Table 2 can be described using pseudocode below. For DO and water temperature, the pumps will activate automatically but the design will also allow the user to turn on or off the air pump and water pump as needed. The water heating does not have the same functionality because if the heater is left on and reaches the high temperature threshold then it is simply wasting power and risking the health of the fish and plants.

Pseudocode for aquaponics system:

|  |
| --- |
| If dissolved\_oxygen is low OR airpump\_button\_on:   * Turn on air pump   Else If dissolved\_oxygen is high OR airpump\_button\_off:   * Turn off air pump   If pH\_level is high OR low:   * Turn on alert   If water\_temp is low:   * Turn on heater   Else turn off heater  If water\_temp is high OR waterpump\_button\_on:   * Turn on water pump   Else if water\_temp is not high OR water\_temp is low OR waterpump\_button\_off:   * Turn off water pump |

## HMI

The human-machine interface (HMI) is the final node which the user can access using a browser in kiosk mode. This will only allow access to Node-Red’s user interface (UI) and will display information on the pH, DO and water temperature of the tanks. This can be implemented on any tablet device for convenience so the user can easily transport it while checking the tanks of the aquaponics system.

# Data Encoding/Scaling

Detail the data encoding and scaling across the various transmission channels in the system.

Scaling for pH: whole range needs to fit into 0-14.

Scaling for water temperature: range needs to fit into -55 to 125 C.

Scaling for DO: range needs to fit into 0-100 mg/L (https://atlas-scientific.com/probes/dissolved-oxygen-probe/)

# ICT security risks

A discussion of potential ICT security risks in the system and potential ways to alleviate those risks.

\*\*\*

Potential unauthorized access to HMI – requires physical presence. To mitigate this the device can be locked with a password only the user knows.

“The main security threats of all the used protocols for IoT derive from the following aspects: authentication, authorization and package encryption” [7]. “By default, the messages transferred over the network are not secured in any way, being sent in plaintext. TLS is used to secure the connections but that can lead to overheads related to bandwidth and CPU” [6].

IoT threats:

* Tampering with data - sending incorrect information or changing [7]
* DDOS attacks could occur – one of the most common attacks in IoT [6] [7].

However there is no sensitive information being transmitted through the network – just the sensor date – so risk of fraud or identity theft is minimal.

“Most of the IoT devices are vulnerable due to bugs on protocols implementation, device management issues, or improper handling of communication messages [[17](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8779830/#B17-sensors-22-00567)]. In order to fix such issues, the developers need to patch the IoT devices through firmware updates. Unfortunately, most of the IoT devices are not capable of being updated as they are not designed to receive updates over-the-air [[18](https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8779830/#B18-sensors-22-00567)]. Thus, it puts billions of IoT devices at risk, as they are incapable of receiving updates and hence remain unprotected, insecure, and vulnerable.” [8]

Modbus TCP is also vulnerable to DDoS attacks as it was originally designed for serial connections so had no security features. [9]

## Risk Mitigation

“Setting up the authorization for each node of the system is a key factor for accessing the exposed resources. Even if a node is compromised it shouldn’t have the permission to perform any malicious operation that can affect the system.” [6]

# Conceptualisation

Conceptualisation and documentation of the system and code to achieve the functionality.

This includes the local network configuration. This needs to include details such as the assumptions you have made, function definitions and shortcomings of the implementation and potential improvements. This section should be supported by block diagrams, flow charts etc as appropriate.

# References

[1] M.M.M. Mahmoud, R. Darwish and A.M. Bassiuny, “Development of an economic smart aquaponic system based on IoT,” *J. Eng. Res.*, Aug 2023, doi: https://doi.org/10.1016/j.jer.2023.08.024.

[2] M. F. Taha et al., “Recent Advances of Smart Systems and Internet of Things (IoT) for Aquaponics Automation: A Comprehensive Overview,” *Chemosensors*, vol. 10, no. 8, Aug 2022, doi: https://doi.org/10.3390/chemosensors10080303

[3] S. Fu, W. Xing, J. Wu, J. Chen and S. Liu, “Research and design of an intelligent fish tank system,” *PLoS ONE*, vol. 18, no. 5, May 2023, doi: <https://doi.org/10.1371/journal.pone.0285105>.

[4] F. A. Z. Shaikh and U. Bhaskarwar, “Smart Aquarium using IoT,” *Int. J. Res. Appl. Sci. Eng. Tech. (IJRASET),* vol. 10, no. 3, Mar 2022. [Online]. Available:<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4089695>

[5] C.-H. Chiung, Y.-C. W, J.-X. Zhang and Y.-H. Chen, “IoT-Based Fish Farm Water Quality Monitoring System,” *Sensors,* vol. 22, no. 17, Sep 2022, doi: https://doi.org/10.3390/s22176700.

[6] A. Zamifroiu et al. “IoT Communication Security Issues for Companies: Challenges, Protocols and The Web of Data,” *Proc. 14th Int. Conf. Bus. Exc. 2020*, vol. 14, no. 1, pp. 1109-1120, doi: 10.2478/picbe-2020-0104.

[7] B. Russell and D. Van Duren, “Practical Internet of Things Security,” Packt Publishing, 2016.

[8] M. Hunain et al. “Preventing MQTT Vulnerabilities Using IoT-Enabled Intrusion Detection System,” *Sensors*, vol. 22, no. 2, doi: 10.3390/s22020567.

[9] E. Gamess, B. Smith and G. Francia III, “Performance Evaluation Of Modbus Tcp In Normal Operation And Under A Distributed Denial Of Service Attack,” *Int. J. Comp. Net. Comm. (IJCNC)*, vol. 12, no. 2, doi: 10.5121/ijcnc.2020.12201.

[10] *Introduction To Modbus TCP/IP*, Acromag, Wixom, MI, USA, 2005.

[11] *Modbus Application Protocol Specification,* v1.1b3, Modbus, Andover, MA, USA, 2012.