Underwater Swarm Robots for Mapping Diluted Bitumen in Freshwater Lakes

MREN 403 Proposal

Smith Engineering at Queen's University

This document has been modified for public distribution. Selected personal identifiers (e.g., student numbers) have been redacted or updated.

Sophie Villemure (20svv2@queensu.ca), Sabrina Button (sabrina.button@queensu.ca),
Jai Moraes (20jxjm@queensu.ca), Stuart Logan (20sml6@queensu.ca)

October 1st, 2025

Contents

Table 1: Acronyms

Acronym	**Meaning**
API	Application Programming Interface
BCU	Body Control Unit
BMS	Battery Management System
EKF	Extended Kalman Filter
GPS	Global Positioning System
IMU	Inertial Measurement Unit
NED	North-East-Down
RTS	Rauch–Tung–Striebel
UUV	Unmanned Underwater Vehicle
UV	Underwater Vehicle

1 Executive Summary

This project proposes the design and development of a swarm of small, low-cost unmanned underwater vehicles (UUVs) for detecting and mapping diluted bitumen (dilbit) spills in freshwater lakes. Dilbit spills pose ecological, economic and societal risks. Submerged dilbit is challenging to detect with conventional monitoring methods due to their limited spatial coverage, slow data collection, and unreliability in inclement weather conditions. These constraints highlight the need for a modular, scalable, and easily deployable approach, capable of detecting and mapping the dilbit spills. Swarm robotics provides a robust and scalable approach to autonomous environmental monitoring. By deploying multiple agents, the swarm can achieve high spatial and temporal resolution while reducing operational costs. This approach is designed for freshwater lakes, which present fewer challenges than ocean environments.

Stakeholders for this project include, but are not limited to, the supervising research team, who define system objectives, and ecological researchers, who guide data quality standards and field-testing needs. The agents are designed to be upgradable per stakeholder objectives. Each agent consists of a base robot with limited capabilities, and additional modules, providing advanced functionality. The base robot is inspired by submarines and includes a cylindrical acrylic chassis; power system; safety-related sensors; actuators; and a body control unit (BCU) responsible for actuation control, collision avoidance; and safety system management. The modules are easily swappable add-ons to the base robot; they provide hardware and software functionality for localization, state estimation, intra-swarm communications, swarm autonomy and mapping data collection, among others.

The development plan consists of a preliminary development phase, in which component selection, unit test development, and sketch model iteration will be done; a bench testing and calibration phase, which will consist of assembly of hardware components and individual subsystem tests; a module-level verification phase, in which the base robot and modules will be assembled from their subsystems and verified independently; and an integration phase, which will begin with single agent testing and conclude with swarm-level trials validated against communication, autonomy, and mapping requirements.

This project aims to demonstrate the feasibility of a swarm-based, cost-effective, approach to submerged dilbit monitoring. By validating a modular multi-agent system, the proposed project lays the foundation for future extensions, including enhanced sensing, communication, and adaptive swarm behaviours.

2 Problem Definition

Diluted bitumen (dilbit) is a light petroleum often carried in pipelines above or beneath freshwater lakes. Oil spills in lake environments pose a significant threat to ecosystems and human activities [1]. Though dilbit often forms a slick on the surface, the natural evaporation of light compounds, photooxidation, dispersion, and biodegradation may cause trace oil to submerge to depths of 1 to 5 m [2], [3]. Classical methods of oil spill cataloguing include aerial radar and in-situ water-column rosette samplers with spectrometers or fluorometers. Aerial mapping methods often fail under inclement weather conditions, and rosette samplers require large ships and are limited in mobility [4], [5]. In contrast, robot swarms offer a distributed, mobile, in-situ approach to environmental monitoring, overcoming these challenges [6], [7].

Despite advances in swarm robotics, there remains a need for a practical and scalable system. Developing such a system poses challenges in multi-robot coordination, sensor integration, and autonomous navigation under variable lake conditions. This project focuses on designing an underwater robotic swarm solution that balances operational effectiveness, cost, and feasibility. The following problem definition identifies the key stakeholders, outlines available resources, defines the stages of development, and specifies the scope and guiding assumptions.

2.1 Stakeholders

The following internal and external stakeholders inform the scope, requirements, and design of the underwater swarm robot.

Internal Stakeholders

- **Professor Matthew Robertson:** Project supervisor and primary client. Oversees the project, sets research goals, and provides guidance on system requirements and integration. Defines high-level system objectives, sets integration and reliability requirements, establishes scope constraints, and provides approval for testing protocols and deployment strategies.
- **Graziella Bedenik:** PhD student presently developing an oil concentration sensor and, in future years, an underwater acoustic communication module. The sensor platform provides defined technical specifications for interfacing, including support for a wearable device, a dedicated signal generator slot, and SMA connector interfaces. Supports the long-term development goal of incorporating underwater communications.
- **Dr. Diane Orihel:** Principal investigator of the oil spill characterization research project by Environment and Climate Change Canada. Expert in oil spill research and mapping. Provides background knowledge on the nature of oil spills and potential field-testing support. Helps guide data quality standards and ecological needs.
- **Beaty Water Research Labs:** Research institution. May inform constraints impacting testing protocols, system robustness validation, and desired performance metrics under controlled conditions.

External Stakeholders

- **Field Scientists:** End users of the swarm agents in rivers and lakes. Define deployment/retrieval methods, user interface design, robustness under varying conditions, and data collection reliability requirements.
- **Environment and Climate Change Canada:** Funding body for the oil spill characterization project, which includes the underwater swarm robots as a research tool. Informs the problem definition, use case, scope, and involved stakeholders.
- **Freshwater Ecosystems:** Rivers, lakes, and other freshwater systems. Impose constraints on disturbance, pollution, and habitat impact; influence regulatory compliance requirements. Define assumptions for safe operational envelopes and constraints to minimize ecological disturbance.
- **Legal and Regulatory Bodies:** Federal and provincial authorities (Fisheries Act, CEPA, SARA, Ontario Water Resources Act). Define legal constraints and operational limits for safe, compliant deployment of underwater robots. Directly influences system design and allowable deployment methods.

2.2 Resources

The subsequent list describes the accessible resources which collectively enable the design, construction, and testing of the underwater swarm agents while ensuring safety, feasibility, and alignment with project objectives.

- **Access to Funds:** The budget of this project is expected to be $300, with some additional funding available by request to Professor Robertson. Use of funds must be approved by faculty and MREN 403 course staff.

- **Manufacturing:** The team has access to basic mechanical and electrical tools, both through the course and personal supplies. This includes saws, drill sets, screwdriver sets, clamps, multimeters, power supplies, soldering irons, pliers, and wire cutters. Two personal 3D printers are available for the team's use, in addition to those provided by the course. Laser cutters, CNC machines, and water jets are potentially available through consultation with course instructors and consultation with machinists in McLaughlin Hall.

- **Safety and Personal Protective Equipment:** Personal protective equipment, including gloves and goggles, is available through the MREN 403 course supplies. Lithium-ion safe boxes will be available for battery storage.

- **Software and Simulation:** The team will use open-source software to design, simulate and program each agent. This includes CAD programs such as Fusion360, Fritzing and KiCAD, and development languages and frameworks Python, C++, and Arduino.

- **Existing Parts:** The team has electrical hardware and microcontrollers available in personal supplies, including but not limited to Arduino Mega, Uno, and Nano; a Raspberry Pi 5; assorted sensors; fixed colour LEDs; solid core wiring; and servo motors. Use of expensive personal components must be extensively tracked. Parts may be borrowed from the project supervisor or other faculty members overseeing the course upon request.

- **Bench Testing:** Bench testing setups can be created in the reserved MREN 403 room located at Mitchell Hall 177. The laboratory in Beamish-Munro-Hall 314 may be used to test small-scale electrical equipment.

- **Field Testing:** The team has been offered the use of various aquariums and tanks by Professor Robertson for underwater testing; a small tank will be used for preliminary testing. Larger tanks are available through contacts in the Queen's Biology Department, and larger test pools may be available through the Beaty Water Research Center, both contingent on access demand. Tests of a complete system can be carried out in a freshwater lake, likely at Queen's University Biological Station, through contacts in the Biology Department.

2.3 Stages of Development

Presented are the proposed development stages of the swarm's robotic agents. Each builds on the previous stage and informs the agents' design. A visualization of each stage beyond Stage 0 is provided in Figure 1. Stage 4 presents a near-complete distributed, mobile, live mapping system.

- **Stage 0, Base Robot with Open-Loop XYZ Movement:** Each robot has a waterproof chassis with actuation modules, basic compute, power, and collision avoidance. It can move according to a predefined sequence under open-loop control, but does not have swarm capabilities or communications.

- **Stage 1, Surface Communications and Self-Directed Diving:** Agents localize globally and communicate while surfaced, then disperse to the desired planar swarm formation. Agents dive, take measurements at depth, and rise, with no underwater communication.

- **Stage 2, Underwater Self-Localization:** Each agent performs multiple measurements at discrete underwater positions with improved self-localization and collision avoidance.

- **Stage 3, Underwater Swarm Localization:** Agents can localize each other underwater via visual cues or low-fidelity short-range communication, enabling coordinated dispersion and measurement.

- **Stage 4, Live Mapping and Map-Based Replanning:** Agents communicate map data underwater and recenter the swarm based on detected concentration values, swarming toward areas of high concentration for optimal mapping.

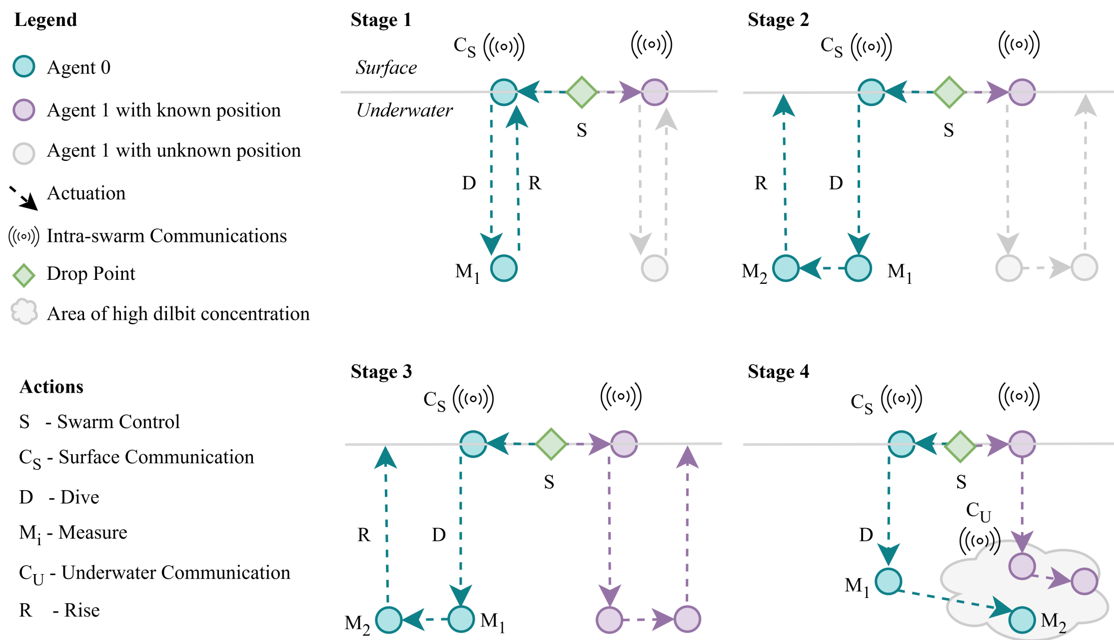

Figure 1: Diagram describing Stages 1-4 of the underwater robot swarm with two agents, from the perspective of Agent 0. 'Agent 0' is an agent's identifier for itself, and agents of higher IDs are neighbours.

2.4 Scope and Assumptions

The scope of this project is to create 1-3 agents with sufficient capabilities for Stage 1. This encompasses the mechanical design of the agent, electrical systems, safety systems, offline mapping of scientific data, and rudimentary autonomy capabilities (control, localization, planning). The scope does not include underwater communications, live data from the agents to the operator, advanced planning, or oil sensing.

As such, the following assumptions are made:

- the agents are operating in freshwater lakes with minimal current,
- GPS data is available at the water surface,
- weeds in the lake are negligible,
- and the only obstacle is the lake bottom, which may not be a flat surface.

2.5 General Constraints and Requirements

Table 2 presents the general constraints of the project informed by stakeholders and research. Requirement codes listed in Appendix B follow the format of XX-YY-Z, where XX is the system initials, YY indicates functional or non-functional requirements, and Z is the enumerator, e.g. CH-NFR-1 for chassis non-functional requirement one.

Table 3 provides the requirements for the complete system, as informed by the constraints. A subsystem-level breakdown of requirements is provided in Appendix B.

3 Design Overview

This section provides an outline of the design of a single agent in the swarm, inspired by submarines. The design relies on communication and GPS systems available at the water surface, but is capable of diving underwater to take measurements using the payload sensor. The swarm design is mostly decentralized; the autonomy systems rely only on data from the agent and its closest neighbours. Decentralized approaches are more scalable and robust than their centralized counterparts [8]. Mapping of the payload sensor data is performed offline by a post-processing script.

The design is split into the base robot, presented in Section 2.3 as Stage 0, and modules which support Stage 1. The base robot contains the subsystems required for basic mobility, including: Chassis, Power, Actuation, and the Body Control Unit (BCU).

Table 2: Constraints for the whole system.

Code	Short Description	Details / Reasoning
G-1	Budget	Total project cost must remain below 300$, limited by course resources and funding.
G-2	Permanent Infrastructure	Robots must operate without permanent infrastructure, reducing scope and regulatory overhead.
G-3	Agent Size	Agents must be smaller than commercial freshwater UUVs to allow simple bucket deployment.
G-4	Power Consumption	Components must use minimal power to maximize operational longevity.
G-5	Environmental Impact	Agents must leave no trace, minimizing ecosystem disturbance.
G-6	Operational Area	Agents must maintain communication with at least one neighbour to prevent loss.
G-7	Underwater Localization and Communication	Agents must localize without GPS underwater, and cannot communicate underwater due to Constraint G-1.
G-8	Deployment and Retrieval	Agents must be deployable and retrievable by a small team without large vessels.
G-9	Depth Rating	Agents must not exceed their pressure rating to prevent structural failure.
G-10	Fault Tolerance	Loss of one agent must not compromise swarm operation, ensuring robustness.
G-11	Safety	Agents must avoid hazards to swimmers, wildlife, and watercraft.
G-12	Data Storage	All mission data must be recoverable even if communication fails.

The modules contain advanced functionality such as intra-swarm communications, autonomy, and mapping. The modules are designed to be replaced and upgraded as the project needs evolve. The agents' subsystems as they relate to the base and modules, and their interactions, are presented in Figure 2.

The agent is designed to carry an oil concentration sensor as the payload. Since the sensor of interest is still in development as per Section 2.1, a placeholder sensor will be used in the design. The design decisions presented here are informed by the literature review in Appendix A. Appendix B includes a list of labelled functional and non-functional requirements by subsystem.

3.1 Chassis

The chassis is the watertight cylindrical base component to which all other components are mounted. The chassis must be waterproof in accordance with CH-FR-1. The chassis is clear and constructed from acrylic tubing, which is a non-toxic material in accordance with CH-NFR-3, and the endcaps are removable to allow easy inspection and maintenance [9]. Interior and exterior mounting rails allow base robot and module components to be added and removed easily. A secondary waterproofed case inside the chassis hosts particularly sensitive electronics. LEDs, photodiodes, temperature sensors and water detection sensors used by the safety system are mounted throughout. Each chassis and module mount contains counterweights to ensure the center of mass and center of buoyancy align.

3.2 Power

As shown in Figure 3, the power system comprises a multi-cell battery pack with a BMS board, a fuse, a relay, and a buck converter. This allows us to automatically cut power to compromised components in

Table 3: System requirements for the agent.

Code	Requirement	Details	Pass Condition
G-FR-1	Mission Depth	Each agent must operate at depths up to 5 m.	Agent sustains continuous operation at 5 m depth for 10 minutes without failure.
G-FR-2	Mission Period	System (agents + base station) must run for 1 hour without maintenance or charging.	Continuous operation for 1 hour in deployment conditions without intervention.
G-FR-3	Battery Life	Each agent must achieve at least 2 hours of operation on one charge.	Agent operates for 2 hours at nominal load before battery depletion.
G-FR-4	Max Amperage	System current must remain below the safe continuous operating rating of the battery.	Current draw during peak loads does not exceed datasheet rating (e.g., ¡5 A).
G-FR-5	Buoyancy	Agents must maintain neutral buoyancy within FS=0.15, where 0 FS ¡ 0.5.	Released at mid-water, agent does not sink/float uncontrollably; vertical velocity 0.1 m/s.
G-FR-6	Movement	Agents must maneuver in all 3 dimensions (x, y, z).	Agent demonstrates controlled forward, lateral, and vertical movement.
G-FR-7	Maintenance Access	Subsystems must be accessible for inspection, adjustment, or replacement.	One agent disassembled and reassembled within 15 minutes without damage.
G-FR-8	Retrieval	Agents must be retrievable by a simple, semi-automated process.	One operator retrieves the agent without water entry in under 5 minutes.
G-NFR-1	Agent Cost	Cost per agent must be $100.	BOM review confirms $100 per agent.
G-NFR-2	Swarm Size	Swarm must scale to an arbitrary number of agents.	Communication/control tested with 10 agents in simulation or deployment.
G-NFR-3	Optimality over Reliability	Swarm prioritizes global solution quality over individual reliability.	System meets mission goals with 80% of agents active despite failures.

the event of a leak in the main chassis. There are two power lines: a main voltage line for powering the sensors and actuators, and a low-voltage line for powering the microcontrollers and LEDs.

The bulk of the power system is contained within a secondary waterproof enclosure inside the main chassis in accordance with CH-NFR-2. The BCU, discussed further in a later section, is contained alongside the power system and connected directly to the battery's output so that it may drive the safety relays. To reduce strain on connectors and keep the main body uncluttered, wiring is routed through designated channels within the chassis.

3.3 Body Control Unit

The Body Control Unit (BCU) is a microcontroller built into the body of the agent. It runs three software modules: Actuation Control, Collision Avoidance, and Safety; each elaborated on further in its own section below. To fulfill each of these tasks, the BCU communicates with other onboard compute modules via a wired connection. The BCU has a set of predefined messages and response templates, identified by a message ID number. These messages are de-

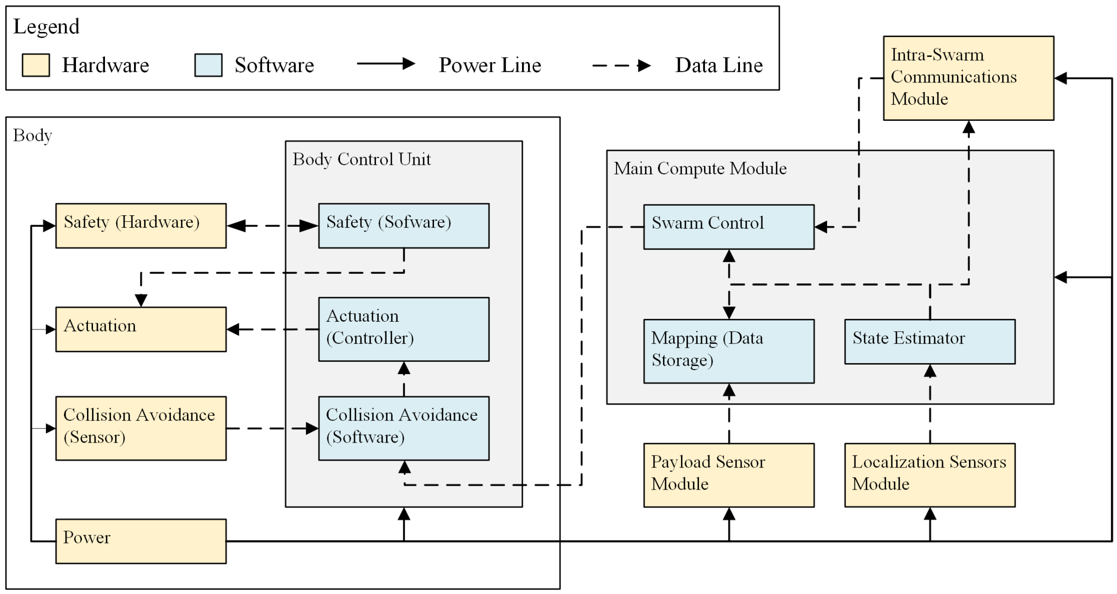

Figure 2: System architecture for a single agent.

signed to be CAN-compatible for future development.

The BCU also provides some secondary functionality. Via the message system, the agent's body LEDs can be written, and an accurate system clock module can be adjusted or queried for internal and intra-swarm synchronization.

3.4 Actuation

The actuation system is the hardware responsible for physically moving an agent and their controllers. Each agent will contain three actuators: a Main Propeller for horizontal propulsion, an Auxiliary Propeller for adjusting heading, and a Syringe Ballast for controlling depth. Each actuator is directly driven by the BCU according to its Actuation Controller program. Figure 5 and Figure 4 shows the coordinate systems for the controllers.

- **Syringe Ballast:** Draws water into a syringe placed within the chassis, placed such that it adjusts the total mass of the agent without greatly affecting the centre of mass. This adjusts the gravitational force on the agent, enabling depth control.
- **Main Propeller:** Mounted on the rear of the agent, and is driven by a magnetically coupled motor within the chassis. Control is achieved by adjusting the motor torque, which is limited to prevent stalling or magnetic decoupling.
- **Auxiliary Propeller:** Mounted parallel to the Main Propeller on the rear face of the Agent, and is smaller than the Main Propeller.

The system can be described in a four-dimensional state space $\mathbb{Q} = \mathbb{R}^3 \times \mathbb{S}^1$, with the holonomic constraints that pitch and roll are constant. Since the four-
dimensional system has three actuators and forward and lateral motion are coupled via the Auxiliary Propeller, the system is full rank. Thus, the system is controllable, complying with AC-NFR-1.

The Actuation Controller is the software running on the BCU responsible for taking generated state errors from the Collision Avoidance, calculating the corresponding actuator commands, and sending control signals. It is also responsible for prioritizing input from the safety system. Finally, the Actuation Controller compensates for fluctuations due to increased internal pressure of the agent and syringe hysteresis.

3.5 Collision Avoidance

This subsystem prevents the agent from colliding with the bottom or edges of the lake. Range-finding sensors mounted at the front and bottom of the agent inform the system of approaching surfaces. The collision avoidance software intercepts and overwrites desired states sent to the controller that would bring

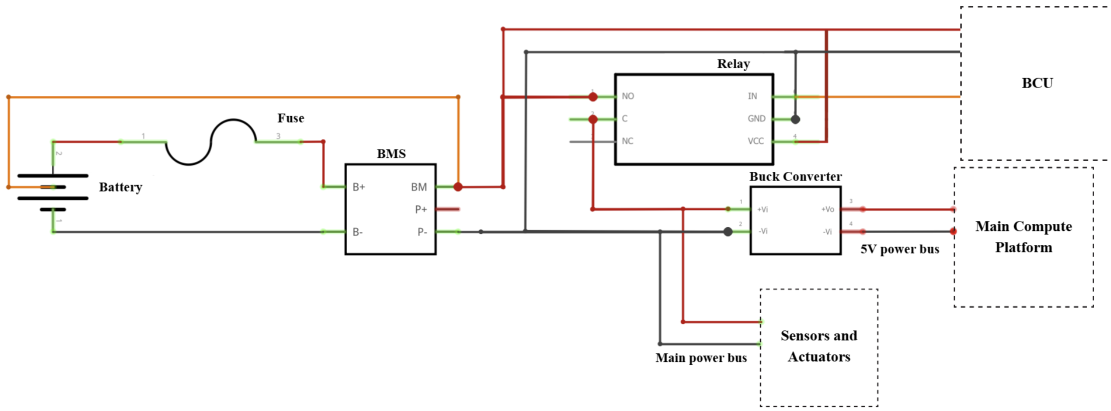

Figure 3: Draft power system.

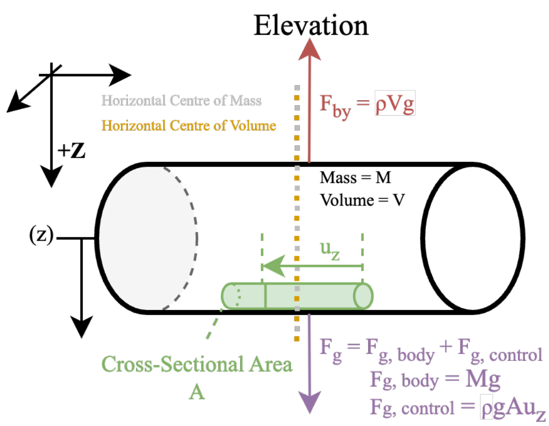

Figure 4: Depth control diagram of a single agent.

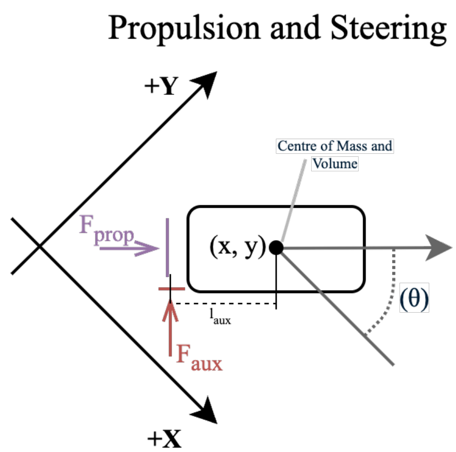

Figure 5: Propulsion and steering diagram of a single agent.

the agent too close to detected surfaces. The collision avoidance software is processed on the BCU.

3.6 Safety

The safety system runs on the BCU, monitoring the internal status of the chassis and using body LEDs to indicate issues. Water detection, temperature, and photodiode sensors are connected to the BCU for this purpose. The Safety System executes a Mission Cancel or Immediate Surface operation when it detects an issue. It broadcasts irregular states of the agent via the body LEDs, reads the state of neighbouring agents via photodiodes, and reports safety issues to all compute modules connected to the BCU.

- **Mission Cancel:** Executes when the external facing photodiodes detect a Mission Cancel pattern being flashed by a neighbouring agent or other source. It relays this signal and begins surfacing unless explicitly overridden.
- **Immediate Resurface:** Begins execution if water is detected in the chassis, humidity in the chassis increases, or temperature climbs too high. Unique body LED statuses are set for each case. Each of these has three keypoint values: at the first, the safety system notifies other compute modules and begins surfacing, but can still be overridden by the main compute; at the second, it begins surfacing but cannot be overridden; at the third, power is cut to the chassis from the battery box.

Any of these cases can also be triggered by a message to the BCU. Additionally, the default state of the agent will be buoyant to comply with legal codes and enhance safety in accordance with CH-FR-2.

3.7 Main Compute Module

The Main Compute Module is a computer module attached inside the chassis. It acts as the 'brain' of the system, running all the high-level software. This includes monitoring and cataloguing readings, calculating a desired position and state estimation, communicating externally, and all other high-level software. The Main Compute Module has complete control of the BCU via the BCU messaging system, except in the non-overridable cases mentioned in the safety section.

3.8 Intra-swarm Communications

The communication module for each agent is a standalone module which is connected to the top of the chassis so that when the agent surfaces, the communication systems are fully out of the water allowing for surface communication techniques as defined in Stages and Development stage 1. The module consists of a transceiver connected to the main computer platform, which processes the data from its neighbours and transmits its global location.

3.9 Localization Sensors

The localization module contains three sensors: a GPS receiver for global localization, an IMU for tracking horizontal movement, and a depth sensor for tracking vertical movement. All sensors will connect to the Main Compute Module. The module is mounted on top of the chassis so the GPS can be above water while the robot surfaces. The IMU is mounted close to the center of mass.

3.10 State Estimation

Each agent's state is defined as

$$\vec{q_0} = \Big(x, y, z, \theta\Big)^T,$$

where x, y, and z are expressed in the North–East–Down (NED) frame. An Extended Kalman Filter (EKF) fuses measurements from the Localization Sensors to provide q_0, the IMU provides $\dot{q}_0$, and control inputs are used to estimate $\ddot{q}_0$. Because GPS is unavailable underwater, the EKF will reject GPS updates when the depth sensor indicates submergence or when GPS readings deviate significantly from prior estimates. The EKF output will be provided in real-time to the Swarm Autonomy loop for control and decision making.

To meet requirement MA-FR-1 on measurement-position accuracy, a Rauch–Tung–Striebel (RTS) smoother will post-process trajectories after surfacing. Once GPS is reacquired, the RTS will correct stored dilbit measurement positions for drift. These smoothed estimates are used only for data correction and are not fed back to the live swarm controller.

3.11 Swarm Autonomy

Each agent uses a two-controller approach, the first controller discussed in Section 3.4 minimizes error in the agent's state q_0. The second controller, named the Swarm Controller, minimizes error in the swarm formation characterized by the swarm state s_0. Figure 6 shows the control diagram for a single agent's autonomy stack.

Swarm Autonomy software runs on the Main Compute Module and comprises the Swarm State Estimator, the Swarm Controller, the Planner and the Formation Error Estimator.

The swarm state vector,

$$\vec{s_0} = \Big(z, d_1, \theta_1, d_2, \theta_2, ...\Big)^T,$$

tracks the desired dive depth, z, and planar position of the agent relative to its neighbours, d_i, θ_i. The Swarm State Estimator is responsible for collecting the states of all agents in the swarm $q_0, q_1, q_2, ...$ and performing trigonometric operations to calculate the swarm state of the agent. Neighbour positions are communicated when the agents are surfaced. However, the swarm state estimator always produces an estimate, even when intra-swarm communications are unavailable after diving. The Swarm Controller minimizes error in the swarm state, and thus the swarm's formation error. The controller seeks to maintain an equilateral triangle (K3) formation. It outputs the desired state needed by the Collision Avoidance and Actuation Controller subsystems.

Planning is responsible for providing the desired depth and the desired swarm state, i.e. the distance between neighbouring agents. The dive maneuver is triggered by the total Formation Error falling below a threshold. The formation error is a measure of how much the layout of the swarm deviates from the desired formation.

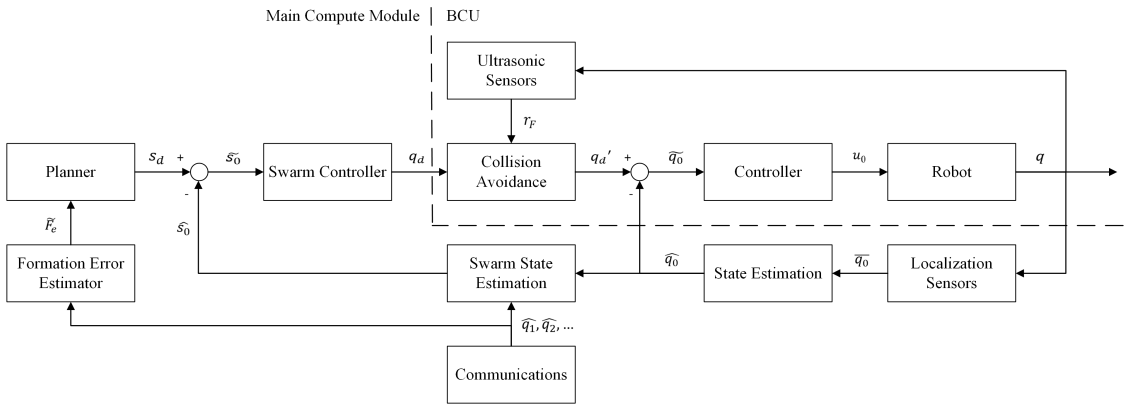

Figure 6: Control Diagram for a single agent.

3.12 Mapping

Spatiotemporal mapping of diluted bitumen concentrations is proposed as a post-processing step after robot retrieval. Before deployment, all robot system clocks are synchronized, and a global measurement time is defined. At measurement time, each robot records a measurement using its Payload Sensor and logs the corresponding timestamp and estimated position. Positions are initially computed with an EKF and corrected for drift using surface GPS data via an RTS smoother (Section 4.13.1).

After retrieval, each agent transfers its onboard measurements to a central computer, where a data collection script stores the raw data. A subsequent mapping script integrates all measurements to construct the final concentration map. Maps can be purely spatial or spatiotemporal.

4 Development and Testing

This section outlines the development and testing phases of the project. Test results will be checked against the subsystem requirements listed in Appendix B.

4.1 Preliminary Development

This phase is for creating low-cost prototypes of key systems to inform component selection and mechanical design. During this phase:

- Cardboard sketch models will be used to determine the approximate required volume of the chassis and module mounts.
- The sensors, actuators, and communication hardware will be selected. A detailed component list will be created and used to estimate maximum power draw. A safety factor will be applied to ensure the power system can support the system safely and allow for additional modules.
- An early prototype of the swarm autonomy software will be developed and tested in a low-fidelity particle simulation environment. This simulation won't include depth, the lake bottom, or communication blackouts while underwater.
- The EKF and RTS Smoother will be tested in a different simulation environment. This simulation will evaluate combinations of GPS, IMU, and depth sensor models for the state estimator in scenarios where sensor data is unavailable and water current may be present.

4.2 Component Development and Testing

During this phase, components of the various subsystems will be developed and tested.

- **Chassis:** Higher-fidelity chassis and module mount prototypes will be used for waterproof testing and hydrostatic balance testing. Waterproof and hydrostatic balance testing of the parts will be performed in a small water tank without any sensitive electronics. During balance testing, placeholders of the same weight and size as the electronics will be used.

- **Power:** The battery will undergo bench tests with the fuse and BMS board under varying loads to ensure safe charge and discharge behaviour. The tests will be repeated with the system in a sealed container, while monitoring system temperatures to determine if any cooling systems are needed.

- **Sensors and Actuators:** Calibration tests for the collision avoidance and payload sensors will take place underwater; all other sensors will be tested and calibrated using a bench setup. Actuators will also be tested on a bench setup using constant inputs from the BCU. Data collected from the actuator tests will be used to inform Actuation Controller calculations and simulation.

- **BCU:** BCU Communications will be developed as a program for the BCU with an API for the Main Compute. Unit tests will be developed to be ran with each software change. Once safety sensor calibration is complete, it will be integrated with the communication system and a second set of unit tests will be developed for the safety system. Bench tests for triggering the safety system naturally will be ran, both to test and determine sensor values for triggering a takeover.

- **Intra-swarm Communications**: Communication hardware will be bench-top tested with the Main Compute Module. We will build two communication modules to perform tests. The tests will evaluate range, data loss, latency and minimum elevation out of water for reliable operation.

- **Swarm Autonomy, State Estimation, and Collision Avoidance:** Simulation fidelity will be improved by adding depth, the lake bottom and the communication blackouts while underwater. The same simulation environment will be used to develop and test the collision avoidance software.

- **Mapping:** The mapping script will be tested on manually generated data. The script will also test pulling data from the main compute module.

4.3 Subsystem Tests

This phase involves integrating individual subsystems, starting with the chassis and module mounts. These parts will undergo the final round of waterproof and hydrostatic balance testing. The chassis and module mounts will be used for testing other subsystems. The power system will also be finalized during this phase. To do so, we will add the buck converter, the relay system, and the BCU to test the functionality of the emergency cutoff system. Then, each of the other electrical components will be added individually, with system tests for each one, until we achieve a full electrical system test. The test will run until the power source is depleted, and the battery life under full load will be determined from the results.

All other components will be integrated into their respective subsystems and tested against the bench test results to validate their performance. Software subsystems such as State Estimation, Swarm Autonomy and Mapping will be tested using data from the sensors, actuators and communication hardware.

4.4 System Integration Tests

During this phase, the subsystems will be integrated and tested together; the following tests take place in small water tanks. Each test builds on the last and metrics for each subsystem will be measured and evaluated against the requirements.

- **Base Robot:** Include the chassis, power system, actuation, collision avoidance and safety subsystems. The goal is to have a simple robot that can remain neutrally buoyant and correctly identify and respond to safety signals.

- **Closed Loop Base Robot:** The Main Compute Module, Localization Sensors and State Estimator are added one at a time. The agent should be able to move to and hold a desired position.

- **Stage 1 Agent:** The Intra-swarm Communication, Payload Sensor, and Swarm Autonomy subsystems will be introduced sequentially. The second communication module developed for testing will be used to mock other agents to verify swarm functionality. Data from this test will be used to test the offline mapping script.

References

[1] T. A. Black et al., "Surface oil is the primary driver of macroinvertebrate impacts following spills of diluted bitumen in freshwater," *Environmental Pollution (Barking, Essex: 1987)*, vol. 290, p. 117 929, Dec. 1, 2021, ISSN: 1873-6424. DOI: 10.1016/j.envpol.2021.117929.

[2] *Spills of Diluted Bitumen from Pipelines: A Comparative Study of Environmental Fate, Effects, and Response*. Washington, D.C.: National Academies Press, 2015, ISBN: 9780309380102. DOI: 10.17226/21834. Accessed: Sep. 26, 2025. [Online]. Available: http://www.nap.edu/catalog/21834.

[3] V. Palace, P. C. Bunker, L. Timlick, C. Brewster, J. McCourt, and D. Dickins, *Assessing the capabilities of oil detection canines to detect submerged weathered oils*, 2025. DOI: 10.2139/ssrn.5352793. Accessed: Oct. 1, 2025. [Online]. Available: https://www.ssrn.com/abstract=5352793.

[4] W. Alpers, B. Holt, and K. Zeng, "Oil spill detection by imaging radars: Challenges and pitfalls," *Remote Sensing of Environment*, vol. 201, pp. 133–147, Nov. 1, 2017, ISSN: 0034-4257. DOI: 10.1016/j.rse.2017.09.002. Accessed: Sep. 26, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0034425717304145.

[5] H. K. White, R. N. Conmy, I. R. MacDonald, and C. M. Reddy, "Methods of oil detection in response to the deepwater horizon oil spill," *Oceanography*, vol. 29, no. 3, pp. 76–87, Aug. 22, 2016. DOI: 10.5670/oceanog.2016.72. Accessed: Sep. 26, 2025. [Online]. Available: https://tos.org/oceanography/article/methods-of-oil-detection-in-response-to-the-deepwater-horizon-oil-spill.

[6] M. Dunbabin and L. Marques, "Robots for environmental monitoring: Significant advancements and applications," *IEEE Robotics & Automation Magazine*, vol. 19, no. 1, pp. 24–39, Mar. 2012, ISSN: 1558-223X. DOI: 10.1109/MRA.2011.2181683. Accessed: Sep. 26, 2025. [Online]. Available: https://ieeexplore.ieee.org/document/6161683.

[7] Y. Tan and Z.-y. Zheng, "Research advance in swarm robotics," *Defence Technology*, vol. 9, no. 1, pp. 18–39, Mar. 1, 2013, ISSN: 2214-9147. DOI: 10.1016/j.dt.2013.03.001. Accessed: Sep. 21, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S221491471300024X.

[8] J. C. Barca and Y. A. Sekercioglu, "Swarm robotics reviewed," *Robotica*, vol. 31, no. 3, pp. 345–359, May 2013, ISSN: 0263-5747, 1469-8668. DOI: 10.1017/S026357471200032X. Accessed: Sep. 22, 2025. [Online]. Available: https://www.cambridge.org/core/journals/robotica/article/swarm-robotics-reviewed/C31F3EC5FC09AC2ED9DF91083C0FD886.

[9] K.
bibinitperiod H. LLP, *Canadian court invalidates plastics 'toxic' designation*, Web, Published November 22, 2023, 2023. [Online]. Available: https://www.khlaw.com/insights/canadian-court-invalidates-plastics-toxic-designation?utm_source=chatgpt.com.

[10] "CTD general practices – CalCOFI," Accessed: Oct. 1, 2025. [Online]. Available: https://calcofi.org/ctd-general-practices/.

[11] W. Ji, A. G. Slaughter, and G. M. Coelho, "Optimized underwater detection of dispersed oils using scanning fluorometry," *International Oil Spill Conference Proceedings*, vol. 2024, no. 1, 2024. DOI: 10.7901/2169-3358-2024.1.313.

[12] G. Bedenik, M. Greeff, and M. Robertson, *Towards underwater detection of diluted bitumen with interdigital sensors*, version: 2, Jul. 16, 2025. DOI: 10.48550/arXiv.2507.03781. arXiv: 2507.03781. Accessed: Sep. 26, 2025. [Online]. Available: http://arxiv.org/abs/2507.03781.

[13] I. Akyildiz, D. Pompili, and T. Melodia, "Underwater acoustic sensor networks: Research challenges," *Ad Hoc Networks*, vol. 3, pp. 257–279, May 2005. DOI: 10.1016/j.adhoc.2005.01.004. [Online]. Available: https://www.researchgate.net/publication/222826396_Underwater_Acoustic_Sensor_Networks_Research_Challenges.

[14] H. M. Oubei, C. Shen, H. Kang, T. K. Ng, B. S. Ooi, and M. Alouini, "Light based underwater wireless communications," *IEEE Communications Magazine*, vol. 57, no. 11, pp. 98–104, 2019. DOI: 10.7567/JJAP.57.08PA06. [Online]. Available: https://www.researchgate.

net/publication/326448801_Light_based_underwater_wireless_communications.

[15] Water Linked, *Applications: Underwater communication*, Accessed: 2025-09-23, 2023. [Online]. Available: https://waterlinked.com/applications/underwater-communication.

[16] M. Domingo, “Magnetic induction for underwater wireless communication networks,” *IEEE Transactions on Antennas and Propagation*, vol. 60, no. 6, pp. 2929–2939, 2012. DOI: 10.1109/TAP.2012.2194670. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/6183466?casa_token=cnGo3KFlHbcAAAAA:2HCRi-bbdEJcZhQnOrrGQLY4XmjKJrhfgCbELikHcfDeO6Slw-ArkhwJ2bhR-XtcLwKotIvoIA.

[17] A. Wibisono, M. J. Piran, H.-K. Song, and B. M. Lee, “A survey on unmanned underwater vehicles: Challenges, enabling technologies, and future research directions,” *Sensors (Basel, Switzerland)*, vol. 23, no. 17, p. 7321, Aug. 22, 2023, ISSN: 1424-8220. DOI: 10.3390/s23177321. Accessed: Oct. 1, 2025. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10490491/.

[18] S. Woods, “AUTOMATED BALLAST TANK CONTROL SYSTEM FOR AUTONOMOUS UNDERWATER VEHICLES,” Apr. 5, 2012. Accessed: Oct. 1, 2025. [Online]. Available: http://hdl.handle.net/10222/14609.

[19] BrickExperimentChannel. “RC submarine 4.0 – background (1/10),” Brick Experiment Channel, Accessed: Oct. 1, 2025. [Online]. Available: https://brickexperimentchannel.wordpress.com/2022/06/25/rc-submarine-4-0-background-1-10/.

[20] I. Bogrekci, P. Demircioglu, and G. Ozer, “Autonomous underwater vehicle design and development: Methodology and performance evaluation,” *Journal of Automation Mobile Robotics Intelligent Systems*, vol. 18, pp. 47–61, Dec. 2024. DOI: 10.14313/JAMRIS/4-2024/30. [Online]. Available: https://www.researchgate.net/publication/386334310_AUTONOMOUS_UNDERWATER_VEHICLE_DESIGN_AND_DEVELOPMENT_METHODOLOGY_AND_PERFORMANCE_EVALUATION.

[21] J. Proenza, A. Ortiz, G. Bernat, and G. Oliver, “A cost-effective hardware architecture for fail-safe autonomous underwater vehicles,” in *ICECS’99. Proceedings of ICECS ’99. 6th IEEE International Conference on Electronics, Circuits and Systems (Cat. No.99EX357)*, vol. 3, 1999, 1487–1490 vol.3. DOI: 10.1109/ICECS.1999.814451. [Online]. Available: https://ieeexplore.ieee.org/document/814451.

[22] Seamor Marine Ltd., *How do rovs survive high pressure?* [Online; accessed 27-Sep-2025], 2025. [Online]. Available: https://seamor.com/how-do-rovs-survive-high-pressure/.

[23] R. Schwerz, M. Roellig, and B. Frankenstein, “Robust and reliable encapsulation of electronics for underwater applications,” in *2016 17th International Conference on Thermal, Mechanical and Multi-Physics Simulation and Experiments in Microelectronics and Microsystems (EuroSimE)*, 2016, pp. 1–6. DOI: 10.1109/EuroSimE.2016.7463339. [Online]. Available: https://ieeexplore.ieee.org/document/7463339.

Appendix A: Literature Review

The following section reviews academic content in several topics relevant to the project. These sources inform the problem definition, constraints, and requirements.

Diluted Bitumen Spill Monitoring

Diluted bitumen (dilbit) is a crude oil commonly transported in pipelines beneath freshwater lakes. Bitumen, a heavy petroleum, is thinned with a lighter diluent to enable transport. Dilbit has a maximum density of 0.94 g/cm^{-3}, lower than freshwater (1.00 g/cm^{-3}). After a spill, separation of petroleum and diluent causes dense oil to submerge as the diluent dissolves (more soluble than hydrocarbons) or evaporates, promoting sinking, accumulation, biodegradation, and natural dispersion [2]. Field and experimental studies report submerged/weathered dilbit occurring at shallow depths (commonly 1–5 m below the surface) and, in some incidents, accumulating in sediments, indicating both short-term submergence in the water column and longer-term deposition to the bed [3]. Predicting the underwater movement of spilled oil in freshwater lakes is challenging due to wind, current, and strong wave action [2]. Underwater detection is critical because underwater ecosystems suffer severe effects even from small dilbit spills; for example, a study using limnocorrals in a boreal lake found that emergent insect emergence fell by 93-100% over 11 weeks in the highest dilbit volume treatment, indicating catastrophic impact on benthic invertebrate communities [1].

Oil spill monitoring therefore aims to track suspended material and forecast deposition zones for manual removal [2]. Detection methods include sonar, underwater cameras, surface visual observation, bottom sampling, water-column sampling, in-situ mass spectrometry, in-situ fluorometry, and aerial imaging [2]. Rosette samplers, used for water-column sampling, require large vessels to raise and lower the mass spectrometry system and can only collect data from a single vertical water column (one GPS coordinate) per deployment, forcing the vessel to reposition for each additional sampling site [5]. Typical Conductivity–Temperature–Depth (CTD) rosette operations take tens of minutes to about 50 minutes per cast, depending on depth, further limiting the rate of sample collection [10]. In-situ commercial fluorometers provide promising real-time detection but fail within days of a spill, as photooxidation of oil degrades polycyclic aromatic hydrocarbons—the fluorescent component—reducing signal strength [11]. Interdigital capacitive sensors are another in-situ approach that detect dilbit through changes in water permittivity and conductivity [12].

Aerial mapping methods effectively image surface slicks but cannot detect submerged oil and are unreliable under overcast conditions. Spaceborne polarimetric synthetic aperture radars (SARs), the most promising remote sensing technique, suffer from noise limitations [4]. Moreover, visual algorithms used to distinguish oil films from biogenic slicks rely on subjectively interpreted training data and are rarely validated by chemical measurements [4].

Environmental sensor networks using multirobot swarms offer an emerging alternative to bulky, fixed analytical stations [6]. Key challenges include interoperability, sensor calibration, communications, and power longevity. Developing inexpensive, low-power sensors with high sensitivity and selectivity is therefore a research priority [6]. Advances in battery technology have extended swarm endurance; underwater robots have operated beneath Arctic ice sheets for over 25 h, but many missions require durations of months to years [6]. Cooperative swarms are particularly advantageous in GPS-denied environments such as underwater, where inter-robot triangulation enables localization [6].

Swarm Robotics

Swarm intelligence refers to the collective intelligence of a group of agents. Examples of swarm intelligence can be found in nature, such as schools of fish, flocks of birds and human societies. Swarm robotics refers to the application of swarm intelligence concepts in robotics problems. Swarm robotics approaches enable groups of small, simple robots to tackle complex objectives typically reserved for larger, more complex robots [7].

Communication Network Approaches

Swarm robots require a communication network to transmit data and synchronize activities. A robot swarm's communication network can be centralized, decentralized, or a combination of the two [8].

In a fully centralized network, a leader agent receives data from and sends instructions to all agents of the swarm. This approach gives the leader and, by extension, the operator, full control over all agents and network data. However, centralized networks require significantly higher bandwidth and complex planning algorithms. Fully centralized systems are also less robust and scalable than decentralized approaches [8].

In fully decentralized networks, agents operate on simple instructions and local data, and complex behaviour emerges from the interactions between the agents. As a result, planning algorithms are simpler, and the system is scalable and robust to malfunctioning or lost agents. Decentralized approaches require less communication bandwidth since data is not being transmitted across the network. This means that in fully decentralized networks, no agent has access to all data in the network, which significantly complicates map generation and control over swarm behaviour [8].

In most cases, a hybrid approach is used to leverage the advantages of both methods.

Swarm Formation

Maintaining swarm formation is crucial for the success of the robot swarm. There are several methods for swarm generation, including graph theory, morphogen gradients, potential fields and Voronoi diagrams. Formations are optimized for certain tasks. For example, the equilateral triangle (k3) pattern generated from graph theory optimizes covering the largest area with the fewest agents [8].

Moving in formation introduces several problems; agents must maintain formation when possible while simultaneously being capable of changing the formation to dodge obstacles. Agents must also synchronize their headings and speeds, which is often accomplished through consensus algorithms. Swarms must also maintain communications connectivity to be effective, which can be difficult when there are obstacles in the environment [8]. It is worth noting that the task of creating and maintaining a formation is distinct from planning and can be modelled as a control problem.

Underwater Communications

Underwater communication between UVs has historically relied on acoustic communication devices, which use sound waves to propagate information through the water. These remain the most widely used solution in today's systems due to their ability to operate over long distances despite low data rates [13]. More recently, optical techniques, such as blue and green LEDs and lasers, have been employed for short-range high-bandwidth communication in clear water environments [14]. Other modern systems also rely on compact modems to integrate communication and positioning for UVs [15]. Experimental methods such as magnetic induction take advantage of changing current to induce fluctuations in a magnetic field, which a receiver coil can pick up and convert to electrical signals [16].

For a cost-effective mass-producible swarm robot, acoustic systems are challenging due to the large cost of commercial hardware and high power consumption[13]. The same difficulty occurs for modems because of the lack of easily available commercial products in the low-cost and compact form required **oubie2019**. A custom acoustic device could be developed around these constraints, which is currently being worked on by a third party under Dr. Robertson. Magnetic induction is still very experimental and would have the same development issues as a custom acoustic device. Magnetic induction also has a very low range and potentially large power consumption, which would be undesirable for swarm robotics [16].

For a system where communication between agents does not need to be continuous, a surfacing technique could be applied, where the agents surface every few minutes to communicate with each other. A more basic underwater LED communication system can be implemented for communicating agent status and initiating return sequences.

UUV Actuation and Control

Actuation in traditional UUVs varies greatly due to the range of viable underwater actuators. A 2023 review published by NIH [17] identified four main options being focused on in recent research: propellers, ballast tanks, undulating and adjustable fins, and hydro jets. Omnidirectional movement was achieved by one configuration in the review, consisting of propellers in each direction, combined with a ballast to control depth. Control for this configuration required the propellers to compensate for the change of centre of mass caused by filling the ballast. This change in center of mass can be leveraged by multiple ballast tanks for precise control of roll and pitch, along with depth [18], typically paired with fixed propulsion [17]. Yaw can be controlled by an auxiliary propeller mounted perpendicularly to the main propulsion [19], or by the use of adjustable fins [17].

When considering ballasts in small UUVs, syringe ballasts [19] or pump-based ballasts [18] may be implemented depending on the size, power, and depth constraints of the project. Syringe ballasts require only one actuator to operate the syringe, but must be able to hold against the water pressure at any given depth. They also experience hysteresis [19] and fill unevenly. Pump ballasts require an air pump and a water pump. They are constrained by the flow rate of the pumps, which decreases at extreme depth. They occupy a larger fixed space and fill evenly. Regardless of ballast type, depth control will fail if chassis volume shrinks such that the buoyant force is less than the gravity of the UUV with empty ballasts.

When using propellers on UUVs, waterproofing is a main concern. Externally mounted propellers need to have wire passthroughs rated for depth, while internal motors must have some sort of waterproof coupling applied, such as a magnetic coupling [19]. Magnetic couplings need low-friction surfaces and coatings applied, which must not be soluble in water [19]. Care must be taken not to allow a propeller motor to stall due to tangle, or for a magnetic decoupling to occur [19].

The 2023 review identified five methods of control typically used in UUVs: PID control[17], useful for simple applications; MPC control, which predicts future behaviour of the system, works well against strong currents; Herd localization and control uses AI and machine learning techniques to track and determine behaviour based on other members of a swarm; Adaptive Control (AC), which identifies issues proactively and changes output accordingly, and Sliding Mode Control (SMC).

Waterproof Material and Fixtures

The most common method of waterproofing used in small to mid-sized UVs is pressure housing using acrylic or aluminum robots with O-rings and cable penetrators. This keeps electronics, motors, and sensors at one atmosphere, which is practical for moderate depths up to 100m and allows for easy maintenance [20]. For deeper operations, many UVs use pressure-compensated oil-filled housings. In these housings, dielectric fluids are used to equalize pressures to reduce structural loads and lubricate moving parts [21]. Other low-cost UVs utilize floodable hulls with sealed or potted electronics systems, avoiding differential pressure on the hull and localizing failures [22]. For electronics boards, conformal coatings or epoxy potting is a common technique used to protect against water. Potting is typically reserved for small, low-power modules where reparability is not important. For connectors, purpose-built penetrators or wet-mate connectors can provide robust cable feedthroughs [23].

Appendix B: Subsystem Requirements

The following appendix outlines specific requirements as they align with each subsystem. Each requirement has a code of the format subsystem-type-number, XX-YY-ZZ. The subsystem codes are provided in Table 4, whereas the Table 5. The complete list of requirements is in Table 6.

Table 4: Subsystem codes.

Code	**Subsystem**
G	General
AC	Actuation
BC	BCU (Body Control Unit)
CA	Collision Avoidance
CH	Chassis
CM	Intra-Swarm Communications
LS	Localization Sensors
MC	Main Compute
PS	Payload Sensor
PW	Power
SA	Swarm Autonomy
SE	State Estimation
SF	Safety
MA	Mapping

Table 5: Requirement type codes.

Type	**Meaning**
FR	Functional Requirement
NFR	Non-Functional Requirement

Table 6: Functional and non-functional requirements by subsystem.

Code	Requirement	Pass Condition
AC-NFR-1	Simple Kinematics	Actuation dynamics can be modelled and controlled using linear or first-order approximations without numerical instability.
AC-NFR-2	Sustained Angular Rate	Agent can demonstrate sustained angular velocity of up to ≥ 1 rad/s under nominal load.
AC-NFR-3	Sustained Linear Velocity	Agent can demonstrate forward linear velocity of up to ≥ 0.5 m/s.
BC-FR-1	Ports	BCU exposes ports for MC input, body sensors, safety sensors, safety relay, and drive actuators. Verification by interface check.
BC-FR-2	Processing	BCU executes kinematics, control commands, safety checks, collision avoidance, and MC comms in real time.
CA-NFR-1	Compute Resources	Collision avoidance algorithms run on BCU without exceeding 80% CPU utilization.
CA-NFR-2	Collision Avoidance Range	Agent does not approach within 15 cm of surfaces in front/below. Tank tests with obstacles verify buffer zone maintenance.
CH-FR-1	Watertightness	Sealed chassis maintains acceptable humidity and no water ingress over $N\times$ mission period in test with humidity sensors.
CH-FR-2	Fail-Safe Buoyancy	In power-loss test, chassis surfaces autonomously within 2 min without manual intervention.
CH-FR-3	Environmental Impact	Chassis geometry and sensors prevent physical damage to aquatic habitats/species in collision tests.
CH-NFR-1	Agent Size	Chassis dimensions smaller than $25 \times 25 \times 40$ cm^3 and deployable by single operator.
CH-NFR-2	Battery Isolation	Battery housed in a separately sealed compartment, verified by inspection and leak testing.
CH-NFR-3	Connectivity	Agent provides SMA or equivalent swappable connectors for sensor/antenna attachment.
CH-NFR-4	Non-toxic Materials	Materials leach $<$ regulatory thresholds in freshwater (per CEPA/Fisheries Act).
CM-FR-1	Communication	Inter-agent and MC comms maintained continuously during surface operation (field tests).
MA-FR-1	Data Logging	All mission data tagged with timestamp and position, retrievable post-mission.
MA-FR-2	Data Acquisition	Data retrievable by wired/wireless link to PC/storage device within 5 min/agent.
MA-FR-3	Data Visualization	Post-mission visualizer renders 3D spatiotemporal data in replay tests.
MC-NFR-1	Compute Capability	Main Compute runs all module software without exceeding 90% CPU or 80% memory.
MC-NFR-2	Pinout	MC interfaces with BCU + all required modules; validated by integration testing.
SA-FR-1	Swarm Connectivity	Agents maintain continuous communication links at surface.
SA-FR-2	Synchronous Dive	$\geq 90\%$ of agents initiate dive within 10 s window.
SA-FR-3	Formation Keeping	Formation error ≤ 1 m RMS relative to leader/desired geometry.
SA-FR-4	Output Rate	Controller outputs desired state at ≥ 5 Hz, even if comms/sensors drop.
SA-NFR-3	Settling Time / Overshoot	Swarm controller settles within 5 s with overshoot $< 20\%$ in step-response test.
SE-NFR-1	Surface Localization	RMS error < 0.5 m over 60 s stationary/slow-drift test using GPS truth.
SE-NFR-2	Submerged Localization	Depth RMS error < 0.1 m; horizontal error ≤ 1.0 m for 95% of a 10 min dive.
SF-FR-1	Power Override	Leak event triggers power cutoff in < 1 s.
SF-FR-2	Control Override	Emergency input overrides normal control within 0.5 s.
SF-FR-3	Mission Cancel	Mission-cancel light signal detected; agent surfaces immediately.
SF-FR-4	Safety Protocol	MC logs and overrides all safety takeover events.
SF-NFR-1	Redundancy	Each safety-critical component includes ≥ 2 independent mitigation measures.