Software Design Description (SDD)

1. Introduction

1.1 Purpose

This Software Design Description details the architecture and design of the Autonomous Drone Delivery System (ADDS) software components that implement the requirements specified in the SRS.

1.2 Scope

The SDD covers the Control Center Subsystem (CCS), the integration with the Aerial Vehicle Subsystem (AVS), and the User Interface Subsystem (UIS), including key interfaces, data models, and error-handling strategies.

2. System Architecture

2.1 High-Level Architecture

ADDS is organized into three logical layers:

1. **Presentation Layer:** Web and mobile applications built with React and React Native.

2. **Application Layer:** Backend microservices implemented in Python 3.11 using FastAPI.

3. **Data Layer:** PostgreSQL database and a message bus for telemetry.

2.2 Major Components

- **Mission Planner Service (MPS):** Selects drones, schedules routes, and initiates missions.

- **Telemetry Processor Service (TPS):** Consumes telemetry data from drones and detects anomalies.

- **Notification Service (NS):** Sends push notifications and emails to customers.

- **Security Gateway (SG):** Terminates external TLS connections and performs authentication.

3. Detailed Design

3.1 Mission Planner Service

3.1.1 Responsibilities

- Implements SRS REQ-002 and REQ-010 for mission selection and concurrency.

- Maintains an in-memory mission registry with active missions.

3.1.2 Design Constraints and Limits

- The default deployment tier supports **up to 40 simultaneous active missions** before requiring horizontal scaling.

- A soft limit of 40 missions is enforced through admission control to avoid CPU saturation.

3.2 Telemetry Processor Service

3.2.1 Data Flow

1. Drones publish telemetry messages to MQTT topics: `telemetry/<drone_id>`.

2. TPS subscribes to these topics and writes processed records to the `telemetry` table.

3. TPS raises alerts when values exceed defined thresholds.

3.2.2 Link Loss Handling

- Upon GNSS signal loss, the CCS logic instructs the drone to **descend to a predefined safe landing zone** and land autonomously.

- After landing, TPS flags the mission as “Emergency_Land” and notifies the operator.

3.3 Notification Service

- Implements SRS REQ-009.

- Uses a message queue `notifications_out` to buffer customer notifications.

- Guarantees delivery within **20 seconds** under nominal load.

3.4 Security Gateway

3.4.1 Encryption and Authentication

- External HTTPS endpoints use **TLS 1.2 or later**.

- Command and telemetry messages are encrypted with **AES-128** using rotating keys.

- Operator logins are secured using username and password only; multi-factor authentication is planned for a future release.

3.5 Data Retention

- Mission records are stored in the `missions` table for **30 days** before being archived to cold storage.

- Telemetry records are retained online for **30 days**, after which summarised statistics are kept.

4. Interface Specifications

Interface ID	Direction	Protocol	Description
IF-001	Drone → CCS	MQTT over TLS	Telemetry data uplink
IF-002	CCS → Drone	HTTP/REST	Command API (RTH, terminate, etc.)
IF-003	CCS ↔ Mobile Apps	HTTPS/REST	Delivery tracking and notifications

5. Environmental & Hardware Considerations

- Flight controllers are rated for payloads up to **5 kg** with current hardware.

- Propulsion and motor controllers are tested for sustained winds of up to **30 knots**.

- The design assumes operation is possible in moderate rain with appropriate waterproofing.

6. Logging and Monitoring

- All services log to a centralized logging system.

- Metrics are exposed via Prometheus-compatible endpoints.

- Anomaly counters are maintained per drone for trend analysis.

7. Traceability to Requirements

| SRS Requirement | Implementing Component |

|---|---|

| REQ-001 | Mission Planner + UIS |

| REQ-002 | Mission Planner |

| REQ-004 | Telemetry Processor |

| REQ-005 | Telemetry Processor + Storage Layer |

| REQ-006 | Security Gateway |

| REQ-007 | Data Layer (missions & telemetry tables) |

| REQ-009 | Notification Service |

| REQ-010 | Mission Planner Service |

8. Future Enhancements

- Introduce full MFA integration with identity providers.

- Upgrade encryption to AES-256 consistently across all links.

- Increase tested capacity from 40 to 120 concurrent missions via autoscaling.