IMU Health Monitor - Software Requirements Specification

Document Information

Field	Value
Document ID	SRS-IMU-001
Version	1.0.0
Standard	DO-178C DAL A
Date	2026-01-31

1. Introduction

1.1 Purpose

This document specifies the software requirements for the IMU Health Monitor module, a safety-critical component for Ardupilot flight controllers.

1.2 Scope

The IMU Health Monitor monitors redundant IMU sensors, detects failures, and triggers appropriate failsafe actions to ensure safe flight operations.

1.3 Definitions

Term	Definition
IMU	Inertial Measurement Unit
WCET	Worst-Case Execution Time
DAL	Design Assurance Level
Failsafe	Automatic safety response

2. Functional Requirements

REQ-IMU-001: Redundant Sensor Monitoring

Priority: Critical
DAL: A

The system shall monitor up to 3 redundant IMU sensors simultaneously.

Rationale: Redundancy is required for fault tolerance in safety-critical systems.

REQ-IMU-002: Accelerometer Validation

Priority: Critical
DAL: A

The system shall validate accelerometer readings by comparing the measured magnitude against expected gravity (9.81 m/s²) with a tolerance of ±0.5 m/s².

Rationale: Detects sensor drift, failure, or calibration issues.

REQ-IMU-003: Gyroscope Validation

Priority: Critical
DAL: A

The system shall validate gyroscope readings by checking for excessive bias or noise during stationary conditions.

Rationale: Detects sensor drift that could cause attitude errors.

REQ-IMU-004: Cross-Validation

Priority: Critical
DAL: A

The system shall cross-validate readings between redundant IMU sensors to detect inconsistencies.

Rationale: Detects single-sensor failures that might pass individual checks.

REQ-IMU-005: Health History Tracking

Priority: High
DAL: A

The system shall maintain a health history buffer of 8 samples for trend analysis.

Rationale: Prevents false positives from transient noise.

REQ-IMU-006: Automatic Failover

Priority: Critical
DAL: A

The system shall automatically switch to a backup IMU when the primary sensor fails.

Rationale: Maintains flight capability during sensor failures.

REQ-IMU-007: Failsafe Actions

Priority: Critical
DAL: A

The system shall trigger appropriate failsafe actions:
- NONE: Normal operation (2+ healthy IMUs)
- WARN: Single healthy IMU
- LAND_IMMEDIATELY: Only degraded IMUs available
- TERMINATE: All IMUs failed

Rationale: Graduated response proportional to system health.

REQ-IMU-008: Timing Constraint

Priority: Critical
DAL: A

The main update function shall complete within 100 microseconds at 400 Hz update rate.

Rationale: Real-time performance requirement for flight control.

REQ-IMU-009: No Dynamic Allocation

Priority: Critical
DAL: A

The system shall not use dynamic memory allocation.

Rationale: DO-178C Level A requirement for deterministic behavior.

REQ-IMU-010: Diagnostic Reporting

Priority: Medium
DAL: B

The system shall provide diagnostic reporting capability for ground station telemetry.

Rationale: Enables post-flight analysis and maintenance.

3. Non-Functional Requirements

3.1 Performance

Metric	Requirement
Update Rate	400 Hz
Max Latency	100 µs
Stack Usage	< 4096 bytes
Code Size	< 8 KB

3.2 Safety

- No recursion allowed
- All loops must be bounded
- Integer overflow must be prevented
- Array bounds must be checked

3.3 Reliability

- MTBF: Consistent with flight controller lifetime
- No single point of failure in monitoring logic

4. Interface Requirements

4.1 Input Interface

```
typedef struct {
    Vector3_I32 accel;      // Accelerometer (mm/s²)
    Vector3_I32 gyro;       // Gyroscope (mrad/s)
    uint32_t timestamp_us;  // Timestamp
    bool valid;             // Data validity flag
} IMU_Reading;
```

4.2 Output Interface

```
typedef enum {
    FAILSAFE_ACTION_NONE,
    FAILSAFE_ACTION_WARN,
    FAILSAFE_ACTION_SWITCH_IMU,
    FAILSAFE_ACTION_LAND_IMMEDIATELY,
    FAILSAFE_ACTION_TERMINATE
} Failsafe_Action;
```

5. Traceability

See `traceability.md` for requirement-to-code mapping.