REPORT ON FAILSAFE MECHANISMS IN DRONES

Atharv Prasad
Swarm Robotics
MIT, Manipal
Manipal, India
atharvprasad6@gmail.com

***Abstract*—This paper presents an exhaustive technical review of the failsafe architectures within the PX4 flight stack. Beyond standard battery and signal loss protections, this report details advanced failure detectors including QuadChute logic, traffic avoidance (ADSB), environmental safeguards (wind/flight time), and preventative pre-flight consistency checks. We analyze the hierarchical state machine that governs transition logic between *Normal*, *Failsafe*, and *Emergency* states, providing a critical reference for system integrators and operators.**

***Index Terms*—PX4, Failsafe, UAS Safety, State Machine, QuadChute, Flight Termination, Autonomous Systems**

I. Introduction

In unmanned aviation, a failsafe is not merely a reaction to failure but a deterministic state transition designed to preserve the airframe and surrounding environment. The PX4 autopilot utilizes a centralized "Commander" module to monitor system health at varying frequencies (typically 50-100Hz). When a constraint is violated, the system prioritizes safety over mission execution, executing a "Graceful Degradation" of capabilities where possible, or a "Hard Failsafe" where necessary.

II. Signal and Control Failsafes

These mechanisms address the loss of external control inputs.

A. Radio Control (RC) Loss

Triggered when the pulse-position modulation (PPM) or serial receiver input stops updating.

- **Trigger:** No valid RC frame for `COM_RC_LOSS_T` (default 0.5s).
- **Logic:**
  - *Manual Modes:* Immediate transition to configured safety action.
  - *Auto Modes:* Configurable via `COM_RCL_EXCEPT`. Often disabled in Mission mode to prevent unnecessary abortions during temporary signal shadowing.
- **Parameter:** `NAV_RCL_ACT` (Hold, Return, Land, Terminate).

Prepared for Advanced UAS Operations Coursework.

B. Data Link (GCS) Loss

Monitors the heartbeat from the Ground Control Station (e.g., QGroundControl) via MAVLink.

- **Trigger:** No heartbeat for `COM_DL_LOSS_T` (default 10s).
- **Criticality:** Essential for BVLOS (Beyond Visual Line of Sight) operations.
- **Action:** Defined by `NAV_DLL_ACT`. commonly set to *Return* or *Hold*.

III. Power and Health Failsafes

A. Battery Failsafe

A three-tiered protection system based on voltage or consumed capacity (mAh).

1) **Warning:** `BAT_LOW_THR`. visual/audio alert only.
2) **Critical:** `BAT_CRIT_THR`. Triggers *Return to Launch (RTL)*.
3) **Emergency:** `BAT_EMERGEN_THR`. Triggers immediate *Land* to prevent battery cutoff in flight.

B. Flight Time Failsafe

Independent of voltage, this limits the maximum duration of a sortie.

- **Max Time:** `COM_FLT_TIME_MAX`. Triggers RTL when timer exceeds this value.
- **Low Energy Return:** `COM_FLTT_LOW_ACT`. Triggers if the estimated energy required to return home exceeds available reserves.

IV. Navigation and Environmental Failsafes

A. Position (GPS) Loss

If the Extended Kalman Filter (EKF2) variance exceeds safe limits (`COM_POS_FS_EPH`), the drone cannot hold position.

- **Graceful Degradation:** If RC is available, drops to *Altitude Mode* (manual drift control).
- **Hard Failsafe:** If no RC is available, triggers *Land* or *Flight Termination* based on `COM_POSCTL_NAVL`.

B. Geofence Breach

Enforces virtual airspace boundaries.

- **Geometry:** Cylinders (`GF_MAX_HOR_DIST`) or complex polygons.
- **Action:** `GF_ACTION`. Typically *Hold* (stop at fence) or *RTL*.

C. Traffic Avoidance (ADSB)

Uses ADS-B IN data to detect manned aircraft.

- **Parameter:** `NAV_TRAFF_AVOID`.
- **Behaviors:** Warn pilot, lower altitude, or immediate RTL if separation drops below thresholds.

D. Wind Failsafe

Uses airspeed sensors or groundspeed/wind estimation to detect dangerous gusts.

- **Trigger:** Wind speed $>$ `COM_WIND_MAX`.
- **Action:** `COM_WIND_MAX_ACT` (Return or Land).

V. Mechanical and Dynamic Failsafes

A. QuadChute (VTOL Specific)

A critical safety feature for Hybrid VTOL (Vertical Takeoff and Landing) aircraft. If the fixed-wing flight phase fails, the system "chutes" (transitions) back to multicopter mode.

- **Triggers:**
  - Altitude drops below setpoint.
  - Pitch/Roll exceeds limits (instability).
  - Airspeed drops below stall threshold.
- **Result:** Immediate transition to MC Hover and typically RTL.

B. The Failure Detector

A background process monitoring vehicle attitude and motor health.

- **Attitude Failure:** If pitch/roll exceeds 60-90 degrees (configurable) for a set time, the drone assumes loss of control.
- **Action:** Often leads to *Lockdown* (disarm) or *Flight Termination* (parachute).
- **Imbalanced Propeller:** Detects vibration signatures consistent with damaged props (`FD_IMBALANCED_PROP`). Triggers a warning or landing advice.

VI. Preventative Failsafes

Failsafes that prevent the flight from starting or continuing unnecessarily on the ground.

A. Pre-flight Arming Checks

Prevents arming if sensors are inconsistent.

- `COM_ARM_MAG_ANG`: Check magnetometer consistency.
- `COM_ARM_IMU_ACC`: Check accelerometer bias.
- `COM_ARM_EKF_HGT`: Check height estimate stability.

B. Automatic Disarm

- **Land Disarm:** `COM_DISARM_LAND`. Disarms n seconds after landing detection (default 2s).
- **Pre-flight Disarm:** `COM_DISARM_PRFLT`. Disarms if pilot does not take off within n seconds of arming (default 10s).

VII. Flight Termination vs. Lockdown

It is crucial to distinguish these two final states.

TABLE I
Termination States

State	Behavior	Use Case
Lockdown	Motors Disarmed. Servos centered.	Crash detection on ground; Kill switch.
Termination	Controllers stopped. PWM outputs set to *Failsafe Values*.	Catastrophic failure in air. Deploys parachute / airbag.

Configuration: The parameter `CBRK_FLIGHTTERM` must be enabled (set to 0) to allow the Failure Detector to trigger a true flight termination event.

VIII. Conclusion

The PX4 failsafe system is a hierarchical, state-based safety architecture. It ranges from preventative checks (Arming) to mission preservation (RTL on Battery/RC Loss) and finally to catastrophic mitigation (Flight Termination). Mastery of these parameters is essential for airworthiness certification and safe UAS operations.