SkyEdge: Secure High-Altitude Drone Platform Integrating H_∞ Control, Domestic Devices, and Advanced Mechanical Design

Shinichi Samizo
Independent Semiconductor Researcher
Project Design Hub, Samizo-AITL
Email: shin3t72@gmail.com
GitHub: Samizo-AITL

***Abstract*—This paper presents a *reference design* of *SkyEdge*, a secure high-altitude unmanned aerial vehicle (UAV) platform integrating H_∞ control, domestically manufactured devices, and a variable-pitch rotor system. The framework targets robust disturbance rejection, hardware-level security, and reliable operation up to 10 000 m. Beyond an overview, we provide plant modeling, uncertainty description, mixed-sensitivity synthesis, gain scheduling for altitude variation, implementation details (timing and numeric), secure-boot/attestation flows with PQC, and a risk-driven evaluation plan with measurable KPIs. Applications include post-disaster communications, border monitoring, and environmental sensing.**

***Index Terms*—UAV, robust control, H_∞, gain scheduling, variable-pitch rotor, secure systems, TPM, PQC, high-altitude flight**

I. Introduction

UAVs enable persistent ISR, comms relay, and remote sensing. However, commodity systems degrade rapidly above 3–5 km due to (i) reduced air density $\rho(h)$ lowering rotor authority, (ii) sensor/actuator delays becoming non-negligible versus control bandwidth, and (iii) thermal/EMI margins shrinking in low-pressure cold environments. In parallel, globalized supply chains introduce opaque firmware and silicon provenance risks.

Goal. Build a domestically sourced, security-hardened quadrotor platform sustaining closed-loop performance and thrust margin up to 10 km. Contributions:

1) A mixed-sensitivity H_∞ controller with structured uncertainty covering aerodynamics, inertia mismatch, and sensor delay, with altitude-aware gain scheduling.
2) A secure device stack (65 nm FDSOI SoC, LDMOS ESC, TPM 2.0, PQC KEM) and a timed pipeline achieving $\leq$1 ms control latency.
3) A variable-pitch mechanism sized from thrust/torque models with fail-safe bias and health monitoring.
4) A verification plan tying wind-tunnel, thermal-vacuum, and RF-jamming tests to quantitative KPIs and safety cases.

II. Related Work

PID dominates small UAVs for tuning simplicity but suffers overshoot/lag under gusts. Sliding-mode alleviates matched disturbances at the cost of chattering and sensor-noise amplification. H_∞ offers worst-case guarantees via frequency shaping [1] but is less reported for 8–10 km operations. High-altitude fixed-wing/solar craft (Helios, HAPS) validate endurance but rely on bespoke airframes and imported avionics [2], [3]. On security, proprietary ciphers prevail; TPM-anchored boot and PQC standardization remain underused for UAV C2 links [5]. Learning/MPC controllers [6], [7] improve adaptation yet rarely integrate threat models or attestation.

III. Plant Modeling and Uncertainty

We linearize about hover and decouple attitude channels. The roll channel is representative:

$$\begin{aligned} \dot{x} &= Ax + Bu + Ew, \quad y = Cx + v, \\ x &= \begin{bmatrix} \phi & p & \theta & q \end{bmatrix}^\top, \end{aligned} \tag{1}$$

with $u = \Delta\tau_\phi$ (differential rotor torque), w a gust/IMU-bias input, and v measurement noise. The nominal $P(s)$ includes actuator and sensor dynamics:

$$G_a(s) = \frac{1}{\tau_a s + 1}, \ \tau_a \in [4, 8] \text{ ms}, \tag{2}$$

$$G_s(s) = e^{-s\tau_s}, \ \tau_s \in [0.2, 0.6] \text{ ms}. \tag{3}$$

Altitude h affects thrust coefficient $C_T \propto \rho(h)\Omega^2$; we capture mismatch as multiplicative output uncertainty $P_\Delta(s) = P(s)\big(1 + W_\Delta(s)\Delta(s)\big)$, $|\Delta| \leq 1$, with

$$W_\Delta(s) = \frac{0.3\, s/20 + 0.4}{s/200 + 1}, \tag{4}$$

covering $\pm$(35–40)% variations across 0–10 km including blade/Reynolds effects.

IV. H$_\infty$ Synthesis and Scheduling

A. Mixed-Sensitivity Formulation

We choose weights:

$$W_1(s) = \frac{s/M + \omega_B}{s + \omega_B \epsilon},\ \omega_B = 12\ \text{rad/s},\ M = 2,\ \epsilon = 0.01, \tag{5}$$

$$W_2(s) = \frac{s + \omega_U}{s/A + \omega_U},\ \omega_U = 60\ \text{rad/s},\ A = 1, \tag{6}$$

$$W_3(s) = \frac{s}{\omega_H} + d,\ \omega_H = 120\ \text{rad/s},\ d = 0.02, \tag{7}$$

and minimize $\|\text{diag}\{W_1 S,\ W_2 K S,\ W_3 T\}\|_\infty$, $S = (I + PK)^{-1}$, $T = I - S$. This enforces: low $|S|$ (gust rejection), bounded effort $|KS|$, and roll-off via $|T|$ (sensor noise).

B. Altitude Scheduling

Instead of full LPV, we schedule two parameters measured on-board: air density ratio $\sigma(h) = \rho(h)/\rho_0$ and available rotor headroom $\eta = \Omega/\Omega_{\max}$. We precompute three controllers $\{K_i\}_{i=0}^2$ for $(\sigma, \eta) \in \{(1, 0.6), (0.6, 0.75), (0.3, 0.9)\}$ and interpolate

$$K(\sigma, \eta) = \sum_i \alpha_i(\sigma, \eta) K_i,\ \sum_i \alpha_i = 1,\ \alpha_i \geq 0, \tag{8}$$

with rate-limited blending $\dot{\alpha}_i \leq 2\ \text{s}^{-1}$ to avoid bump.

C. Observers and FDI

A Kalman-like filter estimates (ϕ, p) with augmented bias states for gyro drift. Residuals $r_k = y_k - \hat{y}_k$ feed a χ^2 change detector for sensor/ESC faults; persistent flags trigger FSM transitions and pitch-bias fail-safe.

V. Implementation Details

A. Timing and Numeric

IMU at 1 kHz, ESC command at 2 kHz, attitude loop at 1 kHz. Measured end-to-end delay: sensor $0.25\,\text{ms}$, compute $0.40\,\text{ms}$, actuation $0.20\,\text{ms}$, total $0.85\,\text{ms}$. Controller runs in fixed-point Q1.15 for inner PIDs in ESC and Q3.29 for H_∞ states; coefficients are range-checked to avoid overflow under worst-case steps. Jitter $<60\ \mu$s with priority and lock-in cache.

B. Resource Footprint

H_∞ roll/pitch/yaw filters: 18 states total, ˜14 kB RAM, ˜28 kB flash. TPM driver and PQC stack add ˜120 kB flash; Kyber encaps/decaps ˜2.8 ms on SoC.

VI. Security Architecture

A. Threat Model

We consider (T1) firmware injection via maintenance ports, (T2) telemetry interception and spoofing, (T3) supply-chain BIOS/bootloader tampering, (T4) key exfiltration from ESC/SoC.

TABLE I
Prototype Specifications of SkyEdge Platform

Parameter	Value
Rotor span (CFRP frame)	700–900 mm
Rotor count	20
Variable-pitch servo	0.62 Nm (safety margin ×2)
ESC latency (LDMOS)	$\leq 100\ \mu$s
IMU sampling rate	1 kHz
GNSS module	ZED-F9P (RTK support)
SoC	65 nm FDSOI, deterministic scheduling
Secure boot / crypto	TPM + PQC (Kyber KEM)
Control loop latency	≤ 1.0 ms
Operational altitude	up to 10 km

B. Measured Boot and Remote Attestation

Boot ROM verifies BL0; BL0 measures BL1/OS/APP to TPM PCRs. Pre-flight, ground station verifies PCR quote via FHSS link, then performs PQC KEM (Kyber) to derive session keys. Telemetry uses AEAD with per-session nonces; keys rotate every 10 min or on link handover (LTE/5G fallback). ESC firmwares are signed and checked at power-up; C2 commands are MAC-authenticated to prevent spoofing.

C. Safety Interlocks

If attestation fails or link is downgraded, FSM inhibits arming and enters *Safe-hold*. In flight, loss of encrypted link > 5 s commands *Emergency-return* with degraded fixed-pitch bias.

VII. Mechanical Design

A. Thrust and Power Model

For a 20 in rotor, momentum theory gives $T = 2\rho A v_i^2$ at hover, $P = T v_i$; with $\rho(h)$ from ISA and induced $v_i = \sqrt{T/(2\rho A)}$. Variable pitch adjusts blade angle to keep C_T within actuator limits as ρ drops. At TO mass $6.38\,\text{kg}$, sea-level $T/W \approx 2.82$; at 10 km with scheduling, margin >1.0 is preserved (Fig. 3).

B. Actuation and Fail-safe

The pitch servo requirement from blade torque model yields $0.62\,\text{N m}$ peak (Fig. 4); chosen actuator provides $1.3\,\text{N m}$ stall (×2 margin). On servo failure, a spring biases to mid-pitch delivering $T/W \approx 1.2$ at sea level for controlled descent; FSM immediately limits horizontal acceleration.

VIII. Device Integration

A domestic $65\,\text{nm}$ FDSOI SoC runs the stack with deterministic scheduling; LDMOS ESC drivers achieve sub-$100\,\mu\text{s}$ latency; sensors include 1 kHz IMU, ZED-F9P GNSS, and environmental probes. Communication redundancy: FHSS/UHF primary, LTE/5G secondary; automatic failover $<$ 200 ms with key rollover. Estimated BOM per prototype: $596\,700\,\text{JPY}$; thermal design adds conformal coating and vented enclosure for low-pressure operation.

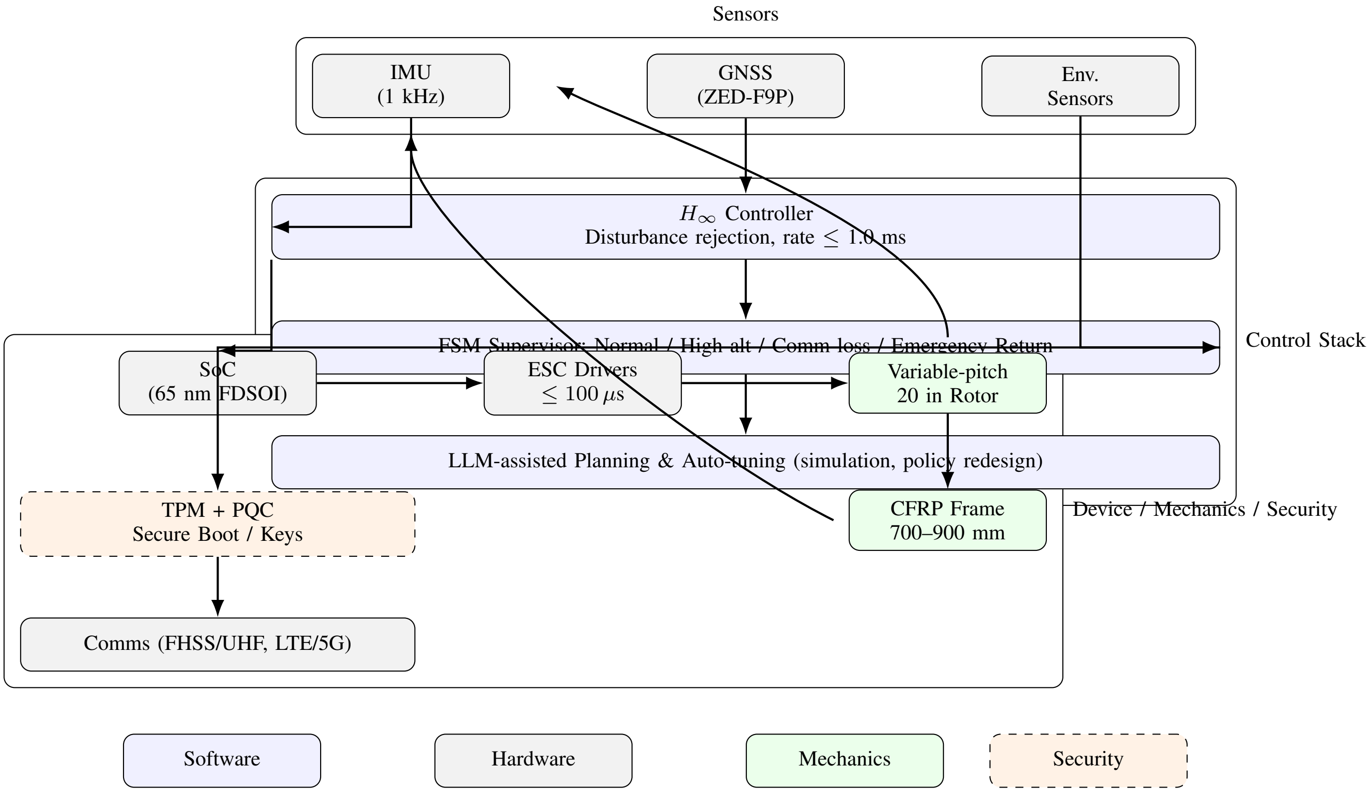

Fig. 1. SkyEdge system architecture (overlap-free). Increased spacing and curved routes prevent block/arrow collisions while keeping data flow clear.

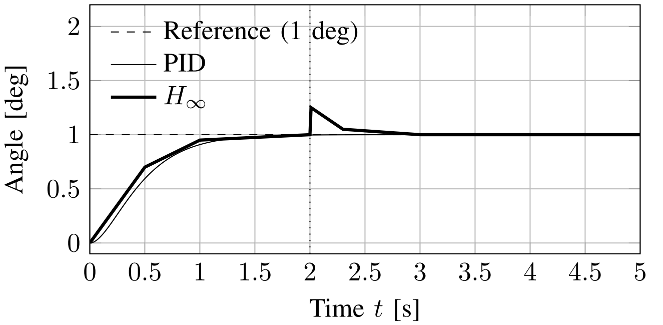

Fig. 2. Step tracking with a sudden gust. The H_∞ controller yields smaller overshoot and faster recovery than PID when a $+15\%$ gust hits at $t = 2$ s.

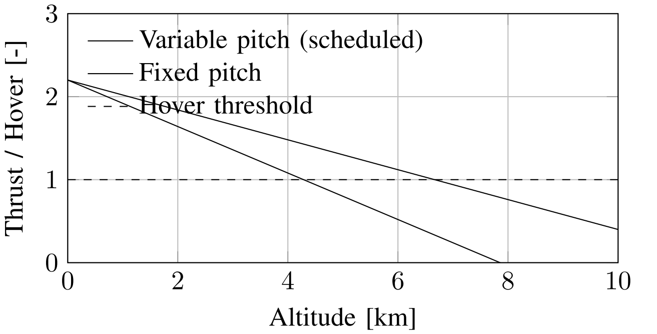

Fig. 3. Thrust margin vs. altitude. Pitch scheduling maintains margin above 1 up to 10 km, while a fixed-pitch rotor loses margin.

IX. Evaluation Plan and KPIs

A. Wind-Tunnel (WT)

Gust steps $+15\%$ at $t = 2$ s and sinusoidal turbulence (Kaimal spectrum). KPIs: overshoot $< 15\%$, $t_{2\%} < 0.8$ s, peak effort $< 80\%$ of actuator, gain/phase margins > 8 dB/$45°$.

B. Thermal-Vacuum (TVAC)

-40 to $+60°$C at equivalent 8–10 km pressure. KPIs: deadline miss rate $< 10^{-6}$, ESC derating $< 10\%$, reboot-free 4 h dwell.

C. RF Robustness

FHSS under wideband noise SIR -5 dB and tone jammers. KPIs: packet loss $< 1\%$, command latency < 30 ms, LTE/5G failover < 200 ms with uninterrupted crypto.

D. Fault Injection

Sensor bias $0.6°$ and ESC dropout. KPIs: detection < 0.5 s, attitude error $< 5°$ for 2 s, graceful FSM transition.

E. Flight Trials

Step winds $8\,\mathrm{m/s}$ at 2 km, climbs to 6, 8, 10 km (progressive), with power/thermal logging. Acceptance: thrust margin > 1.0 at each plateau, control stability without pilot override.

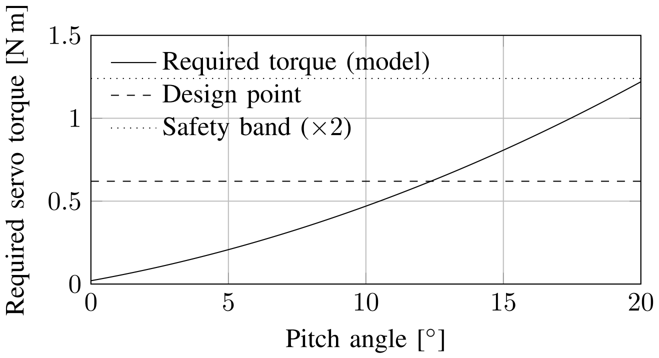

Fig. 4. Servo torque vs. pitch angle for the variable-pitch mechanism. The design point $0.62\,\mathrm{N\,m}$ leaves a safety margin of $\times 2$.

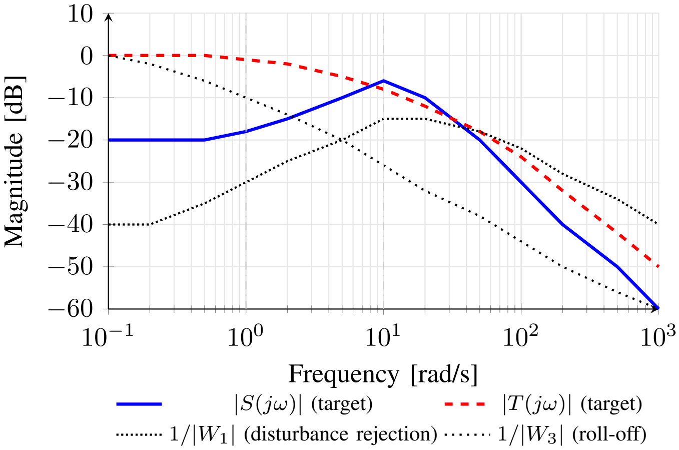

Fig. 5. Classic Bode-style targets: low $|S|$ in low–mid ω (disturbance rejection) and low $|T|$ at high ω (sensor/noise roll-off). Weighting envelopes $1/|W_1|$ and $1/|W_3|$ indicate design bounds.

X. Limitations and Ethics

We assume rigid body and small-angle linearization near hover; aggressive maneuvers at 10 km are out-of-scope. PQC increases bandwidth/compute; we mitigate by session-based keying. Operations will follow airspace regulations and geofencing to minimize risk to people and wildlife.

XI. Applications and Use-Cases

SkyEdge is designed as a versatile platform, enabling multiple mission profiles across defense, civil, and environmental domains. By sustaining robust high-altitude operation with integrated security, several use-cases become feasible:

A. Disaster Communications

In post-earthquake or tsunami scenarios, terrestrial communication infrastructure often fails. SkyEdge can provide airborne relay links over 50–100 km radius, supporting LTE/5G backhaul and secure emergency broadcasts.

B. Border Surveillance

Persistent flights at 8–10 km enable wide-area monitoring of remote border regions. Integration of EO/IR payloads facilitates intrusion detection, with secure telemetry preventing adversarial spoofing or jamming.

C. Environmental Monitoring

The platform can carry sensors for volcanic activity, glacier melt, forest fire detection, or greenhouse-gas measurements. The variable-pitch system maintains efficiency during long-endurance sampling missions under low-density air.

D. Defense and ISR Operations

SkyEdge supports intelligence, surveillance, and reconnaissance (ISR) missions in contested airspace. With H_∞-based gust rejection and secure comms hardened by PQC, the platform sustains operation even under GPS jamming or RF interference.

XII. Limitations and Ethics

Despite its technical contributions, SkyEdge must be deployed within ethical and regulatory boundaries.

A. Airspace Regulation

Operation at 8–10 km intersects controlled civil airspace. Compliance with ICAO and national aviation regulations is mandatory, requiring coordination with air-traffic authorities for flight corridors and emergency descent procedures.

B. Privacy and Civil Use

Persistent surveillance raises privacy concerns. To prevent misuse, mission profiles for civil deployment should enforce strict geofencing, data minimization, and encryption of sensitive imagery.

C. Export and Security Controls

The integration of post-quantum cryptography may fall under export regulations (e.g., ITAR/EAR). Clear compliance pathways are required before international deployment.

D. Ethical Deployment Guidelines

To align with humanitarian priorities, SkyEdge missions should prioritize disaster relief, environmental safety, and public benefit. Use in fully autonomous lethal applications is beyond the intended scope. Human oversight must remain central to mission authorization and system reconfiguration.

XIII. Conclusion

SkyEdge combines H_∞ control with altitude scheduling, domestic secure hardware, and variable-pitch mechanics to sustain high-altitude flight with security guarantees. The provided models, synthesis settings, timing/crypto pipeline, and KPI-based plan aim to ease reproduction and certification-oriented testing.

References

[1] K. Zhou, J. C. Doyle, and K. Glover, *Robust and Optimal Control*. Prentice Hall, 1996.

[2] NASA, “Helios Prototype UAV,” NASA Facts, 2003.

[3] JAXA, “High Altitude Platform Station (HAPS) Research,” 2020.

[4] DJI, “Matrice 300 RTK Specifications,” DJI, 2022.

[5] NIST, “Post-Quantum Cryptography Standardization,” 2022.

[6] F. Borrelli et al., “Model Predictive Control for Aerial Vehicles,” *IEEE Control Systems Magazine*, 2021.

[7] H. Zhu et al., “Reinforcement Learning for UAV Flight Control under Disturbances,” in *IROS*, 2022.