

Minimum-Disclosure Civil-Military Deconfliction for UAS Traffic Management in Thailand: A Simulation Study

Cattleya Delmaire; Pannapat Suwisutthimontree; Settapong Malisuwan*

Excellence Center of Space Technology and Research (ECSTAR), International Academy of Aviation Industry (IAAI), King Mongkut's Institute of Technology Ladkrabang, Bangkok, Thailand

*Corresponding author

Abstract

Background: Unmanned aircraft system traffic management (UTM) depends on information exchange for conflict management, yet civil-military coordination creates tension between safety visibility and operational security. **Objective:** This study develops and evaluates a trusted minimum-disclosure broker that computes on protected civil and military intent while releasing only a time-limited conflict token and safe-action advisory. **Methods:** A reproducible Monte Carlo experiment compared no cross-domain sharing, five-second delayed state sharing, full trajectory sharing, and the minimum-disclosure broker across three civil traffic densities, three service-latency levels, three navigation-error levels, and 250 replications per condition. **Results:** Across 27,000 policy evaluations, 72,446 encounter events generated 17,029 modeled conflicts before intervention. The broker left 2.60% unresolved (95% cluster-bootstrap interval: 2.36%–2.86%), compared with 2.43% for full sharing, 15.80% for delayed sharing, and 37.49% for no sharing. Its paired difference from full sharing was 0.17 percentage points (95% interval: –0.13 to 0.49), satisfying a one-percentage-point engineering noninferiority margin while exposing no raw military trajectory states to the civil domain. **Conclusion:** The findings support staged evaluation of a Thai UTM architecture in which safety decisions are shared but sensitive mission intent remains compartmented. Operational use requires hardware-in-the-loop, cybersecurity, and field validation.

Keywords

UAS Traffic Management; Civil-Military Coordination; Conflict Deconfliction; Operational Security; Monte Carlo Simulation; Thailand.

1.Introduction

Low-altitude unmanned aircraft system (UAS) operations are moving from isolated flights toward networked, repeatable, and beyond-visual-line-of-sight services. In this setting, conventional voice coordination does not scale. The Federal Aviation Administration (FAA, 2025) describes UTM as a collaborative ecosystem of regulatory requirements, interoperable services, and automated interfaces that support flight planning, authorization, surveillance, and conflict management. The European U-space framework likewise requires digital services for identification, geo-awareness, traffic information, and flight authorization (European Commission, 2021; European Union Aviation Safety Agency [EASA], 2024). These models assume that operators exchange sufficient operational information to keep aircraft from occupying unsafe combinations of space and time.

That assumption becomes difficult when civil and military UAS share or adjoin the same low-altitude environment. Civil operators need timely constraints and deconfliction decisions, but a military

authority may be unable to disclose exact routes, schedules, aircraft identities, sensor tasking, or mission changes. Withholding all information preserves secrecy but weakens anticipation. Publishing complete intent improves strategic coordination but may expose operational patterns. Delaying position information is an intuitive compromise, yet a delayed state can be both sensitive enough to reconstruct a route and too stale to support safe resolution of a fast-changing encounter. The design problem is therefore not whether to share everything or nothing, but which safety-relevant decision can cross domains without the underlying intent crossing with it.

Thailand is a useful case for this problem. Civil UAS registration and operating permissions are administered through the Civil Aviation Authority of Thailand (CAAT) UAS portal, while radio equipment and spectrum-related registration involves the National Broadcasting and Telecommunications Commission (NBTC) (CAAT, 2025; NBTC, n.d.). The Geo-Informatics and Space Technology Development Agency (GISTDA, n.d.) has also described the AMETHYST project as a UTM prototype intended for standardized testing and eventual service provision. Publicly available material, however, does not define how a future service should deconflict sensitive state missions with civil operations while limiting cross-domain disclosure. This statement concerns the public design record; it does not assert that Thai security agencies lack internal coordination procedures.

This paper addresses that design gap through a new, reproducible simulation rather than through interviews, classified data, or claims of field deployment. It proposes a trusted broker that calculates conflict risk inside a protected computation boundary and releases only a short-lived decision token. The study asks: (1) how does the broker compare with full, delayed, and absent cross-domain sharing in conflict resolution; (2) how sensitive are the results to traffic density, communication latency, and navigation error; and (3) what disclosure-efficiency trade-off does the broker create? The contribution is threefold: a specific civil-military information boundary, an auditable simulation model, and implementation recommendations tied to Thailand's emerging UTM environment.

2.Literature Review

2.1UTM deconfliction and information exchange

The International Civil Aviation Organization (ICAO, 2020) frames UTM as an air traffic management subsystem requiring interoperable information protocols, cybersecurity, and coordinated access to constraints and operational intent. NASA flight demonstrations similarly treated strategic deconfliction as a cooperative information-sharing problem. Rios et al. (2020) evaluated strategic deconfliction during the Technical Capability Level 4 demonstration, while the FAA's second UTM pilot phase demonstrated shared operational intent and UAS volume reservations across service providers (FAA, 2021). These programs establish that automation requires structured data exchanges rather than ad hoc notifications.

Conflict detection can use either declared intent or an extrapolation of current state. Hoekstra and Ellerbroek (2021) explain that state-based methods project relative motion to a closest point of approach, whereas intent-based approaches use flight plans or transmitted future states. Boronat et al. (2023) showed that a centralized service can process future-position messages for thousands of simulated UAVs and provide approximately 11 seconds of conflict anticipation. Such architectures are technically promising, but their performance is obtained by giving the central controller detailed future locations. The present study retains centralized conflict computation while changing what is released to the other operational domain.

2.2.Privacy, security, and minimum disclosure

UTM security research has focused on authentication, integrity, access control, and auditability. Allouch et al. (2021) proposed a blockchain-supported architecture to protect UTM flight-path transactions. Baptista et al. (2024) developed DFly to make registration and flight authorization publicly auditable while preserving privacy. These studies demonstrate that traceability and confidentiality need not be treated as opposites. However, cryptographic integrity alone does not answer how much mission intent another operator should see.

A more direct precedent is the privacy-preserving airspace-allocation work of Maheshwari et al. (2025), which coordinates capacity-constrained advanced air mobility routes without requiring operators to reveal all private preferences. NASA's Technical Capability Level 3 observations also

recorded a practical tension: participants did not wish to share all data, although they accepted that some exchange was necessary for UTM value (Martin et al., 2019). The current paper applies that minimum-necessary principle to civil-military deconfliction. It does not claim a cryptographically private implementation. Instead, it evaluates a logical broker and defines the security boundary that a later implementation must enforce with encryption, hardware security, access control, independent audit, redundancy, and fail-safe procedures.

2.3. Research gap and design proposition

Existing UTM work therefore provides mature concepts for intent exchange, centralized and distributed deconfliction, and secure transaction handling. The unresolved design question is whether a brokered decision can approach the safety performance of full trajectory sharing without exposing the trajectory to the civil domain. For Thailand, this question is more immediately actionable than proposing another broad national authority chart: it specifies one interface that could be tested inside a regulatory sandbox or future AMETHYST-related demonstration. The proposition evaluated here is that a protected broker can be practically non-inferior to full sharing for modeled conflict resolution, provided that it has timely internal access to both intents and returns a conservative, enforceable advisory.

3. Materials and Methods

3.1 Proposed architecture

Figure 1 presents the logical architecture. Civil operators submit their operation plans through a civil UTM service interface. The military mission system submits encrypted intent to a trusted deconfliction broker. Exact military intent remains inside the protected boundary. The civil output contains a pseudonymous conflict token, validity interval, and safe-action code such as hold, altitude reassignment, route exclusion, or authorization denial. The military domain receives only an acknowledgment unless its own action is required.

Governance services manage policy, keys, audit records, continuity, and post-event accountability. The broker is a functional role rather than a presumption that one agency must own the system.

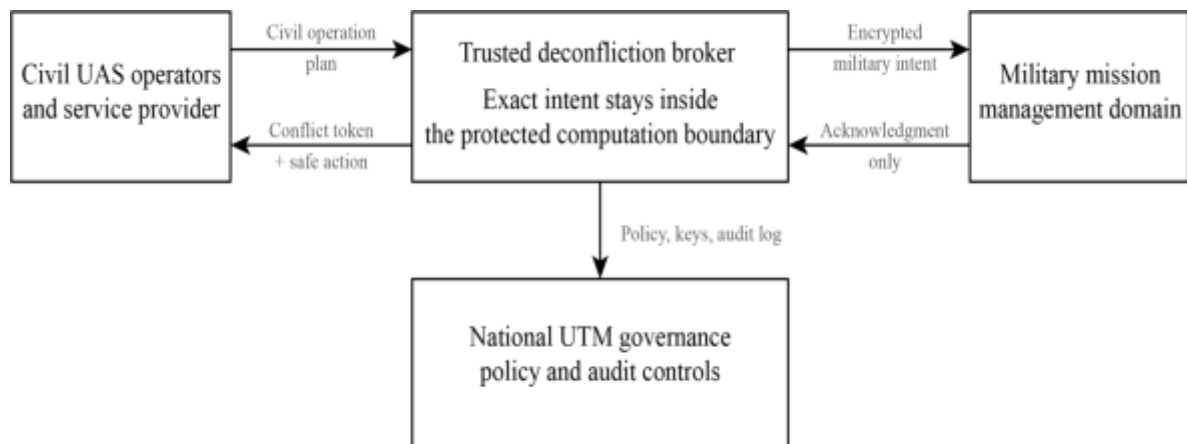


Figure 1. Proposed minimum-disclosure civil-military UTM architecture.

The architecture assumes mutual authentication, encrypted transport, data-at-rest protection, role-based access, immutable audit evidence, separation between operational and administrative identities, and redundant service instances. Those controls are requirements for implementation, not simulated achievements. The simulation isolates the information-policy question: what happens when full intent is available inside the decision boundary but is not released across it?

3.2. Compared information policies

Table 1. Cross-domain information policies evaluated in the simulation.

Policy	Look-ahead	Information available for deconfliction	Trajectory disclosure
No sharing	10 s	Current relative state available only to local/onboard sensing	0 raw states
Delayed state	30 s	Military state delayed by 5 s; no future intent	60 states per military flight-minute
Full trajectory	60 s	Current state plus 60 future states every 5 s	732 states per military flight-minute
Minimum-disclosure broker	60 s	Exact intent used internally; only decision token crosses domain	0 raw states; tokens only

Note. Disclosure counts raw trajectory states received outside the military domain; internal protected computation is not counted as cross-domain release.

Full trajectory sharing and the broker used the same 60-second horizon and the same horizontal and vertical alert buffers. This controls the detection logic so that the comparison tests disclosure architecture rather than giving the proposed method a more favorable conflict threshold. Delayed sharing used a five-second source delay and a 30-second extrapolation horizon. The no-sharing condition represented a local or onboard last-line warning with a 10-second horizon. It does not represent a complete detect-and-avoid system and should not be interpreted as a certification claim.

3.3. Encounter model and factorial experiment

The experiment was implemented in Python with NumPy, pandas, and Matplotlib. It models candidate civil-military encounters at their closest point of approach (CPA), which is a standard abstraction for conflict analysis (Hoekstra & Ellerbroek, 2021). For encounter i , a pre-intervention loss of separation was recorded when both conditions were true:

$$C_i = I(d_{h,i} < R_h \wedge d_{v,i} < R_v).$$

Here, $d_{h,i}$ and $d_{v,i}$ are the horizontal and vertical distances at CPA, $R_h = 60$ m, and $R_v = 30$ m. These are experimental thresholds selected for policy comparison; they are not presented as Thai regulatory separation minima.

Each 600-second scenario contained three military flights and 30, 60, or 90 civil flights. Candidate encounter counts followed a Poisson distribution with mean 0.060 times the product of civil and military flight counts. To obtain adequate observations near the safety boundary, 35% of encounters were generated from a controlled stress distribution: horizontal miss distance followed a Rayleigh distribution with 40 m scale and vertical distance followed a half-normal distribution with 12 m standard deviation. The remaining 65% were near-but-safe background encounters with horizontal distance equal to 60 m plus an exponential random variable with 45 m scale, capped at 250 m; their vertical levels were centered at 0, 30, or 60 m. This mixture is an explicit stress-test device and is not an estimate of Thailand's real encounter frequency.

Table 2. Principal simulation parameters.

Parameter	Value or distribution
Scenario duration	600 s
Civil traffic	30, 60, or 90 flights
Military traffic	3 flights
Median service latency	0.3, 1.0, or 3.0 s; lognormal dispersion 0.35
Horizontal navigation error	3, 10, or 20 m standard deviation
Relative speed	Uniform, 12-25 m/s
Maneuver intensity	Beta(2, 3)
Resolution lead-time requirement	8 s
Replications	250 per factorial condition
Random seed	20260827

Note. All inputs are synthetic and are documented in the supplied source code. The full and broker policies predicted CPA using protected intent with navigation and latency error. The delayed policy added uncertainty proportional to five seconds of source delay, relative speed, and maneuver intensity. The no-sharing policy used a shorter state-based horizon. An alert resolved a true conflict when the predicted distances entered the policy buffer and the remaining lead time after source and service latency was at least eight seconds. Conservative alerts on safe encounters produced modeled delay but no safety credit. The mean delay per civil flight included all flights, including those that received no advisory.

3.4. Metrics and statistical analysis

Safety metrics were alert recall, alert precision, resolution rate, and unresolved-conflict rate. Efficiency was represented by mean modeled delay per civil flight. Disclosure was measured as raw trajectory states exposed per military flight-minute. A full-intent update contained the current state plus 60 future states and occurred every five seconds; delayed state sharing released one state each second. The broker released no raw military states, although it generated conflict tokens when an advisory was required. This disclosure measure is intentionally narrow: it does not quantify information that might be inferred from repeated advisories.

The full factorial included three traffic densities, three latency levels, three navigation-error levels, 250 replications, and four policies. The resulting 6,750 scenario replications were evaluated under every policy, giving 27,000 policy evaluations. Proportions were pooled across encounters. Ninety-five percent uncertainty intervals for unresolved-conflict rates were calculated by 3,000 cluster-bootstrap samples of the paired scenario replications. The broker-full comparison preserved pairing, and a one-percentage-point upper margin was selected as a practical engineering non-inferiority criterion. No hypothesis of real-world operational equivalence is made.

4. Results

4.1. Overall performance

The simulation generated 72,446 candidate encounters, of which 17,029 met the modeled loss-of-separation definition before intervention. Table 3 reports pooled results. No cross-domain sharing detected many conflicts, but its short horizon and latency left 37.49% unresolved. The five-second delayed state reduced the unresolved rate to 15.80%, but it had the lowest alert precision because maneuver and staleness enlarged prediction error. Full trajectory sharing produced the lowest unresolved rate at 2.43%. The minimum-disclosure broker produced 2.60%, a difference of 0.17 percentage points.

Table 3. Overall safety, efficiency, and disclosure results.

Policy	olved conflicts, % (95% CI)	Recall, %	Precision, %	ean delay, s/flight	Raw states/min
No sharing	37.49 (36.32-38.67)	89.65	81.83	0.90	0
Delayed state	15.80 (15.22-16.38)	86.83	57.79	1.08	60
Full trajectory	2.43 (2.19-2.68)	97.65	56.41	0.95	732
Minimum-disclosure broker	2.60 (2.36-2.86)	97.45	56.18	1.05	0

Note. Mean delay is averaged over every civil flight, including unaffected flights. Raw states/min is measured per military flight-minute.

The paired bootstrap interval for the broker-minus-full difference was -0.13 to 0.49 percentage points. The upper bound remained below the one-percentage-point criterion. The broker achieved this result without raw military state release; it issued

an average of 4.38 decision tokens per 10-minute scenario. Its mean delay was 0.10 seconds per civil flight higher than full sharing because conservative conflict tokens generated slightly more interventions. The similar recall and precision values for full and brokered sharing reflect their common internal horizon and buffers.

4.2. Traffic density and latency sensitivity

Figure 2 shows that the two intent-aware policies remained close across traffic density. Broker unresolved rates were 3.02%, 2.85%, and 2.30% at 30, 60, and 90 civil flights, respectively; the non-monotonic pattern is within Monte Carlo variation and reflects pooled navigation and latency conditions. The principal effect of greater traffic was more conflict tokens and a modest increase in average delay, not a systematic deterioration in broker safety.

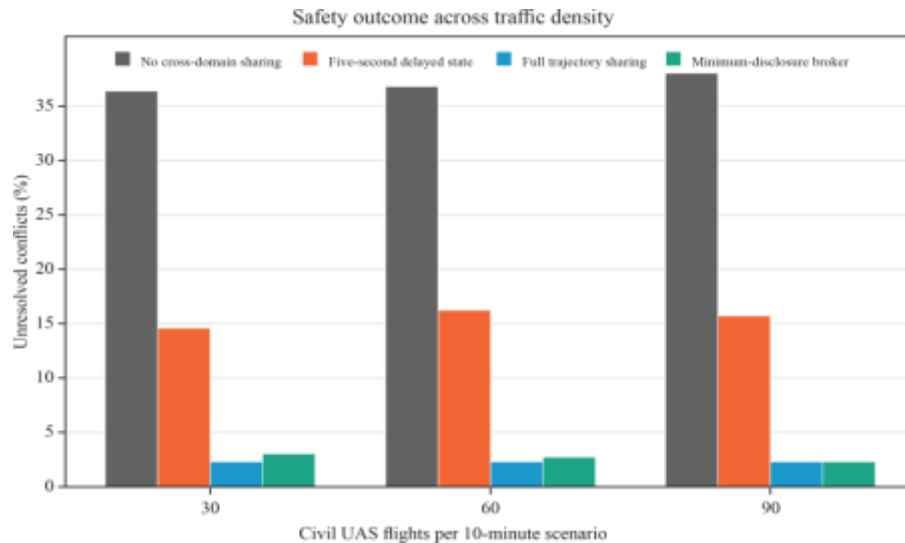


Figure 2. Unresolved-conflict rate by civil traffic density, pooled across latency and navigation-error conditions.

Latency separated the intent-aware policies from short-horizon methods more clearly (Figure 3). At 0.3, 1.0, and 3.0 seconds median latency, broker unresolved rates were 2.55%, 2.17%, and 3.07%; full sharing produced 2.11%, 2.19%, and 2.98%. In contrast, the no-sharing condition rose from 10.55% to 88.83% at the stressed three-second latency because a 10-second local warning frequently failed to preserve the required eight-second resolution margin. Delayed state sharing rose from 11.98% to 20.96%. This result is a consequence of the modeled horizons and should be interpreted as a sensitivity finding, not as a measured communication performance claim.

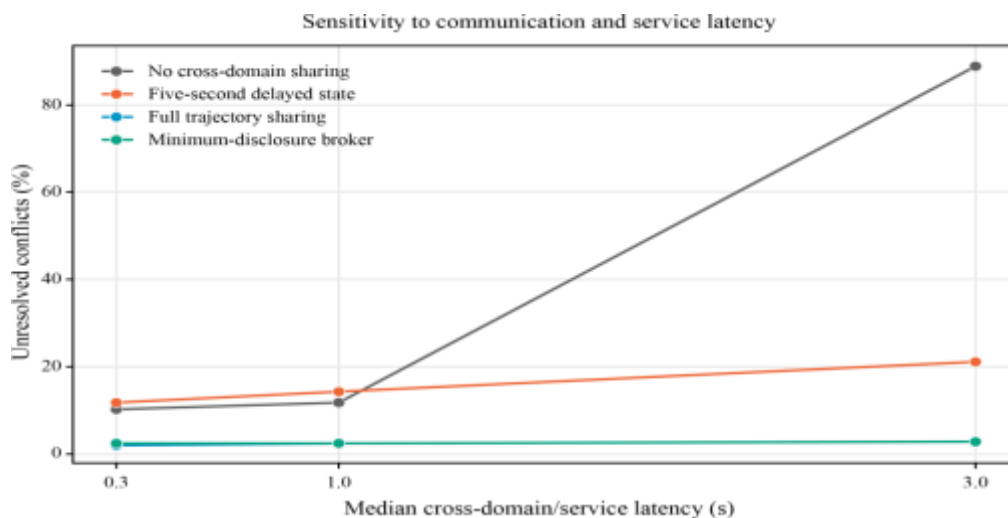


Figure 3. Sensitivity of unresolved-conflict rate to median communication and service latency.

4.3.Safety-disclosure trade-off

Figure 4 places safety outcome against raw trajectory disclosure. Full sharing achieved the best point estimate but released 732 trajectory states per military flight-minute under the experimental message design. Delayed sharing released 60 states and retained a substantially higher unresolved rate. The broker and no-sharing conditions both released zero raw military states, but their safety outcomes were sharply different because the broker could compute on protected intent before issuing a decision. The comparison illustrates the central design claim: non-disclosure to another operator does not require non-use of the data inside a trusted safety boundary.

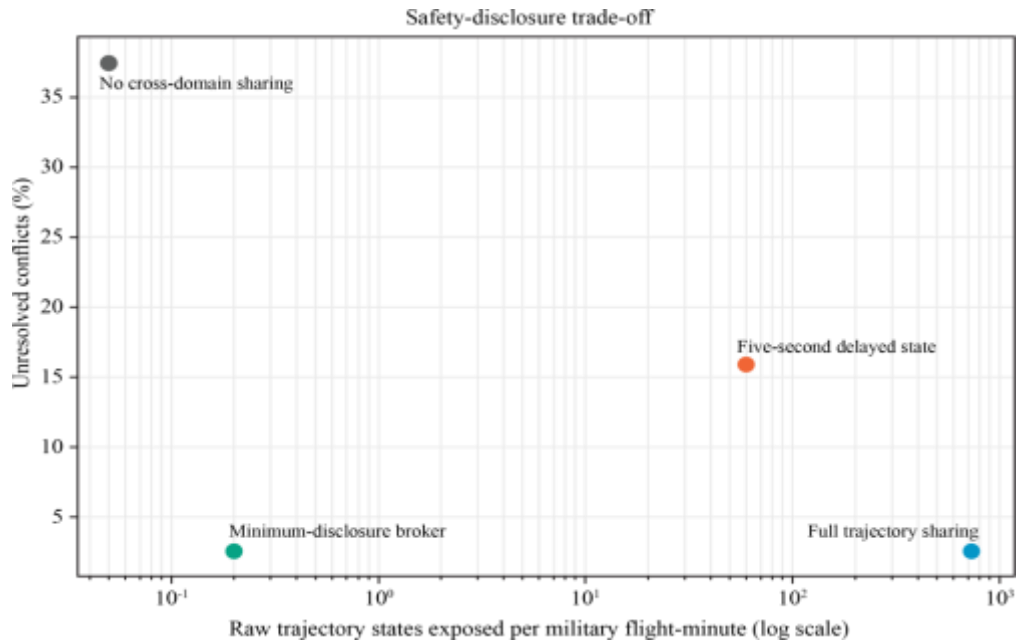


Figure 4. Safety-disclosure trade-off. Zero-disclosure policies are slightly separated on the log-scale axis for visibility; both have a reported value of zero raw states.

5.Discussion

5.1Interpretation

The results do not show that secrecy is cost-free. They show that the location of computation matters. Full sharing and the broker used equivalent intent-aware detection logic, so their safety outcomes were close. The broker's benefit came from controlling the output boundary, not from a superior conflict algorithm. Delayed state sharing performed worse because it sacrificed both prediction quality and confidentiality: historical states still reveal movement patterns, while staleness degrades maneuver prediction. No sharing preserved the data boundary but depended on a short final warning that became fragile under service delay.

Alert precision near 56% for both intent-aware policies may appear low, but it results from deliberately conservative buffers and the inclusion of many near-safe encounters in the stress design. In an operational system, false advisories consume capacity and can reduce trust; they cannot simply be ignored. The broker's slightly higher mean delay therefore identifies a real tuning problem. Buffer size, token granularity, priority rules, and the choice among hold, altitude, and reroute actions should be optimized jointly rather than treating minimum disclosure as a binary privacy feature.

5.2Implications for Thailand

For Thailand, the proposed interface could be tested as a bounded service within existing civil UAS modernization rather than requiring immediate institutional consolidation. CAAT or an authorized service provider could submit civil operation plans; a defense-controlled gateway could retain military

intent; and a jointly governed broker could return time-limited decisions. GISTDA's stated objective of a standardized, tested UTM prototype provides a plausible research environment, although this paper does not claim participation in or endorsement by GISTDA, CAAT, NBTC, or the Ministry of Defence.

A staged sandbox should begin with synthetic and prerecorded routes, then progress to hardware-in-the-loop testing, segregated flight trials, and only later limited operational demonstrations. Acceptance criteria should cover safety performance, service latency, token replay protection, key compromise, insider misuse, denial of service, auditability, continuity, and emergency override.

Governance must also define who may reconstruct events after an incident, under what legal authority, and how long protected intent and audit evidence are retained. The broker should fail predictably: if trust, connectivity, or timing is lost, it should default to a predefined protected volume, landing action, or other approved contingency rather than silently authorizing a flight.

5.3.Limitations

This study has six main limitations. First, all trajectories are represented by synthetic CPA encounters; no Thai operational flight records or military routes were used. Second, the encounter mixture intentionally oversamples close approaches and cannot estimate national collision frequency. Third, the 60 m horizontal and 30 m vertical thresholds are modeling choices, not regulatory prescriptions. Fourth, conflict resolution is abstracted as successful when sufficient alert lead time exists; vehicle dynamics, wind, command-and-control loss, pilot response, and airspace obstacles are not modeled explicitly. Fifth, the trusted broker is a logical architecture without a cryptographic protocol, certified security kernel, or penetration testing. Sixth, the raw state count captures direct disclosure but not inference attacks from repeated tokens.

Accordingly, the results support feasibility for further engineering, not operational approval. Future work should implement the broker using a dual-domain guard or confidential-computing environment, quantify token inference risk, model three-dimensional route resolution, test mixed crewed-uncrewed encounters, compare centralized and federated ownership, and validate performance with Thai regulators and operators under an approved research protocol.

6.Conclusion

Civil-military UTM does not need to choose between complete trajectory publication and operational silence. In this simulation, a trusted minimum-disclosure broker approached full-sharing safety while releasing no raw military trajectory states to the civil domain. Its unresolved-conflict rate was 2.60%, compared with 2.43% for full trajectory sharing, and the paired upper confidence bound remained within a one-percentage-point engineering margin. Delayed sharing and no sharing were materially less effective, particularly under stressed latency. For Thailand, the practical next step is a controlled prototype that validates the information boundary, service performance, contingency behavior, and legal accountability. The proposed architecture is therefore best viewed as an auditable design hypothesis for a regulatory sandbox, not as a deployed national UTM solution.

Acknowledgments

Not applicable.

Conflict of Interest

The authors declare no conflict of interest.

Funding

This simulation study received no external funding.

Ethical Approval

Not applicable. The study used synthetic computer-generated encounters and involved no human participants, animals, personal data, or operational military data.

Data Availability

The simulation source code, parameter definitions, random seed, aggregate results, and replication-level output are supplied as supplementary material with the submission.

Author Contributions

All authors contributed to conceptualization, methodology, interpretation, manuscript review, and approval of the submitted version.

References

- Allouch, A., Cheikhrouhou, O., Koubâa, A., Toumi, K., Khargui, M., & Nguyen Gia, T. (2021). UTM-Chain: Blockchain-based secure unmanned traffic management for Internet of Drones. *Sensors*, 21(9), 3049. <https://doi.org/10.3390/s21093049>
- Baptista, F., Dehez-Clementi, M., & Detchart, J. (2024). DFly: A publicly auditable and privacy-preserving UAS traffic management system on blockchain. *Drones*, 8(8), 410. <https://doi.org/10.3390/drones8080410>
- Boronat, P., Pérez-Francisco, M., Wubben, J., Calafate, C. T., Cano, J. C., & Casado, R. (2023). Assessing the limits of centralized unmanned aerial vehicle conflict management in U-Space. *IET Intelligent Transport Systems*, 17(12), 2493-2504. <https://doi.org/10.1049/itr2.12426>
- Civil Aviation Authority of Thailand. (2025, January 16). Important things to know before using drones [Thai]. <https://www.caat.or.th/do-you-know/135237/>
- European Commission. (2021). Commission Implementing Regulation (EU) 2021/664 of 22 April 2021 on a regulatory framework for the U-space. https://eur-lex.europa.eu/eli/reg_impl/2021/664/oj/eng
- European Union Aviation Safety Agency. (2024). Easy access rules for U-space. <https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-u-space>
- Federal Aviation Administration. (2021). UAS Traffic Management Pilot Program Phase 2 progress report. https://www.faa.gov/sites/faa.gov/files/uas/research_development/traffic_management/utm_pilot_program/UTM_Pilot_Program_Phase_2_Progress_Report.pdf
- Federal Aviation Administration. (2025, May 2). Unmanned Aircraft System Traffic Management (UTM). https://www.faa.gov/uas/advanced_operations/traffic_management
- Geo-Informatics and Space Technology Development Agency. (n.d.). Development of Unmanned-Aircraft-System Traffic Management - UTM. Retrieved August 27, 2026, from <https://sapace.gistda.or.th/en/services/space-technology-research-center-s-trec/unmanned-aircraft-system-traffic-management/>
- Hoekstra, J. M., & Ellerbroek, J. (2021). Aerial robotics: State-based conflict detection and resolution (detect and avoid) in high traffic densities and complexities. *Current Robotics Reports*, 2, 297-307. <https://doi.org/10.1007/s43154-021-00061-6>
- International Civil Aviation Organization. (2020). Unmanned Aircraft Systems Traffic Management (UTM): A common framework with core principles for global harmonization (3rd ed.). <https://www.icao.int/safety/UA/Documents/UTM%20Framework%20Edition%203.pdf>
- Maheshwari, C., Mendoza, M. G., Tuck, V. M., Su, P.-Y., Qin, V. L., Seshia, S. A., Balakrishnan, H., & Sastry, S. (2025). Privacy-preserving mechanisms for coordinating airspace usage in advanced air mobility. *ACM Journal on Autonomous Transportation Systems*, 2(4), Article 19. <https://doi.org/10.1145/3732290>
- Martin, L. H., Wolter, C. A., Jobe, K. K., Homola, J. R., Cencetti, M., Dao, Q., & Mercer, J. (2019). TCL3 UTM (UAS Traffic Management) flight tests (NASA/TM-2019-220347). National Aeronautics and Space Administration. <https://www.nasa.gov/wp-content/uploads/2024/04/2019-martin-tm-220347-tcl3-utm-508-0.pdf>
- National Broadcasting and Telecommunications Commission. (n.d.). Registration portal for unmanned aerial vehicle radio equipment. Retrieved August 27, 2026, from <https://anyregis.nbtc.go.th/>
- Rios, J. L., Homola, J. R., Craven, N., Verma, P., & Baskaran, V. (2020). Strategic deconfliction performance: Results and analysis from the NASA UTM Technical Capability Level 4 demonstration (NASA/TM-2020-5006337). National Aeronautics and Space Administration. <https://www.nasa.gov/directorates/armd/aosp/utm/utm-nasa-technical-documents-papers-and-presentations/>