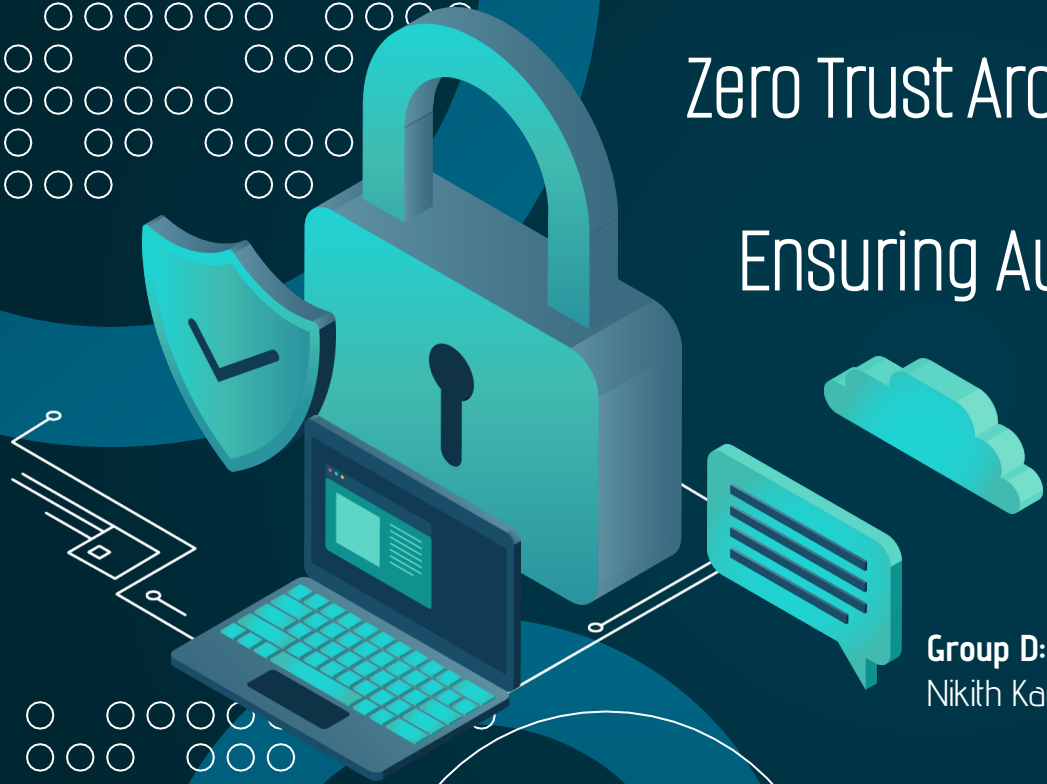
Zero Trust Architecture in Securing UAV Systems - Ensuring Authorized Access to UTM Services



Group D: Noor Qadir, Shriya Pasyavala, Rahul Patel, Blake Lainhoff, Nikith Kadambi, Arshraj Singh & Solomon Paime-George

Overview

01 PROBLEM & MOTIVATION

02 THREAT ANALYSIS & REQUIREMENTS

03 PROPOSED SOLUTION & ENTREPRENEURIAL VALUE

04 CONCLUSION

Problem Statement

UAV Adoption Accelerating in Commercial and Public Sectors

- Brings forth more challenges
- UTM security needs stronger safeguards

Operational View

- Unauthorized access undermines compliance
- Results in loss of critical information, causes flight disruption

Technical View

- Static Access Models lack continuous verification, leave UTM services vulnerable
- ZTA eliminates implicit trust, enforces continuous verification, least privilege

Scalability

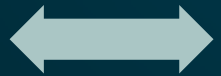
- Security is a strong, present barrier for growth
- Modern Ai-powered adversaries invalidate perimeter models
- Strong identity and access controls allow for commercial and public sector scalability

Relevance in Cybersecurity Systems Engineering

Security
- Constant, continuous verification

- Securing UTM systems represents a direct application of security, safety, and resilience principles
- With ZTA, these principles are applied with the "never trust, always verify" methodology

Safety
- Securing UAVs against hijacking



Resilience
- Proactive security mechanisms, like Microsegmentation

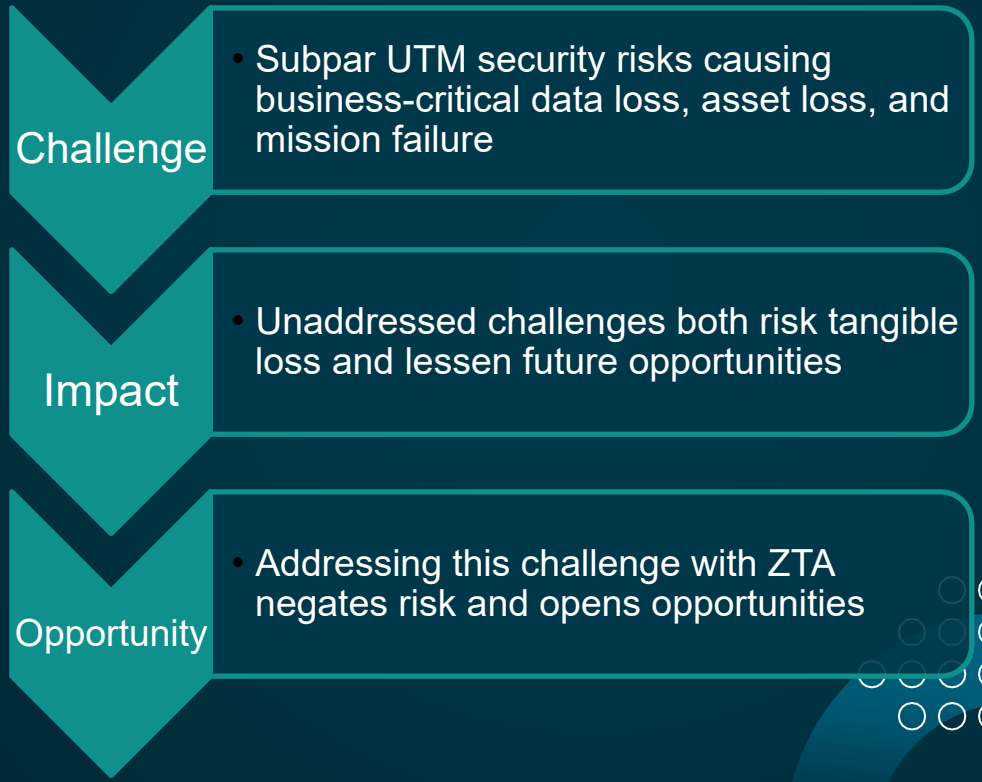
Challenges in Unmanned Traffic Management (UTM)

Risks of subpar UTM security:

Critical data loss	Asset loss	Mission failure	Reputational damage

With ZTA-based security, we can mitigate these risks, allowing for safe UAV adoption at scale

Challenges in Unmanned Traffic Management (UTM)



Background & Gaps

1	Static Credentials	1	Real Time Credentialing
2	No Continuous Verification	2	Continuous Trust Engine
3	Weak Telemetry	3	Secure Telemetry Pipelines
4	Long Lived Sessions	4	Limited Session Engine
5	No Tamper Evident Logs	5	Immutable Audit Logging

Primary Threats

Command Spoofing

Impersonating operators, UAVs, and USS entities

Data Manipulation

Altering GPS, telemetry, and flight-plans in transit

Information Disclosure

Intercepting credentials, routes, telemetry or mission data

Denial of Service (DoS)

Flooding UTM/USS servers with requests to weaken availability

Privilege Escalation

Gaining elevated permissions to alter missions or access restricted systems & information

Repudiation

Preventing accountability when performing malicious changes

Attack Surfaces

Authentication Points

- Spoofed entities (fake UAV/USS/ATC)
- Stolen operator credentials
- Weak or long-lived session keys

Data Exchange Channels

- Manipulation of telemetry & GPS
- Injection of false flight plans
- Interception of confidential mission data
- Poorly encrypted communication links

Database & Core Systems

- Weak access controls over flight and mission data
- Data tampering: paths, operator identities, and authorization rules

System Performance

- DoS flooding of USS/UTM services
- Overloaded servers → missed updates → flight disruption

UTM Modules At Risk

Access Control Services:

Risks: Spoofing, credential theft, and privilege escalation

Consequences: Unauthorized entities gain system access and break trust across the entire network

Flight Planning Module:

Risks: Route modification and false authorization changes

Consequences: UAVs can be rerouted, misaligned, or placed into collision paths

Data Exchange Module (UAV ↔ USS ↔ ATC):

Risks: Interception, manipulation, and injection of mission-critical data

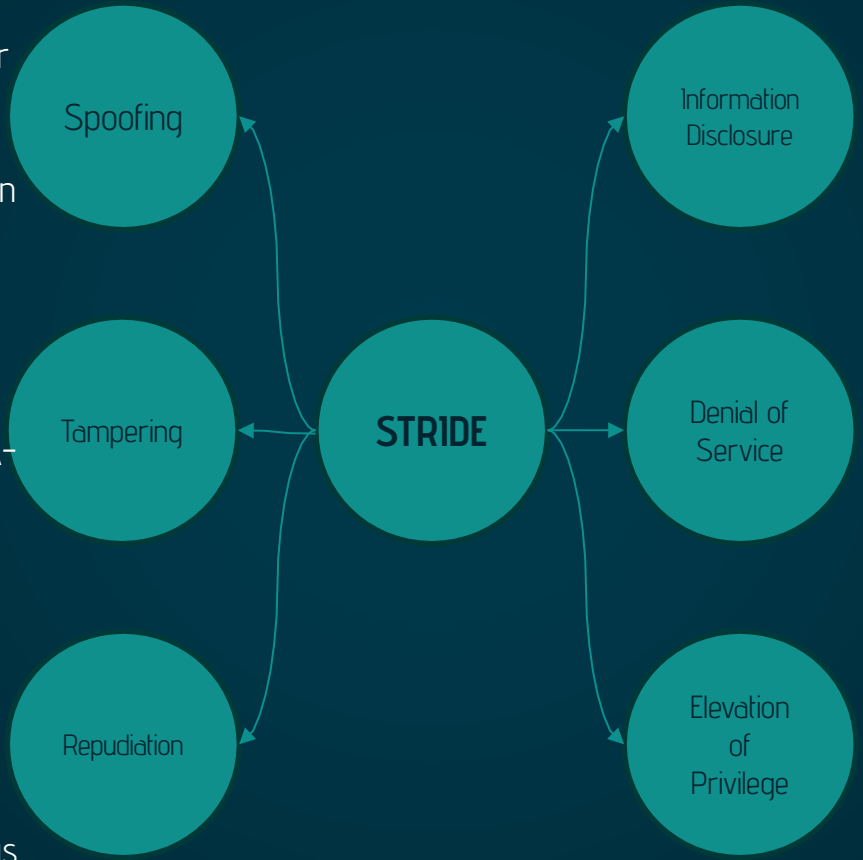
Consequences: Compromised telemetry and commands disrupt operations and expose sensitive mission data

Flight Operations & Navigation Systems:

Risks: GPS/telemetry spoofing and altered navigation data

Consequences: UAV behavior becomes unreliable, unsafe, and potentially mission-terminating

STRIDE Analysis & Mitigations



Risk: Fake UAV/Operator sends false commands
Mitigation: TLS 1.2 + X.509 identity verification

Risk: Flight plan/GPS data altered
Mitigation: HMAC + SHA-256 + AES-256 protection

Risk: Attackers deny malicious commands (no logs)
Mitigation: Immutable, digitally-signed audit logs

Risk: Credentials, flight plans, telemetry leaked
Mitigation TLS 1.3 in transit + AES-256 at rest + PKI/ZTA

Risk: Flooded servers → mission disruption
Mitigation: Rate limiting + AI/ML anomaly detection

Risk: Unauthorized access to sensitive systems
Mitigation: ZTA + short-lived JWT tokens

LINDDUN Analysis & Mitigations

LINDDUN

Linking

Threat: Operator and Flight activity linkability
Mitigation: Rotate identifiers & restrict service access

Non-Compliance

Threat: Failure to notify breach
Mitigation: Audits and documentation

Identifying

Threat: Operator Identification through Metadata

Mitigation: Pseudonymize identifiers and encrypt all data

Non- Repudiation

Threat: Untraceable changes to U- Plans

Mitigation: Digital signatures and tamper-evident logs

Detecting

Threat: Takeoff detection via RF

Mitigation: Encrypt telemetry & limit metadata

Data Disclosure

Threat: Unauthorized flight plan access

Mitigation: Secure coding, strong encryption & strict access controls.

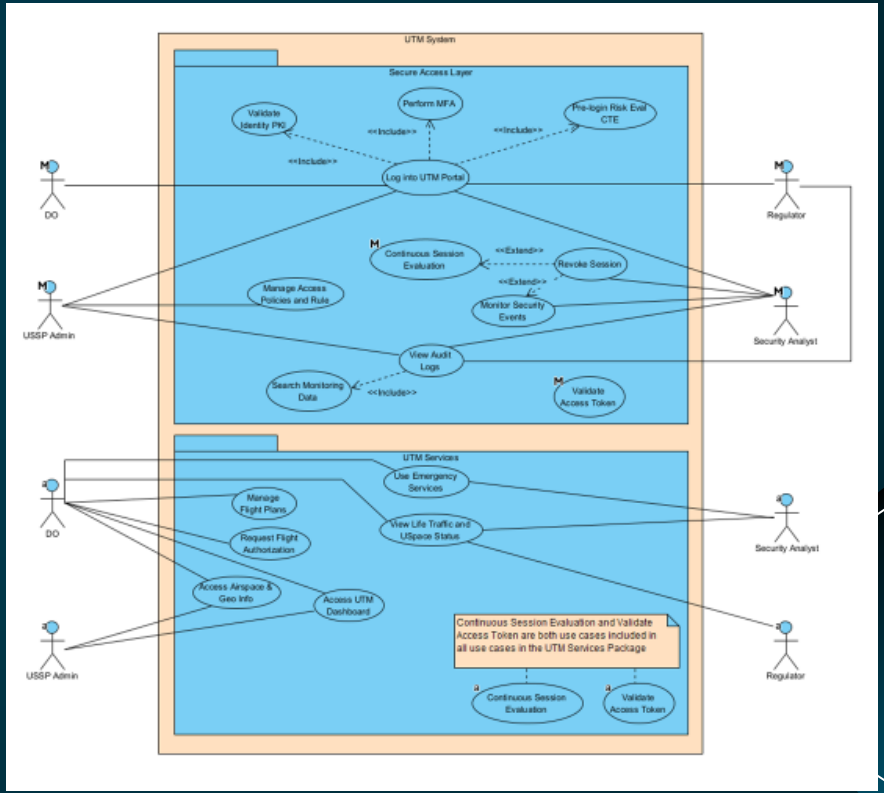
Unawareness

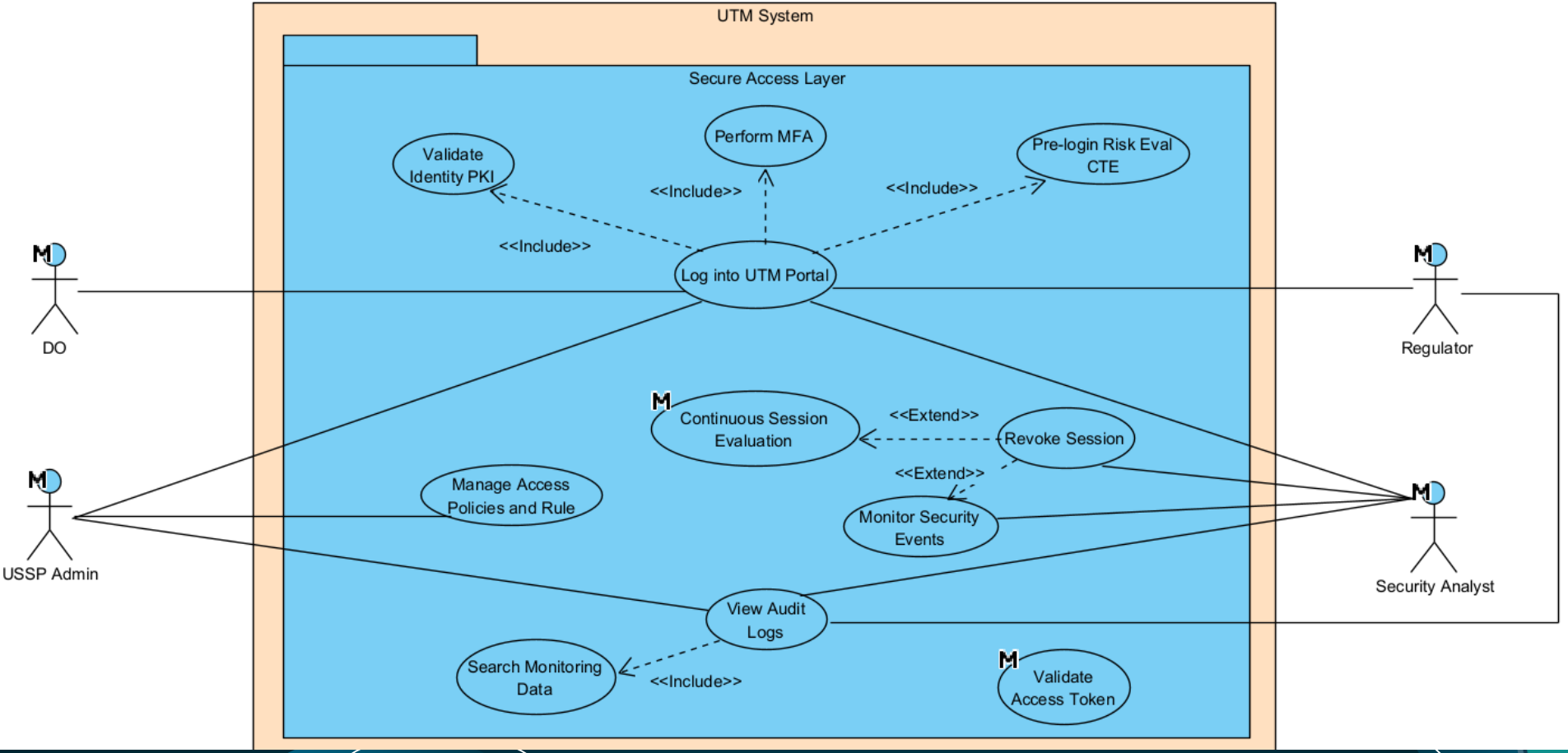
Threat: Operator Data Use Uncertainty

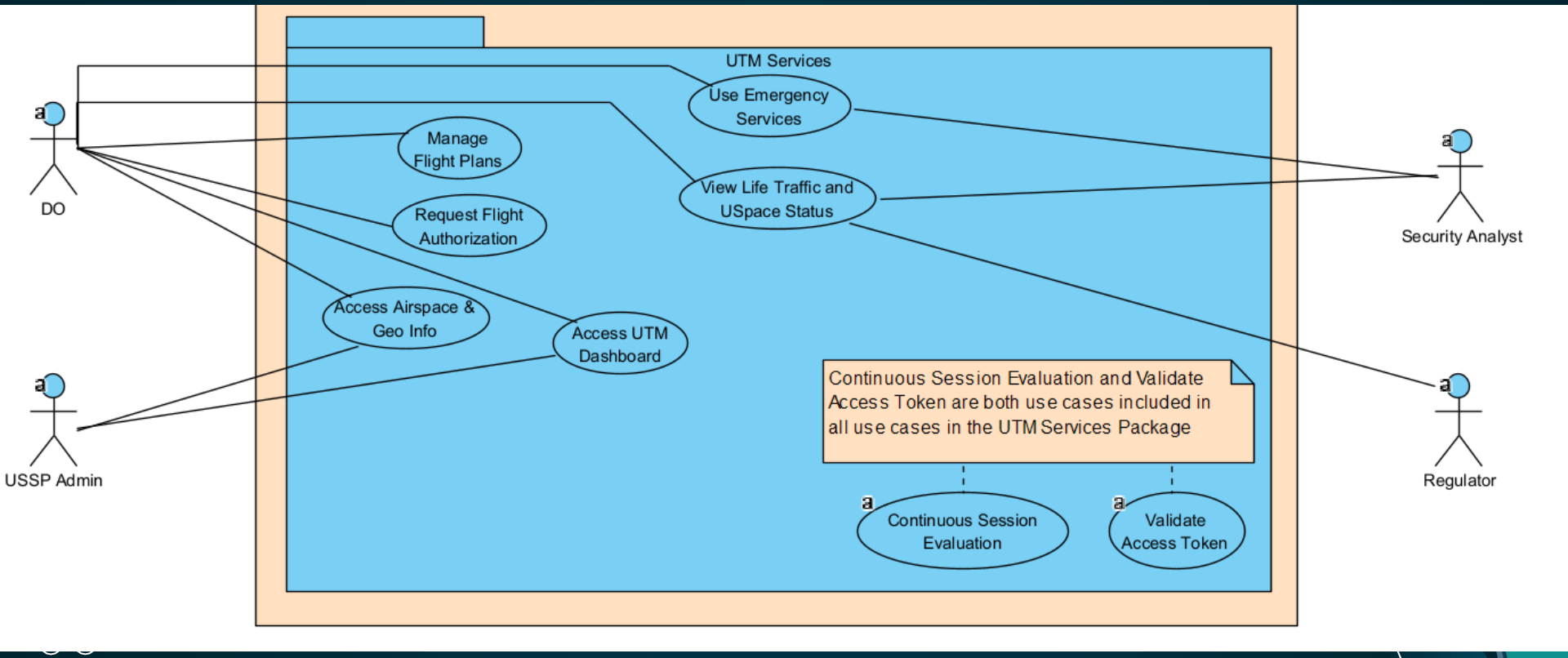
Mitigation: Clear notices and consent control for users

System Solution Architecture Diagram

- Identity and Access Management
- Multi-Factor Authentication
- Short lived tokens
- Least Privilege Enforcement
- Continuous Trust Engine
- Real-Time Session Evaluation
- Audit logging and Compliance




UTM System
Secure Access Layer
Validate Identity PKI
Perform MFA
Pre-login Risk Eval CTE
<<Include>>
<<Include>>
<<Include>>
Log into UTM Portal
DO
Regulator
Continuous Session Evaluation
<<Extend>>
Revoke Session
<<Extend>>
Manage Access Policies and Rule
Monitor Security Events
USSP Admin
Security Analyst
View Audit Logs
Search Monitoring Data
<<Include>>
Validate Access Token


UTM Services
Use Emergency Services
Manage Flight Plans
View Life Traffic and USpace Status
Request Flight Authorization
Access Airspace & Geo Info
Access UTM Dashboard
DO
USSP Admin
Security Analyst
Regulator
Continuous Session Evaluation and Validate Access Token are both use cases included in all use cases in the UTM Services Package
Continuous Session Evaluation
Validate Access Token

Solution Implementation

- **Applied security/privacy principles**
  - Continuous authentication & adaptive authorization
  - Least privilege enforcement across UTM functional blocks
  - Micro-segmentation of UTM services
  - End-to-end encryption & secure session lifecycle
  - Privacy-by-design: data minimization & purpose limitation

- **Technical rigor with stakeholder value (who benefits, why would they adopt)**
  - Operators: safer mission execution, fewer disruptions
  - UTM Administrators: reduced insider/credential-reuse risk
  - Regulators: improved compliance with aviation cybersecurity mandates

Entrepreneurial Value and Validation Plan

- **Entrepreneurial Value**
  - UAV operators and providers get non-disruptive security.
  - Aviation regulators and authorities gain proactive, auditable visibility.
  - Market growth builds public trust.
- **Validation Plan**
  - A Security simulation which is quantitative technical proof
    - Unauthorized Access Denial Rate (UADR)
    - Mean Containment Time (MCT)
  - High fidelity mockup which is a visual proof of value
    - UTM Administrator Dashboard
    - Demo scenario
    - Confirms ZTA is easy to adopt and operationally superior

Demo and Technical Feasibility

Demo and Technical Feasibility

https://drive.google.com/file/d/1tgHE5r_kc1uOPfkPo2HTxmcWptcXySVQ/view

Conclusion

- Introduced a Zero-Trust architecture that eliminates the #1 barrier to UAV scaling: insecure UTM access
- Positioned UTM security as not just protection—but an enabler of commercial UAV growth
- Continuous verification and secure telemetry are non-negotiable for safe national-scale UAV operations
- Regulators, operators, and service providers all want the same thing: trustable autonomy at scale
- Expand the solution across multi-operator and multi-agency UTM networks
- Build a deployable prototype to validate performance, user experience, and regulatory fit

References

iStockphoto. *Drone icon. iStock.* https://www.istockphoto.com/vector/drone-icon-copter-quadcopter-with-action-camera-gm1453962362-489751086.

iStockphoto. (2024). *Zero trust security with identity and data saefty protection outline diagram.* iStock. https://www.istockphoto.com/vector/zero-trust-security-with-identity-and-data-safety-protection-outline-diagram-gm2081067355-565213804.

PNGTree. (2019). *Shield safe line icon vector.* PNGTree. https://pngtree.com/freepng/shield-safe-line-icon-vector_5175136.html.

Shutterstock. *Drone tracking black line icon.* Shutterstock. https://www.shutterstock.com/image-vector/drone-tracking-black-line-icon-gps-1610580421?dd_referrer=https%3A%2F%2Fwww.google.com%2F.

Vecteezy, Data exchange line icon. Vecteezy. https://www.vecteezy.com/vector-art/14812568-data-exchange-line-icon.

Thank You!

Questions?