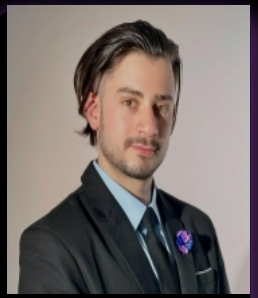
Zero-Trust Architecture for securing UAV systems

THE TEAM



Yazan Barmil

Team Lead/
Grad Student

Fatima Majid

Grad Student

Mohamed Cheikh Abdallahi

Grad Student

Huy Than

Grad Student

Karthik Calanji Sridhar

Grad Student

Pablo Sejas

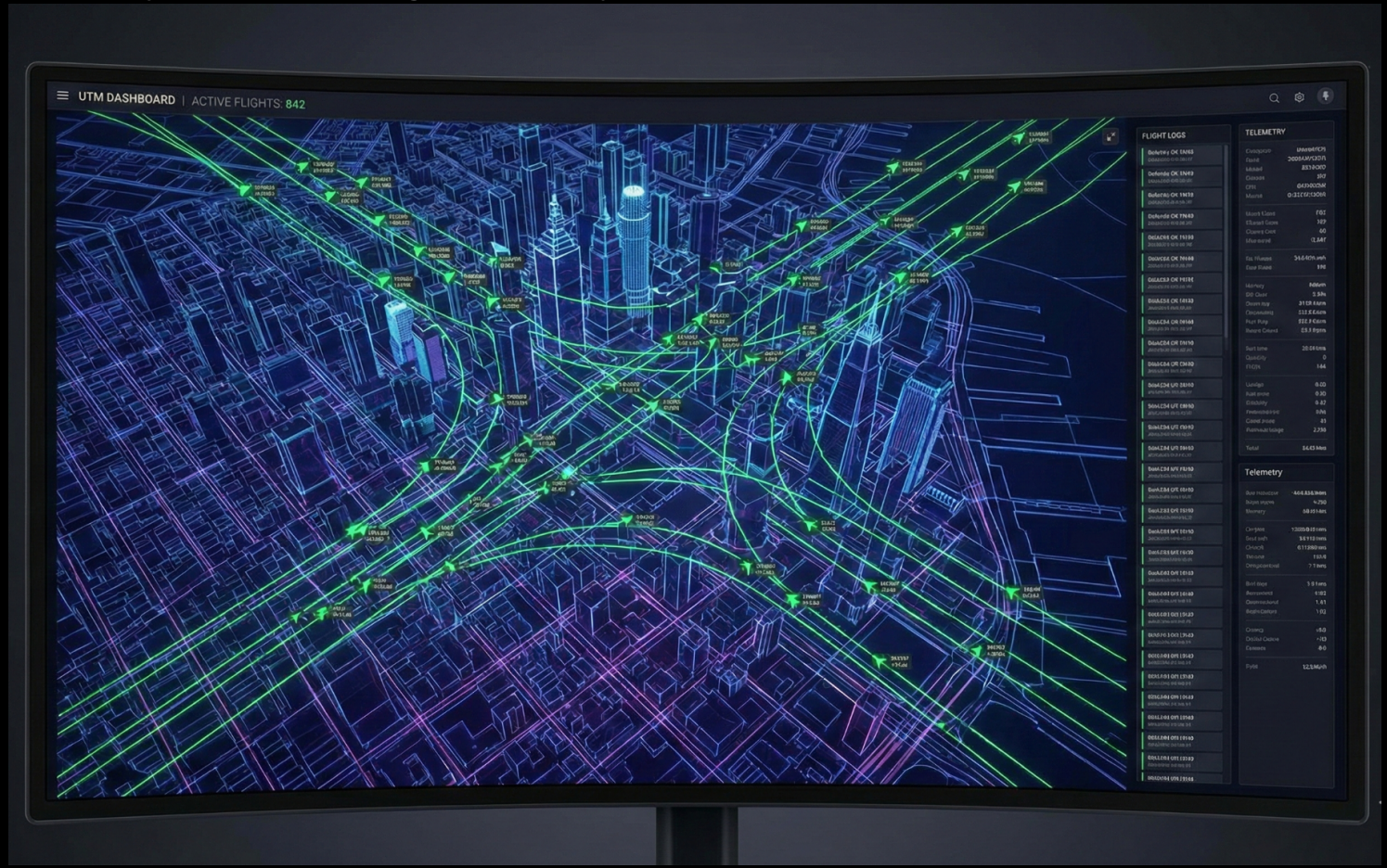
Grad Student

Edward Hickey

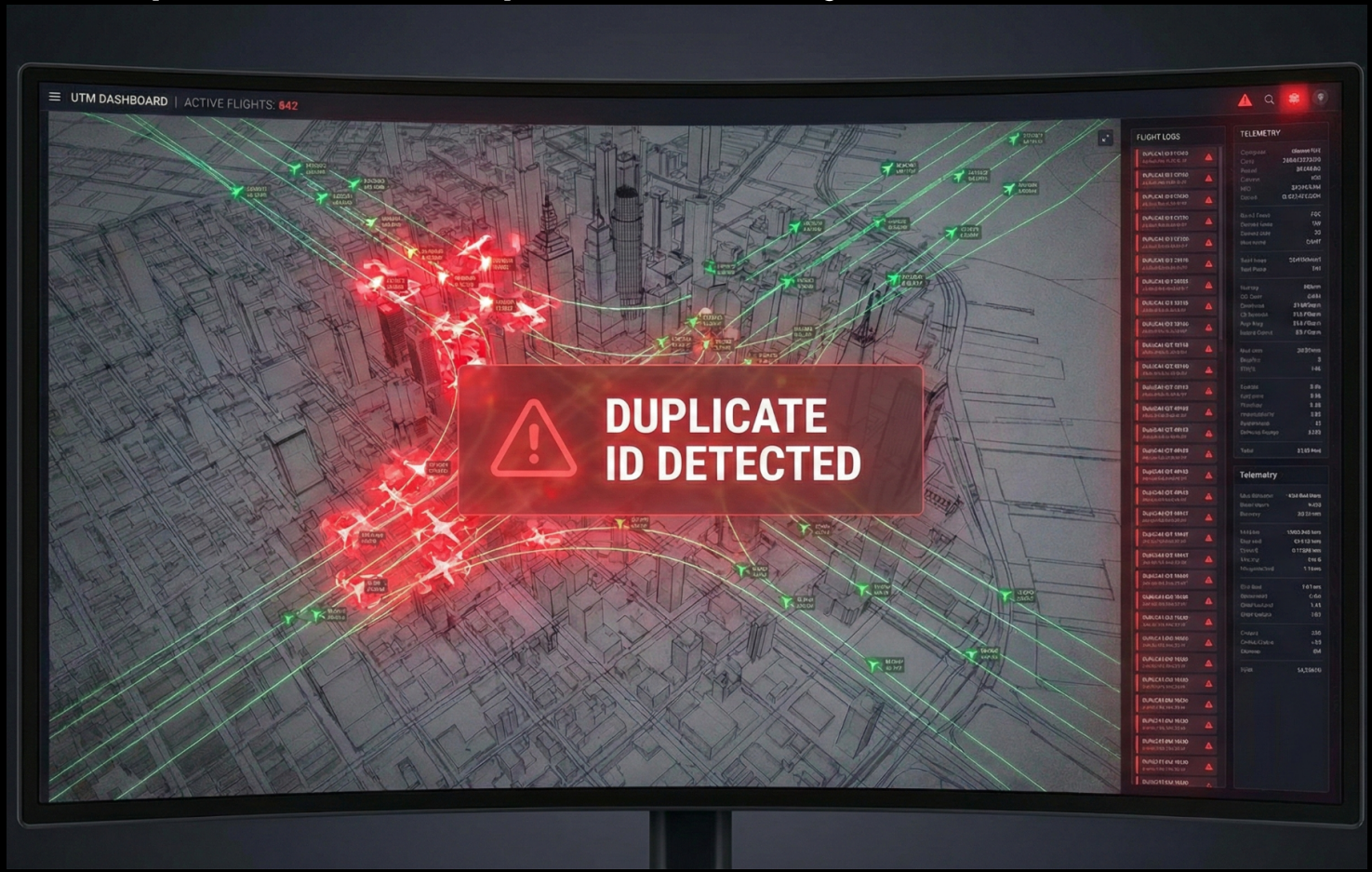
Grad Student

Problem and Motivation

The Opportunity: Secure, High Density UTM Infrastructure



The Problem: Implicit Trust and Operational Paralysis



The Motivation: Stakeholder Impact and Strategic Risks

The Public

REPUTATIONAL DAMAGE

Increased scrutiny of safety and damage to brand image

Regulators

REVOCATION THREAT

Loss of BVLOS Waiver or Operating Authority

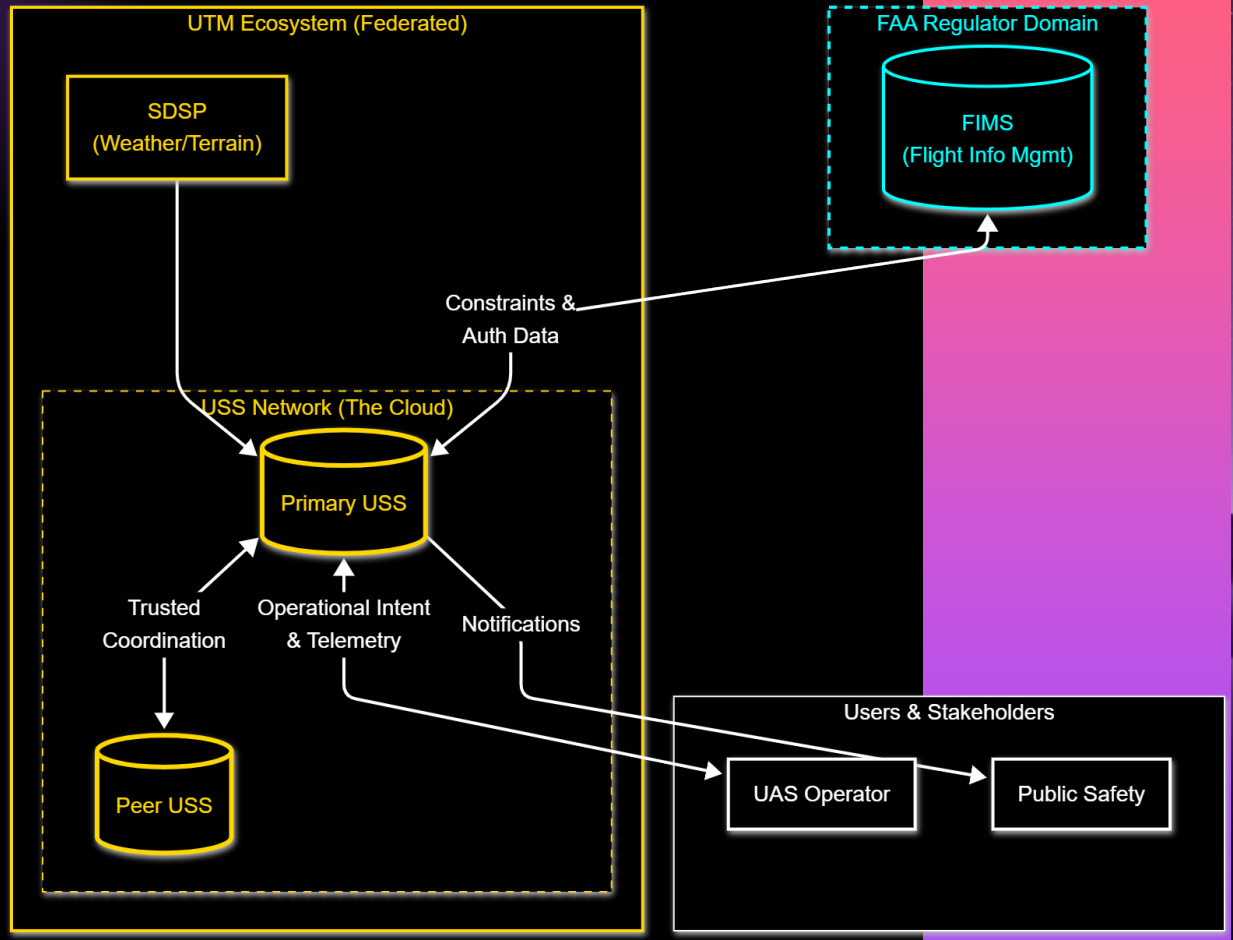
The Business

LOSS OF REVENUE AND LIABILITY EXPOSURE

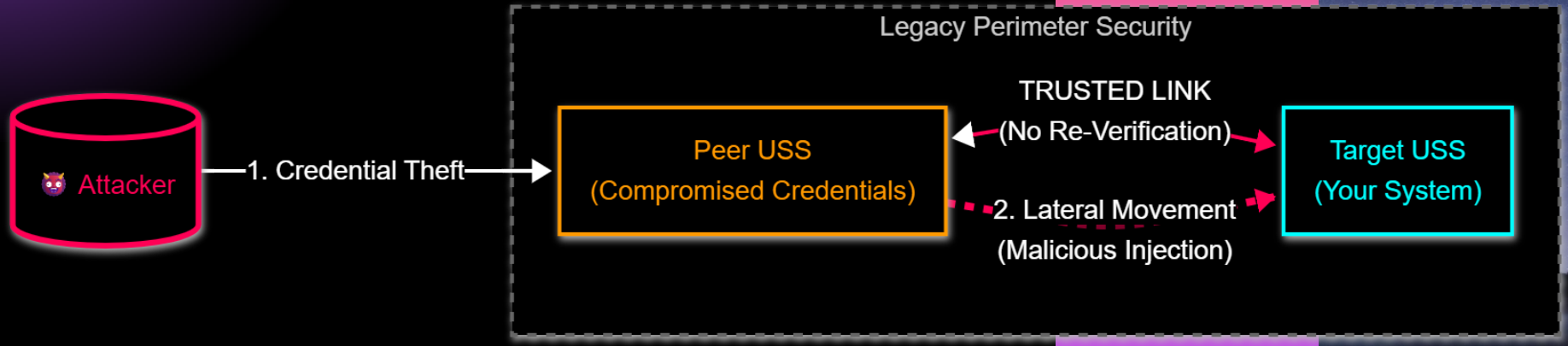
Loss of revenue due to lost operating time and performance penalties

Background and Gaps

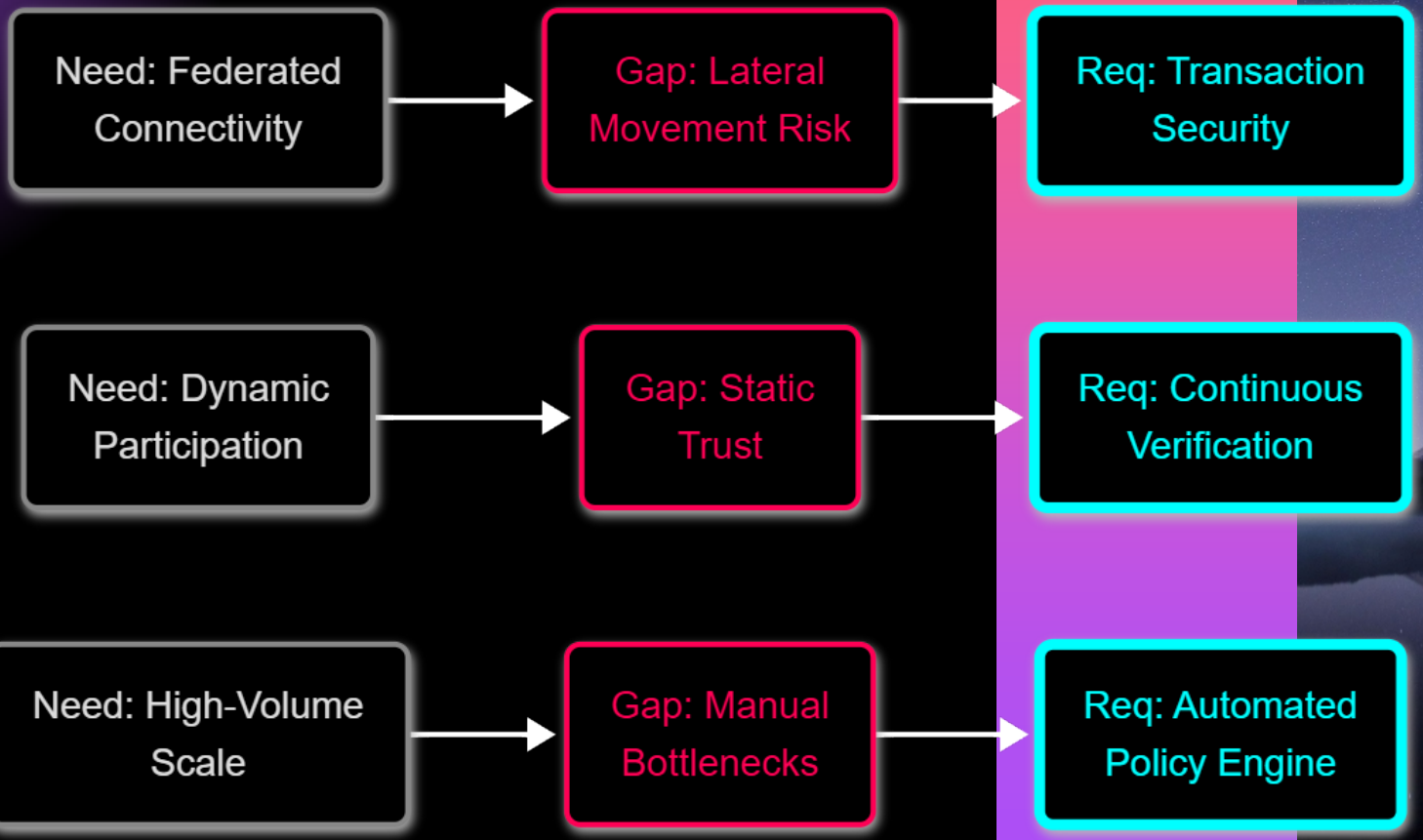
Context: The Federated Architecture of FAA UTM ConOps



The Technical Gap: Static Trust Failure



Systems Engineering Approach: High Level Requirements



Threat Analysis & Requirements

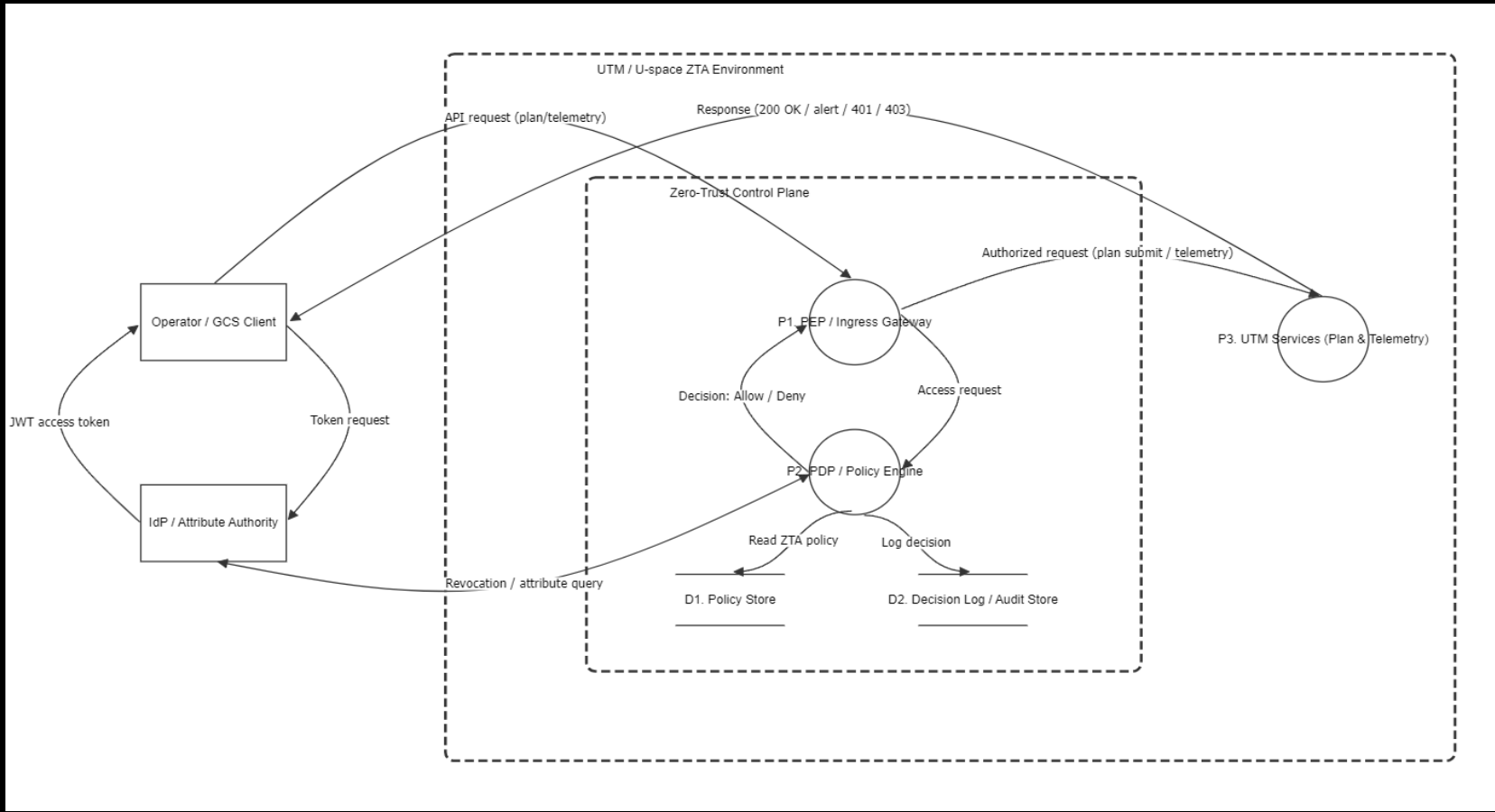
Topics in this section:

Zero Trust Data Flow Diagram DFD

STRIDE Threat Analysis

LINDDUN Privacy Risk and Mitigations

ZTA Data Flow Diagram in the UTM/ U-Space Environment



Threat Analysis & Requirements: STRIDE

STRIDE Category	Cause	Action	Impact	Asset
Spoofing (Token Replay)	Stolen JWT captured on network or device	Attacker replays mission-submit	Unauthorized mission accepted	PEP, Token Service
Tampering (Telemetry)	Attacker modifies telemetry packets	Sends false location/velocity	Incorrect conformance decision	Telemetry Pipeline
Repudiation	Operator denies submitting U-plan	Claims no mission change/modification	Loss of accountability	Mission Repository, Audit Logs
Information Disclosure	Weak access policy or leaked credentials	Reads sensitive flight plans	Privacy & safety risk	Mission Repository
Denial of Service	Attacker floods API Gateway	Overloads mission/telemetry endpoints	Mission delays & safety risk	API Gateway (PEP)

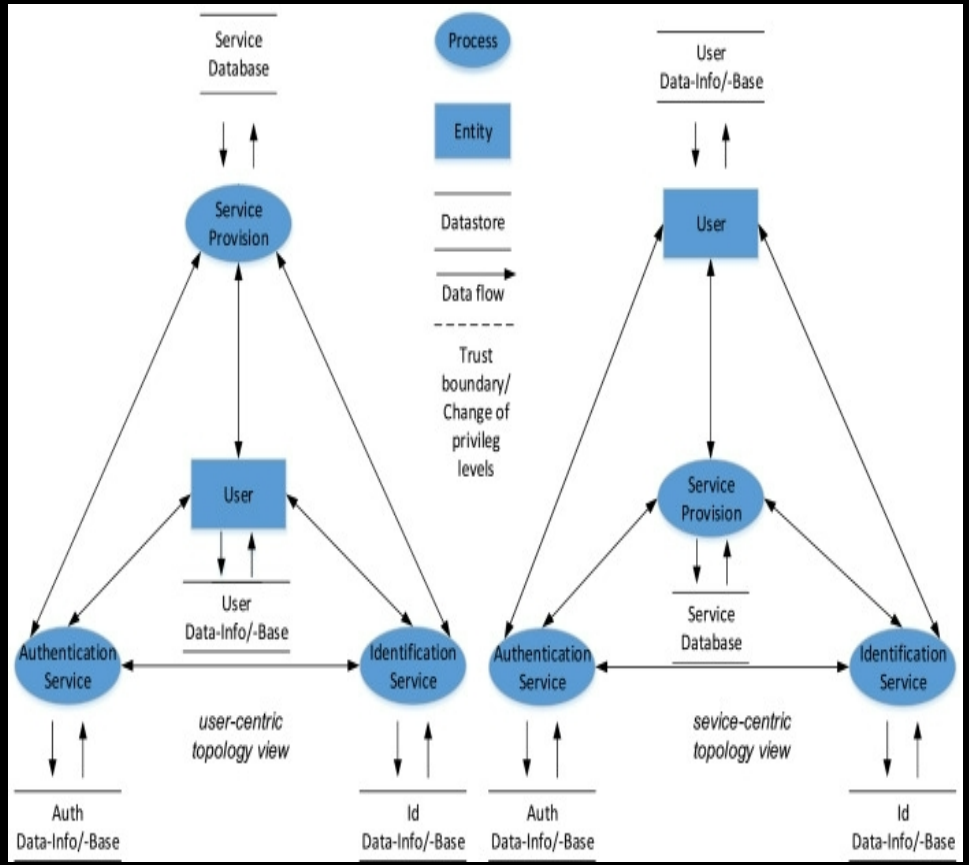
LINDDUN highlights with mitigations

Privacy Risks

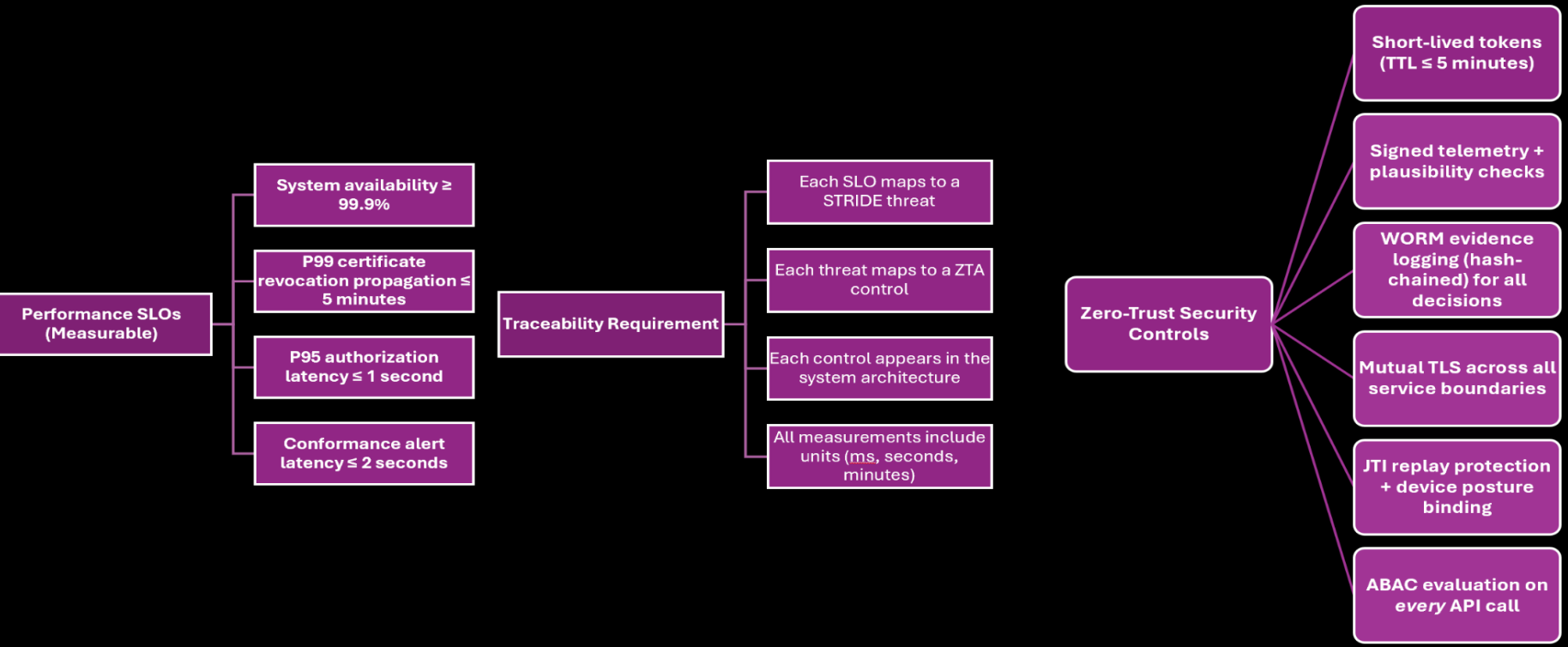
- Remote ID exposure: Enables tracking of operators, aircraft behavior patterns, or sensitive operations.
- Mission data leakage: Reveals flight paths, surveillance targets, critical infrastructure locations, or operational routines.

Mitigations

- **Ephemeral / rotating Remote ID identifiers** to prevent long term tracking.
- **End to end encrypted telemetry and mission messages** across operator ↔ GCS ↔ USSP.
- **Access controlled mission logs** with strict role-based permissions.
- **Data minimization:** Store only what is required for compliance and safety.
- **Protected post-flight records** using signed, tamper evident storage.



Formal requirements: SLOs + controls



Proposed Solution and Architecture

Topics in this section:

Our Solution

Why ZTA

Entrepreneurial value and who benefits?

SO, WHAT IS THE SOLUTION?

Integrating **Zero-Trust Architecture** in Unmanned Traffic Management environments

ZTA overview: “Never trust, always verify”, eliminating implicit trust and enforcing continuous authentication/authorization

Components: Core NIST components are:

- Policy Decision Point (PDP)
- Policy Information Points (PIP)
- Policy Enforcement Point (PEP)

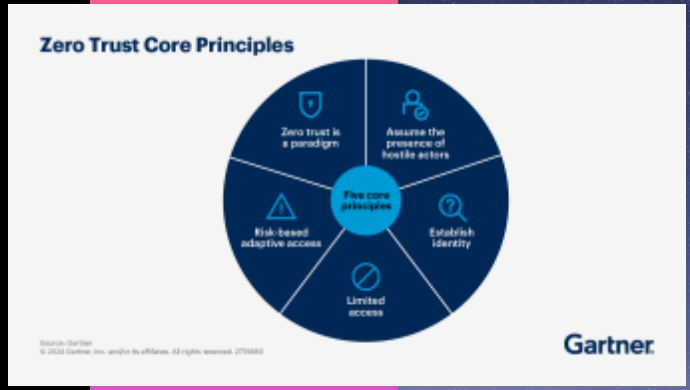
With supporting elements such as:

- Identity Access Management (IAM)
- Network micro-segmentation
- Encryption

Why **Zero Trust Architecture (ZTA)** is a **MUST !**

ZTA Solves UTM Security Gaps

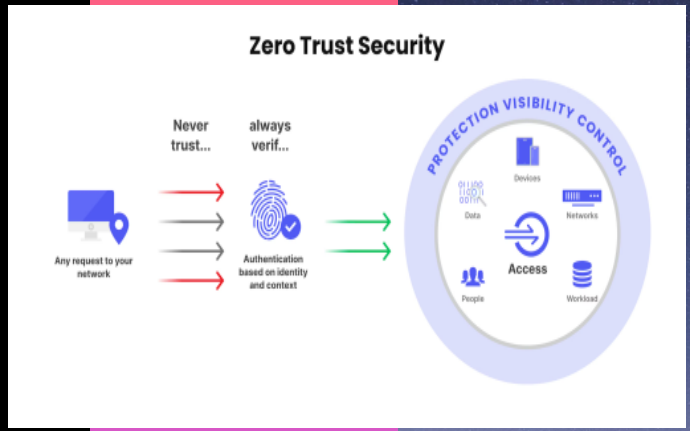
- **Continuous authorization** via PEP + PDP architecture prevents replay and spoofing.
- Device posture, mission context, and identity claims are verified on **every** transaction.
- Short-lived tokens and rapid revocation (≤5 minutes) **block** compromised credentials quickly.



Entrepreneurial Value

Operational Benefits & Entrepreneurial Value

- Prevents unauthorized flights and airspace violations.
- Enables real-time conformance monitoring and rapid threat containment.
- Preserves safety, public trust, and regulatory compliance through measurable Service Level Objectives



Who benefits

Commercial Operators Gain safer operations with reduced risk of mission hijacking, airspace violations, and lost revenue.

Regulators (FAA and national authorities) Receive verifiable compliance, stronger safety oversight, and reduced investigative workload through audit-ready logs.

UTM Service Providers (USSPs) Unlock scalable multi-tenant architectures, premium service offerings, and stronger market differentiation.

Public & Critical Infrastructure Stakeholders Benefit from safer skies, reduced chance of malicious drone misuse, and increased trust in unmanned systems.

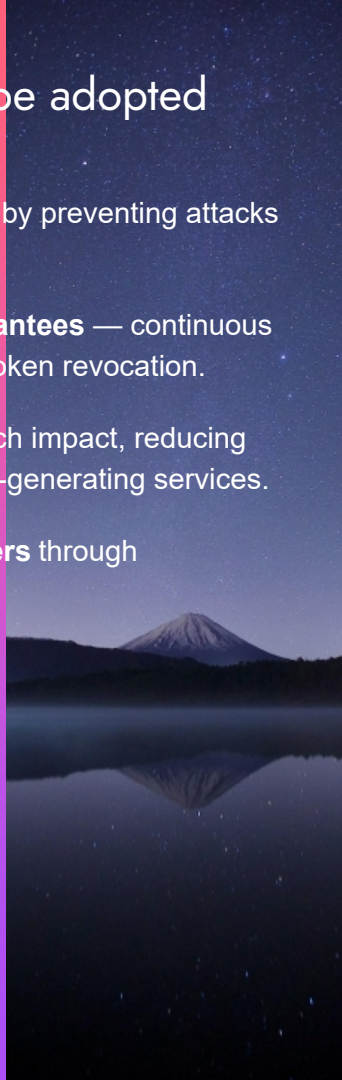
Why this solution should be adopted

Reduces operational and regulatory risk by preventing attacks that can ground fleets and revoke waivers.

Demonstrates measurable security guarantees — continuous authorization, geofence enforcement, and token revocation.

Creates economic value by lowering breach impact, reducing insurance costs, and enabling new revenue-generating services.

Builds trust with regulators and customers through transparent, auditable, Zero-Trust controls.



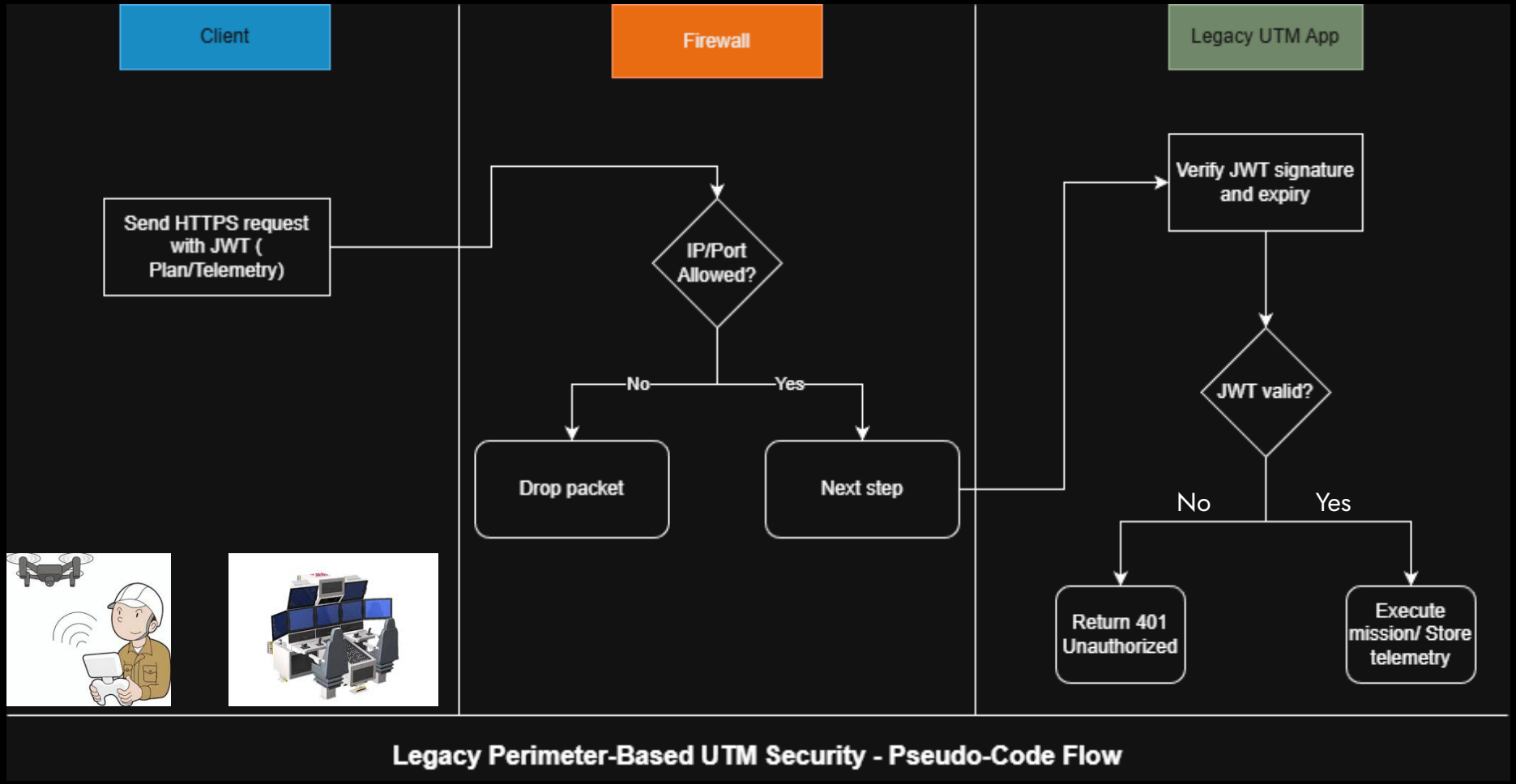
Implementation & Demo – How our ZTA actually works

Topics in this section:

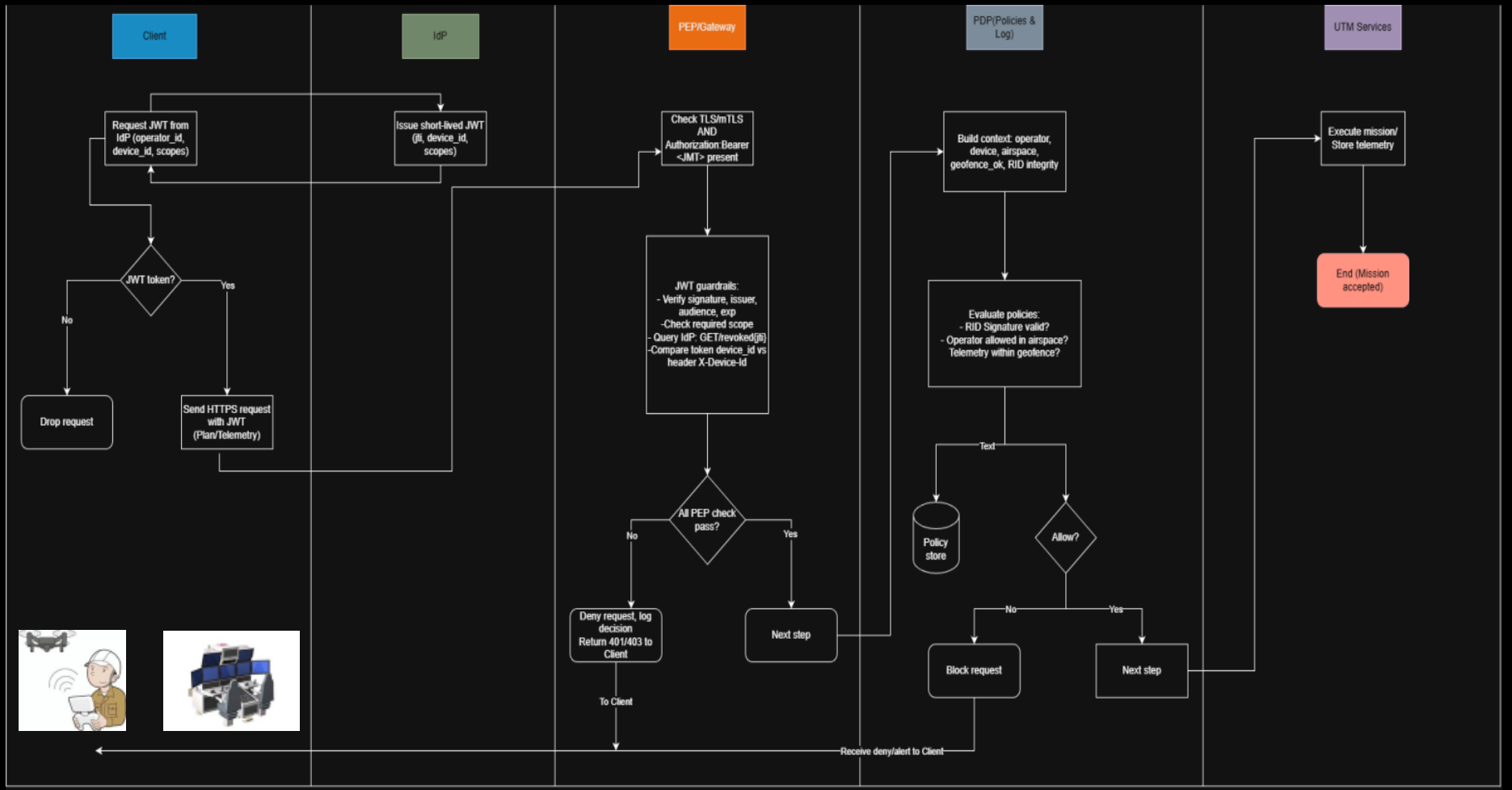
Legacy perimeter flow vs. Zero-Trust gateway

Demonstration of 2 Unmanned Traffic Management attack scenarios, and how they’re handled by the legacy vs ZTA systems

What this means for operators, regulators, and the public

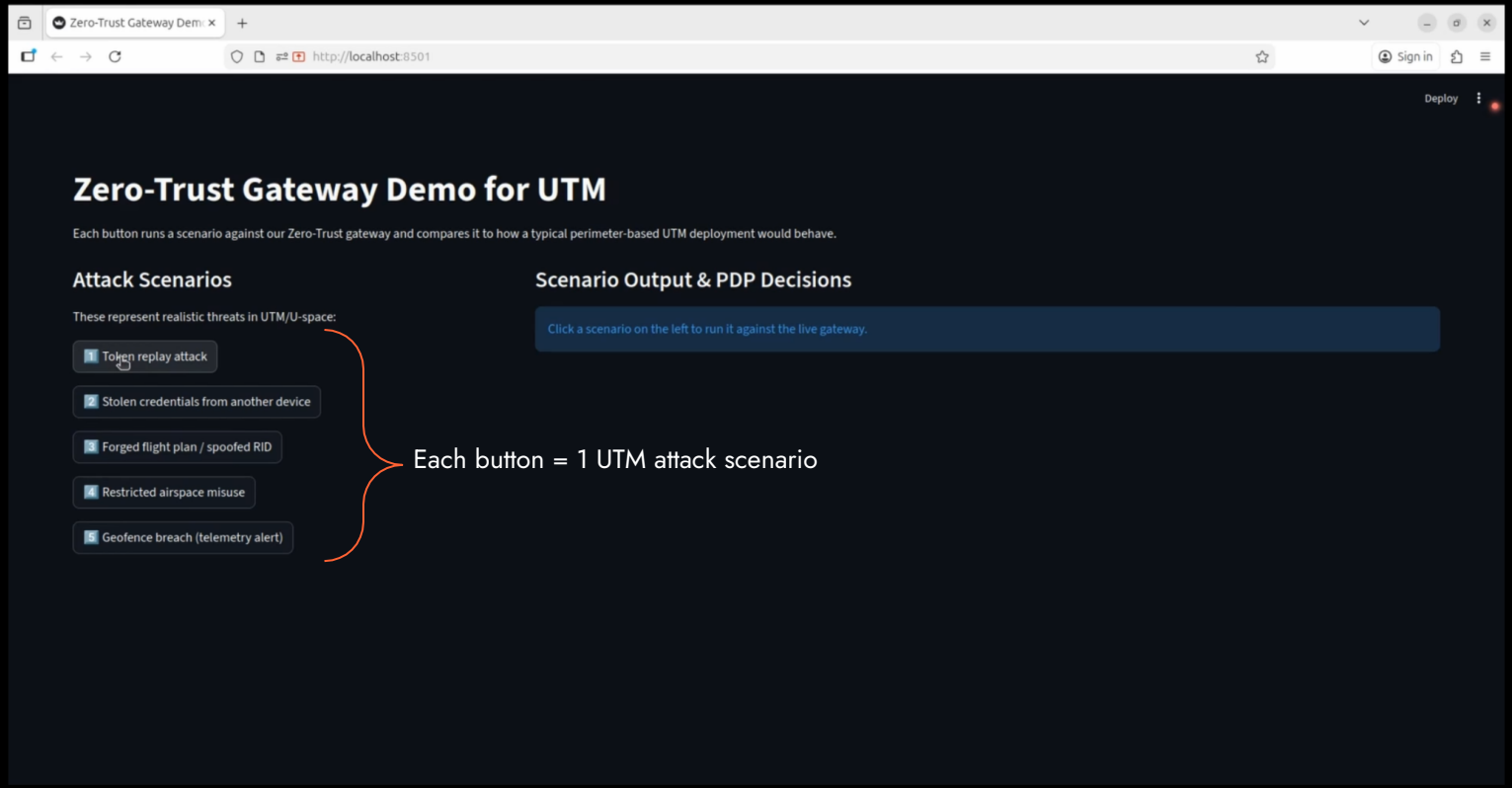


Legacy Perimeter-Based UTM Security - Pseudo-Code Flow



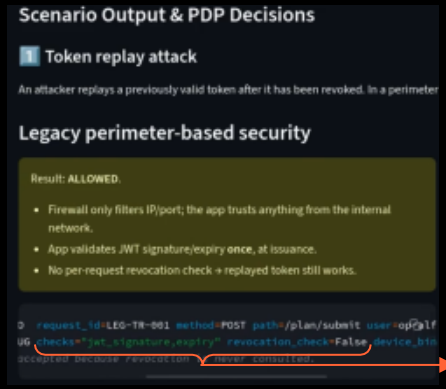
Zero-Trust UTM Security (PEP/PDP) - Pseudo-Code Flow

Live Demo – Legacy vs ZTA Gateway



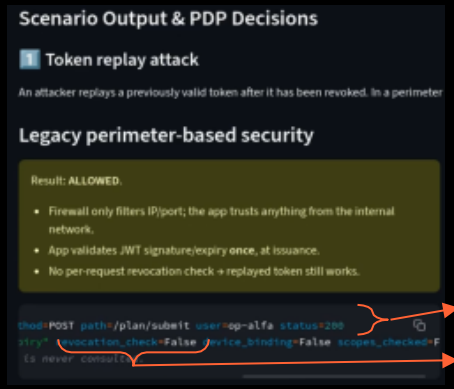
Token replay attack

(credential abuse / revocation)



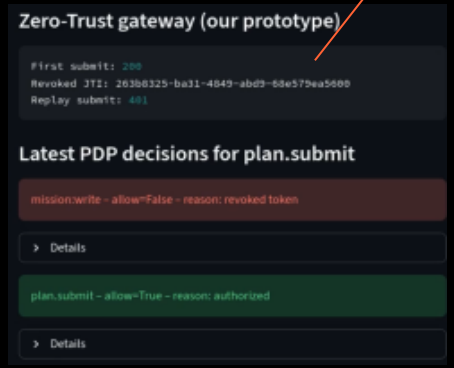
Legacy checks: jwt_signature, expiry

Missing: revocation_check → token status is never consulted per request.



Replay request log: status=200 on /plan/submit

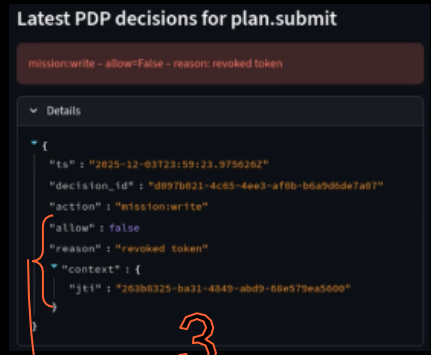
Never consults revocation: *revocation_check=False*. Replayed token still treated as fully valid.



2

Zero-Trust gateway behaviour over time":

- First submit: 200 OK (valid mission)
- Replay submit: 401 Unauthorized (same token after revocation is blocked)

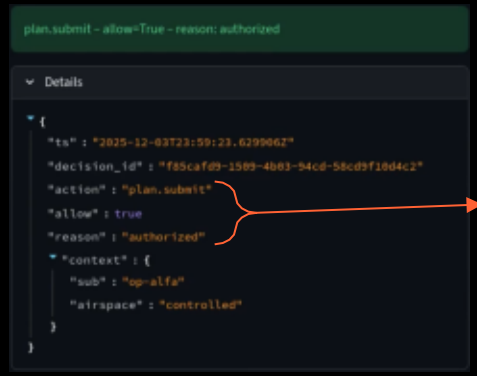


3

Replay blocked by Zero-Trust gateway:

PDP decision:
- allow: false
-reason: "revoked token"
-context.jti=<id>

Replay fails because this token ID is now on the **revocation list**

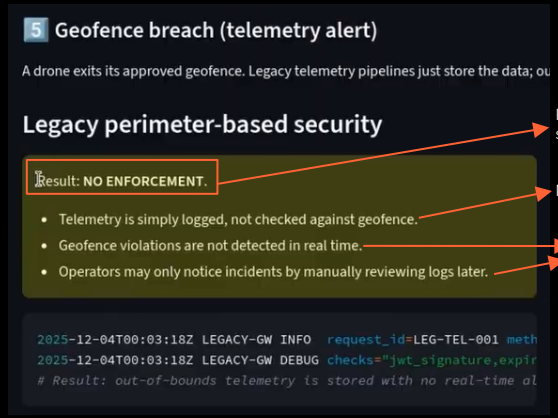


1

Legitimate mission
PDP decision *allow: true, reason: "authorized"* – the operator's original flight plan is accepted.

Telemetry geofence breach

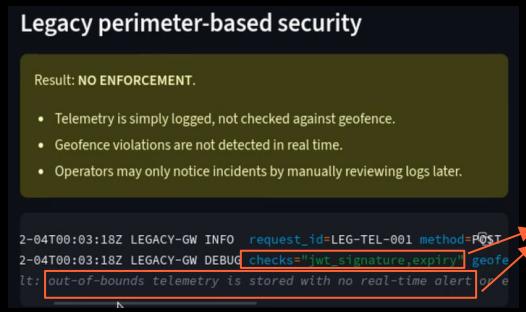
(real-time safety monitoring)



Result: no real-time enforcement – telemetry is just stored.

No geofence check → data in, no decision.

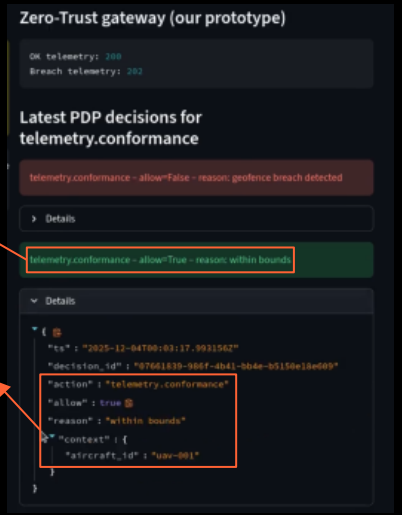
Violations only visible after the fact



Gateway only checks JWT; no telemetry.conformance policy evaluated.

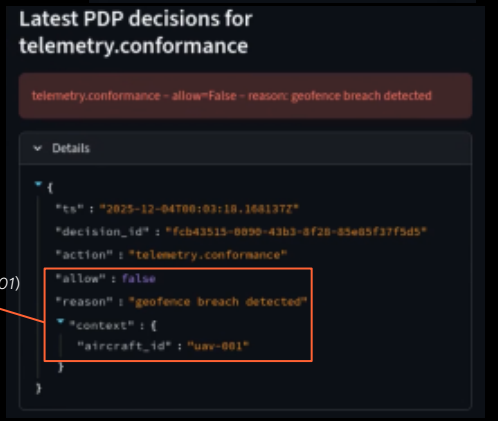
The system sees the data, but never asks *"Is this inside the geofence?"*

PDP decision = allow;
reason: drone is within bounds.



Structured log:
action = telemetry.conformance, allow=true, reason='within bounds', tied to *aircraft_id="uav-001*

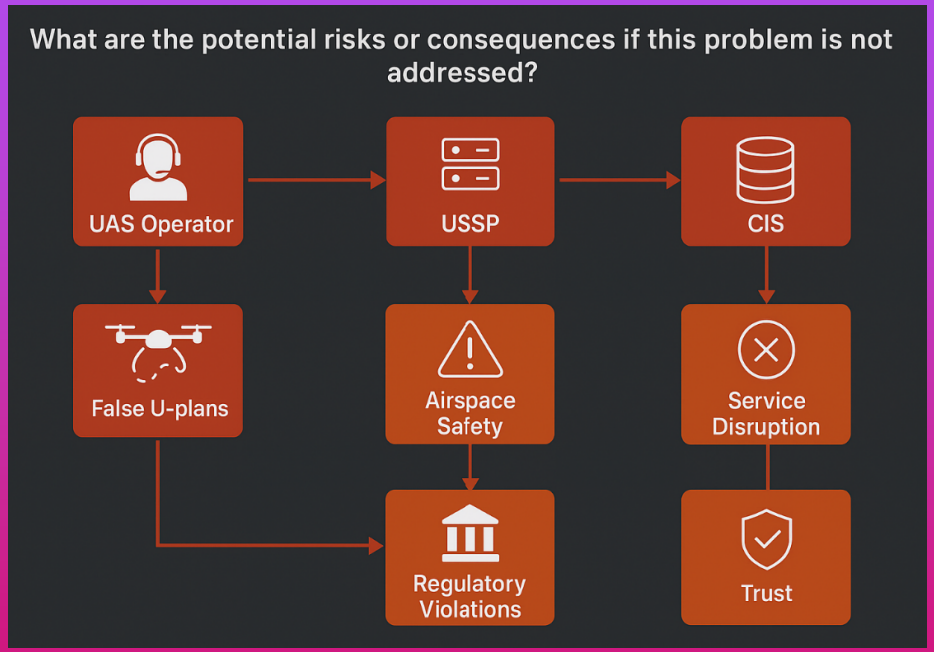
This shows that even the "OK" case is an explicit decision, not just blind logging



Decision log: this specific aircraft (*uav-001*) is out of bounds and flagged.

RISKS, RESULTS & VALIDATION

Risks & Consequences



What are the potential risks or consequences if this problem is not addressed?

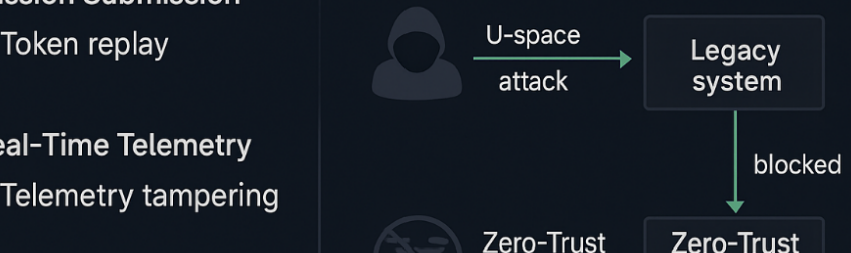
- False U-plans submitted under stolen identities
- Airspace safety hazards & collision risk
- Regulatory violations for operators & USSPs
- Service disruption at CIS
- Loss of trust in U-space operations

Validation Strategy: Use Cases & Experiments

Experimental Results

- 100% of attacks bypassed legacy
- 100% blocked or flagged by Zero Trust
- Measured overhead: +35–50 ms per request

- **Mission Submission**
  Token replay
- **Real-Time Telemetry**
  Telemetry tampering
- **Airspace Access**
  Airspace misuse



- 3 real-world UTM use cases tested
- Token replay, telemetry tampering, airspace misuse
- Legacy vs. Zero-Trust comparison

Quantitative & Qualitative Benefits of Zero-Trust Integration

Quantitative Benefits (Measurable Impact)

- 100% of tested attacks blocked
  (token replay, telemetry tampering, airspace misuse)
- < 50 ms policy evaluation overhead
- < 20 ms telemetry validation
- < 1 min token revocation propagation
- 0 false accepts in all experiments
- Reduced U-space workload: fewer alerts sent to human operators

Qualitative Benefits (Operational & Stakeholder Value)

- Higher airspace safety through continuous verification
- Increased regulatory compliance with full audit trails
- Improved operator trust & transparency
- Stronger resilience against identity misuse & insider threats
- Scalable for multi-USSP environments

Conclusion and Future Plan

Topics in this section:

Key takeaways

Lessons learned

Future plan, feedback and final statement

Key Takeaways

U-space/UTM cannot rely on perimeter trust	Five realistic attacks all bypassed legacy controls	Zero-Trust gateway (PEP/PDP) stopped or flagged each one
1	2	3

Lessons Learned

Lesson 01

Continuous verification > one-time authentication

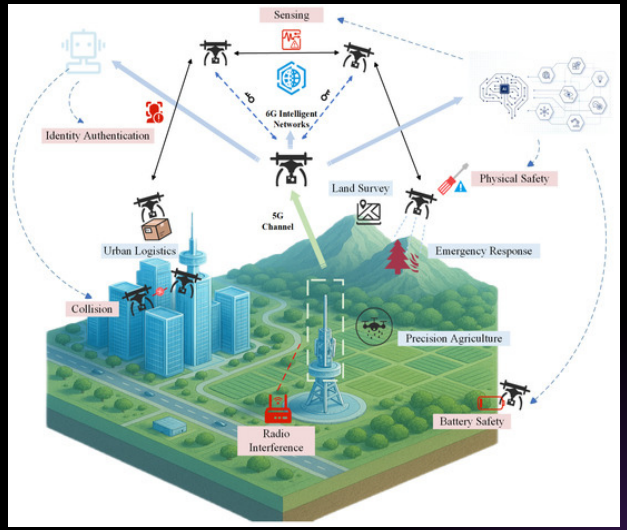
Lesson 02

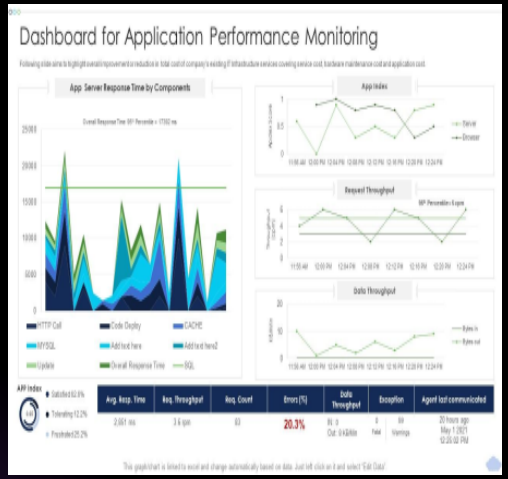
Attribute-based policies match U-space reality

Lesson 03

Logging decisions is critical for audit & incident response

Future Work & Impact





Full UTM stack & standards integration (e.g., CONOPS, RID)

Expand policies (performance, scalability, multi-tenant ops)

Quantitative evaluation
> latency,
> availability
> attack coverage

Feedback/Investor questions

1. Which risks matter most for operational adoption - latency, compliance, or inter-USSP complexity?

1. Which validation scenario would give you the greatest confidence in real-world deployability?

Final Statement

THANK YOU