

UAS Cybersecurity for Utility Applications

Threat Mitigation for Customers and Suppliers

Bri O'Neill



ALTIMETIS

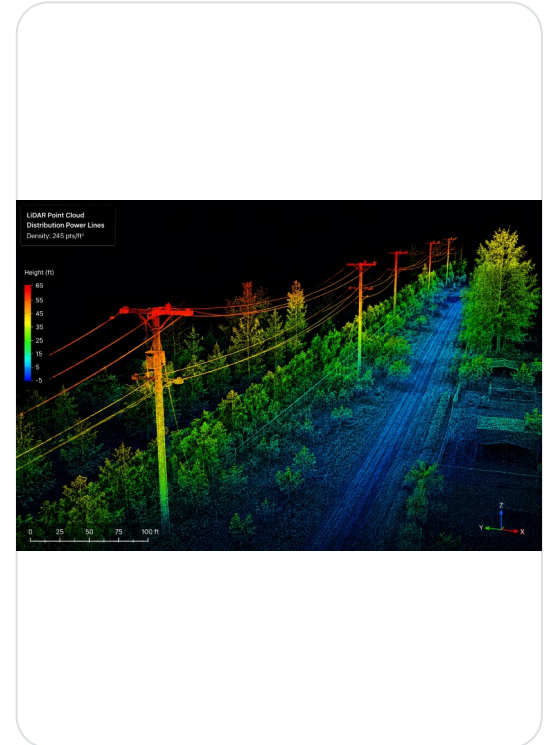
Protect the Payload Data

THREAT SCENARIO

A leaked inspection dataset lets an adversary map substation weak points.

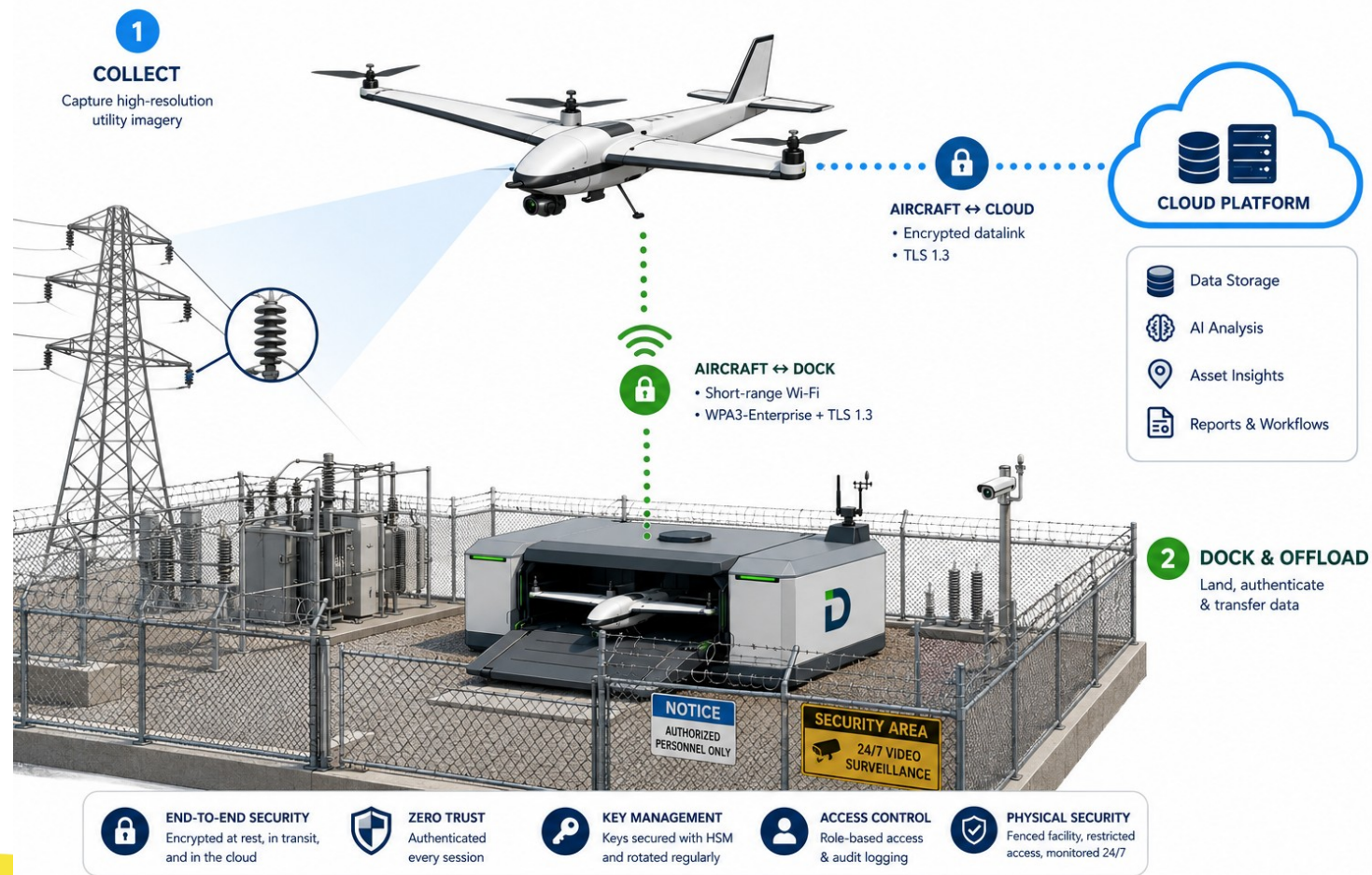
✓ Leaked infrastructure data = a targeting aid

✓ NERC/FERC: seven-figure penalties, per violation, per day



(Source: NERC CIP Compliance Checklist for 2026, ztekcyber.com)

The Data Path, End to End



Step 1: Capture & Onboard Protection

THREAT SCENARIO

An aircraft executes an emergency landing outside of a secured ELZ.



Encrypted at the point of capture, on the aircraft



AES-256 at rest — keys never travel with the data



Lost or captured airframe ≠ compromised dataset



ASK YOUR OEM

What protects data if the aircraft is stolen?

OEM, PROVIDE

Encryption standard, key management, HW security capabilities.

Step 2: Aircraft-to-Dock Offload Link

THREAT SCENARIO

Someone walks up with a tablet and tries to join the dock's wifi network.

✓ WPA3-Enterprise + TLS 1.3, token-based access policy

✓ “Short-range” isn't “trusted” — authenticate every time



ASK YOUR OEM

Is the handoff authenticated, or is any device trusted?

OEM, PROVIDE

The authentication method for the offload link.

Step 3: The Dock-Side Hardware Gateway

THREAT SCENARIO

A known vulnerability in the cellular modem's firmware gives an attacker remote code execution.



WAN devices isolated from LAN behind a hardware gateway



mTLS, short-lived tokens, HSM-backed keys, DMZ for low-trust devices



No standing trust — every session authenticated



ASK YOUR OEM

What stops a compromised WAN device from reaching the payload computer directly?

OEM, PROVIDE

What enforces the WAN/LAN boundary and what's on each side.

Step 4: Physical Security of the Dock

THREAT SCENARIO

Someone in a hi-vis vest walks up to the dock claiming to be on the maintenance schedule.



Crypto is only as strong as the box it's bolted to



Tamper-evident and intrusion-sensing enclosure, access-restricted and video monitoring



Physical breach = trust-loss event



ASK YOUR OEM

What happens if the dock is physically breached?

OEM, PROVIDE

Tamper-response behavior on intrusion.

Key Takeaways

THREAT SCENARIO

A single unchanged default password anywhere in this chain undermines every other control.



Every handoff = a deliberate security boundary



Protect the data like you protect the grid

ASK YOUR OEM

Walk us through this chain for your platform.

OEM, PROVIDE

A one-page architecture map of every boundary.

THANK YOU

Questions?

Bri O'Neill

Bri@Altimetis.com



ALTIMETIS