

Securing the Modern Ground Segment

Cyber risks and mitigations for DIFL-based satellite ground systems
Scott Register | DIFL PlugFest USA 2026 Showcase | October 8, 2026

REPORTED INCIDENT · 2017

The Original Fishing Attack

A connected aquarium system became the entry point to a casino's high-roller database.

Unnamed North American casino; aquarium sensors managed temperature, salinity and feeding

About 10 GB sent to a rare external host

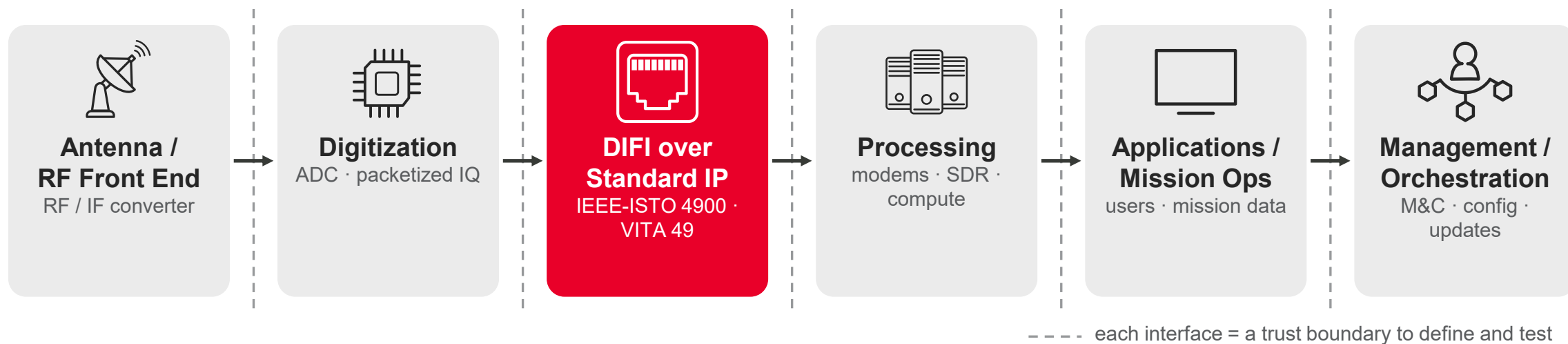
Spotted as anomalous network behavior

The lesson isn't about fish.
It's about attack surface.



DIFI Changes More Than the Interface

Digitization and IP transport add flexibility — and new trust relationships to manage



Multi-vendor by design

Independent implementations of one standard can behave differently at the edges — test behavior, not just exchange.

Every interface is a trust boundary to define — and a behavior to test.

DIFI inherits the flexibility of IP — along with IP-network security challenges.

In a Contested Environment, Cyber Becomes Mission Risk

Three operational properties the ground segment has to protect



INTEGRITY

Is the signal I am receiving the signal that was sent? Has telemetry, command, or data been modified in transit or at a processing node?



AVAILABILITY

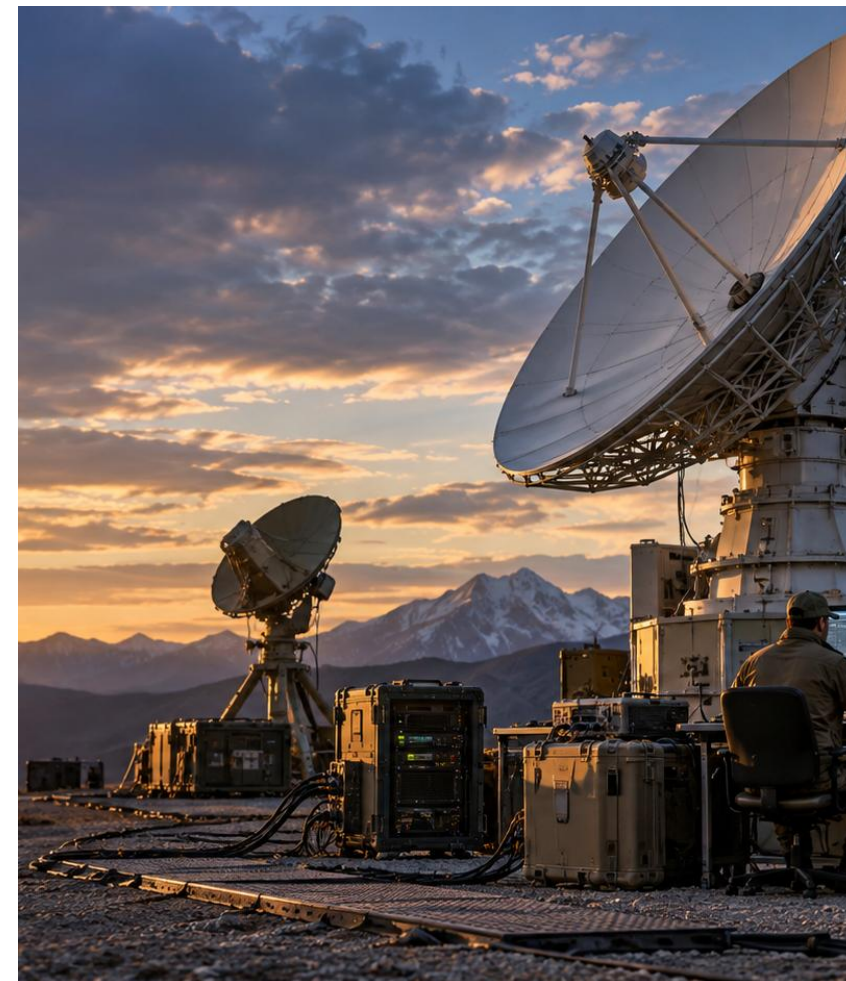
Can I access the ground segment when I need it? Can I recover from disruption within mission timelines?



OPERATIONAL CONFIDENCE

Do I trust the system enough to act on what it tells me? Uncertainty has operational cost.

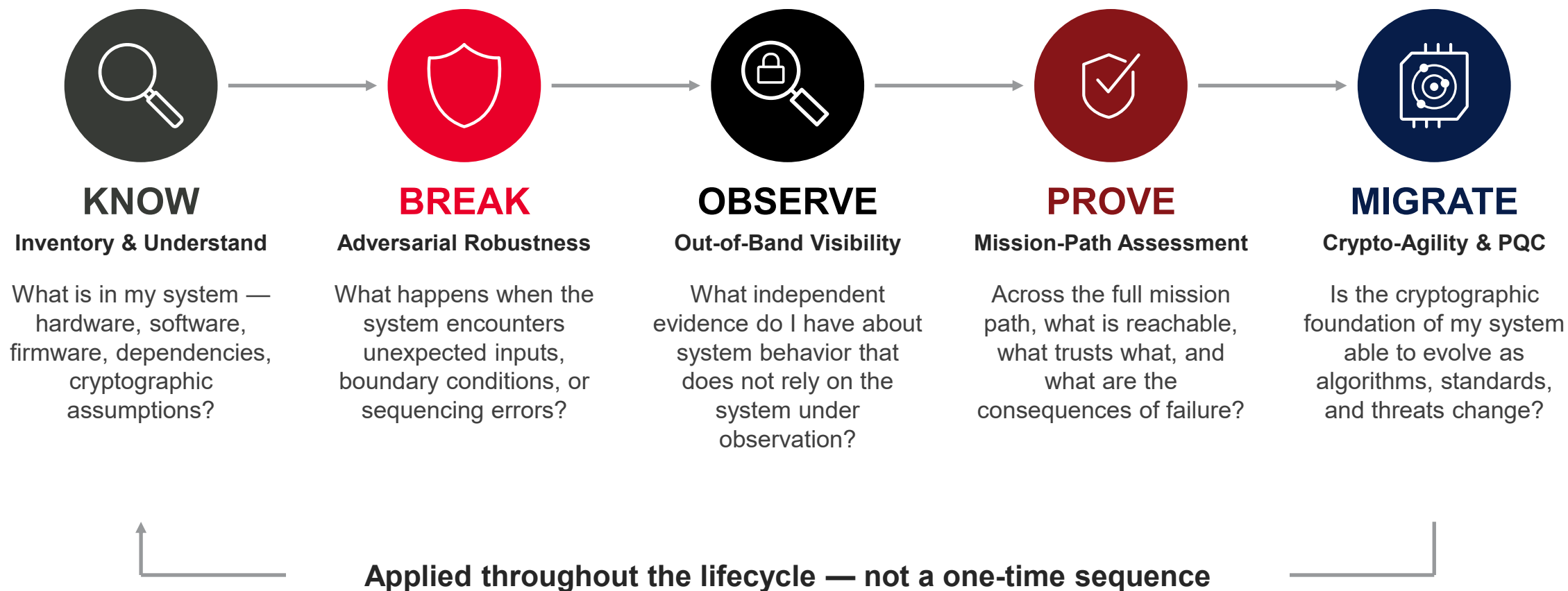
An adversary does not need to destroy infrastructure — degrading confidence or introducing doubt about signal integrity can have the same operational effect.



Stanislov Petrov?

Secure the Whole System

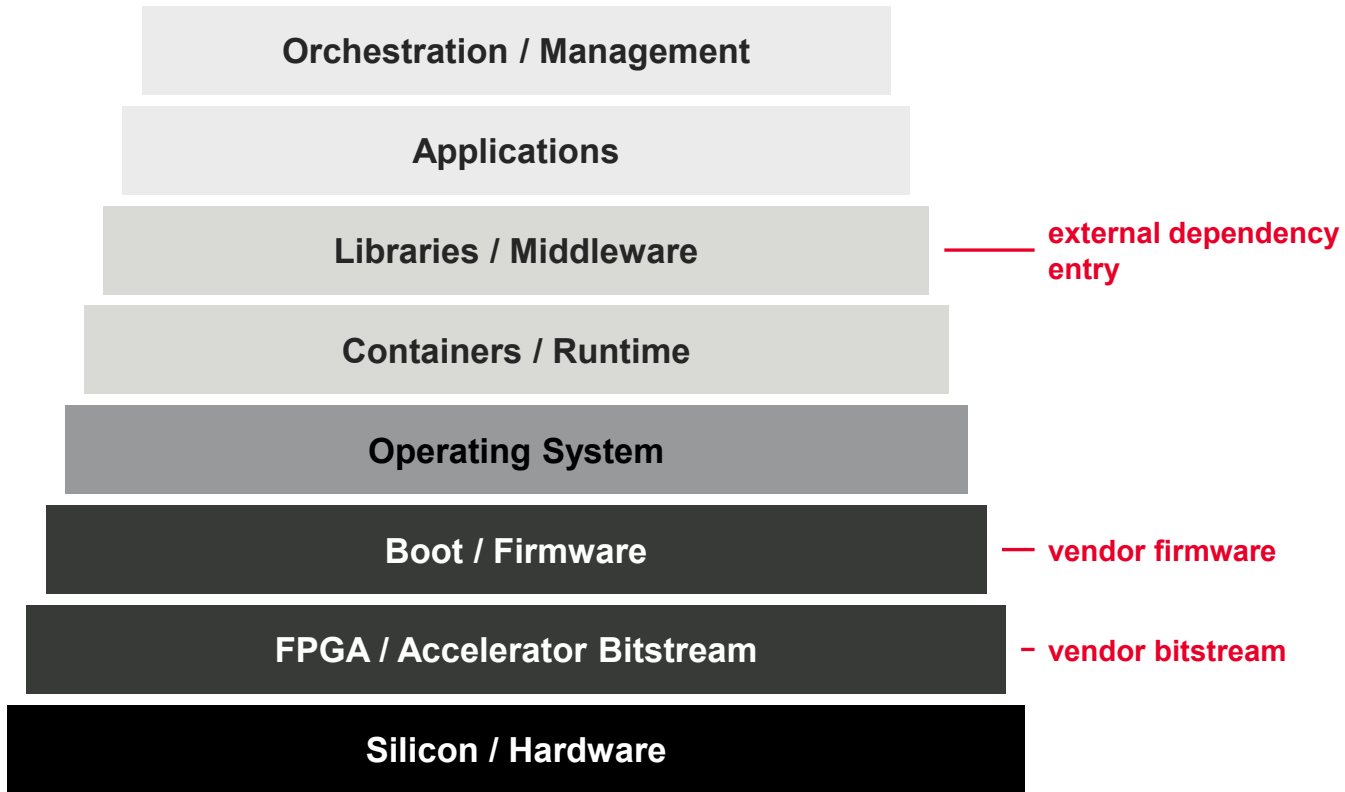
Five assurance disciplines — each answers a specific engineering question



Any meaningful change — new software, interface, vulnerability, or threat knowledge — restarts the cycle.

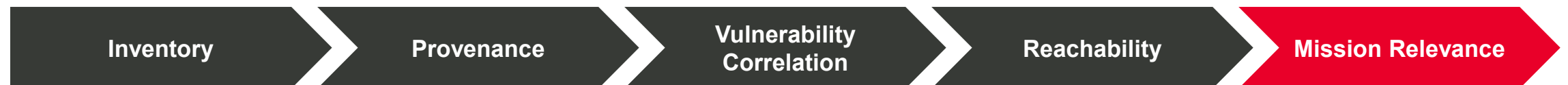
KNOW — You Can't Secure What You Can't Enumerate

A modern ground system is a dependency stack, not a box



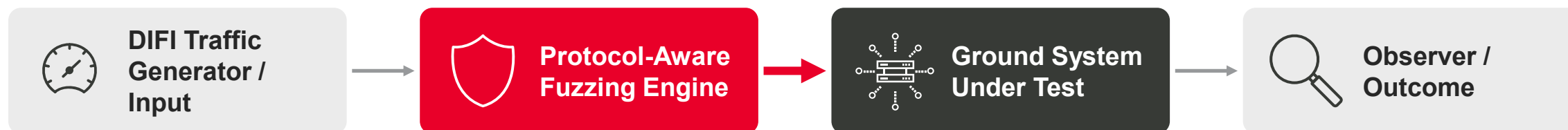
An SBOM tells you what is there. It does not tell you what matters.

An exposed vulnerable component and an unreachable one can carry very different operational risk.



BREAK — Fuzz the Conversation, Not Just the Packet

Conformance tells us valid traffic works. Fuzzing asks what happens when reality gets messy.



What the fuzzer manipulates



Malformed Fields & Lengths

Unexpected values and lengths



Boundary & Edge Cases

Zero-length, maximum, overflow candidates



Sequencing & State Errors

Out-of-order messages, invalid transitions



Timing & Rate Anomalies

Bursts, delays, unexpected pacing



Grammar-Aware Inputs

Mutate within DIFI packet structure



Differential Behavior

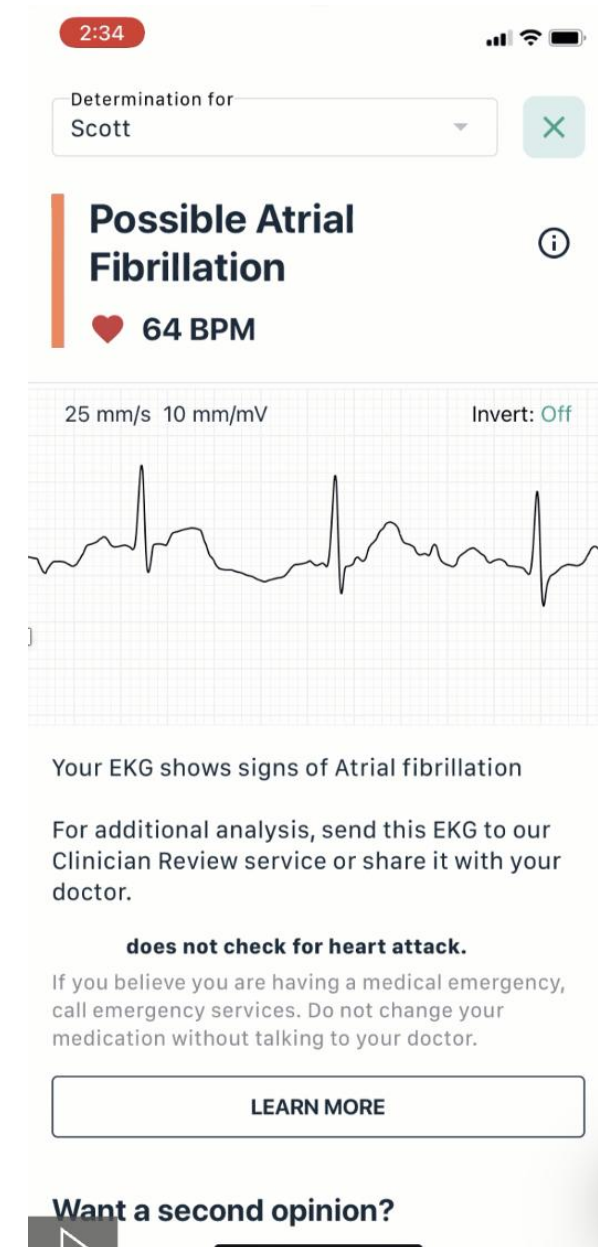
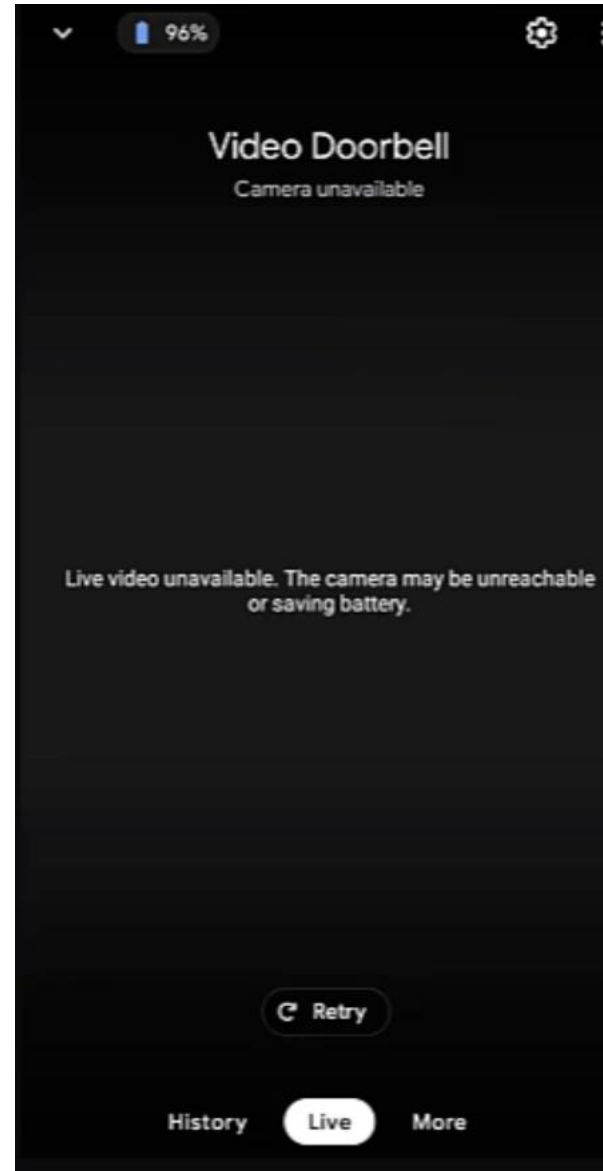
Compare responses across implementations

What are we looking for?

- **Accepted** processed as if valid
- **Rejected** refused cleanly
- **Degraded** slower, lossy, impaired
- **Crash** process or device fails
- **Hang** stops responding
- **Divergent** implementations disagree

Behaviors to investigate — not a severity ranking

Fuzzing for Fun & Profit



PROVE — Assess the Mission Path, Not Just the Host

A vulnerability's impact depends on where it sits in the mission path



WHAT IS REACHABLE?

From which network interfaces can an attacker or malformed input reach this component?



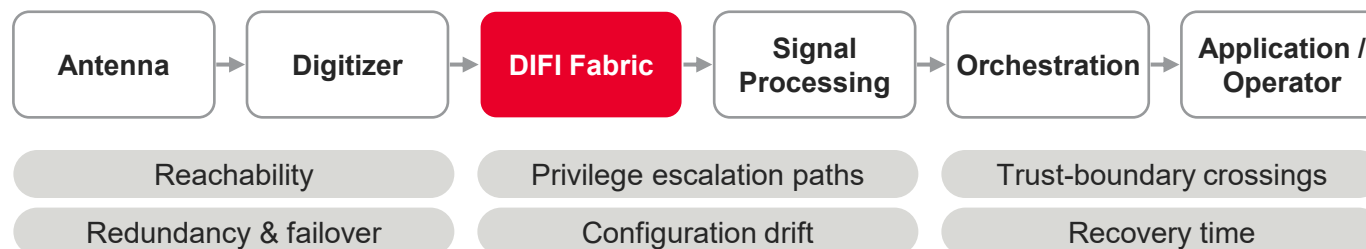
WHAT TRUSTS WHAT?

Which components accept commands, data, or updates from this component without independent verification?



WHAT HAPPENS IF A NODE FAILS OR IS COMPROMISED?

What is the operational consequence, and how far downstream does it propagate?



A host-level vulnerability report is a starting point. Mission-path assessment adds context, consequence, and prioritization.

MIGRATE — Cryptography Is Now a Lifecycle Problem

Post-quantum migration is an engineering program, not an algorithm swap



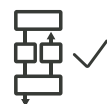
NIST finalized the first three PQC FIPS standards in 2024.

The challenge now is engineering the migration.

ML-KEM — FIPS 203

ML-DSA — FIPS 204

SLH-DSA — FIPS 205



Protocols

Algorithm negotiation across transport and application protocols



Certificates & PKI

Certificate chains, signing, revocation, and lifecycle



Key Management

New sizes and mechanisms affect generation, storage, rotation



Hardware Accelerators

Fixed-function crypto can constrain algorithm support



Performance & Bandwidth

Key, signature, and compute costs can affect links and processing



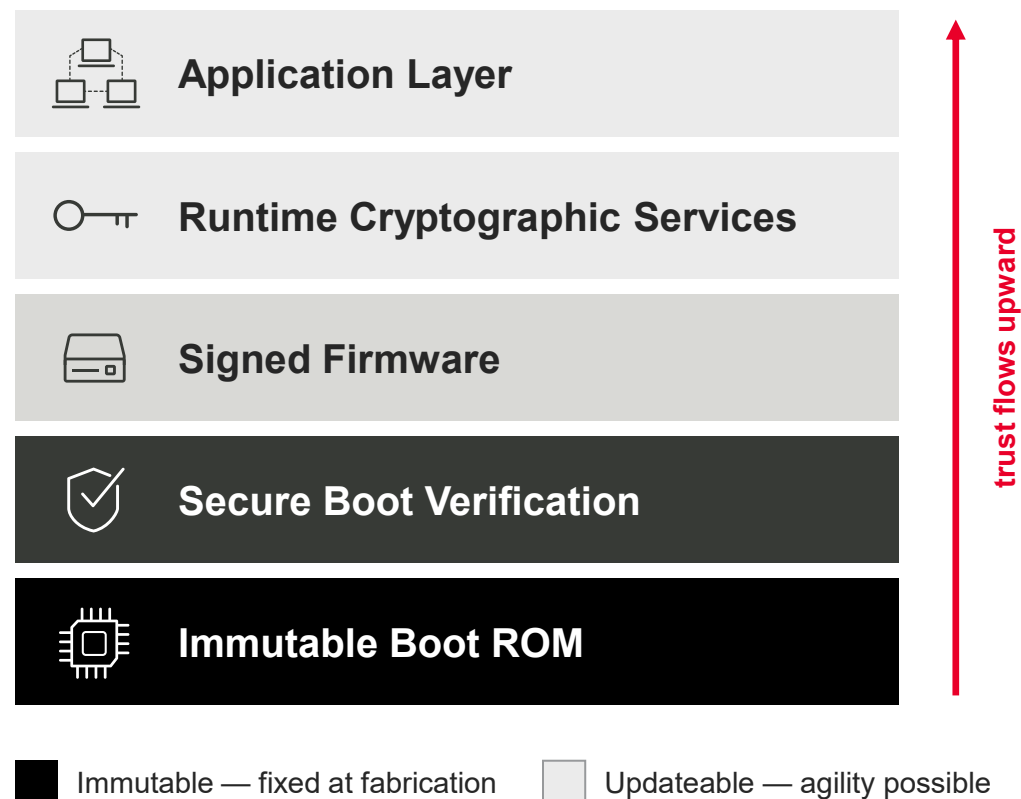
Long-Lived Assets

Satellites and ground hardware can outlive embedded crypto assumptions

PQC migration is a system-engineering problem — not an algorithm swap.

Crypto-Agility Has to Reach the Root of Trust

The lowest layers constrain what the application layer can ever change



Where agility gets constrained

Immutable ROM Algorithm selection can be fixed at fabrication and cannot be patched at the application layer.

Secure Boot Verification algorithms must match what the root trusts.

Signed Firmware Updates Update signing keys and algorithms must themselves be migratable.

Secure Elements / TPM Roots Key-size and algorithm constraints can be fixed at hardware design time.

Crypto Accelerators Fixed-function hardware may constrain supported algorithms.

Migration path for hardware-rooted systems: hardware replacement programs, or architectures that keep classical roots while adding agility above them, may be required.

Crypto-agility must reach the hardware foundation — not just the application layer.

Test the Migration Before the Mission Depends on It

Validate behavior across real conditions — before deployment



Interoperability

Classical, hybrid, and PQC endpoints negotiate and complete exchanges



Performance

Latency, throughput, and resource use with larger keys and signatures



Key & Certificate Lifecycle

Issue, rotate, revoke, and renew with new algorithms



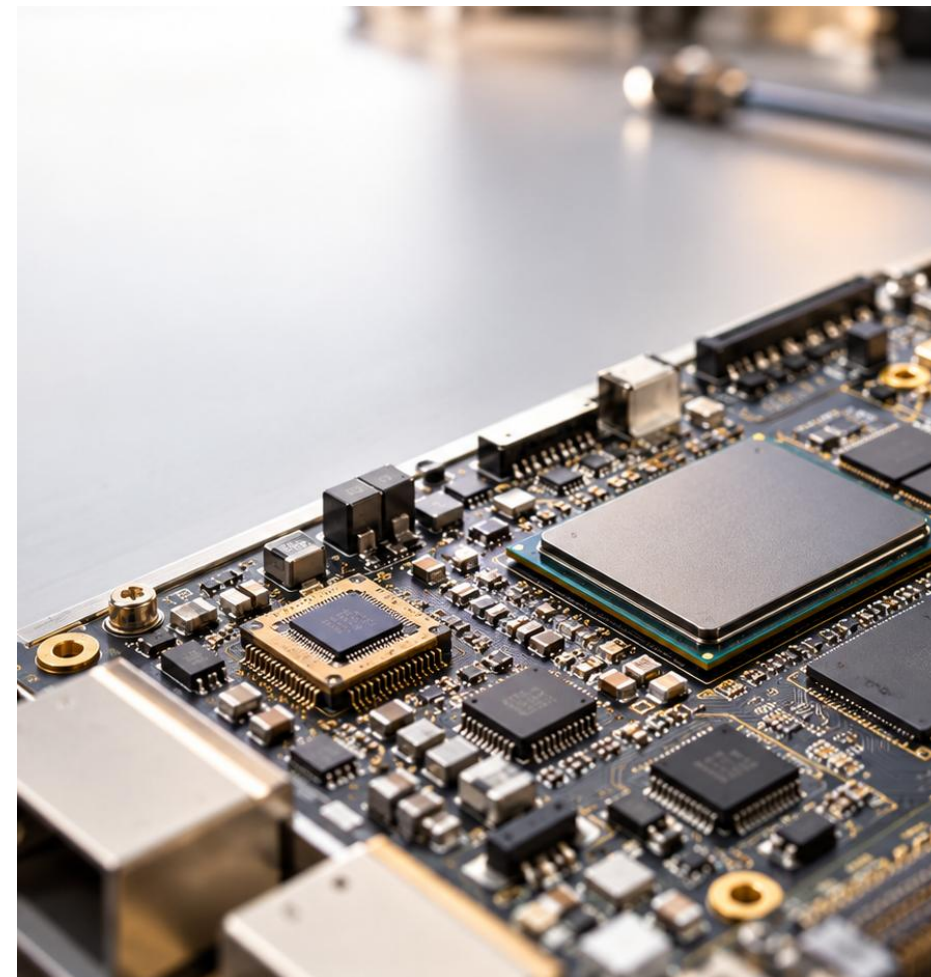
Mixed Generations

Old and new equipment coexist; downgrade and rollback stay controlled



Recovery & Resilience

Failures fail safe and restore within mission timelines



Find the issues in the lab — not in the field.

ASHTON
KUTCHER

THE GUARDIAN



RISK EVERYTHING SEPTEMBER

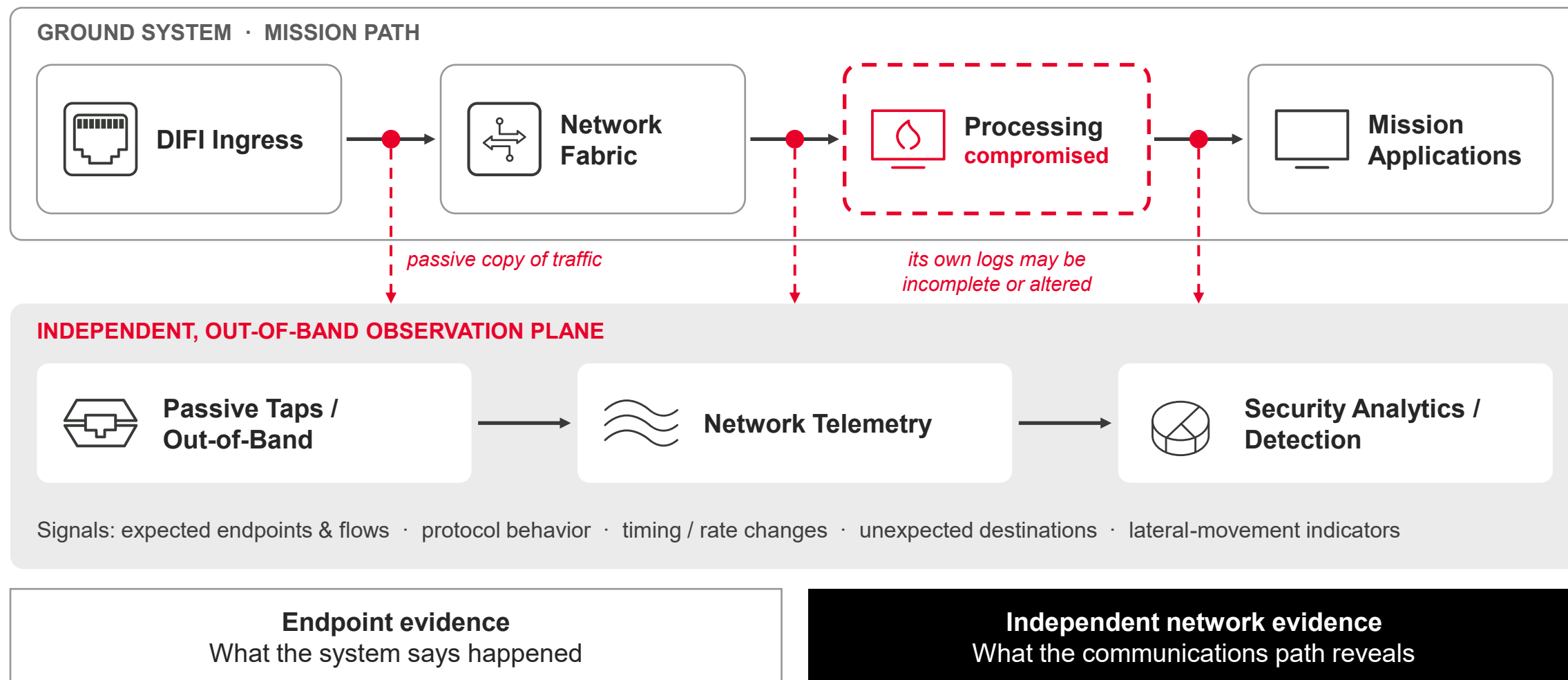
guardianmovie.com

 Teachmean

Because you still have the ability to think.

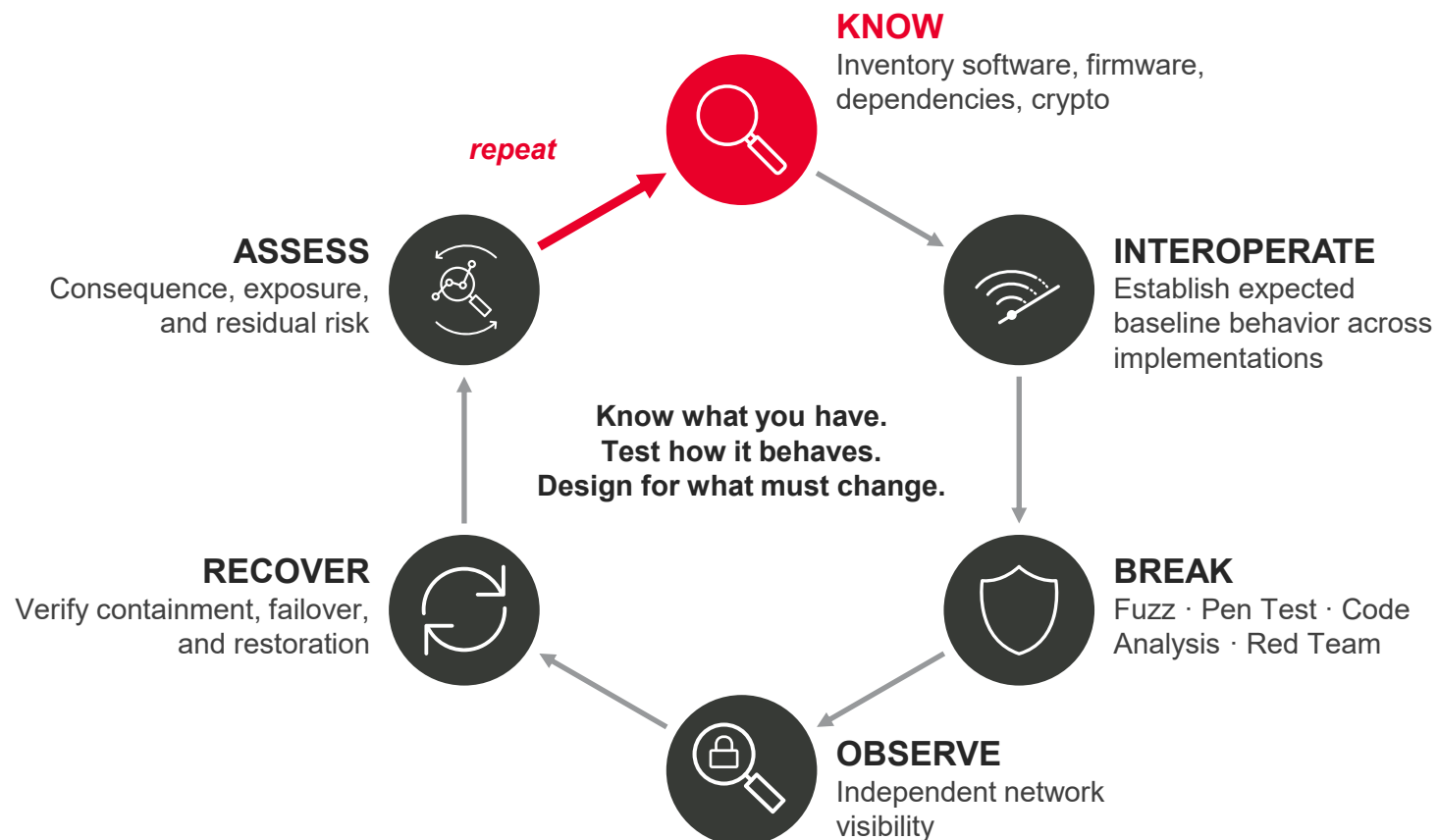
OBSERVE — Don't Let the Compromised System Be Your Only Witness

Do not rely on a potentially compromised system as your only source of evidence



Make Security Validation Part of Interoperability

A practical PlugFest loop that puts the five disciplines to work



Build security into the definition of interoperable.

