HACKING PHYSICS AT 300 KPH: Securing the Cyber-Physical Edge in F1

How Project Apex Validates Telemetry Integrity in Real-Time Racing

Timothy D. Harmon, CISSP | Lead Enterprise Architect | Cisco Insider Champion

BSides San Diego 2026 | April 4, 2026

Motorsport UK · BMMC · SMMC · SCCA San Diego

The 2026 Reality Check

"I have to look at my steering wheel every three seconds… It's why I don't see the debris. You have to look at the steering wheel to see what's going to happen, otherwise you're going to end up off the track."

- Lando Norris, World Champion
Melbourne, March 6, 2026

- **50:50 hybrid = attack surface explosion (thermal + electrical + software interdependencies)**
- **Drivers = blind to anomalies (cognitive load maxed, data visibility gaps)**
- **Data integrity = mission-critical (unvalidated sensor input = untrusted data plane**
- **ML deployment algorithms update beyond driver control - one snap of oversteer changes the whole system state**

The Threat Landscape

Human Factor

60Hz (3,600 reads/min) ⟶ Critical Anomalies Lost in Noise

***Threat**: Noise obscures signal; malicious or degraded data hides in stream*

Data Trust Gaps

No Validation Layer | Sensors aren't cross-verified

***Threat**: Unvalidated sensor input is untrusted data; one corrupted sensor can cascade*

Physics Anomalies

Thermal + squat + energy | No baseline to catch them

***Threat**: Hardware faults and software bugs exploit the physics blind spot*

No dedicated integrity validation layer exists in F1 today.

Why This Talk Belongs at BSides

1. IDS/IPS for the Physical World
   - Signature detection (physics envelopes)
   - Severity classification (GREEN/YELLOW/RED)
2. Zero Trust, Motorsport Edition
   - “Never trust, always verify” applies to telemetry
   - Even internal sensors need validation
3. Edge Computing Under Pressure
   - Real-time constraints (60Hz, <10ms)
   - Mission-critical reliability
4. Security as Competitive Advantage
   - Championship margins: milliseconds
   - Data integrity = operational superiority

Project Apex: Real-Time Physics Validator

- **Validator**: Validates telemetry against physics baselines
- **Cyber-Physical**: Tags events with severity (GREEN/YELLOW/RED)
- **Edge**: Forwards enriched telemetry to Splunk
- **SIEM**: Surfaces anomalies to engineers

What v1.1 IS NOT

X NOT a gating layer - Apex observes, doesn't block. (Data flows; Apex validates in parallel)
X NOT predictive - Apex detects, doesn't predict. (Signature detection, not ML forecasting)
X NOT a black box - Apex is deterministic physics validation (Transparent rules, human-verifiable decisions)
X NOT attestation (v1.0 roadmap). Apex v1.1 focuses on real-time physics validation. (Cryptographic sensor auth = future layer)

Runs in parallel. Human engineers stay in control.

MCL40 Physics Baseline (2026 Regs)

Each parameter is an attack surface. Violations = sensors corrupted, software faulted, or physics violated.

Parameter	Value	Why It Matters
Car Mass:	768 kg	Energy Base
Vertical Energy Limit:	100 J (std) 80J (high thermal)	Oscillation Cap
Thermal Threshold:	130°C	Engine Expansion
Aero Stall RH:	28 mm	Diffuser Stall

Anomaly Signature: When [temp >130°C AND vertical energy >80J AND rear RH <28mm] → RED alert. (Physics envelope violated)

Multi-Threaded Edge Engine

Air-Gapped Edge Intrusion Detection: Processing at the Sensor Layer

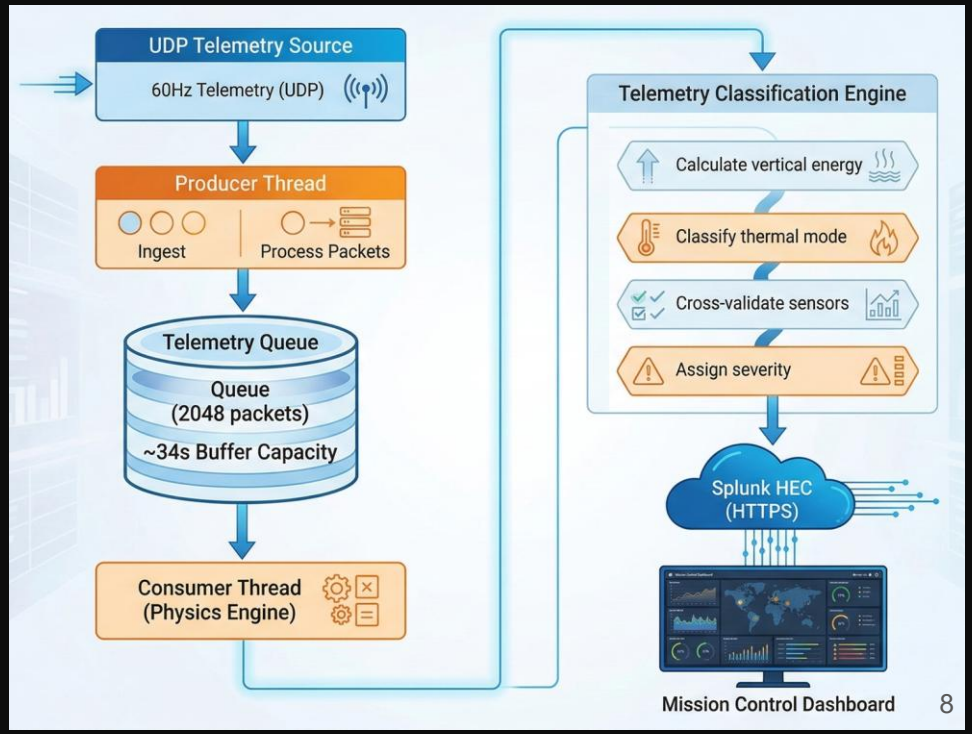
Key Stats:

- Latency: <10ms edge processing
- Throughput: 3,600 events/min sustained
- Resilience: Tail-drop on overflow

Dynamic Mass Model:

- Energy = $0.5 \times m \times v_z^2$

Benefit: Eliminates the network attack surface; anomaly detection happens before data leaves the garage.



YELLOW → RED Alert: Trending → Anomaly Detected

```
YELLOW: TRENDING
engine_temp_c = 135°C
vertical_energy = 85J
```

```
RED: ANOMALY_DETECTED
engine_temp_c = 138°C
vertical_energy = 95J
rear_rh_mm = 26mm
```

➔ **Purpose**: Early warning

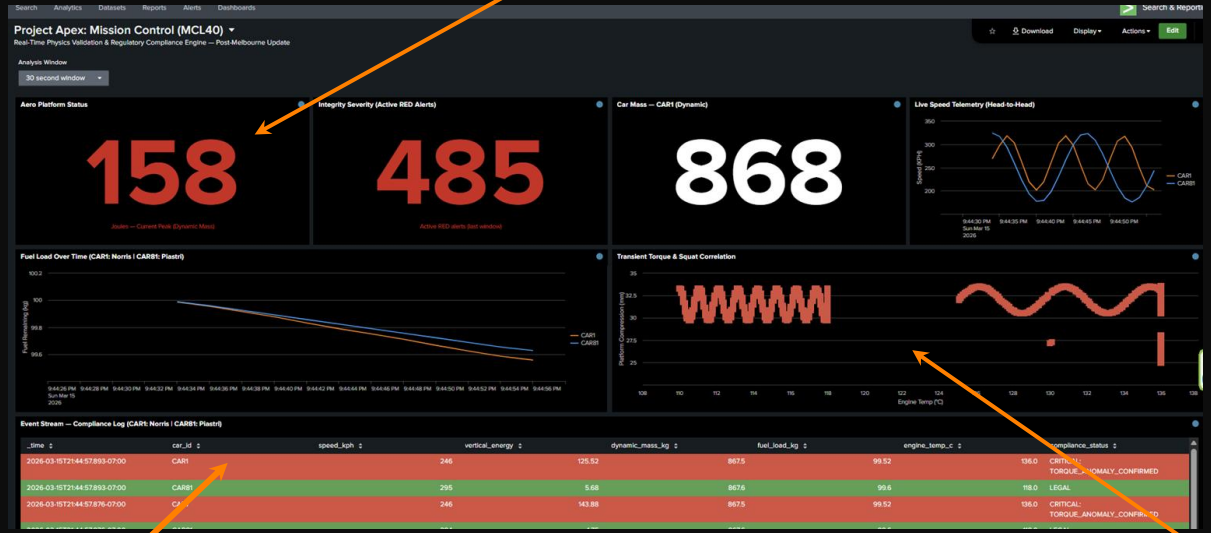
➔ **Action**: Monitor closely

➔ **Purpose**: Critical anomalies

➔ **Action**: Engineers to Splunk

Real-Time Integrity Visualization

Engineer decision support

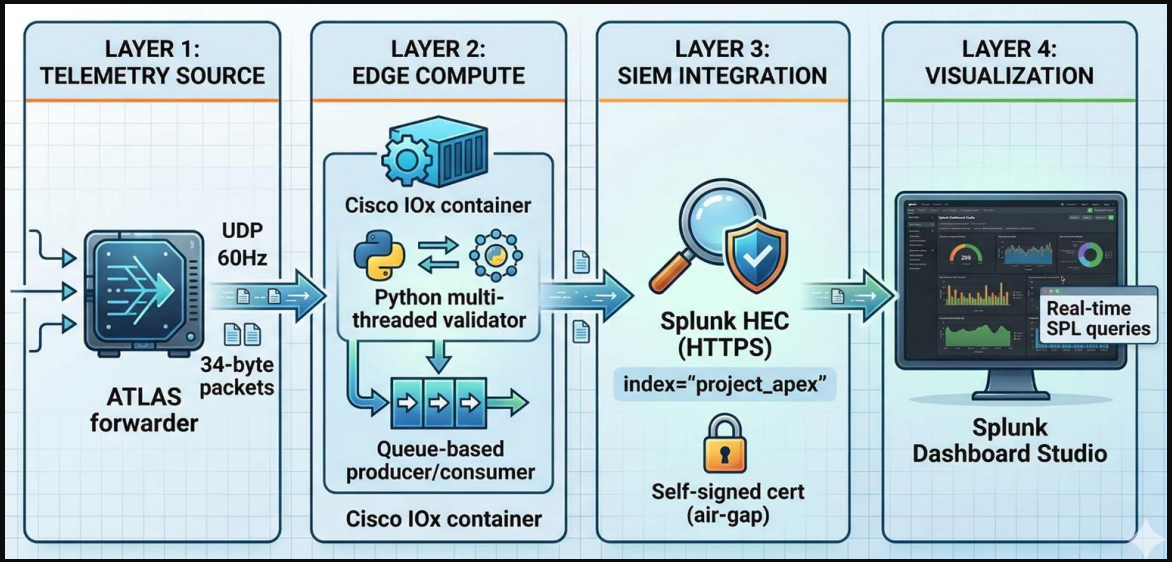


Severity-aware event log

Real-time physics correlation

Production-Grade Edge Deployment

Security Posture: Air-gapped deployment, zero exfiltration risk, production-architecture validated.



Air-gapped garage network | 99.8% uptime Melbourne 2026 | Zero data loss | 18ms edge processing latency

Why This Matters Right Now

0. Oliver Bearman - 50G Crash, Spoon Curve, Suzuka (March 29, 2026) - Two cars at full throttle, 50kph closing speed differential, zero warning. FIA issued official statement same night acknowledging “high closing speeds.” The system had no mechanism to surface the energy state difference before it became a wall impact

1. Driver Cognitive Load Maxed Out
   Driver attention = limited

2. Oscar Piastri Crashed on Recon Lap (March 8, 2026) → 100kW surge → cold tyres, empty battery

3. FIA Changed Rules Mid-Weekend (Melbourne) → Energy cap shift mid-weekend

4. McLaren-HPP Timeline Integration Gap - Customer teams learn PU exploitation in production, at race speed, without a works team’s pre-season simulation runway. Independent validation accelerates the learning curve.
   Five incidents in three weekends - FIA officially acknowledged the system’s visibility gap on the same night as the Japanese GP.

5. FIA changes qualifying energy limits between events - again. Apex reconfigures in 60 seconds.

Three Real Examples: Cyber-Physical Security Failures (March 2026)

1. Leclerc's 95% Throttle (Shanghai Sprint Qualifying)
   SECURITY FAILURE: Sensor threshold misaligned from physical reality
   THREAT: Invalid threshold = corrupted decision data at 300 kph

   Sensor divorced from reality → Throttle cut when driver should have full power

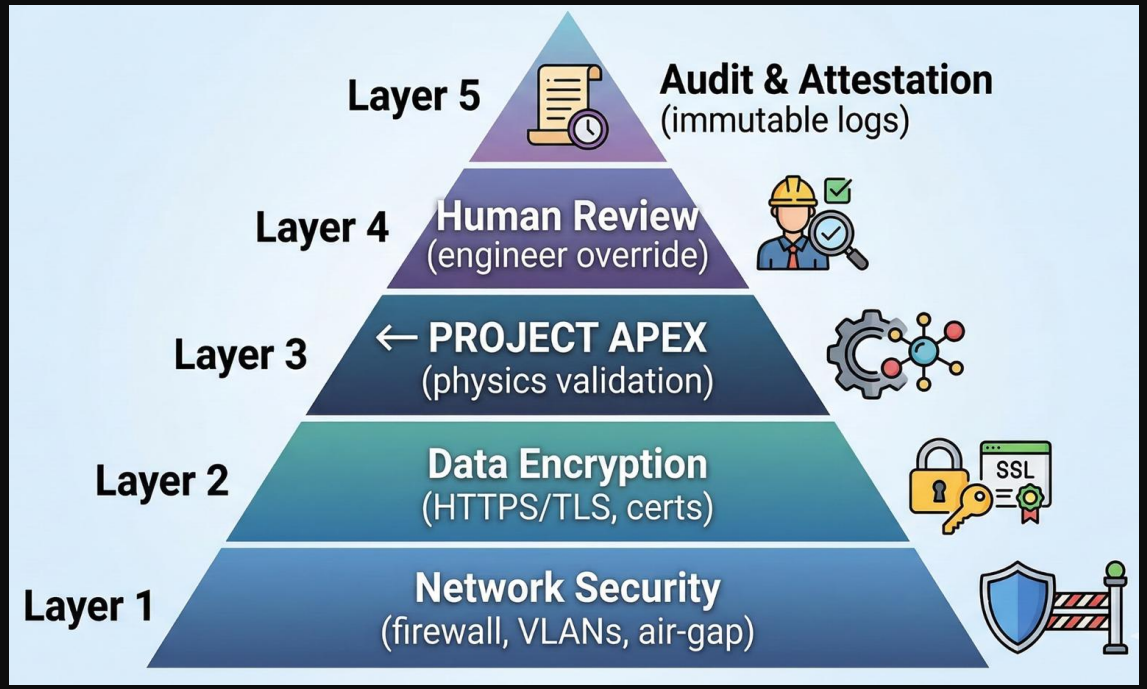
2. Piastri's Recon Lap (Melbourne)
   SECURITY FAILURE: Hardware fault undetectable from available telemetry
   THREAT: Battery failure without precursor signal

   100 kW surge, telemetry blind → Cold tyres compound the failure

3. Mercedes Two-Phase Wing (Regulation Blind Spot)
   SECURITY FAILURE: Physical behavior hidden from both telemetry and regulators
   THREAT: Aero envelope violated; validation layer missed it

   Physical act hidden from regulators

Cyber-Physical Security Layers



Most teams stop at Layer 2. Apex adds the missing physics layer.

Layer 3 (v1.0): Threshold-based physics validation. Cryptographic attestation is roadmap.

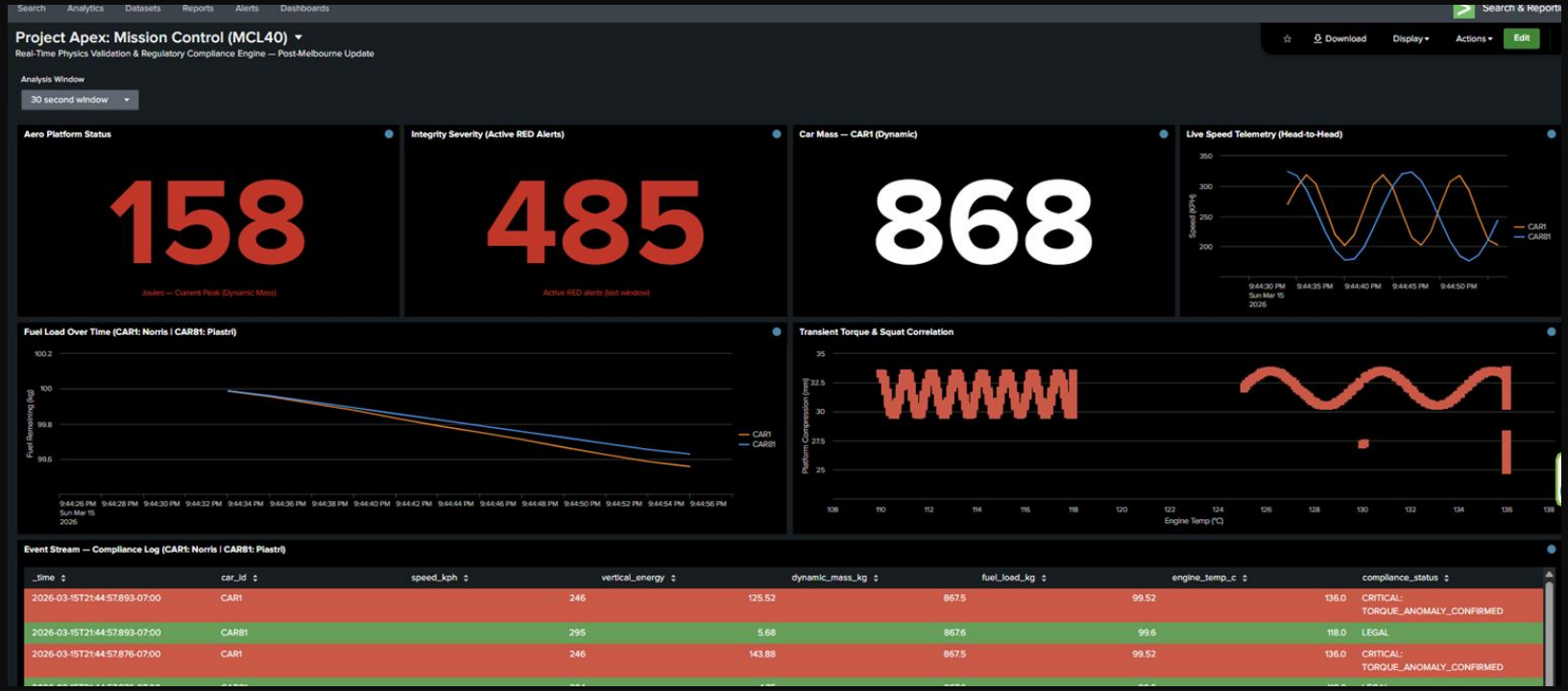
v1.0 BOUNDARIES & v1.2 Roadmap

- ✗ Inline gating or data holds
- ✗ Multi-lap trajectory prediction
- ✗ Machine learning anomaly detection
- ✗ Cryptographic sensor attestation

- Multi-channel correlation
- Per-circuit adaptive baselines
- Cryptographic sensor attestation
- Advanced alerting workflows

v1.0 Focus: Threshold-based physics validation with human-in-the-loop decision making.

Apex in Action



What You Can Use Monday

1. Cyber-physical systems need physics-aware validation
   - OT/ICS principles apply to motorsport, AVs, drones
2. Edge compute + SIEM = powerful architecture
   - Process at source, centralize visibility
3. Human-in-the-loop is a feature
   - RED alerts surface, engineers decide

Let’s Talk Cyber-Physical Security

- LinkedIn: /in/timharmon
- GitHub: github.com/SecurityCyberGeek/project-apex-telemetry
- Medium: Formula One Forever publication

#BSidesSanDiego2026 #ProjectApex #CyberPhysical

McLaren FORMULA 1 TEAM

Thank You!

This work began with a simple question watching Formula 1: how do we make the fastest cars on earth safer through better data? Grateful for everyone who helped turn that question into Project Apex.

- McLaren Racing - operational excellence
- FIA University - motorsport technical education
- Motorsport UK - marshal and safety training
- Cisco IOx Team - edge compute platform
- Splunk Community - SIEM best practices
- BSides San Diego - platform to share