

SensAbility Snapshot

Device Authenticity and Counterfeit Detection

How SensAbility helps verify authentic hardware at the physical layer

Applications

Predictive maintenance
Device validation and authentication
Supply chain verification
Fielded asset validation
Counterfeit hardware detection

Partnership Opportunities

SensAbility is building a partner ecosystem with sensor OEMs, DAS/ICS/OT monitoring vendors, supply chain assurance platforms, and system integrators. Partners can integrate SensAbility into condition monitoring, device validation, and asset integrity offerings to verify authentic hardware, detect counterfeit or substituted devices, and improve confidence across multi-vendor environments.

Contact Information

Kirk Byles, CEO | Kirk@rapiertechgroup.com | 303-886-6379

Overview

Counterfeit or substituted hardware can look correct on paper while still changing device integrity in the field. A cloned board, swapped component, or tampered sensor may match expected labels, protocols, and specifications well enough to pass ordinary checks.

SensAbility addresses that gap by monitoring devices at the physical layer. It compares live signal behavior against a trained baseline from authentic hardware to validate identity and flag counterfeit, cloned, swapped, or manipulated devices without teardown or disruption.

The Problem

In industrial, embedded, and regulated environments, visual inspection, serial numbers, and vendor metadata do not prove that installed hardware is genuine. Counterfeit or altered devices can imitate higher-layer behavior while introducing reliability issues, performance uncertainty, or unapproved substitutions that are difficult to see with conventional checks.

The SensAbility Approach

SensAbility uses passive physical-layer fingerprinting to establish a trusted signature for authentic hardware. It then compares new observations against that baseline to validate device identity and detect meaningful variation. This allows teams to authenticate hardware without firmware access, disassembly, or reliance on external markings.

What It Can Help Detect

- Cloned or counterfeit components in the supply chain
- Unauthorized board or device swaps in the field
- Post-deployment hardware manipulation or replacement
- Signal-level deviations from authentic hardware baselines

Operational Value

By validating hardware at the physical layer, SensAbility can help organizations:

- Improve confidence in supply chain and fielded assets
- Respond faster to counterfeit or substituted hardware
- Reduce teardown and manual inspection

Deployment Fit

SensAbility is suited for environments where teardown is impractical, uptime is critical, or fleets include a mix of COTS, embedded, and mission-critical equipment. It supports wired or wireless deployments across SaaS, enterprise, OEM, and edge models.