```
---
layout: paper
title: "When Signals Lie: Why Traditional ICS Security Fails at the Physics Layer"
date: 2026-03-09
version: "Research Essay"
description: "A technical essay on signal manipulation, trust boundaries, and why
traditional industrial cybersecurity controls fail when the physical layer is
compromised."
pdf: /assets/papers/when-signals-lie-physics-layer-ics.pdf
---
```

Abstract

Traditional cybersecurity controls are designed to protect digital communications, authenticated identities, and network boundaries. Industrial control systems, however, depend on physical signals that represent pressure, temperature, voltage, timing, speed, and position. When those signals are manipulated before they enter the digital domain, downstream authentication, encryption, and monitoring may all function correctly while the system still acts on false data.

This paper argues that many ICS and OT security models still treat the analog-to-digital boundary as implicitly trustworthy. Using examples from harmonics, amplitude manipulation, timing attacks, phase distortion, and signal-path abuse, it explains why traditional controls often fail at the physics layer and what defenders should do differently.

Note on Responsible Disclosure

All signal manipulation techniques discussed in this article are drawn from publicly available academic research, industry standards, and government security guidance. The goal is to help defenders understand threats they may not have considered, not to provide attack tutorials. Where specific techniques are mentioned, citations are provided to peer-reviewed research published for defensive purposes.

When Harmonics Become Attack Vectors

Industrial control systems are built on an assumption: that input signals follow predictable physical laws. A 4–20mA current loop should vary smoothly. A 60Hz AC waveform should be sinusoidal. A sensor reporting temperature should change gradually, not instantaneously.

But physics also gives us harmonics — integer multiples of fundamental frequencies that naturally occur in electrical systems. A 60Hz power signal generates harmonics at 120Hz, 180Hz, 240Hz, and so on. In normal operation, engineers design systems to filter out these harmonics because they represent noise or inefficiency.

Here is the security problem: many control environments validate the fundamental frequency but do not verify harmonic content. They ask “is this a 60Hz signal?” without asking “is this a clean 60Hz signal?”

Why This Matters for Defenders

An adversary with physical or RF access does not necessarily need to compromise authentication systems or break encryption. They can inject harmonic content that:

- Causes sensors to misreport values
- Triggers protective relays prematurely
- Bypasses simplistic signal validation

This concern is not theoretical. Prior research has shown that physical signal injection can manipulate sensing behavior in systems such as MEMS sensors, and the same defensive concern applies to industrial sensing environments where downstream logic assumes clean inputs.

The Detection Challenge: Why Fourier Analysis Is Not Enough

If you have an electrical engineering or signal processing background, your first instinct might be to use Fourier analysis to detect anomalous harmonic content. The mathematics are sound — a Fourier transform decomposes a signal into its constituent frequencies, revealing harmonics that should not be there.

In theory, defenders could establish a baseline harmonic profile for each signal path and alert when the frequency spectrum deviates. But operational reality is more complicated:

- Time-frequency tradeoff
- Real-time constraints
- Baseline complexity
- Adversary adaptation

The bigger problem is that most ICS environments are not performing signal-level analysis at all. Legacy systems were not architected for it, field devices often lack the computational headroom, and most security teams were trained to analyze packets rather than signals.

The Trust Boundary Problem

This maps closely to software and data integrity failures, but at the physical layer. Application code may validate digital inputs correctly, but if the sensor or time source is receiving manipulated analog or RF signals, that validation happens too late in the chain.

Traditional IT security asks: “Is this data from an authenticated source?”

Physical-layer security must also ask: “Does this signal’s shape, timing, and behavior match what physics says it should be?”

Authentication happens after signal interpretation.

What Defenders Actually Need

The mathematics for detecting many of these anomalies have existed for decades. What is missing is the security mindset that says defenders should analyze signals, not just packets.

If you are protecting critical infrastructure, your security program needs:

1. Signal integrity monitoring
2. Multi-sensor correlation
3. Physics-based baselines
4. Analog domain expertise

The electronics technician in me knows this: every signal has a signature. Clean sensor data looks different from manipulated data if you know what to measure.

The Broader Implication

Harmonic injection is one example of a larger class of physical-layer attacks that traditional cybersecurity tools cannot reliably detect. This is where OT security fundamentally differs from IT security.

In IT, we often assume our inputs are digital and well-defined. In OT, our inputs are interpretations of physical phenomena — voltage representing pressure, frequency representing speed, current representing flow, timing representing sequence and coordination.

And physics can be manipulated in ways that bypass every digital security control built downstream.

If your security program does not account for this, you have a blind spot at the most fundamental layer of your system.

Beyond Harmonics: The Broader Signal Manipulation Landscape

Harmonic injection demonstrates a broader principle: if you can manipulate the physical signal, you can bypass every digital security control downstream. But harmonics are only one example. Amplitude, frequency, phase, timing, and modulation can all become attack surfaces when systems trust signals without validating their physical integrity.

Amplitude Manipulation: Making Sensors Lie

A 4–20mA current loop is a core industrial signaling method. If an attacker can inject or attenuate current on that loop, they may be able to make the receiving system believe the process variable is safe when it is not.

Timing Attacks: When Nanoseconds Matter

Many critical systems rely on GPS or GNSS for timing. If that timing source is spoofed or manipulated, systems can continue operating “normally” while making decisions based on false temporal assumptions.

Phase Manipulation: Three-Phase Power and Beyond

In three-phase electrical systems, the phase relationship can matter as much as amplitude or frequency. Manipulating phase while staying within expected ranges can create abnormal effects that traditional parameter checks may not catch.

Modulation Attacks: Hiding Messages in Messages

RF and telemetry systems rely on modulation. Where receivers are designed for resilience rather than suspicion, malicious variation inside an otherwise valid signal path may cause misinterpretation without triggering classic network alarms.

Where Traditional Security Controls Fail

Network Segmentation: Protecting the Wrong Boundary

Segmentation protects digital communication paths. It does not protect analog sensor lines, timing sources, or RF signal paths that bypass the network entirely.

Authentication: Trusting Verified Sources That Trust Unverified Inputs

A legitimate device can still faithfully report a false value if the signal it interprets has already been manipulated.

Encryption: Protecting Data That Is Already Wrong

Encryption protects data in transit after digitization. It does not validate the physical correctness of the signal that produced the data.

Intrusion Detection: Looking for the Wrong Signatures

Network IDS and protocol-aware monitoring tools detect anomalies in traffic patterns and message structure. They generally do not establish ground truth for whether a measured signal corresponds to physical reality.

The Air Gap Illusion

Air gaps reduce remote network access. They do not eliminate sensor cables, field wiring, radio links, power paths, or GPS dependencies.

Why Security Vendors Have Not Solved This

Several factors slow progress at the physics layer:

1. Market maturity mismatch
2. Deployment complexity
3. Expertise gap
4. False positive risk

5. Weak ROI visibility

The result is a persistent assumption gap: defenders keep protecting digital trust boundaries while leaving the physical-signal boundary comparatively under-modeled.

The Fundamental Assumption Gap

Traditional security controls often assume that inputs from sensors and timing references represent ground truth.

That assumption breaks when the physical layer is compromised.

You cannot digitally authenticate an analog signal.
You cannot encrypt a voltage to verify its accuracy.
You cannot firewall a wire.

The controls we have built are necessary, but they are not sufficient.

References

[1] National Institute of Standards and Technology. (2023). *Guide to Operational Technology (OT) Security: NIST Special Publication 800-82 Revision 3.* https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/final

[2] Cybersecurity and Infrastructure Security Agency. *ICS Advisories.* https://www.cisa.gov/ics-advisories

[3] Shepard, D. P., Humphreys, T. E., and Fansler, A. A. (2012). “Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks.” *International Journal of Critical Infrastructure Protection*, 6(3–4), 146–153.

[4] Scott, L. (2003). “Practical Cryptographic Civil GPS Signal Authentication.” *Navigation*, 50(1).

[5] Wesson, K. D., et al. (2013). “GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals.” *IEEE Transactions on Aerospace and Electronic Systems*, 49(4).

[6] Amin, S., et al. (2009). “Analytic Models for Sensor Attack Detection.” *IEEE International Conference on Technologies for Homeland Security.*

[7] Son, Y., et al. (2015). “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors.” *USENIX Security Symposium.*

[8] Hossain-McKenzie, S., et al. (2017). “Analysis of Synchrophasor Data under GPS Spoofing and Jamming Attacks.” Sandia National Laboratories / IEEE PES General Meeting.

[9] IEEE Standards Association. (2022). *IEEE Standard 519-2022: IEEE Standard for Harmonic Control in Electric Power Systems.*

[10] Igure, V. M., et al. (2006). “A Survey of SCADA System Vulnerabilities.” *ACM Computing Surveys*, 38(1).

[11] Stamp, J., et al. (2003). “Security Issues in SCADA Networks.” *Computers & Security*, 22(6).

[12] Brigham, E. O. (1988). *The Fast Fourier Transform and Its Applications.* Prentice Hall.

[13] National Institute of Standards and Technology. *Cybersecurity Framework.* https://www.nist.gov/cyberframework

[14] IEC 62443 Series. *Industrial Communication Networks – Network and System Security.*

About the Author

Norris Cornell is an Identity and Access Management Analyst and Technical Lead in the financial sector, where he manages IAM and PCI DSS compliance during a core banking system modernization project. With nearly 20 years of electronics technician experience, he brings a unique perspective on the convergence of RF/SIGINT, ICS/OT security, and cyber-physical systems.

Norris holds a Master’s degree in SCADA Cybersecurity from Wilmington University and previously held DoD Secret clearance. He has been a volunteer and organizer for BSides Delaware since 2015 and recently presented “When Cyber Meets the Spectrum” at BSides Delaware 2025, focusing on satellite cybersecurity and critical infrastructure protection.

Norris operates CornellSecurity.com as a cybersecurity research platform. His research focuses on helping defenders understand physics-layer security threats in critical infrastructure environments.