WHITE PAPER

Closing the Signal Trust Gap in Aerospace and Cyber-Physical Systems

Toward Signal-Level Authentication for Resilient Navigation, Communications, and Autonomous Platforms

Trust the signal before trusting the data.

Signal-level evaluation focuses on whether an incoming waveform is consistent with a continuously generated real-time transmission, not merely whether the decoded data remains cryptographically valid.

Prepared for	Technical and policy audiences in aerospace cybersecurity, cyber-physical systems engineering, and secure communications architecture
Document type	Technical white paper
Date	March 2026
Primary thesis	Digital message authentication is necessary but insufficient where the physical signal itself may be recorded, delayed, relayed, replayed, or synthesized.

Contents

Document Orientation

Reader Need	White Paper Section	Core Question Answered
Policy and executive overview	Executive Summary	Why signal authenticity is a distinct security problem.
Technical problem definition	Sections 1-2	Why valid decoded data may still arrive in an invalid or deceptive signal.
Receiver architecture concept	Section 3	How waveform-level trust assessment can precede data trust.
Mission-domain relevance	Section 4	Where signal replay, relay, spoofing, and meaconing matter operationally.
Emerging threat context	Section 5	How AI-enabled synthesis and future computing pressure existing assumptions.
Deployment pathway	Section 6	How signal-level evaluation can complement existing standards and certification processes.

Executive Summary

Aerospace systems increasingly depend on radio signals whose authenticity cannot always be verified by traditional cybersecurity methods. Satellite navigation signals determine position and velocity, communication links transmit commands to spacecraft and unmanned platforms, and distributed sensor networks provide information used by autonomous systems to guide real-time decisions.

Security mechanisms for these systems have historically focused on protecting the digital information carried within those signals. Encryption, authentication protocols, and message integrity checks help ensure that transmitted data cannot be easily modified or forged by unauthorized parties. These mechanisms remain essential components of modern cybersecurity architectures.

However, protecting digital data does not guarantee that the signal delivering that data represents a genuine real-time transmission. In many cyber-physical systems, receivers authenticate decoded messages but do not evaluate whether the signal itself was generated live by the expected transmitter. Signals that have been recorded, delayed, relayed, or replayed may therefore still pass cryptographic verification. Attacks such as GNSS spoofing, meaconing, command replay, and signal relay exploit this vulnerability [1,2].

This discrepancy between data authenticity and signal authenticity can be described as the signal trust gap.

Closing this gap may require extending cybersecurity beyond data authentication to include evaluation of the signal waveform itself. By analyzing the temporal behavior and physical characteristics of incoming signals before decoding them, receivers may be able to detect replayed, delayed, or artificially synthesized transmissions.

This paper introduces the concept of the signal trust gap and examines how signal-level trust evaluation could complement conventional cybersecurity mechanisms. When combined with encryption, authentication, and system monitoring, waveform-level analysis may help create more resilient aerospace security architectures.

As aerospace systems become more autonomous and interconnected, future security architectures may need to verify not only the authenticity of digital data, but also the authenticity of the signals that deliver it.

Key Takeaways

- The signal trust gap arises when decoded data appears authentic while the physical signal may be replayed, delayed, relayed, or synthesized.
- Traditional cryptography remains essential but does not, by itself, prove that a received waveform was generated live by the expected transmitter.
- Signal-level trust evaluation adds a preprocessing layer that analyzes temporal behavior and waveform continuity before decoded data is trusted.
- Aerospace, navigation, timing, command, sensing, and autonomous systems are high-value domains because they depend on external signals for real-time decisions.
- Future resilient architectures should combine cryptographic, protocol, system-monitoring, and physics-based signal verification layers.

1. Introduction and Problem Statement

Modern aerospace systems rely extensively on externally transmitted signals to support navigation, communication, timing, and distributed sensing. Satellite navigation signals provide position and velocity estimates, communication links transmit commands and mission data, and distributed sensor networks supply information used by increasingly autonomous platforms to guide operational decisions. As aerospace systems become more interconnected and automated, the reliability of the signals they depend upon becomes increasingly critical to mission success.

For decades, the security of these systems has focused primarily on protecting the digital information carried by those signals. Encryption safeguards confidential data, authentication verifies the identity of communicating systems, and integrity checks ensure that transmitted information has not been altered. These mechanisms remain essential components of modern cybersecurity architectures.

However, digital security mechanisms verify the integrity of data rather than the authenticity of the signal that delivers it. In many communication architectures, security checks are applied only after a received signal has been demodulated and decoded into digital information. As a result, a receiver may authenticate a message even when the signal carrying that message has been recorded, delayed, or retransmitted by an adversary. The data may remain cryptographically valid while the signal itself no longer represents a genuine real-time transmission.

This discrepancy between data authenticity and signal authenticity can be described as the signal trust gap. The signal trust gap arises because most communication systems authenticate decoded data while implicitly assuming that the received signal itself is a genuine transmission.

Addressing this challenge may require extending cybersecurity beyond conventional data authentication to include evaluation of the signal waveform itself. By analyzing the temporal behavior and physical characteristics of incoming signals before decoding them, receivers may be able to determine whether a transmission is consistent with a continuously generated signal.

This paper introduces the concept of the signal trust gap and explores how signal-level trust evaluation could strengthen the resilience of aerospace communication, navigation, and autonomous systems.

Working Principle

Trust evaluation should begin at the waveform level when the authenticity of the signal-generation process affects system safety, timing, navigation, or command execution.

Trust the signal before trusting the data

2. The Signal Trust Gap

2.1 The Traditional Cybersecurity Model

Modern cybersecurity frameworks were designed primarily for protecting digital information. Within this model, the central objective is to ensure that data arriving at a system satisfies three core properties: confidentiality, integrity, and authenticity.

Confidentiality prevents unauthorized parties from reading information during transmission. Integrity ensures that the content of a message has not been altered. Authentication verifies that the sender of the message is who they claim to be.

These principles have proven highly effective for protecting data exchanged between computers and networks. Encryption protocols such as TLS, secure messaging standards, and digitally signed communications are now widely deployed across both civilian and defense infrastructure.

However, the traditional model implicitly assumes that the physical process of signal transmission is trustworthy. It focuses on verifying the digital information extracted from the signal rather than the signal generation process itself.

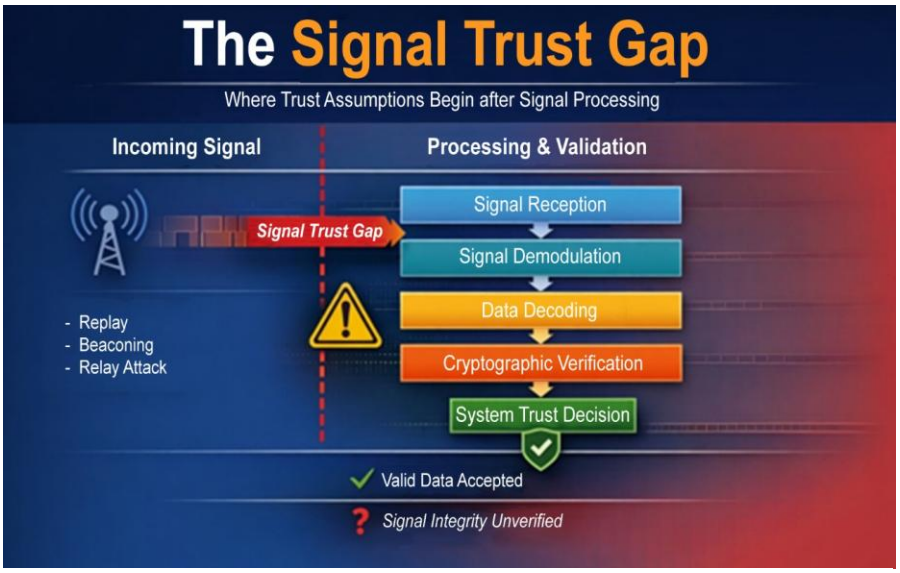

Figure 1. *Traditional receiver processing commonly evaluates trust after demodulation and decoding, leaving the waveform-generation process insufficiently verified*

In many cyber-physical systems, this assumption no longer holds.

Signals used by aerospace platforms often travel through open environments where adversaries may intercept, manipulate, or retransmit them. Under such conditions, it becomes possible for an attacker to exploit the difference between data authenticity and signal authenticity.

2.2 When Valid Data Does Not Mean a Valid Signal

Consider a scenario in which an adversary records a legitimate signal transmitted by an authorized system. The recorded signal is then retransmitted later, without any modification to the digital data it carries.

From the perspective of conventional cybersecurity controls, nothing appears suspicious. The message remains cryptographically valid. Authentication checks pass. Integrity checks confirm that the data has not been altered.

Yet the signal itself may be misleading because it no longer represents the real-time state of the system that originally transmitted it.

This type of attack is known as a replay attack.

In other words, the system verifies that the message is correct, but it cannot verify that the signal delivering the message is genuine in time.

2.3 The Expanding Threat Landscape

The importance of this vulnerability is growing as aerospace and cyber-physical systems become increasingly reliant on external signals for decision making. Navigation receivers rely on satellite transmissions to compute position. Autonomous vehicles rely on remote sensor networks and communication links to coordinate actions. Distributed command systems depend on remote signals to authorize and execute operations.

One widely studied example is meaconing, a form of attack against satellite navigation systems leading to incorrect position calculations [1,2]. In a meaconing attack, an adversary receives legitimate navigation signals from satellites and retransmits them with a delay. The receiving navigation system interprets the delayed signals as if they were genuine transmissions from the satellites, leading to incorrect position calculations.

Because the navigation messages themselves remain authentic, traditional authentication mechanisms cannot detect the deception [1,2,4].

Similar vulnerabilities exist in command-and-control systems. A recorded command signal may be retransmitted at a later time, potentially triggering unintended actions. In distributed sensing systems, previously transmitted sensor data may be replayed to create a false perception of environmental conditions.

These attacks exploit a simple fact: most systems have no direct way to determine whether a signal is being generated live or merely replayed.

2.4 The Limits of Protocol-Level Freshness

Engineers have long recognized the replay problem, and many communication protocols attempt to mitigate it through mechanisms designed to enforce message freshness. These mechanisms often include timestamps, sequence numbers, nonces, and challenge-response exchanges [4].

While useful, these approaches introduce their own limitations. Freshness mechanisms rely on assumptions about clock synchronization, system state, and communication latency. They can be disrupted by network delays, packet loss, or timing jitter. In complex distributed systems, maintaining consistent timing across nodes becomes increasingly difficult.

Furthermore, many aerospace signals-particularly navigation and broadcast signals-are not structured as interactive protocols. They are continuous transmissions intended to be received by many users simultaneously. Incorporating protocol-style freshness mechanisms into such signals can be impractical or inefficient.

Even when freshness mechanisms are present, carefully engineered replay attacks may remain within acceptable timing tolerances. An attacker who rebroadcasts signals with small delays may still deceive receivers that expect some degree of timing uncertainty.

2.5 Physical-Layer Security Approaches

Recognizing the limitations of digital and protocol-level defenses, researchers have explored techniques for evaluating signals at the physical layer. These approaches attempt to identify characteristics of the transmitted waveform that indicate the identity of the transmitter or the authenticity of the transmission.

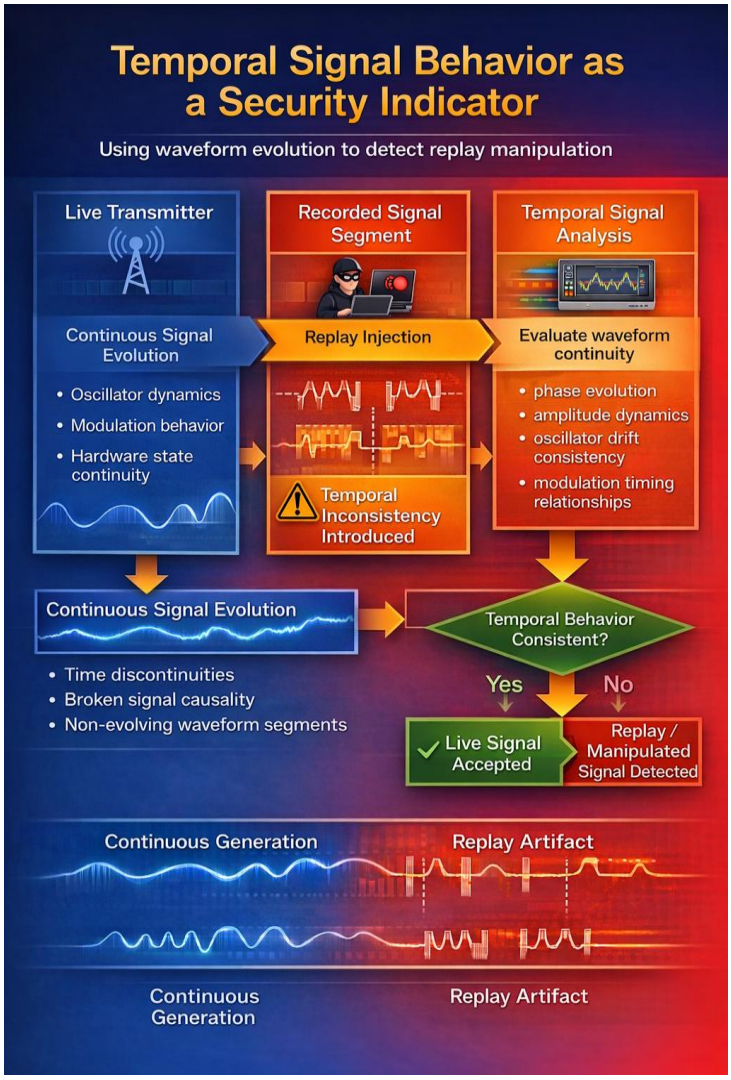

Figure 2. *Temporal behavior provides a signal-level indicator that can help distinguish continuously generated transmissions from replayed, delayed, or synthesized signals.*

Examples include RF fingerprinting, angle-of-arrival estimation, signal strength analysis, and channel-state measurements [7-9].

While these methods provide valuable tools for detecting certain types of interference or impersonation, they also face significant challenges.

Many physical-layer characteristics depend heavily on environmental conditions such as multipath propagation, atmospheric effects, and receiver location. These factors introduce variability that complicates reliable identification.

Moreover, many physical-layer techniques rely on relatively static features of transmitter hardware. As signal generation technologies improve, adversaries are increasingly able to replicate or imitate these characteristics [9-11].

These limitations suggest that a more robust approach to signal authenticity may require examining not only instantaneous signal properties, but also how signals evolve over time.

3. Signal-Level Trust Evaluation

3.1 The Importance of Temporal Behavior

Signals generated by physical systems exhibit dynamic behavior. The waveform observed at a receiver is not merely a static pattern but the result of a continuous process unfolding in time.

When a signal is recorded and replayed, the waveform itself may appear identical, but the underlying generative process has been removed. The signal is no longer evolving according to the same physical dynamics that produced it originally.

If a receiver can analyze the temporal evolution of a signal and determine whether it behaves consistently with a continuously generated process, it may be possible to detect replayed or manipulated signals even when the digital data they carry remains valid.

This concept introduces the notion of temporal authenticity as a security property [14]

3.2 A New Security Principle

Conventional communication systems treat signals primarily as carriers of digital information. A received waveform is demodulated, decoded, and converted into data before security mechanisms evaluate whether the message is authentic. This sequence implicitly assumes that the signal itself represents a legitimate real-time transmission. In signal-dependent cyber-physical systems, that assumption may no longer be sufficient. An alternative approach evaluates the authenticity of the signal before trusting the information it carries.

By examining the temporal behavior and physical characteristics of the waveform prior to decoding, receivers may be able to determine whether a transmission is consistent with a continuously generated signal from a legitimate source. In this model, the signal itself becomes an object of security evaluation. Only after the signal passes this initial trust evaluation does the system proceed to decode and interpret the data it contains.

By introducing a signal-level trust evaluation stage, systems gain the ability to detect forms of deception that would otherwise bypass traditional cybersecurity controls. The concept of evaluating signal authenticity before data decoding can be represented as a modified receiver architecture in which waveform-level trust assessment precedes conventional demodulation and cryptographic verification.

3.3 Physics-Based Evaluation of Signal Authenticity

Implementing signal trust evaluation requires examining the physical characteristics of the waveform itself rather than relying solely on the digital data extracted from it. In traditional communication receivers, the primary goal of signal processing is to recover encoded information as efficiently and accurately as possible. However, from a security perspective, the waveform contains additional information about how the signal was generated and transmitted. By analyzing these physical properties, a receiver can evaluate whether the signal behaves in a manner consistent with a genuine, continuously generated transmission.

One approach involves reconstructing a high-fidelity representation of the received waveform from digitized samples. Modern receivers already perform high-resolution sampling and digital signal processing to recover modulation and timing information. The same data can also be used to reconstruct a representation of the waveform that preserves its temporal structure and dynamic behavior. This representation allows the receiver to analyze how the signal evolves over time rather than examining isolated signal features.

These observables may include characteristics such as phase progression, amplitude dynamics, frequency drift, modulation timing, and other temporal relationships embedded in the signal. Importantly, these properties are often influenced by the physical processes inside the transmitter, including oscillator stability, modulation control loops, and hardware timing mechanisms [7,8].

Because these processes operate continuously, the resulting waveform typically exhibits a coherent pattern of evolution over time. Successive portions of the signal are not independent; instead, they are connected by underlying physical dynamics that govern how the transmitter produces the waveform. These relationships can be expressed through observables that capture how the signal changes from one moment to the next.

When a signal is replayed, delayed, or artificially synthesized, this natural continuity may be disrupted. A replayed signal, for example, represents a recording of a past transmission rather than a signal being generated in real time. Although the waveform may initially appear identical to the original transmission, its temporal context has been altered. Similarly, signals produced by artificial synthesis systems may replicate certain static features of legitimate transmissions while failing to reproduce the deeper temporal relationships associated with continuous generation [9,11].

If such manipulation occurs, the relationships between the extracted observables may deviate from the patterns expected of a live signal. For instance, phase evolution may exhibit discontinuities, frequency drift may behave inconsistently with oscillator dynamics, or modulation timing may appear detached from the natural progression expected in a real transmission. These deviations may be subtle and may not affect the decoded digital data, yet they can provide important clues about the authenticity of the signal.

By evaluating these deviations, the receiver can compute a quantitative measure of signal trust before relying on the information the signal carries [14]. This trust metric may reflect how closely the observed temporal behavior of the waveform aligns with the expected characteristics of signals generated by legitimate transmitters operating under normal conditions. Signals that exhibit strong temporal consistency may be assigned higher trust values, while signals that show significant deviations from expected patterns may be flagged for additional scrutiny or rejection.

As communication systems become more complex and adversaries develop increasingly sophisticated methods of signal manipulation, approaches that leverage the underlying physics of signal generation may play an important role in strengthening the resilience of cyber-physical systems. By combining waveform analysis with conventional cryptographic and protocol-based protections, future receiver architectures may be better equipped to distinguish authentic signals from deceptive ones.

Finally, autonomous systems may use signal trust metrics as part of supervisory decision logic. If incoming signals fall below defined trust thresholds, the system may switch to alternate navigation modes, rely more heavily on onboard sensors, or transition into safe operational states.

The implications of signal-level trust evaluation extend across multiple aerospace mission domains.

Timing distribution networks are another critical domain. Many communication systems, financial networks, and infrastructure platforms depend on accurate timing derived from external signals. Detecting delayed timing transmissions could prevent cascading synchronization errors.

Signal-level analysis may also strengthen command and control links used by spacecraft, unmanned aerial vehicles, and distributed defense platforms. Detecting replayed or relayed commands can prevent unintended system behavior.

Navigation receivers represent one of the most visible use cases for signal trust evaluation. Because satellite navigation signals propagate across large distances and arrive with very low power levels, they are especially vulnerable to spoofing and relay attacks.

3.4 Introducing Signal-Level Trust Evaluation

In traditional receiver designs, signals are rapidly processed through demodulation and decoding stages so that the embedded data can be interpreted and validated. However, by the time the signal has been converted into digital data, much of the contextual information about how the waveform was generated and transmitted has already been discarded. Introducing a signal-level trust evaluation stage preserves the opportunity to analyze this information before it is lost.

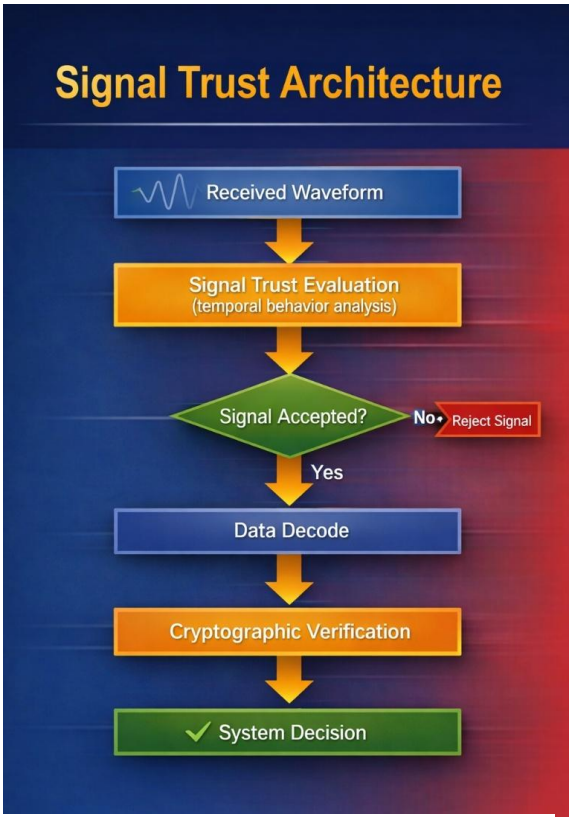

Figure 3. *A receiver can evaluate signal trust before data decoding and cryptographic validation, enabling earlier rejection or escalation of suspicious signals.*

Within this extended architecture, the receiver performs an initial assessment of the waveform immediately after signal capture and digitization. Instead of proceeding directly to demodulation and decoding, the system evaluates characteristics of the waveform that reflect the dynamics of the transmitter and the physical transmission process. These characteristics may include timing relationships within the waveform, phase and frequency evolution, modulation continuity, and other temporal features that naturally arise when signals are generated by a live transmitter operating in real time.

The underlying premise is that signals produced by functioning communication systems exhibit patterns of continuous temporal behavior that are tied to the internal dynamics of the hardware and control processes that generate them. Oscillators drift gradually, modulation states evolve according to protocol timing, and signal generation mechanisms follow predictable physical constraints. When signals are captured and replayed, or when synthetic signals are generated to imitate legitimate transmissions, these natural temporal relationships may become inconsistent or disrupted.

By examining these patterns across time, receivers may identify deviations that suggest the signal is no longer part of a continuously generated transmission.

When a signal is captured and replayed, these natural relationships may be partially disrupted. Even when the waveform appears identical over short intervals, subtle inconsistencies may emerge when longer temporal segments are analyzed.

For example, oscillator phase typically evolves gradually rather than discontinuously. Modulation states transition according to defined timing patterns, and hardware control loops introduce characteristic drift and stability behaviors.

Signals generated by physical transmitters evolve through time according to the dynamics of oscillators, modulation circuits, and control systems. These processes create continuous relationships between successive portions of the waveform.

By analyzing these properties before data decoding occurs, the receiver gains the ability to detect anomalies that may not be visible in the decoded data itself. Replay attacks, delayed retransmissions, and certain forms of signal synthesis can introduce subtle inconsistencies in timing, waveform continuity, or signal evolution.

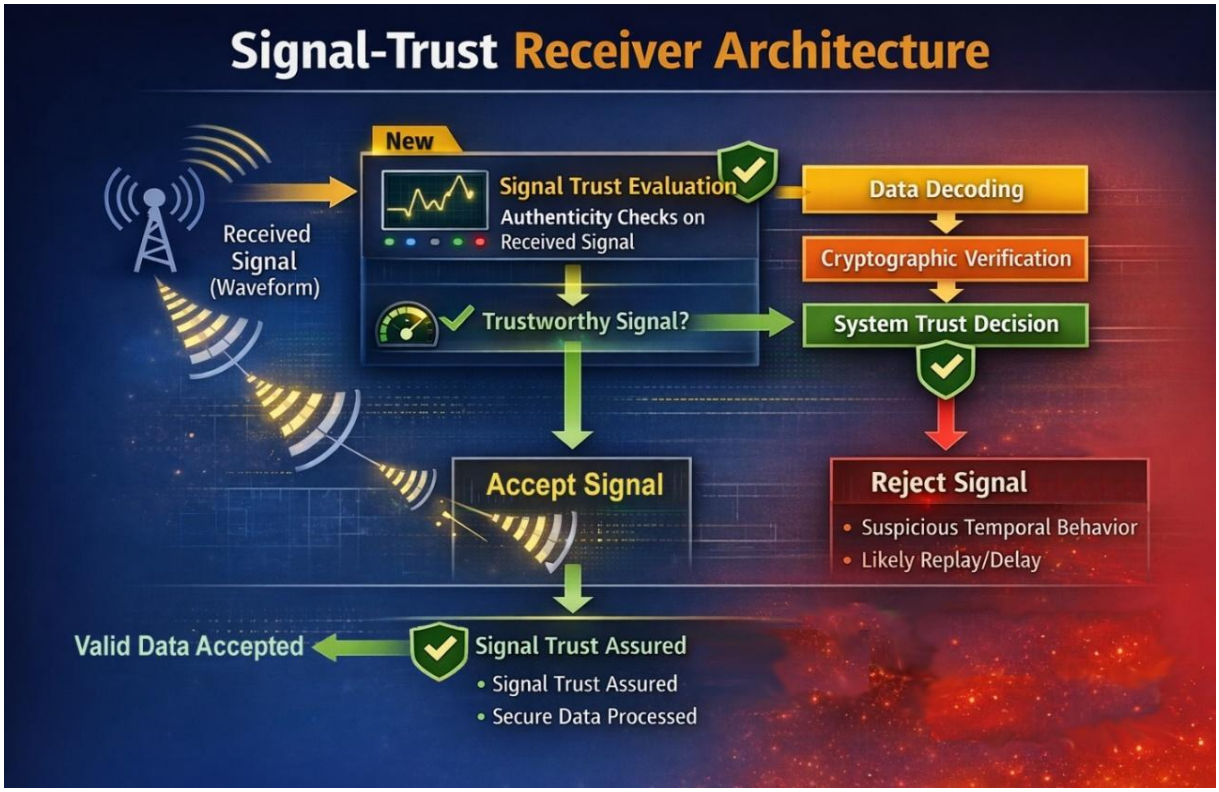

Figure 4. *Signal-level trust assessment can be integrated into the receiver chain as a preprocessing layer before data interpretation.*

The conceptual placement of signal-level trust evaluation within a receiver processing chain is illustrated in the associated figure.

The layered relationship between cryptographic protection, protocol safeguards, system monitoring, and signal-level trust evaluation is illustrated conceptually in the associated figure,

While these inconsistencies may not alter the digital message content, they can reveal that the signal does not reflect a genuine real-time transmission.

Importantly, signal-level trust evaluation is not intended to replace conventional security mechanisms such as cryptographic authentication or protocol validation. Instead, it functions as an additional layer of protection that complements existing safeguards. Cryptographic mechanisms ensure that message content has not been altered and that it originates from an

authorized source, while signal-level analysis evaluates whether the physical signal carrying that message behaves in a manner consistent with a legitimate transmission.

In this way, the receiver gains a broader perspective on signal authenticity. Rather than relying solely on the validity of decoded data, the system also considers whether the signal itself exhibits the temporal characteristics expected from a live transmitter. Integrating this evaluation step into the receiver architecture can therefore provide an early indication of potential signal manipulation, allowing the system to reject suspicious signals or apply additional scrutiny before they influence higher-level decision processes.

4. Aerospace and Cyber-Physical Applications

4.1 Applications in Aerospace Systems

Signal-level trust evaluation has significant implications for aerospace systems that depend on externally transmitted signals. Aerospace platforms routinely depend on signals that originate from distant transmitters, including navigation satellites, command stations, sensor nodes, and other vehicles operating within a coordinated network. Because these signals frequently guide critical functions such as navigation, timing, and command execution, ensuring their authenticity becomes an essential element of system security.

By incorporating signal-level trust evaluation into receiver architectures, aerospace systems gain the ability to assess not only whether a signal carries valid data but also whether the signal itself behaves like a genuine real-time transmission. This additional layer of verification can help address vulnerabilities that arise when attackers exploit the physical signal environment rather than the digital data content.

One of the most immediate applications appears in navigation systems, which rely on externally transmitted signals to determine position, velocity, and timing. Systems such as satellite-based navigation receivers continuously process signals that originate from remote transmitters and propagate across large distances before reaching the platform. In traditional designs, the receiver focuses primarily on extracting navigation data and verifying message integrity. With signal-level trust evaluation, the receiver could also analyze the temporal behavior of the incoming waveform to determine whether it is consistent with a live satellite transmission. Such analysis may help detect replayed, delayed, or artificially generated navigation signals, potentially reducing vulnerability to spoofing and meaconing attacks that attempt to manipulate a platform's perceived position.

Signal trust evaluation can also enhance the security of command and control systems used in spacecraft, unmanned aerial vehicles, and distributed defense platforms. These systems depend on command signals transmitted from authorized control stations to direct vehicle actions and mission operations. In a replay or relay attack, an adversary may capture a legitimate command transmission and retransmit it at a later time or from a different location. Because the digital content of the command remains unchanged, conventional authentication mechanisms may still validate the message. By evaluating the temporal behavior of the received waveform, however, the receiver may be able to determine whether the signal reflects a real-time transmission from the control station or a replayed signal originating elsewhere. This capability can help prevent previously issued commands from being used to trigger unintended actions.

Another important application arises in timing distribution networks, which play a crucial role in many aerospace systems. Precise timing signals are used to synchronize navigation systems, communication networks, sensor arrays, and onboard computing processes. If an attacker can delay or replay a timing signal, the resulting shift in system clocks may propagate through the network and disrupt coordinated operations. Signal-level trust evaluation allows receivers to examine whether timing signals exhibit the temporal continuity expected from a genuine transmission. By detecting delayed or manipulated timing signals, systems may be able to prevent subtle clock offsets that could otherwise degrade navigation accuracy or disrupt synchronized operations.

Distributed sensor networks also stand to benefit from this approach. Aerospace systems increasingly rely on networks of sensors that share environmental measurements and situational awareness data across multiple platforms. These networks may include radar systems, remote sensing satellites, ground-based monitoring stations, and onboard sensors distributed across multiple vehicles. If adversaries capture and replay recorded sensor transmissions, they could potentially create a false representation of environmental conditions or threat activity. Incorporating signal-level trust evaluation into sensor receivers allows the system to assess whether incoming measurement streams originate from genuine real-time observations or from previously recorded signals. This capability can improve the reliability of situational awareness systems and reduce the risk of misleading sensor inputs.

The implications are particularly significant for autonomous platforms, which depend heavily on remote signals to guide their behavior. Autonomous aircraft, spacecraft, and cooperative vehicle swarms often integrate navigation signals, sensor data, and communication inputs directly into their decision-making algorithms. Because these systems must respond rapidly and often operate without continuous human supervision, they may be especially vulnerable to deceptive signals that appear authentic. By incorporating signal trust evaluation into supervisory control logic, autonomous platforms can assess the reliability of incoming signals before acting upon them.

Across these applications, signal-level trust evaluation introduces a new dimension to aerospace security by extending trust assessment into the physical signal domain. Instead of assuming that incoming signals represent genuine transmissions, systems gain the ability to evaluate whether the waveform itself behaves in a manner consistent with the dynamics of a legitimate transmitter. As aerospace systems continue to become more interconnected and increasingly dependent on remote signals, this capability may play an important role in enhancing the resilience of future aerospace architectures.

4.2 GNSS Spoofing and Meaconing in the Real World

Despite the sophistication of GNSS technology, the signals themselves are extremely weak by the time they reach the Earth's surface. This physical reality makes them susceptible to interference and manipulation by relatively modest equipment [1,2].

One of the earliest and most well-known classes of attack against GNSS systems is meaconing. In a meaconing attack, an adversary captures legitimate navigation signals and retransmits them with a delay. Because the navigation receiver assumes that the signals are arriving directly from the satellites, the introduced delay alters the calculated distance to the satellites and therefore the computed position.

From the receiver's perspective, the signals appear authentic. The navigation messages themselves remain unchanged, and cryptographic authentication-where present-may still validate the message contents. The receiver therefore has little reason to suspect that the signals are being manipulated.

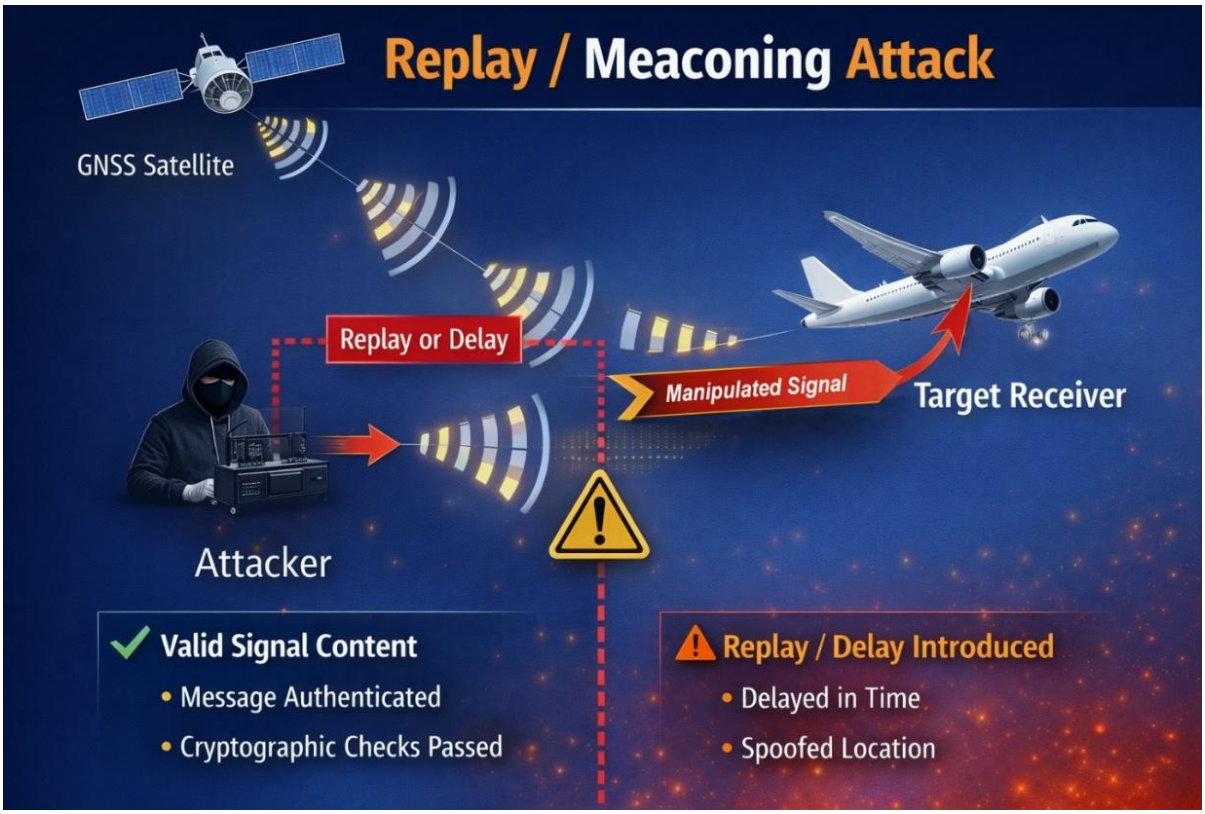

Figure 5. A delayed rebroadcast of valid navigation signals can preserve message authenticity while altering the receiver's inferred position or timing state.

In practice, this type of attack can cause a navigation receiver to compute an incorrect position while still believing that the system is functioning normally.

Over the past decade, researchers and security analysts have demonstrated numerous GNSS spoofing scenarios that exploit this vulnerability [1,2,5]. In several controlled experiments, spoofing transmitters have successfully induced navigation receivers to report positions that gradually drift away from their true location. In other demonstrations, receivers have been caused to report sudden position changes or to lock onto entirely fabricated satellite signals.

One widely discussed incident occurred in the maritime domain, where vessels operating in certain regions reported GNSS positions that placed them several kilometers inland [6]. Investigations suggested that spoofed navigation signals were responsible for the anomalous positions observed by multiple ships simultaneously.

The implications of such attacks extend beyond navigation alone. Many critical systems-including telecommunications networks, financial systems, and power grids-rely on GNSS signals for precise timing synchronization. Manipulating these signals can therefore affect infrastructure far beyond the immediate navigation receiver.

4.3 Signal Relay and Command Channel Manipulation

Navigation systems are not the only aerospace systems vulnerable to signal replay or relay attacks. Command and control links used by spacecraft, unmanned aerial vehicles, and distributed defense systems may face similar risks.

In a command relay attack, an adversary intercepts legitimate command signals transmitted from an authorized control station. The adversary then retransmits those signals through a separate transmitter, potentially introducing delays or modifying the spatial origin of the signal.

Because the digital content of the command remains unchanged, conventional authentication mechanisms may still validate the command. The receiving system therefore interprets the signal as a legitimate instruction from the authorized source.

Such attacks can allow adversaries to manipulate system behavior without breaking encryption or forging credentials. Instead, they exploit the system's inability to verify that the command signal was generated at the expected time and location.

In distributed sensor networks, replay attacks may be used to create false situational awareness. Recorded sensor data streams can be retransmitted to suggest environmental conditions that no longer exist, potentially misleading autonomous systems that rely on those sensors for decision making.

These scenarios highlight the broader challenge facing cyber-physical systems. Signals often carry both data and implicit information about the state of the system that generated them. When signals are replayed or manipulated in time, that implicit information is lost, yet conventional security mechanisms rarely detect the discrepancy.

In most communication systems, incoming signals pass through several processing stages before the underlying data is evaluated or acted upon by the system. This sequence can be illustrated using a simplified flow diagram, that represents the basic operations performed by a receiver as it converts an electromagnetic waveform into meaningful digital information.

The process begins when the receiver captures the incoming radio-frequency waveform through its antenna and front-end electronics. These components amplify the signal, filter unwanted frequencies, and convert the analog waveform into a form suitable for further processing. The signal is then digitized using analog-to-digital converters, allowing digital signal processing algorithms to extract the modulation structure and encoded data contained within the waveform.

Once digitized, the receiver performs several signal processing steps such as synchronization, carrier recovery, demodulation, and decoding. These operations reconstruct the transmitted data bits from the modulated waveform and organize them into packets, frames, or command messages according to the communication protocol being used.

Only after the data has been successfully decoded does the system typically apply higher-level security checks. These checks may include cryptographic authentication, message integrity verification, or protocol-level validation procedures designed to ensure that the data originates from an authorized source and has not been altered during transmission.

This sequence implicitly assumes that the signal itself is trustworthy. In other words, the system focuses its security checks on the decoded digital content rather than on the physical signal that

carried that content to the receiver. The receiver verifies the authenticity of the message, but it does not necessarily verify the authenticity of the signal as a real-time transmission.

The vulnerability emerges because replayed or delayed signals can traverse the signal processing chain without modifying the underlying data content. If an adversary captures a valid transmission and later retransmits the same waveform, the receiver may demodulate and decode the signal exactly as it did during the original transmission. Since the digital message remains unchanged, the cryptographic verification process may still confirm that the message is authentic.

By the time authentication checks are performed, however, the system has already lost the opportunity to examine whether the signal's temporal behavior is consistent with a genuine transmission. Information about when and how the signal was originally generated may no longer be available once the waveform has been reduced to a stream of decoded data bits.

In this traditional architecture, trust is therefore evaluated only after the signal has been converted into digital data. Any deception technique that preserves the encoded data-such as replay attacks, relay attacks, or delayed retransmissions-may pass through the system undetected because the receiver is verifying message authenticity rather than signal authenticity.

4.4 Replay Attack Illustration

In most communication systems, incoming radio signals pass through a sequence of processing stages before their data is interpreted by the receiving system. The antenna and front-end electronics capture the electromagnetic waveform and convert it into a digitized signal that can be processed by digital signal processing algorithms. The receiver then performs synchronization, carrier recovery, demodulation, and decoding operations to reconstruct the transmitted data. Only after these steps are completed are higher-level security mechanisms-

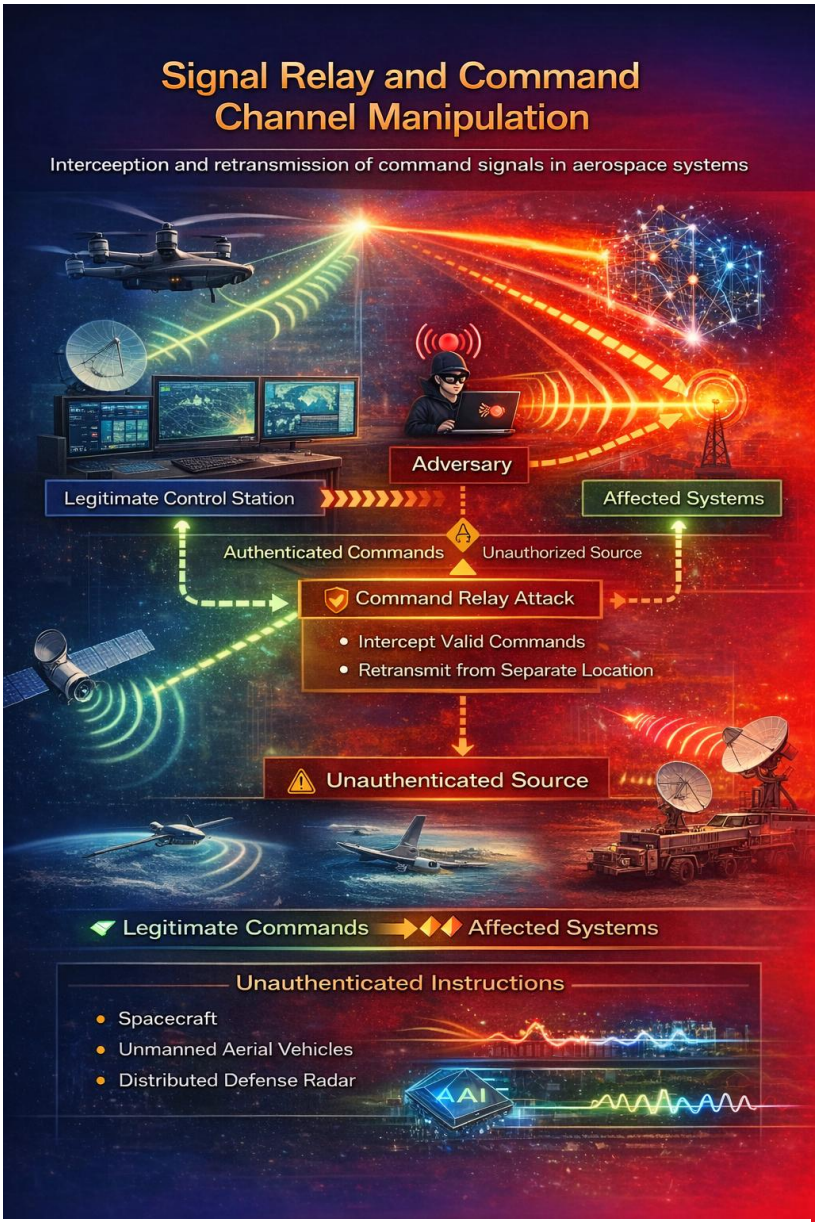

Figure 6. *Command relay attacks can exploit a receiver's inability to determine whether an authenticated command signal was generated live by an expected source.*

such as cryptographic authentication or protocol validation-typically applied to the decoded message. This architecture implicitly assumes that the received signal itself represents a legitimate real-time transmission. As a result, a signal that has been recorded and later retransmitted may pass through the signal processing chain unchanged. Because the encoded data remains intact, the receiver may demodulate and authenticate the message successfully even though the signal no longer reflects a genuine transmission from the original source.

4.5 Implications for Future Aerospace Architectures

As aerospace systems evolve toward greater autonomy and interconnectivity, the signals that guide their operation will become even more central to mission performance and system safety. Modern aerospace platforms increasingly rely on continuous streams of external information to determine position, maintain situational awareness, coordinate operations, and execute commands. Navigation systems provide position and velocity estimates, sensor networks supply environmental and threat information, and communication links connect distributed vehicles with one another and with command authorities.

In many emerging architectures, these signals are not merely advisory inputs but foundational elements that influence real-time decision making. Autonomous aircraft, spacecraft, and distributed defense platforms often incorporate external signals directly into control loops, guidance algorithms, and collaborative coordination mechanisms. As a result, the reliability and authenticity of the signals that feed these systems become critical determinants of system behavior.

In such environments, the distinction between a valid signal and a deceptive one may determine the success or failure of a mission. A navigation signal that appears legitimate but carries manipulated timing information could shift a vehicle's perceived position. A spoofed command signal could redirect an unmanned platform or disrupt coordinated actions among multiple vehicles. Even subtle manipulations in sensor data streams could cause autonomous systems to misinterpret environmental conditions, potentially leading to degraded performance or unsafe decisions.

The challenge becomes particularly significant in contested or adversarial environments, where signals may be intentionally manipulated as part of electronic warfare or cyber-physical attack strategies. In these contexts, adversaries may attempt to exploit the reliance of aerospace systems on remote signals by injecting deceptive transmissions that imitate legitimate communications or sensor outputs. Because many existing systems primarily verify the digital content of messages rather than the physical authenticity of the signals themselves, these attacks may bypass conventional cybersecurity safeguards.

Future aerospace architectures may therefore incorporate mechanisms for evaluating signal authenticity at earlier stages of the signal processing chain. Rather than relying solely on cryptographic verification of decoded data, receivers may analyze the physical properties of incoming waveforms to determine whether they are consistent with signals generated by legitimate transmitters. Techniques that examine temporal behavior, waveform continuity, and dynamic signal evolution could provide additional indicators of authenticity that are difficult for adversaries to replicate convincingly.

These approaches represent a shift toward physics-informed security, in which the physical characteristics of signals and devices become part of the system's trust evaluation framework [7,10,14]. By integrating waveform-level analysis with traditional digital security mechanisms, aerospace systems can evaluate both the integrity of message content and the authenticity of the signal that carries it. This layered approach helps ensure that even if a deceptive signal contains valid data, inconsistencies in its physical behavior may reveal the manipulation.

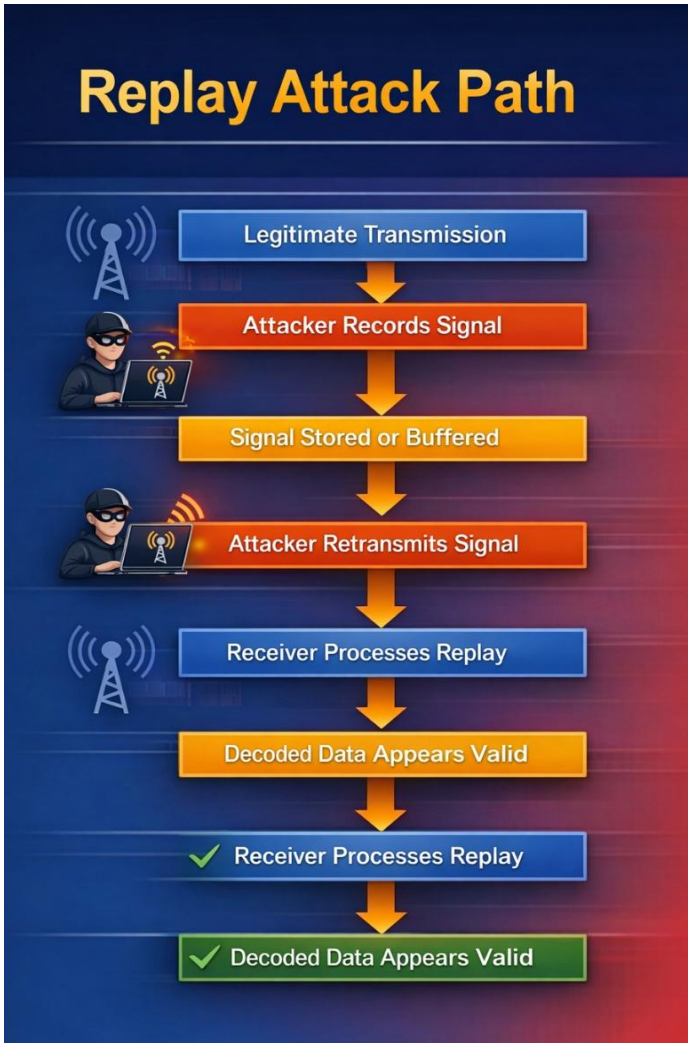

Figure 7. A valid signal can be recorded, stored, retransmitted, decoded, and authenticated while no longer representing a genuine real-time transmission.

Incorporating signal-level verification capabilities into future architectures may also influence the design of autonomous decision-making systems. Platforms could assess the trustworthiness of incoming signals before incorporating them into navigation algorithms, sensor fusion processes, or mission planning decisions. When signal authenticity falls below a defined threshold, systems might switch to alternative sensing modalities, rely on internal navigation methods, or enter safe operational states until signal integrity can be restored.

Ultimately, combining digital cybersecurity with signal-aware analysis moves aerospace engineering toward a new generation of resilient systems. Such architectures acknowledge that information delivered through physical signals carries both digital content and contextual information about the process that generated it. By evaluating both aspects, engineers can develop systems that maintain trust even when operating in complex, contested, or adversarial environments.

As aerospace networks continue to expand and autonomous technologies become more widespread, the ability to distinguish authentic signals from deceptive ones will become a foundational requirement for operational resilience. Systems that can evaluate signal authenticity across multiple layers-physical, protocol, and digital-will be better equipped to maintain reliable performance and mission success in the increasingly sophisticated threat environments of the future.

5. Emerging Adversary Capabilities

5.1 Security in an Era of AI and Quantum Computing

The need for stronger signal authentication is becoming increasingly urgent as emerging technologies reshape the broader cybersecurity landscape. Two particularly transformative developments-artificial intelligence and quantum computing-are beginning to influence both the defensive and offensive sides of cyber-physical security. While these technologies promise significant benefits for communication systems and aerospace operations, they also introduce new challenges that may weaken traditional security assumptions.

Advances in quantum computing may eventually affect the foundations of modern cryptographic security. Many widely deployed cryptographic systems rely on mathematical problems that are computationally difficult for classical computers to solve. Certain quantum algorithms, however, have the potential to solve some of these problems more efficiently. If large-scale quantum computers become practical, some currently used encryption and digital signature systems could become vulnerable.

The cybersecurity community is actively developing post-quantum cryptographic algorithms designed to resist attacks from both classical and quantum computers [12.13]. These new cryptographic standards are intended to provide long-term protection for digital communications. However, transitioning global infrastructure to new cryptographic systems will require significant time and coordination. Aerospace platforms, satellite systems, and other long-lived infrastructure may operate for decades, making rapid updates to cryptographic algorithms difficult in practice.

In this evolving technological environment, security architectures that rely solely on digital cryptography may face increasing pressure [10]. While cryptographic protections remain essential for safeguarding message integrity and confidentiality, they do not address all potential vulnerabilities-particularly those involving manipulation of the physical signal environment. Attackers may exploit weaknesses in how signals are transmitted, received, or interpreted without necessarily breaking the underlying cryptographic algorithms.

Signal-level trust evaluation offers a complementary layer of protection that operates independently of the specific cryptographic mechanisms used to protect message content. Rather than focusing exclusively on the validity of decoded data, signal-level analysis evaluates whether the waveform itself behaves like a genuine transmission generated by a legitimate system. By examining temporal relationships, waveform continuity, and other dynamic signal properties, receivers may detect manipulations that leave digital data unchanged.

This approach introduces a form of physics-based security [7,14], in which the authenticity of signals is evaluated using the physical principles that govern signal generation and transmission. Because these characteristics arise from the dynamics of real hardware and communication processes, reproducing them convincingly-particularly in real time-may be significantly more difficult than simply replicating digital message content.

By verifying the physical authenticity of signals themselves, systems gain an additional defense against both present and emerging forms of cyber deception. Even if future adversaries use advanced artificial intelligence to generate highly realistic signals, or exploit weaknesses in

digital cryptography, signal-level trust evaluation can provide an independent method for assessing whether the received waveform reflects a genuine real-time transmission.

As aerospace and communication systems become increasingly dependent on remote signals and interconnected networks, combining digital cryptography with physics-based signal verification may form the basis of more resilient security architectures. In an era shaped by rapid advances in artificial intelligence and quantum computing, layered approaches that integrate multiple forms of trust evaluation will likely become essential for protecting critical cyber-physical infrastructure.

5.2 Autonomous Systems and AI-Enabled Signal Deception

Advances in artificial intelligence are accelerating the development of tools capable of generating highly realistic synthetic communication signals. Machine learning models trained on large datasets of signal waveforms can learn the statistical properties of legitimate transmissions, including modulation patterns, spectral signatures, and channel characteristics. Once trained, these systems may be able to synthesize signals that closely imitate authentic transmissions produced by real transmitters [11].

These capabilities raise the possibility of AI-assisted spoofing, in which adversaries generate signals specifically designed to deceive receivers [11]. Instead of relying solely on recorded signals or simple signal generators, attackers may be able to produce synthetic waveforms that adapt dynamically to the behavior of the target system. Such systems could potentially observe how a receiver processes incoming signals and adjust their transmissions in real time to maintain the appearance of authenticity.

As these techniques mature, systems that rely primarily on static signal characteristics-such as fixed spectral signatures or known modulation formats-may become increasingly vulnerable [9,11]. Protocol-level checks that validate message structure or communication rules may also be insufficient to distinguish between authentic signals and AI-generated imitations. If an attacker can replicate both the digital content and many observable signal properties, traditional detection methods may struggle to identify the deception.

The rapid expansion of autonomous and semi-autonomous systems in aerospace introduces an additional dimension to the signal trust problem. Modern aerospace platforms increasingly depend on automated decision-making systems to perform tasks that were once managed exclusively by human operators. These systems rely on continuous streams of external information to perceive their environment, assess conditions, and guide their behavior in real time.

Autonomous platforms often integrate multiple sources of incoming signals into their operational frameworks. Navigation signals provide estimates of position, velocity, and timing. Distributed sensor networks contribute information about surrounding conditions, threats, or mission targets. Communication links coordinate actions between multiple vehicles, satellites, or command centers operating across large geographic areas. Together, these signals form the informational foundation upon which autonomous systems build their situational awareness.

Unlike human operators, autonomous systems must make decisions continuously and frequently within extremely short time intervals. Guidance algorithms, sensor fusion systems, and control loops often operate on timescales measured in milliseconds or microseconds.

Because of these rapid decision cycles, the reliability and authenticity of incoming signals become critically important. The system must interpret signals and act on them almost immediately, often without the opportunity for extended verification or human oversight.

A misleading signal that appears authentic can therefore have significant consequences. If a navigation signal contains deceptive information, an autonomous platform may adjust its estimated position or trajectory in response. A manipulated sensor signal may cause the system to misinterpret its environment, potentially altering mission priorities or triggering incorrect responses. Similarly, deceptive communications between platforms could disrupt coordination among multiple vehicles or misdirect collaborative operations.

As autonomy increases, the potential impact of deceptive signals may become even more severe. Many modern control architectures incorporate external signals directly into their decision-making processes. Navigation inputs may feed directly into flight control systems, sensor data may drive automated threat responses, and communication signals may influence coordinated maneuvers between platforms. When these signals are trusted implicitly, adversaries may be able to influence system behavior indirectly by manipulating the signals that inform those control algorithms.

In such scenarios, an attacker does not necessarily need to compromise the internal software or hardware of the autonomous system itself. Instead, the attacker may attempt to manipulate the external signals that the system relies upon for guidance and coordination. If those signals are accepted as authentic, the system may unknowingly incorporate the deceptive information into its internal decision processes.

The increasing sophistication of artificial intelligence technologies introduces additional complexity to this challenge. Machine learning models can be trained on large collections of signal data to learn the statistical properties and patterns associated with legitimate transmissions. These models can then generate signals that imitate many of the observable characteristics of real communications, including modulation structures, spectral signatures, and channel effects.

Such capabilities raise the possibility of AI-driven signal synthesis, in which adversaries generate signals specifically designed to deceive receivers. Rather than relying solely on recorded transmissions, attackers could potentially produce adaptive signals that evolve dynamically to resemble legitimate transmissions. These synthetic signals might replicate known signal characteristics closely enough to bypass traditional detection methods that rely on static signal features.

In a highly autonomous aerospace environment, this evolving threat landscape highlights the need for more advanced methods of evaluating signal authenticity. Systems that depend heavily on external signals must be able to assess whether those signals reflect genuine real-time transmissions or artificially generated imitations. Approaches that examine deeper properties of signal behavior-such as temporal continuity and dynamic evolution-may offer one avenue for strengthening trust evaluation in such environments [14].

As autonomous aerospace systems become more capable and more widely deployed, ensuring the integrity of the signals that guide their behavior will become an increasingly important component of system resilience. Protecting these systems will likely require integrating traditional cybersecurity mechanisms with new forms of signal-aware analysis that can detect deception even when signals appear superficially authentic.

Artificial intelligence technologies are accelerating the ability of adversaries to exploit this vulnerability. Modern machine learning models can generate signals that imitate many characteristics of legitimate transmissions. Neural networks trained on large signal datasets can reproduce modulation patterns, spectral signatures, and channel characteristics with remarkable accuracy.

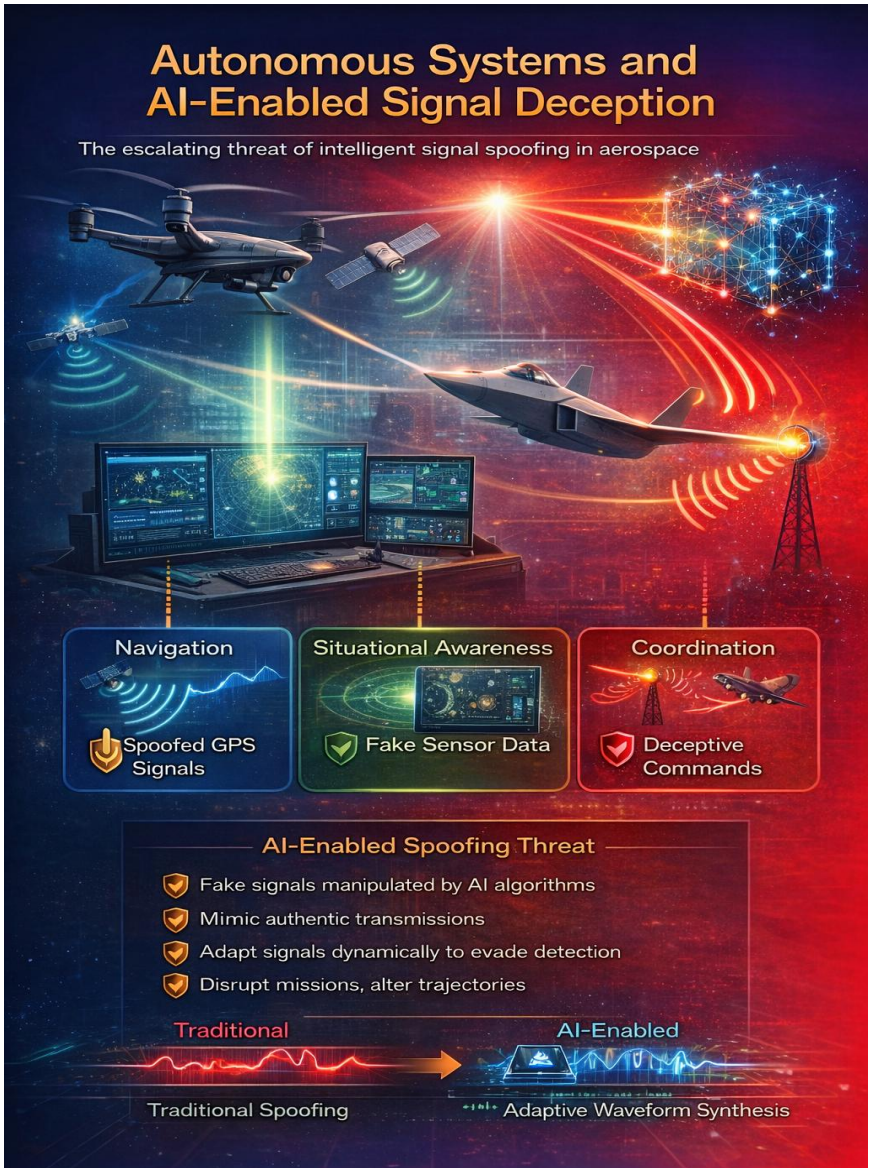

Figure 8. *Autonomous platforms may require signal-level trust metrics to reduce reliance on spoofed or AI-synthesized external inputs.*

These capabilities are already being explored in research environments for applications such as adaptive waveform generation and intelligent communications systems. The same techniques could potentially be adapted to generate spoofed signals designed to deceive receivers.

In traditional spoofing attacks, adversaries often rely on recorded signals or relatively simple signal generators. AI-driven signal synthesis introduces the possibility of adaptive spoofing, in which generated signals evolve dynamically to imitate legitimate transmissions.

Such systems may be capable of observing the behavior of a target receiver and adjusting transmitted signals in real time to maintain the appearance of authenticity.

This evolving threat environment raises important questions about how autonomous systems evaluate trust in the signals they receive. If signals can be synthesized to mimic static transmitter

characteristics or replicate known modulation patterns, receivers must rely on deeper properties of signal behavior to detect deception.

Temporal authenticity analysis offers one potential approach. Because continuously generated signals reflect the internal dynamics of the systems that produce them, reproducing those dynamics convincingly in real time may be significantly more difficult than imitating static signal properties.

For autonomous systems, incorporating signal trust evaluation into decision-making architectures may provide an additional layer of resilience. Rather than accepting external signals at face value, autonomous platforms could assess the consistency and temporal behavior of those signals before incorporating them into control algorithms.

In practice, this may allow systems to reduce reliance on potentially compromised signals, switch to alternative sensing modalities, or transition to safe operational states when signal trust falls below acceptable thresholds.

As aerospace systems become more autonomous and increasingly dependent on remote signals, the ability to distinguish between authentic and deceptive signals will become a key component of operational resilience.

6. Security Architecture, Standards, and Certification

6.1 Toward Resilient Cyber-Physical Infrastructure

As aerospace systems continue to evolve toward greater autonomy and connectivity, security must extend beyond the protection of digital information alone.

Figure 9. *Signal-level trust evaluation complements cryptographic protection, protocol security, and system-level monitoring rather than replacing them.*

The signals that carry that information represent the interface between the digital world and the physical world. Ensuring the authenticity of those signals is therefore essential for protecting the integrity of cyber-physical systems.

Future resilient architectures will likely combine multiple layers of protection, including digital cryptography, protocol-level safeguards, system-level monitoring, and physics-based signal authentication [10].

Together, these mechanisms can provide a more comprehensive framework for defending against attacks that exploit the gap between digital data validity and signal authenticity.

6.2 Security Architecture, Standards, and Certification Considerations

The integration of signal authenticity evaluation into aerospace systems also raises important questions regarding system architecture, standards, and certification.

Aerospace systems are subject to rigorous design and verification requirements intended to ensure safety, reliability, and interoperability. Communication and navigation systems in particular must adhere to well-established standards governing signal formats, protocols, and operational performance.

Introducing new mechanisms for evaluating signal authenticity therefore requires careful consideration of how such mechanisms interact with existing system architectures and regulatory frameworks.

Figure 10. *A resilient architecture combines signal-level analysis, system monitoring, protocol mechanisms, and cryptographic protection.*

One important architectural principle is that signal-level authenticity mechanisms should complement rather than replace established cybersecurity controls. Encryption, authentication, and secure communication protocols remain essential for protecting digital information. Signal-level evaluation introduces an additional layer of assurance focused on verifying the physical authenticity of transmissions.

Often, this layer may operate transparently alongside existing systems. Signal authenticity evaluation can be implemented within receiver processing chains without altering the structure of transmitted data or requiring modifications to communication protocols. This approach allows new security capabilities to be introduced incrementally while maintaining compatibility with existing infrastructure.

Standards organizations and regulatory bodies are already addressing related challenges as aerospace systems evolve toward greater autonomy and connectivity. Navigation authentication

schemes are being introduced to strengthen trust in satellite navigation signals [3,4]. Post-quantum cryptographic standards are being developed to prepare for future advances in computing technology [12,13]. Security frameworks for cyber-physical systems are being refined to address the unique challenges posed by interconnected infrastructure.

An example of this trend is the Galileo Open Service Navigation Message Authentication (OSNMA) capability, which provides cryptographic authentication of navigation messages. While OSNMA strengthens confidence in message origin and integrity, it does not by itself establish that a received waveform represents a genuine real-time transmission, illustrating the distinction between message authentication and signal authenticity [3].

Signal authenticity evaluation aligns with these broader efforts by addressing vulnerabilities that exist at the intersection of physical signal transmission and digital information processing.

From a certification perspective, implementing such mechanisms would require demonstrating that signal authenticity evaluation improves system resilience without introducing unacceptable complexity or failure modes. This may involve extensive testing under realistic operational conditions, including controlled replay and spoofing scenarios designed to evaluate detection performance.

Over time, as the importance of signal trust becomes more widely recognized, it is possible that standards organizations will incorporate signal authenticity considerations into future system specifications. Just as encryption and authentication have become standard features of modern communication systems, mechanisms for evaluating the temporal authenticity of signals may eventually become a standard component of secure cyber-physical architectures.

7. Conclusion

The evolution of aerospace systems is steadily increasing their dependence on external signals. Navigation receivers determine position from satellite transmissions. Distributed sensing architectures rely on remote data streams to construct a picture of the operating environment. Command and control systems coordinate actions across platforms separated by vast distances. Autonomous vehicles depend on these signals to guide decisions that must often be made within fractions of a second.

For decades, cybersecurity strategies have focused on protecting the digital information carried by these signals. Encryption and authentication mechanisms have proven indispensable for ensuring that messages remain confidential and unaltered during transmission. Yet the growing complexity of cyber-physical systems has revealed a fundamental limitation in this approach. Digital security mechanisms verify the accuracy of data, but they do not necessarily verify the authenticity of the signal that delivered that data.

The consequences of this vulnerability are particularly significant in aerospace environments. Navigation systems may compute incorrect positions if satellite signals are rebroadcast with carefully introduced delays [1.2.5]. Command receivers may accept replayed instructions that appear authentic at the data level. Distributed sensor networks may incorporate outdated or manipulated measurements into operational decisions. As systems become more autonomous, these forms of deception may influence control algorithms directly, amplifying their potential impact.

In this evolving environment, protecting cyber-physical systems requires more than verifying the integrity of digital information. It requires establishing trust in the signals themselves.

One promising direction involves evaluating signals at the waveform level before decoding the data they contain [7,14]. By examining the temporal behavior of a signal-how it evolves over time-it may be possible to determine whether the signal is consistent with a live, continuously generated transmission. Evaluating signals at the waveform level therefore introduces a new dimension of trust in cyber-physical systems. By assessing the authenticity of the transmission process itself, receivers may detect deception even when the digital data appears valid.

Rather than assuming that the signal carrier is trustworthy and focusing solely on the data extracted from it, systems can assess the authenticity of the transmission process itself. Only signals that exhibit characteristics consistent with genuine generation are allowed to influence higher-level system decisions.

This approach does not replace traditional cybersecurity mechanisms. Encryption, authentication, and protocol safeguards remain essential components of secure communication architectures. Instead, signal authenticity evaluation provides an additional layer of defense-one that addresses vulnerabilities arising at the boundary between the physical and digital domains [10,14].

As aerospace systems become more interconnected and increasingly autonomous, the importance of signal trust will continue to grow. Navigation, timing, communications, and sensing infrastructures will all depend on signals whose authenticity must be evaluated under increasingly complex and contested conditions.

In doing so, future aerospace systems may achieve a deeper and more robust form of trust-one grounded not only in the correctness of data, but also in the physical reality of the signals upon which those systems depend.

In future cyber-physical systems, resilient security architectures may need to verify not only the authenticity of digital data, but also the authenticity of the signals that deliver it.

References

[1] M. L. Psiaki and T. E. Humphreys, “GNSS Spoofing and Detection,” Proceedings of the IEEE, vol. 104, no. 6, pp. 1258–1270, 2016.

[2] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O’Hanlon, and P. M. Kintner Jr., “Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer,” Proceedings of the ION GNSS Conference, 2008.

[3] European Union Agency for the Space Programme (EUSPA), “Galileo Open Service Navigation Message Authentication (OSNMA) Service Definition Document,” Issue 1.4, 2025.

[4] M. Yuan et al., “Authenticating GNSS Civilian Signals: A Survey,” Satellite Navigation, vol. 4, no. 1, 2023.

[5] F. Rothmaier, Y.-H. Chen, S. Lo, and T. Walter, “A Framework for GNSS Spoofing Detection Through Combinations of Metrics,” IEEE Transactions on Aerospace and Electronic Systems, vol. 57, no. 6, pp. 3923–3938, 2021.

[6] International Civil Aviation Organization (ICAO), “GNSS Interference and Mitigating Measures,” ICAO Navigation Systems Panel Working Paper, 2024.

[7] N. Xie, Z. Li, and H. Tan, “A Survey of Physical-Layer Authentication in Wireless Communications,” IEEE Communications Surveys & Tutorials, vol. 23, no. 1, pp. 282–310, 2021.

[8] V. Brik, S. Banerjee, M. Gruteser, and S. Oh, “Wireless Device Identification with Radiometric Signatures,” Proceedings of ACM MobiCom, pp. 116–127, 2008.

[9] L. Alhoraibi, A. Al-Hasan, and M. Younis, “Physical Layer Authentication in Wireless Networks Based on Machine Learning: A Survey,” Sensors, vol. 23, no. 3, 2023.

[10] National Institute of Standards and Technology (NIST), “Framework for Cyber-Physical Systems,” NIST Special Publication 1500-201, 2017.

[11] Z. Wang et al., “Advancing RF Sensing with Generative AI: From Synthetic Data to Foundation Models,” Connected and Autonomous Systems, vol. 2, no. 1, 2025.

[12] National Institute of Standards and Technology (NIST), “FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard,” Federal Information Processing Standards Publication 203, 2024.

[13] National Institute of Standards and Technology (NIST), “FIPS 204: Module-Lattice-Based Digital Signature Standard,” Federal Information Processing Standards Publication 204, 2024.

[14] C. M. Hymel, “Systems and Methods for Latency-Reduced Authenticity-Sensing Acquisition,” Patent-Pending Technical Disclosure, 2026.

Appendix A. Key Terms

Term	White Paper Usage
Signal trust gap	The discrepancy between the authenticity of decoded digital data and the authenticity of the physical signal that delivered that data.
Signal-level trust evaluation	A receiver-side assessment of waveform behavior before decoded data is accepted as trustworthy.
Temporal authenticity	The property that a signal behaves consistently with a live, continuously generated transmission process.
Replay attack	An attack in which a valid signal or message is recorded and later retransmitted to trigger unintended trust or system behavior.
Meaconing	A navigation-focused replay or relay attack in which legitimate navigation signals are rebroadcast with delay, leading to position or timing errors.
Protocol-level freshness	A message freshness mechanism using timestamps, nonces, sequence numbers, or challenge-response exchanges.
Physics-informed security	A security approach that evaluates physical properties of signals, devices, or environments as part of the trust model.
Trust metric	A quantitative or qualitative indicator representing whether a signal appears consistent with expected live-transmission behavior.

Appendix B. Figure Inventory

Figure	Title	Purpose
Figure 1	The Signal Trust Gap	Traditional receiver processing commonly evaluates trust after demodulation and decoding, leaving the waveform-generation process insufficiently verified.
Figure 2	Temporal Signal Behavior as a Security Indicator	Temporal behavior provides a signal-level indicator that can help distinguish continuously generated transmissions from replayed, delayed, or synthesized signals
Figure 3	Signal Trust Architecture	A receiver can evaluate signal trust before data decoding and cryptographic validation, enabling earlier rejection or escalation of suspicious signals.
Figure 4	Signal-Trust Receiver Architecture	Signal-level trust assessment can be integrated into the receiver chain as a preprocessing layer before data interpretation.

Figure	Title	Purpose
Figure 5	Replay / Meaconing Attack	A delayed rebroadcast of valid navigation signals can preserve message authenticity while altering the receiver's inferred position or timing state.
Figure 6	Signal Relay and Command Channel Manipulation	Command relay attacks can exploit a receiver's inability to determine whether an authenticated command signal was generated live by an expected source.
Figure 7	Replay Attack Path	A valid signal can be recorded, stored, retransmitted, decoded, and authenticated while no longer representing a genuine real-time transmission.
Figure 8	Autonomous Systems and AI-Enabled Signal Deception	Autonomous platforms may require signal-level trust metrics to reduce reliance on spoofed or AI-synthesized external inputs.
Figure 9	Layered Cyber-Physical Security Model	Signal-level trust evaluation complements cryptographic protection, protocol security, and system-level monitoring rather than replacing them.
Figure 10	Toward Multi-Layer Signal Security	A resilient architecture combines signal-level analysis, system monitoring, protocol mechanisms, and cryptographic protection.