GPS (Global Position Satellite) is playing a mission-critical role in driving innovation and digital transformation in aviation.

The reliance on GPS (Global Position Satellite) in airport operations underscores the importance of understanding and mitigating the associated risks and threats. Airports must take a proactive approach to safeguard critical functions to ensure the safety and efficiency of their operations.

Understanding the risks and threats associated with GPS within mission-critical airport services is crucial. Airports rely heavily on GPS technology for various essential functions, and any disruption or compromise of GPS signals can have serious consequences.

GPS Spoofing: GPS spoofing can mislead aircraft regarding their exact positions during takeoff, landing, or taxiing.

GPS Jamming: Deliberate interference or blocking of GPS signals can cause loss of GPS functionality. For aircraft relying on GPS for navigation or landing, this can pose significant safety risks.

Loss or Incorrect GPS Time Synchronization: Airport operations interconnected systems (ATC Servers, Ticketing, Baggage Handling, Security, etc.) rely on accurate GPS synchronized time sources to ensure smooth and efficient operations.

Understanding the landscape

GNSS (Global Navigation Satellite System) is a generic term that refers to a group of satellite navigation systems that provide global coverage for navigation and positioning applications. GPS (Global Positioning System), on the other hand, is a specific satellite navigation system developed and operated by the United States government.

The key difference between GNSS and GPS is that GPS is a subset of GNSS. While GPS is the most widely recognized and used satellite navigation system, other GNSS systems exist as well, including GLONASS (Russia), Galileo (Europe), BeiDou (China), and NavIC (India).

In terms of functionality, GNSS and GPS operate on the same basic principle of triangulation, in which signals from multiple satellites are used to determine the precise location of a receiver. However, because GNSS includes multiple satellite systems, it is generally more reliable and accurate than GPS alone, particularly in areas with limited satellite visibility or interference.

In practice, many modern devices and applications use multiple GNSS systems simultaneously to achieve the highest accuracy and reliability possible. This approach, known as multi-constellation positioning, allows devices to combine signals from multiple satellite systems to reduce errors, improve accuracy, and increase overall reliability.

GPS Communications

The satellite-based Global Positioning System (GPS) uses microwave radio signals in various frequency bands. The primary GPS frequency bands used for communication between GPS satellites and GPS receivers on the ground are as follows:

- **L1 Frequency Band:** The L1 frequency band is used for the primary civilian GPS signal. It operates at approximately 1575.42 MHz (megahertz) and is used for essential positioning and navigation.

The L1 signal carries Coarse/Acquisition (C/A) code, which provides lower accuracy but is accessible to the general public.

- **L2 Frequency Band:** The L2 frequency band operates at around 1227.60 MHz. It originally carried the Precision (P) code, intended for military use. However, modernized GPS signals use the L2 band for the more accurate L2C civilian signal, which offers improved accuracy for commercial users.

- **L5 Frequency Band**: The L5 frequency band operates at around 1176.45 MHz. This frequency is used for the L5 signal, intended for aviation and other high-precision applications. The L5 signal improves accuracy and reliability, making it suitable for safety-critical applications.

- **L-band and Other Frequencies**: Besides the primary L1, L2, and L5 frequency bands, some GPS systems use additional frequencies in the L-band, such as the L3, L4, and L6 bands. These additional frequencies are used for specialized purposes and are less widely used than the leading frequency bands.

It's important to note that while these frequencies are associated with the original GPS constellation operated by the United States, other global navigation satellite systems (GNSS) like GLONASS, Galileo, and BeiDou also operate in similar frequency bands for their own positioning and navigation signals.

Understanding GPS Risks and Threats

Understanding the risks and threats associated with GPS within mission-critical airport services is crucial. Here are some key considerations regarding the risks and threats to GPS in airport operations:

- **Navigation and Aircraft Guidance:** GPS is fundamental for aircraft navigation and landing procedures, including precision approaches and runway alignments. Any interference or disruption in GPS signals can lead to incorrect navigation data, affecting the safety of flights during takeoff, landing, and taxiing.

- **Airport Ground Operations:** Airports use GPS for various ground operations, such as vehicle tracking, runway maintenance, and air traffic control. Any disruption of GPS signals can lead to inefficiencies, delays, and potential safety hazards on the ground.

- **Security Vulnerabilities:** GPS can be vulnerable to intentional interference, such as jamming and spoofing. Jamming involves broadcasting radio signals on the same frequencies as GPS satellites, disrupting the reception of GPS signals. Spoofing involves sending counterfeit GPS signals to deceive receivers. Both can pose significant security risks..

- **Communication Systems:** Many communication and surveillance systems used at airports rely on GPS time synchronization. Disruptions in GPS signals can affect the accuracy and reliability of these systems.

- **Emergency Response:** GPS is essential for emergency response and search-and-rescue operations at airports. Any disruption in GPS signals can hinder the ability to locate and respond to emergencies effectively.

- **Technology Dependency:** As airports become increasingly reliant on GPS technology, the potential consequences of GPS disruptions or vulnerabilities grow more severe. It's essential to have backup systems and redundancy in place to mitigate risks.

- **Regulatory Compliance:** Regulatory bodies like the Federal Aviation Administration (FAA) have specific requirements regarding the use of GPS in aviation. Non-compliance can result in safety violations and legal issues.

- **Cybersecurity:** Protecting GPS systems from cyber threats is critical. Unauthorized access to GPS infrastructure or control systems could lead to vulnerabilities and potential disruptions.

To mitigate risks and threats, airports should consider the following measures:

- **Redundancy:** Implement redundant navigation and communication systems to ensure continued operations even during GPS disruptions.
- **Security Measures:** Employ security measures to protect against jamming, spoofing, and cyber threats. Regularly update and patch GPS equipment and systems.
- **Monitoring and Detection:** Use monitoring and detection systems to promptly identify any interference or anomalies in GPS signals.
- **Training:** Train personnel to recognize and respond to GPS-related issues effectively.
- **Regulatory Compliance:** Ensure compliance with aviation and cybersecurity regulations related to GPS use.
- **Emergency Response Plans**: Develop and test emergency response plans that account for potential GPS disruptions.

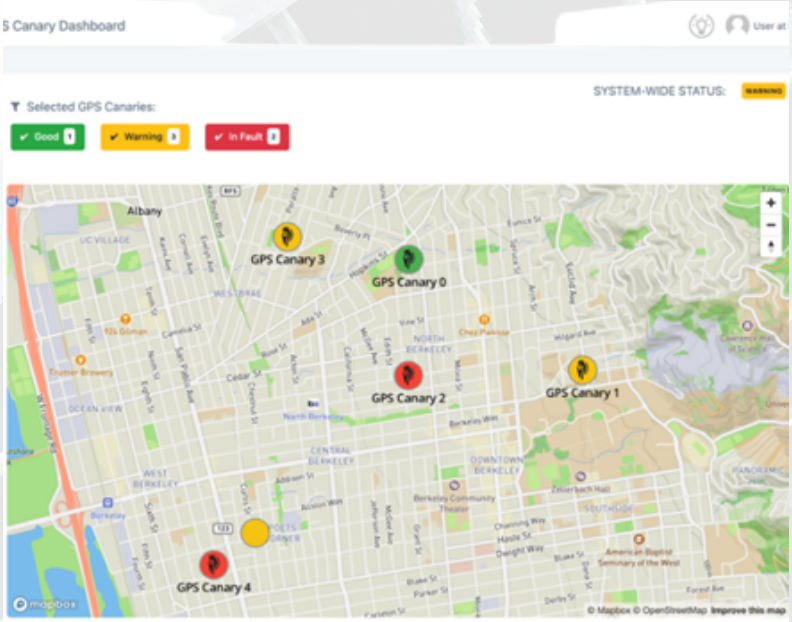
The reliance on GPS in airport operations underscores the importance of understanding and mitigating the associated risks and threats. Airports must take a proactive approach to safeguard critical functions and ensure the safety and efficiency of their operations.

To mitigate these threats, technologies like AirShield GPS Canary can serve as an early warning system, detecting RF jamming and/or spoofing, thereby ensuring your systems remain operational even amidst GPS attacks.

Additionally, 7x24 monitoring of the GPS threat landscape can help identify and respond to potential GPS-related security incidents.

AirShield(™) GPS Canary Key Features

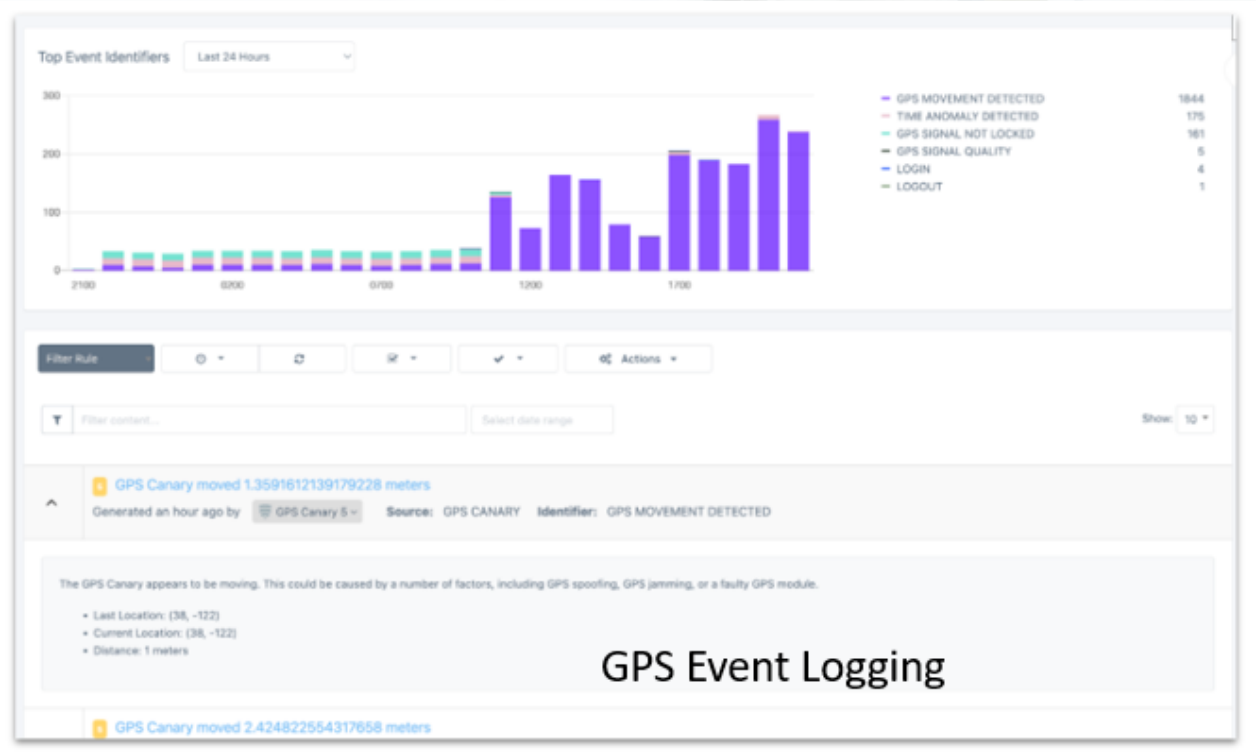
- **Decode L1 satellites:** GPS L1 C/A, QZSS L1 C/A L1S, GLONASS L1OF, BeiDou B1I/B1C, Galileo E1B/C, SBAS L1 C/A: WAAS, EGNOS, MSAS, GAGAN.
- **Monitor for deviation** in calculated location and/or time (Spoofing, Meaconing)
- **Monitor state changes:** Signal loss, Signal Lock, Jamming, Spoofing, Online, Offline.
- **Present epoch-based history** of events observed across all GPS Canaries on a centralized cloud dashboard

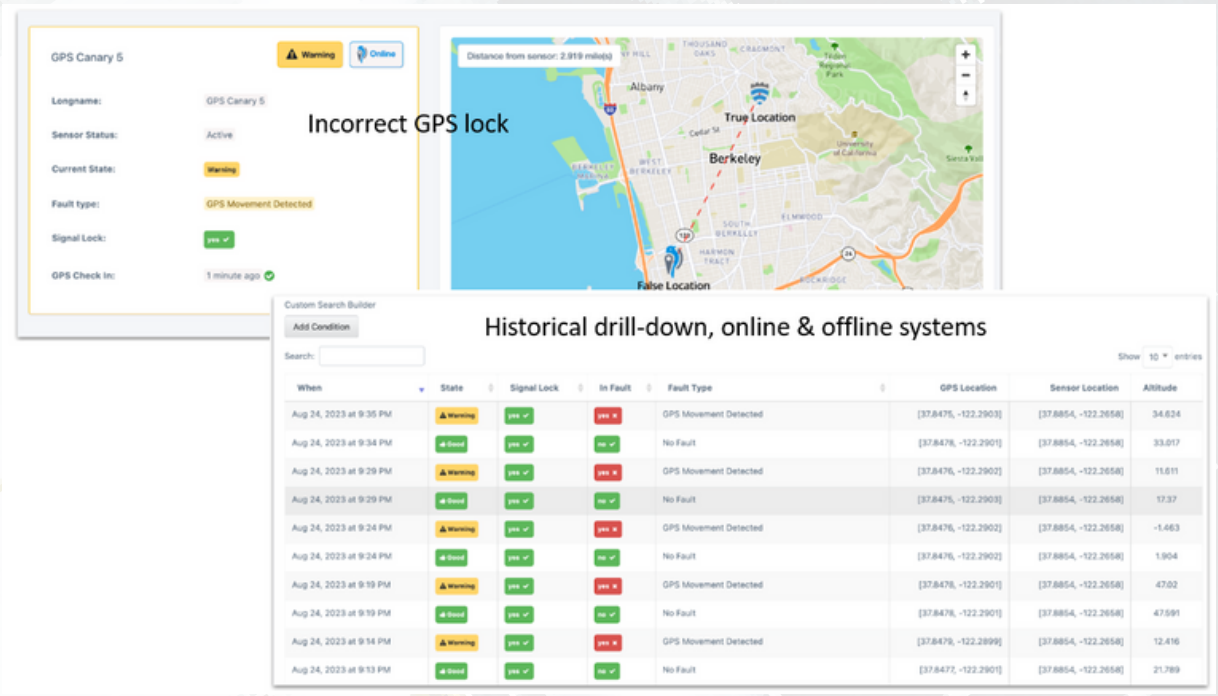


Detect GPS Jamming and Spoofing

- **Forwarding of events** to third-party logging and incident response platforms through our Notification and API system.
- **Big screen dashboard** of GPS Canary health
  - Provides current and historical health of the immediate area for GPS reception.
  - Help to narrow locations with impacted operations due to signal faults.

GPS Event Logs





About LOCH

LOCH is a global leader in wireless threat monitoring.

LOCH's flagship product, AirShield(™), provides actionable threat intelligence across LTE/4G/5G, broad-spectrum IoT, Bluetooth/BLE, Wi-Fi, and GPS (Global Position Satellite) to detect, access, and mitigate RF risks, helping organizations improve their security posture and reduce risk. AirShield leverages AI-driven artificial intelligence and machine learning to respond to all RF threats in real-time.