Executive Summary

As the GPS satellites themselves have evolved over the years, so have the systems that allow operators to take the benefit of satellite navigation. SPACEKEYS presents the ultimate evolution of GNSS RAIM prediction solution. It provides for worldwide RAIM predictions for all aircraft types and for all navigation and surveillance specifications. Integration of Honeywell capabilities based on avionics actual performance will enhance the operational benefits to customers.
Black Box Design Solution

One solution for ALL users.

- Airlines
- Flight Planning
- Business Jets
- General Aviation
- Weather
- Flight Following

- CAAs
- ANSPs
- Airports

- GPS-Galileo Working Group C
- Industry Collaboration
RAIM Pro: Requirements (GNSS Receivers)

The RAIM solution performs predictions for all currently known receiver types in commercial aviation. This includes receivers compliant with TSO-C129, TSO-C196 and TSO-C145/146. The system is Future Ready For Multi-Constellation Receivers and Advanced Horizontal RAIM.

The following GNSS receiver parameters are supported:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Options</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm</td>
<td>FD or FDE</td>
<td>The option „On only on Failure“ provides the user the possibility to apply BA only in case the RAIM prediction resulted in an outage excluding BA. This is only available in the Spacekeys RAIM prediction solution.</td>
</tr>
<tr>
<td>Barometric Aiding</td>
<td>ON, OFF or ON only on Failure</td>
<td></td>
</tr>
<tr>
<td>Selective Availability</td>
<td>ON or OFF</td>
<td></td>
</tr>
<tr>
<td>Mask Angle</td>
<td>-25° to 30°</td>
<td></td>
</tr>
<tr>
<td>HAL Multiplier</td>
<td>Any certified value</td>
<td>Some aircraft are certified to apply a horizontal alert limit bias during RAIM predictions.</td>
</tr>
</tbody>
</table>
RAIM Pro: Requirements (Navigation)

The RAIM solution performs predictions in compliance with the following navigation specifications. Terrain screening is performed as required for RNP AR predictions.

<table>
<thead>
<tr>
<th>FAA (U.S.A.)</th>
<th>RNAV 10</th>
<th>RNAV 5 Basic-RNAV</th>
<th>RNAV 2 US RNAV Type A</th>
<th>RNAV 1 P-RNAV US RNAV Type B</th>
<th>RNP 4</th>
<th>RNP 2</th>
<th>RNP 1</th>
<th>RNP Approach</th>
<th>RNP AR Approach</th>
<th>MNPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC 90-105A (replaces Order 8400.12C)</td>
<td>AC 90-96A</td>
<td>AC90-100A</td>
<td>AC90-100A</td>
<td>AC 90-105A (repl. order 8400.33)</td>
<td>AC90-105A</td>
<td>AC 90-105A</td>
<td>AC 90-105A</td>
<td>AC 90-105A (LNAV, LNAV/VNAV)</td>
<td>AC 90-107 (LP, LPV)</td>
<td>AC 90-101A AC20-138D</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EASA (EU, EFTA and other countries)</th>
<th>AMC 20-12</th>
<th>AMC 20-4A JAA TGL 2</th>
<th>AMC 20-16 JAA TGL 10</th>
<th>AMC 20-16 JAA TGL 10</th>
<th>AMC 20-16</th>
<th>AMC 20-27 (LNAV, LNAV/VNAV)</th>
<th>AMC 20-28 (LP, LPV)</th>
<th>AMC 20-26</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>CASA (Australia)</th>
<th>AC91.U-01 AC 91U-2(0) (replaces AC91U-II-B-2(0))</th>
<th>AC91.U-01 (replaces AC 91U-II-B-3(0))</th>
<th>AC91.U-01 (replaces AC 91U-II-B-3(0))</th>
<th>AC91.U-01 (replaces AC 91U-II-C-2(0))</th>
<th>AC91.U-01</th>
<th>AC91.U-01 (replaces AC 91U-II-C-3(0))</th>
<th>AC91.U-01 (replaces AC 91U-II-C-5 (LNAV))</th>
<th>AC 91U-II-C-5 (RNP AR)</th>
<th>AC91.U-01 (replaces AC 91-U-II-C-6)</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>SVRSOP (Latin America)</th>
<th>AC 91-001</th>
<th>AC 91-002</th>
<th>AC 91-003</th>
<th>AC 91-004</th>
<th>AC 91-005</th>
<th>AC 91-006</th>
<th>AC 91-008 (LNAV)</th>
<th>AC 91-010 (LNAV/VNAV)</th>
<th>AC 91-009</th>
</tr>
</thead>
</table>

| Transport Canada | AC 700-006 | AC 700-015 | AC 700-019 | AC 700-019 | AC 700-006 | AC 700-038 | AC 700-025 | AC 700-023 | AC 700-024 |
RAIM Pro: Requirements (Surveillance)

The RAIM solution performs predictions in compliance with the FAA ADS-B 2020 specification AC90-114B. As other Worldwide surveillance requirements are developed, the system will ensure all requirements are complied with.

---

Advisory Circular

Subject: Automatic Dependent Surveillance-Broadcast Operations
Date: 12/30/19
Initiated by: AFS-400
AC No: 90-114B
Change:

In May 2010, the Federal Aviation Administration (FAA) issued Title 14 of the Code of Federal Regulations (14 CFR) part 91, §§ 91.225 and 91.227. This rule requires Automatic Dependent Surveillance-Broadcast (ADS-B) Out performance when operating in designated classes of airspace within the U.S. National Airspace System (NAS) after January 1, 2020, unless authorized by air traffic control (ATC). This advisory circular (AC) provides users of the NAS guidance regarding how to conduct operations in accordance with §§ 91.225 and 91.227. The appendices in this AC provide guidance for additional operations enabled by ADS-B, including ADS-B In.

Robert C. Carty
Deputy Executive Director, Flight Standards Service
RAIM Pro: Core Features

• Real time integration with 3rd party systems, such as flight planning and flight following systems, using SOAP and/or REST APIs
  • API to request a location RAIM prediction for any airport with specific RNP levels
  • API to request a trajectory RAIM prediction for any trajectory of a flight

• Responsive Web UI
  • Manual ad-hoc operations including ad-hoc location predictions or route predictions
    • ICAO flightplan copy/paste
    • Interactive map
  • Save ad-hoc predictions for re-usage
  • Configure automated reports

• Customizable daily RAIM reports
  • Configure aircraft types/reg and GPS receivers
  • XML Flight Plan Import (e.g.: ARINC 633)
  • Full Worldwide area map display
  • Activity Log / RAIM Prediction History
  • Service Status Monitor
RAIM Pro: Core Features

• Terrain screening for RNP-AR operations
  • For RNP-AR approach procedures, potential obstruction of satellites by the surrounding terrain could affect RAIM availability. SPACEKEYS dynamic terrain screening engine analyzes the surrounding terrain for every RNP-AR request to ensure compliance with this requirement.

• Architecture / SLA
  • 99.95% system uptime.
  • New Almanac Processing within 2 minutes.
  • New NANU processing within 10 minutes.
  • 24/7 support.
Incidents of GNSS interference and jamming have increased dramatically over the last decade.
GNSS Interference / Jamming

Who is causing the interference/jamming and why?

• Perception by many individuals that GPS tracking technologies and being misused for nefarious purposes

• Increasing number of individuals are using easily accessible GPS jamming devices or concealing GPS jamming in everyday devices to prevent personal tracking by unknown persons/agencies
GNSS Interference / Jamming

Who is making and using these GNSS jamming devices?

- Growing community of ‘hacktivists’ are designing electronics and publishing ‘how-to’ documents
- With just a little Internet searching, a keen amateur electronics enthusiast can easily find the information on how to build a GPS jamming device
GNSS Interference / Jamming

Or...

- Simply buy a cheap Software Defined Radio (SDR) device
- Easy to configure
- Very little specialist knowledge needed
- ...
- With a little extra software programming, an SDR can be used to spoof GPS

**LimeSDR**
- Cost: $250 USD
- Frequency Range: 100 kHz to 3.8 GHz
- ADC Resolution: 12 Bits
- Max Bandwidth: 81 MHz
- TX/RX: TX and RX
- Processors: None
- Release Date: April 2016

The LimeSDR appears to be one of the "next generation" of experimenter focussed RX/TX capable SDR devices, it falls into a similar category as the HackRF and BladeRF. It was crowdfunded on Crowdsupply and at the time of writing this (January 2019) is in its initial production stages.

**ADALM PLUTO (PlutoSDR)**
- Cost: $299 USD (Base), $449 USD (Pro)
- Frequency Range: 320 – 3800 MHz (default), 70 - 6000 MHz (with firmware hack)
- ADC Resolution: 12 Bits
- Max Bandwidth: 20 MHz (default), 56 MHz (with firmware hack)
- TX/RX: TX and RX (Full Duplex)
- Processors: None
- Release Date: Mid 2017

The PlutoSDR is a low cost full duplex TX and RX receiver designed by the big alkron company Analog Devices. It is designed mostly for University students to use for learning about RF and SDR concepts, but it can also find use as a general purpose experimenter SDR.

**BladeRF**
- Cost: $430 USD (4G), $650 USD (11G)
- Frequency Range: 300 MHz – 3.6 GHz
- ADC Resolution: 12 Bits
- Max Bandwidth: 28 MHz
- TX/RX: TX and RX (Full Duplex)
- Processors: None
- Release Date: July 2013

Another TX and RX capable SDR is the BladeRF. The BladeRF has a smaller frequency range compared to the HackRF, but has a greater ADC resolution, larger maximum bandwidth and is capable of full duplex transmissions. It also uses USB 3.0 which is required to support the data rates needed for its wide bandwidth and 12 bit ADC. From the specs the BladeRF is a better receiver compared to the HackRF due to its larger ADC resolution, but it misses out on the frequencies below 300 MHz. Frequencies below 300 MHz can be received with a $200 transceiver add on board however.

**HackRF One**
- Cost: $299 USD
- Frequency Range: 1 MHz to 6 GHz
- ADC Resolution: 8 Bits
- Max Bandwidth: 20 MHz
- TX/RX: TX and RX (Half Duplex)
- Processors: None
- Release Date: April 2014

The HackRF One is one of the first "low cost" software defined radios that is capable of receiving and transmitting, although only in half duplex mode (cannot TX and RX simultaneously). It has received the most media attention out of any SDR and it seems to be marketed towards hackers and security researchers, but it should be just as capable for general ham or hobbyist users.
GNSS Spoofing

Cheap SDR Electronics Device

Freely available GPS receiver/emulator source code

A Little ‘Know-how’

GPS Interference, Jamming, or Spoofing
Internal GPS navigation or ‘GPS Coverage Extension’ is becoming more commonplace
  - Navigation in underground or covered environments
    - Carparks
    - Rail / Metro stations and tunnels
    - Large buildings

These systems do work, BUT ...
- GPS coverage extension ‘leakage’ is a known issue that can cause unintended GPS Spoofing
  - Tunnels, especially close to airports,
  - Runway underpass,
  - ...
GNSS Interference – What is being done to protect GNSS?

• Governments & Industry determined to combat GNSS interference, jamming and spoofing

• Jan 2021, US Presidential Memorandum – Space Policy Directive 7 (SPD7)
  • Clearly states that protecting GPS (and other GNSS) for use by all sectors, including aviation, is a priority
  • US DoT to play a lead role in order to meet SPD7 objectives

• SPACEKEYS are partnering with Honeywell to bring real-time GPS jamming and spoofing detection and alerting to the pilot and airline flight-ops.
  • US DoT have already expressed interest in our initiative and we are progressing future collaboration e.g. comparison of NOTAMs with real time detection
Honeywell Enhancements

Enhanced RAIM with Honeywell HIGH Step II – 100% RNP 0.1 Availability
- HIGH Step II Benefits
- Legacy Architectures
- Integration of Honeywell predictions with SPACEKEYS RAIM Pro

UNITYAir: GPS Threat Detection
- System Overview
- Integration of Honeywell Threat Detection with SPACEKEYS UNITYAir
- Value of Threat Detection
Upon entry into this RAIM hole just after $T = 15$ min, the GPS Receiver HIL instantly responds to the degraded satellite geometry.

The HIGH Step II integrity solution incorporates inertial measurements, resulting in a less abrupt reaction to the change in satellite geometry. In this case, the HIL increases slowly at the inertial drift rate.

Overall availability improvement for HIGH Step II users even during nominal satellite geometry changes which are much less severe than this example.

Coasting maintains RNP0.3NM required HIL for 18 min and RNP0.1NM required HIL for 9 min upon loss of GPS

Entry into RAIM Hole, often caused by setting of a Satellite in combination with an already degraded geometry (e.g. 2nd satellite offline for maintenance)
Honeywell: GPS Threat Detection Architecture

**Utilizing Existing ADIRU Install Base**
- Thousands of HON-equipped aircraft around the world
- Detection of GPS jamming and spoofing using data from certified avionics and Honeywell’s inertial system hybrid GPS/inertial algorithms

**Real Time Feedback From Live Flights**
- As individual aircraft encounter jam/spoof, they notify the ground infrastructure with details (e.g., 3D location, other details via ACARS).
- When/if jam/spoof clears, aircraft reports clearance of event.

**Ready When & Where You Need It**
- Metered API of GIS Data that maps known areas of jamming & spoofing

**Aggregated Data for Global Situational Awareness**
- Ground/Cloud Segment Collects all Jam/spoof Data from All Sources
- Maintenance of dynamic GIS data of all known occurrences globally

**Data Integration With SPACEKEYS UnityAir**
- EFB Visualization
- Flight Planning & ATC
Honeywell: Threat Detection – GPS L1 Advisory Service

**Airborne Systems**
- Jamming & Spoofing Detection
- Transmit Report from Aircraft
  - at first detection
  - at recovery, and
  - at periodic rate
- GPSR, FMS, IRS
  - adaptable to existing and future aircraft equipment
- ACMS/CMU

**Ground Systems**
- Build Jamming & Spoofing Advisory Zones
- UnityAir
  - User Display
    - pre-flight planning or
    - post-flight diagnostics
- Build Jamming & Spoofing Advisory Zones
- Honeywell FORGE
  - 2 minute refresh
Honeywell: GPS Threat Detection – Customer Value

**Maintenance**
- GPS loss impacts many aircraft system leading to Flight Deck Effects and Maintenance Messages
- Average 45 min maintenance per incident...up to several hours

**Operational Efficiency**
- GPS loss disrupts RNAV procedures
- $5000 per RNP approach vs non-RNP
- $7000 per delay-hr
- $30,000 per cancellation

**Pilot Workload/Safety**
- Incident documentation, minimum equipment list updates, unclear cockpit indication

**Faster identification of GPS as root cause and faster aircraft return to service**

**Preflight route planning around affected areas in-flight updates**

**Awareness of affected areas to flight crews for faster decision making**

Potential for significant reduction in annual costs for operators
Honeywell: GPS Threat Detection – Key Characteristics

**GPS L1 Threat Detection**
- Detects both Jamming and Spoofing threats.

**Advisory Zones**
- Provides horizontal Advisory Zones which extend to all aircraft altitudes.
- Advisory Zone quality increases as more aircraft encounter the GPS threat.
  - Good quality is achieved with 10 or more aircraft.
- Advisory Zones where at least 2 aircraft have encountered the GPS threat will be displayed to the end user.
  - At least 2 aircraft reporting a GPS threat will avoid false advisories.
  - 2 aircraft will produce a low-quality Advisory zone, which will improve with more aircraft.

**Capabilities**
- Worldwide coverage (everywhere suitably capable aircraft fly).
- Scalable to the number of capable aircraft (1000’s of aircraft flying at the same time)
- Scalable to the number of GPS threat zones (100’s of simultaneous GPS threat zones).
- Robust to aircraft data transmission delays and processing delays.
  - Delayed information is still valid information.
GPS L1 Advisory Service

Worldwide Advisory Zones for GPS Jamming and GPS Spoofing
UNITYAir: SPACEKEYS/Honeywell Integration

GPS L1 Advisory Service

Initial Advisory zone

High Quality Advisory zone

range of the GPS threat

Orange circle is for illustration only, The actual GPS threat source and range are unknown

Advisory zones start small when a single aircraft is impacted by a GPS threat

Many aircraft produce a high quality Advisory zone

over time ... more aircraft ... higher quality
UNITYAir: SPACEKEYS/Honeywell Integration

Route Analysis*

* Prototype mock-ups
Aircraft Jamming/Spoofing Trial – Avionics/Aircraft

Principle

- UNITYAir detects both Jamming and Spoofing threats.
- Important customers asked to nominate aircraft to participate in operational trial.

Aircraft Avionics

- ACMS is the only aircraft equipment that needs to be updated
  - ACMS system and supplier depend on aircraft type
  - Most ACMS programmable without need to recertify (e.g. HON FDAMS, Teledyne FDIMU)
- Honeywell has validated the aircraft configuration and prototyped ACMS updates for B737NG equipped with HON ACMS (called FDAMS)
- HON FDAMS has two components:
  - DFDAU – modifications would most likely require re-certification. We will NOT modify this component.
  - ACMS – modifications do NOT require re-certification. This is the component where we would implement.

Aircraft Type

- Preferred aircraft for trial: B737NG fitted with HON ACMS/FDAMS (pre 2018)
- Other aircraft type or configurations feasible as well, joint assessment required (ACMS, wiring)
UNITY Ground: GNSS Monitoring System

- GNSS signal monitoring
  - Default GNSS: GPS
  - Optional GNSS: Galileo, GLONASS, BeiDou
  - Optional SBAS: WAAS, EGNOS, MSAS, GAGAN
- GNSS interference detection
  - Default GNSS: GPS
  - Optional GNSS: Galileo
- Typical installations at airports, area operations centres and critical infrastructure sites
- Realtime performance monitoring & interference detection
- Realtime performance & interference detection alerting
- Data recording (typically 5-yr history)
- Periodic performance data reporting (typically, monthly based on ICAO Annex10 - SiS Performance Requirements)

UNITY:Hub
- Networked with other UNITY Ground installations
- Data archive to cloud long-term storage
- Access to UNITY Air data