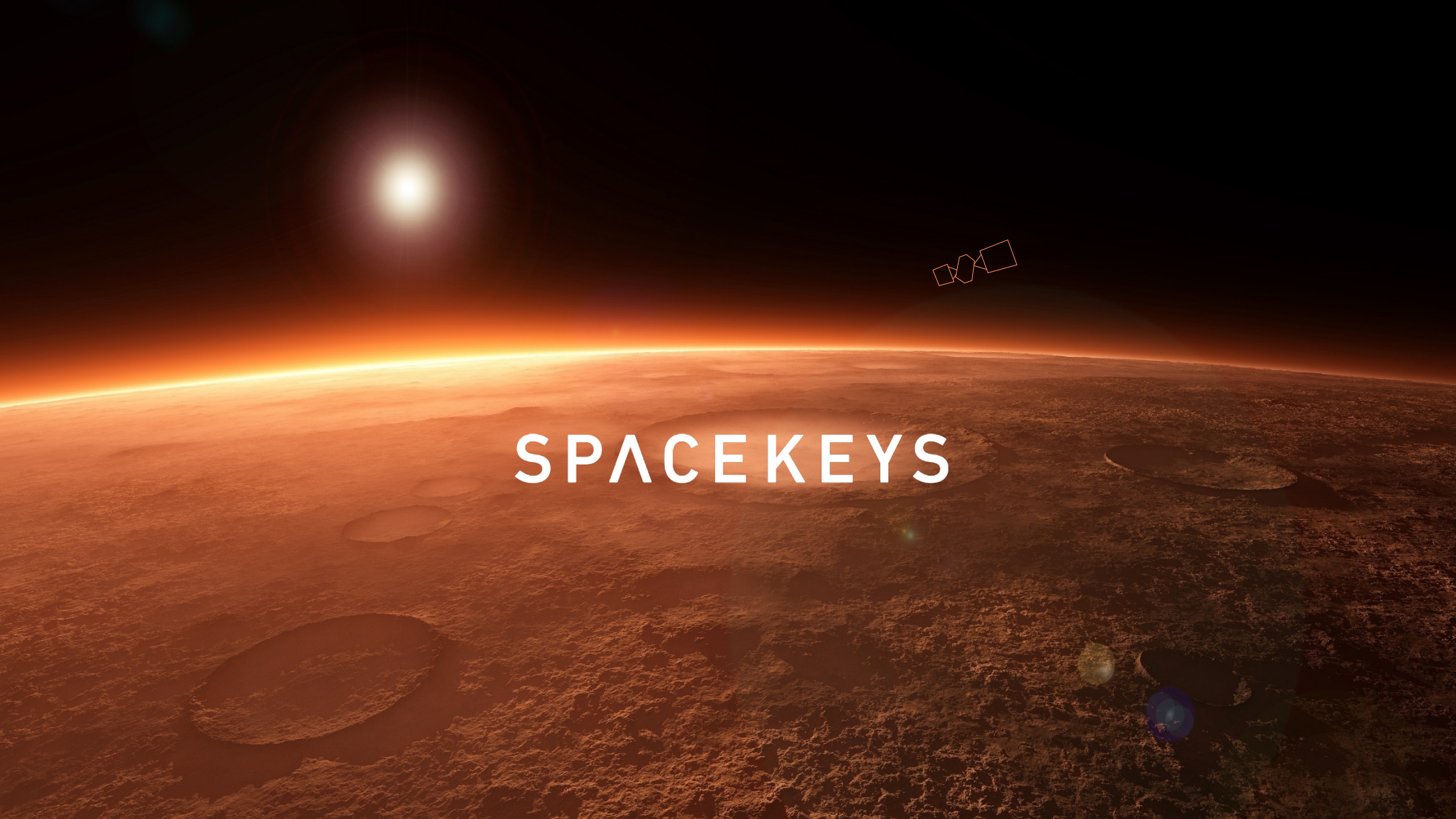
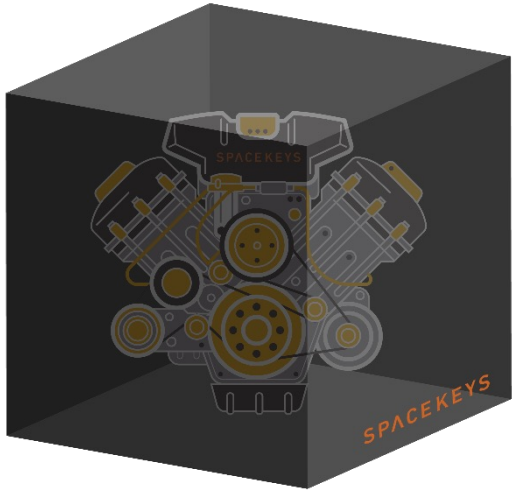

SPACEKEYS

Executive Summary

SPACEKEYS

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.

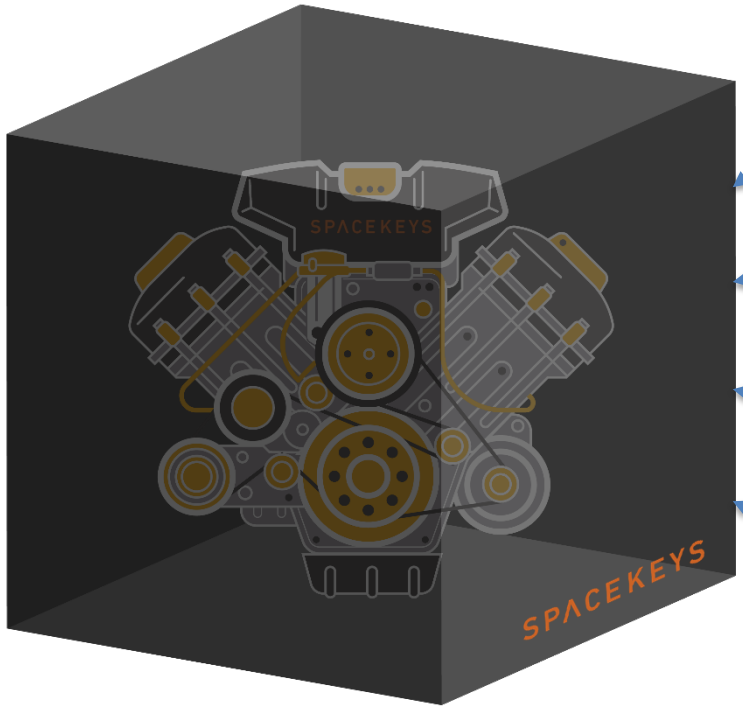


GPS I/II/IIA | GPS IIR | GPS IIR(M) | GPS IIF | GPS III

Black Box Design Solution

SPACEKEYS

One solution for ALL users.



SPACEKEYS RAIM PRO

SPACEKEYS UNITY HUB

SPACEKEYS UNITY AIR

SPACEKEYS UNITY GROUND

SPACEKEYS RAIM ANSP

SPACEKEYS ARAIM TEST BED

- 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)

SPACEKEYS

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:

Parameter	Options	Details
Algorithm	FD or FDE	
Barometric Aiding	ON, OFF or ON only on Failure	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.
Selective Availability	ON or OFF	
Mask Angle	-25° to 30°	
HAL Multiplier	Any certified value	Some aircraft are certified to apply a horizonal alert limit bias during RAIM predictions.

RAIM Pro: Requirements (Navigation)

SPACEKEYS

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

	RNAV 10 RNP 10	RNAV 5 Basic-RNAV	RNAV 2 US RNAV Type A	RNAV 1 P-RNAV US RNAV Type B	RNP 4	RNP 2	RNP1	RNP Approach	RNP AR Approach	MNPS
FAA (U.S.A.)	AC 90-105A (replaces Order 8400.12C)	AC 90-96A	AC90-100A	AC90-100A	AC 90-105A (repl. order 8400.33)	AC90-105A	AC 90-105A	AC 90-105A (LNAV, LNAV/VNAV) AC90-107 (LP, LPV)	AC 90-101A AC20-138D	N8110.60
EASA (EU, EFTA and other countries)	AMC 20-12	AMC 20-4A JAA TGL 2	AMC 20-16 JAA TGL 10	AMC 20-16 JAA TGL 10			AMC 20-16 JAA TGL 10	AMC 20-27 (LNAV, LNAV/VNAV) AMC 20-28 (LP, LPV)	AMC 20-26	
CASA (Australia)	AC91.U-01 AC 91U-2(0)	AC91.U-01 (replaces AC91U-II-B-2(0))	AC91.U-01 (replaces AC 91U-II-B-3(0))	AC91.U-01 (replaces AC 91U-II-B-3(0))	AC91.U-01 AC 91U-3(0)	AC91.U-01 (replaces AC 91U-II-C-2(0))	AC91.U-01 (replaces AC 91U-II-C-3(0))	AC91.U-01 (replaces AC 91U-II-C-5 (LNAV) AC 91U-II-Attachment (LNAV/VNAV))	AC 91U-II-C-5 (RNP AR) AC91.U-01 (replaces AC 91-U-II-C-6)	
SVRSOP (Latin America)	AC 91-001	AC 91-002	AC 91-003	AC 91-003	AC 91-004	AC 91-005	AC 91-006	AC 91-008 (LNAV) AC 91-010 (LNAV/VNAV)	AC 91-009	
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)

SPACEKEYS

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.

U.S. Department of Transportation
Federal Aviation Administration

Advisory Circular

Subject: Automatic Dependent Surveillance-Broadcast Operations

Date: 12/30/19 **AC No:** 90-114B
Initiated by: AFS-400 **Change:**

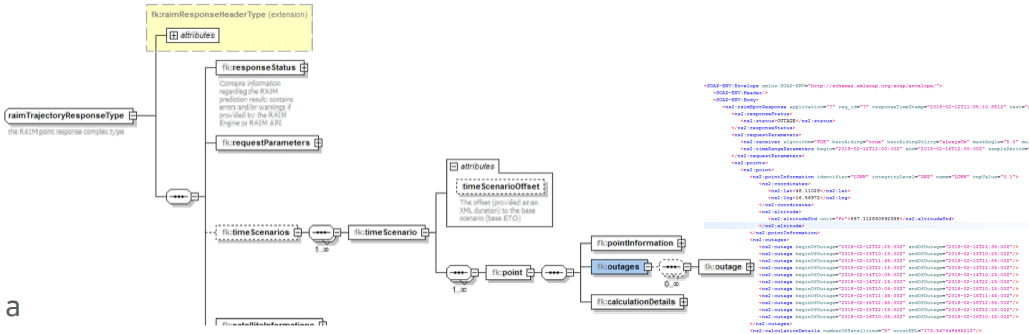
In May 2010, the Federal Aviation Administration (FAA) issued Title 14 of the Code of Federal Regulations (14 CFR) part 91, §§ 91.225 and 91.227. This rule requires Automatic Dependent Surveillance-Broadcast (ADS-B) Out performance when operating in designated classes of airspace within the U.S. National 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

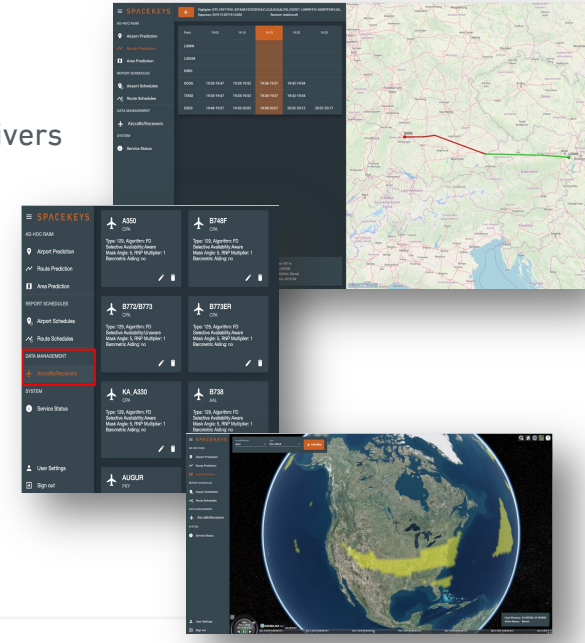
RAIM Pro: Core Features

SPACEKEYS

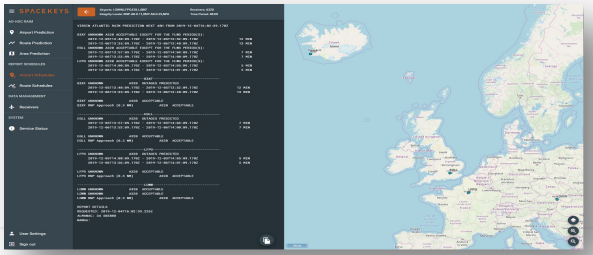
- Real time integration with 3rd party systems, such as flight planning and flight following systems, using SOAP and/or REST APIs
  - API to request a location RAIM prediction for any airport with specific RNP levels
  - API to request a trajectory RAIM prediction for any trajectory of a flight



- 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
- 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



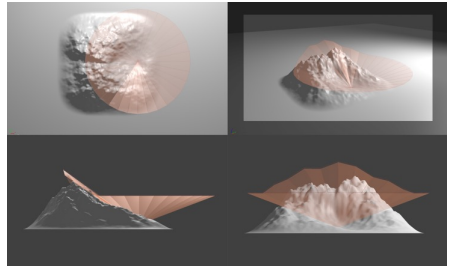
- Customizable daily RAIM reports

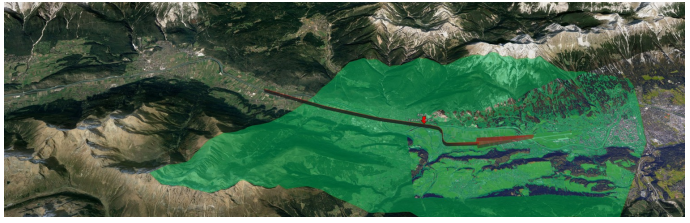


RAIM Pro: Core Features

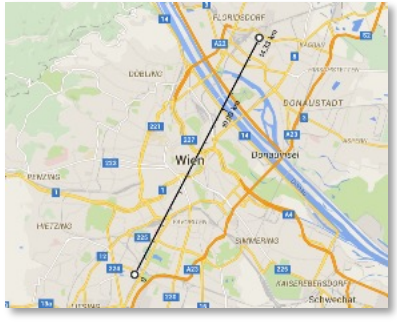
SPACEKEYS

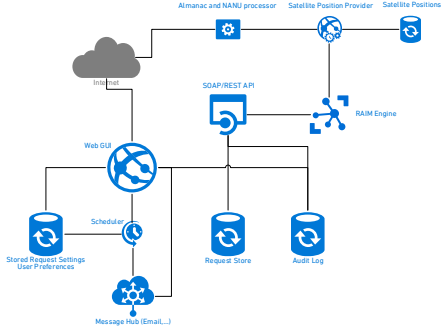
- Terrain screening for RNP-AR operations
  - For RNP-AR approach procedures, potential obstruction of satellites by the surrounding terrain could affect RAIM availability. SPACEKEYS dynamic terrain screening engine analyzes the surrounding terrain for every RNP-AR request to ensure compliance with this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





- Architecture / SLA
  - 99.95% system uptime.
  - New Almanac Processing within 2 minutes.
  - New NANU processing within 10 minutes.
  - 24/7 support.

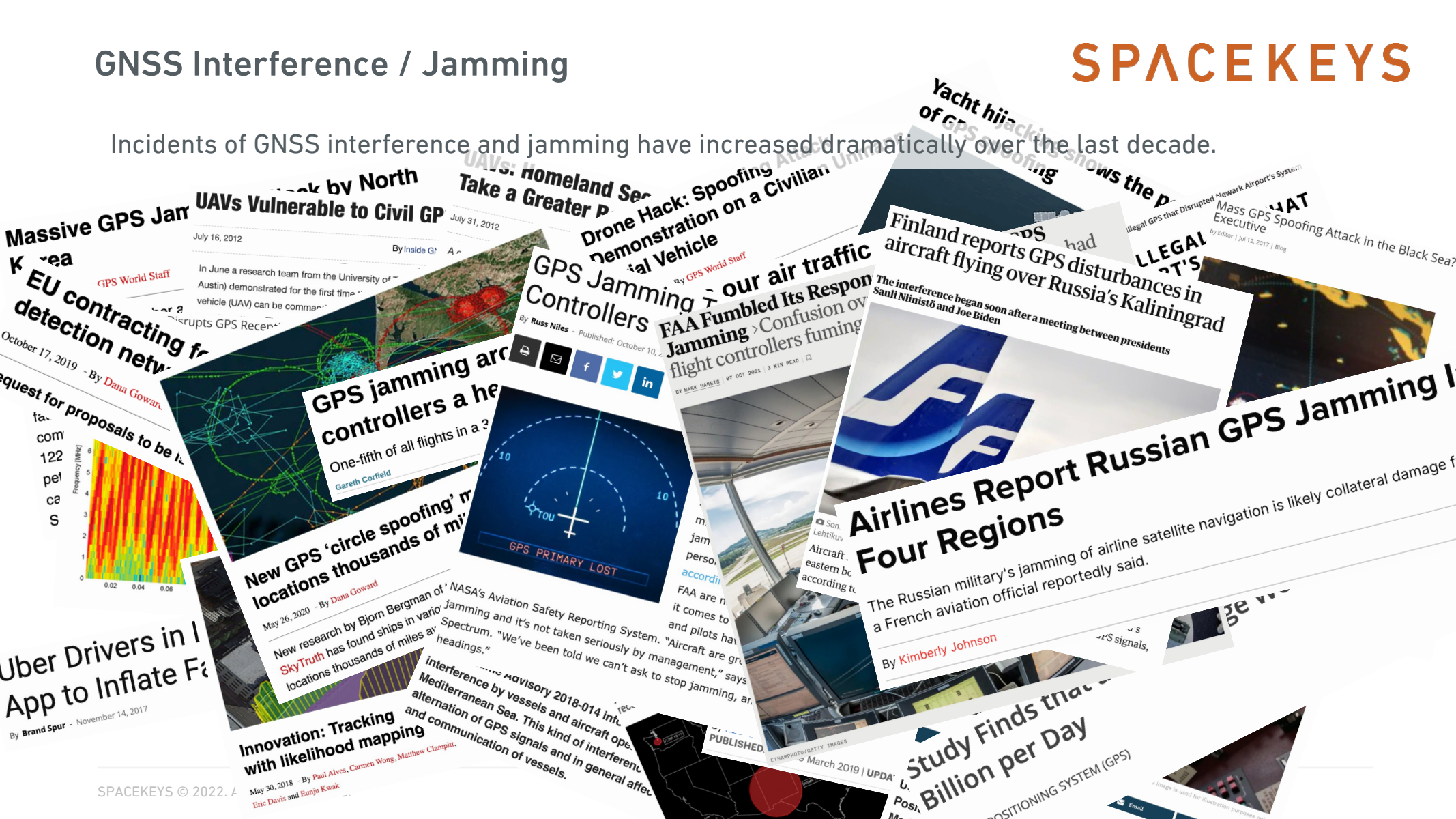




GNSS Interference / Jamming

SPACEKEYS

Incidents of GNSS interference and jamming have increased dramatically over the last decade.

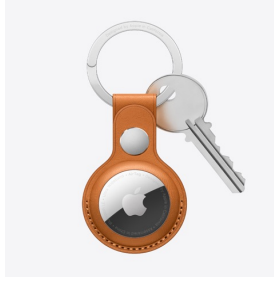


GNSS Interference / Jamming

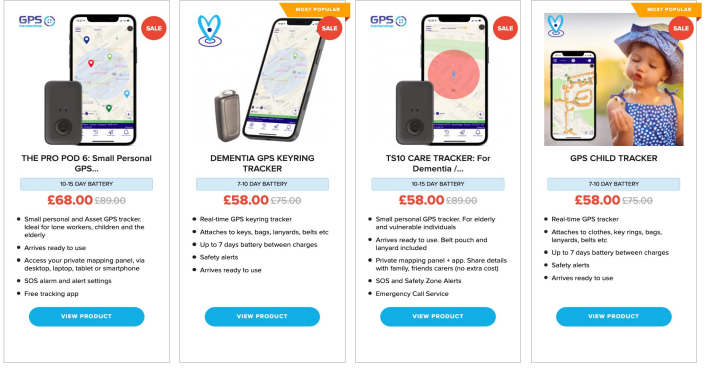
SPACEKEYS

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

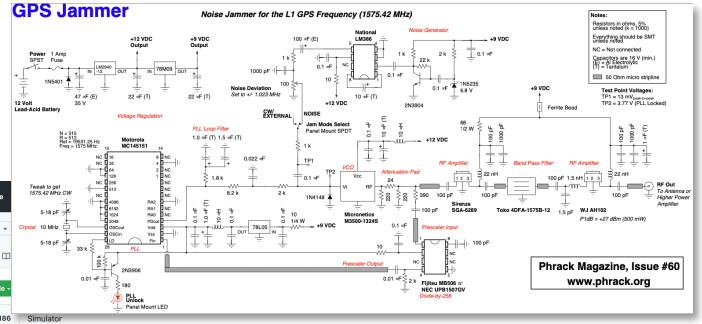


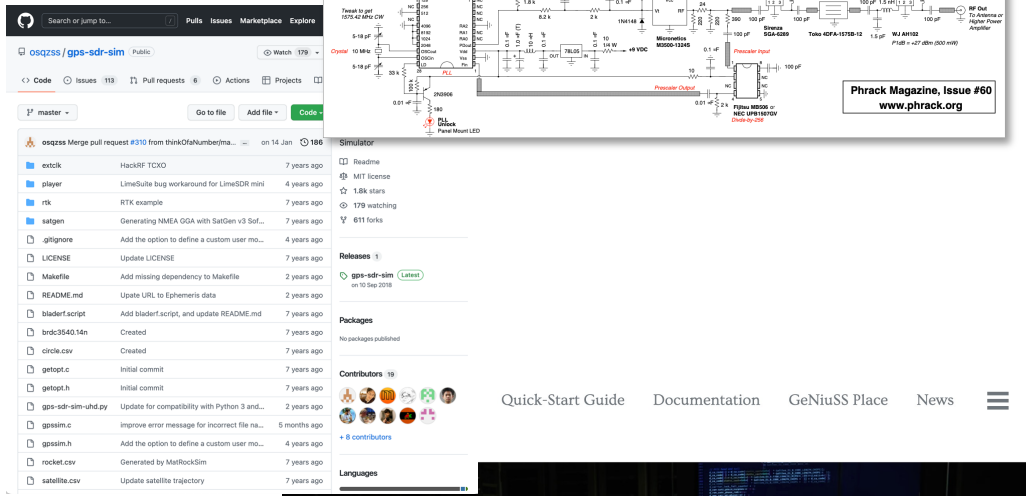
GNSS Interference / Jamming

SPACEKEYS

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

SPACEKEYS

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: $299 USD
Frequency Range: 100 kHz to 3.8 GHz
ADC Resolution: 12 Bits
Max Bandwidth: 61.44 MHz
TX/RX: TX and RX
Preselectors: None
Release Date: April 2016

The LimeSDR appears to be one of the 'next generation' of experimenter focused 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 2017) is in its initial production stages.

ADALM PLUTO (PlutoSDR)*

Cost: $99 USD (Special), $149 USD
Frequency Range: 325 – 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)
Preselectors: None
Release Date: Mid 2017

The PlutoSDR is a low cost full duplex TX and RX receiver designed by the big silicon 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 experimenters SDR.

BladeRF

Cost: $420 USD (x40), $650 USD (x115)
Frequency Range: 300 MHz - 3.8 GHz
ADC Resolution: 12 Bits
Max Bandwidth: 28 MHz
TX/RX: TX and RX (Full Duplex)
Preselectors: 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 transverter 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)
Preselectors: None
Release Date: April 2014

The HackRF 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

SPACEKEYS

Cheap
SDR Electronics
Device

```
int generateNavMsg(gpstime_t g, channel_t *chan, int init)
{
  int iwrd,isbf;
  gpstime_t g0;
  unsigned long wn,tow;
  unsigned sbfwrd;
  unsigned long prevwrd;
  int nib;

  g0.week = g.week;
  g0.sec = (double)(((unsigned long)(g.sec+0.5))/30UL) * 30.0; // Align with the full frame length = 30 sec
  chan->g0 = g0; // Data bit reference time

  wn = (unsigned long)(g0.week%1024);
  tow = ((unsigned long)g0.sec)/6UL;

  if (init==1) // Initialize subframe 5
  {
    prevwrd = 0UL;

    for (iwrd=0; iwrd<N_DWRD_SBF; iwrd++)
    {
      sbfwrd = chan->sbf[4][iwrd];

      // Add TOW-count message into HOW
      if (iwrd==1)
        sbfwrd |= ((tow&0x1FFFFUL)<<13);

      // Compute checksum
      sbfwrd |= (prevwrd<<30) & 0xC0000000UL; // 2 LSBs of the previous transmitted word
      nib = ((iwrd==1)||(iwrd==9))?1:0; // Non-information bearing bits for word 2 and 10
      chan->dwrd[iwrd] = computeChecksum(sbfwrd, nib);

      prevwrd = chan->dwrd[iwrd];
    }
  }
  else // Save subframe 5
  {
    for (iwrd=0; iwrd<N_DWRD_SBF; iwrd++)
    {
      chan->dwrd[iwrd] = chan->dwrd[N_DWRD_SBF+N_SBF+iwrd];

      prevwrd = chan->dwrd[iwrd];
    }
```

+

Freely available
GPS receiver/
emulator
source code

A Little
'Know-how'

=

GPS
Interference,
Jamming, or
Spoofing

Gotta Catch 'Em All! – WORLDWIDE! (or how to spoof GPS to cheat at Pokémon GO)

The moment, when your team leader asks you to cheat at Pokémon GO...everyone knows it, right? No? Well, I do

GPS Spoofing Set

GNSS Spoofing - Intentional & Legal Sources of GPS Spoofing

SPACEKEYS

- 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?

SPACEKEYS

- 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

SPACEKEYS
Honeywell

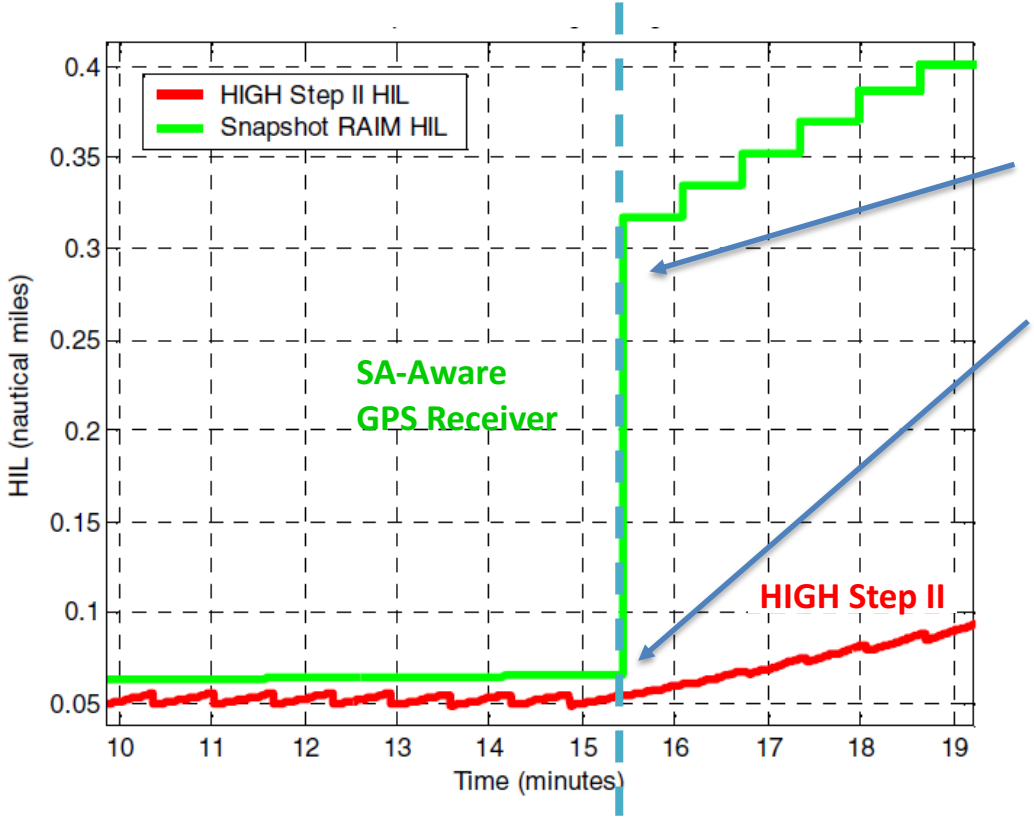
Enhanced RAIM with Honeywell HIGH Step II – 100% RNP 0.1 Availability

- HIGH Step II Benefits
- Legacy Architectures
- Integration of Honeywell predictions with SPACEKEYS RAIM Pro

UNITY^{Air}: GPS Threat Detection

- System Overview
- Integration of Honeywell Threat Detection with SPACEKEYS **UNITY^{Air}**
- Value of Threat Detection

Honeywell: Benefits of HIGH Step II



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

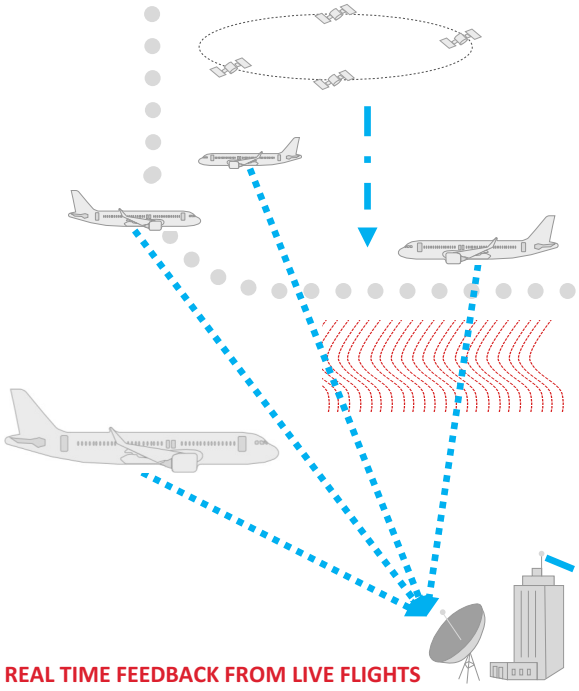
Entry into RAIM Hole, often caused by setting of a Satellite in combination with an already degraded geometry (e.g. 2nd satellite offline for maintenance)

Honeywell: GPS Threat Detection Architecture

SPACEKEYS
Honeywell

UTILIZING EXISTING ADIRU INSTALL BASE

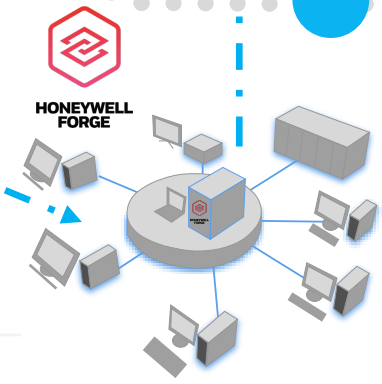
- Thousands of HON-equipped aircraft around the world
- Detection of GPS jamming and spoofing using data from certified avionics and Honeywell's inertial system hybrid GPS/inertial algorithms



REAL TIME FEEDBACK FROM LIVE FLIGHTS

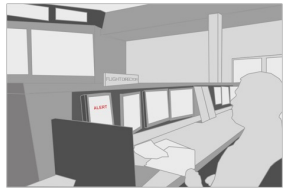
- As individual aircraft encounter jam/spoof, they notify the ground infrastructure with details (e.g., 3D location, other details via ACARS.
- When/If jam/spoof clears, aircraft reports clearance of event.

HONEYWELL FORGE



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

SPACEKEYS UNITY AIR

DATA INTEGRATION WITH SPACEKEYS UNITY Air

- EFB Visualization
- Flight Planning & ATC

Honeywell: Threat Detection – GPS L1 Advisory Service

SPACEKEYS
Honeywell

Airborne Systems

Jamming & Spoofing Detection

GPSR, FMS, IRS

adaptable to existing and future aircraft equipment

Transmit Report from Aircraft

- at first detection
- at recovery, and
- at periodic rate

ACMS/CMU

aircraft position

from aircraft via ACARS

Ground Systems

Build Jamming & Spoofing Advisory Zones

Honeywell FORGE

2 minute refresh

UNITY Air User Display

- pre-flight planning or
- post-flight diagnostics

Honeywell: GPS Threat Detection – Customer Value

SPACEKEYS
Honeywell

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

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

Operational Efficiency

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

Preflight route planning around affected areas
in-flight updates

Pilot Workload/Safety

- Incident documentation, minimum equipment list updates, unclear cockpit indication

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

SPACEKEYS
Honeywell

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.

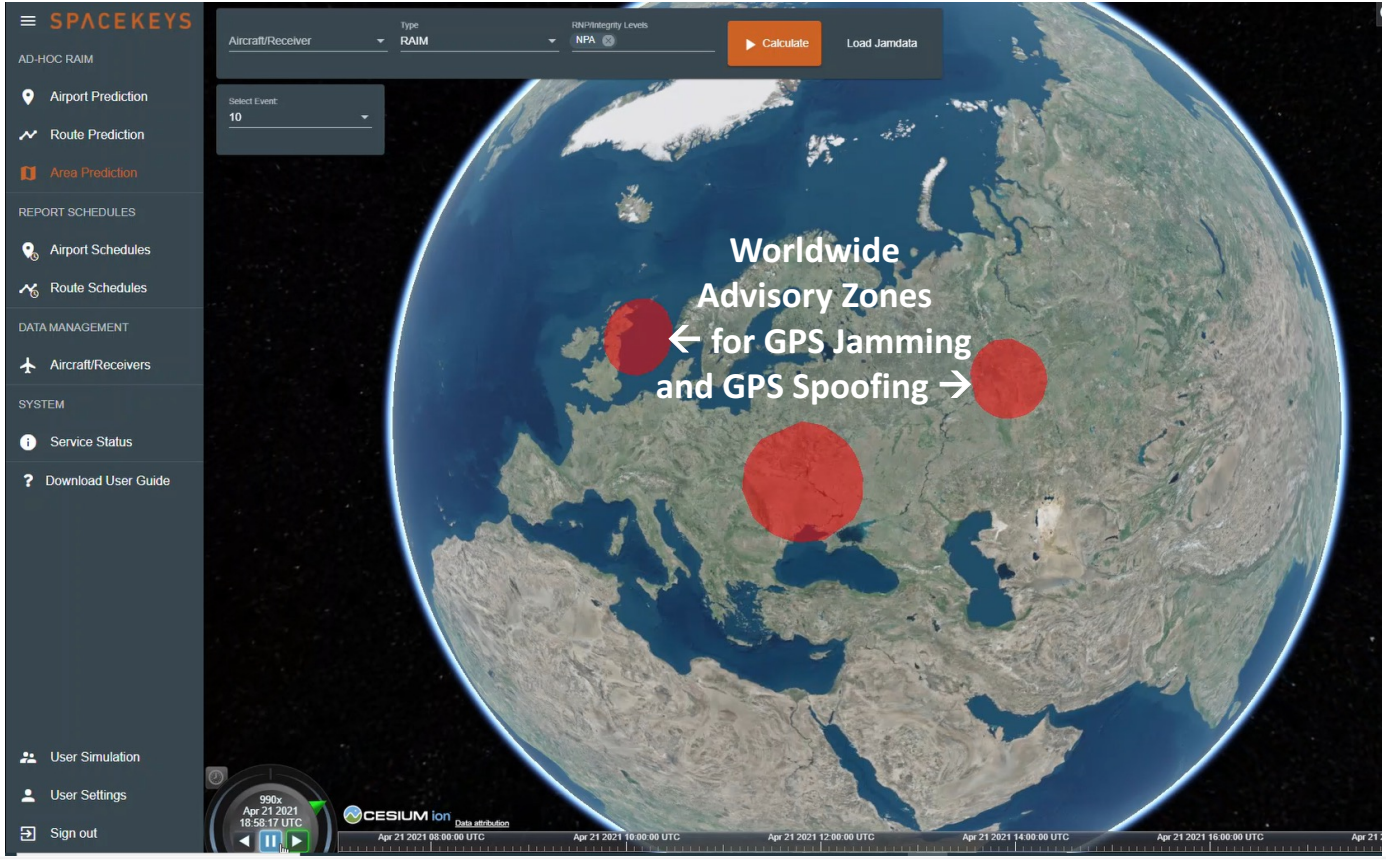
Capabilities

- 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.

UNITY[Air]: SPACEKEYS/Honeywell Integration

SPACEKEYS

GPS L1 Advisory Service

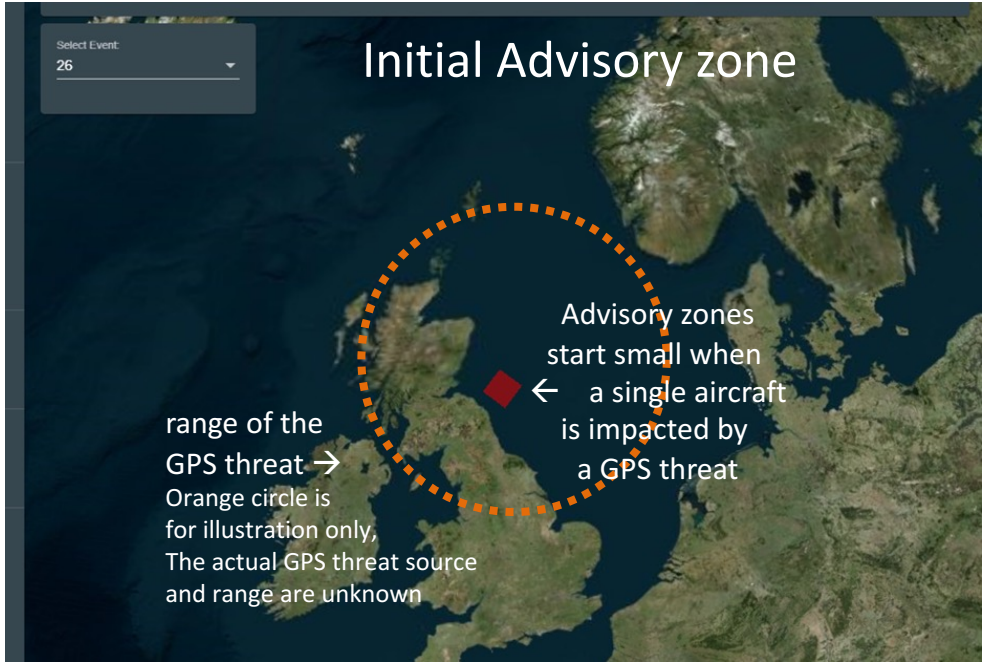


SPACEKEYS UNITY AIR

UNITY[Air]: SPACEKEYS/Honeywell Integration

SPACEKEYS

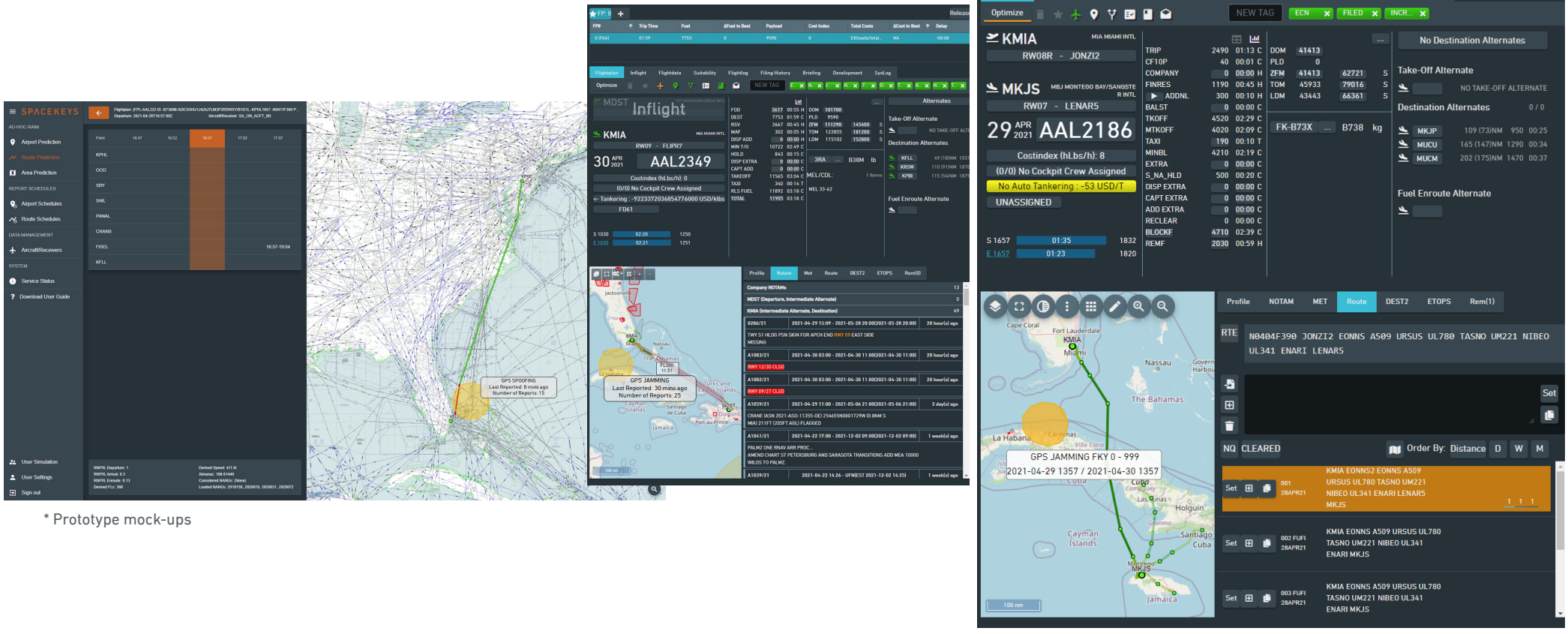
GPS L1 Advisory Service



over time … more aircraft … higher quality

UNITY[Air]: SPACEKEYS/Honeywell Integration

Route Analysis*



* Prototype mock-ups

Aircraft Jamming/Spoofing Trial – Avionics/Aircraft

SPACEKEYS
Honeywell

Principle

- UNITY^{Air} 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

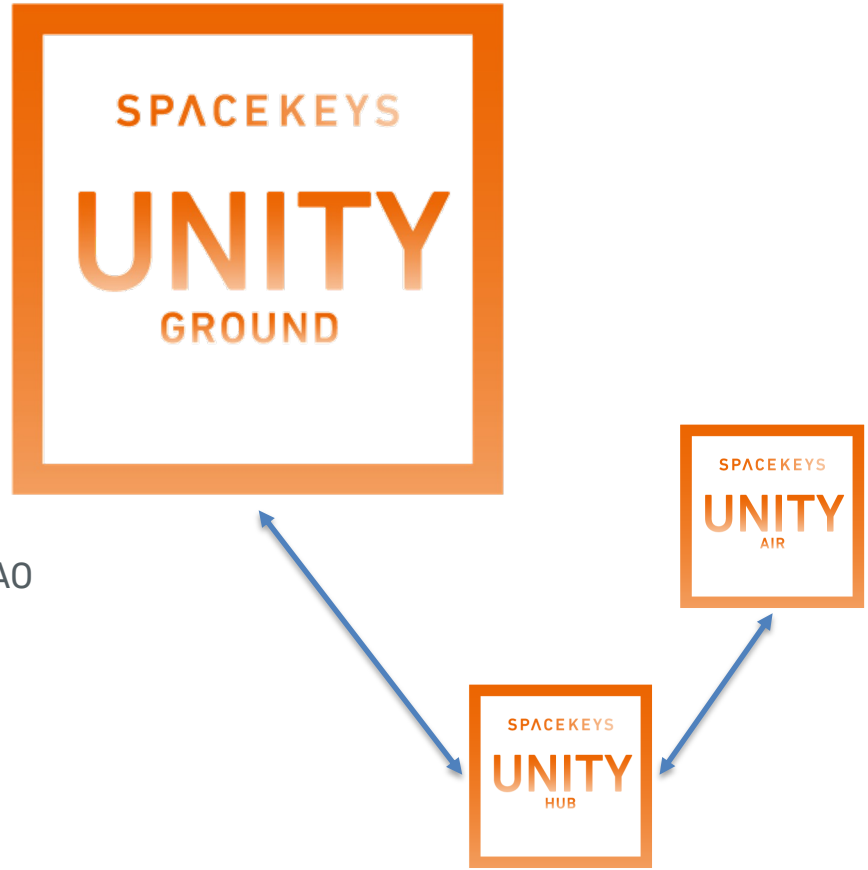
SPACEKEYS

- 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




THANK YOU!
SPACEKEYS ©2022