COLOSSUS

Crowd-sourced platform for GNSS anomaly identification, isolation and attribution analysis

Mark Dumville / Mike Pattinson
Nottingham Scientific Limited

Baska, 8 May 2018

Governments are using GNSS….

Slovakia has experienced the largest extension of road tolling networks worldwide so far.

Slovakian RUC Network

RUC network until 31/12/2013

RUC network added from 01/01/2014

Source: SkyToll

In addition to Slovakia, Germany, Switzerland and Hungary have successfully implemented GNSS-based tolling. Other countries are also leveraging the benefits:

- Belgium and Russia have launched similar projects implementing GNSS-based schemes.
- France, Finland, Bulgaria, Denmark, The Netherlands and Lithuania have all declared their interest in GNSS-based schemes.

GNSS based Truck tolling

Call

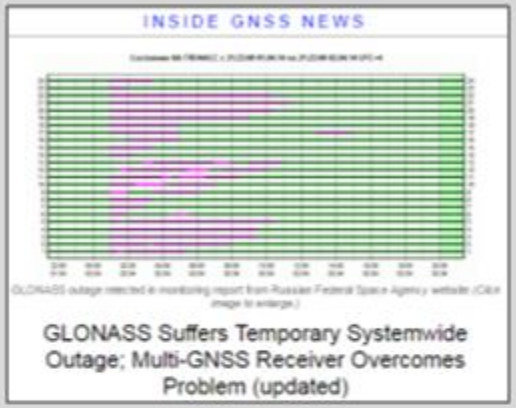
GNSS based road user charging

Remotely Piloted Aircraft Systems

Offender monitoring

Fisheries Policy

Governments trust GNSS.....



1. GNSS system issues

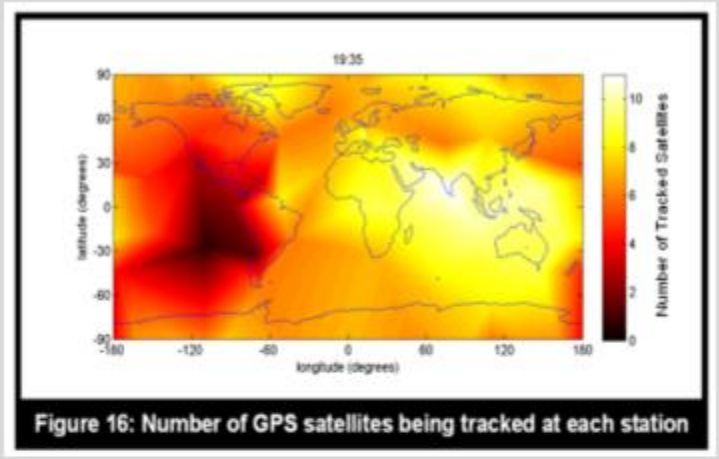
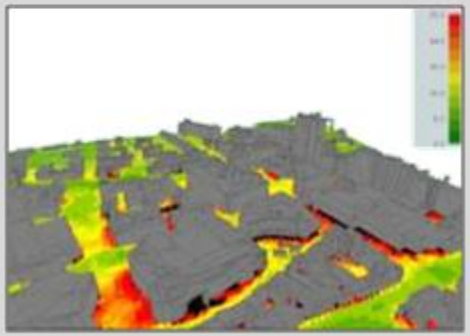


Figure 16: Number of GPS satellites being tracked at each station

2. Solar Flare



3. Masking, obscurations and blockages

4. High ionospheric activity

We must defend against threats.....

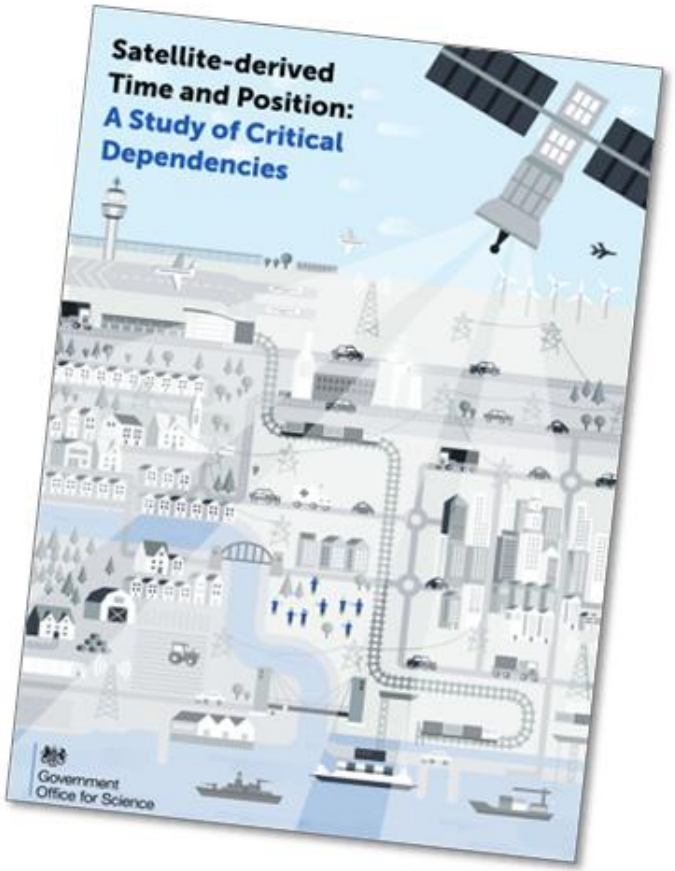
Fines up to 50,000 euros for truckers with GPS jammer to avoid toll

COMMENTS

SAVE ARTICLE

TOLL Truckers who use a GPS jammer to avoid the toll, risking fines up to 50,000 euros. That is informed today at Viapass, the government agency that coordinates the kilometer charge. Moreover, there are three ways in which the fraud is detected: via fixed porches above the road, and flexible control over the mobile control units. In addition, irregularities can be noted in the billing says Edward Claessens of Viapass.

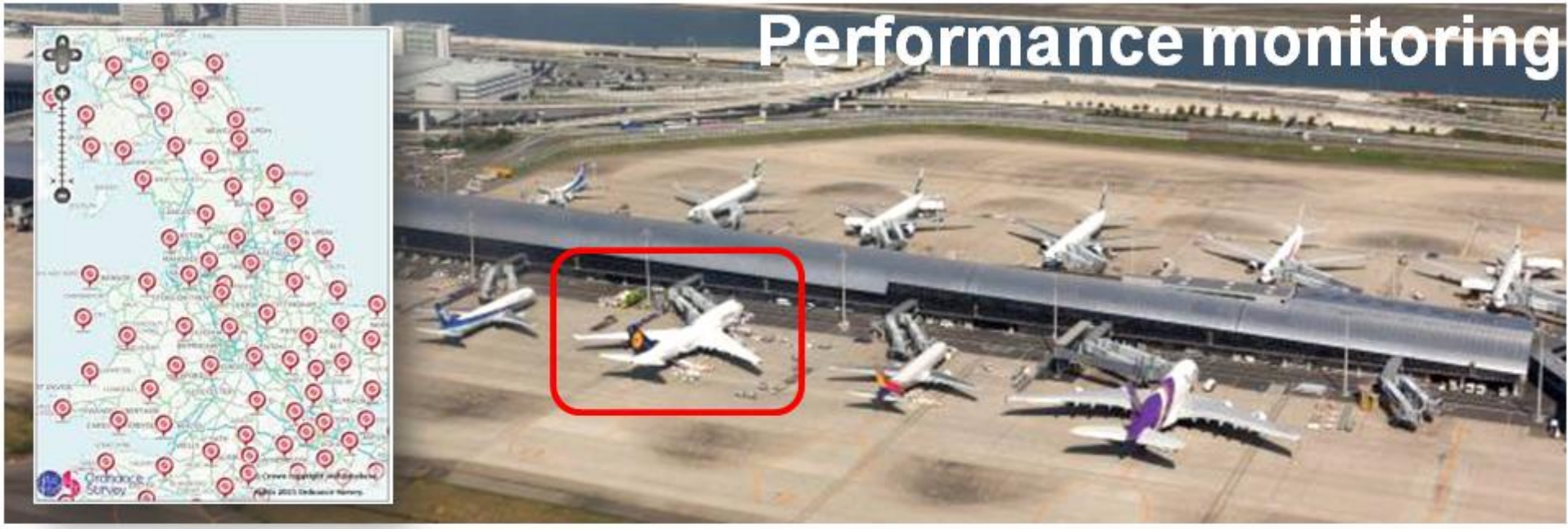
GNSS performance is critical...



Value at risk from UK loss of GNSS is £5B over 5 days

The purpose of this report is to lay out the breadth, scale and implications of our reliance on GNSS

GNSS performance is monitored…



- Use of **Continuously Operating GNSS** networks
- Assessing performance of GNSS for airspace users
- Meeting International Standards (eg, ICAO)
- Accuracy, Integrity, Availability and continuity

GNSS Interference is monitored...

Detector
Fingerprinting GNSS Threats

Detect, characterise, locate GNSS jammers

Identify the impact of interferences on GNSS

Protect critical GNSS applications and infrastructures

Helping to harden next generation GNSS receivers

COLOSSUS

- **Crowd-sourced platform for GNSS anomaly identification, isolation and attribution analysis**

- Project sponsored by ESA under the NAVISP Programme
  - Navigation Innovation and Support Programme

- Start date: October 2018
- End date: March 2020.

esa
European Space Agency

COLOSSUS Overview

- COLOSSUS processes **crowd-sourced GNSS RINEX** data to identify, isolate and attribute GNSS faults and failures into causation groupings.

- COLOSSUS identifies **common mode** GNSS failures, **constellation** failures, **atmospheric** events and **single satellite** failures by persistent monitoring across all GNSS constellations and all GNSS frequencies throughout different geographical scales and receiver network densities.

- COLOSSUS is able to identify **inter-GNSS failures** and **inter-GNSS dependencies** within GNSS receivers by processing RINEX data from multiple GNSS receiver types.

COLOSSUS Objectives

1. To be “**scalable**” to any size of GNSS network, any volume of GNSS data

2. To assemble and maintain a “**database**” of probabilities of occurrences of GNSS anomalies and the associated impact of faults, failures and events

3. To become the “**reference**” for GNSS performance monitoring, GNSS fault reporting, GNSS investigatory analysis and for the assembly and provision of GNSS incident reports, warnings/alerts and reliability statistics.

4. To understand what “**trust**” to place in GNSS and in doing so support the development of next generation GNSS applications.

- **COLOSSUS can also detect GNSS interference...**

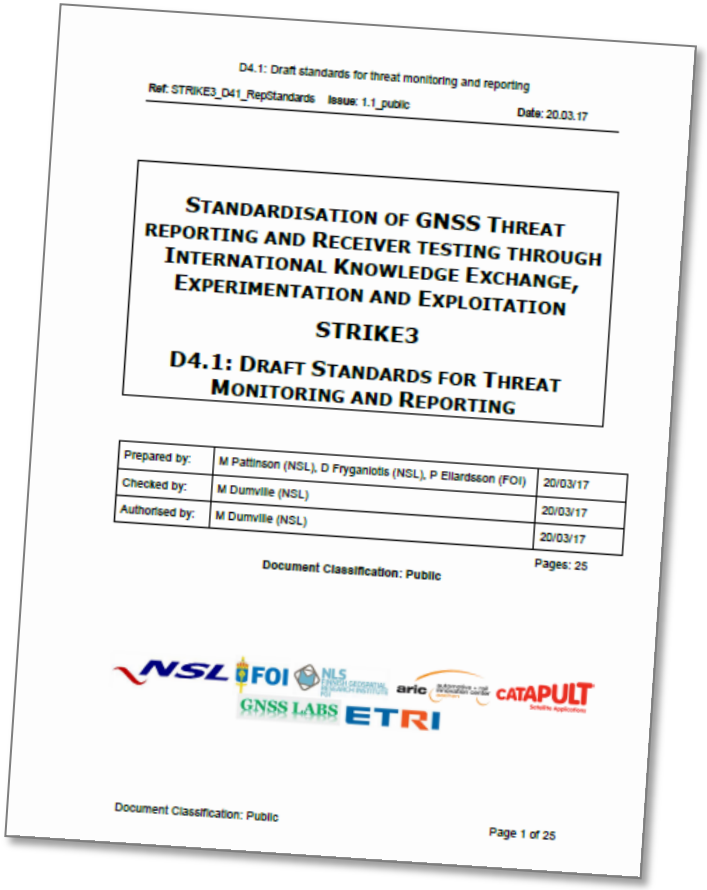
COLOSSUS was not designed for GNSS RF interference detection

Using Crowd-sourced GNSS Data

- Continuously Operating Reference Stations (CORS) data
- CORS receivers are typically multi-GNSS, multi-frequency
- Global, regional, national, local CORS networks
- 10,000s of GNSS receivers deployed
- Real-time, offline (and archives)
- Data is accessible (free or small fee)
- Impact of an anomaly on the GNSS receiver is observed

Quality? Trust? Continuity?

Crowd-sourced GNSS interference



D4.1: Draft standards for threat monitoring and reporting

Ref: STRIKE3_D41_RepStandards Issue: 1.1_public Date: 20.03.17

STANDARDISATION OF GNSS THREAT REPORTING AND RECEIVER TESTING THROUGH INTERNATIONAL KNOWLEDGE EXCHANGE, EXPERIMENTATION AND EXPLOITATION

STRIKE3

D4.1: DRAFT STANDARDS FOR THREAT MONITORING AND REPORTING

Prepared by:	M Pattinson (NSL), D Fryganiotis (NSL), P Ellardsson (FOI)	20/03/17
Checked by:	M Dumville (NSL)	20/03/17
Authorised by:	M Dumville (NSL)	20/03/17

Document Classification: Public Pages: 25

NSL FOI NLS GNSS LABS ario CATAPULT ETRI

Document Classification: Public Page 1 of 25

1. A **draft standard** for Threat Monitoring and Reporting exists

2. Developed under STRIKE3 project

European Global Navigation Satellite Systems Agency HORIZON 2020 STRIKE3

3. Provides recommendations for data fields to be provided from **GNSS receivers** to support GNSS RF interference reporting.

4. **Applicable to all types** of GNSS receiver which enables them to be used in “crowd-sourcing” applications

Available from: www.gnss-strike3.eu

Crowd-sourced GNSS Interference

1. Crowd-sourced GNSS (RINEX) data over region-of-interest
2. Batch processing (multi-GNSS, multi-frequency GNSS data)
3. Identification of poor/lost data
4. Compare against internal rules/thresholds
5. Generate indicators of “interference”

No guarantee that interference is being detected

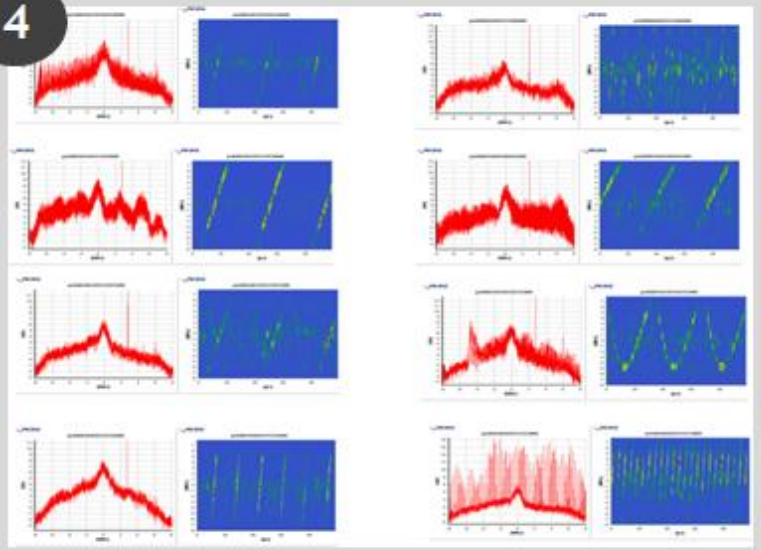
Proof of concept validation

COLOSSUS

1

2

4



- CORS network reports problems at select sites
- Processing CORS RINEX identifies poor/lost data
- Deploy GNSS interference detection system at sites
- Detects and Characterises multiple jammers

3

Crowd-sourced GNSS can identify hotspots

Limitations of Crowd-sourced GNSS Data

- Continuously Operating Reference Stations (CORS) sites are chosen for good GNSS signal reception
  - Clear view of the sky
  - No Obstructions
  - No industrial machinery

Not expecting to see GNSS RF interferences

- Professional grade GNSS receiver and antenna
  - Not typical of user receiver
  - Receivers are implementing “interference cancellation”

- No characterisation possible
  - Difficult to distinguish interference and jammer

Crowd-sourcing *additional* GNSS data?

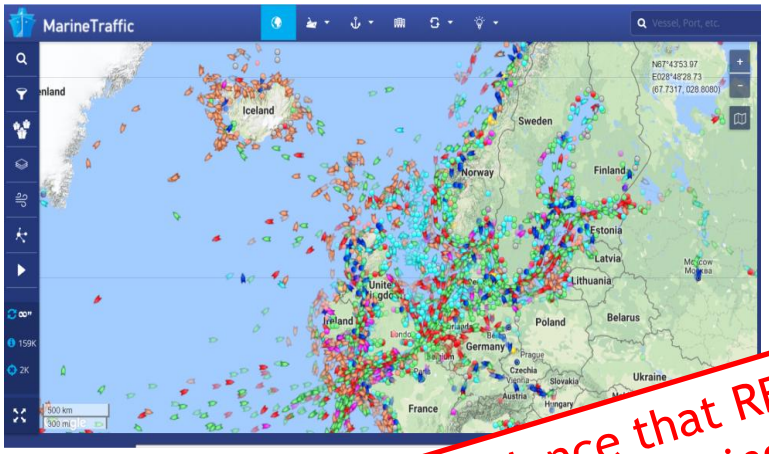
COLOSSUS

- New potential from **Android Phones**
  - Observables, SNR
  - AGC values(*)
- Multi-constellation GNSS
- Multi-frequency* (L1/L5/E1/E5a)

www.flamingognss.com

- Automotive GNSS receiver technology
  - Observables, SNR, Interference indicators

- AIS & ADS-B position reports
  - identify “jumps” and “gaps” in data
  - Identify reporting “holes”

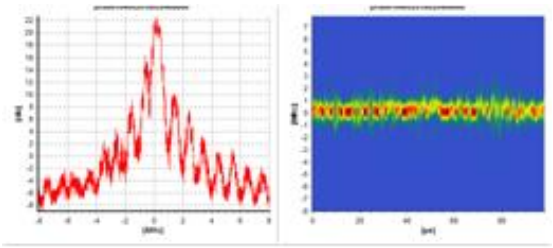


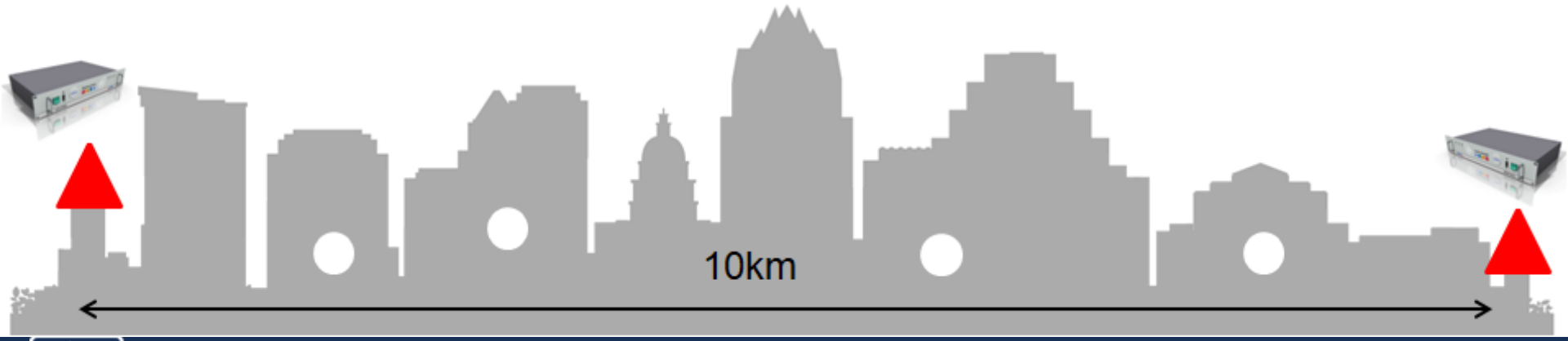
No confidence that RF interference is being detected

Preliminary Conclusions

- **Crowd-Sourcing *benefits* from DETECTOR equipment**
  - Use of DETECTOR equipment to identify CORS site is clean prior to installation
  - Use of DETECTOR equipment to calibrate/validate crowd-sourcing detection algorithms (ie, trigger thresholds)
  - Use of DETECTOR equipment to diagnose detected events

- **DETECTOR *benefits* from Crowd-sourcing techniques**
  - Use of Crowd-sourcing to identify interference "hotspots"
    - To support incident resolution and removal of interference
  - Use of Crowd sourcing to assess impact of known event
    - ***High power events*, *New waveforms*, *Exotic waveforms***





COLOSSUS

thank you

Mark.Dumville@nsl.eu.com
Michael.pattinson@nsl.eu.com

Image courtesy of GSA

Please see GOOGLEs website

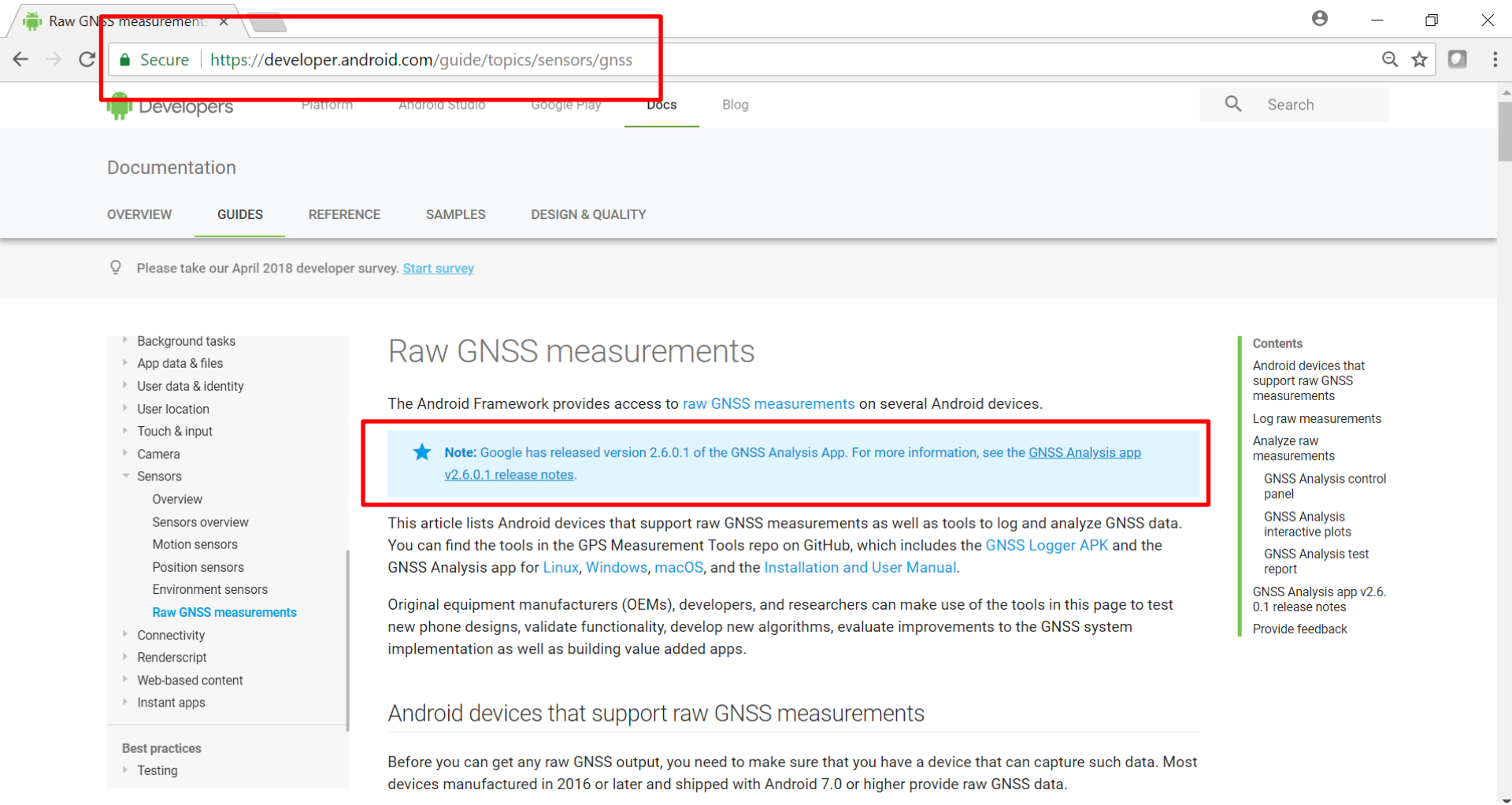


Image courtesy of Google

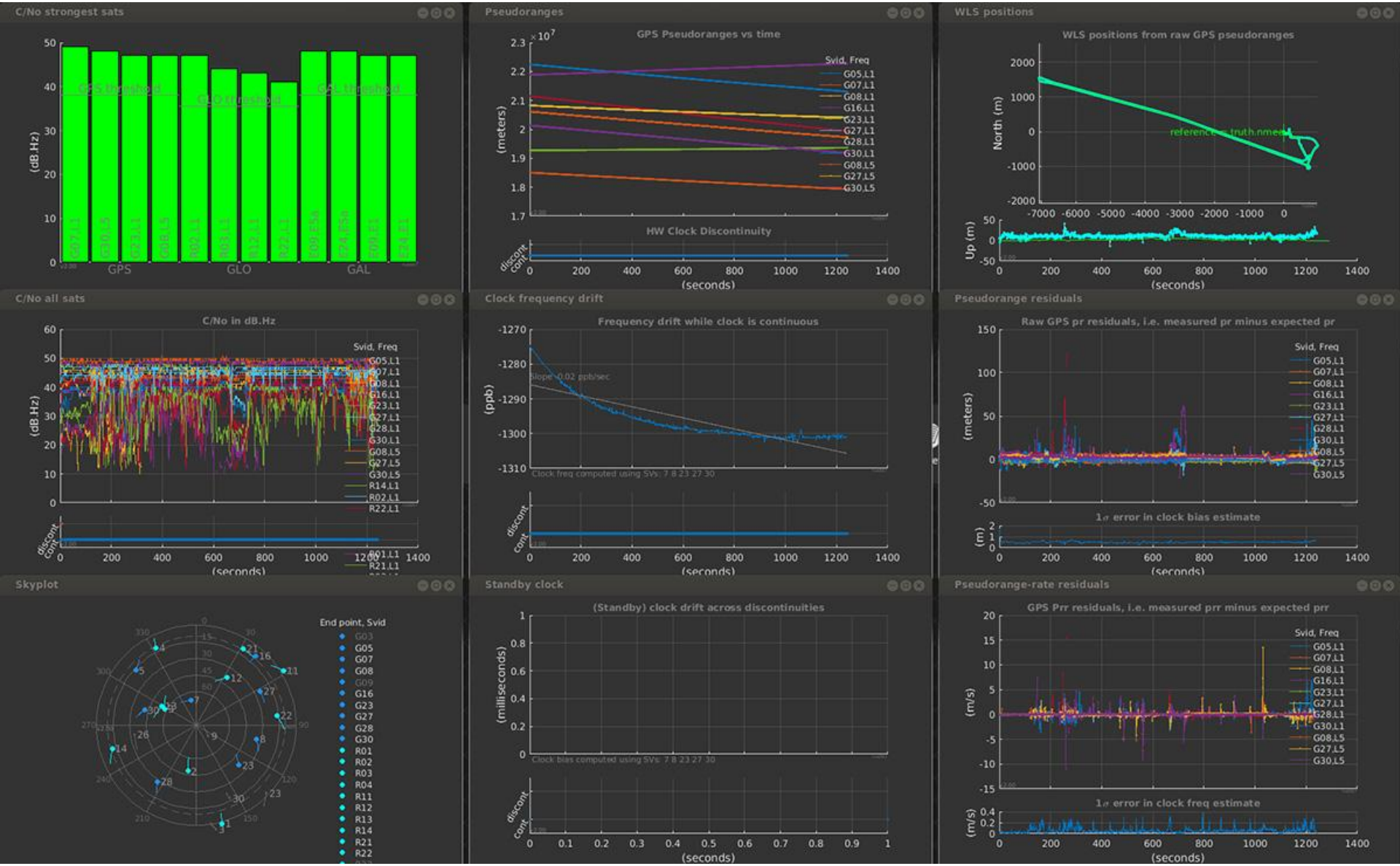
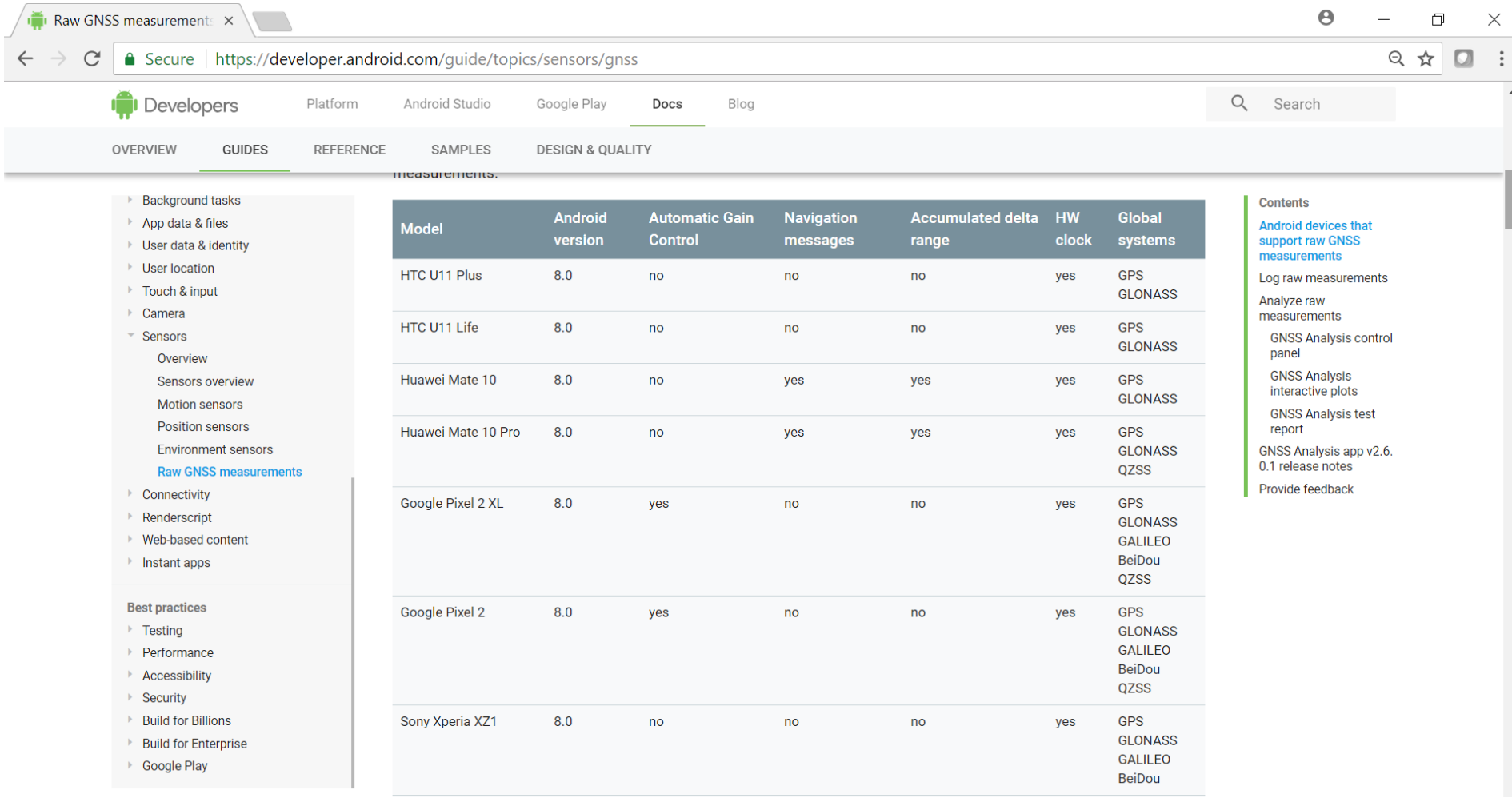


Image courtesy of GPS World



Model	Android version	Automatic Gain Control	Navigation messages	Accumulated delta range	HW clock	Global systems
HTC U11 Plus	8.0	no	no	no	yes	GPS GLONASS
HTC U11 Life	8.0	no	no	no	yes	GPS GLONASS
Huawei Mate 10	8.0	no	yes	yes	yes	GPS GLONASS
Huawei Mate 10 Pro	8.0	no	yes	yes	yes	GPS GLONASS QZSS
Google Pixel 2 XL	8.0	yes	no	no	yes	GPS GLONASS GALILEO BeiDou QZSS
Google Pixel 2	8.0	yes	no	no	yes	GPS GLONASS GALILEO BeiDou QZSS
Sony Xperia XZ1	8.0	no	no	no	yes	GPS GLONASS GALILEO BeiDou

Image courtesy of Google

GNSS Raw Measurements Task Force

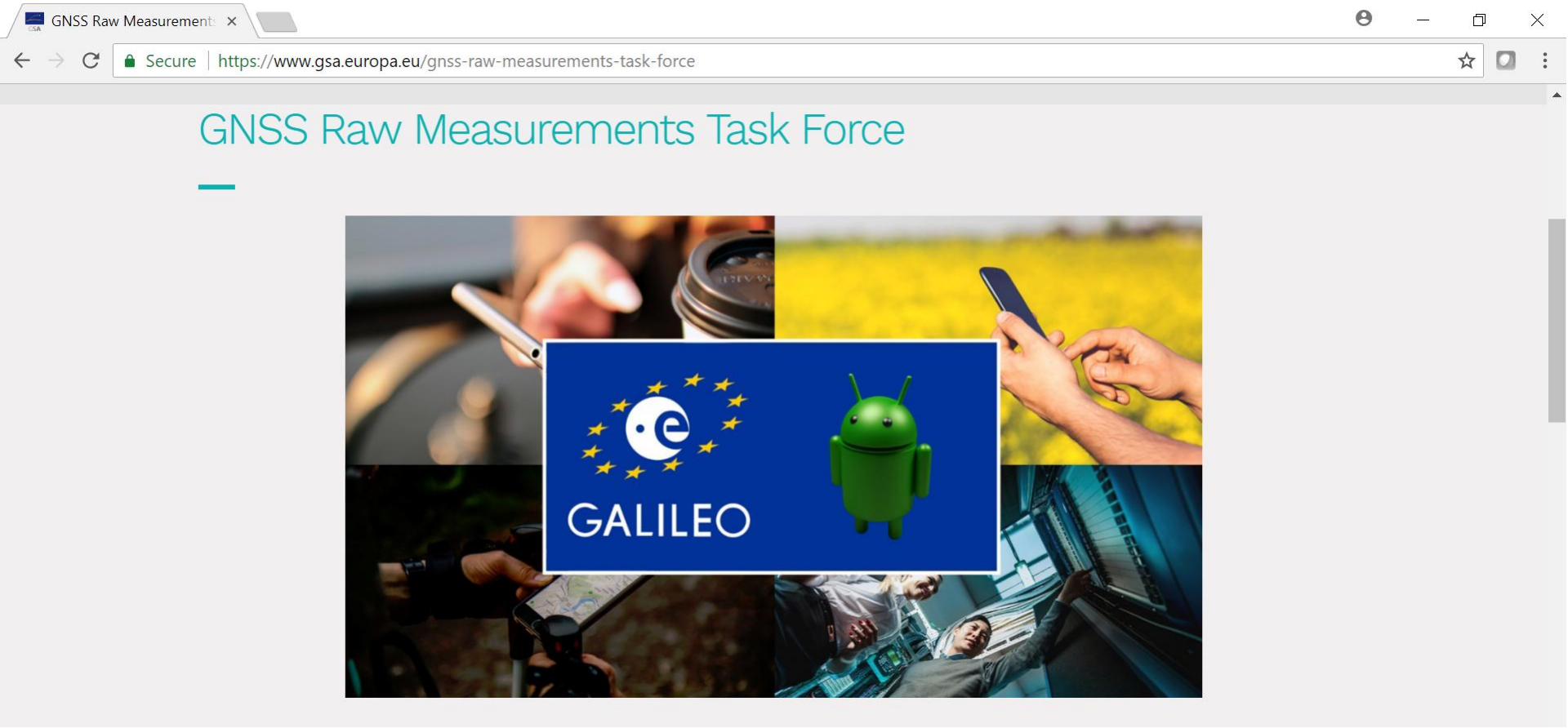


Image courtesy of GSA

Members of the *GNSS Raw Measurements Task Force*

Image courtesy of GSA

The GNSS Raw Measurements Task Force has published a White Paper on

“Using GNSS Raw Measurements on Android devices”

The Paper provides application developers with a broader insight into the topic, including testing results using various positioning techniques, practical tips, and an outloo on its use.

The White Paper is available for download:

www.gsa.europa.eu/gnss-raw-measurements-task-force

Image courtesy of GSA

European Global Navigation Satellite Systems Agency

GNSS Raw Measurements Taskforce Workshop "GNSS Raw Measurements: from research to commercial use"

GSA Headquarters, Prague, 30 May 2018

Draft Agenda

09:00 – 9:30	Welcome coffee
09:30 – 9:40	**Welcome by the GSA management**
09:50 – 10:00	**Galileo and GNSS Raw Measurements Task Force introduction** GSA MKD
10:00 – 10:30	**Google's vision on advanced location services** Frank van Diggelen, Google
10:30 – 11:30	**Android GNSS Raw Measurements for high accuracy applications**
	Quicksurv: smartphone-aided accurate and affordable surveying, Miquel Garcia-Fernandez, Rokubun
	Performance analysis of GPS+Galileo smartphone raw measurements, Augusto Mazzoni, University of Rome "La Sapienza"
	Joshua Critchley-Marrows, NSL, Title TBC
	Accepting proposals
12:15 – 13:00	**Android GNSS Raw Measurements for robustness/crowdsourcing applications** *Name TBC, NSL, Title TBC*
	Lukasz Bonenberg, University of Nottingham, Title TBC
	Initiative for collection of crowdsourced GNSS Android data for GNSS positioning performance studies Renato Filjar and Nenad Sikirica, University of Rijeka
13:00 – 14:00	Lunch
14:00 – 15:15	**Android GNSS Raw Measurements for testing/optimisation applications**
	Moises Navarro-Gallardo, Airbus, Title TBC
	Paolo Crosta, European Space Agency, Title TBC
	Ajay Vemuru, Spirent, Title TBC
	Miguel Ortiz, IFSTTAR, Title TBC
	Raw GNSS data under Android 7 or later: Observable quality and positioning performances René Warnant, University of Liege
15:15 – 16:00	**Future outlook for geolocation in mass market including Galileo contribution**
	Vision on how dual frequency will change the performance levels in mass market Miguel Torroja, Broadcom
	Galileo Differentiators for mass market Name TBC, GSA
	Research and development opportunities Name TBC, GSA
16:00 – 16:30	**Q&A and Final remarks**

Image courtesy of GSA

FLAMINGO

Fulfilling enhanced location accuracy

Looking forward to seeing you on 30 May 2018.