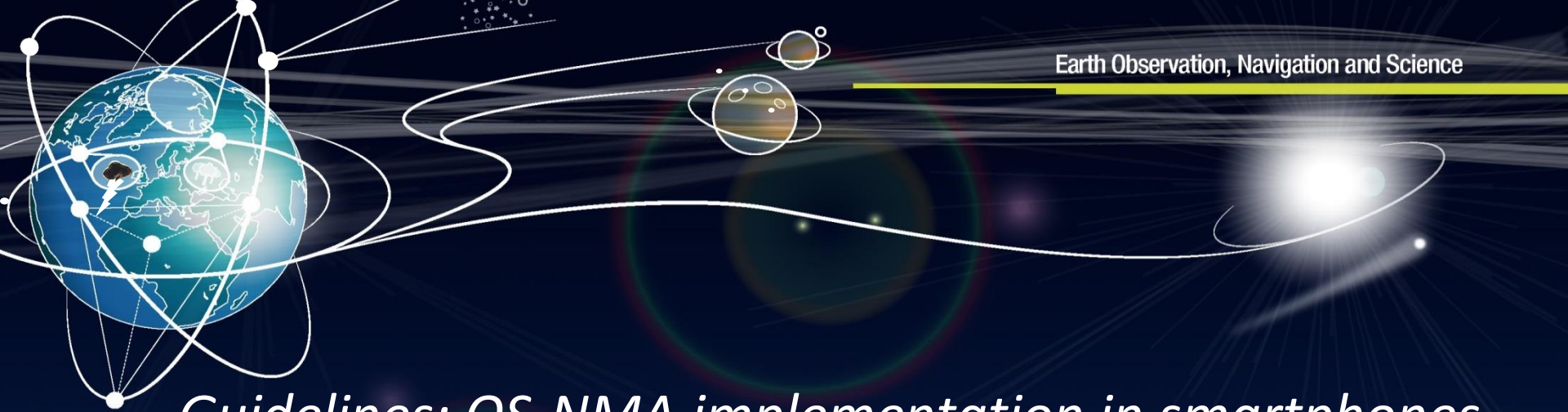


Guidelines: OS-NMA implementation in smartphones

3rd Raw Measurement Task Force Work Shop

Moisés Navarro-Gallardo

26.06.2019

AIRBUS

Agenda

DEFENCE AND SPACE

- GNSS Security & Threats
- OS-NMA
  - Concept
  - Bits allocation

- Android
  - Galileo Navigation Pages
  - Android Smartphones
    - Broadcom Smartphones
      - Pilot Tracking
      - Data Tracking
      - Duty Cycle

- Conclusions

Security

- GNSS signals are weak (10E-16 or -160dBW) → Can easily be overwhelmed by terrestrial signals
- Signal designs are open and unencrypted → Anyone can generate signals that are perceived as valid
- Many motivations to interfere with GNSS → Privacy, economic, criminal, military…

Threats

- Jamming: signal interference, not significant correlation with GNSS signals
- **Spoofing**: GNSS-like signals that may be tracked instead (or along) the intended signals
  - Simulators: Replicate satellite signals without (necessarily) live input
  - Repeaters (meaconing): rebroadcast of live signals with common delay across PRNs
  - Re-radiators: rebroadcast of live signals with different delays

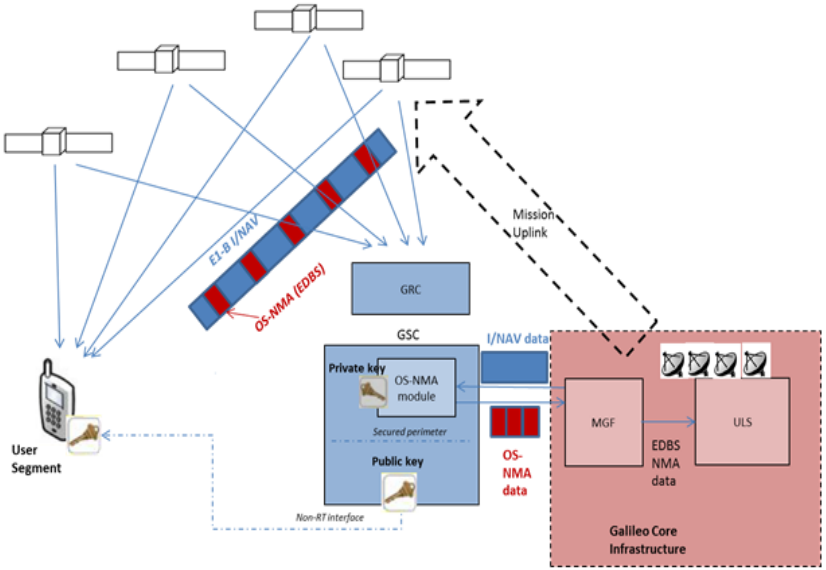
OS-NMA (Navigation Message Authentication)

- The goal is to determine if the message has been generated by Galileo System.

- Galileo System generates the OS-NMA bits. They are included in the I/NAV message broadcasted in E1 Band.

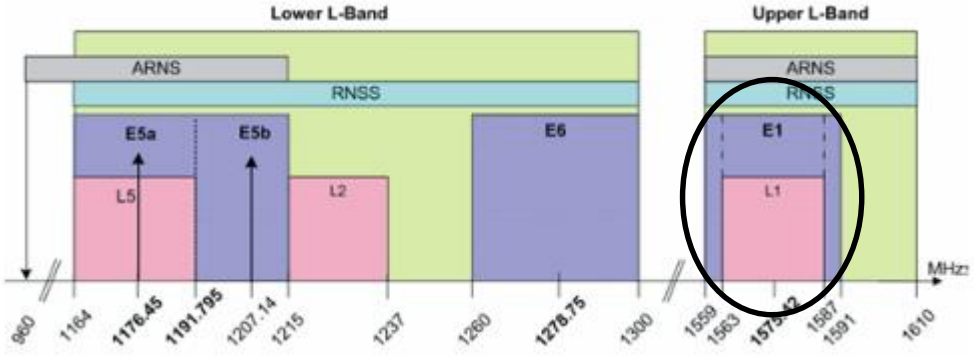
- OS-NMA is Based on TESLA

(Time Efficient Stream Loss-tolerant Authentication)



Galileo is the only GNSS implementing NMA in OS signals

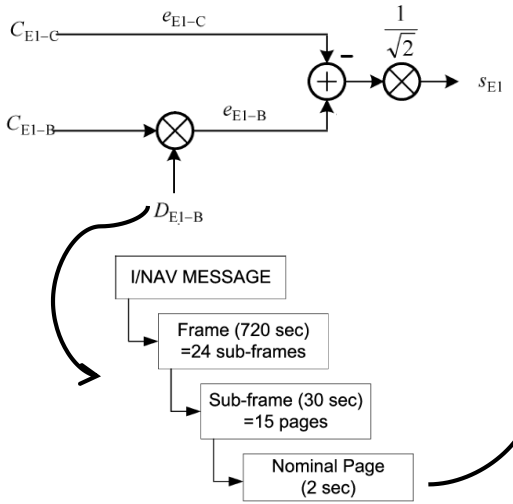
AIRBUS

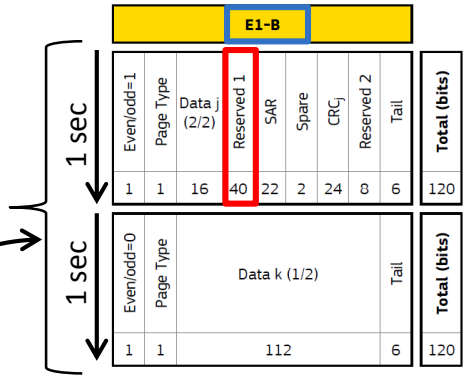


- It is transmitted in the E1 Band
- It is part of the Galileo Open Service
- Two components are transmitted in E1
  - ~~E1C → Pilot Component~~
  - E1B → Data Component

I/NAV Message

OS-NMA





Android provides the raw bits of each GNSS system

Android provides the 228 bits of I/NAV messages (excluding the tail bits)

Only the E1 I/NAV pages contains the OS-NMA 40 bits (Reserved 1)

The method *getData* from the class *GNSSNavigationMEssage* provides the Galileo bits

Android GnssNavigationMessage

getData

Added in API level 24

```
public byte[] getData ()
```

Gets the data of the reported GPS message.

The bytes (or words) specified using big endian for

- For GPS L1 C/A, Beidou D1 & Beidou D2, each
into the last 30 bits in a 4-byte word (skip B31
period of 6, 6, and 0.6 seconds, respectively.
- For Glonass L1 C/A, each string contains 85 c
bytes, with MSB first (skip B86-B88), covering
- For Galileo F/NAV, each word consists of 238
bytes, with MSB first (skip B239, B240), covering a time period of 10 seconds.
- For Galileo I/NAV, each page contains 2 page parts, even and odd, with a total of 2x114 = 228 bits, (sync & tail excluded) that should be fit into 29 bytes, with MSB first (skip B229-B232).

d (30 bits) should be fit
s, covering a time
hould be fit into 11
should be fit into 30-

E1-B

	Even/odd=1	Page Type	Data j (2/2)	Reserved 1	SAR	Spare	CRC$_j$	Reserved 2	Tail	Total (bits)
	1	1	16	40	22	2	24	8	6	120

	Even/odd=0	Page Type	Data k (1/2)	Tail	Total (bits)
	1	1	112	6	120

Developers

https://developer.android.com/reference/android/location/GnssNavigationMessage

AIRBUS

QUALCOMM

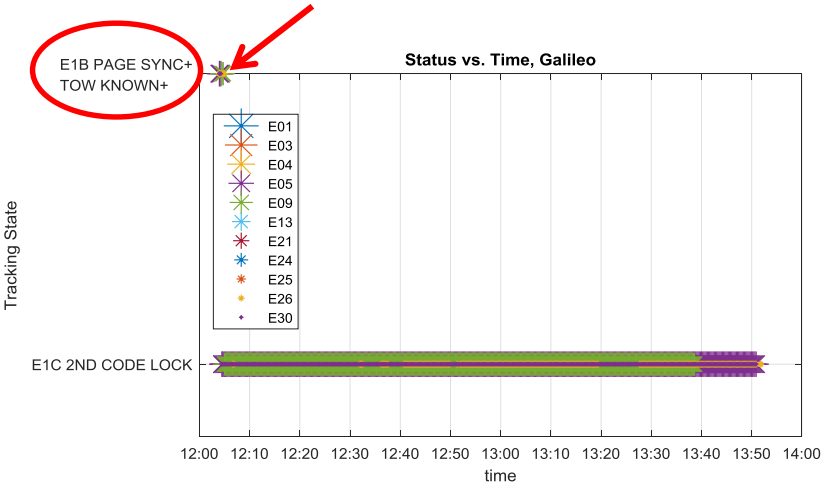
- Currently smartphones based on QUALCOMM GNSS chipsets do not provide navigation messages (nor carrier phase measurements)
- They Cannot be used for OS-NMA

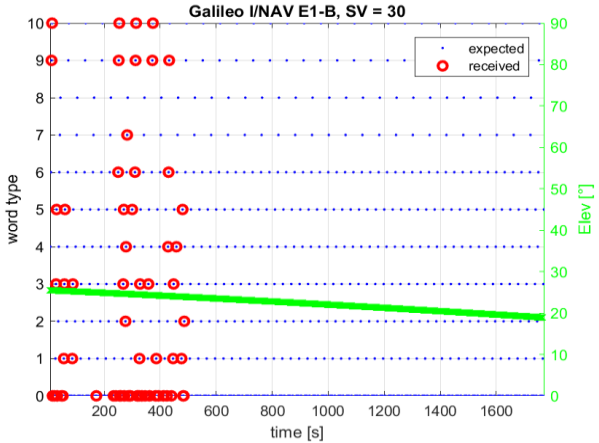
BROADCOM

- Smartphones based on Broadcom GNSS chipsets provide navigation messages and carrier phase measurements
- However there are some limitations
  - Tracking of E1C (pilot component)
  - Duty cycle
- These limitations can be sorted out or mitigated in a certain extent

BROADCOM

- The GNSS chipset only tracks the Galileo Data Component (E1B – OS-NMA) at the beginning of the location request.
- When the navigation data is obtained the tracking moves to the Pilot (2nd Code Lock) → **No Nav Pages**





BROADCOM

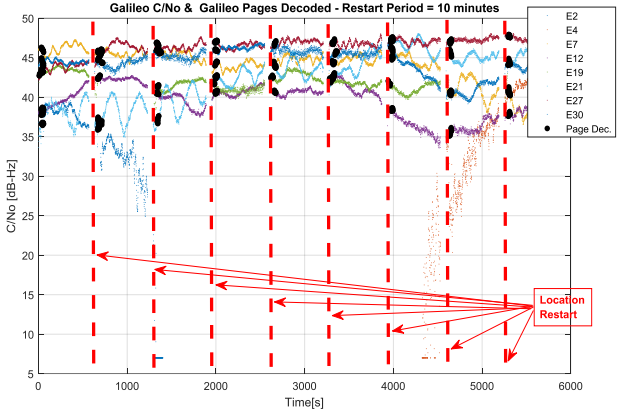
- Sat 30 → The GNSS chipset is able to decode all the word types: Ephemerids & clocks, timing and almanac
- The occurrence is really low

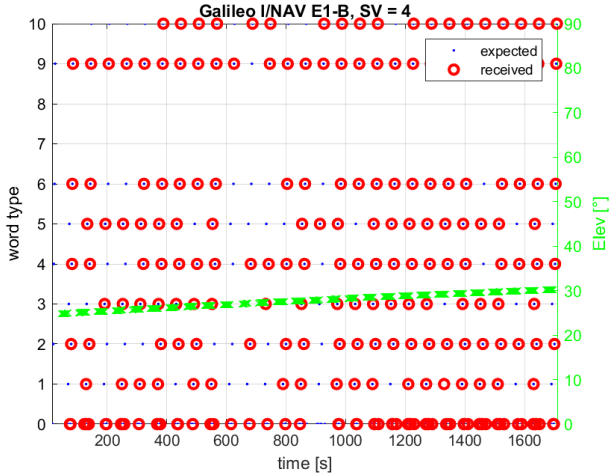
Smartphones:
(Samsung S8, Huawei P10, etc)

Pilot Tracking: Increasing the Number of Pages

The following steps are conducted:

- The Android Location is requested continuously
- After some seconds the Location is Stopped
- There is no request of location during few seconds
- The assisted data is cleared and the Location request starts again



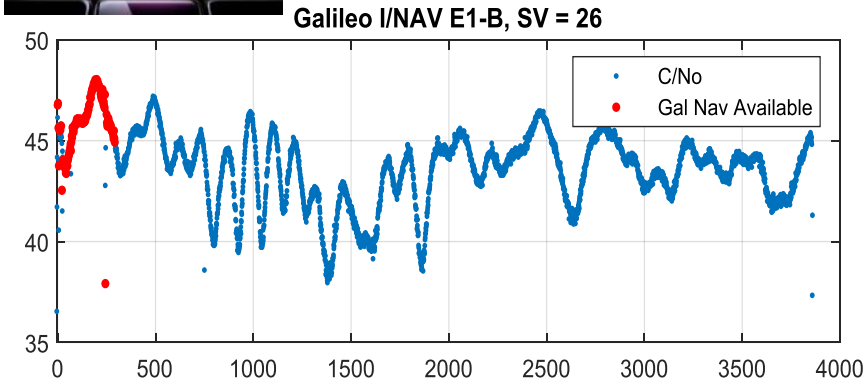


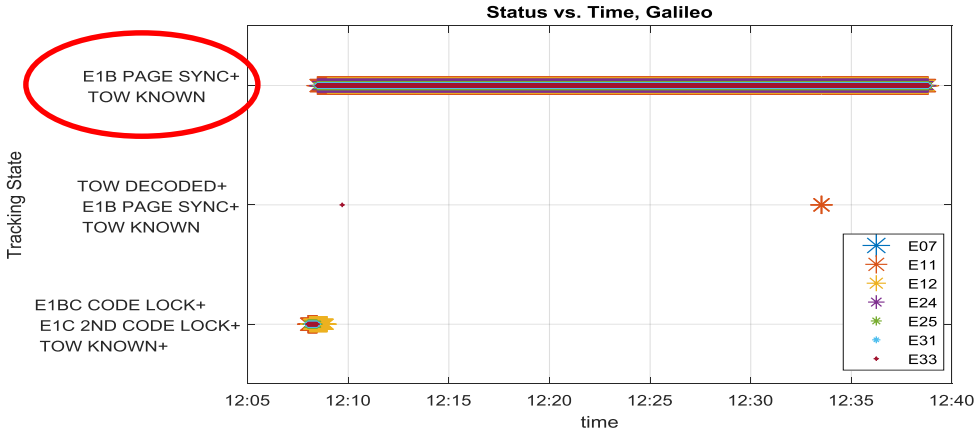
- Several rest and location request times have been tested in order to assess the best performance, i.e. the bigger number of Galileo Decoded Navigation Pages:
  - 30 seconds requesting Location
  - 20 seconds resting
- The occurrence of Decoded Galileo Pages has increased considerably compared to the continuous tracking

Data Tracking

- Few smartphones based on Broadcom track the Galileo Data Component (E1B – OS-NMA) continuously

Smartphones: Samsung S10/S10+





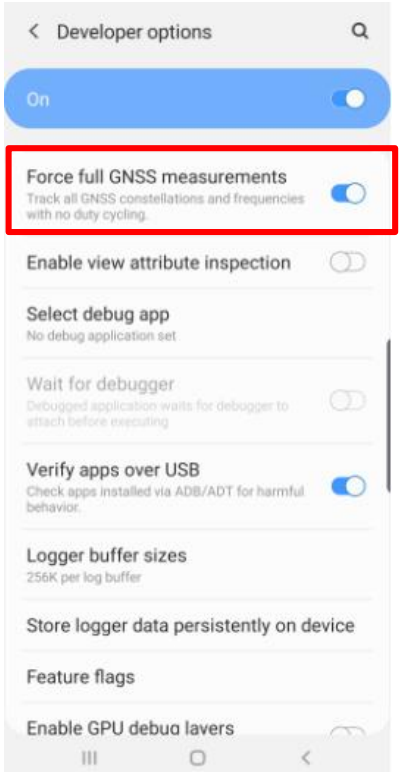
Data Tracking: Duty Cycle

- The tracking is based on the **Galileo Data Component** during all the measurements
- Galileo Navigation Pages are decoded during 300 seconds (5 minutes) → High occurrence
- However, after 300 seconds no more Galileo Navigation Pages are decoded
- The GNSS Chipset is affected by the **Duty Cycle → after 5 minutes**

Data Tracking: <u>Duty Cycle Disabled</u>

- Android 9 offers the option to disable the Duty Cycle
- Enable Developer Options and activate:

Force full GNSS measurements



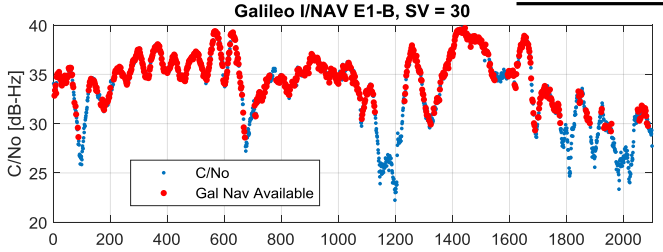
Data Tracking: <u>Duty Cycle Disabled - Bug</u>

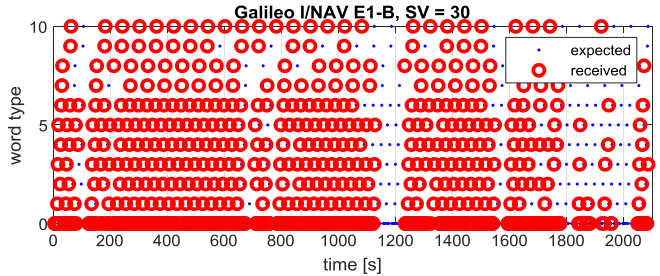
- However, even when the Duty Cycle is disabled, the smartphone is not able to provide Galileo Pages after 5 minutes
- The smartphone goes in to Duty Cycle
- **This bug will be fixed in coming firmware updates**

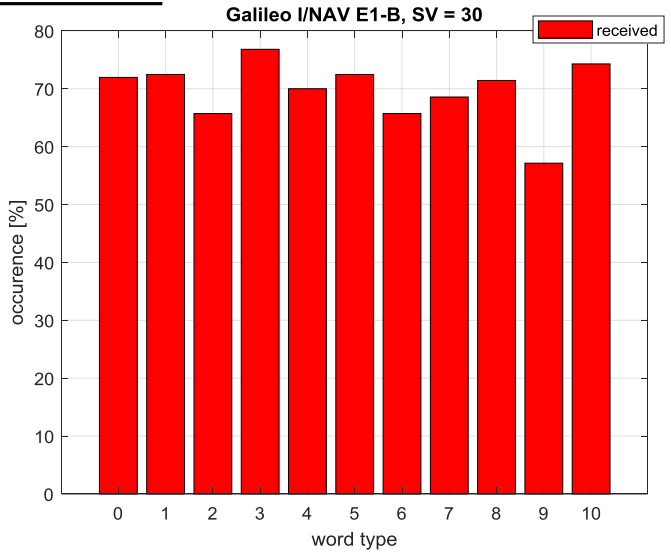
Data Tracking: Specific Firmware Version

- GSA has a Samsung S10+ unit with a specific Firmware version that solves the Duty Cycle bug
- **Navigation Pages are decoded during all the pass** (2100 seconds)
- Almost 75% of the pages are properly decoded

Windowsill Scenario







OS-NMA: Android Smartphone Summary

	Suitable for OS-NMA?	
	Pilot Tracking*	**Data Tracking****
Broadcom	**NO**	**YES**
QUALCOMM	No Navigation messages are currently provided	

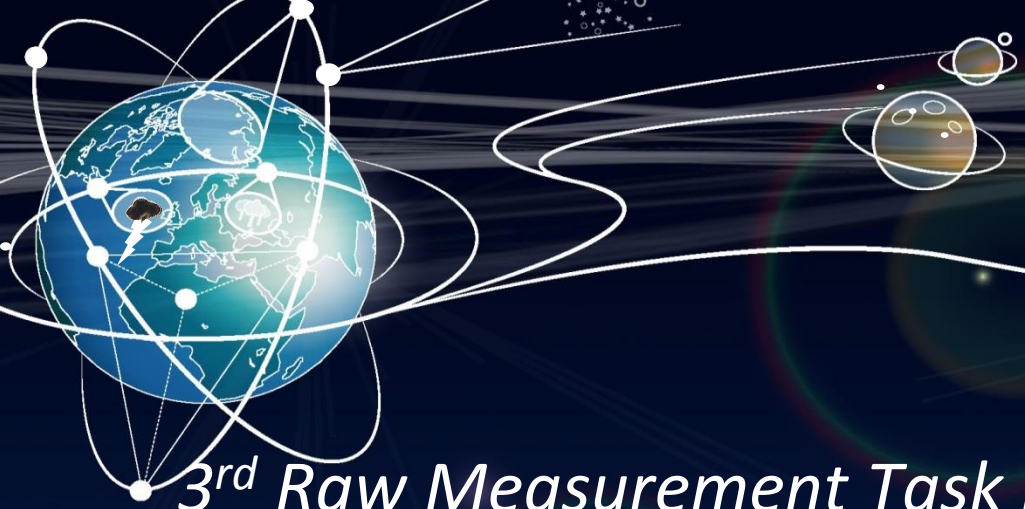
* It provides a more robust tracking. Request of Location must be restarted after some minutes to increase the number of pages

** Currently only Samsung S10/S10+ are based on Data tracking. Duty cycle must be disable (a bug does not allow it yet). GSA has specific units to support developers until bug is fixed.

Conclusions

- Android brings the capability to make available the Galileo Navigation Pages to the final users
- Currently only smartphones based on Broadcom chipsets provide Galileo Navigation Pages
- **Almost all Broadcom chipsets privilege Galileo Pilot tracking over Data tracking** (more robust)
  - A reset location process has been shown in order to increase the number of decoded pages
- Few Broadcom chipsets allow for continuous data decoding: **Samsung S10/S10+**
  - Possibility to disable the Duty Cycle is existing, but not working properly yet
  - A further firmware version is expected to come soon
- **GSA makes a working unit available for developers to test their new NMA based solutions!!**

Now is your time to Develop!!!



Earth Observation, Navigation and Science

3rd Raw Measurement Task Force Work Shop

Moises Navarro-Gallardo

Moises.navarro-gallardo@airbus.com

AIRBUS