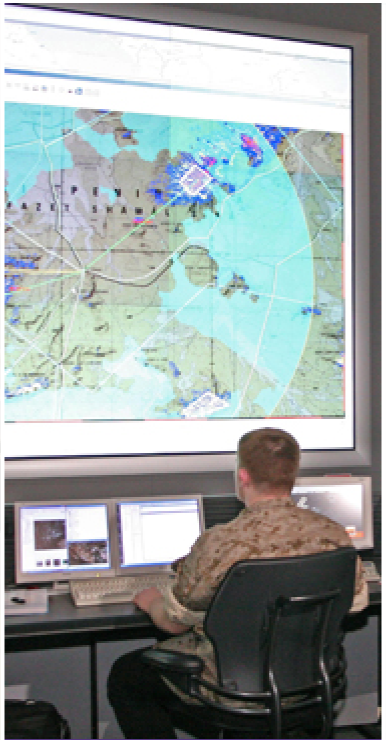




Hybridizing Signals of Opportunity and Global Navigation Satellite Systems within Cognitive Radios

SDR'11 Winncomm, session 7B, Brussels, June 24

François Delaveau, Dominique Heurguier

SUMMARY

Introduction – Objectives of geo-referenced sensing
- Cognitive Radios and sensing
- New need expressions for geo-referenced sensing
- Considerations about GNSS principles - example of GPS
- Considerations about frequency coverage

Concept of Augmented Navigation (A-GNSS)

Use of Signals of Opportunity (SoO)

Why and how merging geo-referenced sensing and navigation within CR ?

A few ideas for processing and procedures

Signal processing - Special case of data aided technique

Practical implementations
- Content of a GNSS device
- Example of possible architecture

Conclusion - perspectives

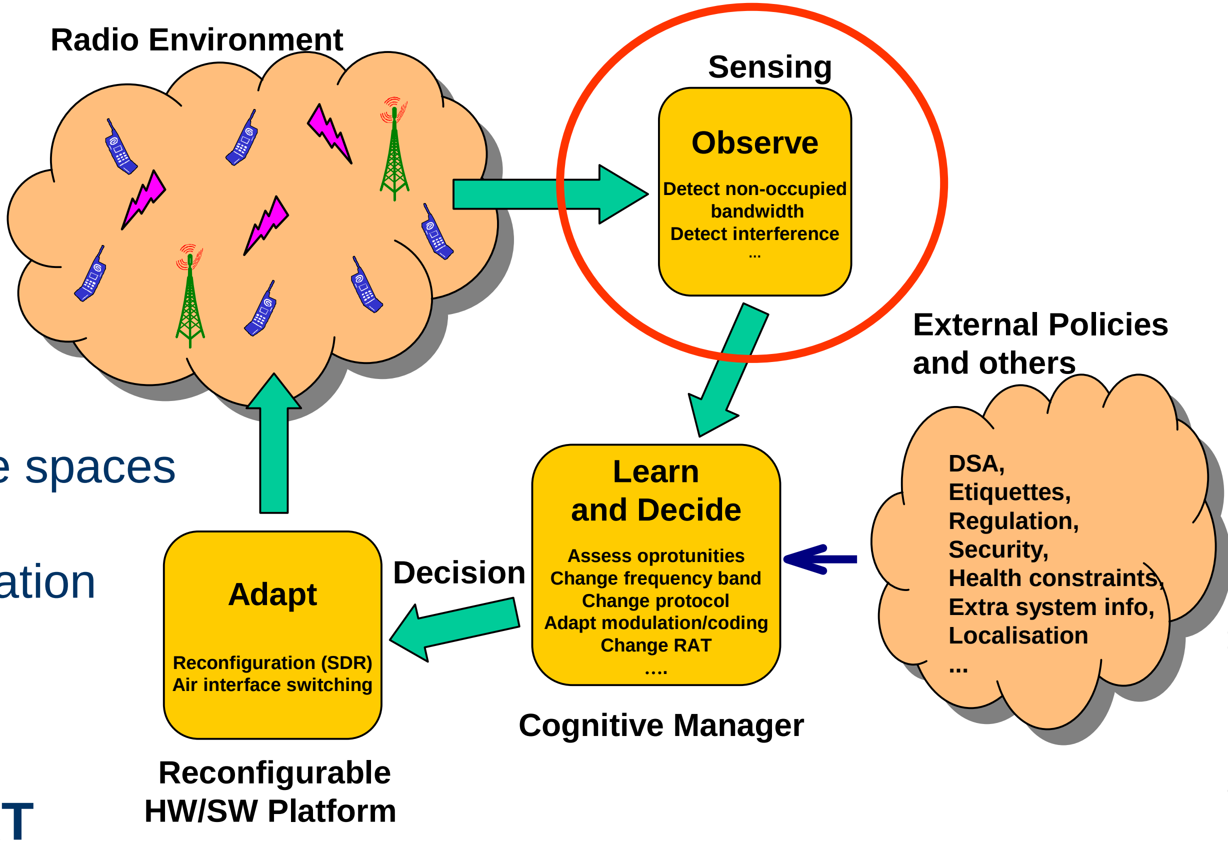
THALES

Glossary - Definitions

AOA:	Angle of Arrival
ASIC:	Application Specific Integrated Circuit
CR:	Cognitive Radio
GNSS:	Global Navigation Satellite Systems
A-GNSS:	Augmented (Aided) GNSS
COM:	COMmunication (device, terminal..)
DVB-T/H:	Digital Video Broadcast –Terrestrial/Handheld
EGNOS:	European Geostationary Navigation Overlay Service
FF:	First Fix (first position estimation by navigation systems)
FPGA:	Field-programmable Gate Array
GAL:	GALileo Navigation Systems (CEE)
GLO:	GLObal NAvigation Systems (CEI)
GPS:	Global Positioning Systems (US and worldwide)
IF:	Intermediate Frequency
IP:	Intellectual Property (meaning vitual component implanted within FPGA)
NAV:	Navigation (Device)
NoO :	Network of Opportunity
Oor:	Order of range
PRN:	Pseudo Random Noise (code used for synchro. measurement inside GNSS systems)
RA:	Radio Access
RAT:	Radio Access Technology
SBAS:	Satellite-Based Augmentation System
SDR:	Software Defined Radio
SM:	Spectrum Monitoring
SoO:	Signal of Opportunity
TDOA:	Time (Difference) Of Arrival
TOA:	Time Of Arrival
TTFF:	Time To First Fix
UHF:	Ultra High Frequency
VHF:	Very High Frequency
WF:	Wave Form

Introduction – Objectives of sensing within Cognitive radios

Sensing is part of the cognitive process



Sensing provides radio information elements to the cognitive manager

- search { for free carriers / for spectrum white spaces
- enhance the radio access
- facilitate interference mitigation

=> Sensing is mainly "communication and RAT oriented"

Introduction – New need expressions for geo-referenced sensing

UIT-R, RSPG and CEPT:

- **Radio Spectrum Policy Group SE43(11)Info01 «Opinion on Cognitive Technologies»** (relevant to disseminated Spectrum Monitoring)
- **CEPT SE43(11)04 "Combination of geo-location database and spectrum sensing techniques"** (relevant to geo-referenced sensing)
- **Initiative ANFR/Thales : NEW QUESTION ITU-R [SPEC-MONIT-EVOL]/1**
  - What are the new considerations for monitoring of radiocommunication systems that are based on new technologies?
  - What are the new approaches that may be required in terms of organisation, procedures and equipment to monitor systems based on future radiocommunication technologies?
  - What are the needs for administrations in order to implement the new approaches to monitor systems based on future radiocommunication technologies?
- **Version 2011 of the "Spectrum Monitoring Handbook"**

Joe Mittola:

- **Conference "Secure Geospatial Dynamic Spectrum Access"**

  at GDR ISiS TELECOM Paris tech 9 Mai 2011 "10 ans de Radio Intelligente : bilan et perspectives"

  (http://www.lirmm.fr/soc_sip/index.php/journees-thematiques/methodes-et-outils-de-conception-ams-a-rf)

Introduction – New need expressions for geo-referenced sensing

Operators’ interest:

- **Maps of network radio environments**
  - Locate zones where interference and propagation artefacts are present
  - Identify and locate hHot spots for access demand and spectrum use
  - Location of spectrum white spaces
- **Self synchronization and Self Location within ad-hoc network**
- **Upgrade of reliability and duration of synchronization procedure**
- **RAT upgrade of SDR and CR: see below**

Upgrade of Radio Access Technologies:

- **Better management of Space Division Multiple Access (SDMA)**
- **Upgrade of MIMO technology performances for RA**
  - Self Location of terminals & infrastructure + information of Cognitive Manager
  - Space/time estimation of propagation channel filter
  - Lead to optimal MIMO RA schemes

Regulators UIT-R, RSPG and CEPT interest:

- **Opportunity of geo-referenced sensing for disseminated spectrum sensing**

  See conf SDR’11 Winncomm Europe session 6B “Oriented processing of communication signals for Sensing and disseminated spectrum monitoring”

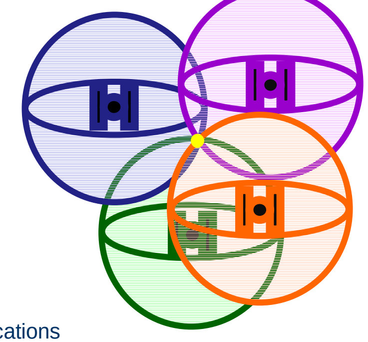
THALES

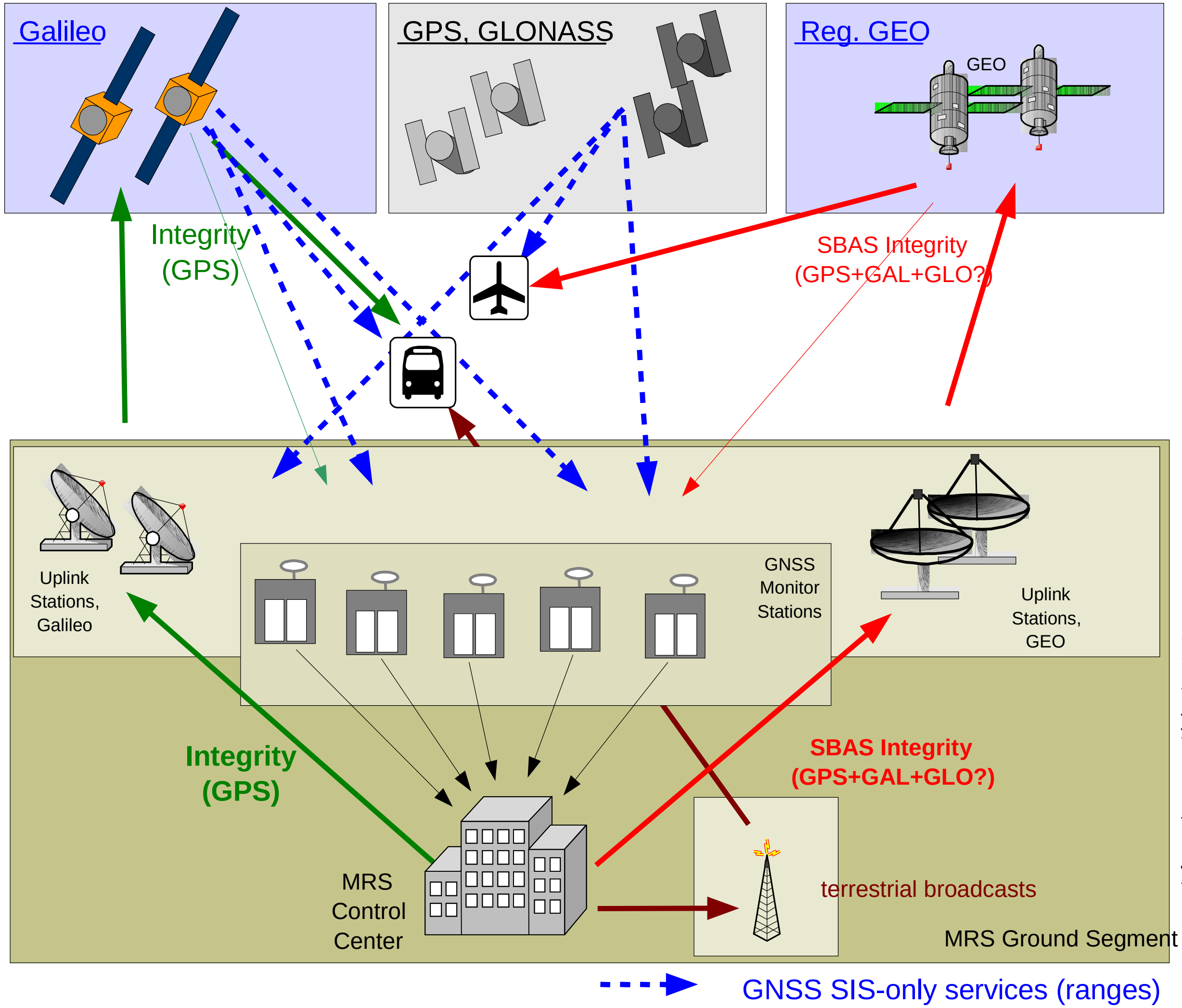
Introduction – considerations about GNSS principles

1/ LEO (700 km alt.) satellites transmitting PRN codes

2/ Measurements of Propagation delays of PRN codes
+ NAV msg decoding

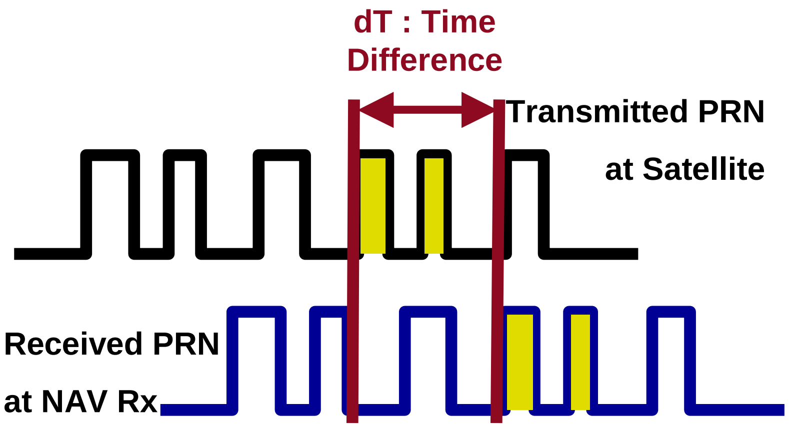
Accurate 3D location
(x,y: 13m ; z: 22m)
when ≥ 4 received and decoded satellites
(4th sat. for recovering clock errors)



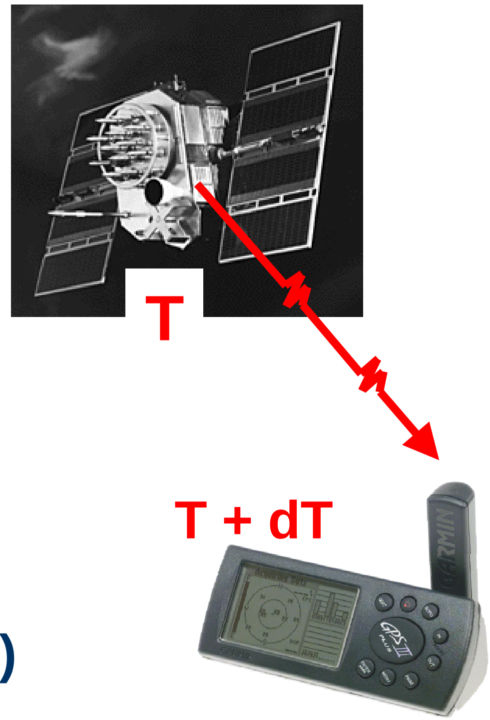


Introduction – example of GPS

Delay measurement at "PRN" codes + decoding of NAV messages (PRN number, GPS system time, propagation correction, orbitography info., etc.)

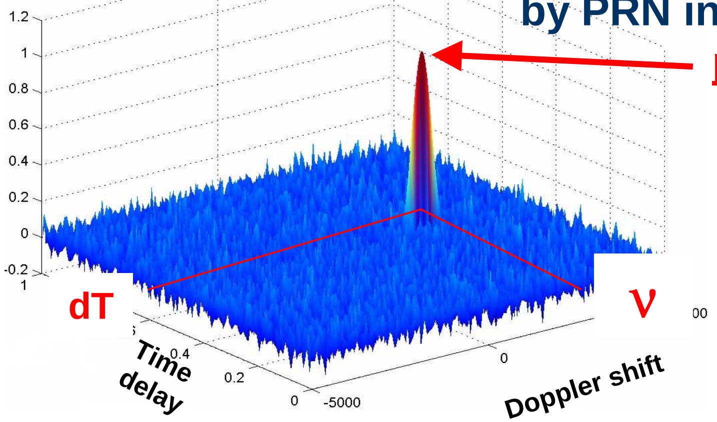


Transmitted signal at instant T (known by decoding NAV msg)



Detection and synchronization: by PRN intercorrelation computation

peak { at time dT / at Doppler ν



Sat-Rx Range = f(dT)

- → **3D TOA location**
- → **First Fix = first Position estimate**
- → **Tracking of Position / Speed / Time**

Introduction – considerations about frequency coverage

Example of Frequency plans that CR/sensing have to deal with (potential SoOs and NoOs for A-GNSS)

System:	Uplink Frequency Band [MHz]	Downlink Frequency Band [MHz]	Channel spacing	Modulation	Max. Output Power
GSM 900 DCS 1800 PCS 1900	890 - 915 1710 - 1785 1850-1890	935-960 1805 - 1880 1930 - 1970	200 KHz	GMSK + 3π/8 QPSK	~2W
W-CDMA	890 - 915 1920 - 1980	935-960 2110 - 2170	5 MHz	OCQPSK	0,25 W
LTE	890 - 915 2500-2570	935-960 2620-2690	1,4 - 5 MHz	OFDMA SC-FDMA	0,25 W
WIMAX	2402 – 2480 3400 – 3600 5150 - 5850		10 MHz	OFDM	0,25 W
WIFI	2402 - 2480 5150 - 5850		20 MHz 20 – 80 MHz	OFDM	0,1 W
Bluetooth	2402 - 2480		157 KHz	0.5BT - GFSK	0,01 W
WiGig	57 – 65 GHz		2 GHz	QPSK, QAM OFDM	0,1 W

Source : A Kaiser, GDR Soc Sip Paris tech - 10 Mai 2011

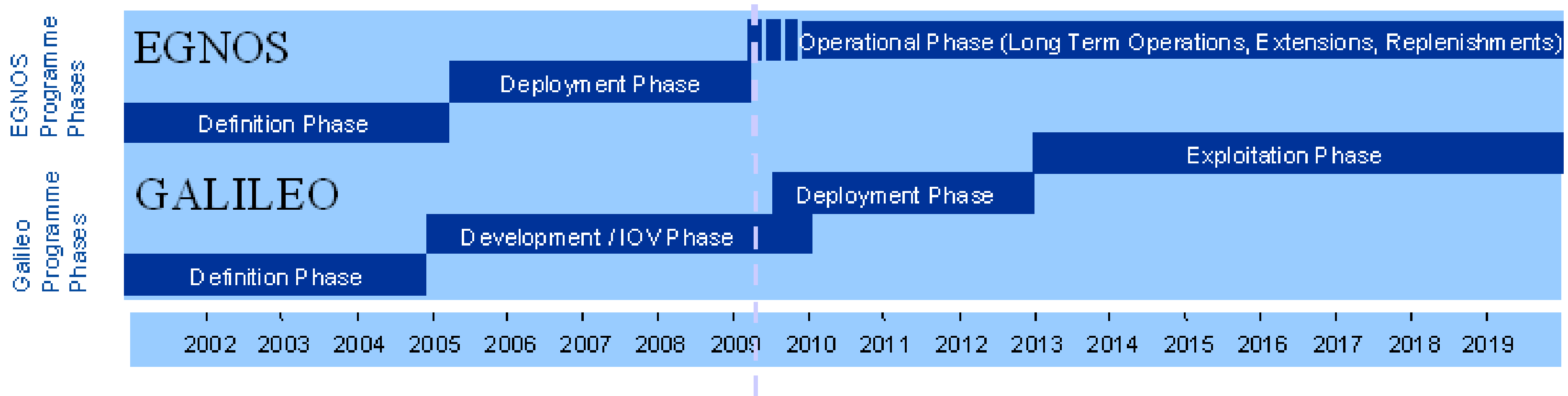
GNSS frequency plans

L1 : 1200 MHz
L2 : 1600 Mhz
+
L band extension
(GPS GAL GlO)
+
Prospective S&C band extensions

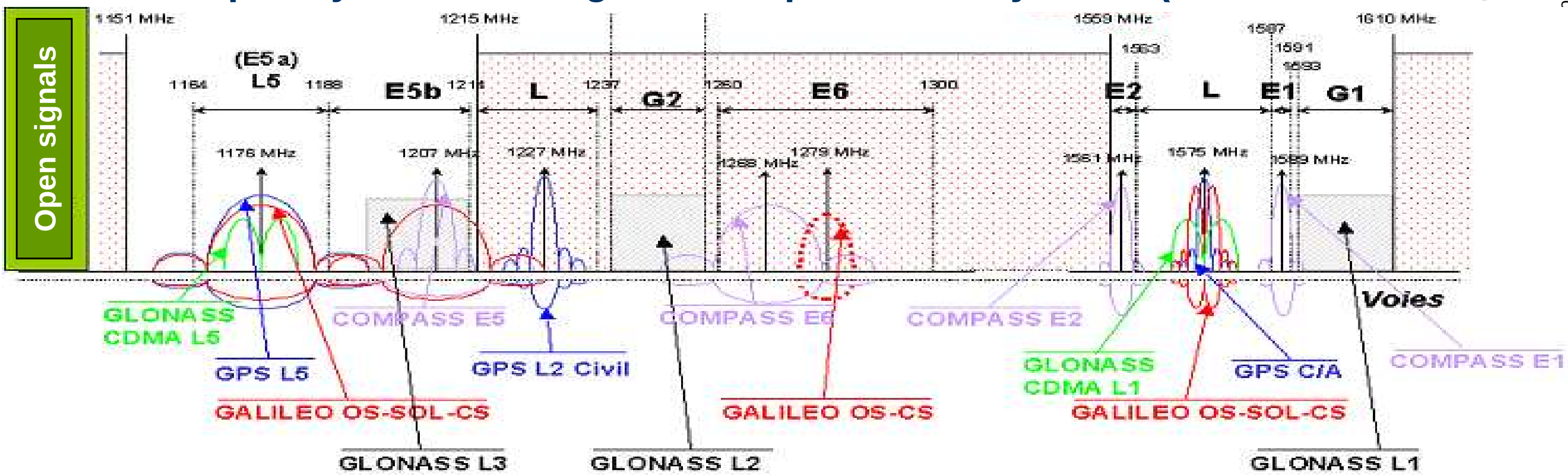
are close to 4G frequency plans

Introduction – considerations about frequency coverage

GNSS system Developments plans by ESA, GSA and CEE



Frequency share among L band open GNSS systems (Galileo, GPS, Glonass)

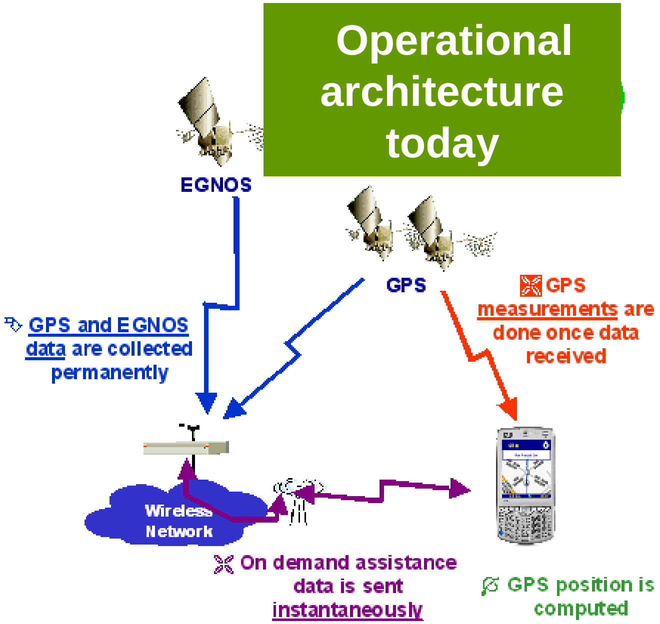


Concept of augmented navigation (A-GNSS)

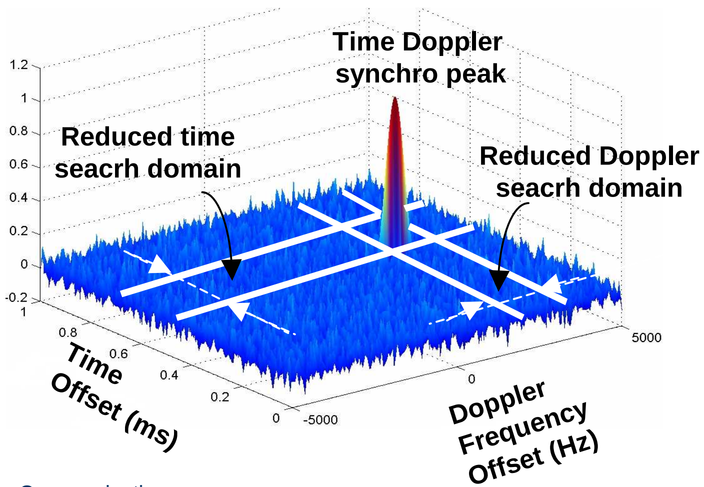
1/ Decode broadcasted signaling relevant to network topology of cellular networks (Tx or cell identity+location+synchro., etc.)

2/ Decode dedicated NAV messages (ephemerids, system time, propagation corrections, PRN number, etc.)

3/ Reduce the time/Doppler/code domain for NAV providing the FF



Assisted GPS

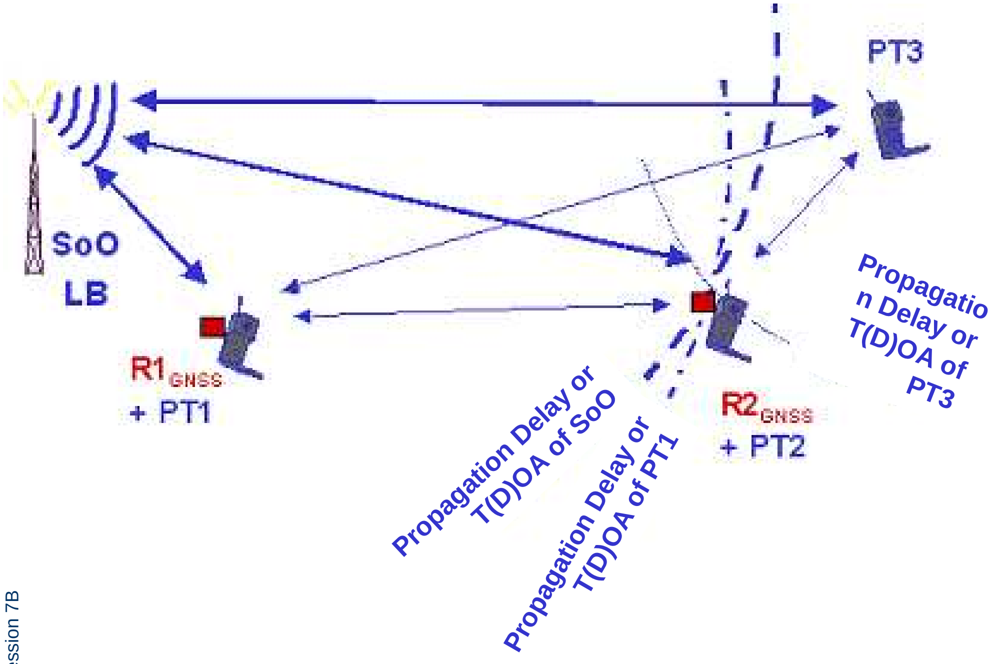


Reference Location	• Cell Size <35km (typ. Urban : 1km)
Reference Time	• GPS Time Tag • BTS clock Stability : 10^{-9}
Navigation Model	• Ephemeris + Clock Correction (Frame 1-3 GPS message)
Ionosphere Corrections	•Klobuchar model
Differential Corrections	•DGPS
Real Time Integrity	•Real Time Alerts
Almanacs	•Constellation Almanacs
UTC Model	•UTC Parameters
Acquisition Assistance	•List of Visible Satellites, Code phase, Doppler
Ephemeris Extensions	•Extended validity ephemeris (7 days)

THALES

Hybridizing SoOs and GNSS within cognitive radios

Use of Signals of Opportunity (SoOs)



First concept: Direct use of SoOs Low HDW impact

1/ Demodulates COM signals and decodes broadcasted signaling.
2/ Exploits COM synchronization and propagation delay estimates
3/ Merges informations at PT2,
4/ transmits to $R2_{GNSS}$

5/ → reduces Time / Doppler / Code research domain for FF inside $R2_{GNSS}$

Advanced concept : Complete use of NoOs Higher HDW impact

1/ Upgrades synchronization of Wide band COM Signals over multiples carriers
2/ Computes and exploits the "Time (Difference) Of Arrival"

3/ Merges infos within PT2
4/ Fuses synchro. + location estimators
5/ Transmits to $R2_{GNSS}$

6/ Replaces the FF inside $R2_{GNSS}$

Why merging geo-referenced sensing and navigation within CR ?

I/ Close frequency ranges of both sensing and GNSS applications

see above

II/ Close hardware and software performances requirements

CR/SDR : expected BW are 10 to 40 MHz, expected noise factor are 5 to 6 dB
embedded computing capabilities
NAV devices : usual BW are no more than 20 MHz, same o.o.r. for radio performances

III/ Weakness of "GNSS"in adverse env^{TS} where radios are still present

Indoor
urban canyon
tunnels
} **are expected to be well covered by 3G/4G radios**

IV/ → Strong hopes for a mutual enhancement of sensing and NAV

IV-A/ Geo reference is a strong added value for sensing of SDR/CR
IV-B/ GNSS time and location is a strong added value for Dynamic and opportunistic RA
IV-C/ Sensing directly provides detection of SoOs and NoOs + relevant information:
{ Identities and location of components (network Data Base).
synchronization and delay measurement, etc.

=> A natural trend is to merge sensing and SoOs capabilities within SDR/CR by adding suitable estimators of position for the FF

How merging geo-referenced sensing and navigation within CR ?

A-GNSS/SoOs indoor solutions based on WiFi

Existing narrow range location solutions are provided by operators for indoor
=> identification of WiFi BS
=> directly leads to location

Digitial TV SoO solutions (ex ROSUM corporation developments)

Based on synchronization of multiple DVB-T/H signals (synchronized DVB-T Tx)

See http://www.prnewswire.co.uk/cgi/news/release?id=231072 and http://www.rosum.com

Augmented-GNSS within 2G/3G Radio cell Networks

Numerous existing solution provided by 2G/3G operators for emergency calls and for commercial applications.

⇒ **Merging these applications within the same SDR/CR device**

⇒ **Upgrading GNSS coverage integrity and accuracy by introducing**

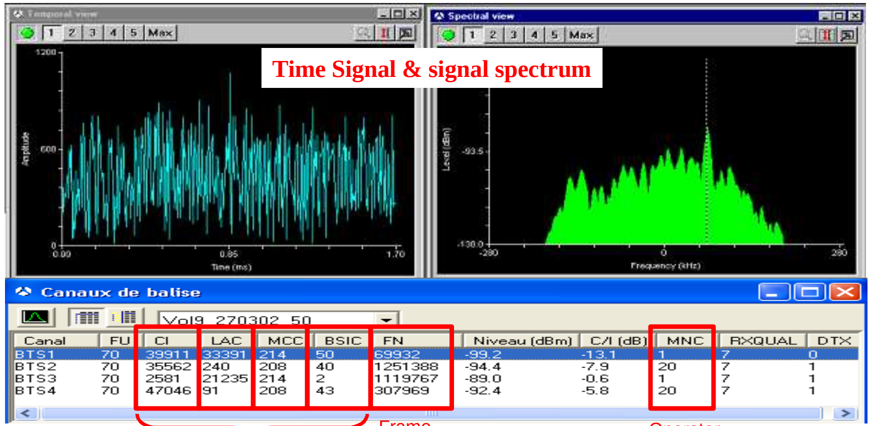
. Highly accurate synchronization and T(D)OA+AOA estimators on SoOs

. Advanced fused location estimators of { symbolic information (decoded in signaling) / physical parameters measured at radio links.

Hybridizing SoOs and GNSS within cognitive radios

A few ideas for processing and procedures

GSM EXAMPLE



Canal	FU	CI	LAC	MCC	BSIC	FN	Niveau (dBm)	C/I (dB)	MNC	RXQUAL	DTX
BTS1	70	39911	33391	214	50	69932	-99.2	-13.1	1	7	0
BTS2	70	35562	240	208	40	1251388	-94.4	-7.9	20	7	1
BTS3	70	2581	21235	214	2	1119767	-89.0	-0.6	1	7	1
BTS4	70	47046	91	208	43	307969	-92.4	-5.8	20	7	1

Cell identity

Frame Synchro.

Operator identity

Decoded Cell frequency allocation

BTS1

BTS2 70 101

BTS3 113 114 115 116 117 118 119 120

Pb within frequency planning

Decoded Neighbour beacon frequencies

70 98 99 100 102 103 104 107 108 111

90 94 100 104 110 116 118 124 675 681 689 697 705

70 101 103 110

Example of decoded frequency planning within GSM signaling

A/

Exploit synchronizations of SoOs at very large frequency plans

(requires ambiguity management)

+

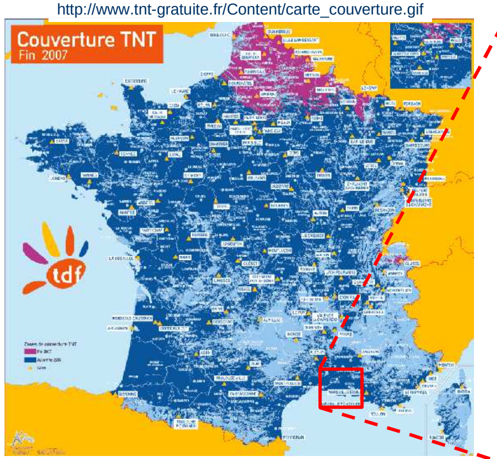
Exploit the broadcasted signaling of NoOs - GSM Example

B/

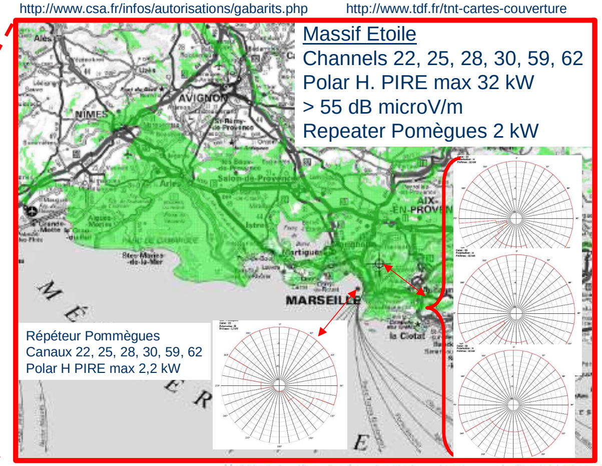
Exploit existing data bases about NoOs

DVB-T Example

http://www.tnt-gratuite.fr/Content/carte_couverture.gif



http://www.csa.fr/infos/autorisations/gabarits.php http://www.tdf.fr/tnt-cartes-couverture



THALES

A few ideas for processing and procedures

I/ Stand Alone processing

When you have no knowledge at all

=> first step is blind procedure

=> second step is oriented processing when you have got info. From 1st step

"Exotic" signals or military signals

II/ Oriented processing,

When you have partial knowledge (semantic description of signal)

When you have data bases of signal characteristics

=> expert approach

Most of civilian SoO

III/ "Data aided" or cooperative processing

When you have complete information of parts of the signal

(GSM middambles, UMTS scrambling codes, DVB/Wimax/LTE pilots, etc.)

When you have data bases of signal sequence + low search combinatory

=> inter-correlation / matched filter approach

All GNSS signals
Most of civilian digital standardized SoOs

THALES

Signal processing - Special case of data aided techniques

"Direct" Inter-correlation with reference known signals

GSM middamble, UMTS codes, DVB/Wimax/LTE pilots, etc.

- Early detection and recognition
- Protocol structure recovery
- **Accurate synchronization**

Direct identification

- Modulation parameters
- Radio access protocol
- Set of coding schemes

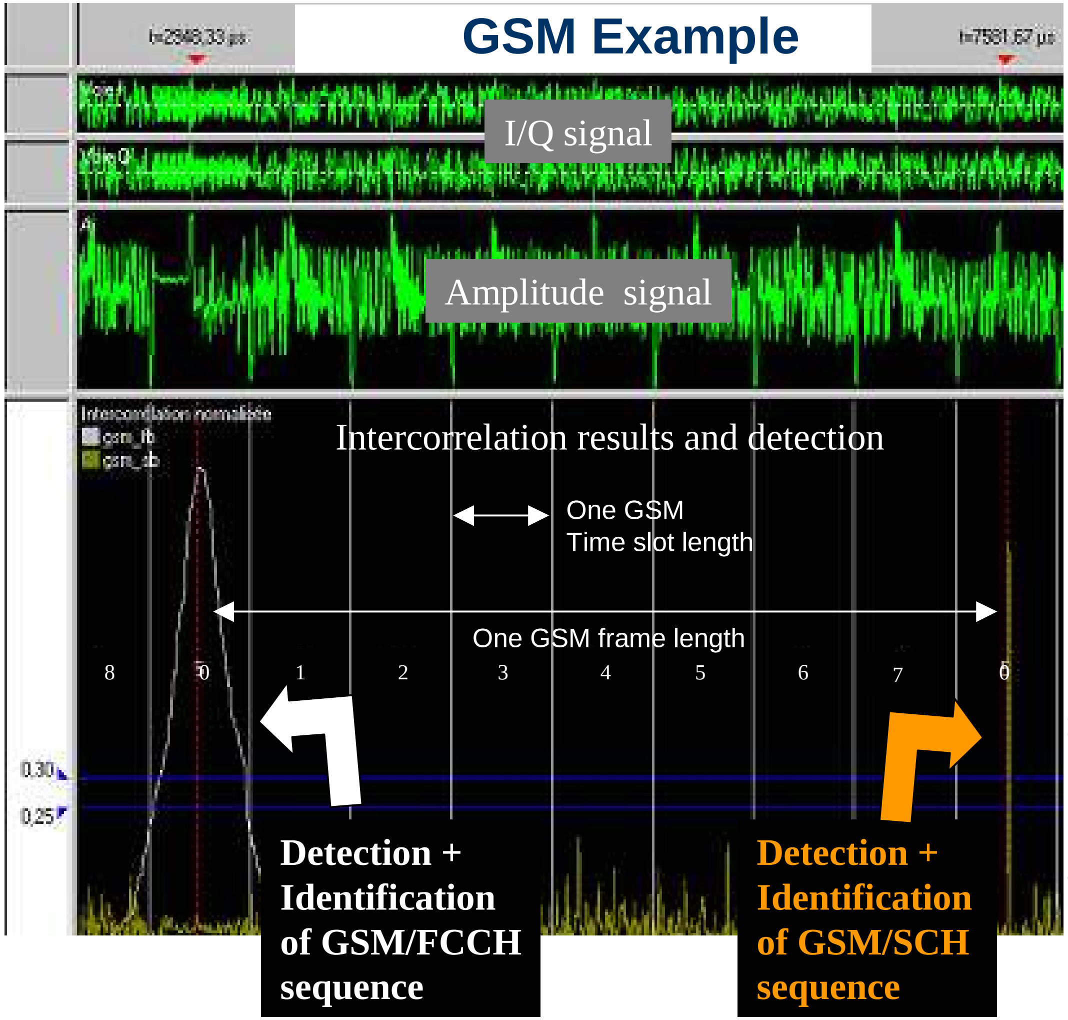
Advantages

=> reduced complexity

=> real Time OK

> Processes low powers signals

> Processes medium ratios for signal to noise+interference



THALES

Practical implementations – content of a GNSS device

Hardware Components

- ANTENNA RF TRANSPOSITION AND AND SAMPLING
- ASIC, FPGA, DSP, GPP ⊃ Hardware correlators (up to several thousands)
- Usually extra CEE Import Component (US,…)
- Component produced by CEE industrials

Software Components

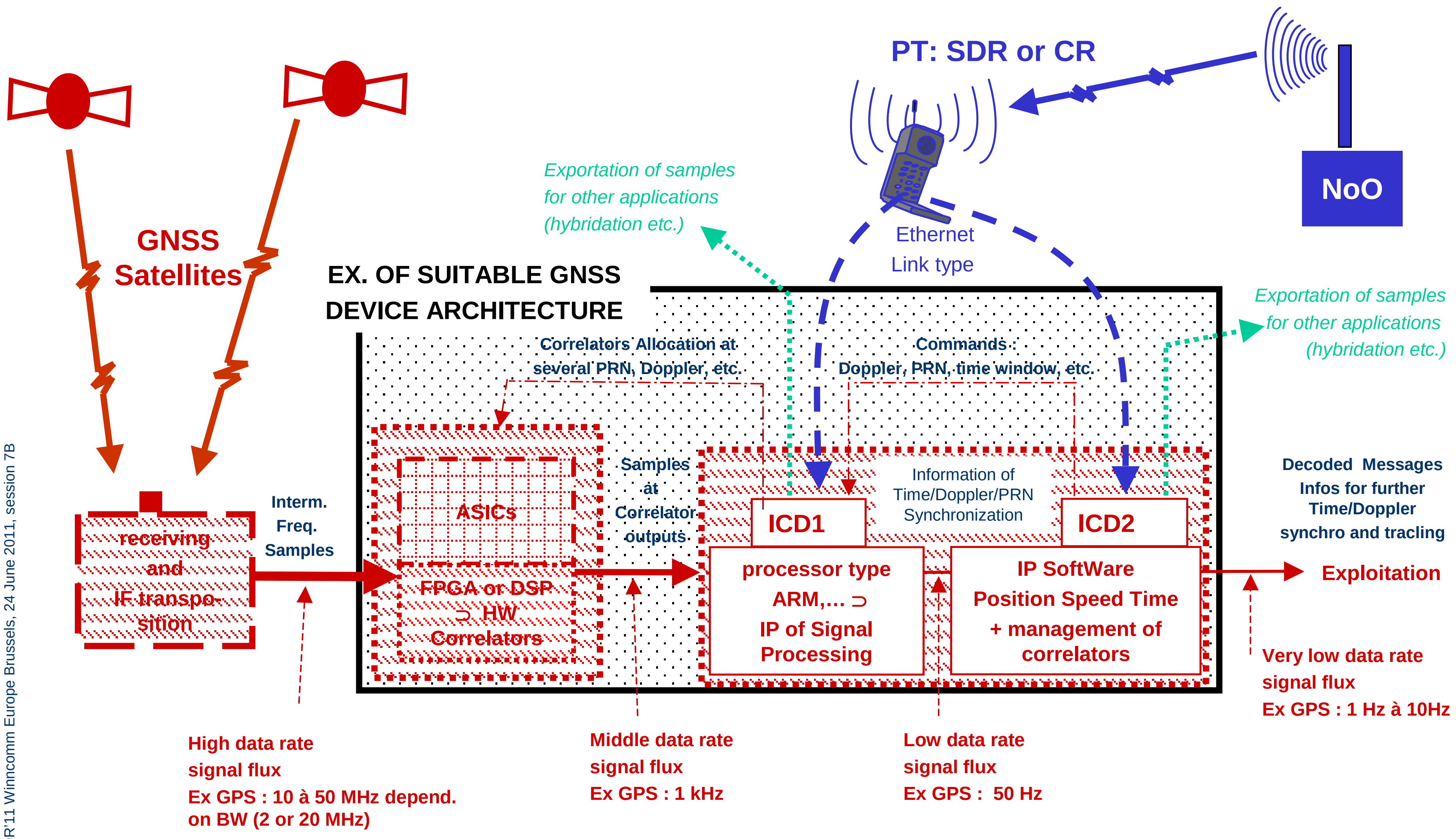
- Radio and Correlator management
- FF computation
- Position/Speed/Time tracking
- Input/output management

⊂ FPGA IP and/or DSP routines and/or software DLL

Flux and links

- GNSS signal Flux
- GNSS Commands and feedbacks
- GNSS data export
- Data input from external devices
  Example : SDR or CR with suitable ICD and Ethernet link type

Practical implementations – example of possible architecture



ICD: Interface Command Definition

IP: FPGA processing component

THALES

Conclusions – perspectives

I/ Several technical and operational arguments in favor of

- Geo-referenced sensing within CR
- Merging sensing, SoOs exploitation and navigation within CR
- Implementation of data aided signal processing for SoOs enhanced navigation:
  - Synchronization and location performances are largely upgraded,
  - Computations are often reduced.

  Applies to self synchronization and self Location within ad hoc network
  Upgrades reliability and reduces duration of synchronization procedures

II/ Relevant requirements should meet the current standardizations 4G trends

- Low added radio frequency performances are required for cognitive terminals.
- The added complexity should be compatible with future embedded computers
- Secured transmissions of geo-located sensing info to CM are required

III/ What about including hydride sensing + A-GNSS/SoO in the standardization efforts for 4G (5G ?) radio networks ?