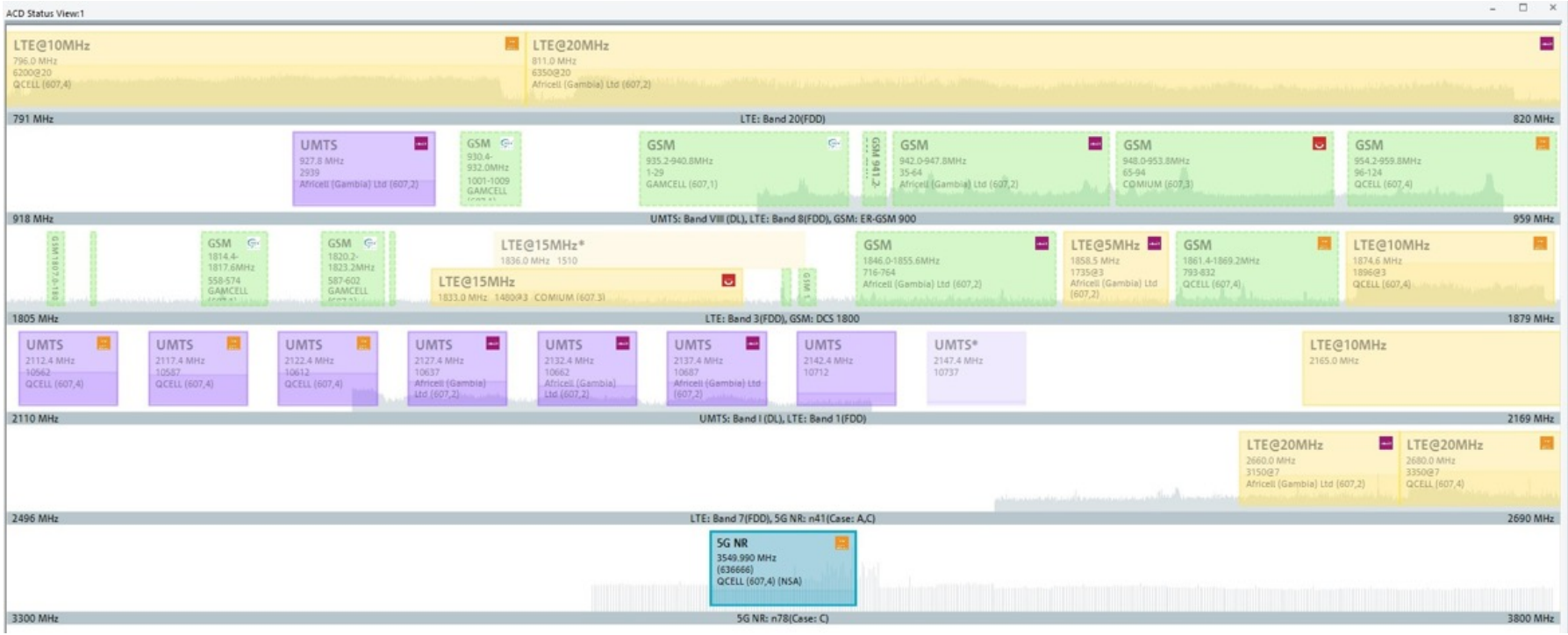
SIGNAL RECOGNITION AND CLASSIFICATION

ENHANCE NETWORK EXPERIENCE BY USING WIRELESS NETWORK DECODING

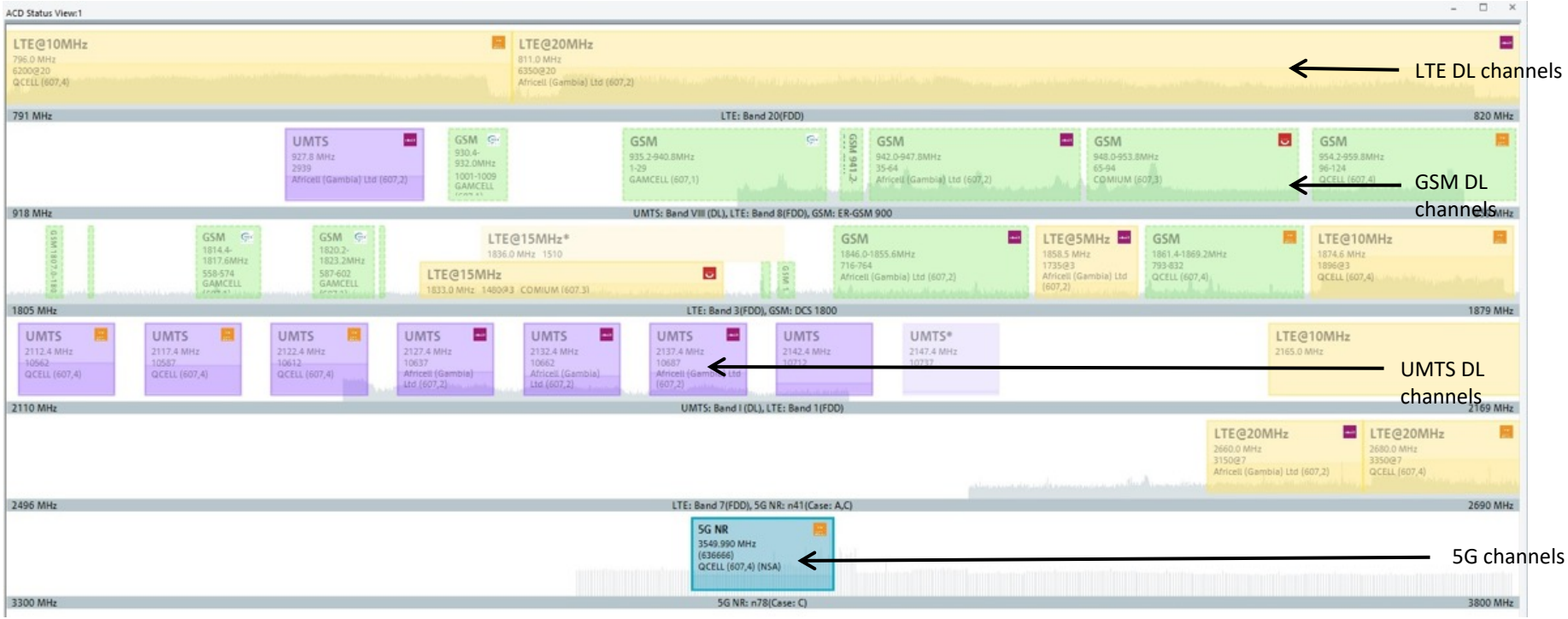
ROHDE&SCHWARZ

Make ideas real

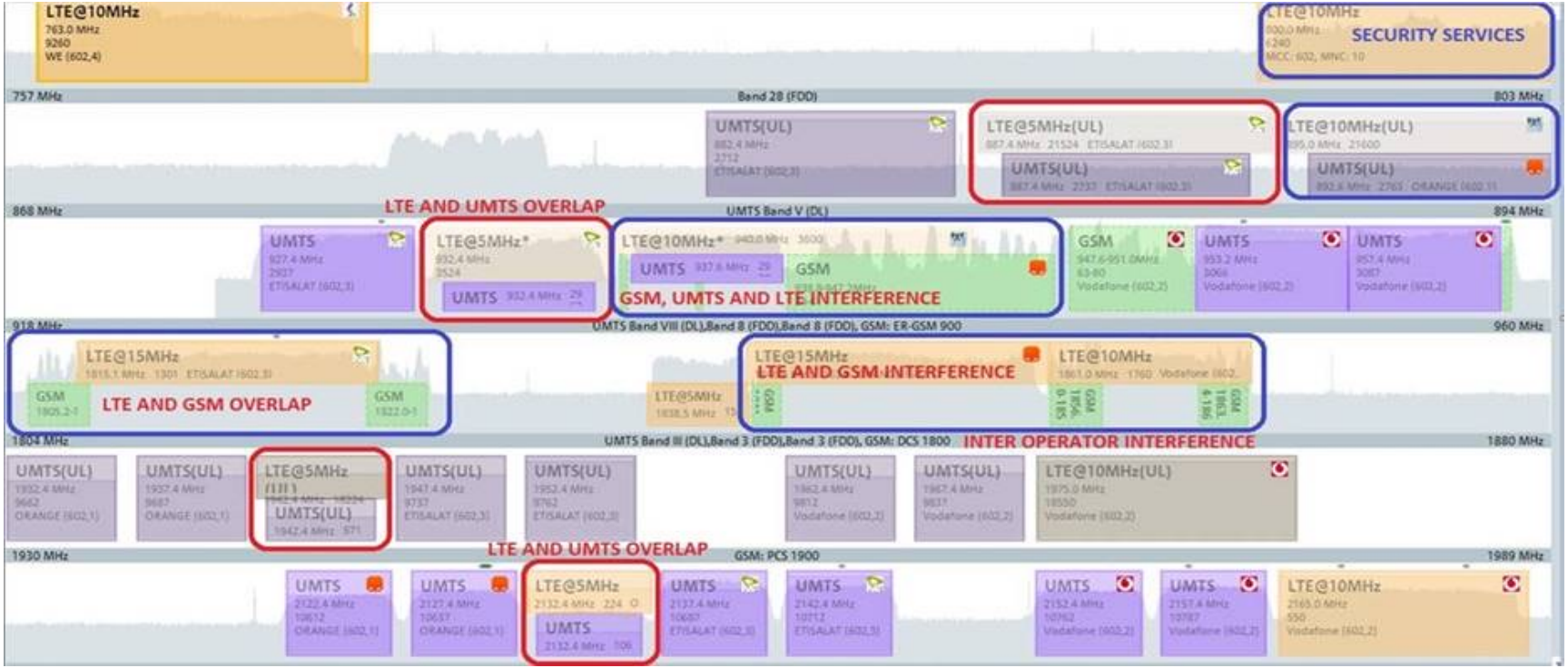
HOW DOES “YOUR” MOBILE RADIO NETWORK LOOK LIKE??



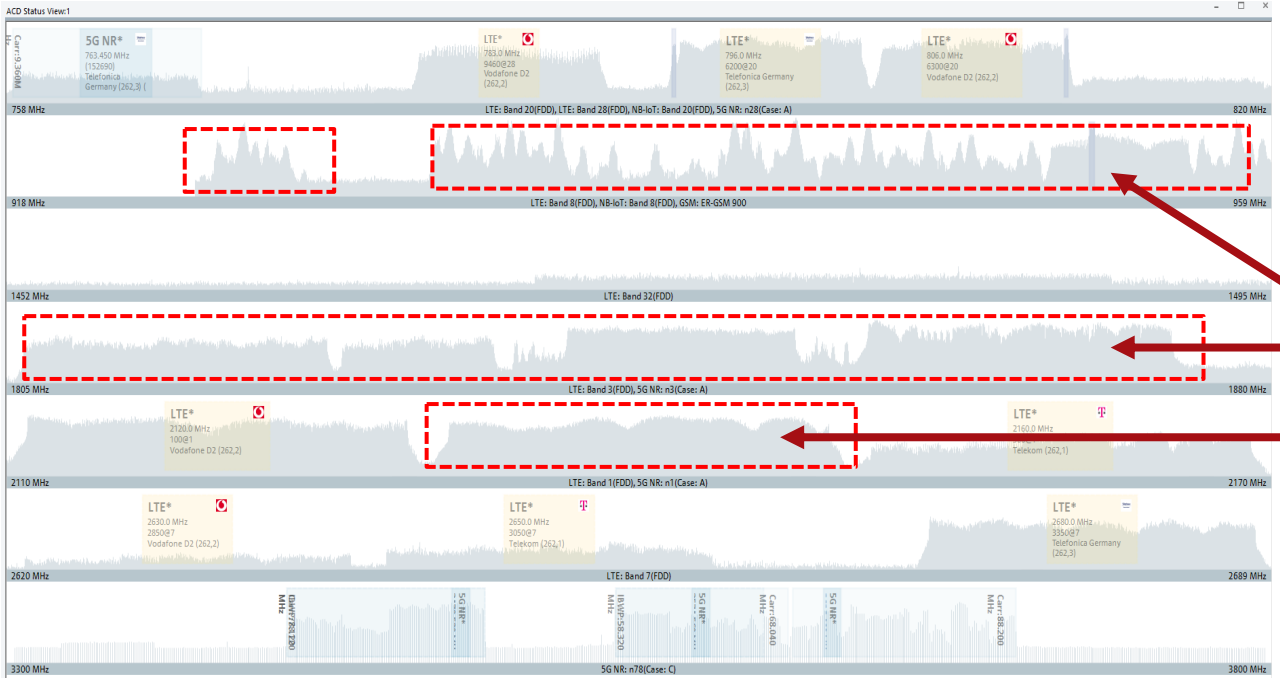
AUTOMATIC CHANNEL DETECTION



CROSS BORDER – FREQUENCY SPECTRUM OVERLAP



RECOGNISE AND CLASSIFY KNOWN RADIO PATTERNS



Scanner algorithm sweeps over the spectrum and searches for known signal sequences such as LTE, 5G NR…

We do Cross Correlation and look at the Shape of the Signal and identify the Radio patterns.

Finder Modules continuously keep on running in a 3 Step Process:

1) Sweep and correlate the Radio Pattern
2) Run Algorithms to identify correct information is obtained
3) Decode the Signal and all Broadcasted channel information

APPLICATION AND USE CASES OF ACD

- Simplify and safe time for the inital configuration of the measurement equipment when starting a measurement campaign without knowing the RF environment

- ACD runs smoothly in the background → Detection of new channels / technologies during a measurement campaign to not miss any channel

- Identify potential candidates for carriers on air based on neighbor cell lists or inter/intra RAT lists from system information messages

- Get the spectrum usage at a glance; this is interesting in particular for regulators
- Verify spectrum usage at country borders (overshooting, overlapping channels)

- Check other enabled features at a glance (e.g. 5G NSA/SA, MCC,CN, channel bandwidth,…)

DECODING TO THE NEXT LEVEL…

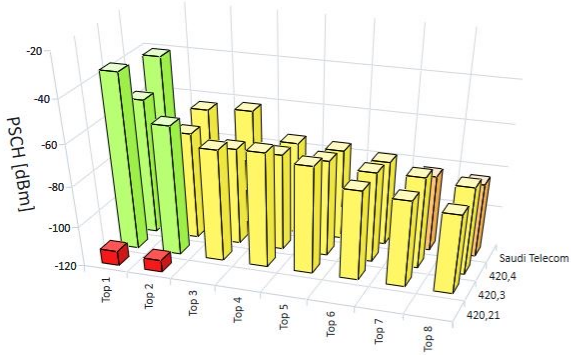
GSM Scanner Top N View:1 R&S GSM NWS[1] R&S GSM NWS[2]

Top N: Show all TopN Pools | Auto Width | Hide Chart

List

#	I	ARFCN	BSIC	PSCH[...	Mode	C/I[dB]	Ptotal[...	CI	LAC	MCC	MNC	BTS Name	Dist....	Decisi...
1	1	961	60	-112.64	Avg	---	-103.52	10411	601	420	21	---	---	-112.64
2	2	957	60	-114.00	Avg	---	-104.00	10432	601	420	21	---	---	-114.00
1	1	1	17	-34.88	Avg	---	-34.16	10482	1221	420	3	---	---	-35.12
2	2	3	32	-56.48	Avg	---	-56.32	10481	1221	420	3	---	---	-58.44
1	1	979	44	-53.92	Avg	---	-53.36	10053	22101	420	4	---	---	-55.32
2	2	981	11	-67.44	Avg	---	-65.68	14561	22101	420	4	---	---	-66.52
1	1	124	76	-40.40	Avg	---	-39.36	53739	448	420	1	---	---	-39.60
2	2	115	24	-63.12	Avg	---	-62.40	53738	448	420	1	---	---	-62.24

Chart | Show Grid



GSM Scanner BCH View:1 R&S GSM NWS[1]

- MCC: 420, MNC: 21 [3/3]
- MCC: 420, MNC: 3 [52/52]
- MCC: 420, MNC: 4 [33/33]
- Saudi Telecom (MCC: 420, MNC: 1) [61/61]
  - GSM 900 [61/61]
    - BTS - LAC:00055 CI:07729 ARFCN:11
      - System Information Type 1
      - System Information Type 2quater
      - System Information Type 3
    - BTS - LAC:00055 CI:12241 ARFCN:107
    - BTS - LAC:00055 CI:12242 ARFCN:109
    - BTS - LAC:00055 CI:12243 ARFCN:119
    - BTS - LAC:00055 CI:18491 ARFCN:109
    - BTS - LAC:00055 CI:18493 ARFCN:122
    - BTS - LAC:00055 CI:21477 ARFCN:118
    - BTS - LAC:00055 CI:21478 ARFCN:106
    - BTS - LAC:00055 CI:21479 ARFCN:115
    - BTS - LAC:00055 CI:22070 ARFCN:121
    - BTS - LAC:00055 CI:22080 ARFCN:108
    - BTS - LAC:00055 CI:22090 ARFCN:123
    - BTS - LAC:00055 CI:22150 ARFCN:124
    - BTS - LAC:00055 CI:22160 ARFCN:118
    - BTS - LAC:00055 CI:22180 ARFCN:113
    - BTS - LAC:00055 CI:36534 ARFCN:120
    - BTS - LAC:00055 CI:36535 ARFCN:114
    - BTS - LAC:00055 CI:36536 ARFCN:112
    - BTS - LAC:00306 CI:06732 ARFCN:111
    - BTS - LAC:00306 CI:10412 ARFCN:122
    - BTS - LAC:00306 CI:12281 ARFCN:121
    - BTS - LAC:00306 CI:12283 ARFCN:118
    - BTS - LAC:00306 CI:21740 ARFCN:118
    - BTS - LAC:00306 CI:21870 ARFCN:111
    - BTS - LAC:00306 CI:33065 ARFCN:117
    - BTS - LAC:00306 CI:34001 ARFCN:112
    - BTS - LAC:00306 CI:34003 ARFCN:117
    - BTS - LAC:00306 CI:36014 ARFCN:120
    - BTS - LAC:00306 CI:41662 ARFCN:114
    - BTS - LAC:00306 CI:41663 ARFCN:121

PDU Variant List <<<

TimeStamp

00:11:27

Details <<<

System Information Type 1
- L3Message 2
  - Protocol Discriminator (6) Radio Resource Mgmnt
  - PdRadioResourceManagement 3
    - Skip Indicator (Skip Indicator) 0
    - Message Type (25) System_Info_Type_1
    - System Info Type 1 (3) _System_Info_Type_1
      - Cell Channel Description
        - Complete CA info
        - Bitmap 0, RF channels belonging to the BCCH allocation:
          - 99
          - 108
      - RACH Control Parameters (7) _RACH_Control_Parameters_V
        - Max Retrans (2) Max 4 retransmissions
        - Tx Integer (15) 50 slots used to spread TX
        - Cell Barr Access (0) Cell is not barred
        - RE (0) Call reestablishment allowed
        - AC 11-15 (Access control class N) 0
        - EC 10 (0) Emergency Call allowed
        - AC 0-9 (Access control class N) 0
      - SI 1 rest octets (2) _SI_1_rest_octets_V
        - NCH Position Ind (0) No NCH Position Indication
        - NCH_Position_Ind_0 (2) __NCH_Position_Ind_0_2
          - Band indicator (0) ARFCN indicates 1800 band (L)
          - Spare 6 (6 spare bits) 43

Text Filter

SIB/MIB MESSAGES DECODED FOR EACH BROADCAST CHANNEL

MAP

MULTIPLE TECHNOLOGY PLOTS ON MAP

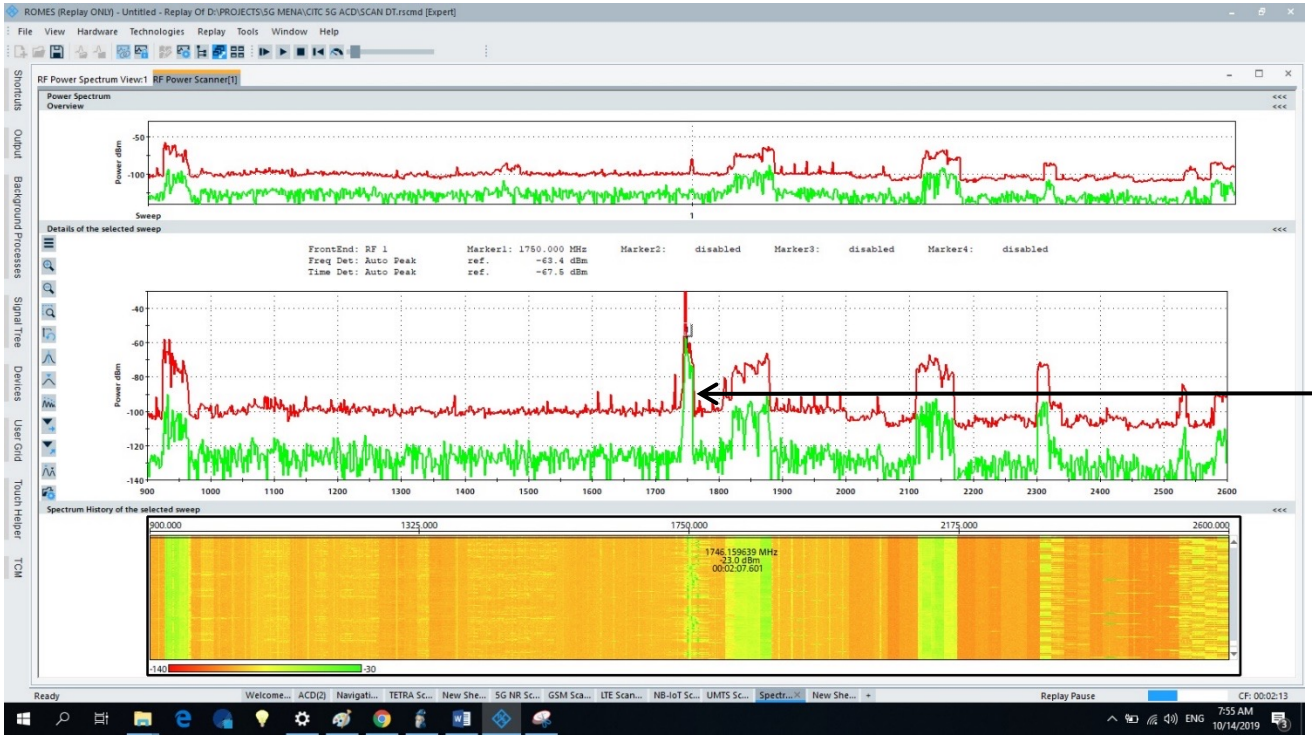
MAP VIEW – ALL TECHNOLOGIES (GSM, UMTS, LTE, NB IOT, 5G) FOR EACH OPERATOR

SPECTRUM SCANNING

SPECTRUM SCANNING

SPETRUM SCANNING FOR ALL BANDS – AND SPECIFIC BANDS AS WELL

INTERFERENCE OBSERVED AT 1750 MHZ

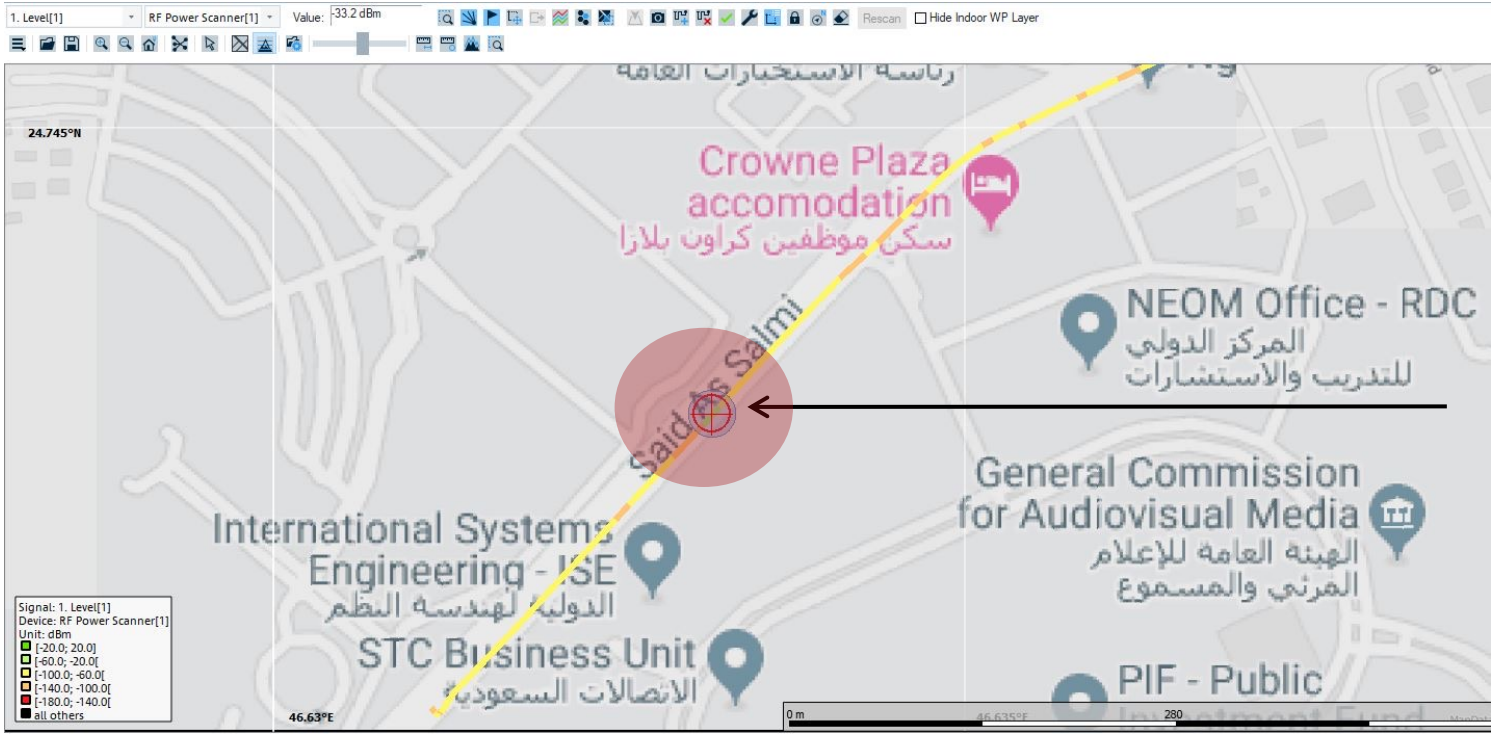


HIGH NARROWBAND INTERFERENCE OBSERVER AT 1750 Mhz.

THIS IS THE UPLINK LTE 1800 BAND FOR ZAIN, STC AND MOBILY.

THIS IS PRIMARILY AFFECTING ZAIN AS IT HAS LTE UL AT 1755 Mhz

INTERFERENCE OBSERVATION PLOT ON MAP



INTERFERENCE PEAK WHEN PLOTTED ON THE MAP SHOWS ONE PARTICULAR AREA WHERE THIS PEAK GETS HIGH AND AFTER MOVING FROM THIS AREA, THE INTERFERENCE LEVEL DROPS

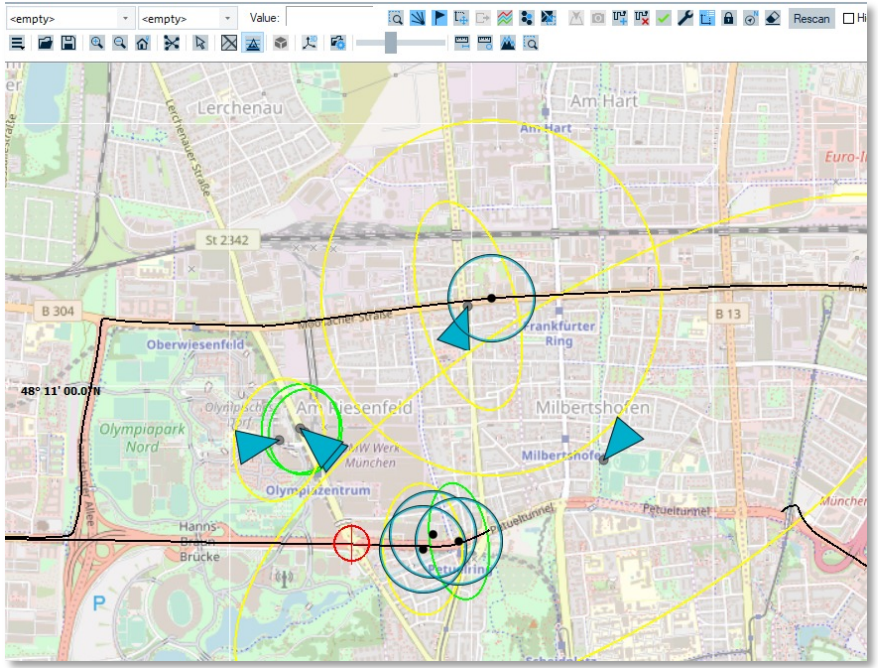
BTS ESTIMATION

MOBILE NW BASE STATION SIGNAL DETECTION AND ESTIMATION

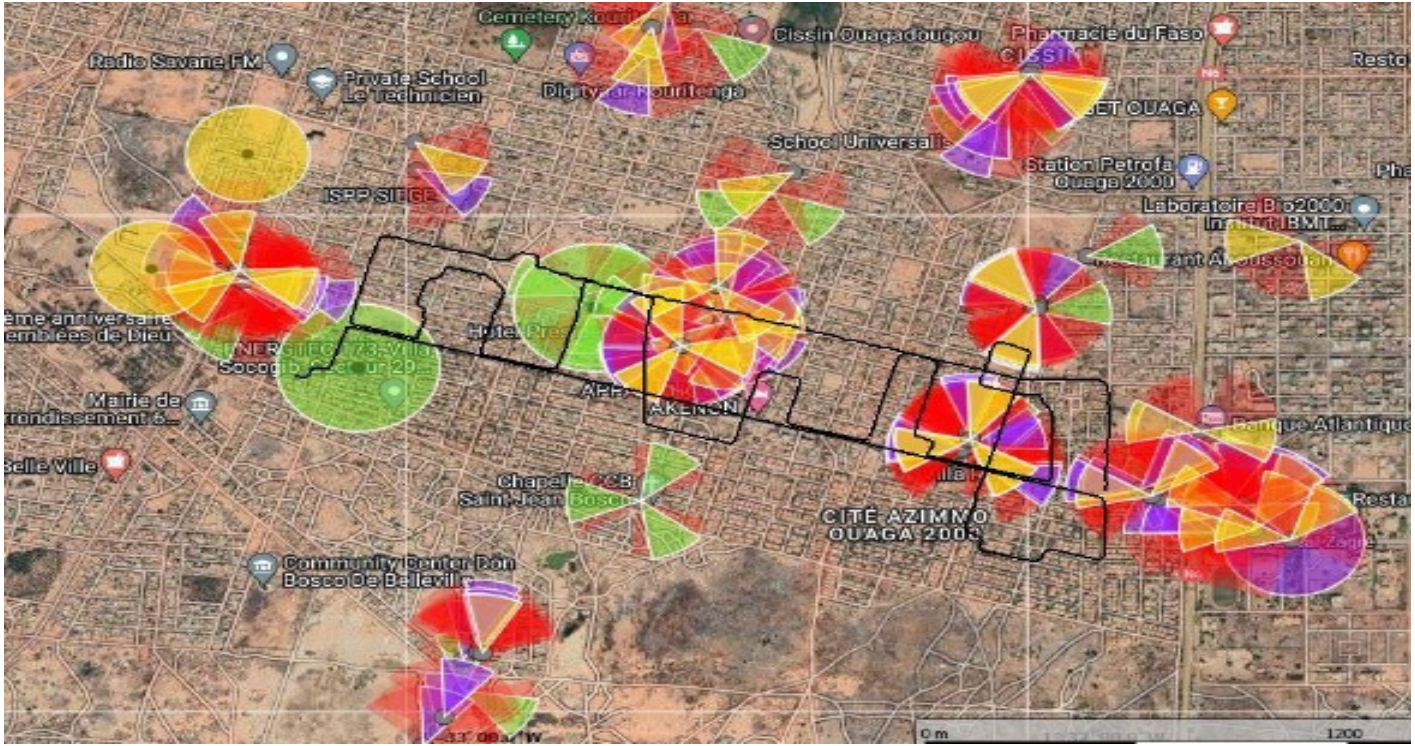
POSITION ESTIMATION (BTS AND SECTOR)

Following factors are taken into account:

- ► POWER OF ARRIVAL
- ► TIME OF ARRIVAL
- ► CHANNEL IMPULSE RESPONSE (Multi path)
- ► TRIANGULATION
- ► HALF POWER BEAMWIDTH

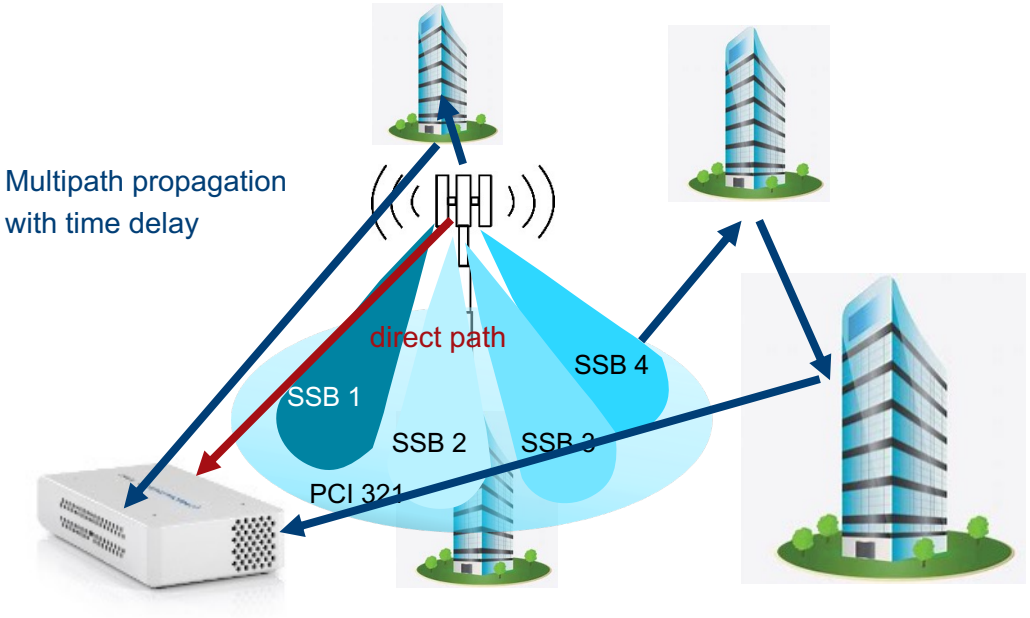


BASE STATION ESTIMATION TESTING



CIR AND RB LEVEL DRILL DOWN

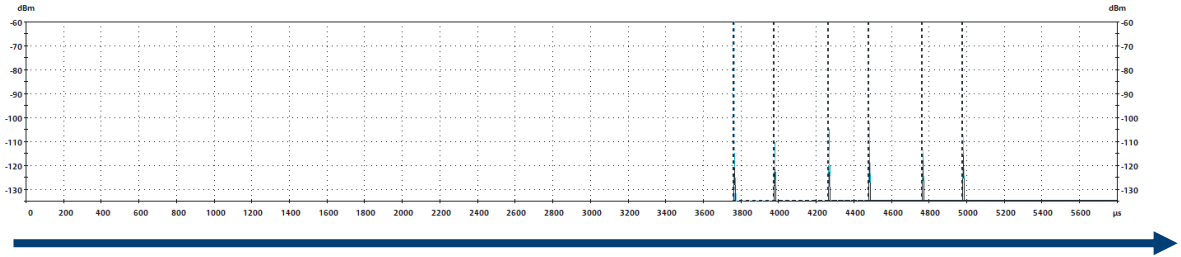
CHANNEL IMPULSE RESPONSE AND MULTIPATH PROPAGATION



- Electromagnetic waves can be reflected or transmitted at / through obstacles
  - Reflection: A certain part of the energy is reflected at an obstacle **which causes multipath propagation. Multipath proagation adds a time delay compared to the direct path.** The waves can be reflected several times at obstacles.
  - Transmission: A certain part of the energy propagated through an obstacle (e.g. outdoor to indoor propagation)

SCANNER IS ABLE TO MEASURE MULTIPATH PROPAGATION – CIR CHART

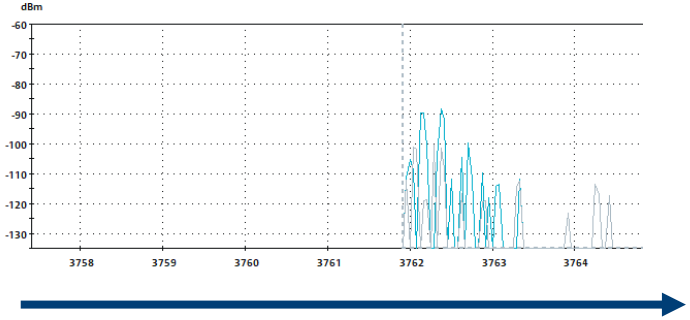
- Zoom level 1 – SSS-PBCH CIR view



Arrival time of SSBs ~ 200 µs distance

Relative time base

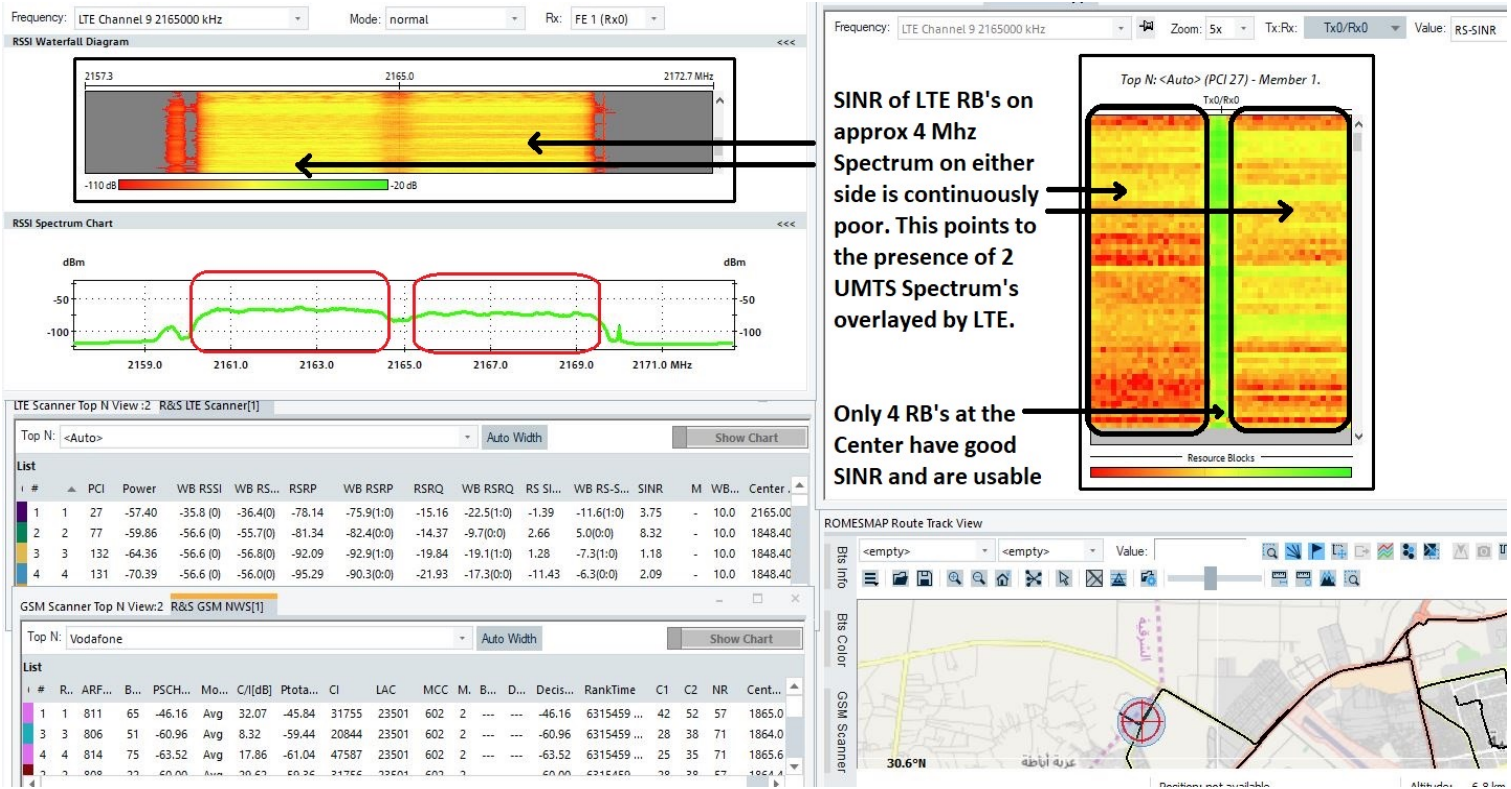
- Zoom level 2 - SSS-PBCH CIR view



Multipath receptions with time delay and their power

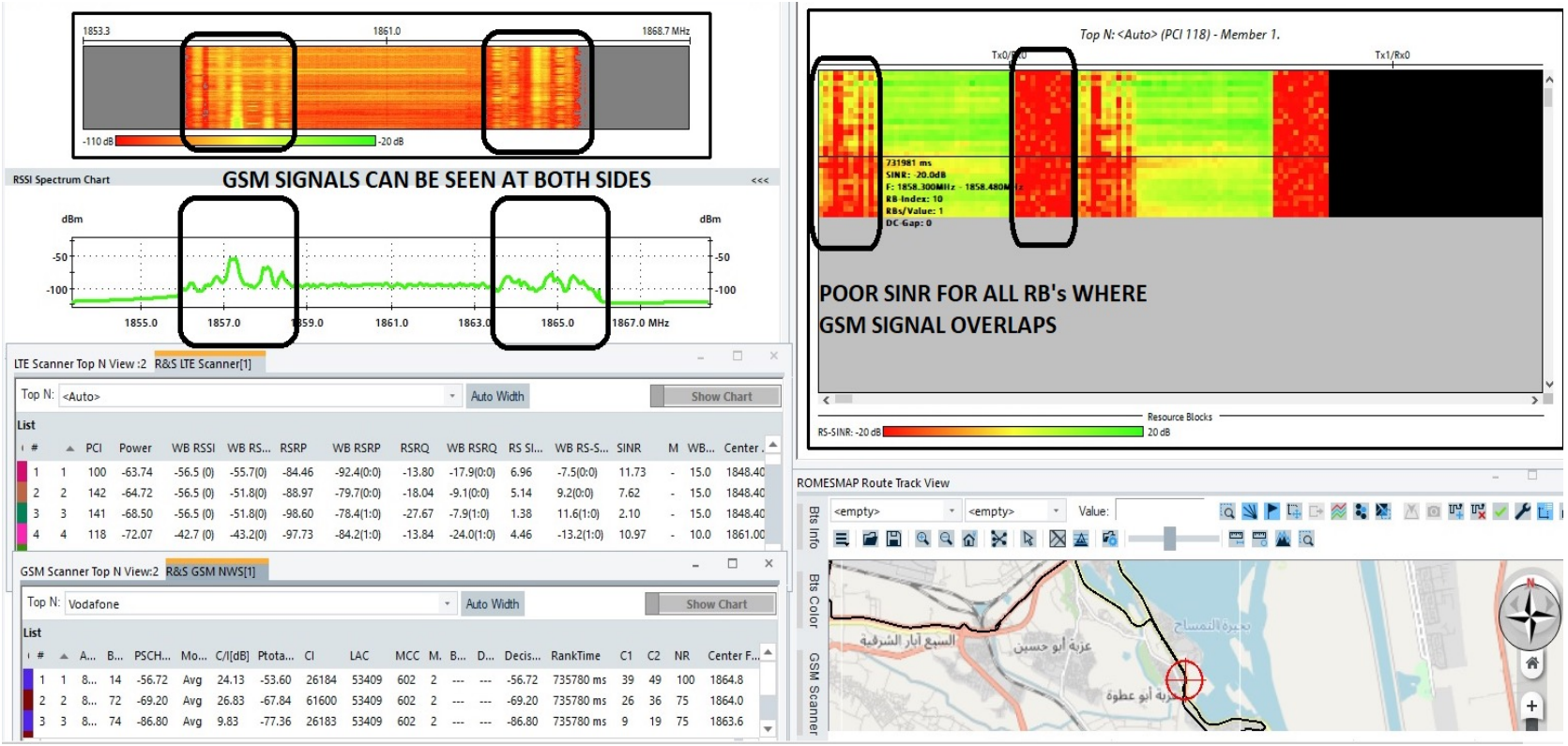
Relative time base

LTE RESOURCE BLOCK LEVEL DRILL DOWN – EXAMPLE 1



CHECK THE POWER AND SIGNAL TO NOISE RATIO OF EACH RESOURCE BLOCK IN LTE

RESOURCE BLOCK VIEW – EXAMPLE 2



SCANNER VS MOBILE PHONE

DIFFERENCE BETWEEN SCANNER AND MOBILE PHONE MEASUREMENTS

Measurement device		
Measurement mode	Passive: just receiving, no SIM required	Active: SIM-based connection to its operator
Measurement accuracy	Accurate (+/- 1dB)	+/- 6dB
Measured cells	All receivable cells (all operators, all configured frequency bands)	Connected cell and neighbors (limited), own operator
Measurement speed / frequency	+	-
Use case	Reference RF measurement	Real world, comparability

5G NR RF SCANNER MEASUREMENTS
PROS AND CONS

- Scanner View:

Pros

- Independently of the network settings, a neutral look into the radio access performance (best cells sorting according to the rules set by the user: RSRP/RSRQ, SINR)
- MIMO measurements (best possible rank, condition number, spectrum scan, path quality)
- 5G measurements on synchronization block for all on-air channels – on cell and beam level
- Spectrum scanning
- Synchronization measurements (ToA, TAE) and Frequency Accurancy measurements
- Uplink interference emasurements (Time Gated)
- Automatic Channel Detection, Position Estimation
- MIB/SIB decoding

Cons

- No Uplink visibility: RACH statistic, UL transmit power, reporting (CSI)
- No ressource and connection handling details/Layer3 signalization, QoS/QoE
- No Mobility measurements

5G NR UE BASED MEASUREMENTS
PROS AND CONS

► UE View:

Pros

- ► Detailed connection reporting (for the operator defined with the SIM in the UE)
- ► Complete Uplink visibility, reporting, radio access procedures and performance
- ► Layer 3 / RRC signalization
- ► Mobility measurements / Events

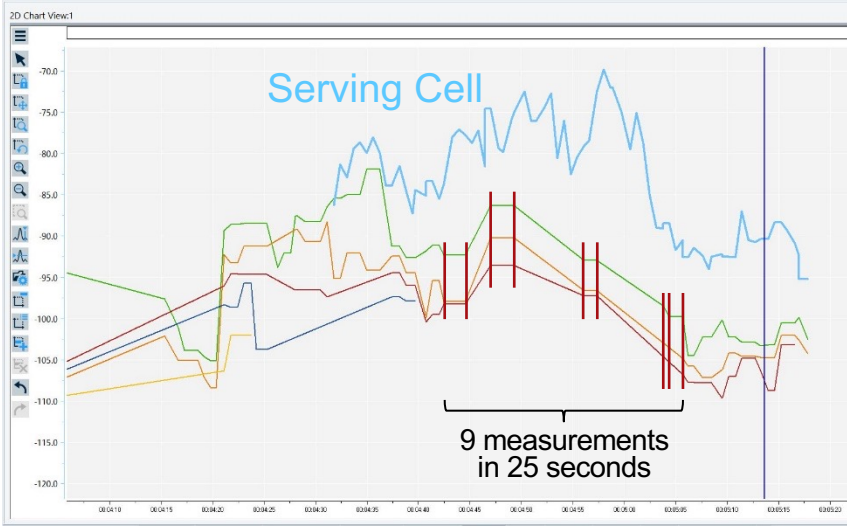
Cons

- ► We are able to measure only what UE is reporting / capable and what is being instructed by the network, maybe not the best possible situation. Examples:
  - – UE reports MIMO 2x2, even though radio environment is good enough for MIMO 4x4
  - – UE reports one PCI as the best one, even though the other PCI has better radio environment
  - – UE camping on specific frequency, even though other one is better

How to verify this?

By adding additionally the scanner

DIFFERENCE BETWEEN SCANNER AND MOBILE PHONE: MEASUREMENT SPEED



60 seconds

LTE RSRP measurements of a **smartphone**:

- Serving cell
- + neighbor cells sporadically

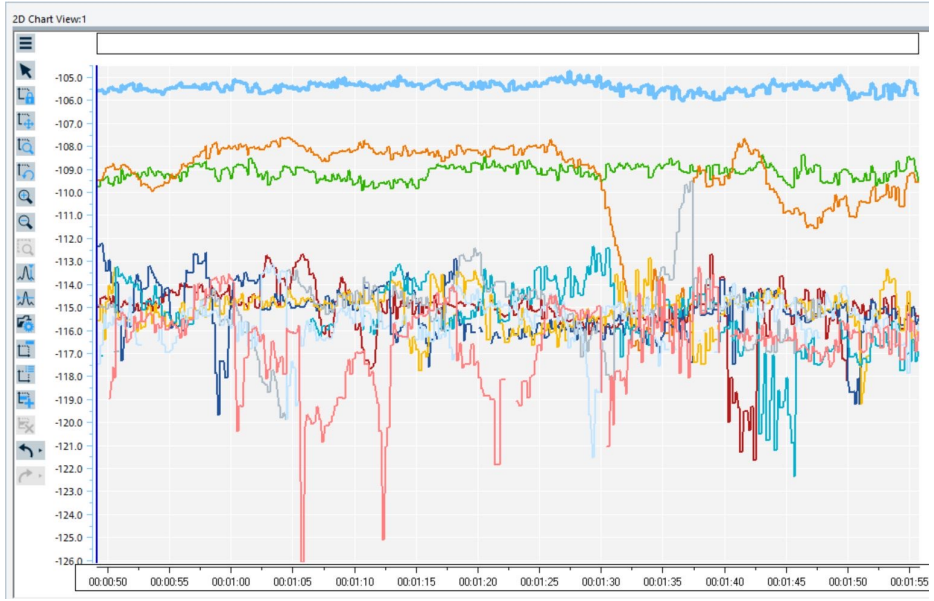
(from **own** operator, 1 band)

LTE RSRP measurements of a **scanner**:

- All cells

(from **all** operators, 1 band)

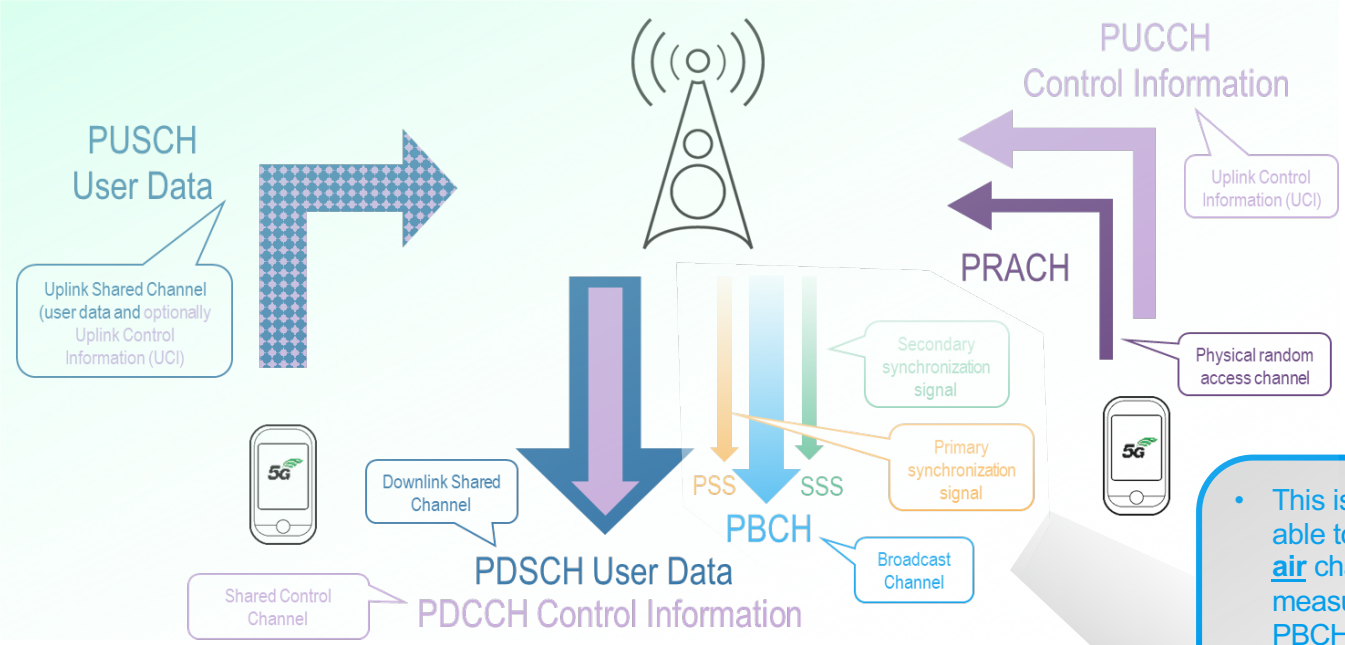
Just 10 cells were configured here.



60 seconds

Scanner or UE?

Scanner is powerful, but there is so much more on air…

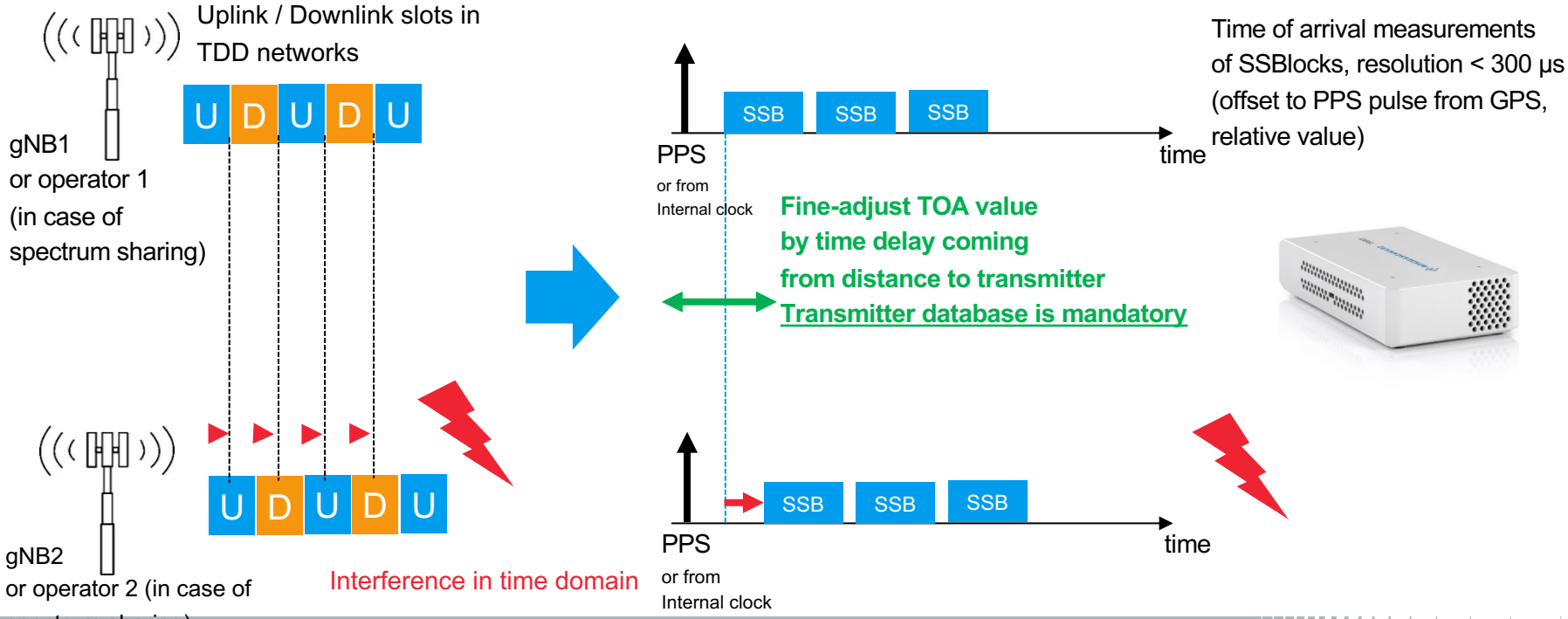


- In addition to PBCH, all other channels can be measured only with the UE and **for the registered connection determined by the SIM card**

- This is where Scanner is able to measure **on all on-air** channels: Scanner measures on PBCH/PSS/SSS only

5G SIGNAL DECODING AND SYNCHRONISATION

5G network synchronization measurements



TIME GATED TRIGGERING

Identification of PCIs and SSBs

Demodulation of SIBs

Automatic configuration of the time-gate via SIBs (if broadbasted)

otherwise manual onfiguration

Configured Time-gate

Configured Time-gate

UL	DL	UL
UL	DL	UL
UL	DL	UL

UL power spectrum

UL power spectrum

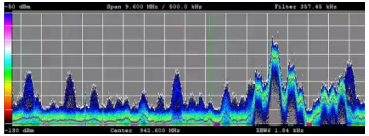
A time-gate on the uplink slots is applied

The 5GNR scanner speed is slowed down i. o. to provide a real-time spectrum view

Result:

Real time

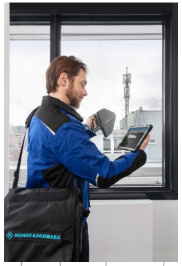
Uplink power spectrum



Panoramic acorss the spectrum and focussed view on the interferred spectrum

Interference detection

Interference hunting



SPECTRUM ANALYZER VS SCANNER

- No demodulation capability in 5G NR
- Manual and cumbersome configuration
  - Relatively long time to wait until the TDD configuration can be determined from the spectrum
- Specialist needed (SSBs and TDD slots have to be identified from the spectrum)
- No ACD
- No synchronization on the radio frame

- Demodulation capability
- One-click configuration
- Auto-synchronization on the radio frame
- Simple configuration
- ACD available

- All-in-one (code-selective, RF measurements, ACD, network synchronization measurements, multi tech…)