

R&S® NESTOR CELLULAR NETWORK ANALYSIS SOFTWARE

Accurate multitechnology RF measurements
for deep network insights



Product Brochure
Version 11.00

ROHDE & SCHWARZ

Make ideas real



AT A GLANCE

R&S®NESTOR is a Windows based software for analyzing cellular networks over the air interface. It is widely deployed by law enforcement agencies, intelligence services, armed forces and regulatory authorities. R&S®NESTOR is used together with Rohde & Schwarz mobile network scanners and QualiPoc smartphones, which offer the most advanced technology worldwide. The software supports all relevant applications that public authorities and security organizations need to gather information about cellular networks. R&S®NESTOR is used in vehicles, trains, aircraft, drones, on ships and on foot.

R&S®NESTOR combines a cutting-edge touchscreen software architecture with top-of-the-line mobile radio acquisition equipment from Rohde & Schwarz. In addition to direct acquisition, visualization and real-time analysis of all measurement data (online), the software enables users to carry out in-depth postprocessing and long-term analysis (offline).

The R&S®TSME6 and R&S®TSMA6 mobile network scanners perform parallel measurements of GSM, UMTS, LTE (TDD and FDD), 5G NR (mmWave and sub 6 GHz), CDMA2000® and EV-DO signals in all frequency bands, while the R&S®TSME, R&S®TSMA and R&S®TSMW mobile network scanners carry out parallel measurements of GSM, UMTS, LTE (TDD and FDD), CDMA2000® and EV-DO signals in all frequency bands.

R&S®NESTOR supports the following applications:

- ▶ Automatic detection of all GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO networks, bands and channels
- ▶ Autonomous acquisition of cell information, signal power and signal quality
- ▶ Mobile radio coverage measurements and determination of cell boundaries
- ▶ Creation and management of cell lists including geographic positions
- ▶ Retrieval of coverage data for forensic investigations
- ▶ Detection and analysis of misconfigured cells (mobile and stationary applications)
- ▶ Spectrum analysis in uplink and downlink bands

R&S®NESTOR architecture supports direct (live), autonomous (offline) and networked operations as well as client/server operation over IP based links.



KEY FACTS

- ▶ Cellular network analysis to measure parameters and read out data from these networks
- ▶ Parallel measurements of all supported technologies and bands to generate comprehensive, reliable measurement data
- ▶ Real-time analyses during data acquisition
- ▶ Data postprocessing for in-depth analysis
- ▶ Intuitive operation for complex tasks
- ▶ Free map data (OpenStreetMap)
- ▶ User interface available in multiple languages

BENEFITS

- Easy operation for complex tasks
 - ▶ page 4
- Everything that cellular network analysis software needs
 - ▶ page 6
- Automatic channel detection
 - ▶ page 8
- Cellular network scanning
 - ▶ page 10
- Cellular network coverage analysis
 - ▶ page 11
- Cell position estimation
 - ▶ page 12
- Detection and monitoring of suspicious cells
 - ▶ page 14
- Installation of new cell sites
 - ▶ page 16
- Forensic investigations
 - ▶ page 17
- Configurations for mobile use
 - ▶ page 18

EASY OPERATION FOR COMPLEX TASKS

User-friendly interface for easy customization

R&S®NESTOR is simple and consistent to operate, allowing even inexperienced users to achieve fast, conclusive results.

Since R&S®NESTOR has just a few, uniformly designed control elements, both experienced and inexperienced users can quickly learn how to use the software. Only minimal training is needed to efficiently acquire information.

Touchscreen and/or mouse and keyboard operation

R&S®NESTOR is optimized for Windows 10 touchscreen operation – a plus for mobile users, who often work on foot with a tablet or smartphone.

The software can also be operated with a mouse and keyboard, for example when installed in vehicles, and for offline analysis of larger amounts of data.

Automatic hardware configuration

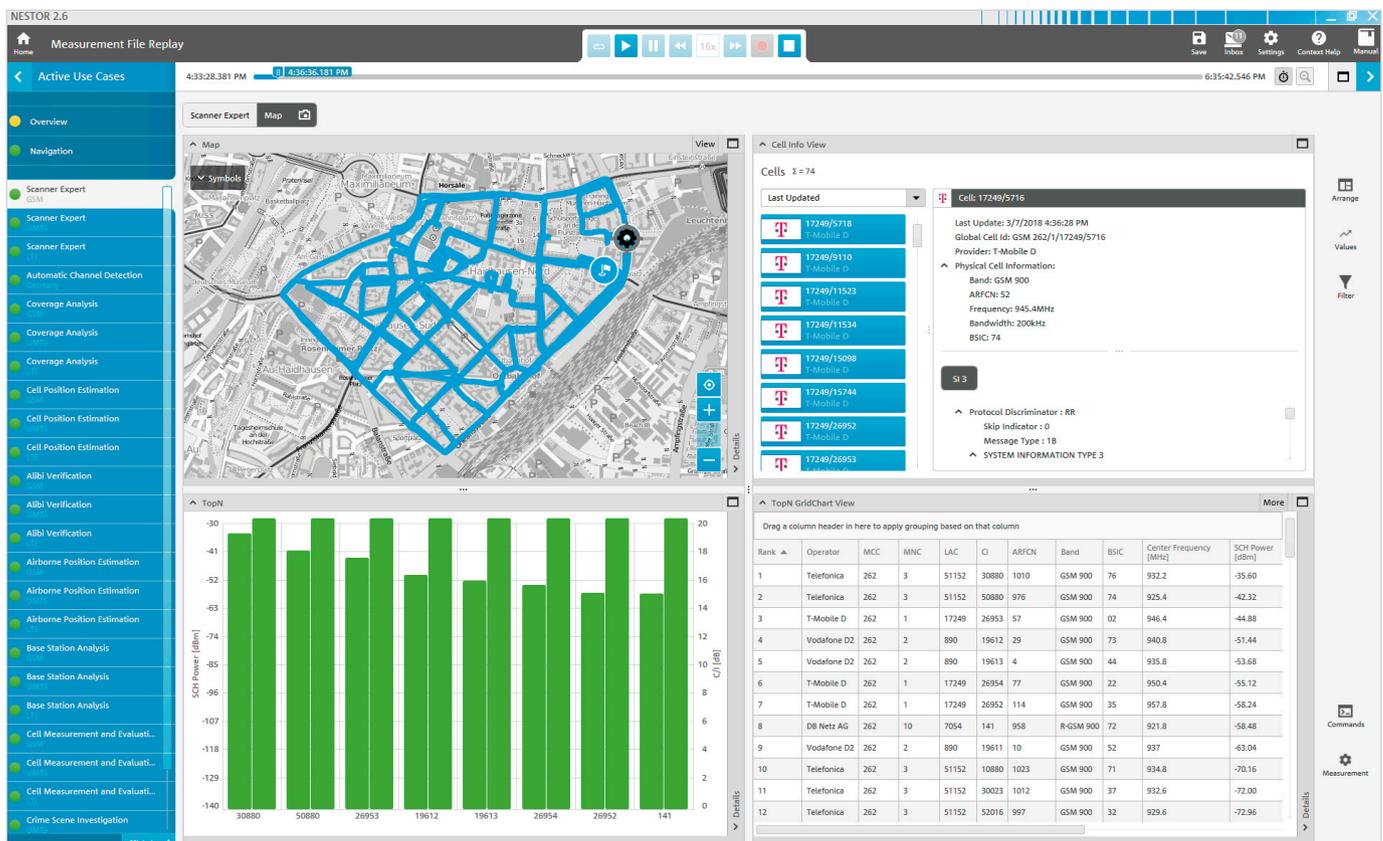
The scanners, QualiPoc smartphones and navigation hardware connected to the PC or tablet are automatically detected and configured by R&S®NESTOR as soon as the software is started, and a standard measurement is performed immediately. Status displays continuously inform the user about the status of all connected devices. Predefined workspaces can be loaded or started automatically. No other system inputs are required for preconfigured measurements.

Straightforward display of all measurements

Each workspace contains one or more use cases, which each fulfill a specific task (e.g. GSM cell position estimation). Each use case has a standard display with several views for the measurement task. The user can change the standard display, but this is usually not necessary.

Simultaneous use of any number of use cases
A significant feature of R&S®NESTOR is its ability to compile all available use cases as often as desired and in any combination.

Display of measurement results



Use cases with overlapping scanner measurements intelligently ensure that the scanner carries out such measurements only once. As a result, combining an LTE scanner measurement, a coverage analysis and a scanner cell position estimation generally requires just one set of measurement data instead of three.

All available parameters are synchronized across all use cases (coupled focus on time axis and geographic position) to display measurement and analysis results in the correct combination during measurement and replays.

Settings modifiable during measurements

Flexibility is a key characteristic of R&S®NESTOR. All devices, settings and views can be changed online during measurement, recording and analysis without interrupting the measurement.

Changes are also documented in the measurement results and can be seen during replays and analysis.

Convenient filter options for displaying and processing measurement data

The comprehensive filter concept is an important feature of R&S®NESTOR. The software uses a mobile network scanner to acquire extensive measurement data that it can filter and display as needed. Filters are used for the following applications:

- ▶ Individual views
- ▶ Use cases
- ▶ Data exports
- ▶ Reports

R&S®NESTOR includes standard filters for the most common measurement data, technologies, network operators, geographic locations and (groups of) cellular network cells. All associated views are immediately updated when filters are activated or deactivated.

Multilingual

R&S®NESTOR is available in English, German, Spanish, Russian, French, Chinese, Turkish, Italian, Portuguese (Brazil) and Arabic.

New versions every three months

A new version of R&S®NESTOR will be available for download via an FTP server in the middle of every quarter. Users registered on the Rohde&Schwarz customer support website are automatically notified of the new version.

QualiPoc smartphone



EVERYTHING THAT CELLULAR NETWORK ANALYSIS SOFTWARE NEEDS

OpenStreetMap

OpenStreetMap (OSM) is a user-editable world map available at www.openstreetmap.org

OSM is a wiki project in which users can participate by downloading, editing and uploading geographical information such as GPS tracking data or the course of a road or river. This world map is growing daily.

OpenStreetMap data can be used freely under the terms of the Creative Commons Attribution Share Alike 2.0 license.

Support of the R&S®TSME6, R&S®TSMAG, R&S®TSME, R&S®TSMAG and R&S®TSMW mobile network scanners

R&S®NESTOR supports the second, third and fourth generation Rohde & Schwarz mobile network scanners.

Parallel measurements in all GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO bands

R&S®NESTOR uses one or more mobile network scanners to carry out parallel and synchronous measurements, ensuring that every GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO cell is measured within the same fixed time interval. It also measures IEEE 802.11 a/b/g/n/ac in parallel with dedicated hardware.



OpenStreetMap compatibility

R&S®NESTOR uses the free OpenStreetMap system. Maps are accessed via the internet for online use and saved on the control computer for offline work. The software also supports other map formats such as MapInfo and ESRI shapefiles.

Support of cell databases

Cellular network cells are central components for R&S®NESTOR. This means that creating and processing cell lists associated with measurements and analyses is of major importance.

Cell databases are either imported as existing lists in a configurable text format (e.g. CSV) or created by the system via measurements and position estimation. Cell lists are exported, processed using common spreadsheet programs and reimported into R&S®NESTOR. Technologies and network operators are clearly separated on the maps. Use case views involving cellular network cells include information on those cells. Filter functions relating to cellular network cells indicate measurement data and analyses for the selected cells only.

R&S®NESTOR installed on an R&S®TSMAG6 mobile network scanner remotely controlled via a tablet



Status displays for all connected devices, use cases and workspaces

Status displays provide information on the status of all connected devices. Status information for all use cases, use case groups and workspaces is displayed in separate windows. All connected devices can be activated and deactivated, even during measurements.

A higher-level reporting system saves all system messages and displays them in a mailbox.

Preconfigured templates for use cases and workspaces

Straightforward operation is one of the key features of R&S®NESTOR. This is why even the basic version includes a large number of templates for complete workspaces and for displaying use cases and configuring measurements. All templates can be edited and saved.

Live analysis and data export during measurements

All settings, views, analyses and data exports can be modified online during measurement data acquisition. All of the information from ongoing measurements is used as a basis for further operations.

Analysis and export of all measurements during data postprocessing

All measurements can be analyzed and exported during postprocessing.

License-free replay versions

R&S®NESTOR can be installed without a license as often as desired, making it possible to replay each measurement exactly as recorded.

AUTOMATIC CHANNEL DETECTION

Automatic detection of all occupied GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO RF channels

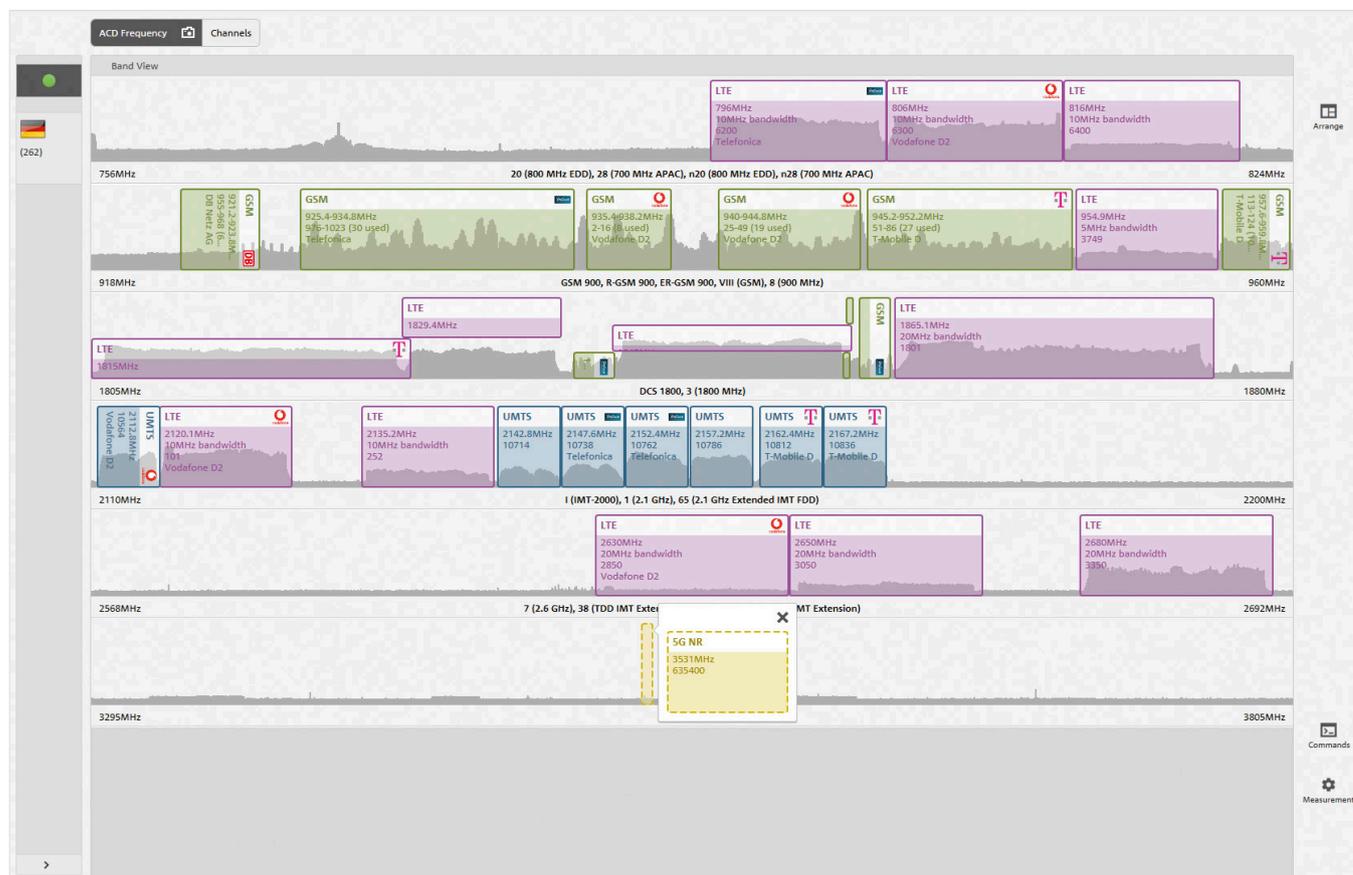
R&S®NESTOR detects deployed technologies and occupied bands and channels in unknown terrain. It identifies which technologies can be measured via the air interface and finds the associated channels and bands in all frequency ranges covered by the scanner in use.

This process couples sophisticated spectrum analysis with background technology information and a brute force approach to enable the fastest possible acquisition of the cells that are visible on the air interface.

If there is no or not enough information about the cellular network environment, the software searches the entire frequency range from a maximum of 80 MHz to 6 GHz for occupied RF channels.

R&S®NESTOR measures known bands and technologies very quickly and returns the channel numbers for all occupied channels. The software delivers a graphic display of occupied frequency bands along with a list of channel numbers on which signals were measured.

Automatic channel detection (ACD) for GSM, UMTS, LTE and 5G NR



Automatic forwarding of detected channels to all use cases for seamless measurement of all cellular network signals

During automatic channel detection, the bands found to carry cellular network signals are forwarded to all other use cases for further analysis. The system seamlessly proceeds from initial channel detection to a long-term cellular network analysis of the detected channels.

During regular scanner measurements (acquisition of cell parameters, signal power and signal quality), cell position estimation and cellular network coverage analysis are carried out at the same time.

Creation of use case templates for easy configuration of future measurements

A template for scanner settings (use cases) is automatically created with the channel detection results for each technology and band. The templates can be used directly for future measurements without automatic channel detection.

Preselection of cellular radio bands for automatic channel detection (ACD)

Technology preselection

Selected radio access technologies: GSM, UMTS, LTE, 5G NR

Select all radio access technologies

GSM UMTS LTE 5G NR CDMA EVDO

GSM radio band selection: GSM

Select all radio bands

GSM 450 GSM 480 GSM 850 GSM 900 R-GSM 900 ER-GSM 900 DCS 1800 PCS 1900

UMTS radio band selection: UMTS

Select all radio bands

I (IMT-2000) II (U.S. PCS) III (DCS) IV (AWS) V VI VII (IMT-E) VIII (GSM) IX X XI (Japan 1.5 GHz) XII (SMH) XIII (SMH) XIV (SMH) XIX XX XXI XXII XXV XXVI

LTE radio band selection: LTE

Select all radio bands

<input checked="" type="checkbox"/> 1 (2.1 GHz)	<input type="checkbox"/> 2 (US PCS 1900)	<input checked="" type="checkbox"/> 3 (1800 MHz)	<input type="checkbox"/> 4 (AWS)	<input type="checkbox"/> 5 (850 MHz)	<input type="checkbox"/> 6 (UMTS only)
<input checked="" type="checkbox"/> 7 (2.6 GHz)	<input checked="" type="checkbox"/> 8 (900 MHz)	<input type="checkbox"/> 9 (1700 MHz)	<input type="checkbox"/> 10 (Extended AWS)	<input type="checkbox"/> 11 (Japan 1.5 GHz)	<input type="checkbox"/> 12 (Lower 700 MHz, A+B+C)
<input type="checkbox"/> 13 (Upper 700 MHz)	<input type="checkbox"/> 14 (Public Safety)	<input type="checkbox"/> 17 (Lower 700 MHz, B+C)	<input type="checkbox"/> 18 (800 MHz)	<input type="checkbox"/> 19 (Digital Dividend)	<input checked="" type="checkbox"/> 20 (800 MHz EDD)
<input type="checkbox"/> 21 (1.5 GHz)	<input type="checkbox"/> 22 (3.5 GHz)	<input type="checkbox"/> 23 (2 GHz 5-Band)	<input type="checkbox"/> 24 (L Band)	<input type="checkbox"/> 25 (US PCS + G Block)	<input type="checkbox"/> 26 (800 MHz IDEN)
<input type="checkbox"/> 27 (850 MHz lower)	<input checked="" type="checkbox"/> 28 (700 MHz APAC)	<input type="checkbox"/> 29 (Media FLO DL CA only)	<input type="checkbox"/> 30 (2.3 GHz WCS)	<input type="checkbox"/> 31 (450 MHz)	<input type="checkbox"/> 32 (1.5 GHz L-Band DL CA only)
<input type="checkbox"/> 33 (TDD 2000)	<input type="checkbox"/> 34 (TDD 2000)	<input type="checkbox"/> 35 (TDD 1900)	<input type="checkbox"/> 36 (TDD 1900)	<input type="checkbox"/> 37 (TDD PCS)	<input checked="" type="checkbox"/> 38 (TDD IMT Extension)
<input type="checkbox"/> 39 (China TDD 1.9 GHz)	<input type="checkbox"/> 40 (China TDD 2.3 GHz)	<input type="checkbox"/> 41 (TDD 2.5 GHz)	<input type="checkbox"/> 42 (TDD 3.4 GHz)	<input type="checkbox"/> 43 (TDD 3.6 GHz)	<input type="checkbox"/> 44 (700 MHz APAC)
<input type="checkbox"/> 45 (China 1500 MHz)	<input type="checkbox"/> 46 (5 GHz Unlicensed TDD)	<input type="checkbox"/> 47 (V2X TDD)	<input type="checkbox"/> 48 (USA 3.5 GHz CBRS TDD)	<input type="checkbox"/> 49 (USA 3.5 GHz LAA TDD)	<input type="checkbox"/> 50 (TDD 1500+)
<input type="checkbox"/> 51 (TDD 1500-)	<input type="checkbox"/> 52 (TDD 3300)	<input type="checkbox"/> 53 (TDD 2500)	<input checked="" type="checkbox"/> 65 (2.1 GHz Extended IMT FDD)	<input type="checkbox"/> 66 (AWS-3)	<input type="checkbox"/> 67 (EU 700 MHz DL CA only)
<input type="checkbox"/> 68 (ME 700 MHz)	<input type="checkbox"/> 69 (IMT-E DL CA only)	<input type="checkbox"/> 70 (AWS-4)	<input type="checkbox"/> 71 (USA 600 MHz)	<input type="checkbox"/> 72 (EU PMR/PAMR 450 MHz)	<input type="checkbox"/> 74 (L-Band)
<input type="checkbox"/> 75 (1500 SDL DL CA only)	<input type="checkbox"/> 76 (NAR x DL CA only)	<input type="checkbox"/> 85 (NAR 700 MHz a+)	<input type="checkbox"/> 87 (EMEA 410 MHz)	<input type="checkbox"/> 88 (EMEA 410 MHz +)	

5G NR radio band selection: 5G NR

Select all radio bands

<input type="checkbox"/> n1 (2.1 GHz)	<input type="checkbox"/> n2 (US PCS 1900)	<input type="checkbox"/> n3 (1800 MHz)	<input type="checkbox"/> n5 (850 MHz)	<input checked="" type="checkbox"/> n7 (2.6 GHz)	<input type="checkbox"/> n8 (900 MHz)
<input type="checkbox"/> n12 (Lower 700 MHz, A+B+C)	<input checked="" type="checkbox"/> n20 (800 MHz EDD)	<input type="checkbox"/> n25 (US PCS + G Block)	<input checked="" type="checkbox"/> n28 (700 MHz APAC)	<input type="checkbox"/> n34 (TDD 2000)	<input checked="" type="checkbox"/> n38 (TDD IMT Extension)
<input type="checkbox"/> n39 (China TDD 1.9 GHz)	<input type="checkbox"/> n40 (China TDD 2.3 GHz)	<input type="checkbox"/> n41 (TDD 2.5 GHz)	<input type="checkbox"/> n50 (x TDD)	<input type="checkbox"/> n51 (x TDD)	<input type="checkbox"/> n65 (2.1 GHz Extended IMT FDD)
<input type="checkbox"/> n66 (AWS-3)	<input type="checkbox"/> n70 (AWS-4)	<input type="checkbox"/> n71 (USA 600 MHz)	<input type="checkbox"/> n74 (L-Band)	<input type="checkbox"/> n75 (1500 SDL DL CA only)	<input type="checkbox"/> n76 (NAR x DL CA only)
<input type="checkbox"/> n77 (TD 3700)	<input checked="" type="checkbox"/> n78 (TD 3500)	<input type="checkbox"/> n79 (TD 4500)			

CELLULAR NETWORK SCANNING

Simultaneous cellular network analysis in all GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO bands

GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO scanner measurements can be configured for entire bands or individual channels. Each use case can be configured individually and in detail. Measured data is accessed in real time by other use cases in the workspace for further processing.

Top N chart and list display for all measured cells

A Top N chart is generated for specific use cases. It displays all relevant parameters for each cell in both graphic and tabular form and can be weighted according to signal power, signal quality or UE emulation (signal power as perceived by the smartphone).

Demodulation of system information

All system information (protocol data units, PDU) from acquired nonencrypted cells is demodulated, displayed in a separate window and can be exported.

Automatic measurement rate settings for synchronous measurements of all technologies

R&S®NESTOR automatically sets all measurement rates so that all GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO cellular network cells are measured at identical time and space intervals.

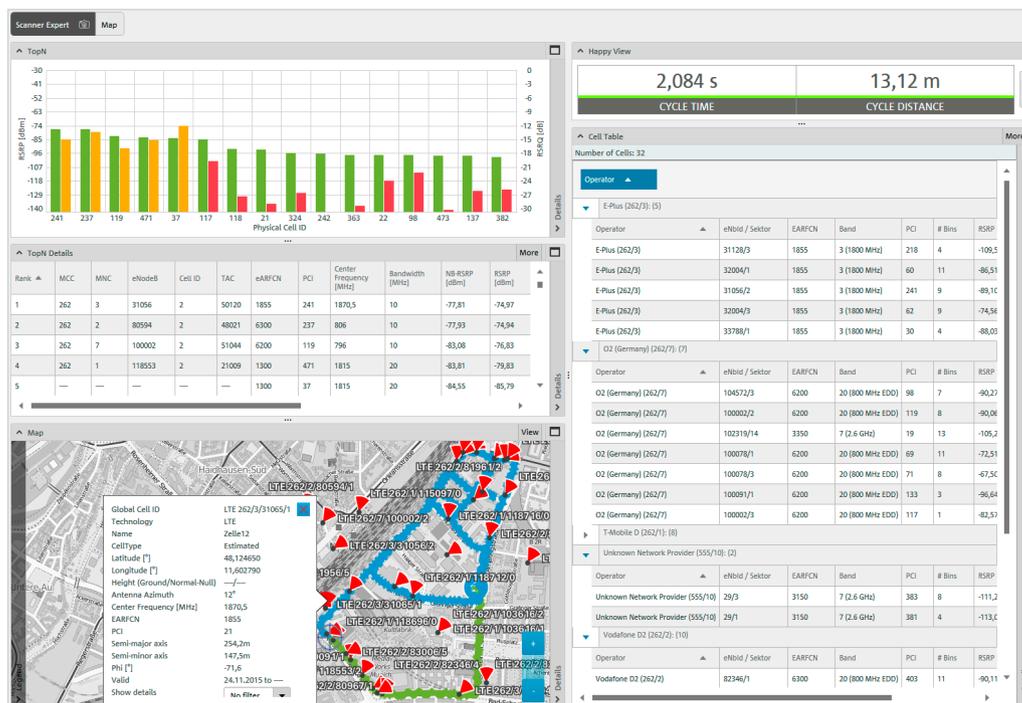
Map display of route and dedicated maps for specific measurements

The route traveled is displayed on a higher-level map. Individual maps are generated for specific use cases and use case groups, each map displaying relevant use case content. The cellular network coverage analysis map shows information such as the aggregated power values of measured cells, while the cell position estimation map displays detected cells along with positions and error ellipses.

Intuitive, high-performance display and processing filters

A set of data and display filters is available for every R&S®NESTOR use case. If one or more filters are active, the system behaves as if exclusively the filtered data was collected or as if only the filtered cells were present; this becomes evident, for example, when measurement results for analysis and export are displayed. The most important filters are those for network operators, location areas, towers, cells and geographic areas (defined by polygon geofencing).

Expert scan (SCN)



CELLULAR NETWORK COVERAGE ANALYSIS

Generation of geographically aggregated (binned) GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000®, EV-DO and IEEE 802.11 a/b/g/n/ac coverage data

Cellular network coverage analysis aggregates signal power, signal quality and UE emulation (signal power as perceived by the smartphone) into geographic bins based on UTM MGRS squares. The measured values are highly volatile, so they are aggregated into bins, and a single value for each bin is displayed on the map. Users can select a bin size between 1 m × 1 m in built-up/indoor areas and 1000 m × 1000 m in rural areas.

Top N chart, list and map display for all aggregated data

Aggregated measurement data for signal power, signal quality and UE emulation is displayed in a variety of formats, e.g. Top N chart, list and map display. This measurement data can be exported and processed externally, for example using planning software.

Live summary of cellular network coverage analysis

During network coverage analysis, geographic bins are generated, displayed and updated live with each new data set.

The R&S®NESTOR filter options are essential to efficient network coverage analysis. In conjunction with scanner

measurements, they quickly provide information for statistical and geographical analyses of network operators, selected areas, individual cells and cell groups.

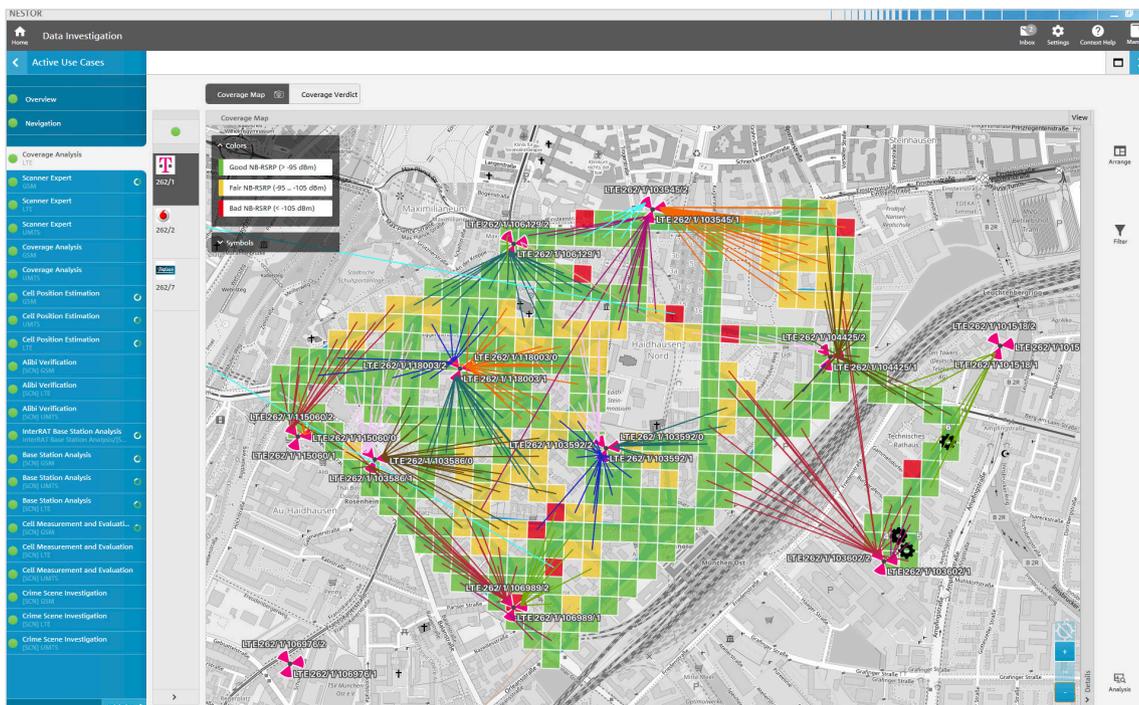
Best server plot for selected areas

Aggregated cellular network coverage data is represented in a variety of ways. The best server plot illustrates one of the most important analyses, showing the cell best suited for a cellular radio link on a map.

Cell measurement (CME)



Coverage analysis (COV)



CELL POSITION ESTIMATION

Geographic position determination for all GSM, UMTS, LTE (TDD and FDD), 5G NR, CDMA2000® and EV-DO cells as well as WLAN access points

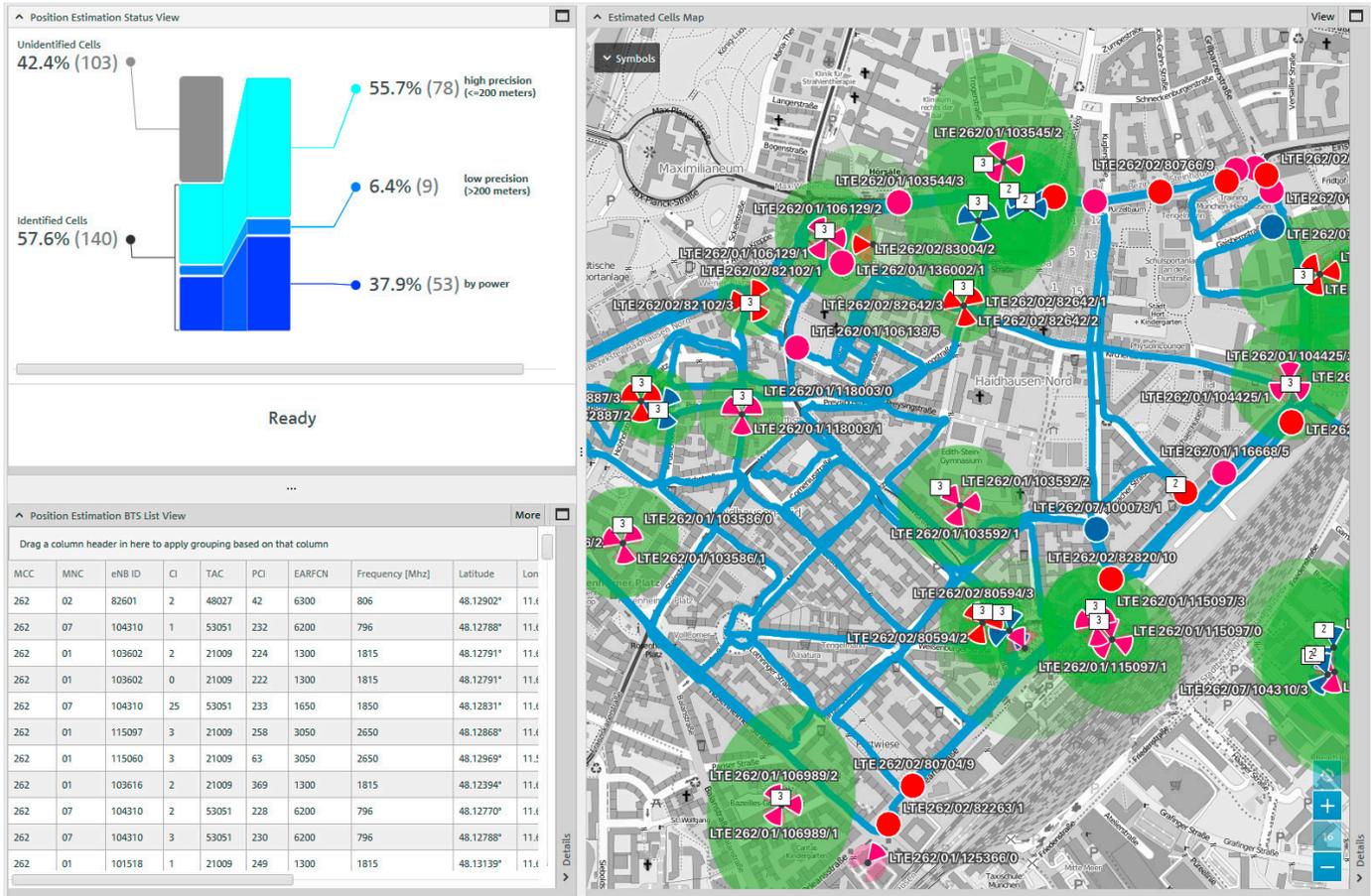
Cell position estimation is used to determine the geographic positions and sector azimuths of all measured cells during scanner measurements. Measurement data acquisition must take place while the system is in motion. Positions and sector azimuths are estimated in quick succession using advanced signal separation algorithms. This approach delivers excellent results even in difficult environments with weak signals, multipath propagation and fading.

A special algorithm recognizes whether measured sectors can be assigned to a single tower. This information is used to correlate signal processing for these sectors and obtain more accurate results. All cells are measured almost simultaneously in all bands and for all technologies.

Live map display of all position-estimated cells

Maps and lists are used to display all position-estimated cells and sectors. Fast signal processing enables high update rates so that the estimated cell positions are displayed online on the maps with continuously increasing accuracy. The position estimation error ellipses and sector confidence representations are also displayed and allow users to assess the position estimation and sector azimuth accuracy for each cell.

Cell position estimation (CPE)



Export of position-estimated cells for further processing

Position-estimated cellular network cells are not only included in R&S®NESTOR cell lists, they can also be exported for further processing. This makes it possible to create new cell lists and update existing lists. Cell lists contain channel numbers, cell positions, error ellipses, MCC, MNC, LAC, cell identities (CID), neighbor lists and other system information.

Intuitive, high-performance display and processing filters

The comprehensive R&S®NESTOR filter options for cell position estimation make it possible to carry out extensive analyses for a broad range of use cases in cellular network analysis and cell position estimation.

Airborne cell position estimation using airplanes, helicopters and commercial drones

The cell position estimation use case can be extended for airborne estimation up to an altitude of 20 000 feet for cellular network technologies.

A directional mobile radio antenna is used on the aircraft to minimize interference. Stored NASA altitude profile data provided by Rohde & Schwarz is used to determine the height above ground. An algorithm calculates cell positions, taking the height above ground into account.

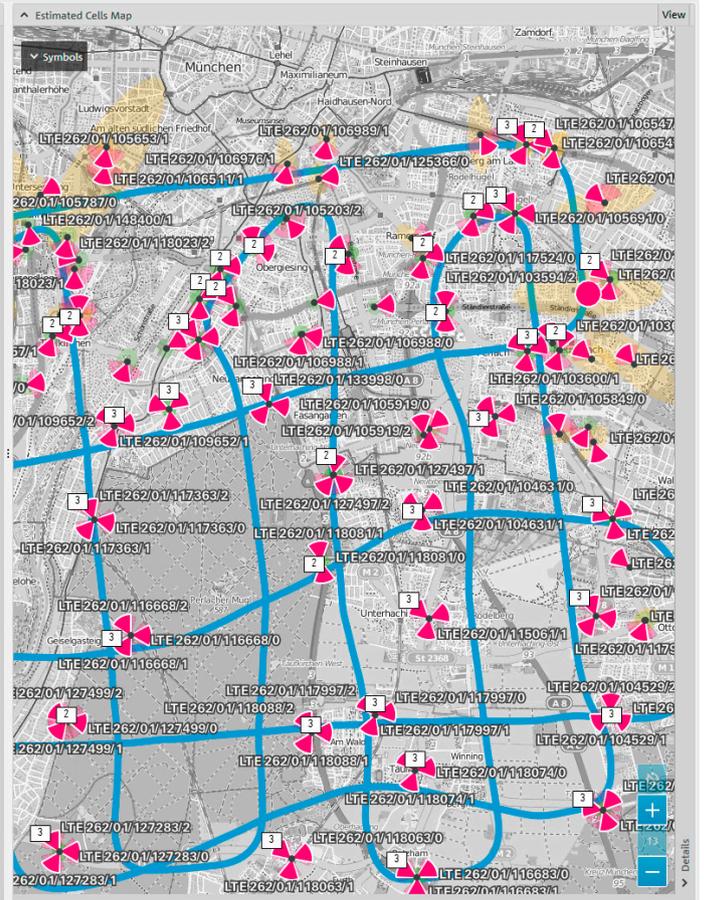
Cell position estimation accuracy is approximately the same for airborne and ground based estimations: typically 50 m for GSM and LTE, and 100 m for UMTS.

Airborne position estimation (APE)

Position Estimation BTS List View

Drag a column header in here to apply grouping based on that column

MCC	MNC	eNB ID	CI	TAC	PCI	EARFCN	Frequency [Mhz]	Latitude	Longitude	Phi [°]
262	01	145805	0	21005	296	1300	1815	48.08290°	11.17135°	-12.1°
262	01	145711	1	21005	470	1300	1815	48.17219°	11.11715°	0°
262	01	118465	1	21020	315	1300	1815	48.30753°	10.96576°	-40°
262	01	118037	1	21005	216	1300	1815	48.17717°	11.24455°	-17.7°
262	01	146164	1	21002	395	1300	1815	48.11912°	11.12781°	0°
262	01	115759	1	21005	464	1300	1815	48.16374°	11.22077°	-177.4°
262	01	118995	1	21005	229	1300	1815	48.14629°	11.34267°	-130°
262	01	118009	2	21005	225	1300	1815	48.10954°	11.28792°	-41.6°
262	01	118095	2	21005	331	1300	1815	48.10721°	11.30194°	-47°
262	01	118060	1	21005	326	1300	1815	48.12037°	11.30430°	0°
262	01	105855	1	21005	438	1300	1815	48.12995°	11.34915°	-176.2°
262	01	106203	2	21005	305	1300	1815	48.11919°	11.36857°	-176.8°
262	01	117986	2	21005	242	1300	1815	48.12100°	11.36339°	-179.5°
262	01	106203	1	21005	303	1300	1815	48.11919°	11.36857°	-176.8°
262	01	117986	0	21005	240	1300	1815	48.12100°	11.36339°	-179.5°
262	01	117986	1	21005	241	1300	1815	48.12100°	11.36339°	-179.5°
262	01	105835	1	21005	295	1300	1815	48.12951°	11.36527°	-176°
262	01	106203	0	21005	304	1300	1815	48.11919°	11.36857°	-176.8°
262	01	106018	1	21005	407	1300	1815	48.12693°	11.37603°	-177.8°
262	01	118086	2	21005	67	1300	1815	48.12162°	11.40099°	-168.4°
262	01	118086	1	21005	66	1300	1815	48.12162°	11.40099°	-168.4°
262	01	117520	2	21030	45	1300	1815	48.10858°	11.43286°	-0.7°
262	01	119985	2	21030	238	1300	1815	48.10778°	11.41540°	-7.8°
262	01	118000	1	21030	96	1300	1815	48.11789°	11.42965°	-177.1°
262	01	118000	2	21030	97	1300	1815	48.11789°	11.42965°	-177.1°
262	01	118000	0	21030	98	1300	1815	48.11789°	11.42965°	-177.1°
262	01	105537	2	21030	235	1300	1815	48.11299°	11.45149°	-9.4°
262	01	117520	0	21030	46	1300	1815	48.10858°	11.43286°	-0.7°
262	01	105939	1	21030	454	1300	1815	48.11622°	11.44933°	-4.4°
262	01	119441	1	21030	299	1300	1815	48.12412°	11.45111°	-6.1°



DETECTION AND MONITORING OF SUSPICIOUS CELLS

Monitoring and detecting irregular and interfering cellular radio cells in GSM, UMTS and LTE

A growing problem in cellular radiocommunications is the deployment of nonconforming base stations that were not included in the network operator's original network.

R&S®NESTOR offers unique capabilities to:

- Search for nonconforming cells in vehicles or on foot
- Permanently monitor large areas or in the vicinity of buildings to detect activities in nonconforming cells

Analysis of cells that deviate from operators' usual network settings

Cells that deviate from regular network settings are categorized and displayed separately with a detailed description of detected deviations. This includes unknown cells that are not found in the network operators' reference database, as well as cells with settings that deviate from the information stored in the system.

These differences can vary in significance depending on how a conspicuous cell is configured. There might be just one significant deviation or a number of deviations. An algorithm weights the deviations and a score is calculated for each cell. The score indicates the probability of a misconfigured cell. Based on this analysis, the user decides whether a measured cell should be classified as a misconfigured cell and stores this information in the system.

Determination of broadcasted system information messages, dedicated layer 3 messages and geographic positions of suspicious cells

All these measured cells are analyzed in detail using the R&S®NESTOR measurement functions. Their system information is demodulated, and the position and coverage of these cells are determined.

In addition, a connected QualiPoc smartphone allows the analysis of dedicated layer 3 procedures for unexpected behavior (e.g IMSI request during a location update procedure).

This information is used to immediately create a report or exported to a CSV file and further processed.

Searching for and monitoring nonconforming cells (base station monitoring, BSM)

The screenshot displays the BSM interface with a map on the left showing a red location marker for 'LTE 262/1/24720/1'. A central panel lists detected cells, and a right panel provides a detailed view of the selected cell.

Cell List:

14741/1	T-Mobile D	[Icon]
19569/1	T-Mobile D	[Icon]
24720/1	T-Mobile D	[Icon]
27551/1	T-Mobile D	[Icon]
25791/1	T-Mobile D	[Icon]
103594/5	T-Mobile D	[Icon]
105673/3	T-Mobile D	[Icon]
115097/3	T-Mobile D	[Icon]
116668/5	T-Mobile D	[Icon]
M-Berg-a...	T-Mobile D	[Icon]
M-Ostba...	T-Mobile D	[Icon]
100064/13	Telefonica	[Icon]

Cell Details (LTE 262/1/24720/1):

Operator	T-Mobile D	MCC	262	MNC	1		
RAT	LTE	Band	20 (800 MHz EDD)	EARFCN	6400	PCI	223
Center Frequency	816	Bandwidth	5				

Measurements:

TSMA	First measured	Last measured
TSMA 100411	29.11.2017 13:43:59	29.11.2017 13:48:40
TSMA 100402	29.11.2017 13:43:59	29.11.2017 13:48:38
TSMA 100400	29.11.2017 13:44:25	29.11.2017 13:48:38

Live map display

All cells contained in the network operators' reference database and all measured cells are displayed on a map. Cells not included in the reference database and suspicious cells are highlighted in color.

Smart configuration of suspicious cell criteria

The majority of the criteria used to classify cells as misconfigured is set by the user to take into account network operators' local conditions. For each network operator in a known region, it is possible to "train" a set of criteria that describe the operator's network and show deviations due to suspicious cells.

Deployment in mobile and stationary applications

Both mobile and stationary measurements and analyses are possible.

Stationary measurements are used to monitor the network situation in the environment of special facilities over an extended period. Here, R&S®NESTOR is permanently installed with a high-end antenna such as the R&S®HE600, and carries out cell measurements in the facility's environment 24/7. R&S®NESTOR triggers an alarm or emails a description of any irregularity as soon as it is detected.

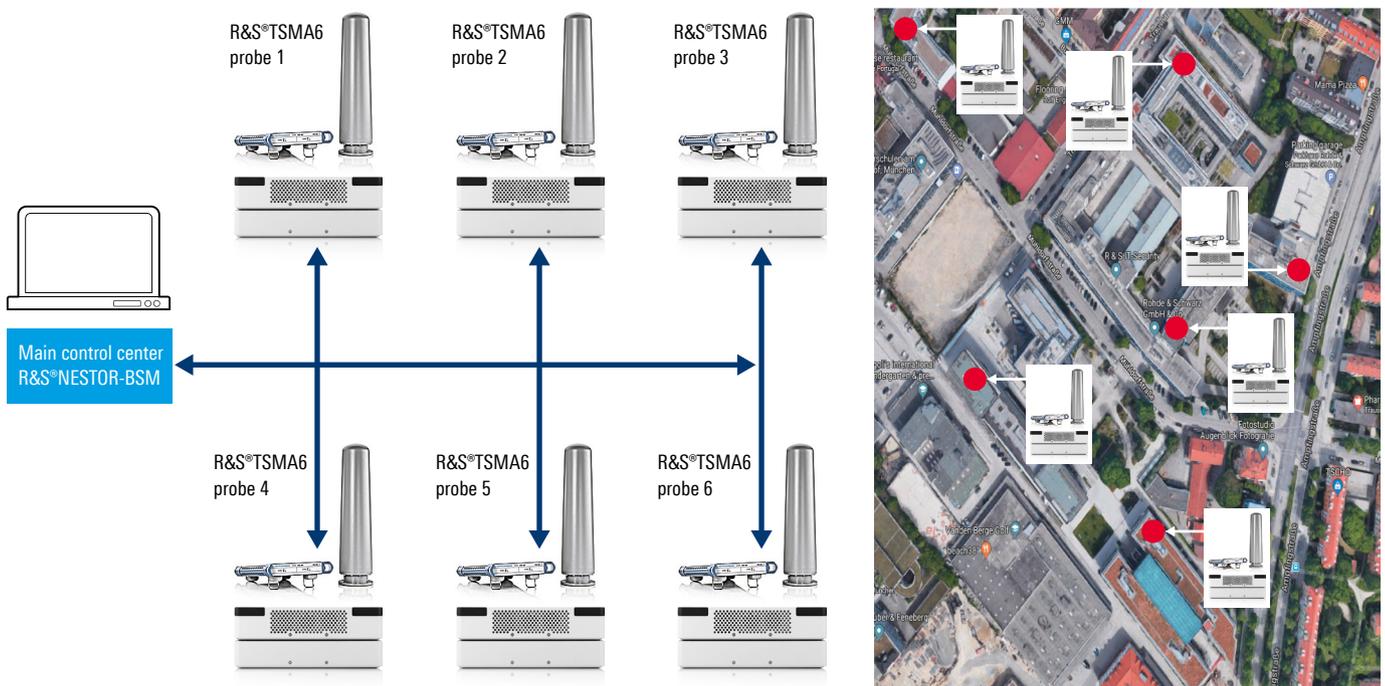
Mobile measurements are used to identify suspicious cells at any location. These measurements are more dynamic, and other criteria are used to detect misconfigured cells.

Online and offline analysis

All measurements can be performed live on site from a vehicle, airplane, helicopter, drone, ship or on foot.

Comprehensive, previously stored measurement data is used to perform subsequent offline analysis.

Example of base station monitoring on the Rohde & Schwarz campus



INSTALLATION OF NEW CELL SITES

Configuring GSM, UMTS and LTE cells to be added to a network environment

With the rising complexity of network topologies (increasing number of technologies and frequency bands to consider, macro and femto cell sites, etc.), deploying new cells in existing mobile operator networks is becoming more complicated. Moreover, the focus is often on quick integration into these networks to cope with higher capacity requirements, e.g. special events at a specific location for a limited duration.

R&S[®]NESTOR offers unique capabilities to:

- ▶ Analyze existing network topologies
- ▶ Determine optimal cell parameters to fit into a network
- ▶ Output this set of parameters for configuration purposes and new cell activation

Analysis of existing network operator cells

Before deploying new cells in a network, it is critical to get an accurate overview of it. The measuring functions of R&S[®]NESTOR allow the demodulation of system information for the existing cells to analyze the network configuration in terms of logical and physical parameters as well as additional settings such as the use of barred cells or topology-specific features, e.g. femto cells. Comprehensive, previously stored measurement data is used to perform subsequent offline analysis.

Determination of optimized cell parameters

Based on the previous analysis, R&S[®]NESTOR can automatically determine a set of suitable physical and logical parameters, channels and neighbor lists that match the current environment. This information is used immediately, exported to other tools or saved for future use.

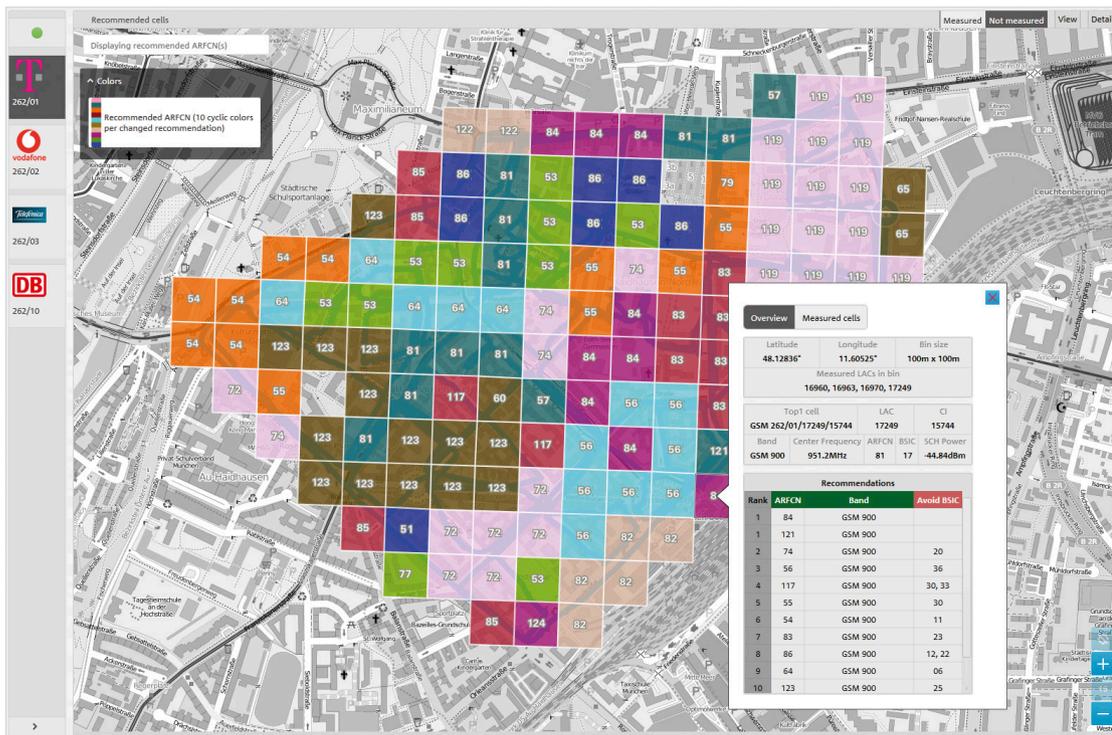
Live map display of best cell for selected areas

The infill cell planning (ICP) map automatically displays the cells that are best suited for a cellular radio link in the measured area. For each network operator in a known region that selects such an area, an overview is created of the parameters that the new cells should use to suit the environment.

Online and offline analysis

The user may perform the analysis before cell deployment, in case measurements from the area of interest are already available, or live during the deployment of the cells to be added.

Infill cell planning (ICP)



FORENSIC INVESTIGATIONS

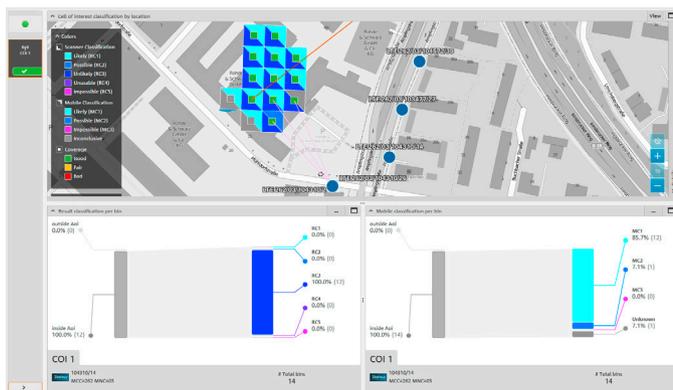
Retrieval of cell coverage data for confined areas (alibi verification)

If communications logs of a suspect's mobile phone have been retrieved from the suspect's cellular network operator, alibi analysis is used to quickly determine whether the suspect's mobile phone was in a specific location or area at a specific time. This communications data can also be used to determine any other location where a suspect might have been instead.

Network coverage is determined using previously measured data or a Rohde&Schwarz mobile network scanner. (QualiPoc smartphones can also be used to fine tune the analysis.) The coverage of the detected cells in the area in question is displayed both graphically and in a table.

Results are classified and describe whether and where the detected cells are best servers and how adjacent cells behave with respect to a best server. The probability of a suspect actually having been in the area in question can therefore be quickly and clearly displayed, provided the cell log information for the suspect's mobile phone has been retrieved from the network operator. This information is used to immediately create a report or exported and further processed.

Result of alibi verification measurement (ALI)



Retrieval of cell coverage data for confined areas (crime scene investigation)

It is often necessary to determine the cells of all network operators that could have been used for communications in a certain area, e.g. where a crime was committed. If the area is known, this analysis makes it possible to quickly identify the cells that were most likely used for communications at a specific time in a specific location or area.

In addition, connected QualiPoc smartphones make it possible to fine tune the analysis by providing information on which cells they consider as serving cells during the investigation.

This information is used to immediately create a report or exported and further processed.

With the list of cells at hand, law enforcement is able to contact network operators to request a list of subscribers that were in the specific location or area at the specific time. This can significantly help to improve criminal investigations.

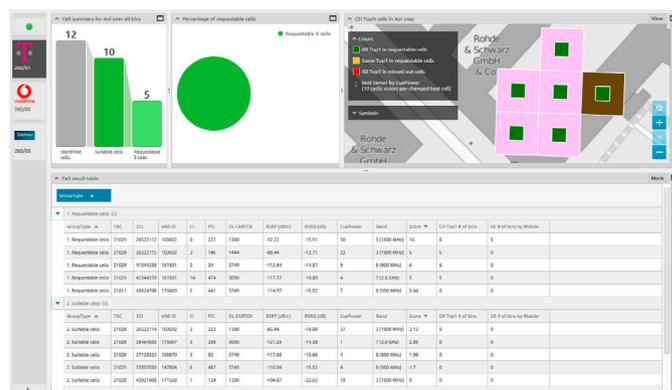
Live map display

During the measurement, analysis results and involved cells are displayed live on a map.

Online and offline analysis

All measurements can be performed live on site from a vehicle, airplane, helicopter, drone, ship or on foot to support law enforcement or any emergency measures. Comprehensive, previously stored measurement data is used to perform subsequent offline analysis.

Crime scene investigation (CSI)



CONFIGURATIONS FOR MOBILE USE

R&S®NESTOR and the connected hardware components (Rohde & Schwarz mobile network scanner, dead reckoning GPS) are mainly used in the following configurations:

- ▶ Customized configuration
- ▶ Carrying bag system
- ▶ Backpack system (open or closed)
- ▶ Test vehicle

R&S®NESTOR for outdoor use in a test vehicle



R&S®TSM6 with carrying bag and Windows tablet



R&S®NESTOR with the R&S®FR4 Freerider 4 backpack system



SYSTEM REQUIREMENTS

R&S®NESTOR system requirements

Minimum recommended equipment

- ▶ PC, notebook or tablet with a quad core CPU (8 threads)
- ▶ 16 Gbyte RAM
- ▶ 256 Gbyte SSD
- ▶ 1 Gbit LAN interface, support of 9k jumbo frames for R&S®TSME6 and R&S®TSME
- ▶ Display resolution: 1440 × 900 pixel
- ▶ Windows 10, 64 bit
- ▶ DirectX 11 compatibility

ORDERING INFORMATION

Designation	Type	Order No.
Cellular network analysis software	R&S®NESTOR	1522.8870.02
Accessories supplied: DVD, microSD card with USB adapter		
Software options		
Driver for Rohde&Schwarz mobile network scanners	R&S®NESTOR-SCN	1521.5031.02
Automatic cell detection	R&S®NESTOR-ACD	1521.5048.02
Coverage analysis	R&S®NESTOR-COV	1521.5077.02
Cell position estimation	R&S®NESTOR-CPE	1521.5054.02
3GPP spectrum analysis	R&S®NESTOR-SCA	4900.3110.02
Airborne cell position estimation	R&S®NESTOR-APE	1527.1709.02
Forensic analysis	R&S®NESTOR-FOR	1521.5060.02
Base station analysis	R&S®NESTOR-BSA	1521.5354.02
Base station monitoring	R&S®NESTOR-BSM	4900.3155.02
Indoor	R&S®NESTOR-IND	4900.3103.02
Infill cell planning	R&S®NESTOR-ICP	1521.5102.02
Driver for WLAN hardware	R&S®NESTOR-WLN	4900.3126.02
Driver for QualiPoc smartphone	R&S®NESTOR-QPD	4900.3161.02
Service options		
Multiversion license, one year	R&S®NESTOR-1Y	1522.8870.82
Multiversion license, two years	R&S®NESTOR-2Y	1522.8870.84
Multiversion license, three years	R&S®NESTOR-3Y	1522.8870.83
Multiversion license, five years	R&S®NESTOR-5Y	1522.8870.85
Hardware		
High performance notebook	R&S®RMS-FX-N2	3059.2550.05
Tablet laptop	R&S®RMS-FX-T1	3060.5889.05
WLAN sensor case	R&S®WLM-SCR	4112.8314.03
Dead reckoning GPS with PPS	R&S®TSMX-PPS2	1515.7120.02
Mobile network scanners		
Autonomous mobile network scanner	R&S®TSMA6	4900.8005.02
Ultracompact drive test scanner	R&S®TSME6	1514.6520.02
Ultracompact downconverter, 24 GHz to 30 GHz	R&S®TSME30DC	4901.1004.02
Autonomous mobile network scanner	R&S®TSMA	1514.6520.20
Ultracompact drive test scanner	R&S®TSME	1514.6520.02
Universal radio network analyzer	R&S®TSMW	1503.3001.03

For more information, see Rohde&Schwarz mobile network scanner data sheets.

Service that adds value

- ▶ Worldwide
- ▶ Local und personalized
- ▶ Customized and flexible
- ▶ Uncompromising quality
- ▶ Long-term dependability

Rohde & Schwarz

The Rohde&Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Sustainable product design

- ▶ Environmental compatibility and eco-footprint
- ▶ Energy efficiency and low emissions
- ▶ Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001

Rohde & Schwarz training

www.training.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support

