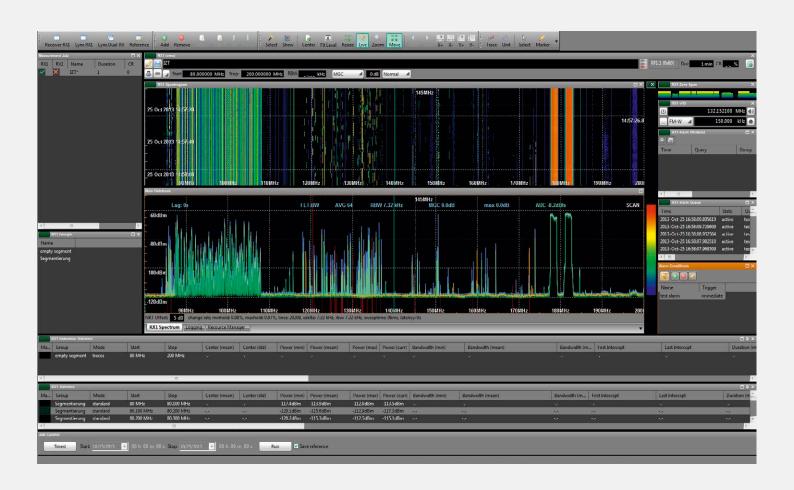# IZT Signal Suite
Anti-Surveillance System LYNX

- RF environment reconnaisance
- Identify unusual transmissions
- Complex signal statistics
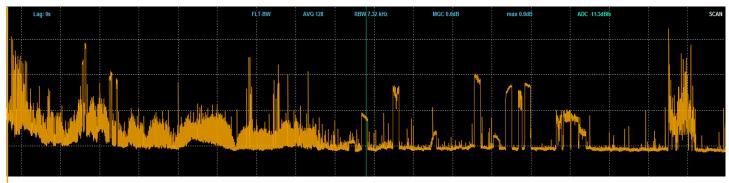- Actions upon alarm criteria
- Data content analysis

IZT Signal Suite Anti-Surveillance System LYNX

FIGURE 1: PANORAMA SCAN SPECTRUM DISPLAY

IZT LYNX is a specially designed anti-surveillance application to check for unusual RF transmissions in buildings and rooms used for confidential meetings. One of the objectives is to detect radio transmitters in secure areas and prevent them from collecting and forwarding confidential information.

TECHNICAL BACKGROUND

IZT LYNX scans for signal activity, analyzes signal statistics and compares current with previously recorded RF environments. This method allows to identify RF emissions from hidden devices like audio bugs or wireless video cameras as well as forbidden communication relying on modern cellular networks.

Signals are analyzed by complex signal statistics algorithms to determine their nature. Detected signals are characterized in a black-list and can activate multiple alarm actions by user specified criteria like power level above noise riding threshold, occupied bandwidth or transmission time and its logical link conditions. A triggered alarm can for example send alert messages, demodulate a signal or record the RF signal for a detailed analysis later on in the lab. Signals identified as harmless can be removed from the alarm list and added to a whitelist.

For efficient and fast detection IZT LYNX supports simultaneous operation of two receivers. The advantage of this configuration is that one receiver can be used for continuous fast scanning of the entire frequency range from 9 kHz to 18 GHz while a second receiver can analyze detected signals. The two receiver setup allows comparing two different antenna signals at different locations in order to establish whether a detected signal is coming from inside or outside the building.

Additional IZT software packages complete the IZT LYNX functionality with off-line analysis, including user access to spectrum, spectrogram or I/Q data via IZT SDK.
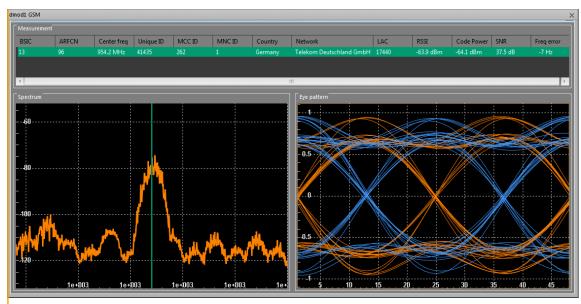

FIGURE 2: PLUG-IN FOR GSM, UMTS & LTE BASE STATIONS DECODING CELL INFORMATIONS
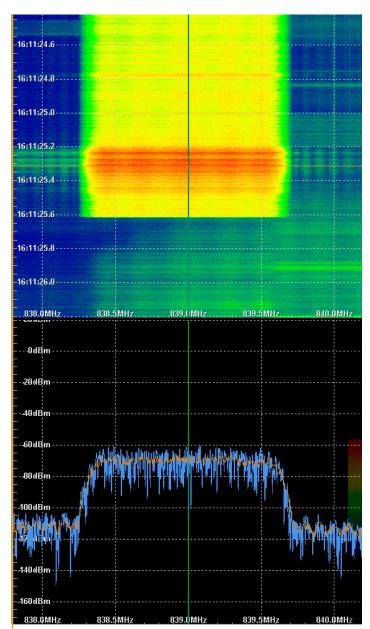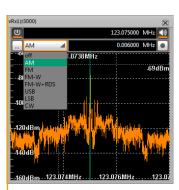
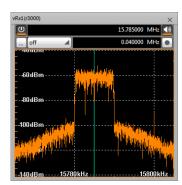**FIGURE 3:** SUB-BAND MONITORING WITH SPECTRUM & SPECTROGRAM DISPLAY

FIGURE 4+5: SPECTRUM, DEMODULATION AND RECORDING OF DETECTED SIGNALS

KEY FEATURES

Identify unusual transmissions at a location
- Gather reference data
- Compare current RF environment with reference data
- Complex signal statistics

Actions upon alarm criteria
- Alert messages
- Whitelist
- Logical operations on alarm conditions
- Automatic recording of I/Q data or demodulated signal

Data Content Analysis
- Digital and analog modulation standards
- Classifier integration
- Histogram and percentile display to identify "hidden" signals
- IZT SDK for MATLAB, C# and C++ data access

USE CASES

- Identify forbidden communication
- Counter surveillance
- Protect confidential meetings
- Directional estimation
- Perform spectrum searches for signal isolation, classification and I/Q recording
- Allow service providers to find "clear" spectrum

BENEFITS

- 9 kHz to 18 GHz fast scan mode
- Alarm based on signal statistics and reference traces
- Customized alarm actions
- Automatic demodulation
- Dual receiver operation with one sensor controller

HARDWARE

- Supports IZT R3000 & R4000 high-end receivers
- Ideally suited for IZT R3410 and IZT R3411
- IZT specified notebooks and sensor controllers

IZT
Innovationszentrum
Telekommunikationstechnik