Debugging of Embedded IoT Systems

Jarno Tervo
Key Account Manager

3-May-2017
Embedded Conference Finland

ROHDE&SCHWARZ

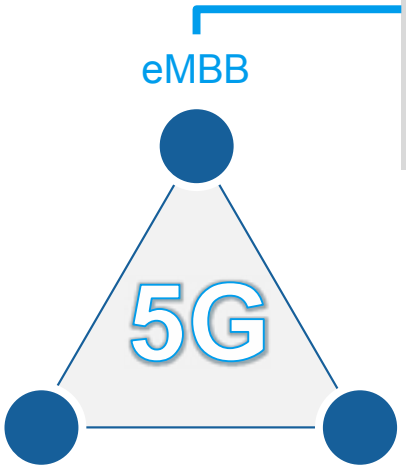
The Triangle of 5G Use Cases

eMBB – the known playground

- Established ecosystem (operators, manufacturers, certification of devices)
- Evolution from existing technologies (LTE-A, 802.11 ad) and revolutionary additions (cm- / mm-wave)
- It's all about data (speed and capacity)

Massive IoT

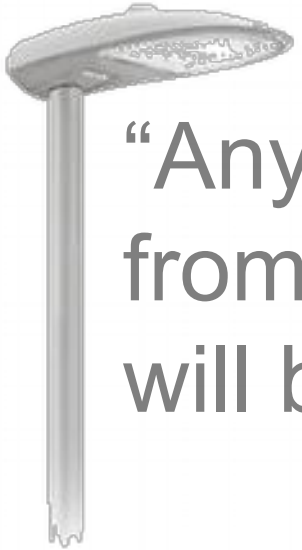
- A diverse ecosystem (operators, manufacturers, local authorities, certification only for some technologies)
- Mix of technologies (GSM, Lora, Zigbee, WLAN, Bluetooth, Cat M, NB-IoT,…)
- It's all about cost efficiency and massive connectivity



URLLC

- A significantly enhanced and diverse ecosystem (operators (?), manufacturers, verticals, certification not existing (yet))
- Existing technologies do not provide sufficient performance
- It's all about reliability and security (data and capacity)

IoT Use Cases



"Anything that benefits from network connection will be connected" *Ericsson, 2010*

Agenda

- **IP Connection Security Analysis**
- Power consumption measurement, Battery lifetime
- Debugging of Embedded IoT Systems with a Multi-Domain Oscilloscope

R&S Test Solution

The common IP data testing solution within the R&S®CMW platform

R&S®CMW500

IP throughput

IP traffic analysis

IP connection security analysis

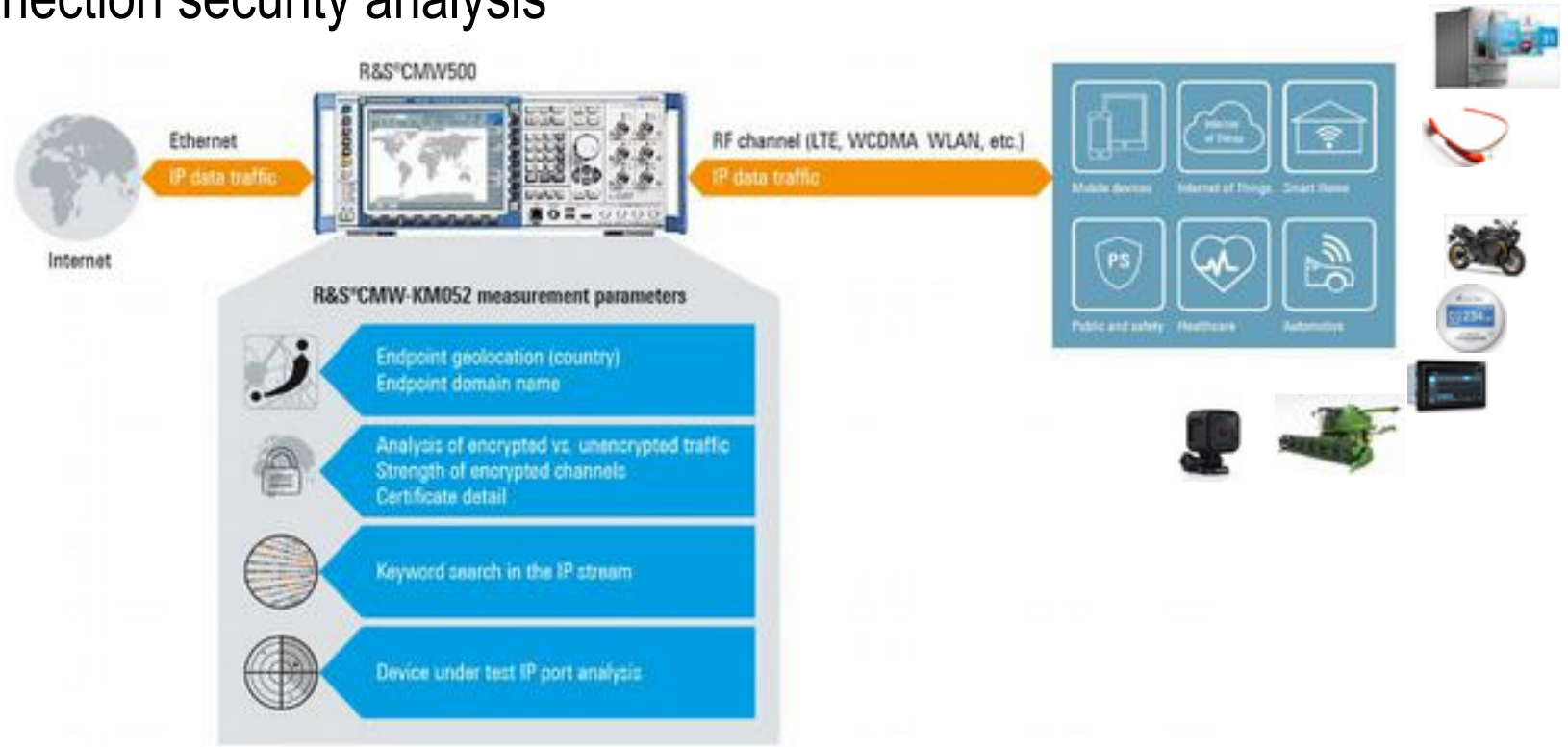
Key features

Data Application Unit – B450D/H:

- Common data testing solution over all technologies in the R&S®CMW platform
- Simple to use, easy to configure “in a box” data testing solution
- IPv4 and IPv6 support
- Data-testing capabilities
  - Server for FTP, HTTP, IMS, DNS and video
  - IMS services: voice, video, SMS and RCS
  - IP impairments (now called quality of service)
  - IP logging, IP protocol statistics and IP connection security analysis
  - PING latency measurements
  - Throughput measurements and generator (iperf)
  - eMBMS broadcasting test solution
  - ePDG interface for easy WLAN offload and VoWLAN testing (one box)

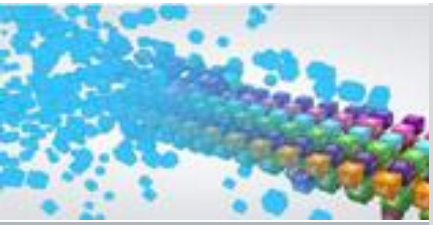
R&S Test Solution

IP connection security analysis



CMW-KM052 IP Connection Security Analysis

- **What is CMW-KM052 IP Connection Security Analysis?**
  - The new option **CMW-KM052 IP Connection Security Analysis** extends the functionality of R&S CMW500 to **collects, summarize and display objective security parameters** of established IP connections **of** both **mobile devices and IoT devices**.
    e.g:
    - **Endpoint geo location (country)**
    - **Encrypted vs. unencrypted traffic**
    - **SSL/TLS handshake details**
    - **Clear text keyword matching analysis**
    - …



*CMW-KM052 solution is based on the **R&S® PACE 2** protocol and application classification and analysis engine from the R&S Cybersecurity division*
https://cybersecurity.rohde-schwarz.com/en/products/network-analytics/rsrpace-2

Summary

- The **first mobile communication tester** combining RF and protocol test in a single instrument, inclusive IP application testing and **IP connection security analysis**.
- IP connection security measurements **under controlled network conditions for cellular and non-cellular technologies** (different countries, different MNOs, repeatable/comparable results from network side)
- **No modification** or additional tools or software **required on device under test**
  - important if no debugging interfaces are available or no modification of the device is possible or allowed
- **Just a few user skills** needed for an overview of IP-CS KPIs (e.g. compared to Wireshark filtering)

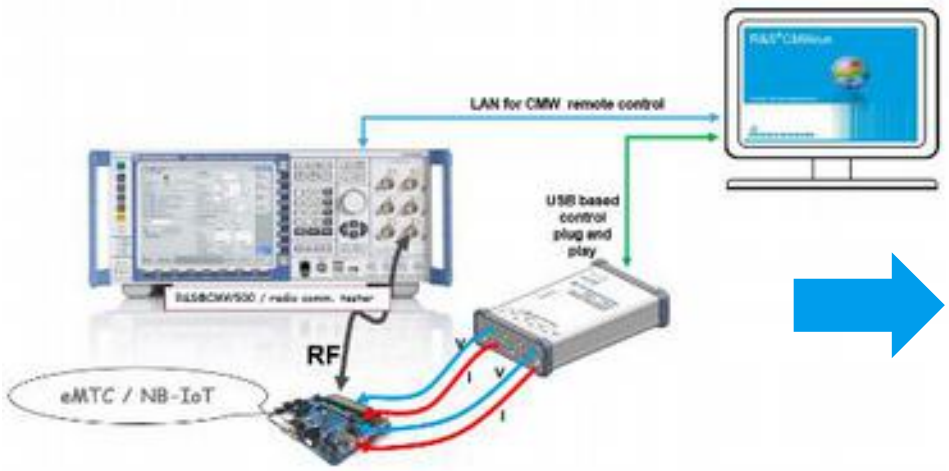
Agenda

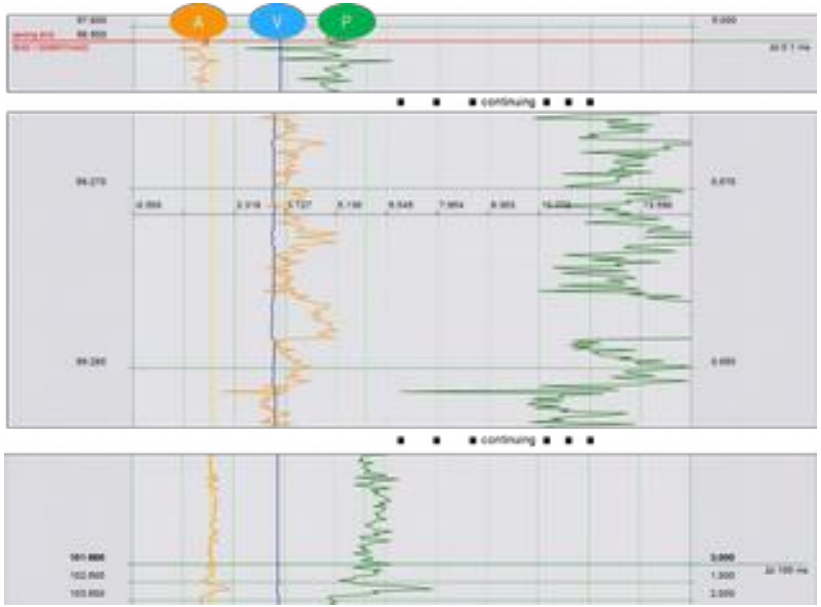
- IP Connection Security Analysis
- **Power consumption measurement, Battery lifetime**
- Debugging of Embedded IoT Systems with a Multi-Domain Oscilloscope

R&S Test Solution

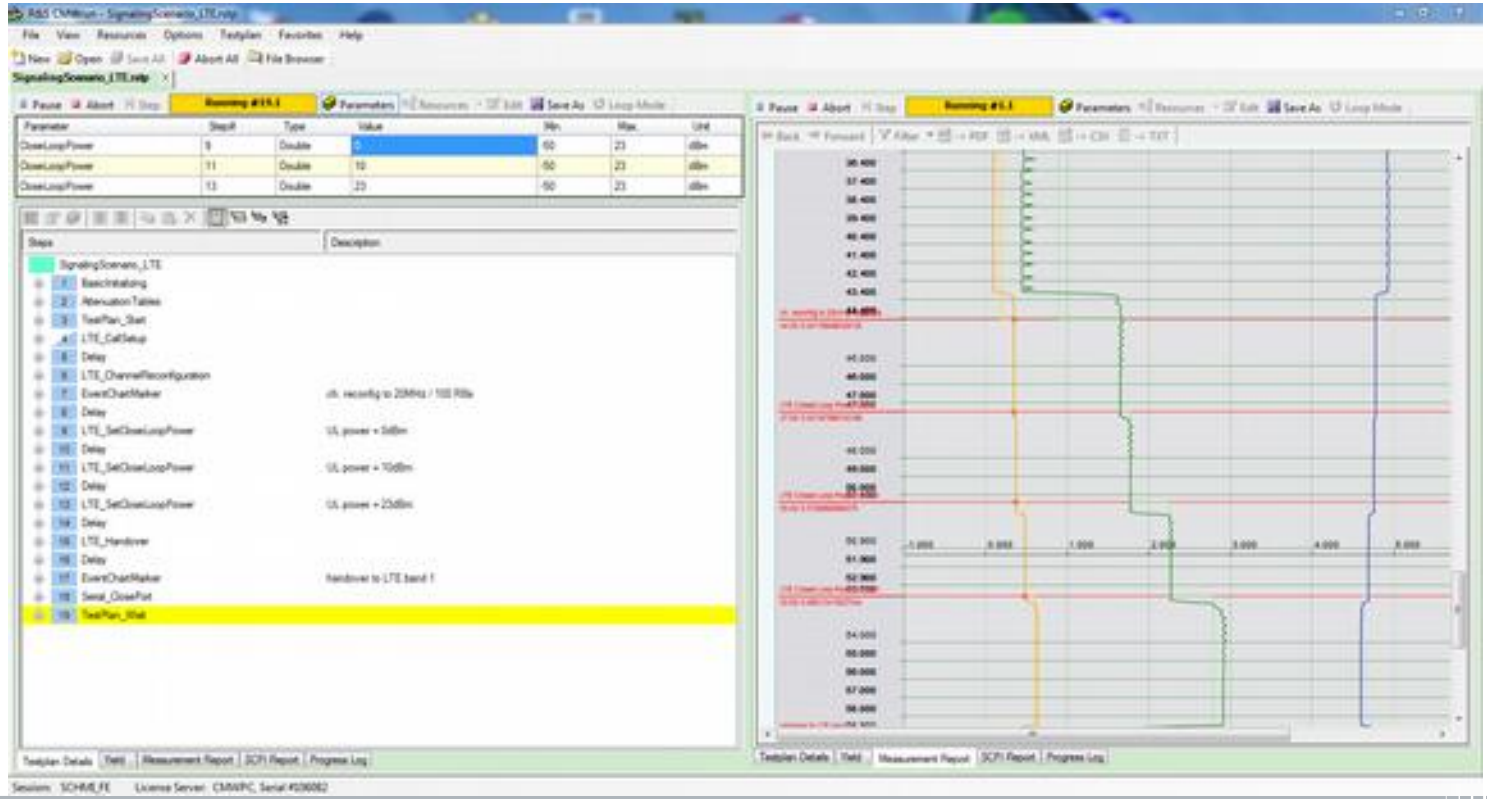
Battery Life Measurements - CMW500 and multi-channel power probe

- Multi-channel power monitoring (2 or 4 ch)
- Total consumed power versus consumed power of parts of the circuit, like the application processor, baseband chip



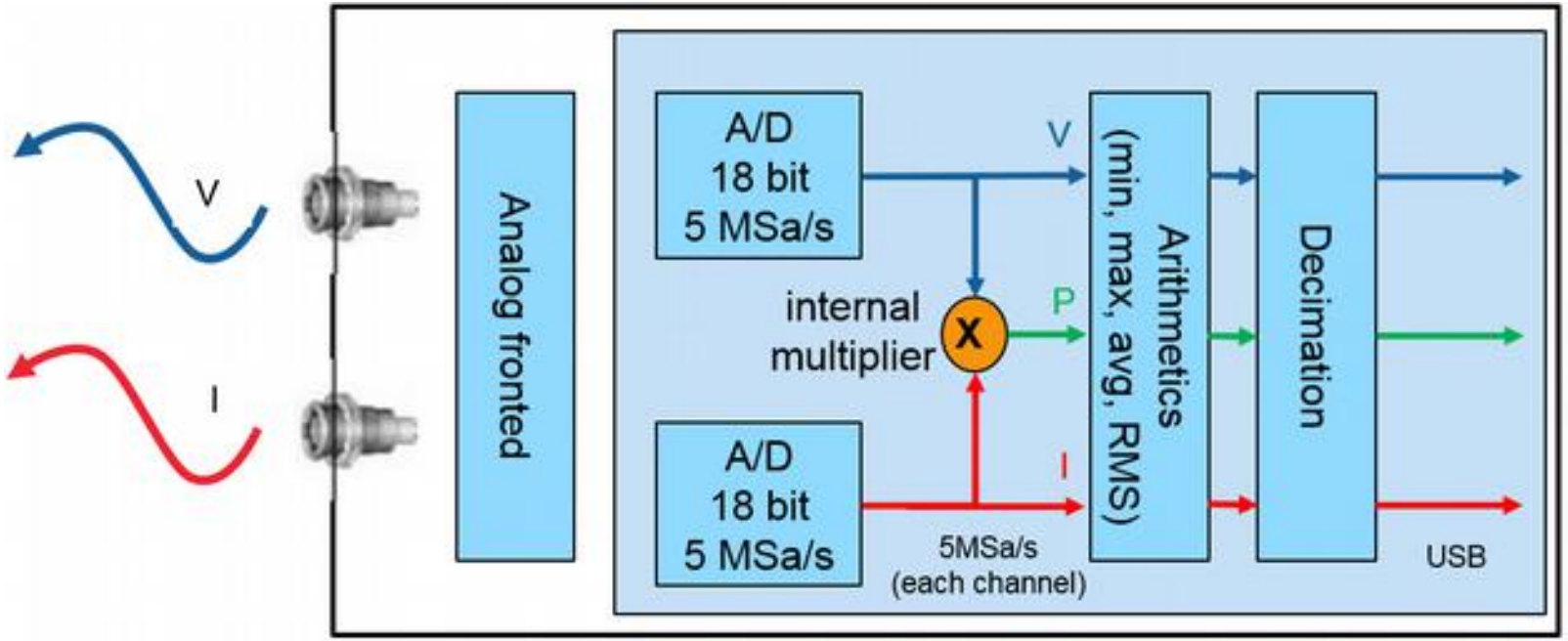


Correlation with signaling states (sig. event markets)



Ideal for testing low currents (~ nA)

- High dynamic range and time resolution



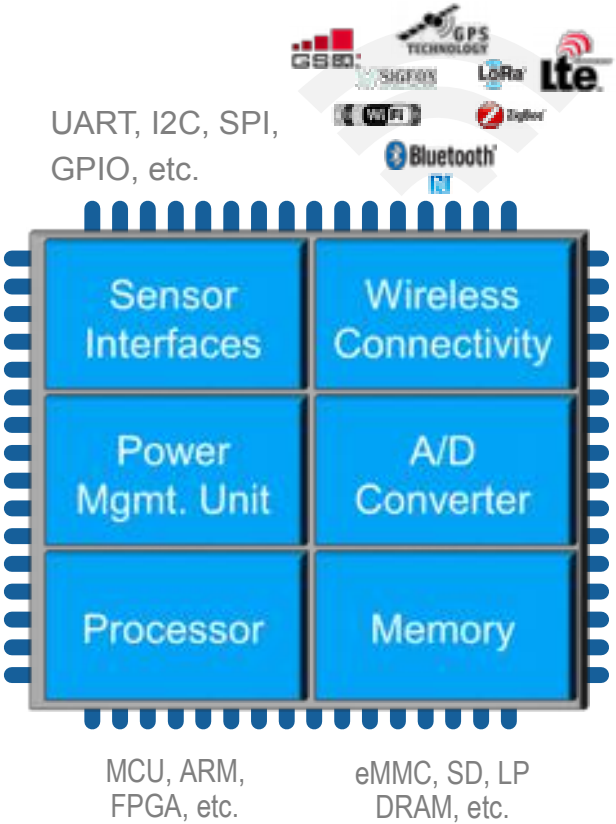
Agenda

- IP Connection Security Analysis
- Power consumption measurement, Battery lifetime
- Debugging of Embedded IoT Systems with a Multi-Domain Oscilloscope

Embedded IoT Devices
Architecture & Challenges

IoT devices combine resources for sensor data collection, computing and connectivity, as well as infrastructure for power management and storage.

- *Embedded Designs with high integration level of different technologies*
- *Often battery powered*



1. Test Challenges

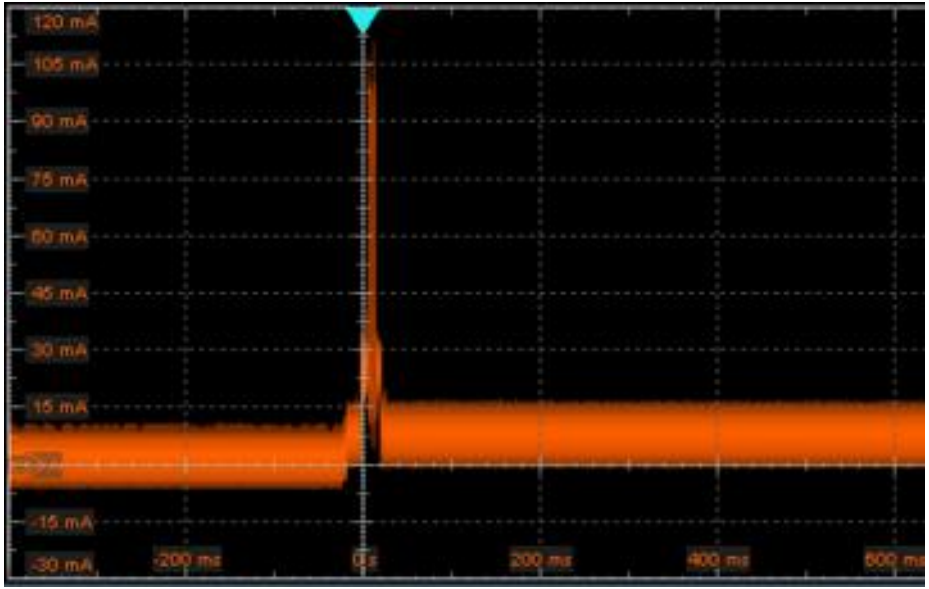
Current Consumption

Challenge

- Battery life time of IoT systems is supposed to be measured in years
- *Optimize system functionality and power consumption*

Requirements for Test Equipment

- Capable to measure fast transitions from single digit mA to several 100 mA
- Time correlation to other T&M equipment



2. Test Challenges

Wireless Interfaces

Challenge

- Many IoT devices use wireless connectivity
- Wireless communication modules are new for many Embedded Design developers

Requirements for Test Equipment

- Capable to capture and analyze wireless signals
- Time correlation to other T&M equipment

3. Test Challenges

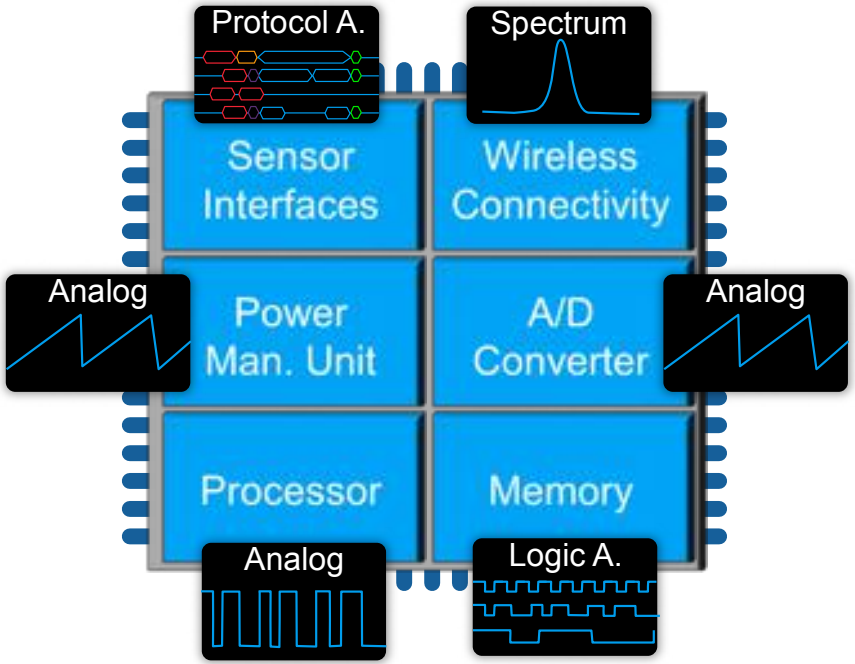
Debugging overall system functionality

Challenge

- IoT systems combine multiple functional cores at very dense space
- Risk of interferences

Requirements for Test Equipment

- Tools to analyze various signals types:
  - DC, analog, current, logic, protocol or spectrum
- Time correlation to other T&M equipment

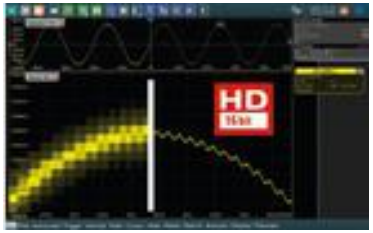


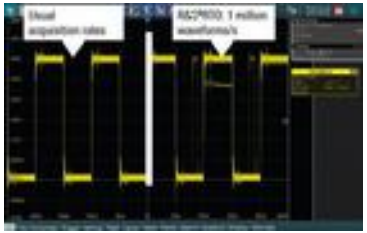
R&S Debug Solution: the R&S®RTO Oscilloscope

R&S®RTO Key Performance Parameters

Best performance

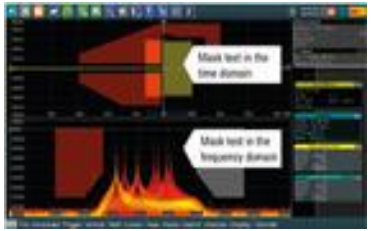
- 6 GHz, 20 Gsample/s, 2 Gsample deep memory
- Low noise, high dynamic, up to 16-bit res.
- Finding signal faults quickly - 1 million wfms/s
- Trigger on any signal details - digital trigger system

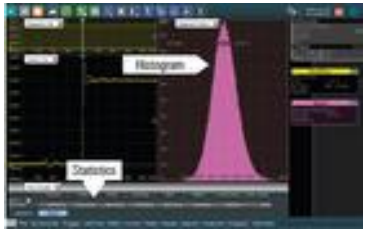




Widest range of capabilities

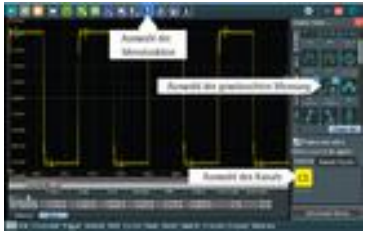
- QuickMeas: key results at the push of a button
- Integrated spectrum analysis
- History: analyze previous acquisitions
- Mask: settings in only seconds
- First Zone trigger in time and frequency domain





Powerful user interfaces

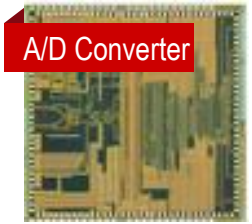
- High-resolution 12.1” capacitive touch screens
- Easy customizable waveform displays
- Fast access to important tools
- Undo/redo forgives your mistakes



R&S®RTO Current Measurements

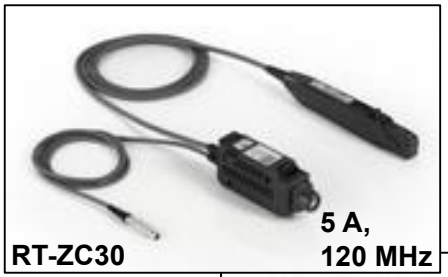
RTO key capabilities for high-sensitivity measurements

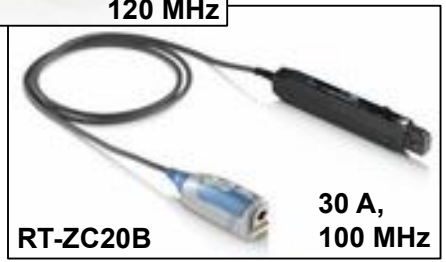
- Low noise, >7 bit ENOB ADC, high sensitivity FE
- 16 bit High Definition mode



Current probes for small currents and high bandwidth

- R&S®RT-ZC30 High-sensitivity current probe
  (120 MHz, 5 A (RMS), 60 uA noise, 1 V/A)
- R&S®RT-ZC20B
  (100 MHz, 30 A (RMS), 1 mA noise, 10 V/A)

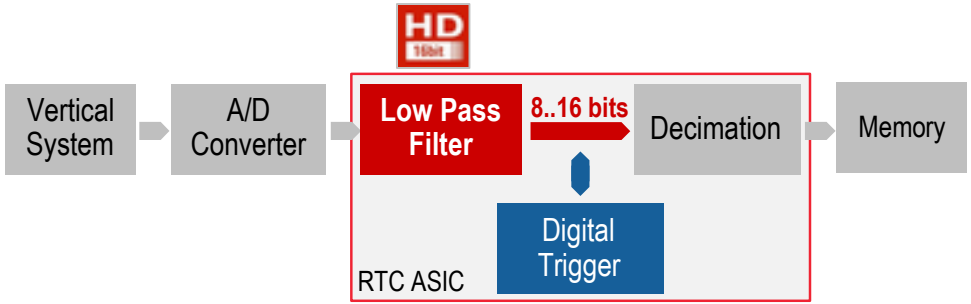




R&S®RTO 16 bit High Definition Mode

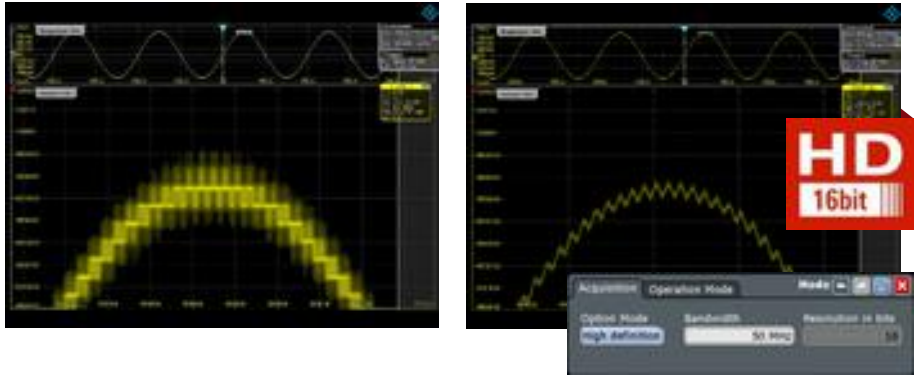
High Definition system design

- Single-core monolithic ADC (10 Gsample/s, > 7 ENOBs)
- 16 bit wide processing architecture



High Definition mode (R&S®RTO-K17)

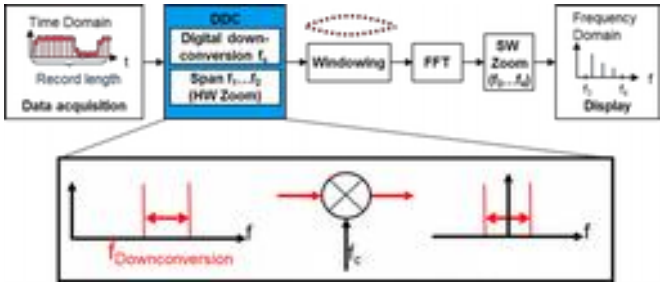
- Up to 16 bit vertical resolution
- More signal details and more precise analysis results
- Real-time triggering on smallest signal details
- No aliasing, no decimation
- High acquisition rate and signal processing
- All in one box!

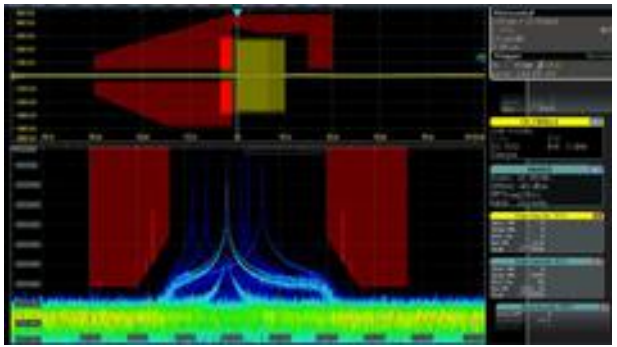


R&S®RTO RF Signal Analysis

Integrated FFT-based Spectrum Analysis

- **Spectrum analyzer like operation**
  - Set START, STOP, SPAN and RBW
- **Overlapping FFT**
  - Fast and accurate detection of rare events
- **Digital down-conversion (DDC)**
  - FFT done on the selected frequency range
  - Higher resolution compared to conventional FFT
- **Zone Trigger in Frequency Domain**
- **… and additionally**
  - Up to 4 channels in parallel
  - Correlated analysis of signals in time- & and frequency domain





R&S®RTO RF Signal Analysis

Enhanced Spectrum Analysis with RTO-K18

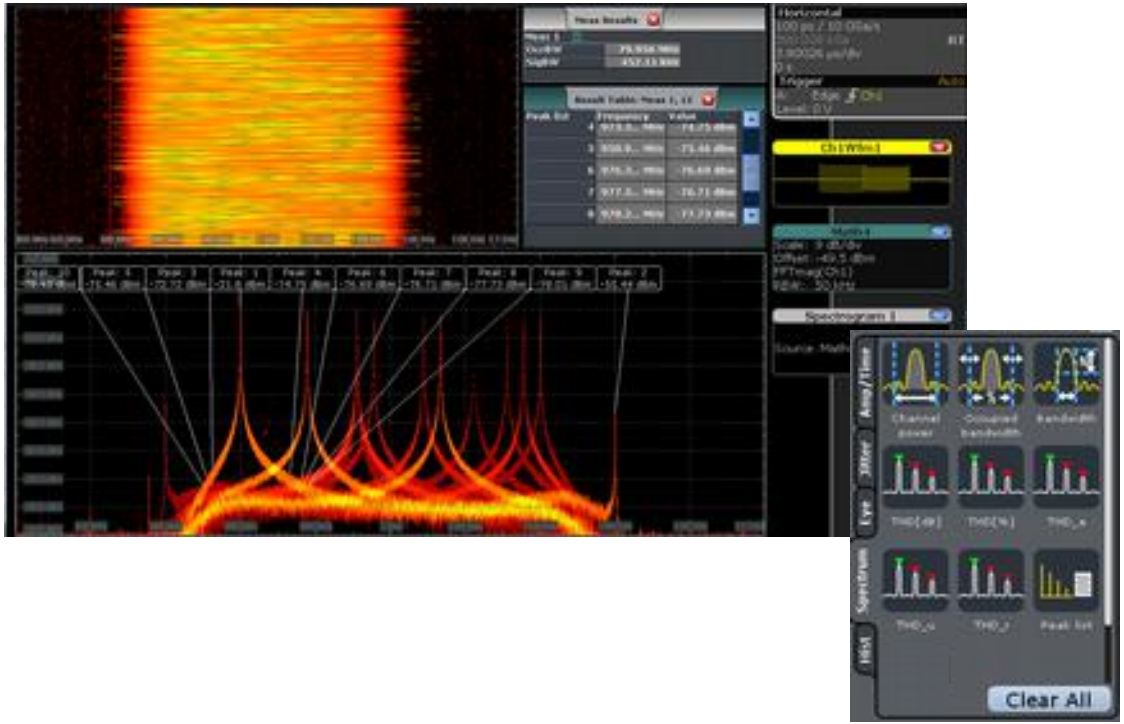
Spectrogram

- **Visualization of changes vs. time**
  - Power vs. time
  - Frequency vs. time

Peak list

- **Peak visualization in frequency domain**
  - Automatic labeling
  - Threshold level for peak detection

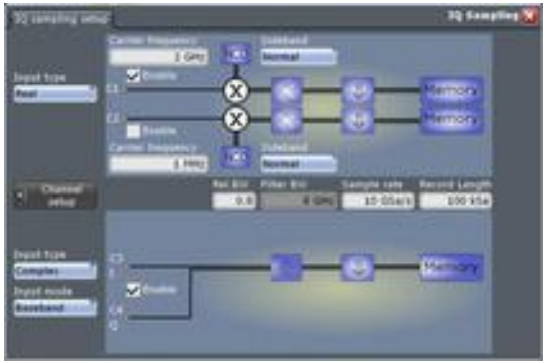
Log-Log scaling



R&S®RTO RF Signal Analysis

IQ Interface with RTO-K11

- Acquisition of modulated signals and delivery of the corresponding I/Q data
- Resampling of the I/Q data to a required sample rate
- Supported input signal formats:
  - RF signals
  - I/Q baseband signals
  - Modulated signals in low-IF range

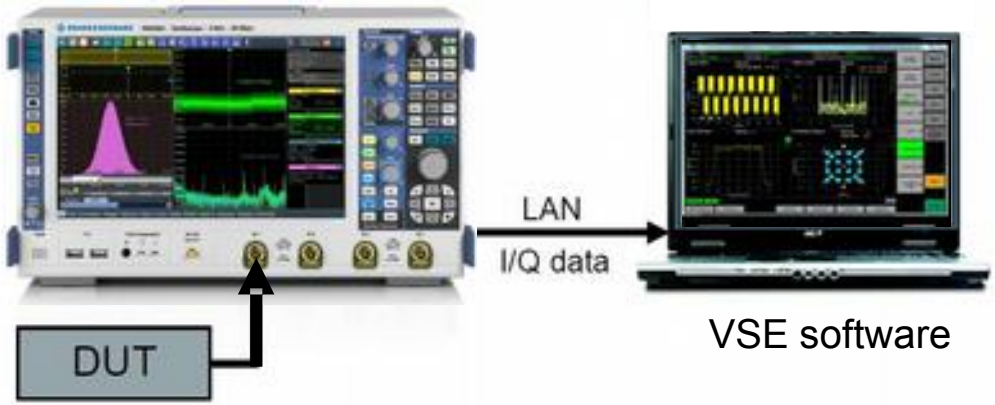


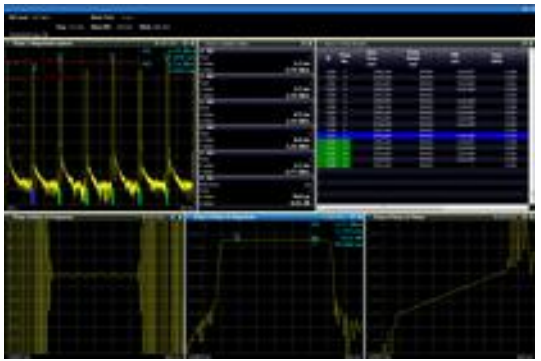
R&S®RTO RF Signal Analysis

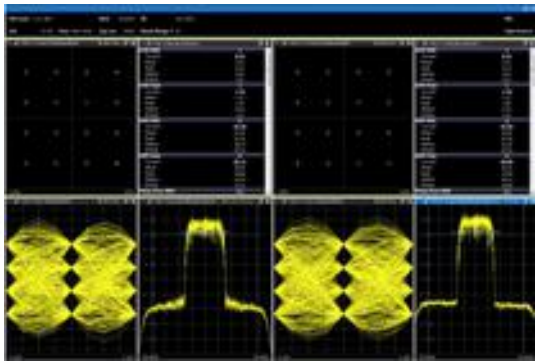
Signal Processing

Vector Signal Explorer SW:

- I/Q Analyzer
- Analog Demodulation
- Vector Signal Analysis (VSA)
- 3G FDD
- GSM
- WLAN
- LTE
- etc.







Measurement Examples

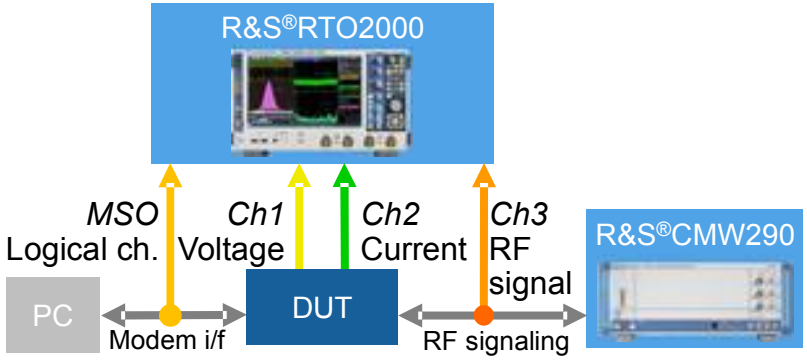
Gemalto 2G Cinterion IoT module Setup

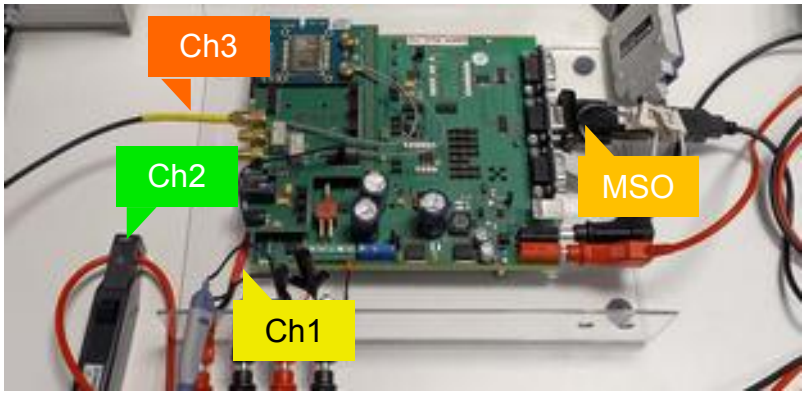
2G Cinterion IoT module from Gemalto

- Quad-Band GSM transceiver and processor
- GPIO / I2C interfaces; Serial modem interface
- Internal flash memory
- Power management unit

Test Equipment

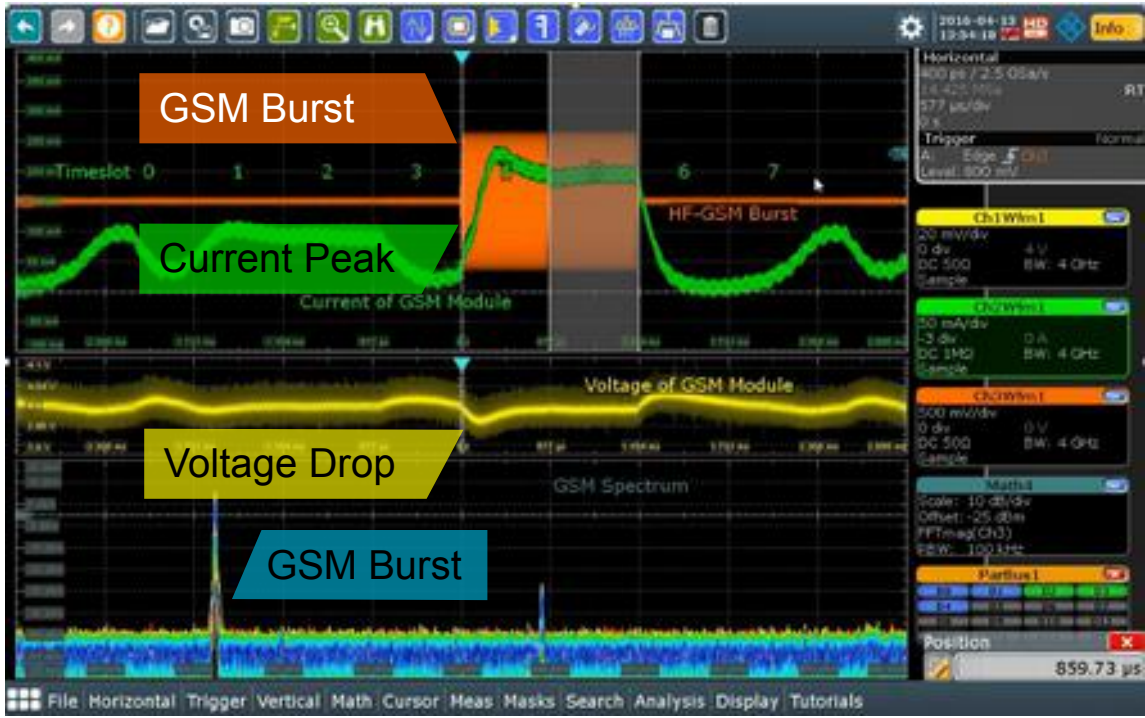
- RTO oscilloscope
  (current, voltage, RF, MSO: UART T&D)
- Communication tester (R&S CMW290)
- Power supply HMP4040
- PC (PuTTY)





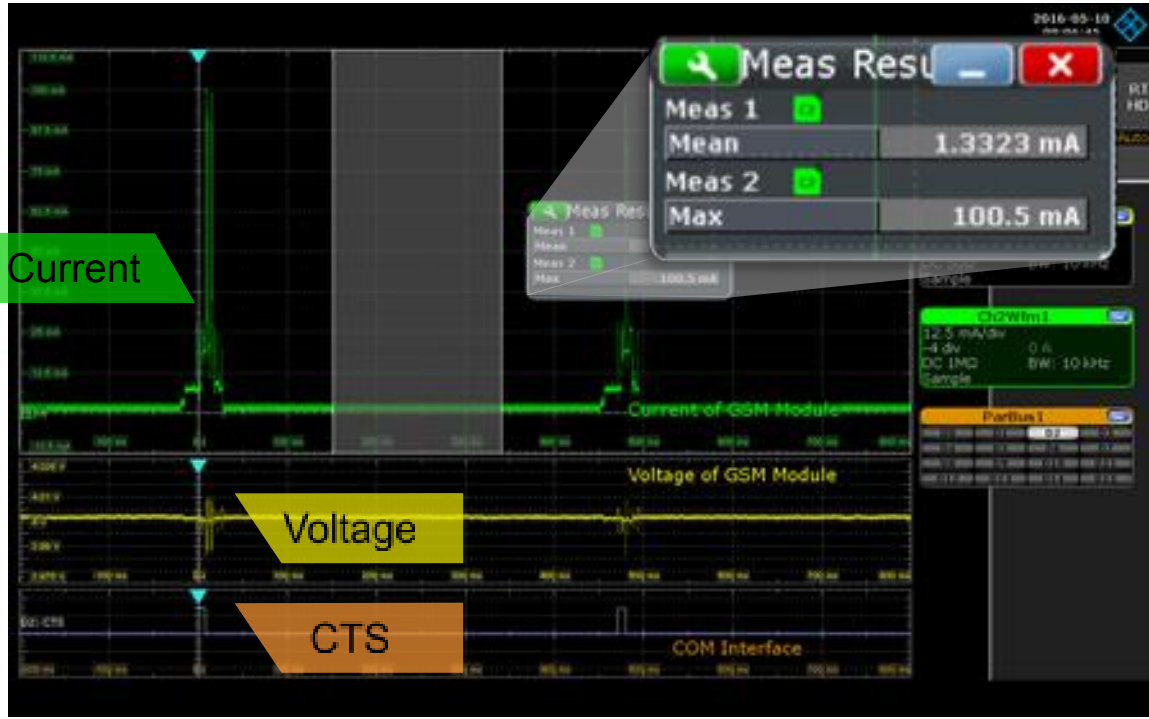
Example 1a: Correlation of Current Consumption with Device Activities

- **Device activity:**
  - GPRS connection in different timeslots
- **R&S RTO2000**
  - Triggers on start of GSM bursts
  - GSM bursts correlate with voltage drops (yellow) and current peaks (green)
  - Display spectrum on gated GSM slot



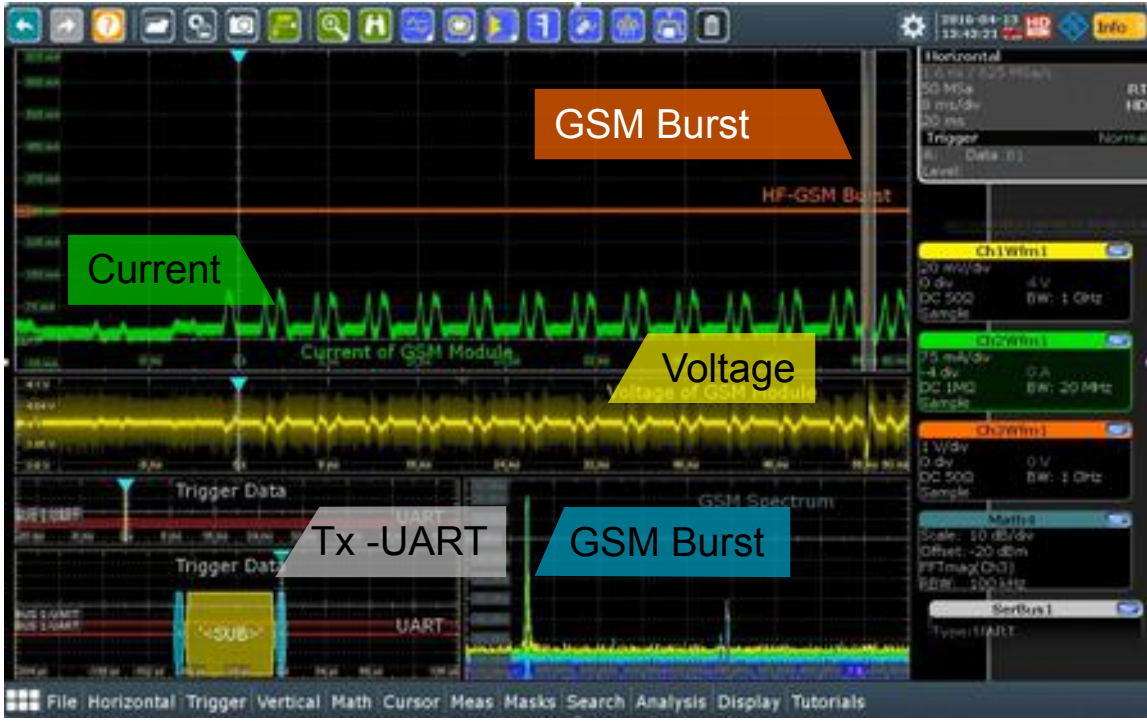
Example 1b: Minimum Current Consumption at Sleep Mode

- **Device activity:**
  - Sleep mode and reacting on paging sequences
- **R&S RTO2000**
  - Trigger on CTS pulse
  - Measures Mean and Max current in sleep interval

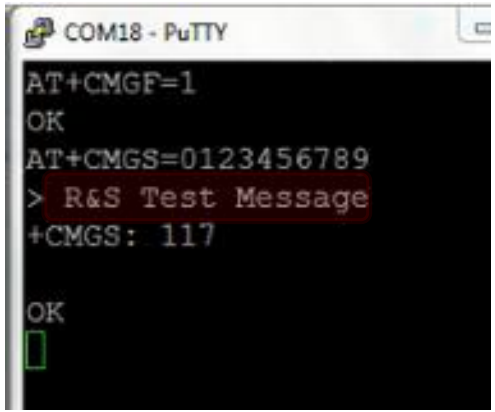


Example 2: Time-correlated Debugging of System Functionality

- **Device activity:**
  - Sent SMS message
- **R&S RTO**
  - Triggers on sending the SMS message at the UART
  - Observe the delay of the GSM burst
  - Correlate GSM burst with current
  - Observe GSM burst in spectrum



Example 2: Time-correlated Debugging of System Functionality (II)



PC

- Writes message (PuTTY)
- Sends message (UART)

R&S RTO Oscilloscope

- Triggers on SMS message sent on UART
- Observe the delay of the GSM burst
- Correlate GSM burst with current
- Observe GSM burst in spectrum

R&S CMW

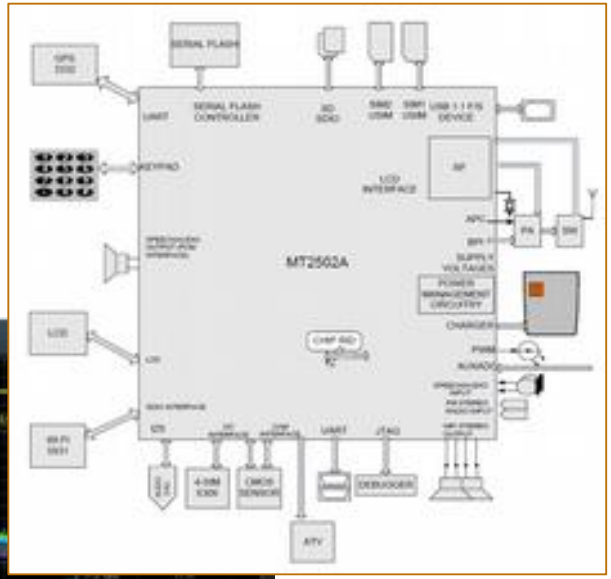
- Receives message,
- Reads message

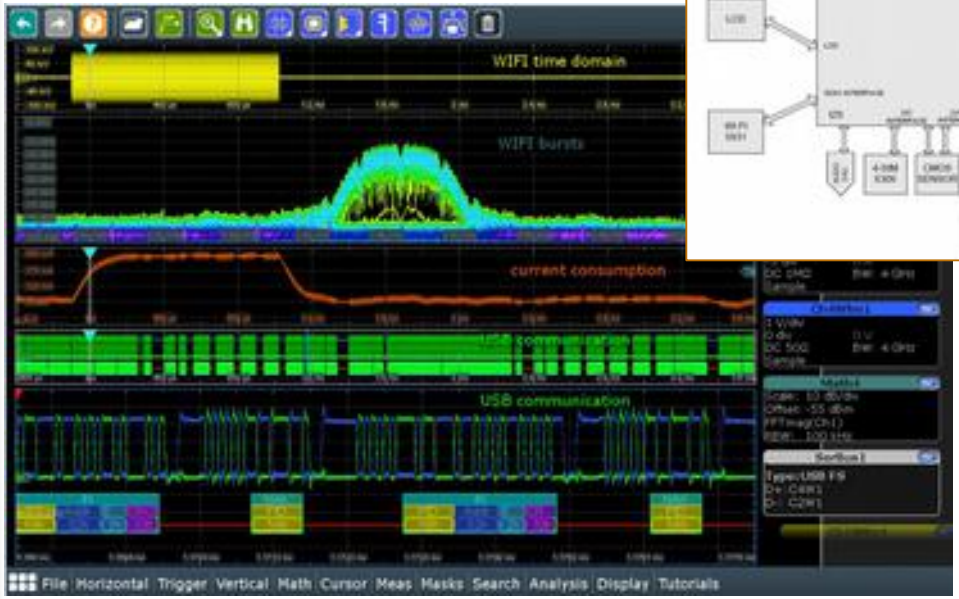
Example 3: Analysis of the Wireless Output Signal

- **Device activity:**
  - Uplink communication of the GSM module
- **R&S RTO2000**
  - Use VSE Analysis SW for GSM signal analysis
    - Synchronization packets, output power, bandwidth, EVM measurements, etc.

Example 4: MediaTek IoT Device: MT2502A

- **Device activity:**
  - WiFi and USB communication
- **R&S RTO**
  - Triggers on WiFi burst related current peak
  - Correlate current / voltage with WiFi and USB traffic





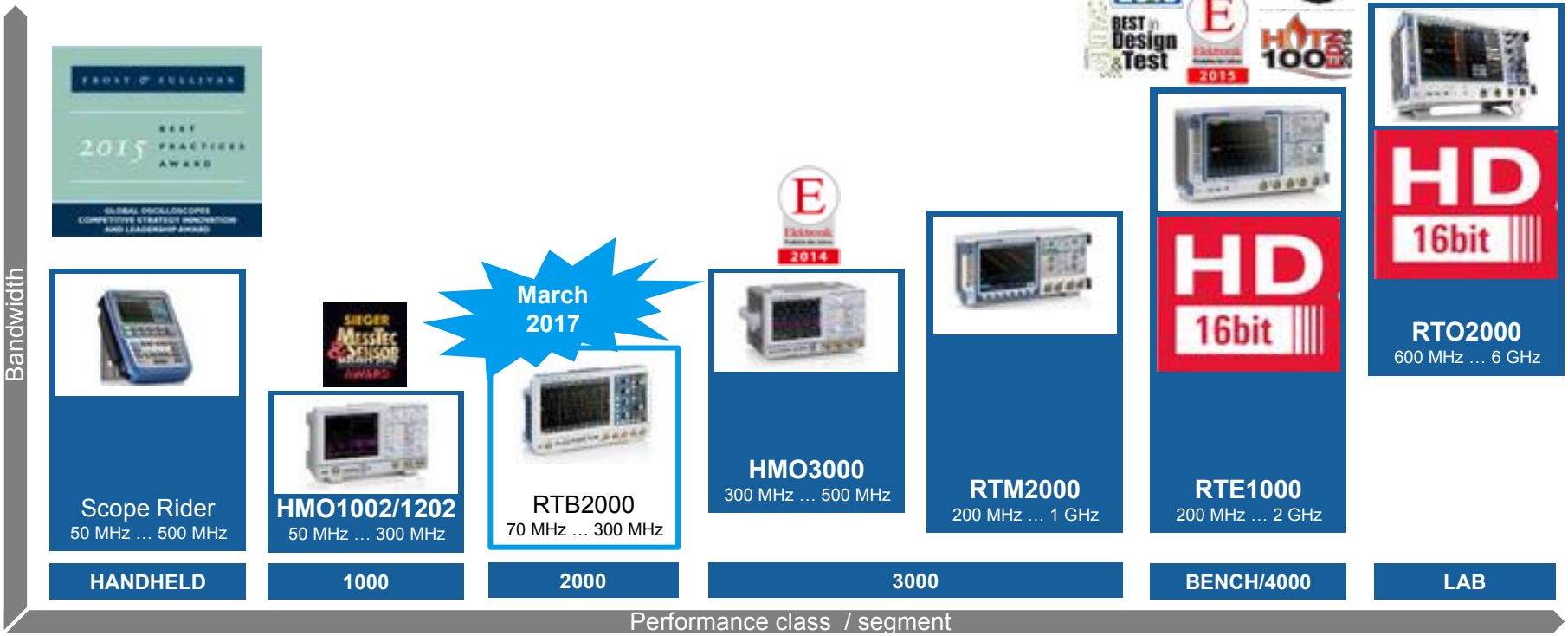
Let‘s sum up

Powerful IoT debug solution

- **R&S®RTO oscilloscope supports:**
  - Time-correlated debugging on system level
    - Analog, logical, protocol and frequency signals
  - Small current measurements
  - Analysis of wireless interfaces
- **Broad R&S T&M portfolio for IoT applications**

The Rohde & Schwarz Oscilloscope Portfolio

50 MHz .. 6 GHz



Thank you.