

# **UMTS**

## **Signaling & Protocol Analysis**

### **(UTRAN & UE)**

#### **Course Duration:**

- ▶ 3 -5 Days.

#### **Note:**

Usually, we perform only parts of this course in a single training class ( $\Leftrightarrow$  3 days). Which parts are actually selected, depends on your requirements. For instance, if you are a UE-supplier, you may not be interested in the signaling procedures and protocols on the lub- and lu-interfaces. Or you are only interested in the analysis of the protocols which are related to the lu-interface. In these cases, the course may be conducted in 3 days. If the full course shall be provided 5 days are required. Irrespective of whether you decide for the short or the long version of the training course, you will always receive the full documentation set.

#### **Course Description:**

- ▶ This unique course focuses on the detailed description and analysis of signaling procedures within the UTRAN.
- ▶ Following a short review of UMTS and UTRA design aspects, the course investigates in full detail the tasks, message structures and parameters of all relevant protocols within the UTRAN (RRC, RLC, MAC, PDCP, NBAP, ALCAP).
- ▶ The major focus of the course is the presentation of all important UMTS-procedures like registration, detachment, call establishment or handover. This part includes the in-depth analysis of particular messages and parameters.
- ▶ Whenever applicable, we use real life examples from various sources to provide a realistic view on UMTS-signaling issues.
- ▶ The course provides in-depth knowledge and reference material about the various signaling procedures within the UTRAN.

As in all INACON courses we integrated several interactive exercises for a perfect learning experience.

## **Pre-Requisites:**

- ▶ The student needs to have *detailed* knowledge about all generic aspects of UMTS like the network architecture, the specifics of W-CDMA and the signal processing chain within UTRAN.
- ▶ It is strongly recommended to take our course “UMTS – Design Details & System Engineering” in advance.
- ▶ Previous knowledge about protocols like SCCP and MTP is favorable.

## **Course Target:**

- ▶ The student is enabled to take, analyze and interpret UMTS recording files on the various interfaces within the UTRAN and on the Uu-interface.
- ▶ The student learns how to use which identifiers to follow single signaling procedures and how to determine possible errors in such signaling procedures.

## **Some of your questions that will be answered:**

- ▶ How can I follow “my” call flow in a recording file? How can I link the various messages of a single call flow to each other?
- ▶ Where in a recording file can I lookup the allocated bearer capabilities or the AMR-coder type?
- ▶ Why do some UMTS protocols like RRC use the Packed Encoding Rules (PER) and how does this impact the protocol analysis?
- ▶ Why are there different types of RNTI's and when is each one used?
- ▶ Which parameters, message types and formatting are used by the various protocols within the UTRAN?
- ▶ How does a Radio Bearer Setup work? Which messages are involved and how is the bearer specified?
- ▶ How is an RRC-connection setup? Which timers are involved?
- ▶ What is the message flow in the various UMTS scenarios?

## **Who should attend this class ?**

- ▶ Everybody who requires detailed knowledge of the UMTS signaling procedures on the Uu- Iub- and Iu- Interfaces.

---

**Table of Contents:**

---

**A Comprehensive Inside View on UMTS**

**The UMTS Network Architecture**

- ⇒ Release 99
  - Access Network (GERAN or UTRAN)
  - Circuit-Switched Core Network
  - Packet-Switched Core Network
- ⇒ The Different Types of RNC's
  - CRNC
  - SRNC
  - DRNC

**The UMTS Protocol Stack with Rel. 99**

- ⇒ Overview
- ⇒ The Circuit-Switched Control Plane
  - Access Stratum Protocols
  - Non Access Stratum Protocols
  - AAL-2 vs. AAL-5
- ⇒ The Circuit-Switched User Plane
- ⇒ The Packet-Switched Control Plane
  - Access Stratum Protocols
  - Non Access Stratum Protocols
- ⇒ The Packet-Switched User Plane
- ⇒ The Broadcast Domain (User Plane only)
- ⇒ Protocol Stack on Iur-Interface
- ⇒ The Transport Network Control Plane

**The Physical Resource on the Uu-Interface (FDD)**

- ⇒ Overview
  - Lower Parts of the Physical Layer
  - Upper Parts of the Physical Layer
- ⇒ Spreading and Modulation in Downlink Direction
- ⇒ Spreading and Modulation in Uplink Direction

**An Overview of Channels in UMTS**

- ⇒ Logical Channels
- ⇒ Transport Channels
- ⇒ Physical Channels

## **Logical-, Transport- and Physical Channels & the QoS**

- ⇒ Example
- ⇒ Applications
- ⇒ Channels
- ⇒ Quality of Service

## **Details of Logical Channels**

- ⇒ Control Channels
- ⇒ Traffic Channels

## **Details of Transport Channels**

- ⇒ Common Transport Channels
- ⇒ Dedicated Transport Channels
- ⇒ Transport Format and Transport Format Set
- ⇒ Semi-Static Part
- ⇒ Dynamic Part
- ⇒ Transport Block and Transport Block Set
- ⇒ Example: Transport Format Set Definition for PCH-TrCH
- ⇒ Example: Transport Format Set Definition for RACH-TrCH

## **CCTrCH and Transport Format Combinations (UE-Side / FDD)**

- ⇒ The CCTrCH
- ⇒ Transport Format Combinations

## **Details of Physical Channels (FDD)**

- ⇒ Dedicated Physical Channels
- ⇒ Common Physical Channels
- ⇒ Layer 1 Signaling in Data Transferring Physical Channels
- ⇒ TPC-Field
- ⇒ Pilot Bits
- ⇒ FBI-Field
- ⇒ TFCI-Field
- ⇒ Example: Slot Format Definition for DPDCH/U and DPCCH/U
- ⇒ Example: Slot Format Definition for DPDCH/D and DPCCH/D
- ⇒ PCPCH-Data and Control (Physical Common Packet Channel)
- ⇒ PRACH-Data and Control (Physical Random Access Channel)
- ⇒ DPDCH/U (Dedicated Physical Data Channel / Uplink)
- ⇒ DPCCH/U (Dedicated Physical Control Channel / Uplink)
- ⇒ PDSCH (Physical Downlink Shared Channel)
- ⇒ S-CCPCH (Secondary Common Control Physical Channel)
- ⇒ DPCCH/D for CPCH (Dedicated Physical Control Channel)
- ⇒ DPDCH/D and DPCCH/D (Downlink DPCH)
- ⇒ PICH (Paging Indicator Channel)

- ⇒ P-CCPCH (Primary Common Control Physical Channel)
- ⇒ S-CPICH (Secondary Common Pilot Channel)
- ⇒ P-CPICH (Primary Common Pilot Channel)
- ⇒ S-SCH (Secondary Synchronization Channel)
- ⇒ P-SCH (Primary Synchronization Channel)
- ⇒ CSICH (CPCH Status Indicator Channel)
- ⇒ CD/CA-ICH (CPCH Collision Detection / Channel Assignment Indicator Channel)
- ⇒ AP-AICH (CPCH Access Preamble Acquisition Indicator Channel)
- ⇒ AICH (Acquisition Indicator Channel)

---

## Signaling & Protocol Analysis in UTRAN

### Medium Access Control (MAC)

- ⇒ Overview: Tasks and Functions

### Mapping of Logical, Transport and Physical Channels (FDD)

- ⇒ Mapping of BCCH and PCCH (UE-Perspective)
- ⇒ Mapping of DCCH and DTCH (UE-Perspective)
- ⇒ Mapping of CCCH (UE-Perspective)
- ⇒ Mapping of CTCH (UE-Perspective)

### MAC-PDU Formats on Logical Channels (FDD / UE-Side)

- ⇒ Format on BCCH, PCCH and CTCH
- ⇒ Format on CCCH
- ⇒ Format on DTCH and DCCH

### The Different RNTI's

- ⇒ C-RNTI
- ⇒ DSCH-RNTI
- ⇒ S-RNTI
- ⇒ D-RNTI
- ⇒ U-RNTI
- ⇒ Example: Allocation of U-RNTI to UE

### The MAC-Architecture

- ⇒ MAC-b
- ⇒ MAC-c / sh
- ⇒ MAC-d

### Traffic Volume Measurements and Radio Bearer Control

### The Random Access Procedure

- ⇒ Initial Conditions

- ⇒ Overview
- ⇒ Access Service Class Selection
  - Transfer of an RRC\_CONN\_REQ-Message
  - Other Cases (MLP)
  - Determination of the Persistence Value P
  - Persistence Value P and Random Number R
- ⇒ PRACH Access Slots and AICH Access Slots
- ⇒ PRACH-Subchannels
- ⇒ Selection of an Appropriate PRACH-Access Slot
- ⇒ Response from the NodeB on AICH / Time Relation
- ⇒ Preambles, Acquisition Indication and Message Part Transfer
- ⇒ RACH / PRACH Configuration in SIB 5 (Part 1)
- ⇒ RACH / PRACH Configuration in SIB 5 (Part 2)

## **Radio Link Control (RLC)**

- ⇒ Operation Modes
  - Transparent Mode (TM)
  - Unacknowledged Mode (UM)
  - Acknowledged Mode (AM)
- ⇒ Tasks and Functions
- ⇒ Configuration of the Size of an RLC-PDU

## **RLC-PDU-Types**

- ⇒ The TMD-PDU
- ⇒ The UMD-PDU
  - Sequence Number (7 bit)
  - E-Bit
  - Length Indicator (7 bit / 15 bit) plus E-Bit
  - Example of an RLC-TMD-PDU
  - Example of an RLC-UMD-PDU
- ⇒ TMD-PDU-Transfer (with segmentation)
- ⇒ TMD-PDU-Transfer (without segmentation)
- ⇒ UMD-PDU-Transfer
- ⇒ The AMD-PDU
  - D/C-Bit
  - Sequence Number (12 bit)
  - P-Bit
  - HE-Field (2 bit)
  - Length Indicator (7 bit / 15 bit) plus E-Bit
  - Example of an RLC-AMD-PDU
- ⇒ The STATUS- and Piggybacked STATUS-PDU (SUFI 1 – 4)
  - NO\_MORE-SUFI
  - WINDOW-SUFI
  - ACK-SUFI

## LIST-SUFI

Example of a STATUS-PDU with SUFI's LIST and ACK

⇒ The STATUS- and Piggybacked STATUS-PDU (SUFI 5 – 8)

## BITMAP-SUFI

## RLIST-SUFI

## MRW-SUFI

## MRW-ACK-SUFI

Example: Operation of the RLIST-SUFI

⇒ The RESET- and RESET-ACK-PDU

## Overflow Protection ⇔ RLC-SDU-Discard

⇒ Timer Based RLC-SDU-Discard

With Signaling

Without Signaling

⇒ Retransmission Based RLC-SDU-Discard

With Signaling

Reset-Procedure

⇒ Transmit Buffer Overflow Based RLC-SDU Discard

## Radio Resource Control (RRC)

⇒ Overview

⇒ Tasks & Functions

## Signaling Radio Bearers

⇒ Signaling Radio Bearer 0 (SRB 0)

⇒ Signaling Radio Bearer 1 (SRB 1)

⇒ Signaling Radio Bearer 2 (SRB 2)

⇒ Signaling Radio Bearer 3 (SRB 3)

⇒ Signaling Radio Bearer 4 (SRB 4)

## The Different RRC-States

⇒ RRC-Idle Mode

UE is unknown in UTRAN

No DCCH's or DTCH's exist

UE monitors PICH / PCH in Downlink (⇔ DRX)

Change to RRC-Connected Mode requires Transmission of RRC\_CONN\_REQ

UE performs Autonomous Cell Reselection but neither Cell Updates nor URA Updates

UE Performs Routing and Location Area Update Procedures

⇒ CELL\_DCH-State

DTCH's exist in Uplink and Downlink Direction

DCCH's are available and can be used; DTCH's may be available

UTRAN knows the Location of the UE on Cell Level

Handover Scenarios are Applicable

- UE performs no Cell Updates or URA Updates
- UE provides Measurement Reports to the RNC
- ⇒ CELL\_FACH-State
  - No DCH's exist in Uplink or Downlink Direction
  - DCCH's are available; DTCH's may be available
  - UE continuously monitors one FACH in Downlink
  - No Soft or Hard Handover Scenarios are applicable
  - UE performs Cell Updates but no URA Updates
  - UTRAN knows the Location of the UE on Cell Level
  - UE provides Measurement Reports to the RNC
- ⇒ CELL\_PCH-State
  - No DCH's exist in Uplink and Downlink Direction
  - DCCH's (and DTCH's) are configured but cannot be used in this State
  - UE monitors PICH / PCH in Downlink (⇔ DRX)
  - Uplink Transmission requires State Change to CELL\_FACH (⇔ Cell Update)
  - No Soft or Hard Handover Scenarios are applicable
  - UE performs Cell Updates but no URA Updates
  - UTRAN knows the Location of the UE on Cell Level
  - UE provides Measurement Reports to the RNC
- ⇒ URA\_PCH-State
  - No DCH's exist in Uplink and Downlink Direction
  - DCCH's (and DTCH's) are configured but cannot be used in this State
  - UE monitors PICH / PCH in Downlink (⇔ DRX)
  - Uplink Transmission requires State Change to CELL\_FACH (⇔ Cell Update)
  - No Handover Scenarios are Applicable
  - UE performs URA Updates
  - UTRAN knows the Location of the UE on URA Level
  - UE provides Measurement Reports to the RNC
- ⇒ RRC State Transitions and Transitions to/from GSM

### **Encoding of RRC-Messages**

- ⇒ ASN.1: Basic Encoding Rules (BER)
  - Nested Information Elements
  - ASN.1 Types
    - The Sequence Type
    - The Choice Type
    - The Enumerated Type
  - Value Assignment
- ⇒ TLV-Encoding
  - The Tag-Field
  - The Length Field
  - Example: Encoding of IMSI
- ⇒ Extension of Tag- and Length-Fields
  - Extension of the Tag-Value (Tag-Values > 30dec)



- Extension of the Length Value (Length Value > 127dec  
Undetermined Length
- ⇒ ASN.1: Packed Encoding Rules (PER) / Unaligned  
Erase Tag and Length Fields  
Minimize the Value Field  
Handling of Optional IE's  
Handling of IE's with Variable Length
- ⇒ Encoding Example: The RRC\_CONN\_REQ-Message

## **RRC-Message Types**

- ⇒ Downlink DCCH-Messages
  - ACT\_SET\_UPD
  - ASSIST\_DATA\_DEL
  - CELL\_CHAN\_UTRAN
  - CELL\_UPD\_CNF
  - COUNT\_CHECK
  - DL\_DIR\_TRANS
  - HO\_UTRAN\_GSM
  - HO\_UTRAN\_CDMA\_2000
  - MEAS\_CTRL
  - PAG\_TYPE2
  - PHYS\_CHAN\_RECONF
  - PHYS\_SHCH\_ALL
  - RB\_RECONF
  - RB\_REL
  - RB\_SETUP
  - RRC\_CONN\_REL
  - SEC\_MODE\_CMD
  - SIG\_CONN\_REL
  - TrCH\_RECONF
  - TFC\_CONTROL
  - UE\_CAP\_ENQ
  - UE\_CAP\_INF\_CNF
  - UL\_PHYS\_CHAN\_CTRL
  - URA\_UPD\_CNF
  - UTRAN\_MOB\_INFO
- ⇒ Uplink DCCH-Messages
  - ACT\_SET\_UPD\_COM
  - ACT\_SET\_UPD\_FAIL
  - CELL\_CHAN\_UTRAN\_FAIL
  - COUNT\_CHECK\_RSP
  - HO\_UTRAN\_COM
  - INIT\_DIR\_TRANS
  - HO\_UTRAN\_FAIL

MEAS\_CTRL\_FAIL  
MEAS\_REP  
PHYS\_CHAN\_RECONF\_COM  
PHYS\_CHAN\_RECONF\_FAIL  
RB\_RECONF\_COM  
RB\_RECONF\_FAIL  
RB\_REL\_COM  
RB\_REL\_FAIL  
RB\_SETUP\_COM  
RB\_SETUP\_FAIL  
RRC\_CONN\_REL\_COM  
RRC\_CONN\_SETUP\_COM  
RRC\_STATUS  
SEC\_MODE\_COM  
SEC\_MODE\_FAIL  
SIG\_CONN\_REL\_IND  
TrCH\_RECONF\_COM  
TrCH\_RECONF\_FAIL  
TFC\_CTRL\_FAIL  
UE\_CAP\_INFO  
UL\_DIR\_TRANS  
UTRAN\_MOB\_INFO\_CNF  
UTRAN\_MOB\_INFO\_FAIL  
⇒ Downlink CCCH-Messages  
CELL\_UPD\_CNF  
RRC\_CONN\_REJ  
RRC\_CONN\_REL  
RRC\_CONN\_SETUP  
URA\_UPD\_CNF  
⇒ Uplink CCCH-Messages  
CELL\_UPD  
RRC\_CONN\_REQ  
URA\_UPD  
⇒ PCCH- (through PCH) and BCCH (through FACH)-Messages  
PAG\_TYPE1  
SYS\_INFO  
SYS\_INFO\_CHANGE\_IND  
⇒ Measurements on the UE-Side  
Example of a MEAS\_CTRL-Message (Part 1)  
Example of a MEAS\_CTRL-Message (Part 2)  
⇒ Important Measurement Parameters  
UTRA Carrier RSSI  
CPICH RSCP  
CPICH Ec/No

Bit Error Rate on TrCH and Physical Channel  
Example: QE in Iub-FP: UL-DATA represents the BER

---

## Important UMTS Scenarios & Call Tracing

### Explanations of the Used Message Descriptors

- ⇒ Message Descriptors on Uu-Interface
- ⇒ Message Descriptors on Iu-CS-, Iu-PS- and Iur-Interface
- ⇒ Message Descriptors on Iub-Interface
  - NBAP-Messages (always over AAL-5)
  - RLC-PDU's (always over AAL-2)
  - ALCAP-Messages (over AAL-5)

### Common Scenarios

- ⇒ NodeB Setup

### Circuit-Switched Scenarios

- ⇒ UE-Registration
  - Initial Conditions
  - Applicability of this Procedure
  - Description
- ⇒ Mobile Originating Conversational Call
  - Initial Conditions
  - Applicability of this Procedure
  - Description
- ⇒ Mobile Terminating Conversational Call
  - Initial Conditions
  - Applicability of this Procedure
  - Description

### Handover Scenarios

- ⇒ Variations of Soft Handover
- ⇒ Softer Handover (Radio Link Addition)
  - Initial Conditions
  - Applicability of this Procedure
  - Description
- ⇒ Softer Handover (Radio Link Removal)
  - Initial Conditions
  - Applicability of this Procedure
  - Description
  - Example: ACT\_SET\_UPD-Message (Link Removal)
- ⇒ Soft Handover (Intra-RNC / Inter-NodeB / Branch Addition)
  - Initial Conditions

- Applicability of this Procedure
- Description
- ⇒ Soft Handover (Inter-RNC / Branch-Addition)
  - Initial Conditions
  - Applicability of this Procedure
  - Description
- ⇒ Hard Handover UTRA-FDD ⇒ GSM
  - Overview
- ⇒ Hard Handover UTRA-FDD ⇒ GSM (Message Flow)
  - Initial Conditions
  - Applicability of this Procedure
  - Description
  - Example: Hard Handover UTRA FDD ⇒ GSM (Message Flow)
- ⇒ Hard Handover GSM ⇒ UTRA-FDD
  - Overview
- ⇒ Hard Handover GSM ⇒ UTRA-FDD (Message Flow)
  - Initial Conditions
  - Applicability of this Procedure
  - Description

## **UTRAN Mobility Management Procedures**

- ⇒ Cell Update (Intra-RNC / Cell Reselection, Periodic, Page Rsp.)
  - Initial Conditions
  - Applicability of this Procedure
  - Description
- ⇒ Cell Update (Inter-RNC / Cell Reselection / UE initiated)
  - Initial Conditions
  - Applicability of this Procedure
  - Description
- ⇒ URA Update (Inter-RNC / Cell Reselection / UE initiated)
  - Initial Conditions
  - Applicability of this Procedure
  - Description

## **Packet-Switched Scenarios**

- ⇒ Attachment
  - Initial Conditions
  - Applicability of this Procedure
  - Description
- ⇒ PDP-Context Activation (Mobile Originating)
  - Initial Conditions
  - Applicability of this Procedure
  - Description

---

**Call Tracing in UTRAN**

- ⇒ Introduction
- ⇒ Related Identifiers

---

**Enclosures for the Practical Exercises**

---

**Solutions for the Practical Exercises**