VOL. 2

GSM

Pocket Guide

Wandel & Goltermann
Communications Test Solutions

Pocket Guide for Fundamentals and GSM Testing

Publisher: Wandel & Goltermann GmbH & Co
Elektronische Meßtechnik
P. O. Box 12 62
D-72795 Eningen u. A.
Germany
e-mail: solutions@wg.com
http://www.wg.com

Author: Marc Kahabka

CONTENTS

1 "Mobility" – The magic word

Hard to fathom, but it really wasn't all that long ago that even a plain old telephone was a luxury item. But, as we all know, technology's only constant is change. In this day and age, many folks need to be accessible everywhere, whether they're at work or play, in the office or at home. To meet this demand, the GSM standard (Global System for Mobile Communications) for mobile telephony was introduced in the mid-1980s. Today, GSM is the most popular mobile radio standard in the world. A boom is underway, such that many GSM users find life without their phone practically inconceivable.

Nowadays, when we speak of GSM, we usually mean "original" GSM – also known as GSM900 since 900 MHz was the original frequency band. To provide additional capacity and enable higher subscriber densities, two other systems were added later: GSM1800 (also DCS1800) and GSM1900 (also PCS 900). Compared to GSM 900, GSM1800 and GSM1900 differ primarily in the air interface. Besides using another frequency band, they use a microcellular structure (i.e. a smaller coverage region for each radio cell). This makes it possible to reuse frequencies at closer distances, enabling an increase in subscriber density. The disadvantage is the higher attenuation of the air interface due to the higher frequency. The rest of this booklet will mainly focus on GSM900.

Where now? A few years ago, Michael Jackson sang ". . . just call my name and I'll be there". While this might seem inconceivable now, it might become reality sooner than we think, given the rapid pace of technological evolution. Faced with a whirlwind of speculation, ETSI

(the telecom standardization authority in Europe) decided to base the air interface of the planned universal mobile telecommunications system (UMTS) on a mix of WCDMA and TD/CDMA technologies. The infrastructure of the existing GSM networks will most likely be used.

This booklet is intended to provide communications engineers & technicians with basic information about the GSM system – a starting point for further study of any given area. A word of warning: Look further if you need complete GSM system specifications. Research sources are listed in the appendix. Also: This booklet assumes you, the reader, have a basic understanding of telecommunications technology.

Enjoy!

Marc Kahabka

2 GSM overview

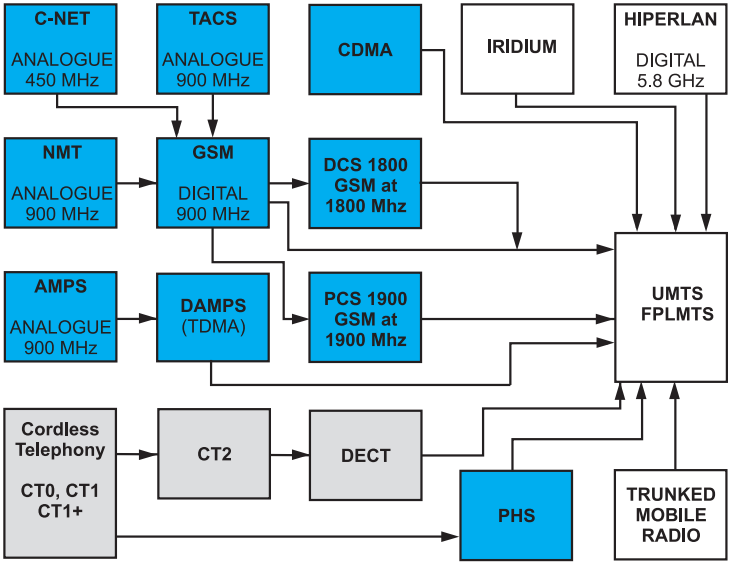

Fig. 1: The Mobile Evolution

Before GSM networks there were public mobile radio networks (cellular). They normally used analog technologies, which varied from country to country and from manufacturer to another. These analog networks

did not comply with any uniform standard. There was no way to use a single mobile phone from one country to another. The speech quality in most networks was not satisfactory.

GSM became popular very quickly because it provided improved speech quality and, through a uniform international standard, made it possible to use a single telephone number and mobile unit around the world. The European Telecommunications Standardization Institute (ETSI) adopted the GSM standard in 1991, and GSM is now used in 135 countries.

The benefits of GSM include:
– Support for international roaming
– Distinction between user and device identification
– Excellent speech quality
– Wide range of services
– Interworking (e.g. with ISDN, DECT)
– Extensive security features

GSM also stands out from other technologies with its wide range of services[1]:
– Telephony
– Asynchronous and synchronous data services (2.4/4.8/9.6 kbit/s)
– Access to packet data network (X.25)
– Telematic services (SMS, fax, videotext, etc.)
– Many value-added features (call forwarding, caller ID, voice mailbox)
– E-mail and Internet connections

[1] Available services vary from operator to operator

3 GSM system architecture

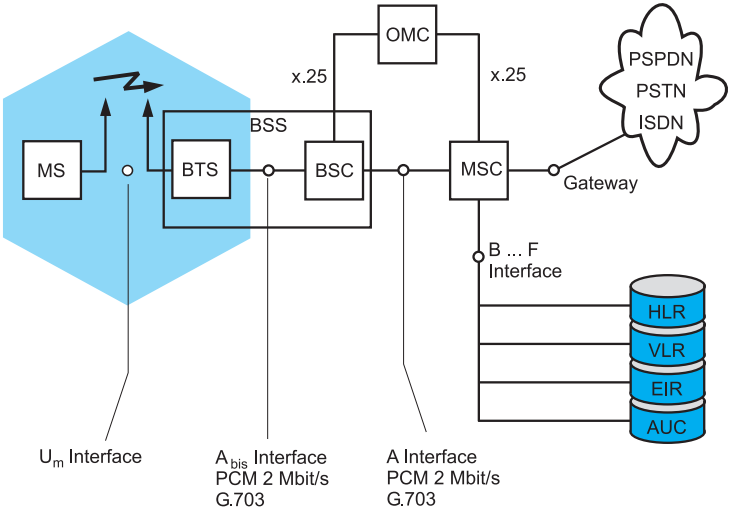

Fig. 2

The best way to create a manageable communications system is to divide it into various subgroups that are interconnected using standardized interfaces. A GSM network can be divided into three groups (see Fig. 2): The mobile station (MS), the base station subsystem (BSS) and the network subsystem.

They are characterized as follows:

The mobile station (MS)

A mobile station may be referred to as a “handset”, a “mobile”, a “portable terminal” or “mobile equipment” ME). It also includes a subscriber identity module (SIM) that is normally removable and comes in two sizes. Each SIM card has a unique identification number called IMSI (international mobile subscriber identity). In addition, each MS is assigned a unique hardware identification called IMEI (international mobile equipment identity).

In some of the newer applications (data communications in particular), an MS can also be a terminal that acts as a GSM interface, e.g. for a laptop computer. In this new application the MS does not look like a normal GSM telephone.

The seemingly low price of a mobile phone can give the (false) impression that the product is not of high quality. Besides providing a transceiver (TRX) for transmission and reception of voice and data, the mobile also performs a number of very demanding tasks such as authentication, handover, encoding and channel encoding.

The base station subsystem (BSS)

The base station subsystem (BSS) is made up of the base station controller (BSC) and the base transceiver station (BTS).
The base transceiver station (BTS): GSM uses a series of radio transmitters called BTSs to connect the mobiles to a cellular network. Their tasks include channel coding/decoding and encryption/decryption. A BTS is comprised of radio transmitters and receivers, antennas, the interface to the PCM facility, etc. The BTS may contain one or more

transceivers to provide the required call handling capacity. A cell site may be omnidirectional or split into typically three directional cells.

- **The base station controller (BSC):** A group of BTSs are connected to a particular BSC which manages the radio resources for them. Today's new and intelligent BTSs have taken over many tasks that were previously handled by the BSCs.
  The primary function of the BSC is call maintenance. The mobile stations normally send a report of their received signal strength to the BSC every 480 ms. With this information the BSC decides to initiate handovers to other cells, change the BTS transmitter power, etc.

The network subsystem

- **The mobile switching center (MSC):** Acts like a standard exchange in a fixed network and additionally provides all the functionality needed to handle a mobile subscriber. The main functions are registration, authentication, location updating, handovers and call routing to a roaming subscriber. The signaling between functional entities (registers) in the network subsystem uses Signaling System 7 (SS7). If the MSC also has a gateway function for communicating with other networks, it is called Gateway MSC (GMSC).
- **The home location register (HLR):** A database used for management of mobile subscribers. It stores the international mobile subscriber identity (IMSI), mobile station ISDN number (MSISDN) and current visitor location register (VLR) address. The main information stored there concerns the location of each mobile station in order to be able to route calls to the mobile subscribers managed by each HLR. The HLR also maintains the services associated with each MS. One HLR can serve several MSCs.

- **The visitor location register (VLR):** Contains the current location of the MS and selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. A VLR is connected to one MSC and is normally integrated into the MSC's hardware.
- **The authentication center (AuC):** A protected database that holds a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and encryption over the radio channel. The AuC provides additional security against fraud. It is normally located close to each HLR within a GSM network.
- **The equipment identity register (EIR):** The EIR is a database that contains a list of all valid mobile station equipment within the network, where each mobile station is identified by its international mobile equipment identity (IMEI). The EIR has three databases:
  – White list: for all known, good IMEIs
  – Black list: for bad or stolen handsets
  – Grey list: for handsets/IMEIs that are uncertain

Operation and Maintenance Center (OMC)

The OMC is a management system that oversees the GSM functional blocks. The OMC assists the network operator in maintaining satisfactory operation of the GSM network. Hardware redundancy and intelligent error detection mechanisms help prevent network down-time. The OMC is responsible for controlling and maintaining the MSC, BSC and BTS. It can be in charge of an entire public land mobile network (PLMN) or just some parts of the PLMN.

4 Interfaces and protocols

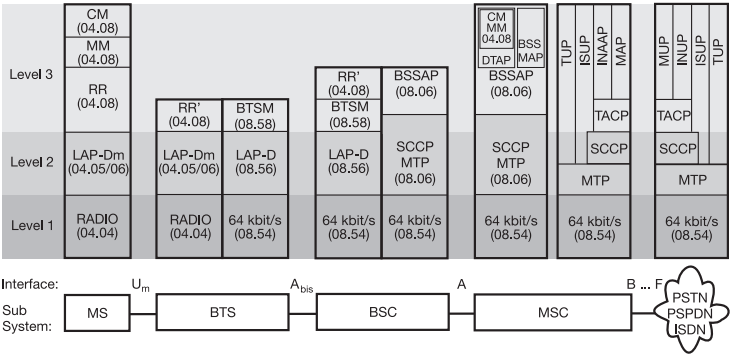

Fig. 3: OSI Layer structure in GSM

Note: Numbers in parentheses indicate the relevant ETSI-GSM Recommendations.

Providing voice or data transmission quality over the radio link is only part of the function of a cellular mobile network. A GSM mobile can seamlessly roam nationally and internationally, requiring standardized call routing and location updating functions in GSM networks. A public communications system also needs solid security mechanisms to prevent misuse by third parties. Security functions such as authentication, encryption and the use of Temporary Mobile Subscriber Identities (TMSIs) are an absolute must.

Within a GSM network, different protocols are needed to enable the flow of data and signaling between different GSM subsystems. Figure 3 shows the interfaces that link the different GSM subsystems and the protocols used to communicate on each interface.

GSM protocols are basically divided into three layers:

- Layer 1: **Physical layer**
  - Enables physical transmission (TDMA, FDMA, etc.)
  - Assessment of channel quality
  - Except on the air interface (GSM Rec. 04.04), PCM 30 or ISDN links are used (GSM Rec. 08.54 on A_{bis} interface and 08.04 on A to F interfaces).
- Layer 2: **Data link layer**
  - Multiplexing of one or more layer 2 connections on control/signaling channels
  - Error detection (based on HDLC)
  - Flow control
  - Transmission quality assurance
  - Routing
- Layer 3: **Network layer**
  - Connection management (air interface)
  - Management of location data
  - Subscriber identification
  - Management of added services (SMS, call forwarding, conference calls, etc.)

5 The air interface U_m

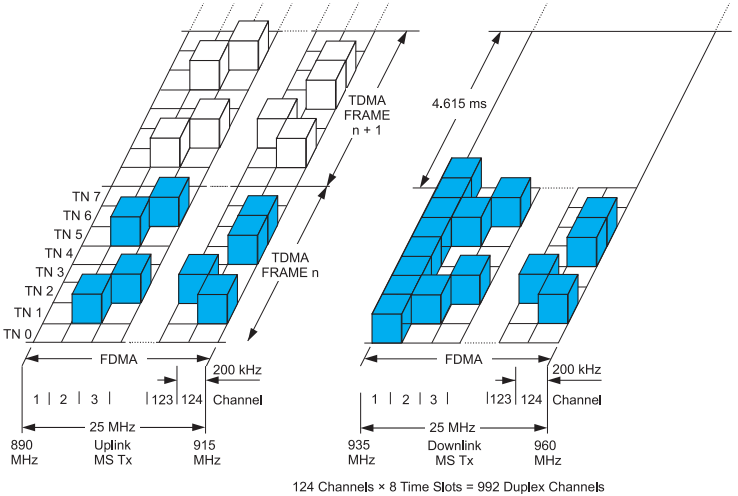

Fig. 4: GSM Air Interface, TDMA frame

The International Telecommunication Union (ITU), which manages international allocation of radio spectrum (among many other functions), has allocated the following bands:

GSM900:

Uplink: 890–915 MHz (= mobile station to base station)

Downlink: 935–960 MHz (= base station to mobile station).

GSM1800 (previously: DCS-1800):
Uplink: 1710–1785 MHz
Downlink: 1805–1880 MHz
GSM1900 (previously: PCS-1900):
Uplink: 1850–1910 MHz
Downlink: 1930–1990 MHz

The air interface for GSM is known as the U_m interface.

Since radio spectrum is a limited resource shared by all users, a method was devised to divide the bandwidth among as many users as possible. The method chosen by GSM is a combination of time- and frequency-division multiple access (TDMA/FDMA). The FDMA part involves the division by frequency of the (maximum) 25 MHz allocated bandwidth into 124 carrier frequencies spaced 200 kHz apart. One or more carrier frequencies are assigned to each base station. Each of these carrier frequencies is then divided in time, using a TDMA scheme. The fundamental unit of time in this TDMA scheme is called a burst period and it lasts approx. 0.577 ms. Eight burst periods are grouped into a TDMA frame (approx. 4.615 ms), which forms the basic unit for the definition of logical channels. One physical channel is one burst period per TDMA frame.

5.1 Logical channels on the air interface

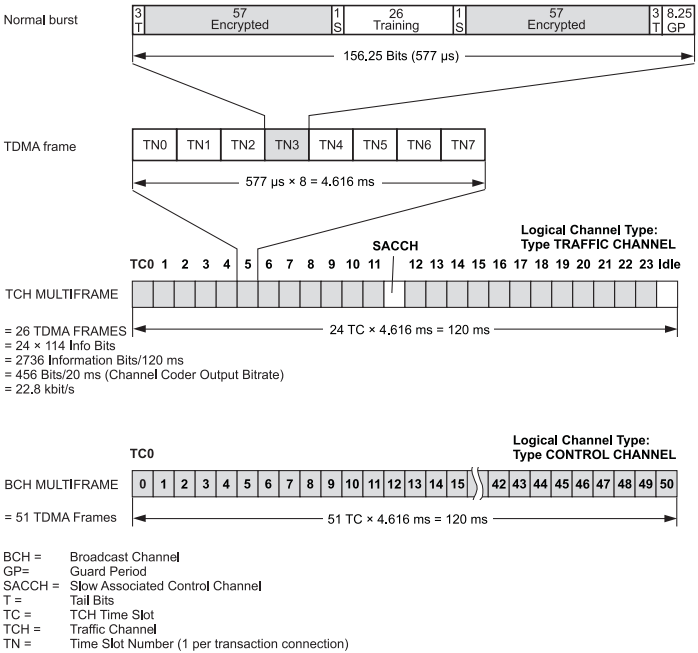

Fig. 5: GSM Air Interface, logical channels

Several logical channels are mapped onto the physical channels. The organization of logical channels depends on the application and the direction of information flow (uplink/downlink or bidirectional). A logical channel can be either a traffic channel (TCH), which carries user data, or a signaling channel (see following chapters).

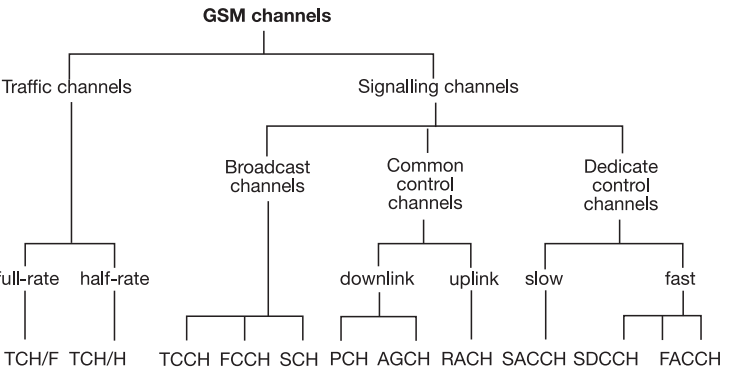

Fig. 6

5.2 Traffic channels on the air interface

A traffic channel (TCH) is used to carry speech and data traffic. Traffic channels are defined using a 26-frame multiframe, or group of 26 TDMA frames. The length of a 26-frame multiframe is 120 ms, which is how the length of a burst period is defined (120 ms divided by 26 frames divided by 8 burst periods per frame). Out of the 26 frames, 24 are used for traffic, 1 is used for the slow associated control channel (SACCH) and 1 is currently unused (see Fig. 5). TCHs for the uplink and downlink are separated in time by 3 burst periods, so that the mobile station does not have to transmit and receive simultaneously, thereby simplifying the electronic circuitry. This method permits complex antenna duplex filters to be avoided and thus helps to cut power consumption.

In addition to these full-rate TCHs (TCH/F, 22.8 kbit/s), half-rate TCHs (TCH/H, 11.4 kbit/s) are also defined. Half-rate TCHs double the capacity of a system effectively by making it possible to transmit two calls in a single channel. If a TCH/F is used for data communications, the usable data rate drops to 9.6 kbit/s (in TCH/H: max. 4.8 kbit/s) due to the enhanced security algorithms. Eighth-rate TCHs are also specified, and are used for signaling. In the GSM Recommendations, they are called stand-alone dedicated control channels (SDCCH).

5.3 Signaling channels on the air interface

The signaling channels on the air interface are used for call establishment, paging, call maintenance, synchronization, etc. There are 3 groups of signaling channels:

- **The broadcast channels (BCH):** Carry only downlink information and are responsible mainly for synchronization and frequency correction. This is the only channel type enabling point-to-multipoint communications in which short messages are simultaneously transmitted to several mobiles.
  The BCHs include the following channels:
  - The broadcast control channel **(BCCH)**: General information, cell-specific; e.g. local area code (LAC), network operator, access parameters, list of neighboring cells, etc. The MS receives signals via the BCCH from many BTSs within the same network and/or different networks.
  - The frequency correction channel **(FCCH)**: Downlink only; correction of MS frequencies; transmission of frequency standard to MS; it is also used for synchronization of an acquisition by providing the boundaries between timeslots and the position of the first timeslot of a TDMA frame.
  - The synchronization channel **(SCH)**: Downlink only; frame synchronization (TDMA frame number) and identification of base station. The valid reception of one SCH burst will provide the MS with all the information needed to synchronize with a BTS.

- **The common control channels (CCCH):** A group of uplink and downlink channels between the MS card and the BTS. These channels are used to convey information from the network to MSs and provide access to the network. The CCCHs include the following channels:
  - The paging channel **(PCH)**: Downlink only; the MS is informed by the BTS for incoming calls via the PCH.
  - The access grant channel **(AGCH)**: Downlink only; BTS allocates a TCH or SDCCH to the MS, thus allowing the MS access to the network.
  - The random access channel **(RACH)**: Uplink only; allows the MS to request an SDCCH in response to a page or due to a call; the MS chooses a random time to send on this channel. This creates a possibility of collisions with transmissions from other MSs.

  The PCH and AGCH are transmitted in one channel called the paging and access grant channel (PAGCH). They are separated by time.

- **The dedicated control channels (DCCH):** Responsible for e.g. roaming, handovers, encryption, etc.
  The DCCHs include the following channels:
  - The stand-alone dedicated control channel **(SDCCH)**: Communications channel between MS and the BTS; signaling during call setup before a traffic channel (TCH) is allocated;
  - The slow associated control channel **(SACCH)**: Transmits continuous measurement reports (e.g. field strengths) in parallel to oper-

ation of a TCH or SDCCH; needed, e.g. for handover decisions; always allocated to a TCH or SDCCH; needed for “non-urgent” procedures, e. g. for radio measurement data, power control (downlink only), timing advance, etc.; always used in parallel to a TCH or SDCCH.

– The fast associated control channel **(FACCH)**: Similar to the SDCCH, but used in parallel to operation of the TCH; if the data rate of the SACCH is insufficient, “borrowing mode” is used: Additional bandwidth is borrowed from the TCH; this happens for messages associated with call establishment authentication of the subscriber, handover decisions, etc.

Almost all of the signaling channels use the “normal burst” format (see section 5.4 Burst formats), except for the RACH (Random Access Burst), FCCH (Frequency Correction Burst) and SCH (SynCHronization Burst) channels.

5.4 Burst formats

A timeslot is a 576 µs time interval, i.e. 156.25 bits duration, and its physical contents are known as a burst. Five different types of bursts exist in the system. They are distinguished by different TDMA frame divisions.

The normal burst (NB): Used to carry information on traffic and control channels, except for RACH. It contains 116 encrypted bits.

The frequency correction burst (FB): Used for frequency synchronization of the mobile. The contents of this burst are used to calculate an

unmodulated, sinusoidal oscillation, onto which the synthesizer of the mobiles is clocked.

The synchronization burst (SB): Used for time synchronization of the mobile. It contains a long training sequence and carries the information of a TDMA frame number.

The access burst (AB): Used for random access and characterized by a longer guard period (256 μs) to allow for burst transmission from a mobile that does not know the correct timing advance at the first access to a network (or after handover).

The dummy burst (DB): Transmitted as a filler in unused timeslots of the carrier; does not carry any information but has the same format as a normal burst (NB).

5.5 Protocols on the air interface

- **Layer 1** (GSM Rec. 04.04): The physical properties of the U_m interface have already been described.
- **Layer 2** (GSM Rec. 04.05/06): Here, the **LAP-Dm** protocol is used (similar to ISDN LAP-D). LAP-Dm has the following functions:
  - Connectionless transfer on point-to-point and point-to-multipoint signaling channels,
  - Setup and take-down of layer 2 connections on point-to-point signaling channels,
  - Connection-oriented transfer with retention of the transmission sequence, error detection and error correction.

- **Layer 3** (GSM Rec. 04.07/08): Contains the following sublayers which control signaling channel functions (BCH, CCCH and DCCH):
  - **Radio resource management (RR):** The role of the RR management layer is to establish and release stable connection between mobile stations (MS) and an MSC for the duration of a call, and to maintain it despite user movements. The following functions are performed by the MSC:
  - Cell selection,
  - Handover,
  - Allocation and take-down of point-to-point channels,
  - Monitoring and forwarding of radio connections,
  - Introduction of encryption,
  - Change in transmission mode.

– **Mobility management (MM)** handles the control functions required for mobility, e.g.:
– Authentication,
– Assignment of TMSI,
– Management of subscriber location.

– **Connection management (CM)** is used to set up, maintain and take down calls connections; it is comprised of three subgroups:
– **Call control (CC):** Manages call connections,
– **Supplementary service support (SS):** Handles special services,
– **Short message service support (SMS):** Transfers brief texts.

Neither the BTS nor the BSC interpret CM and MM messages. They are simply exchanged with the MSC or the MS using the direct transfer application part (DTAP) protocol on the A interface. RR messages are mapped to or from the base station system application part (BSSAP) in the BSCREF for exchange with the MSC.

6 The A_{bis} interface

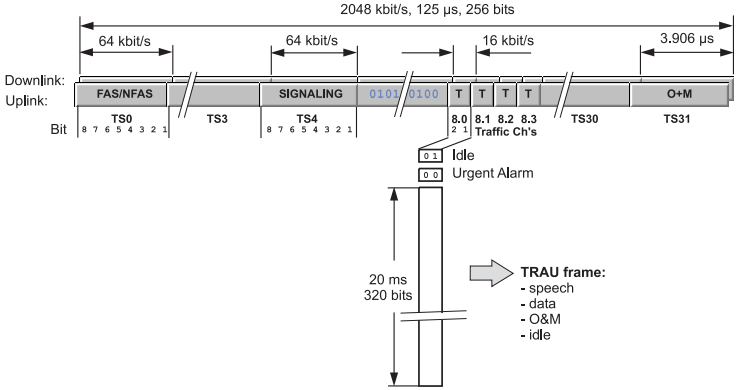

Fig. 7: GSM Abis Interface, PCM timeslot layout

The A_{bis} interface lies within the base station subsystem (BSS) and represents the dividing line between the BSC function and the BTS. The BSC and BTS can be connected using leased lines, radio links or metropolitan area networks (MANs).

Basically, two channel types exist between the BSC and BTS:

– **Traffic channels (TCH):** Can be configured in 8, 16 and 64 kbit/s formats and transport user data,

– **Signaling channels:** Can be configured in 16, 32, 56 and 64 kbit/s formats and are used for signaling purposes between the BTS and BSC.

Each transceiver (TRX) in a BSC generally requires a signaling channel on the A_{bis} interface. The positioning of the user data frames (T = Traffic) and signaling data frames (S = Signaling) varies from manufacturer to manufacturer and from system to system. The only requirement is that the FAS/NFAS frame must be in timeslot 0. A signaling channel can run at either 16 kbit/s (sub-channel signaling) or 64 kbit/s.

6.1 The TRAU frame

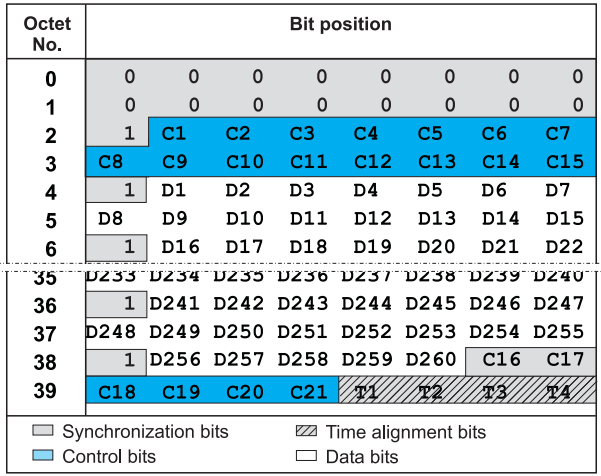

Fig. 8

The TRAU (Transcoder Rate Adapter Unit) frame is the transport unit for a 16 kbit/s traffic channel (TCH) on the A_{bis} interface. It uses 13.6 kbit/s for user data and 2.4 kbit/s for inband signaling, timing and synchronization. It is here that the positions at which the signaling and data bits occur are determined.

The bit names shown in Fig. 8 are interpreted as follows:

(yellow or blue background):	Synchronization bits
C... bits:	Control/signaling bits
T... bits:	Time alignment (TA) bits
D... bits:	User data bits (payload)

The TRAU frame specifications are as follows:

Total bits per frame: 320
Synchronization bits: 25
Control bits: C1 to 15
C17 to 21 (frame dependent and for future applications)

There are four variants for the C, D and T bits, depending on the frame type:

1. Speech frame
   - Data bits: D1 to 260
   - Control bits: C16 to 21
   - TA bits: T1 to 4
2. O&M frame
   - Data bits: D1 to 264
   - Spare bits: S1 to 6
3. Data frame
   - Data bits: D1 to 252
   - First bit of odd octets (5 to 39) is “1”
4. Idle speech frame
   - Like the speech frame, but all data bits are set to “1”

The protocol used on the A_{bis} interface is LAPD, which is adapted from ISDN. LAPD provides the following frame types that can be divided into three groups:

- the unnumbered frames (SABM, DISC, UA, DM, UI),
- the information transfer frame (I)
- the supervisory frames (RR, RNR, REJ, FRMR).

In addition to the radio signaling procedures the A_{bis} interface also provides a means of transport for operation and maintenance procedures for BTSs, as well as a transport mechanism for Layer 2 management procedures inherited directly from ISDN standards.

6.2 Protocols on the A_{bis} interface

The following protocols are used:

- **Layer 1** (GSM Rec. 08.54): 2.048 Mbit/s (ITU-T: E1) or 1.544 Mbit/s (ANSI: T1) PCM facility with 64/32/16 kbit/s signaling channels and 16 kbit/s traffic channels (4 per timeslot)
- **Layer 2** (GSM Rec. 08.56): Here, the **LAP-D** protocol is used as the transport mechanism for data messaging between the BTS and BSC. Within GSM the SAPI refers to the link identifier transmitted in the LAPD protocol that was inherited from ISDN.
- **Layer 3** (GSM Rec. 08.58/04.08): BTS management (BTSM) works mainly in this layer. BTSM distinguishes three logical signaling connections with the SAPI (Service Access Point Identifier). SAPI 0 is used by all messages coming from or going to the radio interface. SAPI 62 provides 0&M message transport between the BTS and BSC. SAPI 63 is used for dynamic management of TEIs as well as for

layer 2 management functions. The addition of another field to the LAPD link layer address is for the TEIs. The TEIs that provide addressing of the TRXs (transmitters and receivers) for the BTS are as follows:

1. **Radio signaling link (RSL):** Traffic management; used for signaling between the BSC and BTS (non-transparent messages, e.g. RR) and transmission of signaling information on the air interface in the form of transparent messages (CM and MM messages)
2. **Operating & maintenance link (OML):** Network management; used to monitor the operating status of the TRXs or BTS; OML messages have priority over other layer 2 messages.
3. **Layer 2 management link (L2ML):** Layer 2 management; controls the TEI management and addressing procedures (allocation, de-allocation of BTS internal transceiver [TRX] addresses)

7 The A interface

The A interface lies between the BSC and MSC. If the BSC contains the transcoder equipment (TCE), a traffic channel (TCH) occupies a complete 64 kbit/s timeslot in the 2 Mbit/s or 1.544 Mbit/s PCM link (layer 1, GSM Rec. 08.04). Out of 32 available timeslots on the PCM link, a maximum of 30 traffic channels can be operated simultaneously, since at least 2 timeslots are needed for control and signaling purposes (TS0 for FAS/NFAS and another TS for signaling, usually TS16) on PCM facilities. One signaling channel supports many 64 kbit/s PCM facilities between one BSC and the MSC. Normally two active 64 kbit/s timeslots are used for this purpose.

If the MSC is equipped with a TCE, the TCHs are converted from 64 kbit/s to 16 kbit/s in the transcoder equipment. If the BCS does not contain a TCE, then the TCHs are 16 kbit/s on the A interface. Between the BSC and MSC, the TCHs are “recorded” from 64 kbit/s to 16 kbit/s in the transcoder equipment (TCE).

7.1 Protocols on the A interface

The signaling protocol (layer 2+3) between the BSC and MSC is based on the SS7 standard, but is transmitted along with the user data within the PCM facility. Normally timeslot 16 (TS16) of the 64 kbit/s frame is used.
The following protocols are employed:

- **Layer 1** (GSM Rec. 08.04): 2.048 Mbit/s (ITU-T: E1) or 1.544 Mbit/s (ANSI: T1) PCM link.
- **Layer 2** (GSM Rec. 08.06): Here, SS7-based protocols are used for layer 2; the message transfer part **(MTP)** protocol (responsible for

transmission security between the BCS and MSC) and the signaling connection control part **(SCCP)** protocol (allows global addressing of network elements and thus offers a service corresponding to the exchange layer). MTP and SCCP also perform layer 3 functions. SCCP is used to transport DTAP and base station management application part (BSSMAP) messages on the A interface, ensuring both conectionless and connection-oriented message flows. The connections can be related to a specific MS or radio channel.
An SCCP connection can be initiated by a mobile station (MS) or an MSC.
An SCCP connection can involve the following protocols:

- From the MS:
  - MM: CM service request
  - RR: Paging response
  - MM: Location updating request
  - MM: CM re-establishment request.
- From the MSC: Initiation of an “external handover” (BSSMAP: handover request).

The MSC always manages an SCCP connection.

- **Layer 3** (GSM Rec. 08.08): Contains the base station system application part **(BSSAP)** protocol. This layer has multiple parts on the MSC end:
  - The base station management application part **(BSSMAP)** protocol is the counterpart to the RR protocol on the air interface.
  - The direct transfer application part **(DTAP)** protocol transmits **CC** and **MM** messages and is transmitted transparently through the BTS and BSC.

8 MSC-based interfaces

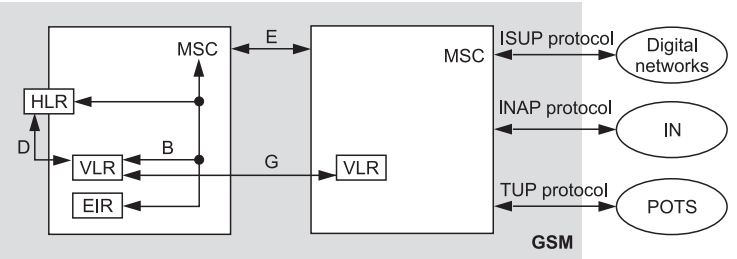

Fig. 9

All of the interfaces around the MSC use SS7-based protocols. The B, C, D, F and G interfaces are referred to as MAP interfaces. These connect either the MSC to registers or registers to other registers. The E interface supports the MAP protocol and calls setup protocols (ISUP/TUP). This interface connects one MSC to another MSC within the same network or to another network's MSC. They are designated as follows (protocols are explained in section 8.1 MSC protocols):

- B interface: between MSC and VLR (use MAP/TCAP protocols)
- C interface: between MSC and HLR (MAP/TCAP)
- D interface: between HLR and VLR (MAP/TCAP)
- E interface: between two MSCs (MAP/TCAP + ISUP/TUP)
- F interface: between MSC and EIR (MAP/TCAP)
- G interface: between VLRs (MAP/TCAP).

Fixed network interfaces:

- via TUP protocol: between MSC and analog/digital networks
- via ISUP protocol: between MSC and analog/digital networks; provides more features than TUP
- via INAP protocol: between MSC and IN.

The SCCP protocol provides connectionless message transport to and from the GSM network databases for TCAP and MAP messaging. Here, two connection types are also distinguished:

- **Circuit-related call control:** Related to ISUP and TUP
- **Non circuit-related call control:** The mobile application part (MAP) protocol is used here, allowing implementation of functions such as location updating/roaming, SMS delivery, handover, authentication and incoming call routing information. The MAP protocol uses the transaction capability application part (TCAP) protocol to transfer real-time information (between MSCs, HLRs and VLRs).

8.1 MSC protocols

MAP (Mobile Application Part): (GSM Rec. 09.02) Used to control queries to the different databases in the mobile radio network (HLR, VLR and EIR). MAP responsibilities include access and location management (e.g. where is the called subscriber currently?), MSC-MSC handover, security functions, O&M, SMS and supplementary services.

TCAP (Transaction Capabilities Application Part): Provides universal calls and functions for handling requests to distributed application processes.

ISUP (ISDN User Part): Controls interworking (e.g. call setup/take-down) between PLMNs and other networks, and provides the same basic functionalities as TUP.

INAP (Intelligent Network Application Part): Implements intelligent supplementary services (e.g. free call, time-dependent routing functions in a central service center).

TUP (Telephone User Part): Implements interworking between PLMNs and other networks. TUP is normally used to provide international connections and is slowly being replaced by ISUP.

9 Call setup

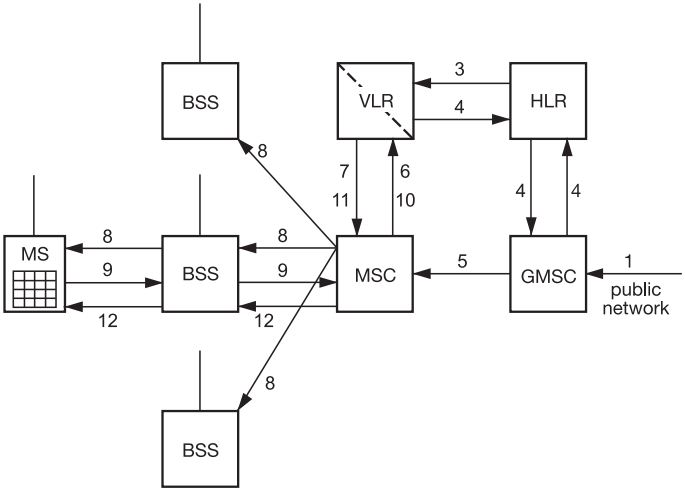

Fig. 10

(To help understand the complexity of a simple phone call, the processes that are necessary in a GSM network to complete a connection to a mobile telephone).

The following example describes a call from a fixed network subscriber to a mobile subscriber in a GSM network:

The incoming call is passed from the fixed network to the gateway MSC (GMSC) (1). Then, based on the IMSI numbers of the called party, its HLR is determined (2). The HLR checks for the existence of the called number. Then the relevant VLR is requested to provide a mobile station roaming number (MSRN) (3). This is transmitted back to the GMSC (4). Then the connection is switched through to the responsible MSC (5). Now the VLR is queried for the location range and reachability status of the mobile subscriber (6). If the MS is marked reachable, a radio call is enabled (7) and executed in all radio zones assigned to the VLR (8). When the mobile subscriber telephone responds to the page request from the current radio cell (9), all necessary security procedures are executed (10). If this is successful, the VLR indicates to the MSC (11) that the call can be completed (12).

10 Test and measurement problems in GSM

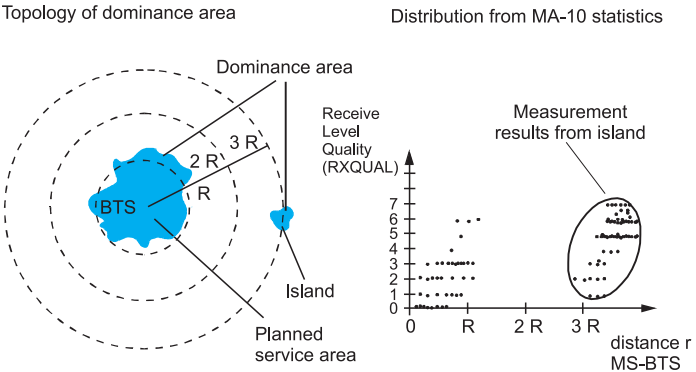

Fig. 11

As you can see from the previous sections, GSM technology is very complex. Naturally, such a technology is a challenge to install, commission, manage and optimize. The following section will consider some sample network problems[1].

[1] For more information on GSM test applications, see the WG Application Notes (available upon request)

Due to the limited nature of resources (not to mention their high cost), network optimization is becoming a more and more critical economic factor. To get a handle on network performance, network utilization, subscriber behavior and quality of service (QoS), the following test methods are useful:

Traffic analysis: Here, the contents of signaling channels in an E1 or T1 PCM frame are monitored and analyzed on the A_{bis} and A interfaces of the GSM network. It does not matter what type traffic the various timeslots transport (speech, data or signaling) since all contribute equally to traffic loading.

Bit error ratio test (BERT): A BERT involves bit error measurement at the PCM level and the GSM-specific level (TRAU frame – TRAU: Transcoder and Rate Adapter Unit). The PCM bit error ratio (BER) is of interest to GSM operators who need to verify the quality of leased lines from fixed network operators.
At the GSM level, by evaluating the control bits in the TRAU, a bit error probability can be determined (uplink) during actual communications (in-service). More accurate BER measurement requires out-of-service simulation in which the 260 data bits in the TRAU frame are checked using a pseudo-random bit sequence (PRBS).

Alarm monitoring: This test type checks all PCM links for layer 1 alarms, including:

- No signal,
- Alarm indication signal (AIS),
- No synchronization,
- Remote alarm,
- CRC alarm.

Network quality test: Includes a number of diverse measurements that work together to provide an indication of network quality and reveal potential areas for improvement. This includes:

- Island problems (see Fig. 11),
- Detection of coverage holes,
- Interference,
- Network load regarding signaling and traffic,
- Handover failures,
- Receive level (RXLEV) surveillance,
- Bit error ratio of a BTS (RXQUAL),
- Multipath interference and propagation delays,
- Frequency interference (due to frequency reuse),
- Call completion/disconnect rate,
- System overload.

Optimally qualifying a GSM network requires extensive protocol analysis in the A_{bis} **and** SS7-based interfaces. This is due to the intersection of the GSM and SS7 protocol worlds, as described in section 8.1 “MSC protocols”.

System features

This section provides a brief description of the GSM network features.

Roaming:

The roaming feature allows a user to make and receive calls in any GSM network and to use the same user-specific services worldwide[1]. This requires a roaming agreement between the individual operators. With worldwide roaming the MS is accessible under the same phone number everywhere.

Handover:

In a cellular network, the radio and fixed voice connections are not permanently allocated for the duration of a call. Handover, or handoff as it is called in North America, means switching an ongoing call to a different channel or cell. The execution and measurements required for handover are a basic function of the RR protocol layer.

There are **four different types of handovers** in GSM, which involve transferring a connection between:

- Channels (timeslots) in the same cell (intra-BTS handover)
- Cells under the control of the same BSC (inter-BTS handover).
- Cells under the control of different BSCs, but belonging to the same MSC (inter-BSC handover)
- Cells under the control of different MSCs (inter-MSC handover)

[1] Identical carrier frequencies (900/1800/1900) are required, therefore, or the telephone needs to support the desired frequency. Dual-band mobiles that support several frequency bands are becoming increasingly popular in this connection.

The first two types of handover involve only one base station controller (BSC). To save signaling bandwidth, they are managed by the BSC without involving the MSC, except to notify it upon completion of the handover. The last two types of handover are handled by the MSCs involved. An important aspect of GSM is that the original MSC, the anchor MSC, remains responsible for most call-related functions, with the exception of subsequent inter-BSC handovers under the control of the new MSC, called the relay MSC.

Handovers can be initiated by either the BSC or the MSC (as a means of traffic load balancing). During its idle timeslots, the mobile scans the broadcast control channel of up to 16 neighboring cells, and forms a list of the six best candidates for possible handover, based on the received signal strength. This information is passed to the BSC and MSC, at least once per second, and is used by the handover algorithm.

The decision on when to initiate a handover is a function of the following parameters:

– receive quality,
– receive level.

Successful handovers in GSM can take place at propagation speeds of up to 250 km/h.

Multipath equalization: At the 900 MHz range, radio waves bounce off everything – buildings, hills, cars, airplanes, etc. Many reflected signals, each with a different

phase, can reach an antenna (also known as “multipath propagation”). Equalization is used to extract the desired signal from the unwanted reflections. It works by finding out how a known transmitted signal is modified by multipath fading, and constructing an inverse filter to extract the rest of the desired signal. This known signal is the 26-bit training sequence transmitted in the middle of every time-slot burst. The actual implementation of the equalizer is not specified in the GSM specifications.

Frequency hopping: The mobile station has to be frequency-agile, meaning it can move between different frequencies in order to transmit and receive data, etc. A normal handset is able to switch frequencies 217 times per second. GSM makes use of this frequency agility to implement slow frequency hopping, where the mobile and the BTS transmit each TDMA frame on a different carrier frequency. The frequency hopping algorithm is broadcast on the broadcast control channel. Since multipath fading is dependent on the carrier frequency, slow frequency hopping helps alleviate the problem. In addition, co-channel interference is in effect randomized. The broadcast and common control channels are not subject to frequency hopping and are always transmitted on the same frequency.

Discontinuous transmission (DTX): To reduce the MS’s power consumption and minimize interference on the air interface, user signal transmission is interrupted during pauses in speech. “Comfort noise” is artificially generated by the MS to avoid disruption due to an abrupt interruption in speech.

Discontinuous reception (DRX):

Another method used to conserve power at the mobile station is discontinuous reception. The paging channel, used by the base station to signal an incoming call, is structured into sub-channels. Each mobile station needs to listen only to its own sub-channel. In the time between successive paging sub-channels, the mobile can go into sleep mode, when almost no power is used.

Power control:

Several classes of mobile stations are defined in the GSM specifications, according to their peak transmitter power. To minimize co-channel interference and to conserve power, both the mobiles and the base transceiver stations operate at the lowest power level that will maintain an acceptable signal quality. Power levels can be stepped up or down in steps of 2 dBm from the peak power for the class down to a minimum of 13 dBm (20 milliwatts for MS).

The mobile station and BTS continually measure the signal strength or signal quality (based on the bit error ratio), and pass the information to the base station controller, which ultimately decides if and when the power level should be changed.

Short Message Service (SMS)

SMS offers message delivery (similar to “two-way-paging”) that is guaranteed to reach the MS. If the GSM telephone is not turned on, the message is held for later delivery. Each time a message is delivered to an MS, the network expects to receive an acknowledgement from this MS that the message was correctly received. Without a posi-

tive acknowledgement the network will re-send the message or store it for later delivery. SMS supports messages up to 160 characters in length that can be delivered by any GSM network around the world wherever the MS is able to roam.

Call Waiting (CW)

CW is a network-based feature that must also be supported by the GSM telephone (MS). With CW, GSM users with a call in progress will receive an audible beep to alert them that there is an incoming call for the MS. The incoming call can be accepted, sent to voice mail or rejected. If the incoming call is rejected, the caller will receive a busy signal. Once the call is accepted, the original call is put on hold to allow a connection to the new incoming call.

Call Hold (CH)

CH must be supported by the MS and the network. It allows the MS to "park" an "in progress call", to make additional calls or to receive incoming calls.

Call Forwarding (CF)

This is a network-based feature that can be activated by the MS. CF allows calls to be sent to other numbers under conditions defined by the user. These conditions can be either unconditional or dependent on certain criteria (no answer, busy, not reachable).

Calling Line ID

Calling Line ID must be supported by the GSM network and the telephone. The GSM telephone displays the originating telephone number of incoming calls. This feature requires the caller's network to deliver the calling line ID (telephone no.) to the GSM network.

Mobility Management (MM)

The GSM network keeps track of which mobile telephones are powered on and active in the network. To provide as efficient call delivery as possible, the network keeps track of the last known location of the MS in the VLR and HLR. Radio sites connected to the MSC are divided into groups called “location areas”. When a call is designated for an MS, the network looks for the MS in the last known location area.

Authentication

Authentication normally takes place when the MS is turned on with each incoming call and outgoing call. A verification that the »Ki« (security code) stored in the AuC matches the »Ki« stored in SIM card of the MS completes this process.
The user must key in a PIN code on the handset in order to activate the hardware before this automatic procedure can start.

11 Outlook

In early 1998, the ETSI standardization committee made up its mind on the future, third-generation mobile radio standard, known as the universal mobile telecommunications system (UMTS). UMTS should support all forms of mobile, satellite-based and fixed-network-based telecommunications. The user should be able to use all services (voice, data, multimedia, etc.) in each of the stated areas.

ETSI agreed to use a combination of wideband code division multiple access (W-CDMA) and time division multiple access (TD/CDMA) on the air interface. W-CDMA will be used to cover larger areas and TD/CDMA for local (indoor) applications. CDMA technology holds the promise of a higher channel capacity and lower power consumption with GSM-like speech quality. Costly frequency planning like that required in GSM networks is unnecessary in CDMA networks.

Now that Europe has made its choice, work is underway towards worldwide acceptance of the UMTS standard. There is still no agreement on the network architecture, but network operators naturally hope to reuse existing GSM networks to save money.

Besides straightforward telephony, data communication is also important in UMTS. Here, the catch phrase is “mobile multimedia”: It should be possible in the future to operate data-intensive applications such as video conferencing via a mobile unit.

12 GSM glossary

AB	Access Burst
AGCH	Access Grant CHannel
AIS	Alarm Indication Signal
AMPS	Advanced Mobile Telephone Service
AuC	Authentication Center
BCCH	Broadcast Control CHannel
BCH	Broadcast CHannels
BER	Bit Error Rate
BERT	Bit Error Rate Test
BSC	Base Station Controller
BSSAP	Base Station System Application Part
BSSMAP	Base Station Management Application Part
BTS	Base Transceiver Station
BTSM	BTS Management
CC	Call Control
CCCH	Common Control CHannels
CDMA	Code Division Multiple Access
CM	Connection Management
CRC	Cyclic Redundancy Check
CT0/1/2	(Standards for) Cordless Telephony 0/1/2
D-AMPS	Dual Mode AMPS
DB	Dummy Burst
DCCH	Dedicated Control CHannels
DCS 1800	Digital Cellular System 1800 (today: GSM1800)
DECT	Digital Enhanced Telecommunications System
DRX	Discontinuous reception

DTAP	Direct Transfer Application Part
DTX	Discontinuous Transmission
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FACCH	Fast Associated Control CHannel
FAS	Frame Alignment Signal
FB	Frequency correction Burst
FCCH	Frequency Correction CHannel
FDMA	Frequency Division Multiple Access
GMSC	Gateway MSC
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HDLC	High Level Data Link Control
HLR	Home Location Register
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
INAP	Intelligent Network Application Part
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
L2ML	Layer 2 Management Link
LAP-D	Link Access Protocol for the (ISDN) D-Channel
LAP-Dm	LAP-D for the GSM U_m Interface
MAN	Metropolitan Area Network
MAP	Mobile Application Part
ME	Mobile Equipment

MM	Mobility Management
MS	Mobile Station
MSC	Mobile Switching Center
MSISDN	MS ISDN number
MSRN	Mobile Station Roaming Number
MTP	Message Transfer Part
NB	Normal Burst
NFAS	Non-FAS
NMT	Nordic Mobile Telephone Network
O&M	Operations and Maintenance
OMC	Operation and Maintenance Center
OML	Operating & Maintenance Link
PCH	Paging CHannel
PCM	Pulse Code Modulation
PCS1900	Personal Communications System 1900 (today: GSM1900)
PHS	Personal Handyphone System
PLMN	Public Land Mobile Network
PRBS	Pseudo Random Bit Sequence
QoS	Quality of Service
RACH	Random Access CHannel
RR	Radio Resource management
RSL	Radio Signaling Link
RXLEV	Received Signal Level
RXQUAL	Received Signal Quality
SACCH	Slow Associated Control CHannel
SB	Synchronization Burst

SCCP	Signaling Connection Control Part
SCH	Synchronization CHannel
SDCCH	Stand-alone Dedicated Control CHannel
SIM	Subscriber Identity Module
SMS	Short Message Service
SMS	Short Message Service Support
SS	Supplementary Service Support
SS7	Signaling System Number 7
TA	Time Alignment
TACS	Total Access Communication System
TCAP	Transaction Capabilities Application Part
TCH	Traffic CHannel
TD/CDMA	Time Division Code Division Multiple Access
TDMA	Time Division Multiple Access
TMSI	Temporary Mobile Subscriber Identity
TRAU	Transcoding and Rate Adaptation Unit
TRX	Transceiver
TS	Timeslot
TUP	Telephone User Part
U_m	Air interface in GSM
UMTS	Universal Mobile Telecommunications System
VLR	Visitor Location Register
WCDMA	Wideband Code Division Multiple Access

13 Bibliography

1. GSM-Technik und Messpraxis [GSM technology and practical testing – in German] – Redl/Weber, Franzis', Poing
2. Microcells in mobile communications – Tibor Rakó, Gyõzõ Drozdy; **http://www.pgsm.hu/english/gsm/more.html**
3. Overview of the Global System for Mobile Communications – John Scourias; University of Waterloo; **http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html**
4. Mobilkommmunikation, Hochschulkolleg [Mobile communications, High-school textbook – in German] – Ulrich Bochtler, Walter Buck, Eberhard Herter; Steinbeis-Transferzentrum, Kommunikationszentrum Esslingen
5. The Global System for Mobile Communications – Michel Mouly, Marie-Bernadette Paulet; Palaiseau, France
6. Vermittlungstechnik und Schnittstellen [Switching technology and interfaces – in German] – Ulrich Bochtler; Steinbeis-Transferzentrum, Kommunikationszentrum Esslingen

Want to know more about WG and GSM?

Please visit our GSM webpage at **http://www.gsm.wg.com** or contact your local Wandel & Goltermann sales office.

Please ask for:

Vol. 1
SDH
Pocket Guide
Fundamentals
and SDH Testing

Vol. 3
SONET
Pocket Guide
Fundamentals
and SONET Testing

E 8.98/WG1/1015/3.5

Nominal charge US$ 10