OT interface protocol specification

HPRM1

SIERRA WIRELESS

2174004
Rev 2.4
March 05, 2013

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless modem in areas where cellular modems are not advised without proper device certifications. These areas include environments where cellular radio can interfere such as explosive atmospheres, medical equipment, or any other equipment which may be susceptible to any form of radio interference. The Sierra Wireless modem can transmit signals that could interfere with this equipment. Do not operate the Sierra Wireless modem in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless modem **MUST BE POWERED OFF**. When operating, the Sierra Wireless modem can transmit signals that could interfere with various onboard systems.

Note: *Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless modems may be used at this time.*

The driver or operator of any vehicle should not operate the Sierra Wireless modem while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

Limitations of Liability

This manual is provided "as is". Sierra Wireless makes no warranties of any kind, either expressed or implied, including any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. The recipient of the manual shall endorse all risks arising from its use.

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Customer understands that Sierra Wireless is not providing cellular or GPS (including A-GPS) services. These services are provided by a third party and should be purchased directly by the Customer.

SPECIFIC DISCLAIMERS OF LIABILITY: CUSTOMER RECOGNIZES AND ACKNOWLEDGES SIERRA WIRELESS IS NOT RESPONSIBLE FOR AND SHALL NOT BE HELD LIABLE FOR ANY DEFECT OR DEFICIENCY OF ANY KIND OF CELLULAR OR GPS (INCLUDING A-GPS) SERVICES.

Patents

This product may contain technology developed by or for Sierra Wireless Inc.

This product includes technology licensed from QUALCOMM®.

This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from InterDigital Group.

Copyright

Trademarks

AirCard® is a registered trademark of Sierra Wireless. Sierra Wireless™, AirPrime™, AirLink™, AirVantage™, Watcher™ and the Sierra Wireless logo are trademarks of Sierra Wireless.

, ®, inSIM®, WAVECOM®, WISMO®, Wireless Microprocessor®, Wireless CPU®, Open AT® are filed or registered trademarks of Sierra Wireless S.A. in France and/or in other countries.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh and Mac OS are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of the respective owners.

Contact Information

Sales Desk:	Phone:	1-604-232-1488
	Hours:	8:00 AM to 5:00 PM Pacific Time
	E-mail:	sales@sierrawireless.com
Post:	Sierra Wireless 13811 Wireless Way Richmond, BC Canada V6V 3A4	
Technical Support:	support@sierrawireless.com	
RMA Support:	repairs@sierrawireless.com	
Fax:	1-604-231-1109	
Web:	www.sierrawireless.com	

Consult our website for up-to-date product descriptions, documentation, application notes, firmware upgrades, troubleshooting tips, and press releases: www.sierrawireless.com

Document History

Version	Date	Updates
001	March 05 2013	Creation
002	April 5, 2013	OT STMA frames added OT L1/MM/RR reports revised

Contents

1. SCOPE

1.1. Introduction

The document details binary Protocol used by OT trace on MRM. PC tool application **(**Spaille2.exe and SagemComOT.exe for instance**)** or even external Applications that needs to decode OT frames must be in accordance with the protocol described hereafter.

OT traces is fully integrated in the already existing Real Time Trace system indeed it uses the same transport protocol. A dedicated TTR identifier will be created to filter on OT traces (TTR_OT).

This document describe version 1.2 of the protocol. Commands dedicated to the control of this feature are detailed in chapter 5.

1.2. Reference

1. 3GPP TS 03.22 V8.7.0 (R99) Functions related to Mobile Station (MS) in idle mode and group receive mode
2. 3GPP TS 23.003 V3.15.0 (R99) Numbering, addressing and identification
3. 3GPP TS 04.04 V8.1.2 (R99) Layer 1 - General Requirements
4. 3GPP TS 04.18 V8.27.0 (R99) Mobile radio interface layer 3 specification; Radio Resource Control (RRC) protocol
5. 3GPP TS 24.008 V3.20.0 (R99) Mobile radio interface Layer 3 specification; Core network protocols; Stage 3
6. 3GPP TS 05.02 V8.11.0 (R99) Multiplexing and Multiple Access on the Radio Path
7. 3GPP TS 05.05 V8.20.0 (R99) Radio Transmission and Reception
8. 3GPP TS 05.08 V8.23.0 (R99) Radio subsystem link control
9. 3GPP TS 05.10 V8.12.0 (R99) Radio subsystem synchronization

1.3. List of abbreviation

ARFCN	Absolute Radio Frequency Channel Number
BCCH	Broadcast Control CHannel
BS	Base Station
CI	Cell ID
DCS 1800	GSM 1800, Digital Communication System
GSM	Global System for Mobile communication
GSM-R	Global System for Mobile – Railway
HMI	Human Machine Interface
IE	Information Element
LA	Location Area

MS	Mobile Station
MRM:	Mobile Radio Module
PBCCH	Packet Broadcast Control Channel
PCS 1900	GSM1900, Personal Communication Service
PLMN	Public Land Mobile Network
RXLEV	Received Signal Level
RXQUAL	Received Signal Quality
SCH	Synchronization Channel
SI	System Information
TBF	Temporary Blok Flow
VBS :	Voice Broadcast Service
VGCS:	Voice Group Call Service

2. TRANSPORT LAYER PROTOCOL

2.1. General Frame overview

Byte \ bit	7	6	5	4	3	2	1	0
Byte 0	STX							
Byte 1	ID							
Byte 2	R	LG (High part)						
Byte 3	LG (Low part)							
Byte 4	OT FRAME							
.								
Byte N								
Byte N+1	CRC							
Byte N+2	ETX							

2.1.1. Starter Byte

- 0x02 : STX (Start of TeXt) it's the synchronization byte.

2.1.2. Identifier

- 0x90 : (TTR_OT) Real Time Trace Outil Test.

2.1.3. Length

Length of the frame coded on 15 bits only. The most significant bit is reserved.

2.1.4. Frame

Frame format is detailed in chapter §4.

2.1.5. Control

The CRC is calculated by a XOR operation done on bytes from ID to the end of OT Frame

2.1.6. ETX

- 0x03 : End of TeXt

3. OT FRAME PROTOCOL

3.1. OT Frame Format

Byte \ bit	7	6	5	4	3	2	7	0
0	Protocol Version							
1	Type			Sub Type				
2	Timestamp (MSB part)							
3								
4	(LSB part)							
5 to N	Message Field							

Careful! The OT Frame length is always even. A padding byte (value = 0) may be added at the end of the Message Field

3.1.1. Protocol Version

Identifies the Protocol Version.

- 00010001b : Version 1.1 (TIGR)
- 00010010b : Version 1.2 (MRM)

3.1.2. Type

The type identifies the category of OT trace transmitted:

- 000b : Measure Report
- 001b : Layer message
- 010b : Reserved
- 011b : Trace information
- 100b : AT Information

3.1.3. Sub Type

This field identifies a type of information within a category.

- Measure Report
  - 00000b : L1 Measure report idle mode
  - 00001b : L1 Measure report dedicated mode
  - 00010b : L1 Measure report listener mode
  - 00011b : RR Measure report idle mode
  - 00100b : RR Measure report without Frequency Hopping
  - 00101b : RR Measure report with Frequency Hopping
  - 00110b : MM Measure report
  - 00111b : Reserved for future use.
  - 01000b : MAC information
  - 01001b : RLC information

- Layer Message
  - 00000b : L3 Messages

- Trace information:
  - 00000b : Start
  - 00001b : Stop
  - 00010b : Marker

- AT information :
  - 00000b : Default

3.1.4. Time-Stamp

This field is built from internal system clock base accessible from *"qostimc*" global variable, and by using only the lower 3 Bytes of this variable. It represents around 21 hours of tests.The tick unit is 4,615 ms and is coded on four bytes, it measures the time since MRM start-up. The clock is reset on MRM start-up or after 220 days.

3.1.5. Message Field

This field depends on the message identification done by type and subtype parameter. Each message is described in dedicated chapter hereunder.

3.2. Layer 1 Measurement report Information

3.2.1. Mode definitions

- **Dedicated mode**: mode when a communication is ongoing and the user uses both the uplink and downlink. This mode includes the talker mode.
- **Idle mode**: default mode when no communication is ongoing.
- **Listener mode**: mode when a group call or a broadcast call is ongoing and the user has not the uplink.

3.2.2. Layer 1 report format

Layer 1 report includes measurement information of the serving cell and the six strongest neighboring cells. Some parameters are not relevant in every MS mode. For example the cell reselection parameters C1 and C2 are calculated only in idle and listener mode. In dedicated mode the handover is managed by the network, therefore the mobile only need to monitor cell level and radio link quality.

The refresh rate depends on the mode of the MS. In IDLE mode, the data are refreshed every 2s. In DEDICATED and LISTENER mode, the refresh rate is 500ms.

Byte \ bit	**7**	**6**	**5**	**4**	**3**	**2**	**1**	**0**
0	Serving Cell Info Length							
1 to N	Serving Cell info							
N+1	One Neighboring Cell info Length							
N+2 to M	Block info of the Six Neighboring Cell							

3.2.3. L1 report : Idle Mode – Serving Cell

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VSCELL	BI	VSCH	VSI3	VC2	Spare		
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	VX	RXLEV						
byte 4	C1							
byte 5	C2							
byte 6	CI (high part)							
byte 7	CI (low part)							
byte 8	Spare	DSC						
byte 9	Spare	DSC MAX						

3.2.4. L1 report : Idle Mode – Neighbors Cell

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VCELL	Spare	VSCH	VSI3	VC2	VSEL	LD	CB
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	VX	RXLEV						
byte 4	C1							
byte 5	C2							
byte 6	CI (high part)							
byte 7	CI (low part)							

3.2.5. L1 report : Dedicated Mode – Serving Cell

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VSCELL	BI	VSCH	VSI3	Spare	TS		
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	VXsub	RXLEV SUB						
byte 4	RXQUAL SUB			RXQUAL FULL			TCH (high part)	
byte 5	TCH (low part)							
byte 6	CI (high part)							
byte 7	CI (low part)							
byte 8	Spare		TA					
byte 9	Spare		PL					
byte 10	VXfull	RXLEV FULL						
byte 11	VRLC	RLC						
byte 12	Spare	RLT						

3.2.6. L1 report : Dedicated Mode – Neighbors Cell

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VCELL	Spare	VSCH	Spare				
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	VX	RXLEV						

3.2.7. L1 report : Listener Mode – Serving Cell

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VSCELL	BI	VSCH	VSI3	VC2	TS		
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	VXsub	RXLEV SUB						
byte 4	RXQUAL SUB			RXQUAL FULL			TCH (high part)	
byte 5	TCH (low part)							
byte 6	C1							
byte 7	C2							
byte 8	CI (high part)							
byte 9	CI (low part)							
byte 10	VXfull	RXLEV FULL						
byte 11	VXb	RXLEV BCCH						
byte 12	VRLC	RLC						
byte 13	Spare	RLT						

3.2.8. L1 report : Listener Mode – Neighbors Cell

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VCELL	Spare	VSCH	VSI3	VC2	VSEL	LD	CB
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	VX	RXLEV						
byte 4	C1							
byte 5	C2							
byte 6	CI (high part)							
byte 7	CI (low part)							

3.2.9. L1 report : Field Definition

Format for Serving and neighboring cell info depends on current communication mode specified in subtype field value of the L1 measure report see [3.1.3].

- **v_scell**: this variable indicates the validity of the BCCH frequency. The full L1 REPORT should be discarded when v_scell is not valid.
  parameter name:VSCELL
  scope: 0,1
  size[1]: 1bit

- **band_indicator**: this variable associates the ARFCN channel numbers to the DCS 1800 or to the PCS 1900.
  parameter name: BI
  scope: 0,1 0 -> ARFCN indicates 1800 band 1 -> ARFCN indicates 1900 band
  The distinction is relevant when the ARFCN is included in the range of DCS or PCS ARFCN.
  size: 1bit

- **bcch_carrier**: this variable contains the ARFCN of the BCCH.
  parameter name:BCCH
  reference: [7]
  scope: 0..1023; GSM covers [0..124], GSM850 [128..251], DCS 1800 [512..885], ER-GSM[940..954], R-GSM [955..974], E-GSM [975..1023], PCS 1900 [512..810]
  size: 10bits

- **v_rxlev:** this variable indicates the validity of the parameter RXLEV.
  parameter name:VX
  scope: 0,1
  size: 1bit

- **rxlev:** this variables contains the received level average of the cell measured in idle mode (RLA_C).
  parameter name:RXLEV
  reference: [8]
  scope: 0..127
  In the standard the measured signal level is mapped to the scope 0-63, and 63 value indicates “greater than -48dBm”, the actual measured signal level can take more values.
  0:less than -110dBm
  1:-110dBm to -109dBm
  2:-109dBm to -108dBm

  ...
  size: 7bits

- **critere_c1**: this variable contains the path loss criterion C1.
  parameter name: C1
  reference: [0] [8]
  scope: -92..+63,

---

[1] The size is the minimum size in bit to cover the full range of the variable.

size:8bits

- **v_c2:** this variable indicates the validity of the parameter C2.
  parameter name: VC2
  scope: 0,1
  size: 1bit

- **critere_c2**: this variable contains the reselection criterion C2.
  parameter name: C2
  reference: [0] [8]
  scope: -123...+189. The value is truncated to +127 to fit into a byte
  size: 8bits

- **f_info_sch**: this variable indicates the successful synchronisation on the SCH of the cell. It indicates the validity of the parameters NCC and BCC.
  parameter name: VSCH
  scope: 0,1
  size: 1 bit

- **ncc:** this variable contains the value of NCC (Network Colour Code).
  parameter name: NCC
  reference: [2]
  scope: --
  size: 3bits

- **bcc:** this variable contains the value of BCC (BS Colour Code).
  parameter name:BCC
  reference: [2]
  scope: --
  size: 3bits

- **f_info_si3**: this variable indicates decoding of the SI3 of the cell. It indicates the validity of the parameters DSC, DSC MAX and CI.
  parameter name: VSI3
  scope: 0,1
  size: 1 bit

- **cell_id:** this variable contains the Cell Identity. Cell Identity allows to identify the cell within one LA.
  parameter name:CI
  reference: [5]
  scope: --
  size: 16bits

- **dsc:** this variable represents the current value of DSC (Downlink Signalling failure Counter)
  parameter name:DSC
  reference: [8]
  scope: 0..45
  size: 6bits

- **dsc_max**: this variable represents the maximum value of DSC
  parameter name: DSC MAX

  reference: [8]

  scope: 90/[2..9] -> 10..45

size: 6bits

- **f_info_sel**: this variable indicates the reading of the SI3 or the SI4 of the cell. It validates the parameters LD and CB.
  parameter name: VSEL
  scope: 0,1
  size: 1bit

- **lai_diff**: this variable indicates if the cell is in the same LA than the serving cell.
  parameter name:LD
  reference: [5]
  scope: 0,1 0-> same LA 1-> different LA
  size: 1bit

- **cell_barred**: this variable indicates if the cell is barred for selection and reselection.
  parameter name: CB
  reference: [0] [8]
  scope: 0,1 0 -> cell not barred1-> cell barred

- **tch_carrier**: this variable contains the ARFCN of the TCH.
  parameter name: TCH
  scope: 0..1023; GSM covers [0..124], GSM 850[128..251], DCS 1800 [512..885], ER-GSM[940..954] R-GSM[955..974], E-GSM [975..1023], PCS 1900 [512..810]. The value 500 is reserved for indicating that the hopping mode is activated.
  size: 10bits

- **timing_adv:** this variable contains the Timing Advance. TA is a signal sent by the BTS to the MS which the MS uses to advance its timings of transmissions to the BTS so as to compensate for propagation delay.
  parameter name: TA
  reference: [3] [9]
  scope: 0..63, the coding of the timing advance value field is the binary representation of the timing advance in bit periods; 1 bit period = 48/13 µs
  size: 6bits

- **power_level:** this variable contains the Power Level. PL is a signal sent by the BTS to the MS which the MS uses to adjust the power level of emission.
  parameter name: PL
  reference: [3] [7]
  scope: 0..31
  for GSM 900 and R-GSM
  0..2 : 39 dBm
  3 : 37 dBm
  4 : 35 dBm
  …
  18 : 7 dBm
  19-31 : 5 dBm
  for DCS 1800 see reference
  for PCS 1900 see reference
  size: 5bits

- **time_slot:** this variable indicates the timeslot number describing the physical channel assigned to the MS.
  parameter name: TS
  reference: [4] [6]
  scope: 0..7
  size: 3bits

- **v_rxlev_full :** this variable indicates the validity of the parameters RXLEV FULL and RXQUAL FULL.
  parameter name: VXfull

- **rxlev_full**: this variable contains the received level average of the cell for the full-set of TCH and SACCH TDMA frames.
  parameter name: RXLEV FULL
  reference: [4] [8]
  scope: 0..63
  size: 7bits

- **rxlqual_full:** this variable contains the received signal quality. The value is deducted from the average BER before channel decoding for the full-set of TCH and SACCH TDMA frames.
  parameter name: RXQUAL FULL
  reference: [4] [8]
  scope: 0..7
  0 BER<0,2 % Assumed value =0,14 %
  1 0,2 %<BER<0,4 % Assumed value =0,28 %
  2 0,4 %<BER<0,8 % Assumed value =0,57 %
  3 0,8 %<BER<1,6 % Assumed value =1,13 %
  4 1,6 %<BER<3,2 % Assumed value =2,26 %
  5 3,2 %<BER<6,4 % Assumed value =4,53 %
  6 6,4 %<BER<12,8 % Assumed value =9,05 %
  7 12,8 %<BER Assumed value =18,10 %
  size: 3bits

- v_rxlev_sub : this variable indicates the validity of the parameters RXLEV SUB, and RXQUAL SUB.
  parameter name: VXfull

- **rxlev_sub**: this variable contains the received level average of the cell for the sub-set of SACCH TDMA frames.
  parameter name: RXLEV SUB
  reference: [4] [8]
  scope: 0..63
  size: 7bits

- **rxqual_sub**: this variable contains the received signal quality. The value is deducted from the average BER before channel decoding assessed for the sub-set of SACCH TDMA frames.
  parameter name: RXQUAL SUB
  reference: [4] [8]
  scope: 0..7 (see RXQUAL FULL)
  size: 3bits

- **v_rxlev_bcch**: this variable indicates the validity of the parameter RXLEV BCCH
  parameter name: VXb

scope: 0,1
size: 1bit

- **rxlev_bcch:** this variable contains the received level average on the physical canal BCCH of the cell.
  parameter name: RXLEV BCCH
  scope: 0..127
  size: 7bits

- **v_rlc**: this variable indicates the validity of RLC and RLT.
  parameter name: VRLC
  scope: 0,1
  size: 1bit

- **rlc**: this variable is the current value of the radio link counter S. If the MS is unable to decode a SACCH message S is decreased by 1. In the case of a successful reception of a SACCH message S is increased by 2. In any case S shall not exceed the value of RADIO_LINK_TIMEOUT. If S reaches 0 a radio link failure shall be declared.
  parameter name: RLC
  reference: [8]
  scope: 0-64
  size: 7bits

- **rlt**: The RADIO_LINK_TIMEOUT is the maximum value of the radio link counter. The RLT parameter is transmitted by each BSS in the BCCH data. The RLT transmitted by the network has been mapped to the number of SACCH blocks.
  parameter name: RLT
  reference: [4] [8]
  scope: 4-64
  size: 7bits

3.2.10. L1 report messages period

L1 report messages are sent every 2 seconds in idle.

L1 report messages are sent every 500 ms in dedicated or listener mode.

3.3. MM Measure report

This mobility information of the MS does not depend on the mobile mode.

3.3.1. MM report format

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VSEL	Spare					Service state	
byte 1	MCC digit 2				MCC digit 1			
byte 2	MNC digit 3				MCC digit 3			
byte 3	MNC digit 2				MNC digit 1			
byte 4	LAC (high part)							
byte 5	LAC (low part)							

3.3.2. MM report field definition

- service_state: this variable indicates the service state.
  parameter name: Service state
  reference: [1]
  scope: 0..3
  Bits: b2 b1
  0 0 : no service available
  0 1 : limited service state: only emergency service available
  1 0 : normal service state: complete service available
  1 1 : undetermined service state
  size: 2bits

- f_info_sel: this variable indicates the reading of the SI3 or the SI4 of the cell. It validates the parameters MCC (digit 1,2,3), MNC (digit 1,2,3) and LAC.
  parameter name: VSEL
  scope: 0,1
  size: 1bit

- mcc_digit1: this variable contains the digit 1 of the Mobile Country Code (MCC). The MCC is coded on 3 digits.
  parameter name: MCC digit 1
  reference: [5]
  scope: 0..9
  size: 4bits

- mcc_digit2: this variable contains the digit 2 of the MCC.
  parameter name: MCC digit 2

scope: 0..9
size: 4bits

- mcc_digit3: this variable contains the digit 3 of the MCC.
  parameter name: MCC digit 3
  scope: 0..9
  size: 4bits

- mnc_digit1: this variable contains the digit 1of the Mobile Network Code (MNC). The MNC consists of 2 or 3 digits.
  reference: [5]
  parameter name: MNC digit 1
  scope: 0..9
  size: 4bits

- mnc_digit2: this variable contains the digit 2 of the MNC.
  parameter name: MNC digit 2
  scope: 0..9
  size: 4bits

- mnc_digit3: this variable contains the digit 3 of the MNC.
  parameter name: MNC digit 3
  scope: 0..9, F indicates that this digit is not used.
  size: 4bits

- lac: this variable contains the Location Area Code (LAC)
  parameter name: LAC
  reference: [5]
  scope: --
  size: 16bits

3.3.3. MM report messages period

MM report messages are sent every 2 seconds in idle.

MM report messages are sent every 2 seconds in dedicated or listener mode.

3.4. RR Measure report

RR reports are delivered in dedicated mode and listener mode:

3.4.1. RR report format : Frequency Hopping Deactivated

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VSCELL	BI	VSCH	Spare	H = 0	TS		
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	channel mode							
byte 4	channel type			subchannel			TCH (high part)	
byte 5	TCH (low part)							

3.4.2. RR report format : Frequency Hopping activated

	b7	b6	b5	b4	b3	b2	b1	b0
byte 0	VSCELL	BI	VSCH	Spare	H = 1	TS		
byte 1	NCC			BCC			BCCH (high part)	
byte 2	BCCH (low part)							
byte 3	channel mode							
byte 4	channel type			subchannel			Spare	
byte 5	Spare		MAIO					
byte 6	Spare		HSN					
byte 7	Spare	Number of frequencies in list						
byte 8	Spare						F1 (high part)	
byte 9	F1 (low part)							
byte 10	Spare						F2 (high part)	
byte 11	F2 (low part)							

3.4.3. RR report Field definition

- **v_scell:** this variable indicates the validity of the parameter of the RR REPORT.
  parameter name:VSCELL
  scope: 0,1
  size: 1bit

- **band_indicator:** this variable associates the ARFCN channel numbers to the DCS 1800 or to the PCS 1900.
  parameter name: BI
  scope: 0,1 0 -> ARFCN indicates 1800 band 1 -> ARFCN indicates 1900 band
  The distinction is relevant when the ARFCN is included in the range of DCS or PCS ARFCN.
  size: 1bit

- **bcch_carrier**: this variable contains the ARFCN of the BCCH.
  parameter name:BCCH
  reference: [7]
  scope: 0..1023; GSM covers [0..124], GSM850 [128..251], DCS 1800 [512..885], ER-GSM[940..954], R-GSM [955..974], E-GSM [975..1023], PCS 1900 [512..810]
  size: 10bits

- **hopping_mode**: this variable indicates if frequency hopping is activated. Format of the RR REPORT depends on the frequency hopping mode.
  parameter name:H
  scope: 0,1 0->frequency hopping is not activated 1->frequency hopping is activated
  size: 1bit

  if hopping_mode == 0

  - tch_carrier: this variable contains the ARFCN of the TCH.
    parameter name: TCH
    scope: 0..1023; GSM covers [0..124], GSM 850[128..251], DCS 1800 [512..885], ER-GSM[940..954] R-GSM[955..974], E-GSM [975..1023], PCS 1900 [512..810]. The value 500 is reserved for indicating that the hopping mode is activated.
    size: 10bits

  if hopping_mode == 1

  - nb_cell: this variable contains the number of cells in the Mobile Allocation list.
    parameter name: Number of frequencies in list
    scope: 1..64
    size: 7bits

  - liste_rf: this variable contains the list of the six first ARFCN of the cells in the Mobile Allocation list
    parameter name: F1, F2,F3,F4,F5,F6
    scope: 0..1023
    size: 6*10bits

  - hsn: this variable contrains the Hopping Sequence Number (HSN).
    parameter name: HSN

reference: [4] [6]
scope: 0..63
size: 6bits

- maio: this variable contains the Mobile Allocation Index Offset (MAIO).
  parameter name: MAIO
  reference: [4] [6]
  scope: 0..63
  size: 6bits

- f_info_sch: VSCH see 3.2.9
- ncc: NCC see 3.2.9
- bcc: BCC see 3.2.9

- channel_mode: this variable contains the channel mode IE.
  parameter name: channel mode
  reference: [4]
  scope: 0..255
  The main channel mode fields are encoded as follows (see reference for more values):
  0x00: signalling only
  0x01: speech full rate of half rate v1 (the channel types associated with this mode are TCH/FS and TCH/HS)
  0x21: speech full rate of half rate v2 (TCH/EFS)
  0x41: speech full rate or half rate v3 (TCH/AFS and TCH/AHS)
  0x0F: data, 14.5 kbit/s radio interface rate (TCH/F14.4)
  0x03: data, 12.0 kbit/s radio interface rate (TCH/F9.6)
  0x0b: data, 6.0 kbit/s radio interface rate (TCH/F4.8 and TCH/H4.8)
  0x13: data, 3.6 kbit/s radio interface rate (TCH/F2.4 and TCH/H2.4)
  size: 8bits

- channel_type: this variable contains the channel type.
  parameter name: channel type
  reference: [4]
  scope: 1..4
  1: SDCCH/4 + SACCH/C4
  2: SDCCH/8 + SACCH/C8
  3: TCH/FS + ACCHs
  4: TCH/HS + ACCHs
  size: 3bits

- Subchannel: this variable contains the subchannel number.
  parameter name: Subchannel:
  reference: [4]
  scope: 0..7
  size: 3bits

- time_slot TS see 3.2.9

3.4.4. RR report messages period

L1 report messages are sent every 2 seconds in dedicated or listener mode.

3.5. Layer Message

3.5.1. Layer 3 frame format

	b7	b6	b5	b4	b3	b2	b0	0
Byte 0	Status	Reserved				Pr	Fr	Dir
Byte 1	LG							
Byte 2	LG							
Byte N	GSM Message Field							
Byte N+1	Reserved						BCCH	
Byte N+2	BCCH							

3.5.2. Status

Indicates message status.

- 1b: status ok
- 0b: status not ok (empty message)

3.5.3. Pr : Short RR protocol

Indicates layer 3 messages using RR short protocol discriminator.

- 1b: layer 3 messages using RR short protocol discriminator.
- 0b: layer 3 message not using RR short protocol discriminator

3.5.4. Frequency information

Indicates availability of BBCH frequency field at the end of the layer frame.

3.5.5. Direction

Dir fields identifies the message direction,

- 1b : Uplink Layer message
- 0b : Downlink Layer message

3.5.6. Length

LG indicates the GSM message field information length in byte.

When the length of the message is 0 and the status of the message is OK. It means than a L2 fill frame has been read on a CCCH.

3.5.7. GSM Message Field

Layer 3 Message Frame is compliant with GSM recommendations [04.08].

In case of standard L3 message (Pr field = 0b), GSM Message Field contains the standard L3 message.

In case of non-standard L3 messages:

- Case A: (Pr field = 0b) BCCH and AGCH/PCH messages: GSM Message Field contains standard L3 message and “Rest Octet” IE
- Case B: (Pr field = 1b) SACCH / SDCCH / FACCH messages sent in unacknowledged mode: GSM Message Field contains the L3 message and the 2-bit link layer header.

The parts of the L3 message present in GSM message field are colored in light red, see [24.007] §11 for detailed L3 message description.

<table>
<tr><td rowspan="2">Standard L3 message</td><td colspan="4">Non-standard L3 message</td></tr>
<tr><td>BCCH and AGCH/PCH messages</td><td colspan="3">SACCH / SDCCH / FACCH messages sent in unacknowledged mode:</td></tr>
<tr><td rowspan="3">Standard L3 message</td><td>L2 pseudo length octet</td><td colspan="3"></td></tr>
<tr><td>Standard L3 message</td><td>RR PD</td><td>Message type</td><td>L2 header</td></tr>
<tr><td>Rest octets</td><td colspan="3">Rest of the message</td></tr>
</table>

3.5.8. BCCH frequency

If frequency bit is set, this field is present and includes the BCCH frequency.

3.6. Trace Information

3.6.1. Start trace

This information indicates the start of a trace session, and is associated with a timestamp. The “qostimc” timestamp is already available in the OT Frame header (bytes 2 to 4). If available, the following date & time information (from RTC) is more convenient to use:

Bit / Byte \	b7	b6	b5	b4	b3	b2	b1	b0
0	Session ID							
1	VT	Spare			Day			
2	Spare				Month			
3	Spare			Hours				
4	Spare			Minutes				
5	Spare			Seconds				

Session ID: Session Number extracted from the TRACE_RECORD_START or LIVE_TRACING_START STMA command

VT: Presence of the RTC date & time information (1 if present, 0 if absent)

Day: Day from the real time clock, from 1 to 31 (5 bits)

Month: Month from the real time clock, from 1 to 12 (4 bits)

Hours: Hours from the real time clock, from 0 to 23 (5 bits)

Minutes: Minutes from the real time clock, from 0 to 59 (6 bits)

Seconds: Seconds from the real time clock, from 0 to 59 (6 bits)

3.6.2. Stop trace

This information indicates the end of a trace session, and is associated with a timestamp. The “qostimc” timestamp is already available in the OT Frame header (bytes 2 to 4). If available, the following date & time information (from RTC) is more convenient to use:

Idem Start Trace

Bit / Byte \	b7	b6	b5	b4	b3	b2	b1	b0
0	Session ID							

1	VT	Spare	Day
2	Spare		Month
3	Spare		Hours
4	Spare		Minutes
5	Spare		Seconds

Session ID: Session Number extracted from the TRACE_RECORD_START or LIVE_TRACING_START STMA command

VT: Presence of the RTC date & time information (1 if present, 0 if absent)

Day: Day from the real time clock, from 1 to 31 (5 bits)

Month: Month from the real time clock, from 1 to 12 (4 bits)

Hour: Hours from the real time clock, from 0 to 23 (5 bits)

Minutes: Minutes from the real time clock, from 0 to 59 (6 bits)

Seconds: Seconds from the real time clock, from 0 to 59 (6 bits)

3.6.3. Marker

The marker information is used to insert a number in the trace.

This number is automatically incremented from 1 to 255, then set to 1 if value 255 is exceeded.

The *"qostimc"* timestamp is already available in the OT Frame header (bytes 2 to 4).

If available, the following date & time information is more convenient to use.

**Bit Byte **	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**b0**
0	Session ID							
1	VT	Spare			Day			
2	Spare				Month			
3	Spare			Hours				
4	Spare			Minutes				
5	Spare			Seconds				
6	Marker Index							

Session ID: Session Number extracted from the TRACE_RECORD_START or LIVE_TRACING_START STMA command

Marker Index: Index of the marker from 1 to 255

VT: Presence of the Time information (1 if present, 0 if absent)

Day:	Day from the real time clock, from 1 to 31 (5 bits)
Month:	Month from the real time clock, from 1 to 12 (4 bits)
Hour:	Hours from the real time clock, from 0 to 23 (5 bits)
Minutes:	Minutes from the real time clock, from 0 to 59 (6 bits)
Seconds:	Seconds from the real time clock, from 0 to 59 (6 bits)

3.7. AT information

3.7.1. AT frame format

Byte\bit	7	6	5	4	3	2	1	0
Byte 0	DIRECTION							
Byte 1 - N	DATA							

3.7.2. Direction

- 0x03 : Command received by the MRM.
- 0x04 : Response sent by the MRM.

3.7.3. Data

AT Command and Response in hexa decimal format. It has to be converted in ASCI format.

4. LINK CONFIGURATION

4.1. Serial Link

4.1.1. Hardware

The default serial com to output the OT traces is the Maintenance com on backplane. PowerQuicc can be reconfigured by parameters to output the traces either on Serial FrontPlane or Key Serial backplane (used for AT command by default). See fields : « **B1.04.01.03** » in [1] referenced document for details.

PIN	Circuit Number	Input / Output	Circuit Name	Abbreviation	Level When OPEN
C 29	---	---	Signal Ground	S-GND	---
C 30	CT 104	Output	Received Data	RxD	
C 31	CT 103	Input	Transmitted Data	TxD	High

4.1.2. Settings

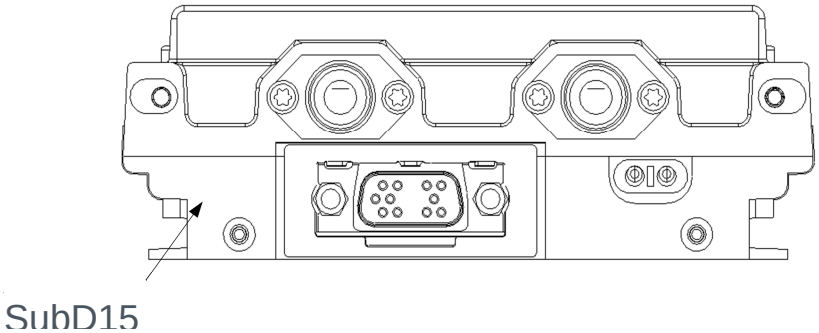
Serial Trace configuration	
Type	RS232
Speed	up to 115200 bit/s
DataBits	8
StopBits	1
StartBits	1
Parity	None
FC	No flow control

4.2. Usb front plan

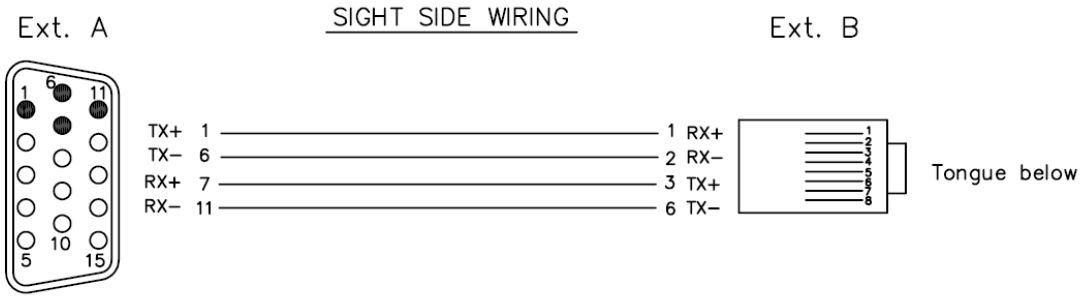
4.3. Ethernet

4.3.1. Hardware

The back pane and the front pane both provide an Ethernet Interface,. The two links are plugged to an internal network switch. So the Ethernet cable can be plugged indifferently in the front or the back.



Following figure present the Specific cable [male RJ-45] on PC side and [male SUB-D 15] on MRM side necessary for the connection.



4.3.2. Priorities for physical links

There is an order in term of priorities for using the physical links:

1. USB (Higher priority)
2. Ethernet
3. Serial

This means that the following conditions must be respected:

Link to use	**Condition**
USB	NA
Ethernet connection	USB cable must not be plugged

Serial	USB cable must not be plugged and no Ethernet connection must be established

4.3.3. Ethernet protocol

For the current version of tracing feature (Version 1.2), only TCP is implemented. The OT protocol is encapsulated into TCP frames.

TCP Server is MRM, TCP client is the host.

4.3.4. Ethernet parameters

Ethernet Trace and STMA configuration	
MRM IP address	10.10.10.3
Protocol	TCP
Ports	9999 for Traces 9998 for STMA

Ethernet FTP configuration	
MRM IP address	10.10.10.3
Protocol	FTP
Port	TCP 21 (standard FTP Port)

5. STMA COMMANDS FRAMES

5.1. General STMA frames command/response format

		<- Length ->						
STX	Length	SAGEM	STMA	operation	STMA ID	DATA	CHKSUM	ETX
0x02	Length N (*)	0xD2	0x05	0x00/0x01 (**)	0x37		(***)	0x03
1 Byte	1	1	1	1	1	N - 4	1	1

(*) Number of bytes from SAGEM field to last byte of DATA Field

(**) Operation field = 0x00 for commands (from host to MRM) or 0x01 for responses (from MRM to host)

(***) CKSUM is a XOR sum calculated on bytes from STX to last DATA byte.

5.2. OT STMA command

5.2.1. OT STMA Identifier

The OT STMA ID is **0x37**

5.2.2. OT STMA command list

Each OT STMA command begins with a sub-type.

Some parameters should follow, only for commands marked with (*).

Each OT STMA response begins with a status code.

Some additional info should follow, only for commands marked with (**)

Sub-Type	Name	Description
0x00	TRACE_RECORD_RESET	Reset the Trace Record

0x01	TRACE_RECORD_TRANSFER_START (*)	Start the Transfer MS->PC of the Trace Record
0x02	TRACE_RECORD_TRANSFERT_STOP	Same as TRACING_STOP
0x03	LIVE_TRACING_START (*)	Start the Live Tracing (MS->PC)
0x04	TRACING_STOP	Stop the current operation (live tracing, recording or transferring)
0x05	TRACE_RECORD_START	Start Recording
0x06	TRACE_RECORD_STOP	Same as TRACING_STOP
0x07	GET_TRACE_INFO (**)	Get miscellaneous info and can be used to poll the MRM state.
0x08	INSERT_MARKER (**)	Insert a Marker into the trace
0x09	SEND_HOST_HORODATE (*)	Send Horodate to MRM
0x0A	RFU	
0x0B	SELECT_TRACE (*)	Chose the kinds of traces (L1, RR, MM, LayerMsg, AT)
0x0C	BOOT_TRACE_MODE (*)	Enable tracing at startup

5.2.3. TRACE_RECORD_START command

The following parameters must follow the command sub-type:

Byte	Description	Length
0	Session ID	1

5.2.4. LIVE_TRACING_START command

The following parameters must follow the command sub-type:

Byte	Description	Length
0	Session ID	1

5.2.5. SEND_HOST_HORODATE command

The following parameters must follow the command sub-type:

Byte	Description	Length
0	Local time year since 2000, BCD format	1
1	Local time month, BCD format	1
2	Local time day, BCD format	1
3	Local time hour, BCD format	1
4	Local time minute, BCD format	1
5	Local time second, BCD format	1

5.2.6. BOOT_TRACE_MODE

This command is used to start automatically the OT Tracing at startup

The following parameters must follow the command sub-type:

Byte	Description	Length
0	0 : Traces Off 1: Live Tracing 2: Trace recording	1

5.2.7. SET_TRACE_FILTER

This command is used to select which kind of trace is enabled

The following parameters must follow the command sub-type:

Byte	Description	Length
0	Bit Field Bit4: L1 Report Bit3: MM Report Bit2: RR Report	1

	Bit1: Layer Message Bit0: AT	

5.3. Standard STMA responses

		<- Length ->							
STX	Length	SAGEM	STMA	operation	STMA ID	STATUS CODE	DATA	CHKSUM	ETX
0x02	Length N (*)	0xD2	0x05	0x01 (**)				(***)	0x03
1 Byte	1	1	1	1	1	1	N - 5	1	1

5.3.1. OT STMA status codes

The first byte into the response data field is always the status code:

Status	Name	Description
0x00	OT_STATUS_OK	Command performed successfully
0x01	OT_STATUS_ERROR_BAD_FRAME	Invalid format
0x02	OT_STATUS_ERROR_FEATURE_INACTIVE	OT Trace is not active
0x03	OT_STATUS_ERROR_BAD_STATE	Operation not allowed in current state
0x04	OT_STATUS_ERROR_SAME_MODE	Operation not performed because the mode is the same
0x05	OT_STATUS_ERROR_MEMORY_FULL	Recording not allowed because memory is full
0x06	OT_STATUS_ERROR_MEMORY_EMPTY	Format not performed because memory is already empty
0x07	OT_STATUS_ERROR_MEMORY_WRITE	File Write not possible, file has to be erased
0x08	OT_STATUS_ERROR_CONFIG_WRITE	OT Trace mode not written into flash memory

5.3.2. GET_TRACE_INFO response

The following info should follow the status code:

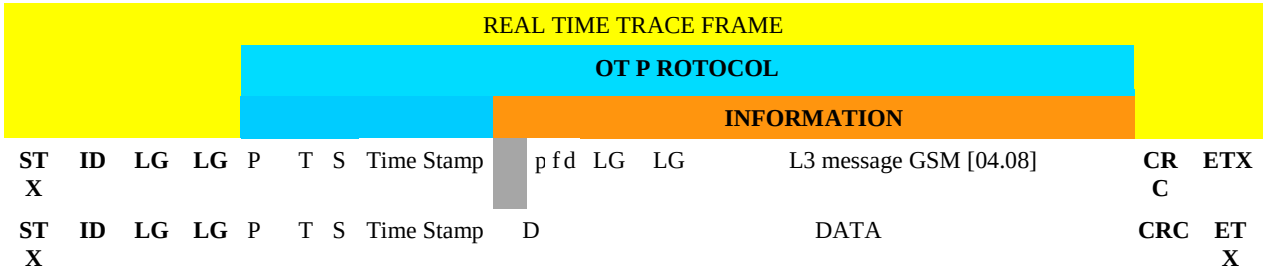
Byte	Description	Length
0	Tag = 2 (Not Used)	1
1	Length = 9 (Not Used)	1
2	Current Trace Mode 0: traces Off 1: Live tracing 2: Record tracing 3: Record transfert	1
3	StartupTrace Mode 0: traces Off 1: Live tracing 2: Record tracing	1
4-7	Record Length in Byte (MSB first)	4
8-11	Total Length of the Memory	4
12-17	Date/Time of the File Same format as SEND_HOST_HORODATE	6
18	OT Traces Filters Bit Field, cf SET_TRACE_FILTER command	1
19	OT File Error 0 : No problem 1: File has to be erased	1

5.3.3. INSERT_MARKER response

The following info should follow the status code:

Byte	Description	Length
0	Index of the new marker (MSB first)	1

6. ANNEXE A Complete Frame Sample



Exemple 1: OT trace emitted when MRM receives AT command : ATI3 (Software Version)

02	83	00	08	12	80	Time Stamp	04	41 54 49 33 0d 00 (ATI3)	f5	03

7. ANNEXE B Information Summary

	Info	mode IDLE	mode DEDICATED	mode LISTENER
Serving cell	Band Indicator	L1 REPORT	L1 REPORT, RR REPORT	L1 REPORT, RR REPORT
	BCCH	L1 REPORT	L1 REPORT, RR REPORT	L1 REPORT, RR REPORT
	NCC	L1 REPORT	L1 REPORT, RR REPORT	L1 REPORT, RR REPORT
	BCC	L1 REPORT	L1 REPORT, RR REPORT	L1 REPORT, RR REPORT
	CI	L1 REPORT	L1 REPORT	L1 REPORT
	MCC (digit 1,2,3)	MM REPORT	MM REPORT	MM REPORT
	MNC (digit 1,2,3)	MM REPORT	MM REPORT	MM REPORT
	LAC	MM REPORT	MM REPORT	MM REPORT
	Measurements for cell reselection			
	C1	L1 REPORT	NA	L1 REPORT
	C2	L1 REPORT	NA	L1 REPORT
	RXLEV (RLA_C)	L1 REPORT	NA	NA
	DSC	L1 REPORT	NA	NA
	DSC Max	L1 REPORT	NA	NA
	Channel description			
	TS	NA	L1 REPORT, RR REPORT	L1 REPORT, RR REPORT
	TCH / Hopping mode	NA	L1 REPORT, RR REPORT	L1 REPORT, RR REPORT
	Timing Advance	NA	L1 REPORT	NA
	Power Level	NA	L1 REPORT	NA
	channel mode	NA	RR REPORT	RR REPORT
	channel type	NA	RR REPORT	RR REPORT
	subchannel	NA	RR REPORT	RR REPORT
	MAIO	NA	RR REPORT	RR REPORT
	HSN	NA	RR REPORT	RR REPORT
	MA frequency list	NA	RR REPORT	RR REPORT
	Radio link control (handover in dedicated mode, cell resel in listener mode)			
	RXLEV-SUB	NA	L1 REPORT	L1 REPORT

	RXQUAL-SUB	NA	L1 REPORT	L1 REPORT
	RXLEV-FULL	NA	L1 REPORT	L1 REPORT
	RXQUAL-FULL	NA	L1 REPORT	L1 REPORT
	RXLEV-BCCH	NA	L1 REPORT	L1 REPORT
	Radio Link Counter	NA	L1 REPORT	L1 REPORT
	Radio Link Timeout	NA	L1 REPORT	L1 REPORT
Neighbouring cells	BCCH	L1 REPORT	L1 REPORT	L1 REPORT
	NCC	L1 REPORT	L1 REPORT	L1 REPORT
	BCC	L1 REPORT	L1 REPORT	L1 REPORT
	CI	L1 REPORT	NA	L1 REPORT
	Same LA identificator	L1 REPORT	NA	L1 REPORT
	Cell Barred	L1 REPORT	NA	L1 REPORT
	Measurements for cell reselection			
	C1	L1 REPORT	NA	L1 REPORT
	C2	L1 REPORT	NA	L1 REPORT
	RXLEV (RLA_C)	L1 REPORT	NA	NA
	Radio link control (handover in dedicated mode, cell resel in listener mode)			
	RXLEV	NA	L1 REPORT	L1 REPORT