Technical Outline of GSM/EGPRS Protocol Stack

More than 250 million CCww-powered terminals shipped each year

Prepared by:
Anthony Cutler
Communications Consultants Worldwide Ltd.

25th March 2013
Revision: 1.9

1 Introduction

This document provides a brief summary of CCww, and a technical outline for CCww's GSM/EGPRS protocol stack (L1, L2, & L3), the development process, and analysis tools.

CCww has taken every care in the preparation of this document. However, this proposal contains preliminary information that may be the subject of revision.

Table of Contents

2 Introduction to CCww

CCww was founded in 1995 by a group of engineers who had pioneered GSM terminal design with Orbitel (later ST-Ericsson) in 1988, developing the world's first GSM handset, and later in 1993 creating the GSM Layer-1 for VLSI (later Philips). In 1995 these engineers formed a company to develop a portable GSM protocol stack from ground-up, independent of base-band and RTOS.

This protocol stack has been ported to 7 chipsets to date, and has powered more than 1B terminals, clearly showing the early vision has been fulfilled beyond original expectation. Major licensees include Qualcomm and Mediatek, who were provided with a technology –handover programme such that CCww's technology became internalised over a ~18 month period.

CCww is privately held by its senior management, and is a growing, profitable company with 6 full-time engineers with experienced partners that provide additional protocol stack development resources, electronic design, manufacture and product support.

CCww continues to licence its protocol stack, the most recent licensee being Q4/11, whilst at the same time addressing specialist handset and M2M niches with its in-house developed GSM/GPRS module. This ensures that CCww's GSM-related engineering expertise is constantly refreshed and its protocol stack remains the leading proven choice for both new chip designs and for chipsets requiring a GSM/EGPRS upgrade.

CCww's engineers remain hands-on, supporting and upgrading the protocol stack in response to the evolving GSM environment and customer needs, so you can be sure of the highest performance and lowest footprint possible, coupled with the most experienced and responsive support. CCww's stack is well into its next 1B shipped units – your chip or terminal could be part of this continuing success.

3 Outline of Protocol Stack

An outline description of the GSM/EGPRS L1, L2 & L3 stack is provided in the following sections.

3.1 Implementation Background

CCww's fully-instrumented GSM/EGPRS handset stack has been designed to optimise:

- Performance, incl high data rates, and low latency
- Footprint: lowest memory use consistent with performance
- Flexibility: rapid implementation with port to alternate base-band, RF chipsets and RTOS without main code changes; source code option
- Debug, validation and field trials process: comprehensive graphical tools

All code is written in ANSI C and has been ported to 7 chipsets to date (e.g. Qualcomm, Mediatek, and ST-Ericsson). Sub-layers are mostly implemented as individual tasks (save for, e.g. RLC/MAC) communicating through message queues. CCww uses NucleusPLUS internally; however, an alternative RTOS may be used through modification to the generic o/s interface layer. A description of the standard L1C, L2 & L3 stack is provided below and in the subsequent sections.

3.2 RTOS

The default RTOS supplied with CCww's protocol stack is Nucleus PLUS, licensed from Mentor Graphics. CCww is able to sub-licence Nucleus Plus to its stack users.

3.3 TCP/IP and PPP Interface

The default Internet protocol stack supplied with CCww's protocol is licensed from Mentor Graphics, comprising NucleusNET and NucleusPPP. The TCP/IP stack interfaces with the GPRS SNDCP sub-layer and provides a standard socket interface for applications. The GPRS serial port protocol (between Nucleus Net and external applications) is PPP as defined in RFC 1661 (see http://www.ietf.org/rfc/rfc1661.txt for more details).

CCww is able to sub-license Nucleus NET and PPP to its users.

3.4 Protocol Stack Footprint

The STAR-Let GSM/GPRS image (CCww L1, L2 &L3 with debug, AT-commands, hardware drivers, ST-E DSP/baseband) requires the following memory:

- RAM: 1.0 MB

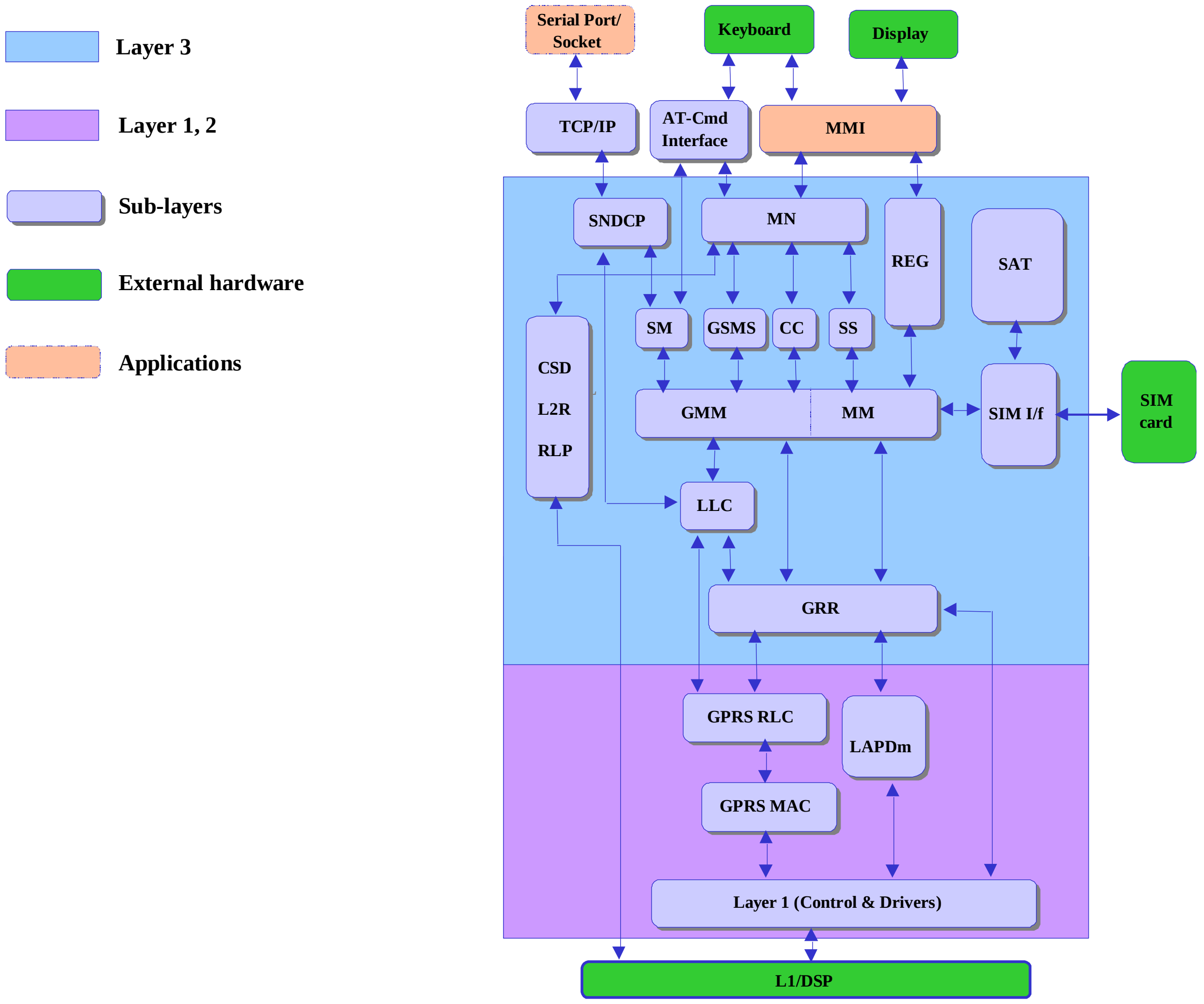
- Flash: 1.5 MB

During a Class 10 GPRS transfer (STAR-Lite M2M), the image (as above) requires 13-14 MIPS.

There are approximately ~1500 source files, incl header and ~860K lines of code, depending on chosen configuration.

3.5 Architecture

The following diagram shows the system architecture; please refer to the section on ‘Protocol Software Deliverables’ for information on the sub-layers to be licensed.



GSM/EGPRS Stack Architecture

3.6 Protocol Stack Summary Features

There follows a brief summary of the stack features:

- Class B implementation multi-slot class 12 to 3GPP Release 1999 June 2007
  - GPRS PDP context. Packet services accessed via integrated TCP/ IP stack, or via PPP using an external PC or PDA.
- Conforms to 3GPP Release ’99 / GCF-CC v3.35 bis (GCF-CC Version 3.35.0 dated 2009-07-06) and NAPRD.03 v5.0 bis (PTCRB NAPRD.03 v5.0) based on STAR-Let200Q M2M platform
- Data rates to 80Kbps (GPRS); 400Kbps (EGPRS)
- Quad-band support
- PBCCH support
- AT Command Interpreter implements 27.007 commands for GSM and GPRS; extended command set
- SIM Interface supports Phase 1 & 2 cards

- Layer 1
  - Type 1, multi-slot class 12
  - Simple primitive interface
  - Generic core design
  - Easily portable
  - Optimal power-saving
- Internet Protocol (TCP/IP) provided by third party (Mentor Graphics)
- Sub-Network Dependent Convergence Protocol (SNDCP)
  - Interfaces to AT command interpreter
  - Interfaces with IP directly or via PPP
  - Compression of TCP/IP headers (option)
- GSM Short Message Service (SMS)
- GPRS Short Message Service (GSMS)
  - MO and MT messages sent / received over GPRS packet link
- Circuit-Switched Data Option
  - Transparent & non-transparent up to 9.6 Kbits/sec (14.4 Kbps option)
  - Group 3 Fax Class 1
- Portable to alternate RTOS through abstraction layer (GHDI, GSDI)

3.7 Recent Certification and Field Trials

The L1-L3 protocol stack was certified April 2008 on the STAR-Lite GSM/GPRS M2M modem (+ voice/SMS; Class 10 GPRS).

- GCF/PTCRB test pass information:
  - GCF-CC V3.27.1 & NAPRD.03 V3.12.0 (R'99)
- Vodacom and MTN operator approval

In Dec '09, the protocol stack was re-certified on the STAR-Let GSM/GPRS M2M module (+ voice/SMS; Class 12 GPRS):

- GCF-CC v3.35 bis: official GCF-CC Version 3.35.0 dated 2009-07-06 plus new 5-day-rule changes.
- NAPRD.03 v5.0 bis: official PTCRB NAPRD.03 v5.0 (GSM Phase 2/2+ R97/98 onwards) plus new 5-day-rule changes.

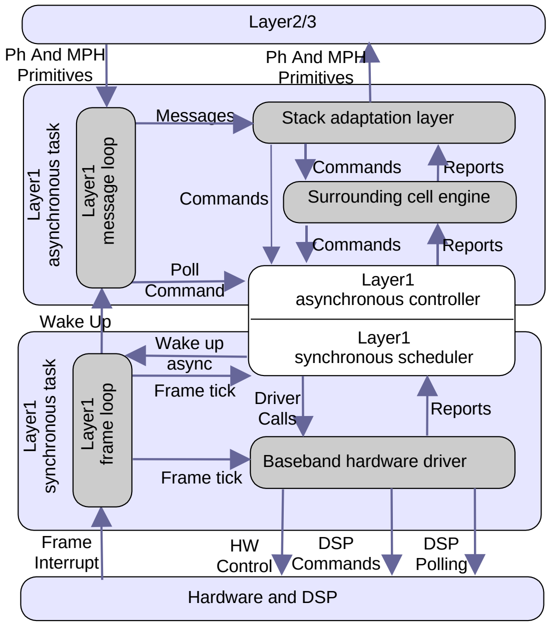
STAR-Lite and STAR-Let are extensively field-tested in the following territories:

- Africa (Central, Southern)
- Bangladesh
- Brazil
- China
- Cyprus
- Egypt
- Finland
- France
- Germany
- India
- Mexico
- Pakistan
- Saudi Arabia
- Spain
- Taiwan
- UK
- USA
- Vietnam

3.8 Layer 1

CCww's Layer 1 supports EGPRS multi-slot Class 12 and GSM single slot CSD. The Layer 1 control software implements all the necessary state and timing control for the TDMA air interface. A clean interface has been defined using MPH, PH and PPH primitives to request services from Layer 1.

The Layer 1 has been structured to be independent of base-band and RF implementation and for rapid adaption to new chipsets. The diagram below shows the separation into synchronous and asynchronous processes. A typical integration with a new chipset only requires a specific set of drivers to be written.



GSM/EGPRS Software Layer 1

The Layer 1 software includes the following features:

- Generic solution, portable to various baseband and RF platforms with new hardware drivers
- Controls DSP plus baseband and RF hardware via hardware drivers
- Compliant USF handling by the MCU depending on chipset.
- Allows type 1 configurations (non-simultaneous Rx/Tx)
- Supports all coding schemes (CS-1 to CS-4, MCS-1 to MCS-9), depending on chipset
- Supports multi-band operation (850, 900, 1800, 1900 MHz)
- Optimal use of available power saving features (e.g. DRx)
- Optional support for circuit switched data traffic channels up to 14.4k
- Supports full rate, enhanced full rate (EFR), half rate and AMR speech
- Handles intra-cell, inter-cell synchronised, inter-cell non-synchronised, inter-cell pseudo-synchronised, and inter-cell pre-synchronised handovers
- Supports ciphering of transmitted and received data between the MS and the network using the A5/1 algorithm (algorithm not provided)

3.9 Layer 2 (DL)

- The Layer 2 software implements the LAPDm data link protocol
- It supports unacknowledged mode on the unidirectional channels; BCCh, PCh, AGCh, CBCh, and both unacknowledged and multiple frame acknowledged mode on the SDCCh and FACCh channels
- The RACh channel information is transferred between Layer 1 and Layer 3, by Layer 2, during the random access procedure
- SAPI 3 on the SACCh is also supported by Layer 2 for short message services.

3.10 Radio Link Control (RLC)

- RLC provides both a reliable (acknowledge mode) and unreliable (unacknowledged mode) transfer of LLC PDUs from the LLC layer to layer1.

- It segments the PDUs and packs them into RLC radio blocks. Selective retransmission and incremental redundancy is used in acknowledge mode. Control messages generated by MAC during a TBF are multiplexed into the data stream as the PACCH channel.

- Received data blocks are reassembled into LLC PDUs and forwarded to LLC.

- RLC uses MAC to create and manage TBFs.

- RLC handles coding scheme changes during a TBF and notifies the network of changes to priority, PFI etc using MAC.

- TBFs are terminated using the countdown procedure.

3.11 Medium Access Control (MAC)

- MAC handles requests from the RLC entity for a TBF required for data transfer across the air interface.

- The full life cycle of the TBF is managed, beginning with resource request to the network (using PRACH channels if supported) and then resource allocation/reallocation as commanded by the network to establish and maintain the TBF

- Allocations as received from the network are decoded and used to configure layer 1.

- TBF Failure modes are also managed.

- MAC compiles and despatches measurement reports as requested by the network.

- It also constantly monitors the Packet System information messages if present.

- Reassembly of received control messages is required at this layer, as well as monitoring for and allocation of resources to handle Relative Reserved Block periods for uplink control messages as requested by the network. Radio Link Control (RLC)

- RLC provides both a reliable (acknowledge mode) and unreliable (unacknowledged mode) transfer of LLC PDUs from the LLC layer to layer1.

- It segments the PDUs and packs them into RLC radio blocks. Selective retransmission and incremental redundancy is used in acknowledge mode. Control messages generated by MAC during a TBF are multiplexed into the data stream as the PACCH channel.

- Received data blocks are reassembled into LLC PDUs and forwarded to LLC.

- RLC uses MAC to create and manage TBFs (Temporary Block Flow).

- RLC handles coding scheme changes during a TBF and notifies the network of changes to priority, PFI etc using MAC.

- TBFs are terminated using the countdown procedure.

3.12 Layer 3

The Layer 3 software is the signalling layer of GSM/EGPRS. The sub-layers are described below:

3.12.1 Radio Resources (RR)

The general purpose of Radio Resource procedures is to establish, maintain and release RR connections that allow a point-to-point dialogue between the network and a mobile station.

The function of RR depends on the current mode:

- It controls the initial selection of a cell, decoding of system information and paging messages for that cell, and system information from neighbour cells.

- It requests power measurements from layer 1 for neighbour cells in order to make decisions on cell reselection

- It responds to paging requests from the network or requests from upper layers to establish RR connections with the network, maintains that connection, including handing over to another cell when commanded by the network, and controls its release.

3.12.2 GPRS Radio Resources (GRR)

The GRR portion of the RR sub-layer handles the GPRS aspects of packet connection establishment:

- It decodes the information required by MAC when a PBCCh is available in the cell
- and handles establishment of packet transfer when no PBCCh exists.

3.12.3 Mobility Management (MM)

The MM sub-layer supports the mobility of the user terminal, in particular:

- informing the network of its present location with the location update procedure
- a routing area update procedure
- providing identity confidentiality by the TMSI and PTMSI reallocation procedure
- performing authentication of the mobile.

It uses the services of RR to request a connection to the network in order to perform any of the procedures, and provides services to the upper layers for PLMN selection, and the establishment of MM connections for use by upper layer procedures.

The runtime integration of GSM procedures is dependent on the network mode of operation.

3.12.4 GPRS Mobility Management (GMM)

The MM sub-layer supports additional mobility of the user terminal for GPRS, in particular:

- informing the network of its present location with the location update procedure or for GPRS

This GMM portion of the MM sub-layer represents the extra functionality within the MM sub-layer required to support GPRS. The GMM is an extension of MM that supports GPRS registration functions (GPRS Attach / Detach, Routing Area Update) as both explicit and combined (with GSM) procedures and also some GSM MM functions in the packet domain. The runtime integration of GSM and GPRS procedures is dependent on the network mode of operation.

3.12.5 Connection Management

The connection management sub-layer divides into three parts - the CC, SS and SMS sub-sections.

3.12.5.1 Call Control (CC)

The call control entity handles the establishment of calls, either on request of upper layers or request from the network, the release of calls, and the exchange of information while a call is in progress. This includes the:

- progress of the call setup,
- indication of alerting to upper layers,
- transfer of call related supplementary services
- and the modification of the call mode.

It uses the services of the MM sub-layer to set up an MM connection which is used for the signalling.

3.12.5.2 Supplementary Services (SS)

The SS entity contains the Layer 3 SS entity necessary to implement Supplementary Services.

It implements the following Supplementary Services:

- Call Forwarding Unconditional (CFU)
- Call Forwarding on Subscriber Busy (CFB)
- Call Forwarding on No Reply (CFNRy)

- Call Fwd. on Subscriber Not Reachable (CFNRc)
- Barring of All Outgoing Calls (BAOC)
- Barring of Outgoing International Calls (BOIC)
- BOIC except calls to Home Country (BOIC-exHC)
- Barring of All International Calls (BAIC)
- Barring of Incoming Calls when Roaming (BIC-Roam)
- Number Identification SS
- Call Hold and Retrieve SS
- Call Waiting SS
- Call Offering SS
- Call Deflection
- Explicit Call Transfer

3.12.5.3 Multi-party SS

- Community of Interest SS
- Advice of Charge SS
- Unstructured SS

The following services are available as options, according to NRE consideration:

- Completion of Call services
- Group Calls

3.12.5.4 SMS

The SMS entity implements the full Short Message Service including reception of Mobile Terminated (point-to-point) messages, and cell broadcast messages and transmission of Mobile Originated messages. Supports concatenation of messages and PDU mode.

3.12.5.5 GPRS Short Message Service (GSMS)

All SMS features and functionality are also available over GPRS. This includes 7-bit compressed text, binary data, PDU mode and concatenation of messages.

3.13 MN Layer

The Mobile-Network Layer is the interface between the MMI and Layer 3. It communicates with the CM sub-layers CC, SS, SMS.

3.14 REG

REG is responsible for PLMN selection. It maintains lists of PLMNs and their capabilities allowing either the user or REG itself to make appropriate selections.

3.15 Session Management (SM)

- Controls the activation, deactivation and modification of PDP Contexts; there is a maximum of 11 PDP contexts
- Allows user to set minimum acceptable QoS
- Handles the notification of PDU sequence numbers to SNDCP (in the case of an inter-SGSN Routing Area Update)
- Handles processing error notifications from SNDCP

3.16 Logical Link Control (LLC)

- Provides a highly reliable logical link between the MS and the SGSN
- Supports both acknowledged and unacknowledged data transfers

- Supports variable-length information frames
- Provides flow control
- Allows information transfer with different service criteria, such that high-priority data transfers may take precedence over lower-priority transfers.
- Provides user data and identity confidentiality by means of a ciphering function.

3.17 Sub-Network Dependent Convergence Protocol (SNDCP)

- Multiplexing of N-PDUs from one or several PDPs onto the appropriate LLC connection
- Establishment, re-establishment and release of acknowledged LLC connections
- User data compression/decompression
- Protocol header compression/decompression
- PDU segmentation/re-assembly

3.18 Supplementary Services (SS)

The SS entity contains the Layer 3 SS entity necessary to implement Supplementary Services.

It implements the following Supplementary Services:

- Call Forwarding Unconditional (CFU)
- Call Forwarding on Subscriber Busy (CFB)
- Call Forwarding on No Reply (CFNRy)
- Call Fwd. on Subscriber Not Reachable (CFNRc)
- Barring of All Outgoing Calls (BAOC)
- Barring of Outgoing International Calls (BOIC)
- BOIC except calls to Home Country (BOIC-exHC)
- Barring of All International Calls (BAIC)
- Barring of Incoming Calls when Roaming (BIC-Roam)
- Number Identification SS
- Call Hold and Retrieve SS
- Call Waiting SS
- Call Offering SS
- Call Deflection
- Explicit Call Transfer

3.18.1 Multi-party SS

- Community of Interest SS
- Advice of Charge SS
- Unstructured SS

The following services are available as options, according to NRE consideration:

- Group Calls
- Completion of Call services

3.19 AT command Interpreter

The AT command interpreter supports all the mandatory commands required by 27.007 and 27.005 as well as a backwards compatible standard modem command set as defined in v25.ter.

CCww also supplies an enhanced set of AT-commands not covered by the standard.

The AT-command interface is compatible with Microsoft Windows Mobile RIL and is tested to Microsoft Logo requirements. Ports to other application O/S would be undertaken on request.

3.20 SIM Interface

The SIM Interface module will work with Phase 1, and Phase 2 SIM cards. The SIM Interface conforms to specifications 02.17 and 11.11.

4 Development, Regression Test, & Analysis Environment

An outline of CCww's development, regression test and analysis environment is provided in the following sections.

4.1 Development Tools and Process

The outline development process is:

- Software is coded in ANSI C, and tested in isolation (unit test) as far as possible ahead of integration
- Existing host tests are modified or additional host tests are created as appropriate
- There is thorough testing at each stage of integration
    - host environment of L2/L3 subsystem using in-house tests and tools
- using jHAT graphical analysis tool
    - on pre-production and production platforms (e.g. STAR-Let modem module and derived TracSure™ products, using CMU200, CRTU-G and other commercial test equipment
- using jHAT graphical analysis tool
– on customer & partner evaluation boards, CCasia reference designs, customer prototype handsets
    - full GCF/PTCRB conformance (Apr '08 and Dec 09), IOT, and field trials
- using jHAT graphical analysis tool to additionally manage live test session on partner and customer platforms
- All released code is automatically tested overnight and discrepancies are summarised and reported to the appropriate engineering team (regression testing)

The main software tools used during the development process are:

- Sunsoft Forte tools are used for configuration management, version management and build state control.
- jhat tool (part of the CCww in-house created environment) is used for protocol stack trace and debug on the host, target and in field trials
- ARM and Greenhills compilers, debuggers and ICE
- Purify

For internal testing on development boards, the CCww uses amongst other the following equipment:

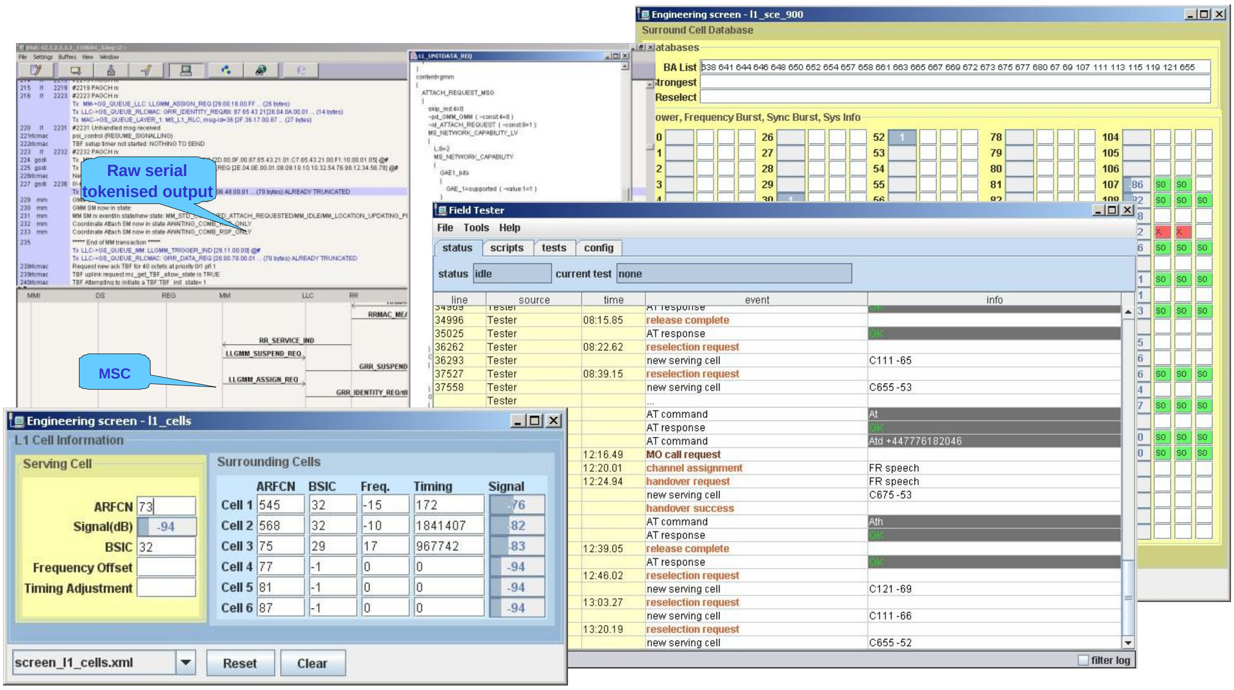
- Basic RF test equipment (spectrum analyzers, signal generators, etc.)
- R&S CRTU-G with 3GPP test suites (CCww)
- R&S CMU-200
- Internally developed software, e.g. protocol stack logging/data analysis tools (jHat)
- Other common laboratory test equipment (e.g. logic analyzers, digital storage 'scope, etc.)

4.2 Graphical Hardware Analysis Tool (jHAT)

CCww has developed a graphical tool (jHAT) that provides a visual and highly productive environment for training, support and development/debug for host, target and field environments. It may be used for:

- Display of host environment execution
- Display and control of target environment execution
- Display and control of field trials, including post-trial analysis
- System integration bring-up (for initial system bring-up of L1 with development hardware)
- The Layer 1 can be exercised manually by injection of primitives from jHAT in absence of L2/3 (system bring-up); system behaviour can be easily viewed / verified

Typical jHAT displays are shown below:



Engineering screen - l1_sce_900

BA List 338 641 644 646 648 650 652 654 657 658 661 663 665 667 669 672 673 675 677 680 67 69 107 111 113 115 119 121 655

Field Tester

status idle current test none

line	source	time	event	info
34996	Tester	08:15.85	release complete	
35025	Tester		AT response	OK
36262	Tester	08:22.62	reselection request	
36293	Tester		new serving cell	C111 -65
37527	Tester	08:39.15	reselection request	
37558	Tester		new serving cell	C655 -53
	Tester		...	
			AT command	At
			AT response	OK
			AT command	Atd +447776182046
		12:16.49	MO call request	
		12:20.01	channel assignment	FR speech
		12:24.94	handover request	FR speech
			new serving cell	C675 -53
			handover success	
			AT command	Ath
			AT response	OK
		12:39.05	release complete	
			AT response	OK
		12:46.02	reselection request	
			new serving cell	C121 -69
		13:03.27	reselection request	
			new serving cell	C111 -66
		13:20.19	reselection request	
			new serving cell	C655 -52

Engineering screen - l1_cells

L1 Cell Information

Serving Cell

ARFCN	73
Signal(dB)	-94
BSIC	32
Frequency Offset	
Timing Adjustment	

Surrounding Cells

	ARFCN	BSIC	Freq.	Timing	Signal
Cell 1	545	32	-15	172	-76
Cell 2	568	32	-10	1841407	-82
Cell 3	75	29	17	967742	-83
Cell 4	77	-1	0	0	-94
Cell 5	81	-1	0	0	-94
Cell 6	87	-1	0	0	-94

screen_l1_cells.xml ▼ Reset Clear

Typical jHAT displays

Features:

- Message sequence chart creation
- Hex, ASCII decodes of all messages
- Multiple engineering screens (user-definable), incl ‘top-6’ base-stations, surrounding-cell engine diagnostics, display received signal strength, synchronisation information
- Injection of commands, e.g. for L1 bring-up or to initiate high-level behaviour
- DIAG interface
- Real time or saved-log review
- De-tokenises raw data from target serial port or host socket
- Log searching & filtering
- Diagnostic control – real-time selection of stack ‘area’ for further detail analysis
- Field trial automation: allows a sequence of test commands to be injected to simplify trials operation; scenarios may be prepared in advance for reliable and repeatable testing world-wide.