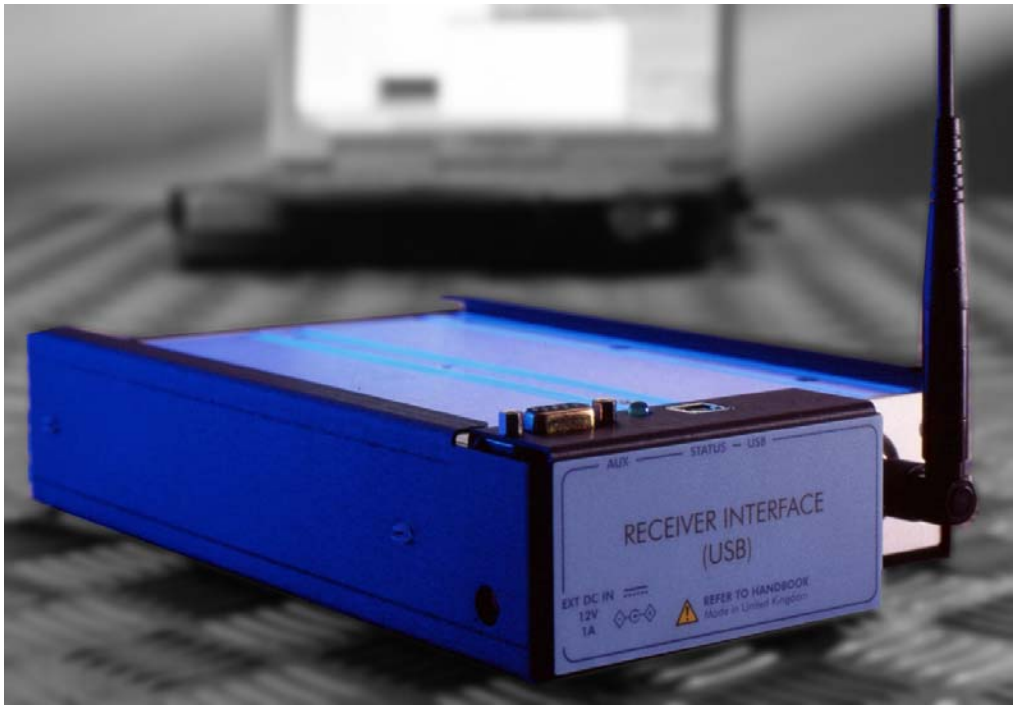
GSM Air Interface Protocol Analyser



Overview

The Smith Myers GSM Air Interface Protocol Analyser enables an engineer to view the information exchange between a cell site base station and a mobile device and to use this to investigate problems with the system configuration.

The equipment will be of use to:

- System Designers
- System Installers
- System Maintainers
- Equipment Designers

The equipment is available for operation on either 900/1800MHz or 850/1900MHz GSM bands. The use of two independent receivers means that it is possible to receive signals from both the uplink and downlink simultaneously which gives the operator the ability to decode and display the full air interface protocol.

The equipment offers the following functionality.

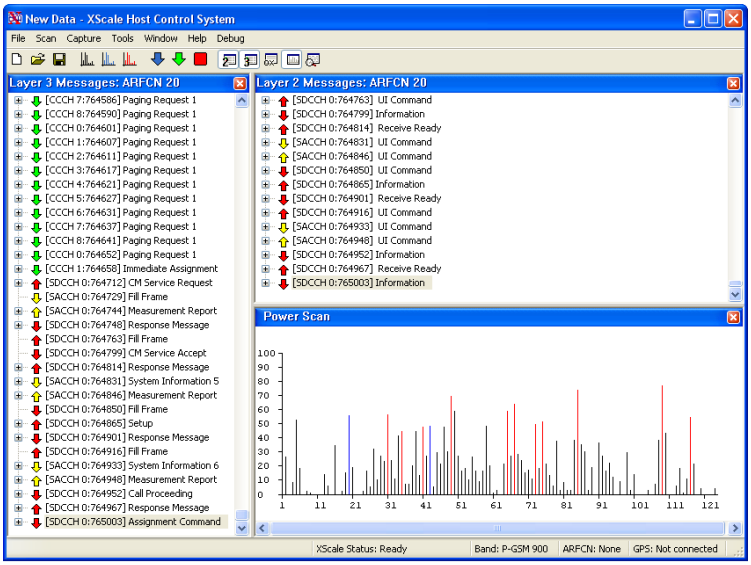
- Determination of the active cell sites in a given operating area
- Measurement of RSSI of a particular site
- Decoding of cell site configuration from broadcast control channels
- Monitoring of mobile registration, call set-up, handover and call completion.
- Logging of data for later analysis

smith myers

Omega Centre
Stratton Business Park
Biggleswade
Beds, SG18 8QB
United Kingdom

Product Description

The equipment features a dual GSM receiver that enables the recovery of the air interface protocol simultaneously from both the uplink and the downlink. The hardware is compatible with the full range of Smith Myers mounting racks enabling multiple units to be used together, driven by a single PC, to analyse the protocol on more than one GSM frequency pair. It has the ability to follow a call from a control channel to a traffic channel and to analyze the protocol of the complete call transaction.

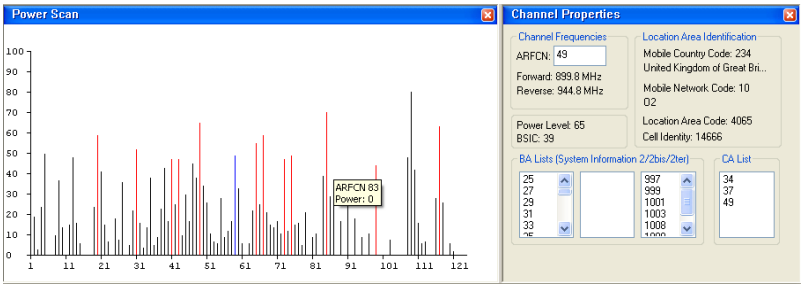


One or more units will interface to a host PC using the industry standard USB interface. This enables them to operate with any modern PC or with a laptop computer for use in the field. There is no need for a dedicated terminal or interface card to enable full use to be made of the functionality of the equipment.

The user interface provides several ways to view the captured data with links between the different views. This enables the equipment to be used by different users who can individually configure it based on their own requirements. Captured data can be saved for subsequent analysis.

Base Station Information

Without reference to a mobile the equipment is able to perform a scan of available GSM channels and present a list of available control channels. These control channels form the starting point for all GSM protocol analysis and are the basis for user selection of an operating frequency. With multiple units more than one frequency can be monitored at the same time.



The equipment can read information being broadcast on the selected control channel. This enables remote access to cell site configuration information. Indeed, it permits access to the information actually being received by mobile devices registered to the network.

Information available from this mode includes:

- Base Station Identification Code (BSIC)
- Cell Identity
- Cell Channel Description
- Neighbour Cell Description
- Location Area Identification

Off-Air Decode

The equipment can be configured to decode GSM channels received on the air-interface. This may be just the BCCH or CCCH channels or there is the option to follow calls to the SDCCH and traffic channels. It supports both cyclical and pseudo-random hopping to enable it to continue to follow a mobile on a system that implements these features.

The use of more than one GSM module in a system allows for the continued monitoring of the common control channels while following one or more mobiles to their respective traffic channels.

Layer 3

The GSM system employs a number of control channels for the transmission of system management data. The system will extract these channels and display them together with information on which time slot they occupy. These control channels include:

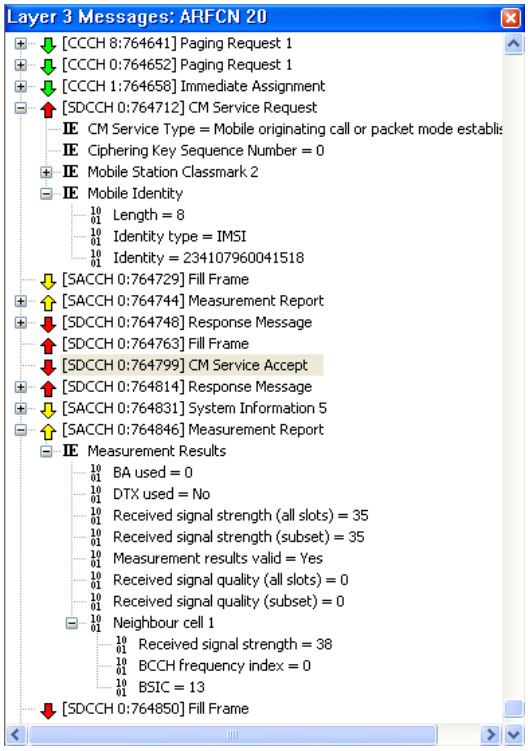
Broadcast Control Channel

Common Control Channels

- RACH
- PCH Paging Channel
- AGCH Access Grant Channel

Dedicated Control Channels

- SDCCH Standalone Dedicated Control Channel
- SACCH Slow Associated control Channel
- FACCH Fast Access Control Channel

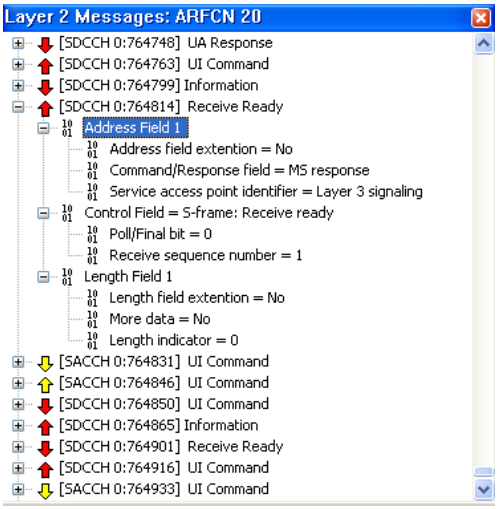


Detailed analysis of the layer 3 data is possible with successive breakdown of the received data to reveal the underlying structure of the transmission down to individual GSM information elements.

Layer 2

The layer 2 display provides a complete breakdown of layer 2 communications. This includes the following information:

- Frame Number
- Link Direction
- Sub-channel
- Address
- Frame Type
- Send and receive sequence numbers
- Length indicators
- Layer 3 Information



The fine detail which can be achieved allows a user to develop a thorough understanding of the underlying protocol and to use this to diagnose faults in the design or deployment of network elements.

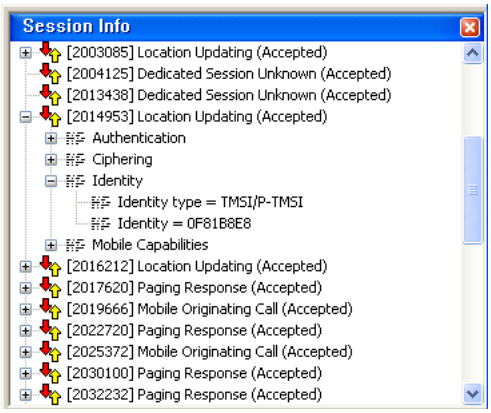
Layer 3 and Layer 2 windows can be synchronised to facilitate easy switching between the two displays.

Session and Identity Logging

At a higher level than the layer 3 protocol the equipment provides an easy overview of the activity on a cellular base station. Each time an SDCCH channel is assigned to a mobile an activity event is created that provides a basic overview of the transaction. Using this an engineer can easily get a broad overview of the traffic on a given channel.

This can also be used to provide easy navigation through the layer 2 and layer 3 windows.

A log can be created of the identity (either IMSI or TMSI) of the phones involved. This information can be extracted from the individual sessions or from paging messages transmitted on the paging channel.



Filtering

A range of easy filtering options are provided allowing the easy isolation of a particular procedure within a large quantity of captured data. With appropriate application of channel filters and selection of procedures a user can rapidly isolate that part of the interface that is of most interest.

Post-capture filtering of data can be applied by channel type or specific messages. Filtering on the session log allows filtering by mobile identity to isolate communications with a target mobile.

Encryption

The equipment supports both A5/1 and A5/2 encryption when used with a test SIM. This allows analysis of call procedures beyond the point where the network normally begins to encrypt transmitted data. If a compatible phone or module is interfaced with the equipment then this functionality becomes available on a live network.

Drive Testing

And finally, because the GSM Protocol Analyzer is capable of rapidly switching between channels under software control it can be used as a sophisticated drive test system. Base station signal levels can be logged together with location information for multiple cell sites. Additional cell site information can be logged if required. This gives the equipment capabilities surpassing those available with conventional mobile phone based drive test systems. The derived data can be post-processed to provide detailed coverage maps for the surveyed area and to show the extent of network coverage for both client and competitive networks.

Contact

In the UK

Smith Myers
Omega Centre,
Stratton Business Park
Biggleswade
Beds, SG18 8QB

Tel + 44 1767 601144
Fax + 44 1767 601180

info@smithmyers.com
www.smithmyers.com

In the USA

Smith Myers USA
1418 Norman St, Suite #11 NE
Palm Bay,
Florida, 32907

Tel 1-800-345-9993
Fax (321)-726-8315