The CERN GSM monitoring system

Carlos Ghabrous
CERN IT department
Route de Meyrin
1211, Geneva-23
Switzerland

Carlos.ghabrous@cern.ch

Abstract. This paper presents the way CERN has approached the problem of monitoring its own GSM infrastructure, especially in the Large Hadron Collider (LHC) accelerator tunnel and other underground facilities, where a leaky feeder cable carries mobile phone signals, and where this technology is the only means for inter-personnel communications.

1. Introduction
In the last decade, the tremendous development of mobile phone services based on the GSM standard has lead many organizations to rely on this new communication technology. As for all IT services, the necessity of monitoring these GSM services has become critical for organizations in order to be able to react appropriately in case of incident.

Even though mobile operators have their own monitoring systems, they do not take into account corporate constraints that, in case of CERN’s GSM network become important due to its specificity. Moreover it is also necessary to independently evaluate an operators’ performance against a service level agreement. After an extensive market survey showed that commercial solutions were not yet mature, the Telecommunication Team decided to develop its own monitoring system. This was done in collaboration with Fastlay, a Swiss company specialized in the design of electronic devices and with the GSM engineers from Swisscom, the Swiss historical telecommunication operator.

1.1. Specificity of CERN’s GSM mobile network
Since 1991 CERN has subcontracted national mobile operators for the installation and maintenance of a GSM network covering all its sites in France and Switzerland. At CERN’s request, the mobile operator implemented a private network offering advanced services to CERN users such as short dialing plan, different roaming classes, flat rate subscriptions, mobile data services (GPRS/EDGE/3G), email to SMS service, etc. Today, with more than 4000 GSM users (CERN staff, external institutes, sub-contractors, etc.), GSM has become one of the most effective ways to communicate at CERN. In addition to all these features, the Telecommunication Team has installed more than 50 km of leaky feeder cable, especially used in tunnel environments, to propagate GSM frequencies in all underground facilities (Experiments, LHC tunnel, PS, SPS, etc.). This leaky feeder cable infrastructure is also used to propagate VHF band radio signals for the CERN fire brigade.
1.2. Necessity of monitoring the CERN GSM mobile network

Even if our mobile operator is monitoring the active equipment of the GSM network, it was not possible to guarantee the availability of GSM services where signals are carried by the leaky feeder cables. A portion of cable can be damaged for whatever reason (cut, pinch, faulty FQ combiner, faulty connector…) degrading the propagation of GSM signals. In addition, we have yet to gain experience to know how many years this infrastructure will survive during LHC operation and how the service will degrade. Given that the fire brigade VHF network also relies on it, it became obvious that to monitor it is essential to be able to inform CERN users in case of incident.

2. Materials and methods

Three main components make up the monitoring system: GSM probes, a central server and a master probe, here called super master. GSM probes, placed in strategic places, send regularly to the central server measures of the GSM signals power. Data is sent over UDP protocol using the GPRS network of our mobile operator. The central server analyzes the received data and determines if there is an alarm by comparing measurements with predefined thresholds. In case of alarm, the server uses the master probe or Supermaster attached to it to close an electric contact, generating an alarm to the CERN Control Center (CCC). The CCC operators can then call the Telecommunication technician on duty, which will undertake appropriate actions. In case of a problem with the GPRS or UDP connection, probes can still send measurements in SMS format to the master probe, which forwards them to the central server. Nevertheless, this “safe mode” takes more time to collect all information from probes. To complete the loop, the central server and the master probe are cross monitoring themselves, and are able to launch an alarm to the CCC in case of failure.

As part of the system, five mobile telephones can be configured in the probes, to allow users of these devices to perform various actions, such as configuring the probes remotely, test their status or simply read their current configuration. For security reasons, three predefined categories of privileges allow granting different level of rights to each mobile telephone.
2.1. GSM probes

The main function of the probe is to measure locally the power of all signals transmitted by a specific mobile operator in the GSM 900 MHz and DCS 1800 MHz bands. The probes can also monitor the room temperature. All measurements performed by probes are transmitted periodically to a central server via GPRS (UDP protocol) or SMS messages (in safe mode). The frequency UDP and SMS messages are sent to the server or master probe is configurable. The current configuration makes probes to send one UDP message every 120 seconds, and a SMS message every 220 seconds.

The physically, GSM probes, or GSP (GSM Supervisor Point) are electronic devices which consist on one GSM/GPRS modem, which is the radio interface towards the mobile network; one SIM card, which allows the modem to join the operator's mobile network; one microcontroller, which controls all the actions performed by the probe by executing the instructions written in the probe's operating system. There is also one Watchdog device, which assures the system restart in case of a problem. The configuration of the probe is registered in a flash EEPROM memory. The probes' software can be flashed over the air and remotely configured. The probes also include a DC/DC converter coupled to a battery and a charger to maintain remote monitoring in case of local power outage up to four hours autonomy. The internal powering unit is regularly auto tested by the probe which can report any problem with the battery, charger or local power supply. Probes being placed in hostile environment (dust, humidity, temperature, magnetic fields, etc.), the external envelop is made of metal with galvanic isolation (protection up to 1000 volts) and is waterproof.

2.2. Central server

Connected to the CERN intranet, the central server collects measurements sent by probes. A web application allows administrators to easily monitor the mobile network status and configure the remote probes. For each probe, the administrator can configure which channels he wants to monitor and, for each one of them, a threshold to activate an alarm. A server can monitor up to 60 probes.

In the current system's configuration, the server is a general purpose computer with CERN's Linux version running on it (SLC4). The application can also be installed on Windows-based computers.

2.3. Master probe (super master)

The master probe, or super master, is the interface that allows the central server to send alarms to a CCC by opening relay contacts. It is also the interface that will be used for receiving measurements from probes in safe mode (GPRS or servers' network interface not operational). The master probe is attached to its server via a serial link. In case of communication failure on this serial link, the master probe generates an alarm to the CCC.

2.4. Monitoring the leaky feeder infrastructure

In CERN's underground facilities, GSM signals are carried over leaky feeder cables directly attached to the GSM base station of the mobile operator. This leaky feeder cable acts as a long antenna allowing propagating “clear” signals in enclosed areas. This infrastructure is also used in the same way to propagate VHF signals from radio relays. GSM and VHF signals are injected in the leaky feeder cables using frequency combiners.

A probe (see Fig.2) is placed close to each GSM base station to monitor the local channels. Another one is placed at the far end of a leaky feeder cable segment to monitor the same channels. If the second probe detects a frequency propagation problem (see Fig.3), provided the first one does not, we can deduce that the segment of leaky feeder cable is not working properly. Even though probes cannot monitor VHF band signals, as VHF band signals are much less sensitive to the variations of leaky feeder cable propagation...
(VHF frequencies operates in the 150 MHz band), one can deduce that these signals are being transmitted properly if GSM signals do.

![Leaky feeder monitoring principle](image1)

Fig 2. Leaky feeder monitoring principle

![Probe detecting a problem](image2)

Fig 3. Probe detecting a problem

3. Results
The monitoring system, along with the monitoring principle, allows not only to monitor the current state of the GSM network, but also the behavior of the leaky feeder cable infrastructure over time, which can be useful to gain experience to know how many years this infrastructure will survive during LHC operation and how the service may be degraded.

The application was designed to simplify the maintenance for administrators using remote configuration tools, software upgrade over the air and remote monitoring tools. In addition, using the special mobile phones, field technicians don’t need a computer to take control over a probe, simplifying thus installation and replacement processes.

Finally, the server and probes are also monitored in the network management server (SNMP platform) to relay alarms via IP to the computer centre.
4. Conclusions
The GSM monitoring system is operational since more than one year in LHC, PS, and SPS facilities. It can monitor the availability of GSM frequencies, GPRS services, and indirectly VHF signals in these underground areas. New probes will be installed on surface to monitor the whole CERN GSM network. This innovative solution is a real success. It is now being proposed by Swisscom to their clients facing the same constraints as CERN.

References
[1] CERN (www.cern.ch)
[2] Eberspächer, Vögel, Bettstetter. GSM Switching, Services and Protocols (Wiley, 2005)