THE APPLICATION OF GPRS FOR SCADA COMMUNICATIONS

Eskom

Author & Presenter: D Gütschow M. Eng – Telecommunications Specialist
Industry Association Resource Centre, Eskom Holdings Limited

Executive Summary

Telecommunications technologies have rapidly advanced in recent years. One such new technology is GPRS (General Packet Radio Service) – a data transmission service implemented on public GSM networks. This paper discusses the possible application of GPRS technology for utility SCADA (Supervisory Control and Data Acquisition) communications. The paper firstly examines the key features of GPRS, followed by a discussion of some of the technical and financial aspects that need to be considered when designing a GPRS solution. Lastly, based on research and experience by Eskom, an architecture is proposed for a GPRS communications system.

1. Introduction

Eskom, like many other electricity utilities around the world, has invested in its own private mobile radio network for SCADA (Supervisory Control and Data Acquisition) communications. Benefits of this traditional technology include the ability to communicate on a point-to-multipoint basis over non line-of-sight paths, low terminal costs, and reasonably high reliability. Its disadvantages however, include low channel capacity and low data rates [1].

Over the last decade Eskom has installed several thousand new RTUs (Remote Terminal Units) and integrated auto-reclosers to monitor and control its power network. As a result data traffic over the radio network has increased dramatically. The combination of high traffic volumes and limited channel capacity has led to an increase in the occurrence of channel congestion, reduced data throughput, and degraded performance of the SCADA system. To address these concerns Eskom embarked on several research initiatives to identify suitable alternative telecommunications technologies.

Presently, one of the most promising new technologies is GPRS (General Packet Radio Service). This paper highlights some of the findings of Eskom's research into GPRS [2]. It firstly investigates the key features of GPRS technology and then discusses some of the technical and financial factors that need to be considered when planning to implement a GPRS solution. The paper also discusses a proposed architecture for a GPRS communication system, before finally drawing a conclusion about the merits of using GPRS for SCADA.

2. GPRS Technology

GPRS is a packet-switched data service that was first implemented on South African GSM networks in October 2002 to supplement other existing methods of data transfer such as Circuit Switched Data (CSD) and Short Message Service (SMS) [3]. It is classified as a 2.5G technology, because it bridges the gap between traditional 2G networks with slow data speeds, and new 3G networks with high data speeds.

2.1 GPRS features

GPRS has a number of key features, the majority of which make it an attractive and promising proposition for SCADA communications. These include:

2.1.1 Data speed

GPRS is often marketed as being capable of supporting data rates up to 171.2 kbps. However, this assumes that all eight GSM timeslots or channels are used and that no error correction is required. In reality this is rarely the case. Most GSM networks only allocate between 1 and 4 timeslots for GPRS traffic depending on the requirement for voice traffic [4], [5], [6]. Furthermore, depending on radio conditions, one of four coding schemes will always be in use for error correction. Therefore the raw data rates available for SCADA will vary between 9.0 kbps and 57.6 kbps, with an average of approximately 20 – 30 kbps.

2.1.2 Immediacy

GPRS is regarded as “always on”, because it facilitates almost instant connections for data transmission as the need arises. No dial-up modem connections are necessary. The initial turnaround delay when establishing a new GPRS session is estimated to be between 4.5 – 8.5 seconds [6], which is acceptable for most unsolicited report-by-exception SCADA applications.

2.1.3 Robust connectivity

GPRS supports robust connectivity and data transmission integrity through mechanisms of coding redundancy and error detection. Up to four different coding schemes (CS1 – CS4) can be used depending on the quality of the radio connection. In addition GPRS also supports selective retransmission of packets when errors are detected in received frames [3].

2.1.4 Security

GPRS utilises the proven authentication and security features of GSM technology [3]. This includes:

- Encryption over the wireless air interface
- Security inherent in the core GSM network
- Authentication by means of information contained in the Subscriber Identity Module (SIM) and information stored on the Home Location Register (HLR) node in the GSM network

Additional authentication can also be achieved by means of the RADIUS (Remote Authentication Dial-In User Services) server, which is discussed later.

2.1.5 Usage based billing

GPRS is billed based on the volume of data transmitted (per Mbyte) rather than the amount of time connected. Initially, when GPRS was launched in South Africa, it was charged at R50 / Mbyte. However, since then tariffs have reduced drastically and currently South Africa’s GPRS rates are amongst the lowest in the world at between R0.49 and R2.00 per Mbyte [7]. Usage based billing is cost-effective for short bursts of data at irregular intervals, and therefore preferred for unsolicited report-by-exception SCADA communications.

2.1.6 Packet switching

GPRS transmits data by means of packet switching and the Internet Protocol (IP). This means that data is split into separate but related IP packets before being transmitted, and again reassembled at the receiving end. Packet switching has the following three main advantages:

- A temporary loss of the radio signal will not cause a disconnection and loss of data
- Multiple GPRS users can concurrently share the same available GSM resources
- Automatic rerouting of data whenever a particular transmission path or network node is unavailable

The disadvantage of packet-switching is that data transmission delays (i.e. data latency) are not constant, but variable.

2.1.7 Data latency

Data latency, or the time taken for data to arrive at its destination, is inherent to packet-switched networks. With GPRS data latency is influenced by the delay of the mobile terminal to request a connection, the delay in establishing the up- and downlink radio connections, over-the-air delays (which are influenced by the packet size and number of retransmissions), and lastly delays introduced by traffic routers in the core GPRS network [8]. Once the necessary radio resources have been allocated to a GPRS session, the typical round-trip data latency for ongoing data transmissions is expected to between 0.5 and 1.5 seconds [9], [10]. Due to the latency variability, GPRS is better suited for unsolicited report-by-exception SCADA communications, than for polled report-by-exception communications.

2.1.8 Geographical coverage

The South African cellular networks claim that GSM/GPRS coverage extends to 87% of

South Africa’s land surface. This includes 100% of all national roads, 95% of all towns and 95% of the total population [7]. However, power lines and substations are often located in low lying areas away from human populations and major roads where there is no GSM/GPRS coverage. Although generally radio links could be engineered to improve GPRS reception, it needs to be considered that GPRS may not be available at all locations. This is a potential limitation factor.

3. Applying GPRS Communications to SCADA

3.1 Technical Considerations

There are a number of technical factors that need to be considered before GPRS can be applied for SCADA:

3.1.1 Access Point Name (APN)

An Access Point Name (APN) is the point at which an external public network (such as the Internet), or private corporate network (for example a SCADA master station) connects to the GPRS network. In a SCADA application an APN effectively provides remote devices with a single number to which they connect to the SCADA master using the GPRS network. For large SCADA systems a private APN is recommended, because an Internet APN, although cheaper, involves unknown delays due to varying Internet contention ratios and queue lengths. Another important reason is that a private APN supports both static and dynamic IP addressing, whereas an Internet APN only supports dynamic address allocation (refer to 3.1.4). A utility can either elect to have its own private APN, or alternatively make use of a third party’s private APN.

3.1.2 Connection to the GPRS network

RTUs would typically connect to the GPRS network by means of GSM/GPRS modems that interface serially to each RTU. However, there are a number of different ways that a corporate network could connect to the GPRS network [2]. Assuming that a private APN is used, two methods of connection are suitable for the SCADA master station. This is summarised in Table 1.

Table 1: Suitable methods to connect the SCADA master station to the GPRS network.

Connection method	**Advantages**	**Disadvantages**
Single modem-to-modem connection (Connection by means of a standalone GPRS modem)	• Simplest configuration • Low set-up cost • No monthly connection fee	• High data latency • Limited traffic capacity • Possible disconnection during network upgrades
Direct leased line (Connection by means of a leased line, ≥ 64 kbps)	• High capacity for traffic • High data speeds • Secure connection	• Initial set-up costs • Monthly leased line rental

3.1.3 Internet Protocol (IP) support

GPRS is a packet-switched technology that communicates via TCP/IP – the *de facto* protocol standard for data networking. However, most SCADA equipment only supports traditional SCADA communication protocols such as DNP3, which are designed to operate over serial links with low and consistent delays. In most instances TCP/IP is not yet supported, because historically it has been considered unsuitable due to unpredictable transmission delays [11], [12]. Therefore, in order to use GPRS for SCADA, the challenge of interfacing to TCP/IP needs to be overcome.

Fortunately this can be achieved through protocol encapsulation, i.e. by appending TCP/IP headers to every SCADA protocol message. Encapsulation requires processing of the SCADA protocol’s data link layer, which could be performed by a software application running on the GPRS modem, or alternatively by an intermediary device. It is estimated that encapsulation would add approximately 50 bytes of overhead to every SCADA protocol message.

3.1.4 IP address allocation

Normally, when a mobile terminal initiates a new GPRS connection the terminal is assigned a dynamic IP address for the duration of the session. However, SCADA applications require that the SCADA master also initiate sessions, and that messages are correctly routed to the intended recipient. With GPRS this can only be achieved by means of static IP addresses. This requires having a private APN and VPN (Virtual Private Network) as well as a RADIUS server. While the APN and VPN ensure that the IP addresses are private, the RADIUS server performs authentication and assigns a unique IP address to each requesting MSISDN (Mobile Station Integrated Digital Services Network) number as determined by an address mapping table.

3.2 Financial Considerations

The three main categories of costs that relate to a GPRS system include (i) initial setup costs, (ii) monthly infrastructure rental and maintenance costs, and (iii) monthly data usage.

Initial setup costs and monthly infrastructure rental/maintenance is a function of the type of connection to the GPRS network, as well as whether a private APN or third party APN is used. Table 2 summarises some expected GPRS costs as published by South Africa's two largest GSM network providers: MTN [13] and Vodacom [14]. It also includes some assumptions about the cost of using a third party's APN and SCADA traffic volumes based on Eskom's experience [2].

Table 2: Typical costs and assumptions related to GPRS based on published tariffs

Cost Category	Setup costs	Monthly rental / maintenance
Own Private APN and supporting infrastructure / services (50 MSISDN numbers included)	R4,000	R3,000
Additional APN MSISDN number associations		R8.77 / MSISDN
APN connectivity to Corporate Application Server (64kbps)	R1,000	R2,000
RADIUS Server	R2,850	R3,800
Data Contract and monthly SIM card fee	R175 / SIM	R44 / SIM
64kbps leased line	R2,000	R2,000
GPRS traffic charges outside of any data bundles: R2.00 / Mbyte		
Assumptions		
3^{rd} party APN access per month: R30 / MSISDN		
Amount of DNP3 data transmitted by each RTU per day: 25 kbytes		

The information in Table 2 was used to calculate the average monthly operating cost per RTU for an unsolicited report-by-exception SCADA system. A single RADIUS server and GPRS network connection was assumed in each case (Dual-redundant connections and servers may be used to improve system reliability if required). The results shown in Figure 1 suggest that the initial cost difference between the various types of GPRS system configurations is quite large, but that this reduces as the number of RTUs increase. For SCADA systems with a large number of RTUs (≥ 2000) the monthly cost per RTU is expected to range between R62 and R83 depending on the particular type of configuration and connection used.

4. Proposed GPRS Architecture

Based on the above technical and financial considerations and Eskom's research, the GPRS architecture in Figure 2 is proposed. The system consists of the following key components:

4.1 GSM Communications Server

The GSM communications server is a standard PC that interfaces serially to the front-end processor of the SCADA master station. A software application enables it to function as a gateway by encapsulating all outgoing SCADA protocol (e.g. DNP3) messages in TCP/IP, and removing the encapsulation on all incoming messages. The destination IP address of each outgoing data transmission is obtained from a lookup table that contains a mapping of DNP3 to IP addresses. The GSM communications server also performs traffic monitoring and keeps a log of all data transactions.

4.2 Intelligent GPRS modems

The GPRS modems at each outstation are intelligent devices with embedded TCP/IP stacks. A software (e.g. J2ME) application encapsulates all outgoing DNP3 messages in TCP/IP, and removes the encapsulation from all incoming messages. The MSISDN of each modem is provisioned on the private APN so that no external modem or device can access the SCADA master station.

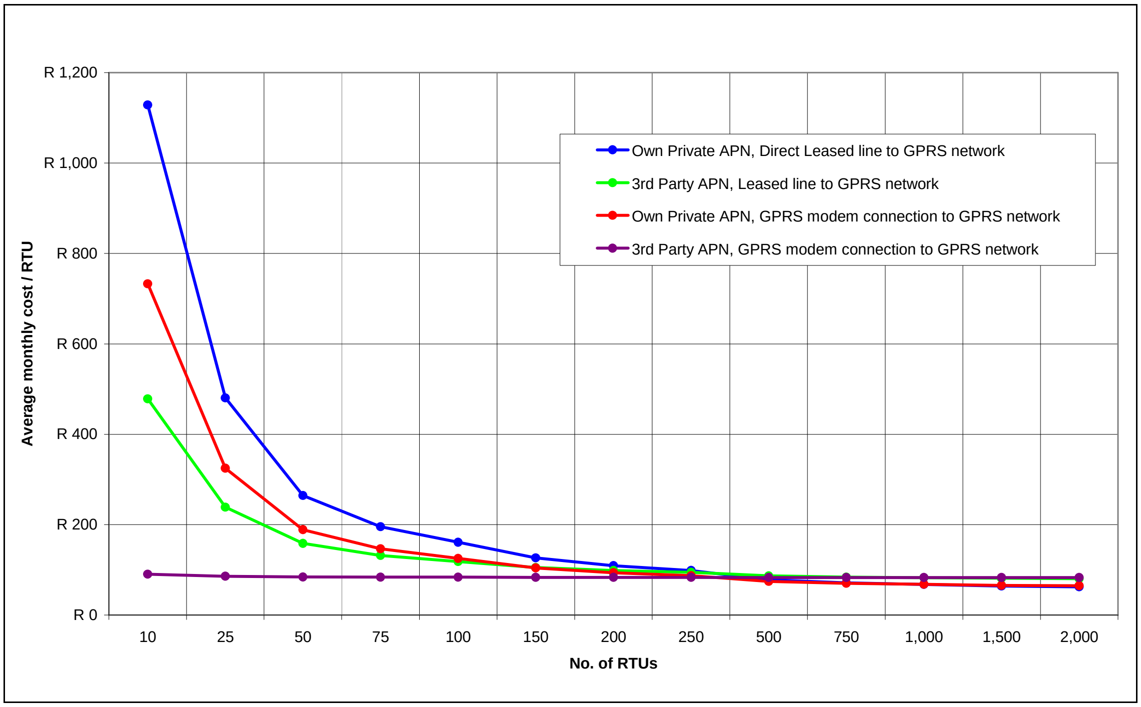

Figure 1: Projected monthly GPRS operating costs per RTU

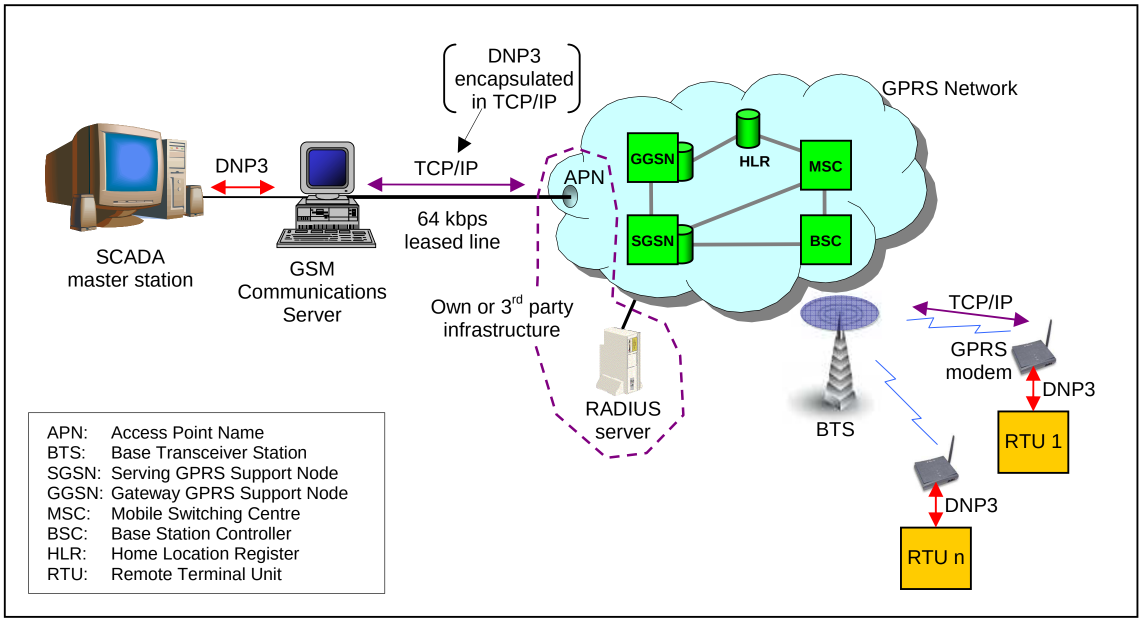
DNP3 encapsulated in TCP/IP
GPRS Network
DNP3
TCP/IP
APN
GGSN
HLR
MSC
SGSN
BSC
64 kbps leased line
SCADA master station
GSM Communications Server
Own or 3rd party infrastructure
RADIUS server
BTS
TCP/IP
GPRS modem
DNP3
RTU 1
DNP3
RTU n
APN: Access Point Name
BTS: Base Transceiver Station
SGSN: Serving GPRS Support Node
GGSN: Gateway GPRS Support Node
MSC: Mobile Switching Centre
BSC: Base Station Controller
HLR: Home Location Register
RTU: Remote Terminal Unit

Figure 2: Proposed GPRS architecture for SCADA

4.3 APN and RADIUS Server

Based on the cost analysis (Figure 1) it is more cost effective to use a value adding third party's APN and RADIUS server for SCADA systems that have less than 500 RTUs, compared to owning and maintaining oneself.

Additional benefits of using a third party's APN may typically include:

- Avoided capital outlay and setup costs
- Avoided monthly infrastructure maintenance costs
- Infrastructure redundancy

- Connectivity to APNs of more than one GSM network to ensure maximum geographical coverage
- Allocation and management of IP addresses
- Reliable IP authentication for additional security
- Real time monitoring for early fault detection and error correction

4.4 Projected performance and cost

Based on Eskom's experience with a pilot site, the expected performance of the proposed system is a session setup time of 4 – 7 seconds, and a round trip delay on subsequent transactions of between 1 – 2.5 seconds. Using a third party's APN, the total monthly cost per RTU is expected to be between R80 – R100. In Eskom's case this is in stark contrast with the total cost of owning a private mobile radio network, which is currently more than 10 times as much per RTU per month.

5. Conclusion

GPRS is a relatively new public telecommunications technology that has many features that make it suitable for SCADA applications. Its potential benefits for utilities include:

- Providing effective SCADA communications wherever there is GSM coverage
- Requires minimal investment in new infrastructure
- The same infrastructure can be utilised for other GPRS applications such mobile computing, remote metering, remote substation access and prepaid vending
- Low operating cost compared to other communications technologies [2]
- Involves little exposure to the risk of technology obsolescence
- Ensures readiness and compatibility for future GSM services such as EDGE and 3G [9]

The only possible risk associated with GPRS is that no quality of service guarantees are currently provided [8], and that possible future oversubscription of the GPRS service could result in unacceptable data latencies. However, the GSM network providers have a vested interest to ensure that the GSM networks always have sufficient capacity, and hence this risk is low.

Therefore, from a technical as well as financial viewpoint, GPRS is an attractive and viable means of communication for SCADA, and a suitable supplement and/or replacement for existing mobile radio technology. The South African financial and retail sectors have already embraced GPRS for real-time applications such as electronic funds transfer and credit card authorisations. The question is: will electricity utilities dare to follow and apply it for SCADA communications?

6. References

[1] D. J. Marihart, "Communications Technology Guidelines for EMS/SCADA Systems", in *IEEE Transactions on Power Delivery*, vol. 16, no. 2, April 2001, pp. 181 – 188.

[2] D. Gütschow, P. Tshabalala, "The application of GPRS for Intelligent Electronic Device (IED) Communications", Eskom research project PRJ04-00538400-2508, Report no. RES/RR/04/23255, April 2005.

[3] A. Sicher, R. Heaton, "GPRS technology overview", February 2002, Available online from www.dell.com/r&d

[4] MTN Network Solutions, Product Guide: Mobile Access Solutions

[5] N. M. Deshpande, J. Gilbert, "GPRS – How does it work and good is it?", Intel DeveloperUPDATEMagazine, October 2002, available online at www.intel.com/update/departments/wireless/wi10021.pdf

[6] R. Dettmer, "Mobilising Packet Data", *IEE review*, July 2001

[7] www.mtn.co.za

[8] www.cellular.co.za/gprs.htm

[9] www.source02.com/help/list_faqs_gprs.htm

[10] ETSI, "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); service description; Stage 1",

ETSI EN 301 113 V6.3.1, November 2000.

[11] K. Mak, B.L. Holland, B.L., "Migrating electrical power network SCADA systems to TCP/IP and Ethernet Networking", *Power Engineering Journal,* Volume 16, Issue 6, December 2002, pp. 305 – 311.

[12] M. Nordman, M. Lehtonen, J. Holmström, K. Ramstedt, P. Hämäläinen, "A TCP/IP based Communication Architecture for Distribution Network Operation and Control", Proceedings, 17th International Conference on Electricity Distribution (CIRED), Barcelona, May 2003, Session 3, Paper 44.

[13] MTN Network Solutions, "Product Guide: Mobile Access Solutions", April 2005.

[14] www.vodacom.co.za

Dieter Gütschow is a Chief Engineer with the Industry Association Resource Centre of Eskom. He obtained his Bachelor's degree in Electrical and Electronic Engineering from the University of Stellenbosch in 1995, and MEng (Distinction) in Engineering Management from the University of Pretoria in 2004.

He is currently responsible for the development of telecommunications strategies, standards and procedures and the co-ordination of telecommunications research for Eskom's Resources and Strategy Division. His areas of interests include utility telecommunications- and telecontrol technologies and systems, and power system automation.

Mr. Gütschow is a registered professional engineer; he is a member of South African Institute of Electrical Engineers (SAIEE), and a member of the IEEE.