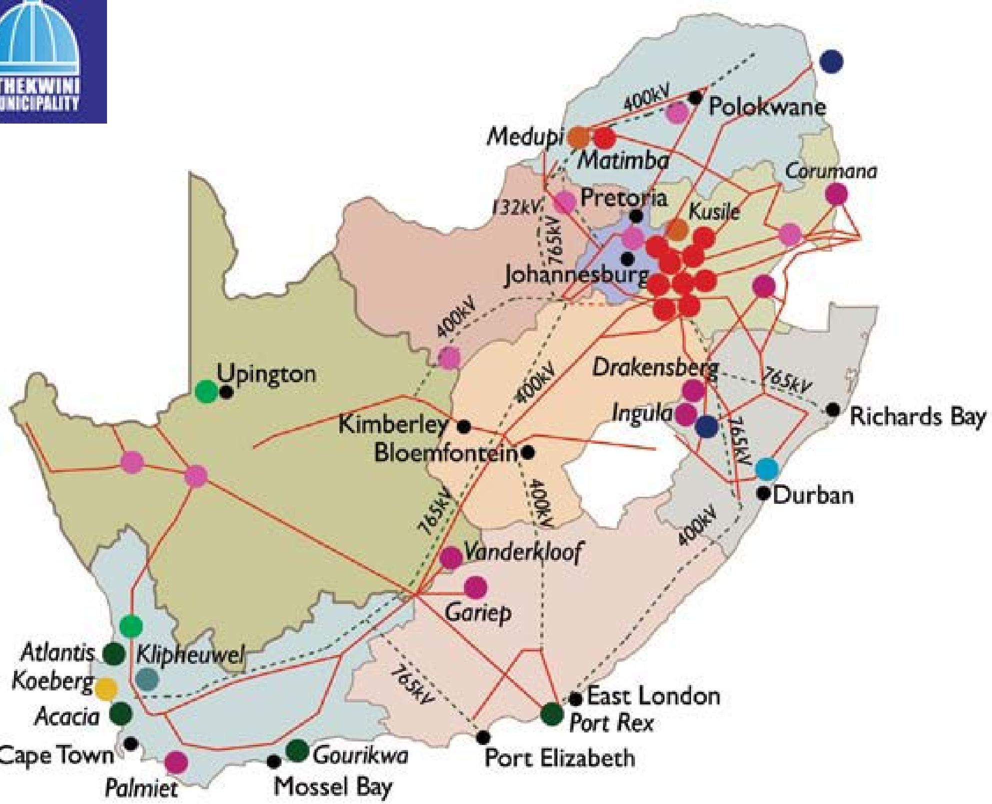
The use of Mobile Data Communications for SCADA Applications

by
Resham Singh
eThekwini Electricity
Durban, South Africa

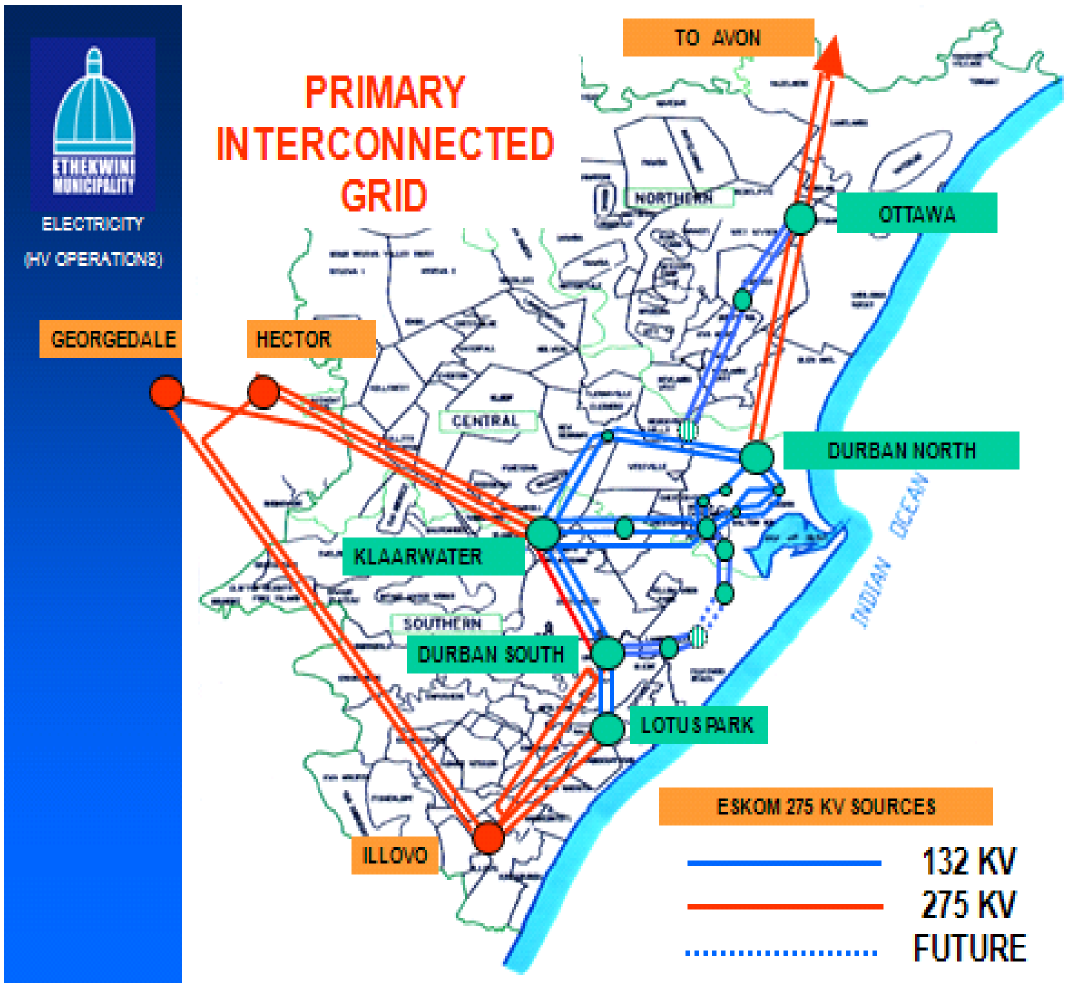
Contents

eThekwini Electricity : Introduction



- Municipal power utility of the city of Durban, on the east coast of South Africa
- 700 000 customer base
- Maximum demand of 1900 MVA
- Customer load 30% residential, 70% industrial/business
- Network covers from 275kV to 230V

eThekwini Electricity : SCADA



- ACS PRISM Master Station
- 110 HV RTUs (RTU560, D400, D20, ERTU)
- 400+ MV RTUs

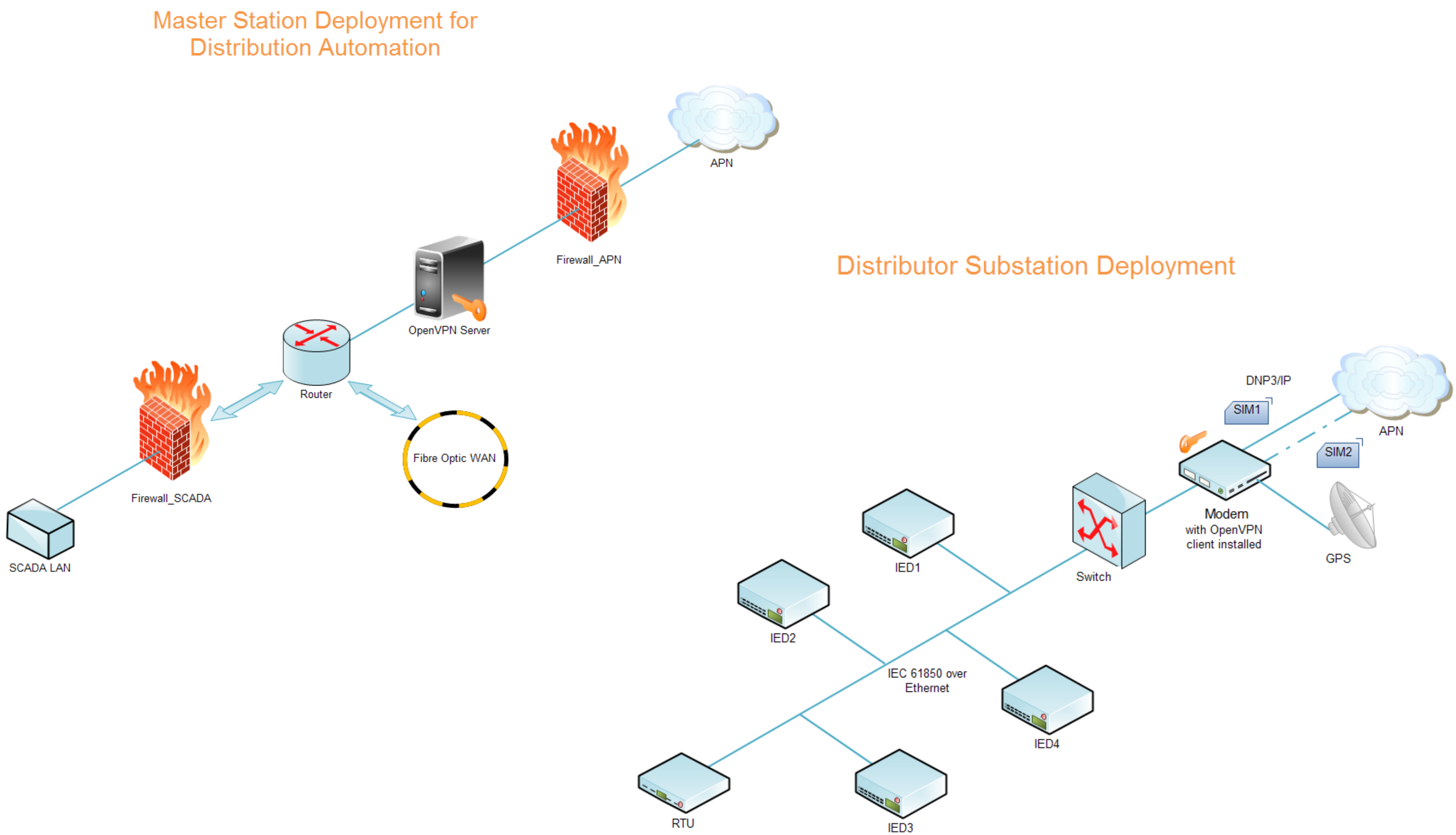
  (RTU540, BECKHOFF)
- 500+ 11kV distributor substations still require RTUs
- 250+ RMU (Talus T200)
- 150+ Nulec Reclosers to be added to SCADA network

Why use GPRS for SCADA?

"You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat."

Albert Einstein

GPRS SCADA Architecture



Performance

1. 3 Distributor Substations selected at geographically dispersed sites with 3G/GPRS modems installed
2. Traffic captured at the SCADA server
3. Analysis of data traffic for bandwidth usage, network latency, and data packet loss
4. Comparison between best performing 3G/GPRS link and a fibre link

Bandwidth Usage

1. Are GPRS speeds sufficient or do we need 3G speeds?
2. Let us investigate the data transmitted from our test sites

	ICC	100 Woodhurst	Zwelibomvu
Avg. packet/sec	0.015 (67)	0.014 (71)	0.010 (100)
Avg. packet size	96 bytes (768 bits)	99 bytes (792 bits)	101 bytes (808 bits)
Avg. bps	768 bps	792 bps	808 bps
Max data stream	2 packets totalling 11 160 bits	1 packet totalling 10 648 bits	1 packet totalling 7 032 bits
Max bps	~11 kbps	~11 kbps	~7 kbps

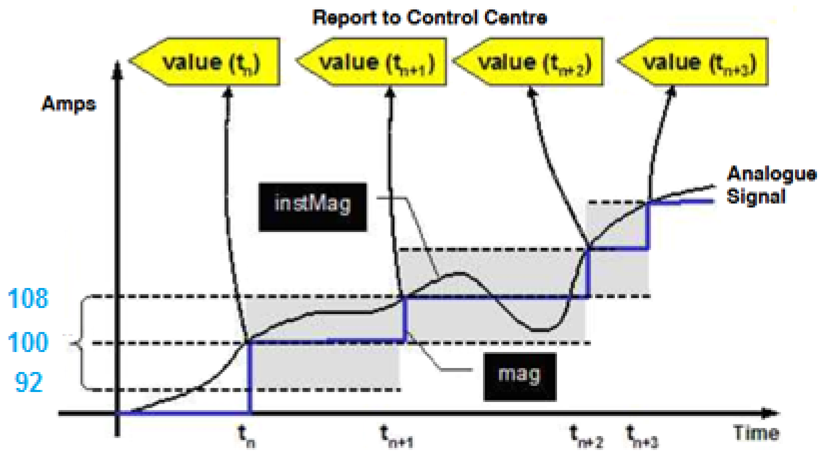
3. Typical speeds are ~14 kbps on the uplink. GPRS with CS-1 coding scheme delivers 8 kbps (worst case)
4. Therefore bandwidth is not an issue - GPRS speeds are sufficient
5. Be careful about trunk links – between APN and SCADA. This may cause a bottleneck. The size of this link should be a multiple of the max bit rate per substation.

Bandwidth Management

1. Controlling the alarming network is imperative as costs are incurred per transaction – consider a sustained period of 11 kbps

2. Manage digital inputs
   - Chatter detection and blocking

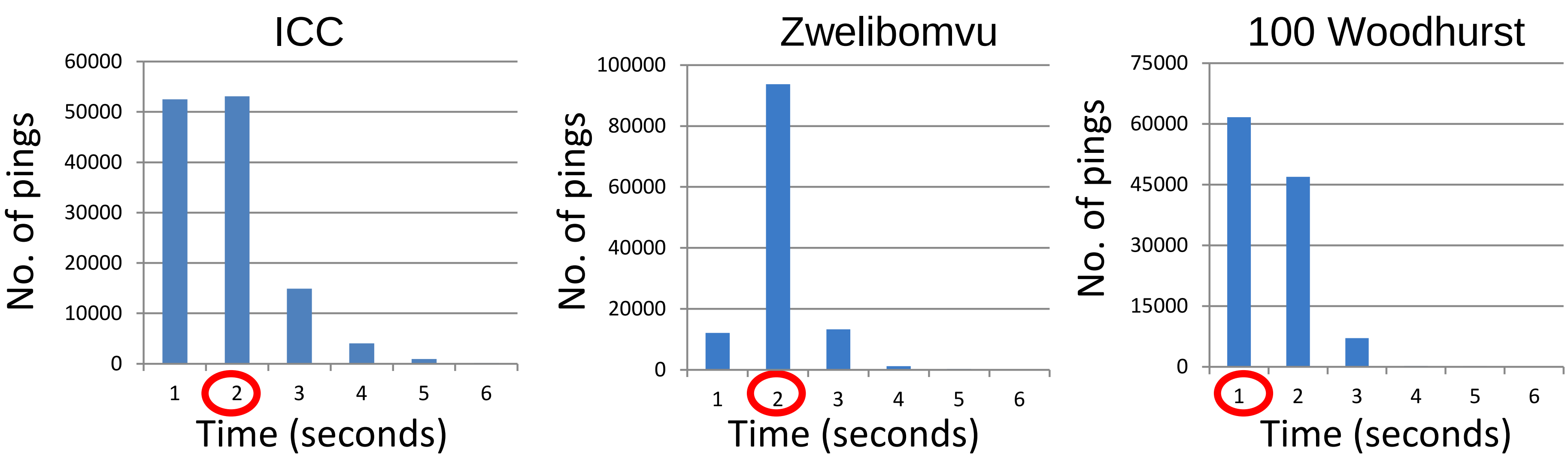
3. Manage analogue inputs
   - Threshold supervision
   - What significant change should an operator detect, 1A?



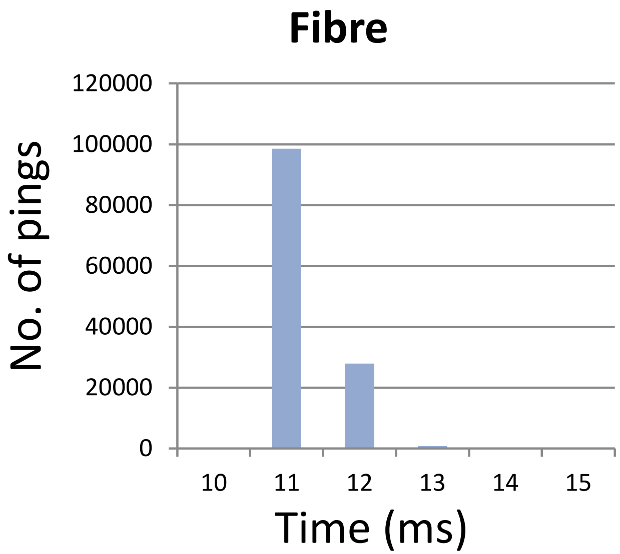
4. Mode of protocol operation
   - Solicited or unsolicited?
   - Read request = ~ 90 bytes every 10 secs = ~ 24 mB per month per substation

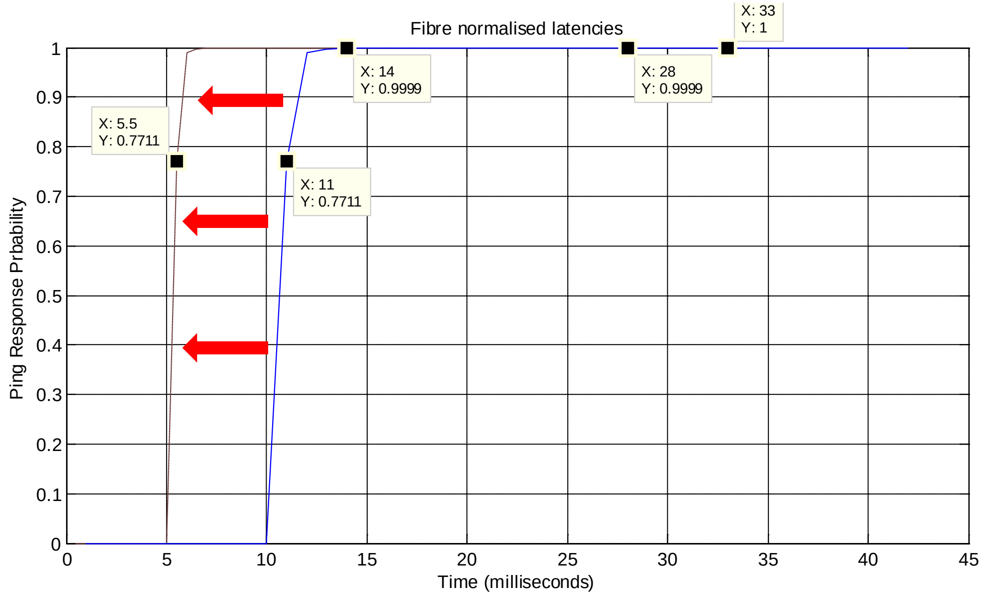
Latency performance (PING test)

Station	ICMP request	ICMP reply	Min response time (milliseconds)	Max response time (milliseconds)
ICC	127756	126016	64	95311
Zwelibomvu	127753	121360	84	33794
100 Woodhurst	127837	116679	58	38118



Fibre Latencies





Fibre - GPRS comparison:

- 11ms vs 1s
- 28ms vs 28s

Protocol Considerations

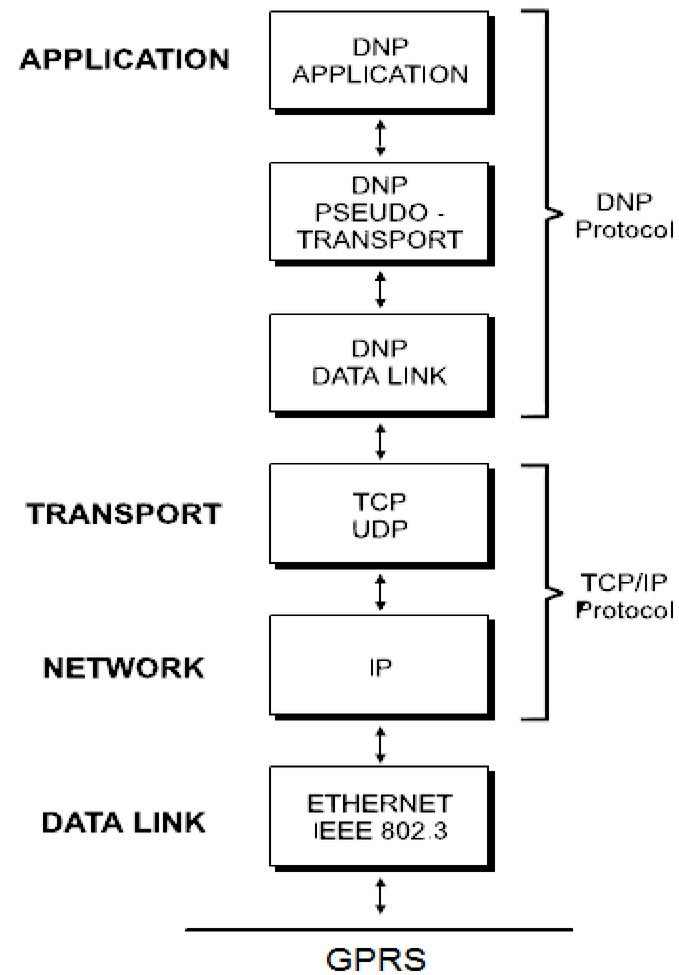
1. Non-deterministic network with varying latencies poses several challenges for the DNP3 protocol implementer

2. DNP3 has several configurable parameters that should be chosen to match the communication network

   – Application layer response timeouts

   – Select Before Operate (SBO) Controls

   – Time synchronisation



Reliability

GPRS/3G Performance

Station	ICMP requests	ICMP replies	ICMP lost	Packet loss %	Longest outage duration (min)	Channel Status Fail
ICC	127756	126016	1740	1.362	28.4	12.0
Zwelibomvu	127753	121360	6393	5.004	34.8	75.0
100 Woodhurst	127837	116679	11158	8.728	43.5	40.0

Performance of a fibre link

IEEE 802-2004 requires less than 0.012%

Station	ICMP requests	ICMP replies	ICMP lost	Packet loss %	Longest outage duration (min)	Channel Status Fail
Wentworth	127755	127750	5	0.004	0.16	0

Reasons for Packet Loss

1. Reasons for high Packet Loss on GPRS/3G network
   - Corrupted packets → FEC
   - Defective network elements → Dispersed sites
   - Signal degradation over the air interface e.g., fading → Signal Strength
   - High loads on the network/congestion → ?
2. Which is the most contributing factor?

Station	ICMP request	ICMP reply	ICMP lost	Packet loss %	Longest outage duration (min)
100 Woodhurst 30 min before the new year '13	181	176	5	**2.762**	0.3
100 Woodhurst 30 min into the new year '13	181	50	131	**72.376**	4.3

Congestion follows crisis

Security

1. Standards – NERC CIP, IEC62351
2. GPRS employs authentication and ciphering methods on the Radio Access Network
3. A RADIUS Server is normally deployed by the service provider to ensure further authentication
4. Best practice is to deploy firewalls at end devices
5. To provide end-to-end security, it is recommended that site-to-site VPN tunnels be deployed. IEC recommends the use of TLS, therefor an OpenVPN network implemented

Conclusion and Recommendations

1. Data speeds offered on the GPRS network is sufficient for the DNP3 protocol.
2. When engineering protocol parameters the following should be taken into account:
   - High latency network with a high corresponding variability
   - Cost model is based on data usage (and not duration) so it is important to design to transmit only what is necessary
   - High packet loss especially during times of congestion. An efficient transport layer protocol is required.
3. Newer cellular radio standards offer promising capabilities
   - QoS Load differentiation mechanisms offered by LTE

The end.

Any questions?