

# 基于 GPRS 模块的 PLC 远程监控

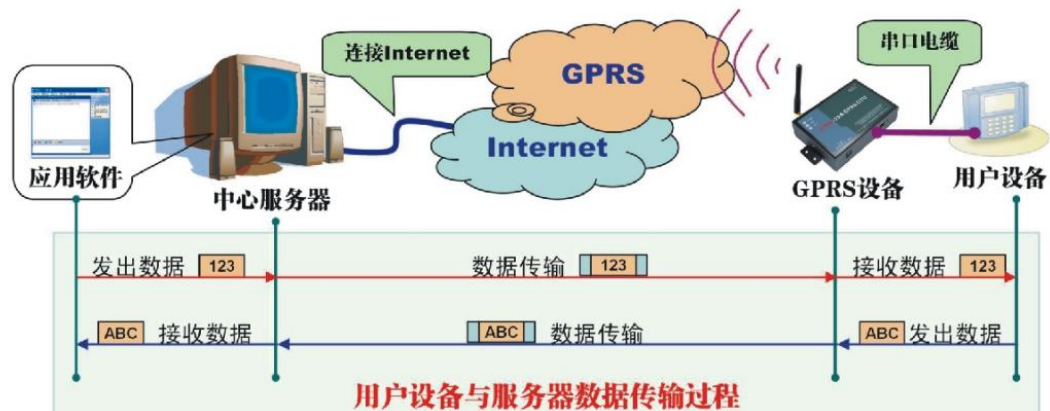
## 概述：

基于 GPRS 模块的 PLC 远程监控，在工业领域获得了很广泛的应用。本文详细介绍了传统的透传 GPRS 模块和广州市巨控电子科技有限公司 GRM200 系列非透传 GPRS 模块的原理，并进行了分析和对比。

## 透传模式：

传统的透传 GPRS 模块，往往在电脑上（需要固定 IP 或者动态域名花生壳）虚拟成一个串口，组态软件发出的用户数据，通过虚拟串口，加上 TCP/IP 的数据包后通过因特网发送给 GPRS 模块，GPRS 模块收到数据后，将 TCP/IP 数据包头去掉，然后再将用户数据透明的传输给远程设备。

简单的说，组态软件给虚拟串口发出的用户数据，没有任何更改的通过 GPRS 模块的 485 接口发送给了远程设备。由于网络传输的数据完全没有经过处理，存在安全隐患。



非透传模式：



巨控 GPRS 模块采用非透传的模式，特点如下：

1. GPRS 模块和 PLC 直接进行通讯，使用 PLC 本身的协议，如西门子 S7-200 的 PPI 协议或 S7-300/400 的 MPI 协议。
2. OpcServer 负责和 GPRS 模块通讯，数据格式和内容经过压缩和打包。
3. 组态软件通过 OPC 接口，从巨控 OpcServer 软件直接获取数据。OPC 作为一种标准的接口，GRM200 对 WINCC，组态王，力控等各种组态都能完全支持！电脑上不需固定 IP 和花生壳域名绑定，只要能上网，任何网络类型均可！
4. 网络上传输的数据经过压缩和打包之后，具备更好的安全性和加密性。

流量比较：

1. 透传模式传输 GPRS 数据的格式如下：

IP 头 (20字节)	TCP头 (20字节)	TCP选项 (一般12字节)	协议头 (3字节)	用户数据 (不定)
----------------	----------------	-------------------	--------------	--------------

用户数据，即组态软件通过虚拟串口发送的有用数据，由此可见，如果用户数据过短，一次 GPRS 数据传输的利用率过低，会导致大量的流量浪费。

2. 传统透传模式，组态软件和 GPRS 模块通讯的数据完全是由组态软件及通讯协议决定，对于不同数据类型的变量，无法打包一次读取，或者即使相同的数据类型，寄存器地址间隔超过一定的值，也无法打包。这就导致每次通讯实际的用户数据并不多，大量流量浪费在 IP 头，TCP 头等无用数据上。
3. 巨控首创的非透传模式 OpcServer 和 GPRS 模块之间完全采用自定义的打包和数据压缩格式，同一包数据中的变量可以不受寄存器类型和地址间隔的限制，一次可以传送上百个用户数据，可以最大程度上降低流量。

IP 头 (20字节)	TCP头 (20字节)	TCP选项 (一般12字节)	协议头 (3字节)	压缩打包 后数据
----------------	----------------	-------------------	--------------	-------------

4. 在一个典型的应用中，使用 GRM200G 的非透传远程监控 100 个 PLC 变量，3S 更新一

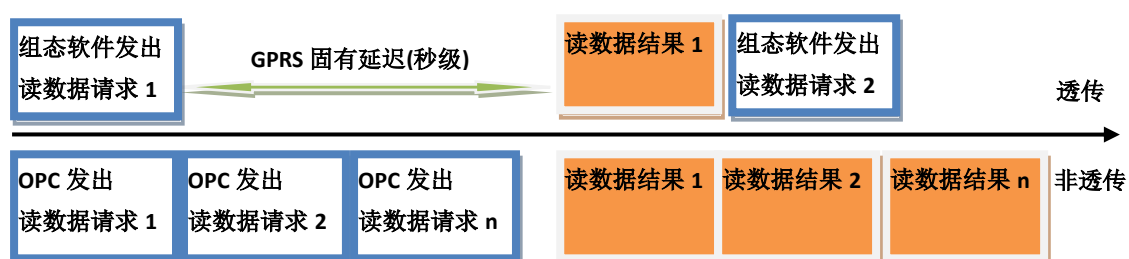
次，一个月只需要 100 多 M 的流量（15 元费用）。

## 速度比较：

传统透传模式，组态软件和 GPRS 模块通讯的数据完全是由组态软件决定，即使只需要访问 PLC 一个变量，也需要上位机发出一次读变量请求后，经过 GPRS 延迟时间（延迟为秒级），从 GPRS 模块获取读取结果。在实际应用中，如果有多个设备通过同一个透传模块和上位机通讯，需要数分钟才能更新一次数据！

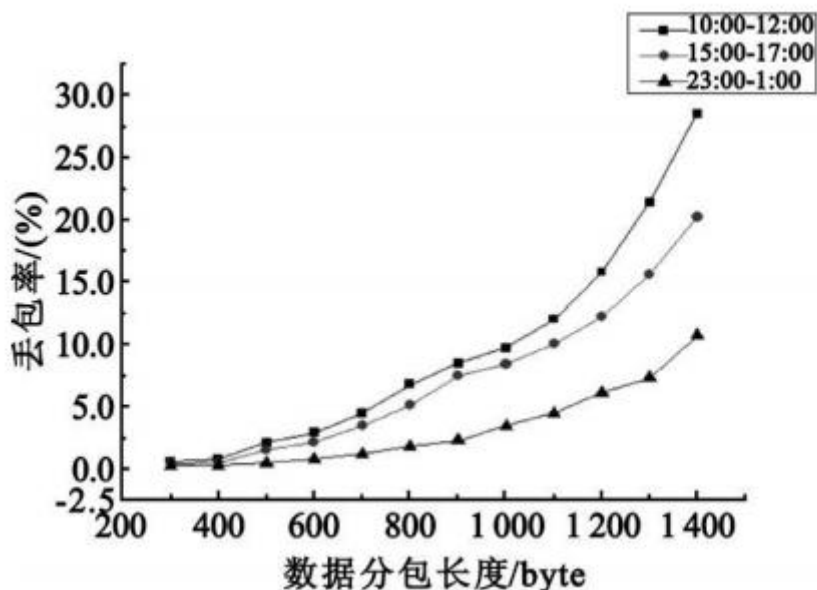
巨控首创的非透传模式，OpcServer 和 GPRS 模块之间完全采用**自定义的打包和数据压缩格式**，可以在一次传输中更新上百个变量（不受寄存器类型和地址间隔的限制，一包内也可以是不同从机设备的数据），在几秒内就可以更新来自不同从机设备的上百个变量！

此外，巨控科技的非透传模式还采用了**多包并发采集**的策略，不需要像传统透传模式一样，发出一次读数据请求后，需等待回复后，才能发送下一次读数据请求，而是可以连续发出多包读命令，然后依次获取读取结果。这样明显加快了读取数据的效率，有效避免了 GPRS 延迟过大的瓶颈！



## 稳定性比较：

1. 传统透传模式，监控电脑往往通过花生壳绑定动态域名的方式来解决需要固定 IP 的问题，而动态域名非常不稳定，导致多年来工控界对于 GPRS 远程监控有了一个结论，不稳定，不实用。此外，绑定动态域名对最终用户来说，也比较繁琐，无法实现即装即用。**巨控模块内置云监控服务，提供稳定的服务，可以完全应用于工业高可靠性场合。监控电脑端只需要能上网，无需固定 IP 和绑定域名，对最终用户而言完全做到即装即用！**
2. 一般来说，GPRS 数据包越长，数据的利用率会越高，有利于提高吞吐量和效率，但是在基站网络比较繁忙的时候，GPRS 的数据包长度越长，丢包率和重发次数会明显增加，反而使效率变得更低，甚至出现通讯中断的情况。如前所述，传统的透传模块的一次传输数据的包长，完全由组态软件当前要读写的数据决定，无法根据网络负载改变。而采用非透传的巨控 GPRS 模块，OpcServer 可以根据网络的延迟情况和当前的丢包率，动态的调整 GPRS 数据分包长度，获得性能和稳定性的较好平衡！



关于 GPRS DTU 其他稳定性的介绍, 请参考文章 鉴别 GPRS DTU 稳定性的方法:  
<http://www.giantcontrol.com/news/html/?395.html>

## GPRS 与短信互补

GPRS 作为主流的通信方式可以轻松应对大部分应用, 但是其不足之处在于, 语音和短信业务的优先级比 GPRS 的优先级更高。当基站覆盖的区域语音业务比较繁忙时可能导致 GPRS 中断, 此时可使用短信来发送一些紧急的数据和消息。

使用透传的 GPRS 模块, 虽然 GPRS 模块本身是具备短信功能的, 但是由于在这种模式下, GPRS 模块只是一个透明的数据转发器, 因此不能使用同一个模块既发短信, 又实现数据透传。通常解决方法是在电脑上再使用一个短信猫, 利用组态软件提供的驱动, 实现一些简单的短信报警。此方案缺陷在于, 短信猫依赖电脑运行, 如果需要短信报警, 必须保障电脑永远开机且不出现死机, 重启, 可靠性不高。此外, 还需要同时保证 GPRS 模块和短信猫 SIM 卡不欠费, 才能完成上述功能, 给管理带来一定的难度。

巨控科技首创的无线方案使用 GRM200G 和 PLC 连接, 完成短信和 GPRS 双重功能, 即使 GPRS 网络中断或者繁忙, 依然可以通过手机短信监控远程设备。通过简单的配置, 可以完成短信报警, 短信读写 PLC 任意寄存器, 定时发送设备信息到值班人员手机等! 此外, GRM200 还具备智能流量和费用查询管理功能, 最大限度降低管理难度, 保障无线监控系统的可靠运行!



## 为什么普通 DTU 无法完全实现 PLC 的监控：

以西门子 S7-200 的 PLC 为例，上位机和 PLC 通讯时一次读写过程如下：

1. 首先上位机发出读写命令，
2. PLC 作出接收正确的响应，
3. 上位机接到此响应则发出确认申请命令，
4. PLC 则完成正确的读写响应，回应给上位机数据。

由于 PPI 协议规定，在第 3 步，上位机必须在毫秒级的时间内迅速发出确认申请命令，否则 PLC 会认为通讯故障，而 GPRS 固有的通讯延迟（一般为 1 秒或几秒）导致传统的透传模式无法达到此要求，实际上，即使采用 3G 透传，也无法达到此实时性要求。

由此可见：**传统的透传模式无法实现西门子 PLC 的 PPI 协议的远程监控**，只能采用 MODBUS 协议，加大延迟时间来间接实现。同理，S7-300 的 MPI 协议，也无法使用透传模块实现远程监控。

巨控科技的非透传模式，很好的解决了这个问题，由 GRM200 模块直接和 PLC 通过 485 通讯，对通讯的实时性可以完全保证！

## 巨控无线通讯模块的其他优势：

1. 可以实现电脑和模块之间 1:N, N:N, N:1 之间的通讯。也就是一个 PLC 可以同时被多个电脑上的组态软件监控，一个电脑也可以同时无线监控多个 PLC。
2. **模块内置 WEB 发布**，只需要用电脑和手机登陆云监控网址，输入模块的密码和序列号，通过网页即可查看和修改 PLC 的数据。
3. PLC 无需编写任何程序，客户无需具备网络知识，只需熟悉组态软件，即可完成远程电脑监控，PLC 短信控制，短信查询，短信报警，以及网页监控 PLC。

## GRM200 通讯模块支持的 PLC：

GRM200 支持以下 PLC 型号，并在实际工程中应用。

1. MODBUS 主机协议，该协议支持所有使用 MODBUS 通讯协议的设备，如 AB，信捷 XC 系列 PLC，台达 PLC，海为 S/H 系列 PLC，艾默生 EC 系列 PLC，凯迪恩 K3 系列

- PLC，德维森全系列 PLC 等。
2. MODBUS 从机协议。
  3. PPI 协议支持 GRM200 与西门子 S7-200 系列 PLC 之间的通讯
  4. MPI 协议支持 GRM200 与德国西门子公司 S7-300， S7-400 PLC 的通讯
  5. 三菱 FX 系列 PLC 协议，使用 485BD 通讯板卡，支持 FX 系列 PLC 全部型号。
  6. 三菱 Q 系列 PLC 协议。
  7. 欧姆龙 HOSTLINK 协议。

## GRM200 支持的组态软件：

通过 OPC 接口，GRM200 支持任意组态软件。以下列出部分实际工程中应用过的组态。

1. 西门子 WINCC
2. GE 公司 IFIX
3. Wonderware 公司 INTOUCH
4. 北京亚控公司组态王
5. 力控组态软件
6. 易控组态软件
7. 昆仑通态组态软件

## 参考文献：

1. 吕捷，GPRS 技术，北京邮电大学出版社，2001
2. 刘方，林晓辉 基于 GPRS 的嵌入式智能家居终端的设计与实现，微计算机信息
3. 田锦，GPRS 数据分包长度和心跳包间隔性能分析，电讯技术
4. Worrall S T, Sadk a A H , Sweeney Backward Compatible User-Defined Data Insertion into MPEG-4 Bit streams Electronics Letters,
5. 巨控科技，GRM200 使用手册
6. 巨控科技，GRM200 驱动手册