Comark RF500 Wireless Monitoring System
Information Technology Paper
21st December 2011

Document Purpose

This document is intended to aid with the integration of the RF500 system with an organisation's current IT infrastructure. The information contained within should be able to answer most questions IT will ask prior to the installation of this system.

Target Audience

This document is aimed at IT professionals.

COMARK
A Fluke Company

Table of Contents

RF500

Description

The RF500 Gateway is an embedded system to provide a web-server interface. Only some of the external connectors are intended for customer use (see *Connector Restrictions*). A number of software ports are in-use and are listed separately below. The Gateway once connected to a network, via Ethernet, allows client users access to the web-server interface via his or her own PC running a suitable web browser, Comark has tested the following browsers:

- Microsoft Internet Explorer 8 and above
- Firefox 4.x & 5.x and above
- Chrome 12.x and above

However additional browsers such as Opera & Safari should work without issue.

Alternately the Gateway can be connected to a PC via crossover cable or through a modem connection (if fitted). There is no software to install for client users to gain access to the system, all interfacing is done through the website. The Gateway stores all data and setup information internally. The Gateway can be backed up remotely using optional PC based software (RF500 & RF500LITE only). The Gateway is battery backed up in the event of mains failure and providing an Autodialler and BT Analogue direct line is connected, alarm messages can be sent from the Gateway during a power-cut. All access to the website is protected by username and password.

Fit and Forget

Unlike other systems, the RF500 Gateway is a fit and forget device. Placement of the Gateway in any system is determined by radio frequency testing during a survey, but essentially can be located anywhere on the LAN. It does have LED's for alarm indication and fault indication but no other user interface is available. All connection to the Gateway for data view, alarm acknowledgement and programming is via password-protected login using the web browser interface.

The Wireless Interface

RF500 utilises a licence free band in the 2.4GHz region. It is important to recognise that although there are some similarities between RF500 and WiFi the two are completely different and should not be thought of as being the same. The radio system used by the RF500 is not WiFi or WiFi based in any way shape or form, hence IP packets cannot be transported over Comark wireless.

The RF500 wireless monitoring system uses the wireless interface only to send data between the Gateway and transmitters using a proprietary format and recognises data packets of our own design.

Basic Specification

Centre Frequency:	2.405GHz
Bandwidth:	5MHz
Transmitted Power:	1mW
Raw Data Rate:	250Kbs
*Actual Throughput (estimated):	2Kbps
Modulation Technique:	QPSK
Spread Spectrum Technique:	DSSS

*This depends on distance from gateway.

The bi-directional RF link between Gateway and transmitters is based on an IEEE 802.15.4 physical layer and an entirely proprietary application layer, thus ensuring the security of the link.

The RF is IEEE 802.15.4 compliant, there is some crossover between the RF500 frequency and some WiFi channels but WiFi utilises a completely different modulation scheme. The RF500 modulation scheme is QPSK with half sine pulse shaping modulation (Quadrature Phase Shift Keying) whereas WiFi uses:

IEEE 802.11b CCK, DQPSK, DBPSK. (Complementary Code Keying, Differential Phase Shift Keying, Differential Binary Phase Shift Keying).
IEEE 802.11g OFDM, (Orthogonal Frequency-Division Multiplexing).

This means that the signals can occupy the same frequency without interfering with each other. The bandwidth required by WiFi is in the order of Mega (Million) Bits per second to allow normal data flow, our systems' bandwidth is only 250 Kilo (Thousand) Bits per second. If it were possible to "hack" the RF link there is no route to get to the Ethernet port of the RF500.

WiFi Channels: *(Europe uses up-to channel 13 this represents the spectrum for the US)*.

Channel	Lower Frequency	Center Frequency	Upper Frequency
1	2.401	2.412	2.423
2	2.404	2.417	2.428
3	2.411	2.422	2.433
4	2.416	2.427	2.438
5	2.421	2.432	2.443
6	2.426	2.437	2.448
7	2.431	2.442	2.453
8	2.436	2.447	2.458
9	2.441	2.452	2.463
10	2.451	2.457	2.468
11	2.451	2.462	2.473

Taken from "OFCOM Higher power limits for license exempt devices" - "Existing wideband data transmission systems in the 2.4GHz band mostly uses Bluetooth or WiFi. Equipment categorized as wideband data must comply with EN300328 and is limited to 100mW EIRP."

Our RF system uses only 1mW ensuring it is not powerful enough to have any significant impact on WiFi.

Connections to Network

Connection to the network is via standard Ethernet connection. However a fixed IP address must be allocated to the Gateway from IT before it is connected. All web-server interfacing and sending of e-mails is done over the Ethernet connection or alternately via the Modem connection (if fitted).

Web-server

Comark uses Apache Server to provide the web-server interface. The interface itself has been written by Comark to provide pages for all data viewing, setup and general management of the Wireless System.

E-mails

The Gateway can be setup to use a mail server on the network to send e-mails. In order to do this the mail server needs to be setup to accept incoming e-mail from the Gateway IP address and the Gateway itself needs to be programmed with the IP address or sever name of the mail server.

The system utilises the SMTP protocol to send e-mails, however the RF500 **cannot** receive e-mails.

Data Outputs and Backup

NOTE: Comark **always** recommends keeping both a backup on a server/local PC and an off-site backup for complete data security irrespective of RF500 model.

The RF500 provides the user with multiple options for backing up data and reporting. The RF500 can output the following data types:

Software Backup Data: (Excluding RF500A/AP) The RF500 backup software will be running as a taskbar application on a Windows PC. Data passed to the RF500 backup software from the RF500 via a constant connection over the network (using ports 8888 & 8889). Individual data files of 5KB (typical size) are sent over this link (over port 8888) as they become available.

Manual Backup Data: From the RF500 website the manual backup option can be invoked from the administration page. The RF500 will generate a single compressed and encrypted file which is then downloaded via the website (using the HTTP port). This method has to be manually triggered by a user.

Standard Backup Data: As data becomes available, the RF500 will generate compressed and encrypted files, these will be copied to a network share backup location.

CSV Output Data: The RF500 can output plain text CSV files if required containing the data for the transmitters. This data can then be manipulated to form reports etc. For each transmitter there will be one CSV file containing data per day from its current task, these files can be typically 50KB per transmitter. The update rate can be configured between 1 – 24 hrs.

Built in Backup: The RF500A & RF500AP include a secondary memory card that mirror's the primary for added security.

Software Backup (RF500 & RF500LITE Only)

An optional PC software package is available to backup the Gateway. This provides customer peace of mind that the Gateway is being backed up and allows for repaired Gateways to be restored to a pre-breakdown condition should the worst happen. The PC software will run on a nominated PC and collects data from the Gateway in a compressed format.

Windows Shares

The following describes the alternative methods for automatically transferring data from the RF500 to remote storage without the need for the automatic backup software.

The option discussed below only apply to the *CSV Output* and *Standard Backup* data types.

Shared Drive Method: The intention is to request a shared drive from the IT department of a company. The RF500 user will supply the machine name and share name onto the configuration page of the RF500 website. This will allow the RF500 to mount the drive and send data (CSV files or backup) to the shared drive (the shared drive can be user name and password protected).

Storage Allocations

Assumes 1min data logging rate.

CSV:	Bytes per day = 50KB * No Transmitters.
For Example:	50KB * 30 Transmitters = 1.5MB per Day For 10 Years = 5.475GB
Standard, Manual and Software Backup:	Bytes per day = 5KB * No Transmitters.
For Example:	5KB * 30 Transmitters = 150KB per Day For 10 Years = 547.5MB

Security

Anti-Virus/Firewalls

The normal system entry points for a virus are email and storage. The RF500 is not able to receive e-mails and has no accessible storage making this very difficult.

Since this is a Linux based system, for a virus to be successful it would have to find a way onto the hard disk and then be manually executed as the root user. A virus needs root user privileges to enable system wide infection.

This would be particularly difficult to gain root access as there is no way to login as a user and an attacker would have to know the following:

- An entrance mechanism to allow login.
- One of the User accounts (user name and password protected) that has permission to “super user up”.
- The root password.

It is also worth remembering there are only a small number of Linux viruses in the wild and hence the likelihood of infection is reduced even further.

Since the RF500 does not provide any storage visible (shared drive or otherwise) to the network it cannot provide storage for any Windows viruses that may spread through network drives.

Therefore to save the on going subscription costs to the customer of Anti-Virus software, the inevitable drop in performance of the system, plus the need for constant daily updates, and in discussions with other IT professionals, Comark has taken the decision that Anti-Virus software is not required. We firmly believe that the safeguards put in place to protect the system and that we have carefully chosen the main system software makes this the correct decision for RF500.

Ports in Use

RF500 & RF500LITE:

Port 80:	HTTP port open for web server access (listening port).
Port 25:	SMTP port open but not listening used for sending e-mails not receiving.
Port 113:	Auth port (listening port).
Port 445:	SMB network share port to access shared drives for sending CSV export data and or data backup.
Port 8889:	RF500 backup software port (existing software listening port).
Port 8888:	RF500 backup software port (existing software).

RF500A & RF500A/P:

Port 80:	HTTP port open for web server access (listening port).
Port 25:	SMTP port open but not listening used for sending e-mails not receiving.
Port 139:	Netbios-ssn (used by shared drive)
Port 445:	SMB network share port to access shared drives for sending CSV export data and or data backup.

The Determined Hacker

Of course no PC or Linux system can be completely safe from the determined hacker especially if they can gain physical access to the equipment. However should a hacker obtain access to the RF500 Gateway we must assume that it has been compromised, All passwords should be changed after a suspected attack. There is no more a threat to the LAN and other connected equipment than if a PC connected to the LAN were compromised.

Operating System

RF500 & RF500LITE

Linux running Apache Server version 1.3.33. Kernel version 2.4.31

RF500A & RF500AP

Linux running Apache Server version 2.2.11. Kernel version 2.6.24.2.

Connector Restrictions

All connections to the Gateway, other than those mentioned above are restricted. These include the USB ports, VGA, Printer, Keyboard and Mouse ports.

RF542 Network Transmitter

Description

The RF542 Network transmitter is essentially an RF512 with the RF communications replaced by Network communications. Task information and data is transmitted to the associated RF500A/AP via a standard TCP/IP type connection.

Connections to Network

This device supports 100Mbps, half duplex. It has a DHCP client so IP address will be assigned by the network, there is no facility to set a static IP address.

Ports in Use

Port 10003: All task and data information is sent over this port, information over this link is bi-directional.

Bandwidth Considerations

During normal operation data is sent within a single TCP/IP packet (maximum size 512KB) at a minimum interval of 60 seconds. During certain events (new firmware/ADR) the transmitter will “burst transmit” for a 10 second period sending as much data as it can within this time, depending on network conditions this could be 20 TCP/IP packets.

Data Encryption

Data is not encrypted in a traditional sense, however nor is it an open format (such as plain text ASCII). The data structure is entirely proprietary to Comark and all data is in a binary format, without knowing the structure the data is unintelligible.

Comark Limited
Bury Mead Road,
Hitchin, Herts. SG5 1RT UK
Tel: +44 (0) 844 815 6599
Fax: +44 (0) 844 815 6598
Email: salesuk@comarkltd.com

Website: www.comarkltd.com

Comark Instruments
PO Box 9090, Everett,
WA 98206, USA
Tel (503) 643 5204
Fax: (503) 644 5859
Email: sales@comarkUSA.com