iris Secure Apps™

IRIS Alarm over IP System
Overview for the IT and Network Managers of Organisations and Companies using IRIS

V1.0

Now certified and compliant with EN50131, EN50136 Security Grade 4 ATS6

Contents

1 Introduction to the IRIS System

This document is provided as an overview and guide to the IT and Network Managers of companies and organisations who are using the Chiron IRIS system for their Intruder alarm communications.

It is written on the basis that the monitoring of the alarms is a service provided by an external central monitoring station, which is generally the case.

Chiron's IRIS Alarm over IP System makes it possible to use an existing IP network for the monitoring and control of Intruder alarm systems and the transmission of alarms to a central monitoring station.

This brings several benefits to the alarm user:

- Cost reduction since dedicated telephone (PSTN) lines for the intruder alarm system are no longer required.
- Further cost reduction as the transmission of alarm signals does not incur call charges.
- Cost effective alarm communications monitoring. For installations where a higher grade of security is needed it is requirement of the European standards that the communication path with the site is monitored (polled). This is far more cost effective on an IP network as compared to the expensive monitoring of PSTN lines.
- An effective platform for enhanced alarm services, such as visual verification and live video monitoring.

The IRIS system can operate with existing alarm installations via an add-on module that takes the existing alarm PSTN interface and converts this to IP.

Alternatively new alarm equipment is now being offered by a number of manufacturers that has integrated IRIS functionality.

The IRIS system has been tested and certified by an independent authority for compliance to the highest grade of security as defined in the European EN50131 specification – Grade 4 ATS6.

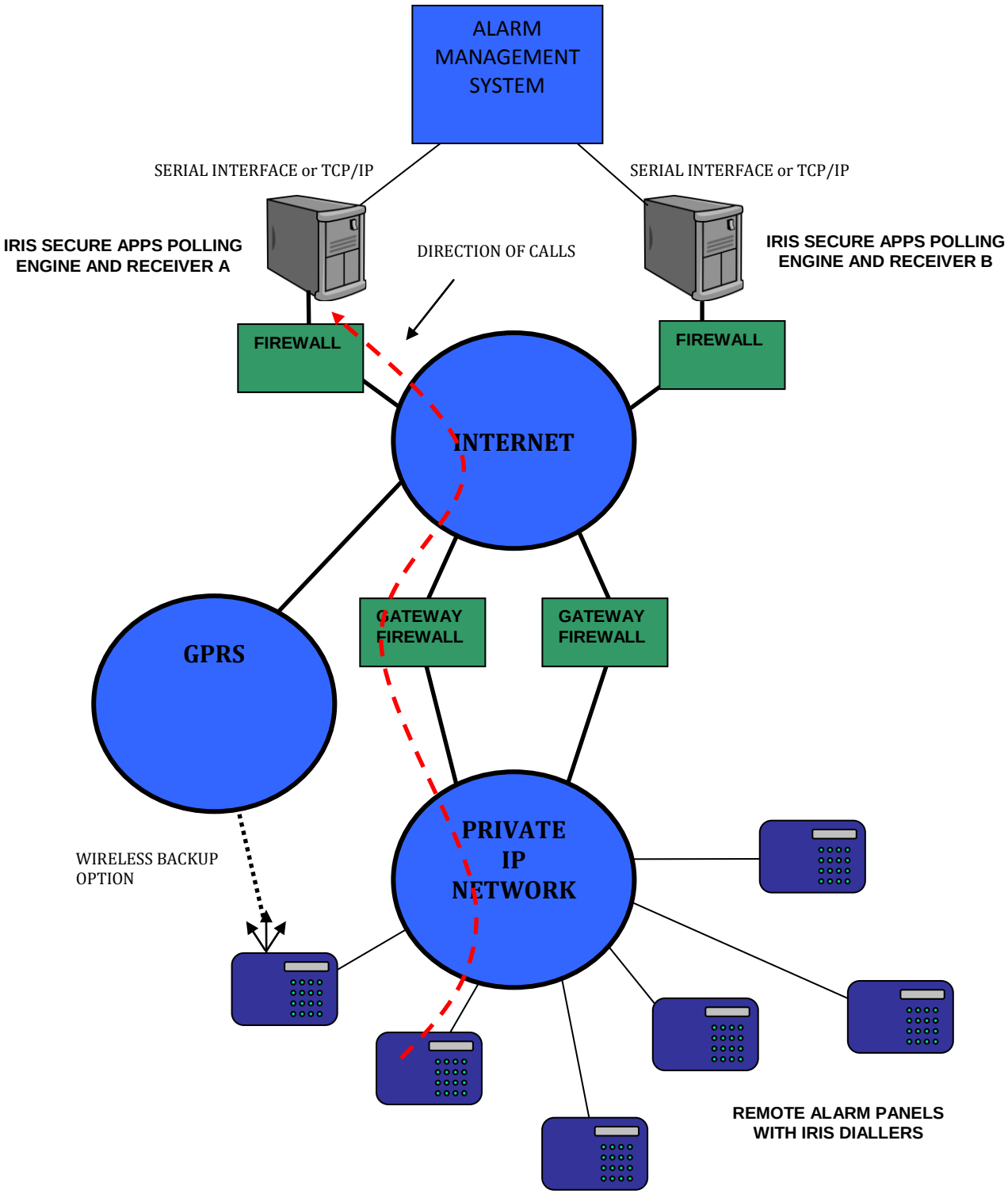
The IRIS System is also designed to be easy to install and operate on any IP network:

- Dynamic addressing (DHCP) by default.
- All calls are outgoing so no security implications and no Port Forwarding required.
- No DNS required.

2 How it Works

The IRIS system is designed to work with existing IP networks with the minimum of setup being required.

An example is shown in the diagram below:



There are a number of backup options as shown, including backup over GPRS and backup to an alternative central station.

The important points to note are:

- The IRIS diallers by default use Dynamic IP Addressing (DHCP). Fixed addressing can also be configured if required.

- All IP communications from the dialler is by outgoing calls, including traffic for Polling, Alarm Transmission and Remote Management and Diagnostics. No port forwarding is required in the network gateway.

- No port mapping or DNS required.

3 Considerations for the IT Manager

Aspects of the IRIS operation that may require some involvement with the IT manager are as follows:

3.1 IP Port Numbers

It is necessary to ensure that the IP port numbers used by the IRIS system are opened in the gateway router to the Internet. Note – this is only for out bound calls from the network and should not cause any problem or security risk. These ports are:

Function	Port	Type
Polling	52737	TCP
Alarm signals	53165	TCP
Remote management and diagnostics	51292	TCP
IRIS Remote Service App for upload/download of alarm panels behind firewalls	10001	TCP
Other upload/download	8738 and 8739	UDP

3.2 IP Destinations

Some IT Managers restrict outbound connections to specific IP addresses, normally the IP address(es) of the monitoring station.

It is also advisable to also allow TCP connections to Chiron Security as this allows anyone installing a new dialler on site to access Chiron's dialler reflashing server to make sure that the dialler has the latest firmware installed.

There are two addresses in use:

- 195.59.117.164
- 80.176.196.134

3.3 Network Traffic Volumes

In general the amount of IP traffic generated by the IRIS system is very small and is mainly dependent on the frequency of the polling of each IRIS dialler.

Given that the frequency of the polling is in almost all cases an order of magnitude higher than the frequency of alarms transmitted (which typically is 2 per day – Open and Close), then the amount of alarm related data is normally insignificant.

Depending on the level of security required this can be set from once every 10s to once every week per dialler.

For each poll the amount of data transmitted, including all TCP/IP overhead and IRIS authentication and encryption is as follows:

347 Bytes out from dialler (assuming a four character account code – add 1 byte for each extra account code character)

193 Bytes in to the dialler

Total: 544 Bytes

For each alarm the amount of data transmitted, including all TCP/IP overhead and IRIS authentication and encryption is as follows:

457 Bytes out from dialler (assuming a four character account code and 13 character alarm message – add 1 byte for each additional character)

234 Bytes into dialler

Total: 691 Bytes

As can be seen, given that there are normally significantly more poll messages than alarm messages, the proportion of data associated with alarms is very small.

3.4 Gateway Capacity

As described above, the amount of IP traffic generated by the IRIS system is very small, although consideration should be given to the capacity of the network gateway to ensure there is adequate bandwidth available.

In most situations where there are minimal alarm transmissions the majority of the traffic is the polling signals. Depending on the level of security required this can be set from once every 10s to once every week per dialler.

The amount of data per poll transaction is described above.

4 Network Security

The IRIS System is very secure and does not impact on the security of the IP network:

- All calls are generated from the diallers within the network. No calling in from an external entity is required.

- The IRIS diallers have embedded software with a proprietary software environment and are not prone to virus attack. This means that the diallers cannot run unauthorised software or scripts for the purpose of attack or access to other servers on the same IP networks.

- All IRIS traffic is in any case fully protected against substitution and interception by the use of a high level of authentication and encryption controlled by a unique security key for each dialler. This uses:

  256 bit key that can be set uniquely for each dialler and changed dynamically
  MD5 hashing
  RC4 encryption

- IRIS diallers cannot act as proxys or routers for an attempt to access or attack other IP based servers that share the same network. This is an inherent hard coded function in the diallers and so cannot be changed, even with configuration changes. In particular, the IRIS uses GPRS only for outgoing connections and there are no circumstances where it can loop back IP packets from GPRS to Ethernet or vice-versa.

5 SIM Card Requirements

If the system is using GPRS then SIM cards will be needed to be fitted to each of the IRIS diallers. In general any SIM card from any provider will work, but the following should be noted:

1) Pay-as-you-go SIM cards should not be used.

2) The SIM card should not have a PIN enabled. If it does, this will need to be cleared in a phone before the SIM is installed in the IRIS dialler.

3) The SIM should have GPRS (for data/internet) enabled (which is almost always the case). This is different from WAP, although a SIM card can support both. SIM cards that only support 3G operation cannot be used.

4) The installer will need to know the Access Point Name (APN) which is a name that the service provider gives for its gateway from GPRS to the wider IP environment. This name will be entered into the IRIS dialler. Sometimes the service provider also issues a User Name and Password and this information will also be required by the installer.

5) The SIM card should be activated before it is sent to site.

6) Also note that the geographical coverage provided by service providers is different and should be taken into consideration. The IRIS dialers contain a network scanning facility so the installer can verify that the service provider chosen is acceptable on a particular site.

The future of security, secured

IP by security professionals, for the professional security industry

Telephone: +44 (0)118 099 0228
E: sales@chironsc.com
www.chironsc.com

Chiron Security Communications Ltd,
Wyvols Court, Swallowfield,
Reading, Berkshire, RG7 1WY UK