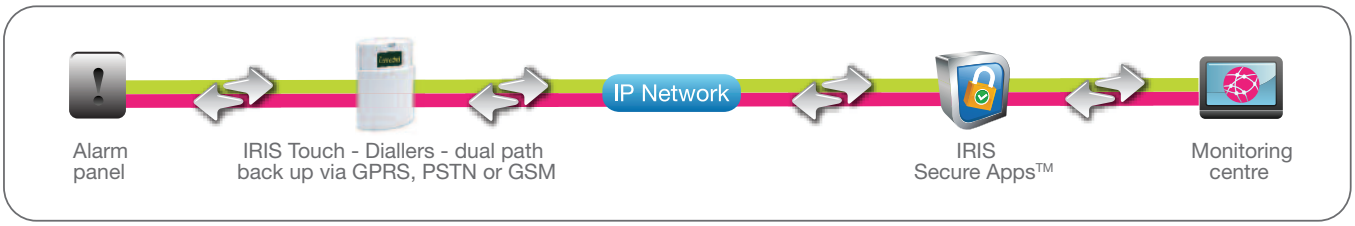
iris touch
IP security to go

IRIS IP system

Chiron's IRIS IP system acts as the interface between an intruder alarm panel, an IP network and the alarm monitoring centre. IRIS Secure Apps™ in conjunction with Chiron's IRIS Touch IP diallers forms a complete alarm transmission system.



The IRIS IP system consists of software modules which form IRIS Secure Apps™ and the various options of IRIS Touch dialler for the alarm panel connection. A single software licence for IRIS Secure Apps™ allows a complete system to be created and managed with multiple receivers and 'hot standby' sites.

IRIS Touch Dialler

Acts as the interface between the alarm panel and the IP network and converts the analogue signals from the alarm panel and vice versa. Alternatively, the interface to the alarm panel can be via inputs, serial data or RS485 bus.

IRIS Touch 200 series
A stand-alone IP solution in an elegant consumer unit with a touch screen.

IRIS Touch 400 series
A touch screen unit designed to bring IP connectivity to existing control panels.

IRIS Touch 600 series
A cost effective unit with full IRIS Touch connectivity for fire panels and superior integration for specific manufacturer panels.

iris Secure Apps™

IRIS Secure Apps™ is an evolving collection of secure "Apps" that are web enabled. The Apps (under complete control of the monitoring centre) function to ensure the monitoring centre has all data at its fingertips, both "real time" and "historical".

Additionally, (also under monitoring centre control), IRIS Secure Apps™ enable client manager and installer/engineers mobile access on their web-enabled notebooks, mobile phones and PDAs, with 2 levels of security.

Monitoring centre IRIS Secure Apps™ include Authoriser, Templator, Allocator, System Detective and System Analyser

In addition, for the monitoring centre and field/mobile use, IRIS Secure Apps™ has Dialler Detective, Dialler Analyser, Dialler Dialogue, Stat App and Mobiliser

All with 2 levels of security and monitoring centre control.

CHIRONsecurity communications
Chiron Security Communications Ltd, Wyvols Court, Swallowfield, Reading, Berkshire RG7 1WY UK
T: +44 (0)118 988 0228 Fax: +44 (0)118 988 1055 E: sales@chironsc.com www.chironsc.com

IRIS IP system

By allowing all alarm management, transmission and monitoring functions to be migrated away from dial-up communications to an IP network, the IRIS system unlocks significant cost savings for the user.

All communication with the remote devices is highly secure with authentication to protect against substitutions and encryption to protect against interception of alarm messages.

Scalability and reliability

A key element of IRIS Secure Apps™ is "polling engines" which act as receivers for alarms and which also regularly monitor the remote IRIS Touch units to check that they are active and the communications paths are available.

By replicating the elements of the IRIS IP system as required, a system can be scaled from a single server managing a few hundred remote devices to a large system with multiple IRIS polling engines managing many hundreds of thousands of remote devices and with 'hot standby' facilities.

Depending on polling frequency and the bandwidth of the IP connection, a receiver/polling engine can manage over 10,000 remote devices. As many polling engines as required can be set up, all managed from a single console and database.

For system resilience each remote device can be assigned a backup polling engine that it will contact in the event of failure to communicate with the primary unit. 'Hot standby servers for all other elements of the system can also be set up to take over in the event of failure.

Standard interface to existing monitoring centre's computer

For operation with an existing monitoring centre's computer, each receiver/polling engine can support a serial connection that emulates an industry standard PSTN alarm receiver.

The standard interface allows the monitoring centres to rapidly integrate IP communications into their existing installation. The serial interface is used to report events from the remote alarm systems - alarm messages, polling and backup communications status changes.

It is also possible for the IRIS database to be linked to an existing monitoring centre's database so that operators can key in new user details only once.

Constant monitoring of remote devices

All remote devices are constantly monitored through the polling mechanism. This mechanism involves the remote device calling into the polling engine on a regular basis to prove that it is operational and the IP communications path is intact. As part of polling, the status of backup communications paths at the remote device is also reported.

In the event of a device failing to poll in or on the indication of a backup path failure, an alarm message is sent on the serial interface to the monitoring centres.

The polling frequency of each remote device is determined by the IRIS database from a period of 10 seconds for high security sites up to 7 days for less sensitive installations. Devices can be set with differing polling periods if required.

It should be noted that as the IP calls are generated from the remote devices, the system does not need to know the physical IP address of that unit. This offers great flexibility as it means that the remote devices can use dynamic IP addressing and operate on a customer's private IP network communicating through a gateway to the IRIS IP system.

Security

All communications with the remote device is secured by a unique security key held by the IRIS IP system for each remote unit. This key is used to authenticate the remote device on each connection for polling and for alarm transmission to detect any attempted substitution.The key is also used for the encryption of the alarm message to prevent interception within the IP network.

Each transaction also incorporates a random element so that it is not possible to playback past transactions or to interpret the communications by observing repeated patterns.

A challenge-handshake technique is used so that the key itself is not transmitted as part of the security procedure. The key in the remote device can be updated from the IRIS IP system as often as required for enhanced system security.

IRIS Secure Apps™ also includes 2 levels of user access security, including username and password and, optionally, a physical token (Authenticator) that must be in the possession of the user at the time they make the access.

Traceability

All activity on the system is logged in text files. A new log file is automatically created on a daily basis.

Several tools are available within IRIS Secure Apps™ for accessing and analysing the information contained within the logs. This can be, for example, alarm history for a site, historical GSM signal strength or availability for a single dialler or the complete system.

Ease of installation

The software is supplied with automatic installation tools and is very simple to set up.

TECHNICAL DETAILS

Recommended server platforms

The recommended minimum specification for each physical server is:

- Quad Xeon 2.5 Ghz processor or equivalent
- 4GB RAM
- 2x250GB HD (RAID-1)
- Windows 2003 Server Standard Edition or above
- Microsoft.Net Framework should be installed on all servers with Internet Information System (IIS)

Please note – it is recommended that, due to loading considerations, virtual machines should not be used.

PSTN receiver emulation

- Surguard MLR2
- Radionics D6600
- Transparent (for local printer connection)
- Serial interface baud rate 4800bps to 115200 bps

Polling

- Configurable polling interval (10s to 7 days)

Alarm protocols

- Fast format (Scancom)
- Contact ID
- SIA (to Level 3) protocols
- Robofon

Security

Diallers

- Authentication using CHAP/MD5 algorithm
- Encryption using RC4 ciphering
- Key length up to 256 bits

IRIS Secure Apps™

- Username and password authentication for users accessing IRIS Secure AppsTM
- Optional physical token (Authenticator)

SQL database containing

- Dialler configuration
- System configuration
- Historical events
- Tools available for access to this database from external systems e.g. the monitoring centre system

*Actual parameters required depend on number of remote devices supported, polling frequencies, and log file storage policy