Quantel Australia

Product Profile

Quantel Gatekeeper

Overview

The Gatekeeper security system is a collection of interlinked devices, which are briefly described as follows:

- Physical access control is provided by Gatekeeper Sentries. Each Sentry is a self-sufficient, self-contained keypad device that affords control of a restricted area. Sentries communicate with each other (and the outside world) using a computer network.
- Each Sentry is fully configurable. This includes assigning authorised users, specifying what features to use, and even what text appears on the display. Sentry management is performed using the Gatekeeper Application.

  This is a user-friendly computer program, operating on a desktop computer, that instructs Gatekeeper Sentries how they should behave. It also receives information from Sentries about the current security status of the system, and provides an easy to read summary for the operator. Currently, the Macintosh is supported; versions are planned for other platforms.
- Management of large installations is simplified by Gatekeeper Security Hubs. These are devices that facilitate the connection and management of a large number of Gatekeeper Sentries. Each hub can supply power and network services to up to sixteen Sentries.

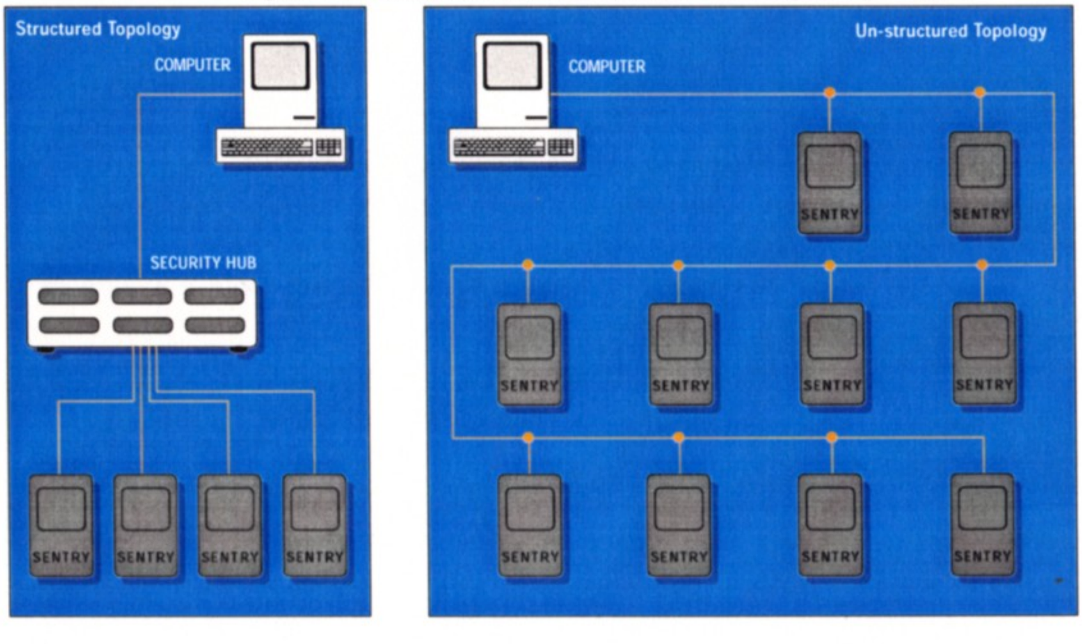
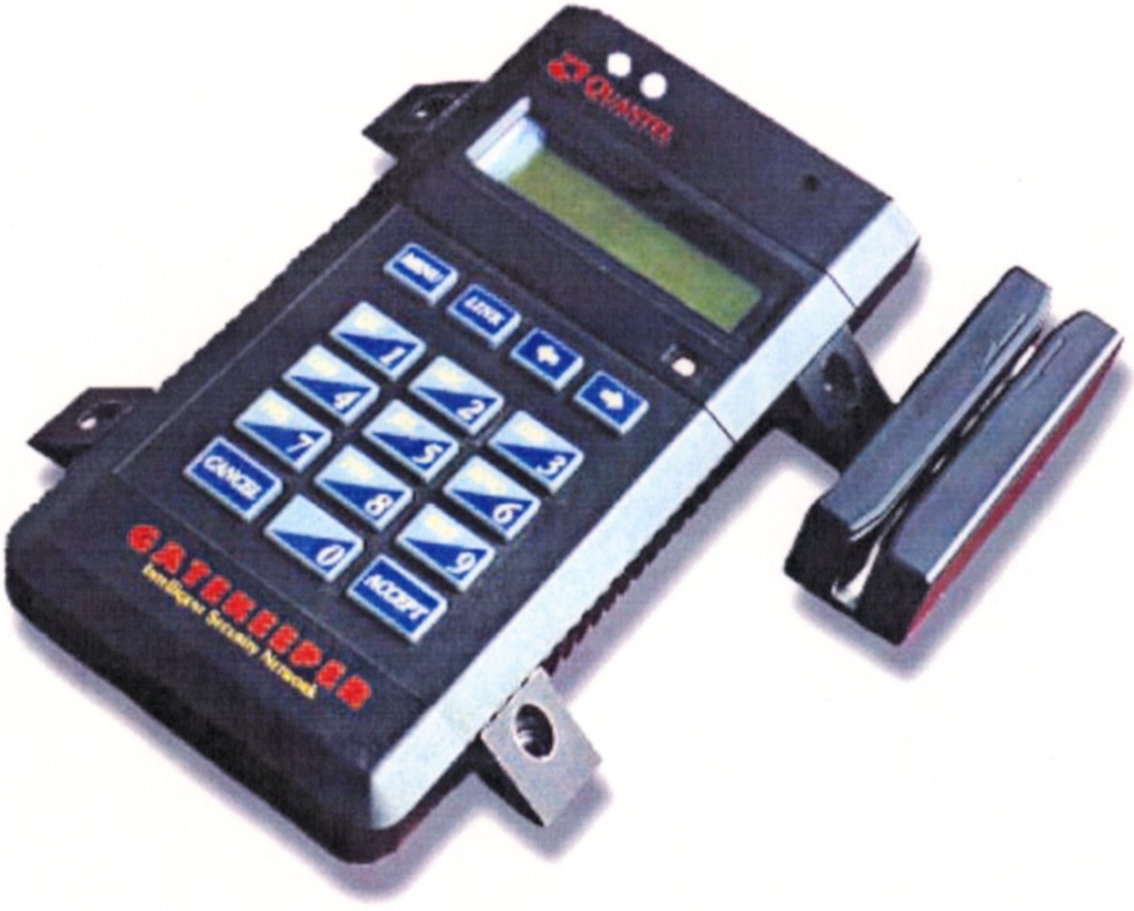


Figure 1: Structured and unstructured Gatekeeper topology's.

Gatekeeper Sentries

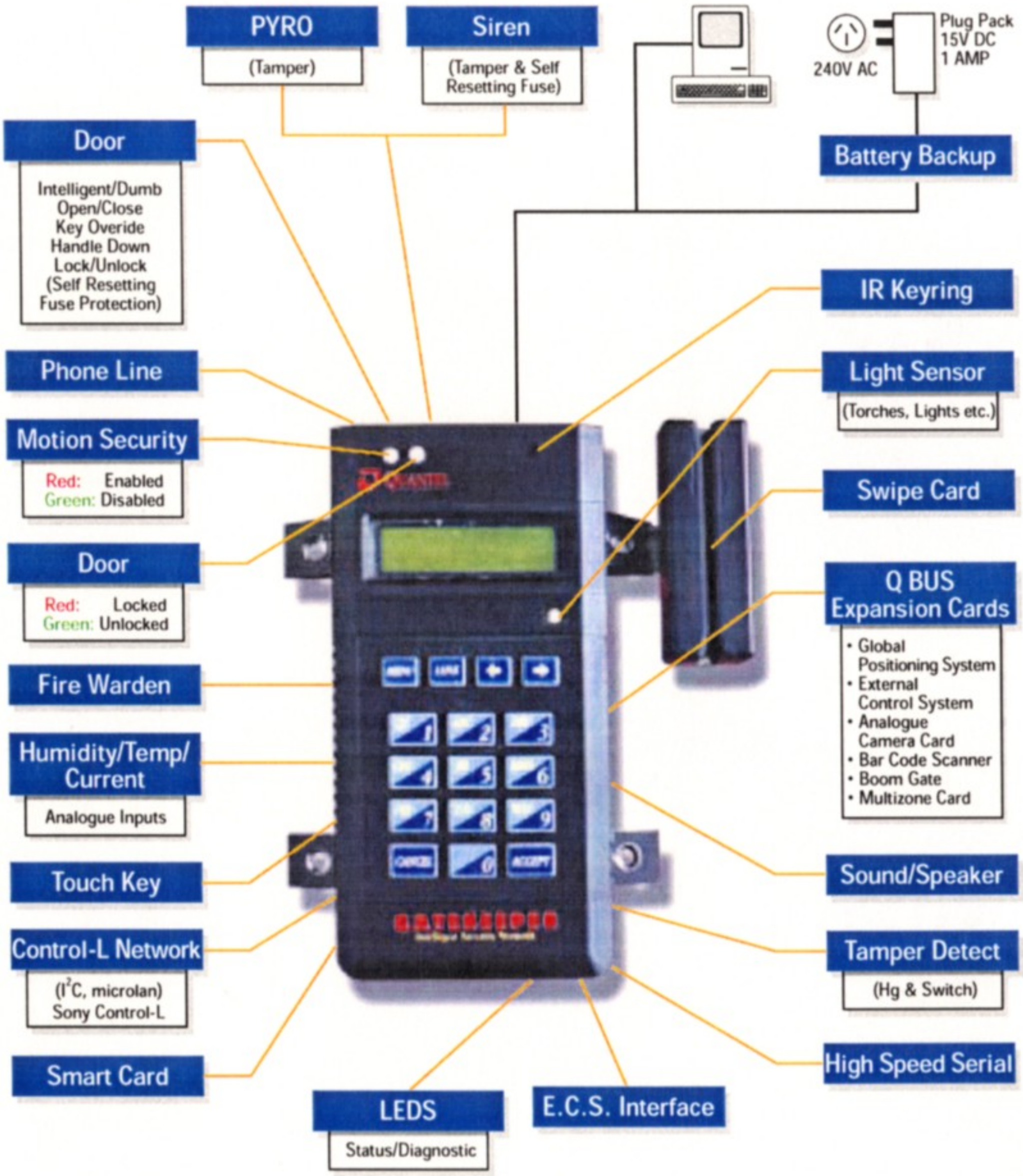
Access control is provided by Gatekeeper Sentries. Each Sentry is, effectively, a computer in its own right. The Sentry consists of a plastic or metal enclosure with four mounting screws, with which it is fixed to the wall. Access codes are entered via a sixteen-key keypad; information such as the current date and time are shown on a backlit liquid crystal display.

Figure 2: A Gatekeeper Sentry.



Each Sentry has a range of built-in features, in addition to a suite of expansion options. Ports are provided for connecting external sirens, motion sensors, fire detectors, analogue devices, touch key receptacles and swipe card readers. Internal plug-in cards have also been designed that interface to smart card readers and analogue video surveillance cameras. Each Sentry includes protected, on-board high-current device drivers, eliminating the need for so-called "driver boards" prevalent in other systems.

Figure 3: Sentry peripherals



Powerful Distributed Database

Each Sentry maintains a local database of users and preferences. The database is non-volatile flash memory, so the Sentry may be shut down without loss of information. Since the database is local, network interruptions are not noticeable to the end user.

Each user may have their access restricted to specific days of the week or even specific times of the day, measured in half-hour blocks. Users may be tagged with an expiry date, or optionally may expire after a certain number of uses. Users may also be marked to expire after a specified amount of idle time, and can be forced to change their password after a pre-determined time interval.

Table 1: Database Capacity

Item	**Capacity**
Users	16,000 per sentry
Conferences	600 pre-scheduled facility bookings
Public Holidays	140 full-day or half-day holidays

Access Technology

Many different access technologies are provided (table 2). Any single user may be assigned keypad access plus one other technology.

Table 2: Access Technologies

Technology	**Status**
Keypad	Built-in
Infra-red	Built-in
Magnetic swipe card	Optional
Touchkey	Optional
Proximity identification	Optional
Smart card	Optional

In addition to straightforward door access, each user may be granted control over any combination of the following:

- Door locking behaviour
  - permanently lock
  - permanently unlock
  - unlock by time
  - unlock for current day
- Overhead lighting control
  - lights on
  - lights off
  - toggle lights

- Motion security system control
  - motion detection on
  - motion detection off
  - toggle motion detection
- ECS control
  - specified port on
  - specified port off
  - toggle specified port
  - all ECS ports on
  - all ECS ports off
  - toggle all ECS ports
- Siren control
  - toggle siren

(Essentially, "control" means that entry of an access code tagged with one of these special options enables that option when the user enters that code.)

Surveillance

Each Sentry may be interfaced to a range of sensing devices, both in-built and external. The Gatekeeper application is used to determine what actions are taken by the Sentry if a sensor changes. A brief list of devices is shown below.

Table 3: Connectable sensors

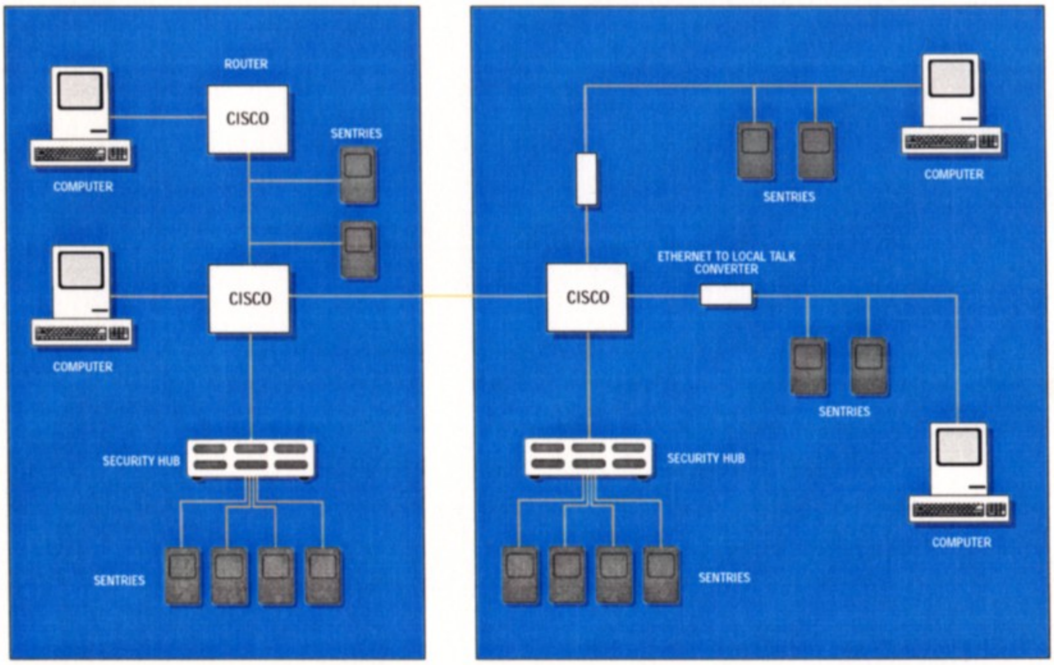
Sensor	**Status**
Light intensity	Built-in
Motion detection	Port provided for external sensor
Tamper detectors	Built-in
Comprehensive power protection	Built-in
Locking mechanism override detection	Built-in
Locking mechanism short circuit detection	Built-in
Four analogue inputs for custom sensors	Ports provided
Analogue surveillance camera	Via QBUS expansion card
Analogue conferencing camera	Via QBUS expansion card
Breakage detector	Via ECS expansion
Trip switch	Via ECS expansion
Window monitor	Via ECS expansion
Boom gate	Via ECS expansion
Etc.	

Integrated Network

Sentries communicate to each other (and the outside world) using the LocalTalk network protocol. LocalTalk is AppleTalk running over twisted pair cable, and is clocked at 230.4 kilobaud. Existing cabling may be used, or new cabling structures can be cheaply installed. Although there is a physical limit on the number of devices that a single LocalTalk network can support, routers and bridges may be used to expand this number almost indefinitely — locally, nationally or internationally.

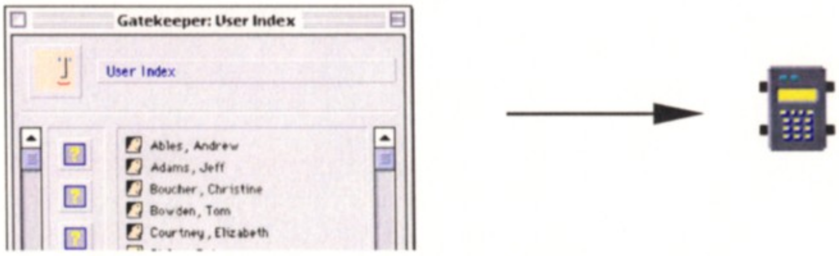
The network is a fundamental aspect of the Gatekeeper security system, since it is used to convey user, preference and security information between Gatekeeper Sentries and the Gatekeeper computer application. Although the network is required to configure each Sentry and to receive notification of security conditions, severing the network will not impede the operation of each Sentry in any way. In addition, all network messages are encrypted and authenticated to prevent unauthorised tampering.

Figure 4: Example AppleTalk network topology



The LocalTalk network is used to convey a variety of information to and from each Sentry.

1. Users

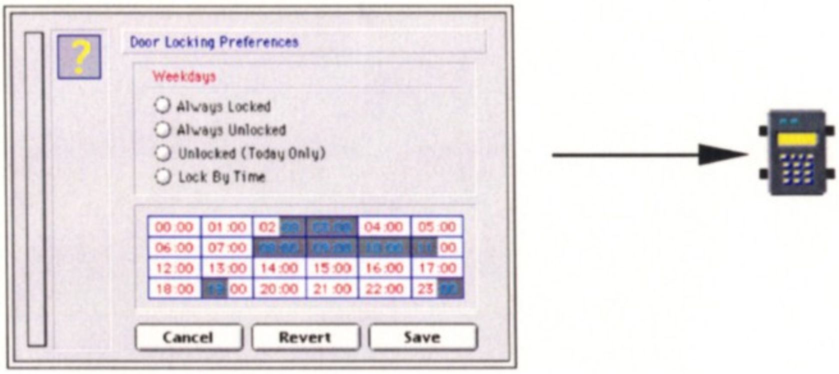


Gatekeeper: User Index

User Index

Ables, Andrew
Adams, Jeff
Boucher, Christine
Bowden, Tom
Courtney, Elizabeth

2. Preferences



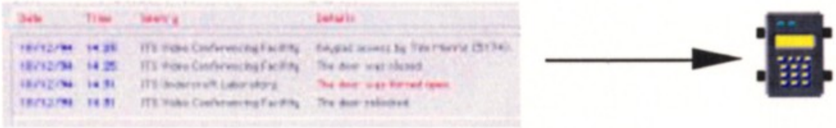
Door Locking Preferences

Weekdays

○ Always Locked
○ Always Unlocked
○ Unlocked (Today Only)
○ Lock By Time

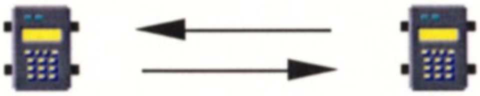
00:00	01:00	02:00	03:00	04:00	05:00
06:00	07:00	08:00	09:00	10:00	11:00
12:00	13:00	14:00	15:00	16:00	17:00
18:00	19:00	20:00	21:00	22:00	23:00

3. Security information



Date	Time	Sentry	Details
18/12/96	14:25	ITS Video Conferencing Facility	Keypad access by [illegible]
18/12/96	14:25	ITS Video Conferencing Facility	The door was closed
18/12/96	14:51	ITS Undercroft Laboratory	The door was forced open
18/12/96	14:51	ITS Video Conferencing Facility	The door relocked

4. Inter-Sentry messages



Logging

Each Sentry maintains an internal log of all transactions. These include standard door accesses, utility transactions (such as on-site password changes and door arming transitions) and exception conditions such as motion detection, forced entry and attempts to guess passwords. In all, seventy-seven distinct events are logged. Each entry is stamped with the precise date and time at which it occurred. The Gatekeeper application is used to examine and store these logs for future reference. Log events are dispatched in real time, so notification of security conditions is instant and effective. Tools are provided so that individual users may be traced.

Reliability

Key aspects of any security system are resistance to failure and resistance to external tampering.

- The Gatekeeper Sentry has been designed so that all vital power sources are internal to the unit.
- Mercury and cover switches detect any attempt to tamper with the Sentry.
- Sensors have been employed to detect short circuit conditions on all external door latches, relays and devices drawing power from the internal supply. Due to the internal modular design, these conditions will not impede normal operation of the unit because each operational section is isolated upon failure.
- Attempts to override the locking relay by applying an external voltage to the door mechanism are detected.
- Failure of integral components such as the real time clock, non-volatile memories and liquid crystal display are detected and immediately reported.
- The Sentry firmware is stored in non-volatile memory which may be reprogrammed over the network in under ten seconds.
- The activation of important solenoids and protection equipment (such as sirens and pyro sensors) is confirmed by the Sentry by means of measured current consumption.

Gatekeeper Security Hubs

Supplying power and network services to a large collection of disparate Sentries can pose logistical and managerial problems. Large installations require an integrated approach to security management. The Gatekeeper Security Hub delivers an effective solution.

Figure 5: A Gatekeeper Security Hub

The Security Hub is a rack-mountable enclosure supplying power and data services to a collection of Sentries. It also provides thirty (30) ECS ports for connection to external devices (see below).

Services

The Gatekeeper Security Hub supplies power and network services to up to sixteen (16) Sentries. Each port includes comprehensive protection. Faults on ECS ports result in isolation of the port, and appropriate action taken to notify the operator. The Security Hub is enclosed in an industry standard 19" rack, which via stacking can provide services to installations requiring an unlimited number of zones and customised services.

Surveillance

Each hub includes thirty (30) ECS ports. An ECS port is a general-purpose port containing three inputs, an output, and protected power. Each port may be connected to a variety of security products (table 4). Almost any "on/off" style device may be interfaced to ECS.

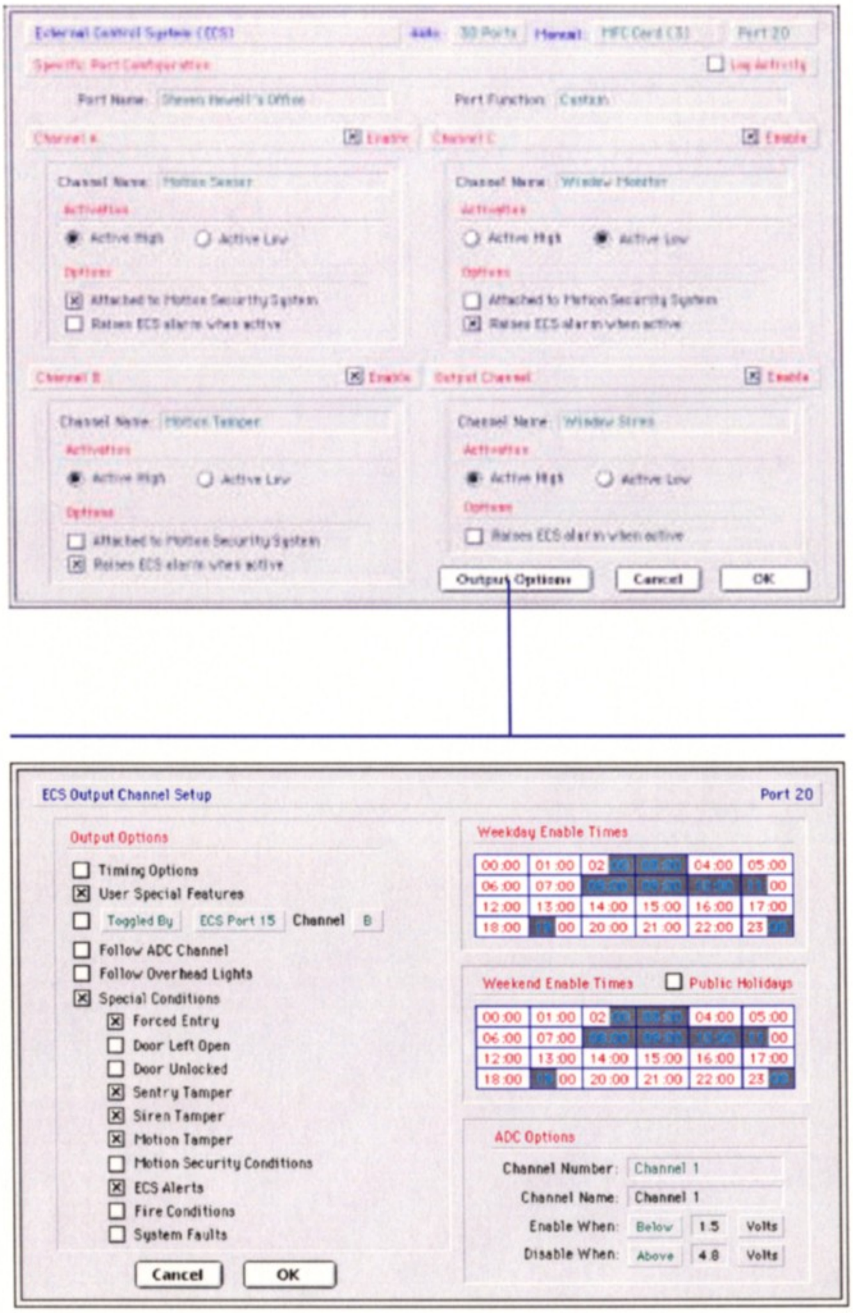
Table 4: Example ECS devices

Devices

Motion sensor
Security light
Beacon
Siren
Boom gate
Window monitor
Pressure pad
Mercury switch
Electronic latch

The Gatekeeper application is used to instruct the Security Hub on what action is taken if a sensor becomes active, and at what time or under what conditions output devices should be activated. Extreme flexibility is provided when configuring these options (figure 6).

Figure 6: ECS port configuration



External Control System (ECS) Auto: 30 Ports Manual: MFC Card (3) Port 20

Specific Port Configuration ☐ Log Activity

Port Name: Steven Hewell's Office Port Function: Custom

Channel A ☒ Enable

Channel Name: Motion Sensor

Activation

● Active High ○ Active Low

Options

☒ Attached to Motion Security System

☐ Raises ECS alarm when active

Channel C ☒ Enable

Channel Name: Window Monitor

Activation

○ Active High ● Active Low

Options

☐ Attached to Motion Security System

☒ Raises ECS alarm when active

Channel B ☒ Enable

Channel Name: Motion Tamper

Activation

● Active High ○ Active Low

Options

☐ Attached to Motion Security System

☒ Raises ECS alarm when active

Output Channel ☒ Enable

Channel Name: Window Siren

Activation

● Active High ○ Active Low

Options

☐ Raises ECS alarm when active

ECS Output Channel Setup Port 20

Output Options

☐ Timing Options

☒ User Special Features

☐ Toggled By ECS Port 15 Channel B

☐ Follow ADC Channel

☐ Follow Overhead Lights

☒ Special Conditions

- ☒ Forced Entry
- ☐ Door Left Open
- ☐ Door Unlocked
- ☒ Sentry Tamper
- ☒ Siren Tamper
- ☒ Motion Tamper
- ☐ Motion Security Conditions
- ☒ ECS Alerts
- ☐ Fire Conditions
- ☐ System Faults

Weekday Enable Times

00:00	01:00	02:00	03:00	04:00	05:00
06:00	07:00	08:00	09:00	10:00	11:00
12:00	13:00	14:00	15:00	16:00	17:00
18:00	19:00	20:00	21:00	22:00	23:00

Weekend Enable Times ☐ Public Holidays

00:00	01:00	02:00	03:00	04:00	05:00
06:00	07:00	08:00	09:00	10:00	11:00
12:00	13:00	14:00	15:00	16:00	17:00
18:00	19:00	20:00	21:00	22:00	23:00

ADC Options

Channel Number: Channel 1

Channel Name: Channel 1

Enable When: Below 1.5 Volts

Disable When: Above 4.8 Volts

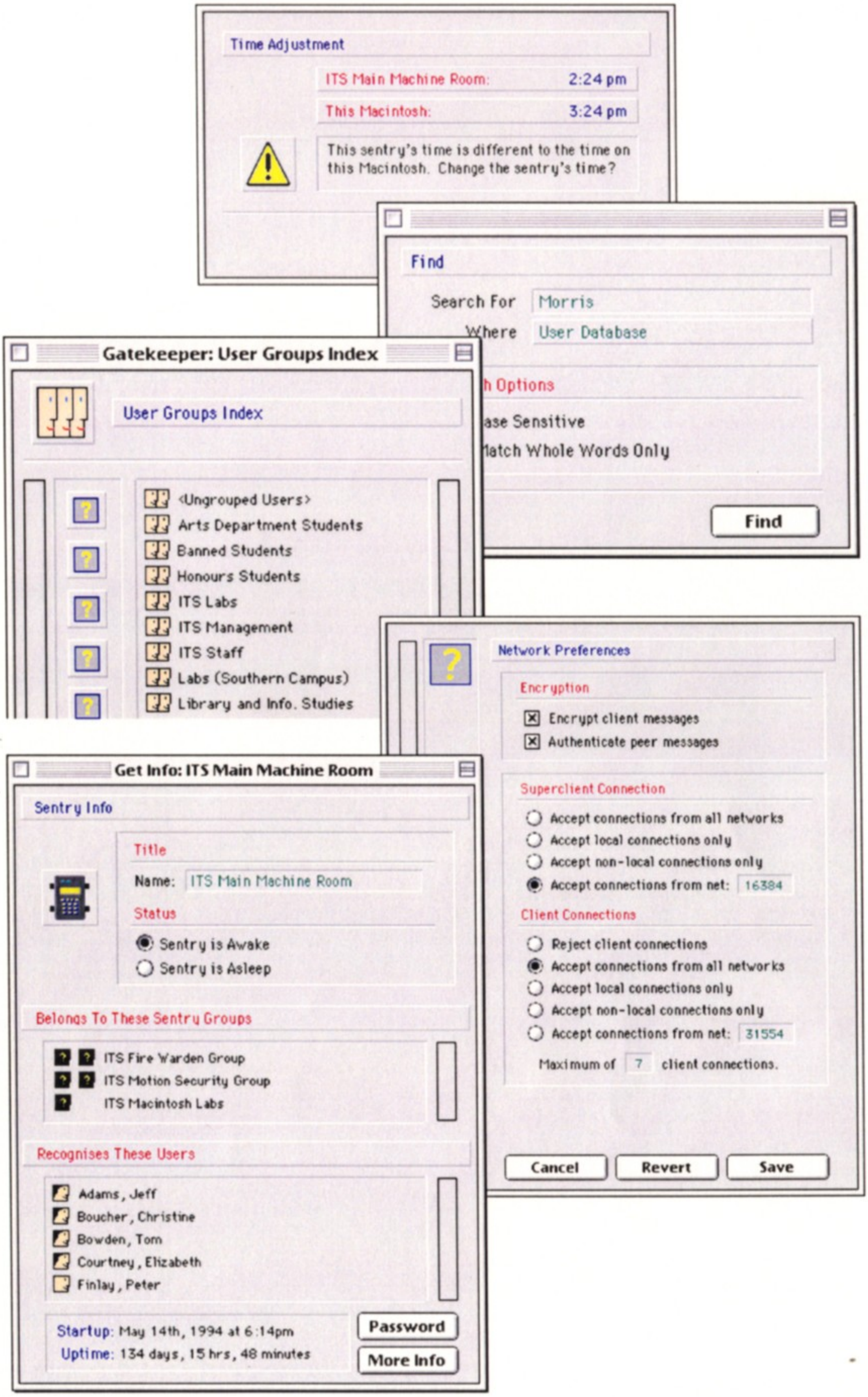
The Gatekeeper Computer Application

The Gatekeeper application is used to manage the security network. All operational parameters may be set from this application using a state-of-the-art point-and-click interface. These include major functions such as the allocation of access codes and configuration of the Sentry arming behaviour, through to minor details such as digital volume and contrast control. Network transactions with the Sentry may occur at any time without affecting the performance of the Sentry. Sentries operate independently of the application, which may be shut down with only marginal loss of system functionality. (The application is required as a server for e-mail, facsimiles and voice mail if these options are enabled.)

Power and Flexibility

The Gatekeeper application delivers remarkable ease of use coupled with unsurpassed power and flexibility. Each window and dialog affords an intuitive, streamlined means of managing the security network. The Gatekeeper design paradigm has resulted in state-of-the-art computer software.

Figure 7: Gatekeeper in action



Time Adjustment

ITS Main Machine Room: 2:24 pm

This Macintosh: 3:24 pm

This sentry's time is different to the time on this Macintosh. Change the sentry's time?

Find

Search For: Morris

Where: User Database

h Options

ase Sensitive

latch Whole Words Only

Gatekeeper: User Groups Index

User Groups Index

- <Ungrouped Users>
- Arts Department Students
- Banned Students
- Honours Students
- ITS Labs
- ITS Management
- ITS Staff
- Labs (Southern Campus)
- Library and Info. Studies

Network Preferences

Encryption

☒ Encrypt client messages

☒ Authenticate peer messages

Superclient Connection

○ Accept connections from all networks

○ Accept local connections only

○ Accept non-local connections only

● Accept connections from net: 16384

Client Connections

○ Reject client connections

● Accept connections from all networks

○ Accept local connections only

○ Accept non-local connections only

○ Accept connections from net: 31554

Maximum of 7 client connections.

Get Info: ITS Main Machine Room

Sentry Info

Title

Name: ITS Main Machine Room

Status

● Sentry is Awake

○ Sentry is Asleep

Belongs To These Sentry Groups

- ITS Fire Warden Group
- ITS Motion Security Group
- ITS Macintosh Labs

Recognises These Users

- Adams, Jeff
- Boucher, Christine
- Bowden, Tom
- Courtney, Elizabeth
- Finlay, Peter

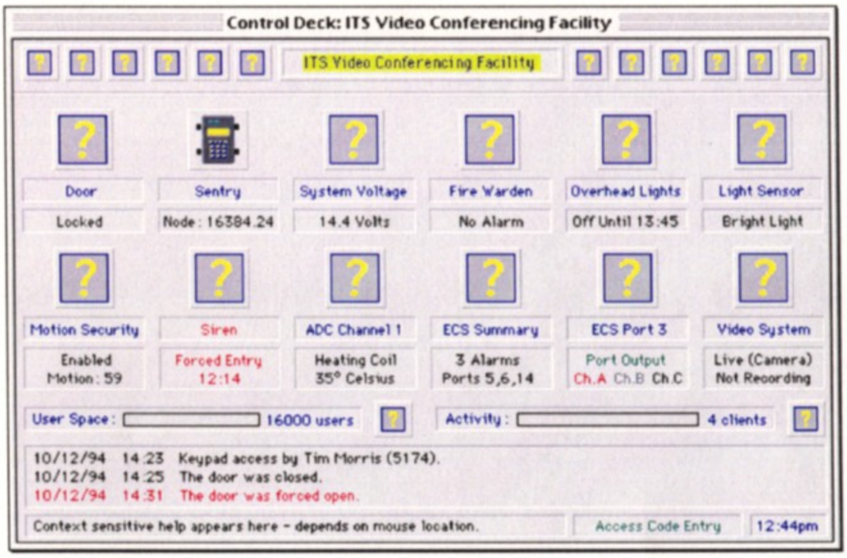
Startup: May 14th, 1994 at 6:14pm

Uptime: 134 days, 15 hrs, 48 minutes

Live Monitoring

Up to eight applications may connect to each Gatekeeper Sentry and "spy" on its operations in real time. The state of each door (open/closed, locked/unlocked) is graphically displayed in a status window (figure 8). Additional conditions such as motion detection and sudden changes in light levels are also shown. All security messages from the Sentry are summarised in a log-extract at the bottom of each window. Alarm conditions are readily and instantly brought to the attention of operators. Doors may be locked or unlocked remotely from any authorised workstation.

Figure 8: Live monitoring



Control Deck: ITS Video Conferencing Facility

ITS Video Conferencing Facility

Door	Sentry	System Voltage	Fire Warden	Overhead Lights	Light Sensor
Locked	Node : 16384.24	14.4 Volts	No Alarm	Off Until 13:45	Bright Light
Motion Security	Siren	ADC Channel 1	ECS Summary	ECS Port 3	Video System
Enabled Motion : 59	Forced Entry 12:14	Heating Coil 35° Celsius	3 Alarms Ports 5,6,14	Port Output Ch.A Ch.B Ch.C	Live (Camera) Not Recording

User Space : 16000 users

Activity : 4 clients

```
10/12/94  14:23  Keypad access by Tim Morris (5174).
10/12/94  14:25  The door was closed.
10/12/94  14:31  The door was forced open.
```

Context sensitive help appears here – depends on mouse location.

Access Code Entry

12:44pm

Independence

All Sentries function independently from the application. If Gatekeeper is shut down, all units continue to operate normally. Upon resumption of program operation, each Sentry forwards a log of transactions detailing all events that occurred in the interim, which may be examined immediately or at the user's convenience.

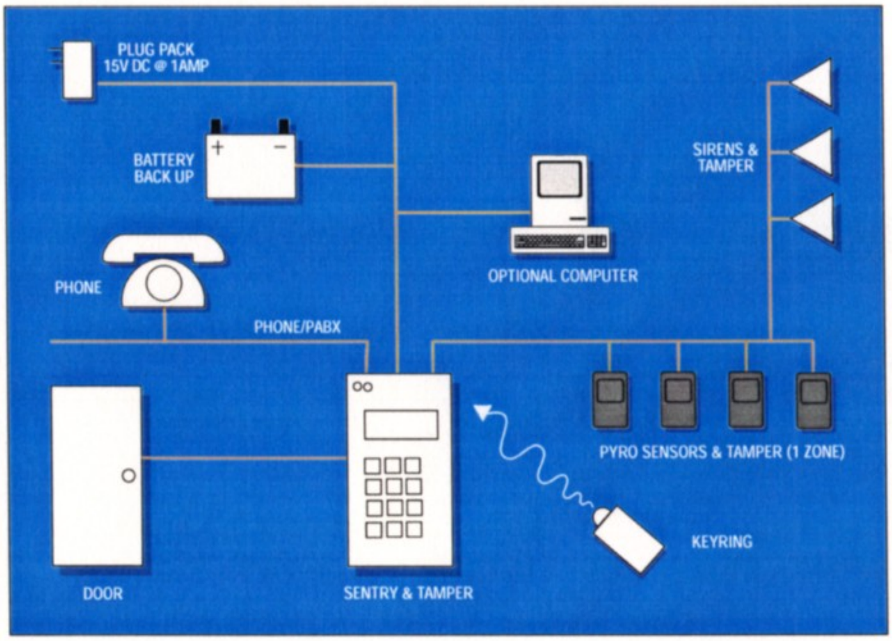
Sample Solutions

Gatekeeper is a scalable security solution, meaning that it can be applied to small sites consisting of a handful of Sentries through to national building networks. Listed below are sample schematic layouts indicating how the components of the Gatekeeper security system may be interlinked to solve a variety of security requirements.

Single Sentry Installation (Home Solution)

The simplest Gatekeeper configuration is a single Sentry, typically installed in a household or small facility.

Figure 9: Single Sentry installation.

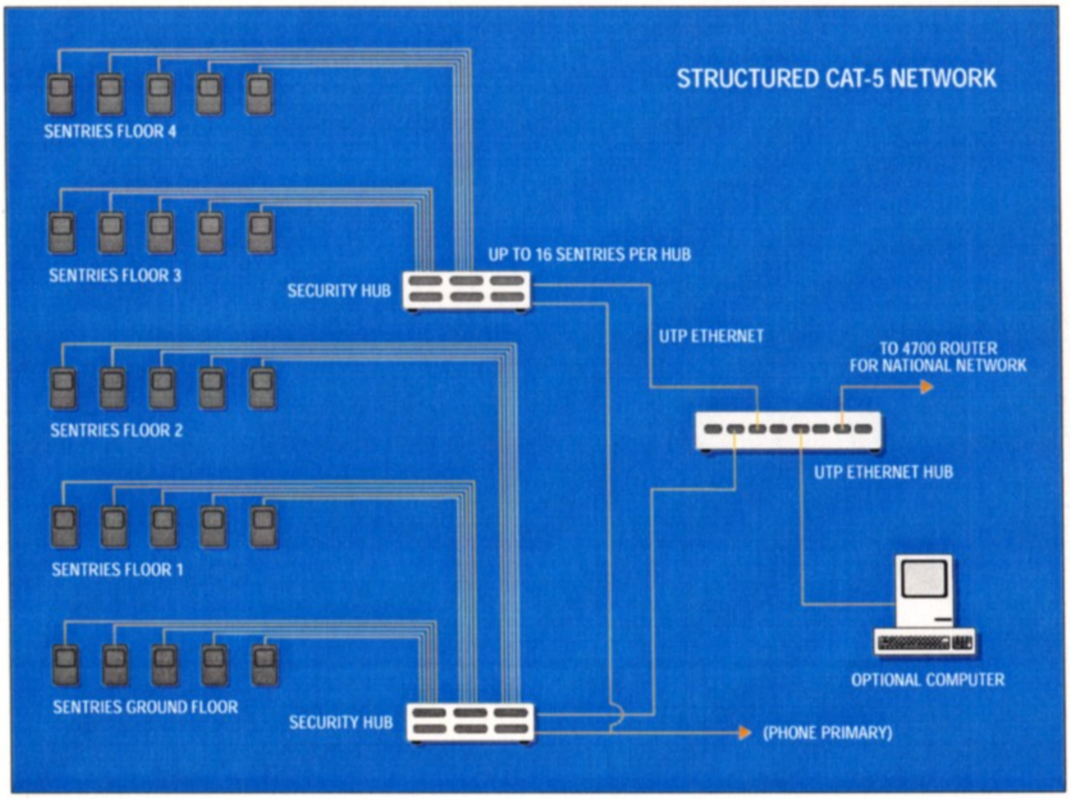


The Sentry can be delivered pre-programmed with users, or, for optimum performance, the Gatekeeper application may be used to manage the unit.

Multiple Sentry Installation (Building Solution)

Building management is provided by a collection of Sentries and one or more Security Hubs. The Hub supplies power and data services to each Sentry, whilst providing comprehensive building monitoring. All Sentries and the Hub are managed using the Gatekeeper software.

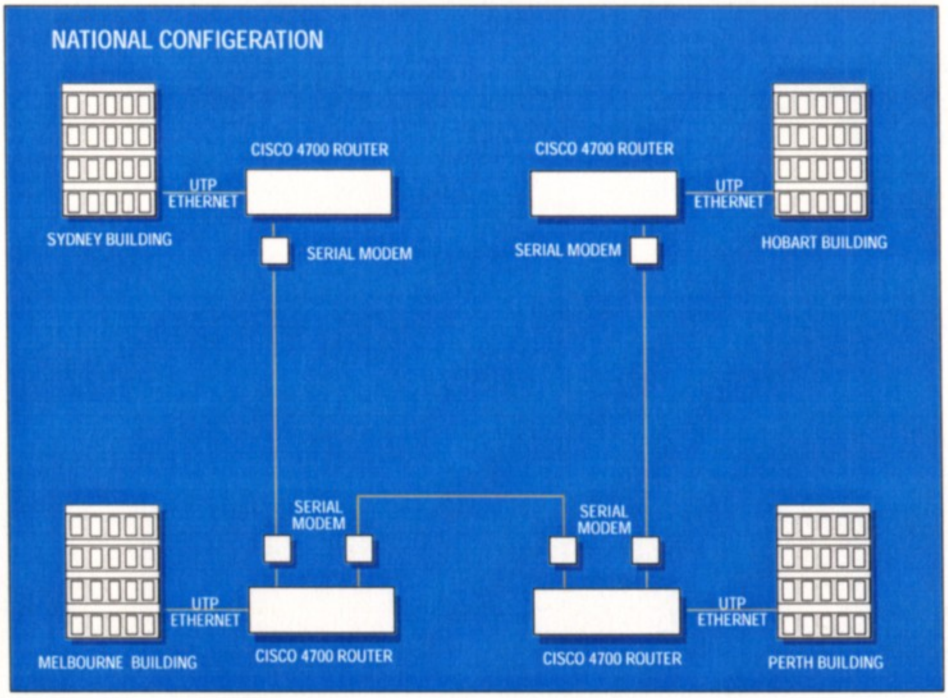
Figure 10: Multiple Sentry installation.



Multiple Site Installation (National Solution)

Multiple sites may be managed by extending the AppleTalk network to encompass each site. One method of implementing this requirement utilises a leased line modem link between two AppleTalk capable routers, such as the Cisco 2505 or Cisco 4700.

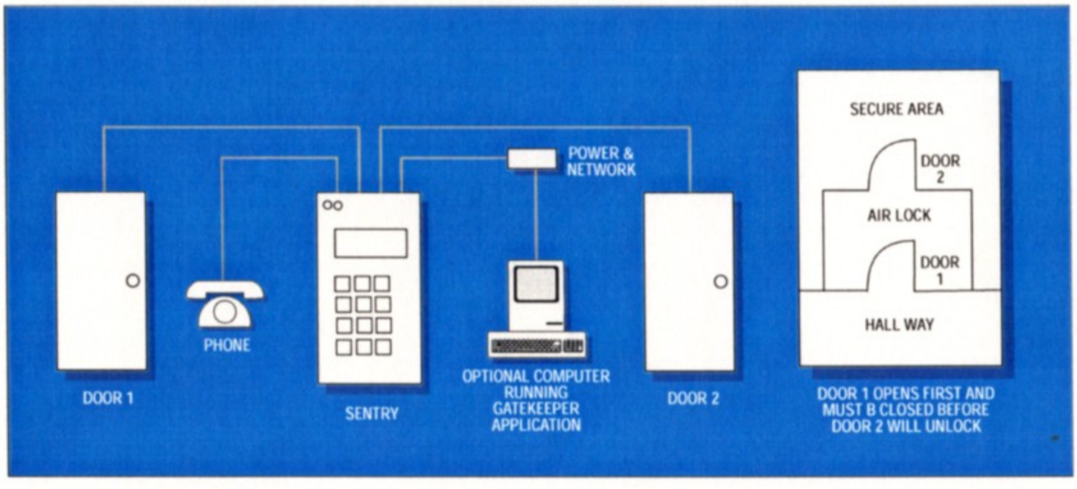
Figure 11: Multiple site installation.



Airlock Installation (Specialised Facility)

A variant installation is the airlock. In this configuration, two doors are controlled by a single Sentry. The doors are synchronised so that only one may be unlocked or opened at a time.

Figure 12: Airlock installation.



Other Installations

Due to Gatekeeper's unprecedented flexibility and open-network architecture, almost any security requirement can be catered for. Gatekeeper puts the power at your fingertips; security management will never be the same.