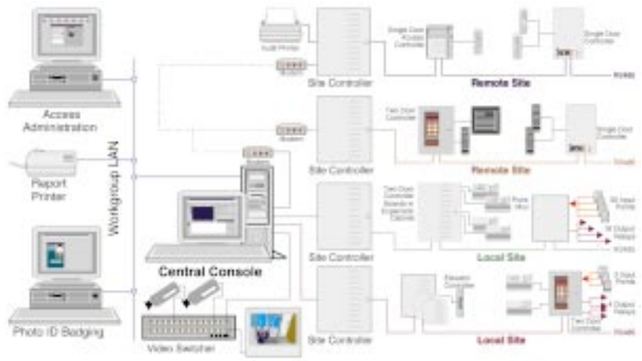
Guardall



INOVA Central Manager System Specifications:

Database Capacity	System and event databases sizes are limited only by the available hard disk capacity.
Transaction Capacity	75,000 transactions/day
Communications	Four (4) RS232C serial ports *Direct connect to local Site Controller panel(s) or* *Dial-up modems with remote Site Controller panel(s)*
Reporting	
Output Devices:	Screen, Printer or File
Database Reports:	10
Activity Reports:	12
Automatic Activity Reports:	Daily and/or weekly reporting

Personal Computer Guidelines:

	Recommended System
Personal Computer:	PC with Intel Pentium™ processor, ≥ 233 MHz
Memory:	≥64 Mb RAM
Graphical User Interface:	Microsoft Windows '95™ or Microsoft Windows for Workgroups™ 3.11 with MS-DOS 6.x
Monitor & Video Adapter:	800x600 pixel resolution in 256 colours ≥15" diagonal, ≤.28 mm dot pitch & ≥70 Hz refresh
Mass Storage:	≥ 1 Gb EIDE or SCSI disk drive, ≤ 10 ms seek time 3.5" 1.44 Mb floppy disk drive CD-ROM drive
Communications ports:	Bus mouse 1 serial port with 16550 type UART & unique IRQ per Site Controller panel
Optional Modem(s):	9600 bps, 100% Hayes™ compatible asynchronous
Printer:	Laser or inkjet printer

For complete computer specifications, consult Guardall's *INOVA Central Manager PC Requirements* document.

Included with the INOVA Central Manager Access Management Software:
- Software on 3.5" diskettes or CD-ROM with activation key
- Serial port expansion board
- Manual

Other Required Items:
- Suitably configured personal computer
- Site Controller(s) panels
- Guardall door controllers
- Card, key or token readers
- Identification cards, keys and/or tokens
- Electric strikes and/or magnetic locks
- Cabling, power supplies, backup batteries, etc.

Optional Items:
- CCTV video switcher, cameras & VCR
- Modem(s)
- Elevator controller(s)
- Point Multiplexer(s)
- Printer
- Second serial port expansion board
- Access administration client(s)
- Integrated photo ID card badging option
- Advanced reporting option
- Database card import option

Available from Guardall

All Guardall products are warranted against defects in workmanship or materials (details available upon request).

Installation guidelines are included in the instructions provided with each unit. Installers are responsible for knowing and complying with any local regulatory fire and building codes.

In the interests of improving quality and design, the right to amend specifications without giving prior notice is reserved.

SUPPLIER:

48-0161 A (8.5" x 11") Rev 1.4

Guardall

ACCESS MANAGEMENT SYSTEM SUITABLE FOR COMMERCIAL AND INDUSTRIAL ENVIRONMENTS

Access Control of Who Goes Where and When

- ❑ Determine who can go where and when from one central location
- ❑ Restrict access to valuable assets and information to those who *need* to have access *when* they need to
- ❑ Centrally manage multiple local and/or remote sites
- ❑ Establish different access security for different areas and floors
- ❑ Automatically change access requirements to reflect security changes based on the time of day and day of the week

Easy Central Administration

- ❑ Microsoft Windows™ compatibility reduces training time & costs
- ❑ Standard forms for regular activities like adding new card holders
- ❑ Groupings of people provides flexibility for multiple departments, operations and facilities
- ❑ Manually lock and unlock doors to handle exceptional situations
- ❑ Authority levels allow access to system information by people in different functions
- ❑ Other applications can be run on the same personal computer

Management Review of Who Went Where and When

- ❑ Access records prevent losses by establishing a belief that undesired activity will be found out
- ❑ Generate automatic daily or weekly reports for review of activity
- ❑ Clarify suspicious activity using manual reports
- ❑ Examine resource utilization by reviewing asset movement

Effective Event Monitoring

- ❑ Alarms identify their importance or priority using colour coding
- ❑ Alarms are related to maps and user-defined instructions to ensure prompt and appropriate response
- ❑ Maps quickly focus operators on events' location(s)
- ❑ Operator notes facilitate investigation of incidents

INOVA®
CENTRAL MANAGER

Access Management & Event Monitoring System

If you value peace of mind as the owner or property manager of commercial or industrial facilities, then an INOVA® Central Manager system is the most valuable purchase you can make for yourself and those using your facilities.

INOVA Central Manager systems give you control of access throughout your facilities by letting you determine who goes where and when. Effective control is provided for both your local site and remote sites communicating via telephone lines.

Restrict access to valuable assets and information to those with a need for access and at appropriate times. Appropriate times can include no restrictions at some times, use of an identification card, up to use of a personal identification number (PIN) with cards to verify that the person using a card is the person authorized to use it.

Where risk management requires limiting movement into areas where hazards or hazardous materials exist, then access can be restricted to two people at a time, or two people where one person is a designated escort.

Reporting who went where and when provides the deterrent needed for effective loss prevention. Automatic reports can help flag suspicious activity or events. Manual reports can then be used to investigate or monitor activity to resolve these incidents. The ability to generate reports based on criteria you define makes this package ideal for multiple tenants or departments requiring separate reporting.

The monitoring capability of INOVA Central Manager software lets you respond to exceptional events. When a prioritized event alarm is received, operators have access to both a map to locate the event and specific instructions on how to respond to it. There is even the ability to command changes right from the central system without physically going anywhere.

QUALITY SECURED

1. Management Information

Find out what happened in your facility . . . and when. Every granting of access, every denial of access, every alarm and every command is recorded with the time of the event and who was involved. Managers can review this information using a wide variety of reports – ranging from all activity at a facility to transactions involving a single person to any overnight alarms received. Reports can be based on your own selected criteria.

Reporting capabilities justify investment in access control. Losses are prevented by establishing a belief that undesired activity will be found out.

Schedule daily or weekly reports to run automatically for review by individual managers, or grouped by department for distribution. Immediate reports can be requested for incident investigation, follow-up on unusual activity, special projects, or ad hoc review.

Standard activity reports include: all valid transactions, all invalid transactions, all alarms, access by department, access to specific areas, access by individual people or vehicles.

Standard database reports include: authorized card holders, temporary cards, automatic commands, door and floor lists and pending card updates.

2. Monitoring

Monitor what is happening in your facility right now. Information from sensors and control devices is presented in the event window as it is received. You see an event description, time and location along the name of the person involved. High priority alarms pop through an alert when other applications are being used.

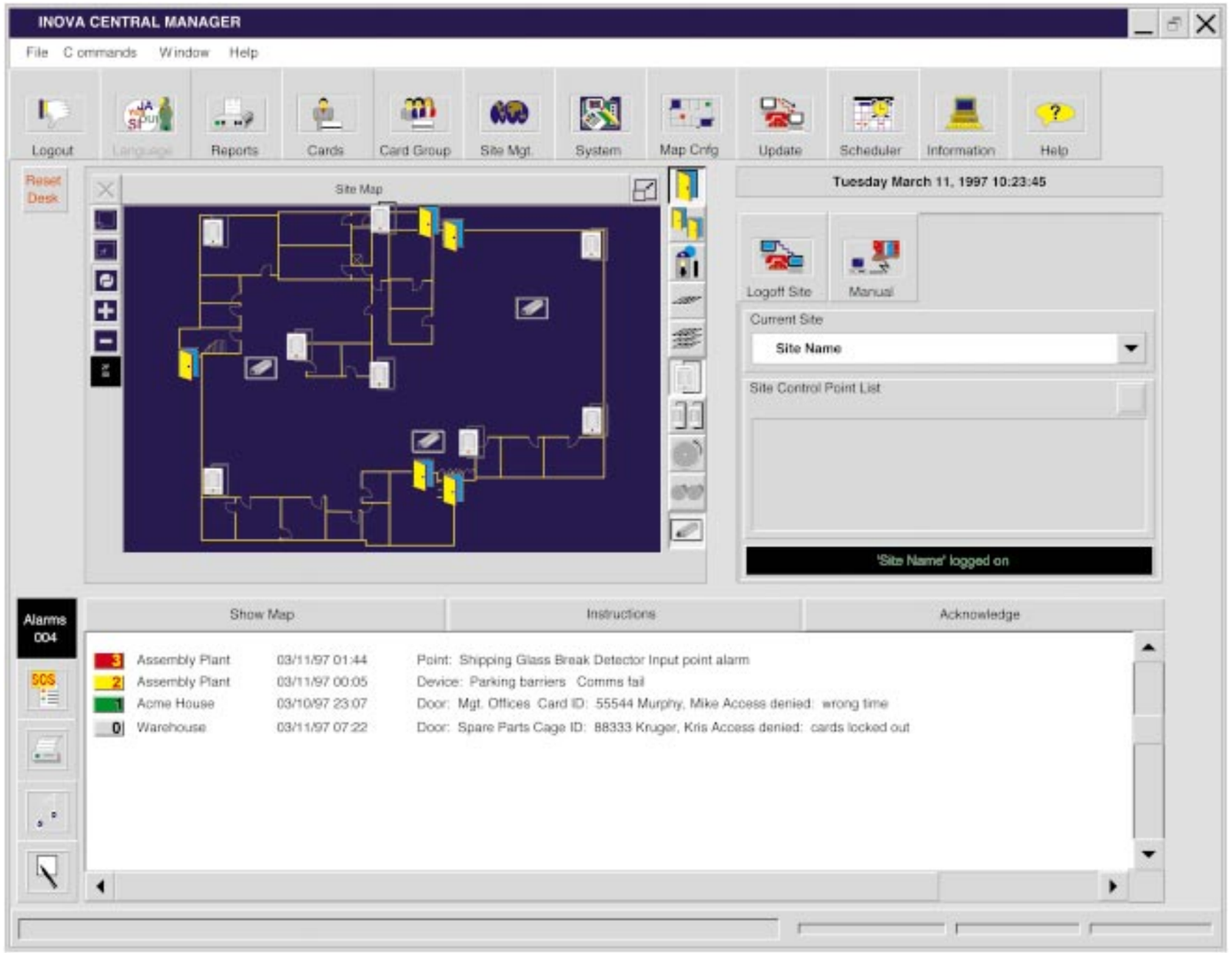
Request more information. See event locations on a facility map – zoom in for a more detailed view if needed. Request a view from a video camera. Review pre-defined response instructions. General emergency response instructions are only a click away as well. When needed, record notes about particular events for later review.

Priority groupings of significant events:

Alarm events reflecting unexpected, and likely undesired, activity as reported by sensors and detectors.

Access alarms telling of entry under duress or unauthorized intrusion attempts including doors forced or held open, requests from invalid cards, or requests during invalid time periods.

Audit information of communications and system activity.



3. Access Administration

Access administration is easy with a standard Microsoft® Windows™ interface. All card administration and system administration is done from a central personal computer. Card data, access security levels, and time schedules are all set up with Windows forms. Groupings of people, doors, floors and schedules make simple work of giving individuals access to multiple facilities and managing numerous people at single or multiple sites.

Numerous access schedules can be assigned to each controlled entrance. These time zones allow one or two time access intervals for both regular or shift schedules. Access schedules can differ for each day of the week and offer two different holiday schedules as well.

Card security options include free access (no card required), access card required and access card + personal identification number (PIN) required. Cards can have future validation dates and temporary cards with expiry dates can be issued.

Access security options include: single card, dual card, escorted dual card access plus supervisory lockout and anti-passback.

Integrated video badging option allows recording and retrieval of card holders pictures as they appear on photo identification access cards.

4. Command Control

Command control addresses your dynamic security needs. Scheduled, manual and input response commands are available to lock & unlock entrances; change card security; change access requirements; activate & deactivate devices; shunt & unshunt alarm monitoring points and groups of points; generate activity reports; and activate lights, bells & buzzers.

Change security levels automatically depending upon time and day. Unlock a door for unrestricted access during business hours and switch to card only access during evenings. Shunt alarm systems and activate lighting systems as well.

Program commands to respond to alarms or monitoring sensors. This automatically provides appropriate response by activating central station dialers, alarm bells or buzzers, lights and/or video cameras.

Manually command action from the central workstation. Operators are given the tools to respond to unexpected or occasional events. Lock and unlock doors. Check status of entrances. Add and delete access authority. Shunt and unshunt alarm sensors. Request CCTV camera views.