



iSTAR is an Ethernet-ready embedded control panel for enterprise-side security management. Intended for use by both corporate security and information technology managers, the iSTAR controller represents a new way to organize and deploy security management solutions by seamlessly integrating with an existing network infrastructure.

Designed with the network in mind, the iSTAR controller enables integration of various event management applications into one single embedded controller.

At the heart of iSTAR is the General Controller Module (GCM). The GCM integrates Windows® CE operating system, Motorola's PowerPC™ processor, network and communication ports, expandable memory and a PC Card Type III slot. The GCM also supports up to two Access Control Modules (ACM) for versatile reader system integration and flexibility.

## FEATURES & BENEFITS

- Ethernet Ready
- Embedded Operating System
- Seamless Integration with C•CURE 800/8000
- Wide Range of Alarm Monitoring
- Advanced Clustering
- Global Anti-Passback by Cluster
- Worldwide Compliance
- Redundant Communications
- Supports up to 16 RM or Wiegand Readers
- Web Diagnostics
- Expandable On-Board Memory
- Secure Communications
- Easily Upgradeable
- Intrusion Zones (version 2.2)
- Keypad Commands (version 2.2)
- Field upgradeable 32 MB and 64 MB SIMMs available

## FEATURES

iSTAR™ is an intelligent, modular controller designed to integrate various event management applications on one controller, providing ease of installation and interoperability among vital applications.

With the innovative iSTAR technology, all database event-directed actions can be downloaded to the controller from the host, enabling local management of events versus host management of events, i.e., door lock/unlock, global anti-passback control by cluster, etc. All communication is asynchronous and no polling is necessary to minimize network traffic.

### General Controller Module (GCM)

The GCM is the base controller card designed around the Windows® CE operating system and Motorola's PowerPC™ processor. It includes network and communication ports, expandable memory and a PC Card Type III slot.

Each GCM supports up to two access control modules (ACM), with eight readers each. The GCM also has embedded support for three unsupervised inputs to detect low battery, power failure and cabinet tamper.

Configuration information sent from the host to the iSTAR controller informs the ACM of monitor inputs, process card data, control card readers and set outputs. Card reader and output states may be affected directly by user commands at the host or by configured time specifications. All access control decisions (door and elevator) are made by the iSTAR controller and are stored as transactions. All information is stored locally in memory.

### Access Control Module (ACM)

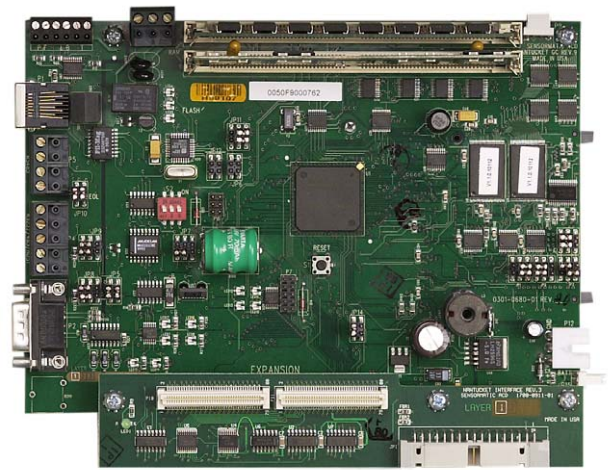
Each ACM has 16 supervised inputs and 8 outputs for door control, and can include a combination of RM series or Wiegand type readers.

The ACM provides LED indicators, which allow for visual inspection of status. Two inputs and two outputs on the RM module provide additional flexibility and expandability. Additional add-on input and output boards are available (I/8 and R/8).

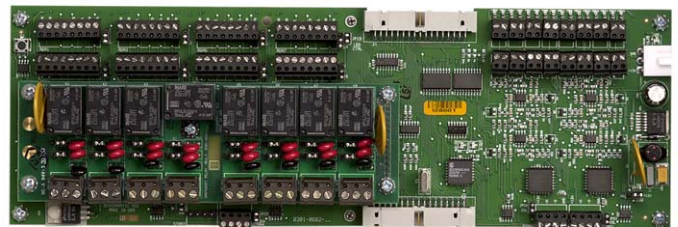
### Global Anti-Passback By Cluster

iSTAR controllers allow the sharing of cardholder anti-passback status among controllers in a C•CURE area within a cluster. Global anti-passback lets you set up areas with doors on any controller in the cluster, dividing a facility into regions to keep track of cardholder locations. Anti-passback violations include a cardholder passing back a card for another person to use (the system receives two access requests for the same card), and tailgating, in which a cardholder follows another cardholder into a region. A timed anti-passback violation occurs when a person tries to access the same area more than once during a specified period.

Consider the example where a user wants to enforce anti-passback for entrance/exit to a parking facility. The operator would place all iSTAR controllers containing parking garage readers in a cluster, define an area for all doors/access points containing those readers, and activate anti-passback for the area. With or without host communication, anti-passback integrity will be maintained and managed by the cluster.



General Controller Module (GCM)



Access Control Module (ACM)

## Data Security

Secure communication is provided at every level of iSTAR including host/master controller, master/alternate master, and alternate master/members. Encryption is provided through RSA Data Security's RC4 technology implemented using Microsoft CryptoAPI. Multi-key authentication for real-time communication and password authentication for use with the local diagnostic/configuration utility provide a barrier against intrusion into iSTAR.

## Configurations Diagnostics

iSTAR utilizes an IP address as its unique communication identifier. Each GCM has an encoded hardware identifier that links to the IP address. Addressing and other initial configuration information is done through a program running on any PC. All other information is downloaded from the C•CURE 800/8000 host.

Diagnostics can be done through any computer with a network path to an iSTAR controller. In addition, real-time status and diagnostics can be accessed remotely via the Internet using a web browser, such as Internet Explorer or Netscape Navigator.

The following information can be accessed:

- Controller time/Boot time
- Total/Available memory
- Hardware (MAC) and IP address
- Connection status
- Firmware and OS versions
- Diagnostic data files

## Communications

iSTAR supports Ethernet and RS-232 communication topologies. It also contains a Type III PC Card (PCMCIA) slot for additional types of communications including a modem. iSTAR communication is point-to-point (daisy chaining is not supported). A single connection from the host supports multiple controllers through a TCP/IP subnet.

Controllers in groups of one or more are defined as a cluster. A cluster is a user-defined grouping that contains up to 20 iSTAR controllers. Each cluster has a master controller as primary connection between the cluster and the host, with an alternate master in case the master controller fails or loses network communication. The master and alternate have no differentiating properties from other controllers other than the possibility of requiring additional memory. Since the master controller communicates all event and cardholder data between the cluster and the C•CURE 800/8000 host, it may require more memory than "member" controllers. Field installable memory upgrade kits are available to increase the storage capacity of the standard 16MB iSTAR. Member controllers in the cluster do not communicate directly with the host; rather, communication to the host is through the master iSTAR controller. The member controllers can communicate directly with other member controllers as needed through the master controller for input/output event linking and anti-passback control.

Communication within a cluster is through TCP/IP over Ethernet. An alternate master controller can also be defined in case of a communication failure to the designated master controller (the member controllers will then communicate through the alternate master controller). The master controller, or alternate master, can be configured for automatic dialup communications to the C•CURE 800/8000 system if network communication is lost.

## Distributed Cluster Event Control

iSTAR supports cluster event linking based on events configured by the C•CURE 800/8000 host. This event linking is not just supported within a controller, but is also supported within a cluster.

An input activated on any iSTAR in a cluster will activate a programmed output on any iSTAR in the same cluster. It is not restricted to output following input, but also includes time-controlled events, door events, area events and others. This effectively provides global event linking without reliance on the host. Actions resulting from an event activation that are outside the programmed cluster will be supported with host intervention.

## Communications with apCs

iSTAR and apCs can operate together with a C•CURE 800/8000 host. They do not communicate directly, nor can they be connected together. However, event linking can easily be configured through the C•CURE 800/8000 host. Although these devices cannot be connected together, they can both exist on the same network.

## Intrusion Zones

Intrusion zones are user-specified groups of inputs, outputs, and doors that define a physical area. Users can define a control zone from any group of objects on the same iSTAR controller. An intrusion zone can include an entire building or laboratory, or a portion of a building or lab. Users can define a door to be unlocked when an intrusion zone is in Access mode, but not when it is in Secure mode.

Grouping inputs and doors into intrusion zones allows easy arming and disarming of physical areas. When an intrusion zone is disarmed (in Access mode), the intrusion zone inputs are disarmed and do not generate activity messages when people enter the intrusion zone. When an intrusion zone is armed (in Secure mode), it is protected. All doors are locked and all intrusion zone inputs are armed. No one can enter the intrusion zone without activating these inputs and causing the system to generate activity messages.

## Keypad Commands

Keypad commands, standard on C•CURE 800/8000 Model 10 and above, allow the user to activate events from an RM keypad connected to an iSTAR controller. A command has a unique number that will be entered on the keypad (with optional prompting) to activate a specific event, such as "unlock/lock door". The event may be configured to execute any allowable event action and thus is not limited to events affecting intrusion zone status. The command may be configured to require a card presentation and optionally a PIN to validate the command.

## SPECIFICATIONS

### Electrical

|                          |   |
|--------------------------|---|
| Power Input .....        | 90 to 260 VAC 60 Hz , 0.5 A, 47 to 440 HZ                                     |
| Power Output .....       | 12 VDC at 3.3 A maximum   |
| Power Consumption .....  | Less than 40 watts typical<br>(12 W typical with 4 RMs, 18 W with 8 RMs)      |
| Auxiliary Hardware ..... | Relay contacts rated at<br>30 V AC/DC 2.5 A inductive,<br>5.0 A non-inductive |

### Mechanical

|                              |  |
|------------------------------|--|
| Dimensions (H x W x D) ..... | 61.6 x 41.9 x 10.2 cm<br>(24.25 x 16.5 x 4.0 in)                                   |
| Unit Weight .....            | 0.49 kg (23.3 lbs)   |
| Construction .....           | 16 AWG metal wall mounted locking cabinet<br>with tamper switches on door and rear |

### Environmental

|   |                              |
|---|------------------------------|
| Operating Temperature .....                 | 0° to 70° C (32° to 158° F)  |
| Storage Temperature .....                   | -25° to 85° C (9° to 185° F) |
| Operating and Storage<br>with Battery ..... | 0° to 50° C (32° to 122° F)  |

### Typical Controller Capacity

|                                 |         |
|---------------------------------|---------|
| iSTAR type with number of Cards |         |
| 16MB iSTAR                      |         |
| Cards with 1 clearance- .....   | 70,000  |
| Cards with 10 clearances- ..... | 50,000  |
| 32MB iSTAR                      |         |
| Cards with 1 clearance- .....   | 200,000 |
| Cards with 10 clearances- ..... | 150,000 |
| 64MB iSTAR                      |         |
| Cards with 1 clearance .....    | 500,000 |
| Cards with 10 clearances .....  | 350,000 |

Note: Memory allocation within iSTAR is dynamic and shared between cardholders, event storage, and configuration information.

