



The photograph above shows full 16-reader capability

SECURITY WITHOUT BOUNDARIES

- **Ethernet Ready**

Direct Ethernet connection with each iSTAR retaining a unique IP address

- **Embedded Operating System**

Windows CE and PowerPC processor broaden application support and enhance speed

- **Seamless Integration with Host**

C•CURE 800/8000 host networks for initial database set-up, managing peripheral hardware, generating activity reports, and managing multi-cluster events

- **Wide Range of Alarm Monitoring**

Supports 2 ACMs, each providing 16 supervised inputs and 8 relay outputs (readers); I/8 and R/8 allow additional input and output modules

- **Advanced Clustering for Unmatched Event Control and Monitoring**

Distributed management is supported through communications within a cluster

- **Global Anti-Passback by Cluster**

Stops or restricts access of personnel attempting to utilize the same security badge

- **Password Protected Web Based Diagnostics**

Remote diagnostics utilizing any networked computer, Web browser, and known iSTAR IP address

- **Expandable On-Board Memory**

On-board memory options supporting expanded databases/events and future add-on functionality

- **Secure Communications**

Industry tested encryption and multi-key authentication for enhanced security

- **System for the Future**

Easily upgradeable flash ROM with future releases

- **Worldwide Compliance**

FCC, CE, C-Tick, UL 294 and UL 1076

C•CURE® iSTAR is an Ethernet ready embedded controller.

iSTAR is designed to integrate various event management and network interoperability among vital security applications. At the heart of the iSTAR architecture is the General Controller Module (GCM). The GCM design integrates Microsoft®'s 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.

Database event-directed actions can be downloaded to the controller from the C•CURE 800/8000 database and journal host.

Communications among multiple iSTARs can be point-to-point via TCP/IP over Ethernet. Remote dial-up is also an option as a secondary back-up communication path. This advanced access control networking allows iSTARs to efficiently communicate directly to one another without host polling or intervention.

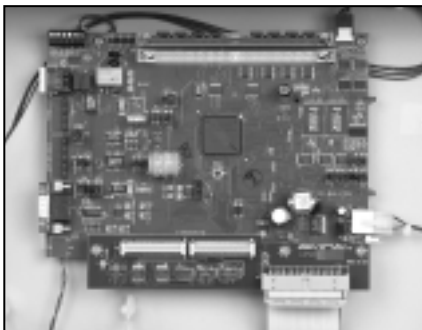
SYSTEM HIGHLIGHTS

C•CURE iSTAR is an intelligent, modular controller designed to integrate event management applications. It enables integration of various event management functions 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, flash ROM support, etc. All communication is asynchronous and no polling is necessary.

GENERAL CONTROLLER MODULE (GCM)

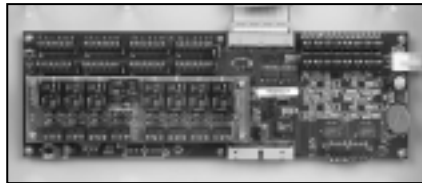
The GCM is the base controller card designed around the Microsoft Windows CE operating system and Motorola's PowerPC processor. It includes network and communication ports, expandable memory and a PC Card Type III slot.



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

ACCESS CONTROL MODULE (ACM)

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.



The GCM supports two types of ACMs: RM Reader only and mixed RM and Wiegand (ACM8 and ACM8W) direct. By utilizing combinations of ACMs, iSTAR can support 8 or 16 readers. Input and output connectors are provided to support direct Wiegand readers, reader modules, supervised inputs, and relay outputs.

The ACM provides LED indicators, which allow for visual inspection of status. The ACM also provides a 16-bit ID number (readable by the software) for general configuration information.

GLOBAL ANTI-PASSBACK BY CLUSTER

Anti-Passback prevents a person from "passing back" a card for another person to use. 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 (or "areas") 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.

INPUTS/OUTPUTS

Each iSTAR GCM contains three unsupervised inputs and one output. The inputs monitor cabinet tamper, low battery, and AC power failure. The output can be programmed to activate on any event. Each ACM contains 16 supervised inputs and 8 dry contact relay outputs. The I/8 and R/8 input boards are also supported on the ACMs. These modules allow remote disbursement of inputs and outputs along any RM reader bus. Two inputs and two outputs on the RM module provide additional flexibility and expandability.

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

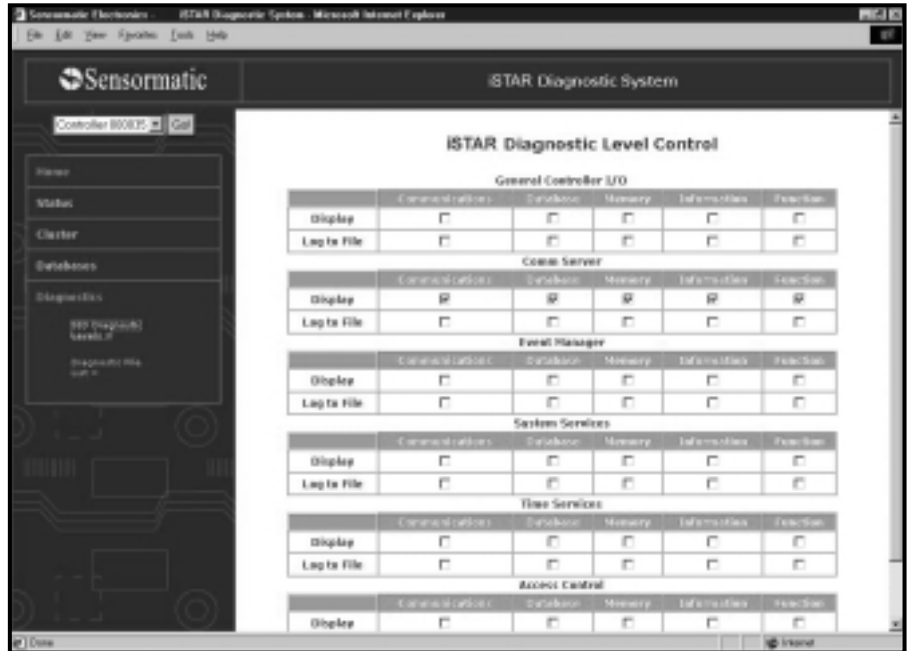
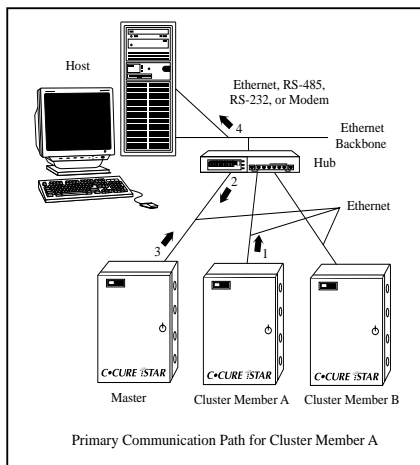
iSTAR utilizes an IP address as its unique communication identifier. Each GCM has an encoded hardware identifier that links to the IP address. Addressing and other initial configuration information is done through a program running on any PC. All other information is downloaded from the C•CURE 800/8000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

COMMUNICATIONS

iSTAR supports Ethernet, RS-232, and RS-485 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 of iSTAR controllers. Each cluster has a master controller as primary connection between the cluster and the host.

The master has no differentiating properties from other controllers other than the possibility of requiring more memory (SIMM). The other cluster members are referred to as member controllers. These are the other members in the cluster that do not communicate directly with the host; rather, communication to the host is through the master iSTAR controller. The member controllers can also communicate directly with other member controllers as needed through the master controller.

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 can be defined to have a secondary communication path to the host. This allows for backup, therefore alleviating any possibilities of communication downtime.

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.

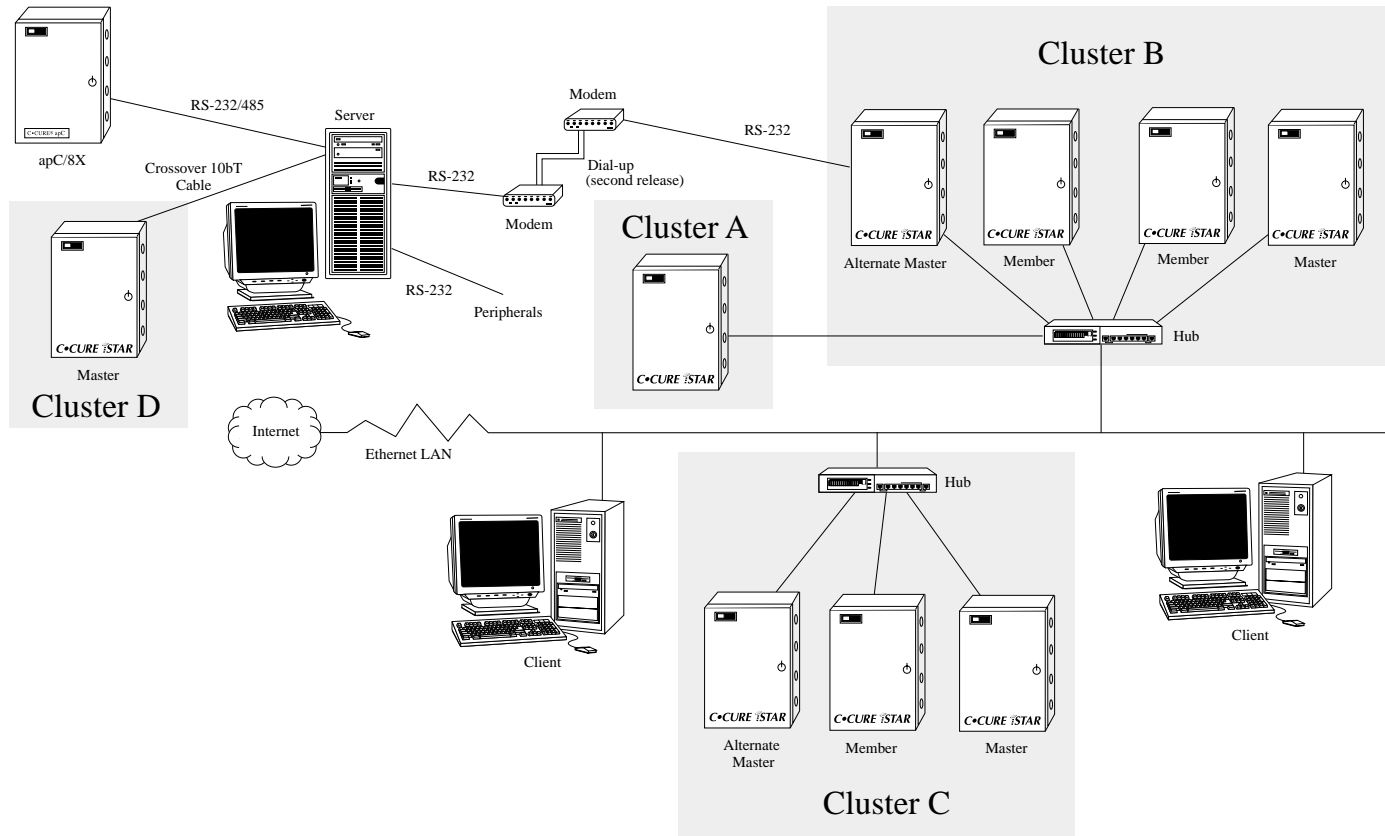
An input activated on any iSTAR in a cluster will activate a programmed output on any iSTAR in the same cluster. It is not restricted to output following input, but also includes time-controlled events, door events, area events and others. This effectively provides global event linking without reliance 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.

C•CURE iSTAR – Intelligent Network Controller

SAMPLE SYSTEM CONFIGURATION



ACM OPTIONS

ACM	Reader Sources	Input Sources	Output Sources
ACM8	<ul style="list-style-type: none"> • 8 RM readers 	<ul style="list-style-type: none"> • 16 Inputs on ACM • 2 Inputs per RM reader • Optional: 8 I/8 Modules (8 inputs each) <p>Max per GC = 192 inputs</p>	<ul style="list-style-type: none"> • 8 Outputs on ACM • 2 Outputs per RM reader (with optional ARM-1 modules) • Optional: 8 R/8 Modules (8 outputs each) <p>Max per GC = 177 outputs</p>
ACM8W	<ul style="list-style-type: none"> • 8 Readers (RM and/or direct Wiegand and/or proximity) 	<ul style="list-style-type: none"> • 16 Inputs on ACM • 2 Inputs per RM Reader • Optional: 8 I/8 Modules (8 inputs each) <p>Max per GC= 192 inputs</p>	<ul style="list-style-type: none"> • 8 Outputs on ACM • 2 Outputs per RM reader • Optional: 8 R/8 Modules (8 outputs each) <p>Max = 177 outputs</p>



Sensormatic Electronics Corporation
Access Control Division

70 Westview Street, Lexington, MA 02421 USA
Tel. +1 (781) 466-6660 Fax +1 (781) 466-9550

For the very latest information on this and other products, visit our website at: <http://www.swhouse.com>



Digital DNA
from Motorola

For more information, contact Sensormatic toll-free at **1 (800) 368-7262**.