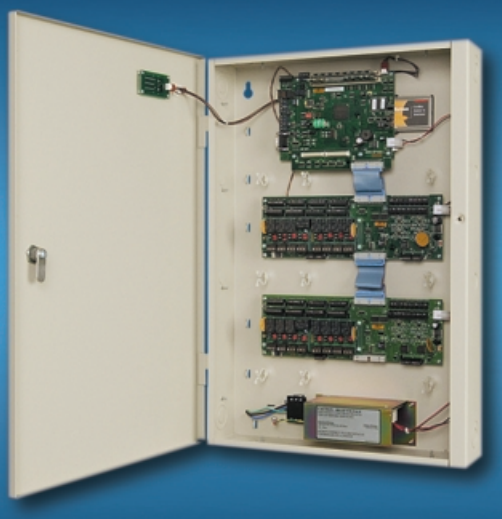
SOFTWARE HOUSE

iSTAR™



iSTAR ist ein Ethernet-fähiger, eingebetteter Controller. Der iSTAR ist so konzipiert, daß er die Integration verschiedener Systeme zur Ereignisverwaltung und den Netzwerkbetrieb zwischen wichtigen Sicherheitsanwendungen gestattet. Kernstück der iSTAR-Architektur ist das allgemeine Controller-Modul (GCM; General Controller Module). Der Aufbau dieses Controller-Moduls umfasst das Microsoft®-Betriebssystem Windows® CE, den Motorola-Prozessor PowerPC™, Netzwerk- und Kommunikationsanschlüsse, erweiterbaren Speicherplatz und einen PC-Kartensteckplatz des Typs III.Außerdem unterstützt das GCM bis zu zwei Zutrittsüberwachungsmodule (ACM;Access Control Module) und bietet somit erhöhte Flexibilität bei der Integration verschiedener Lesersysteme.

Von Datenbankereignissen gesteuerte Vorgänge können aus der C•CURE 800/8000-Datenbank und dem Journal-Host auf den Controller heruntergeladen werden. Die Kommunikation zwischen mehreren iSTAR-Controllern kann mittels TCP/IP von Punkt zu Punkt über Ethernet erfolgen. Die Ferneinwahl ist ebenso als sekundärer Sicherungskommunikationspfad möglich. Dank dieser hochentwickelten Vernetzung der Zutrittsüberwachung können einzelne iSTAR-Controller ohne Abfrage bzw. Intervention des Hosts effizient und direkt miteinander kommunizieren.

- Ethernet-fähig Direkte Ethernet-Verbindung, bei der jeder iSTAR seine individuelle IP-Adresse beibehält
- Eingebettetes Betriebssystem Erhöhte Anwendungsunterstützung und gesteigerte Geschwindigkeit durch das Betriebssystem Windows CE und PowerPC-Prozessor
- Problemlose Host-Integration C•CURE 800/8000-Host-Netzwerke zur Ersteinrichtung von Datenbanken, Verwaltung der Hardware-Peripherie, Generierung von Aktivitätsberichten und zur Verwaltung von Ereignissen in mehreren Clustern
- Umfangreiche Alarmüberwachung Unterstützung von 2 Zutrittsüberwachungsmodulen (ACM), von denen jedes 16 überwachte Meldeeingänge und 8 Relaisausgänge (Leser) besitzt; I/8 und R/8 ermöglichen weitere Meldeeingangs- und Meldeausgangsmodule
- Erweitertes Clustering (Gruppierung) für überlegene Ereigniskontrolle und Überwachung Unterstützung von verteilter Verwaltung durch Cluster-interne Kommunikation
- Globales Anti-Passback nach Cluster Verhindert bzw. beschränkt den Zutritt mehrerer Mitarbeiter mit ein und demselben Sicherheitsausweis
- Kennwortgeschützte Diagnose über das Internet Ferndiagnose über einen beliebigen Netzwerkrechner mit Internetzugang, Webbrowser und bekannter iSTAR IP-Adresse
- Erweiterbarer Hauptplatinenspeicher Optionen für den Hauptplatinenspeicher zur Unterstützung erweiterter Datenbanken/Ereignisse und späterer Erweiterungsfunktionen
- Sichere Kommunikation Branchenerprobte Verschlüsselung und Mehrfachschlüssel-Authentifikation für optimale Sicherheit
- System mit Zukunft Problemlos für zukünftige Versionen aufrüstbares Flash-ROM
- Weltweite Einsetzbarkeit FCC, CE, C-Tick, UL 294 und UL 1076

SOFTWARE HOUSE

WICHTIGSTE MERKMALE DES SYSTEMS

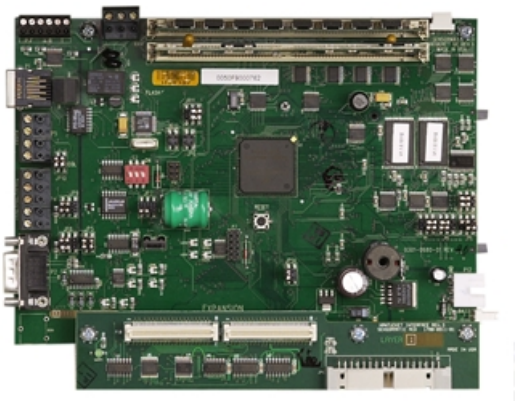
iSTAR ist ein intelligenter, modularer Controller, der für die ntegration von Anwendungen zur Ereignisverwaltung entwickelt wurde. Er ermöglicht die Integration verschiedener Funktionen zur Ereignisverwaltung in einem Controller, ist einfach zu installieren und kann problemlos zusammen mit anderen wichtigen Anwendungen betrieben werden.

Dank der innovativen iSTAR-Technologie kön-nen alle von Datenbankereignissen gesteuerten Vorgänge vom Host auf den Controller heruntergeladen und Ereignisse (Verriegeln/Entriegeln von Türen, globale Anti-Passback- Überwachung nach Cluster, Flash-ROM- Unterstützung usw.) lokal statt auf einem Host verwaltet werden. Sämtliche Kommunikation erfolgt asynchron, so dass Abfragen sich erübrigen.

DAS ALLGEMEINE CONTROLLER-MODUL (GCM)

Bei dem allgemeinen Controller-Modul han-delt es sich um die eigentliche, passend für das Betriebssystem Windows CE von Microsoft und den Motorola-Prozessor PowerPC konzipierte Controller-Karte. Sie enthält Netzwerk- und Kommunikationsanschlüsse, einen erweiterungs-fähigen Speicher und einen PC-Kartensteckplatz des Typs III.

Jedes GCM unterstützt bis zu zwei Zutrittsüberwachungsmodule (ACM). Das GCM bietet außer-dem Unterstützung für drei unüberwachte Eingänge zur Meldung von Störungen wie z. B. niedrige Batteriespannung, Stromausfall oder Sabotage am Schrankgehäuse.



ZUTRITTSÜBER-WACHUNGSMODUL (ACM)

Vom Host an den iSTAR gesendete Konfigurationsdaten informieren das ACM über die Überwachungsmeldeeingänge, die Kartendatenbearbeitung, die Kartenleserüberwachung und Meldeausgangseinrichtung. Der Zustand von Kartenlesern und Meldeausgängen kann direkt durch Benutzerbefehle am Host oder durch konfigurierte Zeitangaben beeinflusst werden. Sämtliche Zutrittsüberwachungentscheidungen (Tür und Aufzug) werden durch den iSTAR-Controller getroffen und als Transaktionen gespeichert.Alle Informationen werden lokal gespe-ichert.

Das GCM unterstützt zwei Arten von Zutrittsüberwachungsmodulen (ACM): Nur RM-Leser bzw.Kombination aus RM und Wiegand (ACM8 und ACM8W) direkt. Durch die Kombination von Zutrittsüberwachungsmodulen kann der iSTAR 8 bzw. 16 Leser unterstützen. Meldeeingangs- und Meldeausgangsanschlüsse dienen der Unterstützung von direkten Wiegand-Lesern, Lesermodulen, überwachten Meldeeingängen und Relaismeldeausgängen.

Für die optische Statusüberprüfung besitzt das Zutrittsüberwachungsmodul LED-Anzeigen. Außerdem bietet es eine (von der Software lesbare) 16-Bit-ID-Nummer für allge-meine Konfigurationsdaten.

GLOBALES ANTIPASSBACK NACH CLUSTER

Mit Anti-Passback wird die unbefugte Weitergabe von Ausweisen an andere Personen unterbun-den. Mit den iSTAR-Controllern können die Controller in einem C•CURE-Bereich innerhalb eines Clusters den Anti-Passback-Status von Ausweisinhabern gemeinsam nutzen. Mit globalem Anti-Passback können Sie auf einem beliebigen Controller im Cluster Bereiche mit Türen definieren und so eine Einrichtung in Regionen (bzw. „Bereiche“) unterteilen, um damit die Standorte der Ausweisinhaber ver-folgen zu können. Zu Anti-Passback-Verletzungen zählen die Weitergabe eines Ausweises durch eine Person an eine andere (das System empfängt zwei Zutrittsanforderungen über ein und densel-ben Ausweis) oder das zu dicht aufeinander-folgende Betreten einer Region durch zwei Ausweisinhaber. Eine Verletzung eines Anti-Passback mit Zeitbegrenzung liegt vor, wenn eine Person mehr als einmal innerhalb eines festgelegten Zeitraums versucht, in den gle-ichen Bereich einzutreten.

Beispiel: Ein Benutzer möchte Anti-Passback für das Betreten/Verlassen eines Parkhauses durchsetzen. Der Bediener würde in diesem Fall alle iSTAR-Controller mit Parkhaus-Lesern in einem Cluster zusammenfassen, einen Bereich für alle Türen/Zutrittspunkte mit diesen Lesern definieren und für den betreffenden Bereich Anti-Passback aktivieren. Die Integrität des Anti-Passback wird - mit oder ohne Host-Kommunikation -durch den Cluster gewahrt und gepflegt.

MELDEEINGÄNGE/MELDE-AUSGÄNGE

Jedes iSTAR-GCM besitzt drei unüberwachte Meldeeingänge und einen Meldeausgang. Die Meldeeingänge überwachen das System bezüglich Störungen wie Sabotage am Schrankgehäuse, niedrige Batteriespannung und Stromausfall. Über den Meldeausgang kann die Aktivierung eines beliebigen Ereignisses programmiert werden. Jedes Zutrittsüberwachungsmodul enthält 16 überwachte Meldeeingänge und 8 Trockenkontakt-Relaisausgänge. Die I/8- und R/8-Eingangsplatinen werden ebenfalls in den Zutrittsüberwachungsmodulen unterstützt. Diese Module gestatten die externe Verteilung von Meldeein- und Meldeausgängen entlang eines beliebigen RM-Leser-Busses. Zwei Meldeeingänge und zwei Meldeausgänge pro RM-Modul sorgen für zusätzliche Flexibilität und Erweiterbarkeit.

DATENSICHERHEIT

Sichere Kommunikation ist auf jeder iSTAR-Ebene (Host/Master-Controller, Master/alternativer Master und alternativer Master/Mitglieder) gewährleistet. Die Verschlüsselung erfolgt über die mittels Microsoft CryptoAPI implementierte RC4-Technologie von RSA Data Security. Mehrfachschlüssel-Authentifizierung für die Echtzeitkommunikation und Kennwortauthentifizierung für die Nutzung des lokalen Diagnose/Konfigurations-dienstpro-gramms bilden einen wirksamen Schutz gegen unbefugtes Eindringen in iSTAR.

KONFIGURATIONS-DIAGNOSE

Als eindeutige Kommunikationskennung verwendet iSTAR eine IP-Adresse. Jedes allgemeine Controller-Modul (GCM) besitzt eine codierte Hardware-Kennung, die mit der IP-Adresse verknüpft ist. Die Adressierung und andere Erstkonfigurationsdaten erfolgen über ein auf jedem PC ausführbares Programm.Alle anderen Informationen wer-den vom C•CURE 800/8000-Host herunterge-laden.

Die Diagnose kann über einen beliebigen Rechner mit Netzwerkpfad zu einem iSTAR-Controller erfolgen. Darüber hinaus ist der Fernzugriff auf die Echtzeitstatus- und Diagnosedaten über das Internet mit einem Webbrowser wie Internet Explorer oder Netscape Navigator möglich. Folgende Informationen können abgerufen werden:

- Controller-Zeit/Startzeit
- Gesamter/verfügbarer Speicherplatz
- MAC- und IP-Adresse
- Verbindungsstatus
- Versionen von Firmware- und Betriebssystemen
- Diagnosedatendateien

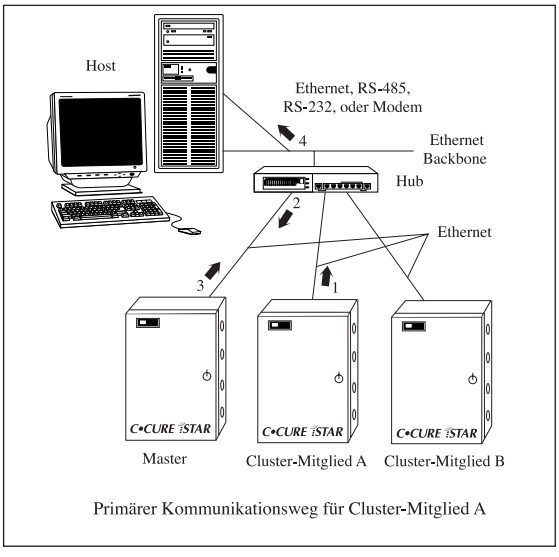
KOMMUNIKATION

iSTAR-Controller unterstützt die Kommunikationstopologien Ethernet, RS-232 und RS-485. Er enthält außerdem einen PC-Kartensteckplatz des Typs III (PCMCIA) für weitere Kommunikationsvorrichtungen wie z.B. ein Modem. Die iSTAR-Kommunikation erfolgt von Punkt zu Punkt (Kettenschaltung wird nicht unterstützt). Eine Einzelverbindung vom Host unterstützt mehrere Controller über ein TCP/IP-Teilnetz.

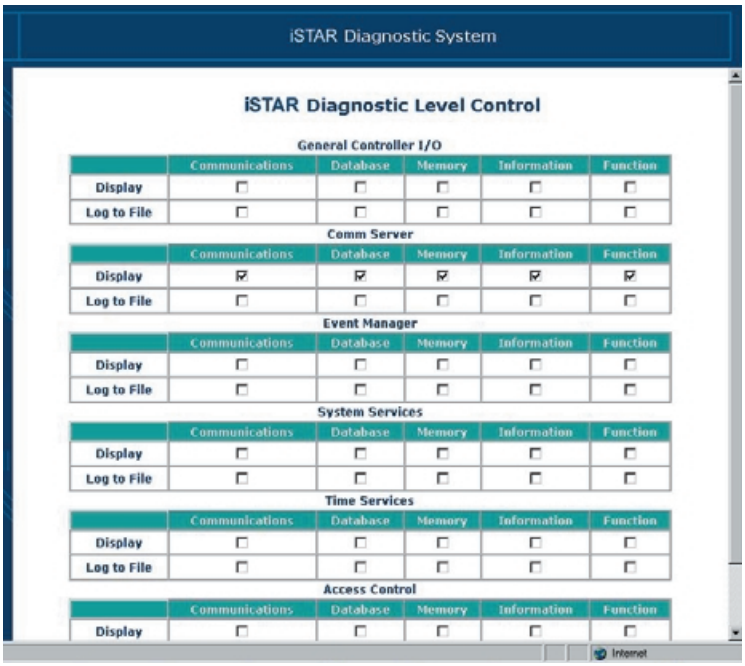
Gruppen von einem bis mehreren Controllern werden als Cluster definiert. Ein Cluster ist eine benutzerdefinierte Gruppierung von iSTAR-Controllern. In jedem Cluster bildet ein Master-Controller die Hauptverbindung zwischen Cluster und Host.

Der Master unterscheidet sich nur insofern von anderen Controllern, als dass er möglicherweise mehr Speicherplatz benötigt (SIMM). Die anderen Controller innerhalb eines Clusters werden als Mitglieds-Controller bezeichnet. Diese Controller kom-munizieren nicht direkt mit dem Host; stattdessen erfolgt die Kommunikation über den iSTAR Master-Controller. Bei Bedarf kön-nen Mitglieds-Controller über den Master-Controller auch mit anderen Mitglieds-Controllern kommunizieren.

Die Kommunikation innerhalb eines Clusters erfolgt mittels TCP/IP über Ethernet. Für den Fall eines Kommunikationsausfalls mit dem zugewiesenen Master-Controller kann auch ein alterna-tiver Master-Controller definiert werden. (Die Mitglieds-Controller kommu-nizieren dann über den alternativen Master-Controller.) Für den Master-Controller kann ein sekundärer Kommunikationspfad zum Host definiert werden. Diese Sicherungsfunktion schließt alle Möglichkeiten eines Kommunikationsausfalls aus.



Primärer Kommunikationsweg für Cluster-Mitglied A



VERTEILTE CLUSTER-EREIGNISÜBERWACHUNG

iSTAR unterstützt die Verknüpfung von Cluster-Ereignissen aufgrund von durch den C•CURE 800/8000-Host konfigurierten Ereignissen. Diese Ereignisverknüpfung wird nicht nur innerhalb eines Controllers unterstützt, sondern auch innerhalb eines Clusters.

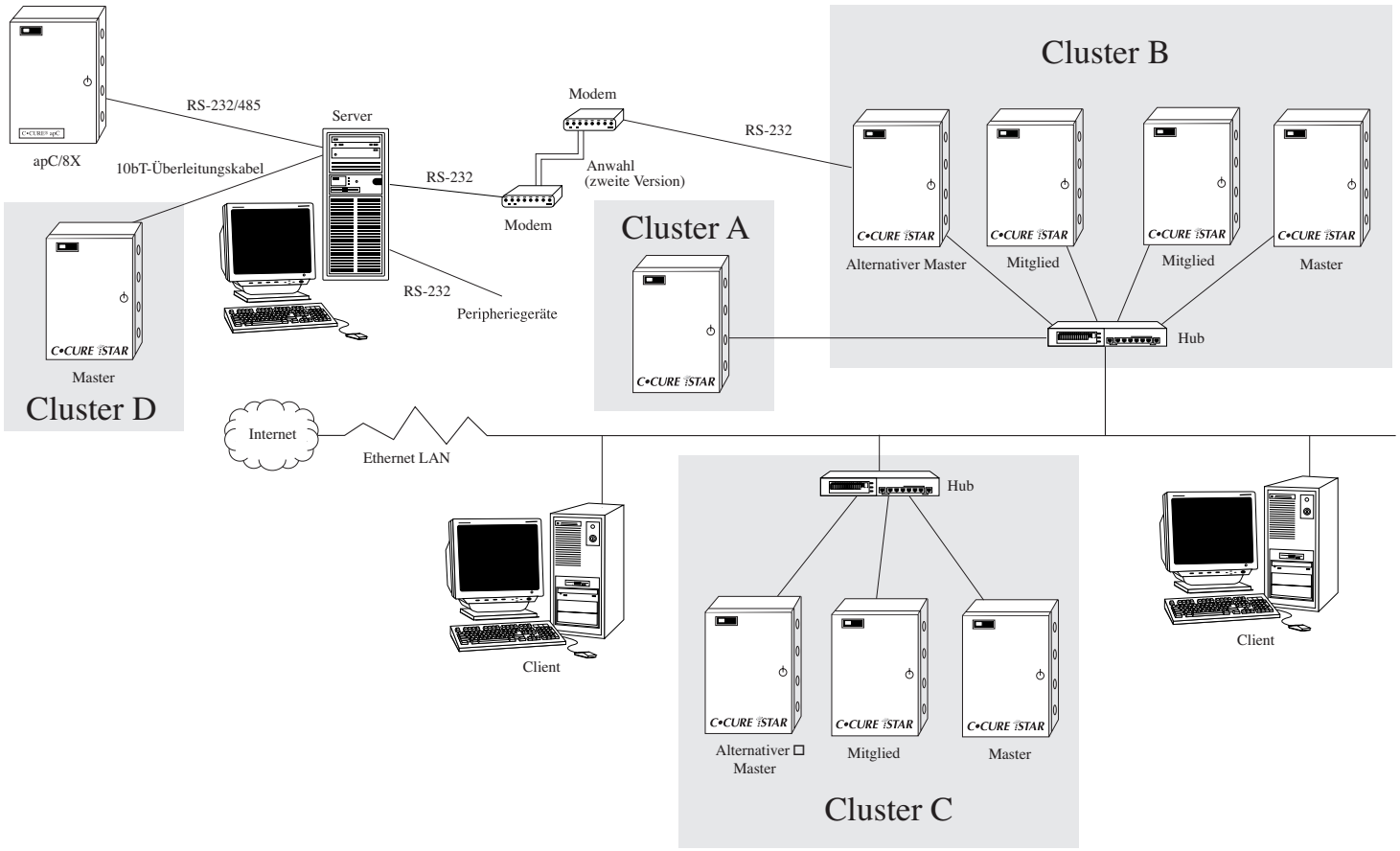
Ein auf einem beliebigen iSTAR in einem Cluster aktivierter Meldeeingang aktiviert einen programmierten Meldeausgang auf einem beliebigen iSTAR innerhalb desselben Clusters. Diese Funktion ist nicht auf „Ausgang nach Eingang“ beschränkt, sondern umfasst auch zeitgesteuerte Ereignisse,Türereignisse, Bereichsereignisse sowie andere Ereignisse. Dies ermöglicht eine effektive, vom Host unabhängige globale Verknüpfung von Ereignissen. Durch die Aktivierung eines Ereignisses ausgelöste Vorgänge außerhalb des programmierten Clusters werden durch Host-Intervention unterstützt.

KOMMUNIKATION MIT APCS

iSTAR und apCs können mit einem C•CURE 800/8000-Host zusammen betrieben werden. Diese kommunizieren nicht direkt miteinander und können auch nicht miteinander verbunden werden. Die Ereignisverknüpfung kann jedoch problemlos über den C•CURE 800/8000-Host konfiguriert werden. Es ist zwar nicht möglich, diese Geräte miteinander zu verbinden, sie können aber im selben Netzwerk installiert werden.

SOFTWARE HOUSE

BEISPIEL EINER SYSTEMKONFIGURATION



OPTIONEN FÜR DAS ZUTRITTSÜBERWACHUNGSMODUL (ACM)

Zutrittsüber-wachungsmodul (ACM)	Leserquellen	Meldeeingangsquellen	Meldeausgangsquellen
ACM8	• 8 RM-Leser	• 16 Meldeeingänge für Zutrittsüberwachungsmodul • 2 Meldeeingänge pro RM-Leser • Optional: 8 I/8-Module (je 8 Meldeeingänge) Maximum pro General Controller (GC) = 192 Meldeeingänge	• 8 Meldeausgänge für Zutrittsüberwachungsmodul • 2 Meldeausgänge pro RM-Leser (mit optionalen ARM-1-Modulen) • Optional: 8 R/8-Module (je 8 Meldeausgänge) Maximum pro GC = 177 Meldeausgänge
ACM8W	• 8 Leser (RM und/oder direkt Wiegand und/oder Proximity)	• 16 Meldeeingänge für Zutrittsüberwachungsmodul • 2Meldeeingänge pro RM-Leser • Optional: 8 I/8-Module (je 8 Meldeeingänge) Maximum pro GC= 192 Meldeeingänge	• 8 Meldeausgänge für Zutrittsüberwachungsmodul • 2 Meldeausgänge pro RM-Leser • Optional: 8 R/8-Module (je 8 Meldeausgänge) Maximum = 177 Meldeausgänge

Weitere Informationen erhalten Sie von Ihrem örtlichen Software House au numéro vertsuivant : 1-800-550-6660
www.swhouse.com