



iSTAR® Controller

IP-fähige Controller: Leistungsstarke Sicherheitstechnik für Unternehmen und Behörden

Funktionen, die mehr können:

- Hochsichere Controller zur Steuerung der Sicherheitstechnik im gesamten Unternehmen – für 4 Türen oder mehrere 1000
- iSTAR eX bietet integrierte FIPS 197-zertifizierte AES Verschlüsselung und macht externe Encryption Boxes überflüssig
- Redundante Sicherung von Konfigurationsdaten
- Zuverlässige Datenbank-Backups auf nichtflüchtigem Flash-Speicher
- LCD mit Controller-Status und wichtigen Diagnoseinformationen
- LEDs für die einzelnen Ausgänge, Ethernet, serielle Schnittstelle und integrierter „Pulsmesser“ für einen kontinuierlichen Betrieb
- Einfache Installation: automatische Zuweisung von IP-Adressen dank DHCP-Unterstützung
- Hochsicher und flexibel: Unterstützt mehrere Karteninhaber pro Karte und verschiedene Formate
- Vollständig kompatibel mit C•CURE® 800/8000 und Unterstützung von Funktionen wie Sicherheitsstufen oder Ereignisfreigabefilter
- Betriebssystem Windows® CE integriert

iSTAR Pro für bis zu 16 Lesegeräte

iSTAR Pro integriert verschiedene Anwendungen des Ereignismanagements in einem einzigen Gerät. Der intelligente, modulare Controller ist einfach zu installieren und ermöglicht die Interoperabilität von entscheidenden Schlüsselanwendungen.

Das Design von iSTAR Pro wurde so optimiert, dass modernste Technik mit einem Minimum an Leiterplatten umgesetzt werden kann. Ergebnis ist eine hochzuverlässige, kosteneffektive Lösung für die unternehmensweite Zugriffskontrolle.

iSTAR Pro verwendet ein GCM (General Controller Module), das standardmäßig mit einem 64-MB-Speicher ausgerüstet ist. Eine nachträgliche Erweiterung mit einem 64 MB SDRAM-Modul auf 128 MB ist jederzeit möglich. Weitere Leistungsmerkmale sind zwei PCMCIA-Steckplätze, ein alphanumerisches LCD und DIP-Schalter zur Konfiguration und Diagnose. Außerdem bietet iSTAR Pro mehrere Netzwerkanschlüsse und serielle Schnittstellen. Das GCM steuert bis zu zwei Zutrittsüberwachungsmodule (ACM), die jeweils bis zu acht Wiegand- oder RM-Lesegeräte unterstützen können. Das ACM verfügt außerdem über 16 überwachte Eingänge und acht Ausgabereleis zur Türsteuerung.

iSTAR eX für bis zu 4 Lesegeräte

iSTAR eX ist ein Ethernet-fähiger Vier-Türen-Controller mit einer FIPS 197-zertifizierten 256-Bit-Verschlüsselung. Der Controller eignet sich besonders für Behörden oder Unternehmen, die ein Maximum an Sicherheit wünschen.

Große Unternehmen mit kleineren Niederlassungen in verschiedenen Ländern können iSTAR eX in Verbindung mit dem skalierbaren C•CURE 800/8000-System und anderen Software House-Controllern einsetzen. So werden auch anspruchsvollste Lösungen unternehmensübergreifend bereitgestellt. Ob in einer Konzernzentrale mit hunderten von Mitarbeitern oder in einer regionalen Filiale mit weit weniger Betrieb: iSTAR eX sorgt dafür, dass die Sicherheitsvorschriften im gesamten Unternehmen einheitlich umgesetzt werden.

Ebenso profitieren auch Behörden von iSTAR eX, wenn es um Hochsicherheit von geheimen Verschlusssachen geht. Derartige Dokumente werden meist in überschaubaren, mit wenigen Türen ausgestatteten Räumlichkeiten gelagert. iSTAR eX schützt diese Bereiche, ohne dass dafür überflüssigerweise ein 8- oder 16-Türen-Controller eingesetzt werden muss. Gleichzeitig ermöglicht das modulare Design von iSTAR eX bei Bedarf eine Erweiterung mit weiteren Modulen für die Türkontrolle.

Funktionen

Einfache Installation dank DHCP, DNS und WINS

iSTAR®-Controller unterstützen DHCP (Dynamic Host Configuration Protocol) für eine einfachere Installation. DHCP ist ein Kommunikationsprotokoll, mit dem Netzwerkadministratoren IP-Adressen zentral verwalten und verteilen können. Außerdem ist es möglich, einem Gerät automatisch eine neue IP-Adresse zuzuweisen, wenn es an einer anderen Stelle im Netzwerk angeschlossen wird. Um die Installation weiter zu vereinfachen, unterstützen die iSTAR-Controller zudem DNS (Domain Name System), das die Domännennamen in IP-Adressen umwandelt, und WINS (Windows Internet Naming Service), ein System zur Bestimmung der IP-Adresse, die einem bestimmten Netzwerkcomputer zugewiesen ist.

Effektive Kommunikation mit Clustern

iSTAR Pro-Controller unterstützen Ethernet und RS-232-Kommunikationstopologien und sind mit einer PC-Karte ausgerüstet. iSTAR eX verfügt über einen Steckplatz vom Typ PC Card Type II (PCMCIA) für zusätzliche Kommunikationsarten. Außerdem bietet iSTAR eX zwei integrierte Ethernet-Anschlüsse zur Kommunikation. Die iSTAR-Kommunikation erfolgt über Peer-to-Peer¹. Dies bedeutet, dass die Controller miteinander kommunizieren, ohne dass ein Host erforderlich ist, und dass eine Einzelverbindung vom Host mehrere Controller über ein TCP/IP-Subnetz steuert.

Cluster sind benutzerdefinierte Gruppen, die aus bis zu 16 Controllern bestehen. Diese können zur weiteren Erhöhung der Sicherheit erstellt werden, indem man verteilte Standorte in mehrere Kontrollbereiche unterteilt. An der Spitze eines Clusters steht ein „Master-Controller“, der die primäre Kommunikation zwischen dem Host-Computer und dem Rest der Controller im Cluster verwaltet. Der Master-Controller überträgt alle Ereignis- und Karteninhaberdaten zwischen dem Cluster und dem C•CURE® 800/8000-Host. Die anderen Controller im Cluster, die „Mitglieder“, kommunizieren über den Master miteinander, um Ereignisse zu verknüpfen und das Anti-Passback im kontrollierten Bereich zu überwachen. Um eine dauerhafte Sicherheit zu gewährleisten, verfügen die Cluster zudem über einen sekundären Kommunikationspfad – für den Fall, dass der Master-Controller ausfällt oder die Verbindung zum Netzwerk unterbrochen wird.

Bessere Sicherheitskontrolle durch globales Anti-Passback

Das globale Anti-Passback ist entscheidend für eine lückenlose Sicherheit. Wird ein Cluster in der oben beschriebenen Konfiguration verwendet, können die iSTAR-Controller problemlos den Status und Standort des Karteninhabers übermitteln. Auf diese Weise können sie C•CURE 800/8000 melden, wenn gegen die Regeln des globalen Anti-Passback verstoßen wird – zum Beispiel, wenn ein Karteninhaber seine Karte an eine andere Person weitergibt oder versucht, innerhalb eines bestimmten Zeitraums denselben Bereich mehr als einmal zu betreten. Ebenso kann registriert werden, ob jemand durch Folgen einer anderen Person und ohne Vorzeigen eines separaten Ausweises einen sicheren Bereich betritt.

Tastaturbefehle für höchste Flexibilität

Tastaturbefehle sind eine effektive Methode, um Ereignisse direkt über ein RM-Lesegerät zu aktivieren. Dies kann von der Fernauflösung von Zwangsankufen und Alarmen bis hin zum Sperren und Entsperren von Türen reichen. Die Befehle können so konfiguriert werden, dass zur Bestätigung ein Ausweis gezeigt und/oder eine PIN eingegeben werden muss.

Erweiterte Ausweisnummern für noch mehr Sicherheit

iSTAR-Controller unterstützen erweiterte Ausweisnummern, so dass bestimmte Vorschriften wie der US-amerikanische Standard FIPS 201 eingehalten werden, die eine CHUID (eindeutige ID des Ausweisinhabers) mit mehreren Feldern erfordern. Darüber hinaus unterstützen iSTAR-Controller Ausweisnummern mit bis zu 256 Bit und machen somit mehrere Anlagencodes, Standortcodes oder Offsets zur Vermeidung doppelter Ausweise unnötig. Längere Ausweisnummern bieten erhöhten Schutz vor Ausweisduplikation und sind besonders interessant für Kunden, die Nummern mit mehr als 10 Stellen benötigen.

Wie viele Karten? Was für Karten? Entscheiden Sie selbst

In Verbindung mit C•CURE 800/8000 können Administratoren mit den iSTAR-Controllern bis zu fünf Karten pro Karteninhaber zuweisen, ohne für jede Karte einen einzelnen Datensatz anlegen zu müssen. Mit Hilfe dieser effektiven Funktion können Benutzer an Stelle eines der Ausweise eine PIN verwenden. Dies ist eine flexible und sichere Lösung, die die Verwaltung und Pflege der Mitarbeiterdaten vereinfacht.

Für zusätzliche Flexibilität unterstützen iSTAR-Controller bis zu 128 Ausweisformate im ganzen System und 10 Ausweisformate pro Lesegerät inklusive Smart Cards. Dank dieser erweiterten Fähigkeit zur Verwendung mehrerer Ausweisarten (z. B. 26 Bit, 37 Bit oder Corporate 1000) an einem einzigen Lesegerät müssen vorhandene Ausweise nicht angepasst oder neu ausgestellt werden.

Einfaches Testen und Fehlerbeseitigung mit Konfigurationsdiagnose

iSTAR-Controller verfügen über eine integrierte Diagnostik zum Testen und Beheben von Fehlern der Hardware-Komponenten. Dazu gehören z. B. Eingänge, Ausgänge, Lesegerätsanschlüsse, zuletzt gelesene Karten, PCMCIA-Karten oder der Akkuladezustand. Zusätzlich können Sie über das Internet in Echtzeit den Status und die Diagnostik für folgende Informationen abrufen:

- Controller-Zeit/Bootzeit
- Gesamter/verfügbarer Speicher
- Verbindungsstatus
- Version der Firmware und des Betriebssystems
- Hardware (MAC) und IP-Adressen

Zudem verfügen iSTAR-Controller für eine einfache Installation und schnelle Fehlerbehebung über ein LC-Display.

(1) Verkettung wird nicht unterstützt

Genauere Informationen

Datensicherheit ist wichtig

iSTAR® eX kombiniert die AES-Verschlüsselung (Advanced Encryption Standard) mit den strengen Richtlinien, die für Hochsicherheitslösungen gelten. AES gibt einen FIPS-zertifizierten Kryptographieverfahren an, der zum Schutz elektronischer Daten verwendet werden kann. Der AES-Algorithmus wandelt Daten in ein für Dritte unverständliches Format um, das Schlüsseltext genannt wird (Verschlüsselung). Anschließend werden die Daten wieder in das Ursprungsformat umgewandelt, das als Klartext bekannt ist (Entschlüsselung). iSTAR eX und C•CURE® 800/8000 kommunizieren über eine FIPS-zertifizierte AES-Verschlüsselung mit 256 Bit und bieten somit das erste Sicherheitssystem auf dem Markt, das die strengen behördlichen Auflagen erfüllt.

Gesichert wird die Kommunikation der iSTAR Pro-Controller über die RC4-Technologie von RSA Data Security, die mit Hilfe von Microsoft CryptoAPI implementiert wird. Multi Key-Autorisierung für Kommunikation in Echtzeit und Kennwortautorisierung für das Konfigurationsprogramm zur lokalen Diagnostik bieten Schutz vor unerlaubtem Zugriff auf die iSTAR Pro-Controller.

Zusätzlich passen sich die iSTAR-Controller den Bedürfnissen der Unternehmen an, um entscheidende Sicherheitsdaten zu schützen. Dank sofortiger Datenbanksicherung und Wiederherstellung der Funktionen bieten iSTAR-Controller eine hochzuverlässige Sicherheitslösung und sorgen für den Schutz wichtiger Daten, auch bei Kommunikationsfehlern.

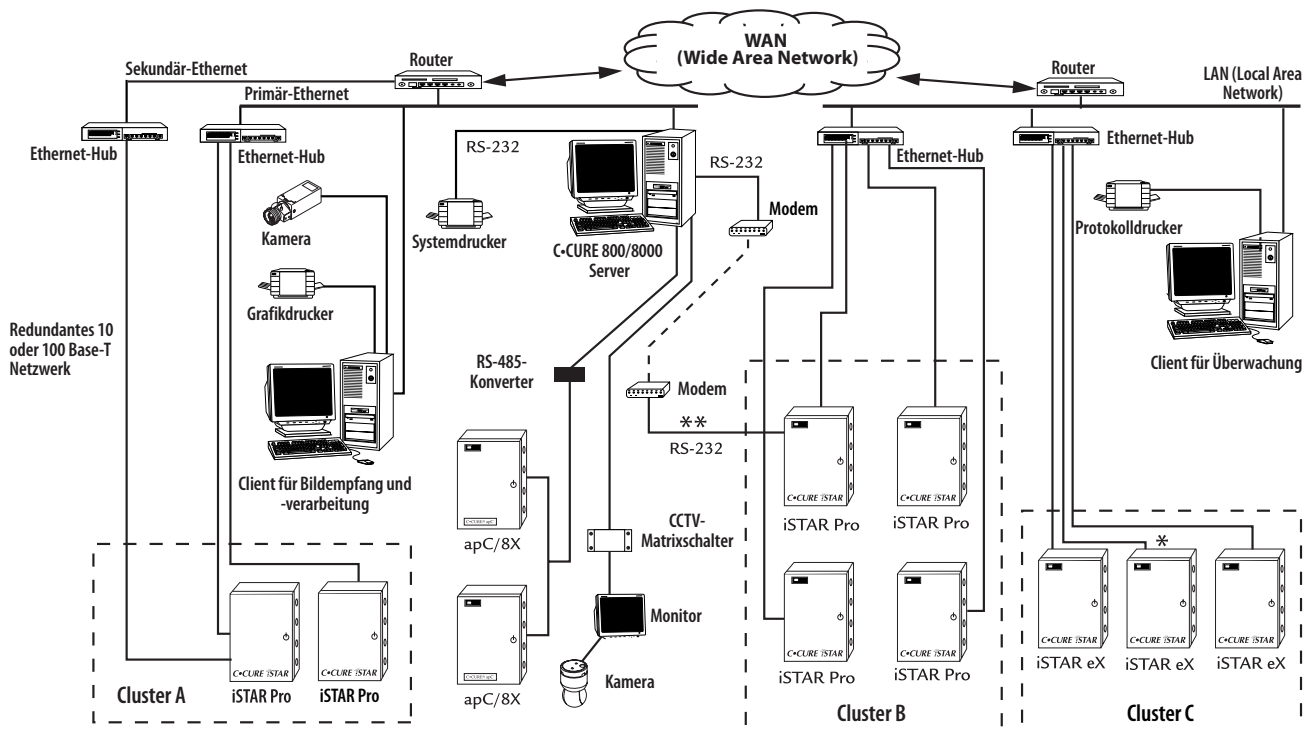
Problemlos aktualisierbar

Alle iSTAR-Controller können Funktionsupgrades direkt vom Host beziehen, sodass die Technologie immer auf dem neuesten Stand ist.

Für jeden Zweck die richtige iSTAR-Architektur

iSTAR Pro und iSTAR eX-Controller können zusammen im selben System verwendet werden und bieten eine Sicherheitslösung, die in puncto Vielseitigkeit und Sicherheit auf dem Markt unübertroffen ist. Es wird der Tatsache Rechnung getragen, dass auch die größten Unternehmen über kleinere Niederlassungen oder Filialen verfügen, die ohne überflüssige Investitionen mit denselben Sicherheitsstandards ausgerüstet werden müssen wie der Hauptstandort.

iSTAR-Controller und apC-Controller können zusammen mit einem C•CURE 800/8000-Host verwendet werden, auch wenn diese nicht direkt miteinander kommunizieren. Das Verknüpfen von Ereignissen kann jedoch problemlos über den Host konfiguriert werden. Auch wenn diese Geräte also nicht direkt miteinander verbunden werden können, können sie sich doch beide im selben Netzwerk befinden.



*Alternativer Master übernimmt, wenn die Master-Bedienungseinheit ausfällt

**Alternativer Kommunikationspfad übernimmt, wenn der primäre Kommunikationspfad ausfällt

***iSTAR Pro und iSTAR eX-Controller dürfen sich nicht zusammen im selben Cluster befinden. Außerdem unterstützt iSTAR eX aktuell kein DFÜ-Modem als primären oder alternativen Kommunikationspfad.

	iSTAR® Pro	iSTAR eX
Stromversorgung		
Eingangsleistung	90 bis 240 VAC, 47 bis 440 Hz, 0,5 A	90 bis 260 VAC, 47 bis 440 Hz, 0,5 A
Ausgangsleistung (des Netzteils)	12 VDC bei maximal 3,3 A	12 VDC bei maximal 6,5 A; interne USV für bis zu vier Stunden Reservezeit
Hilfshardware	Relaiskontakte mit Nennspannung von 30 V AC/DC 2,5 A induktiv, 5,0 A induktionsfrei	Relaiskontakte mit Nennspannung von 30 V AC/DC 2,5 A induktiv, 5,0 A induktionsfrei
Abmessungen/Gewicht		
Abmessungen (H x B x T)	61,6 x 41,9 x 10,2 cm (24,25 x 16,5 x 4,0 Zoll)	61,6 x 41,9 x 10,2 cm (24,25 x 16,5 x 4,0 Zoll)
Gewicht	10,6 kg	16,8 kg mit Batterie
Konstruktion	16 AWG Metallgehäuse zur Wandmontage, abschließbar, mit Einbruchmelder an Tür und Rückseite	16 AWG Metallgehäuse zur Wandmontage, abschließbar, mit Einbruchmelder an Tür und Rückseite
Richtlinien/Zertifizierungen	UL294, UL1076, CE, FCC, RoHS	UL294, UL1076, CE, FCC, RoHS
Umgebungsbedingungen		
Betrieb	0 bis 50°C 5 bis 95 % rel. Luftfeuchtigkeit, nicht kondensierend	0 bis 50°C 5 bis 95 % rel. Luftfeuchtigkeit, nicht kondensierend
Lagerung	-20 bis 70°C	-20 bis 70°C
Betriebs- und Lagertemperatur mit Batterie	0 bis 50°C	-20 bis 40°C

Kapazität Controller	iSTAR Pro 64 MB	iSTAR Pro 64 MB	iSTAR Pro 128 MB	iSTAR Pro 128 MB	iSTAR eX 64 MB
Firmware-Version	bis Version 3.3	Version 4 oder höher	bis Version 3.3	Version 4 oder höher	Version 4.1 oder höher
Anzahl der Mitarbeiterdatensätze mit 1 Freigabe, 1 Karte/Person, 10-stellige Karten	500,000	525,000	1,000,000	1,200,000	410,782
Anzahl der Mitarbeiterdatensätze mit 10 Freigaben, 1 Karte/Person, 10-stellige Karten	295,000	295,000	640,000	680,000	235,774
Anzahl der Mitarbeiterdatensätze mit 1 Freigabe, 5 Karten/Person, 10-stellige Karten	k. A.	170,000	k. A.	375,000	132,820
Anzahl der Mitarbeiterdatensätze mit 10 Freigaben, 5 Karten/Person, 40-stellige Karten	k. A.	110,000	k. A.	250,000	88,546

Hinweis:

- (a) Die Speicherzuweisung erfolgt bei iSTAR Pro und iSTAR eX dynamisch und gemeinsam für Karteninhaber, Ereignisspeicher und Konfigurationsinformationen.
- (b) Hilfe bei der Abschätzung, wie viel Speicherplatz für die Mitarbeiterdatenbank bei iSTAR Pro v4.0 und höher bzw. bei iSTAR eX für mehrere Karten und/oder erweiterte Kartenkapazitäten benötigt wird, finden Sie in der Datei "C•CURE 800 v9.1 README" im Member Center unter www.swhouse.com.
- (c) iSTAR kann bis zu fünf Karten für jeden Karteninhaberdatsatz unterstützen; jede Karte ist unabhängig von jedem Karteninhaber im System.

Die angebotenen Produkte und ihre Spezifikationen können ohne vorherige Ankündigung geändert werden. Die Abbildungen zeigen nicht immer die aktuellen Produkte. Nicht alle Produkte sind mit allen Funktionen erhältlich. Die Verfügbarkeit ist je nach Region unterschiedlich. Wenden Sie sich für nähere Informationen an Ihren Vertriebsbeauftragten. Bestimmte Produktnamen, die in diesem Dokument erwähnt sind, können Markennamen und/oder eingetragene Warenzeichen anderer Unternehmen sein.

© 2007 Sensormatic Electronics Corporation. Alle Rechte vorbehalten. SH0033-DS-200701-R04-A4-DE

www.swhouse.com



tyco / Fire & Security