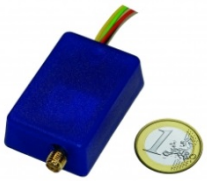
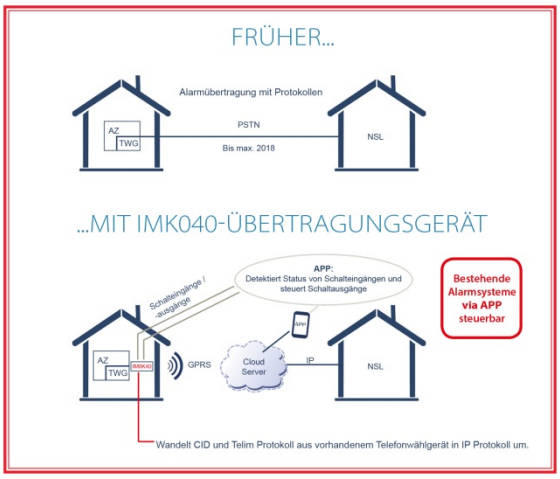
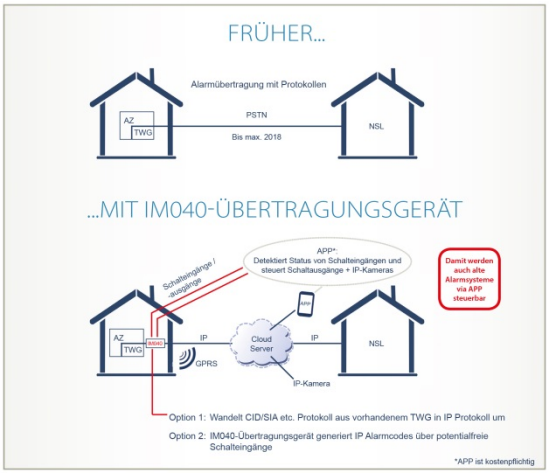
Montageanleitung IM040 / IMK040







Inhalt

Sicherheitshinweise.
Beschränkte Haftung und Herstellergarantie

Bitte lesen und befolgen Sie diese Sicherheitshinweise, um die Sicherheit von Personen einzuhalten:

Bitte lesen und befolgen Sie diese Sicherheitshinweise, um die Sicherheit von Personen einzuhalten:
✓ GSM / GPRS-Kommunikationsgeräte MQ02 und MN01 enthalten einen Funk-Transceiver, in den GSM850 / 900 / 1800/1900 Bändern.
✓ Verwenden Sie das Gerät nicht zusammen medizinischen Geräten, oder anderen Geräten die durch eine Störung eine mögliche Gefahr hervorrufen.
✓ Setzen Sie das Gerät nicht zu hoher Luftfeuchtigkeit, chemischer Umgebung oder mechanischen Einflüssen aus.
✓ Verwenden Sie das Gerät nicht in explosionsgefährdeten Umgebungen. Lagern oder installieren Sie das Gerät nicht in überhitzten, staubig, feucht oder unterkühlten Orten.
✓ Das Gerät wird in Bereichen mit begrenztem Zugang montiert. Alle Systemreparaturen dürfen nur von qualifiziertem, Sicherheitsgeschultem Personal durchgeführt werden. Das Gerät nicht zerlegen oder selbst zu reparieren.
✓ Das Netz muss vor allen Installations- oder Wartungsarbeiten getrennt werden.
✓ Das Gerät muss versorgt werden über eine DC 7-18 V, 400 mA Stromversorgung.
✓ Sicherungen oder andere Komponenten der Geräte dürfen nicht vom Benutzer ausgetauscht werden.
✓ Halten Sie das Gerät trocken. Jede Flüssigkeit wie Regen, Feuchtigkeit, kann das Gerät zerstören oder beschädigen.
✓ Vorsicht. Vibrieren oder schütteln Sie es nicht mit Gewalt.
✓ Reinigen Sie das Gerät nur mit einem trockenen Tuch.

✓ Bitte lesen Sie die Bedienungsanleitung sorgfältig vor der Installation und dem Betrieb der Geräte durch.

Beschränkte Haftung: Der Benutzer stimmt zu, dass trotz der CE Erklärung das Risiko von Feuer, Diebstahl, Einbruchdiebstahl oder andere Gefahren besteht, das Gerät kann solche Ereignisse nicht verhindern. Secplan. wird keine Verantwortung, bezüglich Personen-, Sach- oder Einkommensverlust übernehmen die durch die Nutzung des Geräts entstehen. Das Gerät entspricht den gesetzlichen Bestimmungen. Secplan steht in keinem Zusammenhang mit den verwendeten Mobilfunkbetreibern. Die Netzabdeckung/Netzqualität kann durch Secplan nicht garantiert werden.

Herstellergarantie: Für das Gerät besteht die Gesetzlich festgelegte Gewährleistung. Diese Gewährleistung deckt keine Kosten ab die durch den Einbau/Service an dem Gerät entstanden sind. Diese Garantie deckt keine Bezugsverträge oder Ausfall von Dienstleistungen unter den Bedingungen eines solchen Bezugsvertrages, oder Ausfall von zellulären, GPRR, LAN oder andere damit zusammenhängenden Netzwerkfunktionen und Dienstleistungen ab. Die Garantie gilt nicht für Geräte, die modifiziert oder in anderer Weise als in den vorgesehenen Zweck verwendet wurden und deckt keine Schäden an dem Gerät durch Installation oder Entfernung des Geräts oder eine ihrer Komponenten verursacht wurden. Diese Garantie ist ungültig, wenn das Gerät durch nicht ordnungsgemäße Wartung, SIM-Karten Entfernung, Unfall oder unsachgemäße Verwendung, Fahrlässigkeit, höhere Gewalt, Vernachlässigung, oder aus anderen Gründen beschädigt wurde. Diese Garantie gilt nicht bei Antennenprobleme oder schwachem Signalempfang, Schäden an Software, Zubehör oder Alarmanlage externen Komponenten, kosmetische Schäden oder Schäden aufgrund von Fahrlässigkeit, Missbrauch, nicht beachten der Bedienungsanleitung, versehentlichem Verschütten von Flüssigkeiten, Schäden durch umweltbedingte Ursachen wie Überschwemmungen, Luft Fallout, Chemikalien, Salz, Hagel, Sturm, Feuchtigkeit, Blitzschlag oder extreme Temperaturen, Schäden durch Feuer, Diebstahl, Verlust oder Vandalismus, Schäden durch unsachgemäße Lagerung und den Anschluss an Geräte eines anderen Herstellers, Änderung bestehender Anlagen, fehlerhafte Montage oder Kurzschluss.

In keinem Fall wird Secplan für zufällige, besondere oder Folgeschäden (einschließlich entgangener Gewinne) für die Beendigung von Verträgen, Schadenersatz, Entschädigung für den Verlust des Kunden haften. Es bestehen hierdurch keine Ansprüche seitens des Kunden gegen Secplan.

Allgemeine Bedienprinzipien des IM040 und IMK040 GSM / GPRS-Kommunikationsgeräte

Diese Kommunikationslösung ist eine komplette Kommunikationsplattform für die Datenübertragung von Alarmsystemen an Notrufleitstellen oder Endgeräte (Smartphones, Tablets, PCs, etc.). Die Plattform erlaubt eine bidirektionale Datenübertragung mit Festnetzanschluss, SMS, GPRS-Netz oder LAN. Die Plattform besteht aus Hardware-Geräten (wie IM040 und IMK040 GSM / GPRS Kommunikator n) und einem Cloud-Infrastruktur-Service (CIS). Die Verbindung zwischen dem Gerät und der Alarmanlage erfolgt über digitale Eingänge, serielle Schnittstelle oder Telefonleitungsemulation mit DTMF-Dekodierung. Die GSM / GPRS Kommunikator IM040 und IMK040 halten eine dauerhafte Verbindung zum Cloud Infrastructure Service. Die CIS erfüllen mehrere administrative Aufgaben, wie zum Beispiel konstante Überwachung der meldungen und Zustände sowie das Verteilen auf Notrufleitstelle oder APP.

Der Zugriff auf die Konfigurationseinstellungen und Dienstbefehle kann über eine Web-basierte Software www.m2mservices.com/admin oder durch Android App 'RControl Admin "(kostenlos erhältlich bei Googleplay) durchgeführt werden.

IM(K)040 Ablauf

Leitstelle bekommt einen Adminzugang

Errichter bekommt einen Errichterzugang von uns erstellt.

Bei Verkauf eines Gerätes liegt dem Wählgerät ein Zettel mit Seriennummer, CMS-Key und Config-Key bei.

Errichter loggt sich in sein Konto unter
http://www.residencecontrol.com/InfrastructureAdministration/Login.aspx

Ein.

Hier kann nun über den Button „CMS“->“Config New Device“ das von Ihm erworbene Gerät hinzugefügt werden. Dazu muss die Seriennummer des Gerätes und der Config-Key eingegeben werden.

Nun kann der Errichter für dieses Gerät die Kundenkonten anlegen.

Bei Aufschaltung an die Leitstelle ruft der Errichter die Leitstelle an und nennt der Leitstelle Seriennummer und CMS-Key des Gerätes. Soll die Leitstelle in der Lage sein Änderungen an der Konfiguration des Gerätes durchzuführen teilt der Errichter der Leitstelle auch den Config-Key mit.

Die Leitstelle loggt sich dann mit Ihren Daten unter
http://www.residencecontrol.com/InfrastructureAdministration/Login.aspx

ein und kann über „CMS“ -> „Monitor New Device“ das Gerät Ihrer Leitstelle zuordnen. Hierzu einfach Seriennummer und CMS-Key eingeben. Soll das Gerät auch in der Geräteliste erscheinen und Änderungen an der Konfiguration möglich sein wird ebenfalls der Config-Key eingegeben. Die Leitstelle kann bei advanced das Häkchen bei „Keep Site No.“ Rausnehmen und dann in dem Feld „New Site No.“ Die für dieses Gerät gewünchte Objektnummer eingeben. Ein Klick auf Speichern sollte wenn keine Fehlermeldung kommt das Gerät hinzuffügen und anschliessend kann das Fenster geschlossen werden.

Leistungsmerkmale und Vorteile

- Hohe Zuverlässigkeit durch mehrere Übertragungskanäle (LAN / GPRS / SMS / GSM / PSTN) und redundante Server;
- Verbindungsüberwachung - einstellbare Fehlermeldezeit von nur 20 Sekunden.
- Jamming Erkennung - löst eine Benachrichtigung aus durch den alternativen Kanal oder Aktivierung eines Digitalausgangs.
- Unterstützung beliebiger Alarmsystem über die Digitaleingänge, serielle Schnittstelle oder Telefonemulation und DTMF-Dekodierung.
- Softwarebasierte Empfänger, die eine Vielzahl von Hardware-Empfänger Protokolle emulieren (Sur-Gard MLR2, Visonic RC4000, etc.).
- Webbasierte Software und Smartphone-App für Geräte-Konfiguration und Verwaltung. Firmware-Updates.
- Fernwartung - virtuelle serielle Schnittstelle zur Alarmanlage ermöglicht Fernprogrammierung mit der Alarmzentralen-Software des Herstellers.
- Videoverifikation der Alarmereignisse und kontinuierliche Bildaufzeichnung auf einer SD-Karte.
- Endbenutzer-Smartphone-App - unterstützt Push-Benachrichtigungen, Scharf- / Unscharfschaltung der Alarmanlage, Videoverifikation.

Installationsanleitung

Das Gerät kann zusammen mit der Alarmzentrale in einem Metallgehäuse oder nichtbrennbaren Kunststoffgehäuse montiert werden. Metallgehäuse sollten entsprechend geerdet werden. Die Ein-/Ausgänge können mit 0,50 mm² verdrilltem Kabel bis zu 100 Meter Länge verdrahtet werden.

Montage

1. Falls eine eigene SIM-Karte verwendet wird, dann muss die PIN-Abfrage der SIM-Karte, bevor es in das Gerät gelegt wird deaktiviert werden. Aktivieren Sie den mobilen Datenverkehr für den GSM-Service-Provider.

2. Stecken Sie die GSM-Antenne auf den SMA-Stecker. Bitte nicht die Antenne innerhalb eines Metallgehäuses zu platzieren.

3. Schließen Sie das Gerät an die Zentrale nach der gewünschten Kommunikationsmethode an *(siehe **Konfiguration des Terminals).*** Stellen Sie sicher, dass die Stromversorgung ausreichend ist. Der Ruhestrom des Moduls beträgt 150 mA, im Maximalfall aber bis zu 400 mA. **Achtung:** Die Stromversorgung zum Alarmsystem muss vor jeder Installation oder von Wartungsarbeiten getrennt werden.

4. Nun kann das Gerät eingeschaltet werden. Es sollte in weniger als einer Minute starten. Die GSM-LED-Anzeige sollte AN sein, um eine erfolgreiche Verbindung zum GSM-Netz anzuzeigen. **Bedeutung der LED-Anzeige:**

- Aus - das Gerät ist ausgeschaltet
- Langsames Blinken - keine Verbindung zu einem Server (CIS)
- An - das Gerät ist verbunden mit einem Server ohne Datenübertragung
- Schnelles Blinken - Datenübertragung

5. Überprüfen Sie die GSM-Signalstärke durch die ***Admin-Website*** oder ***Admin-mobile Anwendung***. Ist die Signalstärke nicht ausreichendm muß der Montageort des Geräts bzw. der Antenne geändert werden. Signalstärken unter 10 sind nicht akzeptabel. Empfohlen sind Werte über 14.

Achtung: Montieren Sie das Gerät nicht an Orten mit starken elektromagnetische Störungen (z.B. in der Nähe von Elektromotoren, etc.). Montieren Sie das Gerät nicht in feuchten Orten oder Orten mit hoher Luftfeuchtigkeit.

Konfiguration des Terminals MQ02 GPRS / LAN-Communicator mit 8 Eingängen

Terminals Beschreibung:

- IN1 - IN8: digitale Eingänge, bei anliegendem GND (-) aktiviert, mit Pull-up 2.2KΩ zu 5V.
- IN1 kann als Open-Collector-Ausgang konfiguriert werden.
- RXD und TXD: serielle Schnittstelle TTL (5V)

Konfiguration der Anschlüsse der MQ02 GPRS / LAN mit DTMF-Empfänger und PSTN-Backup

Terminals Beschreibung:

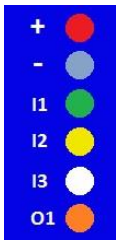
- IN1 - IN4: digitale Eingänge, bei anliegendem GND (-) aktiviert, mit Pull-up 2.2KΩ zu 5V.
- IN1 kann als Open-Collector-Ausgang konfiguriert werden.
- OUT1 und OUT2: Open-Collector-Ausgänge.
- RING und TIP: Verbindung zum analog Wählgerät der Alarmzentrale
- R1 und T1: Anschluß an die PSTN-Leitung

Konfiguration von Terminals MQ02 GPRS Communicator mit 4 Eingängen

Terminals Beschreibung:

- IN1 - IN4: digitale Eingänge, bei anliegendem GND (-) aktiviert, mit Pull-up 2.2KΩ zu 5V.
- IN1 kann als Open-Collector-Ausgang konfiguriert werden.
- RXD und T XD: serielle Schnittstelle TTL (5V)

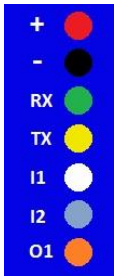
Verdrahtung MN01 Communicator mit 3 Eingängen



Drähte Beschreibung:

- Grün: IN1 (programmierbarer Eingang, vorkonfiguriert Scharf / Unscharf)
- Gelb: IN2 (programmierbarer Eingang, als Alarm vorkonfiguriert)
- Weiß: IN3 (programmierbarer Eingang, vorkonfiguriert als Sabotage)
- Orange: OUT1 (kann als Universalausgang oder als Schlüsselschalter konfiguriert werden)

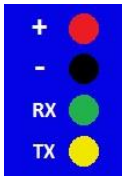
Verdrahtung MN01 Communicator mit serieller Schnittstelle für Paradox



Drähte Beschreibung:

- Grün: RxD, serielle Schnittstelle TTL (5V)
- Gelb: TxD, serielle Schnittstelle TTL (5V)
- Weiß: IN1 (programmierbarer Eingang, vorkonfiguriert Scharf / Unscharf)
- Grau: IN2 (programmierbarer Eingang, vorkonfiguriert als Alarm)
- Orange: OUT1 (kann als Universalausgang oder als Schlüsselschalter konfiguriert werden)

Verdrahtung MN01 Communicator mit serieller Schnittstelle für Texecom oder Teletek



Drähte Beschreibung:

- Grün: RxD, serielle Schnittstelle TTL (5V)
- Gelb: TxD, serielle Schnittstelle TTL (5V)

Verdrahtung MN01 Communicator mit DTMF-Decoder

Drähte Beschreibung:

- Grün: Verbindung mit dem RING (analog Wählgerät) der Alarmzentrale
- Gelb: Verbindung mit dem TIP (analog Wählgerät) der Alarmzentrale
- Weiß: IN1 (programmierbarer Eingang, vorkonfiguriert als Sabotage)
- Orange: OUT1 (kann als Universalausgang oder als Schlüsselschalter konfiguriert werden)

Gerätekonfigurationshandbuch

Ihre Verwaltungstools - Website und mobile Anwendung

In den meisten Fällen, brauchen Sie nur das Gerät zu verdrahten und die Objekt ID zu konfigurieren.

Der größte Teil der Konfiguration, die Sie brauchen, kann über die ***administrative mobile application*** für Android-Smartphones, die Sie hier herunterladen können durchgeführt werden:
https://play.google.com/store/apps/details?id=m2m.AdminMobile
Die mobile Anwendung wurde entwickelt, um eine einfache Konfiguration über 3G und WLAN zu ermöglichen, wenn Sie unterwegs sind.

Sie können auch die Einstellungen ändern mit *der* ***administrative website:*** www.m2mservices.com/admin Einige der Einstellungen, die selten geändert werden, können nur über die ***administrative Website*** konfigurieren.

Am häufigsten verwendete Szenarien

In diesem Kapitel werden einige der am häufigsten verwendeten Verwaltungsszenarien vorgestellt.

Konfiguration eines neuen Gerätes über eine Vorlage (Template)

- Es wird empfohlen, dass das Gerät mit Strom versorgt und mit dem Server (Connected = True) verbunden ist. Auf diese Weise können Sie alle verfügbaren Einstellungen überprüfen und speichern, einschließlich der Online-Einstellungen.
- Sie finden das Gerät durch seinen Controllername. Normalerweise gibt es eine Markierung auf der Rückseite des Gerätes mit den Namen des Controllers (Seriennummer).
- Wählen Sie das Gerät und wählen Sie "Alarm-Einstellungen (Alarm-Settings)" aus dem "Befehle (Commands)" Menü oder aus dem Kontextmenü.
- Es wird empfohlen, die Option "Online-Einstellungen aktivieren"' (Enable Online Settings). Andernfalls werden die Online-Einstellungen aus der Vorlage nicht angewendet. Lesen Sie die aktuellen Einstellungen aus dem Gerät durch Drücken der Taste "Get Current Settings" -Taste.
- Wählen und wenden Sie eine Vorlage mit den gewünschten Einstellungen an.
- Geben Sie die Site Number ein. Hinweis! Wenn Sie die Site Number vor Auswahl der Vorlage eingeben, wird diese wieder gelöscht.
- Speichern Sie die Änderungen.
- Sie können den Signalpegel durch Drücken der "Signalpegel" (Signal Level) Taste überprüfen. Das Gerät muss mit dem Server verbunden sein und 'Enable Online-Settings' aktiviert sein.

Speichern der Einstellungen als Vorlage (Template)

- Öffnen Sie die Alarmeinstellungen (Alarm Settings) von einem entsprechend konfigurierten Gerät
- Speichern Sie die Einstellungen als Vorlage mit dem Button "Als Vorlage speichern"(Save as Template). Wählen Sie einen neuen Namen für die Vorlage oder überschreiben Sie eine bereits vorhandene Vorlage.

Überprüfen des GSM-Signalpegels

- Bei der Installation des Gerätes vor Ort müssen Sie den Signalpegel des GPRS Kommunikators überprüfen. Der Signalpegel wird in Stufen von 0 bis 31 Stufen gemessen, unter 10 ist nicht akzeptabel. Empfohlen wird über 14.
- Suchen Sie das Gerät durch seine Site Number oder durch den Controllernamen der auf der Rückseite des Gerätes zu finden ist.
- Mit einem Doppelklick öffnen Sie die Info-Seite des Gerätes.
- Wählen Sie den Befehl Signalpegel (Signal Level) aus der Liste "Befehl" (Command) und drücken Sie den „Send Command“ 'Button.
- Das Ergebnis hat das Format '+ CSQ: 31,0 ". In diesem Fall ist der Signalpegel 31. Wenn der Signalpegel kleiner ist als 14, versuchen Sie einen besseren Ort für den Communicator zu finden oder versuchen Sie, den Ort oder die Rotation der Antenne zu ändern. Bei einem Pegel weniger als 10, kann es notwendig sein eine Antenne mit längerem Kabel zu verwenden.

Hinweis! Sie können den Signalpegel auch auf der Seite Alarmeinstellungen (Alarm Settings) überprüfen.

Geräte suchen

Die Hauptseite der ***Admin-Website*** bietet Werkzeuge, um Geräte nach verschiedenen Kriterien zu suchen. Sie können auch nach Geräten suchen in der "Search Controllers" Seite der ***Admin Mobile Anwendung:***

- **Serial Number** - das ist die eindeutige Kennung des Gerätes, die auf dem Etikett auf der Rückseite des Gerätes aufgedruckt ist (Bei Erstkonfiguration).

- **Controllername** - das ist der kundenspezifische Name des Geräts, die vom Endkunden geändert werden kann. Anfangs ist es das gleiche wie die Seriennummer des Gerätes.

- **Site Number** - das ist die eindeutige Kennung des Orts, an dem das Gerät installiert ist. Diese Nummer meldet das Gerät an die Notrufleitstelle. Sie werden in der Regel nach diesem Kriterium suchen, wenn die Geräte bereits installiert sind.

- **IMEI** - das ist die eindeutige Kennung des GSM-Moduls. Sie können es auf dem Etikett des GSM-Moduls des Communicators finden.

Weitere Suchattribute - Sie können diese Attribute nur von der ***Admin Website*** suchen:

- **Connection state** - filtert Geräte, ob sie derzeit mit dem Server verbunden sind oder nicht.

- **SIM-Karten-Nummer** - das ist die eindeutige Kennung der SIM-Karte, die Sie auf der SIM-Karte selbst finden. Es ist nur relevant, wenn Sie die SIM-Karte mit dem Gerät registriert haben (Siehe Kapitel "SIM-Karten Registrierung")

- **Phone Number** - Diese ist die Telefonnummer der SIM-Karte des Geräts. Es ist nur relevant, wenn Sie die SIM-Karte mit dem Gerät registriert haben (Siehe Kapitel "SIM-Karten Registrierung")

Auf der administrative site können Sie weitere Filter und Sortierungen der Datensammlung durchführen mit Informationen der Geräte.

Sortieren der Daten: Klicken Sie auf die Überschrift einer Spalte, um die Daten zu sortieren.

Filterung nach mehreren Kriterien gleichzeitig: Bewegen Sie die Maus über den Header einer Spalte und ein Dreieck wird angezeigt. Wählen Sie "Filter" und geben Sie das gewünschte Filter-Attribut.

Ein- und Ausblenden von Spalten: Aus dem gleichen Kontextmenü die Option "Spalten"(Columns) und aktivieren Sie diese, die Sie sehen möchten.

Anzeigen von Informationen eines bestimmten Controllers

Doppelklicken Sie auf ein Gerät aus der Liste der Controller um eine neue Seite mit den Details zu öffnen. Von dieser Seite aus können Sie Befehle an das Gerät senden und sehen die erhaltenen Antworten.

Senden von Befehlen an das Gerät

Da das Gerät eine konstante Verbindung zum Server hält, können Sie Verwaltungsbefehle in Echtzeit senden und empfangen Antworten. Dies kann von der Seite des Controllers durchgeführt werden. Wählen Sie den gewünschten Befehl aus dem Dropdown-Menü "Command" und drücken Sie "Befehl senden" (Send Command) -Taste. Das Ergebnis des Befehls wird in dem Textfeld angezeigt. Wenn Sie "Auto Clear Response" gewählt haben, wird die Antwort des vorherigen Befehls, bevor der nächste Befehl gesendet wird, gelöscht.

Befehle können auch von der Seite mit der Liste aller Geräte gesendet werden. Um dies zu erreichen, wählen Sie das gewünschte Gerät und drücken Sie die "Send Command 'Button. Dieser Ansatz ermöglicht es Ihnen, Befehle an mehrere Geräte gleichzeitig zu senden - zum Beispiel, wenn Sie mehrere Geräte auf einmal neu starten möchten. Wenn Sie jedoch diesen Ansatz wählen, können Sie nicht die Reaktion des ausgeführten Befehls sehen.

Hinweis! Um einen Befehl an ein Gerät senden zu können, muss es mit dem Server verbunden sein.

Beschreibung der Befehle:

- **Restart (Neu starten)** - startet das Gerät neu, beispielsweise nach einigen Konfigurationsänderungen
- **Connection State (Verbindungsstatus)** - Befehl, der ausführliche Informationen über Ein-Zustand, Signalpegel, GSM-Betreiber Auswahlmodus aktuell ausgewählten Betreiber und LAN-Einstellungen (falls vorhanden) zur Verfügung stellt.
- **Signal Level** - Überprüfen Sie die Höhe der GSM-Signal des Gerätes. Die Anzeige ist im Format '+ CSQ: 31,0 ". In diesem Fall ist der Signalpegel 31. Die Bedeutung der verschiedenen Werte des Bereichs finden Sie in der "RSSI Meanings.xls". Der Wert soll über 14 sein.
- **Voltage (Spannung)** - Prüft die Versorgungsspannung in Millivolt.
- **Card No (Kartennummer)** - liest die Seriennummer der SIM-Karte. Um eine SIM-Karte einem Gerät zuzuordnen, siehe Abschnitt "Register SIM-Karte".

Sie können auch den aktuellen Zustand über Android ansehen.

Suchen und navigieren Sie zu dem gewünschten Gerät. Auf der Registerkarte INFO können Sie die folgenden wichtigen Informationen sehen:

- **Connection State (Verbindungszustand)** - wenn das Gerät mit dem Server verbunden ist, wird dies mit einem grünen Symbol dargestellt, sonst ist das Symbol rot. Sie können sehen, ob das Gerät über LAN oder GPRS verbunden ist.
- **Inputs State (Zustand Eingänge)**- eine graphische Darstellung des aktuellen Zustands der Eingänge
- **Voltage (Spannung)**
- **Signal Level**
- **Operator Selection Mode (GSM Provider-Auswahlmodus) –** ob der Provider automatisch oder manuell ausgewählt ist.

- **Current Operator (Aktueller Provider)** - Den Code und den Namen des GSM-Providers, an dessen Netz das Gerät gerade registriert ist.
- **LAN-Einstellungen** -wenn Ger tes unterstützt LAN-Konnektivität Sie hier sehen können, wenn sie für die dynamische IP vom DHCP-Server oder mit einer statischen IP konfiguriert ist. Außerdem können Sie die aktuelle IP, Maske und Gateway.

Alarmeinstellungen des Wählgeräts

Die Alarmeinstellungen des Wählgeräts beinhalten die Site Number (Objekt Nummer), die Programmierung der digitalen Eingänge, serielle Port-Konfigurationen sowie die Konfiguration der Übertragungskanäle zur Notrufleitstelle.

Die Alarmeinstellungen stellen Sie wie folgt ein:

Suchen Sie das gewünschte Gerät (siehe "Geräte suchen" Abschnitt). Doppelklicken Sie auf das Gerät in der Liste der Controller mit den Suchkriterien, um die Info-Seite des Controllers zu öffnen. Wählen Sie im Menü Befehle Alarmeinstellungen.

Sie können das Gerät aus der Liste der Wählgeräte auswählen, der rechten Maustaste darauf und wählen Sie Alarmeinstellungen aus dem Kontextmenü.

Die meisten Einstellungen werden nur auf dem Server gespeichert, so dass Sie eine aktive Verbindung mit dem Gerät nicht brauchen. Manche Einstellungen müssen auf dem Gerät gespeichert werden, so ist es erforderlich, dass das Gerät verbunden ist. Diese Einstellungen werden als Online-Einstellungen bezeichnet.

Um Online-Einstellungen aus der ***Verwaltungs Website*** oder ***Verwaltungs mobile Anwendung*** zu ändern, müssen Sie das "Enable Online-Einstellungen" Kontrollkästchen markieren. Diese Option wird deaktiviert, wenn das Gerät gerade nicht verbunden ist.

Wenn Sie einige Einstellungen bearbeiten, werden die geänderten Felder in gelb gefärbt. Wenn Sie mit dem Programmieren fertig sind, drücken Sie die Schaltfläche Speichern. Die Einstellung wird auf dem Server gespeichert werden und wenn Sie die Online-Optionen aktiviert haben, werden sie auch in das Gerät geschrieben werden.

Um die Alarmeinstellungen von der ***Verwaltungs mobile Anwendung*** zu bearbeiten, gehen Sie folgendermaßen vor:

Suchen Sie das gewünschte Gerät (siehe "Geräte suchen" Abschnitt). Klicken Sie auf das Gerät in der Liste der Wählgeräte, um die Info-Seite zu öffnen. Navigieren Sie zur Registerkarte Einstellungen. Klicken Sie im Menü Alarmeinstellungen, um die Seite Alarm-Einstellungen zu öffnen.

Nachfolgend finden Sie eine Liste der Einstellungen, die Sie konfigurieren können.

Berichterstattung zur Leitstelle (CMS)

Konfigurieren der Leitstellen ID

Bei der Meldung von Ereignissen an die Überwachungszentrale, identifiziert sich das Gerät nach Seiten-Anzahl, manchmal auch als Kontonummer bezeichnet.

Sie können die Site-Nummer auf der Seite Alarmeinstellungen auf beiden konfigurieren das ***Verwaltungs Website*** und die ***Verwaltungs mobile Anwendung.***

Hinweis! Wenn der Communicator an der Alarmzentrale über die serielle Schnittstelle oder digitale Eingänge angeschlossen ist, werden die Ereignisse mit Hilfe der Website-Nummer, die der comm unicator zugeordnet wiesen. Allerdings, wenn der Communicator an das Festnetz Dialer der Alarmzentrale angeschlossen werden die E Öffnungen vom Dialer sind die Nutzung der Website Nummer, die in der Zentrale selbst programmiert wird berichtet. Stellen Sie daher sicher, dass Sie die gleiche Website-Nummer o n beide den Communicator und die Alarmzentrale konfiguriert haben.

Konfigurieren der verschiedenen Website-Nummern für verschiedene Partitionen

Wenn das System in mehrere Partitionen aufteilen, können Sie bieten verschiedene Website-Anzahl für jede Partition. Auf diese Weise können Sie einen einzelnen Communicator konfigurieren Ereignisse aus verschiedenen Standorten in d ependently berichten.

SiteNo4 Felder im Abschnitt Alarmeinstellungen auf die ***administrative Website*** und ***Verwaltungs mobile Anwendung*** - Sie können bis zu 4 zusätzliche Site Zahlen im SiteNo1 angeben. Wenn ein Ereignis von Partition 1 empfangen wird, wird sie mit SiteNo1 portiert wieder werden. Wenn SiteNo1 nicht angegeben ist, wird das Ereignis mit dem Gen-eric SiteNo wiesen. Wenn ein Ereignis von einer Partition außerhalb des Bereichs 1- 4 dann wieder der Ober SiteNo verwendet.

Hinweis! Die ev Eltern vom Dialer und vom seriellen Anschluss der Alarmzentrale enthalten erweiterte Angaben über die Partition. Abgesehen davon, haben Sie immer gespalten können das System in Partitionen e ven, wenn die Platte nur auf die graben ital Eingänge des Communicators verbunden. Beispielsweise können Sie festlegen, dass Eingang 1 Alarmereignis von Partition 1 zu erzeugen und Eingang 2 werden Alarmereignis aus Partition 2 (Siehe "Meldungen von digitalen Eingängen" Abschnitt) zu erzeugen. Auf diese Weise können Sie wieder Ereignisberichte aus verschiedenen unabhängigen erhalten Site Zahlen.

Hinweis! Die allgemeinen Veranstaltungen, die speziell für den Communicator sind zudem nur für einen der Site Zahlen gemeldet werden! Solche allgemeinen Ereignisse sind zum Beispiel die Verbindung unterbrochen Fall Jamming erkannt, regelmäßige Prüfung.

Berichterstattung an Central Monitoring Station

Außerdem sendet die Ereignisse an den Kunden vor Ort und dem Kunden den mobilen Einsatz, das Gerät auch für Central Monitoring Station unter Verwendung von Protokollen verschiedenen populären Hardware-Empfänger ", wie SurGard MLR2 berichten können. Für eine einfache Integration in die meisten Monitoring-Software, Ereignisse können umgeleitet werden, Visonic, KP RCI3300 usw.

Um die Umleitung Daten an eine Überwachungszentrale zu aktivieren, um Alarm-Seite des Gerätes Einstellung gehen in der ***administrativen Website*** oder in ***der Verwaltung mobiler Anwendungen*** und prüfen Sie den "Bericht zur CMS" aktivieren.

Wählen Sie das Transportprotokoll von der "Receiver-Protokoll" -Liste, zB SurGard MLR2.

D ie Format der Nachrichten, die standardmäßig verwendet wird, ist Ademco Contact ID.

Konfigurieren der von der MQ02 und MN01 Kommunikator s selbst erzeugten Meldungen

Konfiguration der Routinemeldung an die Leitstelle

Falls gewünscht kann der IM040 eine Routinemeldung in festgelegten Zeitabständen an die Leitstelle übertragen. Die Routinemeldung wird über die Verwaltungshomepage eingerichtet.

Wird hier nichts eingetragen, sendet das Modul keine Routinemeldung.

Hinweis: Es ist sehr wichtig, um zwischen periodischen Tests und den sogenannten Herzschläge, die verwendet werden, um die Verbindung zwischen dem Gerät und dem Server verfolgen zu unterscheiden. Das Gerät sendet Taktsignale an den Server in sehr kurzen Intervallen, um eine ständige Verbindung mit dem Server aufrechtzuerhalten und den Server zu ermöglichen, zu erkennen, wenn das Gerät abgeschaltet wird und eine Alarmmeldung sendet. Im Allgemeinen kann es einige Sekunden bis einige Minuten betragen. Diese Herzschläge werden nicht als Ereignisse an die Leitstelle weitergeleitet. Ein Alarmereignis wird nur gesendet, wenn der Server erfasst, dass ein Gerät getrennt wird.

Auf der anderen Seite wird die periodische Testnachricht an das Überwachungszentrum gesendet wird, und wird normalerweise in Abständen von einigen Stunden eingestellt. Ziel ist es, das Auftreten von Ereignissen vom Typ 'Keine Termine für Long Time "in der Monitoring-Software zu verhindern.

Der Großteil der übertragenen Daten wird durch den Heartbeat verursacht, aus diesem Grund kann die Zeit für die Heartbeat Intervalle konfiguriert werden. Es ist ein Teil der Service-Vereinbarung. Wenn Sie den Heartberat-Intervall ändern möchten, wenden Sie sich bitte an den Support.

Sie können das Intervall der Test-Nachrichten, die an die Monitoring-Software gesendet werden, konfigurieren.

Programmieren der Digitaleingänge

Sie können das Ereignis welches durch eine Auslösung eines Dig. Eingangs erzeugt wird frei konfigurieren. Dies kann sowohl von der **Verwaltungs Website** und **Verwaltungs mobile Anwendung** aus dem Abschnitt Eingabestifte auf der Seite Alarmeinstellungen durchgeführt werden.

Im Allgemeinen werden die digitalen Eingänge mit GND aktiviert. Bitte beachten Sie die Hardware-Spezifikation für Ihr Gerät.

Sie können die Nachricht, die gesendet wird, wenn der Eingangspegel hoch (GND getrennt) von der "Raising / ON" Seite frei einstellen.

Sie können die Nachricht, die gesendet wird, wenn der Eingangspegel niedrig (GND verbunden) aus dem Bereich "Falling / OFF" für jeden Eingang konfigurieren.

Die Nachrichten werden mit Hilfe des Contact ID Format eingegeben. Von der **Verwaltungs Website** "Bearbeiten" Knopf für jedes Feld, das Sie bearbeiten möchten. Von der **Verwaltungs mobile Anwendung** auf das Feld selbst. Ein Dialog öffnet sich, und Sie sollten die Veranstaltung c ode, die Partition und die Zone / user Komponenten der Kontakt-ID-Meldung anzugeben.

Wenn ein Feld leer gelassen wird, wird diese Digitaleingang nicht berichten Veranstaltungen.

Schwache Batterie und Netzstromausfall Meldungen

Diese Meldungen können über die Admin Web Schnittstelle eingerichtet werden.

Das Gerät überwacht die Versorgungsspannung und kann bei fehlender Netzversorgung oder Batterie eine Nachricht absetzen. Sie können die Nachricht festlegen und die Dauer wie lange die Spannung unterbrochen sein muss, bevor die Meldung abgesetzt wird. Das Gerät überwacht dauerhaft die Betriebsspannung (über 12v). Bricht diese Spannung ein (Grenzwert einstellbar) wird eine Störmeldung erzeugt und übertragen.

Medium verloren

Die Meldung für Medium verloren kann über die Admin Webschnittstelle eingerichtet werden.

Das Gerät sorgt für eine konstante Verbindung zum Server über LAN oder GPRS und sendet Keep-Alive-Herzschläge, um eine sichere Übertragung zum Server zu gewährleisten. Wenn der Server keine Daten vom Gerät empfängt, wird eine Störmeldung erzeugt.

Der meiste Datenverkehr den der Übertrager erzeugt, geht auf die Keep Alive Herzschläge zurück, aus diesem Grund ist es auch möglich den Intervall der Herzschläge zu konfigurieren. Wenn Sie den Herzschlag-Intervall ändern möchten, wenden Sie sich bitte an Ihren Kundenbetreuer.

Kommunikationskanal Meldungen

Diese Meldungen können nur über die Admin Webschnittstelle konfiguriert werden.

Die eingesetzte World SIM Karte verwendet automatisch immer das Beste zur Verfügung stehende Netz. Wird das Hauptnetz gestört, verbindet sich das Gerät automatisch mit einem der anderen zur Verfügung stehenden Netze. Nach einiger Zeit wird es automatisch versuchen, zurück in das Hauptnetz zu verbinden.

Die obige Funktion kann auch mit der Dual-SIM-Version unserer Geräte erreicht werden, mit lokalen SIM-Karten aus zwei verschiedenen Betreibern.

Für die kombinierten LAN + GPRS-Geräte, ist der Hauptkanal LAN und falls es ein Problem mit der LAN-Verbindung gibt wird das Gerät sich automatisch über GPRS zu verbinden. Nach einiger Zeit wird automatisch versucht, wieder über LAN zu verbinden.

Sie können die Meldung definieren die gesendet wird wenn das Gerät das Netz wechselt. Wenn Sie nichts konfigurieren, wird keine Meldung erzeugt. Dies hat keinen Einfluss auf das Umschalten zu dem jeweils besten Netz.

Jamming Meldung

Diese Meldungen können nur über die Admin Webschnittstelle konfiguriert werden.

Das Gerät kann ct Verklemmen Dete und Differenz der Störung und Netzwerkprobleme zu machen. Im Falle eines Staus auf den Server wird zuerst Anschluss verloren Ereignis zu berichten. Das Gerät wird das Verklemmen Meldung erst die Verbindung wiederhergestellt berichten! Wenn Sie LAN + GPRS-Gerät verwenden, dann wird die Jamming Nachricht wird sofort gemeldet werden, wenn sie über den LAN-Kanal erkannt.

LAN-Kabel Meldung

Diese Meldungen können nur über die Admin Webschnittstelle konfiguriert werden.

Die LAN+GPRS Geräte erkennen automatisch ob ein LAN Kabel eingesteckt ist oder nicht. Die Meldung „LAN Kabel angeschlossen“ bedeutet aber nicht automatisch das auch über LAN übertragen wird. Die bedeutet nur dass ein LAN Kabel physikalisch angeschlossen ist. Das Gerät Meldet „Verbunden über LAN“ wenn es tatsächlich per LAN überträgt. (siehe Abschnitt "Kommunikationskanalmeldungen").

Alarm Einstellungsvorlage

Diese Meldungen können nur über die Admin Webschnittstelle konfiguriert werden.

Um die Konfiguration mehrerer Geräte zu erleichtern können Sie die Einstellungen als Vorlage speichern.

Um dies zu tun, geben Sie die entsprechenden Einstellungen für ein Gerät und klicken Sie auf "Als Vorlage speichern". WICHTIG! Das Gerät muss mit dem Server verbunden sein und Sie müssen die Option "Online-Einstellungen aktivieren". Eingeschaltet haben. Dies ermöglicht es, alle Einstellungen in der Vorlage zu speichern, einschließlich derjenigen, die eine Verbindung mit dem Gerät benötigen. Geben Sie einen Namen für die Vorlage ein und speichern Sie sie. Sie können vorhandene Vorlagen auch einfach überschreiben.

Um eine vordefinierte Vorlage auf ein Gerät zu übertragen, öffnen Sie die Seite Alarmeinstellungen des Gerätes, drücken Sie "Vorlage laden" und wählen Sie die entsprechende Vorlage. Alle in der Vorlage gespeichert Felder werden mit den Werten aus der Vorlage gefüllt werden, mit Ausnahme der Site Number. Geben Sie die entsprechende Site-Nummer ein und klicken Sie "Speichern".

SIM-Kartenvergabe

Diese Meldungen können nur über die Admin Webschnittstelle konfiguriert werden.

Wenn eine neue SIM-Karte in das Gerät eingelegt zu, möchten Sie vielleicht, um es auf dieses Gerät in der Datenbank zugeordnet werden. Diese Vorgehensweise ist nicht obligatorisch, aber t er Informationen über Mapping zwischen den SIM-Karten und Geräte könnte während einiger Verwaltungsverfahren hilfreich sein.

Registrierung der SIM-Karte mit dem System automatisch, wenn Sie die Alarmeinstellungen des Gerätes konfigurieren (siehe "Alarm-Einstellungen des Controllers Abschnitt) durchgeführt.

Sie können auch das Registrierungsverfahren für ein oder mehrere Geräte manuell auslösen, indem Sie die gewünschten Geräte aus der Liste auf der Hauptseite und dann die 'Verify-SIM-Karte' Option aus dem Kontextmenü. Die Geräte müssen mit dem Server verbunden werden.

Wenn die SIM-Karte eines Geräts aus irgendeinem Grund ersetzt werden, dann müssen Sie auch diesen Vorgang auslösen. Um das letzte Mal zu sehen, wenn eine SIM-Karte überprüft, sollten Sie die versteckten Spalte "SIM-Karte Verified" einblenden.

Übertragene Meldungen eines Übertragers Anzeigen

Die Alarmmeldungen können zusätzlich zu der Aufschaltung zu einem Wachdienst, auch direkt zu dem Betreiber der Anlage übertragen werden. Sie können die Meldungen auf http://www.residencecontrol.com einsehen.

Darüber hinaus kann der Client-Site direkt vom Verwaltungszentrum zugreifen. Dies ist nützlich, wenn Sie die Geschichte der von einem Gerät von jedem Computer aus über das Internet generierten Ereignisse zu verfolgen, wenn Sie keinen Zugriff auf die Monitoring-Software haben müssen.

Um den Ereignisverlauf für ein Objekt anzuzeigen, suchen Sie das Gerät in der Verwaltungs Website, wählen Sie es in der Liste der Geräte, und wählen Sie "Client Site" aus dem Kontextmenü oder über die "Befehle" -Menü. Ein neues Fenster wird geöffnet und zeigt die Geschichte der Ereignisse für das Gerät.Möglicherweise müssen Sie Pop-ups für diese Seite zu ermöglichen.

Für die administrative Website sowie für die Client-Seite können Sie zusätzliche Konten mit eingeschränkten Berechtigungen erstellen, um nur einige der Controller sehen. Zum Beispiel können Sie ein Endbenutzer Rechte geben kann auch auf die Geschichte der Geräte er besitzt. Sie können die Zonen im Haus nennen Sie Namen, die Benutzer, die das Alarmsystem usw. Sie können Benachrichtigungen per E-Mail oder SMS für verschiedene Veranstaltungen richten Sie den Zugriff geben können.

Es ist eine administrative Anwendung für Android, um das zu erreichen einige der administrativen Aufgaben über Ihr Mobiltelefon. Es gibt auch eine Client-Android-Anwendung, so dass der Endverbraucher können den Verlauf der Ereignisse zu sehen und scharf / unscharf die Alarmanlage von seinem Smartphone.

Anschluss an die Alarmzentrale über Telefon

Verkabelung der Zentrale mit dem GPRS Übertrager

Schließen Sie die A/B Klemmen ihrer Alarmzentrale an Tip u. Ring des GPRS Übertragers an. Die Polung ist hier nicht relevant.

Richtlinien für die Konfiguration der Alarmzentrale

- Wählgerät in der Zentrale muss aktiviert sein
- Wählen Sie DTMF (Ton) Wahl
- Wählen Sie Contact ID Vollkommunikationsformat
- Geben Sie einen einfache Telefonnummer (999999) ein, vermeiden Sie nur ein einziges Zeichen als Telefonnummer zu verwenden..
- Geben Sie die Kundennummer die Sie vom Wachdienst bekommen haben im Panel ein. Die Kundennummer sollte immer 4 Zeichen Lang sein.
- Es wird empfohlen die "Telefonleitungsüberwachung" zu deaktivieren
- Es wird empfohlen die Funktion „Warten auf Wählton“ zu deaktivieren.

Konfigurieren als DTMF Dekodierer

Die DTMF fähigen Geräte sind in der Regel schon richtig vorkonfiguriert. Falls die Einstellungen dennoch ändern möchten, gehen Sie wie folgt vor:

Auf der Admin Webseite navigieren Sie zu „Commands-> Site Alarmeinstellungen“ setzen Sie den Haken bei "Aktiviere Online-Einstellungen" und klicken Sie auf "Get Current Settings", um die Einstellungen aus dem Gerät auszulesen. Das Gerät sollte eingeschaltet und mit dem Server verbunden sein, andernfalls sind Felder ausgegraut. In dem Abschnitt „COM Einstellung“ wählen Sie "None" in dem Tunnelfeld, wählen Sie nun einen entsprechenden DTMF Modi (siehe unten für die

Beschreibung der Betriebsarten). Dadurch wird automatisch die richtige Baudrate und das Format (4800, 8N1) eingestellt. Drücken Sie die Taste "Speichern".

Wenn Ihr Übertrager über einen PSTN Backupweg verfügt können Sie die nachfolgenden Einstellungen wählen.

"DTMF2" – In diesem Modus simuliert das Gerät einen PSTN Anschluss und setzt Meldungen ausschließlich über GPRS ab. Selbst wenn das Gerät mit dem PSTN Netz verbunden ist, wird es dieses nicht nutzen.

"DTMF2 / PSTN" - in diesem Modus werden die Daten über GPRS gesendet. Sollte das GPRS Netz gestört sein, schaltet das Gerät in den Transparent Mode um. Die Alarmanlage kann so direkt über PSTN wählen. Stellen Sie sicher, dass das PSTN Festnetz mit dem T1 und R1 Anschluss des Communicators verbunden ist. Hinweis: Wenn die GPRS-Verbindung wieder hergestellt ist, werden alle Ereignisse, die über das PSTN Festnetz gewählt worden sind, auch über die GPRS übertragen.

"DTMF2 / PSTN Parallel" – In diesem Modus werden alle Meldungen über PSTN und GPRS übertragen. Dieser Modus wird nur empfohlen, wenn Sie aus der Ferne programmierarbeiten an der Zentrale durchführen möchten. **Aktivieren Sie diesen Modus nur bei der Programmierung, deaktivieren Sie in anschließend wieder, stellen Sie DTMF2 oder DTM2 / PSTN ein.**

Es ist sehr wichtig zu verstehen, dass, wenn das PSTN Festnetz nicht richtig funktioniert, die Meldungen auch nicht über GPRS übertragen werden. Der Grund dafür ist, dass die MQ02 nur auf ContactID Ereignisse hören, aber keine Bestätigung zur Alarmzentrale zurück senden. Funktioniert das PSTN Netz aber nicht richtig, wird die Alarmzentrale einige Male versuchen die Meldung abzusetzen um anschließend aufzugeben. Die Anlage wählt nach den eingestellten Wahlversuchen für gewöhnlich nicht erneut zum Wachdienst. Aus diesem Grund erfolgt hier keine weitere Übertragung über GPRS. Wir empfehlen deswegen diesen Modus nur Temporär zu verwenden!

Kontonummer Berichtsarten

Sie können wählen, ob die Alarmereignisse zusammen mit der Kontonummer welche in der Zentrale programmiert ist übertragen wird, oder ob die Kontonummer des IM040 Überträgers verwendet werden soll.

Von der **Verwaltungs Website** , navigieren Sie zu "Commands" -> Alarmeinstellungen“. Wenn ein DTMF Modi aktiv ist, können Sie in diesem Menü den Haken setzen bei „Keep DTMF Account Number“. Wenn diese Funktion aktiviert ist, werden die Alarmereignisse mit der Kontonummer, die in der Zentrale programmiert ist übertragen. Dies kann nützlich sein, wenn Sie verschiedene Kontonummern für die verschiedenen Bereiche in der Alarmzentrale angeben möchten. **Hinweis**: die Ereignisse, die von dem IM040 Kommunikator selbst erzeugt werden, werden immer mit der SiteNo des Überträgers abgesetzt. Sie können die SitNo über die Admin Webseite ändern.

Wird der Haken bei „Keep DTMF Account Number“ nicht gesetzt, werden alle Meldungen mit der Site Number des IM040 Überträgers abgesetzt. Dies kann nützlich sein, wenn in der Zentrale keine SiteNo programmiert werden soll.

Anschluss Meldezentralen über die serielle Schnittstelle

MQ02 und MN01 Kommunikatoren unterstützen die Integration über die serielle Schnittstelle mit einigen Alarmzentralen. Bitte stellen Sie sicher dass die verwendete Alarmzentrale vom IM040 Kommunikator unterstützt wird. Möchten Sie den IM040 Kommunikator Seriell anschließen

benötigen Sie ein entsprechendes Kabel. Die MN01 Kommunikatoren werden bereits mit einem passenden Kabel ausgeliefert.

Auswahl der Alarmzentrale

Von der **Verwaltungs Website** , navigieren Sie zu „Commands-> Seite Alarmeinstellungen“. Klicken Sie auf die Schaltfläche "Aktiviere Online-Einstellungen" und klicken Sie auf "Get Current Settings", um die Einstellungen aus dem Gerät auszulesen. Der Kommunikator muss eingeschaltet und mit dem Server verbunden sein, ansonsten werden die Felder nicht angezeigt. In den COM Einstellungen wählen Sie "None", in dem Tunnel-Feld und im Ereignisfeld wählen Sie die Marke und das Modell der Alarmzentrale welche Sie über die Serielle Schnittstelle anschließen möchten. Die richtige Baudrate sowie Protokoll werden automatisch richtig eingestellt. Sie können diese Einstellungen bei Bedarf ändern. Bei einigen Meldezentralen kann es nötig sein ein Passwort zu hinterlegen um Zugriff auf die Alarmzentrale zu erlangen. Klicken Sie abschließend auf "Speichern".

Siehe unten für Alarmzentrale spezifischen Einstellungen.

Konfigurieren von Texecom Premier Alarmzentralen

Befolgen Sie die Anweisungen im Abschnitt "Auswahl der Alarmzentrale" und wählen Sie die entsprechende Alarmzentrale aus.

Geben Sie im Feld „Pass1“ das UDL Passwort ihrer Texecom Alarmzentrale ein. Wenn Sie es nicht geändert haben, lautet das UDL Passwort 1234.

Fernsteuerung der Alarmzentrale einrichten

Mit dem IM040 Kommunikator wird es möglich bestehende und neue Alarmzentralen aus der Ferne zu steuern. Sie können den aktuellen Status des Systems zu überwachen, den Ereignisspeicher ansehen sowie aktuelle Meldungen einsehen bzw. Push Nachrichten erhalten. Eine Bedienung der Zentrale über eine Smartphone App ist ebenfalls möglich.

Sie können die App im entsprechenden Store ihres Smartphones herunterladen. Suchen Sie einfach nach "RControl M2M", oder nutzen Sie einen der folgenden Links:
https://play.google.com/store/apps/details?id=m2m.mobile
https://itunes.apple.com/bg/app/residence-control/id712098315?mt=8

Um die Funktion der Fernschärfung/Entschärfung zu ermöglichen muss sowohl der Kommunikator als auch die Zentrale richtig konfiguriert sein. Bei einigen Alarmzentralen kann diese Funktion über die Serielle Schnittstelle bereitgestellt werden. Bei manchen Zentralen kann die Funktion nur über die Funktion „Schlüsselschalter“ realisiert werden. Unabhängig welche Variante Sie nutzen, muss ein entsprechender Benutzer mit den rechten zur Fernsteuerung der Anlage eingerichtet werden.

Konfigurieren der Schlüsselschalteroption

Sie können praktisch jede Alarmzentrale aus der Ferne schärfen welche über die Option „Schlüsselschalter“ verfügt.

Das allgemeine Prinzip der Arbeitsweise ist wie folgt:

Konfigurieren Sie einen Ausgang des Kommunikators als Schlüsselschalter. Verbinden Sie diesen Ausgang mit einem Eingang/Zone der Alarmzenrale. Diese Zone bzw. Eingang muss als Impuls Schlüsselschalter programmiert werden. Bei Aktivierung wird der Ausgang des Kommunikators für eine definierte Zeit gegen Masse geschaltet. Jeder Impuls löst entweder die Schärfung oder Entschärfung aus.

Der Kommunikator braucht eine Rückmeldung der Zentrale um den Scharfzustand auszuwerten. Um Dies zu erreichen muss ein Ausgang der Zentrale mit dem Ereignis „Scharf/Unscharf“ oder Scharfstatus programmiert werden. Verbinden Sie diesen Ausgang der Zentrale mit dem Eingang des Kommunikators.

Hinweis! Es ist nicht möglich mehrere Partitionen getrennt zu schalten. Der Kommunikator verfügt über einen Steuerausgang. Programmieren Sie Ihre Zentrale entsprechend so, dass der gewünschte Bereich geschaltet wird.

Den Kommunikator entsprechend konfigurieren

Um einen Ausgang des Communicators als Schlüsselschalter zu konfigurieren öffen Sie die **administrative Website** , navigieren Sie zu „Commands- Seite> Alarmeinstellungen“. Setzen Sie den Haken bei "Aktivieren Online-Einstellungen" und klicken Sie auf "Get Current Settings", um die Einstellungen aus dem Gerät auszulesen. Das Gerät muss eingeschaltet und mit dem Server verbunden sein.

Im Abschnitt „Pins“ wählen Sie die Klemme, die Sie konfigurieren möchten, und wählen Sie die Schlüsselschalter-Option aus der Dropdown-Liste aus. Bei einigen Modellen kann nur der IN1 Kontakt als Keyswitch gewählt werden. Andere Molle mit 3 Kontakten können frei konfiguriert werden.

Nachdem Sie Option „Schlüsselschalter“ eingestellt haben, können Sie verschiedene Optionen konfigurieren:

"Peripheral-Name" – Der Name der in der App angezeigt wird.

"Impulse" - wie lange der Impuls sein soll. Es hängt von der Konfiguration der Alarmzentrale ab, In der Regel funktioniert ein Wert von 1000ms (1s) problemlos.

"Feedback Input" - wählen Sie den Eingang des Communicators, welchen Sie mit dem Ausgang der Alarmzentrale verbunden haben um den Scharfstatus auszuwerten.

"Armed Level" – legt die Konfiguration der Verdrahtung des Eingangs fest. Diese Funktion ist abhängig von der Programmierung der Alarmzentrale. Von Werk aus ist das Gerät so konfiguriert: Unscharf = Kontakt offen, Scharf = Kontakt gegen Masse geschlossen. Beachten Sie dass die Ein und Ausgänge des Kommunikators immer gegen Masse schalten bzw. ausgewertet werden. Daher sollten Sie sicher stellen dass der Zentralenausgang immer gegen GND (0V) schaltet anstatt gegen +V

Allgemeine Richtlinien für die KONFIGURATION des Schlüsselschalters der Alarmzentrale

Nachdem Sie die Schlüsselschalter-Optionen des Communicators konfiguriert haben, sollten Sie die Schlüsselschalter Zone der Alarmzentrale selbst konfigurieren. Schauen Sie dazu in der Anleitung der Alarmzentrale nach. Die Schlüsselschalterfunktion kann nur mit Alarmzentralen genutzt werden

welche über einen Impulsschlüsselschalter geschärft werden können. Weiterhin kann es nötig sein bei einigen Alarmzentralen die Verdrahtung mit einem Abschlusswiderstand abzuschließen.

Hinweis: Gemeinsame Eingangs- / Ausgangsanschlüsse

Bei Allem Modellen des MQ02 Kommunikators kann der IN1 Anschluss frei als Eingang oder Ausgang konfiguriert werden. Bei einigen Modellen ist dies auch bei den Anschlüssen IN7 und IN8 möglich.

Wenn ein Terminalanschluss geteilt wird, kann er als Ein und Ausgang konfiguriert werden, Hier ist es wichtig zu verstehen das die Eingange über einen Pull Up Widerstand von 2,2K auf +5V gezogen werden, dadurch kann die gemessene Spannung zwischen den Pins von 0v abweichen. Möglicherweise funktioniert in diesem Fall die Schlüsselschalterfunktion nur mit einem Zusatzrelais.

*****

Hinweis: Nachdem Sie sowohl den Communicator und die Alarmzentrale erfolgreich programmiert haben, finden Sie im Abschnitt "Erteilen von Remote-Zugriff für Benutzer", nähe Informationen wie der Zugriff für den Kunden eingerichtet wird.

Gewähren von Remote-Zugriff für Benutzer

Sobald die Alarmzentrale sowie der IM040 Überträger für den Fernzugriff entsprechend eingerichtet wurden, muss für den Benutzer ein Konto angelegt werden. Dieses Konto muss nun noch mit der Alarmzentrale verknüpft werden. Beachten Sie die Zugriffsrechte, wenn diese nicht stimmen, wird der Zugriff nicht funktionieren.

Um einem Benutzer Fernzugriff zu gewähren, navigieren Sie zu Commands-> Remote-Seite Benutzer. Um einen neuen Benutzer zu erstellen, drücken Sie die Schaltfläche Benutzer hinzufügen. Um bestehende Benutzer zu bearbeiten, markieren Sie ihn und drücken Sie die Taste Benutzer bearbeiten. In der neuen Seite, geben Sie die erforderlichen Daten ein. Wenn Sie dem Benutzer die Fernschärfung erlauben möchten, setzen Sie den Haken bei „Allow Remote Access“. **Hinweis:** Aktivieren Sie diese Option nur, wenn die Alarmzentrale und der Kommunikator entsprechend konfiguriert sind (Schlüsselschalter oder Serielle Kontrolle der Anlage).

Wenn das Allow Remote Access Kontrollkästchen aktiviert ist, wird dem Benutzer die Standardberechtigungen zur Fernschärfung der Partition 1 zugewiesen. Wenn Sie die Standarteinstellung ändern möchten, drücken Sie die Schaltfläche "Erweitert". Sie können weitere Partitionen (nur für Alarm-Panels, die über die serielle Schnittstelle unterstützt werden) hinzufügen und zur Fernschärfung/Entschärfung freigeben.

Sobald Berechtigungen erteilt, muss ein Secure Pairing V ERFAHREN abgeschlossen, bevor der Benutzer tatsächlich die Platte aus der Ferne steuern. Der Paarungsvorgang fügt zusätzliche Sicherheitsstufe. Es erfordert physischen Zugriff auf das Alarmzentrale, um tatsächlich ermöglichen den Fernzugriff. Auf diese Weise soll ein Installationsprogramm, um heimlich einen neuen Benutzer hinzufügen, die die Alarmzentrale fernsteuern können, zu verhindern.

Nachdem Sie einen neuen Benutzer angelegt haben und diesem die Berechtigung zur Fernschärfung erteilt haben, werden Sie gefragt ob Sie die Kopplung starten möchten. Darüber hinaus können Sie

den Kopplungsvorgang durch Drücken der "Sichere Pairing" -Taste für einen vorhandenen Benutzer starten. Anschließend kann der Kopplungsvorgang vom Benutzer gestartet werden.

Egal für welche Variante Sie sich entscheiden, um die Kopplung zu starten, müssen Sie den Pin Code angeben, welchen der Benutzer in der App verwendet um die Anlage scharf/unscharf zu schalten. Nun haben Sie 30 Sekunden Zeit um die Alarmanlage lokal am Bedienteil mit einem gültigen Code zu schärfen und wieder zu entschärfen. Wenn die 30 Sekunden ablaufen und die Anlage nicht geschaltet wurde, müssen Sie diesen Vorgang erneut durchführen.

Hinweis: Der Remote Pin wird vom Benutzer nur zur Scharf/Unscharf Schaltung aus der Ferne über die App verwendet. Der Remote Pin kann von dem Benutzercode in der Alarmzentrale abweichen!

Der Endbenutzer muss sich in der Mobilen App mit seinen persönlichen Zugangsdaten in der App einloggen. Der Benutzer kann in der App immer eingeloggt bleiben, allerdings wird bei jedem Schaltvorgang der Pin abgefragt um eine missbräuchliche Nutzung zu verhindern.

Hinweis: Sollten Sie Änderungen am Benutzerkonto des Kunden vornehmen, muss sich dieser neu einloggen um die Einstellungen zu übernehmen. Meldet er sich nicht erneut an, kann es passieren das die Steuerung aus der Ferne nicht korrekt funktioniert bis er sich das nächste mal neu anmeldet.

Konfigurieren der LAN-Einstellungen

Der IM040 Kommunikator verwendet zwei redundante Übertragungswege um Meldungen zum Wachdienst zu übertragen. LAN ist in diesem Fall der Primäre übertragungsweg, scheitert die Übertragung, schaltet das Gerät auf GPRS um.

Um die LAN Einstellungen zu ändern öffnen Sie die **administrative Website** , navigieren Sie zu "Befehle" -> LAN-Einstellungen-Menü.

Um die LAN Einstellungen über die Mobile App zu ändern, Öffnen Sie **Verwaltungs mobile Anwendung** , navigieren Sie zu Einstellungen, und wählen Sie das Menü LAN-Einstellungen.

Einer der Hauptvorteile hierbei ist, dass Sie die LAN Einstellungen konfigurieren können während das Gerät über GPRS verbunden ist. Auch ist es nicht erforderlich statische externe IP-Adresse oder irgendwelche Port-Weiterleitungen im Router einzurichten. In den meisten Fällen genügt es, das Gerät über LAN mit dem Router zu verbinden.

Das Gerät unterstützt automatische IP Vergabe von DHCP Server (Werkseinstellung).

Natürlich kann die IP Adresse auch manuell eingerichtet werden. Geben Sie dazu die gewünschten IP Parameter ein. Ein DNS Server muss hierbei nicht vergeben werden.

Weiterhin gibt es die Möglichkeit das LAN Modul komplett auszuschalten. Wir empfehlen allerdings die Nutzung über LAN+GPRS

Hinweis! Es ist ebenfalls möglich Meldungen wie „LAN Kabel verloren“ über die **Verwaltungs Website** zu konfigurieren(siehe "Kommunikationskanal Nachrichten" Abschnitt und Abschnitt "LAN-Kabel Nachricht").

Technische Details

Kommunikation: GPRS, SMS

Unterstützte Protokolle: Ademco Kontakt ID®. Unterstützung beliebiger Alarmsystem über die Digitaleingänge, serielle Schnittstelle oder das Telefonemulation und DTMF-Dekodierung

GSM / GPRS: Quadband (850/900/1800/1900 MHz); GPRS Klasse 12

ARM9-Prozessor, 2 MB RAM, 4 MB Flash-

LAN Ethernet 10/100; Micro SD-Karte bis zu 32 GB

Bis zu 8 digitale und 2 analoge Eingänge; bis zu 3 digitale Ausgänge

3 serielle Schnittstellen - UART, RS232 (300 – 115.200 Kbps), RS485 (300-19.200 Kbps) oder Bluetooth (optional)

Dual-SIM-Karte (optional)

Antennenanschluss: SMA, 50 Ohm

Optionale Erweiterungsmodule:

- ✓ DTMF-Decoder unterstützt Ademco ContactID, Ademco 4 + 2
- ✓ 868 MHz Funk-Transceiver
- ✓ RFID 125 kHz oder 13,56 MHz MiFare / NFC-Kartenleser
- ✓ IP-Kamera

Versorgungsspannung:	7-20 VDC; Spitzenstromaufnahme 400 mA max.
Strom im Standby-Modus verwendet:	150 mA max.
Maße:	110 x 70 x 33 mm
Betriebstemperaturbereich:	-20 ... + 55 °C
Gewicht:	150 g (Gerät)

Hiermit erklärt Secplan Technik GmbH dass sich dieses Gerät in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 1999/5/EG befindet.

Vollständige CE Erklärung unter www.secplan.de/ce