




Benutzerhandbuch für CUBE Einbruchserkennung und Alarmübertragung

Dokumentnummer:  GU-10023-DE

Veröffentlichungsdatum: 01/08/2024

Benutzerhandbuch für CUBE Einbruchserkennung und Alarmübertragung

Inhaltsverzeichnis

| | |
|--|-----------|
| Vorwort | 9 |
| 1. Benötigte Komponenten..... | 9 |
| 2. Software-Version | 9 |
| 3. Voraussetzungen zur Verwendung dieses Handbuchs | 9 |
| 4. Siehe auch | 9 |
| 5. Eigentumsvorbehalt | 9 |
| 6. Glossar | 10 |
| | |
| 1. Hintergrund zur Einbruchserkennung | 18 |
| 1.1. Überblick über die Basisversion von CUBE Einbruch | 18 |
| 1.2. Überblick über die Multi-TILLYS-Variante von CUBE Einbruch | 18 |
| 1.3. Neuheiten und Vorteile von CUBE Einbruch | 20 |
| 1.4. Definition der erwarteten Funktion durch Sicherheitsbeauftragten | 21 |
| 1.5. CUBE Einbruch-Voraussetzungen, die vom Kunden zu implementieren sind | 21 |
| 1.6. Systemmanagement | 21 |
| 1.7. Hintergrundinformationen für Errichter | 23 |
| 1.7.1. Formate der zwischen der TILLYS und der Fernüberwachungsleitstelle ausgetauschten Frames | 23 |
| 1.7.1.1. Von Meldepunkten and die Fernüberwachungsleitstelle gesendete Codes | 24 |
| 1.7.1.2. Ereigniscodes von den Überwachungsbereichen an die Fernüberwachungsleitstelle | 27 |
| 1.7.1.3. Fernsteuerungen von der Fernüberwachungsleitstelle an die TILLYS:..... | 27 |
| 1.7.2. Werte des numerischen Registers für den Gruppenstatus bei CUBE Einbruch | 28 |
| 1.7.3. Register des microcodes, spezifisch für CUBE Einbruch | 30 |
| 1.7.4. Befehl für den microcode, spezifisch für TACTILLYS-IP CUBE | 30 |
| | |
| 2. Workflow bei CUBE Einbruch | 31 |
| 2.1. Vorbereitung der IT-Umgebung | 31 |

| | |
|--|-----------|
| 2.2. Vorbereitung der CUBE Einbruch-Konfiguration durch den TIL-Partner in seinen Räumlichkeiten | 31 |
| 2.2.1. Workflow - Vorkonfiguration von CUBE Einbruch durch den Partner in seinen Räumlichkeiten | 31 |
| 2.2.2. Workflow - Exportieren/Importieren der CUBE EinbruchKonfiguration..... | 31 |
| 2.3. Konfiguration von CUBE Einbruch durch den TIL-Partner am Standort des Kunden | 32 |
| 2.3.1. Workflow - CUBE Einbruch-Konfiguration am Standort des Kunden . | 32 |
| 2.3.2. Workflow - Konfigurieren eines Ausweises zum Zugriff auf Bedienteil TACTILLYS-IP CUBE | 32 |
| 2.3.3. Workflow - Installation, Konfiguration und Parametrierung eines TACTILLYS-IP CUBE-Bedienteils vor seiner Inbetriebnahme | 33 |
| 3. Parametrisierung von CUBE Einbruch durch den TIL-Partner | 34 |
| 3.1. Hardware-Architektur für die Konfiguration von CUBE Einbruch durch den Partner | 34 |
| 3.2. Konfiguration, Parametrierung und Wartung von CUBE Einbruch an der TILLYS | 35 |
| 3.2.1. Konfigurationsschritte für CUBE Einbruch | 35 |
| 3.2.1.1. Zugriff auf Administratorenschnittstelle von CUBE Einbruch an einer TILLYS | 36 |
| 3.2.1.2. Einrichten eines Alarmüberwachungsbereiches..... | 36 |
| 3.2.1.3. Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät | 40 |
| 3.2.1.4. Multi-TILLYS-Konfiguration: Klonen der Verbindung zur Host-TILLYS an einer TILLYS | 41 |
| 3.2.1.5. Konfiguration der CUBE Meldepunkte einer TILLYS | 42 |
| 3.2.1.6. Einrichten eines CUBE-Meldepunkts an einer TILLYS | 45 |
| 3.2.1.7. Einrichten einer CUBE Alarmsirene | 45 |
| 3.2.1.8. Konfigurieren einer CUBE Alarmsirene an einer TILLYS.... | 47 |
| 3.2.1.9. Übersichtsvergleich der Meldepunkte für Multi-TILLYS-CUBE Einbruch | 47 |
| 3.2.1.10. Zuordnung eines TACTILLYS-IP CUBE -Bedienteils zu einer oder mehreren Meldergruppen einer Host-TILLYS | 48 |
| 3.2.1.11. Konfigurieren der Fernüberwachungsleitstelle | 50 |
| 3.2.1.12. Anzeige der Fernüberwachungskonfiguration | 51 |
| 3.2.2. Parametrisierung und Wartung von CUBE Einbruch | 52 |
| 3.2.2.1. Erstellen von Einbruchsprofilen an der Host-TILLYS | 52 |
| 3.2.2.2. Auswahl der Meldergruppen, die von einem TACTILLYS-IP CUBE verwaltet werden | 52 |
| 3.2.2.3. Auswahl des Authentifizierungsmodus (Ausweis oder Ausweis + Code) an einem TACTILLYS-IP CUBE | 53 |
| 3.2.2.4. Auswahl der Applets, die auf einen TACTILLYS-IP CUBE geladen werden sollen | 53 |

| | |
|---|-----------|
| 3.2.2.5. Auswahl der Detailebene für Ereignisse im TILLYS-Protokoll | 53 |
| 3.2.2.6. Wahl der Sicherheitsstufe über IP zwischen TILLYS und TACTILLYS-IP CUBE | 54 |
| 3.2.2.7. Löschen der TACTILLYS-IP-Schlüssel (Desetzen) | 54 |
| 3.2.3. Schritte zur Bewältigung von Einbrüchen | 55 |
| 3.2.3.1. Maskieren oder Wiederereinsatz eines Alarmmelders | 55 |
| 3.2.4. Wartung von CUBE Einbruch | 55 |
| 3.2.4.1. Aktivieren oder Deaktivieren des Ports zur Wartung einer TILLYS 3.2.4.2. Exportieren oder Importieren einer CUBE Einbruch- Konfigurationsdatei | 55 |
| 3.2.4.3. Verlängerung der Gültigkeitsdauer eines Tokens | 56 |
| 4. Installation, Einstellung und Verwendung des Bedienteils TACTILLYS-IP CUBE | 57 |
| 4.1. Installation, Konfiguration und Wartung eines TACTILLYS-IP CUBE-Bedienteils | 57 |
| 4.1.1. Physische Installation und Anschluss eines TACTILLYS-IP CUBE- Bedienteils | 57 |
| 4.1.2. Zugriff auf Administratorenschnittstelle des TACTILLYS-IP CUBE- Bedienteils und Anzeige seiner Einstellungen..... | 57 |
| 4.1.3. Passwortänderung für den Administrator des TACTILLYS-IP CUBE- Bedienteils | 58 |
| 4.1.4. Uhrzeiteinstellung für Bedienteil TACTILLYS-IP CUBE | 59 |
| 4.1.5. Netzwerk-Einstellungen für TACTILLYS-IP CUBE | 60 |
| 4.1.6. Aktualisierung der Firmware für TACTILLYS-IP CUBE | 60 |
| 4.1.7. Einrichten der Ereignisprotokollierung für TACTILLYS-IP CUBE | 60 |
| 4.1.8. Desetzen des TACTILLYS-IP CUBE | 61 |
| 4.2. Parametrierung des TACTILLYS-IP CUBE | 61 |
| 4.2.1. Authentifizierung und Navigation am TACTILLYS-IP CUBE-Bedienteil . | 61 |
| 4.2.2. Abfrage der Betriebseinstellungen des TACTILLYS-IP CUBE | 63 |
| 4.2.3. Parametrierung des TACTILLYS-IP CUBE | 64 |
| 4.2.4. Auswahl der Netzwerkeinstellungen des TACTILLYS-IP CUBE | 64 |
| 4.2.5. Abstellen des Alarms für den Sabotageschutz in der Installationsphase des TACTILLYS-IP CUBE | 64 |
| 4.2.6. Automatisches Abmelden des TACTILLYS-IP CUBE | 64 |
| 4.3. Verwendung des TACTILLYS-IP CUBE | 64 |
| 4.3.1. Manuelles Scharf- oder Unscharfschaltung eines Bereiches..... | 65 |
| 4.3.2. Manueller Maskieren von fehlerhaften Alarmmeldern | 65 |
| 4.3.3. Sirenen ausschalten | 65 |
| 4.3.4. Überschreiben der Scharfschaltung auf Meldergruppe(n) | 66 |
| 5. Konfiguration und Nutzung von CUBE-Einbruch | 67 |
| 5.1. Importieren der CUBE Einbruch-Konfiguration in MICROSESAME | 67 |
| 5.2. Verfahren zur Vorbereitung eines CUBE Ausweises zur Verwaltung von Einbrüchen an einem TACTILLYS-IP CUBE Terminal | 68 |

| | |
|--|-----------|
| 5.2.1. Vorbereitung eines Ausweises zur Kontrolle gegen Einbrüche | 68 |
| 5.2.2. Übernahme eines nicht zugewiesenen ID-Mittels in MICROSESAME | 68 |
| 5.2.3. Zuweisung eines verfügbaren ID-Mittels an einen neuen Benutzer | 68 |
| 5.2.4. Zuweisung von Berechtigungen an einen neuen Benutzer | 69 |
| 5.2.5. Einem neuen Benutzer ein CUBE Einbruchsprofil zuweisen | 69 |
| 5.3. Verwaltung der Einbruchsprofile der Benutzer auf MICROSESAME oder WEBSesame | 70 |
| 5.4. Einrichten der Übersicht auf MICROSESAME | 70 |
| 5.5. Übersicht auf MICROSESAME ansehen | 70 |
| 5.6. Erklärung der Operators für die Erkennung von Einbrüchen auf der TILLYS | 71 |
| 5.7. Test der Anlage zur Erkennung von Einbrüchen | 71 |
| 5.7.1. Testen von Meldepunkten..... | 71 |
| 5.7.2. Test der Kommunikation zwischen TILLYS und TACTILLYS-IP CUBE | 71 |
| 6. Sicherheitsmanagement durch den Sicherheitsbeauftragten | 72 |
| 6.1. Zuweisung von Zugriffsrechten an Benutzer des TACTILLYS-IP CUBE | 72 |
| 6.2. Änderung des ID-Mittels für Einbruch, das bei der Ausweis- und Code- Identifikation auf TACTILLYS-IP CUBE verwendet wird. | 72 |
| 6.3. Abfrage des Verlaufs von Einbrüchen | 72 |
| 7. Schritte im Zusammenhang mit dem Einbruch, die von der Fernüberwachungsleitstelle durchgeführt werden | 73 |
| 7.1. Abfrage der aktuellen Alarme | 73 |
| 7.1.1. Syntax von Polling-Nachrichten | 73 |
| 7.1.2. Syntax der Nachrichten zum zyklischen Test | 73 |
| 7.2. Fernbefehl bei CUBE Einbruch | 74 |
| 7.2.1. Scharfstellung | 74 |
| 7.2.2. Sirenenstopp | 74 |
| 7.2.3. Unscharfschaltung..... | 74 |
| 7.2.4. Änderung des Wertes eines Registers der TILLYS | 74 |

Abbildungsverzeichnis

| | |
|---|----|
| 1.1. Hardware-Architektur der Basisversion von CUBE Einbruch (10010-001) | 18 |
| 1.2. Hardware-Architektur der Multi-TILLYS-Version von CUBE Einbruch (10010-002) | 19 |
| 1.3. Multi-TILLYS-Konfiguration von CUBE Einbruch (10010-003) | 20 |
| 3.1. Einrichten von CUBE Einbruch über Ethernet (10010-004) | 35 |
| 3.2. Position der Navigationsregisterkarten auf dem Konfigurationsbildschirm für CUBE Einbruch der TILLYS (10010-005) | 36 |
| 3.3. Eingeben des Tokens des Host-TILLYS auf einem Gerät-TILLYS (10010-010) | 41 |
| 4.1. Startseite des TACTILLYS-IP (10010-028) | 58 |
| 4.2. Startseite des TACTILLYS-IP CUBE (10010-029) | 59 |
| 5.1. Vorbereiten des Imports der Einbruch-Konfiguration einer TILLYS in MICROSESAME (10010-038) | 67 |

Tabellenverzeichnis

| | |
|---|----|
| 1.1. Geltende Standards für IT-sicherheit | 21 |
| 1.2. Liste der Schritte zur Bewältigung von Einbrüchen mit ihrem Kontext und Modus | 22 |
| 1.3. Vollständige Liste der von den Meldepunkte gesendeten Einbruch-Codes | 24 |
| 1.4. Bedeutung der von den Meldepunkte gesendeten Einbruch-Codes | 24 |
| 1.5. Bedeutung der von den Gruppen gesendeten Ereigniscodes | 27 |
| 1.6. Liste der Fernsteuerungen, die von Fernüberwachungsstelle an die TILLYS gesendet werden können | 27 |
| 1.7. Mögliche Werte des numerischen Registers für den Gruppenstatus | 28 |
| 4.1. Bedeutung der Piktogramme auf dem Bildschirm der Gruppenliste auf dem Bedienteil TACTILLYS-IP CUBE | 62 |
| 4.2. Bedeutung der Piktogramme der Meldepunkte auf dem Terminal TACTILLYS-IP CUBE | 62 |
| 4.3. Bedeutung der Sirenenpiktogramme auf dem Terminal TACTILLYS-IP CUBE | 63 |
| 4.4. Bedeutung der Piktogramme für das Maskieren eines Meldepunktes am TACTILLYS-IP CUBE | 63 |

Vorwort

1. Benötigte Komponenten

Netzwerk für Zutrittskontrolle und Einbruchüberwachung basierend auf [TILLYS TILLYS24-CUBE](#).

Bedienteil bestehend aus einem Einbruchsterminal TACTILLYS-IP CUBE **CDA00TY2025-BBIP** mit Lesegerät **LEC05XF0200-NB6**.

2. Software-Version

Diese Anleitung, **datiert vom¹ August 2024**, beschreibt, wie Sie die CUBE Einbruchserkennung für die MICROSESAME **Softwareversion 2024.2** installieren, konfigurieren und in Betrieb nehmen.

Firmware der TILLYS CUBE **ab 7.0.0**.

Firmware des TACTILLYS-IP **ab 7.0.0**.

3. Voraussetzungen zur Verwendung dieses Handbuchs

Der IT-Verantwortliche am Standort des Kunden wurde vorab informiert und führte die notwendigen Maßnahmen zur Sicherstellung des korrekten Datenaustauschs über IP durch.

Der Sicherheitsbeauftragte hat seine Spezifikationswünsche an den TIL TECHNOLOGIES-Partner oder -Errichter weitergeleitet.

Der TIL TECHNOLOGIES Partner oder Errichter konfiguriert die TILLYS gemäß der Spezifikation in seinen Räumlichkeiten und kopiert diese Konfiguration auf einen USB-Stick. Am Standort des Kunden lädt er diese Konfigurationen auf die TILLYS, dann schließt er über MICROSESAME die TACTILLYS-IP CUBE-Bedienteile an, konfiguriert sie und führt einen Anlagentest durch.

Der Kunde nutzt die Funktionen des TACTILLYS-IP CUBE-Bedienteils zur Scharf-/Unscharfschaltung der Überwachungsbereiche und die Einbruchfunktionen werden an den Fernüberwachungsmonitor weitergeleitet.

Die Fernüberwachungsleitstelle verwaltet die Alarmer aus der Ferne über ein eigenes Terminal.

4. Siehe auch

- [Video zur Vorstellung des CUBE Einbruchmelders](#).
- [Technisches Datenblatt zum TACTILLYS-IP CUBE Einbruch-Terminal](#).
- [Schnellstartanleitung \(GD-10001-DE\)](#).

5. Eigentumsvorbehalt

Die Informationen in diesem Dokument können ohne Vorankündigung geändert werden.

TIL TECHNOLOGIES kann nicht für die in diesem Dokument beispielhaft angegebenen Informationen verantwortlich gemacht werden. Die in den Beispielen verwendeten Organisationen, Namen und Daten sind fiktiv, sofern nicht anders angegeben.

Alle genannten Warenzeichen sind eingetragene Warenzeichen ihrer jeweiligen Eigentümer.

Kein Teil dieses Dokuments darf ohne ausdrückliche Genehmigung von TIL TECHNOLOGIES in irgendeiner Form oder mit irgendwelchen Mitteln verändert, vervielfältigt oder übertragen werden.

Senden Sie Ihre Kommentare, Korrekturen und Anregungen zu diesem Handbuch an documentation@til-technologies.fr.

6. Glossar

Die in diesem Handbuch verwendeten Fachbegriffe werden im Folgenden erläutert.

| | |
|-------------------|---|
| Alarm | <p>Eigenschaft, die ein abnormales Ereignis (Einbruch, technischer Defekt, TZLO usw.) meldet.</p> <p>Der Anlagenzustand wird rund um die Uhr überwacht und geht in den Alarmzustand über, sobald er in die aktive Stufe wechselt.</p> <p>Eine Melderinformation vom Typ Einbruchalarm wird überwacht, wenn der zugehörige Bereich scharfgeschaltet ist. Der Übergang in den Alarm wird daher nicht nur durch den Übergang in den aktiven Zustand bestimmt, sondern auch durch den Überwachungsstatus der Meldergruppe.</p> |
| Maskieren | <p>Maßnahme, um einen oder mehrere Meldepunkte, die sich im Fehlerzustand befinden, von der Überwachung auszuschließen, damit ein Bereich trotzdem überwacht werden kann oder um das Auslösen von Alarmen zu verhindern. Es können verschiedene Arten des Maskierens eingestellt werden: manuell, automatisch mit oder ohne automatische Rückführung oder dauerhaft.</p> |
| Authentifizierung | <ol style="list-style-type: none">1. Im Allgemeinen besteht die Authentifizierung in der Eingabe von ID-Mitteln (Login / Passwort) für den Zugang zu einem Gerät wie die TILLYS, zu einer Anwendung wie CHECKPOINT für die Nutzung des Terminals MOBILIS 3 oder auch zu einem Teil oder der Gesamtheit einer Software wie bei MICROSESAME oder KSM.2. In den Codierungseinstellungen von MICROSESAME ist Authentifizierung ein Vorgang, bei dem überprüft wird, ob der Benutzer berechtigt ist, eine oder mehrere Aktionen mit seinem Ausweis durchzuführen (auf eine oder mehrere Informationen |

| | |
|----------------|---|
| | zugreifen, Daten schreiben, Anwendungen oder Dateien erstellen oder löschen ...). |
| DHCP | <p>Englisches Akronym für "Dynamic Host Configuration Protocol" (Protokoll zur dynamischen Host-Konfiguration).</p> <p>Ein Netzwerkprotokoll, dessen Aufgabe es ist, die IP-Parameter eines Netzwerkgeräts (PC, Server-Arbeitsplatz, Client-Arbeitsplatz ... automatisch zu konfigurieren, indem ihm eine IP-Adresse, eine Subnetzmaske und ein Gateway zugewiesen werden.</p> |
| DTMF | <p>Englisches Akronym für Dual-Tone Multi-Frequency (SF für Stimmfrequenz auf Deutsch).</p> <p>Diese Technologie ermöglicht es, aus der Ferne mit einem Sprachserver zu kommunizieren und von einem Überwachungszentrum aus Befehle zu senden, die das Ansprechen aus der Ferne erlauben und/oder Abhörmikrofone aktivieren.</p> |
| Einbruchprofil | <p>Eine Gruppe von Meldepunkten, auf die ein Operator Einbruch einwirken kann. Dieses Profil besteht aus bis zu drei Listen von Meldergruppen oder Melderinformationen: eine Basisgruppe, die die Scharf-/Unscharfschaltung eines definierten Satzes von Gruppen ermöglicht, und zwei (Teil-)Untergruppen, die die teilweise Scharf-/Unscharfschaltung der Anlage ermöglichen.</p> |
| Empfänger | <p>Bezeichnet beim Einbruchmanagement die Entität, die für den Empfang von Alarmen ausgewählt wurde - in der Regel eine Überwachungsleitstelle (NSL).</p> |
| Gateway | <p>Kommunikations-Gateway: optionale Lizenz, die erworben werden kann, um den MICROSESAME-Server mit Systemen Dritter zu verbinden (LDAP-Server, biometrisches System MORPHO MANAGER ...).</p> <p>Import- oder Export-Gateway: optionale Lizenzen, die die Nutzung von CSV-Dateien zum Abrufen (Importieren) oder Bereitstellen (Exportieren) einer Reihe von Informationen im Zusammenhang mit den Benutzer-IDs des Standorts nutzen.</p> <p>Netzwerk-Gateway: Netzwerkgerät, das IP-Pakete zwischen mehreren Geräten weiterleitet. Meistens handelt es sich dabei um einen Router.</p> |
| ID-Mittel | <p>Element, das den Zutritt eines Benutzers ermöglicht. ID-Mittel können verschiedene Technologien (Schlüsselanhänger, Karte,</p> |

| | |
|-------------------------|---|
| | <p>Nummernschild, Fingerabdruck, numerischer Code ... und verschiedene Lesegeräte zum Auslesen verwenden.</p> |
| IP | <p>Englisches Akronym für Internet Protokoll.</p> <p>Das Internetprotokoll ermöglicht es den Geräten, die es verwenden, über TCP- oder UDP-Pakete miteinander zu kommunizieren.</p> <p>Das IP-Protokoll wird über drahtgebundene lokale Netzwerke transportiert, die das Ethernet-Verbindungsprotokoll verwenden. Netzwerkkarten oder Schnittstellen mit RJ45-Anschlüssen haben physischen Zutritt und werden logisch über ihre IP-Adresse identifiziert.</p> |
| Codierungstabelle | <p>Eine Codierungstabelle ist eine Tabelle, in der wir für jede Art von Alarm (Einbruch, Brand etc.) einen Ereigniscode definieren werden, der an die Überwachungsleitstelle gesendet wird. Diese Codes sind daher mit dem gewählten Fernüberwachungsdienstleister abzustimmen.</p> |
| Kommunikationsprotokoll | <p>Ein Satz von Regeln und Konventionen, der die Kommunikation und Interoperabilität zwischen verschiedenen Computersystemen ermöglicht.</p> <p>Das Protokoll definiert die Struktur der an den Empfänger gesandten Nachricht.</p> |
| Lesegerät | <p>Ausrüstung, die zur Erkennung eines ID-Mittels in einem System zur Zutrittskontrolle verwendet wird. Das ID-Mittel kann verschiedene Formen annehmen: Ausweis, Tastaturcode, biometrischer Fingerabdruck, Nummernschild... Je nach Technologie kann ein Lesegerät verwendet werden, um beispielsweise die</p> <ul style="list-style-type: none">● Sicherstellung der einfachen Erkennung des Trägers des ID-Mittels, z. B. ein Lesegerät vom Typ "transparent", das sich darauf beschränkt, das Vorhandensein eines Ausweises zu erkennen. |

- Zusätzlich das Lesen eines Standard ID-Mittels sicherstellen, z. B. ein "einfaches" Lesegerät, das nur die Seriennummer eines Ausweises lesen kann (*CSN-ID*).
- Zusätzlich die Funktion des Entschlüsselns einer sicheren ID-Mittel gewährleisten, die in einem Ausweis codiert ist, z. B. ein sicheres Lesegerät, in dem der Schlüssel für die Ausweise gespeichert wird.

LVE

Akronym für Lokale Verarbeitungseinheit.

IP-basierte Speicherprogrammierbare Steuerung, die in den Bereichen Zutrittskontrolle, Einbruch und Gebäudeautomatisierung eingesetzt wird. Diese Steuerung verwaltet z. B. den Zutritt von Usern, Informationen von Lesegeräten oder Einbruchschutzsystemen usw. Die LVE von TIL TECHNOLOGIES heißt [TILLYS](#).

Manuelles Maskieren

Eine Maßnahme, mit der ein Benutzer die Überwachung trotz eines Fehlerzustands bei einem oder mehreren Meldepunkten erlaubt.

Meldepunkt

Physischer Meldepunkt: ein Gerät, dessen Aufgabe es ist, einen Einbruch in einem Bereich zu erkennen, und das verschiedene Arten von Sensoren verwendet: Magnetkontakt, Infrarotsensor, Mikrowellensensor... Ein Meldepunkt ist mit zwei Kontakten ausgestattet, die jeweils eine Information liefern: einen Alarmkontakt (*AL-Kontakt* , der eine Erfassungsinformation nennt) und einen Sabotageschutzkontakt (*AP-Kontakt*, der eine Information über das Öffnen oder Herausziehen des Sensors liefert). Bei TIL kann ein physischer Meldepunkt nur zu einer einzigen [Meldergruppe](#) gehören.

Virtueller Meldepunkt: ein logischer Meldepunkt, der mithilfe von TILLYS-internen Registern definiert wird. In einer Installationskonfiguration, in der ein physischer Meldepunkt zu zwei Meldergruppen gehören soll, wird seine Funktion mit der eines virtuellen Melderpunktes verknüpft (z. B. durch microcode). Der physische Meldepunkt wird dann in einer der Gruppen gemeldet und der dazugehörige virtuelle Meldepunkt in der anderen Gruppe.

Meldergruppe

Eine Gruppe von Meldepunkten, die innerhalb desselben Gebäudes, derselben Etage, Abteilung oder Sonstigem durch eine operative logische Verknüpfung verbunden sind und einen gemeinsamen

Modus für :

- das Ein- und Ausschalten der Überwachung,

- das Senden von Alarm-Codes an eine Fernüberwachungsleitstelle
- die Verwaltung einer oder mehrerer Sirenen,
- die Implementierung von Voralarmen oder Überschreibungsmechanismen.

Pro Einbruchfunktion können bis zu 32 Gruppen deklariert werden.

| | |
|-------------------|--|
| Melderinformation | Informationen vom Schlatkontakt, die von einem physischen Meldepunkt (Radar, Türkontakt, Sabotageschutzkontakt ...) oder einem virtuellen Register (internes Register der TILLYS) stammen. |
| microcode | Eine spezielle Programmiersprache, die von TILLYS ausgeführt wird, um die Funktionsweise angesichts von Ereignissen zu definieren, die von allen Geräten, mit denen sie verbunden ist, übermittelt werden. |
| MICROSESAME | Software zur einheitlichen Überwachung, mit der alle elektronischen Informationen des Gebäudes zentralisiert werden können: Zutrittskontrolle, Einbruchserkennung, technische Verwaltung, Video, Gegensprechanlage... Die Steuerung der verschiedenen Funktionen über eine gemeinsame Grafikschnittstelle macht deren Bedienung deutlich einfacher und die Eingriffe effizienter. Da die Interaktionen zwischen den verschiedenen Systemen vollständig automatisiert werden können (Aktionen auf Ereignisse), ist auch die Verarbeitungsgeschwindigkeit gewährleistet. |
| POE | Englisches Akronym für Power Over Ethernet. Netzwerkfunktionalität zur Bereitstellung von Strom über das Ethernet-Kabel. |
| Polling | Polling ist eine Funktion, die bei der Verwendung einer IP-Kommunikation genutzt wird. Sie ermöglicht es der Fernüberwachungsleitstell, die IP-Übertragungsfunktion abzufragen, um sicherzustellen, dass die Verbindung zwischen beiden Geräten funktioniert. |
| Port | Einstiegspunkt zu einem Dienst (Web-Dienst, DNS-Dienst, Mail-Dienst...) auf einem Gerät (PC, Server...), das mit einem Netzwerk verbunden ist. Ports ermöglichen es, dass verschiedene Software und/oder Betriebssysteme miteinander kommunizieren können. |
| RS 485 | In der Industrie verwendeter Kommunikationsstandard. Seine Umsetzung durch TIL TECHNOLOGIES ermöglicht es, Hardware |

| | |
|----------------------|--|
| | <p>in Bus- und/oder Sternform bis zu einer Entfernung von 600 Metern mit der TILLYS zu verbinden.</p> |
| Sirenenfunktion | <p>TILLYS-interne Funktion, die mit der Einbruchsfunktion verbunden ist. Ihre Einstellungen wirken sich auf die verschiedenen Arten von Klingeltönen aus, die bei Ereignissen erzeugt werden, auf das Verhalten der Haupt- und Zusatzsirenenfunktion und deren Auslöseart sowie auf die Zuweisung der entsprechenden Meldergruppen.</p> |
| Sperrung | <p>Bezeichnet den deaktivierten Zustand eines Teils eines Einbruchschutzsystems, in dem das Auftreten einer Einbruch- oder Überfallalarmbedingung nicht an die Notrufzentrale gemeldet werden kann; dies gilt bis zur manuellen Aufhebung.</p> |
| TACTILLYS | <p>TIL TECHNOLOGIES Tastatur, die dem Einbruch-Management gewidmet und mit einem 7-Zoll-Farbbildschirm ausgestattet ist. Es ermöglicht einem Einbruch-Operator, sich zu authentifizieren, um auf bestimmte Aktionen zuzugreifen, die in der Einbruchsfunktion parametrisiert sind. Sie kann mit einem Lesegerät für Ausweise ausgestattet sein, das den einzugebenden Code ersetzt oder im Gegenteil die notwendige Authentifizierung eines Einbruchmanagement-Operator verstärkt (Vorhalten eines Ausweises + Eingabe eines Codes).</p> |
| Tastaturfunktion | <p>TILLYS-interne Funktion, die mit der Einbruchsfunktion verbunden ist. Ihre Parametrierung wirkt sich auf die Verwaltung der betroffenen Meldergruppen und die Verwaltung des internen Summers der verschiedenen definierten Tastaturen aus.</p> |
| TILLYS | <p>Von TIL TECHNOLOGIES entwickelte IP speicherprogrammierbare Steuerung, die über Funktionen für Zutrittskontrolle, Einbruchserkennung und Gebäudeleittechnik verfügt. Über 3 RS 485-Busse (A, B und C) ermöglicht jeder TILLYS den Anschluss von 8, 16 oder 24 Lesegeräten für die Zutrittskontrolle. Sie ist auch eine echte Einbruchmeldezentrale. Siehe auch LVE.</p> |
| Übertragungsfunktion | <p>TILLYS-interne Funktion, die mit der Einbruchsfunktion verbunden ist. Die TILLYS Einstellung wirkt sich auf die der Fernüberwachungsleitstelle (die als "Empfänger" bezeichnet werden und maximal 4 sein dürfen), die genutzten Protokolle, die zu übertragenden Codes und die gewünschten Anrufprofile (gleichzeitige Anrufe oder Backups) aus. Die Übertragungsfunktion ermöglicht es außerdem, bis zu 32 Fernsteuerungen pro Einbruchsfunktion zu definieren, mit denen Operators der Fernüberwachung je nach zugewiesenem</p> |

| | |
|-----------------------------|---|
| | <p>Niveau (2, 9 oder 32 Fernsteuerungen) Fernaktionen am Standort durchführen können.</p> |
| User | <p>Person, die über einen Zutritt zum Standort verfügen muss, der durch das System der Zutrittskontrolle geschützt ist.</p> <p>Ein User kann über eine oder mehrere mehrere ID-Mittel verfügen. Die User können sein:</p> <ul style="list-style-type: none">● Personen, die ständig am Standort arbeiten (User vom Typ "Daueruser"),● Personen, die außerhalb des Standorts tätig sind (User mit einer bestimmten Gültigkeitsdauer, die der Dauer ihrer Tätigkeit entspricht),● Personen, die nur vorübergehend Zutritt zum Standort haben (User vom "Besucher"-Typ). |
| Verbindungsmodus | <p>Einstellung des Modus auf dem MOBILIS-Terminal 3. Dieser kann entweder im Modus "Offline" betrieben werden, dann arbeitet er nach dem Importieren der Datenbank mit den ID-Mitteln vom MICROSESAME-Server im Standalone-Modus, oder im "Online"-Modus, dann ist er über eine WLAN-Verbindung mit dem MICROSESAME-Server verbunden.</p> |
| Vereinfachte Inbetriebnahme | <p>Bei Einbruch wird die Inbetriebnahme standardmäßig vorgeschlagen, wenn sich ein Benutzer an einer Einbruchstatur anmeldet. Das vereinfachte Update zeigt drei verschiedene Meldergruppen an: Die erste enthält alle in der Einbruchfunktion definierten Gruppen, die zweite und dritte sind die sogenannten "Teilgruppen", die die gleichzeitige Inbetriebnahme von vorgewählten Gruppen ermöglichen.</p> |
| Voralarm | <p>Bei der Einbruchfunktion definiert der Voralarm die Verzögerung zwischen einer Aufforderung zur Inbetriebnahme und dem tatsächlichen Start der Überwachung. Der Einsatz des Voralarms wird häufig implementiert, um mit Überschreibungen umgehen zu können. Der Voralarm erzeugt einen speziellen Klingelton, sobald er ausgelöst wird, und warnt potenzielle Bewohner vor der bevorstehenden Bereichsüberwachung, wobei ihnen die Möglichkeit gegeben wird, eine Überschreibung vorzunehmen.</p> |
| WEBSesame | <p>Web-Anwendung der MICROSESAME-Software. Sie ermöglicht die Nutzung eines Großteils der Funktionen von MICROSESAME mithilfe eines einfachen Internetbrowsers (Edge, Chrome, Firefox, Safari...). Man spricht in diesem Fall von einem "leichten Client-Arbeitsplatz".</p> |

Zyklischer Test

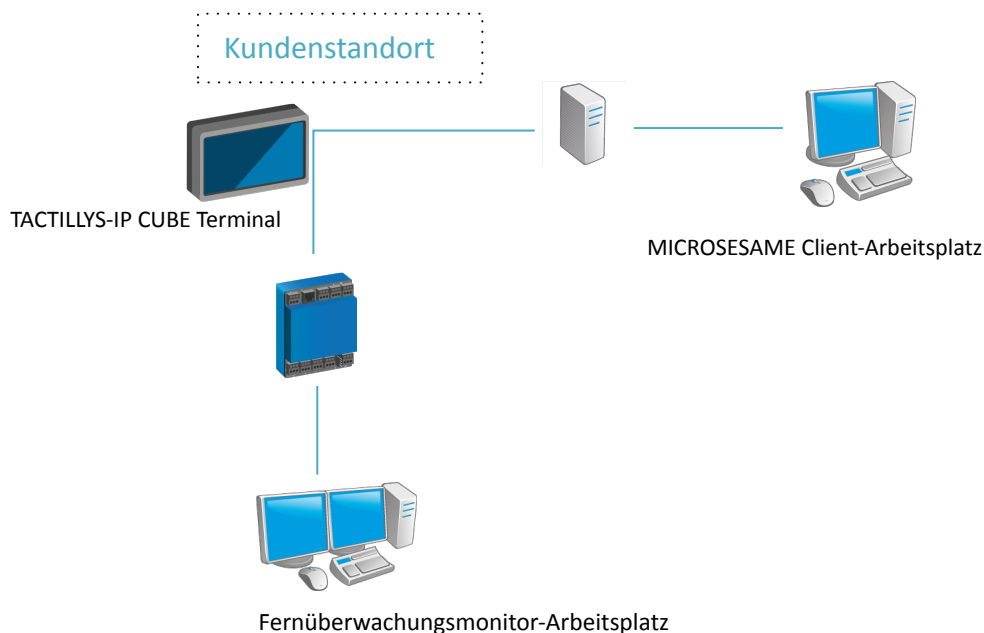
Regelmäßiger Vorgang, der von der TILLYS durchgeführt wird und darin besteht, eine Übertragungsfunktion an einen Empfänger durchzuführen, um die Funktion der Kommunikationseitung zu überprüfen. Seine Periodizität ist einstellbar. Die Übertragung des zyklischen Tests kann zeitgesteuert oder zeitunabhängig sein oder an die Inbetriebnahme einer oder mehrerer Gruppen gekoppelt werden. Es ist möglich, einen zyklischen Test pro Empfänger einzustellen.

Kapitel 1. Hintergrund zur Einbrucherkennung

1.1. Überblick über die Basisversion von CUBE Einbruch

Die Hardware-Architektur ist von der Art, wie sie im folgenden Diagramm dargestellt ist.

Abbildung 1.1. Hardware-Architektur der Basisversion von CUBE Einbruch (10010-001)



Die TILLYS, mit der das Bedienteil ACTILLYS-IP CUBE verbunden ist, verwaltet die Meldergruppe. Ihre Meldepunkte und Sirenen werden verwaltet:

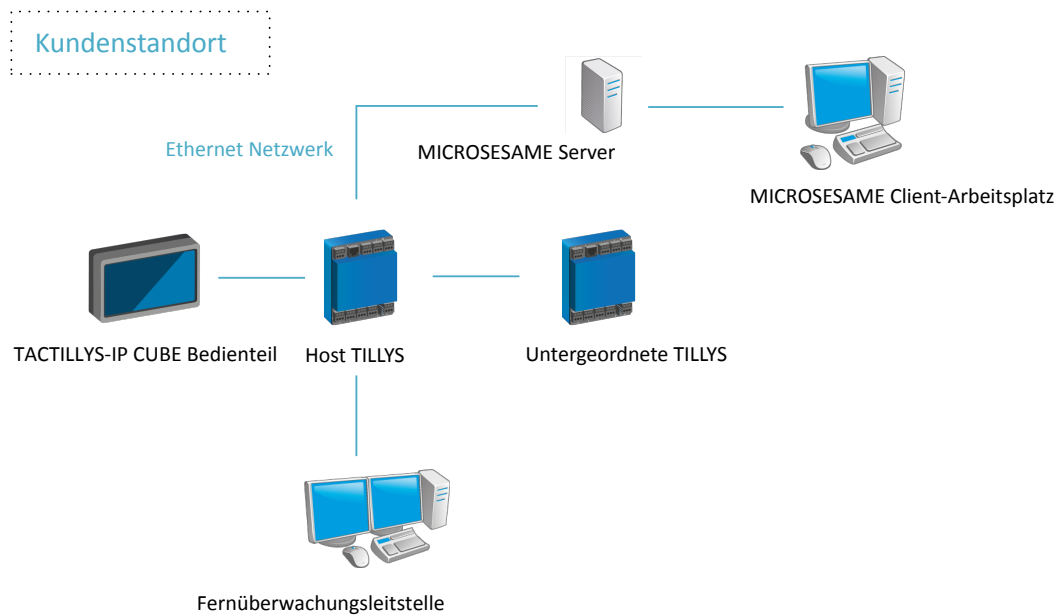
- am Bedienteil TACTILLYS-IP CUBE,
- am Client-Arbeitsplatz MICROSESAME,
- von Fernüberwachungsleitstelle aus.

1.2. Überblick über die Multi-TILLYS-Variante von CUBE Einbruch

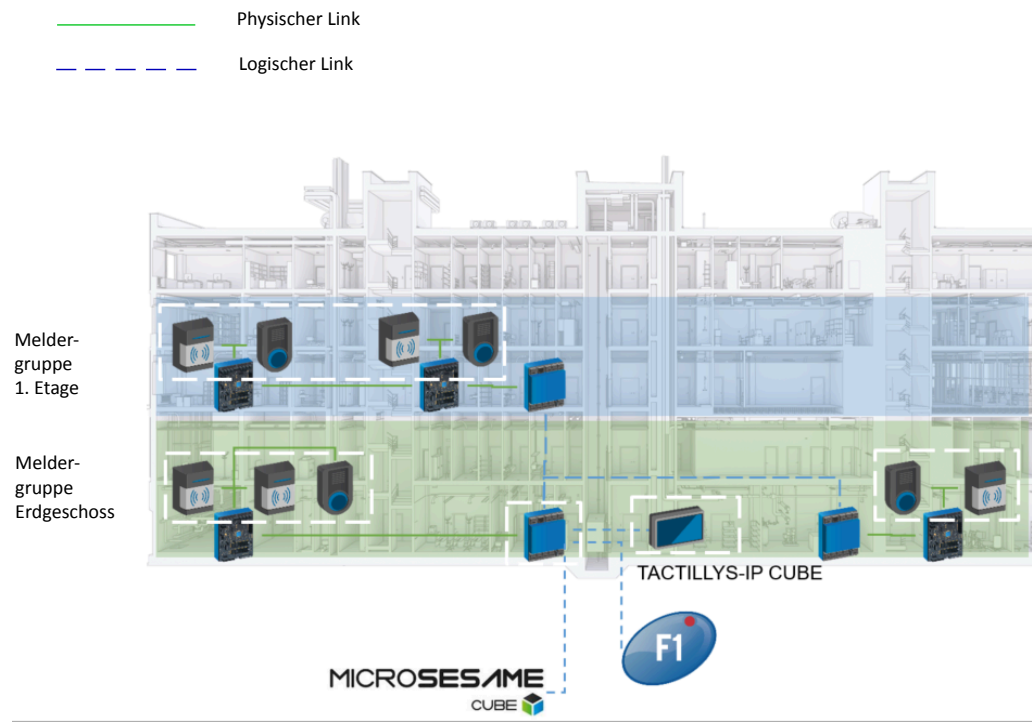
Wenn es notwendig ist, Melder und Sirenen auf mehrere TILLYS zu verteilen, ist dies nun möglich, indem ein Host-TILLYS und ein oder mehrere untergeordnete TILLYS verwendet werden, die über IP in einem Ethernet-Netzwerk verbunden sind.

Die Meldepunkte und Sirenen der untergeordneten TILLYS sind dann virtuell mit der Meldergruppe des Host-TILLYS verbunden, der sie so verwaltet, als wären sie physisch mit ihm verbunden.

Abbildung 1.2. Hardware-Architektur der Multi-TILLYS-Version des CUBE Einbruchs (10010-002)



Die folgende Abbildung zeigt die physischen Verbindungen zwischen den Meldepunkte und den TILLYS in einem Gebäude sowie die logischen Verbindungen über IP. Diese ermöglichen es, virtuelle Meldepunkte und Sirenen auf dem TILLYS-Host zu deklarieren sowie mit MICROSESAME und mit Fernüberwachungssystemen zu kommunizieren.

Abbildung 1.3. Multi-TILLYS-Konfiguration von CUBE Einbruch (10010-003)

1.3. Neuheiten und Vorteile von CUBE Einbruch

Die CUBE Einbruch-Lösung bietet vier wichtige Neuerungen im Vergleich zur vorherigen Version:

- Die Verwendung von IP anstelle des RS 485-Busses zwischen dem Terminal TACTILLYS-IP CUBE und der TILLYS.
- Die Konfiguration wird an der TILLYS vorgenommen, bevor die Informationen in MICROSESAME hochgeladen werden.
- Die Logik Normal zu ist bei Meldern weit verbreitet.
- Die Inbetriebnahme ist ohne Eingabe einer microcode-befehlzeile möglich.

In funktionaler Hinsicht bietet der CUBE Einbruch vier entscheidende qualitative Vorteile gegenüber dem Marktangebot:

- Eine Cybersicherheit auf demselben Niveau wie die Zutrittskontrolle, die eine BSI anerkannte ANSSI Zertifizierung besitzt.
- Integration der Überwachung durch die Verwendung von Meldeobjekten, Meldergruppen und Sirenen.
- Verbesserte ergonomische Nutzung durch native Überwachungsobjekte und Widgets, die in MICROSESAME animiert werden.
- Mehr Leistung bei den Fernüberwachungsfunktionen durch IP-Terminals für mehrere Zentralen und die Nutzung der **SIA-Übertragung**.

1.4. Definition der erwarteten Funktion durch Sicherheitsbeauftragten

Der Sicherheitsbeauftragte legt die erwartete Funktionsweise fest, in einem **Lastenheft** oder einer **Funktionsbeschreibung**.

Dieses Dokument und der **Netzwerk-Adressierungsplan** ermöglichen es dem TIL TECHNOLOGIES-Partner, die Bereiche der Zutrittskontrolle und die Überwachungsbereiche in seinen Räumlichkeiten zu definieren, bevor er sie am Standort seines Kunden einsetzt.

1.5. CUBE Einbruch-Voraussetzungen, die vom Kunden zu implementieren sind

Da die Übertragung der Einbruch-Daten über ein IP-Netzwerk erfolgt, gelten die folgenden Standards.

Tabelle 1.1. Geltende Standards für Computersicherheit

| Titel des Standards | Verweis und Link |
|--|-----------------------------|
| SIA Digital Communication Standard - Internet Protocol Event reporting | [SIA-DC-09] |
| Security Communications - Digital Communications Standard - "SIA Format" Protokoll - for Alarm System Communications (Kommunikation über Alarmsysteme) | [SIA-DC-03] |
| SIA Digital Communications Standard - Receiver-to-Computer Schnittstelle Protocol - for Central Station Equipment Communications (Standard für die Kommunikation zwischen Receivern und Computern) | [SIA-DC-07] |

1.6. Systemmanagement

Dieser Abschnitt enthält eine große Tabelle mit möglichen Schritten, die vom Status des Einbruchschutzsystems abhängen.

Tabelle 1.2. Liste der Schritte zur Bewältigung von Einbrüchen mit ihrem Kontext und Modus

| Alarm-Status | Was und wie? | Warum? | Wo und von wem? |
|---------------------|--|--|--|
| Vor Scharfschaltung | Einrichten von Gruppen Zutrittsverzug Austrittsverzug Automatisch maskieren Automatische Wiedereinführung Dauerhaft maskieren | Bestimmen, was auf der Ebene des Managements von Einbrüchen getan werden kann und wer berechtigt ist, diese Schritte durchzuführen. | an TILLYS-Host (Sicherheitsbeauftragter) |
| In Voralarm | Überschreiben einer Meldergruppe | Erlaubt einem oder mehreren Mitarbeitern, nach der Endzeit in einem bestimmten Bereich für eine aus einer Liste von Werten auszuwählende Dauer weiterzuarbeiten. Maskiert eine fehlerhaften Gruppe. | an TACTILLYS-IP CUBE Bedienteil (Benutzer mit Einbruchrechten) |
| Davon abweichend | Alarm scharfschalten | Beenden der Überschreibung und Alarmscharfschaltung | an TACTILLYS-IP CUBE Bedienteil (Benutzer mit Einbruchrechten) |
| In Voralarm | Manuelles Maskieren eines fehlerhaften Melders | Erzwingt Scharfschaltung der Gruppe. Vermeidet Alarmauslösung beim Verlassen des Gebäudes vor Ablauf | TACTILLYS-IP CUBE Bedienteil (Benutzer mit Einbruchrechten) |

| Alarm-Status | Was und wie? | Warum? | Wo und von wem? |
|----------------|--|---|---|
| | | des Austrittsverzugs. | |
| Bei Austritt | Zügiges Verlassen der Räumlichkeiten | Vermeidet es, den Alarm durch Verlassen des Gebäudes vor Ablauf des Austrittsverzugs auszulösen. | TACTILLYS-IP CUBE Bedienteil (Benutzer mit Einbruchrechten) |
| Alarm scharf | Ausweis an der Tür | Erreichen des Bedienteils TACTILLYS-IP CUBE währd. Zutrittsverzuges | Lesegerät für Zutrittskontrolle (Benutzer mit Einbruchrechten) |
| Bei Zutritt | Ausweis am TACTILLYS-IP CUBE und Alarm unscharf schalten | Betreten der Räumlichkeiten außerhalb der Arbeitszeiten | TACTILLYS-IP CUBE Bedienteil (Benutzer mit Einbruchrechten) |
| Alarm unscharf | Ausweis, um Gebäude zu betreten Ändern bestimmter Einstellungen | Zugang zu den Räumlichkeiten während der Arbeitszeit Konfiguration zum Schutz vor Einbrüchen an die Bedürfnisse anpassen | Lesegeräte für die Zutrittskontrolle TILLYS Host (Sicherheitsbeauftragter) |

1.7. Hintergrundinformationen für Errichter

1.7.1. Formate der zwischen der TILLYS und der Fernüberwachungsleitstelle ausgetauschten Frames

Dieser Teil mit seinen drei Abschnitten liefert **Errichtern** eine Referenzdokumentation aus den Normen **SIA DC-09 und SIA DC-03** sowie Beispiele für ihre Umsetzung durch TIL TECHNOLOGIES.

Die TILLYS überträgt Frames im **SIA-Format DC-09**, die Daten im SIA-Format DC-03 weiterleitet.

Da dieses Format interpretierbar ist, werden die SIA DC-03-Codes, die von der TILLYS an die Fernüberwachungsleitstelle übertragen werden, sowie die Fernsteuerungen, die von den Fernüberwachungssystemen an die TILLYS gesendet werden, in den folgenden drei Abschnitten detailliert beschrieben.

1.7.1.1. Von Meldepunkten an die Fernüberwachungsleitstelle gesendete Einbruch-Codes

Damit Einbruch-Codes für einen Meldepunkt **übertragen** werden, muss der Schalter **Alarme übertragen** im Abschnitt **Allgemeine Informationen** für diesen Meldepunkt aktiviert sein (siehe [Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“](#)).

Die folgende Tabelle enthält eine Liste der mit den Meldepunkten verknüpften Einbruch-Codes.

Tabelle 1.3. Vollständige Liste der von den Meldepunkten gesendeten Einbruch-Codes

| Art des Signals | Erscheinen des Alarms | Verschwinden des Alarms | Sperrung | Entsperrung | Maskieren | Wiedereins. |
|------------------------|-----------------------|-------------------------|----------|-------------|-----------|-------------|
| Einbruch | BA | BR | BB | BU | XW | BU |
| 24/24 | TA | TR | TB | TU | VW | TU |
| Lautloser Einbruch | BA | BR | BB | BU | XW | BU |
| Systemfehler | IA | IR | UB | UU | XW | UU |
| Lautloser Systemfehler | IA | IR | UB | UU | XW | UU |
| Notfall | QA | QR | QB | QU | XW | QU |
| Brand | FA | FR | FB | FU | XW | FU |

Die folgende Tabelle gibt die Bedeutung dieser Codes zunächst in englischer und dann in deutscher Sprache wieder.

Tabelle 1.4. Bedeutung der von den Meldepunkten gesendeten Einbruch-Codes

| Tastaturcode | Englisch | Deutsch | Details |
|--------------|-------------------|------------------------------|--|
| BA | Burglary alarm | Einbruch bei scharfer EMA | Einbruch oder stilles Eindringen in einen scharfgeschalteten einbruchhemmenden Bereich |
| BR | Burglary Restoral | Alarmzustand beseitigt | Verschwinden des Alarm- oder Fehlerzustands |
| BB | Burglary Bypass | Überwachungsbereich umgangen | Das Signal für Einbruch oder stilles Eindringen in einen Bereich wurde gehemmt. |

| Tastaturcode | Englisch | Deutsch | Details |
|--------------|-----------------------------|--|---|
| BU | Burglary Unbypass | Umgehung des Überwachungsbereichs aufgehoben | Deaktivierung oder Wiedereinführung eines Bereichs für Einbruch oder stilles Eindringen |
| FA | Fire Alarm | Brandalarm | Auftreten eines Alarms vom Typ Brand |
| FR | Fire Restoral | Alarmzustand beseitigt | Verschwinden eines Alarms vom Typ Brand |
| FB | Fire Bypass | Umgehung der Brandüberwachung | Der Brandalarm, der in einem Bereich aufgetreten ist, wurde unterdrückt. |
| FU | Fire Unbypass | Umgehung der Brandüberwachung aufgehoben | Deaktivierung eines Feueralarms in einem Bereich oder Rücksetzung dieses Bereichs |
| IA | Equipment Failure Condition | Systemfehler | Alarm aufgrund eines Systemfehlers oder eines stillen Systemfehlers |
| IR | Equipment Fail - Restoral | Systemfehler beseitigt | Alarm aufgrund eines Systemfehlers oder eines stillen Systemfehlers beseitigt |
| UB | Untyped Range Bypass | Bereich unbekanntem Typs umgangen | Sperrung des Signals vom Typ Systemfehler oder stiller Systemfehler |
| UU | Untyped Range Unbypass | Umgehung entfernt | Sperrung des Signals vom Typ Systemfehler oder stiller Systemfehler deaktiviert |
| QA | Emergency Alarm | Notalarm | Alarm bei Notfallsignal |

| Tastaturcode | Englisch | Deutsch | Details |
|--------------|--------------------|---|---|
| QR | Emergency Restoral | Notalarm-zustand beseitigt | Beseitigung von Alarmen bei Notfallsignalen |
| QB | Emergency Bypass | Bereich umgangen | Sperrung des Notrufsignals in einem Bereich |
| QU | Emergency Unbypass | Umgehung aufgehoben | Sperrung des Notrufsignals in einem Bereich aufgehoben |
| TA | Tamper Alarm | Alarmschutz-kasten geöffnet | Offener Alarmschutzkasten (Alarm erscheint bei 24/24-Signal) |
| TR | Restoral Tamper | Alarmschutz-kasten geschlossen | Geschlossener Alarmschutzkasten (Alarm verschwindet bei 24/24-Signal) |
| TB | Tamper Bypass | Umgehung des Sabotage-Kontaktes | Erkennung des Sabotageschutzes wurde gehemmt (Alarmhemmung bei Signaltyp 24/24). |
| TU | Tamper Unbypass | Umgehung des Sabotage-Kontaktes aufgehoben | Die Umgehung des Sabotageschutzes wurde aufgehoben (Disinhibition oder 24/24-Signalerückführung). |
| XW | Forced Point | Meldepunkt zur gleichen Zeit aus dem System maskiert. | Ein Meldepunkt wurde beim Scharfschalten gewaltsam aus dem System maskiert (Auswurf des Signals, unabhängig von der Art des Signals). |

Der im Adressfeld (address field) übertragene Wert ist der Wert der Signalnummer des Melders.

1.7.1.2. Ereigniscodes von Überwachungsbereichen an die Fernüberwachungsleitstelle

Damit Ereigniscodes für eine Gruppe **übertragen** werden, muss der Schalter **Scharf-/Unscharfschalten übertragen** im Abschnitt **Allgemeine Informationen** für diese Meldergruppe aktiviert sein (siehe [Abschnitt 3.2.1.2, „Einrichten einer Gruppe von CUBE Meldern für den Einbruch“](#)).

Die folgende Tabelle listet und beschreibt die Liste der gruppenbezogenen Ereigniscodes.

Tabelle 1.5. Bedeutung der von den Gruppen gesendeten Ereigniscodes

| Tastaturcode | Englisch | Deutsch | Details |
|--------------|-------------------|---|-------------------------|
| ZK | Automatic Closing | Automatische Scharfschaltung des Systems | Bereich oder Meldepunkt |
| OA | Automatic opening | Automatische Unscharfschaltung des Systems | Bereich oder Meldepunkt |
| CI | Fail to close | Automatische Scharfschaltung fehlgeschlagen | Nummer des Bereichs |
| CE | Closing Extend | Überschreiben, um Scharfschaltung zu verhindern | Nutzernummer |

Der Wert, der im Adressfeld (address field) übertragen wird, ist der der Gruppennummer.

1.7.1.3. Fernsteuerungen von der Fernüberwachungsstelle an die TILLYS

Es können die in der folgenden Tabelle aufgeführten Fernsteuerungen verwendet werden.

Tabelle 1.6. Liste der Fernsteuerungen, die von der Fernüberwachungsleitstelle an TILLYS gesendet werden können

| Tastaturcode | Kurzbeschreibung | Weitere Informationen | Bedeutung |
|--------------|------------------|--|---|
| SA | Set Area | x*y set area x to y, (3 = User Defined, 2 = Perimeter Only, A = Armed, 0 = Disarmed) | Befehl zum Scharf- oder Unscharfschalten eines Bereichs |

| Tastaturcode | Kurzbeschreibung | Weitere Informationen | Bedeutung |
|--------------|------------------|--|--|
| SB | Set Bypass | x*y set bypass on Bereich x to y (1 = ON, 0 = OFF) | Befehl zur Sperrung oder Deaktivierung einer Gruppe |
| SS | Set Sounder | x*y set sounder x to y (1 = ON, 0 = OFF) | Befehl zum Stoppen oder Auslösen einer Sirene |
| TP | Trap Account | Konto, das für die Fernprogrammierung verwendet wird | Befehl zum Ändern des Wertes eines benutzerdefinierten Registers "custom TIL". |

Für jede Fernsteuerung müssen die Gruppennummer für die Scharfschaltung und die damit verbundene Verzögerung beim Scharf- und Unscharfschalten (sofort oder mit Voralarm), die Meldersignalnummer für den Muting-Befehl, die Sirenennummer für die Sirenenabschaltung, das Register und dessen Wert für die Fernsteuerung TP usw. angegeben werden.

1.7.2. Werte des numerischen Registers für den Gruppenstatus bei CUBE Einbruch

Diese Informationen richten sich an **Errichter**.

Das numerische Register für den Status von Gruppen wird durch das Attribut regStatus des group-Tags definiert. Jedes Bit in diesem Register entspricht einer Information gemäß der folgenden Tabelle.

Tabelle 1.7. Mögliche Werte des numerischen Registers für den Gruppenstatus

| Bit-Index | Hexadezimal-Maske | Beschreibung | Kommentar |
|-----------|-------------------|--|--|
| 0 | 0x1 | 1 = mindestens ein Fehler vom Typ "Alarm Einbruch" in der Gruppe 0 = kein Fehler vom Typ "Alarm Einbruch" in der Gruppe | Entspricht dem synthetischen Register Schaltkontakt das für den Typ "Alarm Einbruch" festgelegt werden kann. |
| 1 | 0x2 | 1 = mindestens ein Fehler vom Typ "Alarm 24/24" in der Gruppe 0 = kein Fehler vom Typ "Alarm 24/24" in der Gruppe | Entspricht dem synthetischen Register Schaltkontakt, das für den Typ "Alarm 24/24" festgelegt werden kann. |

| Bit-Index | Hexadezimal-Maske | Beschreibung | Kommentar |
|-----------|-------------------|--|---|
| 2 | 0x4 | 1 = mindestens ein Fehler vom Typ "Stiller Einbruch Alarm" in der Gruppe 0 = kein Fehler vom Typ "Stiller Einbruch Alarm" in der Gruppe | Entspricht dem synthetischen Register Schaltkontakt, das für den Typ "Stiller Einbruch Alarm" festgelegt werden kann. |
| 3 | 0x8 | 1 = mindestens ein Fehler vom Typ "Systemfehler" in der Gruppe 0 = kein Fehler vom Typ "Systemfehler" in der Gruppe | Fehler im Logischen Register Schaltkontakt Synthese, der für den Typ "Systemfehler" festgelegt werden kann. |
| 4 | 0x10 | 1 = mindestens ein Fehler vom Typ "Notruf" in der Gruppe 0 = kein Fehler vom Typ "Systemfehler" in der Gruppe | Entspricht dem synthetischen Register Schaltkontakt, das für den Typ "Notruf" festgelegt werden kann. |
| 5 | 0x20 | 1 = mindestens ein Fehler vom Typ "Systemfehler" in der Gruppe 0 = kein Fehler vom Typ "Systemfehler" in der Gruppe | Entspricht dem zusammenfassenden Register Schaltkontakt, das für den Typ "Brand" festgelegt werden kann. |
| 6 | 0x40 | 1 = mindestens ein Fehler vom Typ "Systemfehler leise" in der Gruppe 0 = kein Fehler des Typs "Leiser Systemfehler" in der Gruppe | Synthetischer Schaltkontakt Register-Ausfall, der für den Typ "Stiller Systemfehler" festgelegt werden kann. |
| 16 | 0x10000 | 1 = Gruppe scharf 0 = Gruppe unscharf | |
| 17 | 0x20000 | 1 = mindestens ein Alarm, der auf eine Quittierung wartet 0 = kein Alarm, der auf eine Quittierung wartet | |
| 18 | 0x40000 | 1 = Voralarm läuft | |

| Bit-Index | Hexadezimal-Maske | Beschreibung | Kommentar |
|-----------|-------------------|-----------------------------------|-----------|
| | | 0 = kein Voralarm im Gange | |
| 19 | 0x80000 | 1 = Abweichung läuft | |
| | | 0 = keine Überschreibung im Gange | |
| 20 | 0x100000 | 1 = Austrittsverzug läuft | |
| | | 0 = kein Austrittsverzug läuft | |
| 21 | 0x200000 | 1 = Zutrittsverzug läuft | |
| | | 0 = kein Zutrittsverzug läuft | |

1.7.3. Register des microcodes, spezifisch für den Einbruch CUBE

Die folgenden Register wurden zur Verwendung in MICROSESAME erstellt (siehe [TILLYS Mikrocode-Programmierhandbuch](#) - GP-100006-DE).

Zur Definition von physischen Meldepunkten werden zwei neue Register verwendet: AL_DETECTEUR_ID und AP_DETECTEUR_ID.

Außerdem wurden zwei Virtuelle Register erstellt: ENTRE_AL_DETECTEUR_ID und ENTRE_AP_DETECTEUR_ID.

Schließlich werden neue Arten von Registern verwendet, um den Auswurf von Meldern zu verwalten: EJ_DETEKTOR_ID.

1.7.4. Befehl für den microcode, spezifisch für TACTILLYS-IP CUBE

Der Befehl GET_AP_TACTILLYS wurde erstellt, um die Informationen über den Sabotageschutz des TACTILLYS-IP CUBE in MICROSESAME zurückzusenden.

Kapitel 2. Workflow bei CUBE Einbruch

Dieses Kapitel bietet Geschäftsprozesse nach Benutzerprofilen (Partner, Installateur oder Startseite-Agent).

Sonstige Kapitel enthalten Anweisungen für :

- an den Sicherheitsbeauftragten (siehe [Kapitel 6, Sicherheitsmanagement durch den Sicherheitsbeauftragten](#)),
- Personen, die zur Benutzung des Terminals TACTILLYS-IP CUBE befähigt sind (siehe [Abschnitt 4.3, „Verwendung des TACTILLYS-IP CUBE“](#)),
- an Entwickler von Fernüberwachungssystemen von Drittanbietern (siehe [Abschnitt 1.7.1, „Formate der zwischen TILLYS und Fernüberwachungsendgeräten ausgetauschten Frames“](#)).

2.1. Vorbereitung der IT-Umgebung

Wenn es sich um die erste Inbetriebnahme handelt, lesen Sie bitte die [Kurzanleitung \(GD-10001-DE\)](#).

2.2. Vorbereitung der CUBE Einbruch-Konfiguration durch den TIL-Partner in seinen Räumlichkeiten

2.2.1. Workflow - Vorkonfiguration CUBE Einbruch durch den Partner in seinen Räumlichkeiten

Die Partnerin führt vor ihrem Besuch beim Kunden in ihren Geschäftsräumen folgende Tätigkeiten aus:

1. Physische Verbindung des Laptops mit dem Ethernet-Netzwerk
2. [Abschnitt 3.2.1.1, „Zutritt zur Schnittstelle für den Administrator des CUBE Einbruchs auf einem TILLYS“](#)
3. [Abschnitt 3.2.1.2, „Einrichten einer Gruppe von CUBE Meldern für den Einbruch“](#)
4. [Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“](#)
5. [Abschnitt 3.2.1.7, „Einrichten einer CUBE Einbruch-Sirene“](#)
6. [Abschnitt 3.2.2.1, „Erstellen von Einbruchprofilen auf der Host-TILLYS“](#)
7. [Abschnitt 3.2.1.10, „Zuordnung eines TACTILLYS-IP CUBE-Terminals zu einer oder mehreren Gruppen einer Host-TILLYS“](#)
8. [Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“](#)
9. Weiter mit den Schritten von [Abschnitt 2.2.2, „Workflow - Exportieren/Importieren der CUBE Einbruch Einstellungen“](#): Exportieren der Konfiguration, die der Partner in seinen Räumlichkeiten erstellt hat, und Importieren dieser Konfiguration auf den Standort des Kunden.

2.2.2. Workflow - Exportieren/Importieren der CUBE Einbruch-Konfiguration

Diese beiden Prozesse ermöglichen :

- eine CUBE Einbruch-Konfiguration im Voraus vorzubereiten,
- eine CUBE Einbruch-Konfiguration zu speichern, um sie auf einen anderen TILLYS zu kopieren,
- eine CUBE Einbruch-Konfiguration auf den Standort eines Kunden zu kopieren,
- die Konfiguration eines TILLYS wiederherzustellen, um eine gespeicherte CUBE Einbruch-Konfiguration wiederherzustellen oder wenn dieser TILLYS ersetzt wird.

Um eine Einbruch-Konfiguration zu exportieren oder zu speichern :

1. [Abschnitt 3.2.4.1, „Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS“](#)
2. [Abschnitt 3.2.4.2, „Exportieren oder Importieren einer CUBE Einbruch-Konfigurationsdatei“](#)

So importieren Sie eine gesicherte Einbruch-Konfiguration oder stellen sie wieder her :

1. [Abschnitt 3.2.4.1, „Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS“](#)
2. [Abschnitt 3.2.4.2, „Exportieren oder Importieren einer CUBE Einbruch-Konfigurationsdatei“](#)
3. Weiter auf dem Standort des Kunden mit dem [Abschnitt 2.3.1, „Workflow - CUBE Einbruch-Konfiguration auf dem Standort des Kunden“](#)

2.3. Konfiguration von CUBE Einbruch durch den TIL-Partner am Standort des Kunden

2.3.1. Workflow - CUBE Einbruch-Konfiguration am Standort des Kunden

Der Partner führt direkt in der Kundschaft die folgenden Operationen durch:

1. Physische Verbindung des Laptops mit dem Ethernet-Netzwerk
2. [Abschnitt 3.2.1.1, „Zutritt zur Schnittstelle für den Administrator des CUBE Einbruchs auf einem TILLYS“](#)
3. [Abschnitt 3.2.1.2, „Einrichten einer Gruppe von CUBE Meldern für den Einbruch“](#)
4. [Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“](#)
5. [Abschnitt 3.2.1.7, „Einrichten einer CUBE Einbruch-Sirene“](#)
6. [Abschnitt 3.2.2.1, „Erstellen von Einbruchsprofilen auf der Host-TILLYS“](#)
7. [Abschnitt 3.2.1.10, „Zuordnung eines TACTILLYS-IP CUBE-Terminals zu einer oder mehreren Gruppen einer Host-TILLYS“](#)
8. [Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“](#)
9. Weiter mit [Abschnitt 2.3.2, „Workflow - Konfigurieren eines Ausweises für den Zutritt zum Terminal TACTILLYS-IP CUBE“](#)

2.3.2. Workflow - Konfigurieren eines Ausweises zum Zugriff auf Bedienteil TACTILLYS-IP CUBE

Die Startseite kann Ausweise für den Zutritt mit Einbruch-Rechten vorbereiten.

1. [Abschnitt 5.2.1, „Vorbereitung eines Ausweises zur Kontrolle gegen Einbrüche“](#)

2. [Section 5.2.2, « Erwerb eines nicht zugewiesenen ID-Mittels in MICROSESAME »](#)
3. [Section 5.2.3, « Zuweisung eines verfügbaren ID-Mittels an einen neuen Benutzer »](#)
4. [Section 5.2.4, « Zuweisung von Zutritten an einen neuen Benutzer »](#)
5. [Section 5.2.5, « Einem neuen Benutzer ein CUBE Einbruchsprofil zuweisen »](#)
6. Weiter mit [Abschnitt 2.3.3, „Workflow - Installation, Konfiguration und Parametrierung eines TACTILLYS-IP CUBE-Terminals vor seiner Inbetriebnahme“](#)

2.3.3. Workflow - Installation, Konfiguration und Parametrierung eines TACTILLYS-IP CUBE-Bedienteils vor seiner Inbetriebnahme

Bei der ersten Inbetriebnahme muss der Partner oder der Installateur nacheinander die folgenden Schritte durchführen:

1. [Abschnitt 4.1.1, „Physische Installation und Verbindung eines TACTILLYS-IP CUBE-Terminals“](#)
2. [Abschnitt 4.1.2, „Zutritt zur Schnittstelle für den Administrator des TACTILLYS-IP CUBE-Terminals und Anzeige der Produktmerkmale“](#)
3. [Abschnitt 4.2.2, „Abfrage der Betriebsmerkmale von TACTILLYS-IP CUBE“](#)
4. [Abschnitt 4.2.3, „Parametrierung des TACTILLYS-IP CUBE“](#)
5. [Abschnitt 4.1.3, „Änderung des Passworts für den Administrator des TACTILLYS-IP CUBE-Terminals“](#)
6. [Abschnitt 4.1.6, „Aktualisierung der Firmware des TACTILLYS-IP CUBE“](#)
7. [Abschnitt 4.1.4, „Einstellen der Uhrzeit des Terminals TACTILLYS-IP CUBE“](#)
8. [Abschnitt 4.1.5, „Netzwerk-Einstellungen des TACTILLYS-IP CUBE“](#)
9. [Abschnitt 5.1, „Importieren der CUBE Einbruch-Konfiguration in MICROSESAME“](#)

Kapitel 3. Parametrisierung von CUBE Einbruch durch den TIL-Partner

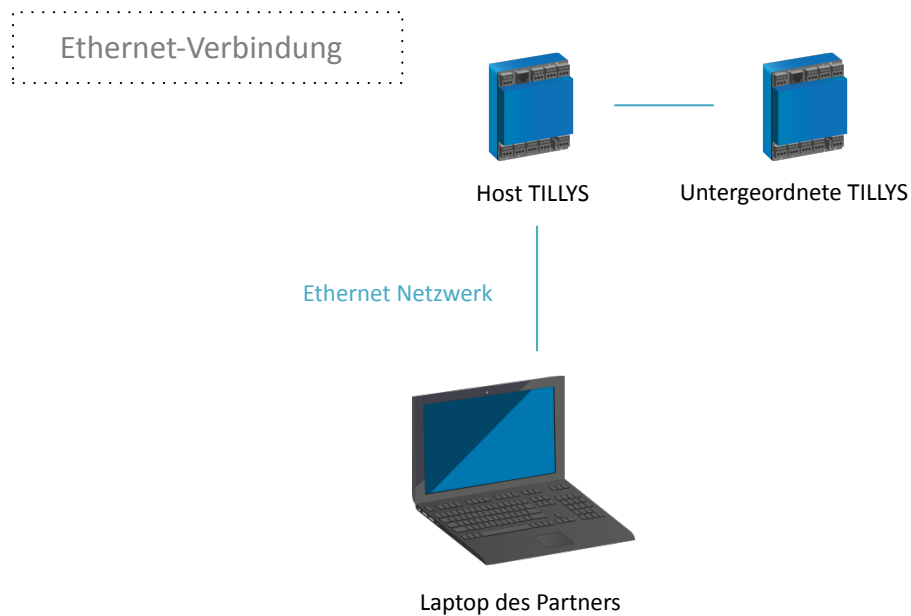
Mit dem Einbruch CUBE wird nun fast die gesamte Parametrisierung an der TILLYS durchgeführt. Dies ermöglicht es den Partnern, die Konfiguration der TILLYS im Voraus vorzubereiten, um sie dann vor Ort schnell zu laden, bevor sie den oder die TACTILLYS-IP CUBE-Terminals installieren. Alle diese Vorgänge können bereits vor der Installation von MICROSESAME durchgeführt werden und einsatzbereit sein.

3.1. Hardware-Architektur für die Konfiguration von CUBE Einbruch durch den Partner

Der Partner kann die Konfiguration bei seinem Endkunden durchführen, aber er kann auch eine CUBE Einbruch-Konfiguration in seinen eigenen Räumlichkeiten vorbereiten, bevor er sich auf den Weg macht, um sie am Standort des Kunden zu implementieren. Die erforderliche Hardware-Architektur besteht einfach aus :

- einem Laptop, der mit Ethernet verbunden ist,
- einer oder mehreren TILLYS (Multi-TILLYS-Konfiguration), die mit demselben Ethernet-Netzwerk verbunden sind.

Abbildung 3.1. Einrichten von CUBE Einbruch über Ethernet (10010-004)



3.2. Konfiguration, Parametrierung und Wartung von CUBE Einbruch an der TILLYS


Die Konfiguration der Einbruchmeldeanlage (die anschließend auf den/die TILLYS heruntergeladen werden muss) kann an einer beliebigen TILLYS vor der Konfiguration der Anlage beim Kunden vorbereitet werden.

Wenn Melder und Sirenen in einer Entfernung angeschlossen werden müssen, die über die zulässige Gesamtlänge des RS 485-Busses (**600 Meter**) hinausgeht, ermöglicht CUBE Einbruch die Einrichtung von untergeordneten TILLYS-Geräten. Die übergeordnete TILLYS Host verwaltet dann die Einbruch-Konfiguration für die Meldepunkte und Sirenen der TILLYS-Geräte, die mit ihr verbunden sind, und ein Token sichert den Informationsaustausch.

3.2.1. Konfigurationsschritte für CUBE Einbruch

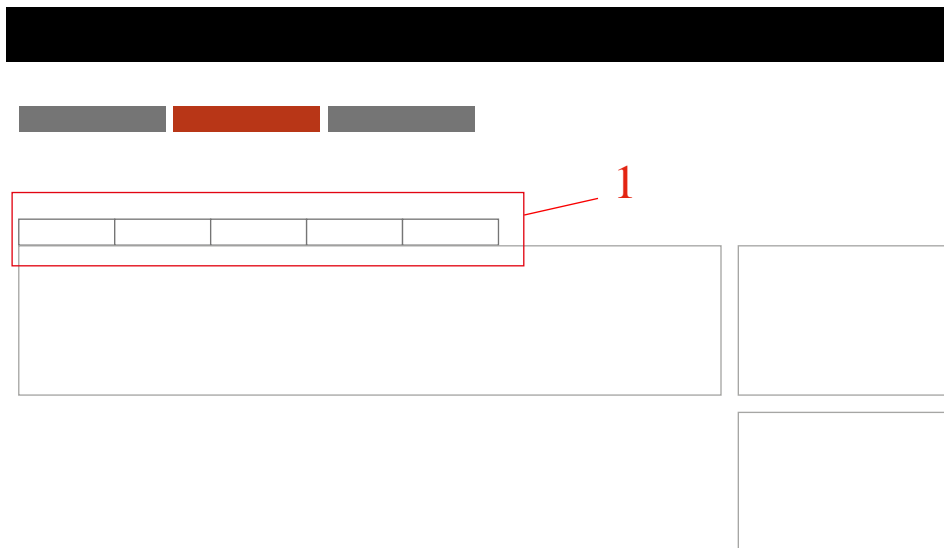
In den folgenden Abschnitten werden alle individuellen Konfigurationsschritte aufgeführt, die über die webbasierte Schnittstelle eine TILLYS über deren IP-Adresse zugänglich sind.

3.2.1.1. Zugriff auf Administratorschnittstelle von CUBE Einbruch an einer TILLYS

1. Öffnen Sie auf dem Laptop, der mit dem Ethernet-Netzwerk verbunden ist, einen Browser und geben Sie die IP-Adresse der TILLYS ein, die Sie konfigurieren möchten.
2. Geben Sie den Login und das Passwort für den Zugriff ein.
3. Folgen Sie im Menü  den Schritten **Einbruch CUBE > Einbruch Konfiguration**.

Die Konfigurationsregisterkarten (Gruppen, Meldpunkte, Sirenen, Profile und TACTILLYS-IP) sind oben im Zentralenabschnitt zugänglich: siehe (1) in der folgenden Abbildung.


Abbildung 3.2. Position der Navigationsregisterkarten auf dem Konfigurationsbildschirm für den CUBE Einbruch eines TILLYS (10010-005)



3.2.1.2. Einrichten eines Alarmüberwachungsbereiches

Mit CUBE Einbruch kann eine Gruppe von TILLY-Host-Meldepunkten und Sirenen verwaltet werden, die physisch an verschiedene TILLYS angeschlossen sind (Multi-TILLYS-Konfiguration). Jeder TILLYS kann bis zu 32 Meldergruppen verwalten. Jede Gruppe kann physische Melder und virtuelle Meldepunkte verwalten, die mit anderen Sonstigen TILLYS verbunden sind.


Es ist völlig unnötig, eine Meldergruppe auf den untergeordneten TILLYS-Geräten zu erstellen. Mit dem CUBE Einbruch können sie ihre Meldepunkte und Sirenen virtuell mit der Meldergruppe der TILLYS-Host verknüpfen.

1. Folgen Sie im Menü  auf dem TILLYS-Host **Einbruch CUBE > Einbruch Konfiguration**.
2. Klicken Sie auf den Reiter **Gruppen** und dann auf die Schaltfläche [+ Hinzufügen].

3. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

| Abschnitt Allgemeine Informationen | Detail der Einstellungen |
|--|--|
| Bezeichnung | Geben Sie einen einschlägigen Namen des Standorts für die Meldergruppe ein. |
| Übertragung der Scharfschaltung / Unscharfschaltung | Wenn die Scharf-/Unscharfschaltung der Gruppe an die Fernüberwachungsleitstelle übertragen werden sollen, klicken Sie auf den Schalter (weiß > blau). |
| Register des Scharfschaltungszustands | Geben Sie unbedingt ein Register Schaltkontakt (M, V oder R, von 1 bis 128) ein, das die Gruppe scharf (Wert 0) oder unscharf (Wert 1) schaltet. |
| Register für den Status (Statusregister) | Geben Sie optional ein numerisches Register (MN, VN oder RN, von 1 bis 128) ein, in das der gesamte Status der Gruppe hochgeladen wird. Siehe auch Abschnitt 1.7.2, „Werte des numerischen Registers für den Gruppenstatus bei Einbruch CUBE“ . |

| Abschnitt Konfiguration der Scharfschaltung | Detail der Einstellungen |
|--|---|
| Zeitplan für die automatische Scharfschaltung | Wenn eine automatische Scharfschaltung nach Zeitplan gewünscht wird, geben Sie die Nummer eines Zeitfensters ein (von 1 bis 250). |
| Automatische Unscharfschaltung | Wenn die Gruppe am Ende eines Zeitfensters unscharf geschaltet werden soll, klicken Sie im Rahmen der Zeitfenster Unscharfschaltung auf den Schalter (weiß > blau). |
| Register der Scharfschaltungsbereitschaft | Gibt an, ob die Meldergruppe scharfgeschaltet werden kann: <ul style="list-style-type: none"> • Das Register ist 1, wenn keines der Meldersignale in der Gruppe im Fehlerzustand ist. • Das Register wird auf 0 gesetzt, wenn mindestens ein Meldersignal in der Gruppe im Fehlerzustand ist. |

| Abschnitt Konfiguration der Scharfschaltung | Detail der Einstellungen |
|---|---|
| | <p>Geben Sie ggf. ein Schaltkontakt-Register ein (M, V oder R, von 1 bis 128).</p> <p> Wenn das Signal eines Melders, der als bei der Scharfschaltung automatisch maskierbar definiert ist, im Fehlerzustand ist, ist der Wert des Registers für den <i>Scharfschaltungsstatus</i> 0.</p> <p>Wenn die Scharfschaltung angefordert wird (automatisch, per Mikrocode oder per Fernsteuerung durch einen Operator), wird der Melder aus der Überwachungsschleife maskiert und die Gruppe scharfgeschaltet.</p> |
| Voralarm-Verzögerung (in Minuten) | <p>Ermöglicht das Einstellen einer Verzögerung, bevor die Scharfschaltung der Gruppe ausgelöst wird.</p> <p>Geben Sie die gewünschte Anzahl von Minuten ein.</p> |
| Zutrittsverzug (in Sekunden) | <p>Geben Sie die gewünschte Anzahl von Sekunden ein, wenn mindestens ein Melder in der Gruppe als Zutrittsverzug konfiguriert wurde.</p> <p>Diese Verzögerung gilt für alle Melder in der Gruppe, die auf "Zutrittsverzug" oder "Ausgeblendet, wenn Zutrittszeit läuft" eingestellt sind.</p> |
| Austrittsverzug (in Sekunden) | <p>Geben Sie die gewünschte Anzahl von Sekunden ein, wenn mindestens ein Melder in der Gruppe als Austrittsverzug konfiguriert wurde.</p> <p>Diese Verzögerung gilt für alle Melder in der Gruppe, die auf "Austrittsverzug" oder "Ausgeblendet, wenn Eingangstempo läuft" eingestellt sind.</p> |

| Scharfschaltung | Detail der Einstellungen |
|---|--|
| Mindestüberschreibung (in Minuten) | <p>Legt den Mindestwert für die vorgeschlagene Überschreibungszeit beim Scharfschalten fest.</p> <p>Geben Sie die gewünschte Anzahl von Minuten ein. Dieser wird dem Operator auf dem CUBE Einbruch-Terminal angeboten.</p> |
| Maximale Überschreibung (in Minuten) | <p>Ermöglicht die Einstellung des maximalen Wertes für die Zeit, die für das Überschreiben der Scharfschaltung benötigt wird. Nach Ablauf dieser Zeit muss der Operator entscheiden, ob er die Gruppe unscharf- oder scharfschalten will.</p> <p>Geben Sie die gewünschte Anzahl von Minuten ein. Dieser wird dem Operator auf dem CUBE Einbruch-Terminal angeboten.</p> |
| Keine Überschreibung (in Minuten) | <p>Legt den Schritt fest, um den die Zeit für das Überschreiben der Scharfschaltung erhöht wird.</p> <p>Geben Sie die gewünschte Anzahl von Minuten ein. Dieser wird dem Operator auf dem CUBE Einbruch-Terminal angeboten.</p> |

| Abschnitt Zusammenfassende Register | Detail der Einstellungen |
|--|--|
| Es ist möglich, den Speicherort von 7 zusammenfassenden Registern festzulegen. | <p>Sie ermöglichen es, ein Register für jeden Alarmtyp zu definieren, das das Vorhandensein eines Fehlerzustands in mindestens einem Signal eines Melders der Gruppe :</p> <ul style="list-style-type: none"> ● Das Register wird auf 0 gesetzt, wenn keines der Meldersignale in der Gruppe im Fehlerzustand ist. ● Das Register wird auf 1 gesetzt, wenn mindestens ein Meldersignal in der Gruppe im Fehlerzustand ist. <p>Geben Sie optional ein Register ToR (M, V oder R, von 1 bis 128) für jeden Alarmtyp ein : Einbruch, Rund um die Uhr, Stillen Einbruch,</p> |


| Abschnitt Zusammenfassende Register | Detail der Einstellungen |
|-------------------------------------|--|
| | Systemfehler, Stiller Systemfehler, Notruf oder Brand. |

- Klicken Sie zur Validierung auf die Schaltfläche [**Speichern**].

3.2.1.3. Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät

Der Anschluss der Meldepunkte und Sirenen der TILLYS Geräte muss unter Verwendung eines Tokens (Wertmarke) pro TILLYS Gerät erfolgen. Dies ermöglicht es, im Falle eines Sicherheitsproblems jedes TILLYS Gerät unabhängig voneinander zu trennen.

Token werden nur einmal generiert und müssen in einer Kundendatei zusammen mit seinen anderen vertraulichen Konfigurationsdaten aufbewahrt werden.

- Folgen Sie im Menü  auf dem TILLYS-Host **Netzwerk und Sicherheit > Sicherheit**.
- Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

| HTTPS-Abschnitt | Detail des Parameters |
|---------------------------|--|
| Select certificate | Im Prinzip gibt es in diesem Abschnitt nichts zu ändern. |

| Abschnitt API-Tokens | Detail der Einstellungen |
|-------------------------------------|--|
| Token name (Name des Tokens) | Geben Sie einen Namen ein, der den entfernten TILLYS eindeutig identifiziert. Aus Sicherheitsgründen werden Sonderzeichen nicht berücksichtigt. |

| | |
|--|---|
| Days of validity (Tage der Gültigkeit) (Ablaufdatum) | Maximal 3 Jahre (d. h. 1096 Tage). |
| Scopes (Betreff) | Klicken Sie auf den Schalter Tillys Konfiguration (weiß > blau). |


- Klicken Sie zur Validierung auf die Schaltfläche [**Request New Token**]. Ein Fenster **Sicherheit** wird angezeigt.
- Ganz rechts auf der Zeile, die für die Eingabe des Passworts vorgesehen ist, befindet sich eine Schaltfläche zum Anzeigen des Passworts und die nächste zum Kopieren des Passworts. Kopieren Sie den Wert dieses Tokens in die Konfigurationsdatei der Client-Installation und notieren Sie dort auch die IP-Adresse des TILLYS-Geräts, für das es generiert wurde.
- Um eine Unterbrechung der CUBE-Einbruchserkennung in bestimmten Bereichen, in denen das Token abgelaufen ist, zu vermeiden, legen Sie bereits jetzt mit dem Kunden den Termin für

den technischen Besuch zur Verlängerung der Gültigkeitsdauer des Token oder der Token fest (z. B. eine Woche vor dem geplanten Ablaufdatum).

3.2.1.4. Multi-TILLYS-Konfiguration: Klonen der Verbindung zur Host-TILLYS an einer TILLYS

Dieser Vorgang ermöglicht es, die Meldergruppe(n) des Host-TILLYS auf einer untergeordneten TILLYS-Gerät anzuzeigen.

Wenn es mehrere TILLYS-Geräte gibt, ist es ratsam, ein Token pro TILLYS-Gerät zu setzen (siehe [Abschnitt 3.2.1.3, „Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät“](#)).

1. Folgen Sie im Menü  des TILLYS Geräts **Einbruch CUBE > Einbruch Configuration** und klicken Sie dann auf die Registerkarte **Groups**.
2. Klicken Sie auf der rechten Seite des Bildschirms auf die Schaltfläche [**Gruppen von einem Remote-Host herunterladen**].

Ein Dialogfenster wird angezeigt.

Abbildung 3.3. Eingeben des Token des Host-TILLYS auf einem Gerät-TILLYS (10010-010)

3. Füllen Sie die verschiedenen Felder gemäß der folgenden Tabelle aus.


| Parameter | Details |
|---|---|
| <i>Der abgesetzte Host verwendet HTTPS</i> | <p>In der Standardkonfiguration ist dieser Schalter aktiviert (weiß > blau) und das Protokoll https muss bei beiden TILLYS aktiviert sein.</p> <p>Ist dies nicht der Fall, wird die Nachricht "Hostgruppen konnten nicht gezogen werden: Host nicht erreichbar" angezeigt.</p> |

| Parameter | Details |
|----------------------|--|
| | Weitere Informationen finden Sie unter Abschnitt 3.2.2.6, „Wahl der Sicherheitsstufe über IP zwischen TILLYS und TACTILLYS-IP CUBE“ . |
| Host | Standardmäßig enthält dieses Feld den Wert "admin". Geben Sie die IP-Adresse des TILLYS-Hosts ein. |
| API-Schlüssel | Fügen Sie den Wert des zuvor erzeugten Tokens ein (siehe Abschnitt 3.2.1.3, „Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät“). |

4. Klicken Sie auf die Schaltfläche [**Gruppen herunterladen**].

3.2.1.5. Konfiguration der CUBE Meldepunkte einer TILLYS

Dies gilt für die TILLYS (Host oder Gerät), mit der die Meldepunkte physisch verbunden sind.

- Gehen Sie im Menü  der TILLYS auf **Einbruch CUBE > Einbruch Configuration**, klicken Sie auf die Registerkarte **Melder** und dann auf die Schaltfläche [**+ Hinzufügen**].
- Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

| Abschnitt Allgemeine Informationen | Details zu den Einstellungen |
|------------------------------------|---|
| Bezeichnung | Geben Sie einen Namen für den Meldepunkt ein. |
| Weiterleiten von Alarmen | Klicken Sie auf den Schalter (weiß > blau), wenn die von diesem Melder erzeugten Alarme an den Fernüberwachungsstelle weitergeleitet werden sollen. |
| Blockierregister | Geben Sie optional ein Register Schaltkontakt (M, V oder R, von 1 bis 128) ein, das im Zustand 1 die Sperrung des Meldepunktes ermöglicht (z. B. für Wartungsarbeiten). |
| Virtueller Melpunkter | Standardmäßig ist der eingestellte Melder ein physischer Melder (der Schalter <i>Virtueller Melder</i> ist weiß). Geben Sie den <i>Bus</i> (A, B oder C), die Adresse des MI-Moduls, an das der Melder angeschlossen ist, und den ML-Eingang, mit dem er verdrahtet ist, ein. Einen virtuellen Melder zu konfigurieren bedeutet, ihn logisch mit einem TILLYS-Host |

| Abschnitt Allgemeine Informationen | Details zu den Einstellungen |
|------------------------------------|--|
| | <p>zu verknüpfen, während er physisch mit einem TILLYS-Gerät verbunden ist. Dazu betätigen Sie den Schalter <i>Virtual Detector</i> (weiß > blau). Die Nummer dieses virtuellen Melders wird dann automatisch festgelegt (ID in der globalen Melderliste vorhanden).</p> |
| Abschnitt Maskieren | Details der Einstellung |
| | <p>Um den Maskieren-Start für den Melder zu wählen, aktivieren Sie die Schalter (weiß > blau) :</p> <ul style="list-style-type: none"> ● <i>Kann manuell maskiert werden</i>: Manuelles Maskieren bei der Inbetriebnahme ● <i>Kann automatisch maskiert werden</i>: Automatisches Maskieren bei Inbetriebnahme ● <i>Kann dauerhaft maskiert werden</i>: Dauerbenutzer Maskieren ● <i>Kann automatisch zurückgesetzt werden</i>: Automatische Rücksetzung nach Fehlerbehebung |
| Abschnitt Zutritt | Details der Einstellung |
| | <p>Um einem Benutzer zu erlauben, nach dem Scharfschalten den Raum zu verlassen oder zum Unscharfschalten zum Einbruchsterminal zu gehen, und um die gewünschte Verzögerungsart zu wählen, aktivieren Sie die Schalter (weiß > blau).</p> <p>Die Verzögerungszeiten in Sekunden müssen in den Einstellungen der Meldergruppen konfiguriert werden.</p> <ul style="list-style-type: none"> ● <i>Aktiviert den Zutrittsverzug</i>: Aktiviert den Zutrittsverzug. ● <i>Auf dem Eingangspfad</i>: Ausgeblendet, wenn der Zutrittsverzug läuft. Der Melder wird vorübergehend gehemmt, wenn ein anderer Melder in der gleichen |

| Abschnitt Zutritt | Details der Einstellung |
|-------------------|---|
| | <p>Meldergruppe einen Zutrittsverzug oder Austrittsverzug hat.</p> <ul style="list-style-type: none">● <i>Auf dem Weg zum Ausgang: Austrittsverzug</i> |
| Abschnitt Signale | Details der Einstellung |
| | <p>Standardmäßig sind beide Signale, Alarm und Sabotageschutz, aktiviert (blauer Schalter). Um eines der Signale zu deaktivieren, klicken Sie auf seinen Schalter (blau > weiß).</p> <p>Der Alarm Einbruch kann ausgelöst werden, wenn die Gruppe scharfgeschaltet ist. Eine Sirenenfunktion wird ausgelöst, wenn sie verknüpft wurde.</p> <p>Der Manipulationsschutz-Alarm ist ein Dauerbenutzer-Alarm, der unabhängig vom Scharfschaltungsstatus der Gruppe ausgelöst wird. Eine Sirenenfunktion wird ausgelöst, wenn sie verknüpft wurde.</p> <ul style="list-style-type: none">● <i>Alarm</i> : Anklicken, um ihn zu aktivieren (weiß > blau). <p><i>Typ</i> (Art des Alarms): Standardmäßig Einbruch. Wählen Sie den gewünschten Typ aus dem Drop-Down-Menü aus.</p> <p><i>Modus</i>(Kontaktart): Wählen Sie einen Wert aus der Drop-Down-Menüleiste aus(<i>Normal zu</i>).</p> <p><i>Nummer für den Fernüberwachungsmonitor</i> : Wert, der an den Fernüberwachungsmonitor übermittelt werden soll.</p> |

| Abschnitt Signale | Details der Einstellung |
|-------------------|---|
| | <ul style="list-style-type: none"> ● <i>Sabotageschutz</i>: Anklicken, um ihn zu aktivieren (weiß > blau). <i>Typ</i> (Art des Alarms): Standard 24/24. Wählen Sie den gewünschten Typ aus dem Drop-Down-Menü aus. <i>Modus</i> (Kontaktart) : <i>Normal zu. Nummer für den Fernüberwachungsmonitor</i> (Fernübertragungsreferenz): Wert, der an den Fernüberwachungsmonitor übermittelt werden soll. |

| Abschnitt Der Gruppe zuweisen | Details der Einstellung |
|-------------------------------|---|
| | <p>Um den Melder einer Gruppe zuzuweisen, wählen Sie seinen Namen aus der Drop-Down-Menüliste.</p> <p>Wenn es sich um einen virtuellen Melder handelt, muss er einer Gruppe des TILLYS-Hosts zugeordnet werden.</p> <p>Mit diesem Drop-Down-Menü können Sie auch einen Melder deaktivieren.</p> |

3. Um die vorgenommenen Einstellungen zu validieren, klicken Sie auf die Schaltfläche [**Speichern**].

3.2.1.6. Einrichten eines CUBE-Meldepunktes an einer TILLYS


In einer Multi-TILLYS-Konfiguration ist das Verfahren bis zur Auswahl der Anschlussgruppe identisch mit dem in [Abschnitt 3.2.1.5, „Konfiguration der CUBE Einbruchmelder einer TILLYS“](#) beschriebenen Verfahren: Wählen Sie die Hauptgruppe, die sich auf der Host-TILLYS befindet. Außerdem muss der Schalter *Virtueller Melder* aktiviert werden.

3.2.1.7. Einrichten einer CUBE Alarmsirene

Dies gilt für die TILLYS (Host oder Gerät), mit der die Sirene physisch verbunden ist.

Jeder Klingelton-Stil hat einen Prioritätsindex. Je höher dieser Prioritätsindex ist, desto höher ist die Priorität des Klingeltons gegenüber den anderen.

Beispiele: Der Alarmton für Einbruch (Priorität 4) hat Vorrang vor dem Alarmton für Voralarm (Priorität 1), und der Alarmton für Feuer (Priorität 6) hat Vorrang vor dem Alarmton für Einbruch (Priorität 4).

1. Gehen Sie im Menü  burger der TILLYS auf **Einbruch CUBE > Einbruchskonfiguration**, klicken Sie auf die Registerkarte **Sirenen** und dann auf die Schaltfläche [+ Hinzufügen].
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

| Abschnitt Allgemeine Informationen | Detail der Einstellungen |
|------------------------------------|---|
| Bezeichnung | Geben Sie einen Namen für die Sirene ein. |
| Befehlsregister | <p>Geben Sie einen gültigen Wert für das Logische Register :</p> <p>Sei ein physisches Register für die Ausgabe eines Moduls, z. B. : "XA0102". Bei einem MLIO16-Modul müssen die Ausgänge zuvor definiert worden sein, damit das Register akzeptiert wird.</p> <p>Oder ein virtuelles Register: Ein Register des Typs M, V oder R von 1 bis 128 kann eingegeben werden, um einen bestimmten, vom Mikrocode definierten Trigger auszulösen.</p> |
| Blockierregister | Geben Sie optional einen Wert für das Logische Register (M, V oder R, von 1 bis 128) ein, der auf 1 gesetzt wird, um die Sperrung der Sirene zu ermöglichen (z. B. für Wartungsarbeiten). |

| Abschnitt Meerjungfrauen-Stile | Detail der Einstellungen |
|--------------------------------|--|
| Voralarm | <p>Konfigurieren Sie die verschiedenen Sirenen mithilfe der Zeichen + und - sowie die Dauer des Klingelns (in Sekunden).</p> <p>Die Konfiguration der Sirenen erfolgt auf der Ebene der Dauer und nicht auf der Ebene der Anzahl der Wiederholungen.</p> <p>Bei der Sirene für den Voralarm, Auslösung vor der Scharfschaltperiode, damit die Person, die die Gruppe scharfgeschaltet hat, das</p> |

| Abschnitt Meerjungfrauen-Stile | Detail der Einstellungen |
|--------------------------------|---|
| | Gebäude verlassen kann oder eine noch anwesende Person am Terminal TACTILLYS-IP CUBE eine Überschreibung beantragen kann. |
| Scharfschaltung | Auslösung zu Beginn der Scharfschaltung der Gruppe. |
| Systemfehler | Auslösung unabhängig vom Scharfschaltungsstatus der Gruppe. |
| Einbruch | Auslösung bei Erkennung eines Einbrechers, wenn die Gruppe scharfgeschaltet ist. |
| Notfall | Notruf. Auslösung unabhängig vom Scharfschaltungsstatus der Gruppe. |
| Brand | Auslösung unabhängig vom Scharfschaltungsstatus der Gruppe. |

| Abschnitt Gruppen zuweisen | Detail der Einstellungen |
|----------------------------|---|
| | Mithilfe dieser Liste können Sie eine Sirene einer oder mehreren Gruppen zuweisen. Um mehrere Gruppen auszuwählen, halten Sie die [CTRL]- Taste gedrückt und klicken Sie nacheinander auf die Gruppen, dann lassen Sie die [CTRL]-Taste los. |

- Um die vorgenommenen Einstellungen zu validieren, klicken Sie auf die Schaltfläche [**Speichern**].

3.2.1.8. Konfigurieren einer CUBE Alarmsirene an einer TILLYS


In der Konfiguration Einbruch CUBE multi-TILLYS ist das Verfahren identisch mit dem unter [Abschnitt 3.2.1.7, „Einrichten einer CUBE Einbruch-Sirene“](#) beschriebenen, bis zur Auswahl der Anschlussgruppe: Wählen Sie die Hauptgruppe, die sich auf dem Host-TILLYS befindet.

3.2.1.9. Übersichtsvergleich der Meldepunkte für Multi-TILLYS CUBE-Einbruch


Die Kombination der Taste [**Windows**] auf der Tastatur mit der linken [**←**] oder rechten [**→**] Pfeiltaste ermöglicht es, ein Browserfenster in Pfeilrichtung um die Hälfte zu verkleinern und zwei Fenster auf demselben Bildschirm nebeneinander zu legen, um ihre Informationen leichter vergleichen zu können.

- Öffne ein Browserfenster und öffne den TILLYS-Host, dann klicke auf die Tasten [**Windows**] + [**←**].

Das Browserfenster wird in der Breite verkleinert und nimmt die linke Hälfte des Bildschirms ein.

2. Gehen Sie im Menü  burger des TILLYS-Hosts auf **Einbruch CUBE > Einbruch Configuration** und klicken Sie auf die Registerkarte **Melder**.
3. Öffnen Sie ein zweites Browserfenster und öffnen Sie das TILLYS Gerät, klicken Sie dann auf die Tasten [**Windows**] + [**→**].


Das Browserfenster wird in der Breite verkleinert und nimmt die rechte Hälfte des Bildschirms ein.

4. Im Menü  burger des TILLYS Geräts folgen Sie **Einbruch CUBE > Einbruch Configuration** und klicken Sie auf die Registerkarte **Detektoren**.

Durch den Vergleich der beiden Konfigurationen auf einem Bildschirm lassen sich mögliche Fehlkonfigurationen erkennen.

3.2.1.10. Zuordnung eines TACTILLYS-IP CUBE-Bedeinteils zu einer oder mehreren Gruppen einer Host-TILLYS

Diese Operation ermöglicht es, ein TACTILLYS-IP CUBE Terminal mit der Host-TILLYS zu verbinden, dessen Gruppe(n) Sensoren, Sirenen sowie alle mit dem Scharf- und Unscharfschalten des Alarms verbundenen Operationen verwaltet/verwalten.

1. Im Menü  burger des TILLYS-Hosts folgen Sie **Einbruch CUBE > Configuration Einbruch**, klicken Sie auf die Registerkarte **TACTILLYS-IP** und dann auf die Schaltfläche [**+ Hinzufügen**].
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.


| Abschnitt Allgemeine Informationen | Detail der Einstellungen |
|------------------------------------|---|
| Bezeichnung | Geben Sie einen Namen für das TACTILLYS-IP CUBE-Terminal ein. |
| IP-Adresse | Geben Sie die IP-Adresse dieses TACTILLYS-IP CUBE-Terminals ein. |
| Port | Geben Sie den Kommunikationsport ein, der für die Nutzung der Kommunikation mit dem Terminal verwendet wird (Standard: 443). |
| Alarmerweiterungen | Klicken Sie auf den Schalter (weiß > blau), damit das Terminal einen Signalton abgibt, wenn im System ein Alarm erzeugt wird. |

| Abschnitt Authentifizierung | Detail der Einstellungen |
|--|--|
| Maximale Inaktivität (in Sekunden) | Geben Sie die gewünschte Anzahl an Sekunden ein, die der Zeitspanne entspricht, in der das Terminal ohne jegliche Aktion des Operators verbunden bleibt. |
| Maximale Anzahl an Versuchen vor dem Sperren | Geben Sie die Anzahl der Verbindungsversuche ein, die akzeptiert werden, bevor das Terminal gesperrt wird. |
| Dauer der Authentifizierungssperre | Geben Sie die Zeit in Minuten ein, für die das Terminal gesperrt bleibt, nachdem die maximale Anzahl an Verbindungsversuchen erreicht wurde. |
| Zeitlimit für die Eingabe des Codes (in Sekunden) | Geben Sie die maximale Zeit in Sekunden ein, die zwischen dem Passieren eines Ausweises und der Eingabe des zugehörigen Codes akzeptiert wird. |
| Willkürliche Position der Tasten auf der numerischen Tastatur | Klicken Sie auf den Schalter (weiß > blau), um die Zufallspositionierung der numerischen Tasten zu aktivieren. |
| Abschnitt Signale | Detail der Einstellungen |
| Manipulationsschutz | Klicken Sie auf den Schalter (weiß > blau), um die Berücksichtigung des Sabotagekontaktes des Terminals zu aktivieren. |
| Typ | Wenn aktiviert, ist der Sabotageschutz standardmäßig auf den Alarmtyp 24/24 eingestellt. Wählen Sie eventuell einen anderen Alarm-Typ aus dem Drop-Down-Menü aus. |
| Nummer für den Fernsender | |
| Abschnitt Verwaltete Gruppen | Detail des Parameters |
| Der Gruppe zuweisen | <p>Mit dieser Liste können Sie ein TACTILLYS-IP CUBE-Terminal der Verwaltung einer oder mehrerer Gruppen zuweisen.</p> <p>Um mehrere Gruppen auszuwählen, halten Sie die [CTRL]- Taste gedrückt und klicken Sie</p> |

| Abschnitt Verwaltete Gruppen | Detail des Parameters |
|------------------------------|--|
| | nacheinander auf die Gruppen, dann lassen Sie die [CTRL]-Taste los. |

3. Klicken Sie zur Validierung auf die Schaltfläche [**Speichern**].

3.2.1.11. Konfigurieren der Fernüberwachungsleitstelle

1. Folgen Sie im Menü  burger des TILLYS-Hosts **Einbruch CUBE > Transmitter-Konfiguration** und klicken Sie dann auf die Schaltfläche [**+ Hinzufügen**].
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

| Abschnitt Allgemeine Informationen | Detail der Einstellungen |
|---|--|
| Abschnitt Allgemeine Informationen | |
| Bezeichnung | Geben Sie einen Namen für den Fernüberwachungsmonitor ein. |
| IP-Adresse | Geben Sie die IP-Adresse des Fernüberwachungsmonitors ein. |
| Port | Geben Sie den Kommunikationsport des Fernüberwachungsmonitors ein. |

| Abschnitt Einstellungen des Empfängers | Detail der Einstellungen |
|--|---|
| Protokoll | SIA-DCS. |
| Abonnenntenummer | Geben Sie die vom Fernsender bereitgestellte Kundenreferenz ein. |
| Anzahl der Verbindungsversuche | Geben Sie die maximale Anzahl an Verbindungsversuchen ein. |
| Zeit zwischen den Versuchen (in Sekunden) | Geben Sie die Mindestzeit zwischen zwei Verbindungsversuchen ein. |

| Abschnitt Einstellungen für den zyklischen Test des Empfängers | Detail der Einstellungen |
|--|--|
| Startzeit | Die Frames des zyklischen Tests werden von der TILLYS an die Überwachungssoftware des Fernüberwachungsmonitors (SIG) gesendet. Es gibt einen zyklischen Test pro Fernüberwachungsmonitor. |

| | |
|---|--|
| Abschnitt Einstellungen für den zyklischen Test des Empfängers | Detail der Einstellungen |
| | Mit dieser Einstellung können Sie die Referenzzeit festlegen, ab der der zyklische Test durchgeführt wird. |
| Intervall (in Minuten) | Mit diesem Parameter können Sie festlegen, wie oft der zyklische Test durchgeführt werden soll. |
| Abschnitt Polling-Einstellungen des Empfängers | Detail des Parameters |
| Der Gruppe zuweisen | <p>Polling-Frames werden von der Host-TILLYS an das Frontend der Fernüberwachung gesendet.</p> <p>Diese Liste ermöglicht es Ihnen, ein TACTILLYS-IP CUBE-Terminal einer oder mehreren Gruppen zuzuordnen.</p> <p>Um mehrere Gruppen auszuwählen, halten Sie die [CTRL]- Taste gedrückt und klicken Sie nacheinander auf die Gruppen, dann lassen Sie die [CTRL]-Taste los.</p> |
| Abschnitt Notrufempfänger | Detail des Parameters |
| Zum Beispiel "Fernüberwachungsmonitor 2". | Um aus diesem Drop-Down-Menü einen Rettungsempfänger auswählen zu können, muss dieser zunächst eingerichtet werden. |

3. Klicken Sie zur Validierung auf die Schaltfläche [**Speichern**].
4. Um einen Fernüberwachungsmonitor zu erstellen, beginnen Sie wieder bei Schritt 1, um diesen neuen Empfänger zu erstellen, bearbeiten Sie dann den Hauptempfänger und weisen Sie ihm im letzten Abschnitt des Eingabebildschirms den neu erstellten Notrufempfänger zu.

3.2.1.12. Anzeige der Fernüberwachungskonfiguration


Im Menü  burger des TILLYS-Hosts folgen Sie **Einbruch CUBE > Senderkonfiguration** und klicken Sie dann auf die Schaltfläche [**Aktuelle Konfiguration**].

3.2.2. Parametrisierung und Wartung von CUBE Einbruch

In den folgenden Abschnitten werden die Einstellungsvorgänge für die CUBE Einbruchfunktion erläutert, z. B. die Detailtiefe der Protokollierungsfunktion, die Sicherheitsstufe für den Austausch über IP und die Verwendung des spezifischen Mikrocodes für die CUBE Einbruchfunktion.

Sie stellen auch die Wartung vor, wie z. B. das Löschen der Schlüssel, bevor ein defektes TACTILLYS IP-Terminal zum Kundendienst geschickt wird, sowie die Maßnahmen zur Sicherung und Wiederherstellung einer Konfiguration.

3.2.2.1. Erstellen von Einbruchsprofilen an der Host-TILLYS

1. Folgen Sie im Menü  burger des TILLYS-Hosts **Einbruch CUBE > Einbruch Configuration**, klicken Sie auf die Registerkarte **Profile** und dann auf die Schaltfläche **[+ Hinzufügen]**.
2. Füllen Sie die verschiedenen Felder gemäß den folgenden Tabellen aus.

| Abschnitt Allgemeine Informationen | Detail des Parameters |
|------------------------------------|--|
| Bezeichnung | Geben Sie einen Namen für das Benutzerprofil Einbruch CUBE ein. |
| Abschnitt Rechte des Profils | Detail des Parameters |
| Sieben Schalter (1 pro Zutritt) | Klicken Sie auf den Schalter (weiß > blau), um das entsprechende Recht zu aktivieren. |
| Abschnitt Verwaltete Gruppen | Detail des Parameters |
| Drop-Down-Menü | Diese Liste ermöglicht es Ihnen, ein TACTILLYS-IP CUBE-Terminal einer oder mehreren Gruppen zuzuordnen. Um mehrere Gruppen auszuwählen, halten Sie die [CTRL] - Taste gedrückt und klicken Sie nacheinander auf die Gruppen, dann lassen Sie die [CTRL] -Taste los. |

3. Klicken Sie zur Validierung auf die Schaltfläche **[Speichern]**.
4. Füge alle benötigten Profile hinzu, indem du die oben genannten Schritte wiederholst.


3.2.2.2. Auswahl der Meldergruppen, die von einem TACTILLYS-IP CUBE verwaltet werden

1. Folgen Sie im Menü  des TILLYS-Hosts **Einbruch CUBE > Configuration Einbruch** und klicken Sie dann auf die Registerkarte **TACTILLYS-IP**.


2. Markieren Sie im ersten Abschnitt auf der linken Seite des Bildschirms das Kontrollkästchen der Gruppe.
3. Wählen Sie im ersten Abschnitt auf der rechten Seite des Bildschirms die Gruppe(n), die mit dem TACTILLYS-IP CUBE verbunden ist/sind, und klicken Sie auf die Schaltfläche [**Zuweisen**].

3.2.2.3. Auswahl des Authentifizierungsmodus (Ausweis oder Ausweis + Code) an einem TACTILLYS-IP CUBE

Informationen zum Einstellen oder Ändern des personalisierten Tastaturcodes eines Benutzers finden Sie unter [Abschnitt 6.2, „Änderung des ID-Mittels Einbruch, das bei der Ausweis- und Code-Identifikation auf TACTILLYS-IP CUBE verwendet wird.“](#).

1. Folgen Sie im Menü  des TILLYS-Hosts **Einbruch CUBE > Configuration Einbruch** und klicken Sie dann auf die Registerkarte **TACTILLYS-IP**.
2. Klicken Sie im zweiten Abschnitt auf der rechten Seite des Bildschirms auf das Drop-Down-Menü Modus für die Authentifizierung. Wählen Sie *Ausweis* oder *Ausweis & personalisierter Tastaturcode* und klicken Sie dann auf die Schaltfläche [**Authentifizierungseinstellungen anwenden**].

3.2.2.4. Auswahl der Applets, die auf ein TACTILLYS-IP CUBE geladen werden sollen


1. Folgen Sie im Menü  des TILLYS-Hosts **Einbruch CUBE > Configuration Einbruch** und klicken Sie dann auf die Registerkarte **TACTILLYS-IP**.
2. Geben Sie im dritten Abschnitt auf der rechten Seite des Bildschirms eine Indexreferenz ein, klicken Sie auf die Schaltfläche [**Durchsuchen**], wählen Sie die Datei aus , die **Sie** herunterladen möchten, validieren Sie und klicken Sie auf die Schaltfläche [**Applet-Einstellungen anwenden**].

3.2.2.5. Auswahl der Detailebene für Ereignisse im TILLYS-Protokoll

Die Protokollierung von Ereignissen hilft dabei, die Ursache von Fehlfunktionen zu finden. Sie kann in einer Datei gespeichert oder im Laufe der Zeit an einen Computer gesendet werden, auf dem **Syslog** Watcher installiert ist.

Die laufende Anzeige der Protokollierung ermöglicht es, die Logs in Echtzeit zu verfolgen. Es ist möglich, beide Optionen zu aktivieren (in einer Datei speichern und im Ereignisticker anzeigen)...

Je höher die Detailtiefe, desto mehr Rechenleistung verbraucht der Prozessor und desto mehr Speicherplatz wird belegt. Dies kann die Leistung verlangsamen.

1. Im Menü  des TILLYS-Hosts folgen Sie **System > Logs**.
2. Um das Protokoll an eine bestimmte IP-Adresse zu senden, geben Sie diese IP-Adresse und den Zielport (standardmäßig 514) ein, klicken Sie auf den Syslog-Schalter (grau > blau) und klicken Sie dann auf die Schaltfläche [**Submit**].

Um das Protokoll in einer Datei zu speichern, klicken Sie auf den Syslog-Schalter (grau > blau) und dann auf die Schaltfläche [**Submit**].

Um das Protokoll direkt in der Debug-Konsole am unteren Rand dieses Bildschirms anzusehen, klicken Sie auf den Weblog-Schalter (grau > blau) und dann auf die Schaltfläche [**Submit**].

Es ist möglich, alle drei Schalter zu aktivieren.

3. Klicken Sie auf die grauen Schaltflächen, um auszuwählen, bei welchen Aspekten ein hoher Detaillierungsgrad erforderlich ist.


Es ist möglich, eine niedrigere Detailstufe wiederherzustellen, indem Sie auf die blauen Schaltflächen [**Normal**] klicken.

Zur Validierung klicken Sie auf die Schaltfläche [**Submit**].

4. Eine Debugging-Konsole mit Filtern und einem Bereich für die Suche ermöglicht es, die Suche zu verfeinern.


3.2.2.6. Wahl der Sicherheitsstufe über IP zwischen TILLYS und TACTILLYS-IP CUBE

Mit dieser Option können Sie die Sicherheitsstufe für den Austausch zwischen TACTILLYS-IP und TILLYS auswählen (Protokoll http oder https). Standardmäßig ist der Modus https, was ein sicherer Modus ist. Es wird nicht empfohlen, den Modus http zu verwenden.

1. Klicken Sie in der Schnittstelle für den Administrator des TACTILLYS-IP auf das Symbol  burger in der oberen linken Ecke und folgen Sie **Configuration > Security**.
2. Wählen Sie im Drop-Down-Menü **Select a certificate** den Eintrag **None** und klicken Sie auf die Schaltfläche [**Submit**].
3. Auf der TILLYS-Ebene muss die gleiche Einstellung im Bildschirm **Netzwerkconfiguration** vorgenommen werden: Folgen Sie **Netzwerk und Sicherheit > Netzwerkkonfiguration**.
4. Scrollen Sie nach unten, deaktivieren Sie die Option **Sichere Kommunikation** (Wechsel von blau zu grau) und klicken Sie auf die Schaltfläche [**Speichern**].
5. Falls erforderlich, wird die Wiederherstellung der Kommunikation im Modus https in denselben Bildschirmen durchgeführt.

3.2.2.7. Löschen der TACTILLYS-IP-Schlüssel (Desetzen)


Diese Möglichkeit sollte genutzt werden, nachdem ein TACTILLYS-IP aus einer Anlage entfernt wurde, um ihn in eine andere Anlage integrieren zu können, oder bevor er zum Kundendienst geschickt wird.

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP auf das Symbol  in der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Erase Keys**.
2. Klicken Sie auf die Schaltfläche [**Erase Keys**].

3.2.3. Schritte zur Bewältigung von Einbrüchen


3.2.3.1. Maskieren oder Wiedereinsatz eines Alarmmelders

Alle diese Schritte werden auf dem Einstellungsbildschirm jedes Melders durchgeführt.


1. Von der Schnittstelle für Administratoren des TACTILLYS-IP CUBE aus klicken Sie auf das Symbol  in der oberen linken Ecke des Bildschirms und folgen Sie **Einbruch Cube > TILLYS-Konfiguration**.
2. Klicken Sie auf die Registerkarte Melder.
3. Klicken Sie auf der Linie des Meldepunktes, den Sie auswerfen oder neu einfügen möchten, auf die Schaltfläche [**Bearbeiten**].
4. Klicken Sie im Abschnitt Auswurf auf den Schalter der Option, die Sie aktivieren möchten (weiß > blau).
5. Klicken Sie unten auf dem Bildschirm auf die Schaltfläche [**Speichern**].

3.2.4. Wartung von CUBE Einbruch

3.2.4.1. Aktivieren oder Deaktivieren des Ports für die Wartung einer TILLYS

1. Von der Schnittstelle zum Administrator eines TILLYS aus klicken Sie auf das Symbol  in der oberen linken Ecke des Bildschirms und folgen Sie **Netzwerk und Sicherheit > Netzwerk-Tools**.
2. Klicken Sie auf die Schaltfläche [**Service-Port aktivieren**], um ihn zu aktivieren (blau) oder zu deaktivieren (weiß).
3. Klicken Sie auf [**Speichern**].

3.2.4.2. Exportieren oder Importieren einer CUBE Einbruch-Konfigurationsdatei

1. Um eine CUBE Einbruch-Konfigurationsdatei auf einem TILLYS exportieren oder importieren zu können, muss dessen Wartungsport aktiviert sein (siehe [Abschnitt 3.2.4.1, „Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS“](#)). Ist dies nicht der Fall, ist die Option Importieren/Exportieren nicht einmal im Menü sichtbar.
2. Von der Schnittstelle für den Administrator des TILLYS-Hosts aus klicken Sie auf das Symbol  in der oberen linken Ecke des Bildschirms und folgen Sie **General > Import/Export Configuration**.
3. Füllen Sie die verschiedenen Felder gemäß der folgenden Tabelle aus.

| Parameter | Details |
|--|---|
| Abschnitt Importieren von Konfigurationen | Um eine Konfigurationsdatei zu importieren, klicken Sie auf die Schaltfläche [Browse], |

| Parameter | Details |
|---|---|
| | wählen Sie eine Datei aus, klicken Sie auf die Schaltfläche [Open] und dann auf die Schaltfläche [Import configuration file]. |
| Abschnitt Exportieren Konfiguration | Um eine Konfiguration in eine XML-Datei zu exportieren, markieren Sie das oder die gewünschten Kästchen (Alle, Safe-Konfiguration, Einbruchskonfiguration, Übertragungskonfiguration) und klicken Sie dann auf die Schaltfläche [Export configuration file]. |
| Abschnitt Download exportierte Konfiguration | Am Ende des Exportierens einer Konfiguration klicken Sie auf die Schaltfläche [Download], um die Konfigurationsdatei im XML-Format abzurufen und diese Datei dann in einem Kundenordner zu speichern. |

4. Deaktivieren Sie den Wartungsport (siehe [Abschnitt 3.2.4.1, „Aktivieren oder Deaktivieren des Ports für die Wartung eines TILLYS“](#)), da es eine Sicherheitslücke darstellt, einen Wartungsport offen zu lassen.

3.2.4.3. Verlängerung der Gültigkeitsdauer eines Tokens

Vor dem Ablauf des Tokens, das die Sicherheit des IP-basierten Austauschs zwischen TILLYS innerhalb einer Multi-TILLYS-Gruppe verwaltet, wurde ein Besuch der technischen Wartung vorgesehen, um eine teilweise Unterbrechung des Dienstes zu vermeiden.

Um die Gültigkeitsdauer eines Tokens zu verlängern, erstellen Sie ein neues Token und weisen Sie es dem TILLYS Gerät zu, dessen Token abläuft (siehe [Abschnitt 3.2.1.3, „Multi-TILLYS-Konfiguration: Generierung eines Tokens auf dem TILLYS-Host pro TILLYS-Gerät“](#)).

Kapitel 4. Installation, Einstellung und Verwendung des Bedienteils TACTILLYS-IP CUBE

4.1. Installation, Konfiguration und Wartung eines TACTILLYS-IP CUBE-Terminals

Diese Operationen werden von dem **Partner** TIL TECHNOLOGIES durchgeführt.

4.1.1. Physische Installation und Anschluss eines TACTILLYS-IP CUBE-Bedienteils

Einige Details zur physischen Installation und die technischen Daten finden Sie im [Datenblatt des TACTILLYS-IP CUBE-Terminals](#).

1. Befestigen Sie die Halterung des TACTILLYS-IP in waagerechter Position an der Wand.
2. Schließen Sie ein RJ45-Kabel an die Rückseite des TACTILLYS-IP an.
3. Stecken Sie ein Lesegerät für Ausweise LEC05XF0200-NB6 in einen der beiden Anschlüsse am TACTILLYS-IP.
4. Schließen Sie an der Rückseite des TACTILLYS-IP ein Stromkabel für Gleichstrom an.
5. Befestigen Sie den TACTILLYS-IP an seiner Wandhalterung.
6. Verbinden Sie das RJ45-Kabel des TACTILLYS-IP mit dem Ethernet-Netzwerk.
7. Verbinden Sie das Stromkabel des TACTILLYS-IP mit einer 12-28 V DC-Stromversorgungsklemme. Das Display des TACTILLYS-IP schaltet sich ein und das TACTILLYS-IP startet.



Wenn der Alarm für den Manipulationsschutz ausgelöst wird, während das TACTILLYS-IP noch nicht an der Wandhalterung befestigt ist, siehe [Abschnitt 4.2.5, „Abstellen des Alarms für den Manipulationsschutz in der Installationsphase des TACTILLYS-IP CUBE“](#).

Es ist auch möglich, die Stromversorgung des TACTILLYS-IP aus- und wieder einzustecken. Dies führt jedoch zu einem Neustart des TACTILLYS-IP (und unterbricht einen eventuell laufenden Einrichtungsvorgang).

4.1.2. Zugriff auf Administratorschnittstelle des TACTILLYS-IP CUBE-Bedienteils und Anzeige seiner Einstellungen

1. Besorgen Sie sich den Netzwerk-Adressierungsplan, um eine verfügbare IP-Adresse für den TACTILLYS-IP CUBE zu finden.
2. Öffnen Sie auf einem tragbaren PC, der mit dem Ethernet-Netzwerk verbunden ist, einen Browser und geben Sie die **Standard-IP-Adresse** des **TACTILLYS-IP CUBE** ein: **172.16.5.240**.

3. Geben Sie den Standard-Login und das Passwort für den Zutritt ein (admin/admin). Der Startseite-Bildschirm (Overview) wird angezeigt. Er enthält Informationen zur Konfiguration des TACTILLYS-IP.


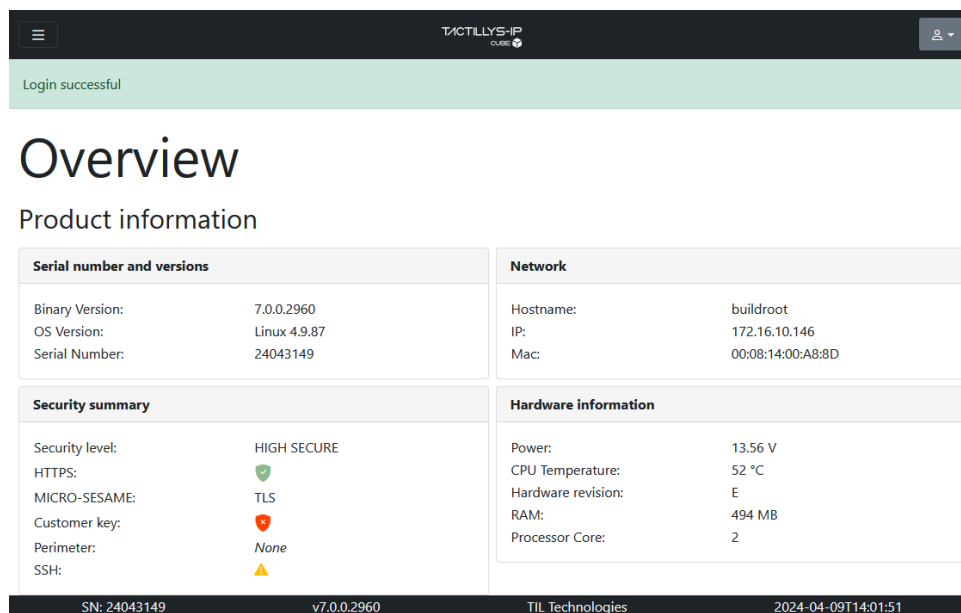
Sie können diesen Bildschirm jederzeit aufrufen, indem Sie auf das TACTILLYS-IP-Logo oben auf dem Bildschirm klicken oder auf das Symbol  burger klicken und dann **System information > Overview** folgen.




Abbildung 4.1. Startseite des TACTILLYS-IP (10010-028)



The screenshot displays the 'Overview' page of the TACTILLYS-IP interface. At the top, a green banner indicates 'Login successful'. Below this, the 'Overview' title is followed by 'Product information'. The page is divided into four main sections: 'Serial number and versions', 'Network', 'Security summary', and 'Hardware information'. A footer bar contains system details like SN, version, manufacturer, and timestamp.

| Serial number and versions | |
|----------------------------|--------------|
| Binary Version: | 7.0.0.2960 |
| OS Version: | Linux 4.9.87 |
| Serial Number: | 24043149 |

| Network | |
|-----------|-------------------|
| Hostname: | buildroot |
| IP: | 172.16.10.146 |
| Mac: | 00:08:14:00:A8:8D |

| Security summary | |
|------------------|---|
| Security level: | HIGH SECURE |
| HTTPS: |  |
| MICRO-SESAME: | TLS |
| Customer key: |  |
| Perimeter: | None |
| SSH: |  |

| Hardware information | |
|----------------------|---------|
| Power: | 13.56 V |
| CPU Temperature: | 52 °C |
| Hardware revision: | E |
| RAM: | 494 MB |
| Processor Core: | 2 |

SN: 24043149 v7.0.0.2960 TIL Technologies 2024-04-09T14:01:51

4.1.3. Passwortänderung für den Administrator des TACTILLYS-IP CUBE-Bedienteils


1. Von der Schnittstelle zum Administrator des TACTILLYS-IP CUBE aus, klicken Sie oben rechts auf dem Bildschirm auf das Symbol  User und folgen Sie den **User settings**.

Abbildung 4.2. Startseite des TACTILLYS-IP CUBE (10010-029)

2. Geben Sie in die beiden Felder **New password** (siehe Abbildung unten) unbedingt ein neues Passwort ein, um das Standardpasswort zu ersetzen (und notieren Sie es an einem sicheren Ort, um seine Sicherheit zu gewährleisten).
3. Klicken Sie auf die Schaltfläche [**Submit**] im linken Bereich des Bildschirms.



Bevor Sie ein neues Passwort wählen, können Sie im Abschnitt rechts auf diesem Bildschirm die Sicherheitsstufe für das Passwort festlegen, die mit der Sicherheitsstufe des Standorts übereinstimmt (Sonderzeichen, Großbuchstaben, Zahlen und Länge des Passworts). Dieser Abschnitt hat eine eigene [**Submit**] - Schaltfläche.


4.1.4. Uhrzeiteinstellung für Bedienteil TACTILLYS-IP CUBE

Die Uhrzeit wird nicht von einem externen NTP-Server verwaltet. Bei einem Neustart oder einer Neukonfiguration wird sie hingegen von der TILLYS in das zugehörige TACTILLYS-IP CUBE-Terminal heruntergeladen.

Sie muss bei der Inbetriebnahme des TACTILLYS IP eingestellt werden, um die Zertifikate zu installieren.

Wenn die Uhren von TACTILLYS-IP und [TILLYS](#) leicht voneinander abweichen, wird die Zeit berücksichtigt, zu der TILLYS die Nachrichten empfängt, oder die Zeit, zu der TILLYS den Standort scharf oder unscharf schaltet.


Bei der Umstellung auf Sommer- oder Winterzeit steuert der TACTILLYS-IP CUBE die Zeitumstellung.

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol  der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Datum & Zeit**.
2. Geben Sie das Datum ein, geben Sie die Uhrzeit ein und klicken Sie dann auf die Schaltfläche [**Submit**]. Das eingegebene Datum und die Uhrzeit werden in der Statusleiste unten rechts auf dem Bildschirm angezeigt.

4.1.5. Netzwerk-Einstellungen für TACTILLYS-IP CUBE


Um Adressenkonflikte beim Hinzufügen mehrerer TACTILLYS-IP CUBEs zu vermeiden und aus Sicherheitsgründen sollte die Standardadresse des TACTILLYS IP nicht beibehalten werden.

Es ist auch möglich, die Netzwerkeinstellungen vom TACTILLYS-IP CUBE Einbruchsterminal aus zu ändern: siehe [Abschnitt 4.2.4, „Auswahl der Netzwerkeinstellungen des TACTILLYS-IP CUBE“](#).


1. Von der Schnittstelle für den Administrator des TACTILLYS-IP CUBE aus klicken Sie auf das Symbol  in der oberen linken Ecke des Bildschirms und folgen Sie **Configuration > Network**.
2. Geben Sie mindestens den Hostnamen (Hostname), die IP-Adresse (IP address), die Subnetzmaske (Subnet mask) und das Gateway (Gateway) ein und klicken Sie dann auf die Schaltfläche **[Submit]**.
3. Auf diesem Bildschirm können Sie im unteren Teil den TCP-Port für den Download (standardmäßig 20300) ändern, falls dieser [Port](#) für andere Anwendungen in Ihrem Netzwerk verwendet wird (im Zweifelsfall wenden Sie sich an den ISSD des Standorts).

4.1.6. Aktualisierung der Firmware für TACTILLYS-IP CUBE

Es ist immer eine gute Idee, die neueste Firmware in den TACTILLYS-IP CUBE zu laden.

1. Laden Sie [im Download-Bereich auf dem Standort des technischen Supports von TIL TECHNOLOGIES](#) die neueste Firmware für das Terminal TACTILLYS-IP CUBE herunter und legen Sie sie auf dem Desktop Ihres Computers ab.
2. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol  der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Firmware Upload**.
3. Klicken Sie auf die Schaltfläche **[Browse]** und wählen Sie auf dem Desktop die Firmwaredatei aus, die auf die TACTILLYS IP **geladen** werden soll, validieren Sie und klicken Sie dann auf die Schaltfläche **[↑ Upload and flash firmware]**. Dieser Vorgang dauert mehrere Minuten, dann wird TACTILLYS-IP neu gestartet.

4.1.7. Einrichten der Ereignisprotokollierung für TACTILLYS-IP CUBE

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol  der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Log tracer**.
2. Um das Protokoll an eine bestimmte IP-Adresse zu senden, geben Sie diese IP-Adresse und den Zielport (standardmäßig 514) ein, klicken Sie auf den Syslog-Schalter (grau > blau) und klicken Sie dann auf die Schaltfläche **[Submit]**.


Um das Protokoll in einer Datei zu speichern, klicken Sie auf den Syslog-Schalter (grau > blau) und dann auf die Schaltfläche **[Submit]**.

Es ist möglich, beide Schalter zu aktivieren.

3. Wählen Sie die Detailstufe für die 7 Spurentypen aus und klicken Sie auf die Schaltfläche [**Submit**].

4.1.8. Desetzen des TACTILLYS-IP CUBE

Bei dieser Wartung werden die standortspezifischen Schlüssel aus einem TACTILLYS-IP CUBE gelöscht. Sie sollte nur durchgeführt werden, wenn ein TACTILLYS-IP CUBE aus einer Installation entfernt wird, um ihn in einer anderen zu installieren, oder bevor er an die TIL TECHNOLOGIES SAV geschickt wird (auf Anfrage der Abteilung Kundenservice).

1. Klicken Sie in der Schnittstelle für Administratoren des TACTILLYS-IP CUBE auf das Symbol  in der oberen linken Ecke des Bildschirms und folgen Sie **Wartung > Erase keys**.
2. Klicken Sie auf die Schaltfläche [**Erase keys**].

4.2. Parametrierung des TACTILLYS-IP CUBE

Diese Operationen werden auf dem Terminal TACTILLYS-IP CUBE von **Benutzern mit Einbruch-Rechten** durchgeführt.

Der Benutzer mit Einbruch-Rechten hält einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE Einbruch-Terminals.

Je nach Konfiguration muss er vielleicht zusätzlich einen Code eingeben (siehe [Abschnitt 3.2.2.3, „Auswahl des Modus für die Authentifizierung \(Ausweis oder Ausweis + Code\) an einem TACTILLYS-IP CUBE“](#)).

4.2.1. Authentifizierung und Navigation am TACTILLYS-IP CUBE-Bedienteil


Um auf die Startseite des TACTILLYS-IP CUBE zugreifen zu können, muss ein Ausweis verwendet werden, der vom System zur Erkennung von Einbrüchen erkannt wird: siehe [Abschnitt 5.2, „Verfahren zur Vorbereitung eines CUBE Ausweises zur Verwaltung von Einbrüchen auf einem TACTILLYS-IP CUBE Terminal“](#).

1. Im Standby-Modus wird auf dem TACTILLYS-IP CUBE-Terminal die Nachricht "Halten Sie Ihren Ausweis an das Lesegerät" angezeigt.
2. Halten Sie einen Ausweis vor das Lesegerät (und geben Sie ggf. den Zugangscode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.

Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf diesem Bildschirm.

Tabelle 4.1. Bedeutung der Piktogramme auf dem Bildschirm der Gruppenliste auf dem Terminal TACTILLYS-IP CUBE



| Piktogramm | Bedeutung |
|---|--|
|  | Uhrzeit der nächsten Scharfschaltung |
|  | Zutrittsverzug oder Austrittsverzug |
|  | 1 = Ausnahmegenehmigung läuft |
|  | 1 = Voralarm läuft |
|  | Scharfgeschaltete Gruppe |
|  | Unscharfgeschaltete Gruppe |
|  | Anzeige der Gruppendetails (grünes Piktogramm) |
|  | Zur Scharfschaltung bereit |
|  | Zur Scharfschaltung nicht bereit |
|  | Anzeige der Übersicht über Alarmer |

3. Berühren Sie das grüne Piktogramm  Lupe.

Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf dem Bildschirm mit den Details einer Gruppe.

Tabelle 4.2. Bedeutung der Piktogramme der Melder auf dem Terminal TACTILLYS-IP CUBE



| Piktogramme an den Meldern | Bedeutung |
|---|---|
|  | Maskierenstatus (orange = maskiert) |
|  | Sperrung (orange = gehemmt) |
|  | Zutrittsverzug oder Austrittsverzug (orange = Verzögerungszeit läuft) |

| Piktogramme an den Meldern | Bedeutung |
|---|---|
|  | 1 = Ausnahmegenehmigung läuft |
|  | Alarmzustand (orange = Alarm, rot = Selbstschutz) |

4. Berühren Sie die Schaltfläche [**Sirenen**].

Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf dem Display der Sirenen.

Tabelle 4.3. Bedeutung der Sirenenpiktogramme auf dem Terminal TACTILLYS-IP CUBE



| Piktogramme auf dem Sirenenbildschirm | Bedeutung |
|--|-------------------------------------|
|  | Alarm-Status (orange = Alarm aktiv) |
|  | Sperrung (orange = gehehmt) |

5. Um den Bildschirm mit den Meldern wieder anzuzeigen, berühren Sie die Schaltfläche [**Melder**].


Um den Startseite-Bildschirm wieder anzuzeigen, berühren Sie die Schaltfläche [**#**], unten links auf dem Bildschirm.

Die folgende Tabelle zeigt die Bedeutung der Piktogramme auf dem Bildschirm "Maskieren", der angezeigt wird, wenn ein Melder einen Fehler aufweist.

Tabelle 4.4. Bedeutung der Piktogramme für den Auswurf eines Melders auf dem Terminal TACTILLYS-IP CUBE


| Piktogramme auf dem Auswurf-Bildschirm | Bedeutung |
|---|---|
|  | Maksierenstatus (orange = maksiert) |
|  | Anzeige des aktuellen Fehlerstatus (orange = Alarm, rot = Sabotageschutz) |

4.2.2. Abfrage der Betriebseinstellungen von TACTILLYS-IP CUBE

Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  burger in der oberen linken Ecke des Bildschirms und dann auf die Option **Über**.

Die Betriebsmerkmale des TACTILLYS-IP CUBE werden angezeigt.


4.2.3. Parametrierung des TACTILLYS-IP CUBE

Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  in der oberen linken Ecke des Bildschirms und dann auf die Option **Einstellungen**.

Die Helligkeit des Bildschirms ist einstellbar, ebenso wie die Lautstärke.


Es gibt 4 Themen und die Schnittstelle ist auf Deutsch, Englisch und Französisch verfügbar. Die neuen Einstellungen werden übernommen, ohne dass eine Validierung oder ein Neustart erforderlich ist.

4.2.4. Auswahl der Netzwerkeinstellungen des TACTILLYS-IP CUBE

1. Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  in der oberen linken Ecke des Bildschirms und dann auf die Option **Netzwerk**.
2. Ändern Sie die Informationen und berühren Sie dann die Schaltfläche [**Speichern**].


4.2.5. Abstellen des Alarms für den Sabotageschutz in der Installationsphase des TACTILLYS-IP CUBE

Während der Einrichtungsphase, in der das Einbruchsterminal noch nicht in seiner Halterung befestigt ist und einen Alarm zum Sabotageschutz auslösen kann, ist es möglich, den Positionssensor zurückzusetzen (wodurch auch der Alarm gestoppt wird).

1. Tippen Sie auf der Startseite des TACTILLYS-IP CUBE auf das Symbol  in der oberen linken Ecke des Bildschirms und dann auf die Option **Einstellungen**.
2. Zeigen Sie den unteren Teil dieses Bildschirms an, indem Sie mit dem Finger nach unten scrollen, und berühren Sie dann rechts neben der Option **Position** die Schaltfläche [**Neu kalibrieren**].

4.2.6. Automatisches Abmelden des TACTILLYS-IP CUBE

Die Zeitverzögerung für den Übergang in den Standby-Modus kann auf dem Bildschirm **Einstellungen** des TACTILLYS-IP CUBE eingestellt werden.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittscode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt.
2. Tippe auf das Symbol  in der oberen linken Ecke des Bildschirms und dann auf die Option **Einstellungen**.
3. Wählen Sie den gewünschten Wert in der Drop-Down-Menüleiste **Standby** aus.

4.3. Verwendung des TACTILLYS-IP CUBE

Je nach Konfiguration und Komplexität der Standorte werden ein oder mehrere TACTILLYS-IP CUBE-Terminals installiert (siehe [Abschnitt 1.2, „Überblick über die Multi-TILLYS-Version des CUBE Einbruchs“](#)).

4.3.1. Manuelle Scharf- oder Unscharfschaltung einer Gruppe

Die Scharfschaltung einer Gruppe erfolgt normalerweise zu der eingestellten Zeit. Bei einem Fehler an einem Melder, dessen automatischer Auswurf nicht vorgesehen ist, kann die Gruppe nicht scharf geschaltet werden.

Wenn ein Mitarbeiter am Wochenende kurz auf das Firmengelände zurückkehren muss, kann er den Alarm vorübergehend unscharf schalten. Es ist möglich, dass diese sich automatisch wieder scharf stellt, damit sie nicht vergessen wird und das Gebäude für den Rest des Wochenendes unbewacht bleibt.



Wenn ein Alarm ausgelöst wird, wird ein Sicherheitsbeamter den Melder überprüfen. Wenn es sich um eine technische Fehlfunktion handelt, kann er anschließend das manuelle Maskieren des fehlerhaften Melders vornehmen, bevor er die Scharfschaltung der Gruppe erneut startet (siehe [Abschnitt 4.3.2, „Manueller Auswurf von fehlerhaften Meldern“](#)).

Das Scharf- und Unscharfschalten ist über MICROSESAME in der Übersicht (siehe [Abschnitt 5.5, „bersicht auf MICROSESAME ansehen“](#)) oder über das Terminal TACTILLYS-IP CUBE möglich.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittscode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.
2. Berühren Sie die Gruppe, die Sie scharf/unscharf schalten möchten, und dann die Schaltfläche [**Scharf**] oder [**Unscharf**].

4.3.2. Manuelles Maskieren von fehlerhaften Meldern



Ein fehlerhafter Melder, dessen automatischer Auswurf nicht vorgesehen ist, kann in der Übersicht (siehe [Abschnitt 5.5, „Übersicht auf MICROSESAME ansehen“](#)) oder am TACTILLYS-IP CUBE Terminal ausgeworfen werden.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittscode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.
2. Tippe auf das Symbol  in der oberen linken Ecke des Bildschirms und dann auf die Option **Auswerfen**.
3. Berühren Sie den fehlerhaften Melder (Piktogramm  orange oder rot) und dann die Taste [**Auswerfen**].

4.3.3. Sirenen ausschalten

Eine Sirene kann in der Übersicht (siehe [Abschnitt 5.5, „Übersicht auf MICROSESAME ansehen“](#)) oder am TACTILLYS-IP CUBE Terminal gestoppt werden.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittscode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.

2. Berühren Sie das grüne Piktogramm  Lupe der Gruppe mit der Sirene, die Sie abschalten möchten.
3. Berühren Sie die klingelnde Sirene (Piktogramm  orange oder rot) und dann die Taste [**Sirenenstopp**].

4.3.4. Überschreiben der Scharfschaltung auf Meldergruppe(n)

Die Scharfschaltung einer Gruppe kann so programmiert werden, dass sie automatisch zu einer bestimmten Uhrzeit erfolgt. Allerdings kann es vorkommen, dass die Nutzer nach der Überwachungszeit noch vor Ort bleiben müssen, sodass sie die Überwachungszeit um die Zeit verschieben müssen, die sie benötigen.

Aus Sicherheitsgründen kann diese Zeit jedoch begrenzt werden, z. B. durch den Sicherheitsbeauftragten.

Wenn der [Voralarm](#) ertönt, müssen die Personen, die sich noch in den Räumlichkeiten befinden, diese vor Ablauf der Ausgehzeit verlassen oder sich, falls sie dazu berechtigt sind, am Terminal TACTILLYS-IP CUBE identifizieren und eine Ausnahmegenehmigung beantragen.

1. Halten Sie einen Ausweis vor das Lesegerät des TACTILLYS-IP CUBE (und geben Sie ggf. den Zutrittscode ein und validieren Sie ihn): Der Startseite-Bildschirm wird angezeigt. Dieser Bildschirm listet die Gruppen auf, die an diesem Terminal verwaltet werden.
2. Berühren Sie die Gruppe, für die Sie eine Ausnahme beantragen möchten, und dann die Schaltfläche [**Überschreiben**].
3. Wählen Sie die Dauer der Überschreibung und validieren Sie.

Kapitel 5. Konfiguration und Nutzung von CUBE Einbruch

Diese werden vom **Sicherheitsbeauftragten** durchgeführt.

5.1. Importieren der CUBE Einbruch-Konfiguration in MICROSESAME

Im Falle einer Multi-TILLYS-Konfiguration müssen alle [TILLYS](#)(LVE) in [MICROSESAME](#) bekannt sein. Daher ist ein vollständiger Download erforderlich.

1. In der Startseite von MICROSESAME folgen Sie **Einstellungen > Hardware > Lokale Verarbeitungseinheit [LVE]**.
2. Doppelklicken Sie auf den Namen des TILLYS, dessen Einstellungen importiert werden sollen.

Abbildung 5.1. Vorbereiten des Imports der Einbruch-Konfiguration eines TILLYS in MICROSESAME (10010-038)

3. Geben Sie den Namen und das Passwort ein (1), überprüfen Sie die Sicherheitsstufe (2) und klicken Sie auf die Schaltfläche **[+ Fügen Sie eine Funktion hinzu]** (3).
4. Klicken Sie in der Drop-Down-Menüleiste auf **Einbruch CUBE**.
5. Klicken Sie auf der rechten Seite des Bildschirms auf die Schaltfläche **[CUBE Einbruch-Konfiguration importieren]**.

5.2. Verfahren zur Vorbereitung eines CUBE Ausweises zur Verwaltung von Einbrüchen an einem TACTILLYS-IP CUBE Bedienteil

Ein Partner von TIL Technologies, ein Empfangsmitarbeiter oder ein Sicherheitsbeauftragter bereitet einen Ausweis für den Zutritt zum TACTILLYS-IP CUBE Bedienteil in MICROSESAME vor, indem er die in den folgenden Abschnitten beschriebenen Schritte ausführt.

5.2.1. Vorbereitung eines Ausweises zur Kontrolle gegen Einbrüche

Die Erfassung eines ID-Mittels in MICROSESAME im Schritt [Section 5.2.2, « Erwerb eines nicht zugewiesenen ID-Mittels in MICROSESAME »](#) erfolgt, indem ein Ausweis an einem Lesegerät zur Zutrittskontrolle vorbeigeführt wird.



Das im Terminal TACTILLYS-IP CUBE integrierte Lesegerät ist kein Lesegerät für die Zutrittskontrolle, sondern ein Lesegerät für die Einbruchserkennung.

5.2.2. Übernahme eines nicht zugewiesenen ID-Mittels in MICROSESAME


1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Überwachung > Ereignismonitor [MON]**.
2. Einen nicht zugewiesenen Ausweis vor das Lesegerät für die Zutrittskontrolle halten. Ein akustisches Signal zeigt an, dass das Lesegerät funktioniert, aber der Zutritt ist abgelehnter Zutritt, da der Ausweis unbekannt ist (er wurde noch nicht zugewiesen).


Sein ID-Mittel wurde von MICROSESAME erworben (es ist im Ereignismonitor sichtbar) und steht für einen neuen Benutzer zur Verfügung.

Wenn das Lesegerät kein akustisches/visuelles Signal ausgibt, wenden Sie sich unter Fehlerbehebung zu den Fehler 00003.

3. Klicken Sie auf das Symbol **[Details]** in der linken oberen Ecke des Bildschirms. Die Details des Ausweises werden im rechten Fenster angezeigt.
4. Rechts neben dem Ort des Fotos markieren Sie die ID-Mittel mit der Maus und geben Sie **STRG + C** ein. Die ID-Mittel wird in den Speicher kopiert: weiter [Section 5.2.3, « Zuweisung eines verfügbaren ID-Mittels an einen neuen Benutzer »](#).

5.2.3. Zuweisung eines verfügbaren ID-Mittels an einen neuen Benutzer



1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Klicken Sie oben links auf  **Hinzufügen**, geben Sie den Vor- und Nachnamen des neuen Users ein und klicken Sie dann auf **Erstellen**.
3. Klicken Sie auf **ID-Mittel**, machen Sie **einen** Rechtsklick im unteren Bildschirmbereich und klicken Sie auf **ID-Mittel erstellen**.

4. Tippen Sie **CRTL + V** ein. Die kopierteID-Mittel (siehe [Section 5.2.2, « Erwerb eines nicht zugewiesenen ID-Mittels in MICROSESAME »](#)) wird in die Spalte Code eingefügt.
5. Geben Sie ein Start- und Enddatum für die Gültigkeit ein und klicken Sie auf Enter.
6. Klicken Sie auf **Speichern** : Das Hochladen dieser Informationen in den TILLYS wird durchgeführt.
7. Gehen Sie im Hauptmenü auf **Nutzung > Überwachung > Ereignismonitor [ERE]** (Anzeige des **Ereignismonitors**) und halten Sie den Ausweis vor das Lesegerät.

Der Ausweis ist nun mit dem Namen der Person verknüpft, die Sie eingegeben haben, aber sein Zustand ist immer noch abgelehnter Zutritt (kein Zugriff auf das Lesegerät), und das ist völlig normal, da er noch nicht mit Zugriffsrechten verknüpft ist.

Er besitzt auch kein CUBE Einbruchsprofil, das ihm den Zugriff auf ein TACTILLYS-IP CUBE Terminal ermöglicht.


5.2.4. Zuweisung von Berechtigungen an einen neuen Benutzer


1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Suchen Sie nach dem zuvor erstelltenUser.
3. Klicken Sie in seiner Datei auf **Zutritt**.
4. Im unteren rechten Bereich klicken Sie auf .
5. Klicken Sie in der sich öffnenden Liste auf **Alle aktuellen und zukünftigen Standorte**.
6. Klicken Sie im daraufhin angezeigten Fenster für die Zugriffseinstellungen auf **OK** (Validierung des 24-Stunden-Zugriffs).
7. Klicken Sie auf **Speichern** .
8. Rufen Sie den **Ereignismonitor** auf (im Hauptmenü unter **Betrieb > Überwachung > Ereignismonitor [ERE]**), halten Sie den Ausweis vor jedes zuvor zugewiesene Lesegerät und überprüfen Sie, dass der Benutzer nicht nur erkannt wird, sondern dass ihm nun auch der Zugang gewährt wird.

5.2.5. Einem neuen Benutzer ein CUBE Einbruchsprofil zuweisen

Die Benutzer, die mit der Verwaltung eines TACTILLYS-IP CUBE-Terminals beauftragt sind, müssen mindestens über das Einbruchsprofil verfügen, das diesem Terminal entspricht.

Sie müssen auch über Zutrittsrechte zum Gebäude an den Lesegeräten für die Zutrittskontrolle verfügen.

1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Suchen Sie nach dem zuvor erstelltenUser.
3. Klicken Sie in seiner Datei auf **Zutritt**.
4. Im unteren rechten Bereich klicken Sie auf .

5. Klicken Sie auf das Burger-Menü in der Mitte der rechten Bildschirmhälfte und markieren Sie dann das Kontrollkästchen CUBE Einbruchsprofile anzeigen.
6. Klicken Sie im rechten Abschnitt auf das Einbruchsprofil. Klicken Sie auf den Pfeil <, um dieses Profil in den linken Abschnitt des Bildschirms zu verschieben.
7. Weisen Sie auf die gleiche Weise die Zutrittsrechte zum Gebäude zu, die dieser ID-Mittel benötigt.
8. Klicken Sie auf **Speichern** .
9. Im Hauptmenü folgen Sie **Einstellungen > Hardware > Lokale Verarbeitungseinheiten [LVE]**.
10. Doppelklicken Sie auf die Linie der TILLYS(LVE), die mit der TACTILLYS verbunden ist.
11. Klicken Sie auf die Schaltfläche , dann auf die Schaltfläche .
12. Markieren Sie das Feld Zutritt und klicken Sie auf die Schaltfläche [**Ausführen**] .

5.3. Verwaltung der Einbruchsprofile der Benutzer auf MICROSESAME oder WEBSesame

Einbruchsprofile können zu den Zutrittsprofilen der Benutzer hinzugefügt werden.

Sie können auch durch das Importieren von CSV-Dateien im richtigen Format verwaltet werden, die von den Personalabteilungen gemäß den von der Organisation, die das Anti-Einbruch-System verwendet, eingerichteten Prozessen vorbereitet wurden.

Siehe [Abschnitt 3.2.2.1, „Erstellen von Einbruchsprofilen auf der Host-TILLYS“](#).

5.4. Einrichten der Übersicht auf MICROSESAME

Ähnlich wie Tür-Objekte die Zutrittskontrolle durch ihre grafische Darstellung vereinfachen, vereinfachen Überwachungsobjekte das Management von Einbrüchen.

1. In der Startseite von MICROSESAME folgen Sie **Einstellungen > Überwachung > Übersichtseditor [EDI]**.
2. Ziehen Sie die Einbruch-Objekte (Melder, Sirenen, TILLYS) aus dem rechten Fenster in den mittleren Bereich an die gewünschte Stelle auf der Grafik oder fotografischen Darstellung des Standorts.
3. Für jedes dieser Objekte kann man auf die drei übereinander liegenden Punkte (rechts oben in jedem Objekt) klicken, um Optionen anzuzeigen. Um die Ereignisse eines Einbruch-Objekts zu erhalten, markiere dessen **Verlaufsfeld**.

Weitere Informationen finden Sie im Abschnitt über den Übersichtseditor im [MICROSESAME-Referenzhandbuch](#).

4. Speichern Sie die Konfiguration.

5.5. Übersicht auf MICROSESAME ansehen

Siehe den Abschnitt über die Anzeige von Übersichten im [MICROSESAME-Referenzhandbuch](#).


5.6. Erklärung der Operators für die Erkennung von Einbrüchen auf der TILLYS

Sobald die Einbruchprofile definiert und diese Konfiguration auf MICROSESAME geladen wurde, können Sie den Personen, die die Scharf- und Unscharfschaltung des Alarms auf dem TACTILLYS-IP CUBE-Terminal verwalten sollen, ein Einbruchprofil zuweisen.

Siehe [Abschnitt 5.3, „Verwaltung der Einbruchprofile der Benutzer auf MICROSESAME oder WEBSESAME“](#).

5.7. Test der Anlage zur Erkennung von Einbrüchen

5.7.1. Testen von Meldepunkten

1. Klicken Sie auf das Symbol  in der oberen linken Ecke des TILLYS-Host-Bildschirms und folgen Sie **Einbruch CUBE > Detector diagnostic**.
2. Bewegen Sie sich in allen Räumen des Gebäudes, in denen ein Melder installiert ist (der Alarm wird nicht ausgelöst).
3. Überprüfen Sie im Ereignisticker, ob alle Melder reagiert haben.
4. Den Modus Detector diagnostic deaktivieren.

5.7.2. Test der Kommunikation zwischen TILLYS und dem TACTILLYS-IP CUBE

Wenn die Verbindung zwischen dem TILLYS und dem Terminal TACTILLYS-IP CUBE funktioniert, aktiviert das Auflegen eines Ausweises mit Einbruchfunktion auf das Lesegerät des Terminals TACTILLYS-IP CUBE dessen Startseite (oder dessen Codeeingabebildschirm).


Kapitel 6. Sicherheitsmanagement durch den Sicherheitsbeauftragten

6.1. Zuweisung von Zugriffsrechten an die Benutzer des TACTILLYS-IP CUBE

Dieser Abschnitt schlägt lediglich eine alternative Formulierung vor: siehe [Section 5.2.5, « Einem neuen Benutzer ein CUBE Einbruchprofil zuweisen »](#) oben.

6.2. Änderung des ID-Mittels für Einbruch, das bei der Ausweis- und Code-Identifikation auf TACTILLYS-IP CUBE verwendet wird.

Die Änderung des ID-Mittels wird in MICROSESAME vorgenommen. Darauf folgt ein manueller Download in die TILLYS.

1. Im Hauptmenü von MICROSESAME folgen Sie **Nutzung > Zutrittskontrolle > Users [USE]**.
2. Klicken Sie auf den Reiter Zugang, wählen Sie das Zutrittsprofil aus und klicken Sie auf die Schaltfläche **[ID-Mittel]**.
3. Scrollen Sie nach unten und sehen Sie sich den vorhandenen Code an oder geben Sie einen neuen Code ein und klicken Sie dann auf  Speichern.
4. Zur Auswahl des Modus für die Authentifizierung siehe [Abschnitt 3.2.2.3, „Auswahl des Modus für die Authentifizierung \(Ausweis oder Ausweis + Code\) an einem TACTILLYS-IP CUBE“](#).

6.3. Abfrage des Verlaufs von Einbrüchen

MICROSESAME- oder WEBSesame-Operatoren loggen sich in die webbasierte Schnittstelle des Host-TILLYS ein.

Kapitel 7. Schritte im Zusammenhang mit dem Einbruch, die vom Fernüberwachungsleitstelle durchgeführt werden

7.1. Abfrage der aktuellen Alarme

Der Fernüberwachungsmonitor kann die Details der aktuellen Alarme auf seinem Terminal einsehen.

Die Informationen, die er erhält, ermöglichen es ihm auch, das reibungslose Funktionieren der Verbindung zu überwachen (siehe [Abschnitt 7.1.1, „Syntax von Polling-Nachrichten“](#) und [Abschnitt 7.1.2, „Syntax der Nachrichten zum zyklischen Test“](#)).

7.1.1. Syntax von Polling-Nachrichten

[Polling](#) ist eine Testnachricht, die von TILLYS alle paar Sekunden gesendet wird, um zu überprüfen, ob die IP-Übertragungsfunktion zwischen TILLYS und dem Fernüberwachungs-Frontend ordnungsgemäß funktioniert. Er wird dann an den Fernüberwachungsmonitor weitergeleitet.

Beispiel für eine Polling-Nachricht

```
E99B0013 "NULL" 0004L0#7005 [ ]
```

Diese Testnachricht enthält eine Nachricht vom Typ "NULL", die keine Daten enthält.

Informationen zum Aktivieren und Konfigurieren von Polling finden Sie unter [Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“](#).

7.1.2. Syntax der Nachrichten zum zyklischen Test

Der zyklische Test ist eine Testnachricht, die von der TILLYS gesendet wird, um zu überprüfen, ob die IP-basierte Übertragungsfunktion zwischen der TILLYS und jedem Fernüberwachungsmonitor ordnungsgemäß funktioniert. Er wird z. B. alle 3 Stunden (180 Minuten) aktiviert.

Beispiel für eine Nachricht über einen zyklischen Test

```
4558001F "SIA-DCS" 0001L0#7005 [ #7005 |NRP ]
```

In dieser Nachricht steht N für neu und RP für den Ereigniscode, der den zyklischen Test bezeichnet.

Informationen zum Aktivieren und Konfigurieren des zyklischen Tests finden Sie unter [Abschnitt 3.2.1.11, „Konfigurieren von Fernüberwachungsmonitoren“](#).

7.2. Fernbefehl bei CUBE Einbruch

Zusätzlich zum Telefonanruf des Standorts, der Polizei oder der Feuerwehr kann der Fernüberwachungsmonitor die unten aufgeführten Aktionen durchführen.

7.2.1. Scharfchaltung

Dies ist zwar möglich, kommt aber praktisch nie vor, da es schwierig ist, aus der Ferne zu überprüfen, ob die Räume leer sind.

7.2.2. Sirenenstopp

Der Fernüberwachungsmonitor kann die Sirenen ausschalten, nachdem er die Alarme quittiert hat.

7.2.3. Unscharfschaltung

Der Fernüberwachungsmonitor kann eine Gruppe bei Bedarf aus der Ferne entschärfen.

7.2.4. Änderung des Wertes eines Registers der TILLYS

Diese Funktion ist nur verfügbar, wenn das Frontend des Fernüberwachungsmonitors und die Überwachungssoftware des Fernüberwachungsmonitors mit dieser Änderung des Registers kompatibel sind.