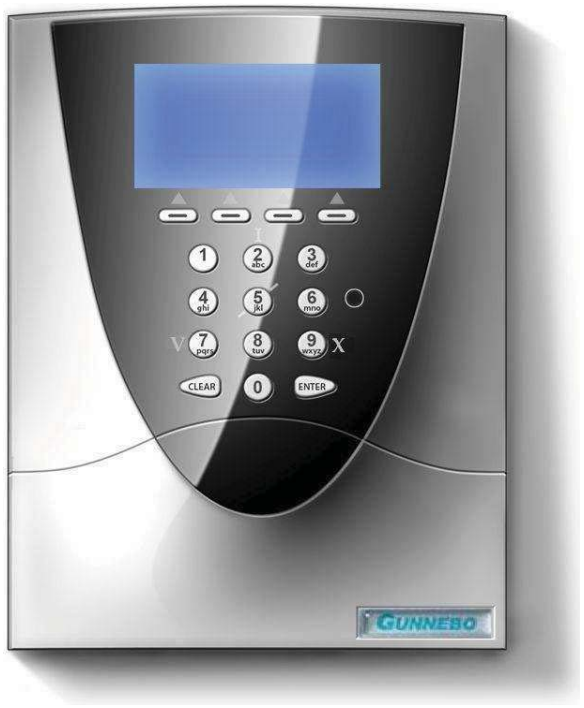
CLAVIS®

Der Schlüssel für Ihren Wertschutz

VdS •ISO 9001 •Service-Unternehmen für Wertbehältnisse



SafeLock GSL 1000 Schloss

Benutzerhandbuch

A0U391G

Kundendienst

CLAVIS Deutschland GmbH
Grüner Weg 38
34117 Kassel

Telefon: +49 (0)561 988 499-0
E-Mail: info@tresore.eu
Internet: www.tresore.eu
www.tresorschloss.de

GUNNEBO
For a safer world®

GSL1000 Benutzerhandbuch

Datum	Version	Beschreibung der Änderung	Autor
01/12/2008	01	Erste Version	
02/02/2009	02	Word-Format	G. LOEHLE
17/02/2009	03	Fehler in Standardcode	G. LOEHLE
31/03/2009	04	Implementierung der Änderungen von Rob Suddaby	L. Loiseau
20/05/2009	05	Änderung der Werksparameter	G. LOEHLE
16/06/2009	06	Einsetzen der Batterien	G. LOEHLE
11/01/2010	07	Funktion USB download /upload + Vorgabe I/O Zustand.	G. LOEHLE

Liste der mit dem Projekt oder Prozess verknüpften Dokumente

(*) : C = in der Erstellung, D = gelöscht, E = bearbeitet, -- = keine Änderung

(*)	Referenz	Vers.	Typ: Titel
			- Benutzerhandbuch

Bearbeitet von Leiter des After Sales Service Name, Vorname: Datum und Unterschrift:	Genehmigt vom Product Technical Mgr or Project Engineer Name, Vorname: Datum und Untschrift:
Anwendbar ab:	

SafeLock GSL Schloss – Benutzerhandbuch
A0U391G – 100025747 – Ausg. 07 – NEX – Juni 2010

SCHUTZ DER UMWELT

Gemäß der Richtlinie 2002/96/EG über Elektro- und Elektronik-Altgeräte muss dieses Produkt am Ende seiner Lebensdauer getrennt vom Hausmüll entsorgt werden.

Dies ist zum Schutz der Umwelt erforderlich.

Die Verpackung des Produkts ist vollständig recycelbar.

Kundendienst

CLAVIS Deutschland GmbH
Grüner Weg 38
34117 Kassel

Telefon: +49 (0)561 988 499-0
E-Mail: info@tresore.eu
Internet: www.tresore.eu
www.tresorschloss.de

GUNNEBO
For a safer world®

Inhaltsverzeichnis

1 Einleitung

In diesem Handbuch werden die Bedienung und die Verwendung des Schlosses beschrieben. Mithilfe dieses Schlosses können Sie Ihr Eigentum angemessen schützen. Eine Eingabeeinheit (IU) steuert 1 bis 16 Betätigungen (SU).

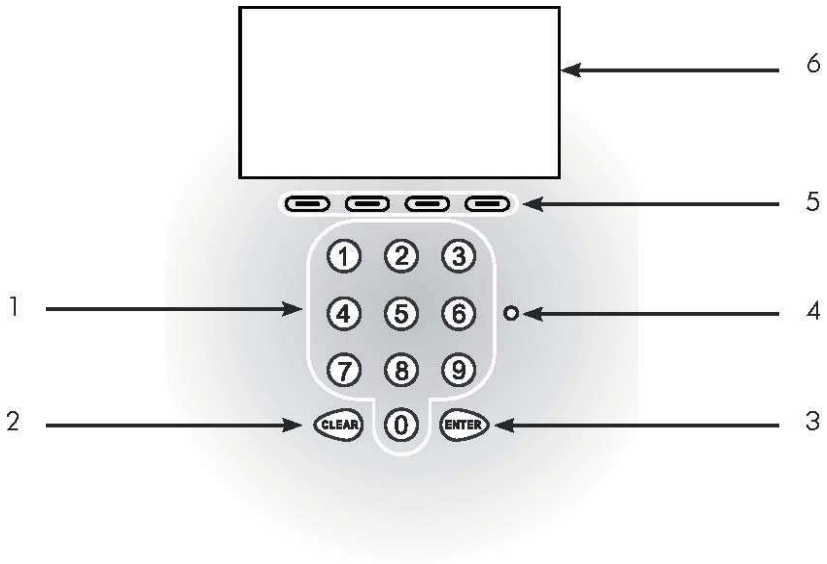
1.1 Symbole in der vorliegenden Anleitung

Achtung:
Ein Achtung-Symbol vor einem Hinweis weist auf besonders wichtige Informationen hin. Lesen Sie die Anweisungen aufmerksam durch, bevor Sie sie umsetzen.

Information:
Wichtige Empfehlungen und Informationen zur Bedienung.

2 Produktbeschreibung

2.1 Eingabeeinheit (IU)



- 1 – Tastenfeld.
- 2 – Taste „Clear“: Löschen der Codeeingabe und Verriegeln des Geräts (abhängig von der Konfiguration).
- 3 – Taste „Enter“: Bestätigen einer Aktion.
- 4 – Anzeige-LEDs: zweifarbige LEDs (rot/grün).
- 5 – kontextabhängige Tasten: Die Funktion der einzelnen Tasten wird in der Anzeige über der Taste beschrieben.
- 6 – Digitale Anzeige.

2.2 Digitale Anzeige

2.2.1 Anzeigebereiche

- 1. Uhr und Symbol für die Stromversorgung: in allen Anzeigen aktiviert.
- 2. Aktiver Bildschirmbereich.
- 3. Navigationstasten: je nach Menü aktiviert oder deaktiviert. Die kontextabhängigen Tasten ändern sich entsprechend den jeweiligen Menüs (Menü, Nach links, Nach rechts, Nach oben, Nach unten, Info, Val ...).
- 4. Kontextabhängige Symbole: je nach Schloss-Zustand aktiviert oder deaktiviert.

Das ausgewählte Schloss wird invers dargestellt.

2.2.2 Zustandssymbole

	Uhr
	Anzeige von Batteriebetrieb und niedrigem Ladestand
	Externe Stromversorgung
	Aktive Zeitsperre
	Alarm nicht quittiert/Alarmmeldung. Dieses Symbol wird nach einem korrekten Öffnungsvorgang gelöscht.
	Falscher Code

2.2.3 Menüsymbole

	Schließvorrichtung geschlossen
	Schließvorrichtung offen
	Schließvorrichtung mit aktiver Verzögerung
	Fingerabdruck
	Einfacher Zugriff
	Vier-Augen-Zugriff (Dual-Modus)
	Erneute Identifizierung nach Verzögerung
	Achtung
	Einmal-Code (OTC)

2.2.4 Kontextabhängige Taste

	Menü
	Nach links
	Nach rechts
	Nach oben
	Nach unten
	Info
	Zurück zum vorherigen Bildschirm

2.3 Akustische Signale

Jeder Bedienungsschritt wird mit einem bestimmten akustischen Signal bestätigt.
Das Schloss ist mit einem akustischen System ausgestattet, das verschiedene Signale ausgibt:

- Signal für positives Ereignis.
- Signal für negatives Ereignis.
- Alarmsignal.
- Signal für Tastenfeldeingabe.

3 Verwenden des Schlosses

3.1 Benutzerkategorien

Die Benutzer werden in drei Kategorien eingeteilt:

- Super Manager:
  Es gibt zwei Super Manager. Dem Super Manager unterstehen die Manager. Jeder Super Manager kann den Code eines anderen Super Managers in der Eingabeeinheit ändern.
- Manager:
  Den Managern unterstehen die Benutzer.
- Benutzer:
  In der Standardkonfiguration kann jeder Benutzer seinen Code oder den Code seines Unterbenutzers ändern.

3.2 Festlegen der Identifizierung

Ein korrekter Code kann 7 bis 10 Ziffern umfassen (2 Ziffern für die Benutzernummer und 5 bis 8 Ziffern für den PIN-Code). Für die Definition des Codes stehen zwei Möglichkeiten zur Verfügung:

1. Benutzernummer + PIN-Code (Standardkonfiguration).
2. PIN-Code + Benutzernummer (Werkseinstellung).

Die Definition des Codes muss vor der Installation erfolgen.
Die Codedefinition kann nur im Werk geändert werden.

Die Benutzernummern für Super Manager sind immer 01 und 02. Die Standardcodes ab Werk für Super Manager sind 01000000 und 02000000.

Die folgenden Identifizierungsarten sind verfügbar:

Nur Code
☞ Geben Sie Ihren Code ein, und drücken Sie die Taste „Enter“.

Code + Fingerprint (optional)
☞ Geben Sie Ihren Code ein, und drücken Sie die Taste „Enter“. Wenn der Code bestätigt wird, wird die Registrierung des Fingerabdrucks verlangt.

Nur Fingerprint (optional)
☞ Drücken Sie die Taste „Enter“, und drücken Sie Ihren Finger auf den Fingerabdrucksensor.

Wenn das Schloss nur für die Identifizierung durch Fingerabdruck konfiguriert wird, verliert es seine Sicherheitsklasse.

3.3 Öffnungsvorgang

☞Schloss auswählen + ENTER

☞Code eingeben + ENTER

Warten.

Bei erneuter Identifizierung nach Verzögerung:
☞ Code nochmals eingeben.

Die Betätigung ist entriegelt.

3.4 Schließungsvorgang

Automatisch: Wenn der Riegelwerkschalter angeschlossen ist, wird das Schloss automatisch gesichert, und das Riegelwerk wird vorgeschlossen.
Manuell: Durch Drücken der Taste „Clear“ wird das Schloss automatisch gesichert.

3.5 Sperre in Notfällen

Drücken Sie in Notfällen die Tasten 7+9, um die Tür zu sichern und für die Dauer von 30 Minuten (einstellbar von 1 bis 99 Minuten) das Öffnen zu verhindern.

Es ist nicht möglich, die Sperrtasten für Notfälle zu ändern.

3.6 Zugriffsmeldungen

Meldung	Ursache	Maßnahme
Stromversorgung!	Stromausfall.	Drücken Sie die Taste „Enter“ oder „Clear“, um zum Bildschirm „Home“ zurückzukehren.
Keine Berechtigung	Der Zugriff wird für den Benutzer verweigert.	
Gesperrt bis 11/07/08 18:00	Der Zugriff wird für den Benutzer mit einer Verzögerung verweigert.	
Zentralschalter	Der Riegelwerkschalter ist geöffnet.	
Falscher Benutzer	Der Benutzer ist nicht genehmigt.	
Falscher Code	Der Code ist falsch.	Drücken Sie die Taste „Enter“ oder „Clear“, um den Vorgang zu wiederholen.
Wert zu hoch	Der Wert ist zu hoch.	Drücken Sie die Taste „Enter“, um zum Einstellungsbildschirm für die Uhrzeit zurückzukehren.
Zeitabschnitt deakt.	Der Zeitraum im Kalender ist unterbrochen.	Drücken Sie die Taste „Enter“ oder „Clear“, um zum Einstellungsbildschirm für den Zeitraum zurückzukehren.
Falsches Startdatum	Das Anfangsdatum ist falsch.	Drücken Sie die Taste „Enter“ oder „Clear“, um zum Einstellungsbildschirm für das Datum zurückzukehren.
Falsches Enddatum	Das Enddatum ist falsch.	
Keine Feiertage def.	Der gesetzliche Feiertag ist nicht festgelegt.	Drücken Sie die Taste „Enter“ oder „Clear“, um zum Einstellungsbildschirm für gesetzliche Feiertage zurückzukehren.
ID Merkmal falsch	Der Benutzer wurde nicht identifiziert.	Drücken Sie die Taste „Enter“ oder „Clear“, um zum Anfangsbildschirm des Vorgangs zurückzukehren.
Alle gesperrt!	Alle Benutzer sind gesperrt.	Drücken Sie die Taste „Enter“ oder „Clear“, um zum Bildschirm „Home“ zurückzukehren.

4 Zugriff auf die Systemkonfiguration

☞Gewünschtes Schloss auswählen.
☞Kontextabhängige Taste „Menü“ drücken.

☞Code eingeben + ENTER

Die Hauptmenüliste wird angezeigt.
☞Funktion auswählen + ENTER

Drücken Sie , um zum vorherigen Bildschirm zurückzukehren.

Der Inhalt des Menüs ist von den jeweiligen Benutzerrechten abhängig. Jeder Benutzer kann nur auf die Funktionen zugreifen, zu deren Verwendung er berechtigt ist.

Die Hauptmenüliste enthält je nach Benutzerprofil alle oder nur einige der folgenden Funktionen:

Bediener Parameter
Zeitplanung
Verzögerung
Kalenderverwaltung
Identifikation Setup
Eingabeeinheit IU
Betätigung SU
System
Service und Wartung
Protokoll Funktion

5 Systemkonfiguration

5.1 Ändern des Öffnungscodes

So ändern Sie Ihren Code:

☞Gewünschtes Schloss auswählen.
☞Kontextabhängige Taste „Menü“ drücken.

☞Code eingeben + ENTER

☞Funktion „Bediener Parameter“ auswählen + ENTER

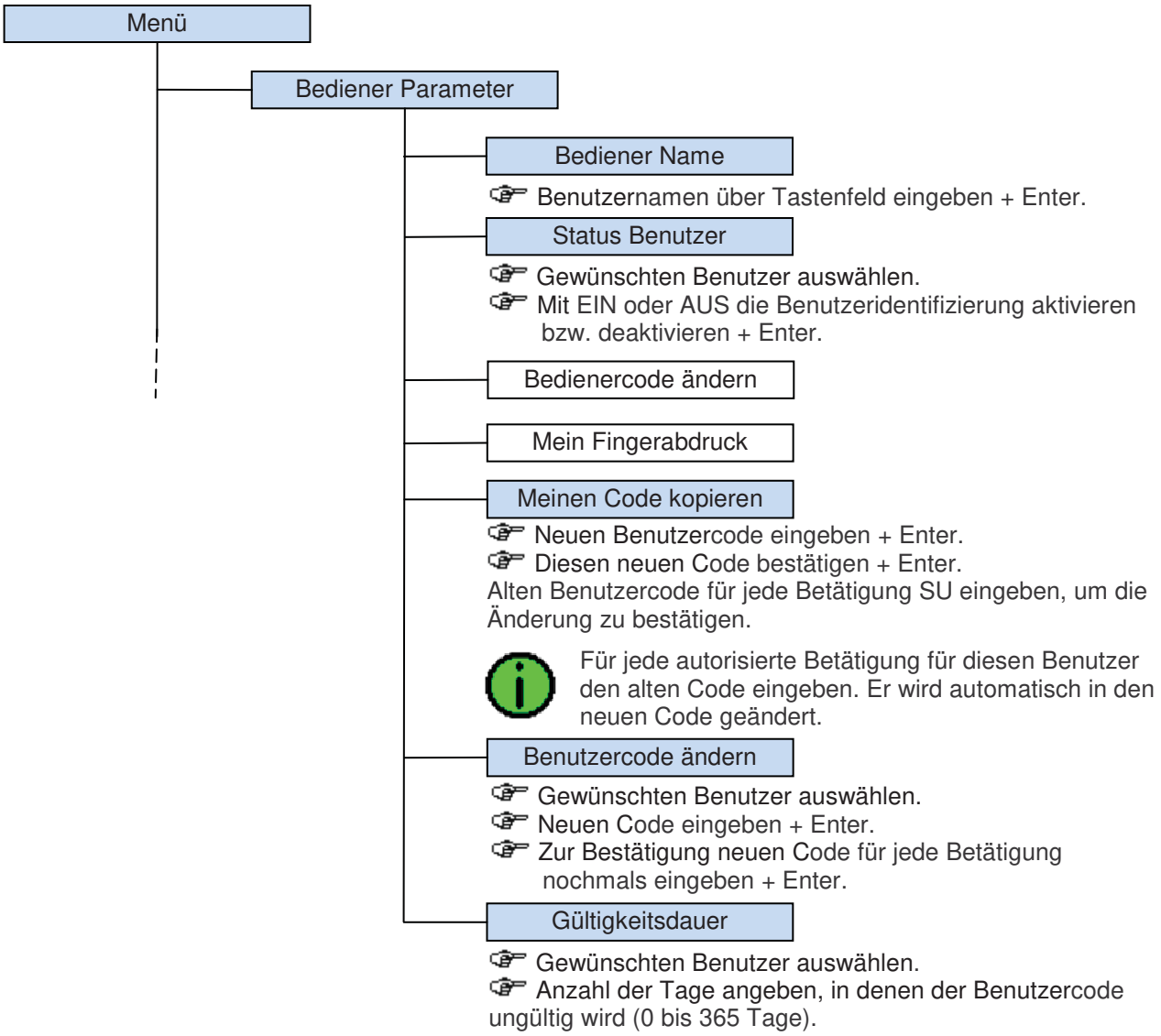
☞Funktion „Bedienercode ändern“ auswählen + ENTER

☞Neuen Code eingeben + ENTER

☞Zur Bestätigung neuen Code nochmals eingeben + ENTER
☞Mit „Home“ Menü verlassen.

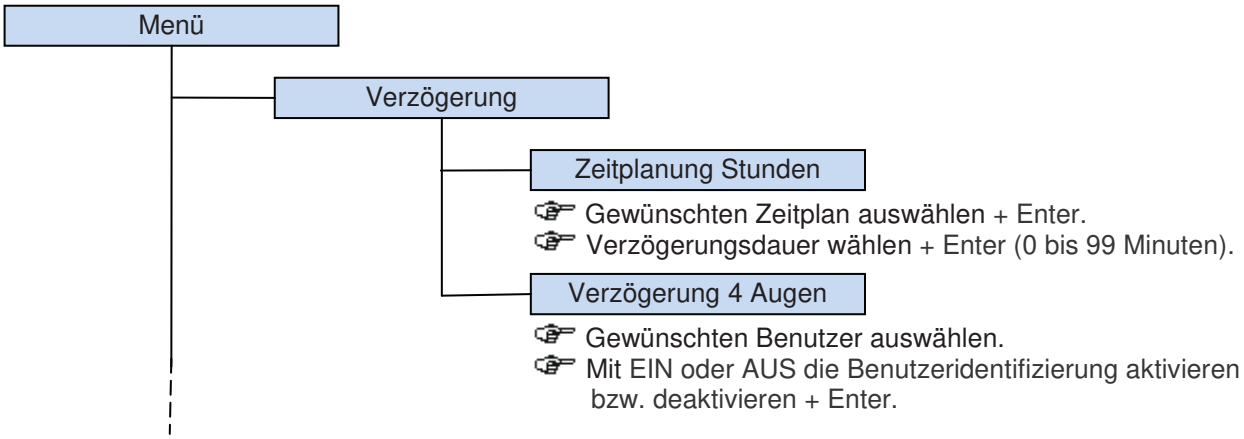
Der Öffnungscode muss vertraulich behandelt werden. Wenn der Code – möglicherweise – einer anderen Person bekannt ist, muss er umgehend durch einen neuen Code ersetzt werden. Persönliche Daten (z. B. Geburtsdatum) oder andere Daten, die ohne weiteres mit dem Benutzer in Verbindung gebracht werden können, sollten vermieden werden.
Triviale Codes sollten ebenfalls vermieden werden. Triviale Codes sind Ziffernreihen in absteigender oder aufsteigender Reihenfolge (z. B. 5-6-7-8-9-0-1-2 oder 3-2-1-0-9-8-7-6) sowie identische Ziffern (z. B. 4-4-4-4-4-4-4-4).

5.2 Festlegen der Benutzerparameter

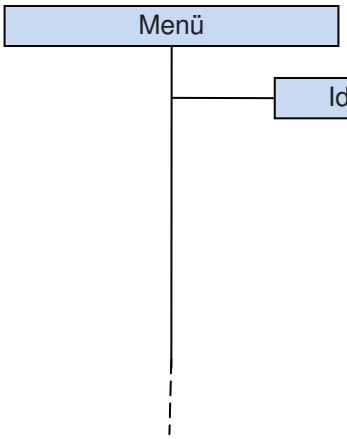


Die Benutzerparameter werden nur für die Betätigung geändert, die vor dem Aufrufen des Menüs ausgewählt war. Wiederholen Sie dieselben Schritte, im die Benutzerparameter für die anderen Betätigungen zu ändern.

5.3 Einstellen der Verzögerungen



5.4 Konfiguration der Identifizierung



Benutzer gesperrt

☞ Gewünschte Gruppenrechte auswählen + Enter.
☞ Anzahl der Tage angeben + Enter (0 bis 365 Tage).

Bei Nichtnutzung für die Dauer von x Tagen wird der Code ungültig.

Code Alterung

☞ Gewünschte Gruppenrechte auswählen + Enter.
☞ Anzahl der Tage angeben + Enter (0 bis 365 Tage).

Nach Angabe der Tage verlangt das Schloss einen neuen Code.

Anti pass-back

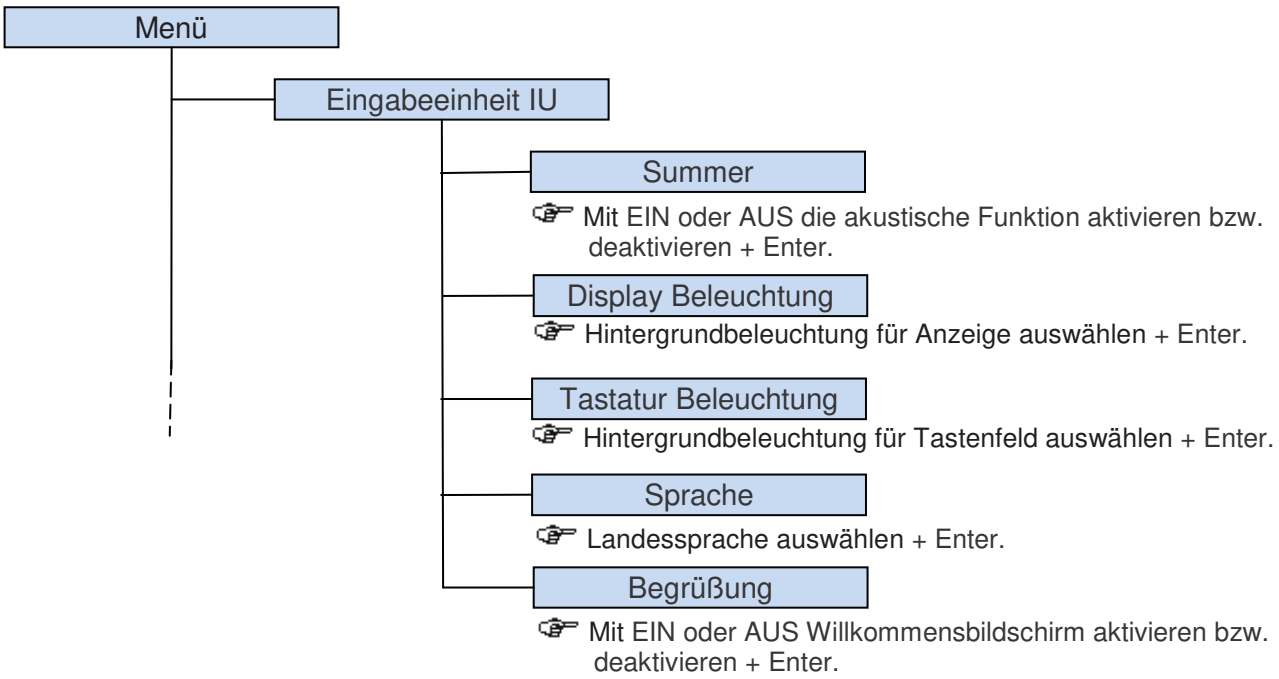
☞ Gewünschte Gruppenrechte auswählen + Enter.
☞ Anti-Pass-back-Modus auswählen (siehe unten) +Enter.

Der Anti-Pass-back-Modus legt die Bedingungen fest, unter denen ein bereits identifizierter Benutzer ein zweites Mal identifiziert wird:

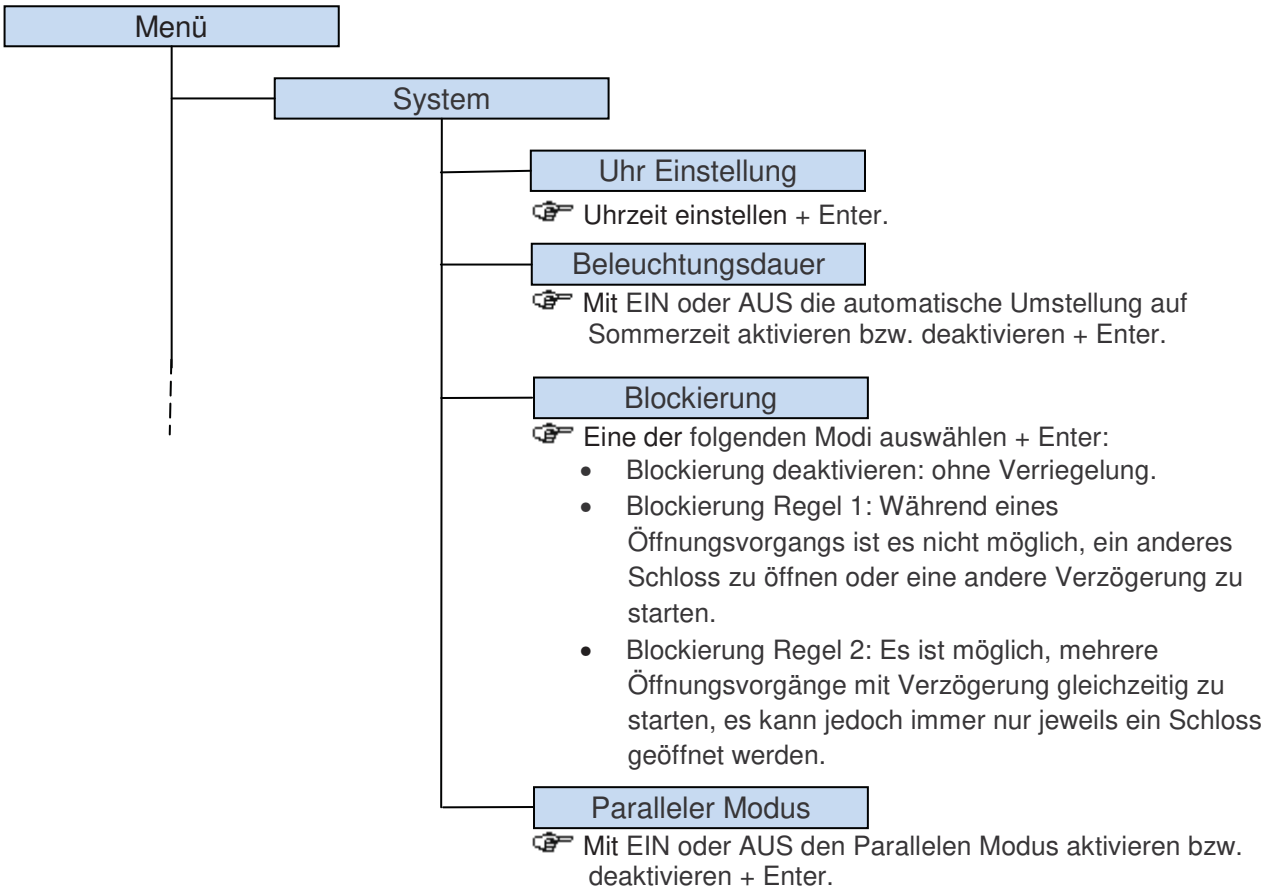
- Deaktiviert: keine Sperre für die zweite Identifizierung.
- Richtige ID: Reaktivierung durch die korrekte Identifizierung eines anderen Benutzers.
- Andere Gruppe: Reaktivierung durch die korrekte Identifizierung eines Benutzers mit anderen Benutzerrechten.
- Rückmeldung aus: Manuelle Reaktivierung an der Eingabeeinheit (Input Unit).

Wenn die Anzahl der Tage für eine inaktive ID geändert wird, startet die Zählfunktion für die Tage nach der ersten Identifizierung.

5.5 Einstellen der Eingabeeinheit (IU)



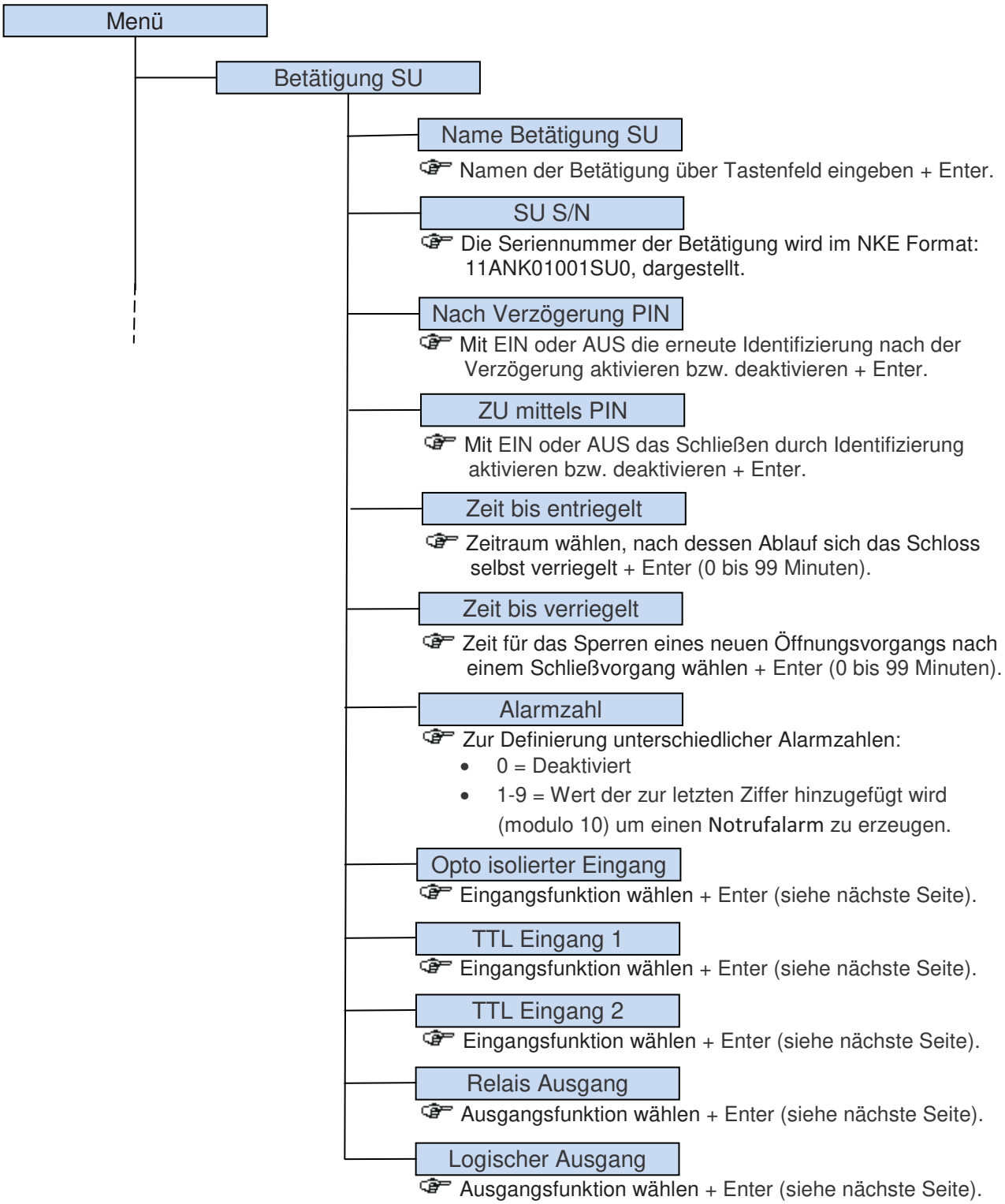
5.6 Einstellen des Systems



Einstellung der Uhr: +/- 75 Minuten.

Uhr Einstellung nur verfügbar wenn im CT-Tool das Recht “Uhrzeit einstellen“ aktiviert ist.

5.7 Einstellen der Betätigung (SU)



Für die Eingangs- und Ausgangsfunktionen gelten einige Beschränkungen auf der Eingabeeinheit (IU).
Verwenden Sie das Konfigurationstool, um auf sämtliche Funktionen zuzugreifen.

Liste der Eingangsfunktionen

Die folgende Liste zeigt die Eingangsfunktionen und den Standard Aktivierungsstatus:

Funktion	Aktivierung
Fernzugriff-Öffnungstaste für Notausgang	Hoher Pegel
Riegelwerksschalter	Hoher Pegel
Eingangsmeldung: Türstellungs-, Bewegungs- und thermischer Melder	Hoher Pegel
Fernfreigabe Benutzer G1: Fernidentifikation G1	Steigende Flanke
Zeitverzögerungsabbruch G2: Fernabschaltung Zeitverzögerung G2	Steigende Flanke
Abbruch laufende Prozedur G3: Fernabschaltung laufende Prozedur G3	Steigende Flanke
Ferngesteuerte Verwendung G4: Verzögerte Verwendungen G4	Steigende Flanke
Alarmabschaltung: Zwangsalarm wenn externer Knopf während der Verzögerung nicht gedrückt wird.	Hoher Pegel
Zugangssperre	Hoher Pegel

Hinweis: « Hoher Pegel » = normaler Betriebszustand (Niedriger Status = offen).

Liste der Ausgangsfunktionen

- Keine
- Verriegelung vollständig zurückgezogen: Der Ausgang wird aktiviert, wenn die Betätigung offen ist.
- Externe Aktivierung von Öffnungs-, seismischem und thermischem Erkennungsalarm.
- Korrekte Identifizierung.
- Verzögerung läuft: Der Ausgang wird während der Öffnungsverzögerung aktiviert.
- Ende der Verzögerung.
- Notrufalarm.
- Alarm blockierte Verriegelung.
- Zeitüberschreitungsalarm für zurückgezogenes Riegelwerk.
- Öffnungs- und Kontakterkennungsalarm.
- falsche Identifizierung beim Blockieren.
- Zeitplan wird blockiert.
- Fernzugriff Relais-Funktion.
- Remote-Summer.
- Verbindungsfehler.
- Einschaltalarm nach dem Schließen.
- IO Board-Alarm manipulierter Schalter.
- Eingabeeinheit hat Schalteralarm manipuliert

Standardmäßig ist die Ausgangsfunktion “ Hoher Pegel ” (Niedriger Status = offen).

5.8 Festlegen von Zeitplänen

Menü

Zeitplan

Zeitplanung Stunde

ODER

Zeitplanung erweit.

☞ Zeitplan auswählen + Enter.
☞ Tag auswählen + Enter.

☞ Stunden mit Tasten „Nach rechts“ und „Nach links“ einst.
☞ Öffnungsmodus mit Taste „Art“ einstellen:

- Keine weiße Linie: kein Zugriff
- 1 weiße Linie: einfacher Zugriff (mit Verz. 1)
- 2 weiße Linien: Vier-Augen-Zugriff (mit 4-Augen-Verz.)

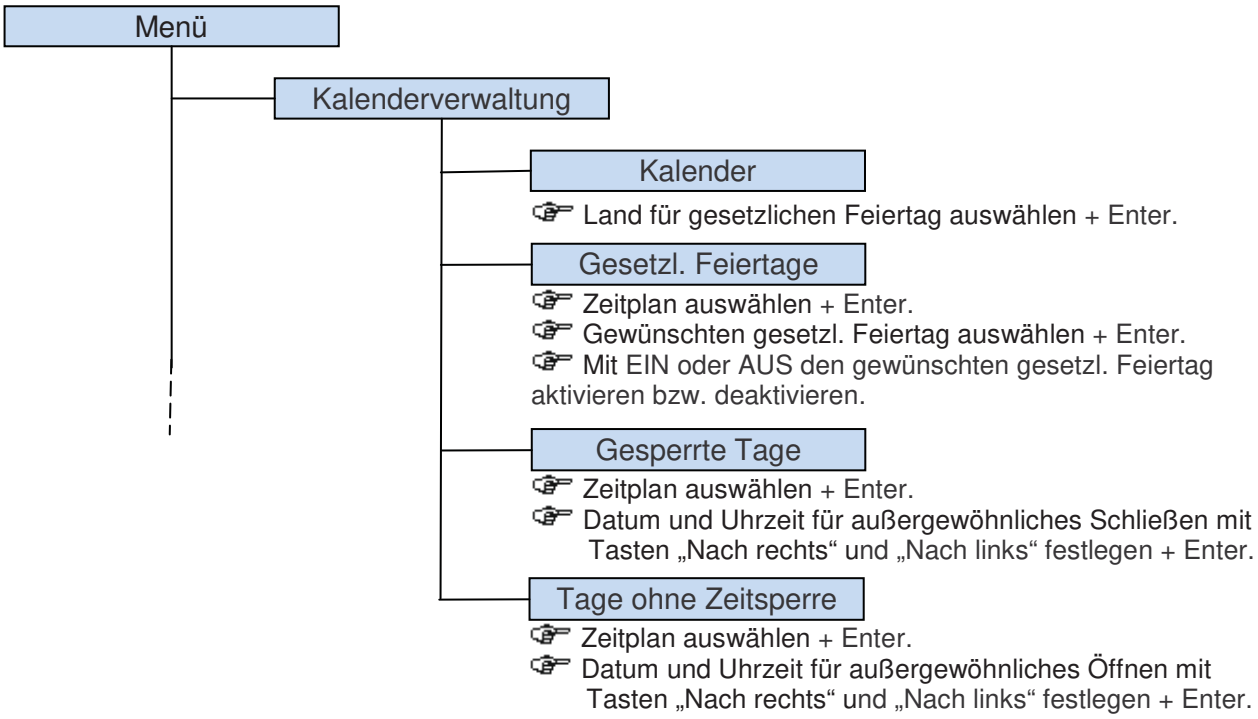
Dauer erweitert

☞ Zeitplan auswählen + Enter.
☞ Verlängerten Zeitraum auswählen + Enter.
☞ Verlängerten Zeitraum mit Tasten „Nach rechts“ und „Nach links“ einstellen + Enter.

Der verlängerte Zeitraum wird angezeigt.
☞ Zur Bestätigung „Enter“ drücken oder , um den Zeitraum zu ändern.

Jede Einstellung kann mit den Tasten „Copy“ und „Einf“ kopiert werden.

5.9 Einstellen des Kalenders



Die Funktion für außergewöhnliches Schließen ermöglicht das Festlegen eines Zeitraums, in dem jede Identifizierung verweigert wird.
Die Funktion für außergewöhnliches Öffnen ermöglicht das Festlegen eines Zeitraums, in dem eine Identifizierung aus Zeitplangründen nicht verweigert werden kann.

„Gesetzl. Feiertage“, „Gesperrte Tage“ und „Tage ohne Zeitsperre“ sind für „Zeitplan 1“, „Zeitplan 2“ und „Zeitplan 3“ identisch.

5.10 Service & Wartung

Menü

Service und Wartung

Automatischer Test

- Ausführen eines Selbsttests der Eingabeeinheit (IU).

Download EIN

- Versetzen der Betätigung in den Download-Modus, um die Konfiguration über das Konfigurationstool zu senden.

Konf Update über USB

Dieses Verfahren erlaubt die Konfigurationsdaten mit einem USB – Stick anzupassen.

☞ Batteriefach öffnen.
☞ USB-Stick einsetzen + Enter.
☞ Warten bis die Übertragung beendet ist.
☞ USB-Stick entfernen.
☞ Batteriefach schließen.

Upload Konifg -->USB

Diese Verfahren erlaubt die Konfiguration auf einen USB – Stick zu sichern.

☞ Batteriefach öffnen.
☞ USB – Stick anschließen + Enter.
☞ Warten bis die Übertragung abgeschlossen ist.
☞ USB – Stick entfernen.
☞ Batteriefach schließen.

Testprogramme

☞ Eines der folgenden Modustesttools auswählen + Enter:

- Test des MF2 Bus.
- Riegel Bewegung.

OTC Modus

☞ Eines der OTC Modi auswählen + Enter:

- keiner
- Safe_lock
- Ev´hora

Einmalcode eingeben

☞ Eingeben des 20-stelligen Freischaltcodes um OTC Funktionen zu aktivieren. Code wiederholen + Enter.

Menü

Service und Wartung

Konf. durch OTC

☞EIN oder AUS + Enter damit OTC Code nötig ist um Zugriff zum IU Menü zu erhalten. OTC Mode muss abweichend von “none“ sein.

Öffnungstest

☞ Beim Betreten des Menüs wird “Zyklus Nummer: 000“ angezeigt. Geben Sie die gewünschte Anzahl der durchzuführenden, kompletten, SU Zentralschalter Zyklen ein.

☞ Um den Test durchzuführen müssen Sie “Öffnungsrechte Betätigung“ (Gruppenrechte Stufe 2) und “Administratorrechte“ (Gruppenrechte Stufe 3) besitzen.

☞ Der Test läuft wie folgt ab:

- Öffnung ohne Verzögerung
- Warten bis SU Zentralschalter geöffnet.
- Kurze Wartezeit (2 Sekunden Zeitgewinn)
- Schließbefehl
- Warten bis SU Zentralschalter geschlossen.
- Kurze Wartezeit (2 Sekunden Zeitgewinn)

☞ Immer wenn ein kompletter Zyklus beendet ist zeigt die Eingabeeinheit die verbleibenden Zyklen an. Wenn kein Fehler auftritt wird am Ende “Zyklus Nummer: 000“ angezeigt. Bei Problemen (u.a: Riegelwerk blockiert) wird “Zyklus Fehler: XXX“ anzeigt (XXX = der Zyklus bei dem der Fehler auftrat z.B. 003).

☞ Wenn Home oder gedrückt wird, wird der Test nach Beendigung des derzeitigen Zyklus abgebrochen.

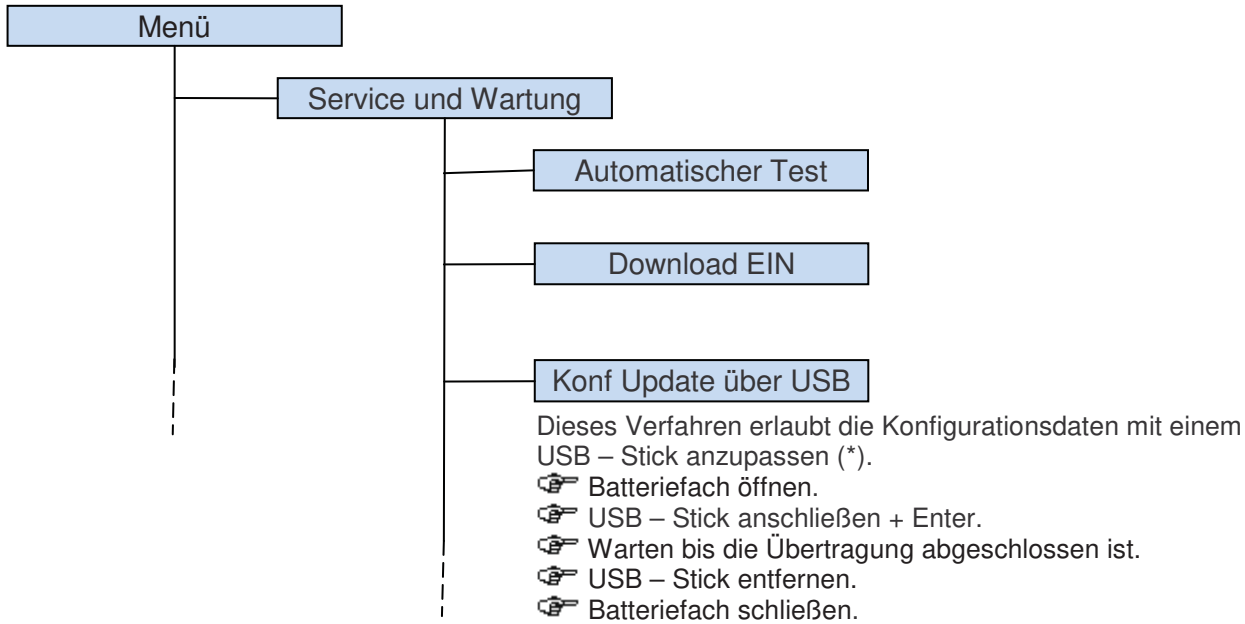
6 Konfigurationsänderung mit USB - Stick

6.1 Einleitung

Eine neue Konfiguration, für das Schloss SafeLock GSL, kann über das Konfigurationstool auf einen USB – Stick geschrieben und dann direkt in die Eingabeeinheit (IU) geladen werden.
Die bestehende Konfiguration des Schlosses kann auf einen USB – Stick geladen und vom Konfigurationstool, zum Abgleich der im Konfigurationstool gespeicherten Daten, ausgelesen werden.

6.2 Aktualisierung der Konfiguration mit einem USB – Stick (« Download »)

Um das USB – Menü verwenden zu können, muss der Benutzer das Recht “Rechte um USB-Speicherschlüssel runter – oder hochzuladen” haben.



(*) Die neue Konfiguration wird sofort übernommen!

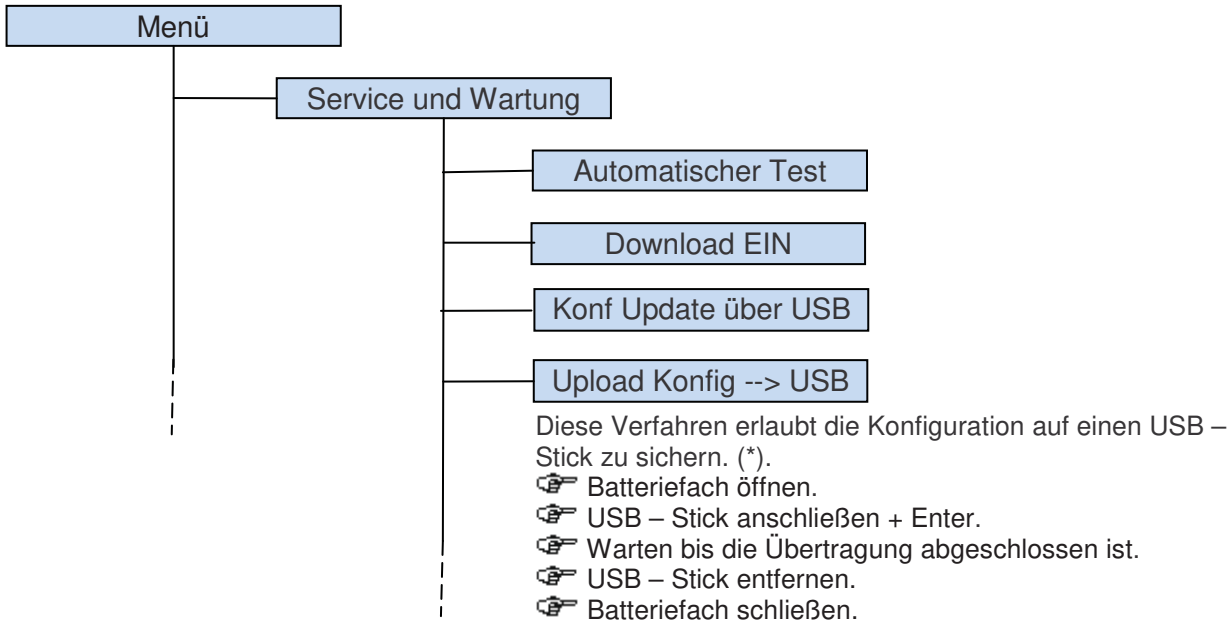
Wenn die bestehende Konfiguration des Schlosses aktueller ist, als die vom USB – Stick, wird SafeLock GSL eine Meldung bringen und eine Bestätigung erwarten.

Wenn der USB – Stick ein Gültigkeitsdatum enthält, ist die Aktualisierung nur möglich wenn das Datum gültig ist.

Nur USB-Sticks verwenden, die mit dem Dateisystem FAT formatiert sind (FAT16 oder FAT32).

6.3 Sichern der Konfiguration auf einen USB – Stick (« Upload »)

Um das USB - Menü verwenden zu können, muss der Benutzer das Recht “Rechte um USB-Speicherschlüssel runter – oder hochzuladen” haben.

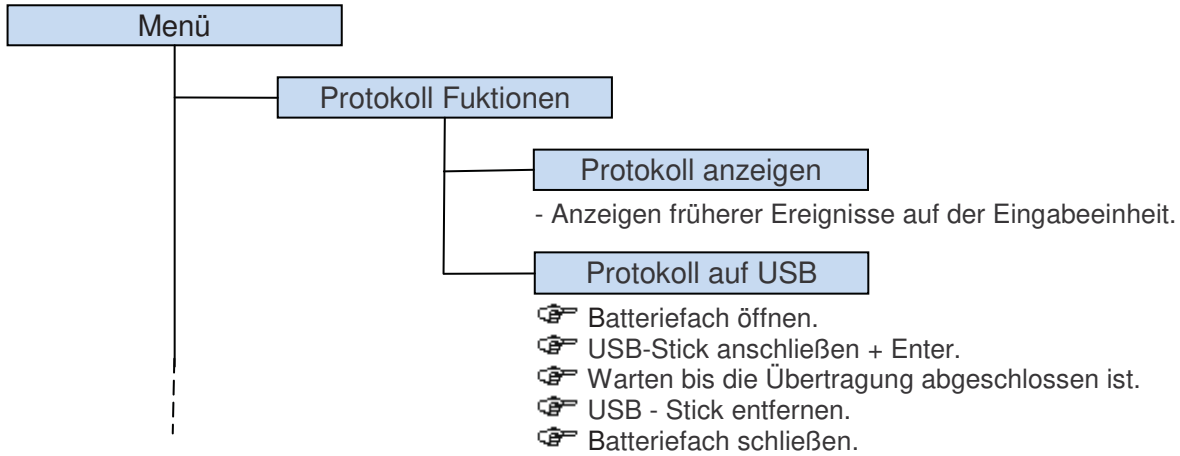


(*) Das Konfigurationstool kann nun die Daten vom USB – Stick einlesen, um die bestehende Konfiguration anzupassen.

Nur USB-Sticks verwenden, die mit dem Dateisystem FAT formatiert sind (FAT16 oder FAT32).

7 Audit

Audit-Ereignisse können direkt auf der Eingabeeinheit angezeigt oder auf einen USB-Stick heruntergeladen oder über das Konfigurationstool direkt auf einen PC heruntergeladen werden.



Während des „Herunterladens auf den USB-Speicher“ können Sie mit der Taste „Home“ zum SU-Auswahlbildschirm oder mit der Taste „  “ (kontextabhängige Taste) zum Menü „Protokoll Funktionen“ zurückkehren.

Über eine Taste können mehrere Audits von verschiedenen Schlössern heruntergeladen werden.
Zum Einsehen des Audits öffnen Sie das Konfigurationstool, wählen Sie „File“ und anschließend „Audit“, und wechseln Sie zu Ihrem USB-Speicher, um Audit-Daten anzuzeigen.

Nur USB-Sticks verwenden, die mit dem Dateisystem FAT formatiert sind (FAT16 oder FAT32).

8 Fingerabdruck

Die Identifizierung per Fingerabdruck kann in zwei Modi erfolgen:

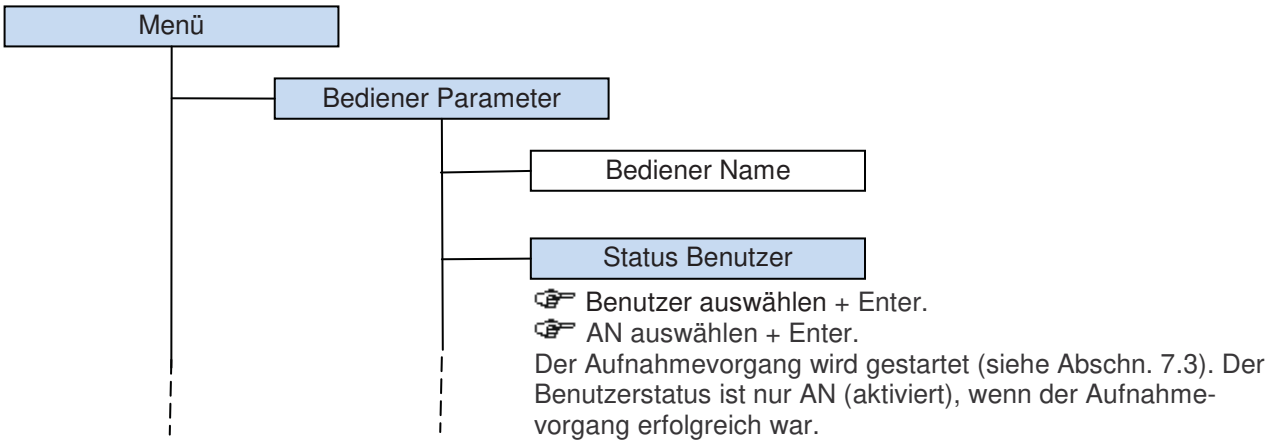
- Code + Fingerprint.
- Nur Fingerabdruck (mit Verlust der Sicherheitsklasse des Schlosses).

Für die Aufnahme des Fingerabdrucks müssen zwei verschiedene Fingerabdrücke registriert werden.

Im Fingerabdruck-Modus können nur acht Benutzer konfiguriert werden.

8.1 Aufnahme im Modus „Nur Fingerabdruck“

In diesem Modus muss ein Manager (oder Super Manager) das Menü aufrufen und den Benutzer auswählen, der aufgenommen werden soll:



8.2 Aufnahme im Modus „Code + Fingerprint“

In diesem Modus kann der Benutzer seinen Fingerabdruck selbst aufnehmen.
Dieser Vorgang erfolgt automatisch, wenn der Benutzer zum ersten Mal ein Zugriffsverfahren ausführt: Der Aufnahmevorgang startet, nachdem die Betätigung ausgewählt, der Code eingegeben und die Taste ENTER gedrückt wurde (siehe Abschn. 8.3).

8.3 Aufnahmevorgang

Der Aufnahmevorgang erfolgt in sechs Schritten:

- Finger 1: „Neuer Finger“
- Finger 1: „Wiederhole Finger“
- Finger 1: „Wiederhole Finger“
- Finger 2: „Neuer Finger“
- Finger 2: „Wiederhole Finger“
- Finger 2: „Wiederhole Finger“

Für jeden Schritt:

- Der Benutzer muss seinen Finger auf den biometrischen Sensor legen und nach vorne abziehen.
- Wenn ein Fehler oder ein Timeout auftritt, kann der Benutzer diese Phase erneut starten.
- Mit der Taste „Home“ oder kann der Benutzer den Vorgang beenden.

Um bessere Ergebnisse zu erzielen sollten Sie vermeiden kleinere Finger (Ringfinger, kleiner Finger) für den Scanvorgang zu benutzen.

8.4 Zugriff per Fingerabdruck

Schloss auswählen + ENTER

Im Modus „Code + Fingerprint“:
Code eingeben + ENTER

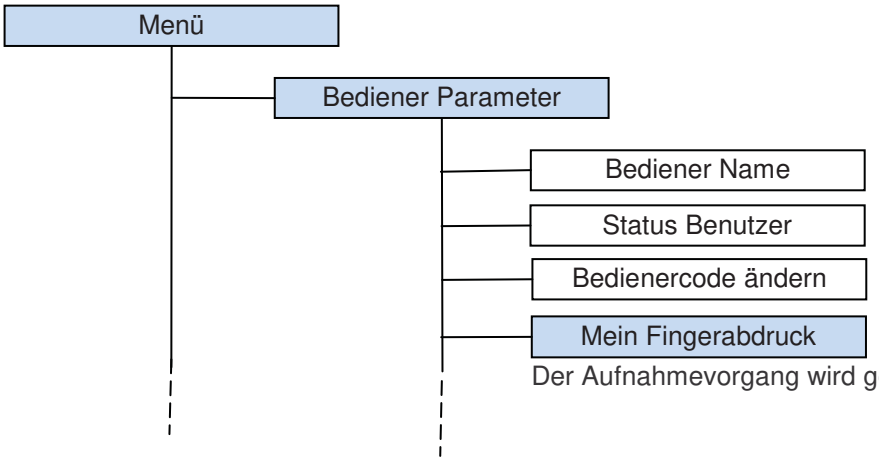
Finger auf den biometrischen Sensor drücken.

Der Zugriffsvorgang ist anschließend mit der Vorgehensweise ohne Fingerabdruck identisch.

Die Identifizierung per Fingerabdruck kann auch zum Aufrufen des Menüs verwendet werden: Drücken Sie nach der Auswahl des Schlosses einfach die Taste „Menü“ anstatt der Taste ENTER.

8.5 Ändern des Fingerabdrucks

Wenn der Benutzer das Recht zum Ändern seines Codes besitzt, kann er auch seinen Fingerabdruck ändern, indem er das Menü aufruft.



Der Aufnahmevorgang wird gestartet (siehe Abschn. 7.3).

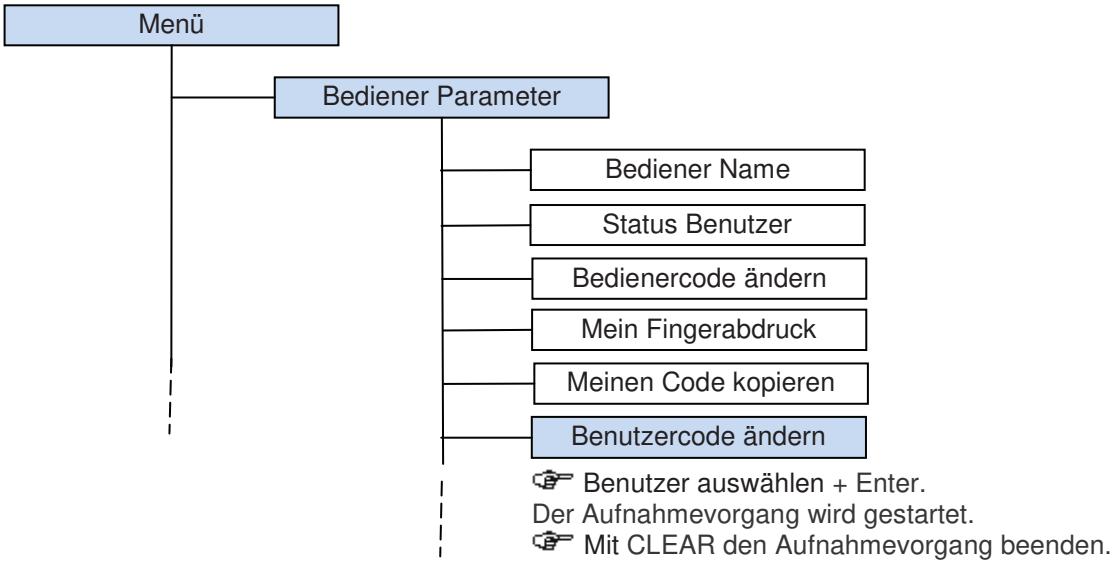
Wenn der Benutzer den Aufnahmevorgang im Modus „Nur Fingerabdruck“ beendet, muss sein Manager den Aufnahmevorgang neu starten (Abschn. 7.1).
Wenn der Benutzer den Aufnahmevorgang im Modus „Code + Fingerprint“ beendet, wird der Aufnahmevorgang automatisch durchgeführt, wenn der Benutzer zum ersten Mal einen Zugriffsvorgang einleitet (Abschn. 7.2).

Wenn der Benutzer nicht das Recht besitzt, seinen Code zu ändern:

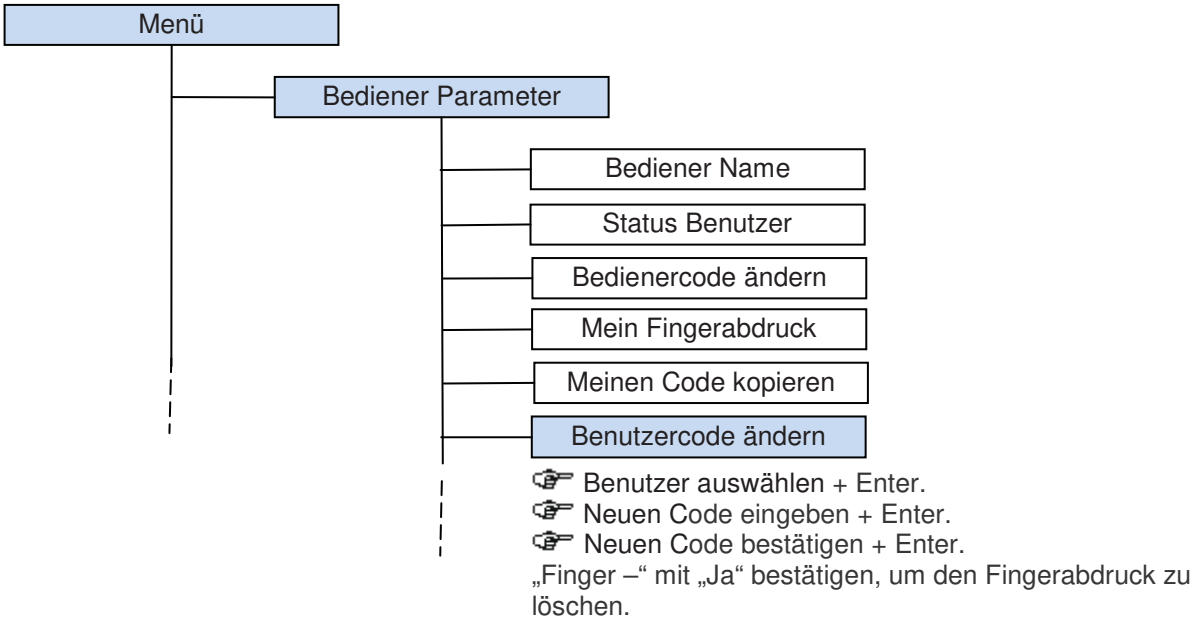
- Im Modus „Nur Fingerabdruck“ ist die Vorgehensweise mit einer neuen Aufnahme identisch (Abschn. 7.1).
- Im Modus „Code + Fingerprint“ muss der Manager zunächst den Fingerabdruck des betreffenden Benutzers löschen. Anschließend entspricht die Vorgehensweise einer neuen Aufnahme (Abschn. 7.2).

8.6 Löschen eines Fingerabdrucks

Im Modus „Nur Fingerabdruck“ muss der Manager (oder Super Manager) das Menü aufrufen, um den Benutzer auszuwählen.



Im Modus „Code + Fingerprint“ muss der Manager (oder Super Manager) das Menü aufrufen, um den Benutzer auszuwählen.



9 Werkseinstellung

Die Standard-Werkseinstellungen sind:

	Identifizierung		Einstellrechte	Öffnungsrecht	Zeitplan
Super Manager 1	01000000	Aktiv	Alle	Nein	6
Manager 1	03000000	Aktiv	Ändern der Codes 06 bis 19	Ja	1
Benutzer 06 bis Benutzer 19	06000000 bis 19000000	Inaktiv	Nein	Ja	1
Manager 2	04000000	Inaktiv	Ändern der Codes 20 bis 26	Ja	2
Benutzer 20 bis Benutzer 26	20000000 bis 26000000	Inaktiv	Nein	Ja	2
Manager CIT	05000000	Inaktiv	Ändern der Codes 27 bis 30	Ja	3
Benutzer CIT 1 bis Benutzer CIT 4	27000000 bis 30000000	Inaktiv	Nein	Ja	3
Super Manager 2	02000000	Aktiv	Alle	Nein	6

Zeitpläne:

- Schedule 1: 6 Uhr bis 22 Uhr jeden Tag.
- Schedule 2: 6 Uhr bis 22 Uhr jeden Tag.
- Schedule 3: 0 Uhr bis 24 Uhr jeden Tag.
- Schedule 6: 0 Uhr bis 24 Uhr jeden Tag.

Es sind kein Jahresplan, keine geschlossenen Zeiträume, keine geöffneten Zeiträume und keine gesetzlichen Feiertage festgelegt.

Verzögerungen:

- Öffnungsverzögerung = 1 Minute.
- Verzögerung bei Bedrohungsalarm = 10 Minuten.
- Verzögerung bei Notsperre = 30 Minuten.
- Verzögerung bei automatischer Sperre nach Schließung = 0.
- Timeout für zurückgezogenen Riegel = 10 Minuten.

Allgemeine Einstellungen

- Bedrohungsalarmmodus = Ändern der letzten Ziffer.
- Akustische Funktion = stumm.
- Rote LED = niedriger Batterieladestand.
- Grüne LED = externe Stromversorgung.
- Sperrregel für falsche Identifizierung = „Swiss rule“.
- Keine Verriegelungsregel.
- Kein „Vier-Augen-Modus“ (Dual-Modus).
- Kein Schließungsvorgang durch Identifizierung.
- Erneute Identifizierung nach Verzögerungs-Timeout:
- Keine Eingangs-/Ausgangsfunktion.

Hinweis:
Für Manager 2 und Operators 27 bis 30 gilt der Modus „Code + Fingerprint“, wenn die Eingabeeinheit (IU) ein Fingerabdruck-Modell ist.

10 Problemlösungen

Meldung	Ursache	Maßnahme
Beschädigungs-modus	Zu große Zeitverzögerung aller SU Uhren	Kontaktieren Sie den Kundendienst
Zeit-synchronisierung	Zu große Zeitverzögerung der angezeigten SU Uhr	Kontaktieren Sie den Kundendienst

11 Glossar

Audit
Chronologisches Ereignisjournal (auch „Ereignisprotokoll“).

Bedrohungscode
Paralleler Code, der Zusatzfunktionen einleitet (Änderung der Verzögerung, Alarm).

Biometrischer Code
Code, der sich aus den Merkmalen eines Menschen zusammensetzt (Fingerabdruck).

Centre national de prévention et de protection (CNPP)
Nationales Zentrum für Risikovermeidung, Schutz und Sicherheit.

CIT – Cash In Transfer
Transport, Lieferung und Empfang von Wertgegenständen.

Code
Erforderliche Identifizierungsinformation, die in ein HSL eingegeben werden kann. Bei korrekter Eingabe ist es möglich, den Sicherheitsstatus des Schlosses zu ändern.

Codeduplizierung
Code, der auf mehreren SUs dupliziert werden kann. Derselbe Code kann verwendet werden, um verschiedene SUs zu öffnen.

CT – Configuration Tool
Software zur Konfiguration aller Parameter des HSL, die auf einem PC ausgeführt wird.

DHCP – Dynamic Host Configuration Protocol
DHCP ist ein Protokoll, das von Netzwerkgeräten (Clients) verwendet wird, um die Parameter abzurufen, die für den Betrieb in einem IP-Netzwerk benötigt werden. Dieses Protokoll verringert die Arbeitslast für die Systemverwaltung, indem es das Hinzufügen von Geräten zum Netzwerk mit nur geringem oder ohne manuellen Konfigurationsaufwand ermöglicht.

DNS – Domain Name System
Das Domain Name System ist ein hierarchisches Benennungssystem für Computer, Dienste oder sonstige Ressourcen, die am Internet teilnehmen. Seine wichtigste Funktion ist die Übersetzung von für die Benutzer sinnvollen Domänennamen in die numerischen (binären) Bezeichner. Beispiel: „www.example.com“ wird übersetzt in „208.77.188.166“.

Dry contact input (Trockenkontakteingang)
Spannungsfreies Eingangssignal (Schalter, Kontakt eines Relais).

Ereignisprotokoll
Chronologisches Ereignisjournal (auch „Audit“).

Ersatzverzögerung
Verzögerung, die bei Bedrohungsalarm anstelle der normalen Verzögerung verwendet wird (im Gegensatz zu einer Zusatzverzögerung, die der normalen Verzögerung hinzugefügt wird).

G1 – Procedure G1
Wenn ein eingangskonfigurierter „G1-Vorgang“ aktiviert wird, sind keine Identifizierungen autorisiert. Nachdem ein Impuls empfangen wurde, autorisiert das System den Zugriff für die Dauer eines einstellbaren Zeitraums (0 bis 180 Sekunden).

G2 – Procedure G2
Wenn ein eingangskonfigurierter „G2-Vorgang“ aktiviert wird, wird die Öffnungsverzögerung aufgehoben.

G3 – Procedure G3
Wenn ein eingangskonfigurierter „G3-Vorgang“ aktiviert wird, wird der Öffnungsvorgang aufgehoben.

G4 – Procedure G4
Wenn ein eingangskonfigurierter „G4-Vorgang“ aktiviert wird, entspricht die Öffnungsverzögerung der „Ersatzverzögerung“.

HMI – Human Machine Interface
Hilfsmittel, über das Menschen mit einer Maschine interagieren.
Auch: Benutzeroberfläche, Man-Machine Interface (MMI).

HSL – High Security Lock
Unabhängige Baugruppe, die normalerweise an Türen von sicheren Aufbewahrungseinheiten angebracht wird, in die Codes eingegeben werden können, die mit gespeicherten Codes verglichen werden (Verarbeitungseinheit). Bei Übereinstimmung eines Öffnungscodes kann eine Sperrfunktion bewegt werden.

ID – Identifizierung
Methode zur Identifizierung eines Benutzers. Für das SafeLock GSL ist dies eine Kombination aus Benutzernummer (zweistellig) und PIN-Code.

IOB - Input Output Board (E/A-Karte)
Schnittstellenkarte, mit der sich die Anzahl der Ein- und Ausgänge erhöhen lässt.

IP – Internet Protocol
Das Internet Protocol (IP) ist ein Protokoll, das zur Kommunikation von Daten über ein Paketvermittlungsnetz verwendet wird. IP ist das primäre Protokoll in der Internet Layer der Internet Protocol Suite (TCP/IP).

IU – Input Unit (Eingabeeinheit)
Bestandteil eines HSL, das Codes an eine Verarbeitungseinheit weitergibt.

MF2
Name des Busses/Protokolls, der bzw. das zwischen den Schließvorrichtungen verwendet wird.

MLI – Multi Link Interface (oder IML)
Schnittstellengerät, das verwendet wird, um eine serielle Verbindung zu konvertieren (USB in Ethernet, USB in MF2 usw.).

Öffnungscode
Identifizierungsinformation zum Öffnen des Schlosses.

Optoentkoppelter Eingang
Die Eingangsleitung ist mit einem optoentkoppelten Chip entkoppelt.

OSTD – Opening Seismic and Thermal Detection
Alarmeingangssignal zur Erkennung von Öffnungsvorgängen, Erdbeben und Temperaturveränderungen.

OTC – One Time Code
Code, der zeitlich und in der Anzahl seiner Verwendungen begrenzt ist. Das GLS1000 kann zwei OTC-Modi verarbeiten: mode 1 = SafeLock mode, mode 2 = Ev'hora mode.

PIN – Personal Identification Number
Kennwort zur Identifizierung einer Person.

Remote-SU-Taste
Mit dieser Taste wird die Adresse der SU repariert.

Riegel (oder Sperrfunktion)
Bestandteil eines HSL, das sich nach der Eingabe des korrekten Öffnungscodes bewegt oder bewegt werden kann, um entweder eine Tür zu sichern oder das Bewegen des Riegelwerks zu verhindern.

Riegelwerk
Sperrfunktion einer Tür. Ein Riegelwerkschalter informiert darüber, ob die Tür geöffnet werden kann oder nicht.

Schloss (oder Schließvorrichtung)
Tourstift(e), der (die) das Bewegen einer Sperrfunktion ermöglicht (ermöglichen) oder verhindert (verhindern).

SU – Secure Unit, (=Betätigung)
Bestandteil eines HSL, das beurteilt, ob der eingegebene Code korrekt ist, und das Bewegen einer Schließvorrichtung erlaubt oder verhindert.

SW – Switch (Schalter)
Beispiel: tamper SW = Schalter, um Manipulationsversuche an einem Gerätekasten festzustellen.

Türstatus
Die normalen Statuszustände einer HSL-Tür sind:

- **geschlossene Tür:** Die Tür ist in ihrem Rahmen bereit zum Vorschließen ihres(r) Riegel(s).
- **verriegelte Tür:** Die Riegel sind vorgeschlossen.
- **gesperrte Tür:** Das Riegelwerk kann aufgrund des HSL nicht zurückgezogen werden.

- **gesicherte Tür:** Die Tür ist geschlossen, verriegelt und gesperrt, wobei sich ein HSL im gesicherten HSL-Zustand befindet.

USB – Universal Serial Bus
Serieller Standardbus als Schnittstelle zum Anschließen von Geräten an einen Host-Computer.

Verriegelungsregel
Regeln, die die Zustände für die Bestätigung eines Öffnungsvorgangs festlegen.

Vier-Augen-Modus (oder Dual-Modus)
Dieser Modus erfordert zwei verschiedene Codes zur Bestätigung eines Öffnungsvorgangs.

Wiederherstellung
Vorgang zur Initialisierung eines Geräts mit den Werkseinstellungen.

Winkelfilter
Optischer Filter auf der Anzeige zur Begrenzung des Sichtfelds (erforderlich für Stufe C).

Wrong identification blocking rule
Regel, die nach Eingabe eines falschen Codes zur Anwendung kommt:

- Swiss rule: 3 falsche Codes = 10-Minuten-Sperre, 4 falsche Codes = 20-Minuten-Sperre, 5 (und mehr) falsche Codes = 30-Minuten-Sperre.
- Fixed time rule: Nach 3 (oder mehr) falschen Codes wird dieselbe Zeit für die Sperre verwendet.

Zulassung
Zertifizierung des Geräts. Unter bestimmten Bedingungen kann es zum Verlust der Zulassung kommen (z. B. Identifizierung nur mit Fingerabdruck).

Kundendienst

CLAVIS Deutschland GmbH
Grüner Weg 38
34117 Kassel

Telefon: +49 (0)561 988 499-0
E-Mail: info@tresore.eu
Internet: www.tresore.eu
www.tresorschloss.de