

TwinLock B670 CashProtect DS **TwinLock C690 CashProtect DS**



Impressum

Copyright © August 2024 INSYS MICROELECTRONICS GmbH

Der Inhalt dieser Anleitung ist urheberrechtlich geschützt. Seine Verwendung ist im Rahmen der Nutzung des Systems zulässig. Eine darüber hinaus gehende Verwendung ist ohne schriftliche Genehmigung des Herstellers nicht gestattet. Für Kritik und Anregungen sind wir jederzeit dankbar. Alle Rechte an dieser Dokumentation und an den Geräten liegen bei INSYS MICROELECTRONICS GmbH Regensburg.

Bei der Zusammenstellung der Texte wurde mit größter Sorgfalt vorgegangen. Trotz aller Bemühungen kann es zu Abweichungen gegenüber den tatsächlichen Funktionen kommen. Für die Richtigkeit des Inhalts kann daher keine Gewährleistung übernommen werden. Für unkorrekte Angaben und deren Folgen können wir weder eine juristische Verantwortung noch irgendeine Haftung übernehmen. Für Verbesserungsvorschläge und Hinweise sind wir jederzeit dankbar.

Das Design von Karten kann von dem gegebenenfalls abgebildeter Musterkarten abweichen. Gleiches gilt für das Design der grafischen Benutzeroberfläche von Programmen.

Warenzeichen und Firmenzeichen

Die Verwendung eines hier nicht aufgeführten Waren- oder Firmenzeichens ist kein Hinweis auf die freie Verwendbarkeit desselben.

Windows® ist ein Warenzeichen von Microsoft Corporation.

INSYS locks® ist eine Marke der INSYS MICROELECTRONICS GmbH.

Herausgeber

INSYS MICROELECTRONICS GmbH

Hermann-Köhl-Str. 22

93049 Regensburg, Deutschland

Internet: <https://www.insys-locks.com>

Technische Änderungen, Auslassungen sowie Irrtum vorbehalten.

Achtung!
Vor Gebrauch sorgfältig lesen.
Aufbewahren zum späteren Nachschlagen.



Ihre Meinung ist uns wichtig. Bitte bewerten Sie uns.

DE: <https://www.insys-locks.com/de/kundenzufriedenheit/>

Zulassungen



VdS 3841:2022-10 (2) / EN 17646:2022

M121313 Hochsicherheitsschloss – Klasse 2(DS) (TwinLock B-DS)

M121314 Hochsicherheitsschloss – Klasse 3(DS) (TwinLock C-DS)

G106016 Sperreinrichtung TwinXT / TwinXT small - Klasse C

G105133 Schalteinrichtung TwinAlarm - Klasse C

G108061 Überfallmelder TwinXT / TwinXT small – Klasse C

G108062 Überfallmelder TwinAlarm – Klasse C

G114106 Verschlussüberwachung TwinXT / TwinXT small – Klasse C

G114107 Verschlussüberwachung TwinAlarm – Klasse C



A2P Zertifikat von CNPP, Frankreich / EN 17646 und T71-2 (11-2021)

Zert. Nr.3182.71-2 Hochsicherheitsschloss TwinLock B - DS Klasse B

Inhaltsverzeichnis

1	Zu dieser Dokumentation	8
1.1	Inhalte und Nutzung	8
1.2	Benutzerqualifikation	8
1.3	Textauszeichnungen und Formatierung	9
1.3.1	Sicherheitshinweise	9
1.3.2	Symbolbedeutungen	10
1.3.3	Handlungsanweisungen	11
2	Sicherheit	12
2.1	Bestimmungsgemäßer Gebrauch	12
2.2	Gefahren durch elektrische Energie	12
2.3	Grundsätzliche Verantwortung des Betreibers	12
2.4	Hinweise für Betreiber von verteilten Systemen	13
2.4.1	Mindestanforderungen an die Systemumgebung	13
2.4.2	Fremdkomponenten	13
2.4.3	Kryptographische Schlüssel	13
2.5	Personalanforderungen	14
2.5.1	Qualifikationen	14
2.5.2	Definition „Elektrofachkraft“	14
2.6	Umweltschutz	14
3	Systembeschreibung	15
3.1	TwinLock B670/C690 CashProtect DS	15
3.1.1	TwinLock B670 CashProtect DS	15
3.1.2	TwinLock C690 CashProtect DS	15
3.2	Systemaufbau	16
3.3	Bedieneinheit QPad	19
3.4	Schlösser INSYS Lock	19
3.4.1	Schloss INSYS Lock 700	19
3.4.2	Schloss INSYS Lock 800	19
3.5	Busverteiler TwinConnect small	20
3.6	Sperreinrichtung TwinXT	20
3.7	Schalteinrichtung TwinAlarm	20
3.8	Netzwerkserweiterungseinheit TwinIP small	21
3.8	Netzwerkserweiterungseinheit TwinIP WiFi	21
3.9	RFID Karten / Anhänger / Bänder	21
3.10	Übersicht: Codes im System	22
3.11	Funktionsübersicht	23
3.11.1	Allgemeine Funktionen	23
3.11.2	Mit optionaler Software einstellbare Funktionen	25
3.11.3	Optionale Funktionen	27
4	Inbetriebnahme verteiltes System (VS)	30
4.1	Aktivierung VS und Pairing mit TwinIP	30
4.2	VS für Betrieb mit Zentralensoftware TwinNet einrichten	32
4.3	Option „Initialcode“ für VS	32
4.4	Option „Codeverteilung“ für VS	32
5	Bedienung	33
5.1	Bedienelemente QPad	33
5.2	Hotkeys	34
5.3	Konfiguration mit CashProtectPro (optional)	34
5.4	Betrieb mit flexiblen Einmalcodes	35

5.4.1	Voraussetzungen für flexiblen Einmalcode	35
5.4.2	Flexible Einmalcodes - Persönliche PIN	35
5.4.3	QR-Codes (nur mit locksAppCIT)	35
5.5	Systemstatus und Betriebs-Parameter	36
5.5.1	Systemstatus	36
5.5.2	Modus / WTU-Funktion	36
5.5.3	Kundenschlüssel	37
5.5.4	Pairing	37
5.5.5	Codeverteilung	37
5.5.6	System ID - Kundenschlüssel	37
5.5.7	Server-Modus	37
5.5.8	Initialcode	38
5.6	Benutzer- / Personalnummern	38
5.6.1	Benutzer- / Personalnummer eingeben	38
5.7	Benutzergruppen	39
5.7.1	Bedienung mit „Benutzergruppen“ aktiviert	39
5.7.2	Master / WTU-Master wählen	40
5.8	Passwörter (VS) / Benutzer autorisieren	40
5.8.1	Passwörter in verteilten Systemen (VS)	40
5.8.2	Benutzer autorisieren	41
5.8.3	Kontrollkästchen der Benutzermatrix	41
5.8.4	Berechtigungen ab Werk via CashProtectPro	43
5.8.5	Berechtigung Master / Benutzer / etc.	43
5.9	Menüführung in der Bedieneinheit	44
5.9.1	Firmwareversion 25/26	44
5.10	PIN-Codes	45
5.10.1	Arten und Anzahl von PIN-Codes in jedem Schloss	45
5.10.2	PIN-Code eingeben	46
5.10.3	PIN-Code mit Menütasten eingeben	46
5.10.4	PIN-Code mit Zifferntasten eingeben	46
5.11	RFID Karten	47
5.11.1	RFID Karte mit Leser einlesen	47
5.12	Öffnen und Schließen	48
5.12.1	Schloss mit PIN-Code öffnen	48
5.12.2	Schloss mit RFID-Karte öffnen	49
5.12.3	Beim Öffnen Stillen Alarm auslösen	50
5.12.4	Schloss mit Codeverknüpfung öffnen	51
5.12.5	Schloss mit Öffnungsverzögerung öffnen	51
5.12.6	Mit Öffnungsverzögerung und Freigabezeit öffnen	52
5.12.7	Schlösser mit Parallelcode öffnen	52
5.12.8	Schloss mit flexiblem Einmalcode öffnen	53
5.12.9	Einbruchmeldeanlage (EMA) unscharf schalten	53
5.12.10	Schloss schließen	54
5.12.11	Schloss mit Code-Eingabe schließen	54
5.12.12	Schloss mit Türschalter automatisch schließen	55
5.12.13	Automatisches Schließen TK	55
5.12.14	Einbruchmeldeanlage (EMA) scharf schalten	56
5.13	Verstecktes System, Status, Netzwerk	57
5.13.1	Verstecktes Menü anzeigen	57
5.13.2	Status / Info des Systems anzeigen	57
5.13.3	Schloss mit Netzwerk verbinden	58
5.14	Einstellungen: Manager	59
5.14.1	Systemmanagercode ändern	59
5.14.2	Mastercode anmelden	60

5.14.3	Mastercode abmelden.....	61
5.14.4	Anzeige Mastercode.....	61
5.14.5	Datum und Uhrzeit einstellen	62
5.14.6	Codeverknüpfung.....	62
5.14.7	Parallelcode.....	63
5.14.8	Zwangsfolge.....	63
5.14.9	Zeitverzögerung	63
5.14.10	Wochenprogramme	63
5.14.11	Alarmgeräte: XT-Erweiterung / TwinAlarm	64
5.14.12	Hinweise zu ‚Pairing einrichten‘	65
5.14.13	Pairing einrichten	66
5.14.14	Kundenschlüssel anzeigen	67
5.14.15	Codeverteilung einrichten	68
5.14.16	Server-Modus ein- / ausschalten	69
5.14.17	Initialcode aktivieren / deaktivieren	69
5.14.18	Initialcode bei Anmeldung am Schloss ändern.....	70
5.14.19	Einmalzugang (OTC Testfunktion)	71
5.14.20	System ID A/B.....	72
5.14.21	Modus / WTU-Funktion festlegen	73
5.14.22	Reset Vorgangszähler im Schloss.....	73
5.14.23	Zwei Benutzergruppen wählen.....	74
5.15	Einstellungen: Master	75
5.15.1	Mastercode ändern	75
5.15.2	PIN-Code für Benutzer anmelden	76
5.15.3	WTU-Mastercode anmelden	77
5.15.4	PIN-Code abmelden	78
5.15.5	PIN-Code Benutzer-Anzeige	79
5.15.6	Codekarte (RFID-Karte) anmelden	80
5.15.7	Codekarte abmelden	81
5.15.8	Codekarte Benutzer-Anzeige	82
5.16	Einstellungen: Mitarbeiter.....	83
5.16.1	Code ändern.....	83
5.17	Service.....	84
5.17.1	Werkseinstellung: Laden Terminal ab Werk	84
5.17.2	Werkseinstellung: Codes Löschen Schloss	86
5.17.3	Motor-Schritt.....	87
5.17.4	Schloss anmelden	88
5.17.4.1	Zusätzliches Schloss	88
5.17.4.2	Schloss wechseln	89
5.17.5	System bei defektem Riegelwerkskontakt schließen.....	90
5.17.6	Lizenzierung	90
5.17.7	Neustart	91
5.17.8	Firmware Update	91
5.18	Import / Export.....	92
5.18.1	Konfiguration und Sprache importieren.....	92
5.18.2	Meldungen beim Lesen der Konfiguration	93
5.18.3	Konfiguration / Protokoll exportieren / drucken	94
5.18.4	Sprache wählen.....	95
6	Wartung, Reparatur und Reinigung	95
7	Störungsabhilfe	96
7.1	System bei Netzausfall mit Spannung versorgen.....	96
7.2	Fehlermeldungen.....	96
7.3	Fehlercodes	102

8	Technische Unterstützung	104
9	Entsorgung	104
10	Glossar	105
11	Anhang	113
11.1	Abbildungsverzeichnis	113
11.2	Notizen	114

1 Zu dieser Dokumentation

1.1 Inhalte und Nutzung

Dieses Handbuch enthält Informationen zu Betrieb, Konfiguration und Pflege des Hochsicherheitsschlosssystems TwinLock B670/C690 CashProtect DS. Für andere Systeme TwinLock CashProtect gibt es ein eigenes Handbuch.

Das Handbuch beschreibt die Bedienvorgänge für die Systemvarianten der VdS-Klassen 2 und 3 und bietet Informationen zu den Einstellungen. VdS Schadenverhütung GmbH ist ein Unternehmen der deutschen Versicherungswirtschaft, das unter anderem Produkte aus dem Bereich der Sicherheitstechnik evaluiert.

Zur Menüführung siehe Abschnitt „Menüführung in der Bedieneinheit“ auf Seite 44, zu den Berechtigungen siehe „Berechtigung Master / Benutzer / etc.“ auf Seite 43.

Informationen zu Montage und zur allgemeinen Inbetriebnahme finden Sie in der Montageanleitung des Systems.

Anleitungen zu Öffnungs- und Schließvorgängen enthält die Kurzbedienungsanleitung.

Diese Anleitungen ermöglichen den sicheren und effizienten Umgang mit dem System. Sie sind Bestandteil des Systems. Die jeweils benötigte Anleitung muss in aktueller Version für Fachkräfte / Personal jederzeit zugänglich nahe beim System aufbewahrt werden.

Der Betreiber eines jeden Systems, das im gewerblichen Bereich eingesetzt wird, hat dafür zu sorgen, dass die Unfallverhütungs- und Umweltschutz-Vorschriften sowie die allgemeinen Sicherheitsbestimmungen für den Einsatzbereich des Systems eingehalten werden.

1.2 Benutzerqualifikation

Dieses Handbuch richtet sich vor allem an qualifizierte und geschulte Fachkräfte. Einrichter und Verwalter von System TwinLock CashProtect müssen fähig und auch sprachlich in der Lage sein, dieses Handbuch zu lesen und zu verstehen, um sich mit den Einrichtungs-, Verwaltungs- und Bedienvorgängen vertraut machen und das System richtig konfigurieren, bedienen sowie Störungen beheben und so den sicheren Betrieb des Systems gewährleisten zu können.

1.3 Textauszeichnungen und Formatierung

1.3.1 Sicherheitshinweise

Gefahr	
	Unmittelbare Lebensgefahr / Gefahr der schweren Körperverletzung und von Gesundheitsschäden. Folgen, die sich aus der Missachtung ergeben können. Anleitung zur Vermeidung oder Behebung der Gefahr.
Warnung	
	Mittelbare Lebensgefahr / Gefahr der schweren Körperverletzung und von Gesundheitsschäden. Folgen, die sich aus der Missachtung ergeben können. Anleitung zur Vermeidung oder Behebung der Gefahr.
Vorsicht	
	Verletzungsgefahr. Folgen, die sich aus der Missachtung ergeben können Anleitung zur Vermeidung oder Behebung der Gefahr.
Vorsicht	
	Gefahr eines Sachschadens. Folgen, die sich aus der Missachtung ergeben können Anleitung zur Vermeidung oder Behebung der Gefahr.
Hinweis	
	Keine Gefahrenmeldung, sondern Zusatzinformation. Hintergrundinformation / Tipps.

1.3.2 Symbolbedeutungen



Benützen Sie die Bedieneinheit.



Für die folgenden Schritte benötigen Sie Werkzeug.



Für die folgenden Schritte benötigen Sie einen PIN-Code für Benutzer.



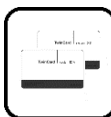
Für die folgenden Schritte benötigen Sie einen Mastercode.



Für die folgenden Schritte benötigen Sie den Systemmanagercode (Managercode des Schlosses 1).



Für die folgenden Schritte benötigen Sie eine optionale RFID Karte.



Für die folgenden Schritte benötigen Sie eine optionale System ID A und B.

1.3.3 Handlungsanweisungen

Text ohne besondere Formatierung gleich nach der Überschrift einer Handlungsanweisung enthält nicht sicherheitsrelevante Hinweise auf Umstände, die bei der Ausführung der Handlung zu beachten sind.

Sie benötigen Text, dem 'Sie benötigen' vorangestellt ist, enthält Hinweise zu Werkzeugen oder anderen Mitteln, die Sie für die erfolgreiche Durchführung der Handlungsschritte benötigen. Achten Sie auch auf die abgebildeten Symbole.

Vorbedingung Text, dem 'Vorbedingung(en)' vorangestellt ist, enthält Bedingungen, die erfüllt sein müssen, bevor Sie die Handlungsschritte ausführen können.

1. So formatierter Text fordert Sie auf, etwas zu tun. Er kann die Namen von Tasten und auf der Bedieneinheit angezeigten `Displaytext` enthalten.
So formatierter Text enthält Resultate, die die Folge davon sind, dass Sie einen Handlungsschritt ausgeführt haben.

So formatierter Text am Ende einer Handlungsanweisung zeigt Ihnen, dass Sie das Ziel Ihrer Handlung erreicht haben.

2 Sicherheit

Dieser Abschnitt bietet einen Überblick der Gesichtspunkte, die zum Schutz von Personen und für einen sicheren und störungsfreien Betrieb des Systems zu beachten sind. Weitere aufgabenspezifische Sicherheitshinweise finden Sie in den nachfolgenden Kapiteln vor der Beschreibung der Handlungsschritte, für die die jeweiligen Hinweise zu beachten sind.

2.1 Bestimmungsgemäßer Gebrauch

Warnung

**Gefahr des Einschließens von Personen.****Lebensgefahr durch Nahrungs- / Luftmangel.**

Stellen Sie vor dem Schließen jedes Schlosses sicher, dass sich keine Personen in dem zu verschließenden Behältnis / Raum befinden.

Verwenden Sie das Hochsicherheitsschlosssystem ausschließlich zum Öffnen und Schließen Ihres Wertbehältnisses sowie zur Verwaltung der Öffnungs- und Schließvorgänge.

2.2 Gefahren durch elektrische Energie

In der Montageanleitung beschriebene Arbeiten, für die Gehäuse von Einheiten des Systems geöffnet werden müssen, dürfen ausschließlich von Elektrofachkräften (Definition siehe S. 14), die von INSYS MICROELECTRONICS oder berechtigten Partnerunternehmen geschult und autorisiert wurden, durchgeführt werden.

Vorsicht

Gefahr von Kurzschluss der elektronischen Komponenten.**Gefahr der Beschädigung des Systems**

Beachten Sie die Anweisungen zur Reinigung des Systems.
Führen Sie Arbeiten an Hardwarekomponenten durch wie in der Montageanleitung beschrieben. Eigenmächtige Umbauten und Änderungen sind verboten.

2.3 Grundsätzliche Verantwortung des Betreibers

Wenn das Hochsicherheitsschlosssystem im gewerblichen Bereich eingesetzt wird, unterliegt der Betreiber des Systems den gesetzlichen Pflichten zur Arbeitssicherheit.

Neben den Sicherheitshinweisen in dieser Anweisung müssen die für den Einsatz des Systems am Einsatzort gültigen Sicherheits-, Unfallverhütungs- und Umweltschutzvorschriften eingehalten werden.

2.4 Hinweise für Betreiber von verteilten Systemen

Die Verantwortung für die Systemumgebung, für Fremdkomponenten sowie für organisatorische Maßnahmen, die geeignet sind, das Sicherheitsniveau des verteilten Systems (VS) (VS bzw. DS [distributed systems]) aufrechtzuerhalten, liegt beim Betreiber. Dem kann durch den Betrieb eines Informationssicherheitsmanagementsystems nach einem anerkannten Standard Rechnung getragen werden (nach ISO 27001, BSI-Grundschrift, VdS 10000, APSAD D32, ANSSI-PA-022-EN o.ä.).

Zur Aufrechterhaltung des Sicherheitsniveaus hat der Betreiber eine Risikoanalyse bezüglich der erforderlichen Vorgaben an die einzusetzende IT-Infrastruktur durchzuführen und die daraus resultierenden Maßnahmen umzusetzen.

Vorsicht

Gefährdung des Sicherheitsniveaus des gesamten Verteilten Systems (VS) durch

- **Einsatz ungeeigneter VS-Komponenten**
- **Einsatz von VS-Komponenten in unsicherer Umgebung**
- **unsachgemäße Bedienung des Systems durch Nutzer.**

Der Betreiber ist verantwortlich dafür, mittels geeigneter Maßnahmen für den sicheren Betrieb eines verteilten Systems zu sorgen.

Der Betreiber hat die Systemumgebung für verteilte Systeme (VS) bereitzustellen. Die Anforderungen an diese Umgebung sollten den aktuellen Richtlinien der entsprechenden Sicherheitsstelle, beispielsweise in Europa der ENISA (Agentur der Europäischen Union für Cybersicherheit) und in Deutschland den Anforderungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) entsprechen.

Dies gilt auch für optionale Fremdkomponenten, die mit dem Hostsystem oder mit dem VS interagieren könnten.

Systeme, die zur Verarbeitung und zum Einsatz von Software des VS verwendet werden, sind durch den Betreiber mit größter Sorgfalt und nach Möglichkeit exklusiv für VS-Anwendungen zu verwenden.

2.4.1 Mindestanforderungen an die Systemumgebung

10.000 Ereignisse können jeweils in der Bedieneinheit und TwinIP gespeichert werden. Vom Benutzer sind mindestens ein Netzwerksanschluss sowie Zugangsdaten für das System bereitzustellen.

2.4.2 Fremdkomponenten

Vom VS benötigte und unterstützte Fremdkomponenten sind eine handelsübliche IT-Infrastruktur (Rechner, Netzwerkdose, Router, Switches etc.). Optional sind USB-Kabel und Radius-Server. Fremdkomponenten, die für den Betrieb des VS benötigt werden, müssen außerdem den Mindestanforderungen von INSYS (Systemspezifikationen Serversoftware, Mindestanforderungen an das Hostsystem, Infrastrukturanforderungen) genügen.

2.4.3 Kryptographische Schlüssel

Die Erzeugung kryptographischer Schlüssel ist ausschließlich in sicherer Umgebung / IT-Infrastruktur durchzuführen. Die Gültigkeit von kryptographischen Schlüsseln sollte zeitlich begrenzt sein. Benutzerabhängige Teilkomponenten sollten vom autorisierten Benutzer regelmäßig in unterschiedlichen Gültigkeitszeiträumen geändert werden. Die Speicherung und Archivierung kryptographischer Schlüssel in Komponenten eines VS muss immer verschlüsselt und gemäß den Vorgaben in Punkt 6.3.2.6 der EN 17646:2022 (D) erfolgen, falls die Schlüssel gespeichert oder archiviert werden, was in diesem System nicht der Fall ist.

Die Schlüssel zur Sicherung der Kommunikation zwischen Bedieneinheit, Motorschlössern und Netzwerkeinheit werden weder gespeichert noch archiviert. Sie werden bei Bedarf aus unterschiedlichen Teilkomponenten mit einem anerkannten kryptographischen Verfahren (AES) jedes Mal neu erstellt. Sie existieren nur für die Dauer der Benutzung im RAM (Random Access Memory). Auf die benutzerabhängige Teilkomponente zur Schlüsselberechnung hat nur ein berechtigter Benutzer (Manager) Zugriff. Sie ist in einem speziell geschützten Bereich im Microcontroller abgelegt.

2.5 Personalanforderungen

2.5.1 Qualifikationen

Die verschiedenen in dieser Anleitung beschriebenen Aufgaben stellen unterschiedliche Anforderungen an die Qualifikation der Personen, die mit diesen Aufgaben betraut sind.

Warnung



Gefahr bei unzureichender Qualifikation von Personen, die das System einrichten.

Unzureichend qualifizierte Personen können die Risiken beim Umgang mit unter Spannung stehenden Elementen nicht richtig einschätzen.

Alle Arbeiten, für die Gehäuse oder Isolierungen von Bestandteilen des Systems entfernt werden müssen, nur von geschulten Elektrofachkräften ausführen lassen.

Unzureichend qualifizierte Personen während solchen Arbeiten aus dem Arbeitsbereich fernhalten.

Ausschließlich von INSYS MICROELECTRONICS oder einem Partnerunternehmen autorisierte und am System geschulte Elektrofachkräfte dürfen Arbeiten ausführen, bei denen die Hardware-Komponenten des Systems geöffnet werden müssen oder die Hardware-Konfiguration verändert wird.

2.5.2 Definition „Elektrofachkraft“

Eine Elektrofachkraft ist aufgrund ihrer fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie der Kenntnis der einschlägigen Normen und Bestimmungen in der Lage, Arbeiten an elektrischen Anlagen auszuführen und mögliche Gefahren selbstständig zu erkennen und zu vermeiden.

Sie ist speziell für das Arbeitsumfeld, in dem sie tätig ist, ausgebildet und kennt die relevanten Normen und Bestimmungen.

2.6 Umweltschutz

Der Betreiber hat dafür Sorge zu tragen, dass alle am Einsatzort gesetzlich relevanten, den Umweltschutz betreffenden Aspekte während des gesamten Lebenszyklus des Produktes beachtet werden.

Siehe auch Kapitel „Entsorgung“ auf Seite 104.

3 Systembeschreibung

3.1 TwinLock B670/C690 CashProtect DS

Die genaue Produktbezeichnung ist TwinLock B670/C690 CashProtect DS. Es gibt die Versionen 1.1 und 2.1. Von TwinLock C690 CashProtect DS gibt es auch Version 3.2.

TwinLock CashProtect bezeichnet dabei die Produktreihe.

Die Buchstaben B, C oder D stehen für die VdS Klasse [B=2(DS), C=3(DS), D=4(DS)]. Die erste Ziffer „6“ steht für die Modellreihe.

B670 steht für Systeme mit Erweiterungseinheit TwinXT und mit Netzwerkserweiterungseinheit, mit der Verwendung von Einmalcode, optional mit Erweiterungspaket „RFID“.

C690 steht für Systeme mit Schlössern der VdS-Klasse 3(DS) mit Erweiterungseinheit TwinXT and TwinIP small / WiFi, und ohne Verwendung von Einmalcodes, optional mit Erweiterungspaket „RFID“.

Die letzten Buchstaben der Bezeichnung, DS, stehen für “distributed systems” (verteilte Systeme mit Netzwerk). Falls angegeben, geben die Ziffern [X.X] nach der Version die Zahl der Schlösser im System sowie die Zahl der Erweiterungseinheiten TwinXT (small) an.

Optional kann Erweiterungspaket „TwinAlarm“ mit Schalteinrichtung TwinAlarm die Sperreinheit TwinXT ersetzen und eine Einbruchmeldeanlage einbinden.

TwinLock B670/C690 CashProtect DS sind modular aufgebaute elektronische Hochsicherheitsschlosssysteme, bei dem die sicherheitsrelevanten Komponenten voll redundant ausgeführt sind.

Es sind Systeme mit mindestens bis zu 100 direkt am Schloss gespeicherten Benutzern. Diese Benutzer können eine Gruppe bilden oder in zwei Gruppen für zwei Mandanten (beispielsweise Geldinstitut und Werttransportunternehmen) aufgeteilt werden. Die Benutzer können sich durch PIN-Code und gegebenenfalls zusätzlich durch RFID-Karten authentifizieren.

TwinAlarm und RFID sind optional bei TwinLock B670/C690 CashProtect DS.

Jedes System enthält eine Bedieneinheit, mindestens ein Schloss INSYS Lock und einen Busverteiler (TwinConnect small oder TwinIP WiFi), der die Komponenten verbindet. Alle Systeme enthalten außerdem ein Bedienungsanleitungsset.

3.1.1 TwinLock B670 CashProtect DS

Mit TwinLock B670 CashProtect DS der VdS-Klasse 2 können zusätzlich flexible Einmalcodes verwendet werden. Benutzer, die flexible Einmalcodes verwenden, können dies ohne vorherige Anmeldung am Schloss tun, wodurch die maximale Anzahl der Bediener steigt. Die Benutzer können sich durch PIN-Code oder gegebenenfalls durch Karten (mit RFID, persönliche PIN) und Einmalcode authentifizieren.

3.1.2 TwinLock C690 CashProtect DS

Mit TwinLock C690 CashProtect DS der höheren VdS-Klasse 3 können keine Einmalcodes verwendet werden. Alle Benutzer sind am Schloss angemeldet. Die Benutzer können sich durch PIN-Code authentifizieren.

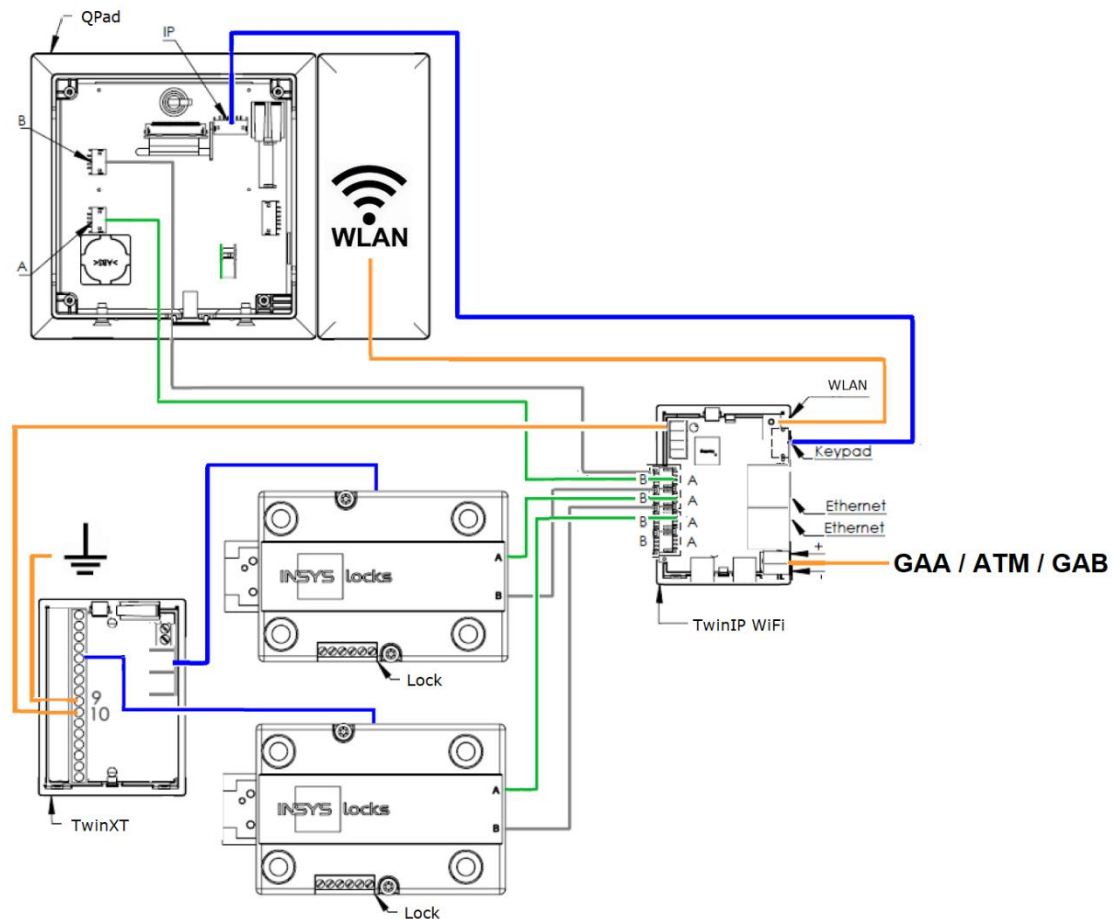


Abb. 2: Systemaufbau von System 2.1 mit TwinIP WiFi

Das System 2.1 enthält im gesicherten Bereich zwei Schlösser. TwinIP WiFi ersetzt in der abgebildeten Variante TwinConnect small und TwinIP small. Alle anderen Komponenten entsprechen System 1.1.

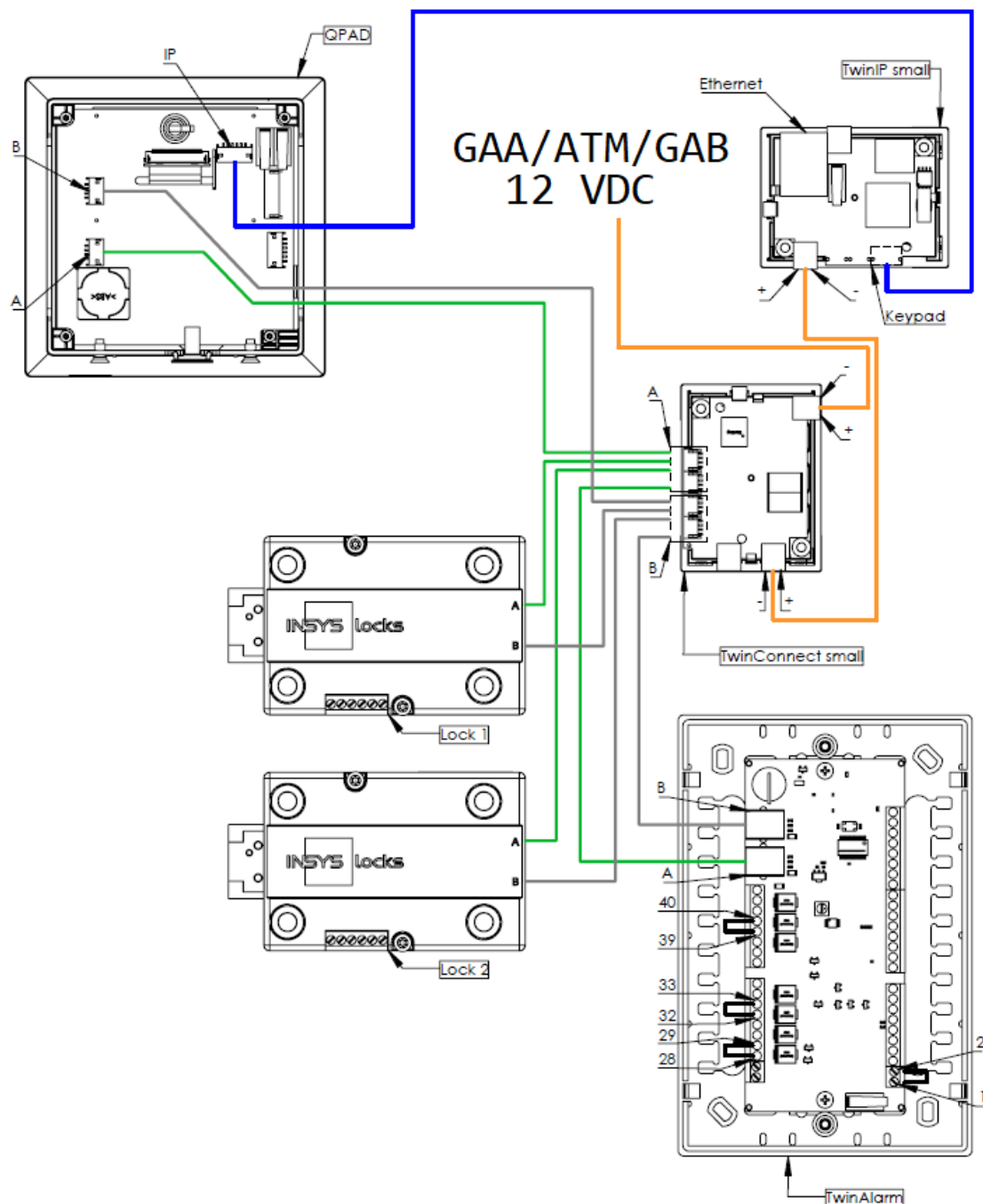


Abb. 3: Systemaufbau von System mit TwinAlarm (Beispiel)

Schaltanlage TwinAlarm für eine Einbruchmeldeanlage (EMA, nicht abgebildet) ist Überfallmelder. Die EMA ist nicht Bestandteil der Erweiterung. TwinAlarm bietet Anschlussmöglichkeit für eine EMA mit Eingängen (Alarmkontakt, Zustandskontakt, Scharfschaltung) aus Richtung der Schaltanlage TwinAlarm und Ausgängen (EMA-Bereit, Unscharf-Sperre, Quittierung, Freigabe-Sperre, Spannungsversorgung) zur Schaltanlage TwinAlarm.

TwinAlarm verfügt auch über einen Riegelwerkszentralschalter und einen Schalter für die Zeitprogramm Sperre für Schloss INSYS Lock 700 / 800.

3.3 Bedieneinheit QPad



Abb. 4: Bedieneinheit QPad

Mit Bedieneinheit QPad können Sie das System einstellen und bedienen. Für Systeme TwinLock B/C6X0 CashProtect gibt es die Ausführung mit Folientastatur. Die Konfiguration erfolgt mit USB. Für eine Beschreibung der einzelnen Bedienelemente siehe den Anfang des Kapitels „Bedienung“ ab Seite 33.

Eine Buchse zum Anschluss des Kabels für die Notstromversorgung befindet sich an der Unterseite der Bedieneinheit. Die Optionsbox RFID ist verfügbar.

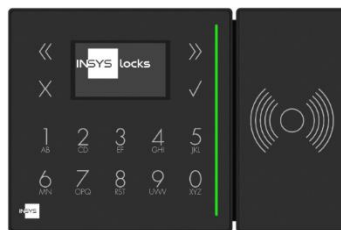


Abb. 5: Bedieneinheit mit Optionsbox RFID

3.4 Schlösser INSYS Lock

3.4.1 Schloss INSYS Lock 700



Abb. 6: Schloss INSYS Lock 700

Mit Schloss INSYS Lock 700 der VdS Klasse 2/2(DS) können Sie das Wertbehältnis ver- und entriegeln. Das Schloss befindet sich im gesicherten Bereich des Systems. Sie können bis zu 2 Schlösser an das System anschließen.

3.4.2 Schloss INSYS Lock 800



Abb. 7: Schloss INSYS Lock 800

INSYS Lock 800 ist das Gegenstück zu INSYS Lock 700 für Systeme der VdS Klasse 3/3(DS). Sie können bis zu 3 Schlösser an das System anschließen.

3.5 Busverteiler TwinConnect small



Abb. 8: Busverteiler TwinConnect small

Über ein redundantes Bussystem verbindet der Busverteiler TwinConnect small wichtige Komponenten Ihres Systems miteinander. Der Busverteiler befindet sich im gesicherten Bereich des Systems.

3.6 Sperreinrichtung TwinXT



Abb. 9: Sperreinrichtung TwinXT

Die optionale Sperreinrichtung TwinXT im gesicherten Bereich des Systems gibt es als Erweiterungseinheit. Mit einer Einheit TwinXT können Sie das System um Ein- und Ausgänge erweitern. Dadurch können bis zu zwei Schlösser gesperrt / freigegeben und mit dem Riegelwerkskontakt versehen werden. Zusätzlich verfügt TwinXT über einen Zustands- und einen Alarmkontakt für den Stillen Alarm.

3.7 Schalteinrichtung TwinAlarm



Abb. 10: Schalteinrichtung TwinAlarm

Die optionale Schalteinrichtung TwinAlarm innerhalb des Wertbehältnisses verbindet das System mit einer externen Einbruchmeldeanlage (EMA). Sie dient als Verteiler für die Einbruchmeldeanlage (Riegel-, Tür- und andere Kontakte sowie Widerstandsüberwachung). In TwinAlarm werden die elektronischen Schlüssel sowie die Eingangssignale der Einbruchmeldeanlage ausgewertet.

3.8 Netzwerkserweiterungseinheit TwinIP small



Abb. 11: Netzwerkserweiterungseinheit TwinIP small

Die Netzwerkserweiterungseinheit TwinIP small ermöglicht die Anbindung von Schlosssystemen an ein Netzwerk via Protokoll TCP/IP.

3.8 Netzwerkserweiterungseinheit TwinIP WiFi



Abb. 12: Netzwerkserweiterungseinheit TwinIP WiFi

TwinIP WiFi (lieferbar ab 2025) kann statt TwinIP small verwendet werden, wenn eine Lösung kabelgebunden nicht möglich / gewünscht ist oder wenn ein Netzwerk-Service-Anschluss erforderlich ist.

3.9 RFID Karten / Anhänger / Bänder



Abb. 13: Design-Beispiele RFID Karte, Anhänger und RFID-Armband

Optionales Zubehör. RFID-Karten oder Anhänger sind mobile Datenträger für die Benutzer eines Systems, in dem die Optionsbox RFID ein Bestandteil der Bedieneinheit ist. Die Öffnung ist nur mit PIN-Code möglich

Damit Benutzer sich am Schloss mit Karte identifizieren können, müssen sie in der Benutzermatrix autorisiert worden sein. Das Medium muss als „Codekarte“ angemeldet sein.

3.10 Übersicht: Codes im System

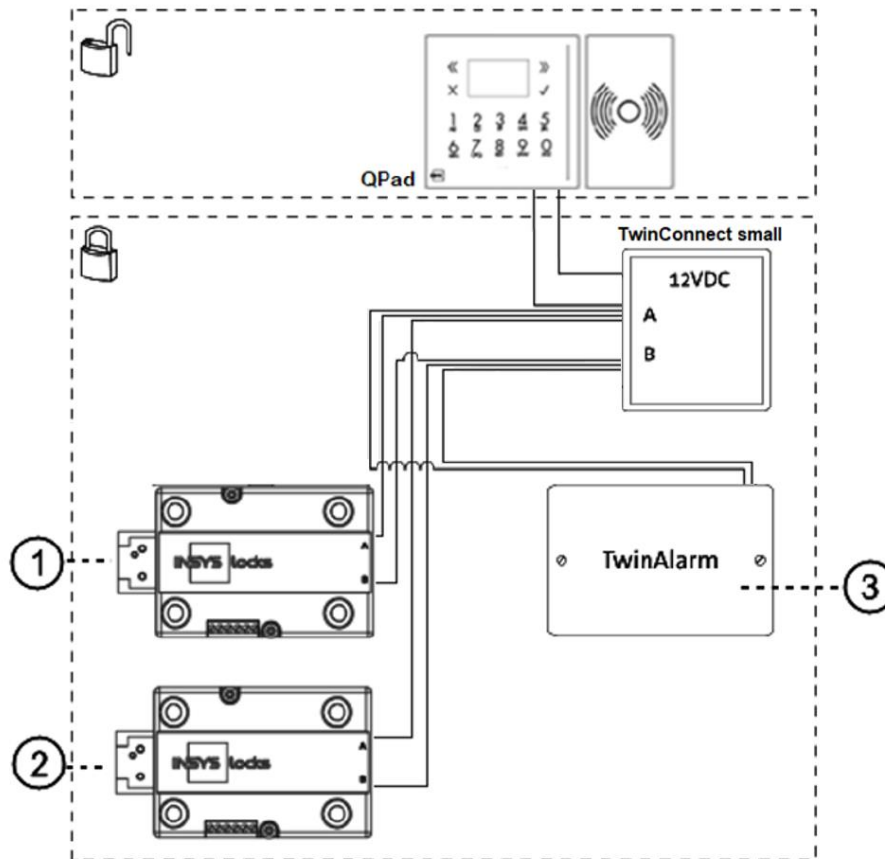


Abb. 14: Übersicht am Beispiel eines Systems mit TwinAlarm

Symbole:

offenes Bügelschloss: ungesicherter Bereich

geschlossenes Bügelschloss: gesicherter Bereich

- 1) **Schloss 1:** Geistige Codes:
 - 1 Systemmanagercode (Managercode von Schloss 1)
 - 1 Mastercode
 - 99 PIN-Codes für Benutzer
- 2) **Schloss 2:** Geistige Codes:
 - 1 Mastercode
 - 99 PIN-Codes für Benutzer
- 3) **TwinAlarm:** Körperliche Codes:
 - 1 Mastercode
 - PIN-Codes für Benutzer

Zusätzlich gibt es gegebenenfalls flexible Einmalcodes.

Vorsicht

Wenn bei Systemen mit TwinAlarm die Benutzercodes vor der Installation / der Aktivierung von TwinAlarm angemeldet werden, werden die Benutzercodes nicht in TwinAlarm gespeichert.

Stellen Sie sicher, dass TwinAlarm installiert und aktiviert ist, bevor Codes an Schloss 1 angemeldet werden.

3.11 Funktionsübersicht

3.11.1 Allgemeine Funktionen

Abhängig von Ausführung und Version des Systems sind alle oder ein Teil der im Folgenden auszugsweise aufgeführten Funktionen vor oder nach der Inbetriebnahme fest einstellbar oder mit der Bedieneinheit nachträglich änderbar.

Öffnen und Schließen

Menügeführte Öffnungs- und Schließvorgänge

Menügeführte Verwaltung und Einrichtung

Öffnen mit Codeeingabe

Öffnen / Schließen mit Parallelcode (2-Schloss-Betrieb)

4-Augen-Prinzip

Automatisches Schließen mit Türschalter

Schließen mit Codeeingabe / ohne Authentifizierung

Schnellöffnung

Feste Öffnungs- / Schließreihenfolge wählbar

Codeverwaltung

1 programmierbarer Systemmanagercode

1 programmierbarer Mastercode je Schloss

99 programmierbare PIN-Codes für Benutzer je Schloss

99 Alarmbenutzer

Anzeige Benutzerstatus

Parallelcode

Schnellöffnungsberechtigung mit Code

Programmierbare Zwangsfolge

Codeverknüpfung (4-Augencode)

Schutz vor Codemanipulation

Programmierbare flexible Einmalcodes (OTC)

Zeitfunktionen

Alarm- / Sabotageverzögerungen

Stiller Alarm

Datums- und Uhrzeitanzeige

Automatische Sommer- / Winterzeitumstellung

Freigabezeit

Öffnungszeitverzögerung

Sondertage

Teilsperzeiten

Wochenprogramme mit Zeitverzögerungen

Komfortfunktionen

Aktivierbare Displaybeleuchtung

Ständige Selbstdiagnose

Spannungsüberwachung

Spracheinstellung flexibel (mit optionalem Zubehör)

Servicefunktionen

Ereignisprotokoll 10.000 Ereignisse
Im- / Export der Konfiguration per USB
Systemstatusanzeige / Feedback via Farbgebung LED Leiste
Reset der Systemkomponenten
Versionsabfrage der Systemkomponenten
Systemkomponenten an- / abmelden
Motortest im Schrittbetrieb
Systemzeile frei programmierbar
Not-Spannungsversorgung bei Spannungsausfall

TwinAlarm-Funktionen und EMA-Anbindung (optional)

Schalteinrichtung TwinAlarm (de-)aktivierbar
Anschluss an Einbruchmeldeanlage (EMA)
(Un-)Scharfschaltung der EMA
Stiller Alarm
1 Zustandskontakt (Relais)
1 Freigabekontakt (potentialfrei)
1 Riegelwerkskontakt (potentialfrei)
Anschlussmöglichkeit für je 2 weitere Riegelwerks- und Türkontakte
Erweiterbare Sabotagelinie
Flächenschutz
Türkontakte
Stützpunkte für Widerstandsüberwachung

Funktionen mit Netzwerks-Erweiterung TwinIP (small) / TwinNet (optional)

Benutzerverwaltung via gesicherte Fernverbindung
Benutzerfreigabe / - Sperre
Flexible Fern-Einstellung von Öffnungs- / Schließzeiten
Fern-Überwachung aller Öffnungs- und Schließvorgänge
Online-Protokollierung
Fern-Überwachung von Manipulationsversuchen / Alarmen
Automatisches Reporting

Funktionen mit Einmalcode / QPad

Vergrößerter Benutzerkreis (flexible Einmalcodes)
Benutzer, persönliche PINs und flexible Einmalcodes sind unabhängig von Schlössern definierbar
Ausgabe von QR-Code bei flexiblen Einmalcodes
Anzeige von Benutzernamen auf Display
Bei RFID-Typ DESFire Unterstützung mit AES-256

3.11.2 Mit optionaler Software einstellbare Funktionen

CashProtectPro ist ein im Lieferumfang enthaltenes Parametrierset für das System TwinLock CashProtect.

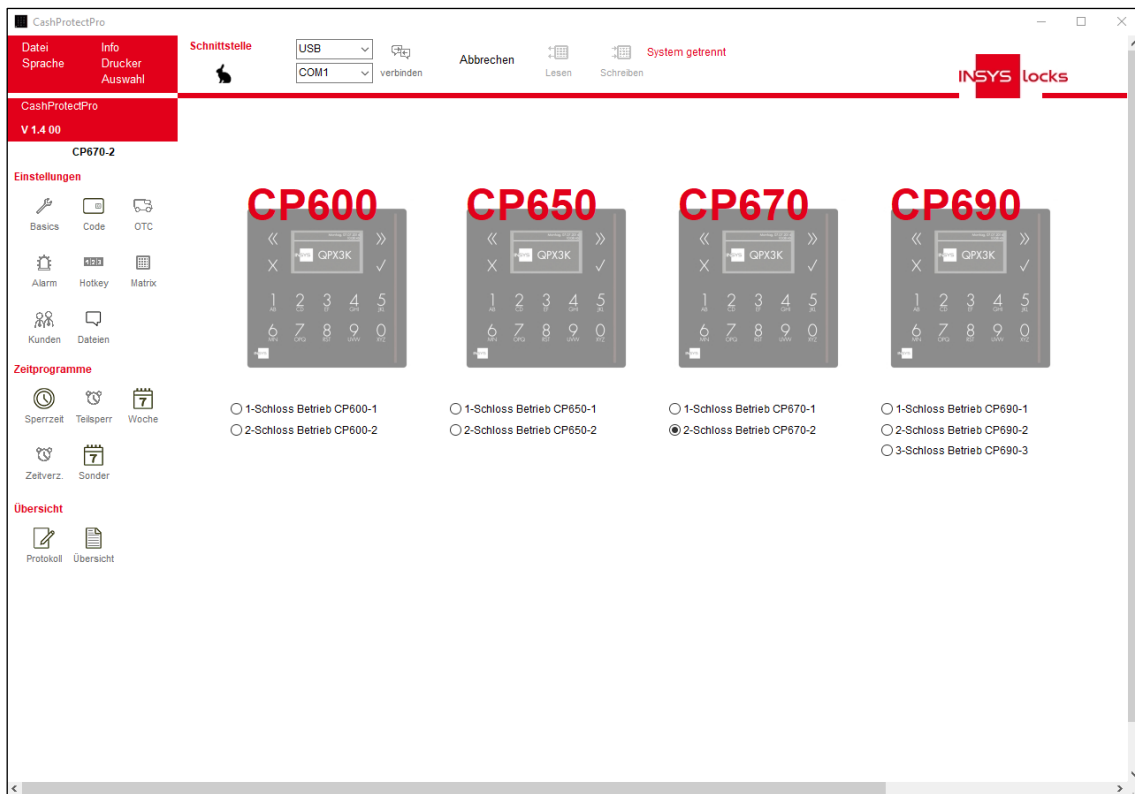


Abb. 15: Beispiel Startseite PC-Software CashProtectPro

Folgende Funktionen können mit CashProtectPro programmiert werden:

Allgemeine Einstellungen

Automatische Umstellung Sommer- / Winterzeit (de-)aktivierbar

Einstellung der Batteriewarngrenze (optional)

Auswertung des Ereignisprotokolls

Freie Programmierung der 16-stelligen Systemzeile

Öffnen und Schließen

Codeverknüpfung gemäß 4-Augen-Prinzip ein- / ausschalten

Parallelcode (de-)aktivierbar

Berechtigung, Schloss trotz Zeitprogramm zu öffnen, für ausgewählte Benutzer einstellbar

Zwangsfolge ein- / ausschalten

Manuelles Schließen mit Codeabfrage ein- / ausschalten

Automatisches Schließen mit Türschalter ein- / ausschalten

Stiller Alarm, auch mit Öffnungsverzögerung ein- / ausschalten

Prüfung auf Trivialcode

Codealterung einstellbar

Türöffnungsüberwachung

Öffnungsintervall Schloss 1 – Schloss 2 einstellbar

Scharf- / Unscharfschalten einer Einbruchmeldeanlage (EMA)

Zeitprogramme

Öffnungsverzögerung einstellbar (0-99 Min.)

Freigabezeit einstellbar (0-99 Min.)

5 Wochenprogramme mit Verzögerungen für jeden Wochentag

Sondertageprogramm für ganztägige Sperrung / Öffnung

3 Teilsperzeiten pro Wochentag

10 Sperr- / Öffnungszeiten

Verwaltungsfunktionen

Übersicht aller Parameter

Protokollanzeige

Kundendatenanzeige

komfortable Systemkonfiguration

Sperreinrichtung TwinXT (de-)aktivierbar

Schalteneinrichtung TwinAlarm (de-)aktivierbar

EMA-Benutzer (Scharfschaltung) festlegbar

Benutzermatrix mit individuellen Autorisierungen einstellbar

optionaler zweiter Benutzerbereich mit eigener Verwaltung

Öffnungsberechtigung zusätzlich gruppenweise konfigurierbar

Anzeige einer Servicetelefonnummer bei Fehlermeldungen

Netzwerkanbindung (TwinIP small)

Konfiguration der Benutzung von flexiblem Einmalcode

3.11.3 Optionale Funktionen

Die Version der Firmware der Bedieneinheit können Sie via Menü **Status / Info** anzeigen. Siehe Seite 57. Einige Funktionen können mit der optionalen PC-Software CashProtectPro programmiert werden. Für Funktionen, die Netzwerk-Anbindung voraussetzen, ist die optionale, web-basierte Software TwinNet erforderlich.

Integration RFID

Voraussetzung ist Hardware mit RFID-Modul. Damit kann netzwerktechnisch (beispielsweise via TwinNet) und lokal (via Bereich „Einstellungen“, Feld „Codekarte“ in CashProtectPro) kann für alle Benutzer eines Systems eingestellt werden, dass sie kontaktlose RFID-Tags / Karten zur Benutzeridentifikation verwenden.

Benutzer öffnen mit Einmalcode

Netzwerktechnisch (beispielsweise via TwinNet) und lokal (via Benutzermatrix in PC-Software) kann für Benutzer individuell eingestellt werden, ob sie mit 6-stelligem Einmalcode öffnen können sollen.

Wenn für Benutzer gewählt, müssen diese zum Öffnen abhängig von den System-einstellungen in der genannten Reihenfolge eingeben:

Benutzer- / Personalnummer -> PIN-Code -> Einmalcode

Stiller Alarm abschaltbar

Netzwerktechnisch (beispielsweise über die Konfiguration des Systems via TwinNet) und lokal (via PC-Software, Menü „Einstellungen“, Bereich „TwinAlarm“, Feld „Stiller Alarm“) kann eingestellt werden, ob Stiller Alarm ausgelöst werden können soll. Falls die Funktion ausgeschaltet wird, kann mit Alarmcode nicht geöffnet werden.

Daten-Export und -Import für ausgewählte Benutzer

Jeder Benutzer kann mit gültigem PIN-Code Konfigurationsdaten exportieren.

Jeder Benutzer mit der Berechtigung „Service“ (via Personenkonfiguration TwinNet / Benutzermatrix PC-Software) kann Konfigurationsdaten importieren.

Einheit TwinIP (small) via Bedieneinheit aktivieren / deaktivieren

Diese Einstellung können Systemmanager im versteckten Menü, Menüpunkt „Netzwerk“ vornehmen, nachdem sie bei angezeigtem Datum zuvor lange ENTER gedrückt haben.

Netzwerk-Parameter schreiben / - lesen via Bedieneinheit

Im Fall einer netzwerktechnischen Anbindung des Systems können die Parameter „IP-Adresse“, „Netmask“ und „Gateway“ über das Menü „Netzwerk“ der Bedieneinheit geschrieben werden:

Bei angezeigtem Datum Taste ENTER lang drücken -> Menü „Netzwerk“ -> Netzwerk JA / Nein -> JA -> Konfiguration -> JA / NEIN -> JA -> oben genannte Parameter schreiben und mit Taste OK bestätigen.

Falls „DHCP an“ angezeigt wird, werden die Parameter automatisch generiert.

Die Parameter „IP-Adresse“, „Netmask“, „MAC-Adresse“ und „Gateway“ können über das Menü „Netzwerk“ der Bedieneinheit gelesen werden:

Taste ENTER lang drücken -> Menü „Netzwerk“ -> Konfiguration -> JA / NEIN -> NEIN -> oben genannte Parameter lesen.

Spermöglichkeit von Benutzern nach Ablauf Gültigkeitsdauer Benutzercode

Netzwerktechnisch (beispielsweise über die Konfiguration des betreffenden Schlosssystems via TwinNet) und lokal (via Bereich „Einstellungen/Code“, Sektion „Code-Änderung“ Feld „Zeitraum bis Sperre“ in CashProtectPro) kann eingestellt werden, ob ein Benutzer nach Ablauf der Gültigkeit seines Codes nach einer einstellbaren Zeitspanne automatisch gesperrt und gelöscht wird.

Schnell- / Eilsperre

Für Benutzer, denen ein Wochenprogramm zugeordnet ist, kann durch langes Drücken der Taste » bei offenem und geschlossenem Schlosszustand eine Schnellsperre programmiert werden. Einmal programmiert, ist für alle zugeordneten Benutzer das Öffnen im aktuellen Zeitfenster des Wochenprogramms gesperrt. Erst wenn das nächste Wochenprogramm beginnt, kann wieder geöffnet werden.

Wochenprogramm-spezifische Verzögerungen

Jedem Wochenprogramm kann eine eigene Öffnungs- und Alarmverzögerung sowie eine Freigabezeit zugeordnet werden.

Konfigurationsmenüs in „Einstellungen“ zusätzlich in Display Bedieneinheit

Untermenüs „Codeverknüpfung“ (4-Augen-Prinzip), „Parallelcode“, „Zwangsfolge“, „Zeitverzögerung“ und „Wochenprogramm“. Die oben genannten Parameter können auch über die Bedieneinheit eingestellt werden.

Systemsperrung / - freigabe**Globale Freigabe**

Markieren Sie das Kästchen, um die globale Freigabe zu aktivieren. Dadurch bewirken Sie, dass die globale Freigabe / Systemsperrung für das ganze System gilt. Wählen Sie zusätzlich mindestens ein Wochenprogramm, um die Sperrdauer zu definieren.

WP1 / WP2 / WP3 / WP4 / WP5

Markieren Sie Kontrollkästchen, um die Wochenprogramme 1-5 zu aktivieren. Dadurch bewirken Sie, dass, wenn „Globale Freigabe“ aktiviert ist, gewählte Wochenprogramme für das ganze System und seine Benutzer gelten (Sperrung / Freigabe, siehe oben) unabhängig davon, ob Benutzer diesen Wochenprogrammen zugeordnet sind oder nicht.

Codekarte / Typ

Hier kann der RFID-Typ spezifiziert werden (wenn auch verfügbar).

Wertebereich: 'DESFire' und '---'. Werkseinstellung: 'DESFire'.

Codealterung**Codealterung [Monate]**

Einstellung der Anzahl von Monaten, nach denen der Benutzercode ungültig wird. Nach Wahl der Option werden die Benutzer aufgefordert, ihren Code zu ändern. Zum Zeitpunkt der darauf folgenden Änderung beginnt die Codealterung. Werkseinstellung: '00' (nicht aktiv).

Codealterung Master [Monate]

Einstellung der Anzahl von Monaten, nach denen der Mastercode ungültig wird. Nach Wahl der Option wird der Master aufgefordert, seinen Code zu ändern. Sonst wie bei „Codealterung [Monate]“, siehe oben.

Codealterung Benutzergruppe 2 [Monate]

Einstellung der Anzahl von Monaten, nach denen bei Einstellung von „2 Benutzergruppen“ die Codes der zweiten Gruppe ungültig werden. Sonst wie bei „Codealterung [Monate]“, siehe oben.

Codealterung Master Benutzergruppe 2 [Monate]

Einstellung der Anzahl von Monaten, nach denen bei Einstellung „2 Benutzergruppen“ der WTU-Mastercode der zweiten Gruppe ungültig wird. Sonst wie bei „Codealterung [Monate]“, siehe oben.

System ist kompatibel mit Software TwinIP

Mit passender Software-Lizenz ist das System kompatibel mit Software TwinIP.

Menüpunkt für Lizenzierung für Software TwinIP

Die Lizenzierung für Software TwinIP kann erfolgen in Menü „Service/Lizenzierung“. Nach korrekter Eingabe der Nummer der Software-Lizenz zeigt Wert „02“, dass das System für TwinIP lizenziert ist. Wert „00“ bedeutet „nicht lizenziert“.

4-Augen (Öffnen Schloss 2)

Separate Konfiguration des Öffnens nur im 4-Augen-Prinzip für Schloss 2.

Automatisches Schließen TK

Option, dass das Schließen automatisch sofort nach dem Schließen der Tür / des Riegelwerks erfolgt, gesteuert vom Türkontakt der Bedieneinheit.

Einmalcode-Funktionalität

Bereich von Einstell-Möglichkeiten für optionalen flexiblen Einmalcode.

Hotkeys

Option, bestimmte Tasten der Tastatur der Bedieneinheit als „Hotkeys“ zu definieren. Wenn Sie diese Tasten zum Aktivieren der Bedieneinheit drücken, „springt“ die Anzeige sofort in das gewünschte Menü.

Die Tasten eine Sekunde gedrückt halten oder nach Aktivierung erneut drücken.

Testfunktion für flexiblen Einmalcode (OTC)

In Menü „Einstellungen“ der Bedieneinheit gibt es Menü „Einmalzugang“ zum Testen von flexiblem Einmalcode.

4 Inbetriebnahme verteiltes System (VS)

Die allgemeine Inbetriebnahme des Schlosssystems siehe Montageanleitung.

Vorsicht

Gefahr, das System nicht mehr öffnen zu können.

Gefahr des Verlusts der Bedienbarkeit des Systems.

Stellen Sie stets sicher, dass genügend Benutzer mit Öffnungsbe-
rechtigung angelegt sind, besonders dann, wenn 4-Augen-Prinzip
oder Parallelcode konfiguriert wurde.

4.1 Aktivierung VS und Pairing mit TwinIP

Hier die Inbetriebnahme eines verteilten Systems (VS) mit TwinIP. Optionale Schritte
in **blau**.

1. Stellen Sie sicher, dass das System korrekt in Betrieb genommen wurde.
Prüfen Sie, ob Öffnen und Schließen korrekt funktioniert.
2. Wählen Sie Taste **X** (Clear) auf der Bedieneinheit.
Datum und Uhrzeit werden angezeigt.
3. Wählen Sie **Enter**.
*Menü **Sprache** des versteckten Menüs wird angezeigt.*
4. Wählen Sie **>>** und **Enter**, um **Netzwerk** anzuzeigen.
Netzwerk | *=Ja *=Nein wird angezeigt.
5. Wählen Sie ***=Ja** mit **Enter**.
Konfiguration | *=Ja *=Nein wird angezeigt.
6. Wählen Sie ***=Nein** mit **Enter**.
Die Einstellungen von TwinIP werden angezeigt.
7. Wählen Sie Taste **X** (Clear) und geben Sie Master- oder Managercode ein.
Werkseinstellung | Managercode,
Werkseinstellung | Mastercode und
Werkseinstellung | Pairingschlüssel werden angezeigt.
Kommunikation zwischen QPad und TwinIP ist nicht möglich.
*Auf Seite „Status“ von TwinIP wird Bedieneinheit QPad angezeigt. Anmeldung
in TwinIP Service ist möglich, wenn das Passwort für Benutzer „twinip“ geän-
dert wurde. Anmeldung in TwinIP Applikation ist möglich, wenn das Passwort
für Benutzer „sysadm“ geändert wurde.*
8. Ändern Sie den Managercode und kopieren Sie ihn. Siehe S.59.
9. Ändern Sie den Mastercode und kopieren Sie ihn. Siehe S. 75.
10. Ab V. 26 (optional bei V. 25): Geben Sie den Pairingschlüssel an der Bedien-
einheit via Menü **Einstellungen / Manager / Pairing** ein.
Siehe „Pairing einrichten“ auf Seite 66.
11. **Nur wenn Sie via TwinIP konfigurieren wollen: Deaktivieren Sie den Servermo-
dus via Bedieneinheit, **Einstellungen / Manager / Server** Modus.**
Siehe auch Schritt 21 unten (Seite 31).

12. Verbinden Sie den Rechner über Netzkabel mit Einheit TwinIP small.
Netzwerkeinstellung des Rechners muss sein: 192.168.1.x (255.255.255.0). Alle Netzwerkdaten werden durch die Systemadministratoren des Betreibers zur Verfügung gestellt.
13. Öffnen Sie den Browser, geben Sie in der Adresszeile `http://192.168.1.1:8080` ein und loggen Sie ein und ändern Sie das Kennwort.
Das Login-Fenster der Web-Oberfläche der Firmware-Applikation wird angezeigt. Login Name ist „twinip“ und Passwort ab Werk ist „hifoko64“.
14. Wenn erforderlich, wählen Sie die Zeile mit dem Systemdatum und der Uhrzeit.
Seite „Set date and time“ mit den Zeitdaten wird angezeigt.
15. Geben Sie die aktuellen Zeitdaten ein, speichern Sie mit dem Diskettensymbol und wählen Sie „Back to login page“.
Aktuelles Datum und aktuelle Uhrzeit werden angezeigt.
16. Geben Sie in der Adresszeile des Browsers `http://192.168.1.1` ein.
Das Login-Fenster der Web-Oberfläche von TwinIP wird angezeigt. Das Systemdatum unter der Login-Anzeige muss aktuell sein.
17. Loggen Sie in der Applikation TwinIP ein und ändern Sie das Passwort.
*Benutzername ist „sysadm“ und Passwort ab Werk ist „sysadm“.
Geändertes Passwort sicher aufbewahren.*
18. Geben Sie auf TwinIP-Seite „Verwaltung“ die Netzwerk-Parameter ein, falls erforderlich.
Stellen Sie sicher, dass TwinIP über diese Parameter erreichbar ist.
19. Entfernen Sie das Häkchen in Kästchen „TwinNet aktiv“ auf Seite „Verwaltung“.
Option bei Nutzung von TwinNet später wieder aktivieren (siehe 4.2 nächste Seite, Schritt 3).
20. Ab Version 26 (optional bei Version 25): Geben Sie auf Seite „Verwaltung“ von TwinIP den Pairingschlüssel ein, überprüfen Sie die Seriennummer der Bedieneinheit (Terminal) und speichern Sie mit dem Diskettensymbol.
Eingabe des Schlüssels in 2 Teilen wie bei „Pairing einrichten“ auf Seite 66. Den jeweiligen Teil im Feld darunter zur Bestätigung wiederholen. „Pairing erfolgreich aktiviert“ wird grün angezeigt und das Kontrollkästchen „Pairing aktiv“ wird markiert angezeigt. Auf Seite „Status“ wird das System korrekt angezeigt.
21. Optional: Konfigurieren Sie das System auf Seite „Schloss“ von TwinIP vorab.
22. Optional, wenn Sie das System via TwinIP konfiguriert haben und Zentralensoftware verwenden wollen: Reaktivieren Sie den Servermodus via `Einstellungen / Manager / Server Modus`.
Dieser Modus wurde zuvor gegebenenfalls deaktiviert (Schritt „Deaktivieren Sie den Servermodus via Bedieneinheit“ oben, S. 30).

Sie haben das System erfolgreich mit TwinIP in Betrieb genommen.

4.2 VS für Betrieb mit Zentralensoftware TwinNet einrichten

1. Stellen Sie sicher, dass das System korrekt in Betrieb genommen wurde.
Prüfen Sie testweise, ob Öffnen und Schließen korrekt funktioniert.
2. Loggen Sie in der Applikation TwinIP ein und ändern Sie das Passwort, falls erforderlich.
*Benutzername ist „sysadm“ und Passwort ab Werk ist „sysadm“.
Geändertes Passwort sicher aufbewahren.*
3. Setzen Sie das Häkchen im Kästchen „TwinNet aktiv“ auf Seite „Verwaltung“.
4. Geben Sie auf TwinIP-Seite „Verwaltung“ die TwinNet-Server-Adresse ein, falls erforderlich und überprüfen Sie die Einstellungen für die Ports.
Wenn Schlosssystem / TwinIP erfolgreich an TwinNet angemeldet wurde, wird das Kontrollkästchen „TwinNet-Pairing“ im gleichen Abschnitt dieser Seite markiert angezeigt.
5. Wählen Sie „TwinNet -Pairing zurücksetzen“, wenn angezeigt, und Schaltfläche „Speichern“ des gleichen Abschnitts.
*Auf Seite „Status“ der Applikation TwinIP zeigt ein Zähler die immer geringer werdende Anzahl an Ereignissen, die noch an TwinNet zu übermitteln sind.
Datum und Uhrzeit werden angezeigt.*

Sie haben das System erfolgreich für den Betrieb mit Zentralensoftware eingerichtet.

4.3 Option „Initialcode“ für VS

Siehe „Initialcode“ (S.38). Mit und ohne Zentralensoftware möglich.

1. Stellen Sie sicher, dass das System korrekt in Betrieb genommen wurde.
Prüfen Sie testweise, ob Öffnen und Schließen korrekt funktioniert.
2. Wenn Sie via TwinIP konfigurieren wollen: Aktivieren Sie den Initialcode via Bedieneinheit, **Einstellungen / Manager / Initialcode**.
Siehe „Initialcode aktivieren / deaktivieren“ (S.69)

Sie haben Option Initialcode erfolgreich für das verteilte System eingerichtet.

4.4 Option „Codeverteilung“ für VS

Siehe „Codeverteilung“ (S.37). Nur mit Zentralensoftware möglich.

1. Stellen Sie sicher, dass das System korrekt in Betrieb genommen wurde.
Prüfen Sie testweise, ob Öffnen und Schließen korrekt funktioniert.
2. Wenn Sie via TwinIP konfigurieren wollen: Aktivieren Sie den Initialcode via Bedieneinheit, **Einstellungen / Manager / Codeverteilung**.
Siehe „Codeverteilung einrichten“ (S.68)

Sie haben Option Codeverteilung erfolgreich für das verteilte System eingerichtet.

5 Bedienung

Mit der Bedieneinheit können Sie das System einstellen und bedienen.

5.1 Bedienelemente QPad

Für System TwinLock B/C6X0 CashProtect gibt es Bedieneinheit QPad mit Folientastatur.

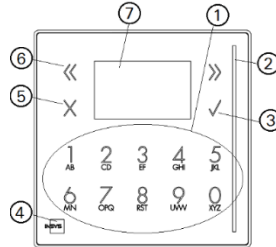


Abb. 16: Bedienelemente der Bedieneinheit QPad

- 1) Ziffernblock, bei Bedarf automatische Umstellung auf Buchstaben
- 2) LED Leiste (LED rot: Aktion fehlerhaft / LED grün: Aktion erfolgreich)
- 3) ✓ Enter-Taste zum Bestätigen
- 4) Logo (LED rot: ungesichert / LED grün: gesichert / LED blau: Parametriermodus)
- 5) ✕ Clear-Taste zum Abbrechen / zum Ziffern löschen bei Codeeingabe / 3 Sekunden gedrückt halten -> zeigt Systemmenü an
- 6) ⏪ Menütaste zurück (und ⏩ vor rechts)
- 7) Display mit Anzeige Schlosszustand (offen / zu) oben, darunter 2-zeiliges alphanumerisches Display mit Beleuchtung; nach Aktivierung und Drücken (3 Sek. Halten) von Clear wird das Systemmenü `Mo 01.07.24 08:30` angezeigt:

Im Display der Bedieneinheit anzeigbare Symbole:

- Schloss, offen (Kopfzeile):
Wenn Option „Zwangsfolge“ (siehe S.112) aus: Systemschloss offen
Wenn „Zwangsfolge“ an: Alle Schlösser offen
- Schloss, geschlossen (Kopfzeile):
Wenn Option „Zwangsfolge“ (siehe S.112) an: Systemschloss geschlossen
Wenn Option „Zwangsfolge“ (siehe S.112) aus: Alle Schlösser geschlossen
- Zeichen „Gesperrt“ (Kopfzeile):
- Bedieneinheit vorübergehend für Benutzereingaben gesperrt, wenn Daten zwischen QPad und TwinIP transferiert werden
- Zeichen „Keine Verbindung zum Server“ (Kopfzeile):
Fehler Verbindung zwischen QPad, TwinIP und Server
- Warnzeichen bei Warnungen und Fehlern

Abhängig von der Systemvariante erfolgt die Codeeingabe über die Ziffern- oder über die Menü- / Clear- / Enter-Tasten.

Eine Buchse zum Anschluss des Kabels für die Notstromversorgung befindet sich an der Unterseite der Bedieneinheit.

Die Anzeige beginnt nach einigen Sekunden zu blinken, nach einigen weiteren Sekunden ohne Eingabe wird sie automatisch ausgeschaltet.

Aktivieren Sie die Anzeige durch Drücken einer beliebigen Taste.

5.2 Hotkeys

Zusätzlich zur Navigation über die Display-Menüs der Bedieneinheit können Sie mit CashProtectPro gegebenenfalls beliebige Tasten von 0-9 als Hotkeys definieren.

Wenn Sie diese Tasten gleich nach dem Aktivieren der Bedieneinheit drücken, „springt“ die Anzeige sofort in das gewünschte, definierte Menü. Die dafür normalerweise erforderliche Navigation wird überflüssig.

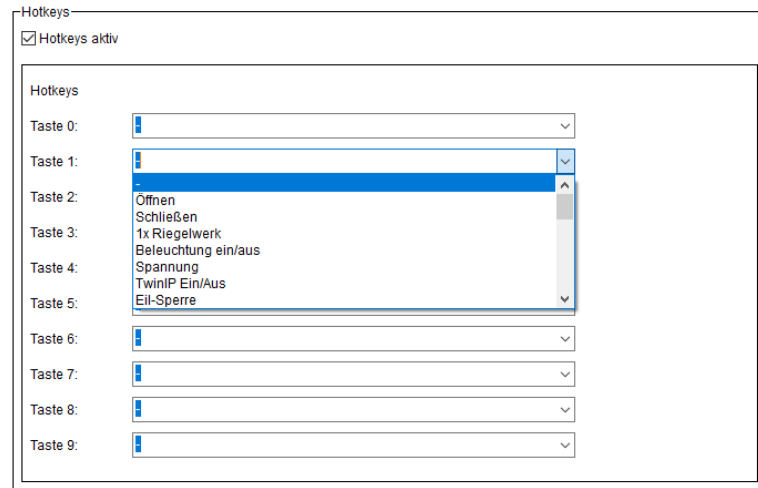


Abb. 17: Definition von Hotkeys (Beispiele)

Falls das System so eingestellt ist, dass auch die Code-Eingabe über die Zifferntasten erfolgt, ist dies wie bisher möglich. Das System stellt die Funktion der Tasten zum richtigen Zeitpunkt automatisch um.

5.3 Konfiguration mit CashProtectPro (optional)

Das System ist ohne PC Software CashProtectPro funktionsfähig. Mit PC Software sind zusätzliche Optionen verfügbar. PC Software vereinfacht die Konfiguration, ermöglicht das Auslesen des Ereignisprotokolls und die Programmierung von Zeitprogrammen. Zusätzlich kann die Autorisierung für Benutzer flexibel angepasst werden. Der Systemverwalter gibt die für die Konfiguration erforderlichen Daten über die grafische Benutzeroberfläche der Software ein.

Der Datenaustausch mit System TwinLock CashProtect erfolgt via Servicefunktion **Import / Export** an der Bedieneinheit über USB:

Stellen Sie sicher, dass das Kabel angeschlossen ist, bevor die Verbindung aufgebaut werden soll. Beenden Sie die jeweilige Verbindung mit **Schliessen** im Menü „Schnittstelle“ von CashProtectPro.

5.4 Betrieb mit flexiblen Einmalcodes

Derzeit (07/2024) für Systeme mit QPad verfügbar über Eingabe von System IDs anstelle von Systemkarten. Der Systemmanager, Benutzer Nr. 225, legt die **System IDs** am Schlosssystem an, die System-ID A (Systemcode A) und die System-ID B.

5.4.1 Voraussetzungen für flexiblen Einmalcode

- Produktversion TwinLock B650 / B670 CashProtect DS
- Der Systemmanager hat System ID A und System ID B programmiert und die Codes sind von allen Systemkomponenten (Bedieneinheit, Online-Schlösser, TwinIP...) gelesen worden
- Für die betroffenen Personen sind **Personalnummern** gespeichert
- System ist konfiguriert für flexible Einmalcodes
- Modus (WTU-Funktion) ist eingestellt auf Wert „1“ oder Wert „2“
- Datum und Uhrzeit sind korrekt und synchron
- Schloss ist korrekt ausgewählt (MultiPad Go!, TwinNet)
- Seriennummern sind überall korrekt (TwinIP small, MultiPad Go!)
- Stand der Vorgangszähler in MultiPad Go! und im Schloss ist synchron

5.4.2 Flexible Einmalcodes - Persönliche PIN

Via MultiPad können in MultiPad Go! mit **Personalnummer** registrierte Personen ihre **persönlichen PINs** eingeben, wenn das System auf **WTU-Modus 1** (gemischt) oder 2 (WTU) eingestellt ist.

Auf derartig eingestellten Systemen können Personen mit persönlicher PIN in MultiPad Go! durch die Eingabe von flexiblem Einmalcode, der ebenfalls via MultiPad Go! erzeugt wird, Schlösser öffnen.

Beim Schließen nach einem Öffnen mit Einmalcode wird ein vierstelliger Rückcode **WTU-Code: XXXX** auf dem Display der Bedieneinheit angezeigt, der beispielsweise telefonisch zurückgemeldet und vom zuständigen Mitarbeiter zum Abschließen des Vorgangs verwendet werden kann. Der jeweils letzte Rückcode kann auch mit Menü **Status / Info** angezeigt werden. Bei offenem System / Riegelwerk werden vier Sternchen **** statt dem Code angezeigt.

Bei dieser Variante brauchen gegebenenfalls weder Benutzer noch Codes im Schloss gespeichert werden. Siehe auch Handbuch TwinNet.

5.4.3 QR-Codes (nur mit locksAppCIT)

Flexible Einmalcodes können mit QPad als QR-Codes generiert werden. Mit der optionalen App locksAppCIT von INSYS locks können sie gelesen und mit „Code anfordern“ wieder als Einmalcode mit Ziffern angezeigt werden. Mit der App kann auch ein Rückcode erzeugt werden, der dann wiederum auf QPad angezeigt werden kann.

5.5 Systemstatus und Betriebs-Parameter

5.5.1 Systemstatus

Systemeinstellungen sind nur bei geöffnetem System möglich.

Bei gesichertem System werden auf dem Display der Bedieneinheit nur die Menüs **Oeffnen**, **Schliessen** und **Status / Info** angezeigt.

Um das System zu entsperren

- öffnen Sie Schloss 1, wenn Option „Zwangsfolge“ (ZF) nicht aktiv ist oder
- öffnen Sie alle Schlösser, wenn Option „Zwangsfolge“ aktiviert ist.

Wenn Option „Zwangsfolge“ aktiviert ist, können Benutzer bei Systemen mit 2 Schlössern nicht auswählen, welches Schloss sie öffnen oder schließen wollen. Siehe auch das Glossar.

Mögliche Zustände des Systems:

Ungesichert: Schloss 1 / alle Schlösser offen, Anzeige aller Menüs, Einstellungen sind änderbar.

Teilgesichert: mindestens ein Schloss offen und ein Schloss (Schloss 1) geschlossen, Systemeinstellungen sind nicht änderbar

Gesichert: Schloss 1 / alle Schlösser geschlossen, Menü-Anzeige eingeschränkt, Öffnungs- und Notfall-Funktionen sind ausführbar, Systemeinstellungen sind nicht änderbar.

Der Systemstatus ist abhängig davon, ob Option „Zwangsfolge“ aktiviert ist oder nicht:

Systemstatus mit deaktivierter Option „Zwangsfolge“

Ungesichert / entsperrt, wenn alle Schlösser offen sind.

Teilgesichert gibt es in diesem Fall nicht.

Gesichert, wenn Schloss 1 verschlossen ist. Menüanzeige eingeschränkt.

Systemstatus mit aktivierter Option „Zwangsfolge“

Ungesichert / entsperrt, wenn Schloss 1 offen ist. Anzeige aller Menüs.

Teilgesichert, wenn mind. ein Schloss geschlossen und eines offen ist.

Gesichert, wenn alle Schlösser geschlossen sind.

Zustandskontakt von TwinAlarm / TwinXT

Nur bei Systemen mit TwinXT / TwinAlarm: Kontakt in Stellung „offen“ / „geschlossen“, wenn Schloss 1 offen / geschlossen.

Systemsignal von Zustandskontakt von TwinAlarm / TwinXT

Nur bei Systemen mit TwinXT / TwinAlarm: Signal in Stellung „offen“ / „geschlossen“, wenn Schloss 1 offen / geschlossen.

5.5.2 Modus / WTU-Funktion

Von dieser Einstellung (Menü „Einstellungen/Manager/WTU Funktion“) hängt es ab, ob die Benutzer flexiblen Einmalcode benutzen müssen, dürfen oder dies nicht tun können.

Modus („WTU-Funktion“) System („1“ und „2“ nur mit B670):

0 = Bank: Benutzer öffnen mit PIN-Codes.

1 = Mix: Gemischter Modus;
Schlosssysteme haben Modus 0 und 2 gleichzeitig.

2 = WTU: Benutzer öffnen Schlösser mit flexiblen Einmalcodes.

5.5.3 Kundenschlüssel

Ab Firmware Version 25/26. Kundenschlüssel gibt es für Pairing (siehe „Pairing“ unten) und für die System IDs (siehe „System ID A/B“ auf S. 72). Falls eigens eingerichtet, gibt es auch einen dritten Schlüssel für die Codeverteilung (siehe „Codeverteilung“ auf S. 37).

Kundenschlüssel von Firmware Version 25 und 26 sind grundsätzlich kompatibel. Ab Firmware Version 26 müssen sie bei Netzwerkanbindung kundenseitig geändert werden. Die Schlüssel müssen systemintern und bei Netzwerkkommunikation auch mit den Daten in der Software TwinIP übereinstimmen. Siehe auch „Kundenschlüssel anzeigen“ auf S.67.

5.5.4 Pairing

Ab Firmware Version 25/26. „Pairing“ ist ein Verfahren, das sicherstellt, dass die Kommunikation zwischen (TwinIP small,) QPad und den Schlössern verschlüsselt erfolgt und dass diese Geräte nicht unautorisiert ausgewechselt werden können. Kundenschlüssel Pairing kundenseitig via Menü „Pairing“ einrichten, auch nach jedem Wechsel der Bedieneinheit. So werden die Schlüssel automatisch in die Schlösser übernommen. Neue Schlüssel müssen bei Netzwerkbetrieb auch auf der Web-Oberfläche der Software TwinIP eingegeben werden. Siehe „Pairing einrichten“ auf S.66 sowie gegebenenfalls das Handbuch TwinIP.

5.5.5 Codeverteilung

Nur mit TwinNet 10.3 und höher, mit Netzwerkanschluss, Netzwerks- und Codeverteilung/Initialcode-Lizenz und mit Pairing, ab Firmware Version 25/26. „Codeverteilung“ ist ein Verfahren, das sicherstellt, dass für alle Benutzer eine Synchronisation ihrer Codes an allen für dieses Verfahren gewählten Schlössern stattfindet. Standardmäßig wird auch für dieses Verfahren der Kundenschlüssel Pairing genutzt, der dazu auf allen Systemen gleich lauten muss. Optional können Sie via Menü „Codeverteilung“ einen eigenen Kundenschlüssel Codeverteilung erstellen. Werkseinstellung: deaktiviert. Siehe „Codeverteilung einrichten“ auf S. 68 sowie das Handbuch TwinIP.

5.5.6 System ID - Kundenschlüssel

Nur mit TwinNet 10.3 und höher, mit Netzwerkanschluss, Netzwerks- und Codeverteilung/Initialcode-Lizenz und mit „Pairing“, ab Firmware Version 25/26. Kundenschlüssel zur Ver- / Entschlüsselung der SystemID-Codes A und B. Der Schlüssel muss auf MultiPad und Bedieneinheit gleich sein.

Siehe „Kundenschlüssel anzeigen“, S.67, „System ID A/B“, S.72, und Handbuch TwinIP.

5.5.7 Server-Modus

Nur mit TwinNet 10.3 und höher und mit Netzwerkanschluss, ab Firmware Version 25/26. „Server-Modus“ wird automatisch eingestellt, wenn eine Netzwerk-Lizenz aktiviert wird. Bei eingestelltem Server-Modus können Schlösser ausschließlich über Server-Anbindung und nicht via TwinIP konfiguriert werden. Werkseinstellung: aktiviert. Siehe „Server-Modus ein- / ausschalten“ auf S.69.

5.5.8 Initialcode

Nur mit TwinNet 10.3 und höher, mit Netzwerkanschluss und Codeverteilung/Initialcode-Lizenz, ab Firmware Version 25/26.

Funktion für neue Benutzer, die mittels Initialcode eigenen Öffnungscode am Schloss anlegen können. Dafür ist keine weitere Person erforderlich.

Via Server-Anbindung oder TwinIP kann Initialcode programmiert werden. Option „Initialcode“ via TwinIP funktioniert nur, wenn der Server-Modus für ein Schloss deaktiviert ist. Siehe auch „Initialcode aktivieren / deaktivieren“ auf S. 69 und „Initialcode bei Anmeldung am Schloss ändern“ auf S.70.

5.6 Benutzer- / Personalnummern

Das System kann via Benutzermatrix der PC-Software so umgestellt werden, dass Personen statt systemspezifischen Benutzernummern ihre gewohnten Personalnummern eingeben können.

Wenn alle Personen am Schloss ihre Personal- statt ihrer Benutzernummern eingeben sollen:

- 1) Markieren Sie Kontrollkästchen „Personalnummer“.
- 2) Geben Sie in Spalte „Personalnummer“ die Nummern der Benutzer ein.

Wenn alle Personen am Schloss ihre Benutzernummer eingeben sollen:

- Entfernen Sie gegebenenfalls die Markierung in Kontrollkästchen „Personalnummer“.

Achtung: Personalnummern dürfen nicht nur Nullen enthalten. Sie können ein- bis sechsstellig sein.

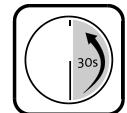
Es findet keine interne Protokollierung darüber statt, welche Art von Nummern von den Personen zu verwenden ist. Die Umstellung gilt auch für die Schlossmaster.

Auch nach Umstellung auf Personalnummern werden in den Menüs „Benutzer-Anzeige“ und PIN-Code „Abmelden“ der Bedieneinheit Benutzernummern angezeigt.

5.6.1 Benutzer- / Personalnummer eingeben

Systeme VdS Klasse 2: Nummern-Eingabe mit Menü- oder Zifferntasten konfigurierbar

Vorbedingungen Für Sie ist Kästchen **Freigabe** in der Benutzermatrix (CashProtectPro) markiert.



1. Führen Sie die Schritte einer Anleitung aus, bis die Identifizierung nötig ist.

Das Display zeigt Code-Eingabe | Master. Wenn Sie nicht sicher sind, mit welchen Tasten Nummern einzugeben sind, probieren Sie es aus. Falls die Eingabe über Menütasten eingestellt ist, können Nummern alternativ auch mit Zifferntasten eingegeben werden.

2. Wählen Sie mit > jeweils eine Ziffer der Nummer und Taste **Enter** oder geben Sie die Ziffern über die Zifferntasten ein. Schließen Sie gegebenenfalls die Eingabe der Personalnummer mit **ENTER** ab.

Das Display zeigt jede eingegebene Ziffer, z.B. Benutzer Nr.: 02. Nach der Eingabe zeigt das Display die jeweils folgende Meldung wie beispielsweise Code-Eingabe oder Bitte warten.

3. Fahren Sie fort wie in der jeweiligen Anleitung beschrieben, falls erforderlich.

Sie haben die Benutzer- / Personalnummer erfolgreich eingegeben.

5.7 Benutzergruppen

Optional (mit Lizenz für Benutzergruppe 2 via Netzwerk). Die an den Schlössern gespeicherten Personen / Benutzer eines jeden Systems können in zwei Gruppen eingeteilt werden:

Der Systemmanager aktiviert Option „Benutzergruppen“ im Menü.

Der Schlossmaster meldet PIN-Code für Benutzer 99 an.

Ab Werk ist eingestellt, dass Benutzergruppe 1 die Benutzer Nr. 01 bis Nr. 09 umfasst und Benutzergruppe 2 mit Benutzer Nr. 10 beginnt und mit Nr. 99 endet. Via optionaler Software kann die Gruppengröße angepasst werden (z.B. CashProtectPro: Code / Benutzergruppen / Beginn 2. Benutzergruppe).

Der Schlossmaster verwaltet die Benutzer der ersten Gruppe, der Benutzer 99, der bei Einstellung „Benutzergruppen“ als WTU-Master fungiert, verwaltet die Benutzer der zweiten Gruppe.

5.7.1 Bedienung mit „Benutzergruppen“ aktiviert

Vorsicht

Ohne autorisierten WTU-Master mit angemeldetem Code kann der WTU-Benutzerbereich nicht verwaltet werden.
Statten Sie Benutzer 99 **vor der Wahl von ‚Benutzergruppen‘** mit allen erforderlichen Rechten aus (siehe Abschnitt „Benutzer autorisieren“) und melden Sie Code für ihn am Schloss an.

Über Feld „Öffnung Benutzergruppen zwingend“ via Bereich „Code Einstellungen“ von CashProtectPro kann eingestellt werden, ob die Gruppenmitglieder bei „4-Augen-Prinzip (Öffnung)“ oder „Parallelcode“

- nur gemeinsam mit Mitgliedern ihrer Gruppe (Wert: „gleich“) oder
- nur mit einem Mitglied der anderen Gruppe (Wert: „verschieden“) oder
- mit einer Person einer beliebigen Gruppe (Wert: „keine“) öffnen können.

Bei der Wahl von ‚Benutzergruppen‘ (siehe „Zwei ‚Benutzergruppen‘ wählen“ in diesem Kapitel) werden die Benutzer jedes Schlosses in zwei Gruppen eingeteilt.

Die Gruppengröße wird via PC-Software definiert (ab Werk Benutzer 01-50 bei Schlossmaster und Benutzer 51-98 bei WTU-Master).

Der Schlossmaster verwaltet die erste Gruppe (Benutzer 01 bis XX-1). Benutzer 99, der zum WTU-Master wird, verwaltet die WTU-Benutzer (Benutzer XX bis 98).

5.7.2 Master / WTU-Master wählen

Schloss- und WTU-Master wählen vor ihrer Code-Eingabe zusätzlich „Master“ beziehungsweise „WTU-Master“:

1. Führen Sie als Master / WTU-Master die Schritte einer Anleitung aus, bis Code-Eingabe nötig ist.
Vor jeder Master- oder WTU-Mastercode-Eingabe zeigt das Display bei aktiver WTU-Funktion: Code-Eingabe | Benutzer: Master und springt nicht weiter zur Code-Eingabe.
2. Bestätigen Sie **Master** mit **Enter** oder wählen Sie mit den Menütasten **<** und **>** **WTU-Master** und **Enter**.
Das Display zeigt WTU-Master oder Master, Code-Eingabe, gegebenenfalls 0123456789 und Code:.
3. Fahren Sie gegebenenfalls fort wie in der jeweiligen Anleitung beschrieben.
Sie haben erfolgreich Master / WTU-Master gewählt.

5.8 Passwörter (VS) / Benutzer autorisieren

5.8.1 Passwörter in verteilten Systemen (VS)

Nur mit TwinNet 10.3 und höher und mit Netzwerkanschluss, ab Firmware Version 25/26. Passwörter in verteilten Systemen müssen aus mindestens 8 Zeichen bestehen und mindestens 2 der Merkmale Groß- und Kleinschreibung, Ziffern oder Sonderzeichen enthalten.

Vorsicht

Mit werksseitigen Passwörtern ist das System nicht gesichert.

Gefahr von Manipulation.

Ändern Sie werksseitige Passwörter aus Sicherheitsgründen sofort nach der Installation.

Passwörter, die einfach sind (z.B. 123456 oder Namen) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden.

Gefahr der unberechtigten Manipulation.

Wählen Sie keine derartigen Passwörter.

Dies gilt auch für Passwörter, die gegebenenfalls von autorisierten Benutzern neu erstellt werden müssen.

5.8.2 Benutzer autorisieren

Vor der Code-Eingabe geben Benutzer ihre Benutzer- oder Personalnummer (Pers-Nr.) ein. Das folgende gilt nicht für den Betrieb mit flexiblen Einmalcodes, für den Personalnummern erforderlich sind. Siehe die Beschreibungen oben.

Davon abgesehen, definiert der Systemverwalter die Autorisierung von Benutzern via CashProtectPro in einer Matrix, indem er für Benutzer Kontrollkästchen aktiviert (Beschreibung der Kontrollkästchen siehe unten). Diese Autorisierung ist fest eingestellt. Mit der optionalen PC-Software ist sie auch änderbar.

Damit diese Berechtigungen im Schlosssystem TwinLock CashProtect gelten, importiert der Systemverwalter die Konfiguration aus der PC-Software in das System TwinLock CashProtect.

Damit ein Benutzer ein Schloss öffnen kann, muss der Schlossmaster (Inhaber des Mastercodes dieses Schlosses) für den Benutzer außerdem mindestens

- PIN-Code beziehungsweise PIN-Code und Karte zur Identifikation am Schloss angemeldet haben.

Wenn für Benutzer das Kästchen **Freigabe** in der Benutzermatrix nicht markiert ist, haben die Benutzer keine Rechte und sind für alle Funktionen gesperrt.

Autorisierung zum Öffnen eines Schlosses mit PIN-Code:

Der Systemmanager aktiviert für den Benutzer die Kontrollkästchen **PIN-Code**, **Freigabe** und **Öffnen**.

Autorisierung zur Benutzer-Identifikation mit RFID:

Der Systemmanager aktiviert für den Benutzer die Kästchen **Chipkarte**, **Freigabe** und **Öffnen**. Zusätzlich muss via CashProtectPro, Seite „Einstellungen“, der passende Wert „DESFire“ für Parameter „Codekarte“ für die Benutzeridentifikation eingestellt sein.

Vorsicht

Gefahr, das System nicht mehr öffnen zu können.

Gefahr des Verlusts der Bedienbarkeit des Systems.

Stellen Sie stets sicher, dass genügend Benutzer mit Öffnungsbeziehung angelegt sind, besonders dann, wenn 4-Augen-Prinzip oder Parallelcode konfiguriert wurde.

5.8.3 Kontrollkästchen der Benutzermatrix

Die Benutzermatrix kann via PC-Software angezeigt und gegebenenfalls auch bearbeitet werden.

Vorsicht

Benutzer können kein Schloss öffnen, wenn sie nicht ausreichend autorisiert sind.

Deaktivieren Sie ab Werk aktivierte Kontrollkästchen in der Benutzermatrix nur, wenn Sie dieses Handbuch gelesen haben und, falls erforderlich, nach Beratung durch eine Fachkraft für das System. Aktivieren Sie bei Bedarf weitere Kontrollkästchen wie „Chipkarte“.

Damit ein Benutzer bestimmte Bedienvorgänge ausführen kann, müssen ihm alle dafür nötigen Berechtigungen verliehen werden.

Benutzer und Schlossmaster (=Benutzer 00) können vom Systemmanager, der selbst nicht öffnen kann, zur Öffnung von Schlössern autorisiert werden.

Hinweis

Zusätzlich zur Benutzer-Autorisierung kann der Systemmanager zwei Benutzergruppen definieren (auf Seite „Einstellungen/Code“ der PC-Software) und für diese Öffnungsbedingungen festlegen. Siehe Abschnitt „Bedienung mit ‚Benutzergruppen‘ aktiviert“ unten in diesem Kapitel.

Es folgt eine Liste aller Kontrollkästchen, die es in der Benutzermatrix gibt. Der Systemmanager kann bestimmte Berechtigungen ändern.

Felder / Kontrollkästchen

PIN-Code	Berechtigung zur Eingabe von PIN-Code
Chipkarte	Berechtigung zur Eingabe via Karte (RFID-Karte)
1 aus x	Berechtigung, entweder mit PIN-Code zu öffnen
2 aus x	Berechtigung, mit 2 Authentifikationsarten zu öffnen (nicht genutzt)
Schnellöffnung	Berechtigung, Schloss trotz aktiver Zeitprogramme (z.B. Wochenprog., Sperrzeit) zu öffnen
Freigabe	allgemeine Freigabe für die Systembedienung
Öffnen	Berechtigung zum Schloss-Öffnen
Schließen	Berechtigung, mit Code-Eingabe zu schließen (falls Schließen mit Code)
Service	Berechtigung, die Konfiguration zu importieren / Wochenprogramme zuzuweisen
2-Augen	Berechtigung, trotz gesetztem 4-Augen-Prinzip allein öffnen / schließen zu dürfen.

Vorsicht

Bei Systemen mit Einbruchmeldeanlage kann ein Benutzer (auch Schlossmaster) ein Schloss nur öffnen, wenn er zum Unscharf Schalten befugt ist.

Entfernen Sie die Markierung aus Kästchen **Unscharf** nicht für Benutzer, die Schlösser öffnen sollen.

Unscharf	Berechtigung zum Unscharf Schalten einer externen Einbruchmeldeanlage.
WP1 – WP5	Berechtigung für Wochenprogramm 1-5
Sprache	Optionale benutzerspezifische Spracheinstellung, nicht verfügbar.
Personal-Nr.	Feld für den Eintrag einer bis zu 6-stelligen Personalnummer. Nur wenn das Kontrollkästchen 'Personalnummer' über der Benutzermatrix markiert ist, geben alle Benutzer an der Bedieneinheit ihre Personal- statt ihrer Benutzernummern ein, bevor sie ein Schloss öffnen können.
Templatename	keine Berechtigung, optional, gegebenenfalls Anzeige des Namens von Benutzern zugeordneten Templates (falls Templates nach Zuordnung nicht gelöscht oder umbenannt wurden)

5.8.4 Berechtigungen ab Werk via CashProtectPro

Diese voreingestellten Berechtigungen sind teilweise in der Benutzermatrix von CashProtectPro sicht- und änderbar.

Manager (Nr.225): PIN-Code | Freigabe | Service (nicht änderbar)

Master (Nr.00): PIN-Code | Freigabe | (erweiterbar)

Benutzer:
(Nr.01-99) keine (programmierbar)

5.8.5 Berechtigung Master / Benutzer / etc.

Übersicht der Berechtigungen von Master (Nr.00), Benutzer (Nr.01-99), Manager (Nr.225) sowie gegebenenfalls von WTU-Master / Master Gruppe 2 (Nr.99) im Menü von QPad.

Beschreibung der Standardeinstellung, via Benutzermatrix teilweise änderbar.

Manager (Nr.225):	eigenen Code ändern, Systemzeit setzen Codes und Karte von Master verwalten, gegebenenfalls System IDs A und B verwalten, WTU-Funktion wählen, Stand des Vorgangszählers prüfen und setzen, Konfiguration und Sprachen im- und exportieren, Protokoll exportieren, Benutzergruppen definieren, Schlösser anmelden, Reset Lizenzeneinstellungen ändern, Netzwerkeinstellungen setzen, Alarmgeräte ein- und ausschalten
optional:	Codeverknüpfung, Parallelcode, Zwangsfolge wählen, Zeitverzögerung pro Schloss / Wochenprogramm setzen, Wochenprogramme definieren
Master (Nr.00):	eigenen Code ändern, Codes und Karten von Schlossbenutzern verwalten, Schlösser öffnen und schließen, gegebenenfalls Einbruch- meldeanlage (EMA) un- / scharf schalten), Motorservice, 1x Riegelwerk ignorieren, Neustart, Sprache wählen und importieren, Konfiguration im- und exportieren, Protokoll exportieren
WTU-Master (Nr.99) / Master Gruppe 2: (optional)	eigenen Code ändern, Codes und Karten für Schlossbenutzer Nr.XX-98 verwalten, Schlösser öffnen und schließen, gegebenenfalls Einbruch- meldeanlage (EMA) un- / scharf schalten, Motorservice, 1x Riegelwerk ignorieren, Neustart, Sprache wählen und importieren, Konfiguration im- und exportieren, Protokoll exportieren
Benutzer (Nr.01-98/99):	eigenen Code ändern, Schlösser öffnen und schließen, gegebenenfalls EMA un- / scharf schalten, 1x Riegelwerk ignorieren, Neustart, Sprache wählen und importieren, Konfiguration und Protokoll exportieren

5.9 Menüführung in der Bedieneinheit

5.9.1 Firmwareversion 25/26

(bei geöffnetem System, alle Menüs aller Systeme)⁸

Systemmenü mit Anzeige Mo 05.08.24 8:35

Oeffnen

Schliessen

Scharfschalten (optional)

Status / Info

Einstellungen	-	Manager	-	Code aendern	
			-	Master	- Anmelden
					Abmelden
					Benutzer-Anzeige
			-	Datum / Uhrzeit	
			-	Codeverknüpfung	
					Oeffnen
					Konfiguration
					Freigabezeit
				Parallelcode	
				Zwangsfolge	
				Zeitverzögerung	
					Schloss
					Wochenprogramme
			-	Wochenprogramm	
			-	Alarmgeräte	
					XT-Erweiterung
					TwinAlarm
			-	Pairing	
			-	Kundenschlüssel	
			-	Codeverteilung	
			-	Server Modus	
			-	Initialcode	
			-	Einmalzugang	(nicht C690)
				System ID A/B	(nicht C690)
					Kundenschlüssel
					Code-Eingabe
			-	WTU Funktion	(nicht C690)
			-	Vorgangszähler	(nicht C690)
			-	Benutzergruppen	(via Netzwerk nur mit Extra-Lizenz)
		Master	-	Code aendern	
				PIN-Code	- Anmelden
					Abmelden
					Benutzer-Anzeige
			-	Codekarte	- Anmelden
					Abmelden
					Benutzer-Anzeige
		Mitarbeiter	-	Code aendern	
Service		Werkseinstellung	-	Terminal	(für neuen Setup des Systems)
			-	Schloss	
		Motor Schritt			
		Schloss anmelden			
			-	Schloss neu	
			-	Schloss wechseln	
		1x Riegelwerk			
		Lizenzierung			
		Neustart		(Parameter unverändert)	
		Firmwareupdate			
Import / Export					

Zusätzlich gibt es das versteckte Menü mit den Punkten

Sprache, Datum/Uhrzeit, Alarmgeräte, Terminal, Protokoll, Batterie und Netzwerk.

Siehe „Verstecktes Menü anzeigen“ auf S. 57.

Die Firmwareversionen CP25/26 sind für B670, die Versionen CQ25/26 für C690.

5.10 PIN-Codes

Vorsicht

Geben Sie Code nur in sicherer Umgebung ein.

Mit werksseitigen Systemmanager- und Mastercodes ist das System nicht gesichert.

Gefahr der unberechtigten Öffnung.

Ändern Sie werksseitige Codes aus Sicherheitsgründen sofort nach der Installation.

Codes und Passwörter, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden.

Gefahr der unberechtigten Öffnung.

Wählen Sie keine derartigen Codes und Passwörter.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

Der Masterode kann gelöscht werden.

Gefahr von Funktionsverlust.

Löschen Sie den Mastercode nicht. Falls erforderlich, kann der Manager den Master neu autorisieren.

5.10.1 Arten und Anzahl von PIN-Codes in jedem Schloss

- 1 Managercode (ohne Berechtigung zur Öffnung des Schlosses)
- 1 Mastercode (mit optionaler Berechtigung zur Öffnung des Schlosses)
- 1 optionaler WTU-Mastercode (mit opt. Berechtigung zur Öffnung des Schlosses)
- 1-99 PIN-Codes für Benutzer (mit optionaler Berechtigung zur Öffnung des Schlosses, siehe auch Abschnitt „Benutzer-Autorisierung“)

Mit dem **Managercode** des Schlosses Nr.1 kann das gesamte System konfiguriert werden. Deshalb wird er als **Systemmanagercode**, kurz als Systemcode, bezeichnet und sein Inhaber als Systemmanager. Der Inhaber dieser Codes verwaltet gegebenenfalls auch die System IDs A und B.

Mit dem **Mastercode** jedes Schlosses können die Benutzercodes des Schlosses an- und abgemeldet werden. Sein Inhaber wird als Schlossmaster bezeichnet. Er kann vom Systemmanager optional zur Schloss-Öffnung autorisiert werden. Managercodes können nicht abgemeldet werden.

Mit jedem vom Schlossmaster am Schloss angemeldeten **PIN-Code für Benutzer** kann das Schloss geöffnet werden, wenn der Benutzer dazu autorisiert wurde.

PIN-Codes für Benutzer sind werksseitig nicht programmiert. Über die Benutzermatrix der PC-Software ist definiert, zu welchen Aktionen sie berechtigen. Sie können vom Schlossmaster an- und abgemeldet werden. Abhängig von ihrer Autorisierung können Benutzer gegebenenfalls ihren Code ändern.

Die Anzahl der Ziffern im PIN-Code (für Benutzer-, Master-, Manager- und Systemmanager) ist abhängig von der VdS-Klasse des Systems.

Die **VdS-Klasse** kann in Menü `Status / Info` auf dem Display der Bedieneinheit angezeigt werden. Systeme der VdS-Klasse 2(DS) enthalten mindestens Schlösser des Typs VdS 2, solche der Klasse 3(DS) mindestens Schlösser des Typs VdS 3. Bei Systemen der VdS-Klasse 2(DS) und 3 / 3(DS) sind PIN-Codes achtstellig, bei Systemen der VdS-Klasse 2 sind PIN-Codes sechstellig oder optional 8-stellig.

Master- und Systemmanagercodes ab Werk		
	Master	System / Manager
VdS Klasse 2	123456 (Benutzer 00)	111111 (Benutzer 225)
VdS Klasse 2 (opt.)/ 2(DS)	12345600 (Ben. 00)	11111100 (Ben. 225)
VdS Klasse 3 / 3(DS)	12345678 (Ben. 00)	11111111 (Ben. 225)

5.10.2 PIN-Code eingeben

Mit welchen Tasten die Benutzer an der Bedieneinheit ihre persönliche PIN oder ihren PIN-Code eingeben können, ist abhängig vom System / der Konfiguration:

Bei VdS Klasse 3 und 2(DS)/3(DS) Schlössern nur mit Menütasten.

Bei VdS Klasse 2 Schlössern optional mit Zifferntasten oder mit Menütasten (via PC-Software / TwinNet einstellbar).

Einmalcode (OTC): nur mit Zifferntasten.

5.10.3 PIN-Code mit Menütasten eingeben

Systeme der VdS Klasse 3/3(DS): Code-Eingabe mit Menütasten.

Systeme der VdS Klasse 2(DS): Code-Eingabe mit Menütasten optional.

Vorbedingungen Sie sind dazu autorisiert worden, mit PIN-Code zu öffnen. Ihr PIN-Code ist am Schloss angemeldet.

1. Führen Sie Schritte einer Anleitung aus, bis Code-Eingabe nötig ist.

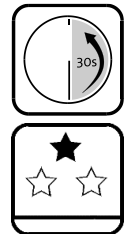
*Das Display zeigt vor der Code- Eingabe unter anderem
0123456789. Der Cursor bei einer beliebigen Ziffer.*

2. Wählen Sie mit > jeweils eine Ziffer des Codes und jeweils Enter.

*Das Display zeigt für jede eingegebene Ziffer ein Sternchen (Asterisk): Code :
***. Nach der Eingabe zeigt das Display die jeweils folgende Meldung wie
beispielsweise Bitte warten.*

3. Fahren Sie fort wie in der jeweiligen Anleitung beschrieben.

Sie haben den PIN-Code erfolgreich eingegeben.



5.10.4 PIN-Code mit Zifferntasten eingeben

Systeme der VdS Klasse 2 (ab Werk).

Vorbedingungen Sie sind dazu autorisiert worden, mit PIN-Code zu öffnen. Ihr PIN-Code ist am Schloss angemeldet.

1. Führen Sie Schritte einer Anleitung aus, bis Code-Eingabe nötig ist.

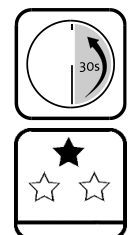
*Das Display zeigt vor der Code-Eingabe **nicht** 0123456789, sondern unter anderem Benutzer Nr. | Code:. Der Cursor steht an der Stelle für die erste Ziffer. Daran ist erkennbar, dass der Code mit den Zifferntasten einzugeben ist.*

2. Wählen Sie die Ziffern des Codes mit den Zifferntasten.

*Das Display zeigt für jede eingegebene Ziffer ein Sternchen (Asterisk): Code :
***. Nach der Eingabe zeigt das Display die jeweils folgende Meldung wie
beispielsweise Bitte warten.*

3. Fahren Sie fort wie in der jeweiligen Anleitung beschrieben.

Sie haben den PIN-Code erfolgreich eingegeben.



5.11 RFID Karten

Vorsicht

Gefahr des Verlustes von Daten / Karten.

Beachten Sie die Sicherheitsrichtlinien und bewahren Sie Karten stets an Orten auf, zu denen nur Sie Zugang haben. Tun Sie dies so, dass die Daten geschützt sind (Alufolie oder geeignete Schutzhüllen, Scrambler-Karten).

Scrambler-Karte: NFC Karte, die Karten in der Nähe gegen Auslesen schützt: Durch erzeugte Störungen wird ein Leser gezwungen, die Kommunikation zu beenden, bevor sensible Daten übertragen werden können.

Optionale **RFID Karten** können nur vom Systemmaster angemeldet werden. Pro Schloss kann für bis zu 99 Benutzer je eine RFID Karte mit oder ohne Benutzercode am Schloss an- und abgemeldet werden. Werksseitig sind die Kartencodes für die Benutzer 01 – 99 inaktiv. Siehe auch Abschnitt „Benutzer autorisieren“. RFID Karten können via Kartenleser angemeldet werden. Siehe auch Handbuch TwinNet.

Über das Register „Einstellungen“ einer Schlosssystemkonfiguration von TwinNet oder CashProtectPro kann die Art der Codekarte beispielsweise auf Mifare DESFire eingestellt werden, womit die RFID Karte zur Codekarte gemacht werden kann. Auf einer RFID Karte können Daten zur Identifikation, die Personalnummer oder die persönliche PIN oder alles zusammen gespeichert werden.

5.11.1 RFID Karte mit Leser einlesen

Für dieses System gibt es RFID Karten. Siehe auch Abschnitt „RFID Karten“ oben. Via RFID Karte können die Personalnummer oder die persönliche PIN (für die Eingabe von flexiblem Einmalcode) oder diese beiden Nummern zusammen gespeichert übermittelt werden.



Vorbedingungen

- Sie sind zum Öffnen auch mit **Karte** autorisiert.
- Der Systemmanager hat ‚DESFire‘ als Codekarte eingestellt.
- für Sie sind zum Öffnen in der Benutzermatrix (CashProtectPro) / Schlosskonfiguration (TwinNet) die Kästchen **Karte**, **Freigabe** und **Öffnen** aktiviert.

Sie benötigen

- eine optionale RFID-Karte



Abb. 18: RFID-Karten und Kartenleser

1. Wenn das Display der Bedieneinheit **Lesen Daten** anzeigt, halten Sie die RFID Karte sehr nahe vor die Optionsbox RFID von QPad.

Die Karte wird gelesen.

2. Warten Sie, bis das Display **Bitte warten** anzeigt.
3. Entfernen Sie die RFID-Karte.

Sie haben die Karte erfolgreich eingelesen.

5.12 Öffnen und Schließen

Je nach Konfiguration des Schlosssystems geben Benutzer vor der Code-Eingabe ihre Benutzer- oder ihre Personalnummer (Pers-Nr.) ein. In den folgenden Beschreibungen wird meist nur eine dieser Möglichkeiten beschrieben.

Vorsicht

Wenn am Display „Neustart oder Stromlos“ angezeigt wird, könnte ein Manipulationsversuch stattgefunden haben.

Unterziehen die Bedieneinheit einer Sichtprüfung auf Beschädigung. Wenn erforderlich, kontaktieren Sie eine Sicherheitskraft. Die Meldung wird nach Code-Eingabe und Öffnung nicht mehr angezeigt.

Bei Systemen mit Einbruchmeldeanlage (EMA) können Benutzer kein Schloss öffnen, wenn sie nicht zum Unscharf Schalten autorisiert sind.

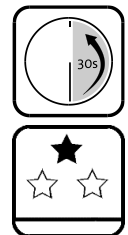
Wenn eine EMA angeschlossen ist, markieren Sie für Benutzer in der Benutzermatrix von PC-Software auch Kästchen Unscharf.

Um das System zu entsperren, öffnen Sie je nach Systemeinstellung alle Schlösser oder nur Schloss 1. Siehe auch Abschnitt „Systemstatus“.

Abhängig von der Konfiguration kann zum Öffnen die Eingabe von Code auch von mehreren Benutzern erforderlich sein.

5.12.1 Schloss mit PIN-Code öffnen

Vorbedingungen Die Kästchen **PIN-Code**, **Freigabe**, (**1 aus x**), **Öffnen** und **Unscharf** sind in der Benutzermatrix für sie markiert. PIN-Code wurde für Sie am Schloss angemeldet.



- Drücken Sie kurz die Taste **Clear**, sowie gegebenenfalls Taste **>** und Taste **Enter**, um **Oeffnen** zu wählen.
Das Display zeigt gegebenenfalls Code-Eingabe | Schloss 1.
- Wählen Sie mit **>** gegebenenfalls das Schloss und **Enter**.
Das Display zeigt gegebenenfalls Code-Eingabe | Standard.
- Bestätigen Sie **Standard** mit Taste **Enter**.
Das Display zeigt Code-Eingabe | Benutzer: Master.
- Wählen Sie mit **>** die Benutzer- oder die Personalnummer und bestätigen Sie gegebenenfalls mit **Enter**.
Das Display zeigt Code-Eingabe | Benutzer: 01 oder Code-Eingabe | Pers-Nr: XXXXXX und Benutzer / Pers-Nr: XXXXXX | PIN-Code.
- Bestätigen Sie mit **Enter**.
Das Display zeigt Benutzer Nr / Pers-Nr: XXXXXX, gegebenenfalls 0123456789 und Code: . Siehe auch „PIN-Code eingeben“ ab Seite 46. Das Display zeigt Code-Eingabe | Benutzer: Master.
- Geben Sie Ihren PIN-Code ein.
Das Display zeigt Oeffnen| Bitte warten. Der Riegel des Schlosses fährt ein. Das Display zeigt Oeffnen | Schloss auf: Nr. und gegebenenfalls System entsperrt.

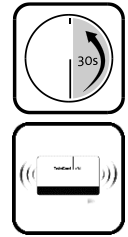
Sie haben das Schloss erfolgreich geöffnet.

5.12.2 Schloss mit RFID-Karte öffnen

Vorbedingungen Die Kästchen **Karte**, **Freigabe**, (**1 aus x**), **Öffnen** und, falls erforderlich, **Unscharf** sind in der Benutzermatrix für sie markiert. Der Schlossmaster hat Ihre Karte am Schloss angemeldet.

Sie benötigen eine optionale RFID-Karte.

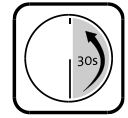
1. Drücken Sie kurz die Taste **Clear**, sowie gegebenenfalls Taste **>** und Taste **Enter**, um **Oeffnen** zu wählen.
Das Display zeigt gegebenenfalls Code-Eingabe | Schloss
2. Wählen Sie mit **>** und **Enter** gegebenenfalls das Schloss.
Das Display zeigt gegebenenfalls Code-Eingabe | Standard.
3. Bestätigen Sie **Standard** mit Taste **Enter**.
Das Display zeigt Code-Eingabe | Benutzer: Master.
4. Wählen Sie mit **>** die Benutzer- oder die Personalnummer und bestätigen Sie gegebenenfalls mit **Enter**.
*Das Display zeigt beispielsweise Code-Eingabe | Benutzer: 01
 und Benutzer Nr. | PIN-Code.*
5. Wählen Sie mit **>** **Karte** und **Enter**.
Das Display zeigt Lese Daten.
6. Lesen Sie die RFID-Karte ein.
*Siehe auch Seite 47. Das Schloss öffnet.
 Das Display zeigt Bitte warten.*
7. Entfernen Sie die Karte.
*Die Eingabe einer weiteren Art von Code ist erforderlich. Wählen Sie PIN-Code
 und geben Sie diese Codeart ein. Siehe oben.
 Falls PIN-Code bereits eingegeben wurde, zeigt das Display
 Oeffnen | Bitte warten. Der Riegel des Schlosses fährt ein.
 Das Display zeigt Oeffnen | Schloss auf: Nr.*



Sie haben das Schloss erfolgreich geöffnet.

5.12.3 Beim Öffnen Stillen Alarm auslösen

So können Sie im Fall einer Bedrohung unauffällig Hilfe verständigen. Der Alarm kann **nicht via Karte** aktiviert werden. Bei PIN-Code wird er wie unten beschrieben aktiviert.



Vorbedingungen Sie sind dazu autorisiert worden, mit PIN-Code zu öffnen und die Einbruchmeldeanlage (EMA) unscharf zu schalten. Ihr PIN-Code ist am Schloss angemeldet. Option „Stiller Alarm“ ist via optionaler Software aktiviert.

Sie benötigen eine aktivierte Einheit TwinXT / TwinAlarm und eine EMA.

1. Drücken Sie kurz die Taste `Clear`, sowie gegebenenfalls Taste `<` oder Taste `>` und Taste `Enter`, um `Oeffnen` zu wählen.
2. Wählen Sie mit `>` und `Enter` gegebenenfalls das Schloss.
3. Bestätigen Sie gegebenenfalls `Standard` mit Taste `Enter`.
4. Wählen Sie mit `<` oder `>` und `Enter` oder mit den Zifferntasten und `Enter` die Benutzernummer.
5. Bestätigen Sie Sie `PIN-Code` mit Taste `Enter`.
6. Wählen Sie mit `<` und `>` alle Ziffern Ihres Codes außer der letzten. Bestätigen Sie jeweils mit `Enter`.
7. Wählen Sie mit `<` und `>` statt der letzten Ziffer (z.B. 8) deren Wert plus der via Software gesetzten Alarmziffer, beispielsweise „+1“, also insgesamt z.B. 9 und bestätigen Sie mit `Enter`.

Falls der die Summe größer 9 ist, geben Sie statt „10“ eine Null ein, statt „11“ „1“, statt „12“ „2“ usw.

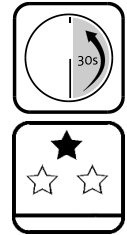
Die Display-Anzeige und gegebenenfalls auch der weitere Öffnungsvorgang sind genau so wie bei einer „normalen“ Öffnung.

Sie haben den Alarmcode eingegeben und erfolgreich Stillen Alarm ausgelöst.

5.12.4 Schloss mit Codeverknüpfung öffnen

Nur wenn jeder der zwei beteiligten Benutzer alle ihm zugeteilten Arten der Authentifizierung durchführt, öffnet sich das Schloss.

Vorbedingung Kontrollkästchen „4-Augen-Prinzip (Öffnung)“ ist aktiviert worden.



1. Drücken Sie kurz die Taste `Clear`, sowie gegebenenfalls Taste `>` und Taste `Enter`, um `Oeffnen` zu wählen.
2. Wählen Sie mit `>` und `Enter` gegebenenfalls das Schloss.
3. Bestätigen Sie gegebenenfalls `Standard` mit Taste `Enter`.
4. Wählen Sie mit `>` und `Enter` oder mit den Zifferntasten und `Enter` Ihre Benutzernummer.
5. Wählen Sie gegebenenfalls mit `ENTER` `PIN-Code` und führen Sie alle Schritte wie beim normalen Öffnen des Schlosses aus.
*Siehe die Beschreibungen „Schloss mit ... öffnen“ am Anfang des Kapitels.
 Den nächsten Schritt führt eine zweite Person aus.
 Das Display zeigt `Code-Eingabe &2 | Master`.*
6. Ein zweiter Benutzer belegt seine Autorisierung am Schloss.
Das Display zeigt `Oeffnen | Schloss auf: Nr.`

Gemeinsam mit einer zweiten Person haben Sie das Schloss erfolgreich mit Codeverknüpfung geöffnet.

5.12.5 Schloss mit Öffnungsverzögerung öffnen

Vorbedingung Die optionale Funktion „Öffnungsverzögerung“ ist eingestellt.



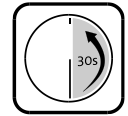
1. Drücken Sie kurz die Taste `Clear`, sowie gegebenenfalls Taste `>` und Taste `Enter`, um `Oeffnen` zu wählen.
2. Wählen Sie mit `>` und `Enter` gegebenenfalls das Schloss.
3. Bestätigen Sie gegebenenfalls `Standard` mit Taste `Enter`.
4. Wählen Sie mit `>` und `Enter` oder mit den Zifferntasten und `Enter` die Benutzernummer.
5. Wählen Sie gemäß Ihrer Autorisierung mit `<` und `>` `PIN-Code` und führen Sie alle Schritte wie beim normalen Öffnen des Schlosses aus.
*Siehe die Beschreibungen „Schloss mit ... öffnen“ am Anfang des Kapitels.
 Das Display zeigt `Oeffnen | Zeit: 00:00`.*
6. Warten Sie, bis die Zeit der Öffnungsverzögerung abgelaufen ist.
*Die Bedieneinheit piept.
 Das Display zeigt `Oeffnen | Schloss auf: Nr.`*

Sie haben das Schloss erfolgreich geöffnet.

5.12.6 Mit Öffnungsverzögerung und Freigabezeit öffnen

Diese Anleitung ist eine Weiterführung der vorhergehenden.

Vorbedingungen Siehe vorhergehenden Abschnitt. Zusätzlich ist Option 'Freigabezeit' aktiviert.



1. Führen Sie Schritte 1-5 der vorhergehenden Handlungsanleitung aus und bereiten Sie sich darauf vor, eingeben zu können.

Das Display zeigt Code-Eingabe | Benutzer: Master.

Ein akustisches Signal zeigt den Ablauf der Verzögerungszeit an.

Während der folgenden Freigabezeit ertönt alle 2 Sekunden ein Signal.

2. Wählen Sie gegebenenfalls mit > das Schloss und Enter.
Das Display zeigt Code-Eingabe | Benutzer: Master.
3. Wählen Sie mit > und Enter oder mit den Zifferntasten Ihre Benutzernummer.
4. Geben Sie Ihre(n) Code(s) ein.

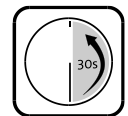
Siehe Schritt 6 der vorhergehenden Anleitung. Ein akustisches Signal ertönt wiederholt. Das Display zeigt Oeffnen | Schloss auf: 1.

Sie haben das Schloss erfolgreich geöffnet.

5.12.7 Schlösser mit Parallelcode öffnen

Ein Benutzer öffnet Schloss 1 und ein zweiter gegebenenfalls Schloss 2. Beide öffnen dabei gemäß ihrer Autorisierung.

Vorbedingungen Option „Parallelcode“ (nur für Systeme mit 2 Schlössern) ist via optionaler Software eingestellt. Für die Benutzer sind in der Benutzermatrix **Freigabe, Öffnen, PIN-Code** und / oder **Chipkarte** (und **Unscharf**) aktiviert. Der Schlossmaster hat PIN-Code (und gegebenenfalls Codekarten) am Schloss angemeldet.



1. Öffnen Sie Schloss 1 gemäß Ihrer Autorisierung.
Siehe die Anleitungen zum Öffnen am Anfang des Kapitels. Schloss 1 öffnet sich. Das Display zeigt Oeffnen | Schloss auf: 1.
2. Ein anderer, zweiter Benutzer wiederholt Schritt 1 an Schloss 2.
Das Display zeigt Oeffnen | Bitte warten. Der Riegel fährt ein. Das Display zeigt Oeffnen | Schloss auf: 2.

Sie haben die Schlösser in Ihrem System erfolgreich geöffnet.

5.12.8 Schloss mit flexiblem Einmalcode öffnen

Siehe auch „Betrieb mit flexiblen Einmalcodes“ auf Seite 35.

Wenn die Voraussetzungen erfüllt sind, können Benutzer Schlösser

- (mit Personalnummer,) mit RFID Karte und Einmalcode oder
- mit Personalnummer, persönlicher PIN und Einmalcode öffnen.

Vorbedingungen

siehe „Voraussetzungen für die Verwendung von flexiblem Einmalcode“ auf Seite 35.

1. Drücken Sie kurz die Taste **Clear**, sowie gegebenenfalls Taste **<** oder Taste **>** und Taste **Enter**, um **Oeffnen** zu wählen.
2. Wählen Sie mit **>** und **Enter** gegebenenfalls das Schloss.
Das Display zeigt gegebenenfalls Code-Eingabe | Standard.
3. Wählen Sie mit **>** und **Enter** gegebenenfalls **Einmalzugang**.
Das Display zeigt Einmalzugang | Master und Pers-Nr: XX.
4. Geben Sie ihre Personalnummer ein und bestätigen Sie mit **Enter**.
Das Display zeigt PIN-Code und Code: . Aus der Anzeige ist ablesbar, wie der Code einzugeben ist. Siehe Abschnitt „PIN-Code eingeben“.
5. Geben Sie Ihre persönliche PIN ein.
Das Display zeigt WTU-Funktion | Code: .
6. Geben Sie Ihren Einmalcode ein.
Das Display zeigt Oeffnen | Bitte warten und gegebenenfalls System entsperrt. Der Riegel des Schlosses fährt ein.

Sie haben das Schloss mit persönlicher PIN und flexiblem Einmalcode erfolgreich geöffnet.



5.12.9 Einbruchmeldeanlage (EMA) unscharf schalten

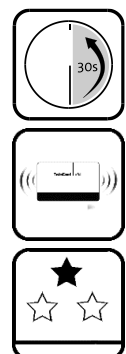
Wenn ein Benutzer nicht zum Unscharf Schalten autorisiert ist, kann er bei angeschlossener und scharf geschalteter EMA kein Schloss öffnen. Das Unscharf Schalten erfolgt automatisch mit dem Öffnen.

Vorbedingungen Für Sie sind **PIN-Code**, **Freigabe**, **Öffnen** und **Unscharf** aktiviert. TwinAlarm und EMA sind angeschlossen, alle Schlösser geschlossen, TwinAlarm ist aktiviert und die EMA scharf. Der Schlossmaster hat Ihren PIN-Code am Schloss angemeldet.

Sie benötigen gegebenenfalls eine RFID-Karte für die Benutzeridentifikation.

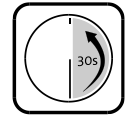
- Geben Sie Ihren PIN-Code ein und zeigen Sie die Codekarte.
Das Unscharfschalten erfolgt automatisch beim Öffnen. Siehe die Anleitungen zum Öffnen oben.

Sie haben geöffnet und die EMA erfolgreich unscharf geschaltet.



5.12.10 Schloss schließen

Beim Schließen nach einem Öffnen mit Einmalcode wird ein vierstelliger Rückcode **WTU-Code: XXXX** (optional QR-Code) auf dem Display der Bedieneinheit angezeigt, der beispielsweise telefonisch zurückgemeldet und vom zuständigen Mitarbeiter zum Abschließen des Vorgangs verwendet werden kann.



Der jeweils letzte Rückcode kann auch mit Menü **Status / Info** angezeigt werden.

Vorbedingung Der Riegelwerkskontakt ist nicht so eingerichtet, dass er bei geschlossenem Riegelwerk ein Schließen des Schlosses verhindert. Über Software ist nicht eingestellt, dass nur mit Code-Eingabe geschlossen werden kann.

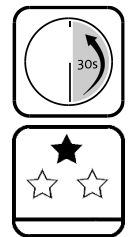
1. Öffnen Sie das Schloss (siehe oben).
2. Wählen Sie mit **>** und **Enter** **Schliessen**.
3. Wählen Sie mit **>** gegebenenfalls das Schloss und **Enter**.
*Das Display zeigt **Schliessen | Schloss zu: Nr.***

Sie haben das Schloss erfolgreich geschlossen.

5.12.11 Schloss mit Code-Eingabe schließen

Für das Schließen mit Code-Eingabe reicht es aus, entweder PIN-Code oder Karten einzugeben.

Vorbedingungen In der PC-Software ist auf Seite „Einstellungen“ Option „Manuelles Schliessen mit Code-Eingabe“ aktiviert.
Für Sie sind in der Benutzermatrix **Freigabe** und **Schließen, PIN-Code** oder **/** und **Chipkarte** aktiviert.



1. Drücken Sie kurz die Taste **Enter**.
Der Systemstatus wird geprüft. Das Display zeigt Uhrzeit und Datum.
2. Wählen Sie mit der Taste **>** **Schliessen** und **Enter**.
*Das Display zeigt **Schliessen** und gegebenenfalls **Schloss 1**.*
3. Wählen Sie mit **>** gegebenenfalls das Schloss und **Enter**.
*Das Display zeigt **Code-Eingabe | Benutzer: Master**.*
4. Identifizieren Sie sich als Benutzer.
Siehe auch „Benutzer- / Personalnummern“ auf Seite 38.
*Das Display zeigt gegebenenfalls **Benutzer Nr. | PIN-Code**.*
5. Wählen Sie **PIN-Code** und schließen Sie das Schloss, indem Sie PIN-Code eingeben.
*Siehe die Anleitungen zum Schloss-Öffnen am Anfang des Kapitels. Das Display zeigt **Schliessen | Bitte warten**. Der Schlossriegel fährt aus.*
*Das Display zeigt **Schliessen | Schloss zu: Nr.***

Sie haben das Schloss erfolgreich geschlossen.

5.12.12 Schloss mit Türschalter automatisch schließen

Diese Funktion kann mit PC-Software eingestellt werden.

Vorbedingungen TwinXT oder TwinAlarm sind angeschlossen und aktiviert. In der PC-Software ist auf Seite „Einstellungen“ Option „Automatisches Schließen mit Türschalter“ aktiviert. Der Riegelwerkskontakt ist nicht so eingerichtet, dass er automatisches Schließen verhindert.

- Schließen Sie die Tür des Wertbehältnisses.
Über Tür- und Riegelwerksschalter, deren Zustand regelmäßig geprüft wird, registriert das System das Schließen der Tür des Behältnisses und schließt das Schloss / die Schlösser automatisch, nachdem gegebenenfalls andere Prozesse noch abgeschlossen worden sind.

Das Schloss hat sich automatisch geschlossen.

5.12.13 Automatisches Schließen TK

Diese Funktion kann mit PC-Software eingestellt werden.

Vorbedingungen TwinXT oder TwinAlarm sind angeschlossen und aktiviert. In der PC-Software ist auf Seite „Einstellungen“ Option „Automatisches Schließen TK“ aktiviert. Der Riegelwerkskontakt ist nicht so eingerichtet, dass er automatisches Schließen verhindert.

- Schließen Sie die Tür des Wertbehältnisses.
Über Tür- und Riegelwerksschalter, deren Zustand regelmäßig geprüft wird, registriert das System das Schließen der Tür des Behältnisses und schließt das Schloss / die Schlösser sofort automatisch. Andere Prozesse werden gegebenenfalls abgebrochen.

Das Schloss hat sich automatisch geschlossen.

5.12.14 Einbruchmeldeanlage (EMA) scharf schalten

Abhängig von der Einstellung via PC-Software („Einstellungen / Alarm / TwinAlarm / Scharfschalten mit Code“ ein / aus) müssen Benutzer zum Scharf-Schalten PIN-Code eingeben oder nicht.



Vorbedingungen TwinAlarm und EMA sind angeschlossen. TwinAlarm ist aktiviert, EMA unscharf und alle Schlösser sind geschlossen. Nur so wird **Scharfschalten** zum Scharfschalten der EMA angezeigt.

In **Einstellungen Service Alarmgeräte** hat der Inhaber der Berechtigung „Service“ TwinAlarm auf **aktiv** gestellt. Für Sie hat der Systemmanager in der Benutzermatrix **Freigabe, PIN-Code** und / oder **Chipkarte** aktiviert.

Diese Einstellung kann auch via verstecktes Menü, Untermenü **Alarmgeräte**., gemacht werden.

Siehe „Verstecktes Menü anzeigen“ auf Seite 57.

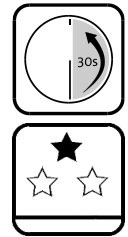
1. Sperren Sie das System, indem Sie Schloss 1 oder alle Schlösser schließen.
Siehe „Systemstatus“ in diesem Kapitel. Das System ist gesichert.
2. Drücken Sie kurz die Taste **Enter**.
Der Systemstatus wird geprüft. Das Display zeigt Datum und Uhrzeit.
3. Wählen Sie mit **<** und **>** **Scharfschalten** und danach **Enter**.
*Falls **! EMA scharf !** angezeigt wird, haben Sie die Aufgabe erfolgreich ausgeführt. Springen Sie zum Ende dieser Beschreibung.*
*Bei aktivierter Option „Scharfschalten mit Code“ zeigt das Display **Code-Eingabe | Benutzer: Master** und **PIN-Code**.*
4. Falls erforderlich, identifizieren Sie sich am Schloss und wählen Sie **PIN-Code** und **Enter**.
Siehe auch „Benutzer- / Personalnummern“ auf Seite 38. Die Code-Eingabe entspricht der beim Öffnen. Siehe die Anleitungen zum Öffnen in diesem Kapitel.
*Das Display zeigt **Benutzer: Nr. | Bitte warten**.*
Die Bedieneinheit gibt ein akustisches Signal aus.
*Das Display zeigt **Benutzer: Nr. | ! EMA Scharf !**.*

Sie haben die Einbruchmeldeanlage erfolgreich scharf geschaltet.

5.13 Verstecktes System, Status, Netzwerk

5.13.1 Verstecktes Menü anzeigen

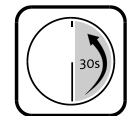
Bestimmte grundlegende Einstellungen können über das versteckte Menü gemacht oder überprüft werden. Jeder Benutzer kann das Menü anzeigen. Für bestimmte Einstellungen wie Sprach-Import, Setzen der Zeit, Einstellung der Alarmgeräte und des Netzwerks (mit Konfiguration oder via Service / Reset) ist der Systemmanagercode erforderlich.



1. Drücken Sie eine beliebige Taste und kurz *Clear*.
Datum und Uhrzeit werden angezeigt.
2. Drücken Sie *Enter* und halten Sie die Taste gedrückt.
Sprache wird angezeigt.
3. Bestätigen Sie *Sprache* mit *Enter* oder wählen Sie mit Taste *>* einen anderen Menüpunkt und bestätigen Sie diesen mit *Enter*.
Die Sprachauswahl, die Terminal-Einstellungen, das Protokoll und die Anzeige „Batteriespannung“ erfordern keinen Systemmanagercode.
4. Um andere Einstellungen vorzunehmen, geben Sie den Systemmanagercode ein und nehmen Sie anschließend die Einstellung vor.
Menüpunkt „Terminal“ betrifft Einstellungen der Bedieneinheit selbst:
„Lautsprecher“ = akustische Signalausgabe ein / aus
„Beleuchtung“ = Licht Display an / aus [Achtung: beeinträchtigt Lesbarkeit].
„Kontrast“ = Kontrast Schriftzeichen und Hintergrund der Bedieneinheit.
Jeweils Einstellung bestätigen, damit die darauf folgende angezeigt wird.

Sie haben erfolgreich das versteckte Menü angezeigt.

5.13.2 Status / Info des Systems anzeigen



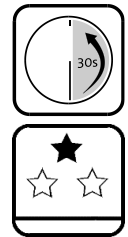
1. Drücken Sie kurz *Enter*.
Datum und Uhrzeit werden angezeigt.
2. Wählen Sie mit *<* und *>* *Status / Info* und bestätigen Sie mit *Enter*.
Mit ⏏ nächsten Punkt anzeigen, mit ⏪ vorherigen mit, Enter anhalten / fortsetzen, mit X (Clear) abbrechen. Es werden angezeigt:
 - Version Bedieneinheit (Terminal) sowie Bootloader-Meldungen
 - Seriennummer Bedieneinheit, gegebenenfalls die Lizenzversion
 - Sprachen Sprachplatz 1-3 inklusive jeweilige Version
 - Softwareversion von TwinIP und Basic TwinIP
 - Info Pairing, TwinAlarm und RFID-Modul, TPFW / TLIB (nicht relevant)
 - WTU Funktion (0=Bank, 1=Mix, 2=OTC), Spannung
 - Protokollzeiger (Zähler; noch nicht übertragen : an TwinIP übertragen)
 - Anzahl der Öffnungen und Stand Vorgangszähler
 - Firmwareversion des Schlosses / der Schlösser (c = verschlüsselt),
 - Art der letzten Öffnung, Benutzer bei Öffnung
 - System Check und gegebenenfalls die VdS-Klasse des Schlosssystems
 - Zustand des Schlosses 1 / 2 / 3 (zu / Mitte / auf)
 - Zustand des Systems (entsperrt / teilgesperrt / gesichert)
 - Zustand optionale EMA (scharf / unscharf)
 - aktueller Rückcode *WTU-Code : XXXX*, falls vorhanden.

Sie haben Informationen zu Systemkomponenten erfolgreich angezeigt.

5.13.3 Schloss mit Netzwerk verbinden

Die Server Adresse über den Browser des Client PCs einstellen: Adresse ab Werk 192.68.1.1 in Browser Eingabezeile eingeben, Namen „twinnet“ und Passwort „twinnetsetup“ in Pop-up Fenster eintragen, Schaltfläche OK wählen und in Feld „Server-Adresse“ der TwinIP Applikation die Server Adresse eingeben und „Accept“ wählen.

Die Netzwerk Einstellungen können über das versteckte Menü gemacht und überprüft werden. Jeder Benutzer kann das Menü anzeigen. Für die Einstellung des Netzwerks (Konfiguration oder automatische Einstellung / Neustart / Service / Reset) ist der Systemmanagercode erforderlich.



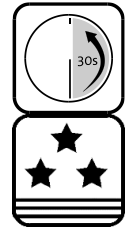
1. Drücken Sie eine beliebige Taste und kurz *Clear*.
Datum und Uhrzeit werden angezeigt.
2. Drücken Sie *Enter* und halten Sie die Taste gedrückt.
Sprache wird angezeigt.
3. Wählen Sie mit Taste < *Netzwerk* und bestätigen Sie mit *Enter*.
Code-Eingabe, Systemmanagercode | Code: wird angezeigt.
4. Geben Sie den Systemmanagercode ein.
*Netzwerk | *=Ja *=Nein wird angezeigt. Wenn Sie Nein wählen, können Sie die Einstellungen weder anzeigen noch ändern.*
5. Wählen Sie mit Taste *Enter* < **=Ja*.
Netzwerk | Gespeichert und Konfiguration wird angezeigt.
6. Wählen Sie mit Taste *Enter* < *Konfiguration*.
*Konfiguration | *=Ja *=Nein wird angezeigt.*
7. Wählen Sie bei inaktivem DHCP mit Taste < **=Ja* und bestätigen mit *Enter*.
Mit „Nein“ können Sie die Einstellungen anzeigen, aber nicht ändern.
Bei inaktivem DHCP werden angezeigt:
IP Adresse z.B. 010.018.060.116
Netzmaske, z.B. 255.255.255.000
MAC-Adresse, z.B. 00:05:B6:01:88:7E
Gateway, z.B. 010.018.060.121
DNS-Server, z.B. 127.000.000.001
*DHCP aktiv | *=Ja *=Nein*
8. Nehmen Sie die gewünschten Einstellungen vor. Wenn die IP Adresse automatisch via DHCP generiert wird, wählen Sie **=Ja* mit Taste < und *Enter*. Wenn nicht, wählen Sie **=Nein* mit *Enter*.
*Bei Einstellung DHCP aktiv | *=Ja werden IP Adresse, Name Server und Host Name angezeigt. Des Weiteren werden angezeigt:*
*Server Modus! | *=Ja *=Nein. Mit Voreinstellung *=Nein können Sie Netzwerk-Einstellungen via TwinIP vornehmen. Im anderen Fall nicht.*
*Initialcode | *=Ja *=Nein. Mit Voreinstellung *=Ja können neue Benutzer ihren Initialcode zu Öffnungscod ändern. Im anderen Fall ist der Schlossmaster für das Anmelden neuer Benutzer erforderlich.*

Sie haben das Schloss erfolgreich mit dem Netzwerk verbunden.

5.14 Einstellungen: Manager

5.14.1 Systemmanagercode ändern

Der Systemmanagercode des Schlosses 1 (=Systemcode) berechtigt nicht zur Schlossöffnung, sondern zur Systemkonfiguration.



Vorsicht

Mit werksseitigem Systemmanagercode ist Ihr System nicht gesichert.

Ändern Sie werksseitigen Code so bald wie möglich.

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden. Gefahr der unberechtigten Öffnung.

Wählen Sie keine derartigen Codes.

Ohne Systemmanagercode können Sie Ihr System nicht mehr konfigurieren.

Speichern Sie den Systemmanagercode an einem sicheren, nur dem Systemmanager zugänglichen Ort.

Gefahr von Funktionsausfall.

Stellen Sie sicher, dass der Systemmanagercode in allen Schlössern des Systems jeweils gleich lautet. Nutzen Sie die Kopierfunktion.

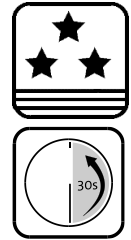
Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie mit Taste > **Einstellungen** und wählen Sie Taste **Enter**.
*Das Display zeigt **Einstellungen | Manager**.*
*Falls **Einstellungen** nicht verfügbar ist, öffnen Sie zuerst das Schloss / die Schlösser.*
3. Bestätigen Sie mit **Enter**.
*Das Display zeigt **Code-Eingabe, Systemmanager, gegebenenfalls 0123456789 und Code:.** Siehe auch „PIN-Code eingeben“.*
4. Geben Sie den Systemcode ein.
*Das Display zeigt **Systemmanager | Bitte warten, danach Managercode neu | Code aendern**.*
5. Geben Sie den neuen Systemcode ein.
*Das Display zeigt **Code bestätigen | Code:.***
6. Wiederholen Sie die Eingabe des neuen Systemcodes.
*Das Display zeigt **Managercode neu | Gespeichert**.*

Sie haben den Systemcode erfolgreich geändert.

5.14.2 Mastercode anmelden

Der Manager kann Mastercode anmelden. Der Master kann am Schloss gespeicherte Benutzer verwalten und den WTU-Master anlegen.



Vorsicht

Mit werksseitigem Mastercode ist Ihr System nicht gesichert.

Ändern Sie werksseitigen Code so bald wie möglich.

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden.

Gefahr der unberechtigten Öffnung.

Wählen Sie keine derartigen Codes.

Ohne Mastercode können Sie die Benutzer des Schlosses nicht mehr verwalten.

Speichen Sie den Mastercode an einem sicheren, nur dem Master zugänglichen Ort.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie mit < oder > und Enter **Einstellungen**.
3. Wählen Sie mit Enter **Einstellungen | Manager**.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
4. Geben Sie den Managercode ein.
Manager | Code aendern wird angezeigt.
5. Wählen Sie **Manager | Master**.
Master | Anmelden wird angezeigt.
6. Wählen Sie **Anmelden**.
Master | Anmelden | Schloss 1 wird gegebenenfalls angezeigt.
7. Wählen Sie das Schloss, falls erforderlich.
Master | Anmelden und
Code-Eingabe | Manager | Code: wird angezeigt.
8. Geben Sie den bisherigen Mastercode ein.
Code-Eingabe | Master | Neuer Code: wird angezeigt.
9. Geben Sie den neuen Mastercode ein.
Code-Eingabe | Master | Code bestätigen: wird angezeigt.
10. Geben Sie den neuen Mastercode nochmals ein.
Bitte warten | Gespeichert wird angezeigt.

Sie haben einen neuen Mastercode erfolgreich angemeldet.

5.14.3 Mastercode abmelden

Der Manager kann Mastercode abmelden.

Vorsicht

**Gefahr von Funktionsverlust.
Möglicherweise können Schlossbenutzer nicht
mehr verwaltet werden.**
Stellen Sie sicher, dass kein Funktionsverlust entsteht.



1. Wählen Sie **Manager | Master**.
Master | Anmelden wird angezeigt.
Vorhergehende Schritte siehe oben, „Mastercode anmelden“, 1 bis 4.
2. Wählen Sie **Master | Abmelden**.
Master | Abmelden | Schloss Nr. wird angezeigt.
3. Wählen Sie das Schloss, falls erforderlich.
Code-Eingabe | Manager | Code: wird angezeigt.
4. Geben Sie den Managercode ein.
Mastercode | Geloescht wird angezeigt.

Sie haben einen Mastercode erfolgreich abgemeldet.

5.14.4 Anzeige Mastercode

Der Manager kann anzeigen, ob Mastercode angemeldet wurde oder nicht.

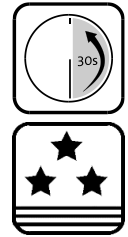
1. Wählen Sie **Manager | Master**.
Master | Anmelden wird angezeigt.
Vorhergehende Schritte siehe oben, „Mastercode anmelden“, 1 bis 4.
2. Wählen Sie **Master | Anzeige**.
Master | Anzeige | Schloss Nr. wird angezeigt.
3. Wählen Sie das Schloss, falls erforderlich.
Ben.-Code: 000 | OK
*Der Master hat Benutzernummer 000 am Schloss.
OK = angemeldet / NOK = abgemeldet.*

Sie haben Mastercode erfolgreich angezeigt.



5.14.5 Datum und Uhrzeit einstellen

Von der richtigen Einstellung von Datum und Uhrzeit sind alle Zeitfunktionen des Systems abhängig, ebenso das Ereignisprotokoll. Die Sommer- / Winterzeit-Umstellung erfolgt werkseingestellt automatisch. Dieses Untermenü gibt es auch im versteckten Menü.

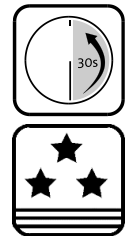


1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie mit Taste > **Einstellungen** und Enter.
*Das Display zeigt **Einstellungen** | **Manager**.*
3. Bestätigen Sie **Manager** mit Enter.
***Manager** | **Code aendern** wird angezeigt.*
4. Wählen Sie mit > **Datum/Uhrzeit** und danach Enter.
*Das Display zeigt **Systemmanager** | **Code-Eingabe** und **Code:**.*
5. Geben Sie den Systemcode ein.
Uhrzeit und Datum werden angezeigt. Es blinkt die erste Ziffer der Uhrzeit.
6. Geben Sie die erste Ziffer der aktuellen Uhrzeit ein und wählen Sie Enter.
Fahren Sie mit der Eingabe fort, bis der aktuell eingestellte Wochentag blinkt.
7. Wählen Sie mit > den aktuellen Wochentag und Enter.
Der Cursor blinkt auf der ersten Ziffer des Datums.
8. Geben Sie Tag, Monat und Jahr ein.
*Das Display zeigt **Manager** | **Code aendern**.*

Sie haben Datum und Uhrzeit erfolgreich eingestellt.

5.14.6 Codeverknüpfung

Möglichkeit der Einstellung von Codeverknüpfung / 4-Augen-Prinzip für das **Oeffnen**, für die **Konfiguration** und die **Freigabezeit**. Nach Wahl der Option können 2 Benutzer gemeinsam Schlösser öffnen oder Parameter ändern oder, wenn „Öffnungsverzögerung“ oder „Freigabezeit“ eingestellt sind, müssen 2 Benutzer nach der Öffnung während der Freigabezeit Code eingeben.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit > **Einstellungen** und Enter.
*Das Display zeigt **Einstellungen** | **Mastercodes**.*
3. Wählen Sie mit > **Schlosssystem** und danach Enter.
*Das Display zeigt **Code-Eingabe**, **Systemmanager**, und **Code:**.*
4. Geben Sie den Systemmanagercode ein.
*Das Display zeigt **Oeffnen**.*
5. Wählen Sie mit Enter **Oeffnen** oder mit > und Enter **Konfiguration** oder **Freigabezeit**.
****=JA** | ***=Nein** wird angezeigt.*
6. Wählen Sie die gewünschte Option mit > und Enter.
Das Programm nimmt die gewünschte Einstellung vor.

Sie haben erfolgreich Codeverknüpfung für die gewählte Funktion eingestellt.

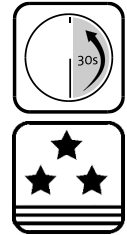
5.14.7 Parallelcode

Möglichkeit der Einstellung von **Parallelcode** für ein Schlosssystem mit 2 Schlössern.

Der erste Benutzer kann Schloss 1 oder 2 öffnen, der zweite das noch geschlossene Schloss.

Kombinierbar mit „**Zwangsfolge**“. Wenn 2 Schlösser im System sind, kann ein Benutzer während einer „**Teilsperrezeit**“ ein Wertbehältnis auch alleine öffnen.

Bei Aktivierung dieser Funktion mit dem optionalen Parametrierset Cash-ProtectPro wird die Funktion „**Codeverknüpfung**“ automatisch deaktiviert. Aktivierung ähnlich „Codeverknüpfung“ (siehe oben).



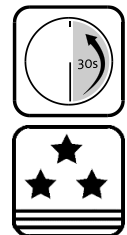
5.14.8 Zwangsfolge

Möglichkeit der Einstellung von **Zwangsfolge** für ein Schlosssystem mit 2 Schlössern.

Möglichkeit, eine Reihenfolge festzulegen, die beim Öffnen und Schließen der Schlösser eingehalten werden muss.

Wenn Sie die Option „Zwangsfolge“ wählen, müssen Benutzer zuerst Schloss 1 und danach gegebenenfalls Schloss 2 öffnen. Die Abfolge wird durch das Schlosssystem vorgegeben. Der Bediener hat darauf keinen Einfluss. Diese Funktion vereinfacht die Bedienung. Nach der Öffnung von Schloss 1 ist das System teilgesichert (entspricht bei Option ZF dem Zustand „gesichert“), nach der Öffnung aller Schlösser ist das System entsperrt und damit unge-sichert.

Beim Schließen muss zuerst gegebenenfalls Schloss 2 und dann Schloss 1 geschlossen werden. Danach ist das System gesichert. Werkseinstellung: deaktiviert. Aktivierung ähnlich Codeverknüpfung (siehe oben).



5.14.9 Zeitverzögerung

Möglichkeit der Einstellung verschiedener Arten von Zeitverzögerung für Schlösser oder für Personen, denen Wochenprogramme zugeordnet sind. Einzustellen sind jeweils 3 zweistellige Werte in Minuten $00 < 00 < 00$.

Der erste Wert entspricht jeweils der Öffnungsverzögerung, der zweite der Freigabezeit und der dritte der Alarmverzögerung oder der Öffnungsverzögerung nach stillem Alarm.

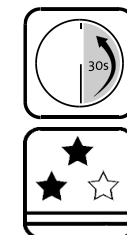
Werkseinstellung: deaktiviert. Aktivierung ähnlich Codeverknüpfung (siehe oben).



5.14.10 Wochenprogramme

Möglichkeit der Erstellung von 5 **Wochenprogrammen**. Einzustellen sind jeweils für jeden Wochentag jeweils 2 Uhrzeiten, der Anfangs- und der Ende-Zeitpunkt, beispielsweise **Mo: 07:00-12:00**.

Im festgelegten Zeitraum kann jeweils geöffnet werden. Werkseinstellung: deaktiviert. Die erstellten Wochenprogramme können bei der Neuanlage von Benutzern diesen Benutzern zugeordnet werden. Aktivierung ähnlich Codeverknüpfung (siehe oben).



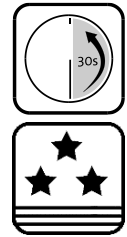
5.14.11 Alarmgeräte: XT-Erweiterung / TwinAlarm

Vorsicht

Gefahr, dass nach dem Aktivieren der Erweiterungseinheit bei Öffnungsversuch am Schloss „Keine Freigabe“ angezeigt wird.

Nach dem Aktivieren der Erweiterungseinheit werden beide Eingänge in Funktion gesetzt.

Deaktivieren Sie Eingang „Freigabe“ via optionale PC-Software oder TwinNet, wenn möglich.



Vorbedingungen Alarmgerät im System verfügbar.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit den Tasten > und Enter **Einstellungen**.
Das Display zeigt Einstellungen | Manager.
3. Bestätigen Sie **Manager** mit Enter.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
4. Geben Sie den Systemmanagercode ein.
Das Display zeigt Manager | Code aendern.
5. Wählen Sie mit > und Enter **Alarmgeräte**.
Das Display zeigt Alarmgeraete | XT Erweiterung.
6. Wählen Sie mit > und Enter **XT Erweiterung** oder **TwinAlarm**.
*Das Display zeigt zum Beispiel XT Erweiterung | * = JA * = NEIN.*
7. Wählen Sie mit < oder > und Enter *** = JA**, oder *** = NEIN**.
*Falls TwinXT mit * = NEIN deaktiviert wurde, zeigt das Display XT aktiv | Geloesch.*
Im anderen Fall zeigt das Display beispielsweise A:1<:1R:1F:0C:0.
A = Eingänge Riegelw./Freigabe (0=aktiv offen/1=aktiv geschlossen)
B = boltwork / Riegelwerk
R = Release / Freigabe
F = TK Bedieneinheit
C = contact / Kontakt
< = Stellung des Cursors
0 = nicht aktiv; 1 = aktiv.
Im Fall von C bedeutet 0 = NO, normal open; 1 = NC, normal closed.
8. Wählen Sie mit 1 oder 0 und Enter die gewünschten Einstellungen.
Das Display zeigt beispielsweise TwinXT aktiv | Gespeichert.

Sie haben erfolgreich ein Alarmgerät eingestellt und / oder ein- oder ausgeschaltet.

5.14.12 Hinweise zu ‚Pairing einrichten‘

Der Manager kann „Pairing“ einrichten. Siehe auch „Pairing einrichten“, S.66 auch „Pairing“, S.37 und gegebenenfalls das Handbuch TwinIP.

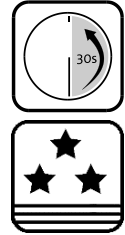
Achtung: Der **Pairingschlüssel** ist auch ein AES-Schlüssel (Advanced Encryption Standard), aber nicht der für die Installation der System IDs (=“**System ID Kundenschlüssel**“).

Pairing für ein System ohne Netzwerk können Sie mit „00000000“ als fiktive Seriennummer TwinIP small einrichten. Bei einem möglichen Update auf ein in ein Netzwerk eingebundenes System muss diese Nummer beim erneuten Einrichten von Pairing durch die Seriennummer der Einheit TwinIP small ersetzt werden.

Vorbedingungen echte (bzw. für Systeme ohne Netzwerk fiktive) Seriennummer TwinIP small und Pairing-Schlüssel (32 St., hexadezimal) verfügbar, TwinIP gegebenenfalls richtig eingerichtet. Bei Systemen der **VDS-Klassen C / D** ist für den Schlüsselzugriff ein **2. Code** (4-Augen-Prinzip) erforderlich. Wählen Sie für diese Systeme „Codeverknüpfung (4-Augen, Dualcode) / Konfiguration“.

5.14.13 Pairing einrichten

Der Manager kann „Pairing“ einrichten. Voraussetzungen siehe „Hinweise zu ‚Pairing einrichten‘“, S.65 sowie „Pairing“, S.37 und gegebenenfalls Handbuch TwinIP.



Hinweis

Verwenden Sie Menü „Pairing“ (siehe Anleitung unten) auch zum regelmäßigen Ändern des Pairing-Schlüssels. Der Schlüssel sollte regelmäßig in unterschiedlichen Intervallen geändert werden. Er wird kundenseitig geändert und sollte für alle beteiligten Systeme (zum Beispiel TwinLock und TwinIP) gleich sein.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie **Einstellungen** mit **>** und **Enter**.
Einstellungen | Manager wird angezeigt.
3. Wählen Sie **Manager** mit **Enter**.
Manager | Code aendern wird angezeigt.
4. Wählen Sie **Pairing** mit **>** und **Enter**.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
5. Geben Sie den Managercode ein und bei VdS-Systemen der Klasse 3 auch einen 2.Code (Dual code / 4-Augen-Prinzip) ein.
Seriennummer | wird angezeigt. Bitte überprüfen.
6. Geben Sie die Seriennummer von TwinIP small ein und wählen Sie **Enter**.
Diese Nummer steht in Bereich „Pairing“ auf Seite „Verwaltung“ der Applikation „TwinIP“. Das Display zeigt 1 / 2 :
7. Geben Sie die ersten 16 Zeichen des Pairingschlüssels ein, prüfen Sie die Eingabe und bestätigen Sie mit **Enter**.
Ebenfalls in Bereich „Pairing“ auf Seite „Verwaltung“ der Applikation „TwinIP“. Eingabe von Hexadezimalzahlen: Ziffern normal eingeben, Buchstaben A-F via Pfeiltasten und jeweils anschließend via Zifferntasten eingeben:

⏪ + 1 = A	⏩ + 1 = B	⏪ + 2 = C
⏪ + 2 = D	⏪ + 3 = E	⏩ + 3 = F

*Die Wahl von **X** (Clear) löscht Einträge. Das Display zeigt 2 / 2 :*
8. Geben Sie die zweiten 16 Zeichen des Schlüssels ein, prüfen Sie auch diese Eingabe und bestätigen Sie mit **Enter**.
Das Display zeigt Pairingschlüssel | Gespeichert, Seriennummer gespeichert und Pairing | OK. Initialmaster | Bitte warten zeigt an, dass auch der Initialmasterschlüssel neu berechnet und in den Schlössern gespeichert wird.

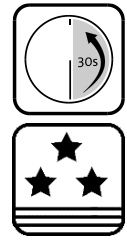
Sie haben Pairing an der Bedieneinheit erfolgreich eingerichtet.

5.14.14 Kundenschlüssel anzeigen

Nur mit TwinNet 10.3 und höher. Siehe auch „Kundenschlüssel“, Seite 37. Bei Systemen der **VDS-Klassen C / D** ist für den Schlüsselzugriff ein **zweiter Code** (4-Augen-Prinzip) erforderlich.

Werkseinstellung wird für Kundenschlüssel angezeigt, wenn sie noch nicht geändert wurden. Ändern Sie die Schlüssel in den entsprechenden Menüs. Siehe „Pairing einrichten“, S.66, „System ID A/B“, S.72 und „Codeverteilung einrichten“ auf S. 68.

Vorbedingungen Netzwerk- und – Codeverteilungs-/Initialcode-Lizenz, Netzwerkanschluss, TwinIP und Pairing eingerichtet.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie **Einstellungen** mit **>** und **Enter**.
Einstellungen | Manager wird angezeigt.
3. Wählen Sie **Manager** mit **Enter**.
Manager | Code aendern wird angezeigt.
4. Wählen Sie **Kundenschlüssel** mit **>** und **Enter**.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
5. Geben Sie den Managercode ein.
Pairing wird kurz angezeigt.
Der Kundenschlüssel für Pairing wird angezeigt.
6. Wählen Sie eine beliebige Taste.
SystemID A/B wird kurz angezeigt.
Der SystemID Kundenschlüssel wird angezeigt.
7. Wählen Sie noch einmal eine beliebige Taste.
Codeverteilung wird gegebenenfalls kurz angezeigt. *Ein eigener Kundenschlüssel für Codeverteilung wird nur angezeigt, wenn er angelegt worden ist. Wenn nicht, wird die Anzeige beendet.*
8. Wählen Sie noch einmal eine beliebige Taste, wenn erforderlich.
Die Anzeige wird beendet.

Sie haben die 2 oder 3 Kundenschlüssel erfolgreich angezeigt.

5.14.15 Codeverteilung einrichten

Nur mit TwinNet 10.3 und höher. Siehe auch „Codeverteilung“, Seite 37 und das Handbuch TwinIP / TwinNet. Prüfen Sie, ob Codeverteilung eingerichtet ist: Wenn ***=JA** markiert ist, ist sie es. Voreinstellung: deaktiviert.

Vorbedingungen Netzwerk- und – Codeverteilungs-/Initialcode-Lizenz, Netzwerkanschluss, TwinIP und Pairing eingerichtet.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie **Einstellungen** mit **>** und **Enter**.
Einstellungen | Manager wird angezeigt.
3. Wählen Sie **Manager** mit **Enter**.
Manager | Code aendern wird angezeigt.
4. Wählen Sie **Codeverteilung** mit **>** und **Enter**.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
5. Geben Sie den Managercode ein.
Codeverteilung | *=JA *=NEIN wird angezeigt.
Mit *** = NEIN** können Sie Codeverteilung ausschalten und das Menü beenden.
Mit ***=JA** können Sie die Codeverteilung einschalten.
6. Wählen Sie mit **>** und **Enter** *** = JA**.
Kundenschluessel | *=JA *=NEIN wird angezeigt.
Mit Einstellung *** = NEIN** wird der Kundenschlüssel Pairing auch für die Codeverteilung verwendet (Standard-Einstellung). Dazu muss der Schlüssel in allen beteiligten Schlosssystemen gleich sein. Menü wird beendet.
Mit ***=JA** können Sie einen eigenen Schlüssel für Codeverteilung erstellen.
7. Wenn gewünscht, wählen Sie mit **>** und **Enter** *** = JA**.
Code-Eingabe | *=JA *=NEIN wird angezeigt.
Mit *** = NEIN** wählen Sie den Kompatibilitätsmodus. Ein gegebenenfalls bereits erstellter Kundenschlüssel Codeverteilung wird verwendet.
Mit ***=JA** können Sie den neuen Kundenschlüssel eingeben und bestätigen.
8. Wenn gewünscht, wählen Sie mit **>** und **Enter** *** = JA**.
Das Display zeigt **Codeverteilung | 1/2:**.
9. Geben Sie die ersten 16 Zeichen ein, prüfen sie die Eingabe und bestätigen Sie mit **Enter**.
Eingabe von Hexadezimalzahlen: Ziffern normal eingeben, Buchstaben A-F via Pfeiltasten und jeweils anschließend via Zifferntasten eingeben:

⏪ + 1 = A	⏩ + 1 = B	⏪ + 2 = C
⏩ + 2 = D	⏪ + 3 = E	⏩ + 3 = F

 Die Wahl von **X** (Clear) löscht Einträge. Das Display zeigt **2/2:**.
10. Geben Sie die zweiten 16 Zeichen des Schlüssels ein, prüfen sie auch diese Eingabe und bestätigen Sie mit **Enter**.
Das Display zeigt **Codeverteilung | Bitte warten** und **Codeverteilung | Gespeichert**.

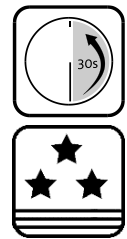
Sie haben erfolgreich „Codeverteilung“ für das Schlosssystem eingerichtet.

5.14.16 Server-Modus ein- / ausschalten

Nur mit TwinNet 10.3 und höher. Siehe auch „Server-Modus“, Seite 37 und das Handbuch TwinIP. Prüfen Sie, ob der Server-Modus eingerichtet ist: Wenn ***=JA** markiert ist, ist er es. Voreinstellung: aktiviert.

Vorbedingungen Netzwerkanschluss und -Lizenz eingerichtet.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie **Einstellungen** mit **>** und **Enter**.
Einstellungen | Manager wird angezeigt.
3. Wählen Sie **Manager** mit **Enter**.
Manager | Code aendern wird angezeigt.
4. Wählen Sie **Server Modus** mit **>** und **Enter**.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
5. Geben Sie den Managercode ein.
Server Modus | *=JA *=NEIN wird angezeigt.
6. Wählen Sie mit **>** und **Enter** *** = JA**.
*Mit *** = NEIN** können Sie den Server-Modus ausschalten.*
Server Modus | Gespeichert wird angezeigt.



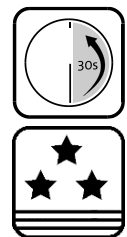
Sie haben erfolgreich „Server-Modus“ für das Schlosssystem eingerichtet.

5.14.17 Initialcode aktivieren / deaktivieren

Mit TwinNet 10.3 und höher. Siehe auch „Initialcode“, Seite 38. Bei auch in TwinNet (geplant: auch in TwinIP) gewählter Option „Initialcode“ können Sie es neuen Benutzern am Schloss ermöglichen, sich selbst PIN-Code anzulegen. Siehe „Initialcode bei Anmeldung am Schloss ändern“, S. 70. Voreinstellung: deaktiviert.

Vorbedingungen Netzwerk- und –Codeverteilungs-/Initialcode-Lizenz, Netzwerkanschluss verfügbar.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit **>** **Einstellungen** und **Enter**.
Einstellungen | Manager wird angezeigt.
3. Wählen Sie **Manager** mit **Enter**.
Manager | Code aendern wird angezeigt.
4. Wählen Sie **Initialcode** mit **>** und **Enter**.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
5. Geben Sie den Managercode ein.
Initialcode | *=JA *=NEIN wird angezeigt.
6. Wählen Sie mit **>** und **Enter** *** = JA**.
*Mit *** = NEIN** können Sie Funktion „Initialcode“ ausschalten.*
*Nach Wahl von *** = JA** wird System gesperrt! | ***=JA *=NEIN** angezeigt.*
7. Wählen Sie mit **>** und **Enter** *** = JA** oder ***=NEIN**.
*Nach der Wahl von *** = JA** können Initialcodes auch bei geschlossenem System zu Öffnungscodes geändert werden. Nach der Wahl von *** = NEIN** können Initialcodes nur bei geöffnetem System zu Öffnungscodes geändert werden.*
Initialcode | Gespeichert wird angezeigt.

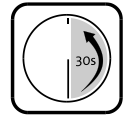


Sie haben Funktion „Initialcode“ erfolgreich für das Schlosssystem eingerichtet.

5.14.18 Initialcode bei Anmeldung am Schloss ändern

Vorbedingungen via TwinNet (/ TwinIP) wurde für Sie Initialcode angelegt.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit der Taste > **Einstellungen** und Enter.
Das Display zeigt **Einstellungen | Manager**.
3. Wählen Sie **Mitarbeiter** mit > und Enter.
Das Display zeigt **PIN-Code | Code ändern**.
4. Bestätigen Sie **Code ändern** mit Enter.
Das Display zeigt **Alter Code, ggf. Schloss 1, und Benutzer: XX**.
5. Wählen Sie gegebenenfalls das Schloss und drücken Sie Enter.
Das Display zeigt **Alter Code | Benutzer Nr..**
6. Wählen Sie die Nummer mit Zifferntasten oder mit > und Enter.
Das Display zeigt **Alter Code, 0123456789, und Code:.**
7. Geben Sie Ihren Initialcode ein.
Das Display zeigt **Benutzercode neu und Code:.**
8. Geben Sie Ihren neuen Code ein.
Das Display zeigt **Code bestätigen ...und Code:.**
9. Geben Sie Ihren neuen Code nochmals ein.
Das Display zeigt **PIN-Code | Bitte warten.**
Das Display zeigt **Benutzer Nr. | Gespeichert.**



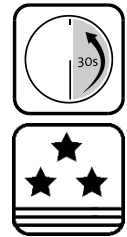
Sie haben erfolgreich Ihren PIN-Code angemeldet.

5.14.19 Einmalzugang (OTC Testfunktion)

Nur mit Version B670. Der Manager kann mit dieser Funktion gegebenenfalls testen, ob die Einstellungen für Einmalcode richtig sind. Siehe auch „Voraussetzungen für flexiblen Einmalcode“ auf Seite 35.

Die Funktion ist nur verfügbar, wenn

- alle Bedingungen für flexiblen Einmalcode erfüllt sind und
- ein Alarmgerät aktiviert wurde
- für den Benutzer Einmalcode erzeugt wurde, z.B. via MultiPad Go!.

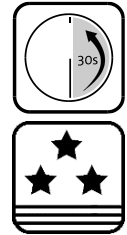


1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie **Einstellungen** mit Taste > und Taste Enter.
Das Display zeigt Einstellungen | Manager.
3. Wählen Sie **Manager** mit Enter.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
4. Geben Sie den Managercode ein.
Manager | Code aendern wird angezeigt.
5. Wählen Sie **Einmalzugang** mit > und Enter.
Manager | Einmalzugang wird angezeigt.
Einmalzugang | Schloss 1 wird gegebenenfalls angezeigt.
6. Wählen Sie das Schloss, falls erforderlich.
Das Display zeigt Einmalzugang | Schloss X und
Code-Eingabe | Benutzer: Master.
7. Geben Sie die erforderliche Personalnummer ein und wählen Sie Enter.
Das Display zeigt PIN-Code und Code: . Aus der Anzeige ist ablesbar, wie der Code einzugeben ist. Siehe Abschnitt „PIN-Code eingeben“.
8. Geben Sie die zugeordnete persönliche PIN ein.
Das Display zeigt WTU-Funktion | Code: .
9. Geben Sie Ihren Einmalcode ein.
Das Display zeigt OK, wenn korrekte Eingaben gemacht wurden.
Das Display zeigt NOK, wenn mindestens eine Eingabe inkorrekt war.
*Das Display zeigt WTU-Funktion | WTU-Code: ****, wenn Schloss oder Riegelwerkseingang an TwinXT offen sind.*
Sind diese Elemente geschlossen, wird der 4-stellige Rückcode angezeigt.
Wie nach einer Öffnung wird der Einmalcode ungültig.

Sie haben die Einstellungen für Einmalcode gegebenenfalls erfolgreich getestet.

5.14.20 System ID A/B

Der Manager kann bei der Installation die System IDs A **und** B installieren. Dies ist eine Bedingung für den Betrieb mit flexiblen Einmalcodes. Siehe S.35. Das System erkennt die Art der ID.



Hinweis

Zur Inbetriebnahme muss der Kundenschlüssel geändert werden, um höchste Sicherheit zu gewährleisten. Der Schlüssel wird kundenseitig geändert und sollte für alle beteiligten Systeme (zum Beispiel Twin-Net, TwinLock und MultiPad Go!) gleich sein.

Teil I) Führen Sie die Schritte 1-5A unten für den Kundenschlüssel aus.

Teil II) Erstellen Sie die System IDs A und B via MultiPad Go!

Teil III) Führen Sie die Schritte 1-6 unten aus – dieses Mal Schritt 5C „Codeeingabe“ wählen - einmal für ID A und ein zweites Mal für ID B.

Teil IV) Nur wenn gewünscht: Führen Sie die Schritte 1-5 unten aus und wählen Sie dieses Mal Schritt 5B „Werkseinstellungen“.

Vorbedingungen System IDs A und B verfügbar.

Für Teil III vorher den System ID Kundenschlüssel ändern.

1. Entsperren Sie das System (alle Schlösser öffnen).
2. Wählen Sie mit Taste > Einstellungen und Enter.
Das Display zeigt Einstellungen | Manager.
3. Wählen Sie System ID A/B mit > und Enter.
Code-Eingabe | Systemmanager | Code: wird angezeigt.
4. Geben Sie den Managercode ein.
Das Display zeigt System ID A/B | Kundenschlüssel.
- 5A. Drücken Sie Enter und geben Sie ein wie unten beschrieben.
Das Display zeigt 1 / 2 :
Geben Sie die ersten 16 Zeichen des Schlüssels ein und wählen Sie Enter.
Eingabe von Hexadezimalzahlen als System ID. Ziffern normal eingeben, Buchstaben A-F via Pfeiltasten und jeweils anschließend via Zifferntasten eingeben:

$\llcorner + 1 = A$	$\llcorner + 1 = B$	$\llcorner + 2 = C$
$\llcorner + 2 = D$	$\llcorner + 3 = E$	$\llcorner + 3 = F$

Die Wahl von X (Clear) löscht Einträge. Das Display zeigt 2 / 2 :
Geben Sie die zweiten 16 Zeichen ein und wählen Sie Enter.
Das Display zeigt Kundenschlüssel | Gespeichert und
Manager | Code aendern, Ende Teil I.
- 5B. Wählen Sie Werkseinstellungen mit Taste > und Enter.
Die Werkseinstellungen für die System IDs werden gesetzt.
Das Display zeigt Werkseinstellungen | Gespeichert und
Manager | Code aendern, Ende Teil IV.
- 5C. Wählen Sie Code-Eingabe mit > und Enter.
Das Display zeigt 1 / 2 :
6. Geben Sie die System ID A / B ein wie den Schlüssel oben (siehe 5A).
Das Display zeigt System ID A/B | Bitte warten und
System ID A/B | Gespeichert (für A und B). Ende Teil III.

Sie haben erfolgreich den Kundenschlüssel eingegeben / Werkseinstellungen gewählt / eine bzw. beide System IDs im System installiert.

5.14.21 Modus / WTU-Funktion festlegen

Nur mit B670. Der Manager kann den Modus / die WTU-Funktion festlegen. Siehe auch Modus / WTU-Funktion auf S. 36.



1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie mit Taste `>` und `Enter` `Einstellungen`.
3. Wählen Sie mit Taste `Enter` `Einstellungen | Manager`.
`Code-Eingabe | Systemmanager | Code:` *wird angezeigt*.
4. Geben Sie den Managercode ein.
`Manager | Code aendern` *wird angezeigt*.
5. Wählen Sie mit `>` und `Enter` `Manager | WTU Funktion`.
`WTU Funktion | Modus: 0<` *wird beispielsweise angezeigt*.
6. Wählen Sie `WTU Funktion | Modus: 0<, 1< oder 2<`.
0< Modus „Bank“, keine flexiblen Einmalcodes möglich
1< Modus „gemischt“, PIN-Codes und flexible Einmalcodes
2< „nur flexible Einmalcodes“, keine PIN-Codes möglich
ACHTUNG: Einstellung „2“ kann den Mastercode löschen.
Ändern Sie die Einstellung auf „1“, um den Master wieder anzumelden.
`Modus: 1<` *wird beispielsweise angezeigt*.

Sie haben den Modus / die WTU-Funktion erfolgreich festgelegt.

5.14.22 Reset Vorgangszähler im Schloss

Der Manager kann den Vorgangszähler im Schloss zurücksetzen.



1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie `Einstellungen` mit Taste `>` und `Enter`.
3. Wählen Sie `Einstellungen | Manager` mit `Enter`.
`Manager | Code aendern` *wird angezeigt*.
4. Wählen Sie `Manager | Vorgangszähler`.
`Code-Eingabe | Systemmanager | Code:` *wird angezeigt*.
5. Geben Sie den Managercode ein.
`Vorgangszähler | 00005` *wird beispielsweise angezeigt*.
Danach wird `Reset | *=JA *=NEIN` *angezeigt*.
6. Wählen Sie „JA“, um den Zähler zurückzusetzen.

Sie haben den Vorgangszähler im Schloss erfolgreich auf „00000“ zurückgesetzt.

5.14.23 Zwei Benutzergruppen wählen

Via Netzwerk nur mit Lizenz verfügbar. Hier legen Sie fest, ob die an Schlössern gespeicherten Benutzer in zwei Gruppen aufgeteilt und so verwaltet werden sollen oder nicht. Zuvor WTU-Master anmelden, siehe Seite 77.



Wertebereich: JA / NEIN, voreingestellter Wert: NEIN

1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie `Einstellungen` mit Taste `>` und `Enter`.
3. Wählen Sie `Einstellungen | Manager` mit `Enter`.
`Manager | Code aendern` *wird angezeigt*.
4. Wählen Sie `Manager | Benutzergruppen`.
`Code-Eingabe | Systemmanager | Code:` *wird angezeigt*.
5. Geben Sie den Managercode ein.
`Benutzergruppen | *=Ja *=Nein` *wird angezeigt*.
6. Wählen Sie `*=Ja`, falls Sie die Benutzer in 2 Gruppen aufteilen wollen.
`Benutzergruppen | Gespeichert` *wird angezeigt*.

Sie haben erfolgreich Option „Benutzergruppen“ gewählt.

5.15 Einstellungen: Master

5.15.1 Mastercode ändern

Der Mastercode des Schlosses berechtigt zum Verwalten der Benutzer des Schlosses sowie optional zum Öffnen des Schlosses.

Vorsicht

Mit werksseitigem Mastercode ist das System nicht gesichert.

Ändern Sie werksseitigen Code so bald wie möglich.

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden.

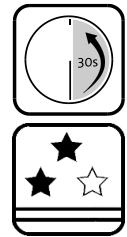
Gefahr der unberechtigten Öffnung.

Wählen Sie keine derartigen Codes.

Ohne Mastercode können Sie die Benutzer des Schlosses nicht mehr verwalten.

Speichern Sie den Mastercode an einem sicheren, nur dem Master zugänglichen Ort.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

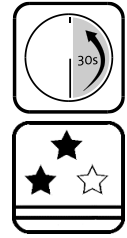


1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie mit Menütaste > `Einstellungen` und bestätigen Sie mit `Enter`.
Das Display zeigt `Einstellungen | Manager`.
3. Wählen Sie mit der Menütaste > `Master` und `Enter`.
Das Display zeigt `Master | Code aendern`.
4. Bestätigen Sie `Code aendern` mit `Enter`.
Das Display zeigt `Code-Eingabe, Master, gegebenenfalls 0123456789 und Code:`. Siehe „PIN-Code eingeben“.
5. Geben Sie den Mastercode ein.
Das Display zeigt `Master | Bitte warten, Mastercode und Code:`.
6. Geben Sie den neuen Mastercode ein.
Das Display zeigt `Code bestätigen und Code:`.
7. Wiederholen Sie Ihre Eingabe des neuen Mastercodes.
*Das Display zeigt `Mastercode neu | Bitte warten`.
Das Display zeigt `Mastercode neu | Gespeichert`.*

Sie haben den Mastercode erfolgreich geändert.

5.15.2 PIN-Code für Benutzer anmelden

Der Inhaber des Mastercodes (Schloss) kann PIN-Codes anmelden. Nur wenn er Berechtigung „Service“ hat, kann er dabei Wochenprogramme zuordnen (siehe unten). Damit ein Benutzer mit PIN-Code öffnen kann, muss er dafür autorisiert sein. Falls „Benutzergruppen“ gewählt ist und der Master PIN-Code für Benutzer 99 anmeldet, wird dieser zum WTU-Master, der PIN-Codes für Benutzer der zweiten Gruppe anmelden kann.



Vorbedingungen Sie sind Schlossmaster / WTU-Master.

1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie mit Taste > **Einstellungen** und Enter.
Das Display zeigt Einstellungen | Manager.
3. Wählen Sie mit > **Master** und bestätigen Sie mit Enter.
Das Display zeigt bei mehreren Schlössern Code-Eingabe | Schloss 1.
4. Bestätigen Sie **Schloss 1** mit Enter oder wählen Sie mit > **Schloss 2** und Enter.
Das Display zeigt Code-Eingabe | Master.
5. Bestätigen Sie mit Enter oder wählen Sie **WTU-Master** mit > und Enter
Master oder WTU-Master und Code: werden angezeigt.
6. Geben Sie den (WTU-)Mastercode ein.
Das Display zeigt Master | Code aendern.
7. Wählen Sie **PIN-Code** und bestätigen Sie mit Enter.
Das Display zeigt Master | PIN-Code und anmelden.
8. Bestätigen Sie **Anmelden** mit Enter.
Das Display zeigt Anmelden | Benutzer 01<.
9. Geben Sie die Benutzer- / Personalnummer ein.
Das Display zeigt Code-Eingabe | Code neu:.
10. Geben Sie den PIN-Code ein.
Das Display zeigt Code-Eingabe | Code bestätigen:.
11. Wiederholen Sie den PIN-Code.
*PIN-Code | Bitte warten und Benutzer Nr. | Gespeichert und optional Wochenprogramm 1 | *=JA | *=Nein werden angezeigt.*
12. Wählen Sie, ob dem Benutzer die Programme 1 – 5 zugeordnet werden sollen.
*Bei Schloss 1 in einem System mit mehreren Schlössern zeigt das Display Code kopieren? *= JA | *= NEIN.*
13. Wählen Sie ***=JA**, um den Code auf Schloss 2 zu kopieren, wenn gewünscht.
*Schloss 2 | PIN-Code und Benutzer XX | Gespeichert sowie Weiterer Code? | *=JA *=NEIN werden angezeigt.*
14. Wählen Sie ***=JA**, wenn gewünscht, und wiederholen Sie die Schritte 9-13.
Das Display zeigt Benutzer XX | Gespeichert.

Sie haben mindestens einen PIN-Code für eine Person erfolgreich angemeldet.

5.15.3 WTU-Mastercode anmelden

Vorsicht

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden.

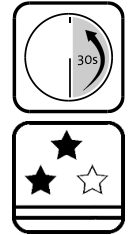
Gefahr der unberechtigten Öffnung.

Wählen Sie keine derartigen Codes.

Ohne WTU-Mastercode können Sie die Benutzer der Gruppe 2 des Schlosses nicht mehr verwalten.

Speichen Sie den Code an einem sicheren, nur dem WTU-Master zugänglichen Ort.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.



Vorbedingungen Parameter „Benutzergruppen“ ist noch nicht gewählt. Dies macht der Systemmanager erst, nachdem der Master den PIN-Code für Benutzer Nr. 99 angemeldet hat, der dann zum WTU-Master wird.

1. Führen Sie die Schritte der Anleitung „PIN-Code für Benutzer anmelden“ auf Seite 76 für Benutzer Nr.99 aus.

Für Benutzer Nr.99, der WTU-Master werden wird, wurde Code angemeldet.

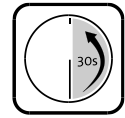
2. Führen Sie die Schritte der Anleitung „Zwei Benutzergruppen wählen“ auf Seite 74 für Benutzer Nr.99 aus.

Die Schlossbenutzer wurden in zwei Gruppen aufgeteilt. Ab Werk ist eingestellt, dass die zweite Gruppe bei Benutzer 50 beginnt (mit optionaler Software ist dies auch beliebig anders einstellbar).

Sie haben den PIN-Code für Benutzer Nr. 99 erfolgreich angemeldet und den Benutzer zum WTU-Master gemacht, der die Benutzer der zweiten Gruppe verwaltet.

5.15.4 PIN-Code abmelden

Der Inhaber des Mastercodes (Schlossmaster) kann PIN-Codes abmelden. Bei Einstellung „Benutzergruppen | * = JA“ kann dies auch der WTU-Master.



Vorsicht

Gefahr eines Konfigurationsfehlers: Schloss kann möglicherweise nicht mehr geöffnet werden.

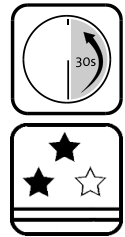
Schlösser mit zu wenig angemeldeten Codes können nicht geöffnet werden. Besonders wenn Sie „Codeverknüpfung“ gewählt haben, stellen Sie sicher, dass am Schloss mindestens so viele zum Öffnen autorisierte Codes angemeldet sind wie erforderlich.

1. Wählen Sie Menü `Einstellungen | Master | PIN-Code`.
Eine detaillierte Anleitung siehe in „PIN-Code für Benutzer anmelden“, Schritte 1-7 auf Seite 76.
`PIN-Code | Anmelden` wird angezeigt.
2. Wählen Sie `PIN-Code | Abmelden` mit `>` und `Enter`.
`Abmelden | Benutzer Nr.: Master` und gegebenenfalls `Schloss 1` wird angezeigt.
3. Wählen Sie gegebenenfalls mit `>` und `Enter` das Schloss aus.
Im WTU-Modus wird `Code-Eingabe | Benutzer: Master` angezeigt.
Mit `>` können Sie WTU-Master wählen und mit `Enter` bestätigen.
Ohne WTU-Modus wird `Code-Eingabe | Master: und Master | Code:` angezeigt.
4. Geben Sie den (WTU) Mastercode ein.
Das Display zeigt `Abmelden | Benutzer: 01`.
5. Wählen Sie mit den Zifferntasten oder `<` und `>` und `Enter` den Benutzer, dessen Code abzumelden ist.
Das Display zeigt `PIN-Code | Bitte warten` und `Benutzer XX | Geloescht`. Danach zeigt das Display optional `Schloss 2 | Code loeschen? | *= ja *=nein`.
6. Wählen Sie `*= ja`, falls Sie den Code auch an Schloss 2 abmelden möchten.
`Weiterer Code? | *= ja *=nein` wird angezeigt.
7. Wählen Sie `*= ja`, falls Sie einen weiteren Code abmelden möchten.
Wiederholen Sie für jede weitere Abmeldung Schritt 5 (und optional Schritt 6).
Wählen Sie `*=nein`, um das Abmelden zu beenden.

Sie haben einen PIN-Code erfolgreich abgemeldet.

5.15.5 PIN-Code Benutzer-Anzeige

Der Schlossmaster und gegebenenfalls der WTU-Master können anzeigen, für welche Benutzer PIN-Codes angemeldet sind. Im WTU-Modus (bei gewählter Option „Benutzergruppen“) können Master und WTU-Master nur die zu ihren Gruppen gehörigen Benutzer verwalten und anzeigen.



1. Wählen Sie Menü **Einstellungen | Master | PIN-Code**.

Eine detaillierte Anleitung siehe in „PIN-Code für Benutzer anmelden“, Schritte 1-7 auf Seite 76.

*Das Display zeigt **PIN-Code | Anmelden**.*

2. Wählen Sie **Benutzer-Anzeige**.

*Das Display zeigt **Code-Eingabe | Master** und gegebenenfalls **Schloss 1**.*

3. Wählen Sie das Schloss, falls erforderlich.

***Master | Code-Eingabe | Code:** wird angezeigt.*

4. Geben Sie den Mastercode des Schlosses ein.

*Das Display zeigt **Bitte warten**. Und danach*

***PIN-Ben.: Anz.** und*

***Ben-Code Nr:OK/NOK**.*

*Oben wird die Gesamtanzahl der PIN-Benutzer angezeigt, unten jeweils eine Benutzernummer und **OK** oder **NOK**.*

5. Blättern Sie mit < und > durch die Nummern der Benutzer.

*Die Buchstaben **OK** oder **NOK** zeigen den Status:*

***NOK** = für den Benutzer ist kein PIN-Code angemeldet*

***OK** = für den Benutzer ist PIN-Code angemeldet.*

Sie haben erfolgreich angezeigt, für wie viele und für welche Benutzer PIN-Code angemeldet ist.

5.15.6 Codekarte (RFID-Karte) anmelden

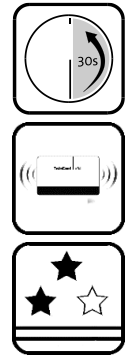
Der Schlossmaster und gegebenenfalls auch der WTU-Master können Codekarten anmelden. Damit sich ein Benutzer mit Karte am Schloss identifizieren kann, muss er auch dazu autorisiert sein.

Vorbedingungen Für Sie als Schlossmaster und für den Benutzer ist in der Benutzermatrix zusätzlich „**Chipkarte**“ aktiviert.

Sie benötigen eine RFID-Karte.

1. Entsperren Sie das System, indem Sie Schloss 1 oder alle Schlösser öffnen.
2. Wählen Sie mit Taste > **Einstellungen** und Enter.
Das Display zeigt Einstellungen | Manager.
3. Wählen Sie mit > **Master** und danach Enter.
Das Display zeigt Master | Schloss 1.
4. Wählen Sie gegebenenfalls mit > das Schloss und danach Enter.
Das Display zeigt Code-Eingabe, Benutzer: Master, gegebenenfalls 0123456789, Master und Code:.
5. Geben Sie den Mastercode ein.
Das Display zeigt Master | Code aendern.
6. Wählen Sie mit < und > **Codekarte** und danach Enter.
Das Display zeigt Codekarte | Anmelden.
7. Bestätigen Sie **Anmelden** mit Enter.
Das Display zeigt Code-Eingabe, Master, ... und Code:.
8. Geben Sie den Mastercode ein.
Das Display zeigt Bitte warten und Anmelden | Benutzer: Master.
9. Wählen Sie die Benutzernummer, für die Sie die Codekarte anmelden möchten.
Das Display zeigt Lese Daten.
10. Lesen Sie die RFID-Karte ein.
Siehe die Anleitungen auf Seite 47.
Das Display zeigt Bitte warten.
11. Entfernen Sie die Karte.
*Das Display zeigt Benutzer Nr. | Angemeldet. Bei mehreren Schlössern zeigt das Display Code kopieren? *= JA | *= NEIN.*
12. Um den PIN-Code auf Schloss 2 zu kopieren, Wählen Sie *=JA.
*Benutzer Nr. | Angemeldet und Weiterer Code? | *= ja *=nein wird angezeigt. Sie können Karten für weitere Benutzer anmelden. Wählen Sie dazu *= ja und wiederholen Sie die Schritte 9-11 mit neuen Benutzerdaten.*

Sie haben erfolgreich eine Codekarte angemeldet.



5.15.7 Codekarte abmelden

Der Schlossmaster und gegebenenfalls auch der WTU-Master können angemeldete Codekarten wieder abmelden. Selbst wenn ein Benutzer zur Identifikation mit Karte autorisiert ist, kann er sich am Schloss nicht identifizieren, wenn seine Karte abgemeldet ist.



Vorsicht

Gefahr eines Konfigurationsfehlers: Schloss kann möglicherweise nicht mehr geöffnet werden.

Wenn Sie Option „Codeverknüpfung“ aktiviert haben, melden Sie an jedem Schloss mindestens so viele zur Öffnung autorisierte Benutzer an wie benötigt. Schlösser mit zu wenig angemeldeten Codes können nicht geöffnet werden.

- Wählen Sie Menü `Einstellungen | Master | Codekarte`.
Eine detaillierte Anleitung siehe in „Codekarte (RFID-Karte) anmelden“, Schritte 1-6 auf Seite 80.
Das Display zeigt `Codekarte | Anmelden`.
- Wählen Sie mit `>` `Abmelden` und bestätigen Sie mit `Enter`.
Das Display zeigt `Code-Eingabe, Master, gegebenenfalls 0123456789, Master und Code:`.
- Geben Sie den Mastercode ein.
Das Display zeigt `Bitte warten und Abmelden | Benutzer: Master`.
- Wählen Sie mit den Zifferntasten oder mit `>` und `Enter` den Benutzer, dessen Codekarte Sie abmelden möchten.
Das Display zeigt `Benutzer Nr | Bitte warten, danach Benutzer Nr | Abgemeldet und optional bei 2 Schlössern im System Schloss 2 und Code löschen? und *= ja *=nein`.
- Wählen Sie gegebenenfalls `*= ja`, wenn Sie die Codekarte auch an Schloss 2 abmelden möchten.
Das Display zeigt `Benutzer Nr | Bitte warten, danach Benutzer Nr | Abgemeldet und schließlich Weiterer Code? | *= ja *=nein`.
Sie können Codekarten für weitere Benutzer abmelden. Wählen Sie dazu `*= ja` *und wiederholen Sie Schritt 9 mit neuen Benutzerdaten.*

Sie haben erfolgreich eine Codekarte abgemeldet.

5.15.8 Codekarte Benutzer-Anzeige

Der Schlossmaster und gegebenenfalls auch der WTU-Master können anzeigen, für welche Benutzer Codekarten am Schloss angemeldet sind. Bei WTU-Betrieb können Master und WTU-Master jeweils nur die Benutzer ihres Benutzerbereichs anzeigen.

1. Wählen Sie Menü `Einstellungen | Master | Codekarte`.

Eine detaillierte Anleitung siehe in „Codekarte (RFID-Karte) anmelden“, Schritte 1-6 auf Seite 80.

Das Display zeigt `Codekarte | Anmelden`.

2. Wählen Sie mit `>` `Benutzeranzeige` und `Enter`.

Das Display zeigt `Code-Eingabe, Master und Code:`.

3. Geben Sie den Mastercode ein.

Das Display zeigt `Bitte warten` und danach beispielsweise

`Karten 098 | Karte 00 (N)OK`.

Die 3 Ziffern nach „Karten“ zeigen die Anzahl der angemeldeten Karten.

Die Ziffern nach „Karte“ stehen für eine Benutzernummer.

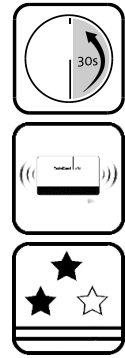
4. Blättern Sie mit `<` und `>` durch die Nummern der Benutzer.

Die Buchstaben `OK` oder `NOK` zeigen den zugehörigen Kartenstatus:

`NOK` bedeutet, dass für den Benutzer keine Karte angemeldet ist.

`OK` bedeutet, dass für den Benutzer eine Codekarte angemeldet ist.

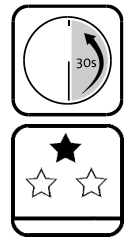
Sie haben erfolgreich angezeigt, für wie viele und für welche Benutzer eine Codekarte angemeldet ist.



5.16 Einstellungen: Mitarbeiter

5.16.1 Code ändern

Jeder Benutzer kann seinen PIN-Code ändern.



Vorsicht

Codes, die einfach sind (z.B. 123456) und solche mit Ziffern, die persönlichen Daten (Geburtsdatum etc.) entsprechen, könnten erraten werden. Gefahr der unberechtigten Öffnung. Wählen Sie keine derartigen Codes.

Nach Codewechsel ist das Schloss mehrere Male bei geöffneter Sicherheitstür zu prüfen.

Vorbedingungen Sie sind dazu autorisiert worden, mit PIN-Code zu öffnen. Der Schlossmaster hat Ihren PIN-Code am Schloss angemeldet.

1. Drücken Sie kurz die Taste `Clear`.
Das Display zeigt das Datum.
2. Wählen Sie mit der Taste `>` `Einstellungen` und `Enter`.
Das Display zeigt Einstellungen | Manager.
3. Wählen Sie mit `>` `Mitarbeiter` und danach `Enter`.
Das Display zeigt PIN-Code | Code aendern.
4. Bestätigen Sie `Code aendern` mit `Enter`.
Das Display zeigt Alter Code, und gegebenenfalls Schloss 1, und Benutzer: Nr.
5. Wählen Sie gegebenenfalls das Schloss und drücken Sie `Enter`.
Das Display zeigt Alter Code | Benutzer Nr.
6. Wählen Sie die Nummer mit Zifferntasten oder mit `<` und `>` und `Enter`.
Das Display zeigt Alter Code, 0123456789, as it may be, and Code:.
Siehe Abschnitt „PIN-Code eingeben“.
7. Geben Sie Ihren bisherigen Code ein.
Das Display zeigt Benutzercode neu und Code:.
8. Geben Sie Ihren neuen Code ein.
Das Display zeigt Code bestätigen...und Code:.
9. Geben Sie Ihren neuen Code nochmals ein.
Das Display zeigt PIN-Code | Bitte warten.
Das Display zeigt Benutzer Nr. | Gespeichert.

Sie haben erfolgreich Ihren PIN-Code geändert.

5.17 Service

Beschreibung der Funktionen des Menüs **Service**. Siehe auch die Übersicht „Menüführung in Bedieneinheit“ auf Seite 44.

5.17.1 Werkseinstellung: Laden Terminal ab Werk

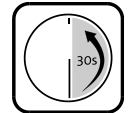
Achtung: Dieses Laden der Werkseinstellungen löscht Benutzer- und Konfigurationseinstellungen.

Vorsicht

Durch das Laden der Werkseinstellungen werden für das System spezifische, auch Hardware- und Benutzer-Einstellungen gelöscht.

Nach dem Hochfahren kann gegebenenfalls nur der jeweilige Schlossmaster öffnen.

Speichern Sie die aktuelle Konfiguration mit optionaler Software, bevor Sie die Werkseinstellungen laden.



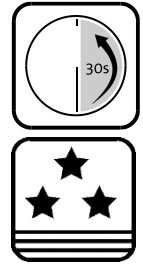
1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit **>** **Service** und Taste **✓** **Enter**.
Das Display zeigt Service | Werkseinstellung. Falls Service nicht verfügbar ist, öffnen Sie alle Schlösser zuerst.
3. Bestätigen Sie mit **Enter**.
Das Display zeigt Code-Eingabe und Systemmanager, gegebenenfalls 0123456789 und Code:.
4. Geben Sie den Systemmanagercode ein.
Das Display zeigt Systemmanager und Terminal.
5. Bestätigen Sie mit **Enter**.
Das Display zeigt Code-Eingabe und Systemmanager, gegebenenfalls 0123456789 und Code:.
6. Geben Sie den Systemmanagercode nochmals ein.
Angezeigt werden Systemmanager | Bitte warten und INITIALISIERUNG | EEPROM LOESCHEN, OK, TwinLock und System Setup.
7. Bestätigen Sie mit **Enter**.
Das Display zeigt gegebenenfalls Sprache | 1 Deutsch. Mit Enter können Sie bestätigen, mit < oder > können Sie eine andere Sprache wählen.
8. Bestätigen Sie die gewählte Sprache mit **Enter**.
Das Display zeigt Deutsch | Gespeichert und danach System - Setup | Neues System.
9. Wählen Sie mit **<** oder **>** **Terminal - Wechsel** und **Enter**.
Das Display zeigt System - Setup | Terminal: 1.
10. Bestätigen Sie mit **Enter**.
Das Display zeigt System - Setup | Anzahl DMS: 1.
11. Wählen Sie mit **<** oder **>** die Anzahl der Schlösser und **Enter**.
Das Display zeigt Seriennummer | Schloss 1 und Code-Eingabe | Systemmanager und Code:.

12. Geben Sie den Systemmanagercode ein.
Das Display zeigt Seriennummer | Bitte warten.
Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.
Das Display zeigt Seriennummer | Gespeichert.
Bei mehreren Schlössern im System zeigt das Display
Seriennummer | Schloss 2 und
Code-Eingabe | Manager und Code:.
13. Geben Sie gegebenenfalls den Managercode des Schlosses 2 sowie gegebenenfalls auch den des Schlosses 3 ein.
Werkseingestellt entsprechen diese dem Systemmanagercode ab Werk.
Das Display zeigt Seriennummer | Bitte warten.
Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.
Das Display zeigt Seriennummer | Gespeichert.
Nach dem letzten Schloss zeigt das Display Datum/Uhrzeit und
Code-Eingabe | Systemmanager und Code:.
14. Wählen Sie die Ziffern des Systemmanagercodes.
System-Uhrzeit und Datum werden angezeigt.
15. Drücken Sie die Taste `Enter`, um Uhrzeit und Datum einzustellen.
16. Geben Sie die Uhrzeit mit `<` und `>` und `Enter` oder mit den Zifferntasten ein.
Im Display blinkt der Cursor vor dem eingestellten Wochentag.
17. Wählen Sie mit `<` und `>` die beiden ersten Buchstaben des aktuellen Wochentags und bestätigen Sie mit `Enter`.
Im Display blinkt der aktuell eingestellte Tag.
18. Geben Sie Tag, Monat und Jahr ein.
Das Display zeigt Datum/Uhrzeit | Gespeichert,
und gegebenenfalls, versionsabhängig Netzwerk | SoftwareV 2.
19. Falls erforderlich, wählen Sie mit `>` Einstellung `0`, wenn das System in kein Netzwerk eingebunden ist oder wenn Sie das Netzwerk deaktivieren wollen oder
wählen Sie mit `>` Einstellung `2`, wenn das System in ein Netzwerk eingebunden ist und wenn Sie das Netzwerk aktivieren wollen und bestätigen Sie mit `Enter`.
Das Display zeigt Schlosssystem | Angemeldet.
Danach zeigt das Display gegebenenfalls Anzahl DMS Aussentuer: 0
und danach Anzahl DMS Innentuer: 0.
20. Geben Sie die Anzahl der Schlösser in Innen- / Außentür ein, falls erforderlich.
Schlosssystem | Angemeldet und
CashProtect | 01.07.24 wird beispielsweise angezeigt.

Sie haben erfolgreich ein Reset durchgeführt.

5.17.2 Werkseinstellung: Codes Löschen Schloss

Achtung: Dieses Löschen der Schlosscodes löscht alle Benutzercodes und den Mastercode. Schlossadresse und Managercode bleiben erhalten.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie mit > **Service** und Taste **✓** Enter.
*Das Display zeigt **Service** | Werkseinstellung. Falls **Service** nicht verfügbar ist, öffnen Sie das Schloss / die Schlösser zuerst.*
3. Bestätigen Sie mit Enter.
*Das Display zeigt **Code-Eingabe** und **Systemmanager**, gegebenenfalls **0123456789** und **Code:**.*
4. Geben Sie den Systemmanagercode ein.
*Das Display zeigt **Systemmanager** und **Terminal**.*
5. Wählen Sie mit < oder > **Schloss** und Enter sowie gegebenenfalls **Schloss 1**, **Schloss 2** oder **Schloss 3** und Enter.
*Das Display zeigt **Code-Eingabe** und **Systemmanager**, gegebenenfalls **0123456789** und **Code:**.*
6. Geben Sie den Systemmanagercode nochmals ein.
*Angezeigt werden **Benutzer 01** | **Geloescht** und **Benutzer 02** | **Geloescht** und so weiter bis **Benutzer 99**. Auch der **Mastercode** wird gelöscht. Das Löschen nimmt einige Zeit in Anspruch.*

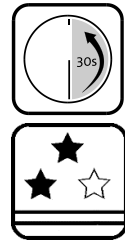
Sie haben erfolgreich alle Benutzerinformationen aus dem Schloss entfernt.

5.17.3 Motor-Schritt

Schlossmaster können mit Menü **Motor-Schritt** den Schlossriegel schrittweise ein- und ausfahren und so den Mechanismus testen.

Hinweis

Falls mit der optionalen PC-Software „automatisches Schließen“ eingestellt wurde, schließt das System das Schloss eine Minute nach der Ausführung der hier beschriebenen Motorschritte.
Falls nicht, bleibt der Riegel in der Position, in die er mit dem letzten Motorschritt gefahren wird.



1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
Siehe Abschnitt „Der Systemstatus“ am Anfang dieses Kapitels.
2. Wählen Sie mit der Taste > **Service** und Taste Enter.
Das Display zeigt Service | Werkseinstellung.
3. Wählen Sie mit > **Motor-Schritt** und wieder Enter.
Das Display zeigt Service | Motor-Schritt.
4. Bestätigen Sie mit Enter.
Das Display zeigt Code-Eingabe | Schloss 01.
5. Wählen Sie mit > gegebenenfalls das Schloss, dessen Riegel Sie schrittweise bewegen wollen, und Taste Enter.
Das Display zeigt Code-Eingabe, Master ... und Code:.
6. Geben Sie den Mastercode ein.
Das Display zeigt Motor-Schritt | <== Auf | Zu ==> .
7. Wählen Sie mit < oder > **Auf** oder **Zu**.
Das Display zeigt Bitte warten.
Der Schlossriegel fährt einen Schritt auf oder zu und stoppt
Das Display zeigt Schritt OK.
8. Wiederholen Sie Schritt 7, wenn gewünscht, auch in Gegenrichtung.

Sie haben den Schlossriegel erfolgreich schrittweise ein- / ausgefahren.

5.17.4 Schloss anmelden

Der Systemmanager kann mit Menü **Schloss anmelden** ein neues Schloss im System anmelden oder ein vorhandenes Schloss ersetzen.

Mit dem Menü **Service | Schloss anmelden** können nur neue, noch nicht adressierte Schlösser im System angemeldet werden – beim Auswechseln eines Schlosses (**Schloss wechseln**) oder beim Erweitern des Systems um ein Schloss (**Schloss neu**).

Zum Anmelden von Schlössern, die bereits zuvor adressiert worden sind, gehen Sie bitte vor wie beim Wechseln der Bedieneinheit. Siehe Beschreibung „Reset“ in diesem Kapitel.



Sie benötigen ein neues, noch nicht adressiertes Schloss

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wählen Sie **Service** mit **>** und **Enter**.
Das Display zeigt Service | Werkseinstellung.
3. Wählen Sie mit **>** **Schloss anmelden** und **Enter**.
Das Display zeigt Service | Schloss anmelden.
4. Bestätigen Sie mit **Enter**.
Das Display zeigt Schloss anmelden | Neues Schloss.
Weiter geht's bei „Zusätzliches Schloss“ im Fall einer Systemerweiterung oder bei „Schloss wechseln“ beim Wechsel eines Schlosses.

5.17.4.1 Zusätzliches Schloss

ist die Fortsetzung von „Schloss anmelden“, falls Sie ein zusätzliches neues Schloss anmelden. Siehe auch „Schloss wechseln“ unten.

5. Bestätigen Sie **Neues Schloss** mit **Enter**.
Das Display zeigt Code-Eingabe und Systemmanager, gegebenenfalls 0123456789, und Code:.
6. Geben Sie den Systemmanagercode ein.
Das Display zeigt Bitte warten | Schloss neu und Schloss 2/3.
Das Display zeigt ! Buskabel ein !. Die angezeigte Schlossnummer ist die, die das neue Schloss im System bekommt (Anzahl der vorhandenen Schlösser + 1).
7. Wenn Sie das Kabel verbunden haben, bestätigen Sie mit **Enter**.
Das Display zeigt Seriennummer | Bitte warten.
Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.
Das Display zeigt Seriennummer | Gespeichert.
Das Display würde Com-Fehler | Setup-Fehler anzeigen, wenn das „neue“ Schloss schon einmal adressiert wurde.
Das Display zeigt Gespeichert, Schloss X, Angemeldet und CashProtect | 02.04.24.

Sie haben das zusätzliche Schloss erfolgreich angemeldet.

5.17.4.2 Schloss wechseln

ist die Fortsetzung von „Schloss anmelden“, falls Sie ein Schloss auswechseln und das System nicht um ein zusätzliches Schloss erweitern. Siehe auch „Zusätzliches Schloss“ oben.

5. Führen Sie Schritte 1-4 der Anleitung „Schloss anmelden“ aus.
Das Display zeigt Schloss anmelden | Neues Schloss.
6. Wählen Sie mit > Schloss wechseln und Enter.
Das Display zeigt Schloss wechseln und Schloss 1<.
7. Wählen Sie mit > das zu ersetzende Schloss und Enter.
Das Display zeigt ! Buskabel ein !.
8. Wenn Sie das Kabel verbunden haben, bestätigen Sie mit Enter.
Das Display zeigt Com-Fehler | Setup-Fehler, wenn das „neue“ Schloss schon einmal adressiert wurde.
Das Display zeigt Seriennummer | Schloss 2/3, Code-Eingabe, Systemmanager, gegebenenfalls 0123456789 und Code:.
9. Geben Sie den Systemmanagercode ein.
Das Display zeigt Seriennummer | Bitte warten.
Die Seriennummer der Bedieneinheit wird im Schloss gespeichert.
Das Display zeigt Seriennummer | Gespeichert,

Schloss | Angemeldet und
CashProtect | 02.04.24.
10. Testen Sie das Öffnen und Schließen und prüfen Sie gegebenenfalls, ob der Riegelwerkskontakt richtig eingestellt ist.

Sie haben erfolgreich ein neues Schloss angemeldet.

5.17.5 System bei defektem Riegelwerkskontakt schließen

Wenn Sie eine Schaltung für einen Riegelwerkskontakt angeschlossen haben, können Sie das System auch bei defektem Schalter einmalig verschließen, indem Sie die folgend beschriebenen Schritte ausführen und dann das System verschließen.

1. Öffnen Sie das Schloss.
Siehe in diesem Kapitel Abschnitt „Öffnen und Schließen“.
2. Drücken Sie kurz **Enter**. Wenn das Display das Datum zeigt, wählen Sie mit der Taste **> Service** und Taste **Enter**.
Das Display zeigt Service | Werkseinstellung.
3. Wählen Sie mit **> 1x Riegelwerk** und danach **Enter**.
*Das Display zeigt 1x Riegelwerk | *=Ja *=Nein.*
4. Wählen Sie mit **> Ja** und danach **Enter**.
Das Display zeigt 1x Riegelwerk | Gespeichert.
Sie können das System nun bei defektem Schalter einmalig schließen.
5. Schließen Sie das Schloss.
Siehe die Beschreibungen „Schloss...schließen“. Das System ist gesichert.

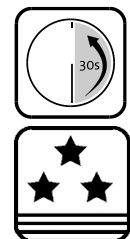
Sie haben das System trotz eines defekten Riegelwerksstellungsschalters erfolgreich verschlossen.



5.17.6 Lizenzierung

Hier geht es um die Lizenzierung weiterer Software wie etwa MultiPad Go! Softwarelizenzen erhalten Sie auf Anfrage von Ihrem Softwarelieferanten.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
2. Wenn das Display nichts anzeigt, drücken Sie kurz Taste **Enter**.
3. Wählen Sie mit **> Service** und bestätigen Sie mit **Enter**.
Das Display zeigt Service | Werkseinstellung.
4. Wählen Sie mit **<** und **> Lizenzierung** und danach **Enter**.
Das Display zeigt Code-Eingabe | Systemmanager und Code:.
5. Geben Sie den Systemmanagercode ein.
Das Display zeigt beispielsweise Lizenzierung und Code:.
Lizenzierung: 00 (Funktionsnummer = 00): Lizenzierung aus.
Wenn die Lizenzierung ausgeschaltet ist, kann die GUI von Software angezeigt, aber nicht gespeichert werden. Es werden keine Daten zum Schloss übertragen. Der Status der Lizenzierung wird in Menü „Status/Info“ angezeigt.
6. Geben Sie eine 10-stellige Ziffernfolge ohne Leerstellen ein, die aus einer 2-stelligen Funktionsnummer und dem 8-stelligen Lizenzierungscode (Liz.-Code) besteht.
Funktions-Nr.: 01 + Liz.-Code -> um „Ben.-Gruppe 2 (Netzwerk)“ freizuschalten.
Funktions-Nr.: 07 + Liz.-Code -> um TwinLock B650 CashProtect zu lizenzieren.
Funktions-Nr.: 08 + Liz.-Code -> um TwinLock B670 CashProtect DS zu lizenzieren.
Lizenzierung: FF wird im Fehlerfall angezeigt. Die Eingabe von „0000000000“ (10x Null) löscht die Lizenzen gegebenenfalls. Das Display zeigt Gespeichert.

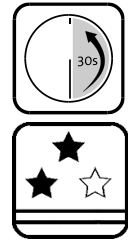


Sie haben die Lizenzierung in / außer Kraft gesetzt.

5.17.7 Neustart

Der Systemmanager kann mit Menü **Neustart** das System mit den aktuellen Einstellungen neu starten.

1. Öffnen Sie das Schloss.
Siehe in diesem Kapitel Abschnitt „Öffnen und Schließen“.
2. Wenn das Display das Datum zeigt, wählen Sie mit der Taste > **Service** und Taste Enter.
Das Display zeigt Service | Werkseinstellung.
3. Wählen Sie mit > **Neustart** und danach Enter.
Das Display zeigt gegebenenfalls Neustart | Schloss 1:.
4. Wählen Sie mit > das gewünschte Schloss und danach Enter.
Das Display zeigt Code-Eingabe | Manager | Code:.
5. Geben Sie den Managercode ein und wählen Sie mit < und > **Neustart** und danach Enter.
Das System startet mit unveränderten Parametern neu.



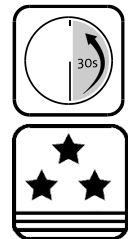
Sie haben das System erfolgreich neu gestartet.

5.17.8 Firmware Update

Nur verfügbar, wenn Firmware hochgeladen. Der Manager kann hochgeladene Firmware Updates verwerfen, verschieben oder freigeben.

Vorbedingungen Update via TwinIP gespeichert, Meldung **Firmware update** wird nach Start auf dem Display angezeigt.

1. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
Siehe in diesem Kapitel Abschnitt „Öffnen und Schließen“.
2. Wenn das Display nichts anzeigt, drücken Sie kurz Taste Enter.
3. Wählen Sie mit > **Service** und bestätigen Sie mit Enter.
Das Display zeigt Service | Werkseinstellung.
4. Wählen Sie mit < und > **Firmwareupdate** und danach Enter.
Das Display zeigt Code-Eingabe | Systemmanager und Code:.
5. Geben Sie den Systemmanagercode ein.
*Das Display zeigt Terminal | *=Ja | *=Nein.*
- 6.A Wählen Sie **Clear** oder warten Sie, um das Update später durchzuführen.
- 6.B Wählen Sie ***=Nein**, um das Update zu verwerfen.
- 6.C Wählen Sie ***=Ja**, um das Update durchzuführen.
Der Updateprozess startet. Die LEDs leuchten weiß. Bitte warten wird 5 Sekunden lang angezeigt. Die LEDs leuchten weiter. Stromversorgung nicht unterbrechen! Nach etwa 2 Min. 15 Sek. meldet sich das Terminal upgedatet wieder.



Sie haben das Firmware Update im Standardfall erfolgreich freigegeben.

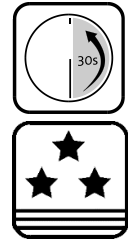
5.18 Import / Export

Optionen des Menüs **Import / Export**. USB wird für den Im- und Export genutzt.

5.18.1 Konfiguration und Sprache importieren

Vorbedingungen Sie haben Manager-Berechtigung.

Sie benötigen USB-Verbindung, siehe Seite 34; Port / Schnittstelle via CashProtectPro.



1. Stellen Sie sicher, dass USB-Anbindung besteht.
Bedieneinheit und Rechner mit USB-Kabel verbinden.
2. In CashProtectPro, Menü „Comm“, „USB“ und den Port wählen.
Um mit der Konfiguration auch eine Sprache zu importieren, laden Sie die gewünschte Sprachdatei via „Einstellungen“, „Dateien“, „Sprachdatei“ und wählen Sie den gewünschten Sprachplatz in QPad (Sprache auf Platz 1 wird gleich nach dem Laden angezeigt). Als „Loggingsprache“ kann gegebenenfalls eine weitere Datei geladen werden (Details bei Redaktionsschluss noch nicht feststehend).
3. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
4. Wählen Sie mit den Menütasten < und > **Import / Export** und bestätigen Sie mit Taste **Enter**.
Import / Export | USB wird angezeigt.
5. Bestätigen Sie mit Taste **Enter**.
Code-Eingabe | Systemmanager | Code: *kann angezeigt werden.*
6. Geben Sie den Managercode ein und bestätigen Sie mit Taste **Enter**.
7. Öffnen Sie die Schnittstelle mit „Öffnen“ in CashProtectPro, Menü „Comm“. **Datenverbindung** wird angezeigt.
8. Starten Sie den Export nach CashProtectPro, indem Sie in CashProtectPro Schaltfläche „Lesen“ wählen, die Konfiguration anpassen und Schaltfläche „Schreiben“ wählen.
Die angepasste Schlosskonfiguration wird ins Schlosssystem importiert.
9. Wenn CashProtectPro „Konfiguration erfolgreich geschrieben“ zeigt, schließen Sie den Port via CashProtectPro, Menü „Comm“: dort „Trennen“ wählen.
„Die Verbindung wurde erfolgreich abgebaut“ wird angezeigt.

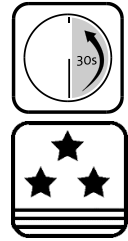
Sie haben die Konfiguration und Sprache erfolgreich ins Schlosssystem importiert.

5.18.2 Meldungen beim Lesen der Konfiguration

Während des Einlesens einer Konfiguration können die im Folgenden aufgelisteten Meldungen angezeigt werden.

In der ersten Zeile des Displays wird **Fehler Konfig.** angezeigt, wenn ein Parameter einen ungültigen Wert aufweist und **Schlosssystem**, wenn die Konfiguration nicht zum System passt.

Ändern Sie ungültige Parameter mit der optionalen Software CashProtect-Pro oder TwinNet und lesen Sie die Konfiguration erneut ein.



Fehlertext in der zweiten Zeile:

Alarm-Verzoeg.

! Alarmverzögerung bei stillem Alarm liegt nicht im zulässigen Wertebereich von 0-99 Minuten.

✓ *Tragen Sie einen zulässigen Wert ein.*

Benutzercodes

! Zu wenig PIN-Codes im System. Falls die Konfiguration eingelesen würde, könnte das Schloss nicht mehr geöffnet werden.

✓ *Erhöhen Sie die Anzahl berechtigter Benutzer im System.*

Sondertage

! Für mindestens einen „Sondertag“ wurde ein ungültiges Datum eingetragen.

✓ *Berichtigen Sie die Daten für das Zeitprogramm „Sondertage“.*

Sperrzeit

! Für „Sperrzeit“ wurde mindestens ein ungültiges Datum eingetragen.

✓ *Berichtigen Sie die Daten für das Zeitprogramm „Sperrzeit“.*

Stiller Alarm

! Der Wert für „Alarmziffer“ liegt nicht im zulässigen Wertebereich von 01-09.

✓ *Tragen Sie einen zulässigen Wert ein.*

Tuer offen

! Der Wert für „Türöffnungsüberwachung“ liegt nicht im zulässigen Wertebereich von 00-99 Minuten.

✓ *Tragen Sie einen zulässigen Wert ein.*

Wochenprogramm

! Für Zeitprogramm „Wochenprogramm“ wurde mindestens eine ungültige Uhrzeit eingetragen.

✓ *Tragen Sie einen zulässigen Wert ein.*

Zeitverzoeigerung

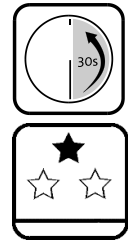
! Der Wert für „Öffnungsverzoeigerung“ / „Zeitverzoeigerung“ des Schlosses liegt nicht im zulässigen Bereich von 00-99.

✓ *Tragen Sie einen zulässigen Wert ein.*

5.18.3 Konfiguration / Protokoll exportieren / drucken

Vorbedingungen Für Sie sind in der Benutzermatrix **Freigabe**, **Service** und **PIN-Code** aktiviert oder Sie haben Master- oder Manager-Berechtigung.

Sie benötigen USB-Verbindung, siehe Seite 34. Port / Schnittstelle via CashProtectPro einrichten.



1. Stellen Sie sicher, dass USB-Anbindung besteht.
Die Bedieneinheit und den Rechner mit USB-Kabel verbinden.
2. In CashProtectPro, Menü „Comm“, „USB“ und den Port auswählen (beispielsweise COM3).
3. Entsperren Sie das System (Schloss 1 oder alle Schlösser öffnen).
4. Wählen Sie mit der Taste > `Import / Export` und Enter.
`Import / Export | USB` wird angezeigt.
5. Bestätigen Sie mit Taste Enter.
`Code-Eingabe | Systemmanager | Code:` *wird angezeigt.*
6. Geben Sie den Managercode ein oder wählen Sie mit > einen berechtigten Benutzer und geben Sie dessen Code ein.
7. Öffnen Sie die Schnittstelle mit „Öffnen“, Menü „Comm“ in CashProtectPro.
`Datenverbindung` *wird angezeigt.*
8. Starten Sie den Export in CashProtectPro, indem Sie in CashProtectPro Schaltfläche „Lesen“ wählen, die Meldung „Konfiguration erfolgreich gelesen“ bestätigen, Bereich „Protokoll“ und dort „Protokolldatei laden“ wählen.
Konfiguration und Protokoll werden nach CashProtectPro exportiert.
9. Wenn Transfer beendet („Protokoll erfolgreich gelesen“), schließen Sie in CashProtectPro den Port, indem Sie [Kommunikation] „Schließen“ wählen.
„Die Verbindung wurde erfolgreich abgebaut“ wird angezeigt.
10. Wählen Sie das Druckersymbol, um das Protokoll zu drucken.
Das Protokoll wird gedruckt. Mit Schaltfläche `CSV export` können Sie es als CSV-Datei exportieren. Sie können auch die Konfiguration drucken, indem Sie „Übersicht“ und das Druckersymbol wählen.

Sie haben Konfiguration und Protokoll erfolgreich nach CashProtectPro exportiert.

5.18.4 Sprache wählen

Jeder Benutzer kann zwischen drei Sprachen wählen, wenn diese in der Bedieneinheit gespeichert wurden.



1. Drücken Sie kurz *Clear*.
Das Display zeigt beispielsweise Mo 01.07.24 15:50.
2. Drücken Sie *Enter* und halten Sie die Taste gedrückt.
Sprache wird angezeigt.
3. Bestätigen Sie *Sprache* mit *Enter*.
Sprache | 1 Deutsch wird angezeigt.
Sie können Deutsch bestätigen oder gegebenenfalls die Sprachen auf Sprachplatz Nr. 2 oder 3 wählen.
4. Wählen Sie die Sprache mit *>* und bestätigen Sie mit *Enter*.
Das Display zeigt Sprache | Gespeichert und Sprache | OK.

Sie haben die Sprache des Displays der Bedieneinheit erfolgreich geändert.

6 Wartung, Reparatur und Reinigung

Das System ist wartungsfrei. Es wurde vor Auslieferung auf 100.000 Öffnungs- und Schließzyklen geprüft.

Der vom Hersteller des Riegelwerks angegebene Wartungszyklus ist für das Riegelwerk einzuhalten.

Reparaturen dürfen ausschließlich von Elektrofachkräften (siehe Definition auf Seite 14), die von INSYS MICROELECTRONICS oder berechtigten Partnerunternehmen geschult und autorisiert wurden, durchgeführt werden.

Vorsicht

Gefahr von Kurzschluss der elektronischen Komponenten.

Gefahr der Beschädigung des Systems

Beachten Sie die Anweisungen zur Reinigung des Systems.

Reinigen Sie die Eingabeeinheit mit sehr wenig Wasser oder mit sehr wenig milder Seifenlösung. Verwenden Sie dazu ein feuchtes, weiches, sauberes und fusselfreies Tuch. Verwenden Sie keine anderen Mittel. Verwenden Sie zur Desinfektion (Wischdesinfektion, Nachwischen mit einem mit Trinkwasser befeuchtetem Tuch) nur Mittel, deren Produktbeschreibung ausweist, dass sie über eine gute Materialverträglichkeit mit den Kunststoffen Polyethylen (PE), ABS und PC-ABS verfügen.

Reinigen Sie alle anderen Komponenten des Systems nur, wenn Ihnen dies unumgänglich erscheint. Benutzen Sie ausschließlich ein trockenes, weiches, sauberes und fusselfreies Tuch.

Wischen Sie über die Oberfläche, ohne großen Druck auszuüben.

7 Störungsabhilfe

7.1 System bei Netzausfall mit Spannung versorgen

Batteriehersteller bieten passende 9 Volt Blockbatterien unter den Bezeichnungen 6LR61 (Alkali-Mangan), 6F22 (Zink-Kohle), 6AM6, 522 an.

Sie benötigen ein Adapterkabel (im Lieferumfang), eine aufgeladene 9 Volt Blockbatterie und Zugriff auf die Bedieneinheit.

1. Verbinden Sie Adapterkabel und Batterie. Achten Sie dabei auf die unterschiedliche Größe der Steckverbindungen von Plus- und Minuspol der Batterie.
2. Stecken Sie den Stecker des Adapterkabels in die Buchse auf der Unterseite der Bedieneinheit.

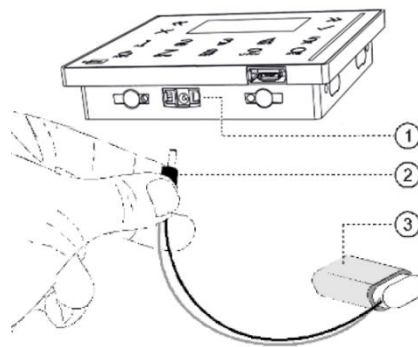


Abb. 19: Adapterkabel mit Eingabeeinheit verbinden

- 1) Buchse für Spannungsversorgung bei Netzausfall
- 2) Mini DC-Stecker des Adapterkabels
- 3) 9 Volt Blockbatterie

Sie versorgen das System erfolgreich mit Spannung.

7.2 Fehlermeldungen

Siehe auch Kapitel „Bedienung“, Abschnitt „Meldungen beim Lesen der Konfiguration“.

Alarm-Codefehler

- ! Fehler beim Speichern eines Codes in TwinAlarm.
- ✓ *Wiederholen Sie den Speicherungsversuch. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Meldung wiederholt angezeigt wird.*

Autorisierung

Codekarte Keine Freigabe Öffnen PIN-Code Schließen&Code
Service Unscharfschalten

- ! Benutzer ist für den gewählten Vorgang nicht autorisiert. Nach einer Sekunde zeigt das Display, welche Art der Autorisierung dem Benutzer in der Benutzermatrix der PC-Software nicht verliehen wurde (siehe unten, „Codekarte“, „Freigabe“...).
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, damit er die Autorisierung in der Benutzerverwaltung von CashProtectPro ergänzt.*

Codekarte

- ! Benutzer darf keine Codekarte benutzen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

Keine Freigabe

- ! Benutzer hat keine Freigabe für die Eingabe von Codes.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

Öffnen

- ! Benutzer darf kein Schloss öffnen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

PIN-Code

- ! Benutzer darf keinen PIN-Code eingeben.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

Schließen&Code

- ! Benutzer darf Schlösser mit der Eingabe von PIN-Code nicht schließen.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

Service

- ! Benutzer darf Protokoll nicht exportieren.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

Unscharfschalten

- ! Benutzer darf Einbruchmeldeanlage nicht „unscharf“ schalten. Behebung siehe oben.
- ✓ *Sprechen Sie gegebenenfalls mit Ihrem Systemverwalter, siehe oben.*

Bus A/B empfangen**Bus A/B senden**

- ! Ein Schloss lässt sich auf Bus A / Bus B nicht mehr ansprechen. Eventuell ist ein Kabel nicht korrekt eingesteckt oder defekt.
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung.*

Codes identisch!

- ! Ein neuer Code entspricht dem bisherigen, zu ändernden.
- ✓ *Melden Sie einen anderen Code an.*

COM-Fehler**Fehler Antwort**

- ! In der Kommunikation zwischen der Bedieneinheit und einer anderen Systemkomponente (z.B. einem Schloss) ist ein Fehler aufgetreten. Die Bedieneinheit hat einen nicht vorgesehenen Befehl empfangen.
- ✓ *Softwarefehler. Setzen Sie sich bitte mit dem Support in Verbindung.*

COM-Fehler

Bus A/B senden Bus A/B empfangen

- ! Ein Schloss lässt sich auf Bus A / Bus B nicht mehr ansprechen. Eventuell ist ein Kabel nicht korrekt eingesteckt oder defekt.
- ✓ *Setzen Sie sich bitte mit dem Support in Verbindung.*

EEPROMfehler AB / DMS / TM

- ! Fehler beim Lesen vom / Schreiben ins EEPROM der Bussysteme (AB)/ von Schloss (DMS) / der Bedieneinheit (TM für Terminal).
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

Eingabefehler

- ! Falsche / ungültige Eingabe. Möglicherweise wurde ein PIN-Code nicht korrekt eingegeben oder bei gewählter Option „Parallelcode“ oder „Codeverknüpfung“ haben nicht zwei verschiedene Benutzer ihren Code eingegeben, sondern nur einer.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

Falscher Code | Sperrzeit

- ! Beim Versuch, ein Schloss zu öffnen, wurde viermal ein falscher Code eingegeben, wodurch eine Sperrzeit aktiviert wurde. Die Sperrzeit verlängert sich bei jeder weiteren Falscheingabe um eine Minute.
- ✓ *Warten Sie ab, bis die Sperrzeit abgelaufen ist, und geben Sie den Code korrekt ein.*
- ✓ *Setzen Sie sich bitte mit Ihrem Systemadministrator / dem Support in Verbindung, wenn Sie nicht im Besitz des korrekten Codes sind.*

Falsche Karte

- ! Ein Benutzer hat eine Karte des falschen Typs in die Bedieneinheit gesteckt, beispielsweise eine Sprach- statt einer Konfigurationskarte.
- ✓ *Wählen Sie die passende Karte. Setzen Sie sich bitte mit dem Support in Verbindung, wenn Sie nicht im Besitz der geeigneten Karte sind.*

Fehler DMS Nr.

- ! Das Schloss mit der angegebenen Nummer meldet einen allgemeinen Fehler.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

Fehler Karte

- ! In der Kommunikation zwischen der Bedieneinheit und einer Chipkarte ist ein Fehler aufgetreten.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

Fehler Motor A**Fehler Motor B**

- ! Der Riegel des Schlosses kann nicht über Bus A / Bus B bewegt werden. Eventuell ist die Platine oder der Motor des Schlosses defekt oder der Riegel erreicht die Endposition nicht.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

Fehler Scharf!

- ! TwinAlarm meldet Fehler beim Scharfschalten der Einbruchmeldeanlage (EMA): EMA kann nicht scharf geschaltet werden, weil das System nicht gesichert ist.
- ✓ *Schließen Sie die Schlösser und wiederholen Sie den Vorgang.*

Fehler: Seriennr.

- ! Die Seriennummern in der Bedieneinheit und im Schloss sind nicht identisch.
- ✓ *Diese Meldung wird angezeigt, wenn Bedieneinheit oder Schloss nicht vorschriftsmäßig gewechselt wurden. Sabotage ist möglich. Bitte setzen Sie sich mit den für die Sicherheit zuständigen Personen in Verbindung.*

Fehler TwinAlarm

- ! In der Kommunikation mit der Schalteinrichtung TwinAlarm ist ein Fehler aufgetreten.
- ✓ *Wiederholen Sie den Vorgang. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

Fehler Unscharf!

- ! TwinAlarm meldet Fehler beim Unscharf-Schalten der Einbruchmeldeanlage (EMA): EMA kann nicht unscharf geschaltet werden, weil von ihr keine Quittierung der Unscharf-Schaltung erfolgt.
- ✓ *Setzen Sie sich bitte mit dem Alarmtechniker / Support in Verbindung, um die Verbindung zur EMA überprüfen zu lassen.*

Firmwareupdate | !!!Fehler!!!

- ! Fehler beim Firmware Update.
- ✓ *Setzen Sie sich bitte mit dem Alarmtechniker / Support in Verbindung, wenn das Firmware Update nicht erfolgreich beendet werden kann.*

Keine Freigabe

- ! Keine Öffnung möglich. Schloss ist über den Eingang FREIGABE von TwinXT (small) / TwinAlarm nicht freigegeben.
- ✓ *Prüfen Sie, ob TwinXT / TwinAlarm richtig angeschlossen ist und ob das Schloss berechtigterweise gesperrt ist. Setzen Sie sich bitte mit dem Support in Verbindung, wenn die Meldung weiterhin angezeigt wird.*

Keine Karte

- ! Es wurde keine RFID Karte vor den RFID Leser gehalten.
- ✓ *Wiederholen Sie den Vorgang und halten Sie eine RFID-Karte nahe vor den RFID Leser.*

Keine TwinAlarm!

- ! Die Schalteinrichtung TwinAlarm ist deaktiviert.
- ✓ *Stellen Sie sicher, dass die Schalteinrichtung richtig angeschlossen und initialisiert ist.*

! Manipulation !

- ! Ein Code wurde mehr als dreimal falsch eingegeben.
 - ✓ *Kontrollieren Sie im Protokoll, welcher Benutzer dies verursacht hat.*

Motorfehler

- ! Der Riegel des Schlosses kann nicht bewegt werden. Eventuell ist die Platine oder der Motor des Schlosses defekt oder der Riegel erreicht die Endposition wegen eines mechanischen Problems nicht.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung.*

RTC-Fehler

- ! Die Uhr (Real Time Clock) der Bedieneinheit funktioniert nicht korrekt.
- ✓ *Bitte setzen Sie sich mit dem Support in Verbindung, wenn die Fehlermeldung weiterhin angezeigt wird.*

Schloss Mitte

- ! Schlossriegel ist weder geschlossen noch geöffnet, sondern in Mittelposition.
- ✓ *Prüfen Sie, ob sich ein Hindernis vor dem Schlossriegel befindet, welches das Ausfahren des Riegels behindert.*
- ✓ *Prüfen Sie, ob sich das Schloss öffnen / schließen lässt. Wenn nicht, setzen Sie sich bitte mit dem Support in Verbindung.*

Schlosssystem

- ! Es wurde versucht, einen Code abzumelden, ohne den das System nicht mehr zu öffnen wäre.
- ✓ *Deaktivieren Sie gegebenenfalls „Codeverknüpfung“ oder „Parallelcode“ oder ordnen Sie die Öffnungsberechtigung für das Schloss weiteren Benutzern zu, bevor Sie den Code abmelden.*

Sondertage

- ! Das aktuelle Datum fällt auf einen „Sondertag“, an dem das Öffnen des Schlosses nicht gestattet ist.
- ✓ *Warten Sie, bis der „Sondertag“ vorbei ist.*
- ✓ *Öffnen Sie das Schloss (mit Autorisierung zur Schnellöffnung).*
- ✓ *Prüfen Sie das an der Eingabeeinheit QPad eingestellte Datum und korrigieren Sie es gegebenenfalls.*

Sperrzeit

- ! Beim Versuch, das Schloss zu öffnen,
 - wurde mehr als dreimal ein falscher Code eingegeben
 - wurde eine Sperrzeit von 90 Minuten aktiviert, weil mindestens ein Schloss während eines Terminalwechsels geschlossen war
 - wurde versucht, das Schloss während eines Sperrzeitraums zu öffnen.
- ✓ *Warten Sie, bis die Sperrzeit abgelaufen ist und geben Sie den korrekten Code ein.*
- ✓ *Lassen Sie anhand des Protokolls / vom für die Sicherheit zuständigen Personal prüfen, ob versucht wurde, am System zu manipulieren.*

stromlos

- ! Das System war getrennt von der Stromversorgung. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Prüfen Sie, ob Datum und Uhrzeit richtig eingestellt sind.*
- ✓ *Überprüfen sie das Protokoll.*
- ✓ *Lassen Sie vom für die Sicherheit zuständigen Personal prüfen, ob am System manipuliert wurde.*

Terminal-Wechsel

- ! Bedieneinheit wurde gewechselt oder zurückgesetzt. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Diese Meldung erfolgt beim ersten Öffnungs-/Schließvorgang nach dem Zurücksetzen (Reset) oder nach dem Wechsel der Bedieneinheit. Sie erfordert keine Maßnahmen.*
- ✓ *Wenn die Meldung unerwartet erfolgt, könnte es sich um einen Manipulationsversuch handeln. Setzen Sie sich in diesem Fall bitte mit dem für die Sicherheit zuständigen Personal in Verbindung.*

trivialer Code

- ! Ein Benutzer hat einen Code eingegeben, der aus einer Folge linear auf -, absteigender – oder gleicher Ziffern besteht.
- ✓ *Aus Sicherheitsgründen kann eingestellt werden, dass solche Codes nicht erlaubt sind. Geben Sie einen anderen Code ein.*

ungültige Karte

- ! Die Codekarte ist ungültig.
- ✓ *Prüfen Sie, ob Sie eine gültige Karte haben. Setzen Sie sich bitte mit dem Systemadministrator / dem Support in Verbindung, wenn Sie keine gültige Karte besitzen.*

Unscharf-Code??

- ! TwinAlarm kann die angeschlossene Einbruchmeldeanlage (EMA) nicht scharf schalten, weil noch kein Code zum Unscharf-Schalten angemeldet wurde.
- ✓ *Aktivieren Sie gegebenenfalls TwinAlarm und melden Sie einen Code zum Unscharf-Schalten an.*

War Neustart oder | stromlos

- ! Das System war getrennt von der Stromversorgung. Nach der Öffnung des Schlosses wird die Meldung nicht mehr angezeigt.
- ✓ *Prüfen Sie, ob am System manipuliert wurde und ob Datum und Uhrzeit richtig eingestellt sind.*

Wochenprogramm

- ! Die aktuelle Uhrzeit liegt nicht innerhalb eines mit der Funktion „Wochenprogramm“ definierten Zeitfensters für die Öffnung des Schlosses.
- ✓ *Warten Sie, bis das Zeitfenster für die Öffnung kommt.*
- ✓ *Lassen Sie das Schloss von einem via Benutzermatrix in CashProtectPro zur „Schnellöffnung“ autorisierten Benutzer öffnen.*
- ✓ *Prüfen Sie das an der Bedieneinheit eingestellte Datum und korrigieren Sie es gegebenenfalls.*

Zeitprog. Abbruch

- ! Statusmeldung. Die Schaltung Zeitprogrammsperre im gesicherten Bereich Ihres Systems ist geschlossen und unterbricht alle aktiven Zeitprogramme oder ein zur „Schnellöffnung“ autorisierter Benutzer hat ein Schloss trotz aktiven Zeitprogramms geöffnet.
- ✓ *Wenn Sie nicht wünschen, dass aktive Zeitprogramme unterbrochen werden, öffnen Sie die Schaltung Zeitprogrammsperre.*

7.3 Fehlercodes

Wenn nach Eingaben eines Bedieners an der Bedieneinheit Übertragungsprobleme auftreten oder beispielsweise Schlösser melden, dass sie nicht bereit sind, wird der Grund für die Probleme als **Fehlercode** ausgegeben. Fehlercodes können Fachkräften / dem Support Hinweise für die Behebung von Fehlern geben.

Zu Fehlercodes werden folgende **Gerätenummern** angezeigt:

- 00** noch nicht adressiertes Schloss (BasisDMS)
- 01** Schloss 1 (DMS1)
- 02** Schloss 2 (DMS2)
- 03** Schloss 3 (DMS3)
- 10** Startprogramm, Bootloader
- 80** TwinAlarm (ABOX)

Fehlercodes gibt es für Übertragungsfehler (**COM-Fehler**), Schlösser (**DMS**), Alarmgeräte (**80**) und Bootloader (**10**).

Fehlercodes für Übertragungsfehler werden nach Anzeige **COM-Fehler** und Gerätefehler werden nach Anzeige **Fehler DMS X** angezeigt.

Fehlercodes bitte notieren und an den Support übermitteln.

Anzeige Gerätefehler (Beispiel):

Fehler DMS X | 01/A:D0 : Schloss 1 (Bus A) schließt / öffnet nicht, weil es 90 Minuten lang Sperrzeit hat.

Fehlercodes für Gerätefehler

- 31** unerwartete Telegrammdaten
- 32** Fehler Bus Kommunikation
- 33** Fehler Telegramm Prüfsumme
- 35** kein gültiges Befehlsbyte
- 36** Code zu lang
- 37** keine Freigabe
- 39** Eilsperre aktiv
- 41** TwinAlarm: falscher Code
- 42** TwinAlarm: keine Rückmeldung Quittierung bei Scharfschalten / Einstellen EMA
- 43** TwinAlarm: keine Rückmeldung Quittierung bei Unscharf schalten / Abstellen EMA
- 44** TwinAlarm: Fehler Ausgang
- 45** TwinAlarm: RS 232 COM Fehler
- 46** TwinAlarm: EMA nicht bereit zum Scharfschalten / Einstellen
- 47** TwinAlarm: Unscharf Sperre aktiv
- 61** falscher Code
- 62** Fehler Bus Kommunikation
- 63** Motorfehler
- 80** [Bootloader] Flash Fehler
- A0** Code kann nicht gespeichert werden, weil ,nur Einmalcode (OTC)' eingestellt
- C0** Letzter Öffnungsbenutzer konnte nicht ermittelt werden
- D0** Schloss hat 90 Minuten Sperrzeit
- D1** Schloss gesperrt, zu viele falsche Codeeingaben
- D2** Befehl nicht ausgeführt, weil EMA scharf
- E0** Prüfung: Code des letzten Benutzers ungültig, weil ,nur Einmalcode (OTC)' eingestellt
- F1** Kundenschlüssel ungültig
- F2** Kundenschlüssel entschlüsselte Prüfsumme ungültig
- F3** Kundenschlüssel Update fehlerhaft

Anzeige Übertragungsfehler (Beispiel):

COM-Fehler | 10/A:21 : Kommunikationsfehler bei erweitertem Spezialbefehl in Bootloader.

Fehlercodes für Übertragungsfehler

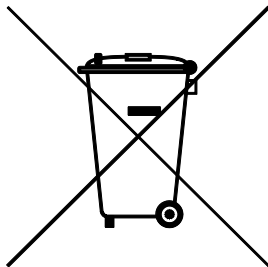
- 01** Sendefehler: I2C-Busfehler bei Anforderung des CTR-Blocks/IV
- 02** Sendefehler: I2C-Busfehler bei Antwort des CTR-Blocks/IV
- 03** Sendefehler: Timeout bei Anforderung des CTR-Blocks/IV
- 04** Sendefehler: Falscher CMD in Antwort des CTR-Blocks/IV
- 05** Sendefehler: Falsche Version in Antwort des CTR-Blocks/IV
- 06** Sendefehler: Problem bei der Berechnung des Session key
- 07** Sendefehler: Problem bei der AES/CBC-Verschlüsselung
- 08** Sendefehler: Problem bei der AES/CTR-Verschlüsselung
- 09** Sendefehler: I2C-Busfehler beim Frame-Senden
- 10** Empfangsfehler: I2C-Busfehler bei Frame-Antwort
- 11** Empfangsfehler: Timeout bei Frame-Antwort
- 12** Empfangsfehler: Problem bei Kundenschlüssel
- 20** unbekannten Befehl von Gegenstelle erhalten
- 21** Kommunikationsfehler bei erweitertem Spezialbefehl
- 22** Gerätefehler (NOK-Fehlercode) von Schloss erhalten
(Bedeutung Fehlercode siehe „Fehlerodes für Gerätefehler“)

8 Technische Unterstützung

INSYS MICROELECTRONICS GmbH
Hermann-Köhl-Sr. 22
93049 Regensburg, Germany
Telefon: +49 941 58692 220
Telefax: +49 941 58692 45
E-Mail: support@insys-locks.de
Internet: <https://www.insys-locks.com>

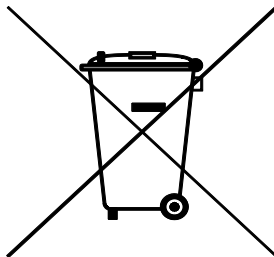
9 Entsorgung

Entsorgen Sie **Plastik-, Elektronikteile und Kabel**, indem Sie sie zu einem zertifizierten Entsorgungsfachbetrieb in Ihrer Nähe bringen oder sie an diese Adresse senden:



Frankenberg – Metallrecycling GmbH
Industriestr.1
D 91448 Emskirchen
Telefon: +49 9104 82622-0
Telefax: +49 9104 82622-22
E-Mail: anfrage@fmr.ag
Internet: <https://www.fmr.ag>

Senden Sie **Schlösser**, gekennzeichnet als „zur Entsorgung“, für eine ordnungsgemäße Rücknahme und Verwertung an diese Adresse:



INSYS MICROELECTRONICS GmbH
Herman-Köhl-Str. 22
D 93049 Regensburg, Deutschland

10 Glossar

Bei Begriffen, die wie **Alarmcode** im Fließtext fettgedruckt sind, handelt sich um Begriffe, zu denen es eigene Einträge im Glossar gibt.

Um die Lesbarkeit nicht zu sehr zu beeinträchtigen, sind nur ausgewählte Begriffe fett gedruckt, die im jeweiligen Kontext eine wichtige Rolle spielen. Lesen Sie auch die Einträge zu diesen Begriffen.

Parameter, die mit Software **CashProtectPro** für Systeme eingestellt werden können, können grundsätzlich auch mit der ebenfalls optionalen, netzbasierten Software **TwinNet** eingestellt werden.

Alle Einträge sind in alphabetischer Reihenfolge aufgeführt.

4-Augen-Prinzip (Öffnung / Konfiguration / Schließen / Freigabe)

siehe **Codeverknüpfung**.

Abmelden

PIN-Codes und Codekarten müssen vom Schlossmaster an einem Schloss angemeldet werden, damit Benutzer das Schloss mit PIN-Code öffnen / sich am Schloss mit Karte identifizieren können. Wenn der Schlossmaster einen PIN-Code / eine Codekarte an einem Schloss abmeldet, kann der zugehörige Benutzer nicht öffnen / sich nicht am Schloss identifizieren.

Alarmcode (für Stillen Alarm)

Aktiviert **Stillen Alarm** und berechtigt zu den gleichen Aktionen wie der zugehörige PIN-Code von Schlossmaster oder (Standard-)Benutzer.

PIN-Code, dessen letzte Ziffer um den in der Software **CashProtectPro** gesetzten Wert für Alarmcode erhöht ist.

Ist beispielsweise die letzte Ziffer Ihres PIN-Codes 9, geben Sie als letzte Ziffer des Alarmcodes die Ziffer „9+eingetragener Wert“ ein. Wenn das Ergebnis dieser Addition zweistellig ist, übertragen Sie nur die zweite Stelle als letzte Codeziffer, beispielsweise nach $9 + 1 = 10$ als letzte Codeziffer „0“.

Anmelden

PIN-Codes und Codekarten müssen vom Schlossmaster an einem Schloss angemeldet werden, damit Benutzer das Schloss mit PIN-Code öffnen / sich am Schloss mit Karte identifizieren können.

Autorisierung

bedeutet hier das, was der **Systemmanager** für Benutzer des Systems via TwinNet oder in der **Benutzermatrix** (für Benutzergruppen via Menü „Code Einstellungen“) von CashProtectPro festlegt. Siehe auch Kapitel „Bedienung“, Abschnitt „Bedienung/Benutzer autorisieren“.

Autorisierung zum Öffnen eines Schlosses mit Benutzercode

Ein Benutzer kann ein Schloss öffnen, indem er seinen PIN-Code eingibt,

- wenn ihn der Systemmanager autorisiert hat (siehe Kapitel Bedienung, Abschnitt „Benutzer autorisieren“) und
- wenn der Schlossmaster für ihn an diesem Schloss PIN-Code und / oder Codekarte (passend zur Autorisierung) angemeldet hat und
- wenn aktuell kein Zeitprogramm das Öffnen unterbindet.

Optional kann das System so konfiguriert werden, dass nur zwei Personen gemeinsam oder zeitlich versetzt ein Wertbehältnis öffnen können (siehe auch **Codeverknüpfung**, **Parallelcode**).

Benutzergruppen

Vorsicht

Ohne autorisierten WTU-Master kann der WTU-Benutzerbereich nicht verwaltet werden.

Autorisieren Sie Benutzer 99 vor Aktivierung von „Benutzergruppen“ ausreichend.

Über Netzwerk nur mit spezieller Lizenz. Bei aktivierter Option „Benutzergruppen“ werden die Benutzer aller Schlösser im System in zwei Gruppen aufgeteilt. Der neue Benutzerbereich bekommt Benutzer Nr.99, der zum „WTU-Master“ wird, als Verwalter. Der ursprüngliche Benutzerbereich verkleinert sich um den neuen Bereich. Die Größe der Gruppen kann fest eingestellt / über das optionale Parametrierset CashProtectPro definiert werden.

Über Feld „Öffnung Benutzergruppen zwingend“ (wird nur angezeigt, wenn Feld „2 Ben.-Gruppen aktiv“ markiert) auf Seite „Codeeinstellungen“ von CashProtectPro kann eingestellt werden, ob die Gruppenmitglieder bei „4-Augen-Prinzip (Öffnung)“ oder „Parallelcode“

- nur gemeinsam mit Mitgliedern ihrer Gruppe (Wert: „gleich“) oder
- nur mit einem Mitglied der anderen Gruppe (Wert: „verschieden“) oder
- mit einer Person aus irgendeiner Gruppe (Wert: „keine“) öffnen können.

Die erste Benutzergruppe (Benutzer Nr.01 bis zu Benutzer Nr.XX-1) wird nach wie vor vom **Schlossmaster** verwaltet. Die neue Gruppe der WTU-Benutzer von Benutzer Nr.XX (= frei definierbare Nr. zwischen 1 und 98) bis Nr.98 wird von Benutzer Nr.99, dem WTU-Master verwaltet.

Benutzermatrix

Registerkarte in Software CashProtectPro, auf der die individuelle Benutzerrechte festgelegt werden; siehe Kapitel Bedienung, Abschnitt „Benutzer autorisieren“. Optionale Gruppenöffnungsregeln (WTU) können auf Registerkarte „Einstellungen“ gesetzt werden.

Benutzern können unter anderem Personalnummern zugeordnet werden. Siehe auch „Optionale Funktionen ab Version IP09“.

CashProtectPro

Optionales Zubehör. Parametrierset, Software für Systeme TwinLock CashProtect. Die Benutzermatrix, in der die grundsätzlichen Berechtigungen für alle Benutzer festgelegt sind, ist ein Teil der Software CashProtectPro.

Code

steht hier für geheime Daten, die ein Benutzer dem System übermitteln muss, bevor er Schlösser öffnen / gegebenenfalls schließen und anderes ausführen darf. Muss in Form von PIN-Code oder Einmalcode übermittelt werden.

Codealterung

Gültig für PIN-Code. Einstellbar von 00-12 Monate, 00 Monate = deaktiviert
Wenn die Option aktiviert ist, wird jeder PIN-Code bei jedem Öffnungsversuch eines Schlosses auf den Zeitpunkt seiner Anmeldung geprüft.

Wenn der Code vor längerer Zeit als dem eingestellten Intervall angemeldet wurde, muss der Benutzer den Code ändern.

Codekarte

RFID-Karte, wird vor Erweiterungseinheit RFID gehalten. Trägermedium von Benutzerdaten zur Identifikation am Schloss.

Codeverknüpfung

4-Augen-Prinzip (Öffnung / Konfiguration / Schließen / Freigabe / ...)

Wenn das entsprechende Kontrollkästchen markiert ist, ist

- die Öffnung von Schlössern,
- die Systemkonfiguration,
- das Schließen von Schlössern beziehungsweise
- die Code-Eingabe während der Freigabezeit

nur möglich, nachdem sich zwei Benutzer am gleichen Schloss authentifiziert haben.

„4-Augen-Prinzip (Öffnung)“ ist nicht zusammen mit **Parallelcode** möglich. Einzelne Benutzer können über die Benutzermatrix dazu berechtigt werden, trotz „4-Augen-Prinzip (Öffnung)“ Schlösser auch alleine zu öffnen.

Werkseinstellung: nicht aktiviert.

Codeverteilung

Nur mit TwinNet 10.3 und höher, mit Netzwerkanschluss, 2 Lizenzen und mit „Pairing“, ab Firmware Version 25/26. „Codeverteilung“ ist ein Verfahren, das sicherstellt, dass für alle Benutzer eine Synchronisation ihrer Codes an allen für dieses Verfahren gewählten Schlössern stattfindet. Siehe „Codeverteilung einrichten“ auf S. 68 sowie das Handbuch TwinIP.

Echtzeituhr

Datum und Uhrzeit werden von einer speziell gepufferten Echtzeituhr generiert und bleiben im Notfall auch trotz mehrtägiger Stromlosigkeit des Systems aktuell.

Wird die Bedieneinheit für längere Zeit von der Stromversorgung getrennt, müssen Systemzeit und Datum neu eingegeben werden. Die automatische Sommer- / Winterzeitumstellung ist werksseitig voreingestellt. Sie kann via CashProtectPro ausgeschaltet werden.

Einmalcode

PIN-Code für Benutzer, der nach einmaliger Verwendung ungültig wird. In der Benutzermatrix zuordenbar. Unabhängig von Option **WTU**.

Fester Code

Nicht verwendet. Optionale Einstellung, dass Benutzer ihren PIN-Code nicht selbstständig ändern können. In der Benutzermatrix optional zuordenbar.

Freigabezeit

Die Freigabezeit können Sie mit der optionalen PC-Software für jedes Schloss auf eine Dauer von 1-99 Minuten festlegen.

Für jedes Schloss können Sie mit CashProtectPro eine **Öffnungsverzögerung** programmieren, während der das Schloss nach der Code-Eingabe eines Benutzers noch geschlossen bleibt.

Bei aktivierter Option „Freigabezeit“ muss der Benutzer nach Ablauf der Öffnungsverzögerung seinen Code während der sogenannten Freigabezeit erneut übermitteln, damit sich das Schloss öffnet.

Wenn Sie die Option „Freigabezeit“ nicht aktiviert haben, öffnet sich das Schloss sofort nach Ablauf der Öffnungsverzögerung.

Initialcode

Nur mit TwinNet 10.3 und höher, mit Netzwerkanschluss und mit zusätzlicher Codeverteilung/Initialcode-Lizenz, ab Firmware Version 25/26. Funktion für neue Benutzer, die mittels Initialcode eigenen Öffnungscode am Schloss anlegen können. Dafür ist keine weitere Person erforderlich. Via TwinNet (geplant: oder TwinIP) kann Initialcode programmiert werden. Option „Initialcode“ via TwinIP funktioniert nur, wenn der Server-Modus für ein Schloss deaktiviert ist.

Managercode

Vorsicht

Mit werksseitigem Systemmanagercode ist die Konfiguration Ihres Systems nicht gesichert.

Ändern Sie werksseitige Codes so bald wie möglich. Verwenden Sie keine persönlichen Daten beim Ändern von Codes. Testen Sie neue Codes mehrmals bei geöffneten Wertbehältnissen.

Für jedes Schloss gibt es genau einen dem Benutzer Nr.225 (Manager) zugeordneten Managercode, der im Schloss gespeichert ist und nicht abgemeldet werden kann. Der Managercode des Schlosses 1, des Systemschlosses, berechtigt dazu, Systemeinstellungen zu machen und wird daher auch als **Systemmanagercode** und kurz als Systemcode bezeichnet. Werksseitig ist der Managercode von jedem Schloss als Code „111111“ (bei Systemen der VdS Klasse 2) oder „11111111“ (bei Systemen der VdS Klasse 3) programmiert.

Mastercode

Vorsicht

Mit werksseitigen Mastercodes ist Ihr System nicht gesichert.

Ändern Sie werksseitige Codes so bald wie möglich. Verwenden Sie keine persönlichen Daten beim Ändern von Codes. Testen Sie neue Codes mehrmals bei geöffneten Wertbehältnissen.

Für jedes Schloss gibt es genau einen dem Benutzer Nr.00 (Schlossmaster) zugeordneten Mastercode, der im Schloss gespeichert sein kann. Der Mastercode berechtigt dazu, Schlossbenutzer zu verwalten. Werksseitig ist der Mastercode für Schlösser der VdS Klasse 2 als Ziffernfolge „123456“ und für Schlösser der Klasse 3 als „12345678“ programmiert. In der Benutzermatrix der optionalen PC-Software CashProtectPro kann der **Systemmanager** festlegen, ob der Mastercode auch zur Öffnung des Schlosses berechtigt.

Menütasten

Vier Tasten, **CLEAR**, **<**, **>** und **ENTER**, die sich direkt unter dem Display der Bedieneinheit befinden und die zur Navigation in den angezeigten Menüs dienen.

Netzausfall

Um Schlösser auch bei Netzausfall öffnen und schließen zu können, wenn das System über ein Netzteil (Netzteilbetrieb über TwinConnect / TwinConnect small) versorgt wird, schließen Sie eine 9 Volt Blockbatterie Typ Alkaline an der Bedieneinheit an. Stecken Sie das Adapterkabel in die Buchse an der Unterseite der Bedieneinheit. Siehe Abschnitt „System während Netzausfall mit Spannung versorgen“.

Öffnungsverzögerung

Für jedes Schloss können Sie mit der optionalen PC-Software eine Öffnungsverzögerung von 1-99 Minuten programmieren. Für diesen Zeitraum bleibt das Schloss auch nach der Code-Eingabe des Benutzers geschlossen. Siehe auch Option „**Freigabezeit**“.

Wenn Sie die Option „Freigabezeit“ nicht aktiviert haben, öffnet sich das Schloss sofort nach Ablauf der Öffnungsverzögerung.

Öffnungszeit

Siehe **Sperrzeit / Öffnungszeit (Zeitprogramm)**.

Pairing

Ab Firmware Version 25/26. „Pairing“ ist ein Verfahren, das sicherstellt, dass die Kommunikation zwischen (TwinIP,) QPad und den Schlössern verschlüsselt erfolgt und dass diese Geräte nicht unautorisiert ausgewechselt werden können. Siehe „Pairing einrichten“ auf S. 66 sowie gegebenenfalls das Handbuch TwinIP.

Parallelcode

Nur möglich bei Systemen mit zwei Schlössern. Der erste Benutzer kann Schloss 1 oder Schloss 2 öffnen und der zweite das noch geschlossene Schloss.

Kombinierbar mit „**Zwangsfolge**“. Wenn 2 Schlösser im System sind, kann ein Benutzer während einer „**Teilsperrezeit**“ ein Wertbehältnis auch alleine öffnen.

Bei Aktivierung dieser Funktion mit dem optionalen Parametrierset CashProtectPro wird die Funktion „**Codeverknüpfung**“ automatisch deaktiviert.

Personalnummern

Benutzern können Personalnummern zugeordnet werden und über ein Kontrollkästchen in der Benutzermatrix von CashProtectPro kann definiert werden, ob sich alle Benutzer mit ihren Personalnummern statt mit ihren Benutzernummern identifizieren.

PIN-Code

Persönliche Identifikationsnummer (PIN) oder Geheimzahl, die Benutzer an Bedieneinheit QPad eingeben. Eine nur einem oder einem Benutzer und dem Schlossmaster bekannte Ziffernfolge, mit der Benutzer sich gegenüber System TwinLock authentisieren können.

Protokoll (Ereignisprotokoll)

Alle wichtigen Ereignisse werden mit Datum und Uhrzeit chronologisch protokolliert und können gegebenenfalls online übertragen werden. Beteiligte Geräte und Benutzer werden aufgeführt. Die jüngsten 10.000 Ereignisse werden im Protokoll gespeichert. Ereignisse sind Programmiervorgänge, Systemfehler, kritische Statusmeldungen sowie Manipulations- und Sabotageversuche. Der gesamte Ereignisspeicher kann auch via USB exportiert und mit der PC-Software CashProtectPro angezeigt und gedruckt werden.

Schlossmaster

Inhaber des Mastercodes eines Schlosses, der die Codes (PIN-Codes) und gegebenenfalls die Identifikationsdaten (Codekarten) der Benutzer dieses Schlosses verwaltet. Ob der Schlossmaster das Schloss selbst öffnen kann, ist abhängig davon, was der Systemmaster in der Benutzermatrix einstellt. Siehe auch **Benutzergruppen**.

Schnellöffnung

Kontrollkästchen in der Benutzermatrix der optionalen Software CashProtectPro. Wenn es markiert ist, kann ein Benutzer ein Schloss trotz programmierter Zeitprogramme öffnen, ohne warten zu müssen.

Dazu müssen für ihn auch alle anderen für die Autorisierung zur Schlossöffnung nötigen Kästchen markiert und sein PIN-Code muss am Schloss angemeldet worden sein.

Server-Modus

Nur mit TwinNet 10.3 und höher und mit Netzwerkanschluss, ab Firmware Version 25/26. „Server-Modus“ wird automatisch eingestellt, wenn eine Netzwerk-Lizenz aktiviert wird. Bei eingestelltem Server-Modus können Schlösser ausschließlich über TwinNet und nicht via TwinIP konfiguriert werden

Service

- 1) Menü im Display der Bedieneinheit für Servicefunktionen
- 2) Kontrollkästchen in der Benutzermatrix der PC-Software. Wenn der Systemmanager das Kontrollkästchen „Service“ für einen Benutzer aktiviert, kann dieser das Ereignisprotokoll mittels Chipkarte aus dem System exportieren und es mit der Software anzeigen und drucken.

Sondertage

Vorsicht

Gefahr von nicht erwünschten Sondertagen.

Schlossöffnung unbeabsichtigt nicht möglich.

Achten Sie darauf, Feiertage wie Ostern, die jedes Jahr auf ein anderes Datum fallen, nicht als „jährlich wiederkehrend“ zu markieren.

Sondertage sind Tage, an denen das System ganztägig nicht geöffnet werden kann. Jeder Öffnungsversuch, der an einem Sondertag erfolgt, wird abgebrochen. Sondertage können auch zu Tagen definiert werden, an denen trotz anderer Zeitprogramme ausnahmsweise ganztägig geöffnet werden darf.

Bis zu 30 Sondertage im Jahr können Sie über optionale Software definieren. Sondertage können als „alljährlich wiederkehrend“ definiert werden. Funktion „Sondertage“ setzt andere Zeitprogramme außer Kraft.

Stellen Sie vor der Aktivierung des Zeitprogramms „Sondertage“ sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind.

Einstellung ab Werk: keine Sondertage

Sperrzeit nach Terminalwechsel bei Schloss in geschlossenem Zustand

Zeitraum von 90 Minuten, in dem ein Schloss gesperrt ist, nachdem ein Terminalwechsel durchgeführt wurde, bei dem mindestens ein Schloss geschlossen war.

Sperrzeit nach Eingabe von falschem Code

Zeitraum von einer bis zu einigen Minuten, während dem ein Schloss trotz Code-Eingabe nicht öffnet, weil ein Benutzer zuvor (wiederholt) Code falsch eingegeben hat. Je öfter falscher Code eingegeben worden ist, desto länger wird die Dauer der Sperrzeit. Siehe auch **Sperrzeit / Öffnungszeit (Zeitprogramm)**.

Sperrzeit / Öffnungszeit (Zeitprogramm)

Eine Sperrzeit ist ein Zeitraum von einem Tag bis zu zwei Monaten, während dem das System ganztägig nicht geöffnet werden kann. Für das System können Sie über PC-Software (optionales Zubehör) bis zu 3 Sperrzeiten definieren. Mit programmierter Sperrzeit wird jeder Öffnungsvorgang abgebrochen, der im definierten Zeitraum erfolgt. Sperrzeiten können auch zu einzuhaltenden Öffnungszeiten definiert werden, außerhalb denen nicht geöffnet werden kann. Werkseinstellung ist „Sperr- / Öffnungszeiten deaktiviert“. Stellen Sie vor der Aktivierung sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind. Siehe auch **Sperrzeit nach Eingabe von falschem Code / ...bei Terminalwechsel....**In allen 3 Fällen ist die Fehlermeldung „Sperrzeit“.

Stiller Alarm

Nur bei Eingabe von PIN-Code. In einer Bedrohungssituation kann durch Eingabe eines speziellen „**Alarmcodes**“ beim Öffnen und Programmieren des Systems ein stiller Alarm ausgelöst werden. Das System verhält sich für Benutzer und Bedroher genau so wie beim normalen Öffnen, nur dass zugleich ein stilles Alarmsignal an die Einbruchmeldeanlage geleitet wird.

Systemmanagercode (=Managercode von Schloss 1)**Vorsicht**

Mit werksseitigem Systemmanagercode ist Ihr System nicht gesichert.

Ändern Sie werksseitige Codes so bald wie möglich. Verwenden Sie in Codes keine persönlichen Daten.

Testen Sie neu programmierte Codes mehrmals bei geöffneten Wertbehältnissen.

Der Systemmanagercode, auch Systemcode genannt, berechtigt dazu, das System über die Bedieneinheit zu konfigurieren. Er wird in Schloss Nr.1 Ihres Systems gespeichert und ist Benutzer Nr.225 zugeordnet.

Werksseitig ist als Code „111111“ (bei Systemen der VdS Klasse 2) oder „11111111“ (bei Systemen der VdS Klasse 3) programmiert.

Systemmanager

Inhaber des Systemmanagercodes, mit dem das System konfiguriert wird. Der Systemmanager selbst kann Schlösser nicht öffnen und schließen.

Teilsperrezeit (3 Zeiträume pro Tag)

Stellen Sie vor der Aktivierung einer Teilsperrezeit sicher, dass Uhrzeit, Wochentag und Datum korrekt eingestellt sind. Für Systeme mit zwei Schlössern können Sie über Software (optionales Zubehör) eine Teilsperrezeit mit drei Zeiträumen pro Tag definieren. Während der Teilsperrezeiten schließt nur Schloss 2, Schloss 1 bleibt offen. Mit aktivierter Teilsperrezeit wird jeder Schließvorgang von Schloss 1 abgebrochen, der in einem definierten Teilsperrezeitraum liegt. Werkseinstellung ist „Teilsperrezeit deaktiviert“.

Soll trotz aktivierter Teilsperrezeit Schloss 01 geschlossen werden:

Drücken Sie die **ENTER** Taste, während **Schliessen | Schloss 1 Teilversperre!** angezeigt wird. Schloss 1 wird geschlossen, die Teilsperre einmalig außer Kraft gesetzt.

Funktion „Teilsperrezeit“ können Sie kombinieren mit Funktion „Automatisches Schließen mit Türschalter“. Die Folge ist, dass Schloss 1 innerhalb der Teilsperrezeit offen bleibt und nach ihrem Ende geschlossen wird.

Wochenprogramm

Über optionale Software können Sie bis zu 3 / 5 Wochenprogramme mit flexibel definierbaren Öffnungszeiträumen für jeden Wochentag einstellen. Über die Benutzermatrix können Sie die Programme individuell Benutzern zuordnen. Mit programmiertem Wochenprogramm wird jeder Öffnungsvorgang abgebrochen, der nicht in einem definierten Öffnungszeitraum liegt. Stellen Sie vor der Aktivierung eines Wochenprogramms sicher, dass Uhrzeit und Datum korrekt eingestellt sind.

Ab Werk sind die Wochenprogramme deaktiviert.

WTU-Funktion / Modus

Modus des Systems. Der Modus kann via Menü „Settings/Manager/WTU Funktion“ festgelegt werden. Von dieser Einstellung hängt es ab, ob die Benutzer flexiblen Einmalcode benutzen müssen, dürfen oder dies nicht tun können.

Modus („WTU-Funktion“ des Systems):

0 = Bank: Benutzer öffnen mit PIN-Codes und ggf. abhängigen Einmalcodes.

1 = Mix: Gemischter Modus; Schlosssysteme haben Modus 0 oder 2

2 = WTU: Benutzer öffnen Schlösser mit flexiblen Einmalcodes.

Zeitprogramm

Das Öffnen der Schlösser kann auf diverse Zeiträume beschränkt werden. Siehe auch die Einträge **Sondertage**, **Sperrzeit**, **Teilsperrezeit** und **Wochenprogramm**. Zeitprogramme / Sperrzeiten können von privilegierten Benutzern unterbrochen werden. Siehe auch „**Zeitprogrammunterbrechung**“ und „**Schnellöffnung**“.

Zeitprogrammunterbrechung

Eine innerhalb des gesicherten Bereichs eingeschlossene Person kann einen im Inneren des Wertbehältnisses angebrachten Druckschalter betätigen, wodurch ein Schloss trotz aktiver **Zeitprogramme** (Wochenprogramm, Sondertage, Sperrzeit oder Teilsperrezeit) von außen durch Benutzerautorisierung (üblicherweise Codeeingabe) geöffnet werden kann. Nach einer Öffnung werden die Zeitprogramme automatisch wieder aktiviert. Der Anschluss eines solchen Druckschalters ist nur an der optionalen Schalteinrichtung TwinAlarm möglich, nicht an der Erweiterungseinheit TwinXT (small). Auch ohne TwinAlarm kann ein Benutzer, der vom Systemmanager zur Schnellöffnung autorisiert wurde (Benutzermatrix). Siehe auch „**Schnellöffnung**“.

Zwangsfolge (ZF)

Möglichkeit, eine Reihenfolge festzulegen, die beim Öffnen und Schließen der Schlösser des Systems eingehalten werden muss.

Wenn Sie die Option „Zwangsfolge“ mit PC-Software programmieren, müssen Benutzer zuerst Schloss 1 und dann gegebenenfalls Schloss 2 öffnen. Nach der Öffnung von Schloss 1 ist das System normalerweise teilgesichert (entspricht bei Option ZF dem Zustand „gesichert“), nach der Öffnung aller Schlösser ist das System mit aktivierter Option Zwangsfolge entsperret und damit ungesichert.

Beim Schließen muss zuerst gegebenenfalls Schloss 2 und dann Schloss 1 geschlossen werden. Erst danach ist das System gesichert.

Werkseinstellung: keine Zwangsfolge.

11 Anhang

11.1 Abbildungsverzeichnis

Abb. 1:	Systemaufbau von System 1.1 mit TwinIP small	16
Abb. 2:	Systemaufbau von System 2.1 mit TwinIP WiFi	17
Abb. 3:	Systemaufbau von System mit TwinAlarm (Beispiel).....	18
Abb. 4:	Bedieneinheit QPad	19
Abb. 5:	Bedieneinheit mit Optionsbox RFID	19
Abb. 6:	Schloss INSYS Lock 700	19
Abb. 7:	Schloss INSYS Lock 800	19
Abb. 8:	Busverteiler TwinConnect small	20
Abb. 9:	Sperreinrichtung TwinXT	20
Abb. 10:	Schalteneinrichtung TwinAlarm	20
Abb. 11:	Netzwerkserweiterungseinheit TwinIP small	21
Abb. 12:	Netzwerkserweiterungseinheit TwinIP WiFi	21
Abb. 13:	Design-Beispiele RFID Karte, Anhänger und RFID-Armband	21
Abb. 14:	Übersicht am Beispiel eines Systems mit TwinAlarm	22
Abb. 15:	Beispiel Startseite PC-Software CashProtectPro.....	25
Abb. 16:	Bedienelemente der Bedieneinheit QPad.....	33
Abb. 17:	Definition von Hotkeys (Beispiele)	34
Abb. 18:	RFID-Karten und Kartenleser	47
Abb. 19:	Adapterkabel mit Eingabeeinheit verbinden	96

!!! Irrtum und technische Änderung vorbehalten!!!

11.2 Notizen

[illegible]