

INHALT

1.	Kurzbeschreibung	2
2.	Hardware	3
3.	Konfiguration	4
3.1	Admin-Konsole	4
3.1.1	Übersicht	4
3.1.2	Benutzer	5
3.1.3	Beschädigungen	7
3.1.4	Einstellungen	8
3.1.4.1	Terminals	8
3.1.4.2	Allgemeine Einstellungen	10
3.1.4.3	Lizenz	12
3.1.4.4	Update	14
4.	Übersicht Schießbahnbelegung	15
5.	Terminal	16
5.1	Stand in Betrieb nehmen	17
5.2	Anmeldung und Abmeldung	19
5.2.1	Anmeldung als Schütze	20
5.2.2	Abmeldung als Schütze	21
5.2.3	Schießbetrieb beenden	22
5.2.4	Wechsel der Aufsicht	22
5.2.5	Sonderfall Aufsicht als Schütze	23
6.	Zugangskontrolle	24
6.1	Parameter	24
6.2	Beispiel	24
7.	Software-Versionen	25

1. Kurzbeschreibung

Jeder Benutzer, Aufsicht oder Schütze, kann sich mit seinem RFID-Chip (maximal 3 Stück je Nutzer) und seiner PIN-Nummer an einem Terminal anmelden, wenn der entsprechende Schießstand durch eine Aufsicht in Betrieb genommen wurde. Der Schütze gibt nur noch das gewünschte Kaliber und die ausgewählte Schießbahn über je einen Tastendruck ein, und das Schießen kann beginnen. Die Schießbahn ist nun für die Dauer des Schießens durch diesen Schützen belegt. Zum Beenden des Schießens wird der RFID-Chip erneut an den entsprechenden Leser gehalten. Falls gewünscht, kann nun die Anzahl der abgegebenen Schüsse oder das Resultat des Schießens (erzielte Ringe) eingetragen werden (abhängig davon, was in der Parametrierung gewählt wurde). Falls das Abmelden vergessen wurde, so kann die betroffene Schießbahn auch durch einen anderen Schützen übernommen werden und der Vorgänger wird abgemeldet. Die Abmeldung der Schützen erfolgt aber auch, wenn das Schießen über die Aufsicht oder das System (Ablauf der Zeit) beendet wird.

Alle Ereignisse werden automatisch protokolliert, handschriftlichen Einträge sind nicht mehr nötig. Am Terminal können jederzeit festgestellte Beschädigungen erfasst werden. Mit der Exportfunktion lassen sich die gesammelten Daten des Journals und die der Beschädigungen auf einen bereitgestellten Datenträger als CSV-Datei herunterladen. Mit einem entsprechenden Programm (z.B. Excel) kann man diese Daten auswerten und dann weiter bearbeiten. Für die Auswertung steht ein kostenloses Excel-Tool zur Verfügung.

Im System fungiert entweder ein beliebiges Terminal als Master, oder wenn gewünscht, kann diese Funktion auch von einem extra Gerät übernommen werden. Auf dem Master befindet sich die zentrale Datenbank. Alle Terminals müssen mit einem LAN-Kabel an einen Router angeschlossen sein. Das Konfigurieren und das Bearbeiten der Benutzer erfolgt mit einem beliebigem Eingabegerät (z.B. ein Tablet), auf dem ein beliebiger Browser läuft. Dazu kann über die IP-Adresse des Masters die Admin-Konsole aufgerufen werden. Von hier aus erfolgen die Parametrierung, die Kontrolle und das Herunterladen der Protokolle und Listen. Am Master lassen sich beliebig viele Schießstände und Terminals anmelden. Das System benötigt für den normalen Betrieb kein Internet.

Wurde ein Schießstand von einer Aufsicht freigegeben, dann können sich die Schützen anmelden. Dies ist solange möglich, bis alle Schießbahnen belegt sind. Außerdem lassen sich durch die Freigabe des Standes bis zu 4 Relais ansteuern. Mit einem Kontakt kann dann z.B. das Hauptlicht, ein Türöffner oder die Lüftung eingeschaltet werden. Auf Wunsch kann das System auf bis zu 8 Kontakte erweitert werden, diese sind in der Software bereits integriert.

2. Hardware

Terminal

Voraussetzung für die Installation der „Digitalen Schießkladde“ ist ein Terminal. Diese Anleitung bezieht sich auf die von uns vertriebenen Terminals und Bausätze. Für „Eigenbauten“ übernehmen wir keinerlei Funktionsgarantie. Die Benutzerführung erfolgt über das 10-Zoll große Touch-Display. Für die An- und Abmeldeprozesse ist ein RFID-Reader integriert. Sollte das Hauptterminal (Master) nicht mit dem Internet verbunden sein, so werden Zeit und Datum von der integrierten Hardware-Uhr bereitgestellt.

Das Betriebssystem und die Programm-Software werden auf eine SD-Karte geschrieben. Diese SD-Karte steckt im SD-Karten-Slot des Mini-PCs.

Auf einem USB-Stick liegt die Datenbank (nur Master) und eventuell benötigte Konfigurations-Dateien. Mit Hilfe von „leeren“ Dateien wird jedes Terminal für die gewünschte Betriebsart konfiguriert (siehe Tabelle) Da der USB-Stick FAT32 formatiert ist, können die Dateien auch mit dem Dateimanager von Windows angelegt werden. Wegen der schnelleren Datenübertragung sollte der USB-Stick immer im USB 3.0-Port (blau) des Mini-PCs stecken.

Tabelle 1

Datei (Flag)	vorhanden	Nicht vorhanden
server_mode	Server (Master)	Client (Slave)
pcsc_mode	externer USB-NFC-Leser	Interner NFC-Leser

RFID-Transponder

Die RFID-Transponder müssen folgendes Format besitzen: **13,56 MHz Classic 1K**

Wichtig:

Bei anderen Mifare-Standards wie z.B.: Ultralight, DESFire, usw. kann es zu Problemen beim Lesen kommen, wenn der Standardleser verbaut ist. Sind kundenseitig bereits Transponder vorhanden, so kann aber jederzeit ein entsprechendes Lesegerät integriert werden.

Externes USB-RFID-Lesegerät

Für die Zuweisung der RFID-Chips ist am besten ein USB-RFID-Reader (13,56 MHz) geeignet, der Keyboard-Emulation unterstützt (mehr unter 3.1.2). Dieser Leser sind im Zubehörhandel erhältlich.

3. Konfiguration

Die Terminals werden über die Admin-Konsole eingerichtet. Dazu muss sich das Gerät des Browsers im selben Netzwerk wie das zu konfigurierende Master-Terminal befinden. Im Kapitel 3.1.4 dazu mehr.

Wichtig:

Für die Synchronisation der Zeit zwischen den einzelnen Terminals muss die IP im Bereich **192.168.000.000 bis 192.168.255.255** (Private Netzwerke) liegen!

Der Server kann dann, mit der vom Router vergebenen IP, mit Hilfe eines Browsers erreicht werden (z.B.: **192.168.178.64:1337** Wichtig: Port **1337** mit angeben!)

Die Terminalnummer und die IP werden nach dem Hochlauf am Display angezeigt. Die Nummer des Terminals wird vom Betriebssystem vergeben und kann nicht verändert werden!

3.1 Admin-Konsole

Passwortschutz

Die Admin-Konsole kann Passwort geschützt werden. Solange in den Einstellungen kein Passwort hinterlegt ist, sind alle Reiter (Seiten) frei zugänglich, ansonsten erscheint das Anmeldefenster zur Eingabe des Passworts.

Wenn ein Passwortschutz hinterlegt ist, so springt das Programm nach 5 Minuten (feste Dauer) wieder zum Anmeldefenster zurück, wenn in dieser Zeit keine Taste gedrückt wurde.

Wichtig:

Um die Daten und Einstellungen gegen Missbrauch zu schützen, empfehlen wir, den Passwortschutz zu aktivieren! Der Passwortschutz wird erst nach dem Neuaufbau einer Seite (Funktionstaste F5) aktiviert, bzw. deaktiviert!

Die Admin-Konsole hat folgende Reiter, die auf den nächsten Seiten beschrieben werden:


Übersicht, Benutzer, Beschädigungen und Einstellungen

Anmerkung:

Beim ersten Aufruf sind alle Listen leer, es gibt keine Benutzer und es sind keine Einstellungen hinterlegt. (Ausnahme Journal: Ladeversuche des Master-Terminal stehen bereits in der Liste).

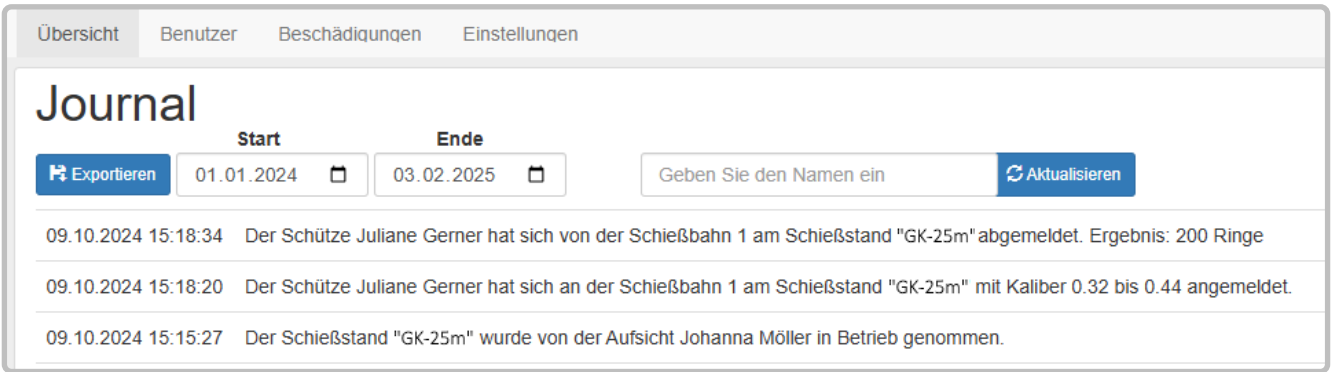
Als erstes müssen die Terminals angelegt werden, da sich die Einstellungen auf alle Terminals oder nur auf ein Bestimmtes beziehen können (siehe Kapitel 3.1.4).

3.1.1 Übersicht

Hier werden die letzten 300, registrierten Ereignisse chronologisch sortiert angezeigt. Die beiden Felder direkt rechts neben der Export-Taste dienen zur Eingabe des Export-Zeitraums. Dort kann das Datum entweder direkt, oder durch das Anklicken der Date-Picker  (Kalenderfunktion) eingegeben werden (siehe Bild 3.1). Die Aktualisierung der Liste erfolgt automatisch. Mit der Taste „Export“ wird das Journal mit dem vorgegebenen Zeitraum als CSV-Datei exportiert. Im Browser erfolgt dies über einen Download. Wurde die Admin-Konsole über ein Terminal aufgerufen, so wird die Datei auf einen (zweiten) USB-Stick geschrieben.

Links neben dem Knopf „Aktualisieren“ befindet sich das Eingabefeld, um bestimmte Benutzer zu Filtern. Hier können Vorname, Nachname oder die Kombination aus beiden (durch ein Leerzeichen getrennt!) eingegeben werden. Es muss nicht auf Groß- und Kleinschreibung geachtet werden. Mit der Taste „Aktualisieren“ wird der Anzeige des Filters auf den aktuellen Stand gebracht.

Bild 3.1



Mit Hilfe eines entsprechenden Programms (z.B.: Excel) können die Daten dann ausgewertet und weiter bearbeitet werden.

Anmerkung:

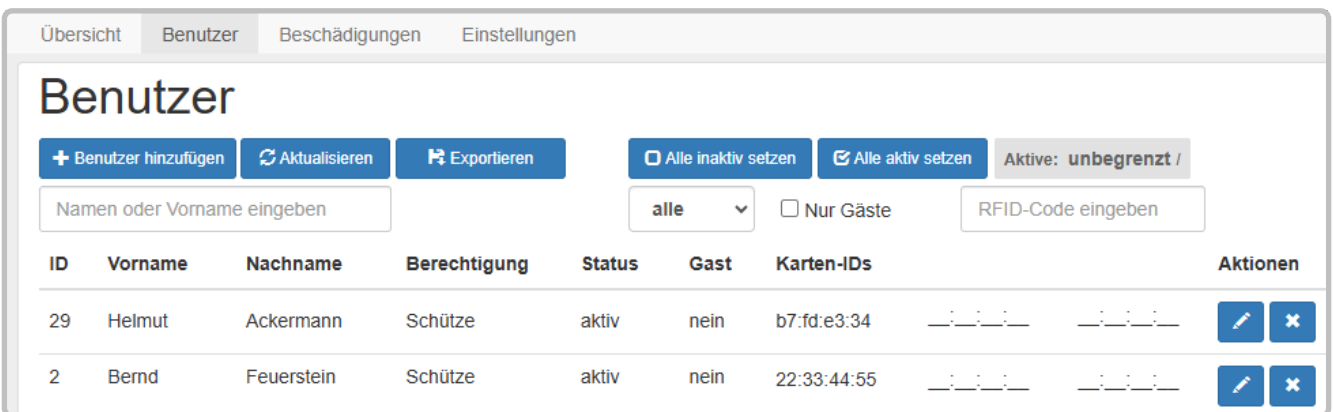
Auf unserer Homepage www.hecht-software.de/downloads steht ein kostenloses Excel-Auswerte-Tool zum Download bereit.

3.1.2 Benutzer

Mit der Taste „Benutzer hinzufügen“ werden neue Nutzer angelegt. Auch hier gibt es die Taste, um die Liste auf den aktuellen Stand zu bringen und eine Taste, um die Benutzerliste zu exportieren. Weiter lassen sich hier alle Schützen auf „inaktiv“, bzw. auf „aktiv“ setzen. Daneben wird angezeigt, wie viele freie Lizenzen noch verfügbar sind. Darunter befindet sich die Zeile mit den Filterfunktionen.

Wieder etwas weiter unten befindet sich die Liste mit den Nutzereinträgen (z.B.: Gastschütze) und den zugehörigen Daten. In jeder dieser Zeilen gibt es zwei Tasten mit denen der jeweilige Eintrag bearbeitet oder gelöscht werden kann.

Bild 3.2



Das Setzen auf „aktiv“ oder „inaktiv“ erfordert zusätzlich eine Bestätigung (siehe Bild 3.3), da diese Aktionen Auswirkung auf alle Einträge haben, aber nur einzeln rückgängig gemacht werden können. Auch das Löschen muss sicherheitshalber bestätigt werden (siehe Bild 3.4).

Bild 3.3

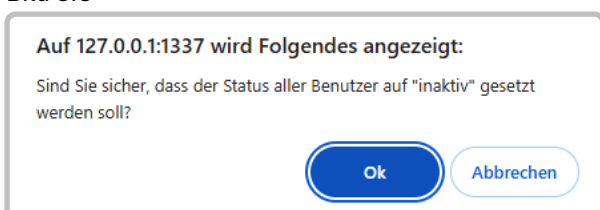
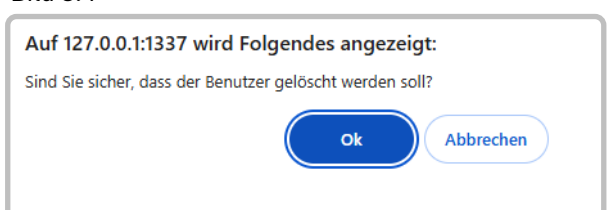


Bild 3.4



Anmerkung:

Hat ein Schütze den Status „inaktiv“, so kann sich dieser nicht mehr an einem Terminal anmelden. So lässt sich z.B. der Verkauf von Monats- oder Jahreskarten steuern.

Es gibt vier Filter:

Bild 3.5



Hier kann die Liste nach folgenden gefiltert werden:

- Um einen bestimmten Benutzer zu finden, wird der entsprechende Name in das erste Feld eingegeben. Dabei ist es egal, ob ein Vor- oder Nachname eingetippt wird. Es muss dabei auch nicht auf Groß- und Kleinschreibung geachtet werden - mit jedem eingegeben Buchstaben, werden alle nicht zutreffenden Einträge, aus der Ansicht herausgefiltert.
- Mit dem Dropdown (Klappmenü über der Spalte Status) können auf aktiv oder inaktiv gesetzte Benutzer angezeigt werden.
- Um Gäste anzuzeigen, wird der Haken in der Checkbox „Nur Gäste“ gesetzt.
- Mit jedem erlaubten Zeichen (gültiger Hexadezimalwert) werden nicht passende RFID-Codes aus der Liste herausgefiltert. Trennzeichen müssen an dieser Stelle nicht eingegeben werden.

Anmerkung:

Diese Filter sind nur Anzeigefilter und haben daher keinerlei Einfluss auf die Datenbank oder auf die Daten der Exportfunktion.

Benutzer hinzufügen

Durch Drücken der Taste „Benutzer hinzufügen“ öffnet das Bearbeitungsfenster (siehe Bild 3.6) mit den entsprechenden Eingabefeldern. Diese können nun der Reihe nach befüllt werden. Die vom System automatisch generierte PIN-Nummer kann auf Wunsch geändert werden. Der Knopf mit dem Auge macht die PIN sichtbar.

Der RFID-Code kann auf drei Arten eingegeben werden:

- Der RFID-Code wird ohne Trennzeichen über die Tastatur eingegeben. Die Doppelpunkte werden nach der Übernahme automatisch eingefügt.
- Alternativ kann ein RFID-Reader mit Keyboard-Emulation an das Eingabegerät angeschlossen werden. D.h. bedeutet, dass der RFID-Code wird über den Tastaturpuffer eingelesen. Der RFID-Reader muss so konfiguriert werden, dass die Codes im HEX-Format und rückwärts eingelesen werden (**8h-r**).

Anmerkung:

Diese Leser sind sinnvoll, wenn man viele Karten eingegeben will. Außerdem werden damit Eingabefehler vermieden.

Ist der RFID-Code eingetragen, dann kann er mit dem Knopf „NEUE KARTE“ übernommen werden.

Der neue RFID-Code wird formatiert in einem Bearbeitungsfeld angezeigt (siehe Bild 3.6). So lassen sich bis zu 3 RFID-Chips je Nutzer hinterlegen. Mit dem Knopf „x“ können ungültige Codes gelöscht werden.

- Eine weitere Möglichkeit besteht darin, den RFID-Chip mit dem Scanner eines Terminals zu lesen. Im Bearbeitungsfenster werden die letzten zehn Anmeldeversuche (mit Datum und Uhrzeit) angezeigt. Falls die Anzeige nicht aktuell ist, kann diese mit dem „Refresh“-Knopf aktualisiert werden. Der weiße Knopf mit dem „Haken“ übernimmt den links von ihm stehenden Code in das Feld „Karten-ID“ (siehe Bild 3.7).

Bild 3.6

Neuer Benutzer✕

Vorname

Nachname

Berechtigung

aktiv? Gast?

PIN

Karten-IDs (max. 3 RFID-Karten)

RFID-Code (Ohne Trennzeichen)

NEUE KARTE

Alternativ: Auswahl aus Liste letzter 10 Anmeldeversuche mit unbekanntem Zugangskarten

Anmeldeversuch	ID	
24.06.2024 10:43:53	04:56:5a:ca	<input checked="" type="checkbox"/>

Bild 3.7

Neuer Benutzer✕

Vorname

Nachname

Berechtigung

aktiv? Gast?

PIN

Karten-IDs (max. 3 RFID-Karten)

Eingabefeld

NEUE KARTE

Mit „Speichern“ werden die Daten in die Datenbank geschrieben und das Eingabefenster wird geschlossen. „Schließen“ blendet das Eingabefenster aus und verwirft die Daten, ohne diese zu speichern.

Ist ein zentraler PC (Raspberry Pi) vorhanden und die Adminkonsole wird über diesen aufgerufen, so kann der Code auch mit einem am USB-Port angeschlossenen NFC-Leser erfolgen. Dieser muss mit Hilfe des Datei-Flags „pcsc-mode“ aktiviert worden sein (siehe Pkt. 2 Hardware).

3.1.3 Beschädigungen

Hier werden die erfassten Beschädigungen chronologisch aufgelistet und können, falls nötig bearbeitet werden. Mit der Taste „Aktualisieren“ wird die Anzeige auf den neusten Stand gebracht und mit der Taste „Export“, wird die Liste mit den Beschädigungen als CSV-Datei exportiert. Im Browser erfolgt dies über einen Download, am Terminal wird die Datei auf einen USB-Stick geschrieben.

Bild 3.8

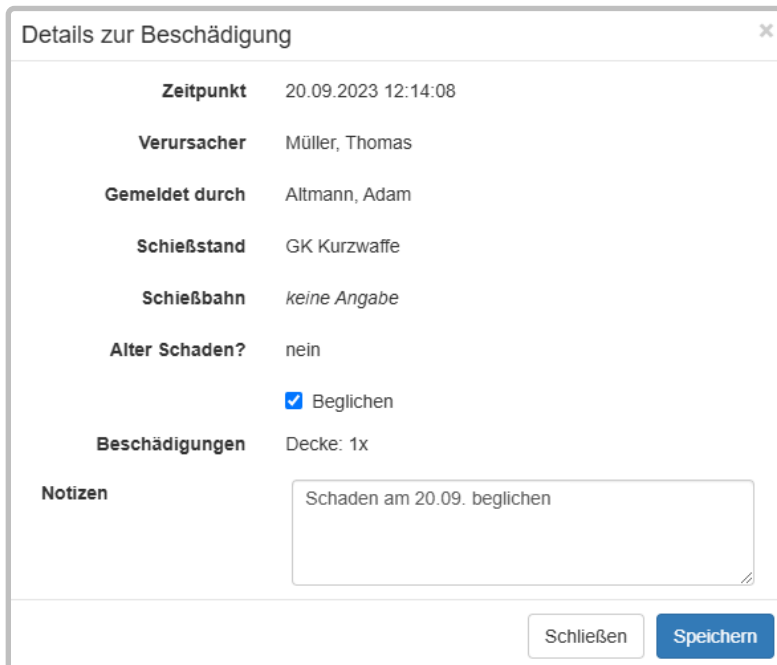
Übersicht
Benutzer
Beschädigungen
Einstellungen

Beschädigungen

ID	Zeitpunkt	Verursacher	gemeldet durch	Schießstand	beglichen?	
2	20.09.2023 12:14:08	Müller, Thomas	Altmann, Adam	GK Kurzwaffe	nein	<input type="button" value="✎"/>
4	12.02.2024 11:49:36	unbekannt	Altmann, Adam	GK Kurzwaffe	ja	<input type="button" value="✎"/>

Durch das Drücken auf die Taste mit dem Stift öffnet sich das Dialogfenster (siehe Bild 3.9) mit den Details zu den gelisteten Beschädigungen. Falls der Schaden beglichen wurde, so kann das mit der Checkbox bestätigt werden. Weiter gibt es noch ein Feld für eventuelle Notizen. Die Tasten „Schließen“ und „Speichern“ funktionieren in gewohnter Weise.

Bild 3.9



Zeitpunkt	20.09.2023 12:14:08
Verursacher	Müller, Thomas
Gemeldet durch	Altmann, Adam
Schießstand	GK Kurzwaffe
Schießbahn	keine Angabe
Alter Schaden?	nein
	<input checked="" type="checkbox"/> Beglichen
Beschädigungen	Decke: 1x
Notizen	Schaden am 20.09. beglichen

3.1.4 Einstellungen

In den Einstellungen gibt es folgende drei Bereiche:

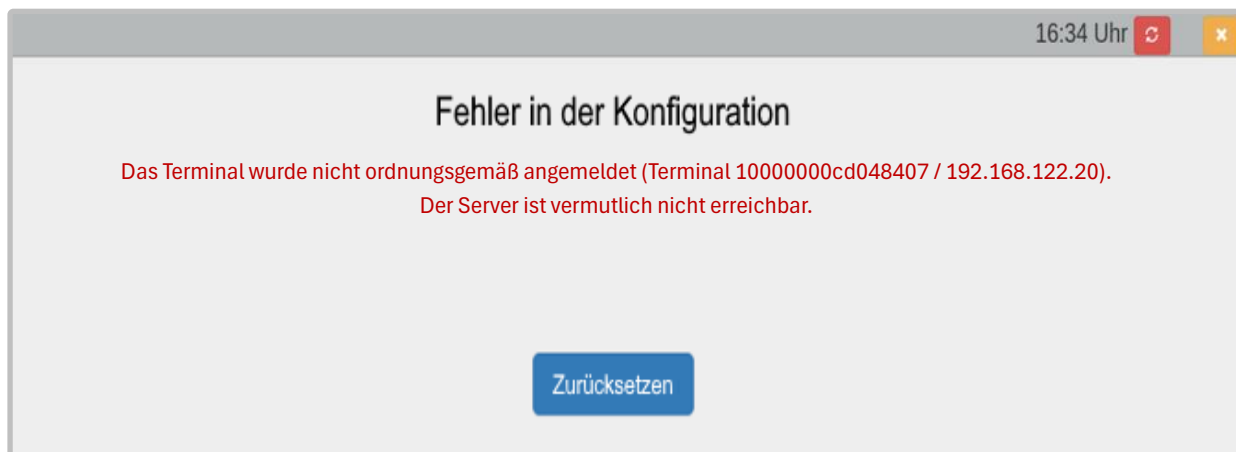
Terminals, Allgemeine Einstellungen und Update

Die verschiedenen Knöpfe funktionieren genauso, wie in den Kapiteln zuvor bereits beschrieben, deshalb werden ab dieser Stelle nur noch Tastknöpfe erklärt, die neue Funktionen haben.

3.1.4.1 Terminals


Um ein Terminal, bzw. einen Schießstand hinzuzufügen, muss die Gerätenummer und ein Name (Schießstand) eingetragen werden. Jedes Terminal zeigt nach dem Hochlaufen seine Gerätenummer an.

Bild 3.10



Mit dem Knopf „+ Schießstand Hinzufügen“ öffnet sich das Dialogfenster zur Eingabe (siehe Bild 3.11) und die Gerätenummer kann vom Display übernommen werden. Anschließend erfolgt die gewünschte Benennung des neuen Standes (z.B.: 25m-Stand, GK-Kurzwaffen, usw.).


Bild 3.11



Nun können alle Terminals und Schießstände eingetragen werden. Dies gilt auch für in der Zukunft liegende Erweiterungen. Der Name wird beim Journal und in der Beschädigungsliste verwendet. Wenn nötig, lässt sich der Name jederzeit ändern.

Bild 3.12



Schießstand	Geräte-Nr.	Aktionen
GK Langwaffe	100000002550539b	 
GK Kurzwaffe	10000000cd048407	 

Terminal mit mehreren Schießständen

Es ist möglich mehrere Schießstände mit einem Terminal zu betreiben. Die Namen der einzelnen Stände werden dann mit der gleichen Geräte-Nr. verknüpft (siehe Bild 3.13).

Bild 3.13



Schießstand	Geräte-Nr.	Aktionen
GK Langwaffe	100000002550539b	 
GK Kurzwaffe	100000002550539b	 

Wird diese Betriebsart gewählt, so muss vor dem Anmeldeprozess mit dem RFID-Chip zuerst der gewünschte Schießstand ausgewählt werden. Der Startbildschirm sieht dann ähnlich wie folgt aus:

Bild 3.13



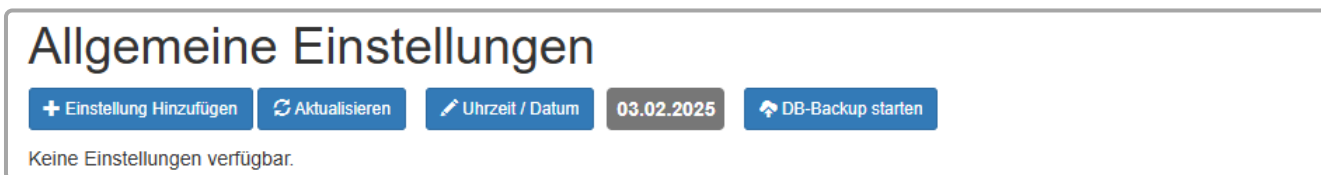
Achtung: In dieser Betriebsart kann je Schießstand nur **eines** der 4 Relais angesteuert werden!

3.1.4.2 Allgemeine Einstellungen

Hier gibt es neben den gewohnten Tasten noch die Möglichkeit Datum und Uhrzeit manuell zu stellen, wenn der Server keine Verbindung zum Internet hat. Hat der Master Verbindung mit dem Internet, dann werden händische Zeiteinträge überschrieben.

Weiter kann per Knopfdruck eine Sicherung der Datenbank ausgelöst werden, wenn ein entsprechendes Speichermedium eingerichtet wurde (siehe Backup-Einstellungen).

Bild 3.14



In der, auf der nächsten Seite stehenden Tabelle, sind die Standardeinstellungen aufgelistet.

Achtung:

Die Grundeinstellungen (blaue Schrift) sollten auf jeden Fall eingetragen werden, da sonst bestimmte Funktionen gesperrt sind, oder ggf. kein Schießbetrieb möglich ist. Bei den Einstellungsnamen und den dazugehörigen Werten ist die **exakte** Schreibweise einzuhalten, da diese vom System sonst nicht akzeptiert werden!

Beim Anlegen der Einstellungen kann angegeben werden, ob der Parameter für alle Terminals gilt, oder ob dieser nur für ein Bestimmtes Gültigkeit haben soll (siehe Bild 3.15).

Bild 3.15

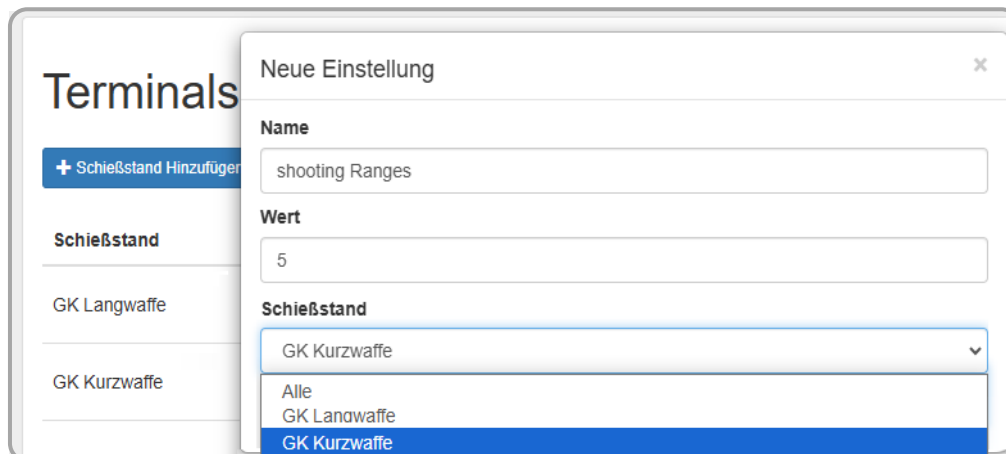


Tabelle 2 - Allgemeine Einstellungen

Name	Wert (Beispiele)	Default	Bemerkung
calibers	.38;.357 Magnum;.44		Trennzeichen beachten! Kein(e) Leerzeichen nach dem Semikolon!
damages	Decke;Boden;Wand;Belüftung	(siehe Bild 5.7)	Trennzeichen beachten! Kein(e) Leerzeichen nach dem Semikolon. Max. 9 Einträge!
duration	300	1	Schießdauer in Minuten (hier z.B. 5h)
enableShootingResult	true		Abfrage Schießergebnis (erzielte Ringe) anstatt Anzahl der Schüsse (nur wenn „true“)
exitAfterStationActivation	true		Nach Standaktivierung zum Login statt zum Aufsichtsmenü navigieren
password	\$hspw4321%		Passwort für Admin-Konsole
relay(Nr.)duration z.B.: relay3duration	0 z.B.: 1000		Schaltdauer des angegebenen Relais (ab Start Standinbetriebsetzung) in Millisekunden. (Nr.) = 1 .. 8 1000 [ms] bedeutet 1 Sekunde (Intervall) 0 [ms] bedeutet, Kontakt bleibt dauerhaft geschlossen (bis Schießbetrieb Ende)
shootingRanges	8		Anzahl der Schießbahnen
showRoleSelectPage	true		Anzeige „Weiter als Schütze/Aufsicht“ nach Authentifizierung
timeout	10	10	Rücksprunzeit zum Hauptmenü in Sekunden (im Terminal)

Die Tabelle auf der nächsten Seite zeigt die Einstellungen für die Sicherung der Daten (Datenbank und Exportdateien). Diese Einstellungen sind ebenfalls optional und haben nur Auswirkungen, wenn ein entsprechendes Speichermedium vorhanden ist. Da diese Einstellungen allgemeine Gültigkeit haben, **muss** die Auswahl beim Anlegen der Einstellung auf „**Alle**“ stehen.

Es werden zwei Protokolle unterstützt: **WebDav** und **FTP**. Dabei kann die Sicherung manuell per Tastendruck oder automatisch zu einer bestimmten Uhrzeit (erfordert den Parameter „**backupTime**“ und eine gültige Zeitangabe im Format **hh:mm**) erfolgen.

Tabelle 3 - Backup-Einstellungen

Name	Wert (Beispiele)	Default	Bemerkung
backupType	2	1	1: WebDAV 2: FTP
backupTime	12:34		Zeiteingabe für die automatische Ausführung des Backups
<i>WebDAV</i>			
webdav_user	hs-backup		WebDAV-Username
webdav_password	\$hspw1234%		WebDAV-Passwort
webdav_host	hs-backup.webdav.hidrive...		WebDAV-Hostname
webdav_port	443		WebDAV-Port
webdav_basePath	/Backup		WebDAV-Pfad
<i>FTP</i>			
ftp_host	192.168.122.1		IP
ftp_port	21		Port
ftp_user	ftpuser		Username
ftp_path	/MeinUSB-Speicher		Pfad

Wichtig:

Die Änderung der Backup-Zeit wird erst nach einem Neustart vom System übernommen.

Anmerkung:

Wird als Router z.B. eine FritzBox verwendet, so kann diese als **NAS**-Laufwerk dienen. Für die Einrichtung gibt es im Internet zahlreiche Beiträge, deshalb wird an dieser Stelle nicht näher darauf eingegangen. Ein Passwort ist in diesem Fall nicht nötig.

Manuelle Sicherung

Grundsätzlich kann die Sicherung der Datenbank auch erfolgen, indem der USB-Stick (mit Datenbank) auf ein anderes Speichermedium kopiert wird. Die USB-Sticks sind FAT32 formatiert und können mit jedem Windows-Betriebssystem gelesen und kopiert werden.

Wichtig:

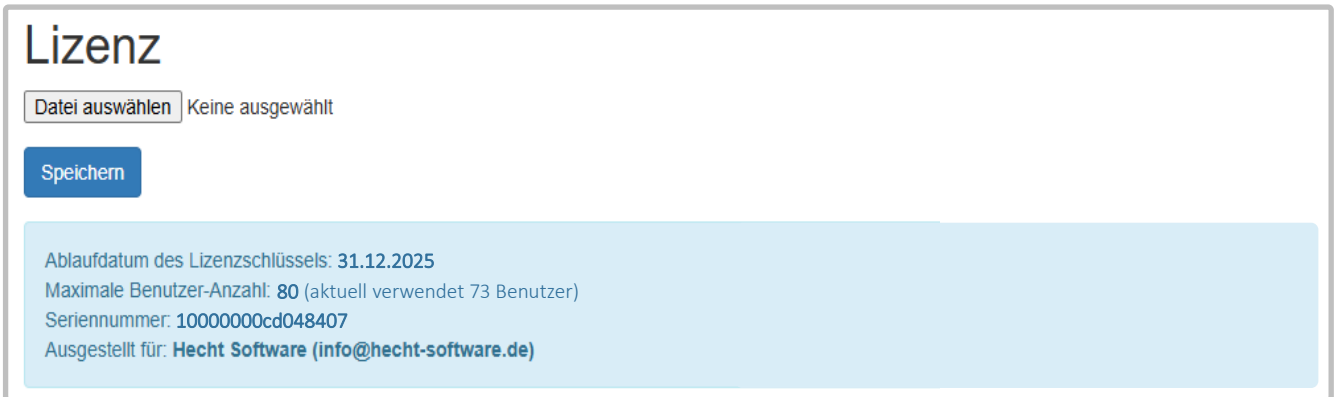
Der Server darf in dieser Zeit keine Daten in die Datenbank schreiben und sollte deshalb abgeschaltet sein (Nicht notwendig bei Sicherung über Backup-Funktion!).

Anmerkung: Wir empfehlen eine regelmäßige Sicherung der Datenbank!

3.1.4.3 Lizenz

Damit die Software funktioniert, muss eine gültiger Lizenz vorhanden sein. Dieser Lizenzschlüssel muss auf einem vom Endgerät (Master) erreichbaren Laufwerk liegen. Mit der Taste „Datei auswählen“ öffnet sich der Dateimanager und die Lizenzdatei kann ausgewählt werden. Findet die Anwendung eine gültige Lizenzdatei, so wird das durch eine hellblau unterlegte Meldung im Fenster mit den Lizenzinformationen angezeigt (siehe Bild 3.16).

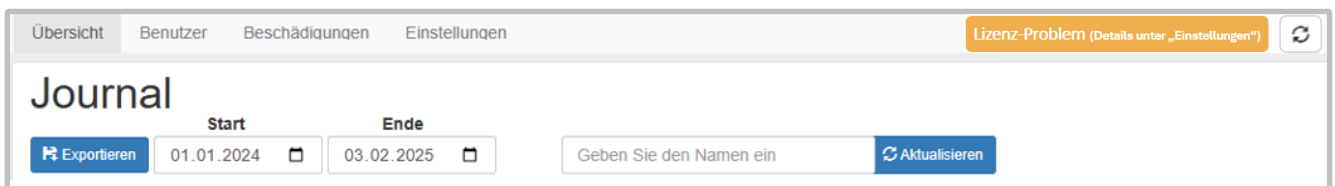
Bild 3.16



Ein falscher, fehlender oder abgelaufener Lizenzschlüssel wird in der Zeile mit den Reitern durch einen orangefarbenen Button (siehe Bild 3.17) signalisiert (Damit kann auch in den entsprechenden Menüpunkt gesprungen werden). In den Terminals erfolgt ebenfalls ein Hinweis, dass die Lizenz erneuert werden muss. Alternativ kann man die Lizenzdatei auf den USB-Stick kopieren - beim Neustart wird diese dann vom System eingelesen und die Lizenz wird auf den aktuellen Stand gebracht.

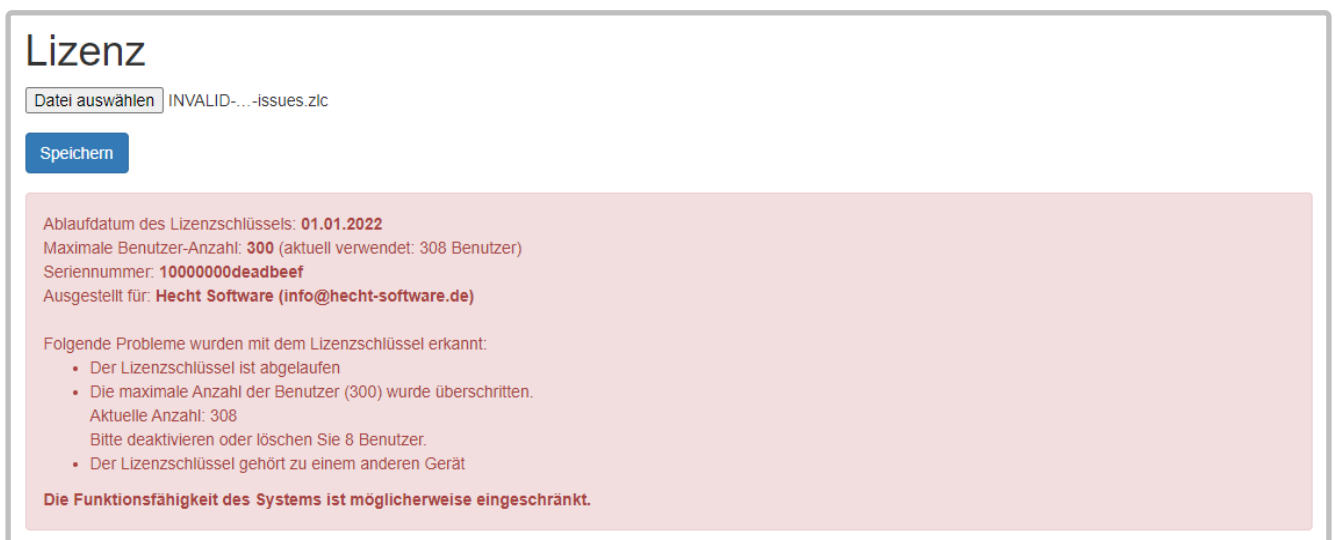
Anmerkung: Dasselbe gilt auch bei Lizenzänderungen (z.B.: Erhöhung der Nutzer) .

Bild 3.17



Mit „Druck“ auf den orangenen Knopf, springt das Programm zum Reiter mit den Einstellungen. Das Meldefenster ist dann rot und die erkannten Probleme sind darin aufgelistet.

Bild 3.18



Wichtig:

Ein ungültiger Lizenzschlüssel kann zu Problemen der Funktionalität führen. Ist der Lizenzschlüssel abgelaufen, so gibt es eine Karenzzeit, um den Schlüssel zu erneuern. In dieser Zeitspanne gibt es keine Einschränkungen der Funktionen!

3.1.4.4 Update

Anmerkung: Der automatische Update-Prozess befindet sich in Überarbeitung.

Dennoch kann ein Update durchgeführt werden, in dem man die Update-Datei manuell auf den USB-Stick kopiert.

1. Terminal Stromlos machen und dann öffnen
2. USB-Stick aus Terminal entfernen
3. USB-Stick in einem PC (z.B. Laptop) stecken und dann die Update-Datei („update.tar.gz“) auf den USB-Stick kopieren
4. USB-Stick zurück ins Terminal stecken
5. Terminal wieder starten - der Updateprozess beginnt

Achtung:

Unterbrechen Sie den Update-Prozess nicht! Die Installation kann mehr als 20 Minuten dauern!

Nach dem das Terminal hochgelaufen ist, steht das Update zur Verfügung. Der aktuelle Softwarestand wird am Display angezeigt.

4. Übersicht Schießbahnbelegung

Auch hier muss sich das Gerät des benutzten Browsers im selben Netzwerk wie das Terminal befinden, dessen Standbelegung angezeigt werden soll. Mit der vom Router vergebenen **IP**, dem **Port** und der **Route** (.../stations) können die Schießstände angezeigt werden (z.B.: **192.168.178.64:1337/stations**). Es gibt für jeden Schießstand einen eigenen Reiter mit dem entsprechenden Namen des Standes und einer Anzeige, ob der Stand beaufsichtigt wird oder nicht:

- Der Stand ist noch nicht von einer Aufsicht in Betrieb genommen worden
- Der Stand wurde durch eine Aufsicht freigegeben

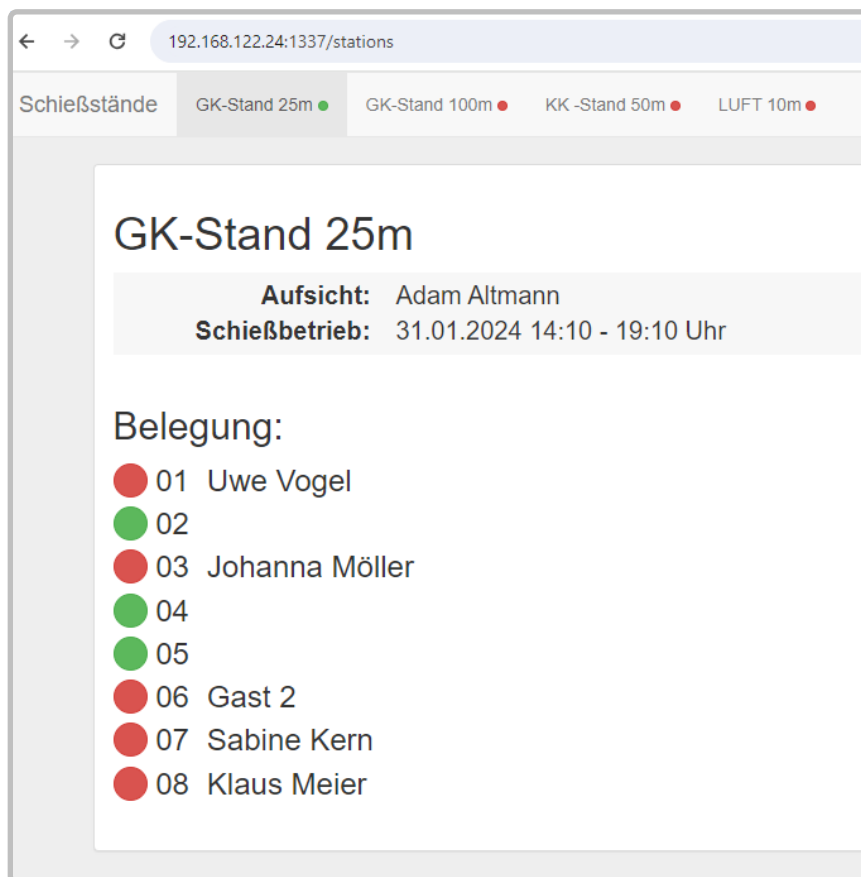
Beim ersten Aufruf ist immer der erste Stand angewählt. Mit dem anklicken des entsprechenden Reiters kann dann der gewünschte Stand ausgewählt werden.

In der Kopfzeile der Seite wird der Name des Standes, die verantwortliche Aufsicht und die Dauer des Schießbetriebs angezeigt. Darunter befindet sich die Liste mit den Schießbahn-Nummern und der Anzeige, ob die Schießbahn belegt ist, oder nicht:

- Die Schießbahn steht noch zur Verfügung.
- Die Schießbahn ist durch einen Schützen belegt.

Ist eine Schießbahn belegt, dann wird der entsprechende Schütze dahinter angezeigt.
Die angezeigten Seiten werden automatisch aktualisiert.

Bild 4.1



5. Terminal

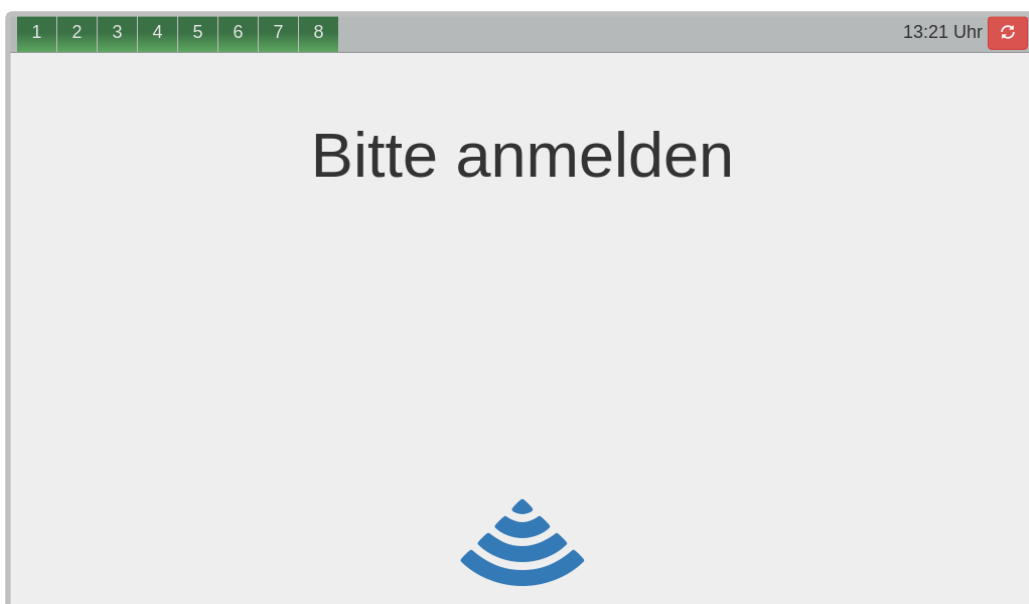
Ist das Terminal ordnungsgemäß angemeldet, so wird der auf dem folgenden Bild dargestellte Bildschirm mit einigen, wichtigen Informationen angezeigt.

Bild 5.1



Nach dem Druck der Taste weiter, wird dann der Startbildschirm angezeigt. Die Statusleiste zeigt die bereits belegten Schießbahnen (hier z. B. Bahn 2), die aktuelle Uhrzeit und die Dauer des Schießbetriebes an. Darunter steht noch die zuständige Aufsicht. Voraussetzung dafür ist, dass alle notwendigen Einstellungen gemacht wurden und dass, Aufsichtspersonen und Schützen hinterlegt wurden (wie im Kapitel 3.1.2 beschrieben).

Bild 5.2

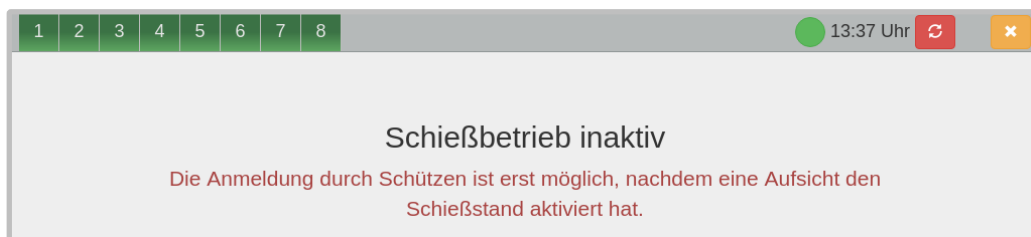


Nun kann der Schießbetrieb beginnen. Dazu wird der RFID-Chip an den installierten Kartenleser gehalten.

5.1 Stand in Betrieb nehmen

Sollte sich noch keine Aufsicht angemeldet haben, so wird folgende Hinweis angezeigt:

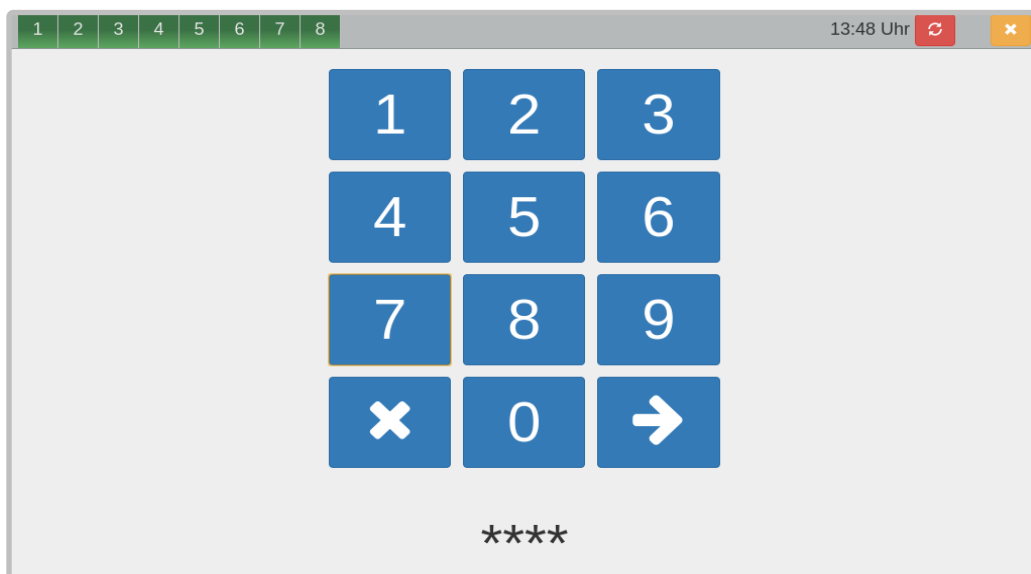
Bild 5.3



Beim Anmelden der Aufsicht verlangt das System die Eingabe der PIN (siehe Bild 5.4). Die Eingabe der PIN-Nummer wird durch das Anzeigen eines Sternchens je Ziffer zurückgemeldet. Die Taste mit dem „Kreuz“ löscht den Eingabepuffer und die PIN kann dann erneut eingegeben werden. Die Taste mit dem „Pfeil“ bestätigt die Eingabe. Abhängig von der vom System vorgegebenen Aktion, wird darauf in das passende Menü gesprungen.

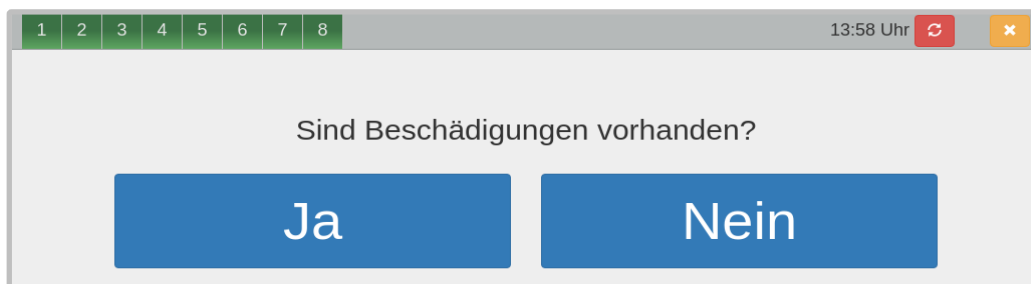
Für alle folgenden Anmeldeprozesse der Schützen und Aufsichten ist immer die Eingabe der PIN in der beschriebenen Weise erforderlich.

Bild 5.4



Ist Aufsicht ist angemeldet, so erfolgt die Abfrage nach eventuellen Beschädigungen, die von der jeweiligen Aufsicht zuvor am Schießstand festgestellt wurden.

Bild 5.5



Sind keine Beschädigungen vorhanden, so ist der Schießstand in Betrieb genommen und die Schützen können sich nun an der gewünschten Schießbahn anmelden (siehe Kapitel 5.2).

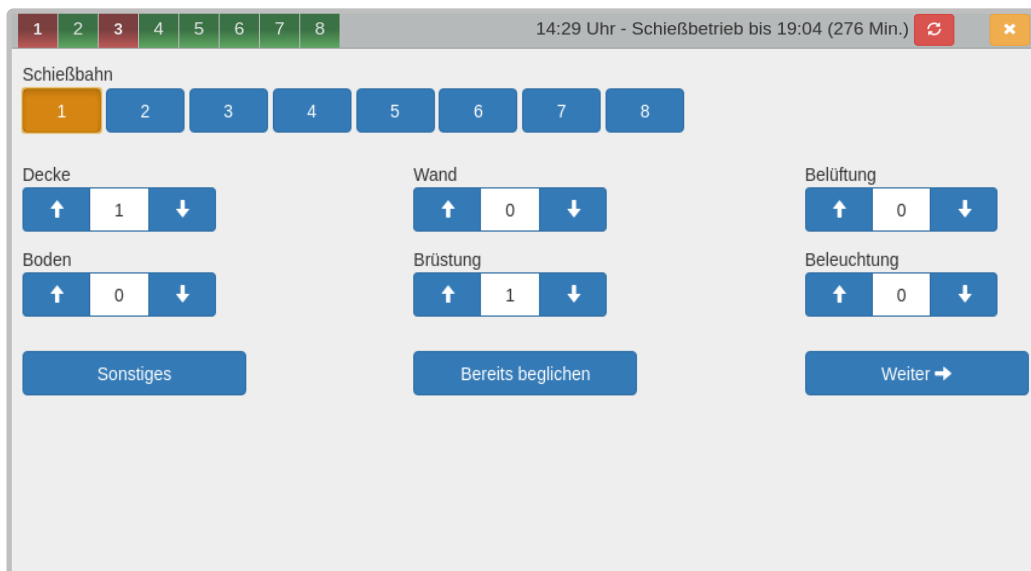
Hat die Aufsicht eine oder mehrere Beschädigungen festgestellt, so wird das folgende Fenster angezeigt.

Bild 5.6



Die Taste „Unbekannt“ dient dazu, um Schäden einzutragen, bei denen der Verursacher (noch) nicht ermittelt werden konnte. Auf der rechten Seite sind die Schützen aufgelistet, die zuletzt an den Ständen angemeldet waren. Für den Fall, dass eine Bildschirmseite für die Anzeige nicht ausreichend ist, so kann mit den beiden „Pfeiltasten“ in der Liste nach unten und oben navigiert werden. Mit dem Druck auf eine der Tasten öffnet sich das Abfragefenster mit den Beschädigungen.

Bild 5.7



Da es Schäden auf verschiedenen Schießbahnen eines Standes geben kann, wird solange in das Menü mit der Schadensabfrage (siehe Bild 5.5) zurückgesprungen, bis die Nachfrage nach weiteren Beschädigungen mit „Nein“ quittiert wird. Dann ist der Prozess beendet und die Schützen können sich anmelden.

Anmerkung:

Beschädigungen können von der jeweiligen Aufsicht auch während des Schießbetriebes erfasst werden.

Anmerkung:

Die in Bild 5.7 eingetragenen Beschädigungen (Decke, Wand, usw.) sind Default-Werte. In den Einstellungen können diese an jeden Schießstand angepasst werden. Es sind hier maximal 9 verschiedene Einträge möglich. Die im Anzeigefenster dargestellten Beschädigungen werden automatisch an die, in den Einstellungen der Admin-Konsole hinterlegten Parameter, angeglichen. Die

Wichtig:

Die Eingabe einer einzigen Beschädigung löscht alle vorhandenen Default-Werte!

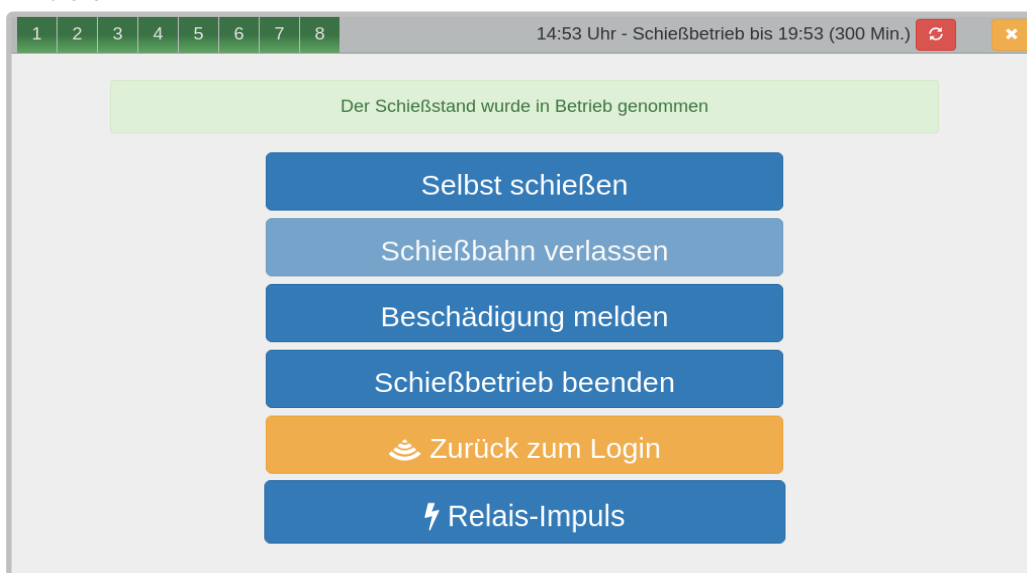
5.2 Anmeldung und Abmeldung

Wurde der Schießstand in Betrieb genommen, so erscheint für die eingestellte Zeit („timeout“) das „Aufsichtsfenster“ mit der entsprechenden Meldung und den verschiedenen Funktionsknöpfen.

Anmerkung:

Dieses Fenster erscheint jedes Mal, wenn die Aufsichtsperson ihren RFID-Chip an den NFC-Raeder hält und die dazugehörige PIN eingibt.

Bild 5.8



- Die beiden ersten Knöpfe erlauben es, dass die Aufsichtsperson selbst schießt (z.B.: noch kein weiterer Schütze anwesend ist)
- Mit dem dritten Knopf können jederzeit Beschädigungen gemeldet oder bearbeitet werden
- Mit dem vierten Knopf wird das Schießen auf dem jeweiligen Stand beendet
- Um die Rücksprungzeit („timeout“) zum Anmeldefenster kann mit dem fünften Knopf umgangen werden
- Sobald in den Einstellungen eine Impulsdauer für ein oder mehrere Relais definiert wurde, so erscheint der Knopf „Relais-Impuls“. Mit diesem gelangt man dann zum Fenster für die manuelle Ansteuerung, in dem die betroffenen Relais wieder durch Knöpfe aufgelistet sind. Dort kann, falls nötig, für jedes aufgelistete Relais manuell ein Impuls ausgelöst werden (z.B.: Beleuchtung nach Stromausfall wieder einschalten, falls dies durch eine Tastfunktion realisiert wurde)

Anmerkung:

Schießt die Aufsichtsperson selbst, so ist die Anmeldung für Schützen gesperrt.

5.2.1 Anmeldung als Schütze

Wie bereits erwähnt, muss eine Aufsicht angemeldet sein und den Stand in Betrieb genommen haben, damit sich Schützen am Stand registrieren können. Das Terminal zeigt das folgende Anmeldefenster (Bild 5.9). Hier wird auch die für den Schießstand verantwortliche Person angezeigt. In der Statusleiste wird, neben der aktuellen Uhrzeit, auch die Dauer des Schießbetriebs angezeigt.

Bild 5.9



Durch das Anlegen der RFID-Karte wird bei registrierten Schützen die PIN-Eingabe aufgerufen und die zur Karte gehörende vierstellige PIN-Nummer kann eingegeben werden (Siehe Bild 5.4).

Anmerkung:

Jede eingegebene Ziffer wird durch ein „Sternchen“ dargestellt. Bei richtiger Eingabe der 4 Ziffern können diese nun mit der „Pfeil“-Taste übernommen werden. Danach wird die Kaliberauswahl aufgerufen. Die Taste mit dem „Kreuz“ löscht den Eingabepuffer, um bei Tippfehlern die PIN erneut einzugeben.

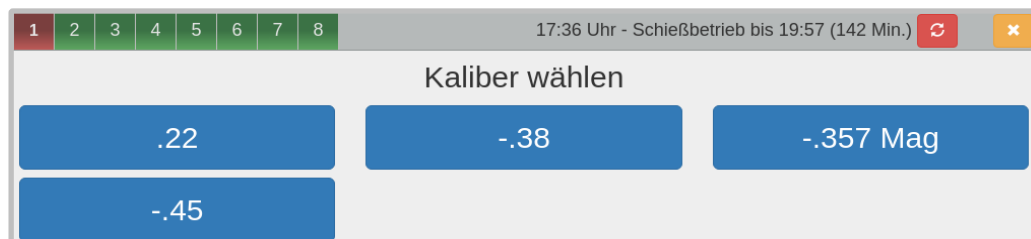
Eine falsche Eingabe wird durch das System gemeldet (siehe Bild 5.10).

Bild 5.10



Ist die PIN korrekt, so wird in die Kaliberauswahl gesprungen.

Bild 5.11



Nachdem das Kaliber festgelegt ist, erfolgt die Wahl der Schießbahn. Sind Schießbahnen bereits belegt, so sind die dazugehörigen Knöpfe rot unterlegt. Im Bild 5.12 sind das die Bahn 1 und die Bahn 3.

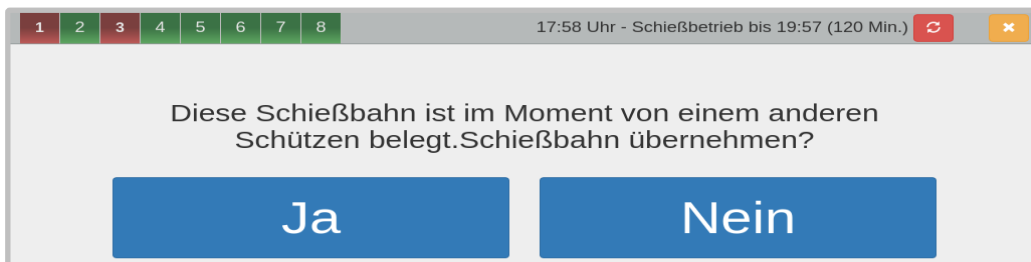
Bild 5.12



Die grün unterlegten Knöpfe sind frei wählbar. Wird eine dieser freien Bahnen gewählt, dann ist der Anmeldeprozess abgeschlossen und das Schießen kann beginnen. Das Display zeigt nun das erneut das Anmeldefenster (siehe Bild 5.9).

Hat sich ein Schütze nicht ordnungsgemäß abgemeldet, dann kann die entsprechende Schießbahn von anderen Schützen trotzdem übernommen werden. Damit dies nicht versehentlich passiert, erfolgt eine Abfrage, ob die Schießbahn auch wirklich übernommen werden soll (siehe Bild 5.13). Mit der Übernahme erfolgt die Abmeldung des Vorgängers und der Rücksprung ins Anmeldefenster.

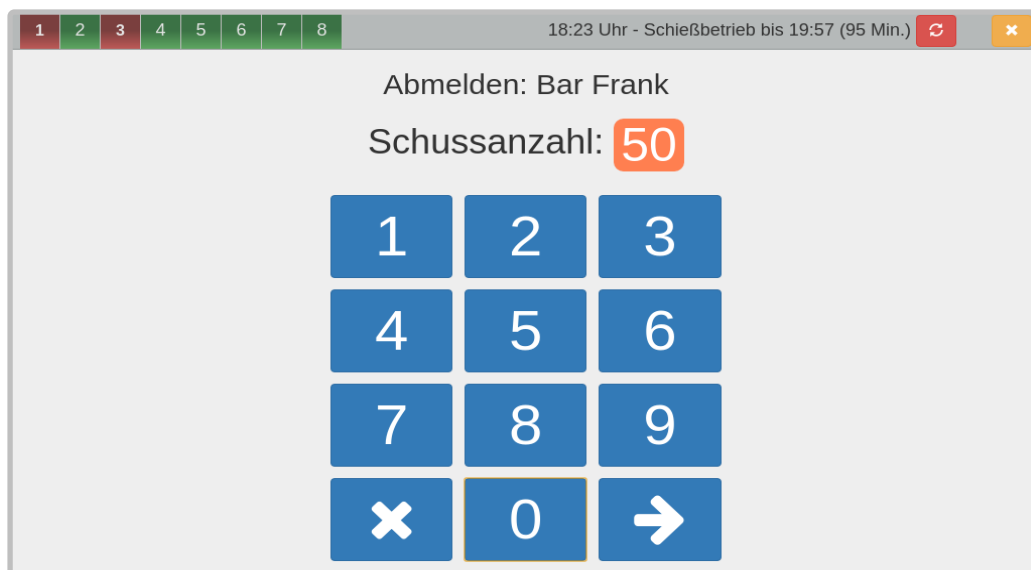
Bild 5.13



5.2.2 Abmeldung als Schütze

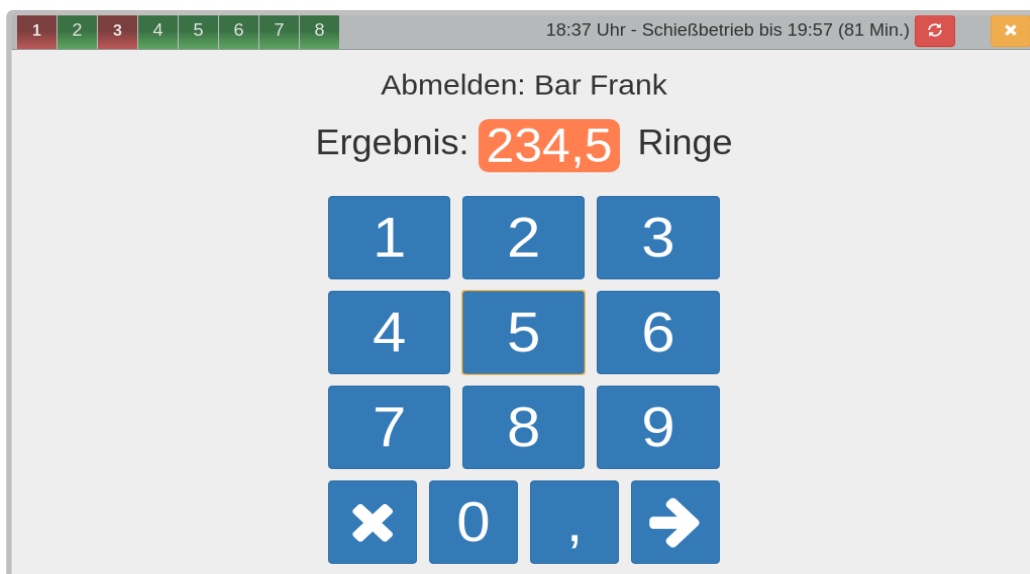
Zum Abmelden eines Schützen, hält dieser seine RFID-Karte an den RFID-Leser. Die Eingabe der PIN ist hier nicht nötig. Je nach Parametrierung (siehe Tabelle 2, Seite 11) wird nun die Anzahl der abgegebenen Schüsse (siehe Bild 5.13) oder das Ergebnis des Schießens (siehe Bild 5.14) eingegeben.

Bild 5.14



Wurde in den Einstellungen die Eingabe eines Schießergebnisses festgelegt, so wird der Nummernblock um die „Komma“-Taste erweitert. So ist auch die Eingabe von Teilern möglich.

Bild 5.15



Wird das Menü ohne Eingabe des Ergebnisses oder einer Schussanzahl verlassen, so wird in die Datenbank an dieser Stelle eine „0“ eingetragen. Die Taste mit dem „X“ löscht eine fehlerhafte Eingabe, während die Taste mit dem „Pfeil“ das Resultat in die Datenbank übernimmt.

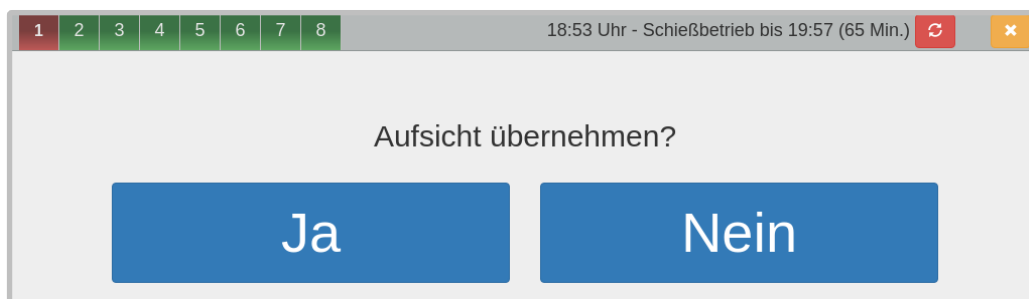
5.2.3 Schießbetrieb beenden

Der Schießbetrieb kann nur durch die verantwortliche Aufsicht beendet werden. Dazu muss zusätzlich zum Lesen des RFID-Chip noch die PIN-Nummer eingegeben werden. Wird der Schießbetrieb eingestellt, so werden alle Schützen noch angemeldeten Schützen automatisch abgemeldet und alle Schießbahnen des Standes sind wieder unbelegt. Das System fragt wieder nach möglichen Beschädigungen (wie schon in Kapitel 5.1 beschrieben).

5.2.4 Wechsel der Aufsicht

Ein Wechsel der Aufsicht während des laufenden Schießbetriebs ist jederzeit möglich. Dies hat keinerlei Einfluss auf den Schießbetrieb, dieser läuft unterbrechungsfrei weiter. Durch das Anmelden der neuen Aufsicht wird die bisherige Aufsicht automatisch abgemeldet.

Bild 5.16



Im Anmeldefenster wird nun die neue Aufsicht angezeigt.

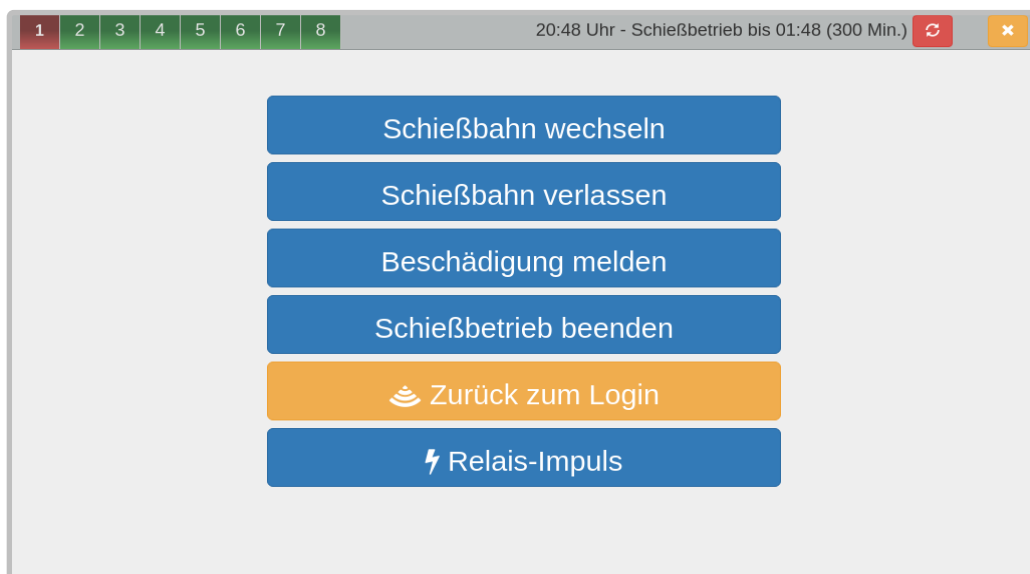
5.2.5 Sonderfall Aufsicht als Schütze

Wichtig:

Zum Zeitpunkt der Veröffentlichung dieser Bedienungsanleitung ist dies laut Gesetz nur zulässig, wenn sich kein weiterer Schütze zum Schießen in der Schießanlage befindet! Deshalb sperrt das System weitere Anmeldevorgänge, wenn die Aufsicht selbst schießt.

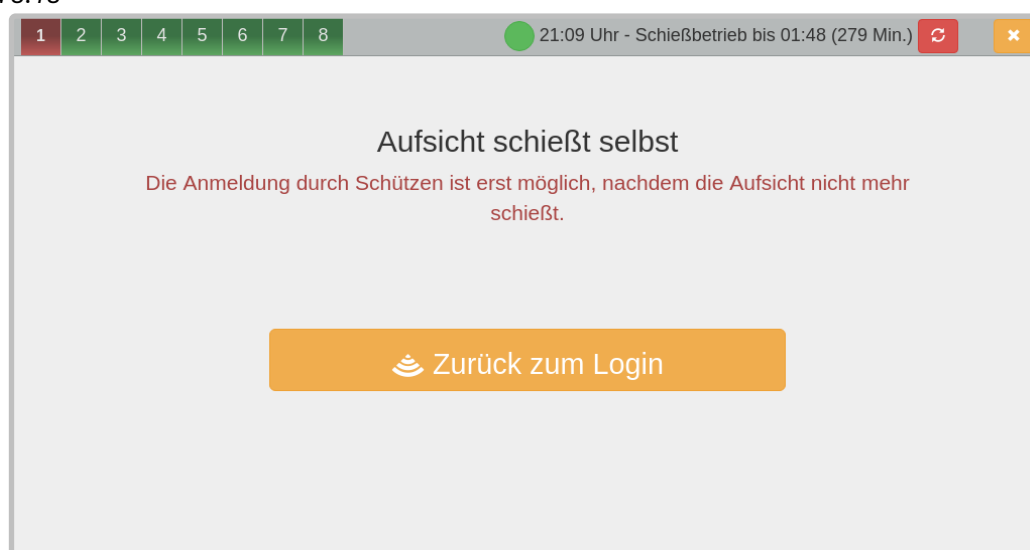
Sobald sich die Aufsicht sich im Aufsichtsmenü zum Schießen angemeldet hat, ändert sich die Funktion des ersten Knopfes von Schießbahn wählen zu Schießbahn wechseln und der zweite Knopf wird aktiviert (siehe Bild 5.17), mit diesem Knopf beendet die Aufsicht ihr Schießen.

Bild 5.17



Will sich nun ein Schütze anmelden, so wird vom System eine entsprechende Meldung ausgegeben. (siehe Bild 5.18).

Bild 5.18



Anmerkung:

Hat sich bereits ein Schütze angemeldet, so kann die zuständige Aufsicht nicht mehr schießen. Der Knopf „Schießbahn wählen“ ist deaktiviert.

6. Zugangskontrolle

Anmerkung:

Die Steuerung der Zugangskontrolle mit Parametern wird noch überarbeitet. Hier wird mittelfristig eine grafisch Benutzeroberfläche integriert.

6.1 Parameter

Für die Zugangskontrolle gibt es neben dem Parameter „relayXduration“ drei weitere Einstellungen, die in der nachfolgenden Tabelle dokumentiert sind. Das „X“ steht dabei für die Nummer des jeweiligen Relais.

Tabelle 4 - Relais-Einstellungen

Name	Wert	Default	Bemerkung
relayXduration	0 > 0		0 = Relais schaltet ein oder aus. Schaltzeit in Millisekunden (z.B.: 3500 = 3,5 Sekunden)
relayXmode	1, 100, 200	1	1: Relais schaltet bei Standaktivierung 100: Relais schaltet nach Anmeldung (Auch Schützen) nach Verlassen des Menüs. 200: Relais schaltet nach Authentifizierung am Wiegand-Codeschloss. (Karte + Pin)
relayXcondition	0,1,2,3,4,4	2	Bedingung, für das Schalten des Relais (Hat keinen Effekt bei Relais-Modus 1 - relayXmode = 1) 0: niemals 1: immer 2: gemäß Zeitplan (schedule) falls verfügbar (s.u.) 3: Wenn Nutzer Aufsicht 4: Wenn Nutzer Aufsicht, sonst gemäß Zeitplan 5: Wenn Nutzer Aufsicht oder Stand aktiv ist
schedule	WThh:mm-WThh:mm;		Mo08:00-10:00;Mo13:00-14:00;Do9:00... usw.

6.2 Beispiel

Die Haupttüre des Vereinsheims soll zu den Schießzeiten am Montag, Mittwoch und Samstag von den Schützen geöffnet werden können. Schießzeit von Montag 18:00 Uhr bis 22:00 Uhr, Mittwoch gleiche Zeit und Samstag 9:30 Uhr bis 12:00 Uhr und 17:00 Uhr bis 23:00 Uhr. Zur Ansteuerung des Türöffners soll Relais 1 verwendet werden. Der Türöffner soll 3 Sekunden betätigt werden.

Dazu sind die Parameter aus Tabelle 5 in den Einstellungen zu ergänzen. Im Beispiel ist der Türöffner am Steuerrelais 1 im Terminal „GK 25m“ angeschlossen.

Tabelle 5

Name	Wert	Schießstand
relay1duration	3000	GK 25m
relay1mode	200	GK 25m
relay1condition	2	GK 25m
schedule	Mo18:00-22:00;Mi18:00-22:00;Sa09:30-12:00; Sa17:00-23:00	GK 25m

7. Software-Versionen

Version	Beschreibung	Datum
1.2.10	Adminkonsole Journal: Filterfunktion verbessert	25.02.2025
1.2.8	Sicherung mit FTP-Protokoll, Anpassung Steuerung für Kunde	29.01.2025
1.2.5	Eingabe Schussanzahl bei Logout	28.01.2025
1.2.4	Zeitsynchronisation zwischen Master und Client, Datenbankabfrage bei Hochlauf überarbeitet	18.07.2024
1.2.3	Warten auf Datenbank beim Start, Anpassung DB-Host-Adresse	12.06.2024
1.2.1	Erweiterung Ansteuerung auf 8 Relais	10.06.2024
1.2.0	Mehrere Stände pro Terminal und Anpassung der Relaisansteuerung, (Grundversion für Docker-Weiterentwicklung)	08.04.2024
1.1.23	Schießergebnis auf Dezimaleingabe erweitert, Ausblenden nicht benötigter Tasten für die Steuerung der Relais, Erweiterung der Benutzerführung, Standbelegung in der Adminkonsole anzeigen	29.02.2024
1.1.21	Anpassung Benutzerführung für Kunde	25.10.2023
1.1.20	Ansteuerung Relais erweitert (Impuls), Zusätzliche Bedienung der Relais am Terminal	05.10.2023
1.1.18	Anpassung Benutzerführung für Kunde	25.09.2023
1.1.16	Anpassung Benutzerführung für Kunde	20.09.2023
1.1.14	Benutzerführung parametrierbar	14.09.2023
1.1.12	Bei Initialisierung Seriennummer anzeigen, Filterfunktion für RFID-Karten, Sicherung der CSV-Dateien mit WebDav	16.08.2023
1.1.11	RFID-Code Längenbegrenzung erhöht, Designanpassungen	27.07.2023
1.1.9	Passwort-Schutz und Idle-Logout Adminkonsole, User inaktiv schalten, Logbuch-Export mit Datumsfilter, User-Export, Aufsicht als Schütze	20.07.2023
1.1.5	Fehlerbehebung Settings	13.06.2023
1.1.4	Uhrzeit und Datum einstellbar über Adminkonsole, Datenbank-Backup mit WebDav	09.06.2023
1.1.3	3-RFID-Chips je User, Anpassung Display-Auflösung auf 10“, Erfassung Schießergebnis	08.05.2023
1.1.2	Aufsicht auf Login-Seite anzeigen	20.05.2022
1.1.0	Grundversion	19.05.2022

Fehlende Versionsnummern sind technisch bedingt. Diese dienen zur schnellen Fehlerbehebung.