INDUSTRIELLE STÖRMELDUNG UND ALARMMANAGEMENT

AS1122

Installationsanleitung

Alarmüberwachungs-, Benachrichtigungs- und Vor-Ort-Warngerät für den Schaltschrankeinbau · 16 Eingänge · 16 Ausgänge

Oktober 2026 · Rev. 1.0
ionia Automation Technologies · ionia-automation.com

Inhalt

1 Zu dieser Anleitung und Sicherheit 4

1.1 Zu dieser Anleitung 4

1.2 Sicherheitshinweise 4

2 Produktübersicht 6

2.1 Was das AS1122 leistet 6

2.2 Gerät und Frontplatte 6

2.3 Geräteetikett 7

3 Montage 7

3.1 Wahl des Montageorts 7

3.2 Montage im Schaltschrank 7

4 Elektrischer Anschluss 8

4.1 Allgemeine Regeln 8

4.2 Spannungsversorgung 8

4.3 Eingänge 8

4.4 Ausgänge 9

4.5 Vor dem Einschalten 9

5 Erste Inbetriebnahme und Einrichtungsassistent 10

5.1 Einschalten 10

5.2 Verbindung mit dem Geräte-WLAN 10

5.3 Einrichtungsassistent 10

5.4 Testnachricht 11

5.5 Wiederherstellungscode 11

6 Netzwerkverbindung 12

6.1 Anlagen-WLAN 12

6.2 Zugriff auf das Panel aus dem Anlagennetz 12

6.3 Geräte-WLAN und Passwort 12

6.4 IT- und Firewall-Anforderungen 13

7 Personen und Benachrichtigungen 15

7.1 Rollen und Berechtigungen 15

7.2 Personen hinzufügen 15

7.3 Benachrichtigungskonto und Telegram 15

7.4 E-Mail 16

7.5 Ziele und Eskalation 16

7.6 Test und Zustellprotokoll 16

8 Inbetriebnahme der Eingänge 16

9 Inbetriebnahme der Ausgänge 18
9.1 Ausgänge benennen und von Hand testen 18
9.2 Erste Ausgangsregel 18
9.3 Test vor Ort 19
10 Mehrere Geräte: Anlage 19
11 Sicherung, Werkseinstellungen und Wiederherstellung 20
11.1 Einstellungssicherung 20
11.2 Werkseinstellungen 20
11.3 Wenn die Administrator-PIN vergessen wurde 20
11.4 Wenn das Passwort des Geräte-WLANs vergessen wurde 21
11.5 Software-Update 21
12 Frontplatte: LEDs und Tasten 21
12.1 Status-LEDs 21
12.2 Tasten 21
13 Fehlerbehebung 22
14 Technische Daten (Übersicht) 23
15 Checkliste zur Inbetriebnahme 23
16 Garantie und Support 24

1 Zu dieser Anleitung und Sicherheit

1.1 Zu dieser Anleitung

Diese Anleitung richtet sich an das Fachpersonal, das das Alert SCADA AS1122 im Schaltschrank montiert, die elektrischen Anschlüsse herstellt und die Ersteinrichtung durchführt. Die tägliche Nutzung (Alarmüberwachung, Quittieren, Ausgangsregeln) ist im **Benutzerhandbuch** beschrieben.

Produkt	Alert SCADA AS1122 — 16 digitale Eingänge, 16 digitale Ausgänge
Zielgruppe	Elektro- / Automatisierungspersonal, das das Gerät montiert, verdrahtet und in Betrieb nimmt; IT-Personal
Zugehörige Dokumente	Benutzerhandbuch · Datenblatt · Garantieschein

Menü-, Seiten- und Schaltflächennamen des Panels sind in dieser Anleitung **fett** und mit ihrer englischen Bezeichnung dargestellt (z. B. **Alarm Settings** → **Rules**). Das Panel ist auf Türkisch und Englisch verfügbar.

In dieser Anleitung verwendete Hinweiskästen:

Gefahr
Bei Nichtbeachtung können Personen oder Sachwerte gefährdet werden.

Warnung
Bei Nichtbeachtung können das Gerät oder die Anlage beschädigt werden oder ein Alarm kann unbemerkt bleiben.

Hinweis
Informationen, die Ihnen die Arbeit erleichtern.

1.2 Sicherheitshinweise

Personensicherheit

Alert SCADA ist ein Störmeldegerät. **Es ersetzt keine Brandmelde-, Gaswarn-, Personenschutz- oder gesetzlich vorgeschriebenen Alarmsysteme** und verfügt nicht über die Zertifizierungen solcher Systeme.

Die Ausgänge des AS1122 dienen **ausschließlich der Warnung und Signalisierung** (Sirenen, Blitzleuchten, Signalsäulen, Hupen). Die Ausgänge sind kein Sicherheitsrelais, kein Not-Halt und kein Maschinensicherheitskreis. **Not-Halt- und Personenschutzkreise bleiben in ihren eigenen Sicherheitssystemen.**

- Montage und elektrischer Anschluss sind von **autorisiertem Elektrofachpersonal** gemäß den geltenden Installationsvorschriften durchzuführen.
- Verdrahten Sie **nur im spannungsfreien Zustand**: Die Versorgung des Geräts, die Signalspannung an den Eingängen und die Versorgung der an die Ausgänge angeschlossenen Lasten müssen abgeschaltet sein.
- Versorgungs-, Eingangs- und Ausgangswerte dürfen die in dieser Anleitung angegebenen Grenzwerte (Abschnitt 4 und Abschnitt 14) nicht überschreiten.
- Montieren Sie das Gerät **in einem trockenen, staubfreien Schaltschrank**.

- Bei Stromausfall und bei einem internen Gerätefehler werden die Ausgänge **freigegeben (abgeschaltet)**. Auswahl, Absicherung und sicherer Betrieb der an die Ausgänge angeschlossenen Betriebsmittel liegen in der Verantwortung des Anwenders.
- Die Zustellung von Benachrichtigungen hängt von der Stromversorgung, der Internetverbindung und Diensten Dritter (Telegram, E-Mail) ab. Versorgen Sie das Gerät in kritischen Anlagen über eine durch eine **unterbrechungsfreie Stromversorgung (USV)** gestützte Leitung und sehen Sie einen alternativen Kommunikationsweg vor.
- Öffnen Sie das Gehäuse nicht. Die Teile im Inneren können vom Anwender nicht ausgetauscht werden; durch das Öffnen des Gehäuses erlischt die Garantie.

2 Produktübersicht

2.1 Was das AS1122 leistet

Das AS1122 überwacht kontinuierlich 16 Kontaktsignale in Ihrem Schaltschrank (Pumpenstörung, Auslösung des Motorschutzes, Tür, Niveauschalter, Maschinenstillstand usw.). Geht ein Signal in den Alarmzustand, benachrichtigt es die zuständigen Personen und warnt auf Wunsch die Personen vor Ort mit Sirene, Blitzleuchte oder Signalsäule.

Überwacht
16 digitale Eingänge (DI00–DI15), 1 ms Abtastung. Schließer- und Öffnerkontakte.

Benachrichtigt
Mehrere Personen gleichzeitig per Telegram und E-Mail. Quittierung, wer wann reagiert hat, und Eskalation nicht quittierter Alarme.

Warnt vor Ort
16 Ausgänge (DO00–DO15): Sirenen, Blitzleuchten, Signalsäulen, Hupen. Eine berechtigte Person schaltet sie von Hand ein und aus, oder sie arbeiten automatisch mit WENN … DANN-Regeln ohne Programmierung.

Protokolliert
Alle Ereignisse, Quittierungen und Ausgangsbefehle mit Datum, Uhrzeit und Person. Strom- und Internetausfälle mit ihrer Dauer.

Das Gerät ist nicht an eine Cloud gebunden: Einstellungen und Aufzeichnungen bleiben im Gerät. Das Internet wird nur zum Senden von Benachrichtigungen und zur Uhrzeitsynchronisation genutzt. Für Einrichtung und Nutzung wird keine App installiert; der Browser eines Telefons, Tablets oder Computers genügt.

2.2 Gerät und Frontplatte

Frontplatte: vier Status-LEDs und drei Tasten; die Anschlussklemmen befinden sich an der Ober- und Unterkante des Gehäuses.

Teil	Beschreibung
Status-LEDs (4)	Von links nach rechts LED1 rot, LED2 gelb, LED3 gelb, LED4 grün. Zeigen an, dass das Gerät läuft, dass es mit dem Anlagen-WLAN verbunden ist, sowie den Aufzeichnungsstatus (Abschnitt 12)
Tasten (3)	Linke, mittlere und rechte Taste. Zum Neustart ohne Computer (Abschnitt 12)
Klemmen	Schraubklemmenblöcke: Versorgung, Eingänge und Ausgänge (Abschnitt 4)
Etikett	Seriennummer, Geräte-WLAN-Daten und QR-Codes (Abschnitt 2.3)

2.3 Geräteetikett

Notieren Sie die Etikettangaben vor der Installation; Sie benötigen sie bei Einrichtung und Service.

Angabe	Beispiel	Zweck
Seriennummer	`ION8-1122-YYAA-NNNN`	Garantie- und Serviceerfassung
Name des Geräte-WLANs	`ION8BOOT_xxxxxx`	Ersteinrichtung und Wartungsverbindung
Passwort des Geräte-WLANs	Auf dem Etikett aufgedruckt	Erste Verbindung; nach der Einrichtung **ändern** (Abschnitt 6.3)
Panel-Adresse	`http://192.168.4.1`	Adresse des Panels bei Verbindung mit dem Geräte-WLAN
QR-Codes	**1** · **2** · kleiner QR	1: verbindet das Telefon mit dem Geräte-WLAN · 2: öffnet das Panel im Browser · kleiner QR: Seriennummer

> **Modellcode**
> Auf dem Geräteetikett und in der oberen Ecke des Panels erscheint der Modellcode **ION8-1122**; dieser Code bezeichnet das Alert SCADA AS1122.

3 Montage

3.1 Wahl des Montageorts

- Montieren Sie das Gerät **in einem trockenen, staubfreien Schaltschrank**. Das Gehäuse bietet teilweisen Schutz gegen Staub; es ist nicht gegen Wasser geschützt.
- Das Gerät verbindet sich über **WLAN** mit dem Anlagennetz. **Ein Metallgehäuse schwächt das WLAN-Signal:** Prüfen Sie vor der Montage mit einem Telefon bei geschlossener Schaltschranktür, ob das Anlagen-WLAN im Schaltschrank ausreichend stark ist. Ist das Signal schwach, verwenden Sie einen WLAN-Access-Point in der Nähe des Schaltschranks.
- Wählen Sie eine Position, an der die LEDs und Tasten der Frontplatte bei geöffneter Schaltschranktür gut sichtbar und erreichbar sind.
- Lassen Sie vor den Klemmen ausreichend Platz für die Verdrahtung.

3.2 Montage im Schaltschrank

1. Montieren Sie das Gerät **mit Schrauben auf einer ebenen Fläche** (Montageplatte). Es gibt 4 Befestigungslöcher mit Ø3,8 mm; Lochabstand (Mitte zu Mitte) **80,4 × 104,1 mm**.
2. Ziehen Sie die Schrauben an, ohne das Gehäuse zu verspannen.
3. Prüfen Sie vor der Verdrahtung, dass Frontplatte und Klemmen gut erreichbar sind.

Mechanik	Wert
Montage	Schraubmontage auf ebener Fläche, im Schaltschrank
Befestigungslöcher	4 × Ø3,8 mm, Mittenabstand 80,4 × 104,1 mm
Abmessungen	115 × 114 × 45 mm (ohne Befestigungslaschen und Steckverbinder)
Gewicht	250 g

4 Elektrischer Anschluss

4.1 Allgemeine Regeln

Nur spannungsfrei verdrahten

Stellen Sie alle Anschlüsse her, während die Versorgung des Geräts, die Signalspannung der Eingänge und die Versorgung der Ausgangslasten **abgeschaltet** sind. Klemmen bei eingeschalteter Versorgung weder anschließen noch lösen.

- Die Klemmen sind Schraubklemmen. Versehen Sie feindrähtige Leiter mit Aderendhülsen; ziehen Sie die Schrauben an und prüfen Sie den Sitz durch leichtes Ziehen am Draht.
- Verlegen Sie Signalleitungen möglichst getrennt von Leistungskabeln.
- Notieren Sie beim Verdrahten, welche Klemme zu welchem Kanal gehört; bei der ersten Inbetriebnahme prüfen Sie jeden Eingang und Ausgang im Panel (Abschnitt 8 und Abschnitt 9).

4.2 Spannungsversorgung

Versorgungsspannung	**24 V DC** nominal, Arbeitsbereich **15–30 V DC**

- Versorgen Sie das Gerät aus der 24-V-DC-Quelle im Schaltschrank. Achten Sie auf die Polarität.
- Für eine unterbrechungsfreie Überwachung nehmen Sie die Versorgung von einer **USV-gestützten** Leitung. Bei Stromausfall arbeitet das Gerät nicht, kann die Eingänge nicht überwachen und alle Ausgänge schalten ab; bei Wiederkehr der Spannung meldet es die Dauer des Ausfalls (Benutzerhandbuch).
- Muss ein an einen Ausgang angeschlossenes Warngerät (z. B. eine Sirene) auch bei Stromausfall funktionieren, versorgen Sie sowohl das Gerät als auch dieses Warngerät über eine USV-gestützte Leitung.

4.3 Eingänge

Anzahl der Eingänge	16 digitale Eingänge (2 × 8), im Panel als **DI00 – DI15** angezeigt
Eingangstyp	**PNP, 24 V DC**: Der Eingang wird aktiv (1), wenn +24 V anliegen; mindestens 15 V für logisch 1
Isolation	Optisch isoliert, 2500 V
Anschließbar	Potenzialfreie Kontakte (Relaiskontakt, Schalter, Taster), Sensoren mit PNP-Ausgang

- **Potenzialfreier Kontakt:** Verbinden Sie eine Seite des Kontakts mit 24 V DC und die andere Seite mit dem Eingang. Schließt der Kontakt, wird der Eingang 1.
- **Schließerkontakt (NO):** Der Eingang wird 1, wenn der Kontakt schließt. Wählen Sie als Alarmbedingung „Signal on (0→1)“ (Signal kommt).
- **Öffnerkontakt (NC):** Der Eingang ist normalerweise 1; er wird 0, wenn der Kontakt öffnet oder **der Draht bricht**. In Kreisen, in denen auch ein Drahtbruch einen Alarm auslösen muss, verwenden Sie einen Öffnerkontakt und die Option **Inverted Logic** (invertierte Logik) des Eingangs (Abschnitt 8).

Nicht verwendete Eingänge

Setzen Sie nicht verwendete Eingänge im Panel auf **Disabled** (deaktiviert; im Auslieferungszustand sind alle Eingänge deaktiviert). So wird verhindert, dass ein offener Eingang durch Störungen Alarme auslöst.

4.4 Ausgänge

Anzahl der Ausgänge	16 digitale Ausgänge (2 × 8), im Panel als **DO00 – DO15** angezeigt
Ausgangstyp	Plusschaltender (PNP-)Transistorausgang; geschützt gegen Überstrom und Übertemperatur
Ausgangsspannung	Folgt der Versorgungsspannung (bei eingeschaltetem Ausgang liegt die Versorgungsspannung an der Last an)
Ausgangsstrom	Max. **100 mA** je Ausgang
Verwendungszweck	Warnung und Signalisierung: Sirenen, Blitzleuchten, Signalsäulen, Hupen, Koppelrelaisspulen
Beim Start	Alle Ausgänge starten ausgeschaltet
Bei Stromausfall / Fehler	Ausgänge werden freigegeben (abgeschaltet)

- Im eingeschalteten Zustand legt der Ausgang die Versorgungsspannung an die Last (plusschaltend). Verbinden Sie eine Seite der Last mit dem Ausgang und die andere Seite mit 0 V der Versorgung.
- DC-Warnleuchten, Koppelrelaisspulen sowie SPS- / Signaleingänge mit einer Stromaufnahme von **höchstens 100 mA** können direkt angeschlossen werden.
- Schließen Sie Sirenen, Blitzleuchten, Signalsäulen oder 230-V-AC-Warngeräte **mit höherer Stromaufnahme** nicht direkt an: Steuern Sie mit dem Ausgang ein **geeignetes Koppelrelais oder Schütz** an und versorgen Sie die Last über dessen Kontakt.
- Wählen Sie die angeschlossenen Betriebsmittel so, dass sie bei ausgeschaltetem Ausgang (Stromausfall, Gerätefehler, Software-Update) in einem sicheren Zustand bleiben. Schließen Sie keine Last an einen Ausgang des AS1122 an, deren Abschalten eine Gefahr verursachen würde.

Die Ausgänge sind kein Sicherheitskreis

Verwenden Sie die Ausgänge des AS1122 nicht in Not-Halt-, Maschinensicherheits- oder Personenschutzkreisen. Diese Kreise bleiben in ihren eigenen zertifizierten Sicherheitssystemen. Die Ausgänge des AS1122 dienen ausschließlich der Warnung und Signalisierung.

4.5 Vor dem Einschalten

✓	Prüfung
☐	Versorgungsspannung im Bereich 15–30 V DC, Polarität korrekt
☐	Eingangskontakte an den richtigen Kanälen angeschlossen; Kontaktart (NO / NC) notiert
☐	Ausgangslasten nicht über 100 mA; größere Lasten über Koppelrelais
☐	Angeschlossene Betriebsmittel im ausgeschalteten Zustand sicher; kein Ausgang an einem Sicherheitskreis
☐	Klemmschrauben fest, Drähte lösen sich beim Ziehen nicht

5 Erste Inbetriebnahme und Einrichtungsassistent

5.1 Einschalten

1. Prüfen Sie die Anschlüsse und schalten Sie die Versorgung ein. Beim Start sind **alle Ausgänge ausgeschaltet.**
2. Die LEDs leuchten zunächst nacheinander auf und zeigen dann den Status an (Abschnitt 12). Blinkt die grüne LED in der ersten Minute langsam, startet das Gerät noch; warten Sie.
3. Nach etwa **1 Minute** erscheint das eigene WLAN-Netz des Geräts (`ION8BOOT_xxxxxx`).

5.2 Verbindung mit dem Geräte-WLAN

1. Scannen Sie **QR-Code 1** auf dem Etikett mit einem Telefon oder wählen Sie den **Namen des Geräte-WLANs** in der WLAN-Liste des Telefons / Computers. Geben Sie **das auf dem Etikett aufgedruckte Passwort** ein.
2. Bei den meisten Telefonen erscheint sofort nach dem Verbinden eine Meldung **„Im Netzwerk anmelden“** und das Panel des Geräts öffnet sich automatisch. Warnt das Telefon „Kein Internet in diesem Netzwerk“, wählen Sie **verbunden bleiben**.
3. Öffnet sich das Panel nicht von selbst, rufen Sie **http://192.168.4.1** im Browser auf oder scannen Sie **QR-Code 2** auf dem Etikett.

> **Wann ist das Geräte-WLAN eingeschaltet?**
> Sobald das Gerät mit dem Anlagennetz verbunden ist, schaltet sich das Geräte-WLAN standardmäßig ab. Es schaltet sich nach jedem Einschalten für die ersten 10 Minuten wieder ein sowie dann, wenn das Anlagennetz verloren geht (Abschnitt 6.3).

5.3 Einrichtungsassistent

Solange im Gerät kein Administrator angelegt ist, öffnet sich das Panel mit dem **Einrichtungsassistenten**. Jeder Schritt kann übersprungen werden; Sie können später über die Seite **Settings** zum Assistenten zurückkehren. Bis die Einrichtung abgeschlossen ist, zeigt die obere Leiste die Warnung „Setup not complete“ (Einrichtung nicht abgeschlossen).

Schritt	Was Sie tun	Empfehlung
1. Administrator	Vollständiger Name und **PIN** (4–6 Ziffern)	6-stellige PIN für Administratoren
2. Gerät	**Gerätename** und **Standort**; erscheinen im Kopf jeder Benachrichtigung	Z. B. „Lagergebäude“ / „Versand“
3. Anlagen-WLAN	Netz mit Internetzugang für Benachrichtigungen (nur **2,4 GHz**); auch die Uhrzeit wird aus dem Internet bezogen	Abschnitt 6.1
4. Eingänge	Name und Alarmbedingung der verwendeten Eingänge: Off · Signal on (0→1) · Signal off (1→0) · On every change	Detaillierte Einstellungen in Abschnitt 8
5. Benachrichtigungsempfänger	Telegram-ID und/oder E-Mail-Adresse der Personen, die Alarme erhalten	Abschnitt 7
6. Testnachricht	Eine Testnachricht an jede Person; beantworten Sie die Frage „Ist sie angekommen?“	Abschnitt 5.4

Schritt	Was Sie tun	Empfehlung
7. Fertig	Zusammenfassung der Einrichtung und **Wiederherstellungscode**	Code notieren und an einem sicheren Ort aufbewahren

Ersteinrichtung nur über das eigene WLAN des Geräts

Solange kein Administrator angelegt ist, können Einstellungen nicht über das Anlagennetz geändert werden. So wird verhindert, dass jemand anderes im Netz ein nicht eingerichtetes Gerät übernimmt.

Der Assistent konfiguriert die Ausgänge nicht. Benennung, Test und Regeln der Ausgänge sind in Abschnitt 9 beschrieben.

5.4 Testnachricht

In Schritt 6 des Assistenten wird an jede Person eine Testnachricht gesendet, und Sie werden gefragt, ob sie angekommen ist. Folgen Sie bei einem Kanal ohne Zustellung dem Hinweis auf dem Bildschirm: Bei Telegram muss die Person im Benachrichtigungs-Bot **Start** gedrückt haben; bei E-Mail prüfen Sie den Junk-(Spam-)Ordner (Abschnitt 7). Die Testnachricht kann jederzeit erneut über die Seite **Notifications** → **Log** gesendet werden.

5.5 Wiederherstellungscode

Jedes Gerät hat einen eigenen 12-stelligen **Wiederherstellungscode** (Recovery Code). Wird die Administrator-PIN vergessen, wird mit diesem Code eine neue PIN festgelegt (Abschnitt 11.3). Der Code ändert sich auch bei einem vollständigen Zurücksetzen auf Werkseinstellungen nicht.

- **Anzeigen:** Bei Verbindung mit dem Geräte-WLAN als Administrator anmelden → **Settings** → **Recovery Code** → **Show code**.
- **Falls eine andere Person den Code erlangt hat:** an derselben Stelle **Generate new code**; der alte Code wird ungültig.

Wiederherstellungscode aufbewahren

Notieren Sie den Code und bewahren Sie ihn zusammen mit den Gerätedokumenten an einem sicheren Ort auf. Gehen sowohl der Code als auch die Administrator-PIN verloren, ist die einzige Möglichkeit, sich als Administrator am Panel anzumelden, ein vollständiges Zurücksetzen auf Werkseinstellungen.

6 Netzwerkverbindung

6.1 Anlagen-WLAN

Zum Senden von Benachrichtigungen und zur Uhrzeitsynchronisation muss das Gerät mit einem WLAN mit Internetzugang verbunden sein.

1. **Notifications** → **WiFi** (oder Schritt 3 des Einrichtungsassistenten) → **Scan Networks** → Netz auswählen → Passwort eingeben → **Connect**.
2. Nach dem Verbinden wird die Adresse des Geräts im Anlagennetz auf dem Bildschirm angezeigt; LED3 (gelb) leuchtet.

> **Nur 2,4 GHz**
> Das Gerät verbindet sich nur mit **2,4-GHz**-Netzen; 5 GHz wird nicht unterstützt. Verwendet Ihr Router denselben Namen für 2,4 und 5 GHz und treten Verbindungsprobleme auf, richten Sie für 2,4 GHz einen eigenen Namen ein.

Wird das gespeicherte Netz nicht gefunden, versucht das Gerät es zunächst häufig, dann seltener erneut (höchstens alle 5 Minuten).

6.2 Zugriff auf das Panel aus dem Anlagennetz

Sobald das Gerät mit dem Anlagen-WLAN verbunden ist, werden **zwei Adressen** zum Aufruf des Panels als anklickbare und kopierbare Links angezeigt: unter **Notifications** → **WiFi** (Karte zum Verbindungsstatus), in den Schritten WLAN und „Fertig“ des Einrichtungsassistenten sowie in der Karte **Settings** → **WiFi**. Von einem Telefon oder Computer im selben Netz:

- **http://ion8-xxxxxx.local** (oder der von Ihnen vergebene Name, z. B. `http://lager.local`), oder
- die IP-Adresse des Geräts (z. B. `http://192.168.1.50`).

Manche Android-Telefone können `.local`-Namen nicht auflösen; verwenden Sie in diesem Fall die IP-Adresse.

Netzwerkname des Geräts (.local). Kann in der Karte **Notifications** → **WiFi** → **Network address** geändert werden. Zulässig sind nur Kleinbuchstaben, Ziffern und Bindestriche (max. 32 Zeichen; darf nicht mit einem Bindestrich beginnen oder enden). Türkische Zeichen werden automatisch umgewandelt (ş→s). Bleibt das Feld leer, wird der automatische Name (`ion8-xxxxxx`) verwendet. Vergeben Sie nicht zwei Geräten im selben Netz denselben Namen.

IP-Adresse: Automatisch / Statisch. Standard ist **Automatic** (der Router vergibt die Adresse, die sich mit der Zeit ändern kann). Bei Auswahl von **Static IP** geben Sie IP-Adresse, Subnetzmaske, Gateway und DNS ein; die Schaltfläche „Use current address“ füllt die Felder mit der aktuellen Adresse. Beim Speichern prüft das Gerät die Adresse im Netz und speichert sie nicht, wenn ein anderes Gerät sie verwendet. Das Gerät prüft die Adresse bei jedem Verbindungsaufbau erneut: Wird die Adresse von einem anderen Gerät verwendet oder hat sich das Netz geändert, wechselt es selbstständig auf automatische IP und zeigt oben im Panel eine Warnung an.

> **Empfohlen**
> Eine **DHCP-Reservierung** für das Gerät auf dem Router / DHCP-Server hält die Adresse fest und ist der zuverlässigste Weg. Geben Sie in Anlagen mit mehreren Geräten oder einer Integration jedem Gerät eine feste Adresse.

6.3 Geräte-WLAN und Passwort

Unter **Notifications** → **WiFi** → **Device WiFi** legen Sie fest, wie sich das eigene WLAN des Geräts verhält:

Option	Verhalten
Off while connected to the plant network (Standard)	Eingeschaltet in den ersten 10 Minuten nach jedem Einschalten, im Einrichtungsmodus, solange jemand mit dem Gerät verbunden ist und wenn das Anlagennetz länger als 30 Sekunden verloren ist; sonst ausgeschaltet
Always on	Das Geräte-WLAN sendet ständig
Hidden	Der Netzname erscheint nicht in der Liste; wer den Namen kennt, kann sich verbinden

Passwort des Geräte-WLANs ändern

Das Passwort auf dem Etikett dient der Ersteinrichtung. **Ändern Sie es nach der Einrichtung immer** und notieren Sie das neue Passwort: **Notifications → WiFi → Device WiFi → Device WiFi password** (auch im WLAN-Schritt des Einrichtungsassistenten verfügbar). Bis das Passwort geändert ist, zeigt das Panel eine Warnung an.

- Das Passwort ist 8–63 Zeichen lang; zulässig sind nur englische Buchstaben, Ziffern und Sonderzeichen. Das Werkspasswort vom Etikett und leicht zu erratende Passwörter werden nicht akzeptiert.
- Ändern Sie das Passwort, während Sie mit dem Geräte-WLAN verbunden sind, bricht die Verbindung nach einigen Sekunden ab; verbinden Sie sich mit dem neuen Passwort erneut.
- Versucht der Computer weiterhin das alte Passwort und zeigt einen Fehler, lassen Sie das Netz in der WLAN-Liste **entfernen** („Vergessen“) und verbinden Sie sich dann mit dem neuen Passwort (am Telefon: Netzwerk entfernen).
- Wenn das Passwort vergessen wurde: Abschnitt 11.4.

6.4 IT- und Firewall-Anforderungen

Das Gerät baut nur **ausgehende** Verbindungen auf; eingehende Verbindungen zum Gerät (Portweiterleitung) sind nicht erforderlich.

Dienst	Ziel	Port
Telegram-Benachrichtigung	api.telegram.org	TCP 443 (HTTPS)
E-Mail-Benachrichtigung	Versandserver (Herstellervorgabe oder Ihr eigener Server)	TCP 465 (SSL)
Uhrzeitsynchronisation	NTP-Server	UDP 123
Namensauflösung	DNS-Server Ihres Netzes	UDP/TCP 53
Webhook (falls verwendet)	Ihr Server	Port in der Adresse (HTTP / HTTPS)

Anforderungen an das lokale Netz. Für den Zugriff auf das Panel von Telefonen / Computern und damit sich die Geräte gegenseitig sehen (Seite Plant, Ausgangsregeln auf Basis eines anderen Geräts):

- Die Geräte und die Telefone / Computer, mit denen das Panel geöffnet wird, müssen sich **im selben Netz** befinden (derselbe Router, derselbe Adressbereich).
- **Die Client-Isolation muss** am Router / Access Point **ausgeschaltet sein** (AP-Isolation, Client-Isolation, „Gastnetz“). Ist sie eingeschaltet, öffnet sich das Panel nicht von Telefonen und die Geräte sehen sich gegenseitig nicht; Telegram- und E-Mail-Benachrichtigungen sind nicht betroffen. Bitten Sie in einem Unternehmensnetz das IT-Team um eine Ausnahme für die Alert-SCADA-Geräte (die MAC-Adresse des Geräts wird auf der Seite Plant angezeigt).
- Die Kommunikation zwischen Geräten erfolgt über lokalen **UDP-48230**-Broadcast; lokale Broadcasts dürfen nicht blockiert werden. Die Pakete sind mit dem Anlagenpasswort signiert (Abschnitt 10).

- Für `.local`-Adressen muss mDNS (UDP 5353) im Netz durchgelassen werden; andernfalls verwenden Sie die IP-Adresse.

> **Panel nicht ins Internet freigeben**
>
> Das Web-Panel verwendet unverschlüsseltes HTTP. Nutzen Sie das Panel nur in einem **vertrauenswürdigen Anlagennetz**; richten Sie keine Portweiterleitung ein. Ist ein Fernzugriff erforderlich, verwenden Sie ein VPN.

7 Personen und Benachrichtigungen

7.1 Rollen und Berechtigungen

- **Person:** ein Benutzer, der sich mit einer PIN am Panel anmelden kann und/oder Benachrichtigungen erhält (max. **32** Personen).
- **Rolle:** eine Gruppe von Personen, der Berechtigungen erteilt werden (max. **16** Rollen; z. B. Administrator, Schichtleiter, Techniker, Bediener). Alarme werden an Rollen oder an einzelne Personen geleitet.

Auf der Seite **Users** → **Roles** erhält jede Rolle folgende Berechtigungen:

Bezeichnung in der Oberfläche	Erlaubt
ACK	Alarme quittieren
Mute	Wiederholte Benachrichtigungen eines Alarms vorübergehend stoppen
Config	Alarmregeln, Ziele, Geräte- und Benachrichtigungseinstellungen; **Ausgänge von Hand schalten**
Add user	Personen hinzufügen / entfernen, Rollen und PINs zuweisen
Service (maintenance)	Serviceeinstellungen — nur autorisierter Service

Voller Administrator = Config + Add user. Einige Vorgänge (Ändern der quittierberechtigten Rolle, Einstellungen des Ausfallberichts, Zurücksetzen auf Werkseinstellungen) können nur von einem vollen Administrator ausgeführt werden.

> **Mindestens zwei Administratoren**
> Legen Sie mindestens **zwei** Administratoren mit PIN an; Administratoren sollten 6-stellige PINs verwenden. Das Gerät lässt das Löschen des letzten Administrators nicht zu.

7.2 Personen hinzufügen

Users → **People** → **Add person**: vollständiger Name, Rolle(n), PIN (falls sich die Person am Panel anmelden soll), Benachrichtigungskanäle (Telegram / E-Mail / Panel), Telegram-ID, E-Mail-Adresse, **Mindest-Schweregrad** (z. B. nur Critical erhalten) und **Arbeitszeiten** (außerhalb der Arbeitszeiten werden nur Alarme oberhalb des gewählten Schweregrads gesendet).

- Die PIN hat 4–6 Ziffern und wird im Gerät in nicht umkehrbarer Form gespeichert.
- Nach 5 falschen PIN-Eingaben wird die Anmeldung für diese Person 5 Minuten gesperrt. Die Sitzung wird nach 30 Minuten Inaktivität beendet.
- Jeder kann die eigene PIN, Telegram- / E-Mail-Angaben und Arbeitszeiten auf der Seite **Settings** → **My Account** ändern.

> **Neue Personen und Alarmziele**
> Eine neu hinzugefügte Person mit Telegram-ID oder E-Mail-Adresse, die noch Ziel keines Eingangs ist, wird automatisch den Alarmzielen aller Eingänge hinzugefügt. Eine später aus den Zielen entfernte Person wird nicht erneut geändert.

7.3 Benachrichtigungskonto und Telegram

Das Gerät wird **mit dem Benachrichtigungskonto des Herstellers einsatzbereit** geliefert: Ein Telegram-Benachrichtigungs-Bot und ein E-Mail-Absender sind bereits eingerichtet; ein separates Konto oder Abonnement ist

nicht erforderlich.

Für Telegram führt jede Person einmalig auf dem eigenen Telefon Folgendes aus:

1. Öffnet in Telegram **den Benachrichtigungs-Bot des Geräts** und drückt **Start**. Der Link zum Bot wird im Einrichtungsassistenten und auf der Seite **My Account** angezeigt. Einer Person, die dies nicht getan hat, kann der Bot keine Nachrichten senden (Regel von Telegram).

2. Ermittelt die eigene Telegram-ID: öffnet z. B. **@userinfobot**, drückt Start und kopiert die **Id**-Nummer aus der Antwort.

3. Trägt die Nummer in das Feld **Telegram ID** der Person ein (**Users** → **People** oder die Person selbst unter **Settings** → **My Account**).

7.4 E-Mail

Füllen Sie das Feld **E-Mail** der Person aus und schalten Sie den E-Mail-Kanal ein. Die ersten Nachrichten können im Junk-(Spam-)Ordner landen; bitten Sie die Empfänger, die Absenderadresse zu den sicheren Absendern hinzuzufügen. Wenn Sie Ihren eigenen E-Mail-Server verwenden möchten, wenden Sie sich an den autorisierten Service.

7.5 Ziele und Eskalation

- In der Tabelle **Alarm Settings** → **Targets** legen Sie fest, welche Rollen und Personen den Alarm jedes Eingangs erhalten.
- Ein nicht quittierter Alarm wird in den in der Einstellung **Escalation** des Eingangs festgelegten Abständen an höhere Ebenen weitergeleitet: bis zu **4 Stufen** einschließlich der ersten Benachrichtigung, jede Stufe mit bis zu 4 Rollen + 4 Personen. Beispiel: Bediener (0 min) → Schichtleiter (+10 min) → Instandhaltungsleiter (+20 min). Die Abstände legen Sie fest.
- Details: Benutzerhandbuch, „Schweregrad, Ziele und Eskalation“.

7.6 Test und Zustellprotokoll

- **Notifications** → **Log**: Senden Sie jeder Person eine **Test**nachricht. Alle Zustellungen, ihre Ergebnisse und etwaige Fehlerursachen werden hier angezeigt.
- Eine Benachrichtigung, die einer Person auf einem Kanal nicht zugestellt werden konnte, wird nur für diese Person und diesen Kanal wiederholt (**Notifications** → **General**: Anzahl der Wiederholungen 0–5).

8 Inbetriebnahme der Eingänge

Die Seite **Alarm Settings** → **Rules** enthält eine Zeile pro Eingang. Änderungen werden beim Drücken von **Save** in das Gerät geschrieben.

1. Geben Sie jedem verwendeten Eingang einen eindeutigen **Channel Name** (Kanalname, z. B. „Störung Kompressor 1“); dieser Name erscheint in Benachrichtigungen und im Panel.

2. Wählen Sie den **Trigger** (Auslöser): **Rising Edge** für einen Schließerkontakt (Alarm bei 0→1); **Falling Edge** oder einen Öffnerkontakt mit **Inverted Logic**, wenn der Wegfall des Signals der Alarm ist; **Both Edges** für Eingänge, die geöffnet / geschlossen melden sollen. Lassen Sie nicht verwendete Eingänge auf **Disabled**.

3. Wählen Sie die **Severity** (Schweregrad: Info · Warning · Alarm · Critical) und geben Sie bei Bedarf einen **Debounce**-Wert ein (Signalfilterung, 0–10.000 ms).

4. Lösen Sie jeden Eingang vor Ort **physisch** aus: Prüfen Sie im Panel, dass sich der richtige Kanal in der richtigen Richtung ändert und die Benachrichtigung ankommt.

Alle Eingangsoptionen (selbsthaltender Alarm, automatische Quittierung, Benachrichtigung bei Rückkehr in den Normalzustand, Texte) sind im Benutzerhandbuch beschrieben.

9 Inbetriebnahme der Ausgänge

> **Sicherheit vor Ort zuerst**
>
> Stellen Sie vor dem Testen der Ausgänge sicher, dass das Betätigen der angeschlossenen Betriebsmittel niemanden gefährdet. Informieren Sie das Personal vor Ort, bevor Sie Sirenen und Blitzleuchten testen.

9.1 Ausgänge benennen und von Hand testen

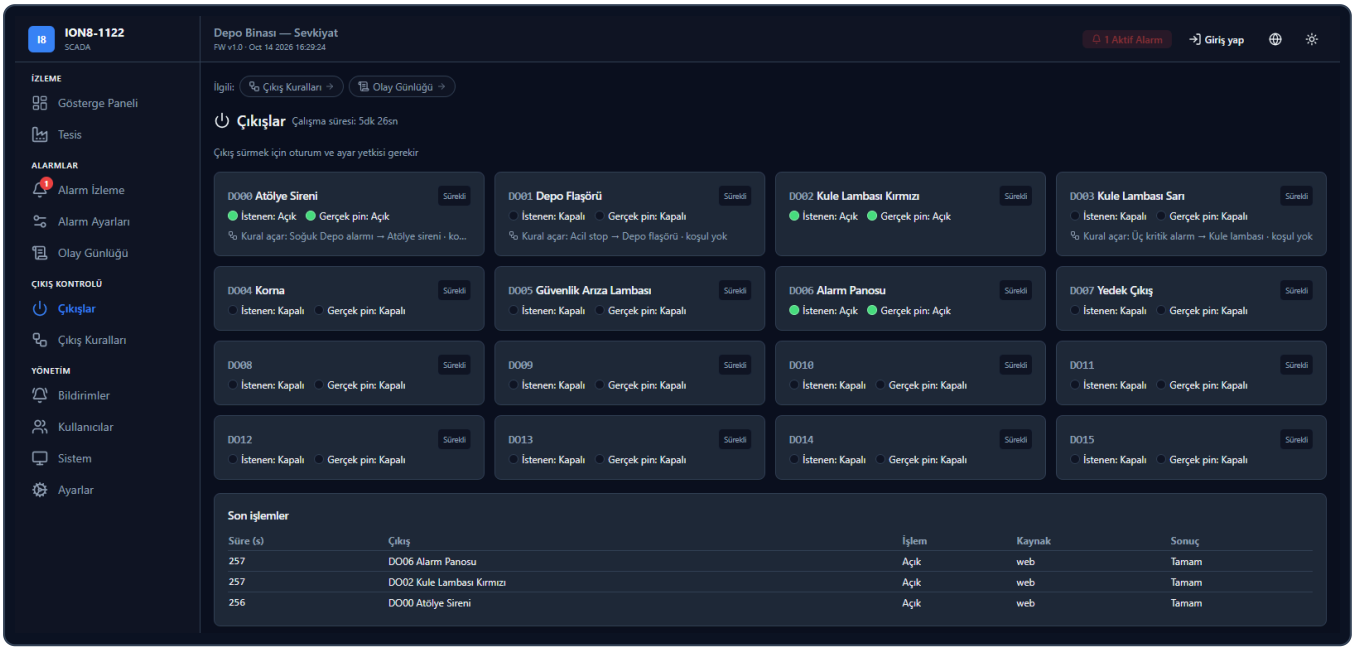
Um die Ausgänge zu schalten, müssen Sie angemeldet sein und Ihre Rolle muss die Berechtigung **Config** haben.

1. Drücken Sie auf der Seite **Outputs** bei jedem verwendeten Ausgang die Schaltfläche ⚙ **Settings** und vergeben Sie einen **Name** (z. B. „Werkstattsirene“, „Blitzleuchte Lager“).

2. Wählen Sie den **Mode**: **Continuous** (Dauerbetrieb; bleibt eingeschaltet, bis er ausgeschaltet wird) oder **Pulse** (Impuls; bleibt eine festgelegte Zeit eingeschaltet und schaltet dann ab; z. B. eine Hupe oder ein Rücksetztaster). Im Dauerbetrieb können Sie aus Sicherheitsgründen eine **Maximum on time** (maximale Einschaltdauer) festlegen.

3. Testen Sie den Ausgang mit **On / Off** (im Impulsbetrieb **Pulse**). Jeder Einschaltbefehl fragt eine Bestätigung ab.

4. Prüfen Sie, dass die Zustände **Requested** (angefordert) und **Actual pin** (tatsächlich) auf der Karte übereinstimmen und vor Ort das richtige Betriebsmittel arbeitet. Weichen sie ab, zeigt die Karte eine Warnung; prüfen Sie die Verdrahtung.



Seite Outputs (türkische Oberfläche): Name, angeforderter und tatsächlicher Zustand jedes Ausgangs, die ihn steuernde Regel; darunter die letzten Vorgänge.

9.2 Erste Ausgangsregel

Damit die Ausgänge automatisch abhängig von Alarmen arbeiten, werden auf der Seite **Output Rules** Regeln eingerichtet (Administratoranmeldung erforderlich). Am schnellsten geht es mit einer der vorgefertigten Vorlagen:

Vorlage	Funktion
Unacknowledged alarm → siren	Die Sirene bleibt eingeschaltet, solange ein Alarm auf Quittierung wartet; sie stoppt bei Quittierung
Critical alarm → output	Ausgang eingeschaltet, solange ein aktiver Alarm mit Schweregrad Critical besteht
Input → output	Ausgang eingeschaltet, solange ein Eingang aktiv ist
Other device's alarm → output	Ausgang hier eingeschaltet, solange ein anderes Alert-SCADA-Gerät der Anlage einen Alarm hat

Lesen Sie die Zeile **Summary** (Zusammenfassung) der Regel und drücken Sie **Save**. Alle Regeloptionen sind im Benutzerhandbuch beschrieben.

9.3 Test vor Ort

Testen Sie jede Ausgangsregel nach dem Einrichten vor Ort:

- Stellen Sie die Bedingung her (z. B. Eingang auslösen); prüfen Sie, dass der Ausgang einschaltet.
- Quittieren Sie den Alarm oder beenden Sie die Bedingung; prüfen Sie, dass der Ausgang abschaltet.
- Gibt es eine Wartungs- / Unterdrückungsregel (KEEP OFF), prüfen Sie, dass der Ausgang nicht einschaltet, solange sie aktiv ist.
- Testen Sie einen Stromausfall: Schalten Sie das Gerät aus und wieder ein; prüfen Sie, dass alle Ausgänge ausgeschaltet starten und die Regeln die Ausgänge anschließend wieder entsprechend den Bedingungen ansteuern.

10 Mehrere Geräte: Anlage

Befinden sich mehrere Alert-SCADA-Geräte (z. B. AS1111 und AS1122) im selben Anlagennetz, zeigt die Seite **Plant** (Anlage) alle Geräte und ihre Alarme auf einem Bildschirm. Ein Alarm an einem Gerät kann einen Ausgang eines anderen AS1122 ansteuern (z. B. lässt eine Störung im Lager die Leuchte im Pförtnerhaus aufleuchten). Es wird kein Server und keine Cloud benötigt; die Kommunikation zwischen den Geräten funktioniert auch ohne Internet.

1. Verbinden Sie alle Geräte mit **demselben Anlagen-WLAN**; stellen Sie sicher, dass **die Client-Isolation** am Router **ausgeschaltet ist** (Abschnitt 6.4).
2. Öffnen Sie auf jedem Gerät als Administrator **Plant → Plant settings** und geben Sie **auf allen Geräten dasselbe Anlagenpasswort** ein. Bis das Passwort geändert ist, zeigt die Seite die Warnung „Plant password is at factory value“ (Anlagenpasswort auf Werkswert).
3. Prüfen Sie auf der Seite Plant, dass alle Geräte als **online** angezeigt werden.

- Geräte akzeptieren nur Pakete von Geräten, die dasselbe Anlagenpasswort kennen.
- Sollen die Alarme dieses Geräts nicht von anderen Geräten aus quittiert werden, schalten Sie die Quittierung von anderen Geräten in **Plant settings** aus.
- Wird ein zuvor gesehenes Gerät 2 Minuten lang nicht gesehen, zeigt die Seite Plant eine Warnung mit möglichen Ursachen (Gerät aus, anderes Netz, Client-Isolation, anderes Anlagenpasswort). Ein dauerhaft entferntes Gerät wird mit der Schaltfläche **remove from list** in der Warnung gelöscht.

11 Sicherung, Werkseinstellungen und Wiederherstellung

11.1 Einstellungssicherung

Settings → **Settings backup** (Administrator):

- **Download backup:** Rollen, Personen, Alarmregeln, Ziele und Eskalation, Eingangsnamen und -texte, **Ausgangseinstellungen und Ausgangsregeln**, Benachrichtigungseinstellungen, Ausfallbericht, Gerätename und Anlageneinstellungen werden in eine einzige `.json`-Datei heruntergeladen. Kontaktdaten der Personen und das Anlagen-WLAN sind nur enthalten, wenn die entsprechenden Kästchen angekreuzt sind. **PINs sind nie enthalten.**
- **Restore:** Datei auswählen → Abschnitte ankreuzen → **Restore selected**. Kann auch im Einrichtungsmodus beim Einrichten eines neuen Geräts verwendet werden; vergeben Sie den neuen Personen ihre PINs auf der Seite **Users**. Ausgangsregeln, die sich auf ein anderes Gerät beziehen, werden nicht wiederhergestellt, wenn dieses Gerät nicht zu dieser Anlage gehört.

Sicherungsdatei schützen

Die Sicherungsdatei kann das WLAN-Passwort und Kontaktdaten von Personen enthalten; bewahren Sie sie sicher auf. Erstellen Sie am Ende der Inbetriebnahme und vor wichtigen Änderungen eine Sicherung.

11.2 Werkseinstellungen

Vorgang	Wo	Gelöscht	Beibehalten
Alarmeinstellungen zurücksetzen	**Alarm Settings**	Eingangsregeln, Kanalnamen, Texte, aktive Alarme	Personen, Benachrichtigungseinstellungen, Ziele
Vollständiges Zurücksetzen auf Werkseinstellungen	**Settings** (nur Administrator, nur über das Geräte-WLAN)	Personen, PINs, Rollen, Ziele, Benachrichtigungs- und WLAN-Einstellungen, Alarmregeln; optional das Ereignisprotokoll. Das Passwort des Geräte-WLANs wird auf das des Etiketts zurückgesetzt	Geräteidentität, Software, Wiederherstellungscode, Gerätename

Nach dem Zurücksetzen der Alarmeinstellungen

Nach dem Zurücksetzen der Alarmeinstellungen **löst kein Eingang mehr Alarme aus**; richten Sie die Eingänge neu ein.

Bei Übergabe des Geräts oder Einsendung zum Service

Erstellen Sie zuerst eine Einstellungssicherung und führen Sie dann ein **vollständiges Zurücksetzen auf Werkseinstellungen** mit angekreuztem **„Also delete event log“** (auch Ereignisprotokoll löschen) durch; personenbezogene Daten werden aus dem Gerät gelöscht.

11.3 Wenn die Administrator-PIN vergessen wurde

1. Verbinden Sie sich mit dem Geräte-WLAN (bei Bedarf das Gerät aus- und wieder einschalten und die ersten 10 Minuten nutzen).
2. **Sign in** → **I forgot my PIN** → Administratorkonto auswählen → **Wiederherstellungscode** und neue PIN eingeben.

3 Keine anderen Einstellungen ändern sich; der Vorgang wird in das Ereignisprotokoll geschrieben.

Die Wiederherstellung ist aus dem Anlagennetz nicht möglich (physische Nähe zum Gerät erforderlich). Nach 5 falschen Code-Eingaben gilt eine Wartezeit von 5 Minuten.

11.4 Wenn das Passwort des Geräte-WLANs vergessen wurde

- Ist das Gerät mit dem Anlagennetz verbunden, melden Sie sich aus dem Anlagennetz als Administrator am Panel an und legen Sie unter **Notifications** → **WiFi** → **Device WiFi** ein neues Passwort fest.
- Ist das Panel weder aus dem Anlagennetz noch über das Geräte-WLAN erreichbar, wenden Sie sich an den technischen Support (support@ionia-automation.com); halten Sie die Seriennummer bereit.

11.5 Software-Update

Updates werden vom **autorisierten Service** über WLAN durchgeführt. Die Pakete sind vom Hersteller signiert; das Gerät weist unsignierte oder beschädigte Pakete zurück. Neue Software wird erst dauerhaft übernommen, nachdem ihr korrekter Betrieb überprüft wurde. **Während des Updates werden alle Ausgänge freigegeben (abgeschaltet)**; nach dem Neustart des Geräts werden die Ausgänge wieder gemäß den Regeln angesteuert. Einstellungen und Aufzeichnungen bleiben bei einem Update erhalten.

12 Frontplatte: LEDs und Tasten

12.1 Status-LEDs

Beim Einschalten oder Neustart des Geräts leuchtet einige Sekunden lang nur die grüne LED. Danach leuchten die LEDs nacheinander auf (etwa 5 Sekunden) und zeigen dann den Status an:

LED	Farbe	Ein	Aus
LED4	Grün	Gerät arbeitet korrekt	Es liegt ein kritisches Problem vor (siehe LED1)
LED3	Gelb	Gerät ist mit dem Anlagen-WLAN verbunden	Kein Anlagen-WLAN oder nicht eingerichtet (Benachrichtigungen werden nicht gesendet)
LED2	Gelb	Speicherkarte eingesetzt und funktionsfähig	Keine Speicherkarte oder sie kann nicht gelesen werden
LED1	Rot	**Kritischer Fehler**: Die beiden Prozessoren des Geräts können nicht kommunizieren oder der Speicher ist auf kritischem Stand	Kein kritischer Fehler

- **Blinkt die grüne LED** in der ersten Minute nach dem Start **langsam**, startet das Gerät noch; warten Sie.
- **Leuchtet LED1**, starten Sie das Gerät neu (Abschnitt 12.2). Bleibt der Zustand bestehen, wenden Sie sich an den autorisierten Service.
- Während eines Vorgangs über die Tasten zeigen die LEDs dessen Fortschritt an; nach Abschluss kehren sie zur Statusanzeige zurück.

12.2 Tasten

Vorgang	Ausführung	Ergebnis
Neustart	**Mittlere Taste 10 Sekunden** gedrückt halten	Das Gerät startet neu; Einstellungen bleiben erhalten. Die Ausgänge schalten während des Neustarts ab

Ein Neustart ist auch über das Panel möglich: **System** → **Restart device** (das Panel ist etwa 1 Minute lang getrennt; die Ausgänge schalten während des Neustarts ab). Ein vollständiges Zurücksetzen auf Werkseinstellungen erfolgt über das Panel (Abschnitt 11.2).

13 Fehlerbehebung

Symptom	Mögliche Ursache	Abhilfe
Geräte-WLAN nicht sichtbar	Gerät ist mit dem Anlagennetz verbunden und im Modus „aus bei Verbindung“	Gerät aus- und wieder einschalten; in den ersten 10 Minuten ist es sichtbar. Oder aus dem Anlagennetz am Panel anmelden
Panel öffnet sich nicht aus dem Anlagennetz	Sie sind in einem anderen Netz / `.local` wird nicht aufgelöst	Im selben Netz sein; IP-Adresse versuchen
Mit dem Anlagennetz verbunden, aber das Panel öffnet sich auch mit der IP-Adresse nicht	Client-Isolation / Gastnetz am Router	Isolation ausschalten oder Gerät und Telefon mit dem Hauptnetz verbinden; im Unternehmensnetz die IT um eine Ausnahme bitten (Abschnitt 6.4)
„Initial setup only from the device's own WiFi…“	Kein Administrator angelegt	Über das Geräte-WLAN verbinden und den Assistenten abschließen
Keine Verbindung mit dem Anlagen-WLAN	5-GHz-Netz, falsches Passwort, schwaches Signal	2,4-GHz-Netz wählen; Passwort prüfen; Signal verbessern (Metallgehäuse)
Telegram-Nachricht kommt nicht an	Bot nicht gestartet, falsche ID, Kanal aus	Abschnitt 7.3; Fehlerursache unter **Notifications** → **Log** prüfen
E-Mail kommt nicht an	Spam-Ordner, falsche Adresse	Spam-Ordner und Adresse prüfen; Log prüfen
Einige Personen erhalten keine Nachrichten	Außerhalb der Arbeitszeiten + niedriger Schweregrad; Person ist kein Ziel	Arbeitszeiten- / Schweregrad-Einstellung der Person und Ziele des Eingangs
Ein Eingang löst nie einen Alarm aus	Eingang Disabled, falsche Triggerrichtung, Verdrahtung	**Alarm Settings** → **Rules**; Eingangszustand im Dashboard beobachten
Derselbe Eingang löst zu oft Alarme aus	Kontaktprellen / Störungen	Entprellzeit erhöhen; „Return to Normal — at least … s“ verwenden
Ausgang als eingeschaltet angezeigt, aber das Betriebsmittel arbeitet nicht	Verdrahtung, Lastversorgung, Koppelrelais	**Requested** und **Actual pin** auf der Karte vergleichen; Lastseite prüfen
Warnung „Requested and actual pin differ“	Problem im Ausgangskreis, Überlast	Laststrom prüfen (max. 100 mA); bleibt der Zustand bestehen, Service kontaktieren
„No connection to output modules“	Interne Geräteverbindung verloren; Ausgänge in den sicheren Zustand freigegeben	Gerät neu starten; hilft dies nicht, Service kontaktieren
„Module fault: DO0-7 / DO8-15“	Ein Ausgangsmodul meldet einen Fehler	Service kontaktieren
Seite Plant: „… device not seen for 2 minutes“	Gerät aus, anderes Netz oder Client-Isolation	Die Ursachen in der Warnung einzeln prüfen
Seite Plant: „plant password … differs“	Unterschiedliche Anlagenpasswörter auf den Geräten	Auf allen Geräten unter **Plant** → **Plant settings** dasselbe Passwort eingeben
Das Gerät startet von selbst neu	Versorgungsproblem	Versorgung prüfen; Ursache unter **System** → **Boot history** an den Service weitergeben
LED1 (rot) leuchtet	Kritischer Fehler	Gerät neu starten; bleibt der Zustand bestehen, Service kontaktieren

Symptom	Mögliche Ursache	Abhilfe
Warnung „Setup not complete“ verschwindet nicht	Administrator, Benachrichtigungsempfänger oder Anlagen-WLAN fehlt	**Settings → Setup wizard**

Halten Sie bei Kontakt mit dem Service bereit: die Seriennummer, einen Screenshot der Seite **System** und den Zeitpunkt, seit dem das Problem besteht.

14 Technische Daten (Übersicht)

Merkmal	Wert
Versorgung	24 V DC nominal, 15–30 V DC
Digitale Eingänge	16 (DI00–DI15); PNP, 24 V DC (logisch 1 ≥ 15 V); optisch isoliert, 2500 V
Eingangsabtastung	1 ms; Signalfilterung 0–10.000 ms je Eingang
Digitale Ausgänge	16 (DO00–DO15); plusschaltender (PNP-)Transistor, Ausgangsspannung folgt der Versorgung; max. 100 mA je Ausgang
Ausgangsbetriebsarten	Dauerbetrieb (optionale maximale Einschaltdauer) · Impuls (festgelegte Dauer, ratenbegrenzt)
Sicherer Zustand der Ausgänge	Ausgänge aus beim Start, während Software-Updates, bei Verlust der internen Verbindung und bei Stromausfall
Ausgangsregeln	Bis zu 16 Regeln; je Regel 8 Bedingungen, 4 ODER-Gruppen, 4 Ausgänge
Kommunikation	WLAN 2,4 GHz 802.11 b/g/n (kein 5 GHz); Client im Anlagennetz + eigener Access Point. Kein Ethernet / Mobilfunk
Benachrichtigung	Telegram · E-Mail · Webhook · Web-Panel
Benutzer	Bis zu 32 Personen, 16 Rollen; 4–6-stellige PIN je Person
Uhr	Synchronisation über das Internet (keine batteriegepufferte Uhr)
Montage	Schraubmontage auf ebener Fläche, im Schaltschrank; 4 × Ø3,8 mm
Abmessungen / Gewicht	115 × 114 × 45 mm / 250 g
Klemmen	Schraubklemmen
Gehäuse	Für die Montage im Schaltschrank; teilweiser Schutz gegen Staub, nicht gegen Wasser geschützt
Garantie	24 Monate ab Rechnungsdatum

15 Checkliste zur Inbetriebnahme

✓	Prüfung
☐	Versorgungs-, Eingangs- und Ausgangsanschlüsse hergestellt; Ausgangslasten nicht über 100 mA
☐	Etikettangaben (Seriennummer, Name des Geräte-WLANs) notiert
☐	**Passwort des Geräte-WLANs geändert**, neues Passwort notiert
☐	Administrator angelegt; **zweiter Administrator** angelegt

✓	Prüfung
☐	Wiederherstellungscode an einem sicheren Ort aufbewahrt
☐	Gerätename und Standort eingegeben
☐	Mit dem Anlagen-WLAN verbunden; Panel öffnet sich aus dem Anlagennetz; Gerät hat eine feste Adresse
☐	Verwendete Eingänge benannt, nicht verwendete Eingänge auf Disabled
☐	Jeder Eingang **physisch** ausgelöst; richtiger Kanal und richtige Richtung im Panel gesehen
☐	Personen hinzugefügt; Start im Telegram-Bot gedrückt; **Testnachrichten erhalten**
☐	Ziele und (bei Bedarf) Eskalation eingerichtet; ein Alarm quittiert und die Benachrichtigung „quittiert“ gesehen
☐	Ausgänge benannt und von Hand getestet; angeforderter und tatsächlicher Zustand stimmen überein
☐	Ausgangsregeln eingerichtet und **vor Ort getestet** (Einschalten, Abschalten, Unterdrückungsregeln)
☐	Bei mehreren Geräten: dasselbe Anlagenpasswort auf allen Geräten, alle auf der Seite Plant online
☐	(Empfohlen) Ausfallbericht eingeschaltet
☐	Einstellungssicherung heruntergeladen und an die Anlagenleitung übergeben
☐	Benutzer haben das Benutzerhandbuch und die Panel-Adresse erhalten

16 Garantie und Support

- **Garantie:** 24 Monate ab Rechnungsdatum gegen Material- und Verarbeitungsfehler. Die Garantie wird unter der Seriennummer erfasst. Die Bedingungen stehen im mit dem Produkt gelieferten Garantieschein.
- Installation und Nutzung entgegen den Anleitungen, Versorgungs- / Eingangs- / Ausgangswerte außerhalb der Grenzwerte, Überspannung, Wasser, Feuchtigkeit, Stöße, unbefugtes Öffnen des Gehäuses sowie Ausfälle von Diensten Dritter (Internet, Telegram, E-Mail) sind nicht von der Garantie abgedeckt.
- **Halten Sie bei einer Supportanfrage bereit:** die Seriennummer (Geräteetikett), die Rechnung, eine Fehlerbeschreibung und nach Möglichkeit einen Screenshot der Seite **System**. Erstellen Sie vor dem Einsenden des Geräts zum Service eine Einstellungssicherung und führen Sie ein vollständiges Zurücksetzen auf Werkseinstellungen durch.

Technischer Support: **support@ionia-automation.com** · Vertrieb und Informationen: **info@ionia-automation.com** · **ionia-automation.com**

Kontakt
Vertrieb und Information: info@ionia-automation.com
Technischer Support: support@ionia-automation.com
ionia-automation.com