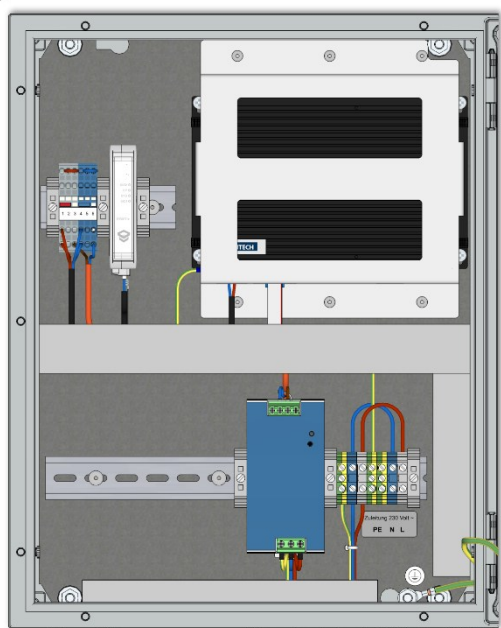


Betriebsanleitung *IRAS-SECURE*

Gefahrenmeldesystem



DE

IFAM GmbH Erfurt
Ingenieurbüro für die Anwendung
der Mikroelektronik
in der Sicherheitstechnik
Gustav-Weißkopf-Straße 9
D-99092 Erfurt
GERMANY
00 49 (0)361 65911 - 0
www.ifam-erfurt.de
ifam@ifam-erfurt.de

Inhaltsverzeichnis

1	Hinweise zu dieser Anleitung	- 13 -
1.1	Allgemeines	- 13 -
1.2	Gültigkeit der Anleitung	- 13 -
1.3	Mitgeltende Dokumente	- 14 -
1.4	Darstellungskonventionen	- 14 -
1.4.1	Verwendete Symbole – Text	- 14 -
1.4.2	Hinweise	- 14 -
1.4.3	Symbole/Zeichen – Hardware	- 15 -
1.4.4	Verweise auf Abbildungen	- 15 -
1.4.5	Handlungsbeschreibungen	- 15 -
1.4.6	Textformatierung	- 15 -
2	Sicherheit	- 16 -
2.1	Bestimmungsgemäße Verwendung	- 16 -
2.2	IRAS-Secure-Gefahrenmeldesystem	- 16 -
2.3	Elektrische Sicherheit	- 16 -
2.4	Umgang mit elektronischen Baugruppen	- 17 -
2.5	Personal – Qualifikation	- 17 -
2.6	Vorschriften (Arbeitsschutz/Umweltschutz)	- 18 -
2.7	Aufbau von Warnhinweisen	- 18 -
2.8	Klassifizierung von Gefahren	- 18 -
3	Lieferumfang	- 20 -
3.1	Prüfen des Systems/Zubehörs	- 20 -
4	Systembeschreibung	- 21 -
4.1	Überblick und Zweckbestimmung	- 21 -
4.2	Bestimmungsgemäße Verwendung	- 22 -
4.3	Nicht-bestimmungsgemäße Verwendung	- 22 -
4.4	Funktionale Komponenten	- 23 -
4.4.1	Kernfunktionen	- 23 -
4.4.2	Kommunikationsschnittstellen	- 23 -
4.5	Betrieb in Brandmeldeanlagen (BMA)	- 23 -
4.6	IRAS-SECURE – Systemaufbau/Baugruppen	- 24 -
4.6.1	Hardware	- 24 -
4.6.2	Funktionen	- 24 -
4.7	Systemerweiterungen	- 24 -
4.7.1	Weitere Informationen	- 26 -
4.7.2	Bestellung	- 26 -

4.8	Systemaufbau	- 27 -
4.9	Anschaltung der Baugruppen.....	- 28 -
4.10	Spannungsversorgung	- 29 -
4.10.1	Klemmblock IRAS-SECURE-Gefahrenmeldesystem	- 29 -
4.10.2	Klemmblock Baugruppen/Hardwareerweiterung.....	- 30 -
4.11	Metallgehäuse – Schließsystem	- 31 -
4.11.1	Magnetisch (Standard).....	- 31 -
4.11.2	Drehgriffe	- 32 -
4.11.3	Doppelbart	- 33 -
4.12	IRAS-SECURE-Industrie-PC	- 34 -
4.12.1	Übersicht	- 34 -
4.12.2	Schutzgitter/Siegel	- 35 -
4.13	ADP4000-IRAS	- 36 -
4.14	ADP4000	- 38 -
4.14.1	Übersicht	- 38 -
4.14.2	Schnittstellen/Anschlüsse	- 39 -
5	Montage	- 39 -
5.1	Sicherheit.....	- 39 -
5.2	Montagort und Betriebsbedingungen	- 39 -
5.3	Montage – Varianten	- 40 -
5.3.1	Wandmontage (direkt).....	- 40 -
5.3.1.1	Befestigungsmaterialien	- 41 -
5.3.2	Wandmontage (Wandhalterungen)	- 42 -
5.4	Montagehinweise.....	- 43 -
5.5	Erdung	- 44 -
5.6	ADP4000–IRAS	- 45 -
6	Installation.....	- 46 -
6.1	Sicherheit.....	- 46 -
6.2	IRAS-SECURE – Spannungsversorgung	- 47 -
6.2.1	USV-Modul	- 48 -
6.3	Integration in die Gefahrenmeldeanlage (GMA)	- 48 -
6.3.1	Integration in einen vorhandenen redundanten Ring	- 48 -
6.3.2	Neuaufbau eines redundanten Rings.....	- 49 -
6.3.3	Anschaltung – Prinzip.....	- 50 -
6.3.4	Anschaltung –Beispiele	- 50 -
6.3.4.1	IRAS-SECURE (allein) – Prinzip	- 51 -
6.3.4.2	IRAS-Secure + 1 Peripheriegerät (Beispiel)	- 52 -
6.3.5	Spannungsversorgung des ADP4000-IRAS.....	- 53 -

6.4	Netzwerk-Anbindung.....	53 -
6.5	Hardware-Erweiterungen (optional)	53 -
7	Inbetriebnahme	54 -
7.1	Sicherheit.....	54 -
7.2	IRAS-SECURE in Betrieb nehmen.....	54 -
7.3	Redundanter Ring – Einmessen der Komponenten	54 -
7.3.1	Ring-Komponenten einlesen.....	55 -
7.3.2	Ring-Komponenten einmessen.....	56 -
8	Konfiguration (GMA/Prog4000).....	57 -
8.1	Allgemeine Einstellungen (Allgemein).....	57 -
8.2	Relais konfigurieren.....	58 -
8.3	BMZ-Schnittstelle	58 -
8.4	Externe Schnittstelle (SEP)	59 -
8.5	Code-Tabellen-Editor	60 -
8.6	Text-Dialog-Editor.....	60 -
8.7	Schreiben der Konfiguration in das Gerät (Upload).....	61 -
8.8	Projekt sichern	62 -
9	Betrieb.....	63 -
9.1	Sicherheit.....	63 -
9.1.1	Datensicherheit.....	63 -
9.1.1.1	Zusätzliche Dokumente	63 -
9.1.2	Sichere Netzwerkverbindung.....	63 -
9.2	Datennutzung	63 -
9.2.1	Methoden zur Reduzierung der Datenmenge	64 -
9.3	IRAS-Website	65 -
9.3.1	Anmeldung.....	65 -
9.3.1.1	Erstanmeldung.....	66 -
9.3.2	Logout/automatische Abmeldung	67 -
9.3.2.1	Logout	67 -
9.3.2.2	Automatische Abmeldung	67 -
9.3.3	Systemzugang sichern.....	67 -
9.3.3.1	Passwort vergeben/ändern	68 -
9.3.3.2	Zwei-Faktor-Authentifizierung einrichten	68 -
9.3.3.3	Pin für Funktionstasten festlegen.....	69 -
9.3.3.4	Recovery Codes.....	70 -
9.3.4	Dashboard.....	71 -
9.3.4.1	Funktionsfelder.....	72 -
9.3.4.1.1	Ereignis-Status	72 -

9.3.4.1.2	Aktuell anstehenden Meldungen	- 72 -
9.3.4.1.3	Statistiken	- 73 -
9.3.4.1.4	Übersicht.....	- 74 -
9.3.4.1.5	Historie	- 74 -
9.3.4.1.6	Betriebsbuch.....	- 75 -
9.3.4.1.7	Features	- 76 -
9.3.4.1.8	Support und Feedback.....	- 78 -
9.3.4.1.9	Setup.....	- 79 -
9.3.4.1.10	System-Status	- 79 -
9.4	Konfiguration	- 81 -
9.4.1	Netzwerkverbindung.....	- 81 -
9.4.1.1	Ethernet	- 81 -
9.4.1.2	SSL/TLS konfigurieren	- 82 -
9.4.2	GMZ-Einstellungen.....	- 84 -
9.4.2.1	Geräteadresse und Protokoll.....	- 84 -
9.4.2.2	Erkundenzeit (optional)	- 85 -
9.4.3	Systemzeit einstellen.....	- 85 -
9.4.4	Ebenen definieren.....	- 86 -
9.4.5	Code-Tabelle	- 87 -
9.4.6	Gruppen verwalten	- 88 -
9.4.6.1	Gruppe anlegen	- 88 -
9.4.6.2	Gruppe konfigurieren	- 88 -
9.4.7	Benutzer verwalten.....	- 90 -
9.4.7.1	Benutzer anlegen.....	- 90 -
9.4.7.2	Benutzer konfigurieren.....	- 91 -
9.4.8	Medien verwalten.....	- 92 -
9.4.8.1	Laufkarten.....	- 92 -
9.4.8.1.1	Laufkarten hochladen.....	- 93 -
9.4.8.1.2	Laufkarten prüfen – SmartMap	- 98 -
9.4.8.1.3	Melderdatei importieren.....	- 99 -
9.4.8.1.4	Verknüpfung mit Meldepunkten	- 100 -
9.4.8.2	Zusätzliche Dokumente	- 101 -
9.4.8.2.1	Zusätzliche Dokumente hochladen	- 101 -
9.4.8.2.2	Verknüpfung mit Meldepunkten	- 102 -
9.4.8.2.3	Verknüpfung mit Laufkarten	- 102 -
9.4.8.3	IP-Kameras	- 103 -
9.4.8.3.1	Vorhandene Kameras verwalten	- 103 -
9.4.8.3.2	Neue Kamera anlegen	- 104 -

9.4.8.3.3	IP-Kamera mit Meldepunkt verknüpfen	- 107 -
9.4.9	Meldepunkte verwalten.....	- 108 -
9.4.9.1	Vorschau (Laufkarte)	- 109 -
9.4.9.2	Meldepunkt mit Dokumenten verknüpfen.....	- 110 -
9.4.9.3	Meldepunkt mit Kamera verknüpfen	- 111 -
9.4.9.4	Bereiche anlegen/verwalten	- 112 -
9.4.9.4.1	Übersicht.....	- 112 -
9.4.9.4.2	Bereich anlegen	- 113 -
9.4.10	Benachrichtigungs-/Ausgabeoptionen.....	- 116 -
9.4.10.1	E-Mail	- 116 -
9.4.10.1.1	Server-Einstellungen.....	- 116 -
9.4.10.1.2	Filter einrichten	- 118 -
9.4.10.2	SMS	- 119 -
9.4.10.3	Drucker	- 119 -
9.4.10.4	App.....	- 119 -
9.4.11	Bedienungsoptionen.....	- 120 -
9.4.11.1	Bedienung am FBF möglich.....	- 120 -
9.4.11.2	Gruppe in den Testbetrieb schalten möglich	- 120 -
9.4.11.3	Gruppen Ein-/Abschalten möglich.....	- 120 -
9.4.11.4	Steuergruppen ansteuern möglich.....	- 120 -
9.4.12	Erweiterungsfunktionen	- 120 -
9.5	Anwendung (Ereignisfall).....	- 121 -
9.5.1	IRAS-Website – Anmeldung	- 121 -
9.5.2	Ereignis-Meldungen	- 122 -
9.5.3	IRAS-App	- 124 -
9.5.4	E-Mail	- 124 -
9.5.5	Optionale Systemerweiterungen	- 124 -
9.6	IRAS-APP.....	- 125 -
9.6.1	Aktivierung von Darstellungsoptionen.....	- 125 -
9.6.2	Bedieneinstellungen	- 125 -
9.6.3	Push-Nachrichten.....	- 126 -
9.6.4	Betrieb (Anwender)	- 126 -
9.6.4.1	Objektübersicht	- 127 -
9.6.4.2	Neues Objekt hinzufügen	- 127 -
9.6.4.3	Objektstatus einsehen	- 128 -
9.7	Backup und Wiederherstellung.....	- 130 -
9.7.1	Backup erzeugen.....	- 130 -
9.7.2	System wiederherstellen.....	- 131 -

9.7.2.1	Vorhandene Backups	- 131 -
9.7.2.2	Upload (Datei)	- 131 -
9.8	Software-Update	- 132 -
9.8.1	Einstellungen	- 132 -
9.8.2	Verfügbare Updates	- 132 -
9.8.3	Manuelles Update	- 133 -
9.8.4	System-Updates	- 133 -
9.9	Systeminformation	- 134 -
10	Störungen/Störungsbeseitigung	- 135 -
10.1	Störungstabelle (häufige Störungen)	- 135 -
10.2	IRAS-Website	- 140 -
10.2.1	Dashboard – Störungsmeldungen	- 140 -
10.2.2	Diagnose	- 140 -
10.2.2.1	Supportzugriff aktivieren	- 141 -
10.2.2.2	Systemlogs	- 141 -
10.2.2.3	Selbsttest	- 141 -
10.2.3	Historie	- 144 -
10.2.4	Betriebsbuch (optional)	- 145 -
10.3	Hardware	- 145 -
10.3.1	ADP4000-IRAS – Diagnose-LEDs	- 145 -
10.3.2	ADP4000 – Diagnose-LEDs	- 146 -
10.4	Gefahrenmeldezentrale (GMZ)	- 147 -
10.5	Prog4000	- 147 -
11	Reset	- 148 -
11.1	IRAS-SECURE	- 148 -
11.2	ADP4000-IRAS	- 149 -
11.3	Prog4000	- 149 -
11.3.1	Geräteneustart	- 149 -
12	Firmware aktualisieren	- 150 -
12.1	Prog4000	- 150 -
13	Wartung	- 152 -
13.1	Allgemeine Empfehlungen	- 152 -
13.2	IRAS-Secure – Metallgehäuse	- 152 -
14	Außerbetriebnahme	- 153 -
14.1	Werksreset	- 153 -
15	Transport und Lagerung	- 154 -
16	Reparatur/Fehlerbehebung	- 154 -
17	Technische Daten	- 155 -

17.1	IRAS-SECURE	- 155 -
18	Produktidentifikation	- 156 -
18.1	Hardware	- 156 -
18.1.1	IRAS-SECURE (System) – Lieferinformationen.....	- 156 -
18.1.2	ADP4000-IRAS.....	- 157 -
18.2	Software	- 158 -
18.2.1	IRAS-Website/System.....	- 158 -
18.2.2	Prog4000	- 159 -
18.2.3	IRAS-App	- 160 -
18.2.4	Firmware (System4000-Geräte).....	- 160 -
19	Normen und Richtlinien	- 161 -
20	CE-Konformitätserklärung	- 161 -
21	Produktpass.....	- 161 -
22	Produktnummern	- 162 -
23	Unterstützungskonzept (Cybersicherheit)	- 162 -
24	Datensicherheit	- 164 -
25	Datenschutzerklärung	- 164 -
26	Support/Unterstützungszeitraum	- 166 -
27	Entsorgung.....	- 167 -
28	Gewährleistung und Garantie	- 167 -
29	Kontakt und Kundenservice.....	- 168 -
30	Urheberrecht	- 168 -
31	Lizenzhinweise	- 169 -
31.1	Pico]OS	- 169 -
31.2	Weitere Lizenzen	- 169 -
32	Glossar	- 171 -
33	Abkürzungsverzeichnis	- 172 -
34	Anhang	- 173 -
34.1	Geräte-/Montagemaße	- 173 -
34.1.1	IRAS-Secure – Montagemaße – Gehäuse/Wandmontage	- 173 -
34.1.2	IRAS-Secure – Gehäuse/Wandhalterung	- 174 -
34.2	CE-Konformitätserklärung.....	- 176 -

ABBILDUNGSVERZEICHNIS

ABBILDUNG 1: IRAS-SECURE – ÜBERSICHT	27 -
ABBILDUNG 2: IRAS-SECURE – ANSCHALTUNG DER BAUGRUPPEN	28 -
ABBILDUNG 3: IRAS-SECURE – KLEMMBLOCK, SPANNUNGSVERSORGUNG (230V-NETZ)	29 -
ABBILDUNG 4: IRAS-SECURE – KLEMMBLOCK/SPANNUNGSVERSORGUNG, HARDWAREERWEITERUNGEN	30 -
ABBILDUNG 5: IRAS-SECURE/METALLGEHÄUSE – SCHLIEßSYSTEM 1: MAGNETISCH	31 -
ABBILDUNG 6: IRAS-SECURE/METALLGEHÄUSE – SCHLIEßSYSTEM 2: DREHGRIFFE	32 -
ABBILDUNG 7: IRAS-SECURE/METALLGEHÄUSE – SCHLIEßSYSTEM 3: DOPPELBART	33 -
ABBILDUNG 8: IRAS-SECURE-INDUSTRIE-PC	34 -
ABBILDUNG 9: IRAS-SECURE-INDUSTRIE-PC – SCHUTZGITTER/VERSIEGELUNG	35 -
ABBILDUNG 10: ADP4000-IRAS	36 -
ABBILDUNG 11: ADP4000-IRAS – GERÄTE-SIEGEL	37 -
ABBILDUNG 12: ADP4000 – ÜBERSICHT	38 -
ABBILDUNG 13: ADP4000 – ANSCHLÜSSE	39 -
ABBILDUNG 14: GEHÄUSE – WANDMONTAGE (BEISPIELDARSTELLUNG)	40 -
ABBILDUNG 15: BEFESTIGUNGSMATERIAL/SCHRAUBE, UNTERLEGSCHIEBE, DICHTRING	41 -
ABBILDUNG 16: BEFESTIGUNGSMATERIAL/DICHTSCHIEBEN	41 -
ABBILDUNG 17: BEFESTIGUNGSMATERIAL/SELBSTDICHTENDE SCHRAUBEN	41 -
ABBILDUNG 18: GEHÄUSE – WANDHALTERUNGEN (BEISPIELDARSTELLUNG)	42 -
ABBILDUNG 19: IRAS-SECURE – GEHÄUSEMONTAGE	43 -
ABBILDUNG 20: IRAS-SECURE – ERDUNG/GEHÄUSE	44 -
ABBILDUNG 21: ADP4000-IRAS – MONTAGE/DEMONTAGE	45 -
ABBILDUNG 22: IRAS-SECURE – ANSCHLUSS 230V-NETZ (BEISPIELDARSTELLUNG)	47 -
ABBILDUNG 23: IRAS-SECURE – VORHANDENER REDUNDANTER RING/ADP4000 (BEISPIEL)	48 -
ABBILDUNG 24: IRAS-SECURE – VORHANDENER REDUNDANTER RING/PERIPHERIEGERÄT (BEISPIEL)	49 -
ABBILDUNG 25: IRAS-SECURE – REDUNDANTER RING/AD4000 UND IRAS-SECURE (BEISPIEL)	49 -
ABBILDUNG 26: ADP4000-IRAS – BEISPIEL-ANSCHALTUNG/ADP4000	51 -
ABBILDUNG 27: ADP4000-IRAS – BEISPIELANSCHALTUNG/1 PERIPHERIEGERÄT (BEISPIEL)	52 -
ABBILDUNG 28: INSTALLATION INDUSTRIE-PC/NETZWERK, MODEM	53 -
ABBILDUNG 29: PROG4000 – EINLESEN/ERKENNUNG (BEISPIEL)	55 -
ABBILDUNG 30: PROG4000 – SEP-EBENE (BEISPIEL)	56 -
ABBILDUNG 31: PROG4000 – ALLGEMEIN (BEISPIEL)	57 -
ABBILDUNG 32: PROG4000 – RELAIS (BEISPIEL)	58 -
ABBILDUNG 33; PROG4000 – BMZ-SCHNITTSTELLE (BEISPIEL)*	58 -
ABBILDUNG 34: PROG4000 – EXTERNE SCHNITTSTELLE (SEP)	59 -
ABBILDUNG 35: PROG4000 – CODE-TABELLEN-EDITOR (BEISPIEL)	60 -
ABBILDUNG 36: PROG4000 – TEXT-DIALOG-EDITOR (BEISPIEL)	60 -
ABBILDUNG 37: PROG4000 – KONFIGURATION SCHREIBEN (BEISPIEL)	61 -
ABBILDUNG 38: PROG4000 – GERÄTEKONFIGURATION SCHREIBEN/STATUS	61 -
ABBILDUNG 39: PROG4000 - UPLOAD	62 -
ABBILDUNG 40: PROG4000 – PROJEKT SICHERN (BEISPIEL)	62 -
ABBILDUNG 41: IRAS-WEBSITE – LOGIN	65 -
ABBILDUNG 42: IRAS-WEBSITE – LOGIN/SICHERHEIT	65 -
ABBILDUNG 43: IRAS-WEBSITE – PASSWORT ÄNDERN	66 -
ABBILDUNG 44: IRAS-WEBSITE – SITZUNG VERLÄNGERN	67 -
ABBILDUNG 45: IRAS-WEBSITE – DASHBOARD/PASSWORT, PIN	67 -
ABBILDUNG 46: IRAS-WEBSITE – PASSWORT/PIN ÄNDERN	68 -
ABBILDUNG 47: IRAS-WEBSITE – TOTP EINRICHTEN (BEISPIEL)	69 -
ABBILDUNG 48: IRAS-WEBSITE – PIN/FUNKTIONSTASTEN FESTLEGEN (BEISPIEL)	70 -
ABBILDUNG 49: IRAS-WEBSITE – DASHBOARD (BEISPIEL)	71 -
ABBILDUNG 50: IRAS-WEBSITE – DASHBOARD/STATUSZEILE, KEINE MELDUNG	72 -
ABBILDUNG 51: IRAS-WEBSITE – DASHBOARD/STATUSZEILE, MELDUNGEN (BEISPIEL)	72 -
ABBILDUNG 52: IRAS-WEBSITE – AKTUELLE MELDUNGEN (BEISPIEL)	72 -
ABBILDUNG 53: IRAS-WEBSITE – STATISTIKEN/ÜBERSICHT	73 -
ABBILDUNG 54: IRAS-WEBSITE – STATISTIKEN, MELDUNGS-HISTORIE (BEISPIEL)	73 -
ABBILDUNG 55: IRAS-WEBSITE – ÜBERSICHT	74 -
ABBILDUNG 56: IRAS-WEBSITE – HISTORIE/ÜBERSICHT	74 -
ABBILDUNG 57: IRAS-WEBSITE – HISTORIE/BEISPIEL	75 -
ABBILDUNG 58: IRAS-WEBSITE – BETRIEBSBUCH/ÜBERSICHT (BEISPIEL)	75 -

ABBILDUNG 59: IRAS-WEBSITE – BETRIEBSBUCH/LISTE (BEISPIEL)	- 76 -
ABBILDUNG 60: IRAS-WEBSITE – FEATURES.....	- 76 -
ABBILDUNG 61: IRAS-WEBSITE - FEATURES/ÜBERSICHT	- 77 -
ABBILDUNG 62: IRAS-WEBSITE – SUPPORT/FEEDBACK	- 78 -
ABBILDUNG 63: IRAS-WEBSITE – SUPPORT/FEEDBACK, FORMULAR	- 78 -
ABBILDUNG 64: IRAS-WEBSITE – SETUP	- 79 -
ABBILDUNG 65: IRAS-WEBSITE – SYSTEMSTATUS/ÜBERSICHT	- 79 -
ABBILDUNG 66: IRAS-WEBSITE – SYSTEMSTATUS/BEISPIEL	- 79 -
ABBILDUNG 67: IRAS-WEBSITE – ETHERNET/LAN-SCHNITTSTELLE	- 81 -
ABBILDUNG 68: IRAS-WEBSITE – SSL	- 82 -
ABBILDUNG 69: IRAS-WEBSITE – SSL/AKTIV	- 83 -
ABBILDUNG 70: IRAS-WEBSITE – BMZ-EINSTELLUNGEN.....	- 84 -
ABBILDUNG 71: IRAS-WEBSITE – SYSTEMZEIT EINSTELLEN	- 85 -
ABBILDUNG 72: IRAS-WEBSITE – EBENEN (BEISPIEL).....	- 86 -
ABBILDUNG 73: IRAS-WEBSITE – CODETABELLE (BEISPIEL)	- 87 -
ABBILDUNG 74: IRAS-WEBSITE – NEUE GRUPPE.....	- 88 -
ABBILDUNG 75: IRAS-WEBSITE – GRUPPE/ÜBERSICHT	- 88 -
ABBILDUNG 76: IRAS-WEBSITE – NEUER BENUTZER	- 90 -
ABBILDUNG 77: IRAS-WEBSITE – BENUTZER/ÜBERSICHT	- 91 -
ABBILDUNG 78: IRAS-WEBSITE – VERFÜGBARE LAUFKARTEN/MELDEPUNKTE (BEISPIEL)	- 92 -
ABBILDUNG 79: IRAS-WEBSITE – DOKUMENTE/LIMIT	- 93 -
ABBILDUNG 80: IRAS-WEBSITE – LAUFKARTEN/UPLOAD, KLASSISCH.....	- 94 -
ABBILDUNG 81: IRAS-WEBSITE – LAUFKARTEN/UNTERSTÜTZT/AUSWAHL (BEISPIEL)	- 95 -
ABBILDUNG 82: IRAS-WEBSITE – LAUFKARTEN/UNTERSTÜTZT/ANALYSE (BEISPIEL).....	- 96 -
ABBILDUNG 83: IRAS-WEBSITE – LAUFKARTEN/UNTERSTÜTZT/KORREKTUR (BEISPIEL)	- 96 -
ABBILDUNG 84: IRAS-WEBSITE – LAUFKARTEN/UNTERSTÜTZEN/UPLOAD (BEISPIEL)	- 97 -
ABBILDUNG 85: IRAS-SECURE – SMARTMAP	- 98 -
ABBILDUNG 86: IRAS-WEBSITE – MELDERDATEIEN IMPORTIEREN.....	- 99 -
ABBILDUNG 87: IRAS-WEBSITE – OPTIONALE DOKUMENTE VERWALTEN	- 101 -
ABBILDUNG 88: IRAS-WEBSITE – OPTIONALE DOKUMENTE/VERKNÜPFUNG	- 102 -
ABBILDUNG 89: IRAS-WEBSITE – IP-KAMERAS (BEISPIEL).....	- 103 -
ABBILDUNG 90: IRAS-WEBSITE – IP-KAMERA/EIGENSCHAFTEN ANPASSEN	- 104 -
ABBILDUNG 91: IRAS-WEBSITE – IP-KAMERA ANLEGEN	- 104 -
ABBILDUNG 92: IRAS-WEBSITE – IP-KAMERA/OHNE BENUTZERAUTHENTIFIZIERUNG	- 104 -
ABBILDUNG 93: IRAS-WEBSITE – IP-KAMERA MIT AUTHENTIFIZIERUNG	- 105 -
ABBILDUNG 94: IRAS-WEBSITE – IP-KAMERA/BESTE QUALITÄT UND KOMPROMISS	- 105 -
ABBILDUNG 95: IRAS-WEBSITE – IP-KAMERA/WENIG VERZÖGERUNG	- 106 -
ABBILDUNG 96: IRAS-WEBSITE – MELDEPUNKTE/ÜBERSICHT.....	- 108 -
ABBILDUNG 97: IRAS-WEBSITE – MELDEPUNKT/VORSCHAU.....	- 109 -
ABBILDUNG 98: IRAS-WEBSITE – MELDEPUNKT/DOKUMENTE	- 110 -
ABBILDUNG 99: IRAS-WEBSITE – MELDEPUNKT/KAMERA.....	- 111 -
ABBILDUNG 100: IRAS-WEBSITE – BEREICHE/ÜBERSICHT	- 112 -
ABBILDUNG 101: IRAS-WEBSITE – BEREICH/NEU ANLEGEN.....	- 113 -
ABBILDUNG 102: IRAS-WEBSITE – BEREICH/NEU ANLEGEN/SMARTMAP	- 114 -
ABBILDUNG 103: IRAS-WEBSITE – MELDEPUNKTE/BEREICHE ZUORDNEN 1	- 114 -
ABBILDUNG 104: IRAS-WEBSITE – MELDEPUNKTE/BEREICHE ZUORDNEN 2	- 115 -
ABBILDUNG 105: IRAS-WEBSITE – E-MAIL/SERVER	- 116 -
ABBILDUNG 106: IRAS-WEBSITE – E-MAIL/FILTER	- 118 -
ABBILDUNG 111: IRAS-WEBSITE – OPTIONEN/BEDIENUNG	- 120 -
ABBILDUNG 112: IRAS-WEBSITE – DASHBOARD/EREIGNISFALL (BEISPIEL)	- 121 -
ABBILDUNG 113: IRAS-WEBSITE – DASHBOARD/STATUSZEILE, KEINE MELDUNG	- 122 -
ABBILDUNG 114: IRAS-WEBSITE – DASHBOARD/STATUSZEILE, VORLIEGENDE MELDUNGEN (BEISPIEL)	- 122 -
ABBILDUNG 115: IRAS-WEBSITE – AKTUELLE EREIGNISSE/EBENE FEUER (BEISPIEL).....	- 122 -
ABBILDUNG 116: IRAS-WEBSITE – EREIGNISMELDUNG/LAUFKARTE	- 123 -
ABBILDUNG 117: IRAS-WEBSITE – EREIGNISMELDUNG/ZUSÄTZLICHES DOKUMENT.....	- 123 -
ABBILDUNG 118: IRAS-WEBSITE – EREIGNISMELDUNG/KAMERA	- 124 -
ABBILDUNG 119: IRAS-WEBSITE – IRAS-APP.....	- 125 -
ABBILDUNG 120: IRAS-WEBSITE – BEDIENUNG/EINSTELLUNGEN	- 125 -
ABBILDUNG 121: IRAS-WEBSITE – PUSH-NACHRICHTEN.....	- 126 -

ABBILDUNG 122: IRAS-APP – STARTBILDSCHIRM.....	- 126 -
ABBILDUNG 123: IRAS-APP – OBJEKTÜBERSICHT	- 127 -
ABBILDUNG 124: IRAS-APP – NEUES OBJEKT ERSTELLEN	- 127 -
ABBILDUNG 125: IRAS-APP – OBJEKTSTATUS/KEINE MELDUNGEN (BEISPIEL).....	- 128 -
ABBILDUNG 126: IRAS-APP – OBJEKTSTATUS/VORLIEGENDE MELDUNGEN – EBENE „STÖRUNG“ (BEISPIEL) -	128 -
ABBILDUNG 127: IRAS-APP – KAMERAS (BEISPIEL).....	- 129 -
ABBILDUNG 128: IRAS-WEBSITE – SICHERUNG	- 130 -
ABBILDUNG 129: IRAS-WEBSITE – UPDATE/EINSTELLUNGEN.....	- 132 -
ABBILDUNG 130: IRAS-WEBSITE – VERFÜGBARE UPDATES	- 132 -
ABBILDUNG 131: IRAS-WEBSITE – MANUELLES UPDATE	- 133 -
ABBILDUNG 132: IRAS-WEBSITE – SYSTEM-UPDATES MANUELL PRÜFEN (BEISPIEL)	- 133 -
ABBILDUNG 133: IRAS-WEBSITE – SYSTEMINFORMATIONEN.....	- 134 -
ABBILDUNG 134: IRAS-WEBSITE – DASHBOARD/STÖRUNG (BEISPIEL).....	- 140 -
ABBILDUNG 135: IRAS-WEBSITE – AKTUELLE EREIGNISSE/STÖRUNGEN (BEISPIEL)	- 140 -
ABBILDUNG 136: IRAS-WEBSITE – DIAGNOSE (BEISPIEL).....	- 141 -
ABBILDUNG 137: IRAS-WEBSITE – SELBSTTEST (BEISPIEL).....	- 141 -
ABBILDUNG 138: IRAS-WEBSITE – STÖRUNGSBESEITIGUNG/HISTORIE.....	- 144 -
ABBILDUNG 139: ADP4000 – DIAGNOSE-LEDS	- 146 -
ABBILDUNG 141: IRAS-WEBSITE – SYSTEM-RESET	- 148 -
ABBILDUNG 142: PROG4000 – GERÄTENEUSTART	- 149 -
ABBILDUNG 143: PROG4000 – FIRMWARE-UPDATE 1 (BEISPIEL)	- 150 -
ABBILDUNG 144: PROG4000 – FIRMWARE-UPDATE 2 (BEISPIEL)	- 150 -
ABBILDUNG 145: IRAS-WEBSITE – WERKSRESET	- 153 -
ABBILDUNG 146: IRAS-SECURE – LIEFERINFORMATIONEN (BEISPIEL)	- 156 -
ABBILDUNG 147: ADP4000-IRAS – TYPENSCHILD (BEISPIEL)	- 157 -
ABBILDUNG 148: IRAS-WEBSITE – SYSTEMINFORMATION	- 158 -
ABBILDUNG 149: PROG4000 – VERSIONSNUMMER (BEISPIEL) - PLATZHALTER	- 159 -
ABBILDUNG 150: IRAS-APP – VERSIONSNUMMER	- 160 -
ABBILDUNG 151: IFAM-WEBSITE – SICHERHEITSINFORMATIONEN.....	- 162 -
ABBILDUNG 152: IFAM-WEBSITE – AKTUELLE SICHERHEITSINFORMATIONEN.....	- 163 -
ABBILDUNG 153: IFAM-WEBSITE – SICHERHEITSINFORMATIONEN/DETAILS (BEISPIEL).....	- 163 -
ABBILDUNG 154: IRAS-WEBSITE – LIZENZEN	- 169 -
ABBILDUNG 155: IRAS-SECURE – GEHÄUSE/WANDMONTAGE MAßZEICHNUNG (VORDERANSICHT).....	- 173 -
ABBILDUNG 156: IRAS-SECURE – GEHÄUSE/WANDHALTERUNG, BEMAßUNG (VORDERANSICHT).....	- 174 -
ABBILDUNG 157: IRAS-SECURE – GEHÄUSE/WANDHALTERUNG, BEMAßUNG (SEITENANSICHT)	- 175 -
ABBILDUNG 158: IRAS-SECURE – CE-KONFORMITÄTSEKTLÄRUNG 1	- 176 -

Tabellenverzeichnis

TABELLE 1: VERWENDETE SYMBOLE	- 15 -
TABELLE 2: KLASSIFIZIERUNG VON GEFAHREN.....	- 19 -
TABELLE 3: IRAS-SECURE – ERWEITERUNGSOPTIONEN	- 25 -
TABELLE 4: STÖRUNGSÜBERSICHT	- 139 -
TABELLE 5: IRAS-WEBSITE - SELBSTTEST/FEHLERMELDUNGEN.....	- 144 -
TABELLE 6: ADP4000-IRAS – DIAGNOSE-LEDS/STÖRUNGSERKENNUNG.....	- 145 -
TABELLE 7: ADP4000 – DIAGNOSE-LEDS/STÖRUNGSERKENNUNG	- 146 -
TABELLE 8: TECHNISCHE DATEN – IRAS-SECURE	- 155 -
TABELLE 9: GLOSSAR	- 171 -
TABELLE 10: ABKÜRZUNGSVERZEICHNIS.....	- 172 -

1 Hinweise zu dieser Anleitung

1.1 Allgemeines



Die vorliegende Betriebsanleitung ist Teil des IRAS-SECURE-Gefahrenmeldesystems.

Heben Sie sie für zukünftige Verwendungen auf. Das Dokument muss bei Betreiber- bzw. Besitzerwechsel weitergegeben werden und bei allen Arbeiten am/mit dem Gerät verfügbar sein. Lesen Sie diese Anleitung vor Beginn der Installation gründlich durch.

Diese Anleitung richtet sich an alle, die IRAS-SECURE (nachfolgend auch als Gefahrenmeldesystem bezeichnet) montieren, installieren, konfigurieren und betreiben. Sie enthält alle notwendigen Informationen, um einen korrekten Betrieb sicherzustellen.

Die Gesamtdokumentation besteht aus den folgenden Dokumenten:

Betriebsanleitung IRAS-SECURE: umfassende Informationen zur Basisversion des Gefahrenmeldesystems und dessen Montage, Installation, Konfiguration und Betrieb.

Betriebs-/Installationsanleitung Erweiterungsoptionen: optionsabhängige Informationen u.a. zu Montage, Installation, Konfiguration und Betrieb der das Basissystem erweiternden Baugruppen/Komponenten.

Beachten Sie alle enthaltenen Anweisungen und Sicherheitshinweise sowie die Inhalte der mitgeltenden Dokumente.

Die IFAM GmbH Erfurt lehnt jede Haftung für Schäden (Personen-, Sach- und Umweltschäden) ab aufgrund von:

- Nichtbeachten der Inhalte dieser Anleitung,
- Nichtbeachten der Inhalte mitgeltender Dokumente,
- Nichtbeachten der enthaltenen Sicherheits- und Warnhinweise,
- bestimmungswidriger Verwendung.

Versuchen Sie auftretende Probleme mit Hilfe dieser Dokumentation zu lösen. Sollten Sie darüber hinaus weitere Fragen haben, wenden Sie sich bitte an den Kundendienst der IFAM GmbH Erfurt.

Der Inhalt dieses Dokuments wurde sorgfältig, unter Berücksichtigung der geltenden Normen und Richtlinien und auf dem aktuellen Stand der Technik erstellt. Es können jedoch zwischenzeitlich technische Änderungen an den Geräten/am Zubehör vorgenommen werden, ohne dass dies gesondert mitgeteilt wird. Informieren Sie sich ggf. auf unserer Homepage bzw. über die Informationsmedien möglicher weiterer genannter Hersteller.

1.2 Gültigkeit der Anleitung

Diese Anleitung gilt ausschließlich für die von der Firma IFAM GmbH Erfurt gelieferten Geräte und deren Zubehör und nur in Verbindung mit den mitgeltenden Dokumenten.

1.3 Mitgeltende Dokumente

Beim Betrieb des IRAS-SECURE-Gefahrenmeldesystems und der zugehörigen Anwendungen in einer vorhandenen Brandmeldeanlage müssen weitere Dokumente berücksichtigt werden. Die vorliegende Betriebsanleitung gilt daher nur in Verbindung mit folgenden Dokumenten:

- Dokumentation der ggf. zu betreibenden Erweiterungsoption*,
- Betriebsanleitung System4000*,
- Technische Information System4000 – M4-Schnittstellenmodule*,
- Konfigurationsanleitung Prog4000*,
- Quickstart – System4000 redundant,
- Hinweisblatt zum Dokumentendownload/IFAM-Website*,
- herstellereigene Dokumentation der Gefahrenmeldeanlage/Gefahrenmeldezentrale,
- herstellereigene Dokumentation der ggf. vorhandenen Hardware-Erweiterungen.
- herstellereigene Montagehinweise für das Drehgriff-Schließsystem/Doppelbart-Schließung (RITTAL).

Beachten Sie alle dort enthaltenen Angaben und Hinweise zu den Geräten/zum Zubehör, insbesondere zu Sicherheit, Montage, Installation und Betrieb, um mögliche Risiken zu minimieren und Gefahren von Verletzungen und Sachschäden zu vermeiden und einen sicheren Betrieb des Gerätes bzw. des Systems zu gewährleisten.

* Die Dokumente der IFAM GmbH Erfurt können (sofern nicht Teil der Lieferung) über die Homepage bezogen (www.ifam-erfurt.de/de/service-support/downloads) oder auf Anfrage auch in gedruckter Form zur Verfügung gestellt werden.

1.4 Darstellungskonventionen

1.4.1 Verwendete Symbole – Text



Querverweis auf eine andere Textstelle des Dokuments, z.B. Kapitel, Abbildung oder Tabelle. In der elektronischen Version (PDF) findet sich an dieser Stelle ein Hyperlink.



Verweis auf ein mitgeltendes/weiteres Dokument.



Verweis auf eine normative oder Rechtsquelle.

1.4.2 Hinweise

Hinweise auf zusätzliche Informationen/Präzisierungen sowie auf Informationen, die nicht unmittelbar für das Funktionieren der Geräte/Systeme oder die Ausführung einer Handlung oder eines Handlungsschrittes erforderlich sind, erfolgen in dieser Form:



Informationstext

Hinweise auf zusätzliche, für das Funktionieren der Geräte/Systeme notwendige, Informationen erfolgen in dieser Form:



Informationstext

1.4.3 Symbole/Zeichen – Hardware

Im IRAS-SECURE-Gefahrenmeldesystem bzw. auf dessen Komponenten finden sich Hinweise, die ggf. durch Symbole ergänzt werden:

Symbol/Zeichen	Erklärung
	Vorsicht im Umgang mit elektronischen Baugruppen. Gefahr der Beschädigung durch elektrostatische Entladung (ESD).
	Erdungspunkt
	Entsorgungshinweis: Nicht im Hausmüll entsorgen. Separate Trennung und Entsorgung nach Material-Gruppen erforderlich. 👉 <i>Siehe Kapitel 27 Entsorgung.</i>

Tabelle 1: Verwendete Symbole

1.4.4 Verweise auf Abbildungen

Bildverweise, u.a. in Form von Positionsnummern (Pos) beziehen sich auf die einem Textabschnitt/Kapitel jeweils vorangestellten oder in den jeweiligen Abschnitt eingebetteten Abbildungen (z.B. Kapitel „Verdrahtung“ auf die Darstellung des Verdrahtungsvorgangs).

Liegen abweichend davon weitere Verweise vor, sind diese durch einen entsprechenden Bezug kenntlich gemacht; ggf. gefolgt von einer Positionsnummer (z.B. **Abbildung 2/4**).

1.4.5 Handlungsbeschreibungen

Anweisungen zum Ausführen von Tätigkeiten werden in einer nummerierten, aufsteigenden Reihenfolge der aufeinander folgenden Arbeitsschritte dargestellt.

Folgen bzw. Zustände, die aus einer Handlung resultieren, werden mit dem Symbol „→“ an die jeweilige Anweisung angeschlossen.

Beispiel:

1. Drücken Sie die Reset-Taste. → Das Gerät startet neu.
2. Schließen Sie den PC über die USB-Schnittstelle an das Gerät an.
3. Starten Sie das Konfigurationsprogramm.
4. ...

1.4.6 Textformatierung

Verweis auf Elemente des IRAS-SECURE-Gefahrenmeldesystems (Hard-/Software)	Großschreibung/unterstrichen Beispiel: <u>DASHBOARD</u>

2 Sicherheit

Beachten Sie vor Beginn der Arbeiten alle in diesem Kapitel gegebenen Sicherheitshinweise sowie die Warnhinweise, die den Kapiteln und Handlungen ggf. vorangestellt sind. Ein Nichtbeachten kann zu Verletzungen von Personen, Sachschäden, Schäden für die Umwelt und zur Beeinträchtigung der Funktion der Geräte/des Systems führen.



Beachten Sie bei allen Arbeiten am/beim Betrieb des IRAS-SECURE-Gefahrenmeldesystems die Sicherheits- und Warnhinweise in den **mitgeltenden Dokumenten!**

➞ *Siehe Kapitel 1.3 Mitgeltende Dokumente.*

2.1 Bestimmungsgemäße Verwendung

Informationen zur bestimmungsgemäßen bzw. nicht-bestimmungsgemäßen Verwendung finden Sie ➞ *in den Kapiteln 4.2 Bestimmungsgemäße Verwendung und 4.3 Nicht-bestimmungsgemäße Verwendung.*

2.2 IRAS-Secure-Gefahrenmeldesystem

- IRAS-Secure darf nicht mit unter direkter Sonneneinstrahlung betrieben werden.
- IRAS-Secure darf nicht in unmittelbarer Nähe von Heizkörpern oder Heizelementen betrieben werden.
- IRAS-Secure darf nur unter den zugelassenen Umgebungsbedingungen betrieben werden. ➞ *Siehe Kapitel 17 Technische Daten.*
- Verwenden Sie ein geeignetes Sicherheitsprotokoll (SSL/HTTPS), um eine sichere Kommunikation zu gewährleisten.

Zur Einrichtung ➞ *siehe Kapitel 9.4.1.2 SSL/TLS konfigurieren.*

2.3 Elektrische Sicherheit

- Verwenden Sie die Geräte nur wie in dieser Anleitung beschrieben.
- Betreiben Sie die Geräte nur mit den angegebenen technischen Parametern.
- Nehmen Sie keine Änderungen an den Geräten vor.
- Prüfen Sie die Geräte 1x monatlich auf Beschädigungen.
- Führen Sie Arbeiten an/mit den Geräten nur im spannungsfreien Zustand durch. Trennen Sie die elektrischen Geräte vor Beginn der Arbeiten von der Stromversorgung.
- Montieren bzw. installieren Sie keine defekten bzw. beschädigten Geräte oder Teilkomponenten.
- Nehmen Sie niemals defekte bzw. beschädigte Geräte und Zubehörteile in Betrieb.
- Setzen Sie sich bei Beschädigungen/bei Reparaturbedarf mit dem Kundendienst der IFAM GmbH Erfurt in Verbindung.
- Führen Sie keine eigenmächtigen Reparaturen an den Geräten durch.
- Reparaturen dürfen nach Rücksprache mit der IFAM GmbH Erfurt nur durch eine ausgebildete Elektrofachkraft und nur in dem ausdrücklich autorisierten Umfang ausgeführt werden.
- Verwenden Sie für die Reparatur ausschließlich Originalersatzteile.
- Verwenden Sie nur die von der IFAM GmbH Erfurt zugelassenen Zubehörteile.
- Bringen Sie die Geräte nicht mit Wasser oder anderen Flüssigkeiten in Berührung.
- Verwenden Sie die Geräte nicht in feuchten Umgebungen.

- Verwenden Sie die Geräte und das elektrische Zubehör nie auf nassen Oberflächen oder im Außenbereich.
- Lagern Sie die Geräte in einer trockenen und staubfreien Umgebung.
- Transportieren/tragen Sie die Geräte nie an vorhandenen Anschlussleitungen/Kabeln oder Datenleitungen.
- Führen Sie keine spitzen Gegenstände in die Geräte (Kontakte) ein.
- Achten Sie darauf, dass Kabel nicht geknickt, eingeklemmt, überfahren werden,
- Bringen Sie die Geräte nicht mit Hitzequellen oder scharfen Kanten in Berührung.

2.4 Umgang mit elektronischen Baugruppen

Im Umgang mit Geräten, die elektronische Bauteile enthalten, z.B. Adaptern und Aufsteckmodulen, sind folgende Hinweise zu beachten:



ACHTUNG!

Gefahr der Zerstörung der elektronischen Komponenten!

Die von der IFAM GmbH Erfurt gelieferten Baugruppen enthalten elektronische Komponenten, die bei unsachgemäßem Gebrauch aufgrund elektrostatischer Entladung (ESD) beschädigt werden können.

- Beachten Sie beim Umgang mit den Baugruppen stets die Anforderungen der ESD-Norm EN 61340-5-1.
- Treffen Sie vor Beginn der Arbeiten stets Maßnahmen zur Ableitung vorhandener statischer Elektrizität.

2.5 Personal – Qualifikation

Allgemeine Arbeiten

Alle Arbeiten dürfen nur durch qualifiziertes Fachpersonal ausgeführt werden. Fachpersonal in diesem Sinne sind (entsprechend DIN VDE 0833-1, 2.13-2.15):

- Elektrofachkraft GMA,
- Eingewiesene Person,
- Sachkundige Person GMA.

Elektrofachkraft GMA

Person, die aufgrund ihrer fachlichen Ausbildung, Kenntnisse und Erfahrungen ... der einschlägigen Normen und Bestimmungen die übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann.

Ausbildung: Nachrichten-, Informations-, Mikroprozessor-, Mess-, Regel- oder der allgemeinen Elektrotechnik.

Aufgaben: Errichten und Instandhalten nach Anforderungen. Inspektion, Wartung, Begehungen.

Eingewiesene Person

Person, die in die für den Betrieb einer GMA erforderlichen Aufgaben eingewiesen wurde und in der Lage ist, selbstständig die Bedienung der GMA vorzunehmen, Einflüsse auf die Überwachungsmaßnahmen ... zu erkennen und eigenverantwortlich ... Inspektion und Störungsbeseitigung zu veranlassen.

Aufgaben: Abschaltungen, Mängelbeseitigung, Beauftragung. Bedienung und Begehungen.

Sachkundige Person GMA

Person, die durch eine Elektrofachkraft für GMA über die übertragenen Aufgaben und die möglichen Gefahren und Folgen bei unsachgemäßem Verhalten unterrichtet wurde und der die baulichen Kenntnisse für die Beurteilung der Objektvoraussetzungen ... belehrt wurde.
Aufgaben: Dokumentationen, Mängel ins Betriebsbuch, Meldung an die Fachfirma. Begehungen.

Alle Personen müssen eine zur Installation/Reparatur von Brandmelde- und Löschanlagen inkl. zugehörigen Komponenten befähigende Ausbildung absolviert haben bzw. die Berechtigung besitzen, Stromkreise und Geräte/Systeme gemäß den Standards der Sicherheitstechnik in Betrieb zu nehmen, zu erden und zu kennzeichnen.

2.6 Vorschriften (Arbeitsschutz/Umweltschutz)

Beachten Sie bei allen Arbeiten am/mit dem Gefahrenmeldesystem und dessen Zubehör die geltenden Arbeits- und Umweltschutz-Vorschriften:

- Gesetzliche Vorschriften zur Unfallverhütung,
- Gesetzliche Vorschriften zum Umweltschutz,
- Berufsgenossenschaftliche Bestimmungen.

2.7 Aufbau von Warnhinweisen

Warn-/Gefahrenhinweise sind an einer herausgehobenen Formatierung erkennbar. Sie können Teil der einzelnen Kapitel sein und stehen in Verbindung mit Handlungs- und/oder Anwendungssituationen.

Der Aufbau folgt nachfolgendem Prinzip:

**SIGNALWORT!****Art und Quelle der Gefahr.**

Erklärung zu Art und Quelle der Gefahr.

- Maßnahmen zur Abwendung bzw. Vermeidung der Gefahr.

2.8 Klassifizierung von Gefahren

Warn-/Gefahrenhinweise folgen festgelegten, nach dem jeweiligen Gefährdungsgrad durchgeführten Abstufungen von Gefahren, die sich in einer bestimmten Umgebung/Situation bzw. während der Ausführung von Tätigkeiten ergeben können.

Hierbei kann es sich um Gesundheitsgefährdungen und/oder Sachschäden oder Beeinträchtigung der Funktionstüchtigkeit von Geräten/Systemen handeln.

Gefahrenzeichen	Signalwort	Erläuterungen
	GEFAHR!	Das Signalwort bezeichnet eine Gefährdung mit einem hohen Risikograd, die eine schwere Verletzung oder den Tod zur Folge hat, wenn sie nicht gemieden wird.
	WARNUNG!	Das Signalwort bezeichnet eine Gefährdung mit einem mittleren Risikograd, die den Tod oder eine schwere Verletzung zur Folge haben kann, wenn sie nicht vermieden wird.
	ACHTUNG!	Das Signalwort bezeichnet das Risiko von Sachschäden und/oder Schäden für die Umwelt und/oder die Beeinträchtigung des Funktionierens von Geräten/Systemen mit mittelbaren und unmittelbaren Folgen.

Tabelle 2: Klassifizierung von Gefahren

3 Lieferumfang

Der Lieferumfang variiert entsprechend der individuellen Kundenbestellung (IRAS-SECURE, Hardware-Erweiterungen, Zubehör u.a.).

Überprüfen Sie nach dem Auspacken der Lieferung den Inhalt auf Vollständigkeit. Gleichen Sie den Lieferumfang ggf. mit dem Bestellumfang ab.

Lieferumfang (Beispiel):

- IRAS-SECURE-Gefahrenmeldesystem:
 - Metallgehäuse (+2 Magnetschlüssel und zusätzliches Montagezubehör),
 - IRAS-SECURE-Netzteil,
 - IRAS-SECURE-Industrie-PC,
 - ADP4000-IRAS,
 - IRAS-SECURE-Website (+Zugangsdaten).
 - IRAS-SECURE-App,
- Erweiterungsoptionen (entsprechend Kundenbestellung),
- Konfigurationssoftware *Prog4000*,
- Quickstart – System4000 redundant,
- Hinweisblatt Dokumentendownload.

IRAS-SECURE wird im vormontierten Zustand ausgeliefert, d.h. die Baugruppen sind bereits montiert und betriebsbereit verkabelt.



Für die Integration des IRAS-SECURE in eine vorhandene Gefahrenmeldeanlage (GMA) ist der Redundanzadapter *ADP4000* erforderlich. **Das Gerät ist nicht Bestandteil des Systems.**

Falls Sie noch nicht über ein solches Gerät verfügen, wenden Sie bitte an unseren Vertrieb.



Die Konfigurationssoftware *Prog4000* und die *IRAS-SECURE APP* sind physisch nicht im Lieferumfang enthalten (CD oder USB-Stick).

Prog4000: Laden Sie die Programme im Download-Bereich der Homepage der IFAM-GmbH Erfurt herunter: www.ifam-erfurt.de/service-support/downloads.

IRAS-SECURE-App: Laden Sie die App im App-Store des jeweils verwendeten Betriebssystems herunter (z.B. Microsoft Store, Apple, Google).

Für die Inbetriebnahme bzw. den Betrieb ist weiteres Zubehör erforderlich, das nicht im Lieferumfang enthalten ist:

- Befestigungsmaterial (Wandmontage),
- LAN-Anschlusskabel (Verbindung mit Betreiber Netzwerk/Internet).
- Standard-USB-Kabel mit Mini-B-USB-Anschluss (für ADP4000 – Anschluss eines PCs).
- Netzanschluss-Teile – elektrischer Anschluss/230V-Netz.

3.1 Prüfen des Systems/Zubehörs

Überprüfen Sie nach dem Auspacken der Lieferung den Inhalt/die Komponenten und das Zubehör auf Unversehrtheit (z.B. physische Beschädigungen, korrekte Platzierung).

Prüfen Sie darüber hinaus:

- IRAS-Secure-Industrie-PC: korrekt im Gehäuse befestigt, Schutzgitter ordnungsgemäß befestigt, Siegel, unversehrt.

- ADP4000-IRAS: Siegel unversehrt.
- Anschlusskabel der Baugruppen: fest verbunden.
- Transportsicherung: vorhanden, in korrekter Position.

Falls ein Lieferbestandteil unvollständig ist oder Beschädigungen aufweisen, wenden Sie sich bitte an den Kundenservice der IFAM GmbH Erfurt.

➞ *Siehe Kapitel 29 Kontakt und Kundenservice.*

4 Systembeschreibung

4.1 Überblick und Zweckbestimmung

Das IRAS-SECURE-Gefahrenmeldeanlage ist ein serverbasiertes Informations- und Managementsystem für Gefahrenmeldesysteme. Es wird innerhalb des Verantwortungsbereichs des Betreibers im zu überwachenden Objekt installiert und betrieben.

Das System dient der zentralen Erfassung, Verarbeitung, Speicherung, Visualisierung und Weiterleitung von Zustands- und Ereignisinformationen innerhalb angeschlossener sicherheitstechnischer Systeme gleicher und/oder unterschiedlicher Hersteller.

IRAS-SECURE verbindet verschiedene Informationsquellen, Kommunikationswege und Endgeräte zu einem gemeinsamen Informationssystem. Hierdurch werden Informationen aus den angeschlossenen Gefahrenmeldeanlagen zentral bereitgestellt und autorisierten Nutzern zur Verfügung gestellt.

Das System unterstützt insbesondere folgende Anwendungszwecke:

- Personen- und Gebäudeschutz durch anlagentechnischen Brandschutz,
- Schnelle und zielgerichtete Informationsübermittlung,
- Visualisierung von Ereignissen und Anlagenzuständen,
- Unterstützung von Interventionskräften bei Informationsbeschaffung,
- Dokumentation von Betriebs-, Instandhaltungs- und Prüfvorgängen,
- Unterstützung organisatorischer Abläufe im organisatorischen Brandschutz.

Typische Informationsquellen sind:

- Bedienelemente von System4000-Komponenten (z. B. ABT4000, FBF4000, GMT4000),
- Eingangsbaugruppen des System4000 (z. B. IMT4-IN, IMT4000-CPU),
- Brandmelderzentralen und Einbruchmeldezentralen,
- Drucker über SNMP,
- Kamerasysteme.

Die bereitgestellten Informationen können insbesondere durch Betreiber, Instandhalter, Sicherheitsdienste und Interventionskräfte genutzt werden. Sie dienen der Unterstützung von Entscheidungen, der Einsatzplanung, der Einsatzdurchführung sowie der Dokumentation von Ereignissen und Zuständen.

Je nach Anlagenkonfiguration können Informationen über lokale Netzwerke, Fernzugriffe oder weitere Kommunikationswege übertragen werden.

IRAS-Secure ist eine Ergänzung oder Erweiterung bestehender Gefahrenmeldeanlagen. Das System ersetzt weder die sicherheitsrelevanten Funktionen angeschlossener Brandmelde-, Einbruchmelde- oder sonstiger Gefahrenmeldeanlagen noch gegebenenfalls

normativ geforderte Erstinformationssysteme. Die primären Detektions-, Alarmierungs- und Schutzfunktionen verbleiben bei den jeweils angeschlossenen Systemen.

Installation, Konfiguration, Instandhaltung und Betrieb erfolgen durch den Betreiber oder durch vom Betreiber beauftragte qualifizierte Fachkräfte.

4.2 Bestimmungsgemäße Verwendung

- IRAS-SECURE ist als zusätzliches Informationssystem zur Verarbeitung und Weiterleitung von Meldungen einer Gefahrenmeldeanlage (GMA) konzipiert.
- Das System und sein Zubehör dürfen ausschließlich in Gefahrenmeldeanlagen, z.B. in Brandmeldeanlagen (BMA) oder Einbruchmeldeanlagen, eingesetzt werden.
- Es ist für die Integration innerhalb eines redundanten Rings konzipiert.
- IRAS-SECURE darf nur innerhalb einer geschützten IT-Infrastruktur betrieben werden.
- Es dürfen nur die vom Hersteller freigegebenen Hard- und Softwarekomponenten und Kommunikationsschnittstellen verwendet werden.
- Installation, Konfiguration, Wartung und Betrieb erfolgen durch den Betreiber oder durch vom Betreiber beauftragte qualifizierte Fachkräfte, entsprechend den ggf. vorliegenden/gültigen Wartungsvorschriften/-plänen.
- Verwenden Sie nur die beschriebenen Funktionen und Kommunikationsschnittstellen.
 *Siehe Kapitel 4.4 Funktionale Komponenten.*
- Montieren, installieren und betreiben Sie die Geräte und deren Zubehör nur im unbeschädigten Zustand und ausschließlich wie in dieser Anleitung und den mitgelieferten Dokumenten beschrieben.

4.3 Nicht-bestimmungsgemäße Verwendung

Eine von der im Kapitel „Bestimmungsgemäße Verwendung“ abweichende Verwendung ist unzulässig.

IRAS-SECURE darf nicht als eigenständige Brandmeldeanlage, Einbruchmeldeanlage oder sonstige sicherheitsrelevante Steuerungseinrichtung eingesetzt werden.

Es darf nicht als Erstinformationsmittel (gemäß DIN 14662) zum Einsatz kommen.

Der Betrieb darf nicht außerhalb der vom Hersteller spezifizierten Einsatzbedingungen erfolgen.

Das Gefahrenmeldesystem darf nur mit den zugelassenen technischen Parametern betrieben werden.

Die System-Baugruppen sowie die mitgelieferten Zubehörteile dürfen weder in ihren Eigenschaften verändert, noch umgebaut werden. Sollten nicht autorisierte Änderungen vorgenommen werden, ist eine sichere Verwendung nicht mehr möglich. Der Gewährleistungsanspruch erlischt.

Darüber hinaus gilt die Nichtbeachtung der Inhalte dieser Anleitung sowie der mitgelieferten Dokumente als nicht-bestimmungsgemäße Verwendung.

4.4 Funktionale Komponenten

4.4.1 Kernfunktionen

- Visualisierung von Ereignissen (BMZ-Nr., Meldergruppen, Gerätetypen, Zusatztexte, Statistiken).
- Benachrichtigung per E-Mail, SMS und mobile App gemäß Ereignistyp (Feuer, Störung, Abschaltung, technischer Alarm etc.).
- Archivierung und Export der Ereignis- und Prüf-Historie
- Ereignisgesteuerter Ausdruck von Feuerwehrinformationen (Laufkarten, Feuerwehrpläne).
- Anzeigen und Verwaltung von Anlagendokumenten (z. B. Feuerwehrpläne, Laufkarten, Sonderpläne, Meldekette).
- Redundanz im Verbindungsserver, Netzwerkverbindung und Anschaltung zur Brandmeldezentrale (BMZ).
- App-Funktionalität für Anzeige, Information und FAT/BBF-Anzeige und Bedienung, inkl. Quittierung.

4.4.2 Kommunikationsschnittstellen

- HTTPS (TLS-gesicherter Zugriff),
- HTTP (nicht empfohlen, jedoch aus Gründen der Kompatibilität vorhanden),
- SMTP (E-Mail-Benachrichtigung),
- SNMP (Drucker Überwachung),
- API-Zugriffe (offen dokumentierte, herstellerspezifische Schnittstelle / proprietäre API)
- Anbindung externer Endgeräte über Mobilfunk / Internet (Konnektivität kundenspezifisch),
- Anbindung an Gefahrenmeldezentrale über redundante Protokolle.

4.5 Betrieb in Brandmeldeanlagen (BMA)

Beachten Sie alle sich aus normativen und rechtlichen Vorgaben ergebenden Aspekte/Pflichten zum Betrieb und zur Wartung in einer Brandmeldeanlage.



IRAS Secure darf in Brandmeldeanlagen nicht als Erstinformationsmittel gemäß DIN14675 / DIN14661 / DIN14662 verwendet werden!

Es darf nur als **zusätzliches** Gerät zur Anzeige und Übermittlung von Zuständen/Meldungen einer BMA Anwendung finden.

4.6 IRAS-SECURE – Systemaufbau/Baugruppen

IRAS-Secure umfasst in der Standardversion folgende Komponenten:

4.6.1 Hardware

- IRAS-SECURE-Industrie-PC,
- ADP4000-IRAS,
- IRAS-SECURE-Netzteil,
- IRAS-SECURE-Metallgehäuse mit Schließsystem,
- Klemmblocks, Spannungsversorgung.

Eine umfassende Beschreibung der Baugruppen finden Sie  [ab Kapitel 4.8 Systemaufbau](#).

4.6.2 Funktionen

Die Beschreibung des Funktionsumfangs (Konfiguration, Bedienung, Ausgabeoptionen u.a.) von IRAS-SECURE finden Sie in  [Kapitel 9 Betrieb](#).

4.7 Systemerweiterungen

Es besteht die Möglichkeit, das Gefahrenmeldesystem mit folgenden Optionen zu erweitern:

Symbol	Erweiterung	Beschreibung
 IRAS-SECURE-Drucksystem	<u>IRAS-SECURE-Drucksystem</u> Softwareerweiterung mit Sonder-Bedienfeld	Ereignisgesteuerter Sofortausdruck mit manuellem Nachdruck durch ein Sonder-Bedienfeld im Gehäuse.
 IRAS-SECURE-Druck	<u>IRAS-SECURE-Druck</u> Softwareerweiterung	Bereitstellung von Daten für den Anschluss eines Netzwerkdruckers und Ausdruck von PDF-Dokumenten (z.B. Feuerwehr-Laufkarten).
 IRAS-SECURE-Mobile	<u>IRAS-SECURE-Mobile</u> Hard- und Softwareerweiterung	Übertragung der Gefahrenmeldung mittels Mobilfunkmodul (nicht redundant).
 IRAS-SECURE-Mobile-Redundant	<u>IRAS-SECURE-Mobile-Redundant</u> Hard- und Softwareerweiterung	Redundante Bereitstellung von Übertragungswegen mittels LAN, WLAN, Mobilfunk (2 x SIM).
 IRAS-SECURE-500	<u>IRAS-SECURE-500</u> Softwareerweiterung	Webbasierendes Gefahrenmeldesystem bis 500 Datenpunkte.
 IRAS-SECURE-Max	<u>IRAS-SECURE-Max</u> Softwareerweiterung	Webbasierendes Gefahrenmeldesystem bis 250.000 Datenpunkte.
 IRAS-SECURE-Dienste	<u>IRAS-SECURE-Dienste</u> Softwareerweiterung	Weiterleitung von GMA-Ereignissen an Dienstleister (z.B. FOXTAG) ohne ADP4000-WEB-Link.
 IRAS-SECURE-Display	<u>IRAS-SECURE-Display</u> Softwareerweiterung für 5 Displays	Gefahrenmeldung für Betreiber und z.B. Feuerwehr auf Panel- und Netzwerk-PCs des Kunden.
 IRAS-SECURE-SmartMap	<u>IRAS-SECURE-SmartMap</u> Softwareerweiterung	KI-gestützte Inbetriebnahme und Laufkartenimport für IRAS-SECURE-Display.
 IRAS-SECURE-Display-Lite	<u>IRAS-SECURE-Display Lite</u> Softwareerweiterung	Anzeige von IRAS-SECURE-Informationen auf einem externen Monitor oder Display. Ermöglicht eine Echtzeitdarstellung ohne Verwendung der IRAS-Website.

	<u>IRAS-SECURE-Betriebsbuch</u> Softwareerweiterung	Bereitstellung eines digitalen Betriebsbuches für Betreiber, Errichter und Feuerwehr.
	<u>IRAS-SECURE-Connect-1-Jahr</u> Softwareerweiterung	IP-basierter Verbindungsdienst für IRAS-SECURE-Mobile über IFAM-Dienst.
	<u>IRAS-SECURE-Connect-5-Jahr</u> Softwareerweiterung	IP-basierter Verbindungsdienst für IRAS-SECURE-Mobile über IFAM-Dienst.
	<u>IRAS-SECURE-Connect-Flat</u> Softwareerweiterung	IP-basierter Verbindungsdienst für IRAS-SECURE-Mobile über IFAM-Dienst.
	<u>IRAS-SECURE-Erkunden</u> Softwareerweiterung	Information der Erkundungszeit für IRAS-SECURE-Display sowie als App für mobile Endgeräte.
	<u>IRAS-SECURE-EMA-TELENOT</u> Softwareerweiterung	Bereitstellung der Alarm-, Störungs- und Bewegungsdaten aus der EMA Hiplex von TELENOT für IRAS-SECURE-Display.
	<u>IRAS-SECURE-USV</u> Hard- und Softwareerweiterung	Überbrückung von Netzausfall durch eine Mini-USV.
	<u>IRAS-Secure-EMA-IFAM</u> Softwareerweiterung	Bereitstellung der Alarm-, Störungs- und Bewegungsdaten aus der EMA <i>MultiFlex</i> von IFAM für IRAS-SECURE-Display.
	<u>IRAS-Secure-EMA-Bosch</u> Softwareerweiterung	Bereitstellung der Alarm-, Störungs- und Bewegungsdaten aus der EMA <i>MAP 5000</i> von Bosch für IRAS-SECURE-Display.
	<u>IRAS-Secure-EMA-Telenot</u> Softwareerweiterung	Bereitstellung der Alarm-, Störungs- und Bewegungsdaten aus der EMA <i>Hiplex von Telenot</i> für IRAS-SECURE-Display.
	<u>IRAS-Secure-EMA-Honeywell</u> Softwareerweiterung	Bereitstellung der Alarm-, Störungs- und Bewegungsdaten aus der EMA <i>MB-Secure von Honeywell</i> für IRAS-SECURE-Display.
	<u>IRAS-SECURE-Control</u> (vormals: Ereignistasten)	IRAS-SECURE-Control ist eine plattformübergreifende Systemintegration und dient zur Steuerung von Brandmeldeanlagen. Es verbindet IRAS-SECURE direkt mit dem System <i>IMT4000</i> und ist für IRAS-SECURE-Display als auch mobil in der IRAS-App verfügbar.

Tabelle 3: IRAS-SECURE – Erweiterungsoptionen

4.7.1 Weitere Informationen



Informationen zu den Erweiterungsoptionen sowie die für eine Bestellung notwendigen Produktnummern entnehmen Sie bitte dem Produktbereich unserer Homepage (<https://ifam-erfurt.de/de/produkte/iras>) oder dem aktuellen Katalog.

4.7.2 Bestellung

Zur Bestellung von Erweiterungsoptionen stehen folgende Möglichkeiten zur Verfügung:

- **IFAM-Website, Produktbereich IRAS:** www.ifam-erfurt.de/de/produkte/iras.
- **IRAS-Website:** ➡ *siehe Kapitel 9.3.4.1.7 Features.*
- **Vertrieb IFAM GmbH Erfurt:** ➡ *siehe Kapitel 29 Kontakt und Kundenservice.*

4.8 Systemaufbau

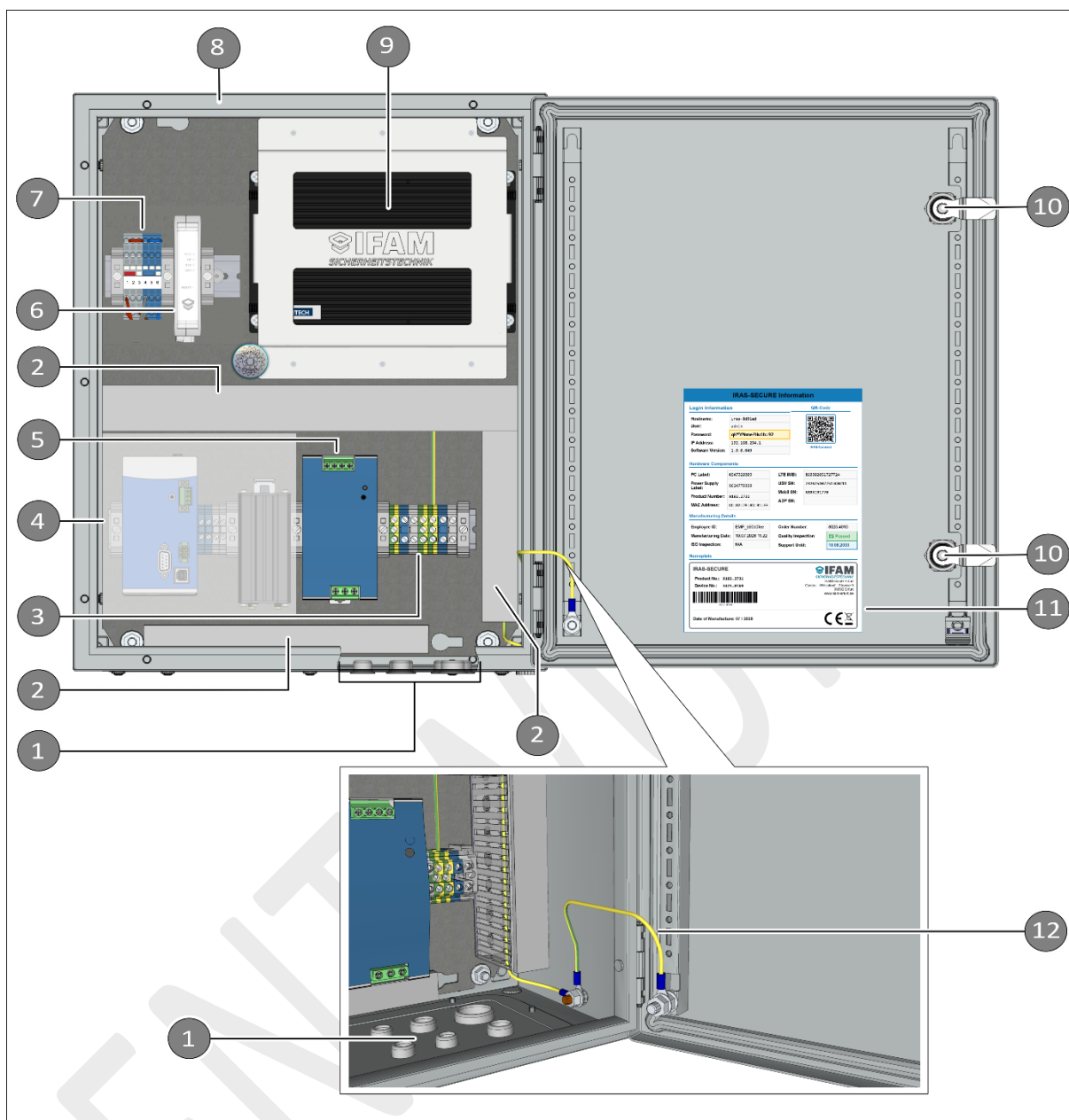


Abbildung 1: IRAS-SECURE – Übersicht

Pos	Beschreibung
1	Kabeldurchführungen – Netzanschluss und LAN-Kabel
2	Kabelkanal – Unterbringung von Anschlusskabeln
3	Klemmblock, Spannungsversorgung – Netzanschluss 230V
4	Hutschiene/Raum für den Einbau von Hardware-Erweiterungen (USV, Modem)
5	Netzteil/Spannungsversorgung
6	ADP4000-IRAS (auf Hutschiene)
7	Klemmblock, Spannungsversorgung – Baugruppen/Hardware-Erweiterungen
8	Metallgehäuse
9	IRAS-SECURE-Industrie-PC
10	Schließung Metallgehäuse
11	Lieferinformationen IRAS-SECURE
12	Erdung

4.9 Anschaltung der Baugruppen

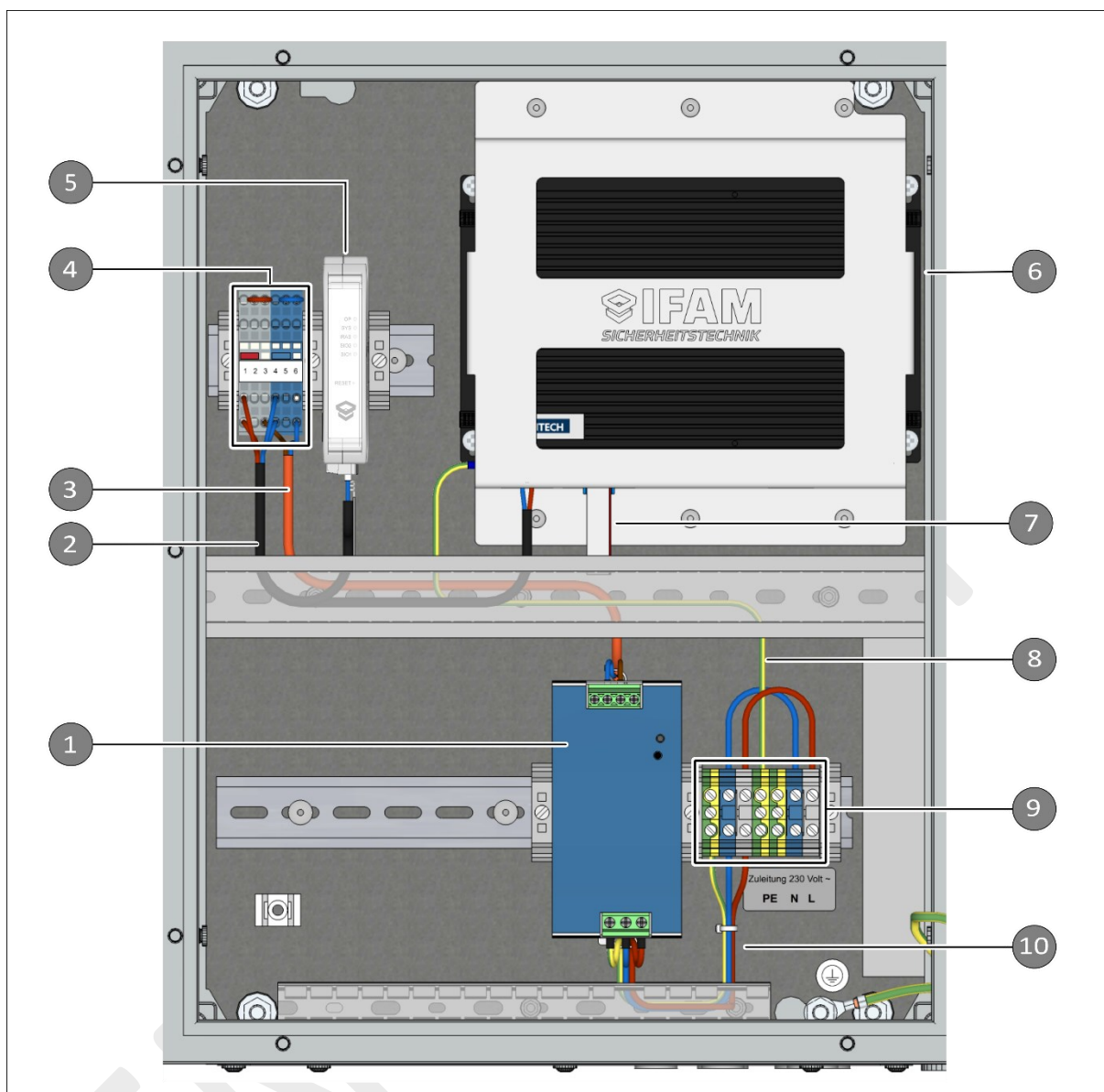


Abbildung 2: IRAS-SECURE – Anschaltung der Baugruppen

Pos	Beschreibung
1	Netzteil – Spannungsversorgung
2	Zuleitung/Spannung – Industrie-PC/ADP4000-IRAS
3	Zuleitung/Spannung – Netzteil/Klemmblock
4	Klemmblock/Spannung – ADP4000-IRAS, USV, Modem
5	ADP4000-IRAS
6	IRAS-SECURE-Industrie-PC
7	Datenverbindung/Flachbandkabel – ADP4000-IRAS/Industrie-PC
8	Erdung – Industrie-PC
9	Klemmblock/Spannungsversorgung – IRAS-SECURE/230 V
10	Zuleitung/Spannung – Klemmblock/Netzteil

4.10 Spannungsversorgung

Die Spannungsversorgung erfolgt durch den Anschluss an ein vorhandenes 230V-Netz. Der Anlagenbetreiber kann, entsprechend den individuellen technischen Gegebenheiten, eine geeignete Anschlussvariante wählen.

Optional besteht die Möglichkeit der Integration eines Akkus (USV intern/extern), der das IRAS-Secure-Gefahrenmeldesystem im Fall eines Netzausfalls absichert und das Versenden von Informationen auch bei nicht vorhandenem 230V-Netz ermöglicht.

Die IFAM GmbH bietet hierfür die Erweiterungsoption IRAS-SECURE-USV an. Diese kann mit ihrer Kapazität eine Netzunterbrechung von ca. 1 Stunde überbrücken.

4.10.1 Klemmblock IRAS-SECURE-Gefahrenmeldesystem

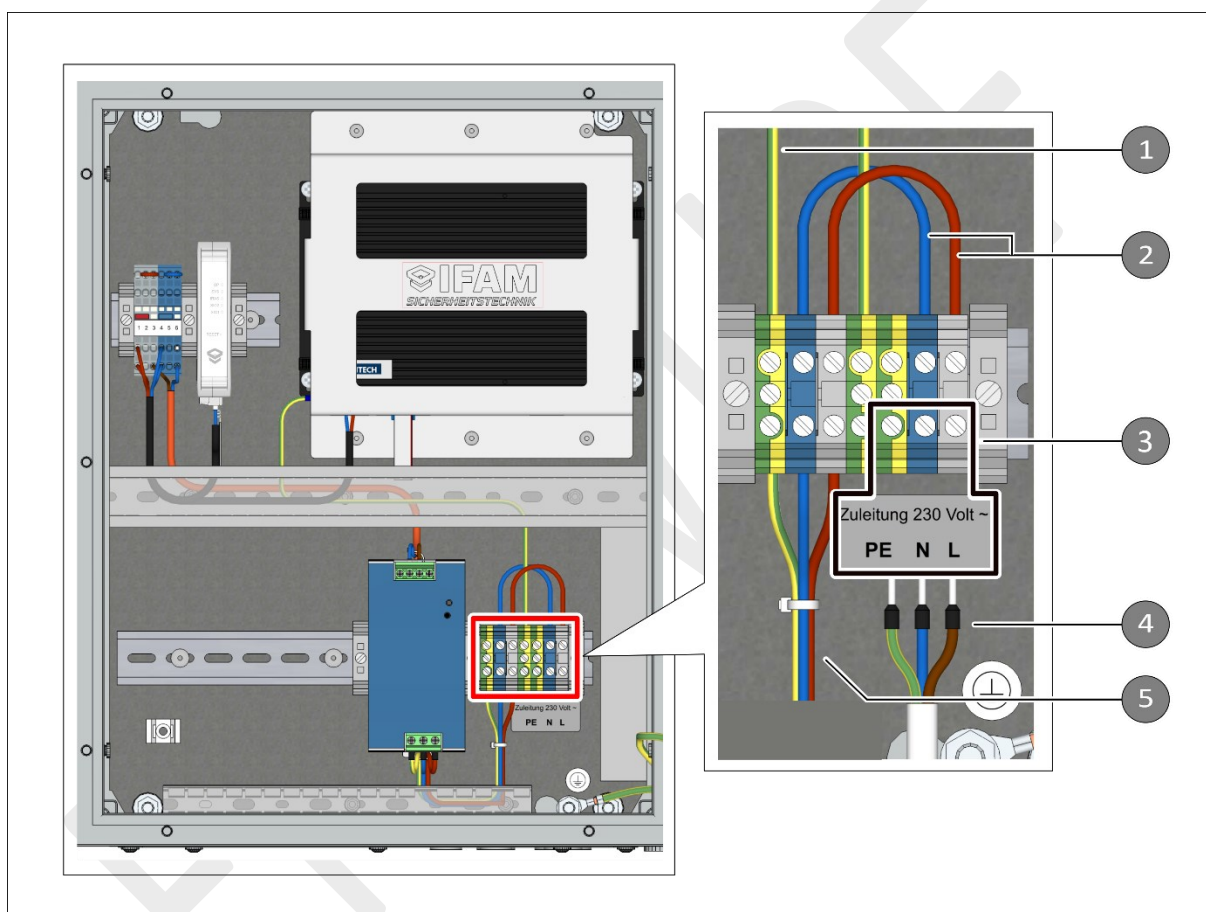


Abbildung 3: IRAS-Secure – Klemmblock, Spannungsversorgung (230V-Netz)

Pos	Beschreibung
1	Erdung
2	Brücke zwischen Anschlussklemmen externe Spannungsversorgung/Netzteil
3	Anschlüsse externe Spannungsversorgung (PE / N / L)
4	Anschlusskabel externe Spannungsversorgung (230V-Netz)
5	Anschlusskabel Netzteil

4.10.2 Klemmblock Baugruppen/Hardwareerweiterung

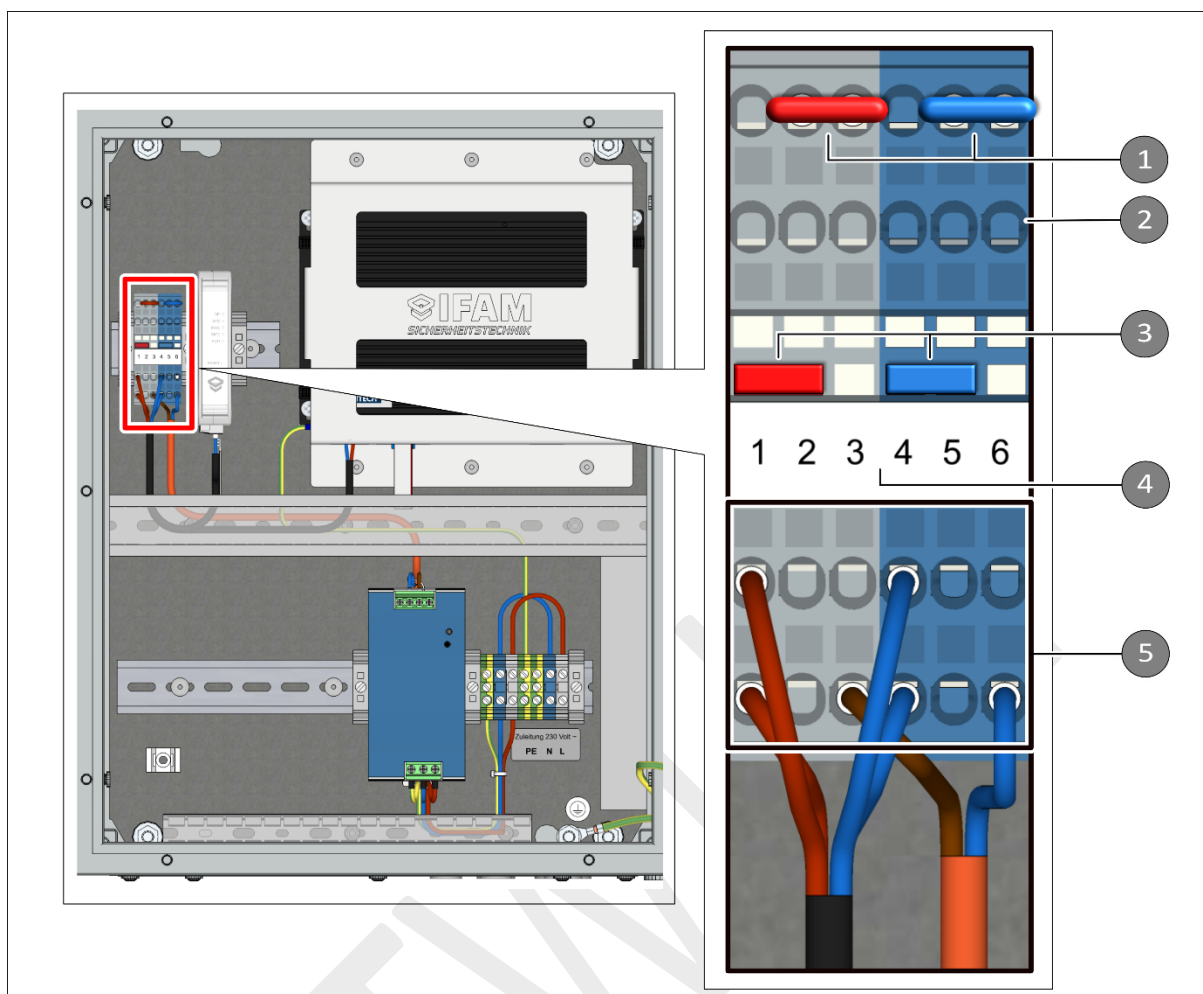


Abbildung 4: IRAS-Secure – Klemmblock/Spannungsversorgung, Hardwareerweiterungen

Pos	Beschreibung
1	Flexible Steckbrücken – Konfiguration zur Anschaltung von Hardware-Erweiterungen
2	Anschlüsse für zusätzliche Verbraucher (24V DC)
3	Feste Steckbrücke (nicht verändern!)
4	Anschlussbezeichnungen zu 2 und 5 1-3 Speisung 24 V DC (1-2 nach USV; 3 vor USV) 4-6 Nullleiter (4-5 nach USV; 6 vor USV)
5	Anschlüsse Hardware (Industrie-PC, ADP4000-IRAS, Hardwareerweiterungen)

4.11 Metallgehäuse – Schließsystem

Als Schließsystem stehen drei Optionen zur Verfügung:

- Verriegelung mit Magnet-Schließsystem (nicht individuell),
- Verriegelung mit Drehgriff-Schließsystem (Doppelbart-Schließung oder Schließzylinder),
- Verriegelung mit Doppelbart-Schließsystem.

4.11.1 Magnetisch (Standard)

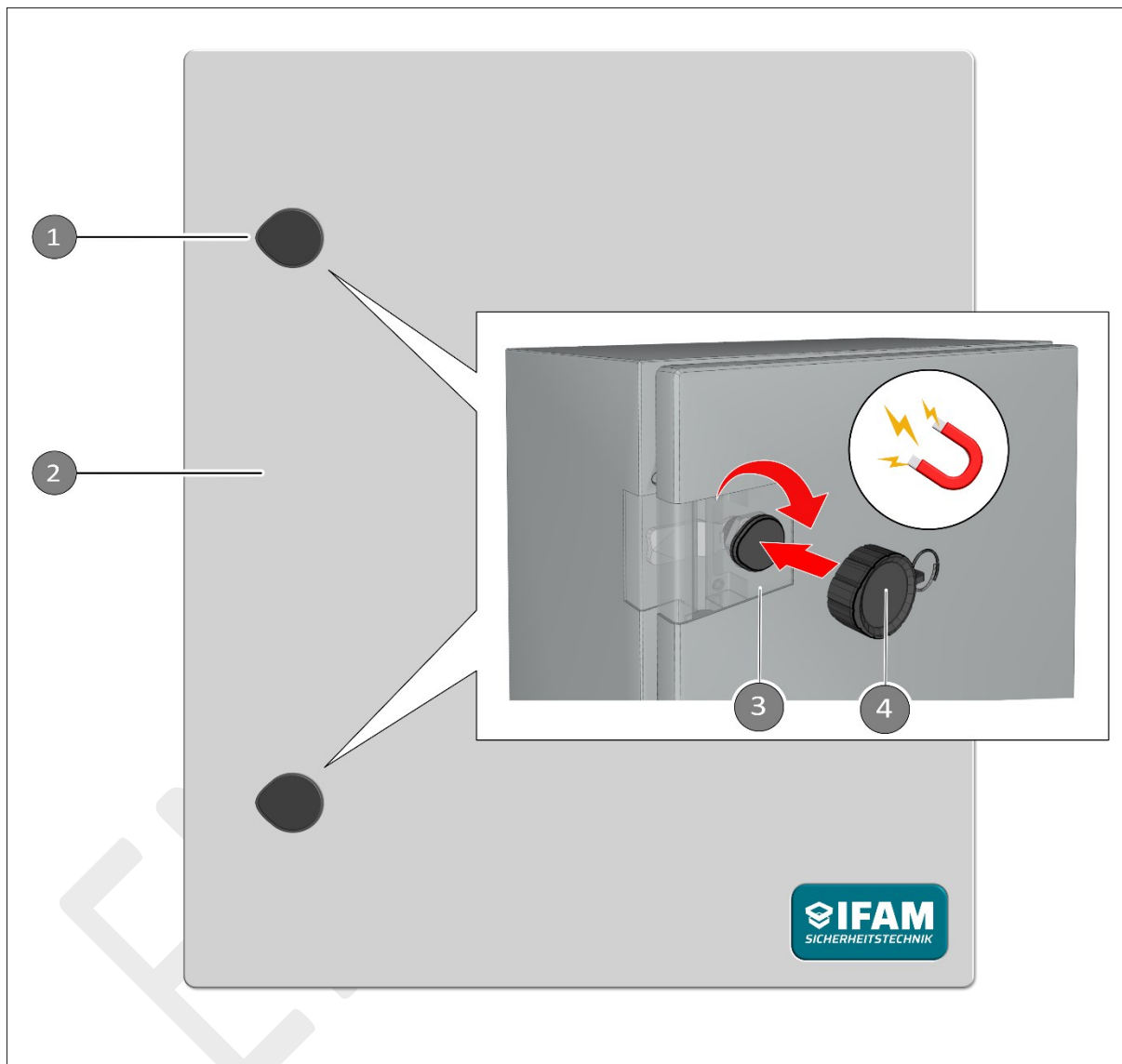


Abbildung 5: IRAS-SECURE/Metallgehäuse – Schließsystem 1: magnetisch

Pos	Beschreibung
1	Magnet-Schließsystem (Verriegelung und Schlüssel)
2	Gehäusetür
3	Verriegelung
4	Schlüssel

Im Falle eines Schlüsselveverlustes wenden Sie sich bitte an den Kundendienst der IFAM GmbH.

➡ [Siehe Kapitel 29 Kontakt und Kundenservice.](#)

4.11.2 Drehgriffe

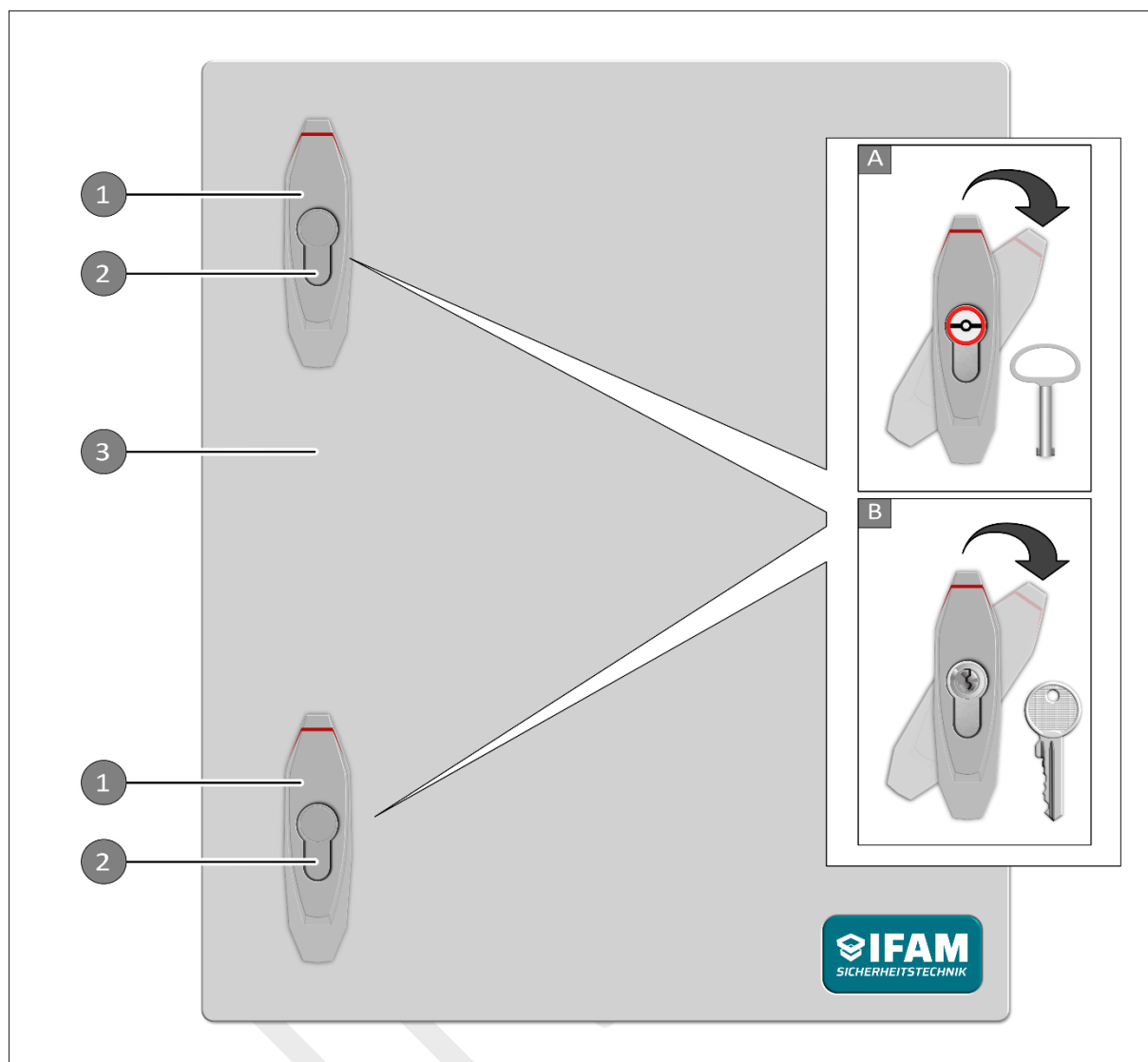


Abbildung 6: IRAS-SECURE/Metallgehäuse – Schließsystem 2: Drehgriffe

Pos	Beschreibung
1	Drehgriff
2	Schließung
3	Gehäusetür

Das Drehgriff-Schließsystem (*Mini-Komfortgriff AX*) kann mit unterschiedlichen Schließungen ausgestattet werden:

- Doppelbart (**A**),
- Profilhalbzylinder (40 bzw. 45 mm) (**B**).

Bei Bestellung des Schließsystems wird ein Gehäuse mit einem Doppelbart-Schließsystem (Abbildung 7) und dem Montagesatz *AX Mini-Comfort-Handle* (RITTAL) ausgeliefert.

Die Montage der Drehgriffe muss durch den Kunden vorgenommen werden.

Folgen Sie hierbei für die Doppelbart-Schließung den beiliegenden Montagehinweisen bzw. für Profilhalbzylinder den Informationen auf der herstellereigenen Homepage der *RITTAL GmbH & Co. KG/Herborn*.



Für weitere Fragen zu Montage und geeigneten Schließungen wenden Sie sich bitte an den Kundendienst der IFAM GmbH Erfurt.

➞ [Siehe Kapitel 29 Kontakt und Kundenservice.](#)

4.11.3 Doppelbart

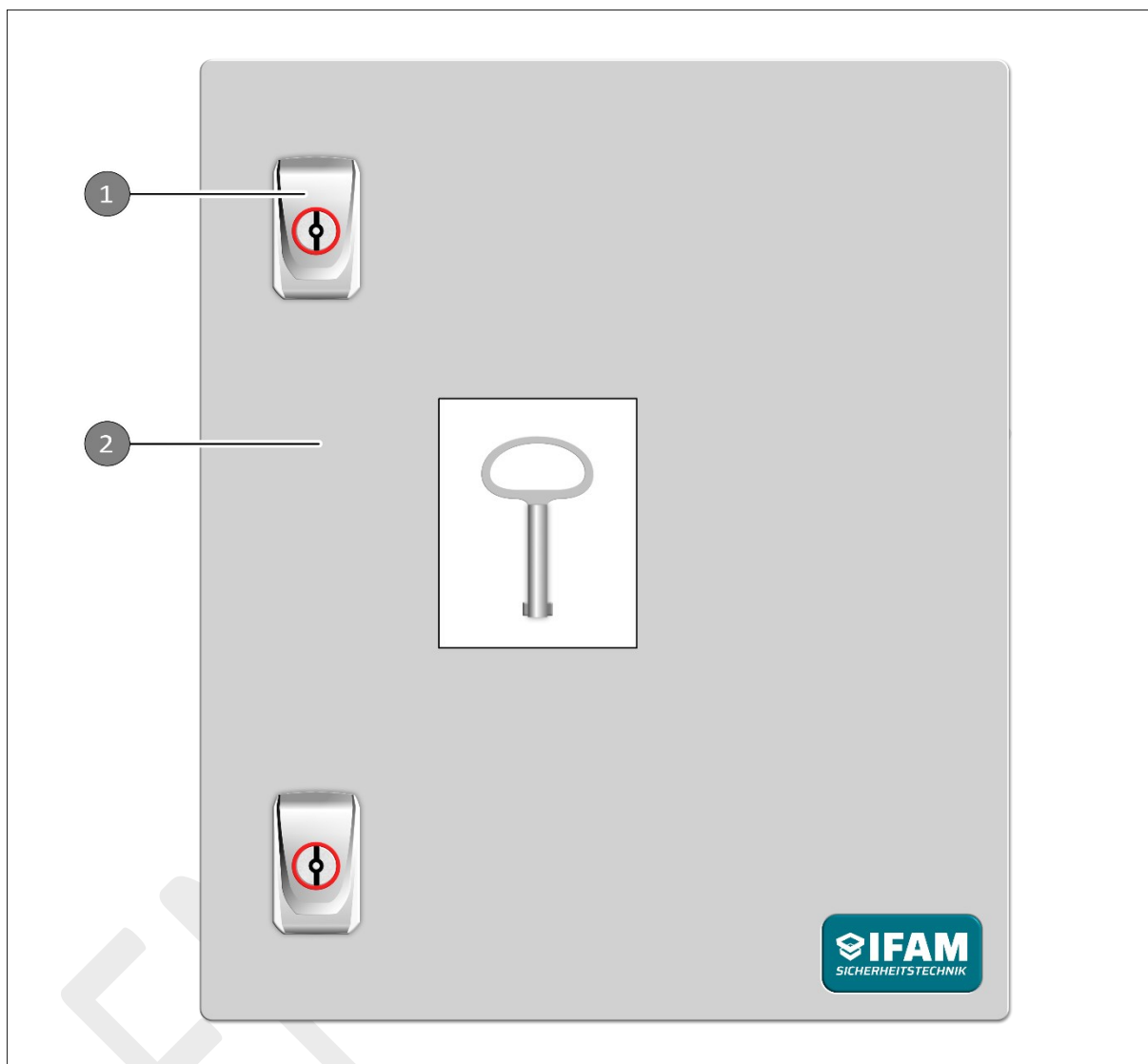


Abbildung 7: IRAS-SECURE/Metallgehäuse – Schließsystem 3: Doppelbart

Pos	Beschreibung
1	Doppelbart-Schließsystem
2	Gehäusetür

4.12 IRAS-SECURE-Industrie-PC

4.12.1 Übersicht

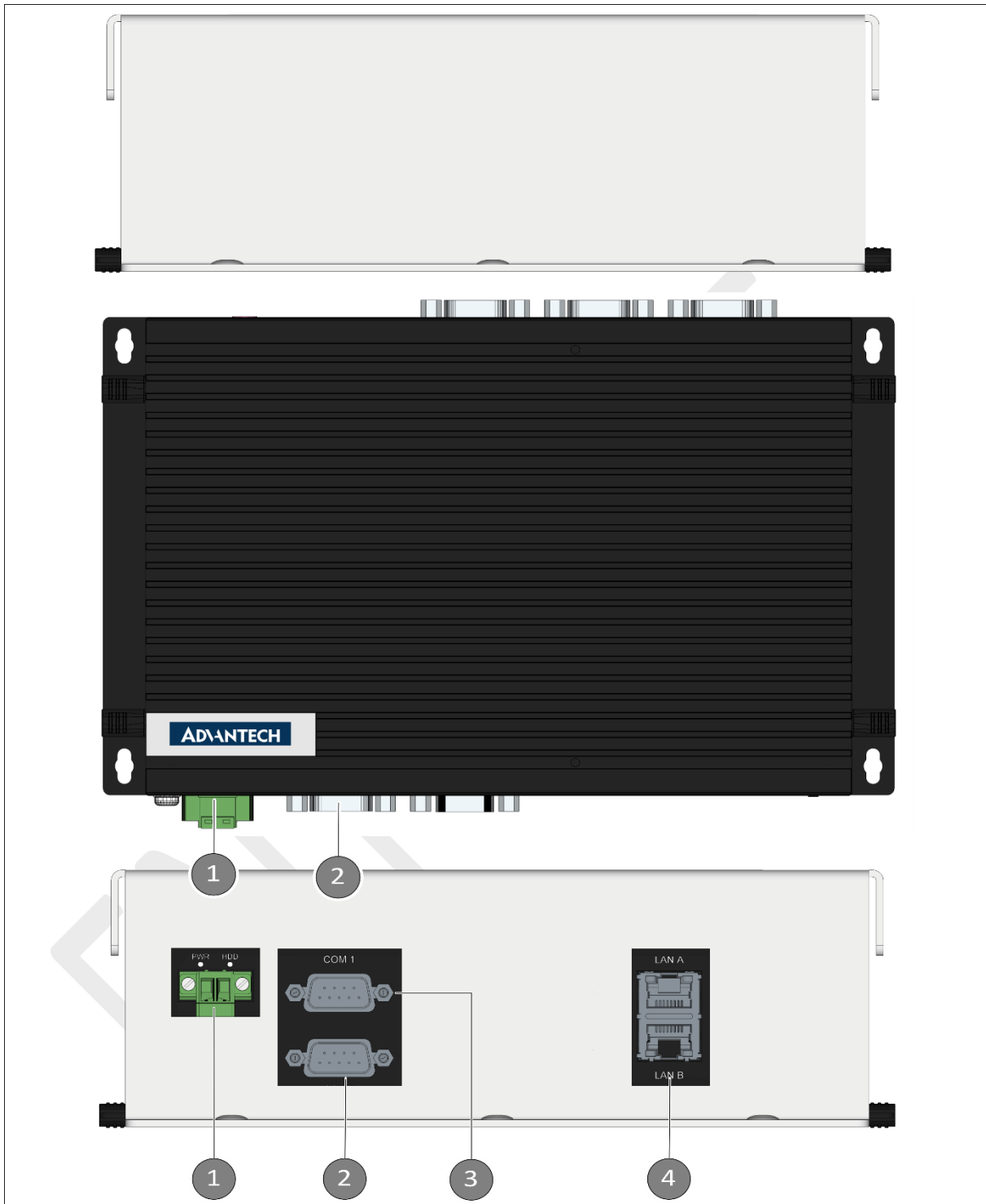


Abbildung 8: IRAS-SECURE-Industrie-PC

Pos	Beschreibung
1	Schnittstelle Spannungsversorgung
2	Datenverbindung USV
3	Schnittstelle Datenkabel (RS232 $\leftrightarrow$ ADP4000-IRAS)
4	RJ45 LAN-Schnittstellen (LAN1/LAN2) (Netzwerk-Verbindung, Anschluss eines Modems)

4.12.2 Schutzgitter/Siegel



Abbildung 9: IRAS-SECURE-Industrie-PC – Schutzgitter/Versiegelung

Pos	Beschreibung
1	Niet
2	IRAS-SECURE-Industrie-PC
3	Schutzgitter
4	Siegel

Der IRAS-SECURE-Industrie-PC ist mit Hilfe eines vernieteten Schutzgitters gegen unbefugten Zugriff gesichert.

Die Unversehrtheit dieser Sicherung wird mit Hilfe eines Siegels (4) nachvollziehbar gemacht.



- **Das Entfernen des Schutzgitters, die Entnahme des Industrie-PCs sowie die Nutzung der nicht für den Betrieb von IRAS-SECURE vorgesehenen Schnittstellen sind nicht gestattet!**
- **Die Unversehrtheit des Siegels muss gewährleistet sein!**
Sollte das Siegel verletzt werden, der Industrie-PC ausgebaut oder unzulässig verwendet oder die nicht-autorisierten Schnittstellen genutzt werden, erlischt die Gewährleistung/Garantie für das gesamte IRAS-SECURE-Gefahrenmeldesystem.
- Bei einem Fehler an der Baugruppe wenden Sie sich bitte stets an den Kundendienst der IFAM GmbH Erfurt.

4.13 ADP4000-IRAS

Der *ADP4000-IRAS* dient der Integration von IRAS-SECURE in die Gefahrenmeldeanlage über einen (vorhandenen) redundanten Ring.

Das Gerät kann über einen Redundanzadapter (*ADP4000*) oder an eine vorhandene Komponente in einen redundanten Ring integriert werden.

Eine zusätzliche Schnittstellen- bzw. Klemmennummerierung wurde zur Vermeidung von Anschlussfehlern angebracht.

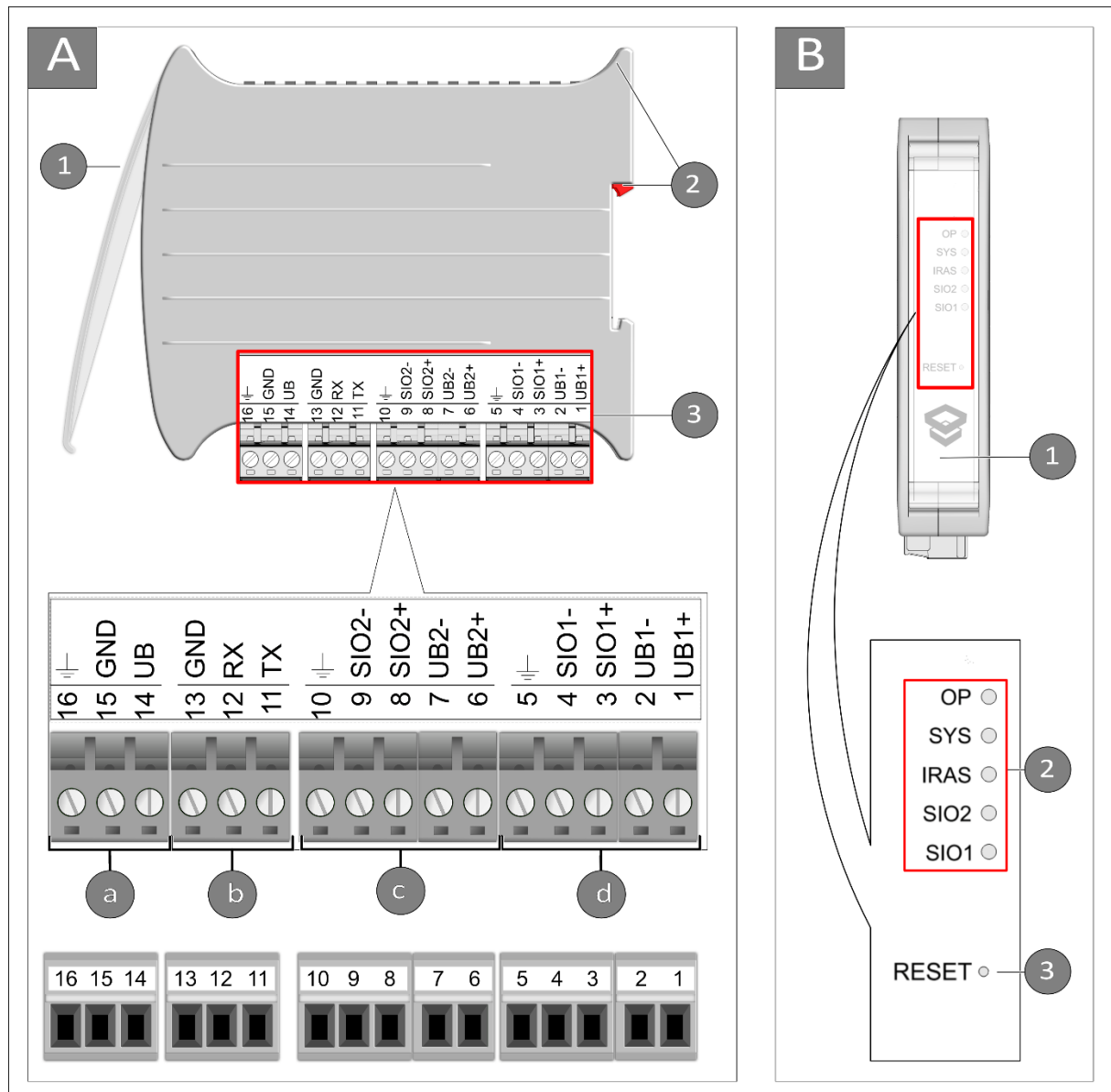


Abbildung 10: ADP4000-IRAS

Pos	Beschreibung
A	Seitenansicht (rechts)
1	Schutzklappe
2	Arretierung/Montage auf Hutschiene
3	Schnittstellen/Kabelklemmen (nummeriert)
a	Spannungsversorgung/Erddung
b	Serielle Schnittstelle, Verbindung zum IRAS-SECURE-Industrie-PC

	c	SIO2/UB2 – Integration in den redundanten Ring
	D	SIO1/UB1 – Integration in den redundanten Ring
B	Vorderansicht	
1	Schutzklappe	
2	Status-/Diagnose-LEDs	
3	Reset-Taster	

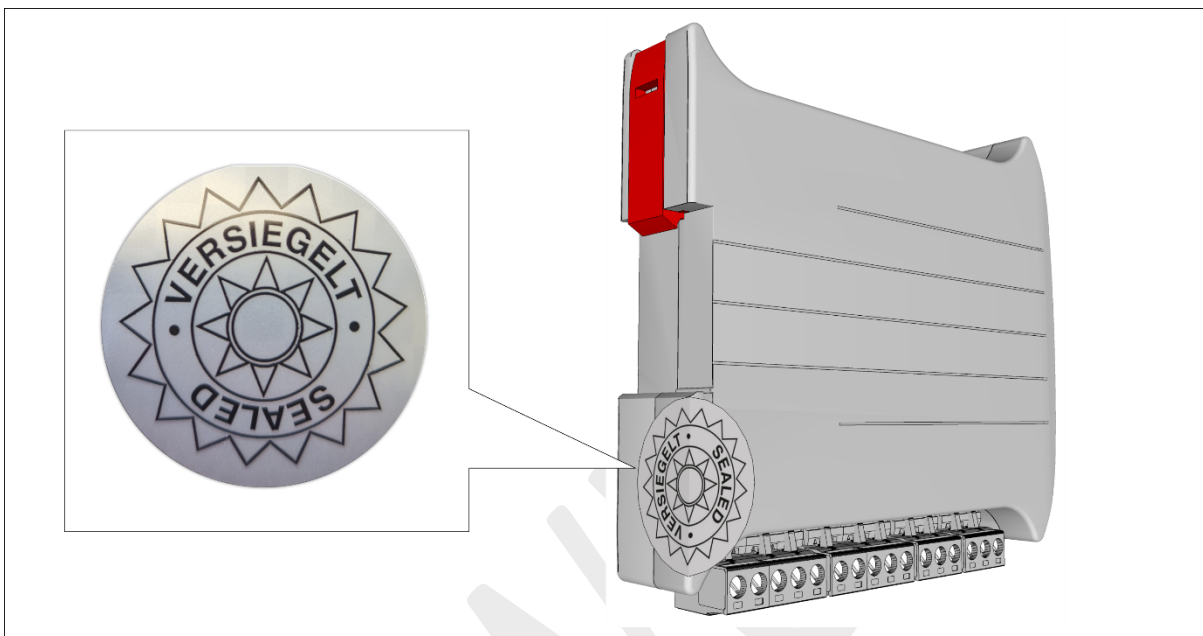


Abbildung 11: ADP4000-IRAS – Geräte-Siegel



- **Das Öffnen des Gehäuses des ADP4000-IRAS ist nicht gestattet.**
- **Die Unversehrtheit des Siegels muss gewährleistet sein!**
Sollte das Siegel verletzt, das Gehäuse geöffnet und der ADP400-IRAS unzulässig verwendet oder die nicht-autorisierten Schnittstellen genutzt werden, erlischt die Gewährleistung/Garantie für das gesamte IRAS-SECURE-Gefahrenmeldesystem.
- Bei einem Fehler an der Baugruppe wenden Sie sich bitte stets an den Kundendienst der IFAM GmbH Erfurt.

4.14 ADP4000



Der **ADP4000** ist nicht (Liefer-)Bestandteil des IRAS-SECURE-Gefahrenmeldesystems. Sollten Sie dieses Gerät noch nicht besitzen, muss es bei der Bestellung berücksichtigt werden.

Die Integration von IRAS-SECURE in eine Gefahrenmeldeanlage erfolgt im Rahmen einer redundanten Anschaltung über den Redundanzadapter **ADP4000**, der die Gefahrenmeldeanlage in eine Ringstruktur einbindet bzw. diese erst ermöglicht.

Der **ADP4000** wird hierbei direkt an die Gefahrenmeldezentrale (GMZ) angeschlossen. Der **ADP4000-IRAS** wird an den **ADP4000** oder ein anderes Peripheriegerät des redundanten Ringes angeschlossen.

4.14.1 Übersicht

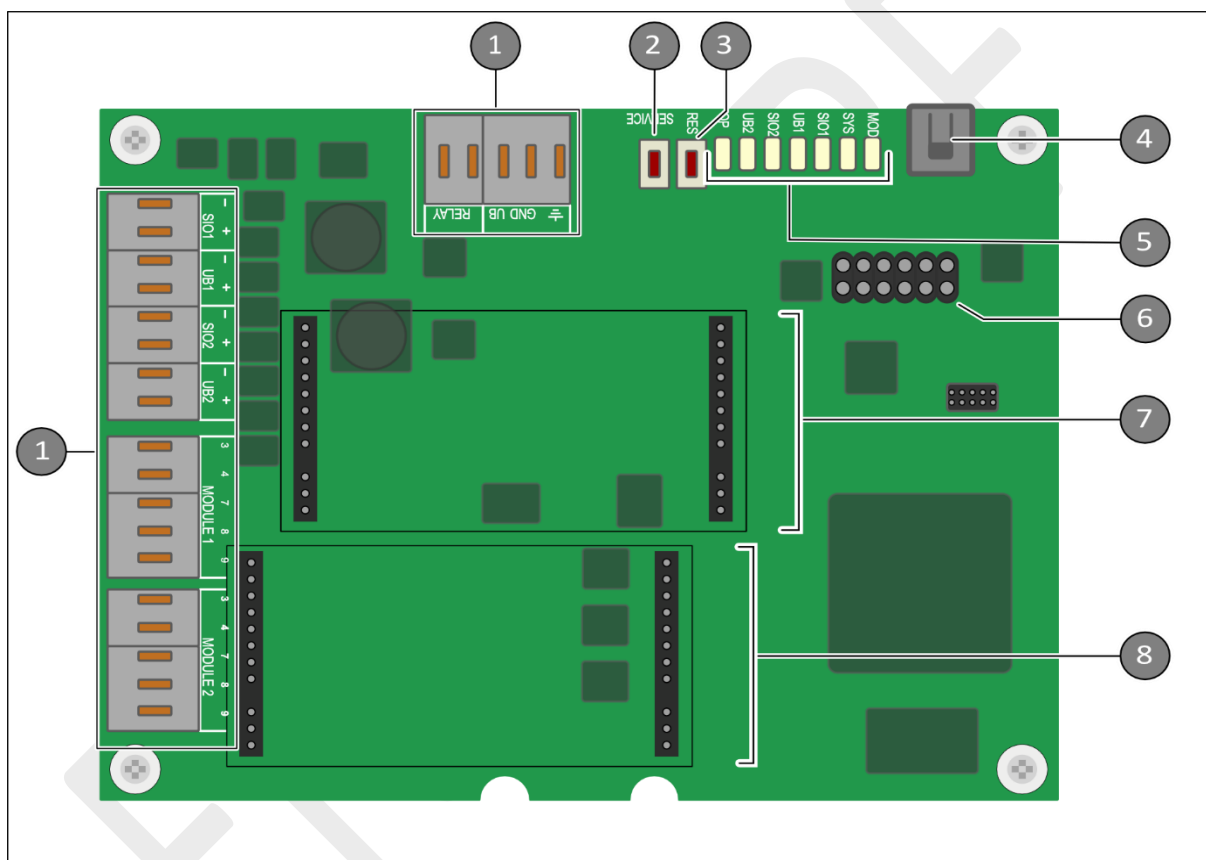


Abbildung 12: ADP4000 – Übersicht

Pos	Beschreibung
1	Schnittstellen/Anschlüsse
2	Service-Taster
3	Reset-Taster
4	USB-Schnittstelle zum Anschluss eines PCs
5	Diagnose-LEDs
6	Schnittstelle für ADP-FBF (parallele FBF-Schnittstelle)
7	Modul-Steckplatz 1 (BMZ)
8	Modul-Steckplatz 2 (externe Schnittstelle)

4.14.2 Schnittstellen/Anschlüsse

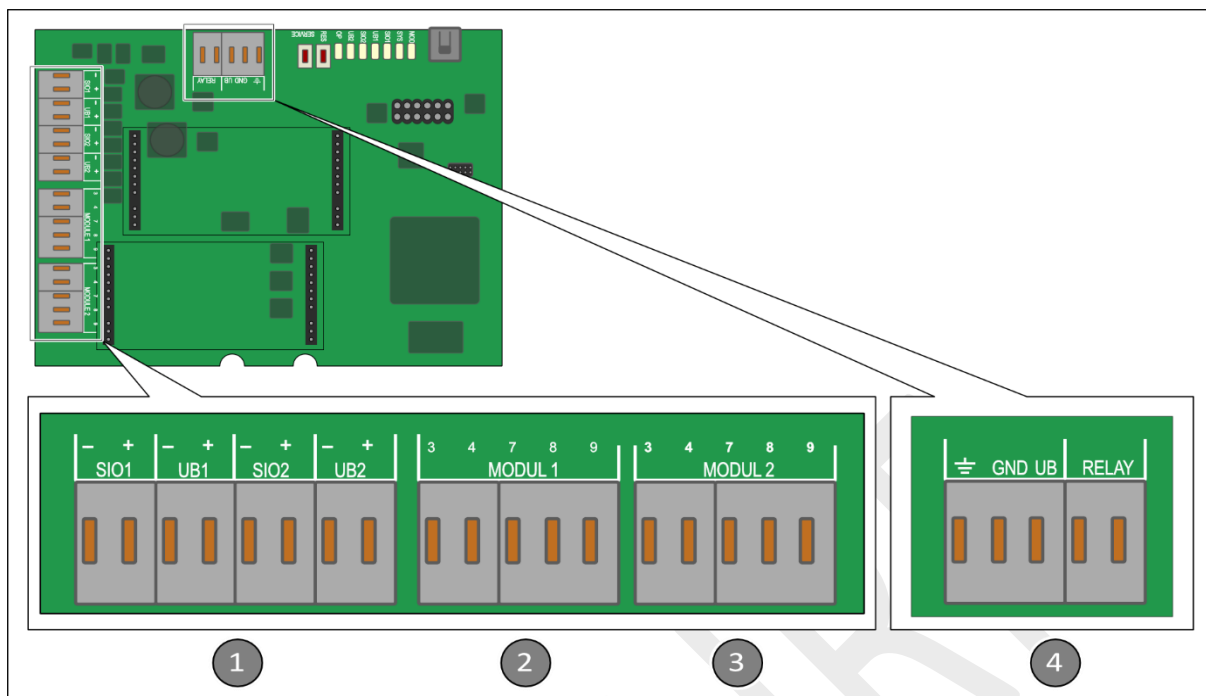


Abbildung 13: ADP4000 – Anschlüsse

Pos	Beschreibung
1	Redundanter Ring-Bus1/Bus2: Anschlüsse für Betriebsspannung (UB) und Daten (SIO) für Geräte des redundanten Rings
2	Anschlüsse Schnittstellenmodul 1 (BMZ)
3	Anschlüsse Schnittstellenmodul 2 (externe Schnittstelle)
4	a.) Ausgang Optorelais für Störungsweiterleitung b.) Spannungsversorgung für ADP4000 und Teilnehmer auf dem redundanten Ring

5 Montage

5.1 Sicherheit



- Das IRAS-SECURE-Gefahrenmeldesystem muss während des Transports, des Aufbau/der Montage sowie der Demontage gegen Umfallen, Herunterfallen und Verrutschen gesichert werden!
- Überprüfen Sie nach Arbeiten am/mit dem Gerät, dass der Deckel ordnungsgemäß verschlossen ist.

5.2 Montagort und Betriebsbedingungen

Für die Montage von IRAS-SECURE gelten als (zusätzliches) Zweitinformationssystem keine normierten Vorgaben in Bezug auf Höhe und Montageort.

IRAS-SECURE sollte:

- für Inspektions- und Wartungsarbeiten frei zugänglich sein,
- ggf. beleuchtet sein,
- ggf. durch ein Hinweisschild gekennzeichnet sein.

Beachten Sie die notwendigen Betriebs-/Umgebungsbedingungen.

➞ [Siehe Kapitel 17 Technische Daten.](#)

Das Gerät besitzt die Schutzart **IP66** (Schutz vor Staub und starkem Strahlwasser) und kann in entsprechenden Umgebungen montiert/betrieben werden.

5.3 Montage – Varianten

IRAS-SECURE ist für die Wandmontage vorgesehen. Hierfür stehen 2 Varianten zur Verfügung: **1.)** direkte Montage (**Standard**) und **2.)** Verwendung von Wandhalterungen (optional).



Wird die Montage mit Wandhalterungen gewünscht, muss dies im Rahmen der Bestellung angegeben werden.

5.3.1 Wandmontage (direkt)

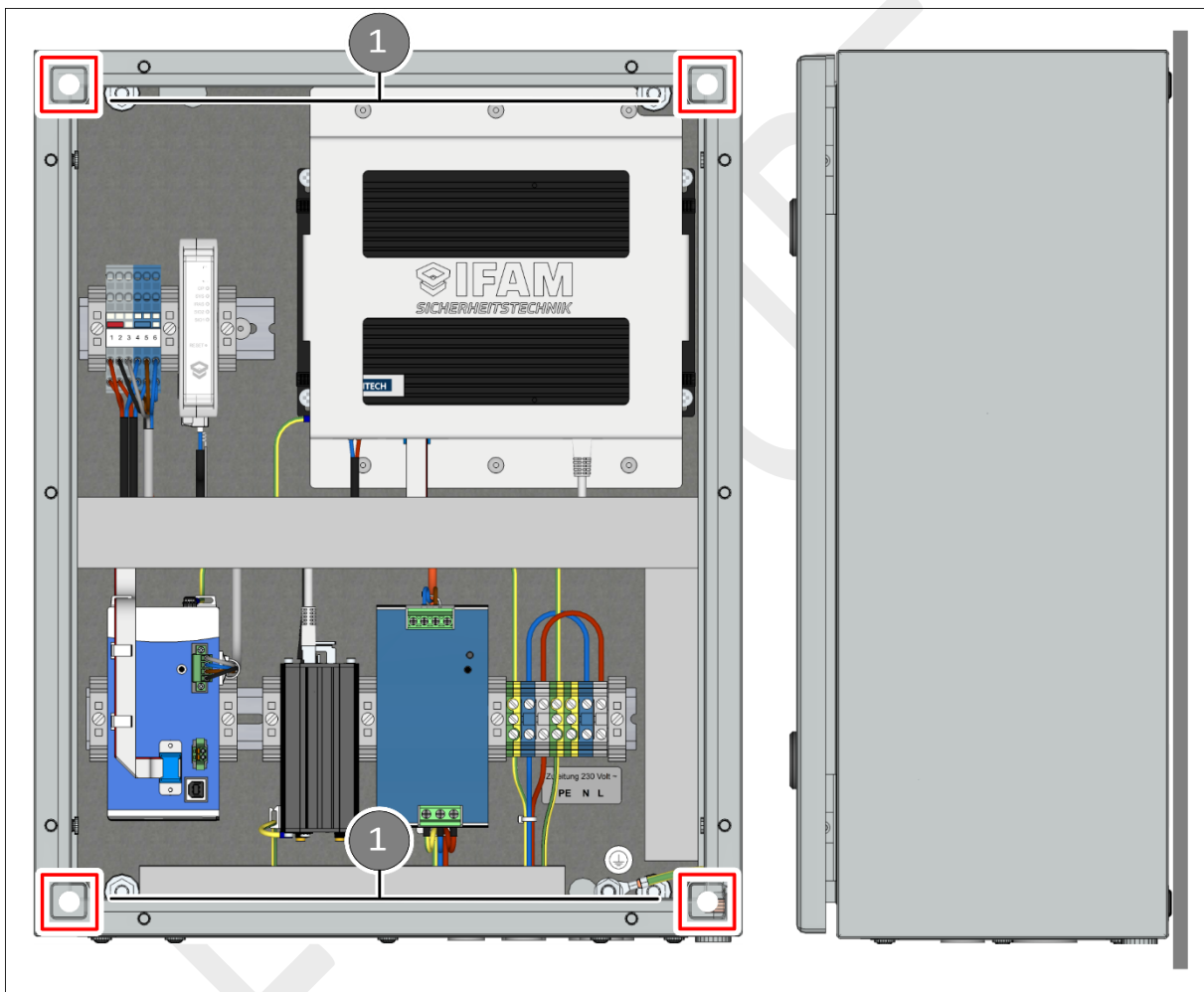


Abbildung 14: Gehäuse – Wandmontage (Beispieldarstellung)

Pos	Beschreibung
1	Montageöffnungen/Gehäuserückwand

Die Gehäuse-/Montagemaße finden Sie im Anhang.

➞ [Siehe Kapitel 34.1 Geräte-/Montagemaße.](#)

5.3.1.1 Befestigungsmaterialien



Für die Staub- und Wasserdichtigkeit des Gehäuses (Schutzart IP66) empfehlen wir die Verwendung von Schrauben mit **Unterlegscheibe** und **Dichtring**, 4 Stck. mind. M 10 x 70 mm.

Ist keine hohe Staub- und Wasserdichtigkeit gefordert, kann auf die Dichtung verzichtet werden.

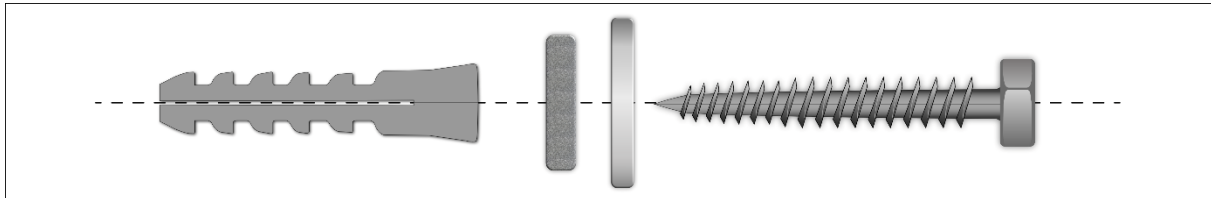


Abbildung 15: Befestigungsmaterial/Schraube, Unterlegscheibe, Dichtring

Alternativ hierzu sind weitere Befestigungsmaterialien verwendbar:

- **Dichtscheiben (Bonded Seals/Dowty-Dichtungen):**
Eine Metallscheibe mit fest vulkanisiertem Elastomer (meist EPDM oder NBR). Sie dichtet unter dem Schraubenkopf zuverlässig gegen die Gehäusewand ab und wird häufig für IP66/IP67-Anwendungen eingesetzt.

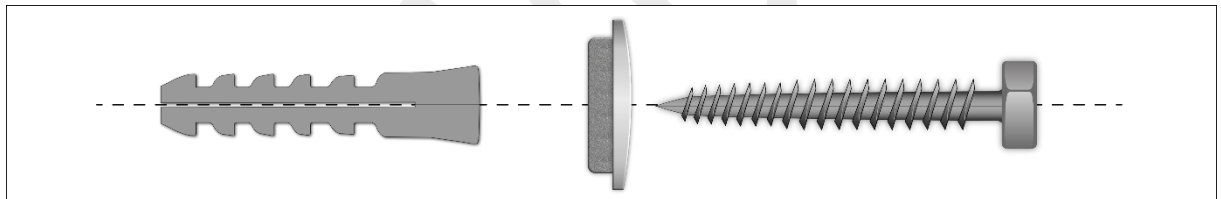


Abbildung 16: Befestigungsmaterial/Dichtscheiben

- **Dicht-Unterlegscheiben aus EPDM oder Silikon:**
Gummischeiben, teilweise mit Metallverstärkung. Sie sind einfacher, aber oft ausreichend für Wandgehäuse.
- **O-Ringe unter dem Schraubenkopf:** Funktionieren nur, wenn der Schraubenkopf und die Auflagefläche entsprechend ausgelegt sind. Ohne definierte Nut können sie sich beim Anziehen verformen und sind daher weniger zuverlässig als Bonded Seals.
- **Selbstdichtende Schrauben:** Einige Hersteller bieten Schrauben mit integrierter Dichtung unter dem Kopf an, diese sind jedoch weniger verbreitet.

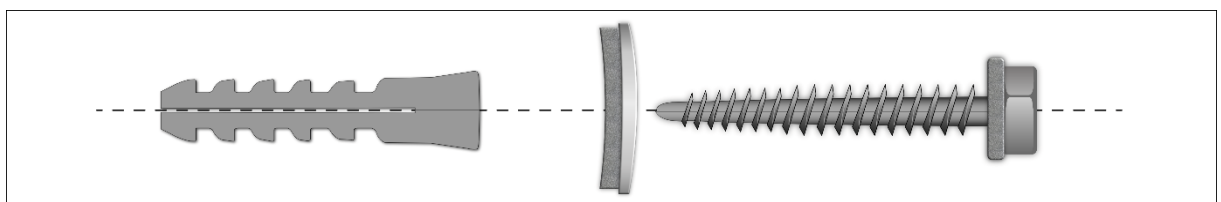


Abbildung 17: Befestigungsmaterial/selbstdichtende Schrauben

5.3.2 Wandmontage (Wandhalterungen)

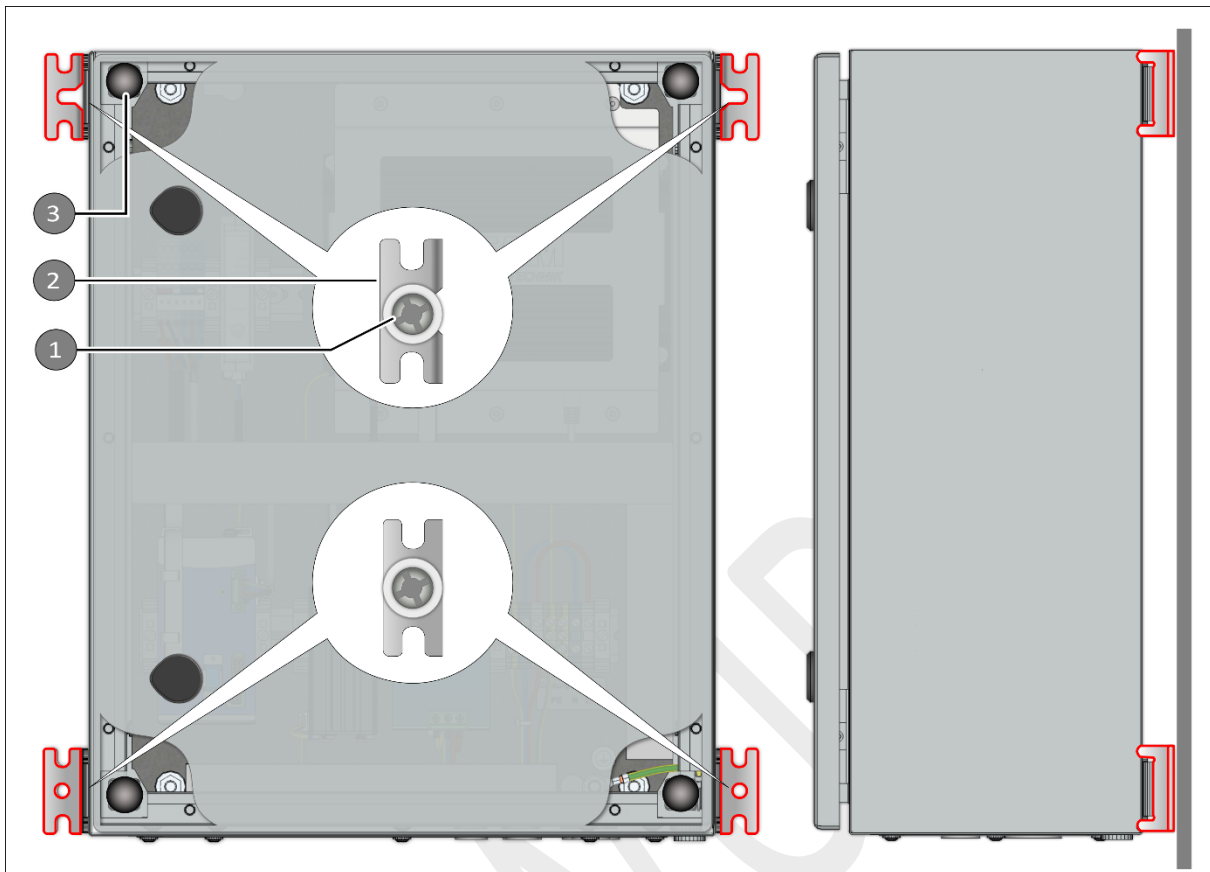


Abbildung 18: Gehäuse – Wandhalterungen (Beispieldarstellung)

Pos	Beschreibung
1	Schrauben mit Unterlegscheiben
2	Wandhalterung
3	Gummistopfen (Abdichtung des Gehäuses)

Für die Anbringung der Befestigungsschrauben/Unterlegscheiben (1) sind die jeweils mittleren Öffnungen zu verwenden.



Zur Erhaltung der mit der Schutzart IP66 verbundenen Eigenschaften müssen die für die direkte Wandmontage vorgesehenen Öffnungen mit den beiliegenden Gummistopfen (3) verschlossen/abgedichtet werden!
 ➔ [Siehe Abbildung 14: Gehäuse – Wandmontage \(Beispieldarstellung\).](#)

Die Gehäuse-/Montagemaße finden Sie im Anhang.

➔ [Siehe Kapitel 34.1 Geräte-/Montagemaße.](#)

5.4 Montagehinweise

Das Metallgehäuse ist an den vorgegebenen Befestigungspunkten auf einer festen Wand ohne mechanische Verspannung zu verschrauben. Die Maße für die erforderlichen Bohrungen finden Sie im Anhang.

➡ *Siehe Kapitel 34.1 Geräte-/Montagemaße.*

Die Anschlusskabel für die eingebauten Komponenten (z.B. Spannungsversorgung, Netzwerk-anbindung) werden von unten durch die vorgesehenen Kabeldurchführungen in das Gehäuse eingebracht.

➡ *Siehe Kapitel 4.8 Systemaufbau.*

Bei der Montage sind zu beachten:

- Eine ausreichende Festigkeit und Tragfähigkeit der Wand.
Geeignete Materialien: Beton oder Vollstein.
- Befestigungsmaterial entsprechend den oben beschriebenen Montagevarianten.
- Berücksichtigung der Betriebsumgebung (Staubbelastung, Feuchtigkeit, mögliches Spritzwasser u.a.) bei der Auswahl der Befestigungsmaterialien (Gewährleistung IP66).
- Adäquate Umgebungsbedingungen für die (optionale) Ausführung einer drahtlosen Kommunikation (Sende-/Empfangsleistung).

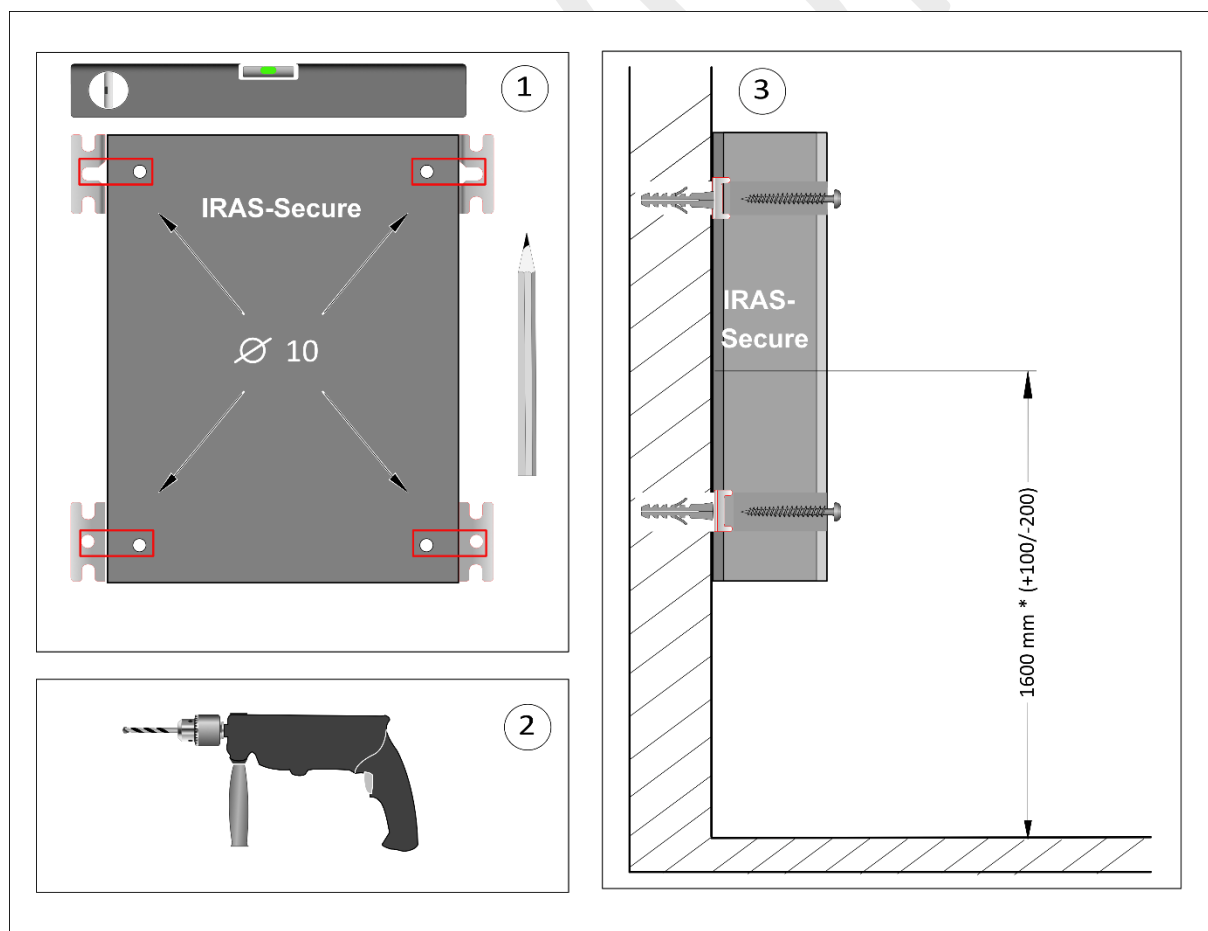


Abbildung 19: IRAS-SECURE – Gehäusemontage

5.5 Erdung



ACHTUNG!

Beeinträchtigung der Funktion von IRAS-SECURE durch fehlende Erdung bzw. Schirmung.

Bei fehlender Erdung des Gehäuses und/oder fehlender Schirmung der Anschlusskabel kann es zu Einschränkungen in der Funktionsweise des Gerätes kommen. Ein Ausfall kann die Folge sein.

Entsprechend den jeweils spezifischen technischen Gegebenheiten kann es notwendig sein, das Metallgehäuse zusätzlich zu erden.

- Das Gehäuse ist unbedingt zu erden.
- Verwenden Sie für die Anschaltung ein geschirmtes Kabel.

➞ [Siehe Kapitel 17 Technische Daten.](#)

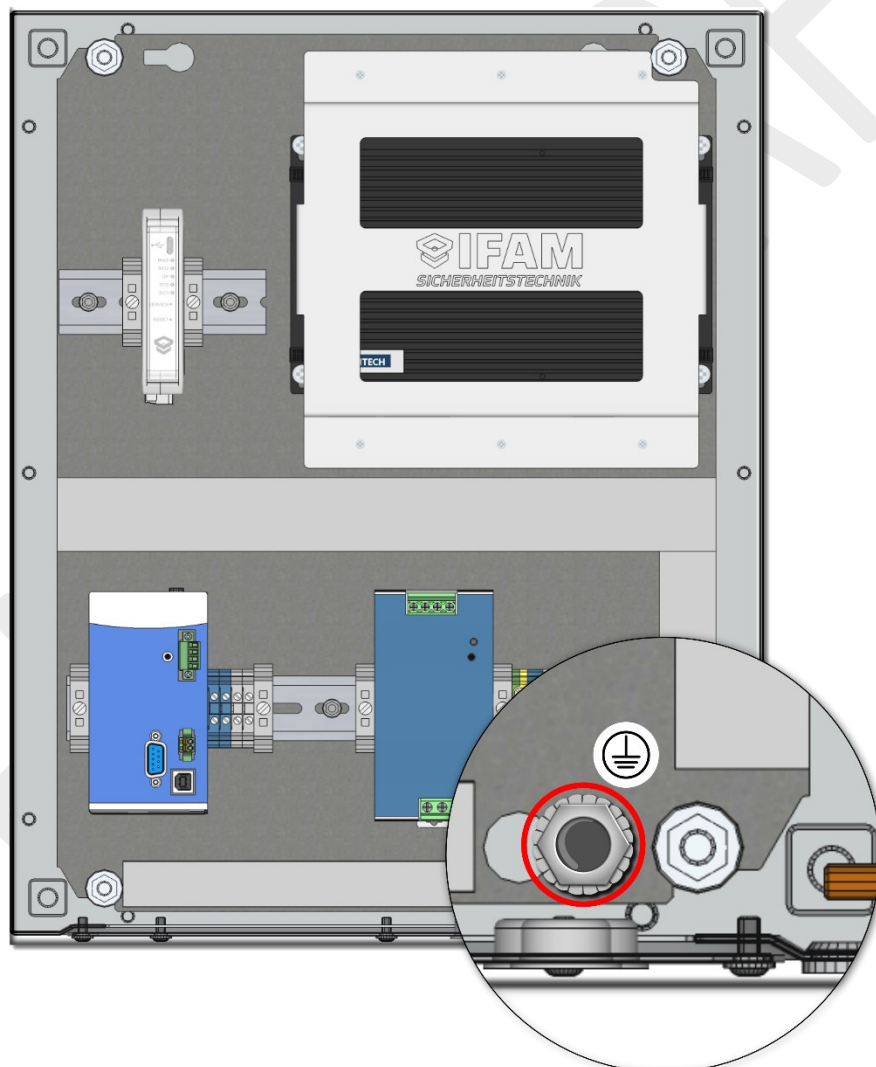


Abbildung 20: IRAS-SECURE – Erdung/Gehäuse

Die Erdung erfolgt im Normalfall über das Kabel der Spannungsversorgung

➞ [Siehe Kapitel 6.2 IRAS-SECURE – Spannungsversorgung](#)).

Als zusätzliche Option steht der Erdungsanschluss im Metallgehäuse zur Verfügung (Abbildung 20).

5.6 ADP4000-IRAS

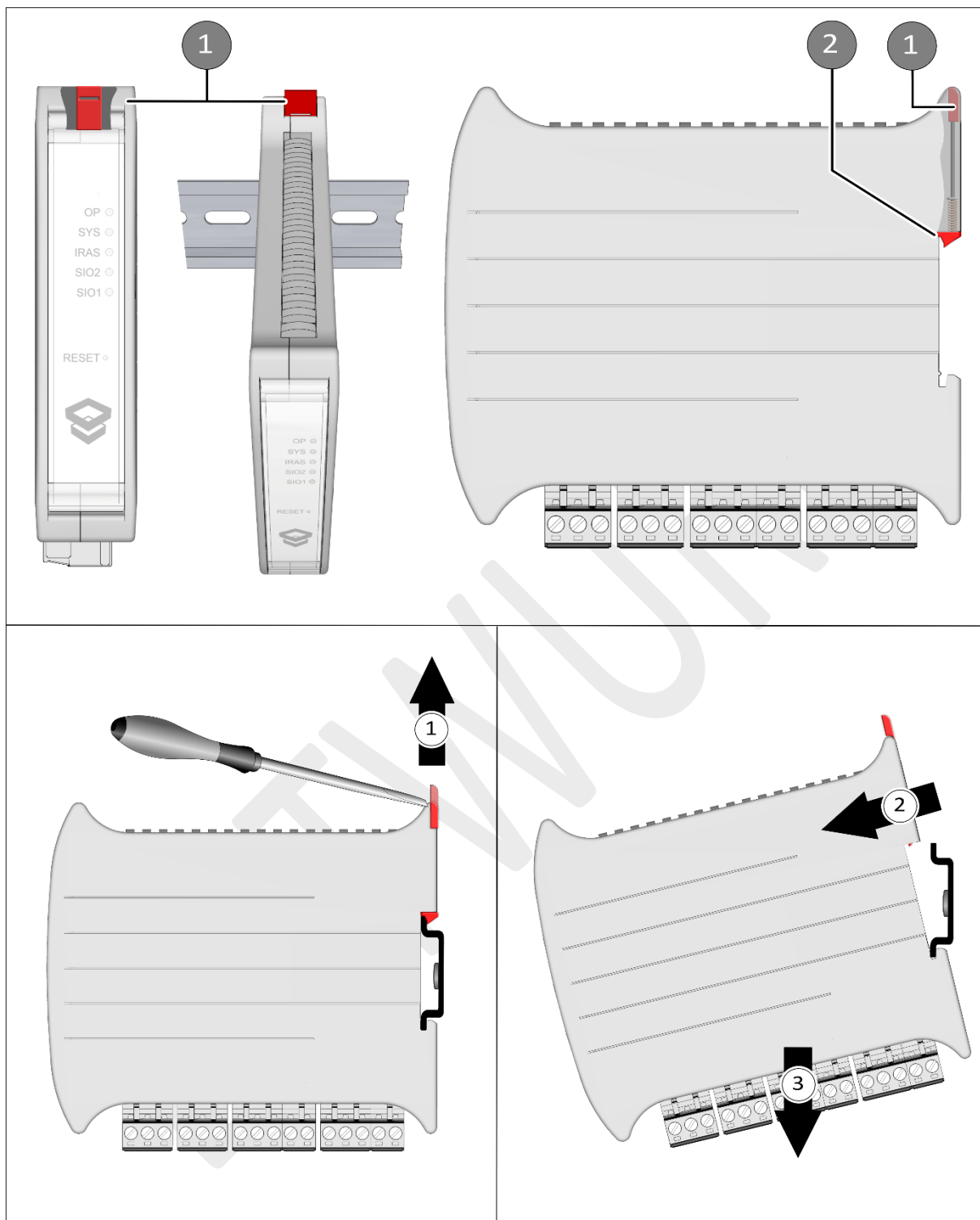


Abbildung 21: ADP4000-IRAS – Montage/Demontage

Pos	Beschreibung
1	Ver-/Entriegelung – Hebel
2	Ver-/Entriegelung – Arretierung auf der Hutschiene

6 Installation

6.1 Sicherheit



GEFAHR!

Lebensgefahr durch Stromschlag!

Durch Berühren spannungsführender Teile kann es zu schweren und tödlichen Verletzungen kommen.

- Elektrische Arbeiten dürfen nur durch eine ausgebildete Elektro-Fachkraft durchgeführt werden.
- Führen Sie Arbeiten am Gefahrenmeldesystem nur im spannungsfreien Zustand (Netz- und Notstromversorgung) durch.
- Trennen Sie die GMZ vor Beginn der Arbeiten von der Stromversorgung.
- Sichern Sie die GMZ vor unbeabsichtigtem Wiedereinschalten.



ACHTUNG!

Kurzschlussgefahr!

Durch unsachgemäßes Verlegen der Anschlussleitungen kann es zu einem Kurzschluss und in der Folge zur Beschädigung und zum Ausfall der Brandmeldeanlage kommen.

- Sichern Sie alle angeschlossenen Spannungs- und Signalleitungen mit geeignetem Befestigungsmaterial, wie z.B. Kabelbindern aus Kunststoff, gegen Verlagerung.
- Verlegen Sie die Spannungs- und Signalleitungen in den dafür vorgesehenen Kabelkanälen.
- Achten Sie darauf, dass die Netzanschlussleitung durch Verlagerung die Signalleitungen (SELV) nicht berühren können.
- Führen Sie Arbeiten am Gefahrenmeldesystem nur im spannungsfreien Zustand (Netz- und Notstromversorgung) durch.



ACHTUNG!

Beschädigung der GMZ und/oder angeschalteter Geräte!

Arbeiten an stromführenden Geräten/GMZ kann zu Sachschäden führen.

- Machen Sie die BMZ vor Beginn der Arbeiten stets stromlos und sichern Sie diese gegen unbeabsichtigtes Wiedereinschalten.



- Prüfen Sie nach abgeschlossener Installation den Isolationswiderstand des verwendeten Netz-Anschlusskabels (230-Netz). (Abbildung 22/A, B).
- Die Anschaltung muss abschließend von einer Fachkraft abgenommen werden.

6.2 IRAS-SECURE – Spannungsversorgung

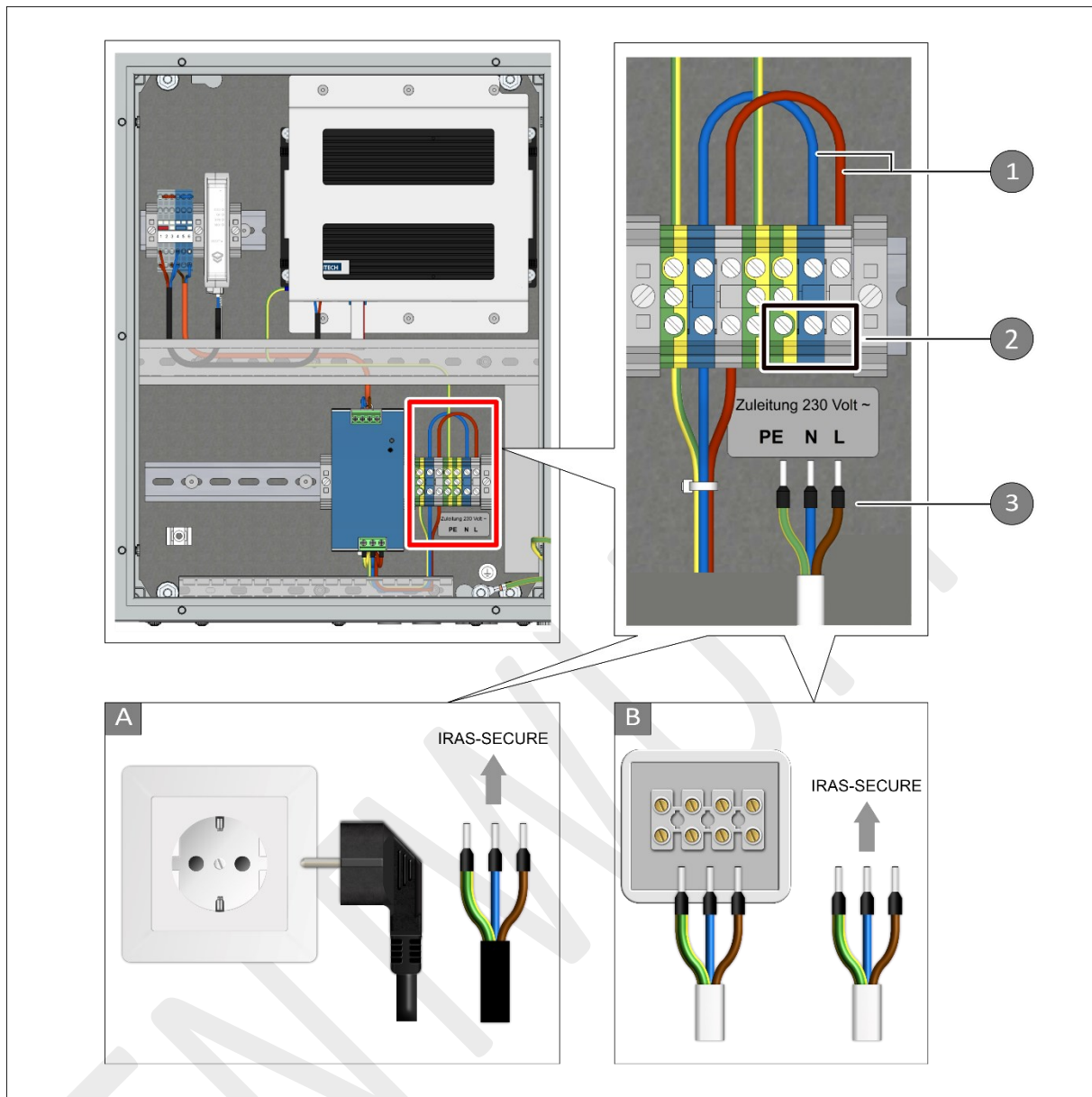


Abbildung 22: IRAS-SECURE – Anschluss 230V-Netz (Beispieldarstellung)

Pos	Beschreibung
1	Brücke Zuleitung Spannungsversorgung → Anschluss Netzteil
2	Anschlüsse Spannungsversorgung (Zuleitung)
3	Anschlusskabel Spannungsversorgung (Zuleitung 230V-Netz)
A/B	<u>mögliche Anschluss-Varianten:</u> Steckdose (A) Wanddose (B)

Der elektrische Anschluss von IRAS-SECURE erfolgt an ein 230 V-Netz. Die Umsetzung kann unter Berücksichtigung der spezifischen technischen Gegebenheiten der jeweiligen Gefahrenmeldeanlage individuell gewählt werden. Als Varianten sind u.a. der Anschluss über eine Steckdose oder eine Wanddose möglich.

Wir empfehlen eine B6 A-Vorsicherung.

6.2.1 USV-Modul



Zur Sicherstellung der Spannungsversorgung, z.B. bei Netzausfall, besteht die Möglichkeit der Integration eines USV-Moduls.

➞ [Siehe Kapitel 4.7 Systemerweiterungen.](#)

Informationen zur Anschaltung des optionalen USV-Moduls finden Sie in der [zugehörigen Betriebsanleitung](#) bzw. der [herstellereigenen Dokumentation](#).

6.3 Integration in die Gefahrenmeldeanlage (GMA)

IRAS-SECURE wird über den *ADP4000-IRAS* als Bestandteil eines redundanten Rings in die Gefahrenmeldeanlage integriert. Hierfür wird der Redundanzadapter *ADP4000* benötigt.

Der *ADP4000* wird an die GMZ angeschaltet. Hierbei muss der Redundanzadapter mit Hilfe eines M4-Schnittstellenmoduls an die jeweilige GMZ-Schnittstelle angepasst werden.

➞ [Siehe Kapitel 4.14 ADP4000.](#)



Umfassende Informationen zu Struktur, Funktion und Baugruppen des *Systems4000* und den Aufbau eines redundanten Systems finden Sie in der [Betriebsanleitung System4000](#).

6.3.1 Integration in einen vorhandenen redundanten Ring

Die Anschaltung von IRAS-SECURE/ADP4000-IRAS erfolgt am Redundanzadapter *ADP4000* oder an einer bereits vorhandenen Ring-Komponente. Dies können *System4000*-Geräte sein, z.B. Brandmeldeperipherie: *FAT4000*, *ABT4000*, *GMT4000* u.a.

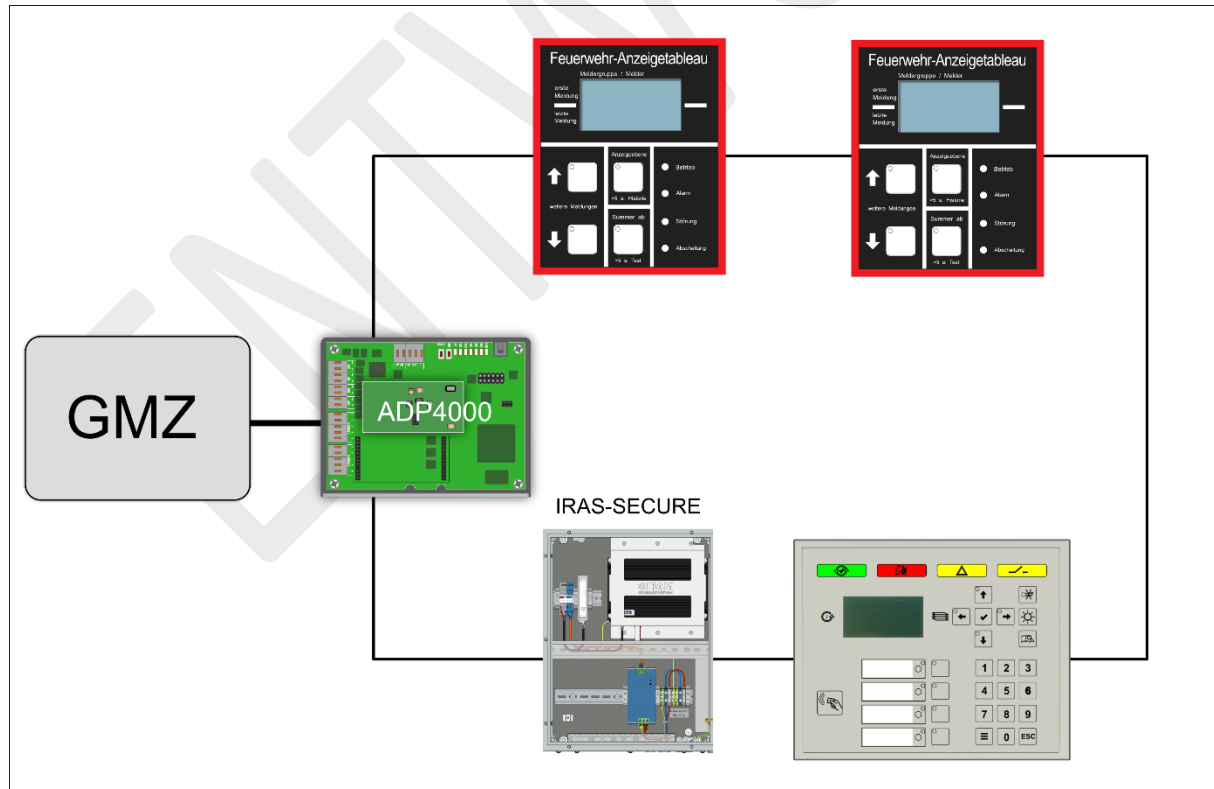


Abbildung 23: IRAS-SECURE – vorhandener redundanter Ring/ADP4000 (Beispiel)

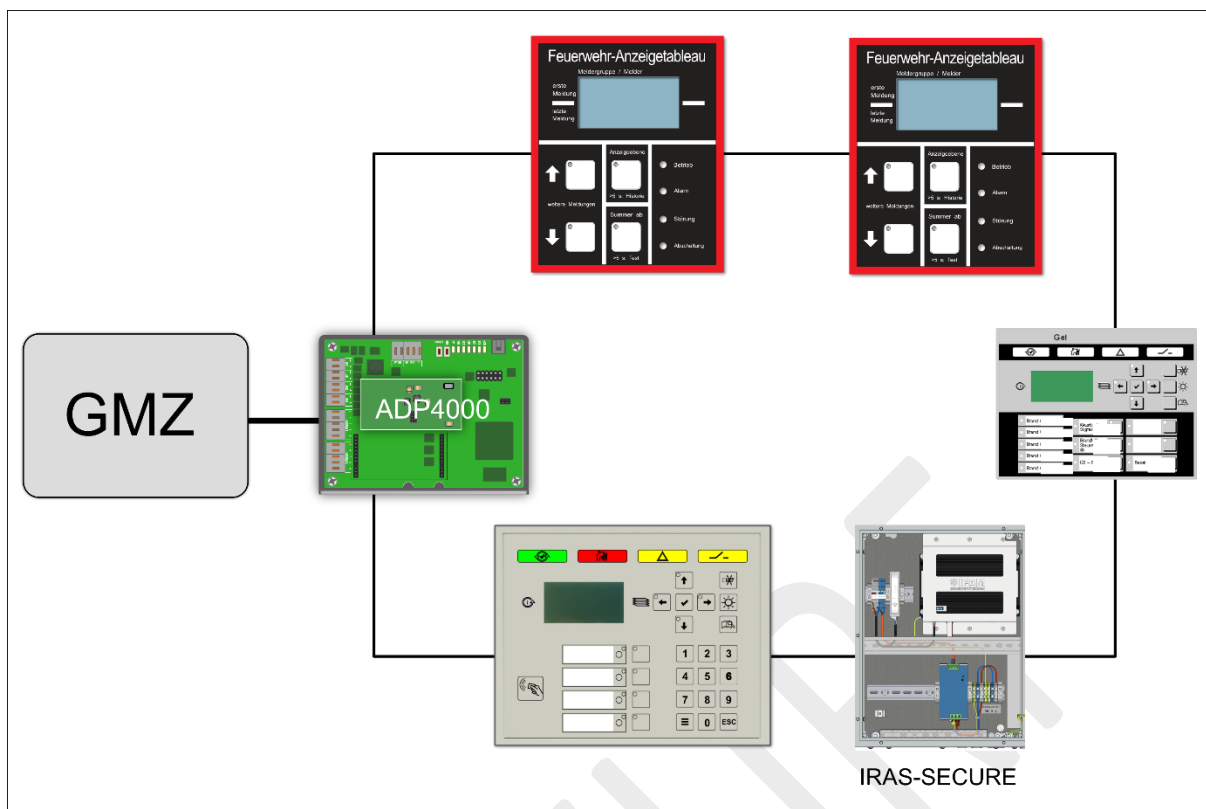


Abbildung 24: IRAS-SECURE – vorhandener redundanter Ring/Peripheriegerät (Beispiel)

6.3.2 Neuaufbau eines redundanten Rings

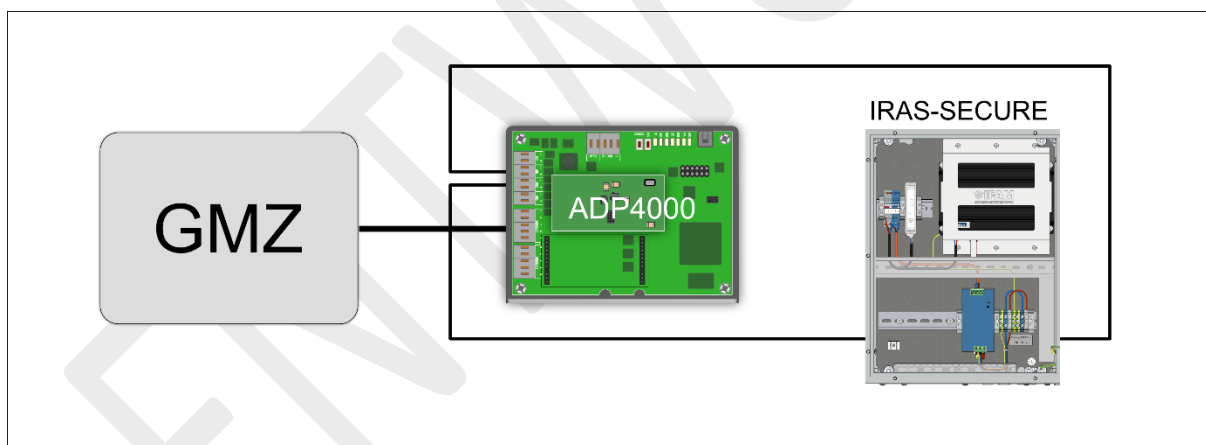


Abbildung 25: IRAS-SECURE – redundanter Ring/AD4000 und IRAS-SECURE (Beispiel)

6.3.3 Anschaltung – Prinzip

Bei einer redundanten Anschaltung werden die Signale **SIO1 und UB1** immer zu den Anschlüssen **SIO2 und UB2** des nächsten Gerätes geführt, bis der Ring wieder geschlossen wird. Das Signal **SIO1+** wird auf **SIO2+** und ebenso **SIO1-** auf **SIO2-** gelegt (Plus- auf Plus-Signal und Minus- auf Minus-Signal), d.h. die SIO-Signalleitungen sind 1:1 verbunden. Dies gilt auch für UB1-UB2-Verbindungen.

Die Schnittstelle der Gefahrenmeldezentrale (GMZ) muss wie in den zugehörigen Anschaltvorschriften angegeben parametrisiert werden.



Informationen zur Anschaltung des Redundanzadapters *ADP4000* an die verwendete Gefahrenmeldezentrale finden Sie in der [GMZ-spezifischen Installationsanleitung](#).

6.3.4 Anschaltung – Beispiele

Nachfolgend finden Sie ausgewählte Beispielanschlaltungen für unterschiedliche Ringstrukturen (redundanter Ring).

- IRAS-SECURE (allein) an ADP4000,
- IRAS-SECURE an eine bereits vorhandene Ringkomponente.

Die Spannungsversorgung von IRAS-SECURE wird durch das im System integrierte und bereits verkabelte Netzteil sichergestellt und ist daher in den Beispieldarstellungen nicht enthalten.

6.3.4.1 IRAS-SECURE (allein) – Prinzip

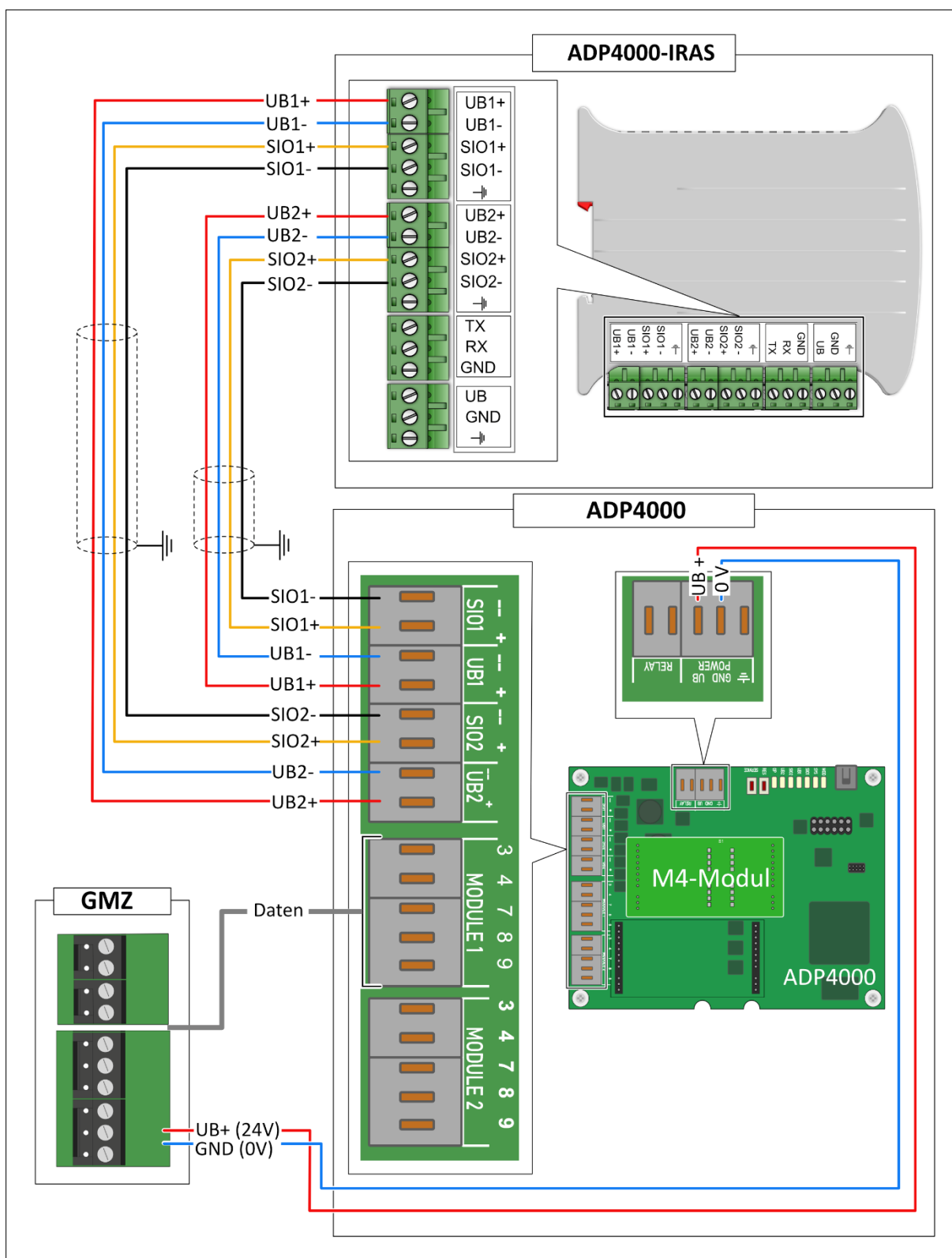


Abbildung 26: ADP4000-IRAS – Beispiel-Anschaltung/ADP4000

6.3.4.2 IRAS-Secure + 1 Peripheriegerät (Beispiel)

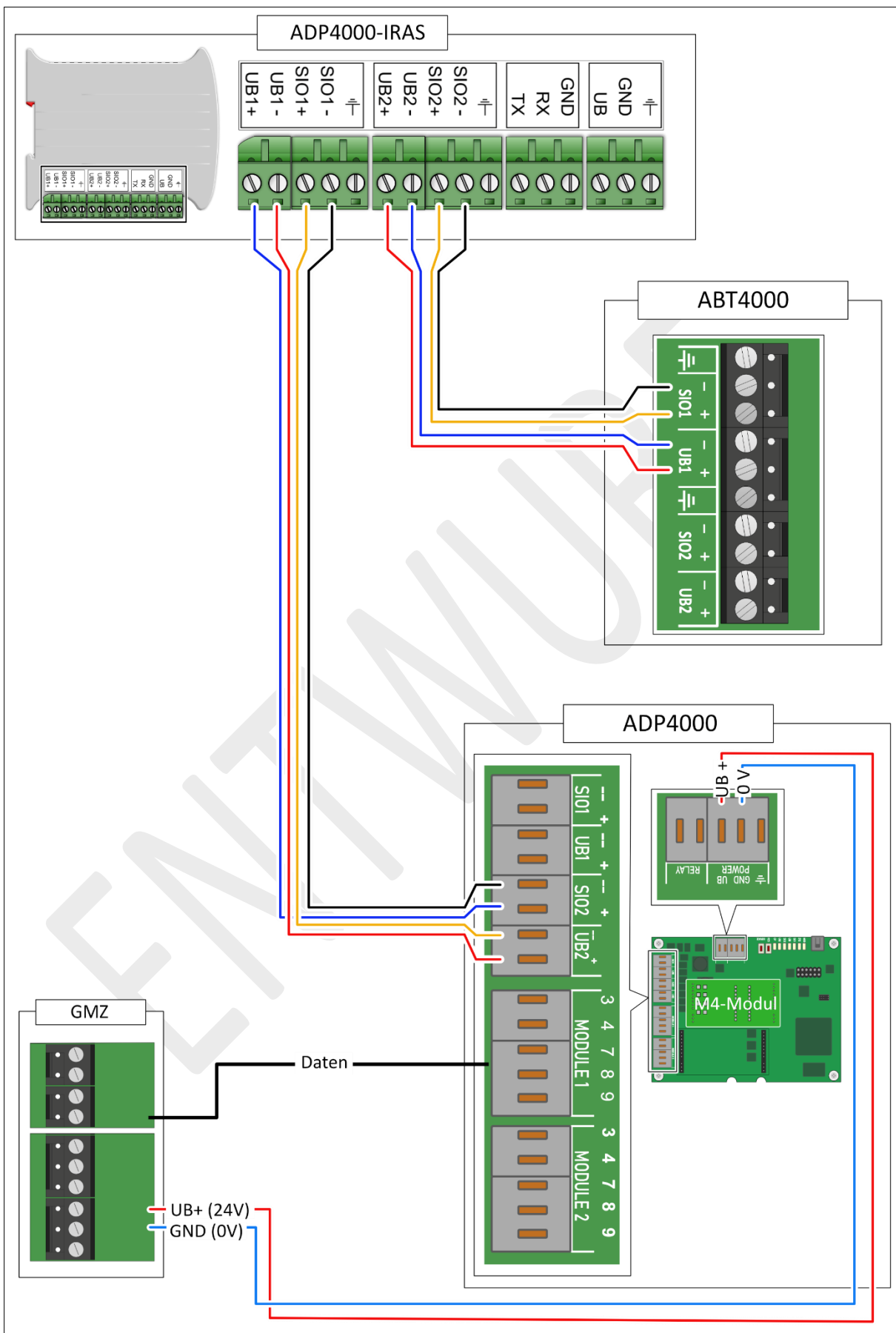


Abbildung 27: ADP4000-IRAS – Beispielanschlutung/1 Peripheriegerät (Beispiel)

6.3.5 Spannungsversorgung des ADP4000-IRAS



Die Stromversorgung des ADP4000-IRAS erfolgt trotz der redundanten Verdrahtung (UB) nicht über den dualen Ring, sondern wird über die gesonderte Spannungsversorgung des IRAS-SECURE-Systems realisiert.

➞ [Siehe Kapitel 4.10 Spannungsversorgung.](#)

6.4 Netzwerk-Anbindung

Für den Betrieb muss das IRAS-SECURE-Gefahrenmeldesystem in das Betreiber-eigene Netzwerk eingebunden werden. Verbinden Sie hierfür IRAS SECURE über die LAN-Schnittstelle (LAN A) (1) des Industrie-PCs mit der Infrastruktur des betriebereigenen Netzwerks. Für die Anschaltung empfehlen wir ein LAN-Kabel vom Typ CAT7/CAT8.

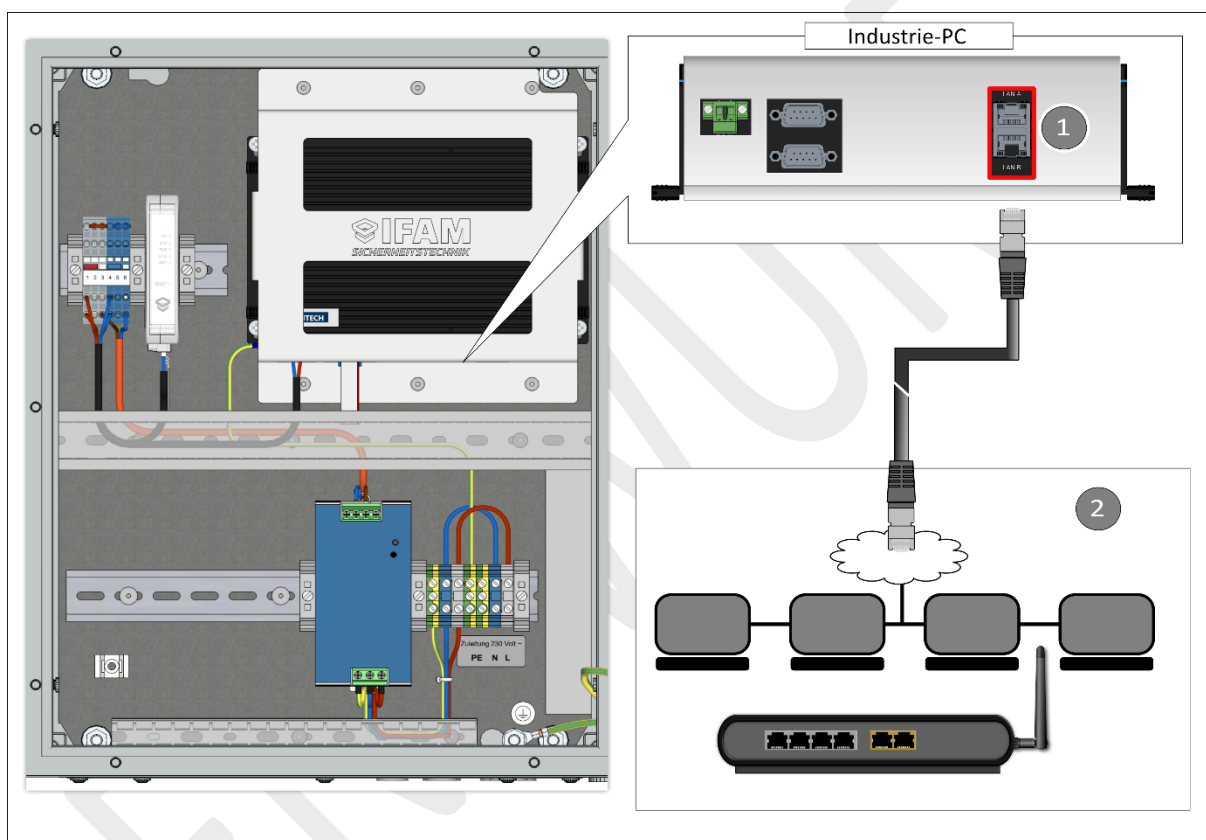


Abbildung 28: Installation Industrie-PC/Netzwerk, Modem



Informationen zu den zu verwendenden LAN-Schnittstellen des Netzwerkes entnehmen Sie bitte der [herstellereigenen Dokumentation der entsprechenden Geräte des Netzwerkbetreibers.](#)

Die gewählte LAN-Schnittstelle des Industrie-PCs muss abschließend konfiguriert werden.

➞ [Siehe Kapitel 9.4.1 Netzwerkverbindung.](#)

6.5 Hardware-Erweiterungen (optional)



Informationen zur Anschaltung von Hardware-Erweiterungen (USV und Modem) finden Sie den in den [Betriebs-/Installationsanleitungen der verwendeten Geräte.](#)

7 Inbetriebnahme

7.1 Sicherheit



- Transportsicherungen vor dem ersten Gebrauch entfernen.
- IRAS-SECURE darf nur mit geschlossenem Gehäuse betrieben werden.

7.2 IRAS-SECURE in Betrieb nehmen

Nach der Installation und der Integration von IRAS-SECURE in die Gefahrenmeldeanlage und anschließender Aktivierung der Spannungsversorgung ist die Hardware funktionsfähig. Ein separates Einschalten des Systems oder einzelner Komponenten ist nicht erforderlich. Erscheint nach dem Aufrufen der IRAS-Website die Login-Oberfläche wird hierdurch das ordnungsgemäße Funktionieren des Systems und dessen Betriebsbereitschaft bestätigt.

➞ *Siehe Kapitel 9.3.1 Anmeldung.*

Sollt dies nicht geschehen, prüfen Sie die Hardware auf Störungen/Fehler und die korrekt ausgeführte Installation (z.B. Anschlussleitungen, Spannungsversorgung).

➞ *Siehe auch Kapitel 10.1 Störungstabelle (häufige Störungen).*

7.3 Redundanter Ring – Einmessen der Komponenten

Nach der Erstinstallation oder Änderung der Topologie des redundanten Rings ist das Einmessen der Komponenten und die Messwert-Übernahme (Leitungen etc.) mit Hilfe der Konfigurationssoftware *Prog4000* erforderlich.



Das Konfigurationstool wird nicht auf einem physischen Datenträger (CD oder USB-Stick) zur Verfügung gestellt, sondern steht in der aktuellsten Version auf der Homepage der IFAM GmbH Erfurt zum Download bereit: www.ifam-erfurt.de/de/service-support/downloads (Bereich: [System4000](#) → [Prog4000](#)).

Laden Sie das Programm herunter und installieren Sie es auf einem PC. Das Konfigurationstool benötigt ein .NET-Framework ab Version 4.7.2. Das Setup-Programm installiert dieses Framework auf dem PC, falls es noch nicht vorhanden ist.



Wenn Sie *Prog4000* bereits verwenden, achten Sie darauf, dass Sie über die aktuelle Version verfügen: mindestens Version 1.3.1.0. Die Konfiguration von IRAS-SECURE ist mit einer älteren Version nicht möglich!

Verbinden Sie den Computer mit der USB-Schnittstelle des *Redundanzadapters ADP4000*.

➞ *Siehe Kapitel 4.14 ADP4000.*

Mit der USB-Verbindung zum *ADP4000* wird über die Hardwareerkennung des Betriebssystems das Gerät erkannt. Die nötigen Treiber sind bereits im Betriebssystem enthalten, sodass keine separate Treiberinstallation nötig ist.

7.3.1 Ring-Komponenten einlesen

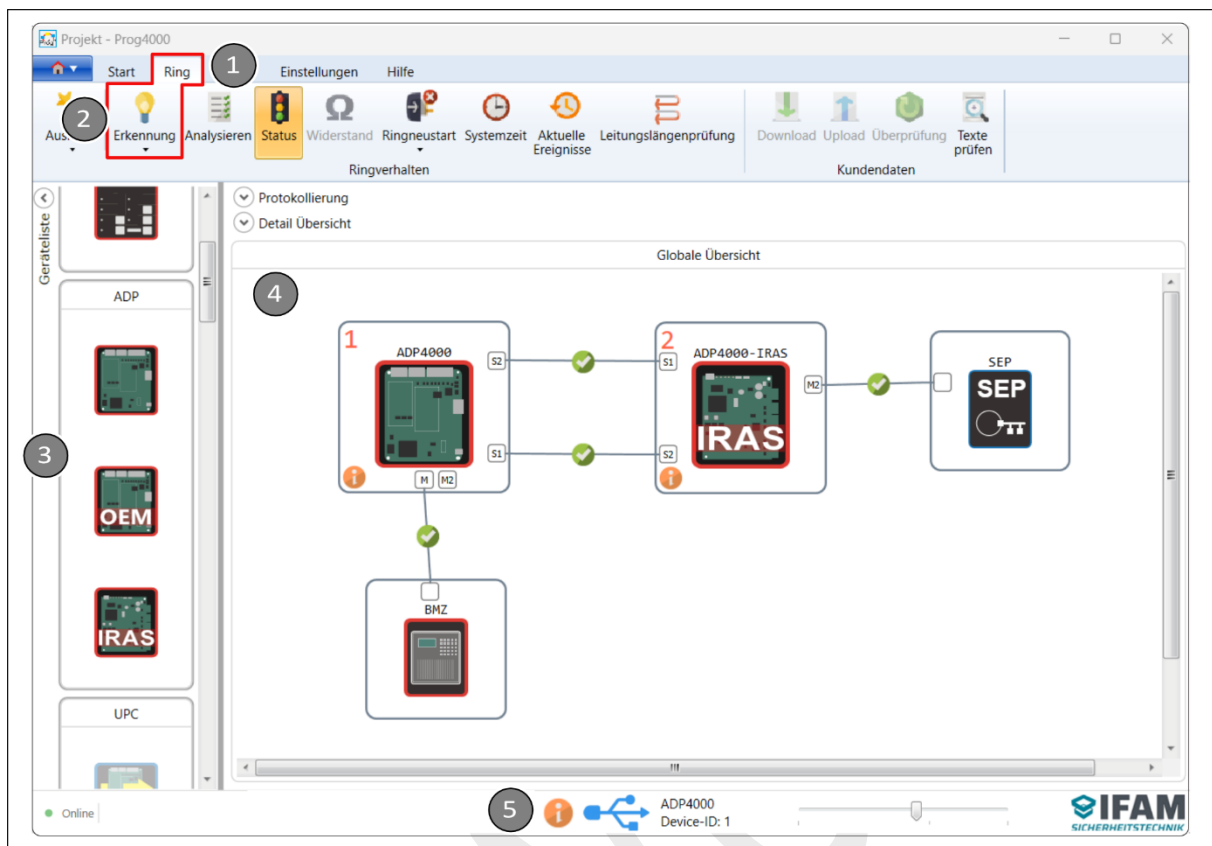


Abbildung 29: Prog4000 – Einlesen/Erkennung (Beispiel)

Für das automatische Einlesen/Erkennen der Komponenten des dualen Rings gehen Sie wie folgt vor:

1. Starten Sie *Prog4000*. → Der Hauptbildschirm wird geöffnet.
2. Wählen Sie im Hauptmenü die Registerkarte RING (1). Aktivieren Sie die Schaltfläche ERKENNUNG (2). → In der Globalen Übersicht (4) wird die Topologie des vorhandenen Systems dargestellt. Am unteren Rand wird die Kennung der aktiven Kopplung (5) angezeigt.

- ✓ Zeigt an, dass die Geräte korrekt miteinander verbunden wurden/keine Störungen vorliegen.
- ✗ Zeigt an, dass eine Störung vorliegt. Klicken Sie doppelt auf das Symbol. → Ein Fenster mit Störungsdetails öffnet sich. Beheben Sie die Störung.
- i Zeigt an, dass eine Meldung/Störungsmeldung für das Gerät vorliegt. Klicken Sie doppelt auf das Symbol. → Ein Fenster mit Informationen/Störungsdetails öffnet sich. Beheben Sie ggf. die Störung.

3. Fügen Sie aus der Geräteleiste das SEP-Protokoll hinzu (falls noch nicht vorhanden) und verbinden Sie es mit dem ADP4000-IRAS.

4. Klicken Sie anschließend doppelt auf das SEP-Symbol. → Die SEP-Ebene öffnet sich.

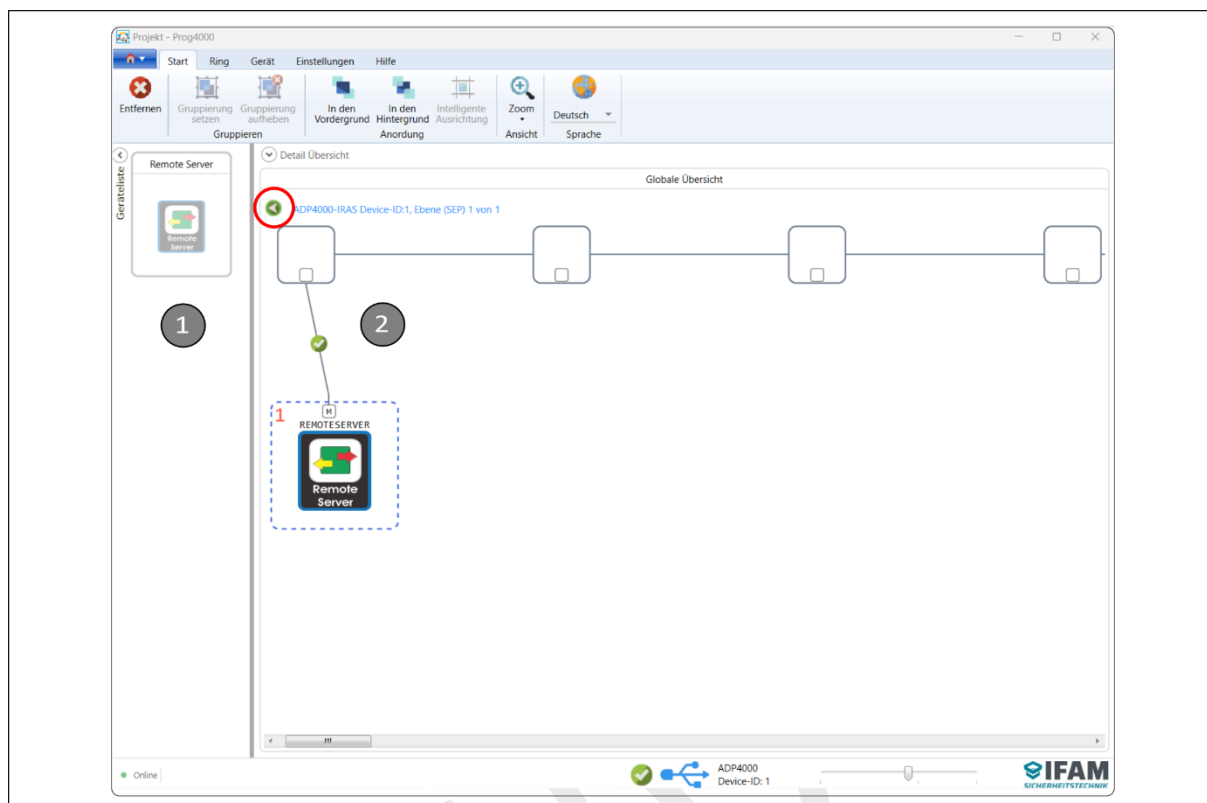


Abbildung 30: Prog4000 – SEP-Ebene (Beispiel)

5. Ziehen Sie das Symbol REMOTE SERVER (1) in die GLOBALE ÜBERSICHT und verbinden Sie es mit dem ersten Knotenpunkt der Stichleitung (2). Kehren Sie zur System-Topologie zurück (←).



Sie haben die Möglichkeit, die erkannte System-Topologie für eine spätere Konfiguration bzw. zur Sicherung zu speichern.

➔ [Siehe Kapitel 8.8 Projekt sichern.](#)

7.3.2 Ring-Komponenten einmessen



Hinweise zum Einmessen der Komponenten des redundanten Rings finden Sie im [Quickstart – System4000 redundant](#) oder in der [Konfigurationsanleitung Prog4000](#).



Ist mehr als ein **ADP4000** im Ring enthalten muss die messtechnische Inbetriebnahme am **ADP1** durchgeführt werden (nur dieser ADP versorgt den Ring mit Betriebsspannung).

8 Konfiguration (GMA/Prog4000)

Nach Abschluss der Installation und dem Einmessen der Komponenten des redundanten Rings muss eine Konfiguration zur Einbindung von IRAS-SECURE in die Gefahrenmeldeanlage mithilfe der Konfigurationstools *Prog4000* vorgenommen werden.

Nachfolgend werden nur die Funktionen des *Prog4000* beschrieben, die für die Inbetriebnahme von IRAS-SECURE notwendig sind.



Umfassende Hinweise zu Struktur und Bedienung der Konfigurationssoftware *Prog4000* finden Sie in der [Konfigurationsanleitung Prog4000](#).

1. Öffnen Sie die Systemtopologie bzw. legen sie diese neu an.
 [Siehe Kapitel 7.3.1 Ring-Komponenten einlesen](#).
2. Klicke Sie doppelt auf das IRAS-/ADP4000-Symbol. → Die Konfigurationsoberfläche wird geöffnet.

Die Konfigurationsoberfläche kann, je nach ausgewähltem Gerät folgende Registerkarten enthalten:

- Allgemein,
- FBF,
- Relais (ADP4000),
- BMZ-Schnittstelle (ADP4000),
- Code-Tabellen-Editor,
- Text-Dialog-Editor,
- Meldungsfilter.

8.1 Allgemeine Einstellungen (Allgemein)

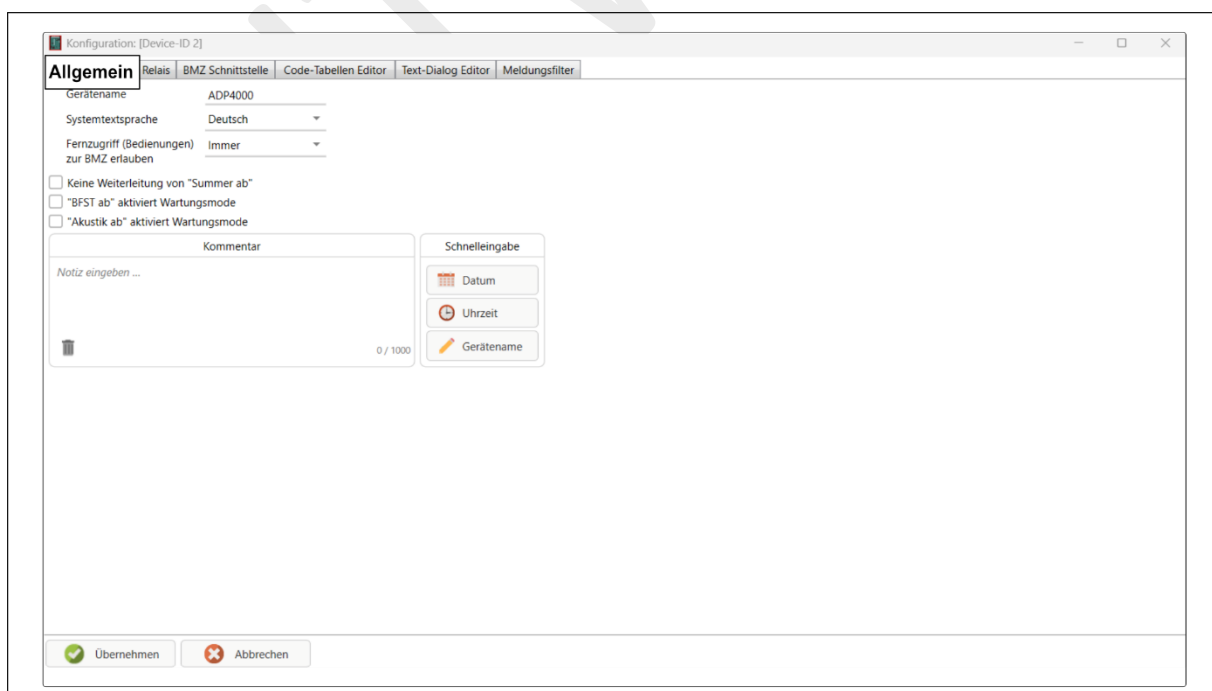


Abbildung 31: Prog4000 – Allgemein (Beispiel)

Auf der Registerkarte ALLGEMEIN können allgemeine Einstellungen (u.a. zur Systemsprache und weiteren spezielle Funktionen) vorgenommen werden.

8.2 Relais konfigurieren

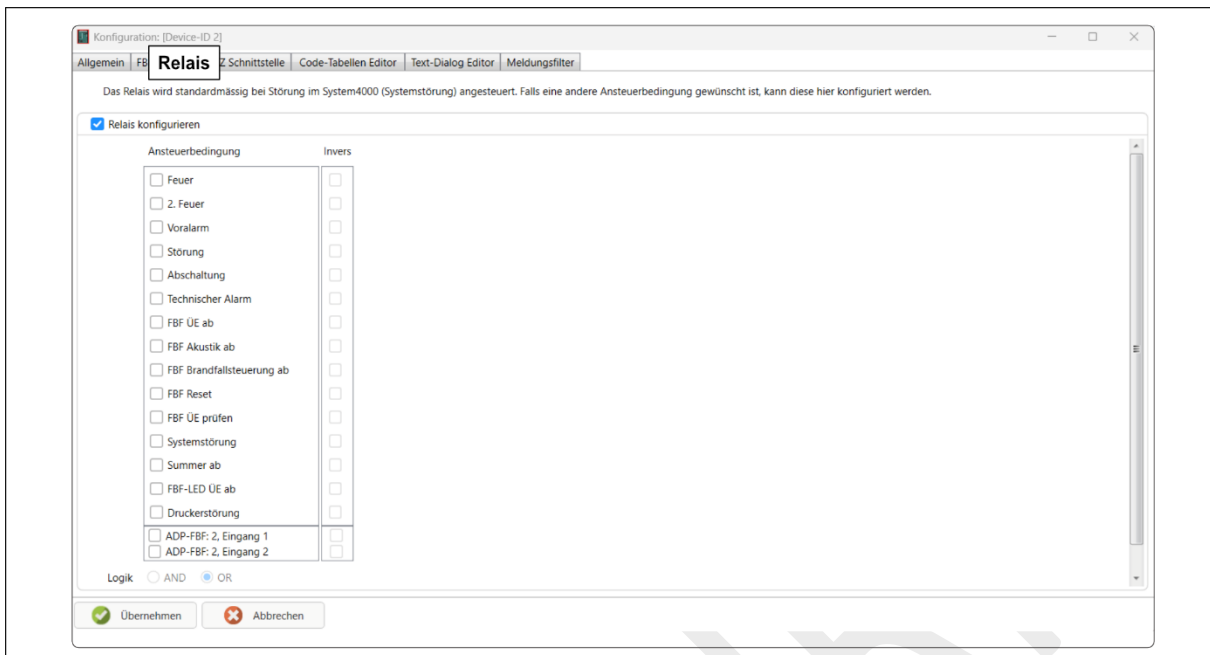


Abbildung 32: Prog4000 – Relais (Beispiel)

Falls am ADP4000 ein Störungsrelais angeschaltet ist, kann es individuell konfiguriert werden. Das Relais wird standardmäßig bei einer Störung im System4000 angesteuert. Falls eine andere Ansteuerbedingung gewünscht ist, kann diese hier angegeben werden.

8.3 BMZ-Schnittstelle

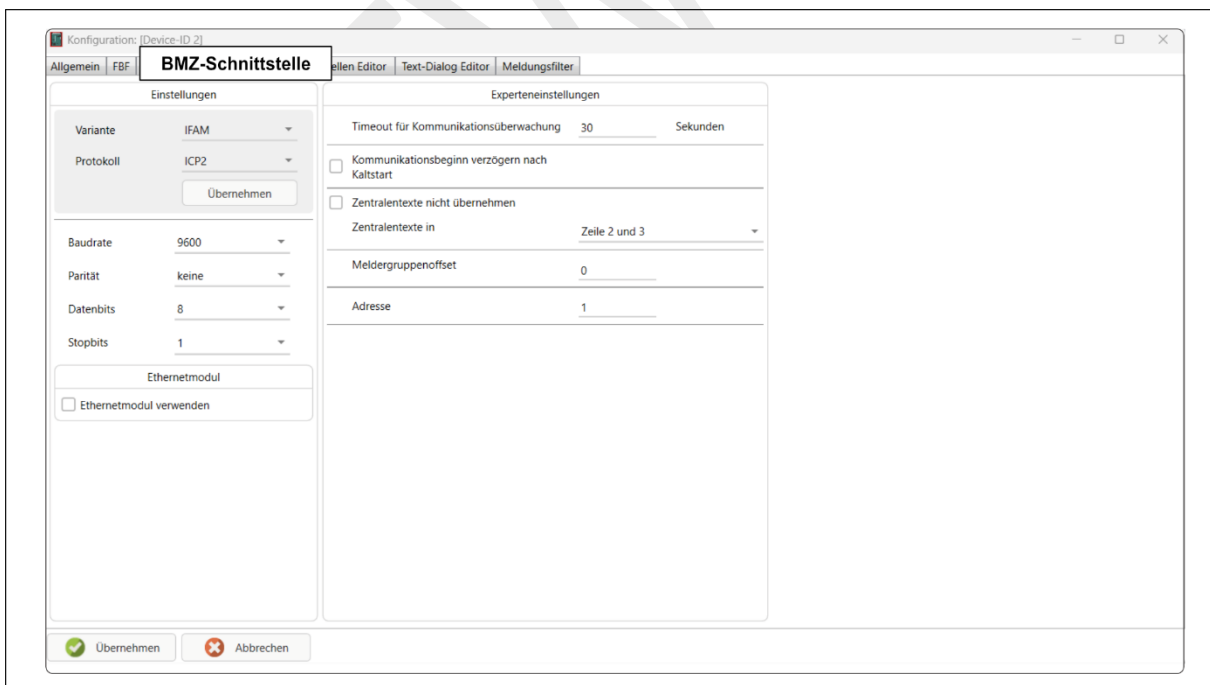


Abbildung 33; Prog4000 – BMZ-Schnittstelle (Beispiel)*

Wurde ein redundanter Ring im Rahmen der Installation neu aufgebaut, muss am ADP4000 die Schnittstelle zur GMZ* konfiguriert werden.

Auf der Registerkarte werden, sofern eine GMZ konfiguriert ist, zur Schnittstelle passende Konfigurationsmöglichkeiten angezeigt. Entsprechend der Variante und dem Protokoll sind bei den Einstellungen Standardwerte vorkonfiguriert. Diese sollten beibehalten werden.

Es können u.a. angezeigt/angepasst werden:

- BMZ-Typ,
- Protokoll,
- Baudrate.
- Parität,
- Datenbits,
- Stopbits,
- Experteneinstellungen (z.B. Kommunikationsüberwachung, Anzeigeoptionen).

* Die verwendete Bezeichnung *BMZ* bezieht sich hier neben Brandmelderzentralen auf alle im Anwendungsbereich von IRAS-SECURE möglichen Arten von Gefahrenmeldezentralen (GMZ).

8.4 Externe Schnittstelle (SEP)

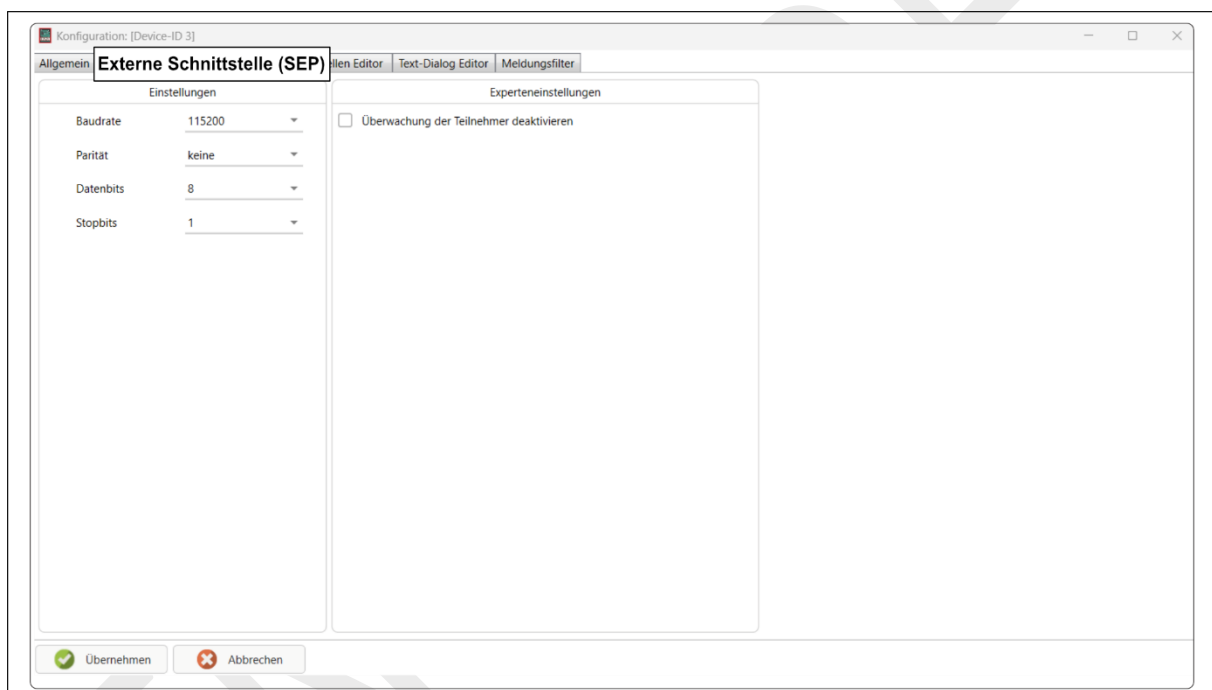


Abbildung 34: Prog4000 – Externe Schnittstelle (SEP)

Auf der Registerkarte EXTERNE SCHNITTSTELLE (SEP) werden zur Schnittstelle des angeschalteten Remoteservers passende Konfigurationsmöglichkeiten angezeigt. Entsprechend der Variante und dem Protokoll sind bei den Einstellungen Standardwerte vorkonfiguriert. Diese sollten beibehalten werden.

Darüber hinaus kann optional eine Überwachung von Teilnehmern aktiviert bzw. deaktiviert werden.

8.5 Code-Tabellen-Editor

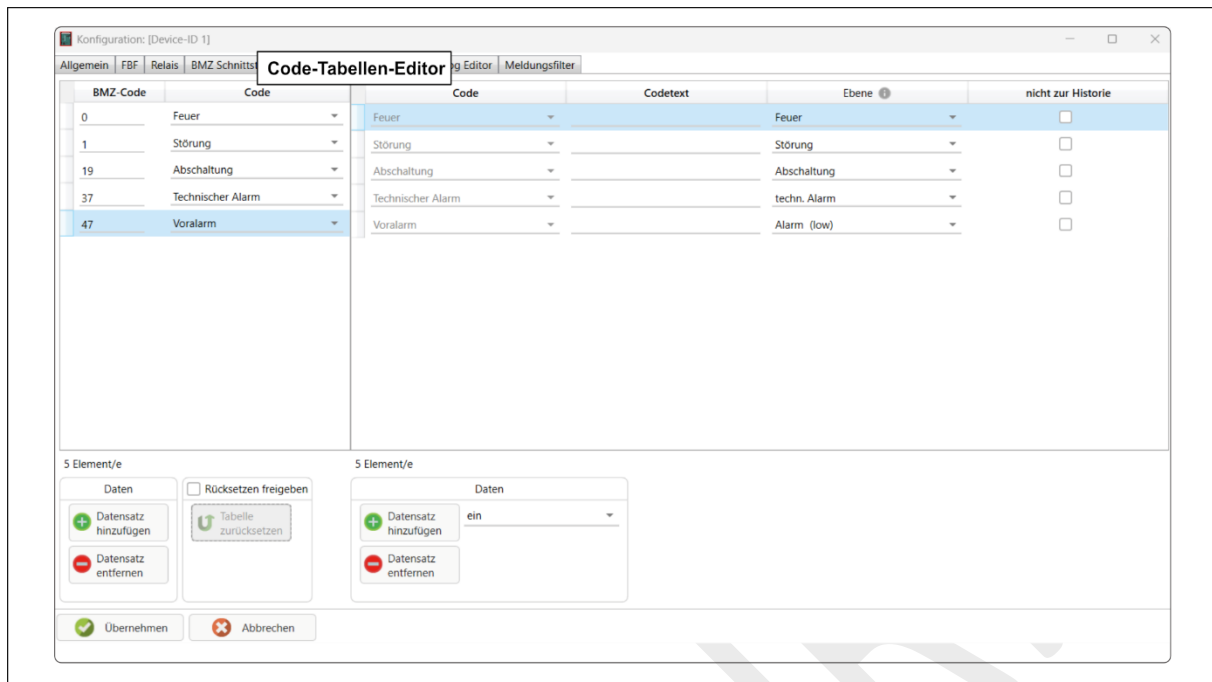


Abbildung 35: Prog4000 – Code-Tabellen-Editor (Beispiel)

In der Registerkarte CODE-TABELLEN EDITOR können die anzuzeigenden Meldungstypen (Codes) sowie die Zuordnung zwischen BMZ-Code, internem Code und der Anzeigeebene festgelegt werden.

8.6 Text-Dialog-Editor

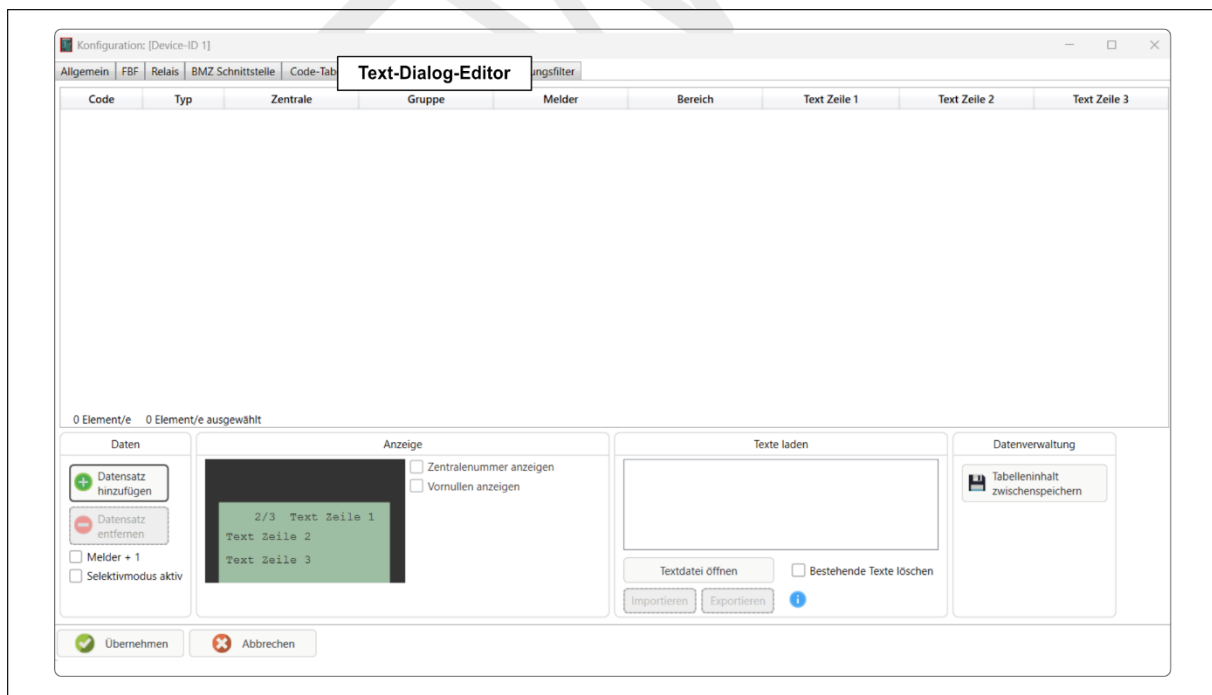


Abbildung 36: Prog4000 – Text-Dialog-Editor (Beispiel)

Falls die Meldungstexte nicht über die Schnittstelle von der BMZ geliefert werden oder wenn spezielle Einstellungen nötig sind, können im Register TEXT-DIALOG EDITOR benutzer-spezifische Texte hinterlegt werden. Darüber hinaus ist auch ein Import/Export von Texten in verschiedenen Formaten möglich.

8.7 Schreiben der Konfiguration in das Gerät (Upload)

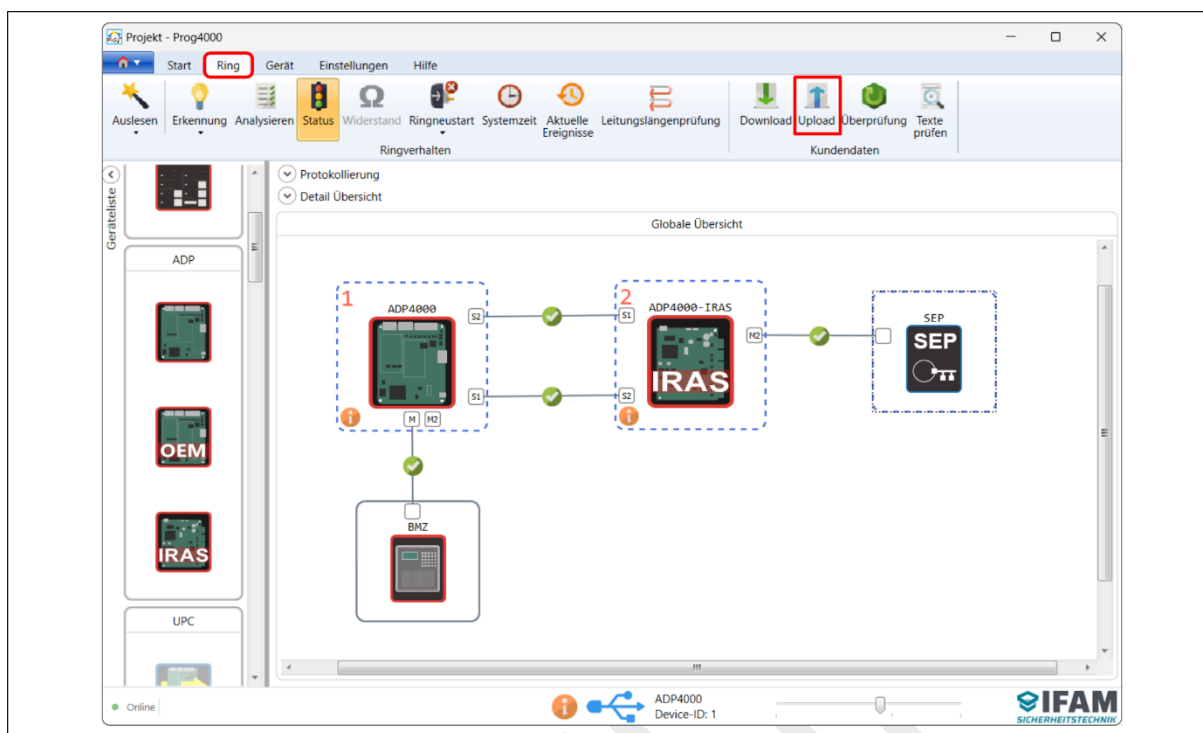


Abbildung 37: Prolog4000 – Konfiguration schreiben (Beispiel)



Abbildung 38: Prolog4000 – Gerätekonfiguration schreiben/Status

Markieren Sie das betreffende Gerät in der GLOBALEN ÜBERSICHT.

Durch die Aktivierung der Schaltfläche UPLOAD auf der Registerkarte RING wird der Vorgang gestartet und in einem separaten Fenster angezeigt (Abbildung 38). Dieses wird nach Abschluss des Vorgangs automatisch geschlossen.

8.8 Projekt sichern

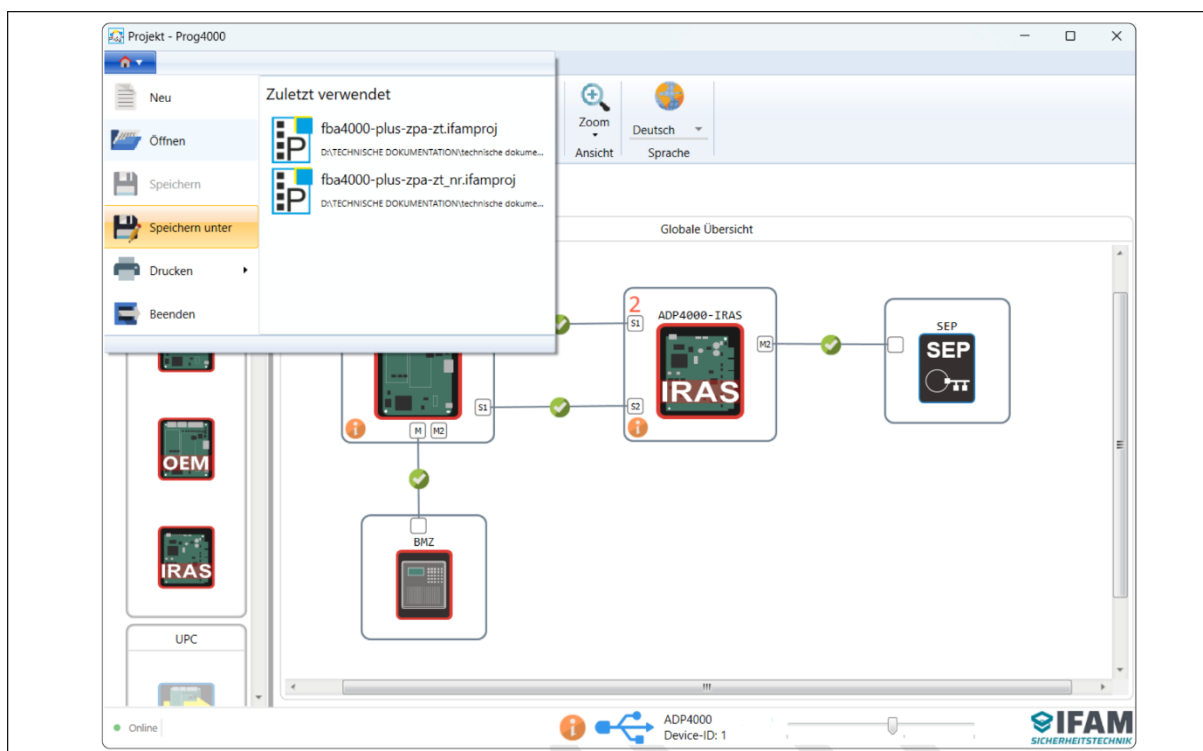


Abbildung 40: Prolog4000 – Projekt sichern (Beispiel)

Vorhandene Systemtopologien und darin vorgenommene Konfigurationen können zur Sicherung auf einem PC oder auf einem externen Medium gespeichert (Menü HAUPTMENÜ | SPEICHERN UNTER) und geöffnet (HAUPTMENÜ | ÖFFNEN) werden.

9 Betrieb

9.1 Sicherheit

9.1.1 Datensicherheit

9.1.1.1 Zusätzliche Dokumente

Als zusätzliche Dokumente werden im allgemeinen Dateien bezeichnet, die Ereignissen oder Meldungen zugeordnet werden können. IRAS-SECURE nimmt diese Dateien in einem Hochlade-Prozess entgegen und stellt sie allen Nutzern ungeprüft und unverändert zur Verfügung. Für den Inhalt der Dateien ist allein der hochladende Nutzer verantwortlich.



Auf dem System, auf dem die Dateien benutzt werden, sollte ein Virens Scanner mit aktueller Virendefinition vorhanden sein.

9.1.2 Sichere Netzwerkverbindung

Um eine sichere Kommunikation zwischen Ihrem Endgerät und IRAS-SECURE zu gewährleisten, sollte **SSL/HTTPS** verwendet werden.

➞ *Siehe Kapitel 9.4.1.2 SSL/TLS konfigurieren.*

9.2 Datennutzung

Beim IRAS-SECURE-Gefahrenmeldesystem handelt es sich um einen Webserver, der Nutzern ein Interface für eine mobile App und eine Web-Oberfläche bietet. Die Datenmenge kann je nach Häufigkeit der Anwendung, Anzahl der Nutzer, Laufkarten, Projekten oder Geräten bei mehreren Gigabyte pro Monat liegen.

Beispiel 1:

Nutzer/ Geräte	tägliche Nutzungszeit	Arbeits-tage je Monat	Events	Revision	Polling Intervall	geschätzte Datenmenge
2	8h	20 Tage	1	Ja	1s	2,304 GB
2	8h	20 Tage	1	Nein	1s	1,152 GB

Die Datenmenge ist abhängig von der Größe und Anzahl der Laufkarten.

Die IP-Kamera wird über IRAS-SECURE zu den gewählten mobilen Geräten getunnelt.

Dadurch fallen die Daten des Streams an. Die jeweiligen Datenmengen sind abhängig von der Bildqualität und den Bildern pro Sekunde der Kamera. Jedes Gerät verursacht eine individuelle Datenmenge auf dem IRAS-Gefahrenmeldesystem.

Das Versenden von Push-Nachrichten und E-Mails beeinflusst ebenfalls die Datennutzung.



Die Nutzung mobiler Netzwerke kann u.U. hohe Kosten verursachen. Bitte prüfen Sie Ihre vertragliche Bedingung und vergleichen diese mit Ihrer monatlichen Nutzung des IRAS-Gefahrenmeldesystem.
(evtl. BA Modem?)



Achten Sie bei der Auswahl Ihres Anbieters darauf, dass eine Datenverbindung auch dann noch möglich ist, wenn die inkludierte Volumengrenze bereits erreicht/ überschritten ist. Dies garantiert Ihnen, auch bei kurzzeitiger Bandbreitenbegrenzung (~32kBit/s), weiterhin Meldungen des Systems zu erhalten.

Beispiel 2:

Die App ist auf 5 Geräten dauerhaft aktiv und im Vordergrund.

Nutzer/ Geräte	tägliche Nutzungszeit	Nutzungsintervall je Monat	Events	Revision	Polling Intervall	geschätzte Datenmenge
5 ⁽¹⁾	24h	31 Tage	0	Nein	1s	26,78 GB

Beispiel 3:

Das Feuerwehrdrucksystem überwacht einen ⁽³⁾ Drucker dauerhaft auf Störungen. Je Anfrage 6KB ⁽²⁾ (kombiniert Up- und Downstream) im Intervall von 60 Sekunden (je nach Firmwarestand) ergeben eine monatliche Datenmenge von 267,84MB (bei älteren Systemen 535,68MB).



Die geschätzten Datenmengen variieren je nach Nutzung des IRAS-Gefahrenmeldesystem und können teilweise erheblich höher liegen.

- (1) Es werden 2KB/s je Nutzer angenommen.
- (2) Es kann zu leichten Abweichungen je nach verwendetem Druckertyp kommen.
- (3) Das Datenvolumen addiert sich für jeden weiteren Drucker dazu.

9.2.1 Methoden zur Reduzierung der Datenmenge

- Anzahl der geöffneten und aktiven Apps reduzieren.

9.3 IRAS-Website

Die IRAS-Website ist das grundlegende Konfigurations-, Anzeige- und Bedienelement des IRAS-SECURE-Gefahrenmeldesystems. Hier werden vorliegende Meldungen und mit den jeweiligen Meldepunkten/Meldergruppen verbundene Informationen/Dokumente für z.B. Ersteinsatzkräfte wie Feuerwehren angezeigt/bereitgestellt. Darüber hinaus kann die Konfiguration des Gefahrenmeldesystems und dessen Komponenten, die Festlegung von Übertragungsoptionen von Meldungen sowie die Wartung und die Verwaltung von IRAS-SECURE durchgeführt bzw. unterstützt werden.

9.3.1 Anmeldung

Für die Anmeldung an der IRAS-Website muss IRAS-SECURE mit dem Betreiber-eigenen Netzwerk/PC verbunden sein.

Rufen Sie die IRAS-Website unter der vergebenen IP-Adresse auf. → Es erscheint die Login-Oberfläche (Abbildung 41).

Abbildung 41: IRAS-Website – Login

Abbildung 42: IRAS-Website – Login/Sicherheit

Geben Sie Ihre Anmeldedaten (Benutzername und Passwort) ein und bestätigen Sie (ANMELDEN).

Nach einer erfolgreichen Anmeldung erscheint die Hauptseite der IRAS-Website, das DASHBOARD (Abbildung 49).

Auf der Login-Oberfläche haben Sie darüber hinaus die Möglichkeit, die **Sprache** der Website anzupassen (Deutsch/Englisch) und das bestehende **Passwort** nach ausgeführtem Login zu **ändern**.



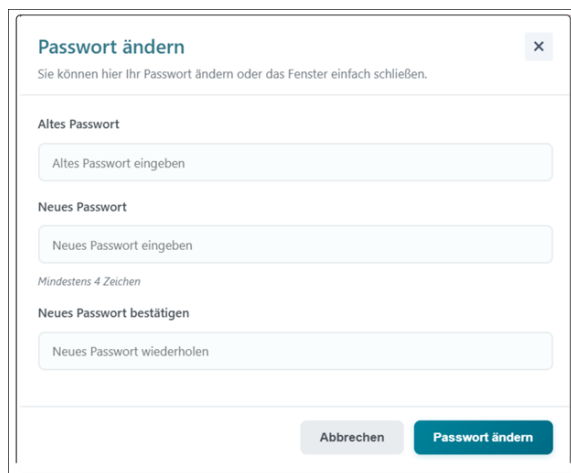
Nach dreimaliger Falscheingabe der Zugangsdaten erfolgt eine Sicherheitsprüfung (Abbildung 42), bei der ein Sicherheitscode durch Eingabe bestätigt werden muss. Hierdurch wird sichergestellt, dass kein unberechtigter, automatisierter Zugriff erfolgt. Die Eingabe dient der Bestätigung eines menschlichen Anwenders.

9.3.1.1 Erstanmeldung

Rufen Sie die IRAS-Website unter der in den Lieferinformationen (auf der Innenseite der Gehäusetür) vermerkten IP-Adresse auf.

Die Daten für die erstmalige Anmeldung Benutzername und (einmaliges) Passwort finden Sie ebenfalls in den Lieferinformationen.

➡ *Siehe Kapitel 18.1.1 IRAS-SECURE (System) – Lieferinformationen.*



Im Rahmen der Erstanmeldung erscheint nach korrekter Eingabe der Anmeldedaten und deren Bestätigung die Aufforderung zur Änderung des Passworts.

Vergeben Sie ein neues, sicheres Passwort (mindestens 4 Zeichen).

Bestätigen Sie die Eingabe abschließend (PASSWORT ÄNDERN).

Abbildung 43: IRAS-Website – Passwort ändern

9.3.2 Logout/automatische Abmeldung

9.3.2.1 Logout

Sie können sich von der Website abmelden, indem Sie die Schaltfläche **BENUTZER ABMELDEN** am rechten Rand der Menüleiste betätigen.

➡ [Siehe Kapitel 9.3.4 Dashboard.](#)

9.3.2.2 Automatische Abmeldung



Beachten Sie, dass die IRAS-Website nach **5 Minuten** der Inaktivität aus Sicherheitsgründen automatisch abgemeldet wird. Für eine Fortsetzung der Arbeit ist dann eine Neuanmeldung erforderlich. Kurz vor Ablauf des Zeitfensters erscheint jedoch am unteren Rand der aktuellen Seite die Aufforderung zur Verlängerung der Sitzung.

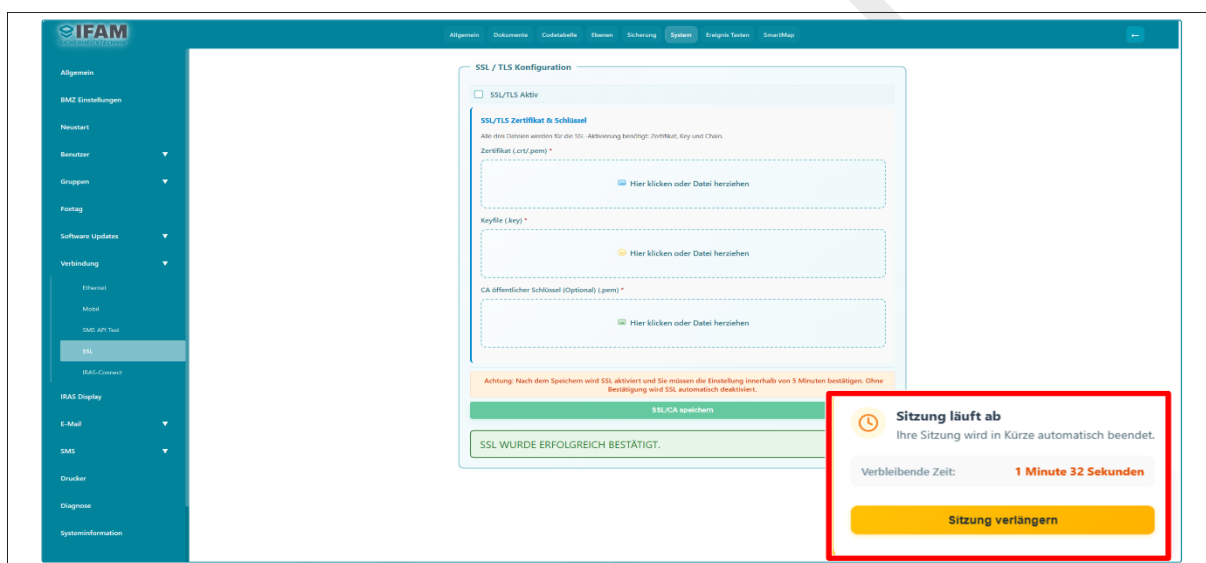


Abbildung 44: IRAS-Website – Sitzung verlängern

9.3.3 Systemzugang sichern

Zur Sicherung des Systemzugangs und zur Berechtigung zum Ausführen ausgewählter Funktionen stehen drei Optionen zur Verfügung:

- Passwort,
- Zwei-Faktor-Authentifizierung,
- (Pin für Funktionstasten im Rahmen der Erweiterung IRAS-CONTROL).

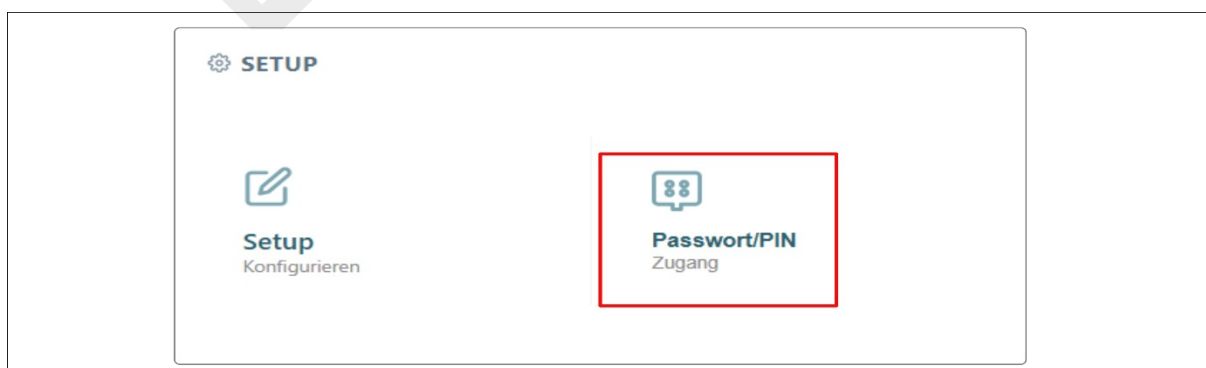


Abbildung 45: IRAS-Website – Dashboard/Passwort, Pin

1. Wählen Sie auf dem Dashboard, im Funktionsfeld SETUP die Option PASSWORT/PIN. → Die Konfigurationsoberfläche zur Auswahl von Sicherheitsoption wird geöffnet (Abbildung 46).

Abbildung 46: IRAS-Website – Passwort/Pin ändern

9.3.3.1 Passwort vergeben/ändern

Zur Vergabe/Änderung eines Passworts zum Systemzugang (IRAS-Website) geben Sie im Bereich PASSWORT ÄNDERN (1) das alte Passwort ein. Bestimmen Sie ein neues (mind. 4 Zeichen) und bestätigen Sie.

➞ Zur Erstanmeldung siehe Kapitel 9.3.1.1 Erstanmeldung.

9.3.3.2 Zwei-Faktor-Authentifizierung einrichten

Die 2-Faktor-Authentifizierung ist als zusätzliche Sicherung eines Benutzerkontos oder als Voraussetzung zur Ausführung bestimmter Systemfunktionen (z.B. Werksreset), möglich/nötig. Der Systemadministrator kann für einen Benutzer auch eine entsprechende Pflicht zur Nutzung dieser Methode festlegen.

Voraussetzung:

Auf einem zweiten Gerät (z.B. Smartphone, PC) muss eine Authenticator-App eingerichtet sein. Wählen Sie hierfür eines der verfügbaren Angebote (z. B. *Microsoft Authenticator*).

1. Wählen Sie im Bereich ZWEI-FAKTOR-AUTHENTIFIZIERUNG (TOTP) die Schaltfläche TOTP EINRICHTEN. (Abbildung 46 (3)) → Die Konfigurationsoberfläche wird geöffnet.

Zwei-Faktor-Authentifizierung (TOTP) NICHT AKTIVIERT

Schützen Sie Ihr Konto mit einem zusätzlichen Sicherheitscode aus einer Authenticator-App (z.B. Google Authenticator, Microsoft Authenticator, Authy).

Schritt 1: QR-Code scannen



Scannen Sie diesen QR-Code mit Ihrer Authenticator-App.

Manueller Code:
RMQHNCN03U0BVFOY

Schritt 2: Code bestätigen

6-stelliger Code aus der App:

Aktivieren **Abbrechen**

Abbildung 47: IRAS-Website – TOTP einrichten (Beispiel)

2. Starten Sie die App und scannen Sie den enthaltenen QR-Code oder geben Sie den manuellen Code in der App ein. → Die Authenticator-App generiert einen (Verknüpfungs-) Code.
3. Geben Sie den Code ein und bestätigen Sie (AKTIVIEREN) (Abbildung 47). → Die 2-Faktor-Authentifizierung ist eingerichtet. Der Aktivierungsstatus wird geändert.

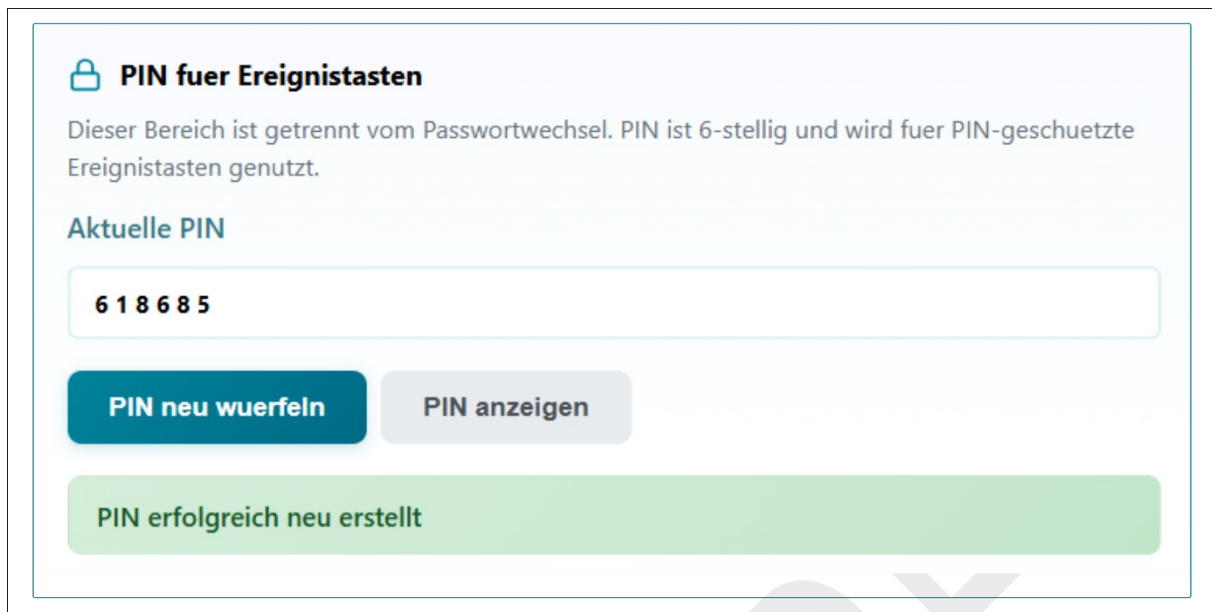
9.3.3.3 Pin für Funktionstasten festlegen

Für die Bedienung und Konfiguration von Funktionstasten kann eine PIN zur Autorisierung festgelegt werden. Deren Anwendung muss dann für die Bedienung der jeweiligen Ereignistaste aktiviert werden.

➞ [Siehe Kapitel 4.7 Systemerweiterungen.](#)

Im Bereich PIN FÜR FUNKTIONSTASTEN (Abbildung 46 (2)) wird bereits eine aktuell gültige PIN für alle Funktionstasten angezeigt.

Sie haben die Möglichkeit, eine neue PIN festzulegen (PIN NEU WÜRFELN).



🔒 PIN fuer Ereignistasten

Dieser Bereich ist getrennt vom Passwortwechsel. PIN ist 6-stellig und wird fuer PIN-geschuetzte Ereignistasten genutzt.

Aktuelle PIN

6 1 8 6 8 5

PIN neu wuerfeln **PIN anzeigen**

PIN erfolgreich neu erstellt

Abbildung 48: IRAS-Website – Pin/Funktionstasten festlegen (Beispiel)

9.3.3.4 Recovery Codes

9.3.4 Dashboard

Das Dashboard (Abbildung 49) enthält in einer Übersicht alle grundlegenden System-Informationen (z.B. anstehende Meldungen, Informationen zu Meldepunkten, Ereignisstatistiken, Systemstatus).

Es wird durch eine Menüzeile (3) und spezifische Funktionsfelder (4-12) strukturiert.

Von hier aus können alle weiteren Funktionen/Unterseiten der Website angesteuert werden.

Das Dashboard kann von jeder beliebigen Unterseite aus durch einen Klick auf das **IFAM-SYMBOL** (1) angezeigt werden.

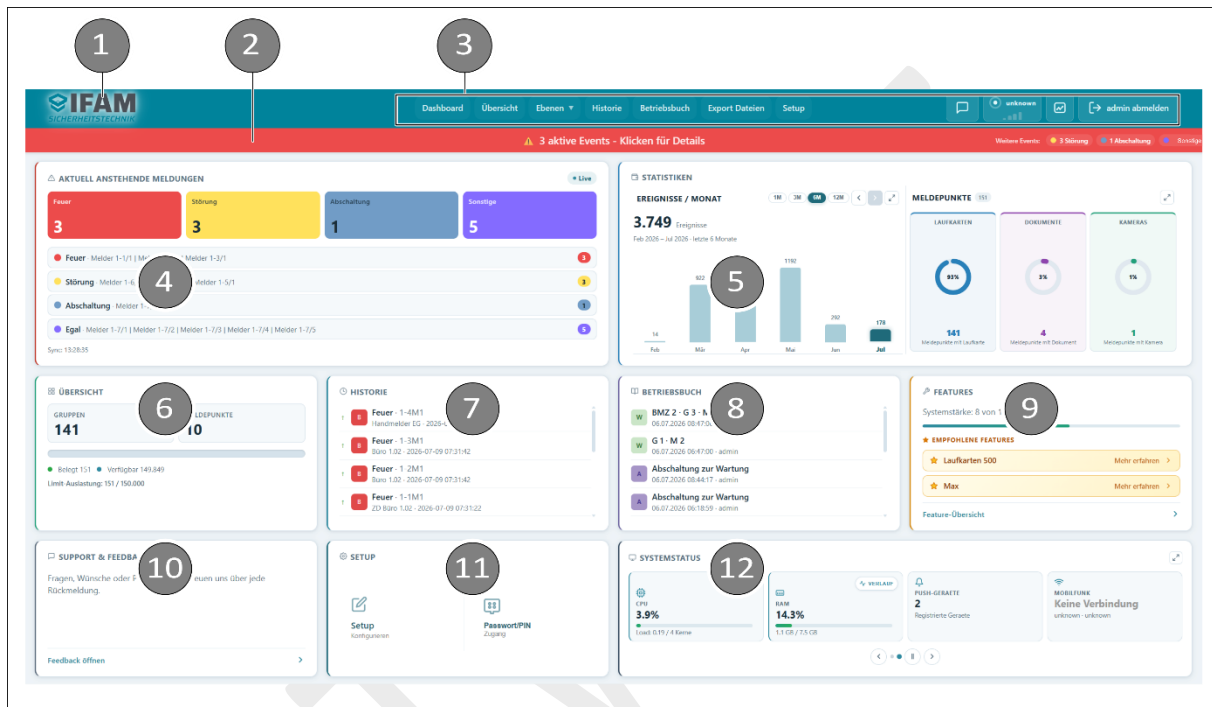


Abbildung 49: IRAS-Website – Dashboard (Beispiel)

Pos	Beschreibung
1	<u>Ifam Symbol</u> (→ Startseite/Dashboard)
2	<u>Statuszeile</u> – Ereignis-Status
3	<u>Menüzeile</u> – Ansteuerung Funktionsbereiche/Abmeldung, Netzwerkstatus
4	<u>Aktuell anstehende Meldungen</u> – aktuelle Meldungen
5	<u>Statistiken</u> – Übersicht der Ereignisse und Meldepunkte
6	<u>Übersicht</u> – Darstellung aller in der GMA vorhandenen Gruppen und Meldepunkte
7	<u>Historie</u> – Darstellung (ausgewählter) vergangener Ereignisse
8	<u>Betriebsbuch</u> – Übersicht (ausgewählter) vorhandener Einträge
9	<u>Features</u> – Überblick über aktuell verwendete und empfohlenen IRAS-Features
10	<u>Support und Feedback</u> – Kontakt zum Kundendienst
11	<u>Setup/PIN</u> – Einrichten von Zugangssicherungen
12	<u>Systemstatus</u> – Informationen zum Status ausgewählter Komponenten/Funktionen

9.3.4.1 Funktionsfelder

9.3.4.1.1 Ereignis-Status

Die Status-Zeile (2) zeigt das Vorliegen/Nicht-Vorliegen von Ereignis-Meldungen an:

Status-Zeile	Bedeutung
GRÜN (Abbildung 50)	Es liegen keine Meldungen vor.
ROT/GELB/BLAU ... (Abbildung 51)	Es liegen Meldungen für eine/mehrere der definierten Ebenen vor. Liegen Meldungen von mehreren Ebenen vor, zeigt die Status-Zeile die Anzahl der Meldungen der Ebene mit der aktuell jeweils <u>höchsten Priorität</u> an: (1.) Feuer 2.) Störung 3.) Abschaltung 4.) Sonstige (Beispiel).

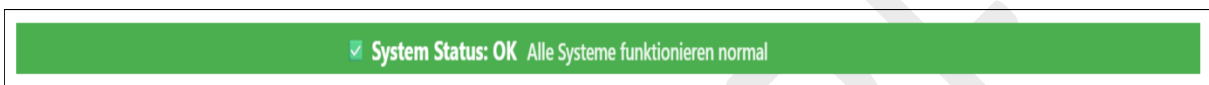


Abbildung 50: IRAS-Website – Dashboard/Statuszeile, keine Meldung

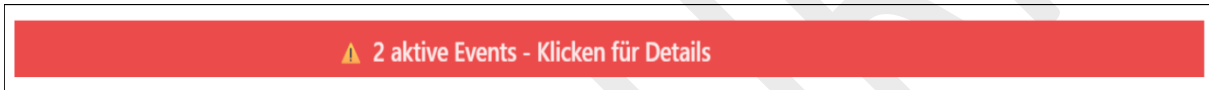


Abbildung 51: IRAS-Website – Dashboard/Statuszeile, Meldungen (Beispiel)

Durch einfachen Klick auf die STATUS-Zeile oder eine der Meldungsebenen (AKTUELL ANSTEHENDE MELDUNGEN), gelangt der Nutzer zu einer Übersicht der Ereignis-Meldungen der jeweils angezeigten Ebene.

9.3.4.1.2 Aktuell anstehenden Meldungen

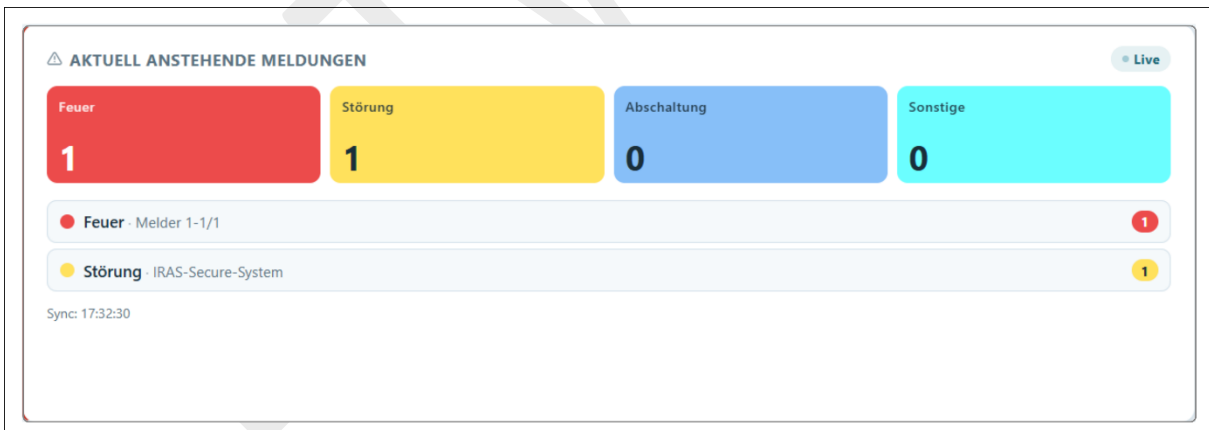


Abbildung 52: IRAS-Website – aktuelle Meldungen (Beispiel)

Im Funktionsfeld AKTUELL ANSTEHENDE MELDUNGEN wird der Meldungsstatus der Gefahrenmeldeanlage angezeigt. In einer Übersicht werden alle definierten Meldungsebenen (z.B. Feuer, Störung, Abschaltung) und ggf. vorliegende Meldungen dargestellt.

Eine tabellarische Übersicht enthält Informationen zur Störungsebene und die betreffenden Melder-Gruppen/Meldepunkte.

Durch einen Klick auf die Meldungsebene öffnet sich eine Übersicht aller hierfür vorliegenden Meldungen; ein Klick auf eine einzelne Meldung in der tabellarischen Übersicht öffnet die Details-Übersicht des jeweiligen Meldepunktes.



Siehe hierzu auch Kapitel 9.5 Anwendung (Ereignisfall).

9.3.4.1.3 Statistiken

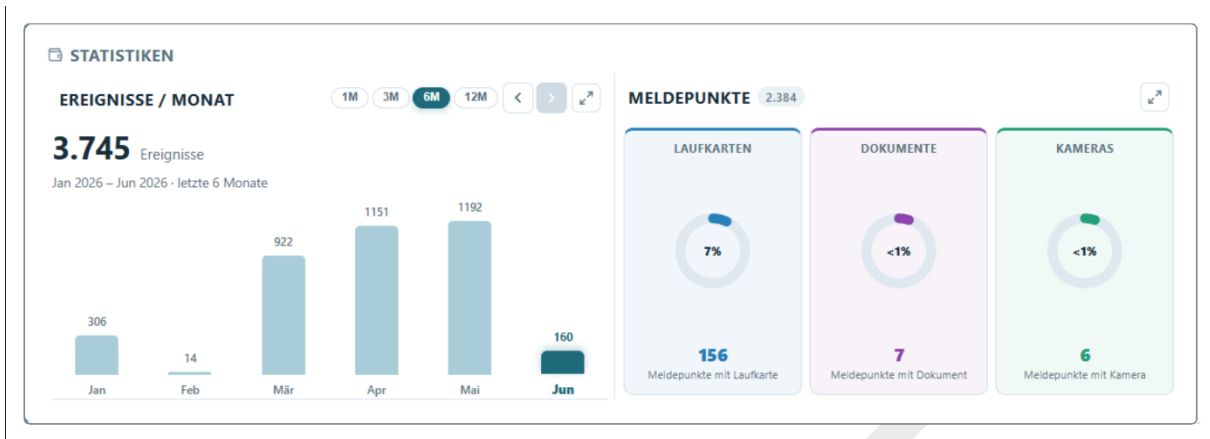


Abbildung 53: IRAS-Website – Statistiken/Übersicht

Das Funktionsfeld **STATISTIKEN** bietet einen zusammenfassenden Überblick aller stattgefundenen Ereignisse. Die Darstellung kann zeitlich variabel strukturiert werden (1/3/6/12 Monate).

Durch Klick auf einen dargestellten Zeitrahmen (z.B. Monat Juli) wird die entsprechende Historie mit Meldungsdetails angezeigt (Abbildung 54).

IFAM SCHÜTTTECHNIK

Dashboard Übersicht Ebenen Historie Betriebsbuch Export Daten Setup

1 aktive Events - Klicken für Details

Historie

Export als CSV Export als PDF

✓ 1192 Treffer • Seite 1 von 24

Alle Ereignisse 01.05.2026 31.05.2026 Objekt auswählen... Text suchen...

Status	Ereignis	Datum	Objekt	Text
➔	Störung	29.05.2026 15:59:29	IRAS-Secure-System	Kommunikation zur BAZ gestört
➔	Feuer	29.05.2026 15:59:10	7M5	!!!Testereignis!!! durch -> admin
➔	Feuer	29.05.2026 15:59:07	7M4	!!!Testereignis gelöscht!!! durch -> admin
➔	Feuer	29.05.2026 15:09:26	7M4	!!!Testereignis!!! durch -> admin
➔	Feuer	29.05.2026 15:09:25	7M5	!!!Testereignis gelöscht!!! durch -> admin
➔	Feuer	29.05.2026 08:54:31	7M5	!!!Testereignis!!! durch -> admin
➔	Feuer	29.05.2026 08:44:50	3-4M5	!!!Testereignis deaktiviert: Feuer2!!! durch -> admin
➔	Feuer	29.05.2026 08:27:04	3-4M5	!!!Testereignis aktiviert: Feuer2!!! durch -> admin

Abbildung 54: IRAS-Website – Statistiken, Meldungs-Historie (Beispiel)

Die Historie kann in den Formaten PDF und CSV exportiert werden.

9.3.4.1.4 Übersicht



Abbildung 55: IRAS-Website – Übersicht

Das Funktionsfeld ÜBERSICHT informiert über die Zahl der vorhandenen Meldergruppen und Meldepunkte des Gefahrenmeldesystems und der Anzahl der hinterlegten/verknüpften Dokumente.

Durch einfachen Klick auf die Funktionsebene öffnet sich eine Übersicht der vorhandenen Meldepunkte und die damit verknüpften Informationsmedien (Laufkarten, zusätzlich Dokumente, Kameras).

9.3.4.1.5 Historie



Abbildung 56: IRAS-Website – Historie/Übersicht

Das Funktionsfeld HISTORIE zeigt eine Liste der Ereignisse der letzten Tage an.

Durch einfachen Klick auf die Funktionsebene öffnet sich eine Übersicht *aller* gespeicherten Ereignismeldungen (Abbildung 57).

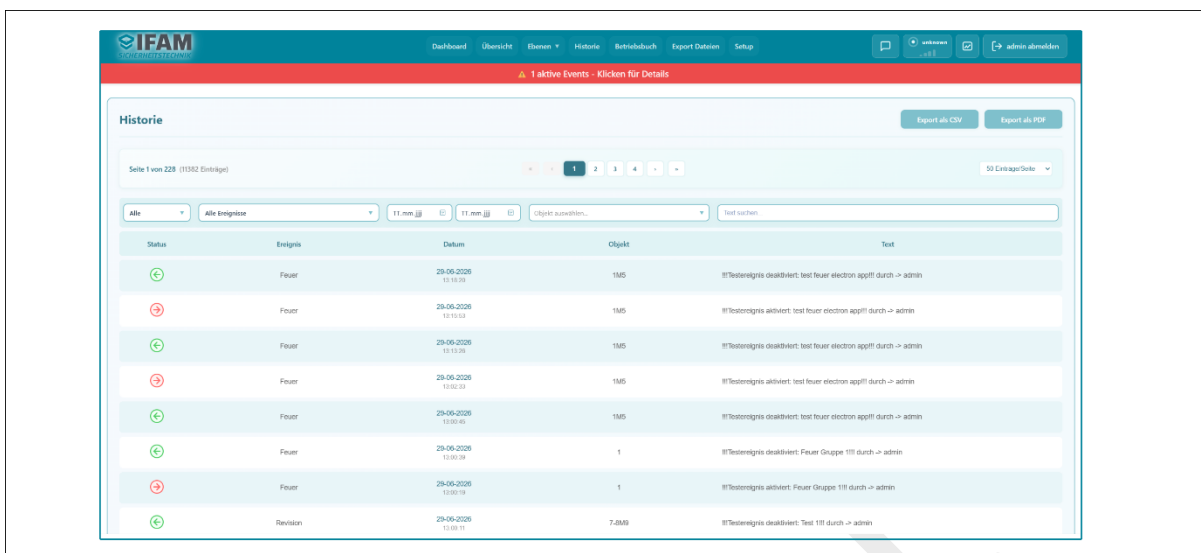


Abbildung 57: IRAS-Website – Historie/Beispiel

Die Einträge können, je nach Bedarf, strukturiert angezeigt werden: Meldungsstatus (kommend/gehend), Ereignistyp/-ebene, Meldeobjekte, Zeitraum.

Die angezeigten Ereignisse können in den Formaten PDF/CSV exportiert werden.

9.3.4.1.6 Betriebsbuch



Abbildung 58: IRAS-Website – Betriebsbuch/Übersicht (Beispiel)

Im Funktionsfeld **BETRIEBSBUCH** werden die vom Errichter, Betreiber oder Instandhalter vorgenommenen Eintragungen zu bestimmten Ereignissen angezeigt (z.B. Wartung, Störung, Abschaltung).

Das Feature IRAS-SECURE-Betriebsbuch ist eine Erweiterungsoption für IRAS-SECURE und daher standardmäßig nicht installiert.



[Siehe Kapitel 4.7 Systemerweiterungen.](#)

Wurde die Option nicht integriert, werden an dieser Stelle exemplarische Einträge zur Demonstration angezeigt.

Bei aktivierter Option öffnet sich durch einfachen Klick auf die Funktionsebene eine Übersicht aller vorhandenen Einträge (Abbildung 59).

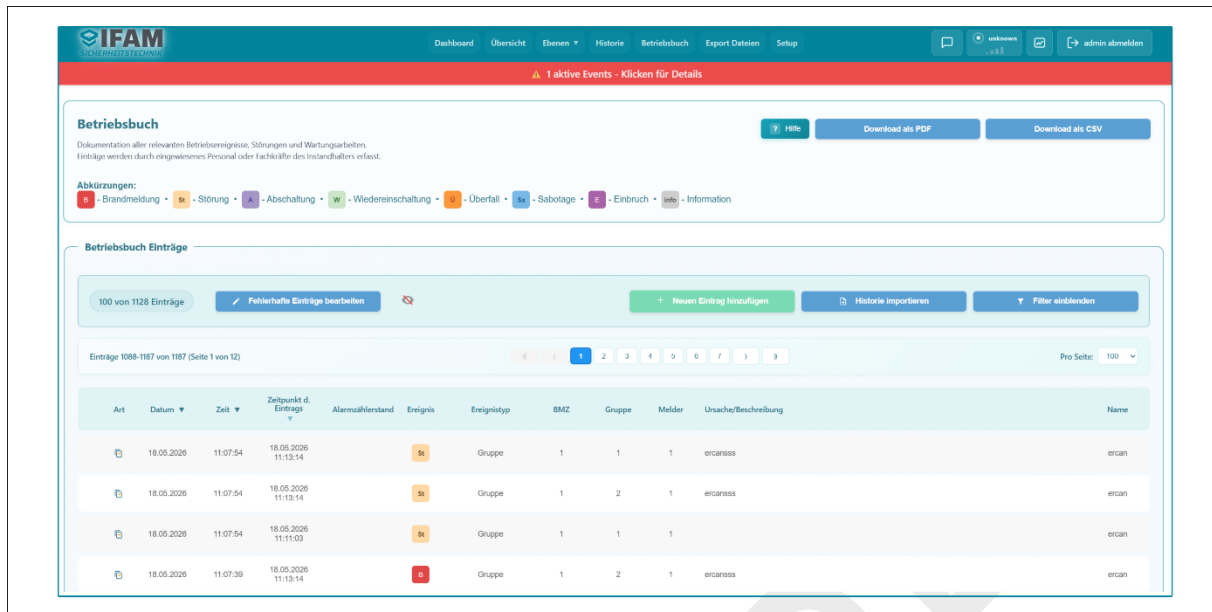


Abbildung 59: IRAS-Website – Betriebsbuch/Liste (Beispiel)

Die vorhandenen Einträge können nach verschiedenen Kriterien (z.B. Erstellungs-Datum, Ereignistyp, BMZ) strukturiert bzw. angezeigt werden.
Der Export als PDF/CSV ist möglich.

9.3.4.1.7 Features

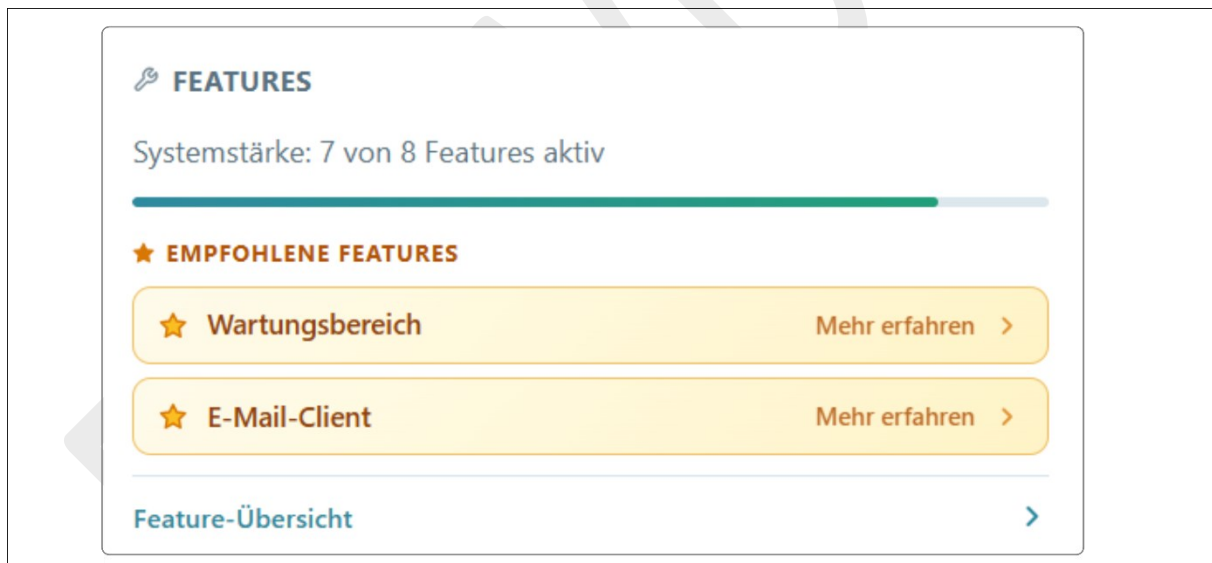


Abbildung 60: IRAS-Website – Features

Das Funktionsfeld **FEATURES** beinhaltet eine Übersicht aktuell vorhandener/installierter Features von IRAS-SECURE.

Durch einfachen Klick auf die Funktionsebene öffnet sich eine Übersicht der genutzten Features, wichtiger Kernfeatures, empfohlener Optionen und einer kurzen Beschreibung (Abbildung 61).

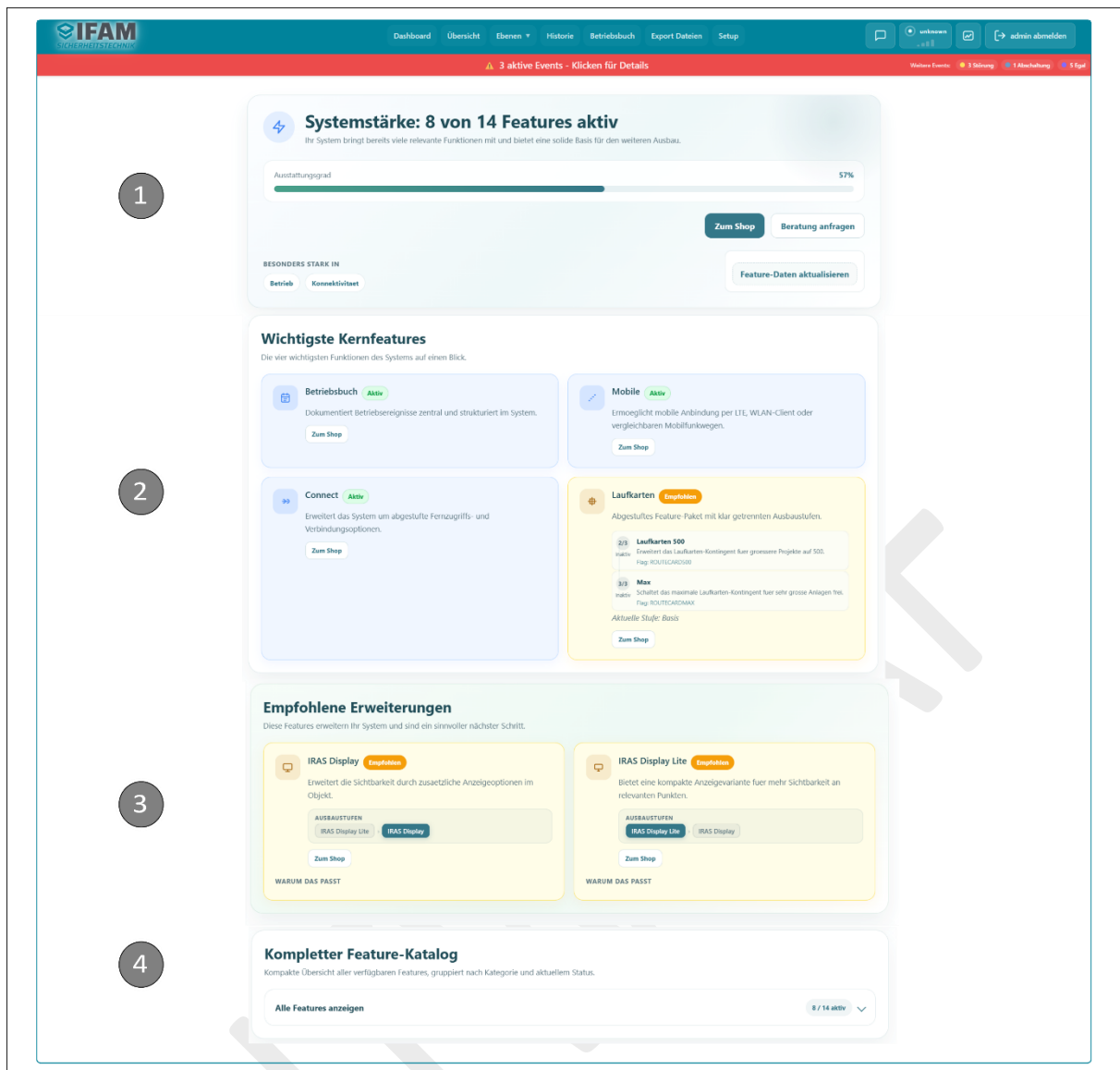


Abbildung 61: IRAS-Website - Features/Übersicht

Die IRAS-Website analysiert die Struktur des aktuell installierten Systems und stellt diese u.a. als Ausstattungsgrad (1) und als Liste bereits vorhandener/aktiver Kernfeatures (2) und empfohlener Erweiterungsoptionen (3) dar.

Ein Katalog aller aktuell möglichen Features (4) ermöglicht den Überblick über das vollständige IRAS-SECURE-Gefahrenmeldesystem und die Struktur Ihres Systems.

Aus den dargestellten Übersichten heraus können gewünschte Features/Optionen durch eine Weiterleitung an den Produktbereich der IFAM-Website direkt bestellt werden.

9.3.4.1.8 Support und Feedback

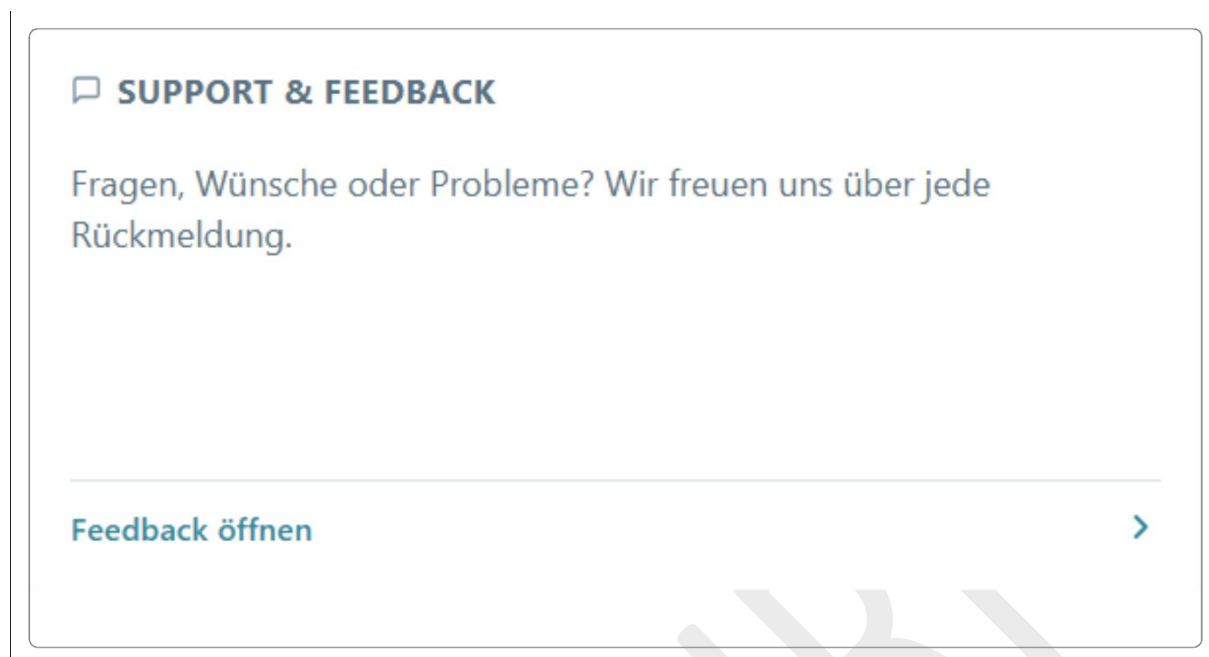


Abbildung 62: IRAS-Website – Support/Feedback

Abbildung 63: IRAS-Website – Support/Feedback, Formular

Das Funktionsfeld SUPPORT & FEEDBACK ermöglicht den Eintrag und das direkte Versenden von Rückmeldungen zu IRAS-SECURE. Durch einfachen Klick öffnet sich ein Eingabeformular (Abbildung 63). Hier können u.a. Anfragen an den Ifam-Kundendienst einschl. ggf. vorhandener Diagnosedaten übermittelt werden.

9.3.4.1.9 Setup

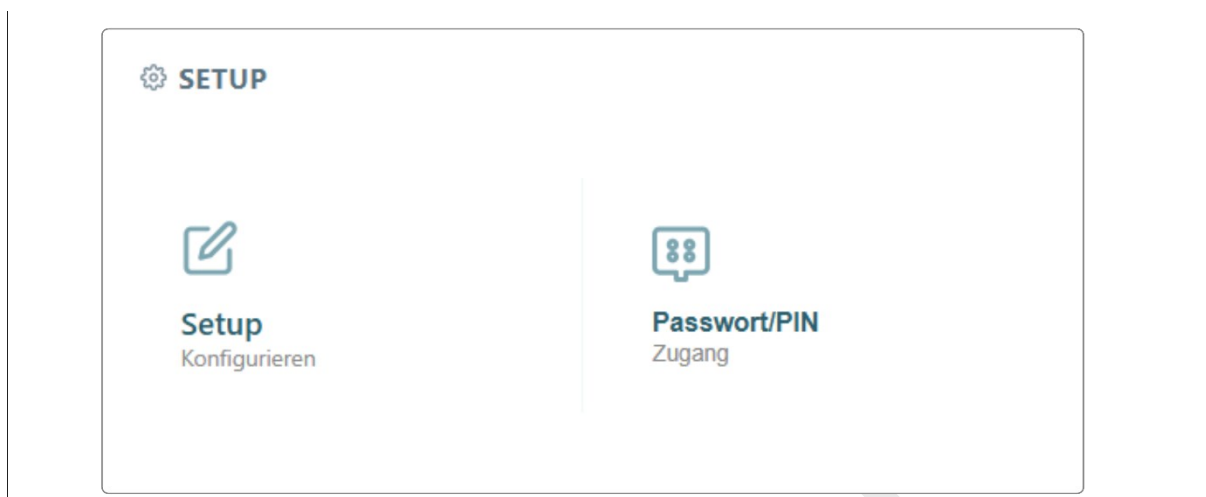


Abbildung 64: IRAS-Website – Setup

Das Funktionsfeld SETUP ermöglicht den Zugang zum SETUP-Bereich, in dem die Konfiguration/Verwaltung der Meldepunkte und der vorhandenen Medien vorgenommen wird. Darüber hinaus kann auf den Bereich zur Einrichtung von Zugangs- und Bediensicherungen (PIN, Passwort, 3-Faktor-Authentifizierung) zugegriffen werden (PASSWORT/PIN).

9.3.4.1.10 System-Status



Abbildung 65: IRAS-Website – Systemstatus/Übersicht

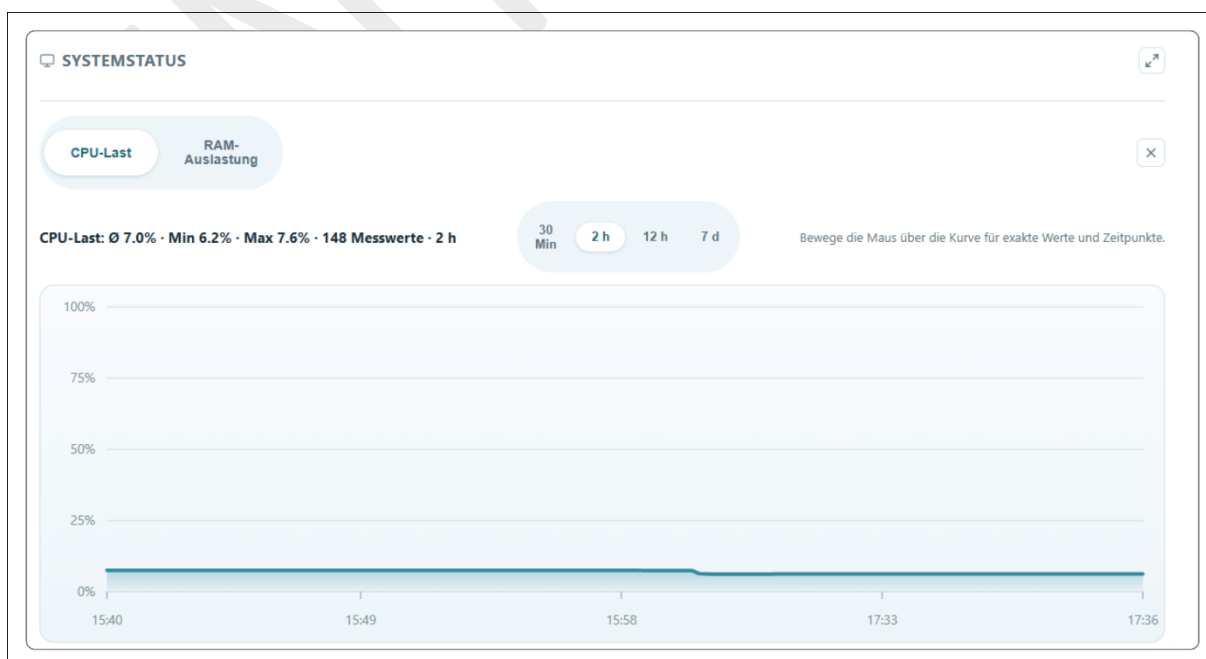


Abbildung 66: IRAS-Website – Systemstatus/Beispiel

Das Funktionsfeld SYSTEMSTATUS enthält Informationen zum Status des Gefahrenmeldesystems sowie ausgewählter Komponenten und Prozesse, z.B. Auslastung von Arbeitsspeicher und Prozessor, vorhandene Mobilfunk-Verbindung, durchgeführte Systemsicherungen und belegter/freier Speicher (Abbildung 65).

Für die Komponenten RAM und CPU kann zudem eine Historie der Last bzw. Auslastung angezeigt werden (VERLAUF), die zeitlich strukturiert dargestellt werden können (0,5/2/12 Stunden; 7 Tage) (Abbildung 66).

9.4 Konfiguration

Für den Betrieb/die Bedienung von IRAS-SECURE müssen grundlegende Konfigurationen/Einstellungen vorgenommen werden:

- Netzwerkverbindung,
- BMZ-Einstellungen,
- Systemzeit,
- Gruppen,
- Benutzer,
- Code-Tabelle,
- Meldungsebenen,
- Bedienung,
- Medien (Laufkarten, zusätzliche Dokumente, Kameras),
- Meldepunkte,
- Funktionstasten (optional),
- Benachrichtigungen/Ausgabeoptionen (E-Mail, SMS, Drucker)
- IRAS-SECURE-App.

9.4.1 Netzwerkverbindung

9.4.1.1 Ethernet

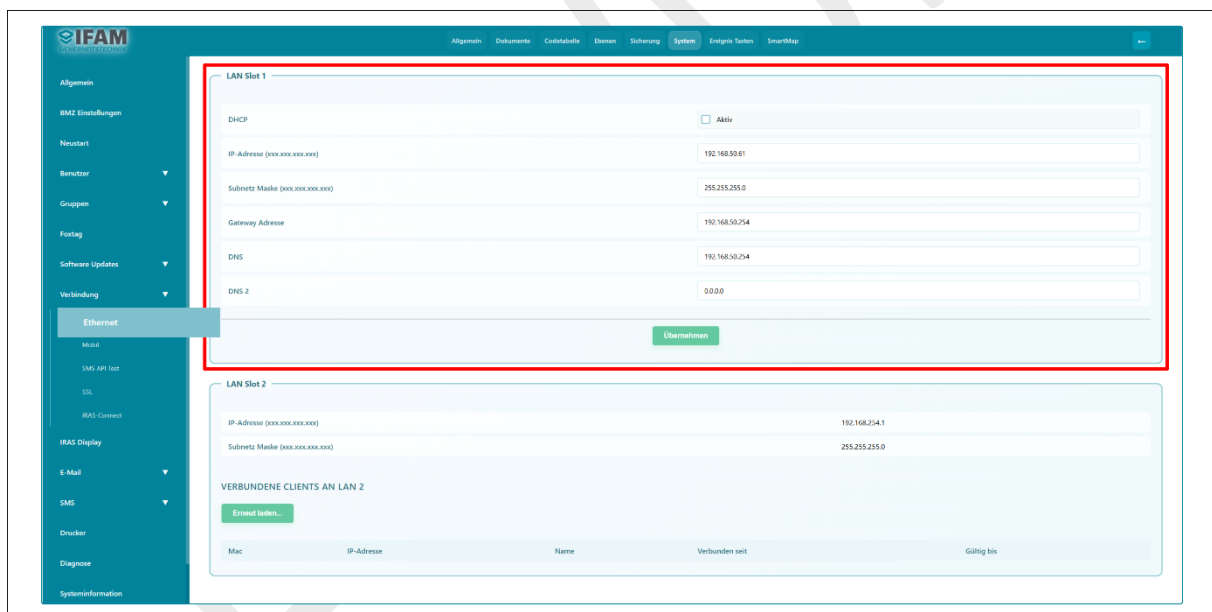


Abbildung 67: IRAS-Website – Ethernet/LAN-Schnittstelle

Das IRAS-Gefahrenmeldesystem besitzt zwei getrennte Netzwerkschnittstellen (**LAN1/LAN2**).

LAN2

Die Schnittstelle verfügt über einen integrierten DHCP Server, der angeschlossenen Geräten dynamische IP-Adressen zuweist. Dadurch kann über diese Schnittstelle die Inbetriebnahme des IRAS-SECURE-Gefahrenmeldesystem erfolgen.

LAN1 stellt eine konfigurierbare Netzwerkschnittstelle dar, die je nach Bedarf oder Anforderung über die IRAS-SECURE-Website parametrisiert werden kann.

Die korrekten Werte für diese Parameter erfragen Sie bitte bei Ihrem zuständigen Systemadministrator.

Für die automatische Vergabe einer Netzwerkadresse haben Sie darüber hinaus, die Möglichkeit, das DHCP-Protokoll zu aktivieren.

Folgende Netzwerkparameter können eingestellt werden:

- IP-Adresse,
- Subnetzmaske,
- Gateway-Adresse,
- Umschaltung zwischen DHCP und statischer IP-Adresse.

Der DNS-Server-Adresse ist für die Schnittstelle LAN1 und LAN2 gleich.

Für die Konfiguration des Systems müssen sich der PC und das IRAS-SECURE-Gefahrenmeldesystem im gleichen physikalischen Netzwerk befinden.

LAN1

Im Auslieferungszustand wird die Netzwerkschnittstelle mit der festen IP-Adresse 192.168.254.1 konfiguriert und befindet sich im Subnetz 255.255.255.0. Diese kann für den späteren Betrieb nicht verändert werden.

Die Eigenschaften sind nicht parametrierbar.



Damit der PC auf das IRAS-SECURE-Gefahrenmeldesystem zugreifen kann, muss er sich im gleichen Subnetz befinden

1. Zur Konfiguration der Ethernet-Verbindung wählen Sie in der Menüzeile den Eintrag SETUP. → Der Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile den Eintrag SYSTEM.
3. Wählen Sie unter VERBINDUNG die Option ETHERNET.

9.4.1.2 SSL/TLS konfigurieren

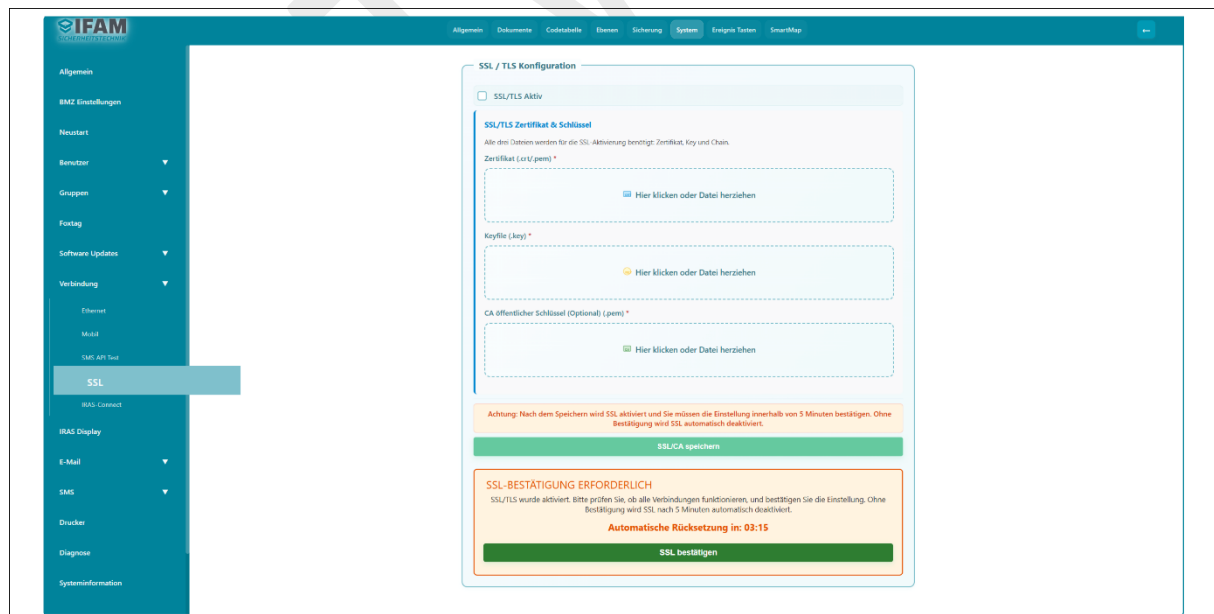


Abbildung 68: IRAS-Website – SSL

Das Menü SSL dient dem Einstellen/Aktivieren einer sicheren Verbindung zum IRAS-SECURE-Gefahrenmeldesystem. Dies gilt für die Kommunikation über den Webserver des IRAS-SECURE sowohl vom Browser eines PC/Laptop als auch von einem mobilen Gerät (Tablet, Smartphone).

1. Zur Konfiguration der Ethernet-Verbindung wählen Sie in der Menüleiste den Eintrag SETUP. → Der Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüleiste den Eintrag SYSTEM.
3. Wählen Sie unter VERBINDUNG die Option SSL.
4. Laden die benötigten Dateien hoch:
 - Zertifikat (*.crt/*.pem),
 - Keyfile (*.key),
 - CA (*.pem) – öffentlicher Schlüssel
5. Speichern Sie (SSL/CA SPEICHERN)

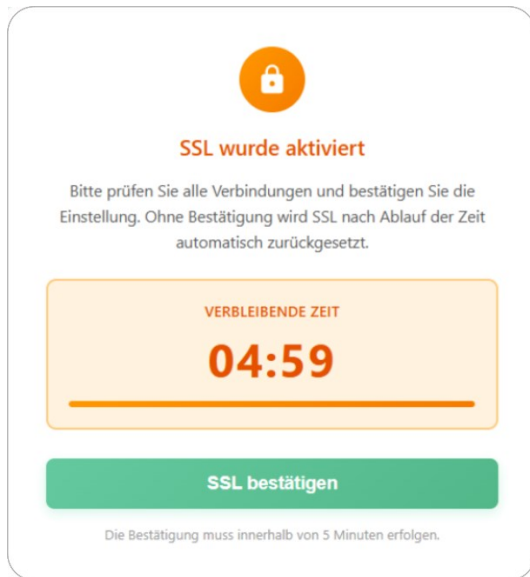


Abbildung 69: IRAS-Website – SSL/aktiv

→ Es wird die Aktivierungsseite angezeigt. Bestätigen Sie die Aktivierung innerhalb von **5 Minuten**.

Nach der Bestätigung werden Sie von IRAS-Website abgemeldet. Melden Sie sich erneut an.

Bei nicht erfolgter Bestätigung wird SSL/TLS wieder deaktiviert.

(SSL WURDE ERFOLGREICH BESTÄTIGT.)?

9.4.2 GMZ-Einstellungen

1. Zur Konfiguration der GMZ-Einstellungen wählen Sie in der Menüzeile den Eintrag SETUP.
→ Der Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile den Eintrag SYSTEM.
3. Wählen Sie die Option GMZ-EINSTELLUNGEN.

Abbildung 70: IRAS-Website – BMZ-Einstellungen

9.4.2.1 Geräteadresse und Protokoll

Auf der IRAS-Website können Konfigurationen der Schnittstelle zum Gerät, an dem IRAS-Secure angeschaltet wurde (z.B. ADP4000) und die Protokoll-Spezifikation vorgenommen werden. [Siehe Kapitel 8 Konfiguration \(GMA/Prog4000\).](#)

Die Geräteadresse (logische Adresse des IRAS-SECURE-Gefahrenmeldesystems) kann bei der Verwendung mit ADP4000 vergeben werden. Sie sollte im angeschlossenen Ring eindeutig sein. Damit können Meldungen, die z.B. durch das Drucksystem erzeugt werden, eindeutig IRAS-SECURE zugeordnet werden.



Werden Änderungen am Aufbau des dualen Rings (Peripherie-Konfiguration) vorgenommen, aus denen sich neue Geräteadressen ergeben, muss dies im IRAS entsprechend aktualisiert werden.

9.4.2.2 Erkundenzeit (optional)

Die Erkundenzeit dient dazu, beim Auftreten des ersten Feuers, vor Ort befindlichen Kräften des Betreibers einen Zeitraum zu gewährleisten, bevor tatsächlich die Meldung an die Feuerwehr ausgelöst wird.

Eine entsprechende Zeit kann im IRAS-SECURE-Gefahrenmeldesystem hinterlegt werden. Ohne weitere Einstellungen wird die Erkundenzeit automatisch mit dem ersten Feuer der GMZ gestartet.

Diese wird in der Folge in der IRAS-APP als auch auf allen registrierten IRAS-Display angezeigt.

Alternativ dazu kann die Erkundenzeit auch mit einem spezifischen Event gestartet werden. Dazu muss der gewünschte Event durch die GMZ übertragen werden.



Die Anzeige der abgelaufenen Erkundenzeit, bleibt in der App und im IRAS-Display (optional) solange bestehen, bis alle Ereignisse zurückgesetzt wurden.



Wenn viele Ereignisse aktiv sind, kann die Auflistung aller Meldungen im Auswahlfenster mit einer gewissen Verzögerung erfolgen

9.4.3 Systemzeit einstellen

Im IRAS-SECURE-Gefahrenmeldesystem kann bei Bedarf die jeweils aktuelle Zeitzone eingestellt werden. Diese Angabe hat direkten Einfluss auf alle Ereignisse, die innerhalb des Gefahrenmeldesystem gespeichert sind.

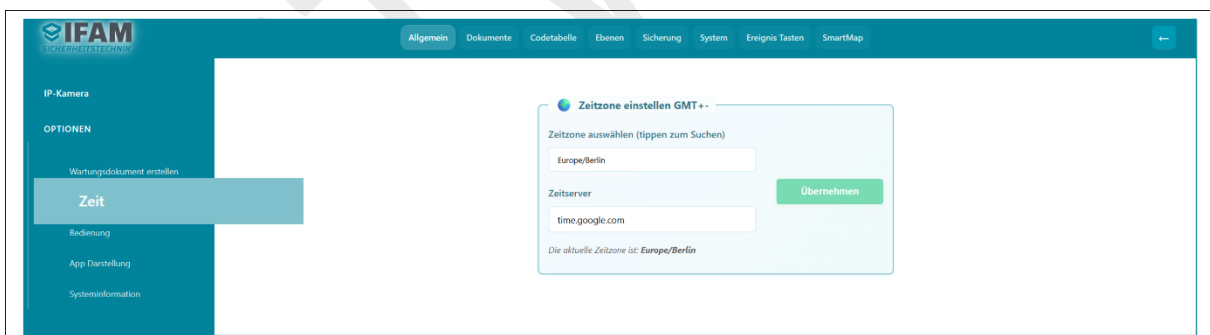


Abbildung 71: IRAS-Website – Systemzeit einstellen

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zur Systemverwaltung wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche ALLGEMEIN.
→ Die Benutzeroberfläche zur Verwaltung von IP-Kameras und weiterer Optionen wird geöffnet.
3. Wählen Sie unter Optionen den Eintrag ZEIT, wählen Sie die entsprechende ZEITZONE und fügen Sie ggf. den gewünschten ZEITSERVER ein. Übernehmen Sie die Angaben.

9.4.4 Ebenen definieren

Zur Klassifizierung von Meldungstypen können spezifische (Meldungs-)EBENEN und damit verbundene Anzeige-Prioritäten definiert werden.

Im Auslieferungszustand sind bereits Standard-Ebenen angelegt, die in ihrer Priorität nicht verändert und nicht entfernt werden können: 1.) Feuer 2.) Störung 3.) Abschaltung.

Diesen Definitionen können weitere Betreiber-eigene Ebenen hinzugefügt und aktiviert/deaktiviert werden.

Für jede Ebene kann eine individuelle Farbkennzeichnung festgelegt werden, die auf dem Dashboard angezeigt und im Meldungsfall entsprechend der vergebenen Kennung (ID) priorisiert dargestellt werden.

➞ [Siehe Kapitel 9.3.4 Dashboard.](#)

1. Wählen Sie in der Menüzeile den Eintrag SETUP.
→ Die Benutzeroberfläche SETUP-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche Ebenen.
→ Die Benutzeroberfläche zur Definition der Ebenen öffnet sich.

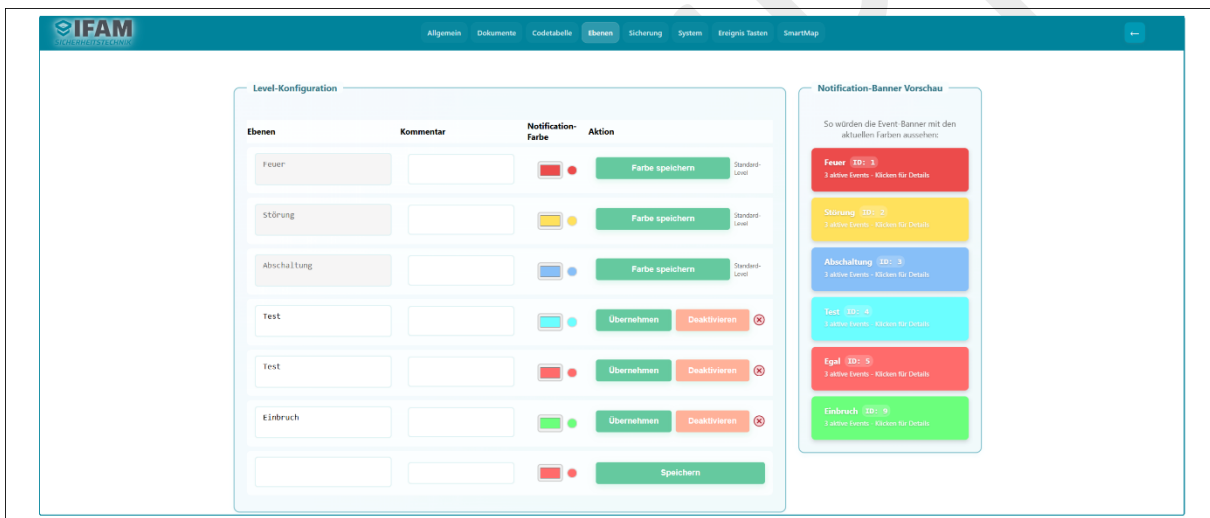


Abbildung 72: IRAS-Website – Ebenen (Beispiel)

9.4.5 Code-Tabelle

Mit der Codetabelle können Codes der Meldungstypen der GMZ verschiedenen Ebenen zugewiesen werden. Damit ist eine Sortierung der einzelnen Meldungen möglich.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche SETUP-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche CODETABELLE.
→ Die Benutzeroberfläche zur Konfiguration der Codetabelle öffnet sich.

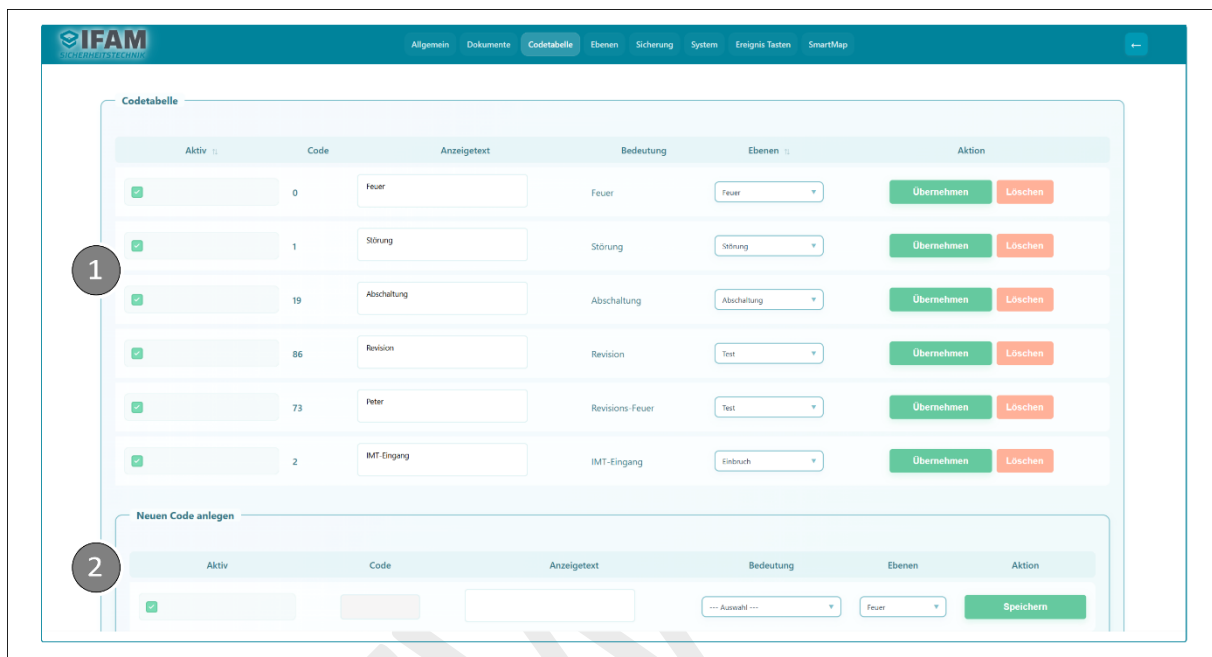


Abbildung 73: IRAS-Website – Codetabelle (Beispiel)

Die Spalten CODE und BEDEUTUNG definieren den Meldungstyp und sind von der Konfiguration des in der GMA integrierten FAT bekannt.

Bei der Erstellung eines neuen Eintrages kann lediglich *ein* Wert eingegeben werden.

Dadurch wird sichergestellt, dass der Code und die Bedeutung immer zueinander passen.

Die Spalte EBENE legt fest, in welcher Meldungsebene dieser Meldungstyp angezeigt wird.

9.4.6 Gruppen verwalten

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Der SETUP-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SYSTEM.
→ Die Bereich Systemverwaltung wird geöffnet.
3. Wählen Sie die Option GRUPPEN. → Eine Übersicht der ggf. bereits vorhandenen Gruppen wird angezeigt.
Nach Auswahl eines vorhandenen Eintrags werden die definierten Eigenschaften der jeweiligen Gruppe angezeigt, die geändert werden können.

➡ *Siehe Kapitel 9.4.6.2 Gruppe konfigurieren.*

9.4.6.1 Gruppe anlegen

Abbildung 74: IRAS-Website – Neue Gruppe

1. Zum Anlegen einer neuen Gruppe wählen Sie den Eintrag NEUE GRUPPE.
2. Vergeben Sie einen Gruppennamen.
3. Wählen Sie ggf. als Vorlage eine der bereits vorhandenen Gruppen.
4. Konfigurieren Sie die gewünschten Eigenschaften.

➡ *Siehe Kapitel 9.4.6.2 Gruppe konfigurieren.*

9.4.6.2 Gruppe konfigurieren

Objekt	Lesen	Lesen/Schreiben	Verwalten
Webcam	☒	☐	☐
Webnutzung (Anmeldung auf Webseite möglich)	☐	☒	☐
Nutzer kann Unterkonten anlegen	☐	☒	☐
Backup & Synchronisation	☐	☒	☐
Setup	☐	☒	☐
Revision	☐	☒	☐
Übersicht	☒	☐	☐
History	☒	☐	☐
Dokumente	☐	☒	☐
FBF	☐	☒	☐
ISAT	☐	☒	☐
Ereignisanzeige	☒	☐	☐
Betriebsbuch	☐	☒	☐
Bedienung Gruppen	☒	☐	☐

Abbildung 75: IRAS-Website – Gruppe/Übersicht

Durch Auswahl einer (neu angelegten) Gruppe (**1**) gelangen Sie zur Konfigurationsoberfläche dieser Gruppe.

Hier können konfiguriert werden:

- Lese-/Schreibrechte für die Ausführung von Funktionen, die Konfiguration oder den Zugriff auf Dokumente,
- Push-Benachrichtigung (bei Revision),
- Benachrichtigungseinstellungen.

ENTWURF

9.4.7 Benutzer verwalten

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Der SETUP-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SYSTEM.
→ Die Bereich Systemverwaltung wird geöffnet.
3. Wählen Sie die Option NUTZER. → Eine Übersicht der ggf. bereits vorhandenen Benutzer wird angezeigt.
Nach Auswahl eines vorhandenen Eintrags werden die definierten Eigenschaften des jeweiligen Benutzers angezeigt, die geändert werden können.
➔ *Siehe Kapitel 9.4.7.2 Benutzer konfigurieren.*



Für IRAS-SECURE ist bereits ein Nutzerkonto ADMIN vorinstalliert. Es dient ausschließlich der Administration des Gefahrenmeldesystems und sollte nicht als normales Nutzerkonto verwendet werden.



Die Verbindung zum IRAS-SECURE-Gefahrenmeldesystem über den Nutzer ADMIN sollte mit den eigenen WLAN-, LAN1- oder LAN2-Zugang und nicht über die mobile Verbindung vorgenommen werden. Andernfalls sind Verbindungsabbrüche möglich.

9.4.7.1 Benutzer anlegen

Abbildung 76: IRAS-Website – Neuer Benutzer

1. Zum Anlegen eines neuen Benutzers wählen Sie den Eintrag NEUER NUTZER.
2. Vergeben Sie einen Nutzernamen.
3. Ordnen Sie den Nutzer einer bestehenden Gruppe zu.
4. Legen Sie ggf. die Pflicht zur TOTP-Sicherung des Systemzugangs fest.
5. Konfigurieren Sie die gewünschten Eigenschaften.
➔ *Siehe Kapitel 9.4.7.2 Benutzer konfigurieren.*

9.4.7.2 Benutzer konfigurieren

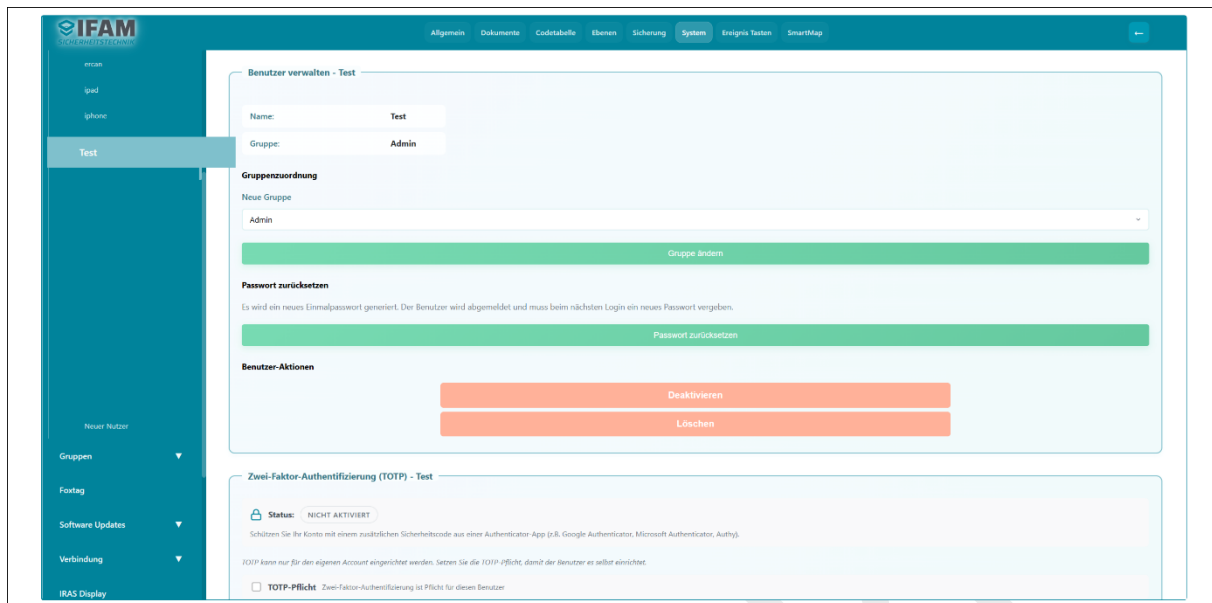


Abbildung 77: IRAS-Website – Benutzer/Übersicht

Wählen Sie in der Benutzer-Übersicht den gewünschten Eintrag. → Die Oberfläche zur Konfiguration der Benutzereigenschaften wird geöffnet.

Hier können konfiguriert werden:

- **Gruppenzuordnung** – Wählen Sie hierzu eine der vorhandenen Gruppen. Allen Mitgliedern einer Gruppe werden die jeweils definierten Eigenschaften zugewiesen.
 ↗ *Siehe Kapitel 9.4.6 Gruppen verwalten.*
- **Passwort** – bei z.B. Verlust kann hier das bestehende Passwort zurückgesetzt werden. Das System vergibt ein neues einmaliges Passwort, das nach Abmeldung und Neuansmeldung geändert werden muss.
- **Zwei-Faktor-Authentifizierung**: die zusätzliche Sicherheits-Option dient dem Schutz des Benutzerkontos. Sie kann als verpflichtende Option für die Nutzung des jeweiligen Kontos festgelegt werden.
- **Lese-/Schreibrechte** für die Ausführung von Funktionen, die Konfiguration oder den Zugriff auf Dokumente.

Im Rahmen der Zuordnung eines Benutzers zu einer Gruppe, werden die dort definierten Lese-/Schreibrechte übernommen.

Abweichend davon können für jeden Benutzer jedoch auch eigene Rechte festgelegt werden.

9.4.8 Medien verwalten

9.4.8.1 Laufkarten

Laufkarten sind Dateien, die Informationen für die Feuerwehr, Betreiber oder Techniker bereitstellen.

Der Informationsinhalt der Dokumente kann vielfältig gestaltet werden. So können neben Lageplänen oder Anfahrtsskizzen auch Sicherheitshinweise oder Flucht- und Rettungswegepläne enthalten sein.

Eine Laufkarte liegt in Form einer PDF-Format vor und kann eine beliebige Seitenanzahl enthalten.

Zur Verwaltung von Laufkarten Sie in der Menüzeile die Schaltfläche SETUP.

→ Die Benutzeroberfläche zur Systemverwaltung/DOKUMENTE wird geöffnet.

The screenshot shows the 'DOKUMENTE' section of the IRAS-Website. The top navigation bar includes 'Allgemein', 'Dokumente', 'Codetabelle', 'Ebenen', 'Sicherung', 'System', 'Ereignis Testen', and 'SmartMap'. The 'Dokumente' tab is active. On the left, a sidebar contains 'Verfügbare Laufkarten / Meldepunkte' and 'Optionale Dokumente' with a sub-menu 'LAUFKARTENIMPORT' containing 'Klassischer Upload', 'Unterstützter Upload', and 'Meldepunkte importieren'. The main area is titled 'LAUFKARTEN/MELDEPUNKTE' and shows a summary of document counts (e.g., 2386 / 150000) and an 'Upgrade' button. Below this is a table of documents with columns: MAPKEY, BMZ, BEZEICHNUNG, ZUSATZINFO, TYP, UNTERPUNKTE, LAUFKARTE, and LÖSCHEN. The table lists various document groups and their associated data. A search bar and pagination controls are also visible.

Abbildung 78: IRAS-Website – verfügbare Laufkarten/Meldepunkte (Beispiel)

Die Seite DOKUMENTE enthält Optionen zur Verwaltung von Laufkarten und zusätzlichen Dokumenten (1) sowie eine Übersicht der im System bereits vorhandenen Meldepunkte der GMA (z.B. Gruppen und Module) (3) und ihrer Eigenschaften und ggf. zugeordneter Dokumente (z.B. Laufkarten).

Die Möglichkeit, Dokumente im System zu speichern, ist durch ein festgelegtes Limit begrenzt. Eine Übersicht der bereits belegten Ressourcen erhalten Sie durch Betätigen der Schaltfläche LIMIT-STATUS (2). Durch Betätigen der Schaltfläche UPGRADE kann die Speicherbegrenzung angepasst werden.

Abbildung 79: IRAS-Website – Dokumente/Limit

→ Eine Übersicht des Auslastungsstatus wird geöffnet.

Zur Anpassung des Speicherlimits betätigen Sie die Schaltfläche LIMIT ERHÖHEN.

Definieren Sie das neue Limit.

9.4.8.1.1 Laufkarten hochladen

Für den Upload von Laufkarten stehen zwei Optionen zur Verfügung:

- Klassischer Upload,
- Unterstützter Upload.

Die hierbei hochgeladenen Dokumente werden dem System als Meldepunkte im Bereich VERFÜGBARE LAUFKARTEN/MELDEPUNKTE hinzugefügt (Abbildung 78) und können dort eingesehen und bearbeitet werden.

9.4.8.1.1.1 Notwendige Eigenschaften von Laufkarten

Die Laufkarte muss in Form einer **PDF-Datei** vorliegen.

Benennung

Für die Vergabe von Dateinamen müssen notwendige Konventionen eingehalten werden.

Dateiname (Struktur): **b-gMm.***

b	zu ersetzen durch	BMZ-Nummer
g	zu ersetzen durch	Gruppennummer
M	zu ersetzen durch	Meldungstyp
m	zu ersetzen durch	Meldernummer
-	als Trennzeichen zu verwenden!	

Beispiel:

1-3M2.pdf = BMZ: 1, Gruppe: 3, Typ: Meldergruppe, Melder: **2**.

Soll nur eine Gruppe bezeichnet werden, wird die Angabe der Meldernummer weggelassen. Damit entfällt dann auch das Trennzeichen „M“.

Beispiel:

1-3.pdf = BMZ: 1, Gruppe: 3, Typ: Meldergruppe

Werden BMZ-Nummern in einem Projekt nicht verwendet, entfällt die Angabe der BMZ-Nummer inklusive des Trennzeichens „-“.

Beispiele:**3M0.pdf** = Gruppe: 3, Typ: Meldergruppe, Melder: 0**3M2.pdf** = Gruppe: 3, Typ: Meldergruppe, Melder: 2**0-3M2.pdf** = BMZ: 0, Gruppe: 3, Typ: Meldergruppe, Melder: 2

Diese Namensvereinbarung gilt in gleicher Weise für die Objektdarstellung (JPG-Dateien), für die Laufkarten (PDF-Dateien) sowie die Textdateien mit den Zusatztexten.

Werden die Elemente wie BMZ-, Gruppe- oder Meldernummer durch eine null (0) ersetzt, wird dieser Wert ignoriert. Das führt dazu, dass Laufkarten mehreren Meldern, Gruppen oder BMZ zugewiesen werden können.

9.4.8.1.1.2 Upload – klassisch

Laufkarten können durch erfahrene Benutzer direkt, ohne weitere Zwischenschritte/Unterstützung hochgeladen werden.

Hierbei können sowohl Einzeldateien als auch mehrere (max. 10.000) Dateien in *einem* Upload-Prozess übertragen werden.



- Beachten Sie die Benennungskonventionen für Laufkarten. Falsch benannte Dateien können nicht hochgeladen/nicht angezeigt/den Meldepunkten nicht korrekt zugeordnet werden.
- Nutzen Sie im Zweifelsfall den UNTERSTÜTZTEN UPLOAD, der u.a. die Dateinamen prüft und ggf. korrigiert.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche SETUP/DOKUMENTE wird geöffnet.
2. Wählen Sie im Seitenmenü die Option LAUFKARTENIMPORT/KLASSISCHER UPLOAD.

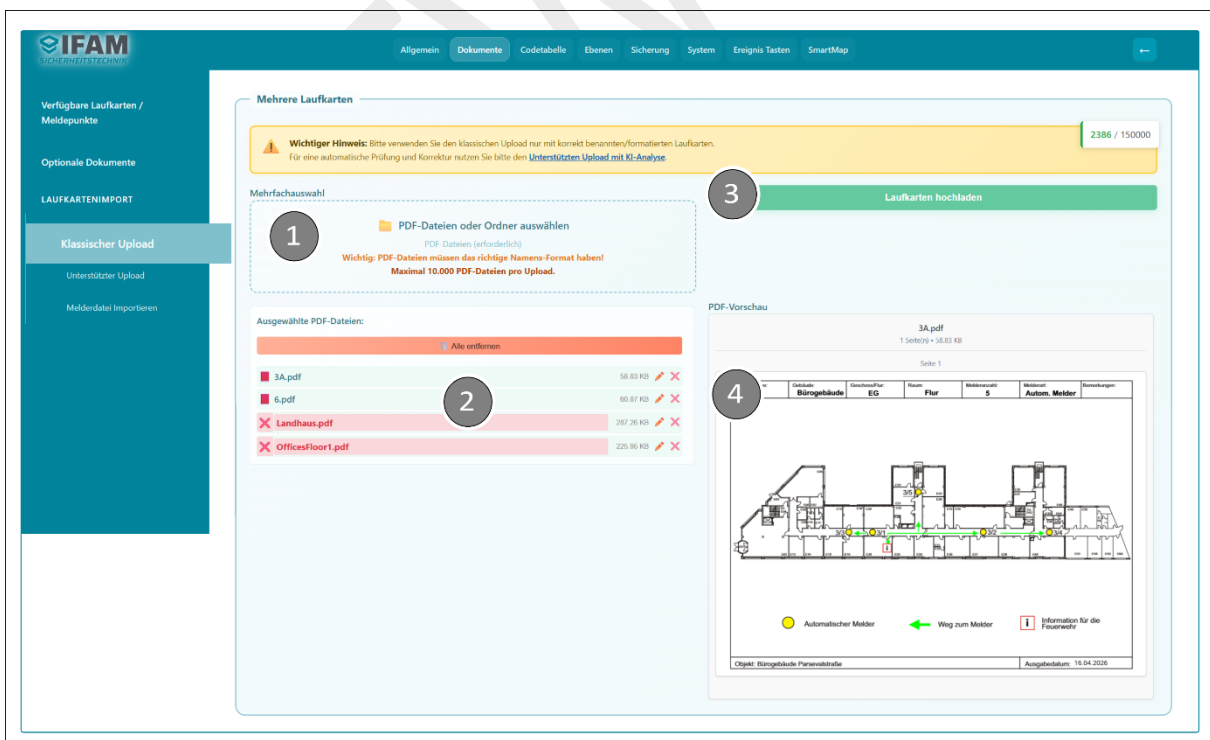


Abbildung 80: IRAS-Website – Laufkarten/Upload, klassisch

3. Klicken Sie in das Feld MEHRFACHAUSWAHL (1) und wählen Sie im sich öffnenden Dialogfeld die hochzuladenden Dokumente/Ordner.
(Alternativ hierzu können die Dateien/Ordner auch per *Drag & Drop*) abgelegt werden.)

→ Die abgelegten Daten werden in einer Übersicht dargestellt (2). Nicht korrekt benannte Dateien sind rot hinterlegt. Diese können nicht hochgeladen werden und müssen entfernt und entsprechend den Vorgaben benannt werden.

Durch einfachen Klick wird eine Vorschau der entsprechenden Laufkarte angezeigt (4).

4. Starten Sie den Upload (LAUFKARTEN HOCHLADEN) (2). → Eine Upload-Zusammenfassung wird angezeigt.
5. Schließen den Upload ab.

9.4.8.1.1.3 Upload – unterstützt

Der UNTERSTÜTZTE UPLOAD begleitet das Hochladen von Laufkarten, analysiert, korrigiert und ordnet die Laufkarten automatisch den vorgesehenen Meldepunkten zu.

Es können sowohl Einzeldateien als auch mehrere Dateien (max. 10.000) in *einem* Upload-Prozess übertragen werden.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche SETUP/DOKUMENTE wird geöffnet.
2. Wählen Sie im Seitenmenü die Option LAUFKARTENIMPORT/UNTERSTÜTZER UPLOAD.

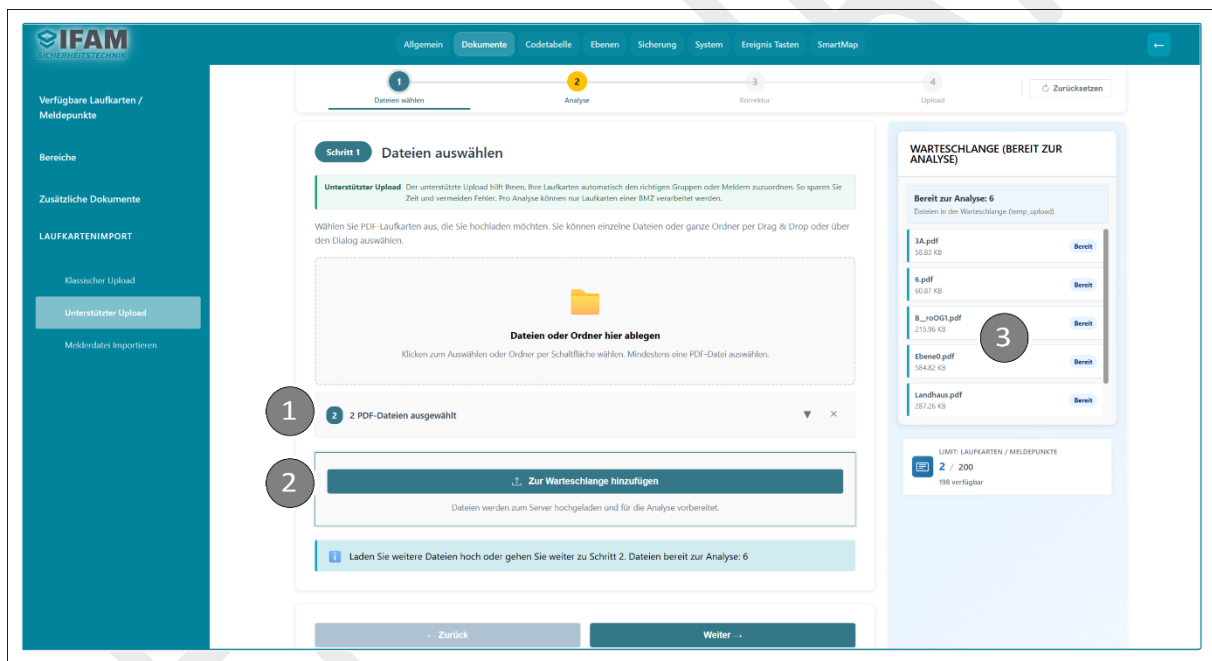


Abbildung 81: IRAS-Website – Laufkarten/unterstützt/Auswahl (Beispiel)

3. Klicken Sie in das Feld DATEIEN ODER ORDNER HIER ABLEGEN und wählen Sie im sich öffnenden Dialogfeld die Laufkarte/den Ordner mit Laufkarten aus. (Alternativ hierzu können die Dateien/Ordner auch per *Drag & Drop*) abgelegt werden.) → Eine Liste der abgelegten Dateien wird angezeigt (1).
4. Für die Analyse von abgelegten Laufkarten wählen Sie die gewünschten Dateien aus und fügen Sie diese der Warteschlange hinzu (ZUR WARTESCHLANGE HINZUFÜGEN) (2). → Die zu analysierenden Dateien werden in einer Liste dargestellt (3).
5. Starten Sie den Analysedurchlauf der Laufkarten (WEITER).

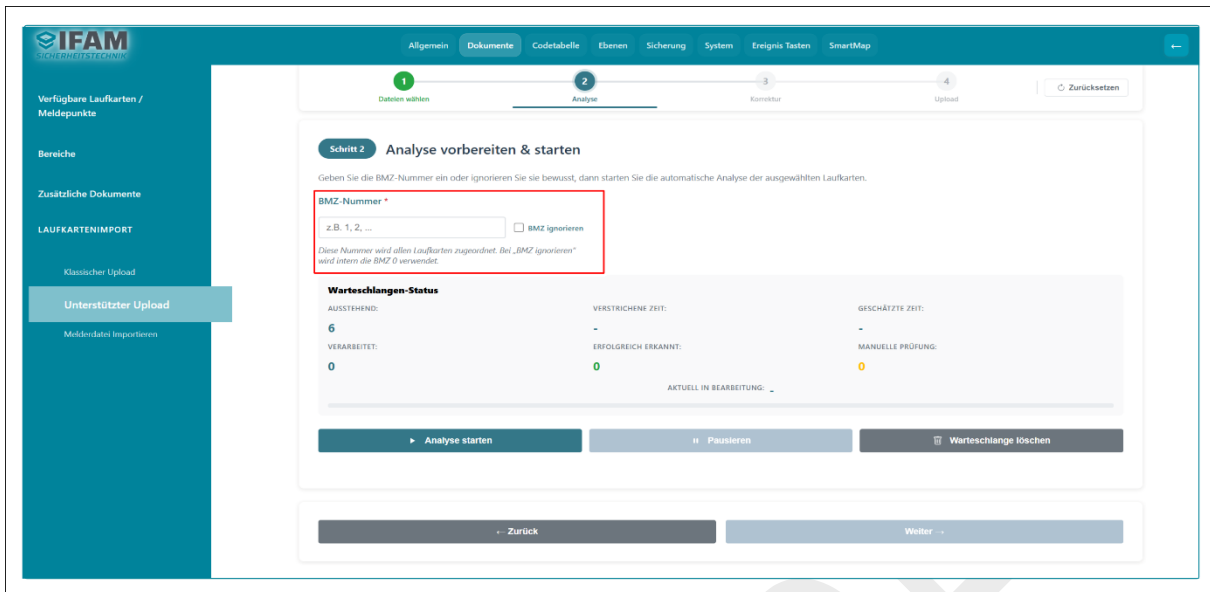


Abbildung 82: IRAS-Website – Laufkarten/unterstützt/Analyse (Beispiel)

6. Geben Sie eine BMZ-Nummer ein bzw. lassen Sie diese unberücksichtigt (BMZ IGNORIEREN)
7. Starten Sie die Analyse. Der Vorgang kann, abhängig von der Anzahl der zu bearbeitenden Dateien, einige Minuten in Anspruch nehmen. Während der Analyse können Sie im Hintergrund weiterarbeiten.

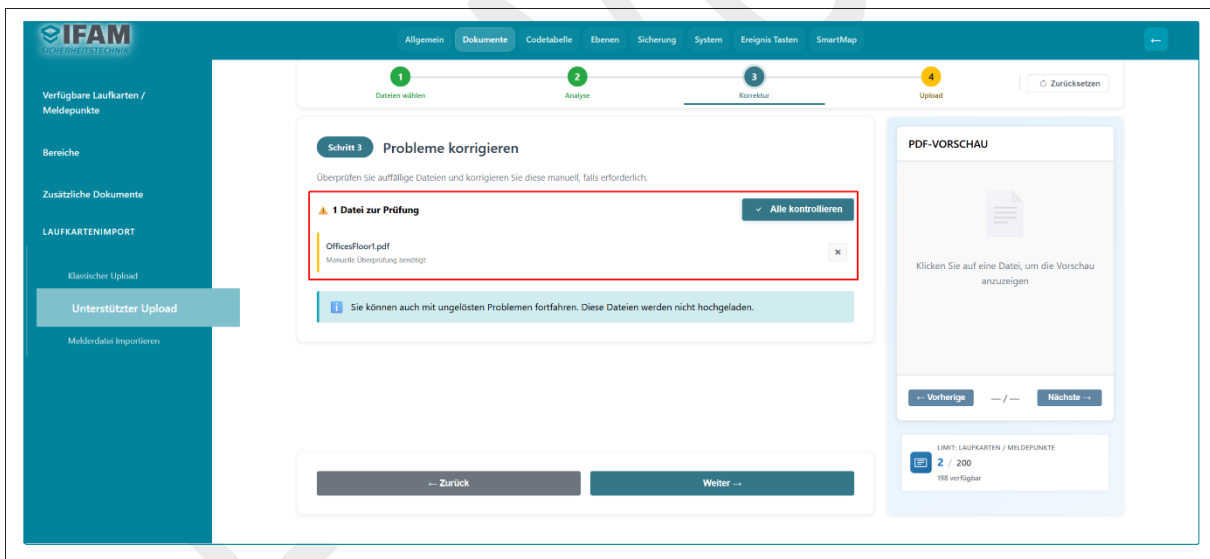


Abbildung 83: IRAS-Website – Laufkarten/unterstützt/Korrektur (Beispiel)

8. Werden fehlerhafte Laufkarten erkannt, werden diese in einer Übersicht dargestellt. Die Fehler können manuell korrigiert werden. Wählen Sie die betreffende Laufkarte aus (einfacher Klick) oder korrigieren Sie alle als fehlerhaft erkannten Laufkarten (ALLE KONTROLLIEREN). Die entsprechenden Laufkarten werden mit einer Eingabeaufforderung zur Korrektur angezeigt (z.B. Gruppen-/ Meldernummer).
9. Folgen Sie den Anweisungen und beenden ggf. Sie die notwendigen Korrekturen (WEITER). → Die Analyse/Korrektur wird abgeschlossen.

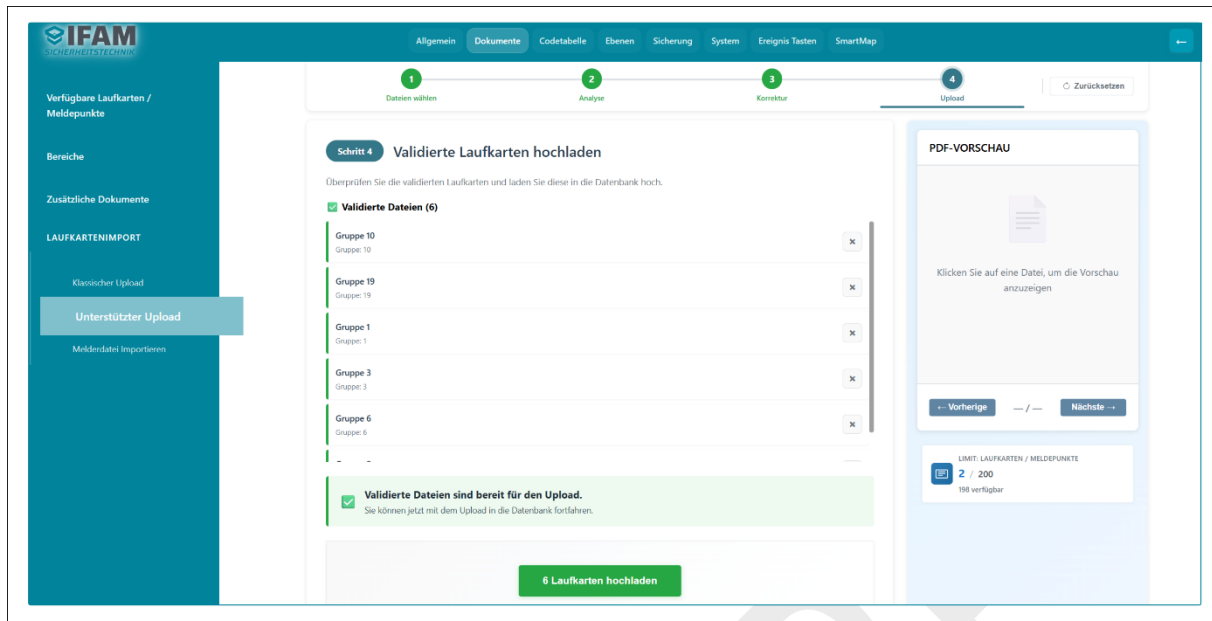


Abbildung 84: IRAS-Website – Laufkarten/unterstützen/Upload (Beispiel)

10. Laden Sie die validierten Laufkarten hoch (...LAUFKARTEN HOCHLADEN). → Eine Upload-Zusammenfassung wird angezeigt.
11. Beenden Sie den Upload.

9.4.8.1.1.4 Verknüpfung mit Meldepunkten

Laufkarten werden im Zuge des Upload-Prozesses in der Regel automatisch den vorhandenen Meldepunkten zugeordnet.

Zusätzlich können die vorhandenen Verknüpfungen manuell angepasst werden, bzw. Laufkarten ohne Verknüpfung zugeordnet werden.

➞ Informationen hierzu finden Sie in [Kapitel 9.4.9 Meldepunkte verwalten](#).

9.4.8.1.2 Laufkarten prüfen – SmartMap

Die IRAS-Secure-Website stellt mit **SMARTMAP** eine Funktion zur Prüfung und Korrektur vorhandener Laufkarten zur Verfügung. Diese Option ist eine Erweiterung des Gefahrenmeldesystems und muss zusätzlich erworben werden.

➡ [Siehe Kapitel 4.7 Systemerweiterungen.](#)

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche des Setup-Bereichs wird geöffnet.
2. Wählen Sie in der Menüzeile den Eintrag SMARTMAP.
→ Die SmartMap-Benutzeroberfläche wird geöffnet.

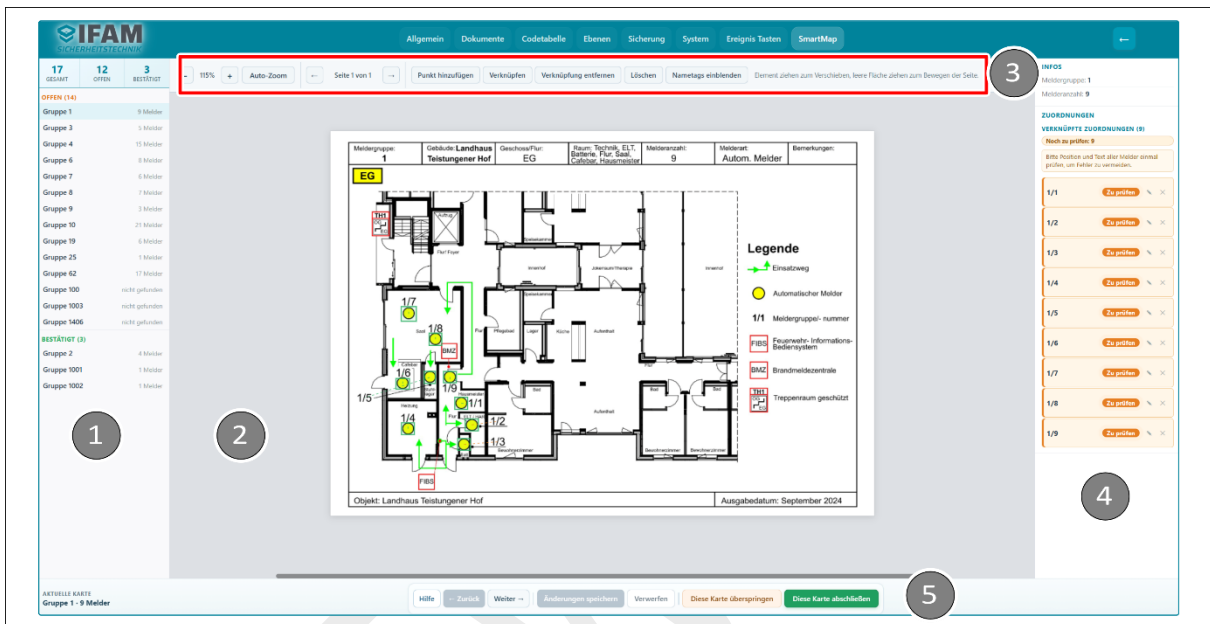


Abbildung 85: IRAS-Secure – SmartMap

9.4.8.1.3 Melderdatei importieren

Einige BMZ-Hersteller bieten die Möglichkeit Melderlisten zu exportieren. Diese können in IRAS-SECURE direkt eingelesen werden. Das Gefahrenmeldesystem importiert dann aus den entsprechenden Melderdateien automatisch alle möglichen bzw. notwendigen Informationen.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche SETUP/DOKUMENTE wird geöffnet.
2. Wählen Sie im Seitenmenü die Option LAUFKARTENIMPORT/MELDERDATEIEN IMPORTIEREN. → Die Oberfläche MELDERDATEI IMPORTIEREN wird geöffnet.
3. Legen Sie das verwendete Dateiformat fest (**1**).
4. Legen Sie die Import-Optionen fest (**3**) (Import Texte/BMZ-Nummern).
5. Wählen Sie die zu importierende Melderdatei (**2**).

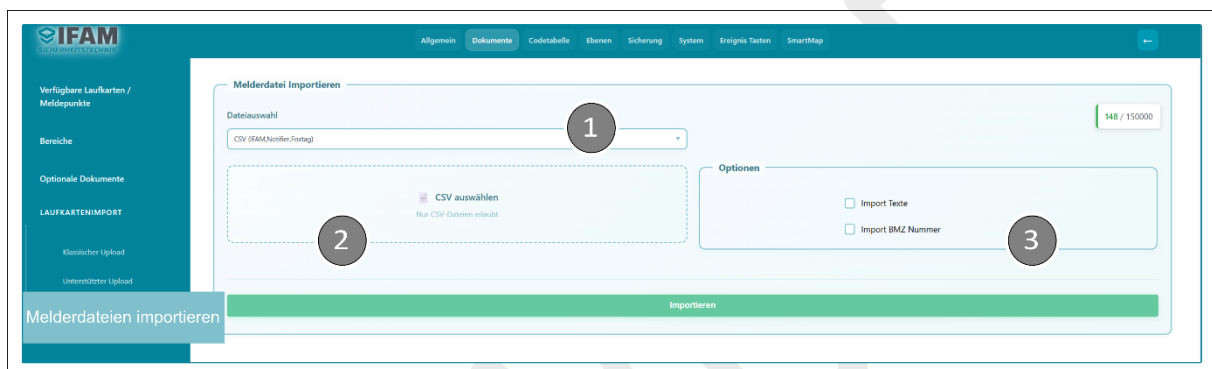


Abbildung 86: IRAS-Website – Melderdateien importieren

9.4.8.1.3.1 Importformate

Für die Integration von Melderdateien werden folgende Herstellerformate unterstützt:

- CSV (IFAM, Notifier, Foxtag),
- PRC,
- MPP,
- XLSX DC3500,
- XLSX Integral,
- CSV Integral.

Bitte fragen Sie den Anbieter der jeweiligen Zentrale, wie Sie an diese Exportdateien gelangen.

9.4.8.1.3.2 CSV (nur IFAM Import)

Über CSV können die Objekte/Melder angelegt werden, ohne dass eine Laufkarte in PDF-Format vorhanden sein muss. Die CSV Datei muss dabei einem vorgegebenen Format entsprechen. Dieses besteht aus einer Zeile mit den Überschriften. In den folgenden Zeilen müssen die Nutzdaten vorhanden sein. Die Reihenfolge der Spalten oder das Vorhandensein von optionalen Spalten wird sehr tolerant beim Import überprüft.

Folgende Spalten sind möglich:

- BMZ,
- Gruppe,
- Melder,
- Kommentar/Text,
- WebCamLink,

- WebCamName,
- DeviceTyp.

Die Trennung der Daten erfolgt ausschließlich mit Semikolon und ohne Leerzeichen zwischen den Spalten.

Groß- oder Kleinschreibung kann ignoriert werden.

Die Spalte **DeviceTyp** gibt an, um welchen Typ es sich bei diesem Meldepunkt handelt. Folgende Typen werden aktuell unterstützt:

- 199 für Gruppe/Melder
- 242 für Steuergruppen/Ausgänge

Wird keine Spalte **DeviceTyp** im CSV gefunden, so werden alle Meldepunkte mit dem Typ 199 importiert und als Gruppe/Melder angelegt.

Beispiele CSV:

BMZ;Gruppe;Melder;Kommentar;WebCamLink;WebCamName;DeviceTyp

```
0;1;0;Gruppe 1 Melder 0;http://www.google.de/.jpg;google cam;199
1;1;1;Gruppe 1 Melder 1;http://www.google.de/.jpg;google cam 2;199
1;1;2;Gruppe 1 Melder 2;http://www.google.de/.jpg;google 3;199
1;1;1;Steuergruppe 1 Ausgang 1; http://www.google.de/.jpg;google 4;242
```



Die maximale Größe einer einzelnen CSV-Datei darf **100 MByte** nicht überschreiten!

9.4.8.1.4 Verknüpfung mit Meldepunkten



Siehe Kapitel 9.4.9 Meldepunkte verwalten.

9.4.8.2 Zusätzliche Dokumente

Zusätzliche Dokumente dienen der Bereitstellung zusätzlicher Informationen zu Meldeobjekten, auf die im Ereignisfall zugegriffen werden kann und auch in der IRAS-APP zum Download zur Verfügung stehen.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zur Systemverwaltung wird geöffnet.
2. Wählen Sie die Option ZUSÄTZLICHE DOKUMENTE.
→ Die Benutzeroberfläche zur Verwaltung von zusätzlichen Dokumenten wird geöffnet.

9.4.8.2.1 Zusätzliche Dokumente hochladen

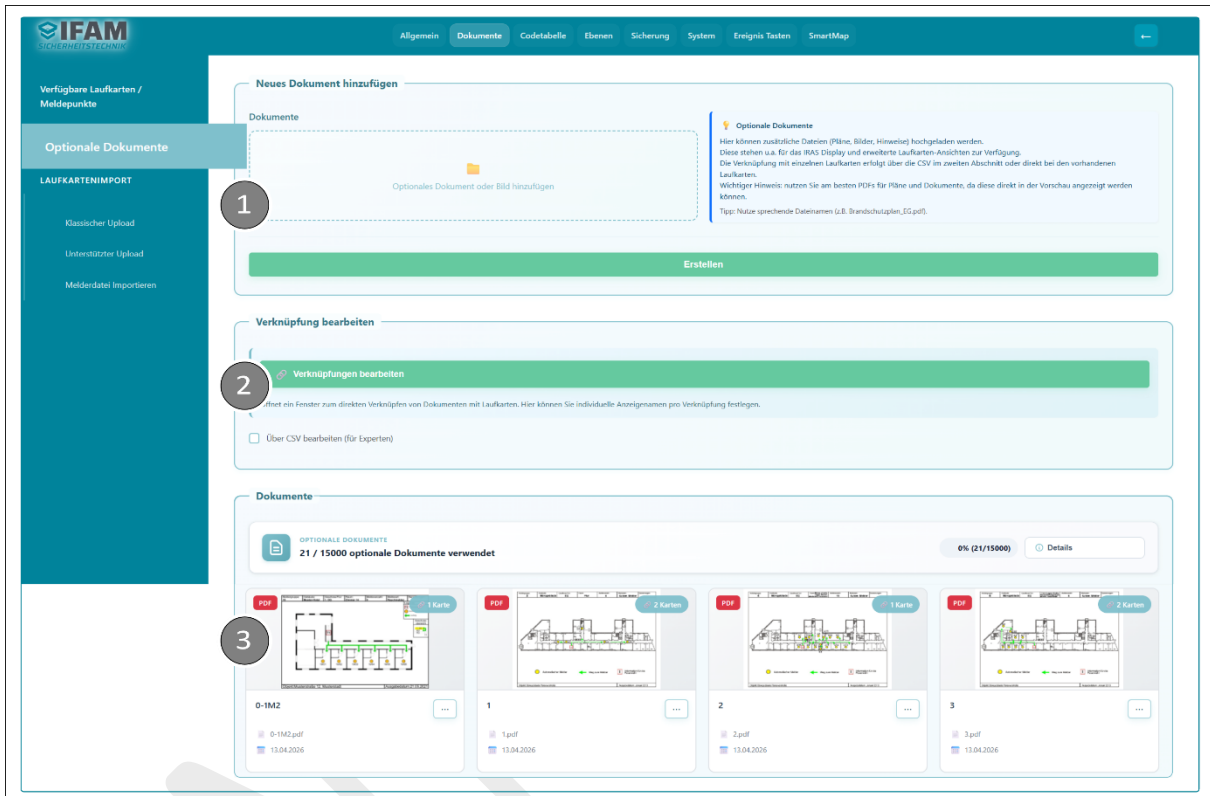


Abbildung 87: IRAS-Website – Optionale Dokumente verwalten

Im unteren Bereich werden bereits vorhandene Dokumente angezeigt (DOKUMENTE) (3).

Zusätzliche Dokumente können im Bereich NEUES DOKUMENT HINZUFÜGEN (1) hochgeladen werden. Mit einem Klick in den Funktionsbereich öffnet sich ein Dialogfeld, in dem die gewünschten Dokumente ausgewählt und hochgeladen werden können.

Ordner mit Dokumenten können per Drag-an-Drop abgelegt werden.

9.4.8.2.2 Verknüpfung mit Meldepunkten

➞ Siehe Kapitel 9.4.9 Meldepunkte verwalten.

9.4.8.2.3 Verknüpfung mit Laufkarten

Zusätzliche Dokumente können mit vorhandenen Laufkarten verknüpft werden. Wählen sie hierzu im Funktionsbereich VERKNÜPFUNG BEARBEITEN (2) die gleichnamige Schaltfläche.

Abbildung 88: IRAS-Website – Optionale Dokumente/Verknüpfung

Das sich öffnende Dialogfeld enthält eine Übersicht der vorhandenen Laufkarten/Meldepunkte (LAUFKARTE).

Neben der Laufkarte findet sich eine Liste der bereits mit ihr verknüpften zusätzlichen Dokumente (VERKNÜPFTE DOKUMENTE).

Mit der Aktivierung der Schaltfläche DOKUMENTE HINZUFÜGEN kann der jeweiligen Laufkarte ein Dokument beigelegt werden.

Wählen Sie ein verfügbares Dokument aus. → Das Dokument wird mit der Laufkarte des Meldepunktes verknüpft und in die Liste eingetragen.

Der für das Dokument angezeigte Name kann individuell vergeben werden ().



Für die Verknüpfung steht zusätzlich eine Experten-Modus zur Verfügung. Aktivieren Sie hierfür den Modus ÜBER CSV BEARBEITEN.

9.4.8.3 IP-Kameras



Wird die Kommunikation zwischen dem IRAS-Gefahrenmeldesystem und der IP-Kamera über einen mobilen Zugang vorgenommen, fallen aufgrund des erhöhten Datenverkehrs, ggf. höhere Gebühren an.

Zum Verwalten/Hinzufügen von IP-Kameras gehen Sie wie folgt vor:

1. Wählen Sie auf dem **DASHBOARD** in der Menüleiste die Schaltfläche **SETUP**. → Die Benutzeroberfläche zur Systemverwaltung wird geöffnet.
2. Wählen Sie in der Menüleiste am oberen Rand die Schaltfläche **ALLGEMEIN (2)**. → Die Benutzeroberfläche zur Verwaltung von IP-Kameras und weiterer Optionen wird geöffnet.

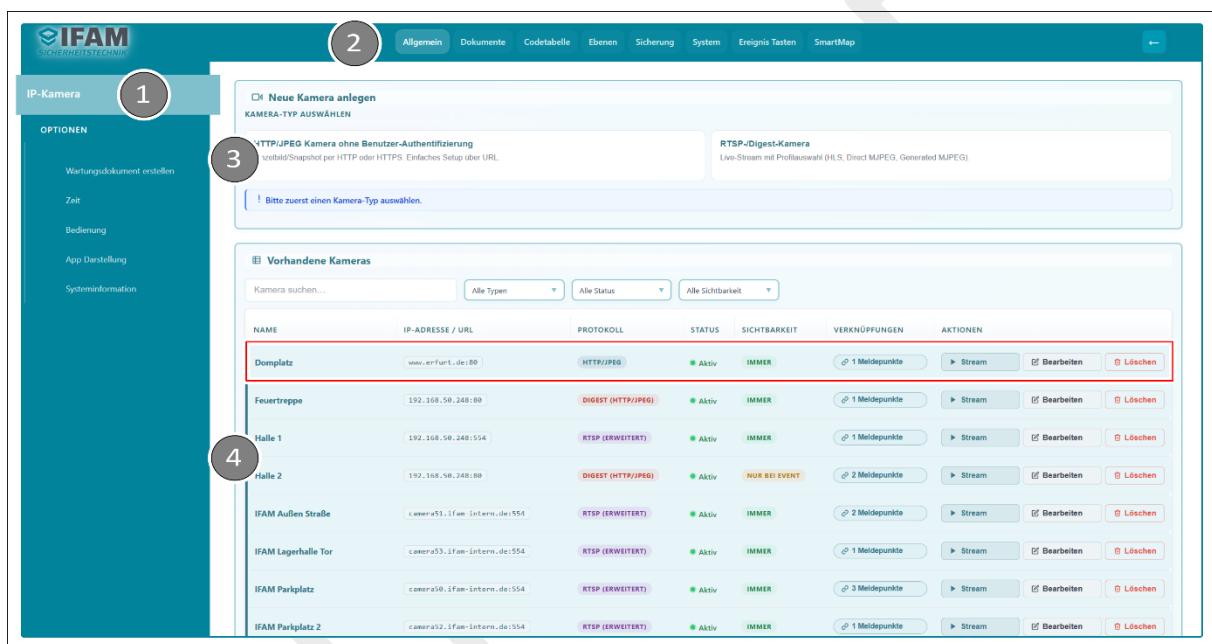


Abbildung 89: IRAS-Website – IP-Kameras (Beispiel)

Im Untermenü **IP-KAMERA (1)** werden in einer Übersicht (4) ggf. bereits vorhandene Kameras und deren Eigenschaften angezeigt (z.B. IP-Adresse, Protokoll, Status, Verknüpfungen). Darüber hinaus können weitere Kameras hinzugefügt werden (3).

9.4.8.3.1 Vorhandene Kameras verwalten

Bereits im System integrierte Kameras können in ihren Eigenschaften angepasst werden. Wählen Sie die anzupassende Kamera (z.B. *Domplatz*) und klicken Sie auf die Schaltfläche **BEARBEITEN**. → Eine Konfigurationsoberfläche wird geöffnet.

Passen Sie die entsprechenden Parameter an und speichern Sie die Änderungen.

Abbildung 90: IRAS-Website – IP-Kamera/Eigenschaften anpassen

9.4.8.3.2 Neue Kamera anlegen

Abbildung 91: IRAS-Website – IP-Kamera anlegen

Wählen Sie im Untermenü IP-KAMERA/Neue Kamera anlegen eine der folgenden Anbin-
dungs-Optionen:

- **HTTP/JPEG-Kamera:** frei zugängliche HTTP/URL, ohne Benutzerauthentifizierung (1)
- **RTSP-/Digest-Kamera:** HTTP/RTSP, mit Benutzerauthentifizierung (2).

9.4.8.3.2.1 HTTP/JPEG – ohne Benutzerauthentifizierung

Abbildung 92: IRAS-Website – IP-Kamera/ohne Benutzerauthentifizierung

- Kamera-Namen vergeben – zur Identifikation der Kamera auf der Webseite,
- HTTP/URL mit Pfad eingeben (z.B. <http://www.erfurt.de:80/webcam/domplatz.jpg>),
- SICHTBARKEIT wählen. Hierbei kann zwischen **immer sichtbar** und **nur bei Feuer-Event** gewählt werden.

9.4.8.3.2.2 RTSP-/Digest-Kamera – mit Benutzerauthentifizierung

☒ Neue Kamera anlegen

KAMERA-TYP AUSWÄHLEN

HTTP/JPEG Kamera ohne Benutzer-Authentifizierung
Einzelbild/Snapshot per HTTP oder HTTPS. Einfaches Setup über URL.

RTSP-/Digest-Kamera
Live-Stream mit Profilauswahl (HLS, Direct MJPEG, Generated MJPEG).

1. STREAM-PROFIL AUSWÄHLEN

1 **Beste Bildqualität (HLS)** **EMPFOHLEN**
Flüssigster & stabilster Stream, beste Bildqualität ~3-7 Sek. Verzögerung.

2 **Wenig Verzögerung**
Kürzeste Verzögerung (wenn von der Kamera unterstützt, z.B. AVIOTEC).

3 **Kompromiss**
Kompromiss aus Verzögerung und Qualität (Generated MJPEG).

Abbildung 93: IRAS-Website – IP-Kamera mit Authentifizierung

Stream-Profil auswählen

- **HLS (1) (empfohlen)**
 - sehr flüssiges Bild,
 - größte Verzögerung zum Livebild (RTSP).
- **Wenig Verzögerung (2)**
 - basiert auf HTTP,
 - mit Nutzernamen und Passwort gesichert ist,
 - Darstellung ähnlich einem Live-Bild, aber deutlich weniger Bilder pro Sekunde,
 - weniger flüssiges Bild.
- **Kompromiss (3):**
 - Mix aus **HLS** und **VERZÖGERUNG**,
 - geringere Verzögerung als über HLS aber nur geringfügig bessere Bildqualität als bei HTTP,
 - arbeitet auch über RTSP.

Stream-Profil einrichten

BESTE QUALITÄT und KOMPROMISS

☒ Neue Kamera anlegen

KAMERA-TYP AUSWÄHLEN

HTTP/JPEG Kamera ohne Benutzer-Authentifizierung
Einzelbild/Snapshot per HTTP oder HTTPS. Einfaches Setup über URL.

RTSP-/Digest-Kamera
Live-Stream mit Profilauswahl (HLS, Direct MJPEG, Generated MJPEG).

1. STREAM-PROFIL AUSWÄHLEN

Beste Bildqualität (HLS) **EMPFOHLEN**
Flüssigster & stabilster Stream, beste Bildqualität ~3-7 Sek. Verzögerung.

Wenig Verzögerung
Kürzeste Verzögerung (wenn von der Kamera unterstützt, z.B. AVIOTEC).

Kompromiss
Kompromiss aus Verzögerung und Qualität (Generated MJPEG).

2. KAMERA-ZUGANGSDATEN EINGEBEN

NAME *

z.B. RTSP Kamera Halle 1

IP-ADRESSE *

192.168.50.248

PORT

554

BENUTZERNAME

optional

PASSWORT

optional

ZIEL-FPS

20

RTSP-PFAD

/

SICHTBARKEIT

Immer sichtbar

AKTIV

☒ Aktiv

+ Erstellen

Abbildung 94: IRAS-Website – IP-Kamera/Beste Qualität und Kompromiss

Die Einrichtung der Stream-Profile Beste **Qualität** und **Kompromiss** ist identisch:

- Aufrufen der Kamera. In den Einstellungen **RTSP** (meist unter Netzwerk) **aktivieren**. **PORT DER KAMERA** notieren (standardmäßig Port **554**). Ort und Art der Kamera-Einstellungen kann, abhängig vom jeweiligen Kamerahersteller, variieren. Informieren Sie sich ggf. in der herstellereigenen Dokumentation!
- **KAMERA-NAMEN** vergeben (zur Identifikation auf der Webseite),
- **IP-Adresse der Kamera** und den korrekten **RTSP-Port** eintragen,
- **Benutzername und Passwort des Kamera-Nutzers** erstellen (ebenfalls auf der Seite der Kamera) (**optional**),
- **Ziel-FPS** (Bildwiederholungsrate) festlegen (**optional**),
- **RTSP-Pfad** festlegen (**optional**) – von den Kameraeinstellungen abhängig. Im Normalfall das vorausgefüllte **“/”** belassen.
- **SICHTBARKEIT** einstellen. Hierbei kann zwischen **immer sichtbar** und **nur bei Feuer-Event** gewählt werden,
- **AKTIVIERUNG (ja/nein)** festlegen – **NEIN**: globale Abschaltung, ohne Anpassung der Zuordnung. Kamera ist z.B. nicht mehr in der Übersicht zur Auswahl oder beim Verknüpfen mit den Gruppen/Meldern etc. sichtbar.

WENIG VERZÖGERUNG

Neue Kamera anlegen

KAMERA-TYP AUSWÄHLEN

HTTP/JPEG Kamera ohne Benutzer-Authentifizierung
Einzelbild/Snapshot per HTTP oder HTTPS. Einfaches Setup über URL.

RTSP-Digest-Kamera
Live-Stream mit Profileauswahl (HLS, Direct MJPEG, Generated MJPEG).

1. STREAM-PROFIL AUSWÄHLEN

Beste Bildqualität (HLS) **EMPFOHLEN**
Flüssigster & stabiler Stream, beste Bildqualität. ~3-7 Sek. Verzögerung.

Wenig Verzögerung
Kürzeste Verzögerung (wenn von der Kamera unterstützt, z.B. AVIOTEC).

Kompromiss
Kompromiss aus Verzögerung und Qualität (Generated MJPEG).

2. KAMERA-ZUGANGSDATEN EINGEBEN

NAME *
z.B. RTSP Kamera Halle 1

IP-ADRESSE *
192.168.50.248

PORT
80
HTTP-Port der Kamera

BENUTZERNAME
optional

PASSWORT
optional

SICHTBARKEIT
Immer sichtbar

AKTIV
☒ Aktiv

BEWEGUNGSERKENNUNG ANZEIGEN **?**
☒ An

+ Erstellen

Abbildung 95: IRAS-Website – IP-Kamera/Wenig Verzögerung

- **KAMERA-NAMEN** vergeben (zur Identifikation auf der Webseite),
- **IP-Adresse der Kamera** und den korrekten **RTSP-Port** eintragen – HTTP muss wie bei RTSP je nach Kamera/Hersteller aktiv sein,
- **PORT DER KAMERA** einfügen (standardmäßig Port **80**),
- **Benutzername und Passwort des Kamera-Nutzers** erstellen (ebenfalls auf der Seite der Kamera),
- **SICHTBARKEIT** einstellen. Hierbei kann zwischen **immer sichtbar** und **nur bei Feuer-Event** gewählt werden,

- AKTIVIERUNG (ja/nein) festlegen – **NEIN**: globale Abschaltung, ohne Anpassung der Zuordnung. Kamera ist z.B. nicht mehr in der Übersicht zur Auswahl oder beim Verknüpfen mit den Gruppen/Meldern etc. sichtbar.
- BEWEGUNGSERKENNUNG ANZEIGEN – bei bestimmten Kameras, z.B. *Bosch Aviotec*, können Bewegungserkennungs-Linien angezeigt werden (z.B. gelber Kasten und grüne Linie im Bild).

9.4.8.3.3 IP-Kamera mit Meldepunkt verknüpfen

➞ *Siehe Kapitel 9.4.9.3 Meldepunkt mit Kamera verknüpfen.*

ENTWURF

9.4.9 Meldepunkte verwalten

Den in einer Gefahrenmeldeanlage vorhandenen Meldepunkten müssen/können spezifische Informationsmedien (Laufkarten, zusätzliche Dokumente, IP-Kameras) zugeordnet werden, die im Ereignisfall eingesehen bzw. versendet werden können.

1. Wählen Sie in der Menüzeile den Eintrag SETUP.
→ Die Benutzeroberfläche SETUP-Bereich wird geöffnet.
2. Wählen Sie die Option VERFÜGBARE LAUFKARTEN/MELDEPUNKTE.
→ Eine Übersicht der vorhandenen Meldepunkte wird angezeigt.



Die Übersicht der vorhandenen Meldepunkte kann exportiert werden (EXPORT). Die erzeugte CSV-Datei wird im Downloadbereich ihres Betriebssystems abgelegt.

MAPKEY	BMZ	BEZEICHNUNG	ZUSATZINFO	TYP	UNTERPUNKTE	LAUFKARTE	LÖSCHEN
0-180	0	Gruppe 1	Zuständig...	GRUPPE	0	✓	🗑️
0-360	0	Gruppe 3	Zuständig...	GRUPPE	0	✓	🗑️
0-600	0	Gruppe 4	Zuständig...	GRUPPE	0	✓	🗑️
0-660	0	Gruppe 6	Zuständig...	GRUPPE	0	✓	🗑️
0-780	0	Gruppe 7	Zuständig...	GRUPPE	0	✓	🗑️
0-960	0	Gruppe 9	Zuständig...	GRUPPE	0	✓	🗑️
0-1040	0	Gruppe 10	Zuständig...	GRUPPE	0	✓	🗑️
0-1260	0	Gruppe 12	Zuständig...	GRUPPE	0	✓	🗑️
0-1360	0	Gruppe 13	Zuständig...	GRUPPE	0	✓	🗑️
0-1560	0	Gruppe 15	Zuständig...	GRUPPE	0	✓	🗑️
0-1680	0	Gruppe 16	Zuständig...	GRUPPE	0	✓	🗑️
0-1760	0	Gruppe 17	Zuständig...	GRUPPE	0	✓	🗑️
0-1960	0	Gruppe 19	Zuständig...	GRUPPE	0	✓	🗑️
0-2260	0	Gruppe 22	Zuständig...	GRUPPE	0	✓	🗑️

Abbildung 96: IRAS-Website – Meldepunkte/Übersicht

Die Übersicht enthält alle vorhandenen Meldepunkte, deren Typ (z.B. Gruppe, Steuerungsgruppe), das Vorhandensein von Laufkarten und ggf. die Anzahl vorhandener Melder.

Meldepunkte können aus der Übersicht/dem Gefahrenmeldesystem gelöscht werden (LÖSCHEN).

Wählen Sie durch einfachen Klick auf den gewünschten Eintrag eine Übersicht mit den Eigenschaften des jeweiligen Meldepunktes (Abbildung 97).

Das Fenster enthält:

- Vorschau ggf. bereits zugeordneter Laufkarten (VORSCHAU).
- Übersicht ggf. bereits vorhandener zusätzlicher Dokumente (DOKUMENTE) (Abbildung 98).
- Übersicht verknüpfter IP-Kameras (KAMERAS) (Abbildung 99).

9.4.9.1 Vorschau (Laufkarte)

Abbildung 97: IRAS-Website – Meldepunkt/Vorschau

Die in der Vorschau angezeigte Laufkarte kann als PDF als exportiert werden (PDF HERUNTERLADEN). Das Dokument wird im Download-Bereich Ihres Betriebssystems abgelegt.

Mit einem einfachen Klick auf die angezeigt Laufkarten-Vorschau wird das Dokument in einem separaten Fenster angezeigt (Abbildung 112). Falls ein Drucker eingerichtet wurde kann es von hier gedruckt werden.

Eine bereits vorhandene Laufkarte kann von der VORSCHAU aus auch ersetzt/getauscht werden (PDF ERSETZEN). Wählen Sie hierzu im sich öffnenden Dialogfeld das gewünschte Dokument und bestätigen Sie (ÖFFNEN).

9.4.9.2 Meldepunkt mit Dokumenten verknüpfen



Abbildung 98: IRAS-Website – Meldepunkt/Dokumente

Mit der Wahl der Option DOKUMENTE werden ggf. bereits verknüpfte (zusätzliche) Dokumente angezeigt (1).

Mit einem einfachen Klick auf die Vorschau wird ein Dokument in einem separaten Fenster angezeigt (Abbildung 113). Falls ein Drucker eingerichtet wurde, kann es von hier gedruckt werden.

Über das Vorschaufenster kann die Verknüpfung eines Dokuments mit einem Meldepunkt wieder aufgehoben werden.

Zur Zuordnung/Verknüpfung eines (zusätzliches) Dokumentes mit einem Meldepunkt, kann aus den verfügbaren Dokumenten (2) eine Datei ausgewählt und dem Meldepunkt zugeordnet werden (VERKNÜPFEN).

9.4.9.3 Meldepunkt mit Kamera verknüpfen

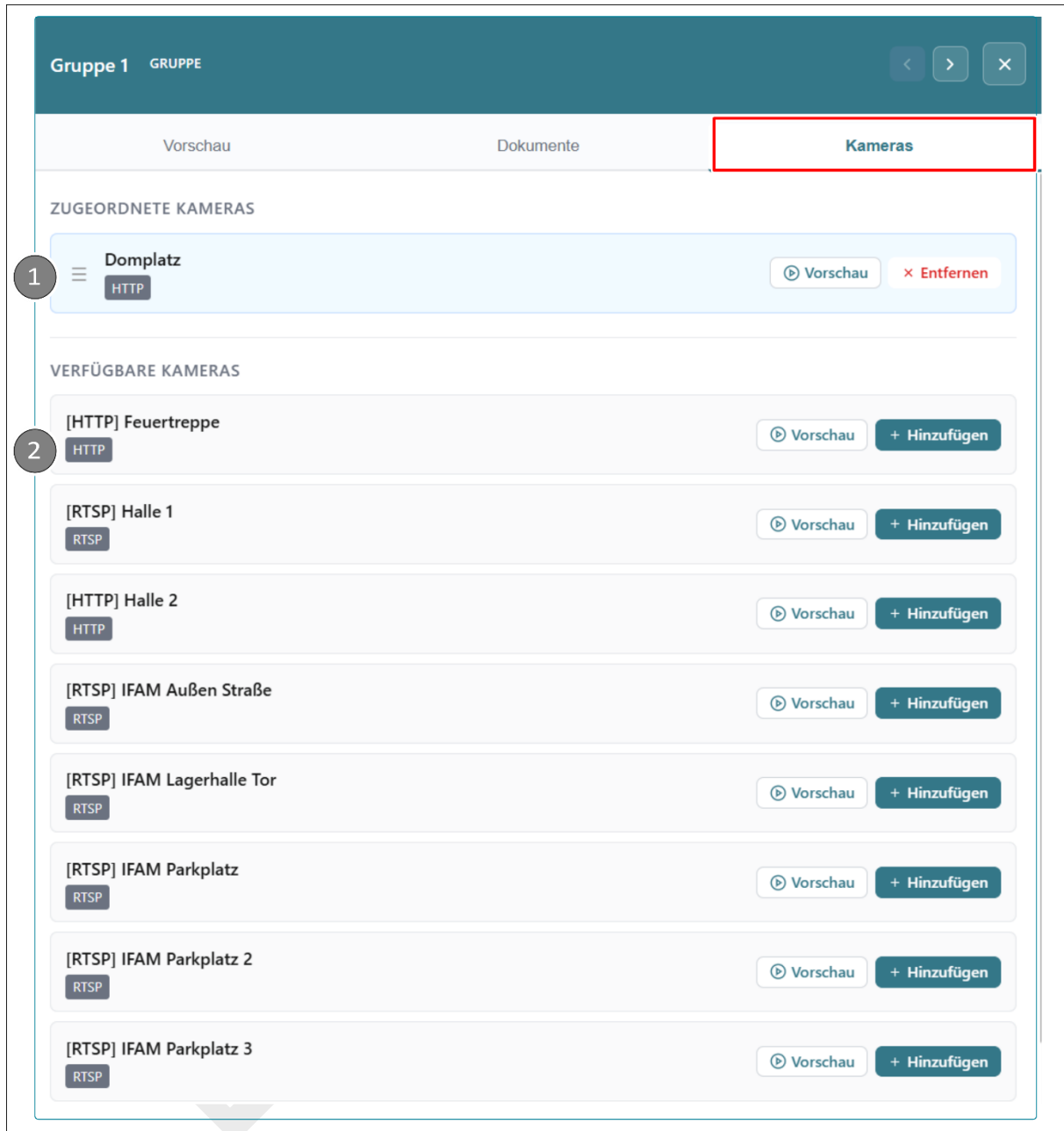


Abbildung 99: IRAS-Website – Meldepunkt/Kamera

Mit der Wahl der Option KAMERAS werden dem Meldepunkt ggf. bereits zugeordnete IP-Kameras angezeigt (1).

Mit einem einfachen Klick (VORSCHAU) auf eine Kamera wird die aktuelle Kameraansicht, entsprechend den konfigurierten Stream-Profilen, in einem separaten Fenster angezeigt (Abbildung 114).

Über die Schaltfläche **ENTFERNEN** kann die Verknüpfung einer Kamera mit einem Meldepunkt gelöst werden.

Zur Zuordnung/Verknüpfung einer Kamera mit einem Meldepunkt, kann aus den VERFÜGBAREN KAMERAS (2) ein Gerät gewählt und dem Meldepunkt zugeordnet werden (HINZUFÜGEN).

9.4.9.4 Bereiche anlegen/verwalten

9.4.9.4.1 Übersicht

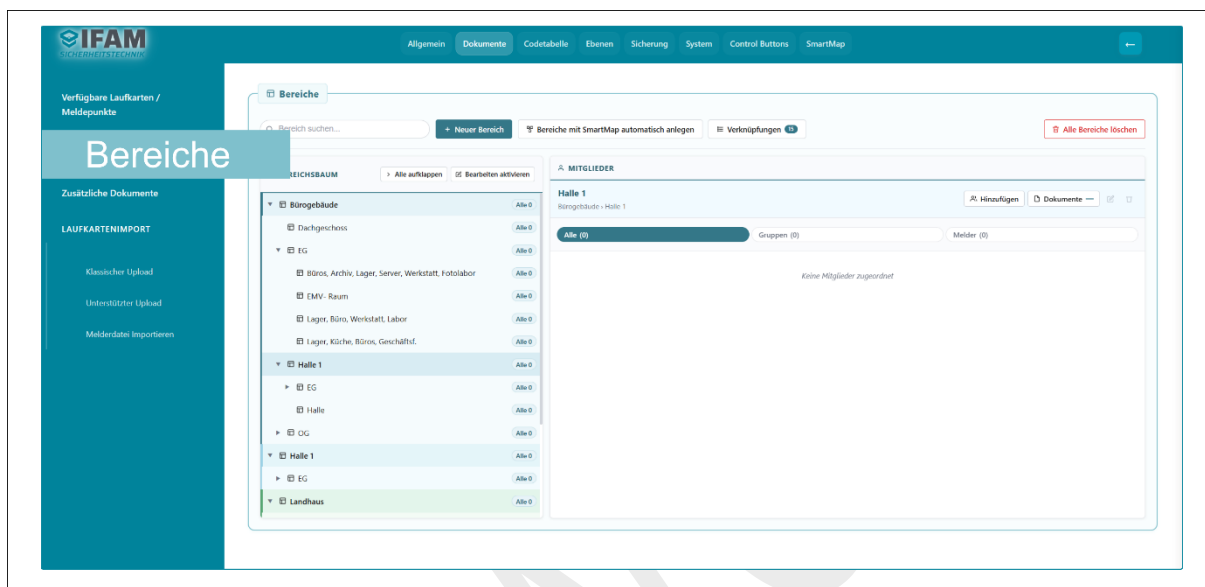
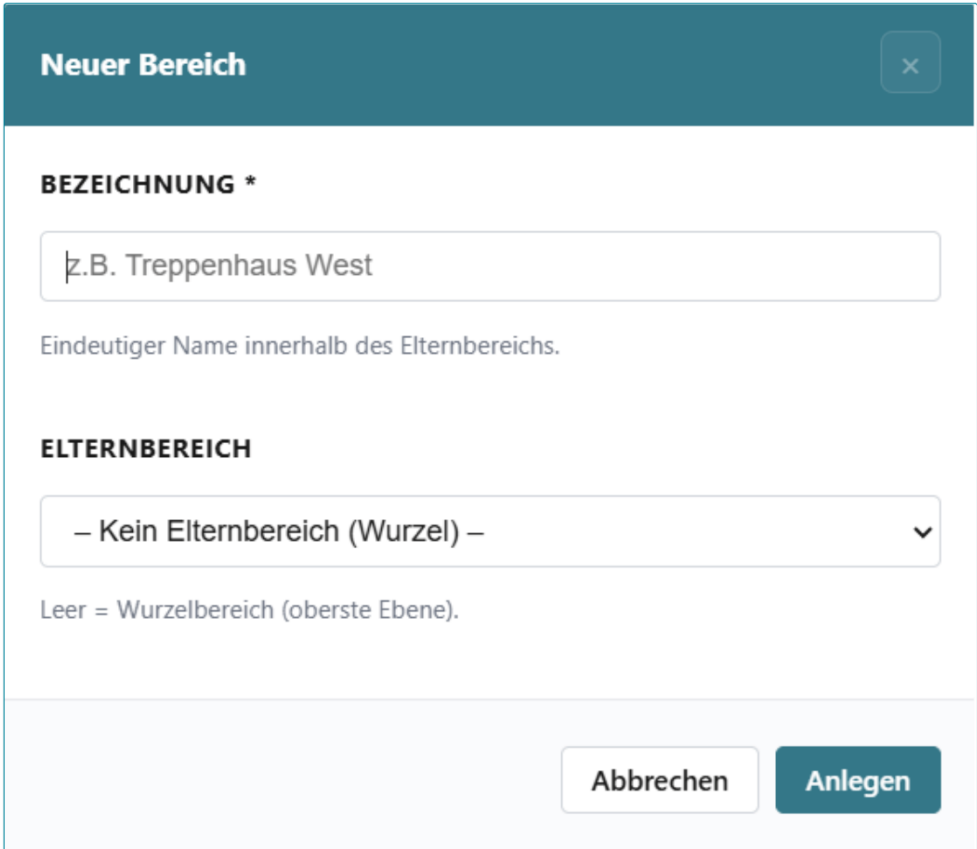


Abbildung 100: IRAS-Website – Bereiche/Übersicht

9.4.9.4.2 Bereich anlegen



Neuer Bereich

BEZEICHNUNG *

z.B. Treppenhaus West

Eindeutiger Name innerhalb des Elternbereichs.

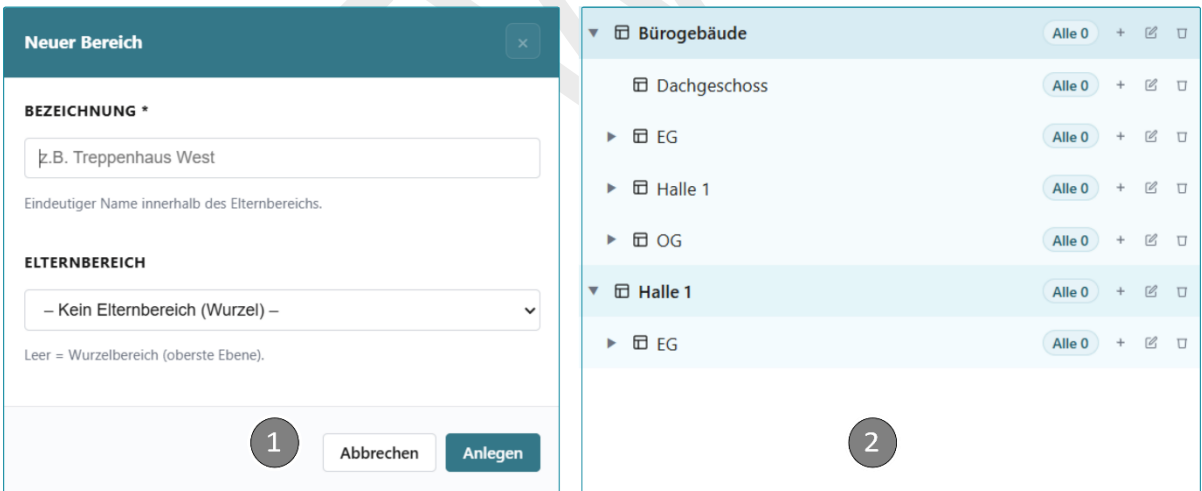
ELTERNBEREICH

– Kein Elternbereich (Wurzel) –

Leer = Wurzelbereich (oberste Ebene).

Abbrechen Anlegen

Abbildung 101: IRAS-Website – Bereich/neu anlegen



Neuer Bereich

BEZEICHNUNG *

z.B. Treppenhaus West

Eindeutiger Name innerhalb des Elternbereichs.

ELTERNBEREICH

– Kein Elternbereich (Wurzel) –

Leer = Wurzelbereich (oberste Ebene).

1 Abbrechen Anlegen

Bürogebäude Alle 0 + [edit] [trash]

- Dachgeschoss Alle 0 + [edit] [trash]
 - EG Alle 0 + [edit] [trash]
 - Halle 1 Alle 0 + [edit] [trash]
 - OG Alle 0 + [edit] [trash]
- Halle 1 Alle 0 + [edit] [trash]
 - EG Alle 0 + [edit] [trash]

2

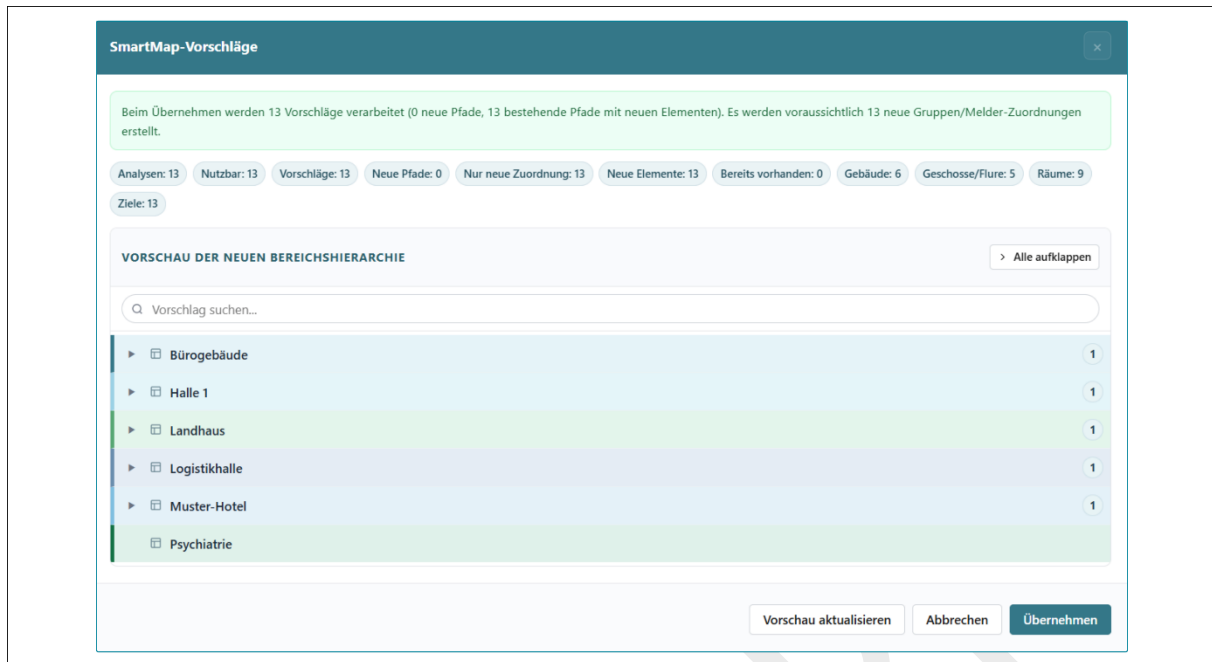


Abbildung 102: IRAS-Website – Bereich/neu anlegen/SmartMap

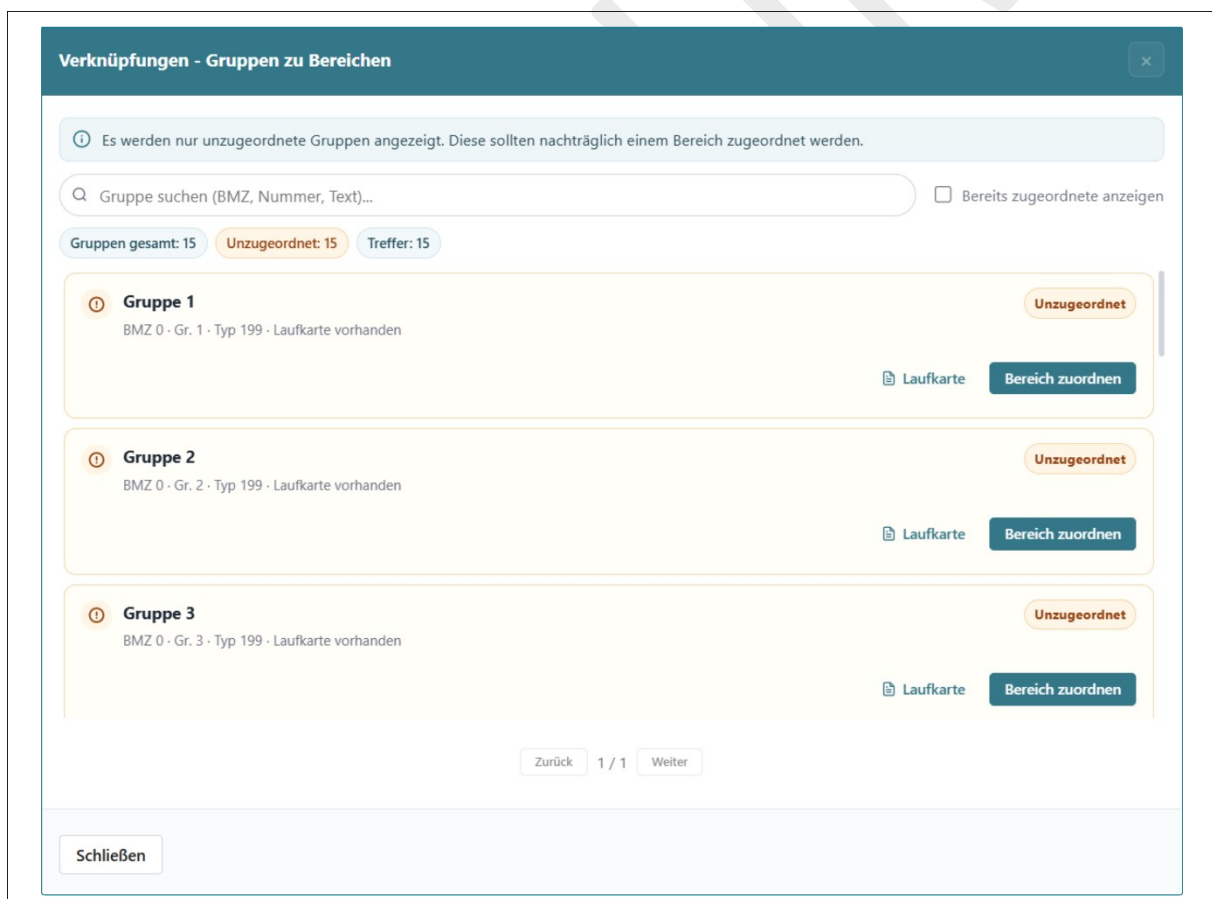
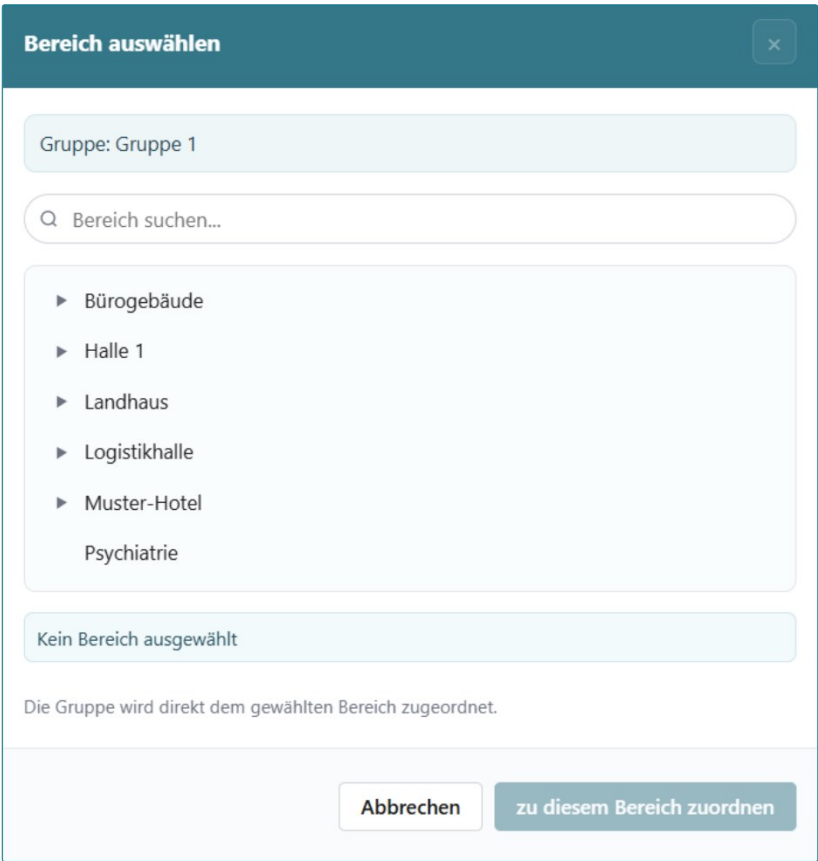


Abbildung 103: IRAS-Website – Meldepunkte/Bereiche zuordnen 1



Bereich auswählen

Gruppe: Gruppe 1

Q Bereich suchen...

- ▶ Bürogebäude
- ▶ Halle 1
- ▶ Landhaus
- ▶ Logistikhalle
- ▶ Muster-Hotel
- Psychiatrie

Kein Bereich ausgewählt

Die Gruppe wird direkt dem gewählten Bereich zugeordnet.

Abbrechen zu diesem Bereich zuordnen

Abbildung 104: IRAS-Website – Meldepunkte/Bereiche zuordnen 2

9.4.10 Benachrichtigungs-/Ausgabeoptionen

9.4.10.1 E-Mail

Für IRAS-SECURE können Benachrichtigung per E-Mail nach den jeweiligen Erfordernissen konfiguriert werden.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zum Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SYSTEM.
→ Der Systembereich wird geöffnet.
3. Wählen Sie die Option E-Mail.

9.4.10.1.1 Server-Einstellungen

The screenshot shows the IRAS-SECURE web interface. The left sidebar contains a menu with 'E-Mail' and 'Server' highlighted. The main content area is divided into several sections:

- Email Benachrichtigung aktivieren:** A checkbox labeled 'E-Mail Benachrichtigungen aktivieren' is shown. A green button labeled 'Übernehmen' is below it. A callout '1' points to this checkbox.
- Server Einstellungen:** This section contains various input fields for server configuration:
 - Serveradresse: w00dlee.kasserver.com
 - Serverport: 587
 - Verschlüsselung: Radio buttons for 'kein', 'SSL', and 'TLS' (selected).
 - Benutzerauthentifizierung: A checked checkbox labeled 'Benutzer-Authentifizierung'.
 - Benutzername: m037dca9
 - Passwort: (empty field)
 - Sender Email-Adresse: Ubuntu@ifam-erfurt.de
 - Anzeigename beim Empfänger: Ubuntu@ifam-erfurt.de
 - Antwortadresse für Empfänger: Ubuntu@ifam-erfurt.de
 - maximal Sendeverzögerung in Sekunden: 30
 A green button labeled 'Übernehmen' is at the bottom of this section. A callout '2' points to the 'Server Einstellungen' header.
- Test E-Mail:** A section with a text input field for 'E-Mail Empfänger:' containing 'test@example.com' and a green button labeled 'Test E-Mail abschicken'. A callout '3' points to this section.
- E-Mail Empfänger verwalten:** A section titled 'Empfänger E-Mail Empfänger verwalten' with a 'Hinzufügen' button. Below it is a table:

ID	E-Mail-Adresse	Aktion
3	niklaschumane.n242@gmail.com	Übernehmen Löchen
4	n.schumann@ifam-erfurt.de	Übernehmen Löchen
5	nik.coc242@gmail.com	Übernehmen Löchen

 A callout '4' points to this table.

Abbildung 105: IRAS-Website – E-Mail/Server

Aktivieren Sie die E-Mail-Funktion (E-MAIL BENACHRICHTIGUNGEN AKTIVIEREN) (1).

Nehmen Sie die notwendigen SERVER-EINSTELLUNGEN (2) vor.

Für die benötigten Informationen wenden Sie sich ggf. bitte an den jeweiligen Provider.

Bestätigen Sie die Eingabe (ÜBERNEHMEN). → IRAS-SECURE führt eine Sicherheitsprüfung durch. Sollte diese fehlschlagen, prüfen Sie bitte die hinterlegten Parameter oder wenden Sie sich an Ihren Provider.



Einige E-Mail-Anbieter lassen keine *unsicheren Anwendungen* zu. Bitte prüfen Sie ihre Einstellungen und die Möglichkeiten ihres Providers.



Nicht alle E-Mail-Anbieter sind kompatibel mit der Funktion des IRAS-SECURE-Gefahrenmeldesystem.
Führen Sie nach der Einrichtung der E-Mail-Funktion eine Funktionsprüfung durch!



Die E-Mail-Funktionalität des IRAS-SECURE-Gefahrenmeldesystems ist von Drittanbietern abhängig. Diese können auch während des Betriebes ihren Funktionsumfang ggf. erweitern/anpassen oder einschränken. Bitte prüfen Sie in regelmäßigen Abständen das ordnungsgemäße Funktionieren der E-Mail-Funktion (Test E-Mail) (3).



Sollten die Daten über den Export gesichert werden, werden innerhalb der Exportdatei weder Passwort noch Nutzernamen für den E-Mail-Account gespeichert.

Um die vorgenommene Konfiguration bzw. den korrekten Versand zu prüfen, haben Sie die Möglichkeit, eine Test-Mail (TEST/TEST-E-MAIL) (3) zu verschicken.

Legen Sie abschließend die für den Ereignisfall zu berücksichtigenden E-Mail-Empfänger fest (EMPFÄNGER/E-Mail-EMPFÄNGER VERWALTEN) (4).

9.4.10.1.2 Filter einrichten

Für den E-Mail-Versand können Filter definiert werden, mit denen Inhalte einer Nachricht, für bestimmte Empfänger präzisiert werden können. Öffnen Sie hierzu die Option FILTER.

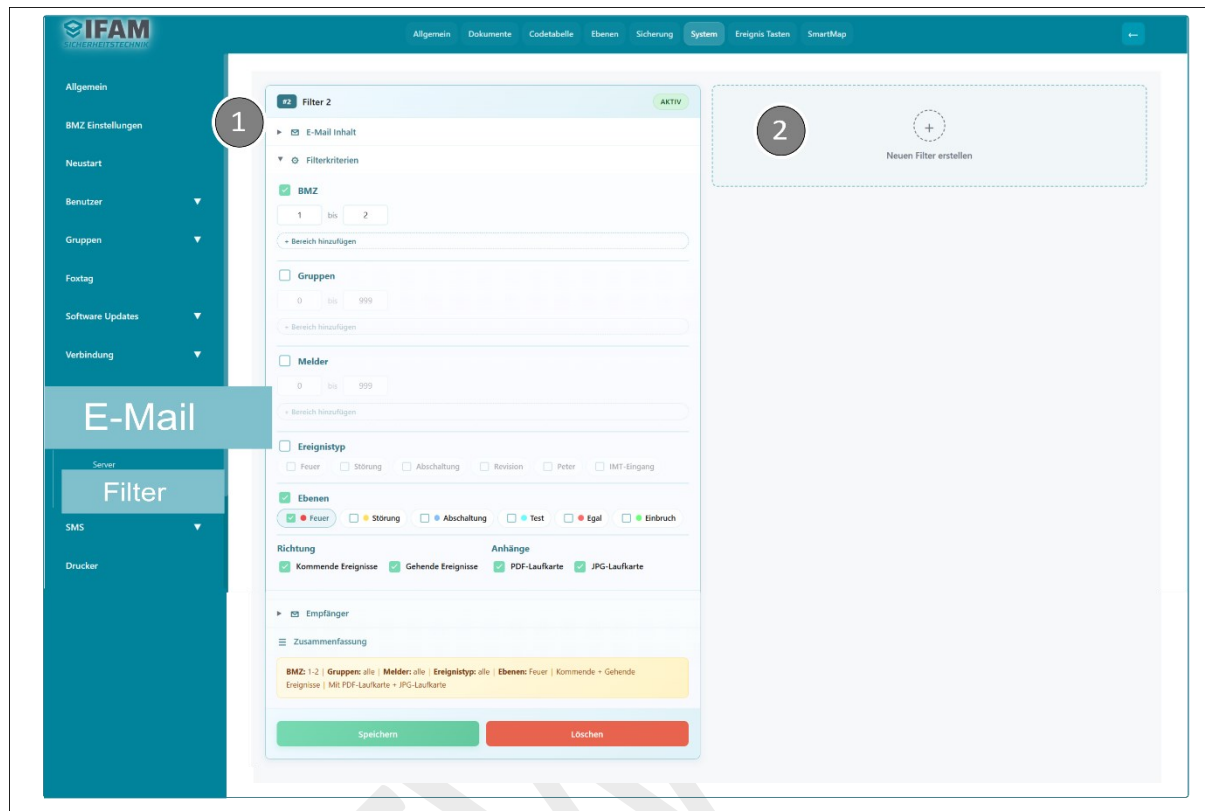


Abbildung 106: IRAS-Website – E-Mail/Filter

Auf der Seite werden ggf. bereits vorhandene Filter angezeigt (1). Zum Hinzufügen eines neuen Filters klicken Sie auf NEUEN FILTER ERSTELLEN (2) (Die Position der Schaltfläche ist, in Abhängigkeit bereits vorhandener Filter, variabel am Ende der Seite positioniert). → Ein Dialogfeld zur Filter-Definition wird angezeigt (letzte Position).

Folgende Angaben können festgelegt werden:

- Betreff (Inhalt),
- Nachrichtentext,
- Filterkriterien,
- Empfänger.

Mit der Anwendung eines Filters kann definiert werden, für welche Ebenen, Ereignisse (gehend/kommend), Meldepunkte und Gefahrenmeldezentralen (GMZ) Nachrichten versendet und ob eine zugehörige Laufkarte beigefügt werden sollen.

Ein definierter Filter muss den vorgesehenen Empfängern (EMPFÄNGER/EMPFÄNGER ZUORDNEN) zugeordnet werden. Wählen Sie hierzu die gewünschten Empfänger aus der vorhandenen Liste, die im Rahmen der Option SERVER angelegt wurde.



- Sollen alle Ereignisse des IRAS-SECURE-Gefahrenmeldesystem per E-Mail versendet werden, müssen mindestens die Option Kommende Ereignisse und GEHENDE EREIGNISSE gesetzt sein.
- Nur aktive Filter (siehe Status-Anzeige: AKTIV) können angewendet werden. Speichern Sie den Filter nach Eingabe der Parameter.

9.4.10.2 SMS



Die SMS-Funktion ist auf der IRAS-Website bereits angelegt, jedoch nur in Verbindung mit der Erweiterungsoption *IRAS-SECURE-Mobile* nutzbar. Die Nutzungsinformationen finden Sie nach dem Erwerb in der zugehörigen Dokumentation.

9.4.10.3 Drucker



Die Drucker-Funktion ist auf der IRAS-Website bereits angelegt, jedoch nur in Verbindung mit der Erweiterungsoption *IRAS-SECURE-Drucker* nutzbar. Die Nutzungsinformationen finden Sie nach dem Erwerb in der zugehörigen Dokumentation.

9.4.10.4 App



Grundlegende Informationen zu Struktur und Bedienung der IRAS-APP finden Sie in  [Kapitel 9.6 IRAS-APP](#).

9.4.11 Bedienungsoptionen

4. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zum Setup-Bereich wird geöffnet.
5. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche ALLGEMEIN.
6. Wählen Sie unter OPTIONEN den Eintrag BEDIENUNG.

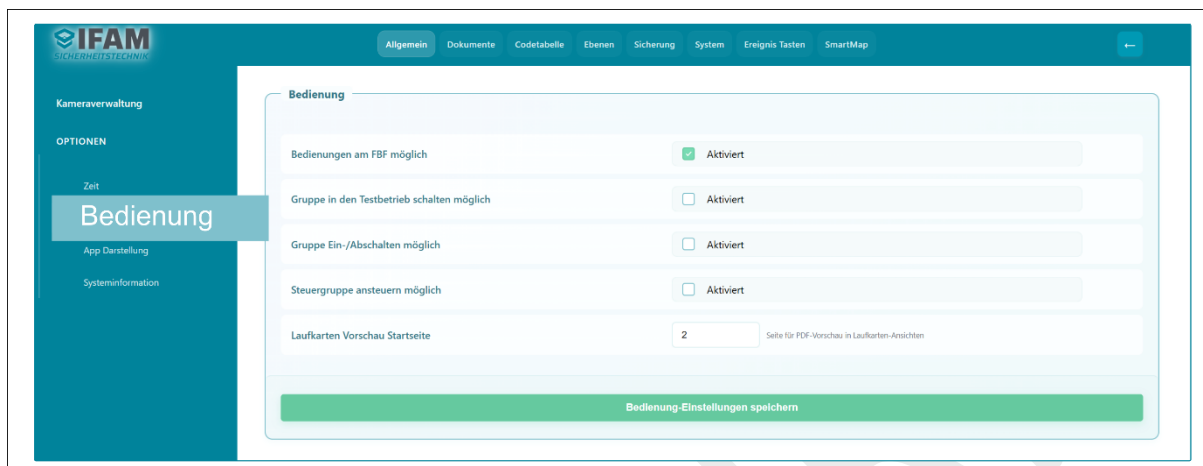


Abbildung 107: IRAS-Website – Optionen/Bedienung

9.4.11.1 Bedienung am FBF möglich

Mit der Aktivierung dieser Option werden im Browser und der App der Menüpunkt Bedienung/FBF möglich.

9.4.11.2 Gruppe in den Testbetrieb schalten möglich

Die Bedienung GRUPPEN IN DEN TESTBETRIEB SCHALTEN wird aktiviert/anwendbar.

9.4.11.3 Gruppen Ein-/Abschalten möglich

Die Funktion *Abschaltung von Gruppen* wird in der App freigegeben.

9.4.11.4 Steuergruppen ansteuern möglich

Wenn die Zentrale eine Ansteuerung der Steuergruppen ermöglicht, kann mit dieser Option die Bedienung freigegeben werden.

9.4.12 Erweiterungsfunktionen

IRAS-Secure kann um zahlreiche Funktionen erweitert werden.

👉 [Siehe Kapitel 4.7 Systemerweiterungen.](#)

Einige Optionen sind im Rahmen der IRAS-Website bereits angelegt, können jedoch erst nach einer gesonderten Freischaltung genutzt werden.

Dies sind:

- IRAS-SECURE-Betriebsbuch,
- IRAS-SECURE-SmartMap.
- IRAS-SECURE-Ereignistasten.



Hinweise zu Konfiguration und Bedienung finden Sie in der [Erweiterungs-spezifischen Betriebs-/Installationsanleitung](#).

9.5 Anwendung (Ereignisfall)

9.5.1 IRAS-Website – Anmeldung

Der Nutzer muss sich mit Nutzernamen und dem zugehörigen Passwort anmelden.

➞ *Siehe Kapitel 9.3.1 Anmeldung.*

Nach erfolgreicher Anmeldung erscheint das DASHBOARD.

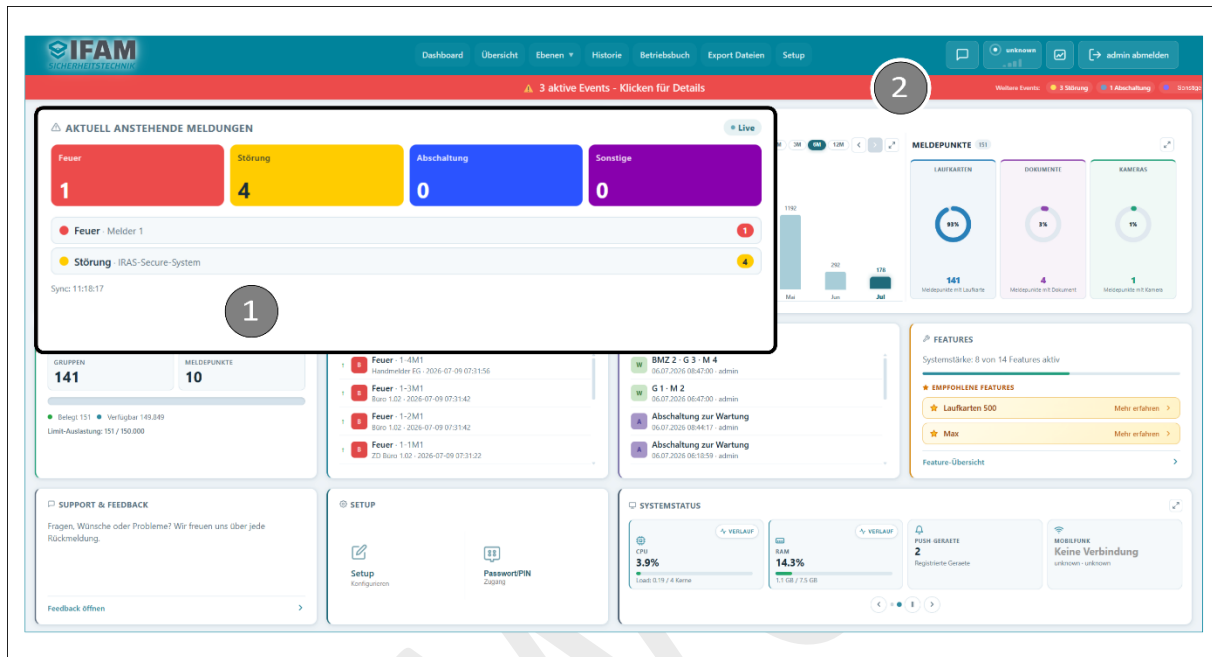


Abbildung 108: IRAS-Website – Dashboard/Ereignisfall (Beispiel)

Pos	Beschreibung
1	<u>Aktuell anstehende Meldungen</u> : aktuelle Meldungen
2	<u>Statuszeile</u> – Ereignis-Status

9.5.2 Ereignis-Meldungen

Werden Meldungen von der Gefahrenmeldezentrale (GMZ) gesendet, für die ein Eintrag in der Codetabelle existiert und für die ein Objekt eingetragen wurde, werden diese Meldungen in der Ansicht automatisch dargestellt. Diese automatische Aktualisierung (Live-Mode) wird beim ersten Aufruf der Webseitenansicht bzw. 30 Sekunden nach einer Bedienung aktiviert. Neu einlaufende Meldungen oder auch gehende Ereignisse werden automatisch berücksichtigt.

Die Status-Zeile (Abbildung 108/2) zeigt das Vorliegen/Nicht-Vorliegen von Ereignis-Meldungen an:

Status-Zeile	Erklärung
GRÜN (Abb. 114)	Es liegen keine Meldungen vor.
ROT/GELB/BLAU (Abb. 115)	Es liegen Meldungen für eine der definierten Ebenen vor. Liegen Meldungen für mehrere Ebenen vor, zeigt die Statuszeile die Anzahl der Ereignisse der jeweiligen Ebenen an. Die jeweils aktuelle Anzeige der Ebenen erfolgt <u>absteigend nach Maßgabe der definierten Priorität</u> : z.B. (1.) Feuer 2.) Störung 3.) Abschaltung 4.) Sonstige.

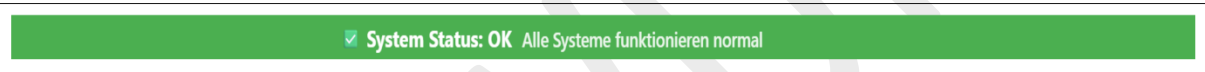


Abbildung 109: IRAS-Website – Dashboard/Statuszeile, keine Meldung

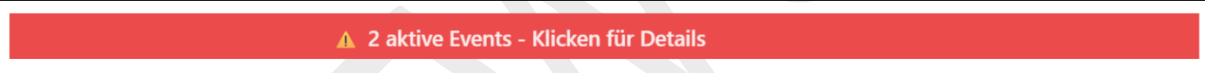


Abbildung 110: IRAS-Website – Dashboard/Statuszeile, vorliegende Meldungen (Beispiel)

Durch einfachen Klick auf die STATUSZEILE oder die Meldungsebene im Funktionsfeld ANSTEHENDE MELDUNGEN (Abbildung 108), gelangt der Nutzer zu einer Übersicht der Ereignis-Meldungen der jeweiligen Ebene (Abbildung 111).

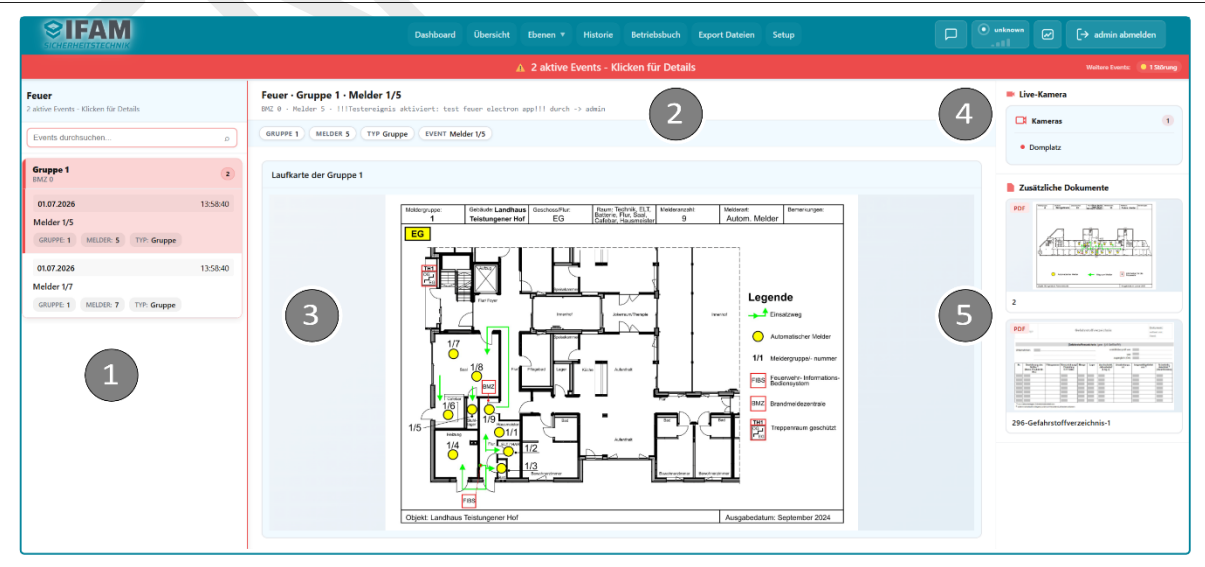


Abbildung 111: IRAS-Website – aktuelle Ereignisse/Ebene Feuer (Beispiel)

Durch Auswahl einer vorliegenden Meldung (1) werden in einer Übersicht Informationen zur Lokalisierung des Ereignisses (2) und die hierfür zur Verfügung stehenden Informationsmedien angezeigt: Laufkarte (3), zusätzliche Dokumente (5) und Kameras (4).

Mit der Auswahl der einzelnen Medien werden die entsprechenden Inhalte in einem separaten Fenster angezeigt.

Laufkarten können exportiert werden (Druck, Speichern). Ein Druck ist nur möglich, wenn ein Drucker am lokalen PC angeschlossen ist.

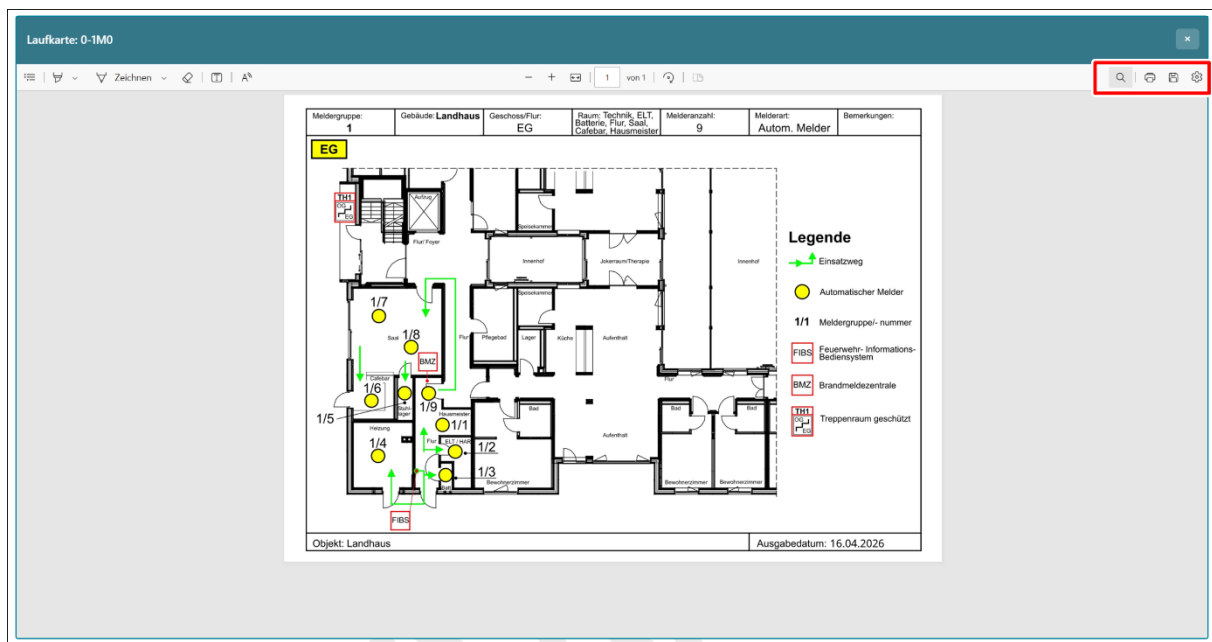


Abbildung 112: IRAS-Website – Ereignismeldung/Laufkarte

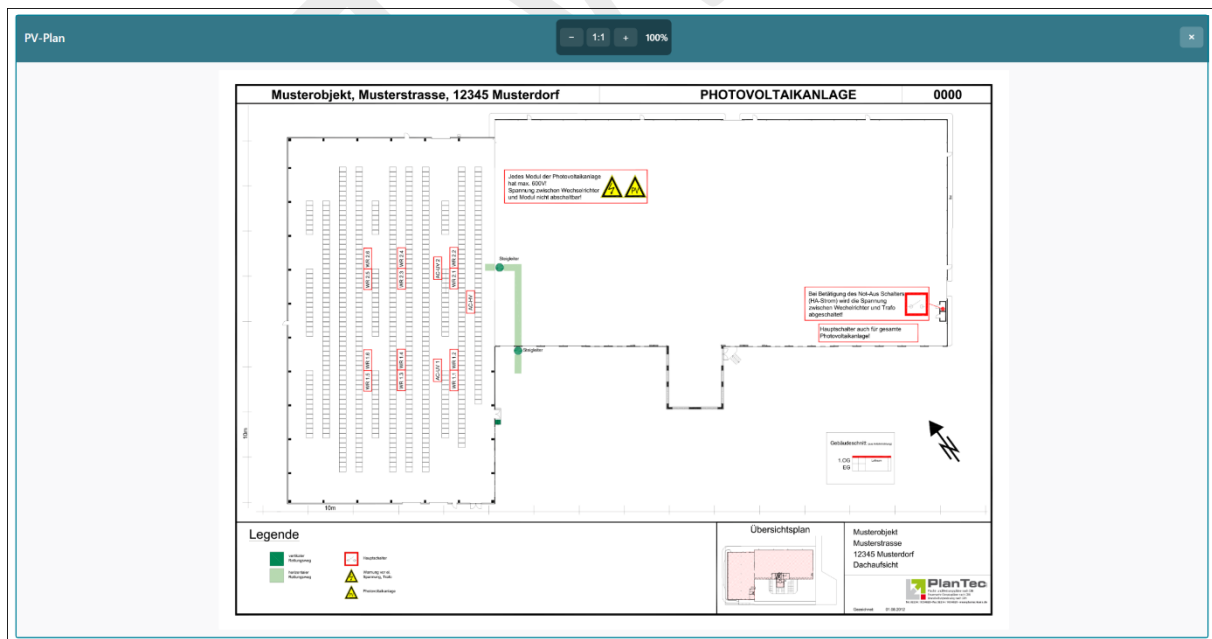


Abbildung 113: IRAS-Website – Ereignismeldung/zusätzliches Dokument

Kameras: Aus dem Anzeigemodus EINZELANSICHT kann eine Übersichtsdarstellung aller für den jeweiligen Meldungspunkt vorhandenen Kameras gewechselt werden (Abbildung 114).

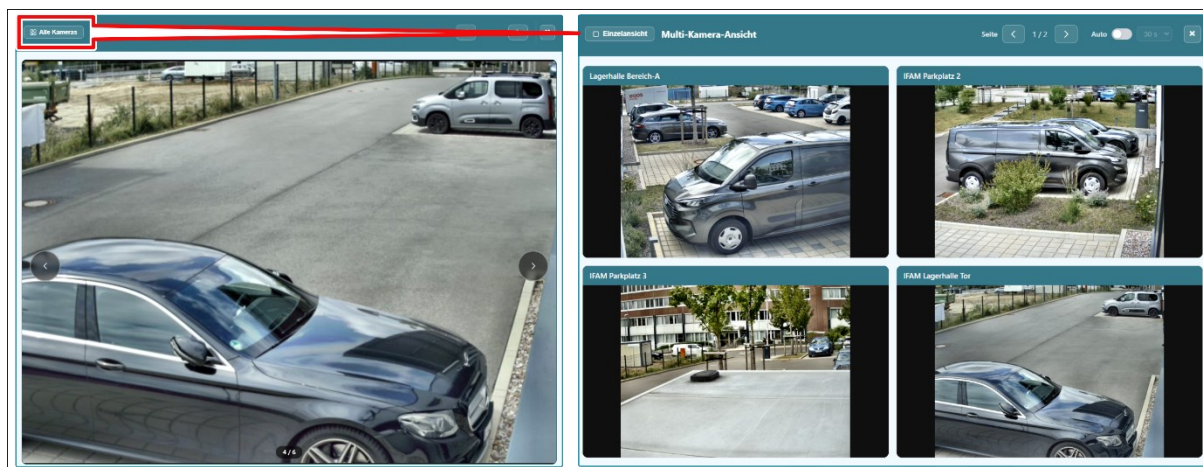


Abbildung 114: IRAS-Website – Ereignismeldung/Kamera

9.5.3 IRAS-App

Mit der IRAS-App können vorliegende Meldungen angezeigt werden. Die Struktur und Darstellung folgen grundsätzlich den Modi der IRAS-Website.

➡ Grundlegende Informationen zur Anwendung der IRAS-APP finden Sie in [Kapitel 9.6 IRAS-APP](#).

9.5.4 E-Mail

Wurde die Übertragungsoption E-MAIL während der Systemeinrichtung konfiguriert, können vorliegende Meldungen des IRAS-SECURE-Gefahrenmeldesystems auf diesem Wege an ausgewählte Empfänger übermittelt und abgerufen werden.

➡ *Zur Einrichtung dieser Option siehe Kapitel 9.4.10.1 E-Mail.*

9.5.5 Optionale Systemerweiterungen



Informationen zur Übermittlung und Bereitstellung von Informationen/Meldungen über mögliche optionale Erweiterungen, finden Sie in den jeweiligen optionsspezifischen Dokumenten.

9.6 IRAS-APP

Die IRAS-App ist eine standardmäßig bereitgestellte Option zur Übermittlung von Meldungen des IRAS-SECURE-Gefahrenmeldesystems.

Sie kann auf einem Smartphone, Tablet oder PC betrieben werden.

9.6.1 Aktivierung von Darstellungsoptionen

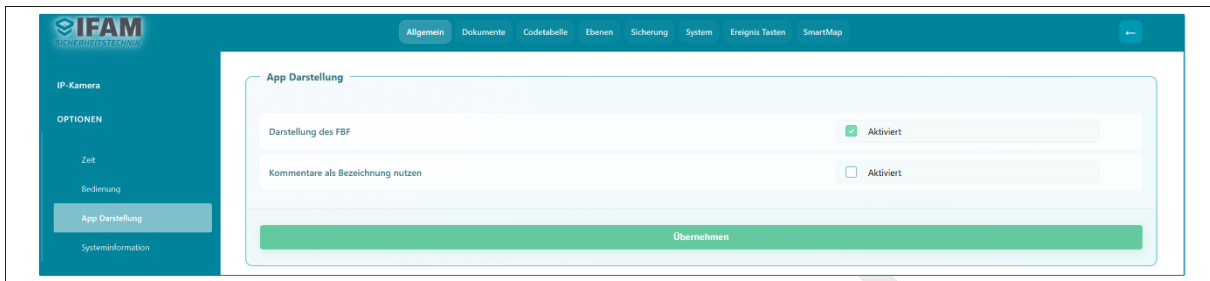


Abbildung 115: IRAS-Website – IRAS-APP

Vor der Nutzung können spezielle Darstellungsoptionen auf der IRAS-Website aktiviert werden (Abbildung 115).

1. Wählen Sie in der MENÜZEILE den Eintrag SETUP. → Der SETUP-BEREICH wird geöffnet.
2. Wählen Sie in der Menüzeile den Eintrag ALLGEMEIN.
3. Wählen Sie unter Optionen den Eintrag APP-DARSTELLUNG.
4. Aktivieren Sie die gewünschte Darstellungsoption: DARSTELLUNG DES FBF und/oder KOMMENTARE ALS BEZEICHNUNGEN NUTZEN. Übernehmen Sie die Einstellungen.

9.6.2 Bedieneinstellungen

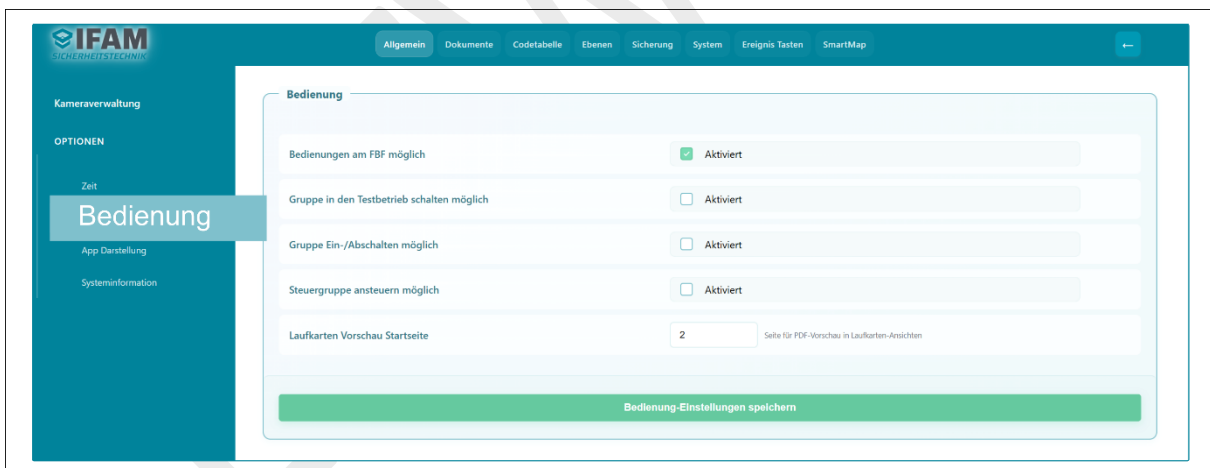


Abbildung 116: IRAS-Website – Bedienung/Einstellungen

9.6.3 Push-Nachrichten

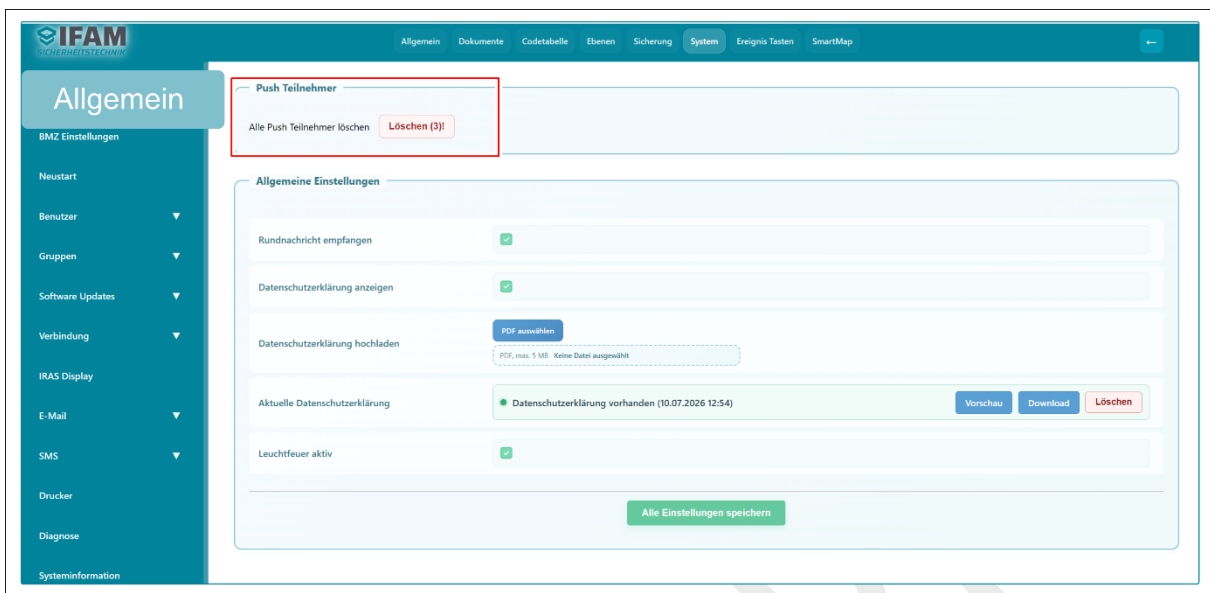


Abbildung 117: IRAS-Website - Push-Nachrichten

9.6.4 Betrieb (Anwender)

Nach dem Start der App erscheint der STARTBILDSCHIRM. Wählen Sie den Modus FEUERWEHR. → Die Übersicht über vorhandene/überwachte Objekte wird angezeigt (Abbildung 119).

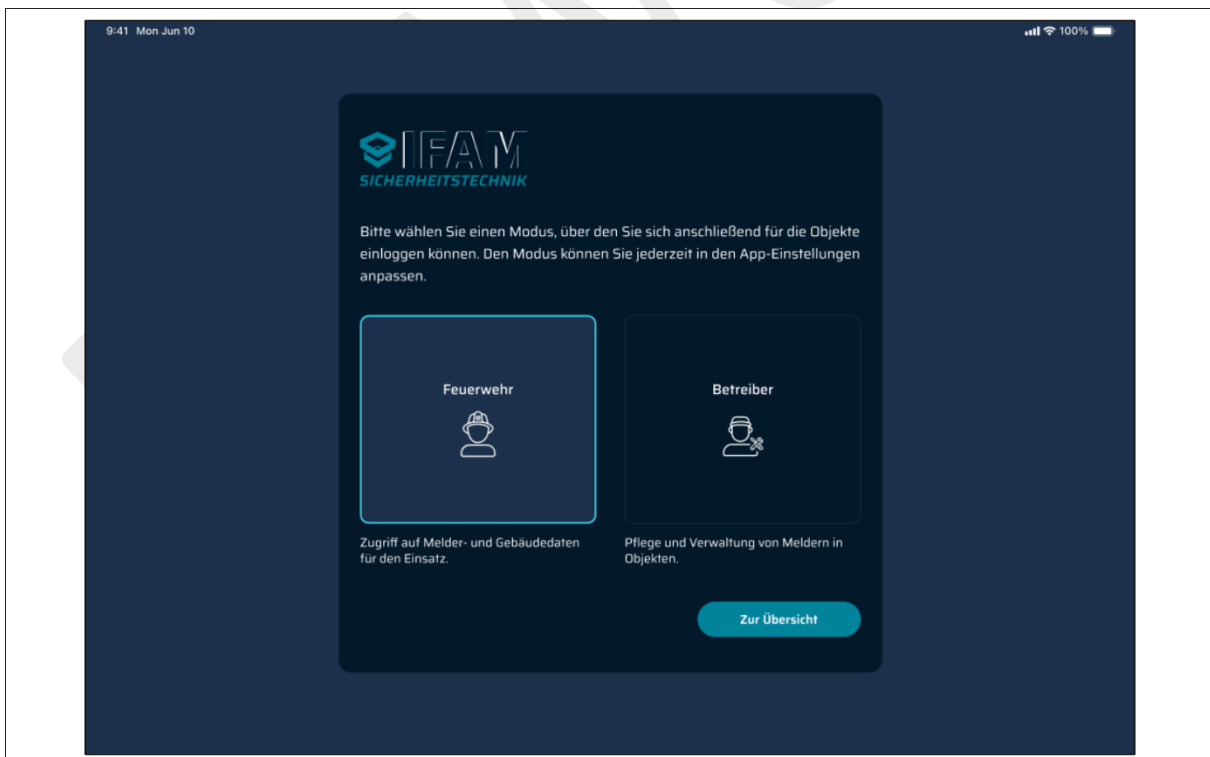


Abbildung 118: IRAS-APP – Startbildschirm

9.6.4.1 Objektübersicht

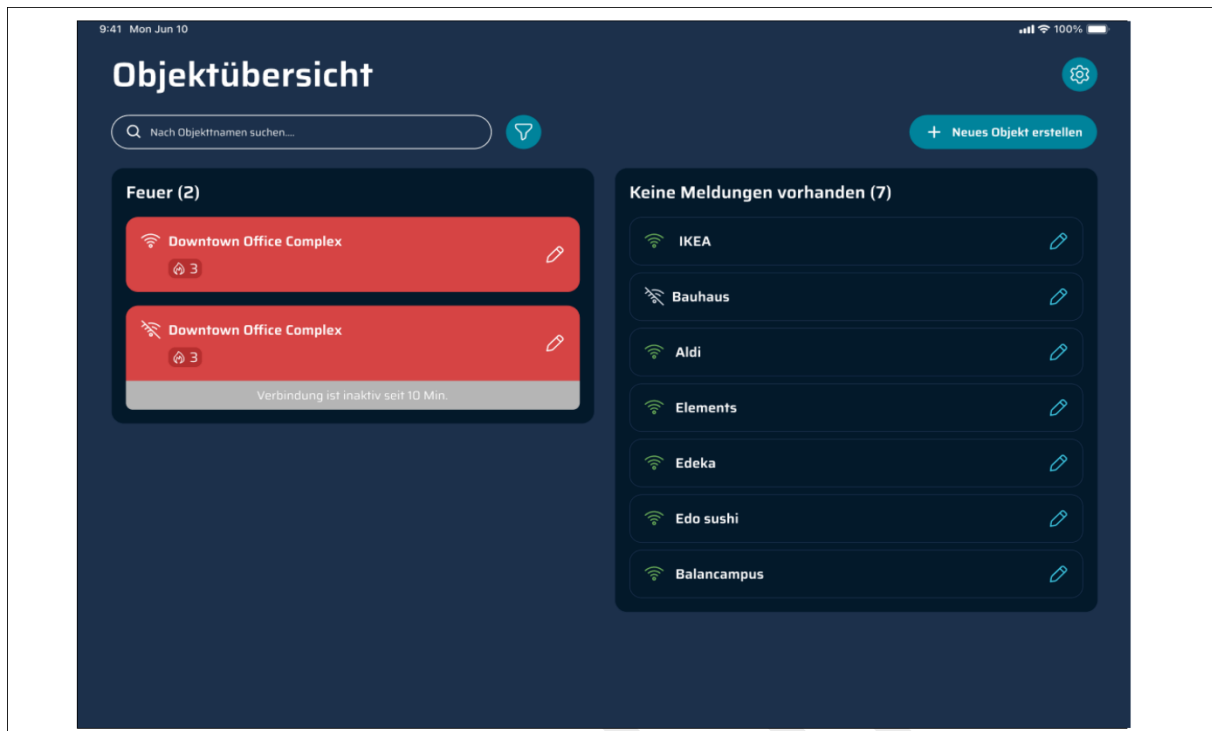


Abbildung 119: IRAS-APP – Objektübersicht

In der OBJEKTÜBERSICHT werden auf der **linken Seite** aktuelle Ereignismeldungen angezeigt (1). Die Darstellung folgt den grundsätzlichen Regeln der IRAS-Website (Kategorisierung, farbliche Kennzeichnung, Prioritäten). Durch Auswahl einer Einzelmeldung werden Informationen zum jeweiligen Ereignis angezeigt. Der Zugang zu den jeweiligen Ereignismeldungen der Objekte ist durch ein Passwort gesichert!

Die **rechte Seite** enthält eine Übersicht der Objekte, für die keine aktuellen Meldungen vorliegen (2).

9.6.4.2 Neues Objekt hinzufügen

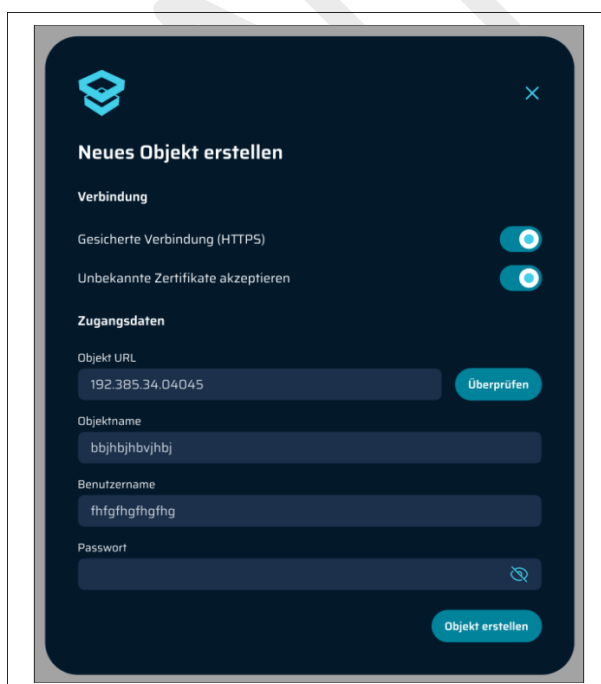


Abbildung 120: IRAS-APP – neues Objekt erstellen

Durch die Wahl der Schaltfläche NEUES OBJEKT ERSTELLEN in der OBJEKTÜBERSICHT (Abbildung 119/3) können neue Objekte, für die Meldungen übermittelt und angezeigt werden sollen, hinzugefügt werden.

Geben Sie die notwendigen Verbindungsoptionen und Zugangsdaten ein.

9.6.4.3 Objektstatus einsehen

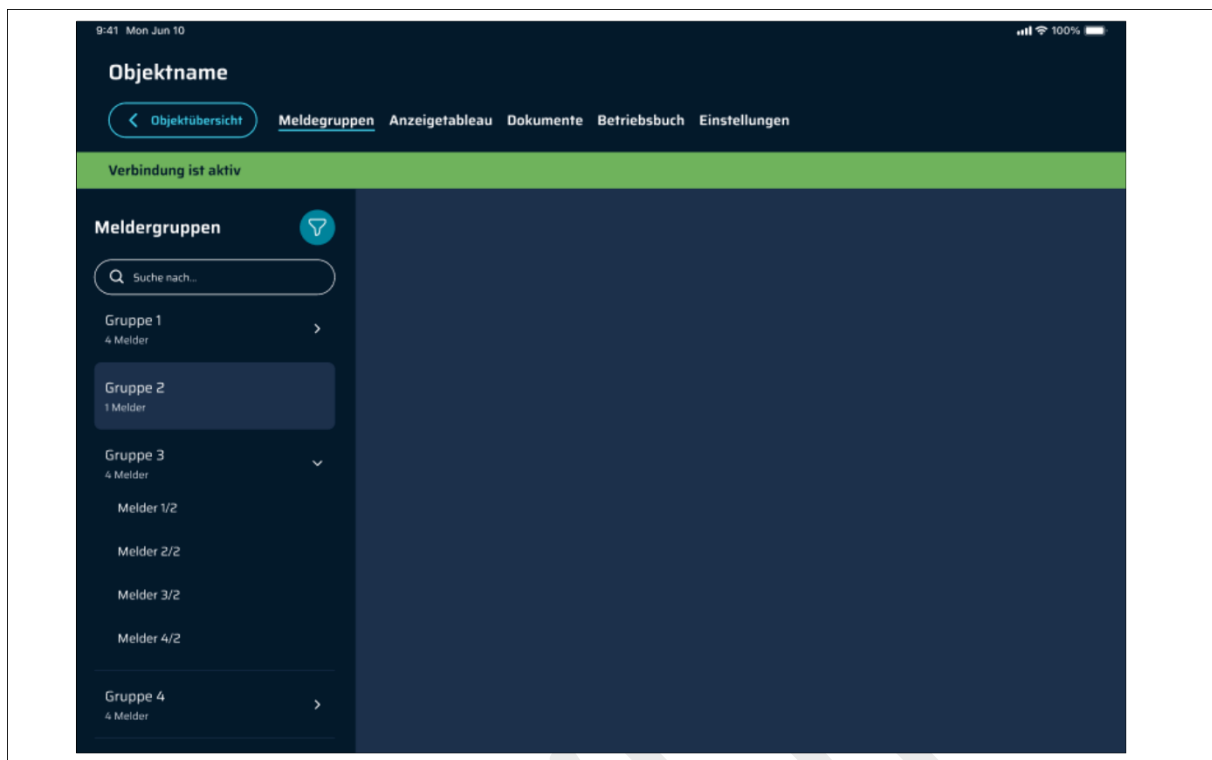


Abbildung 121: IRAS-APP – Objektstatus/keine Meldungen (Beispiel)

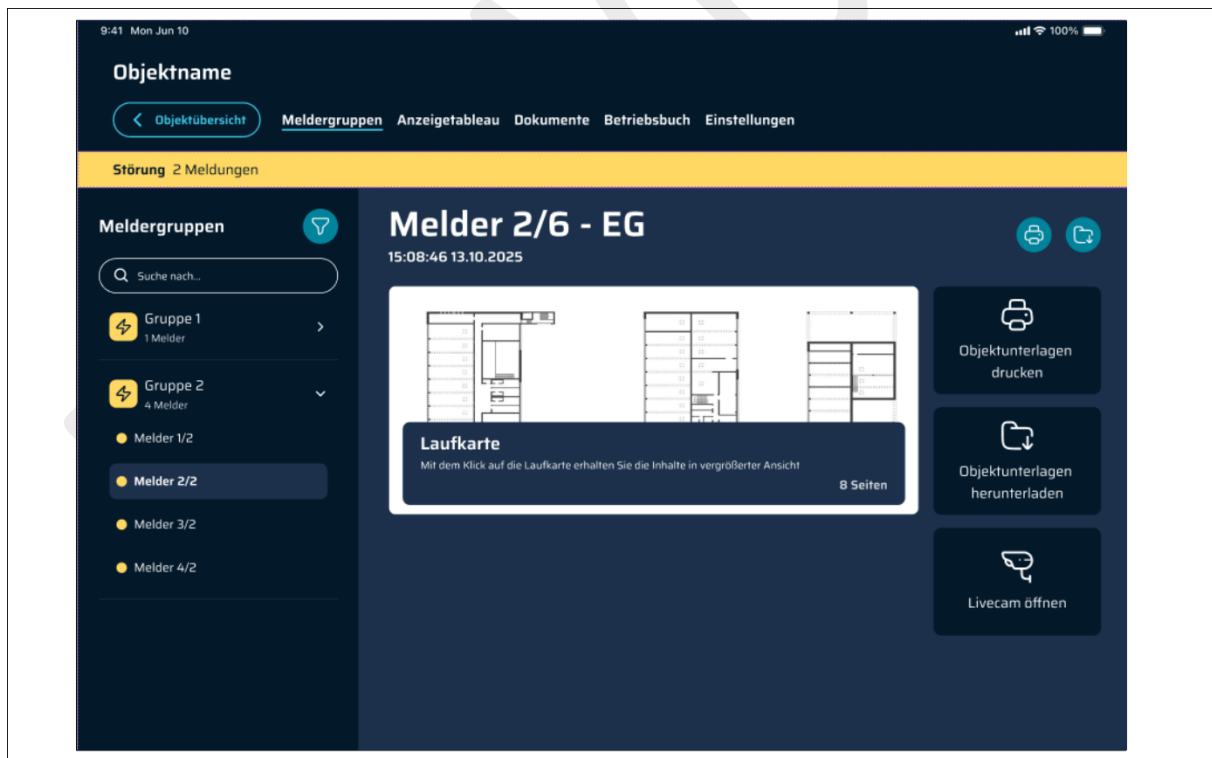


Abbildung 122: IRAS-APP – Objektstatus/vorliegende Meldungen – Ebene „Störung“ (Beispiel)

Nach Auswahl eines Objektes in der Objektübersicht, werden die ihm zugeordneten Meldergruppen und zugehörige Melder in einer Übersicht angezeigt (1).

In einer Statuszeile (2) wird das Vorliegen/Nicht-Vorliegen von Ereignismeldungen dargestellt.

Status-Zeile	Erklärung
GRÜN (Abbildung 121)	Es liegen keine Meldungen vor. Anzeige des Verbindungsstatus' (aktiv/inaktiv).
ROT/GELB/BLAU* (Abbildung 122)	* Die Darstellung folgt den auf der IRAS-Website festgelegten Option. Es liegen Meldungen für eine der definierten Ebenen vor. Liegen Meldungen für mehrere Ebenen vor, zeigt die Statuszeile die Anzahl der Ereignisse der jeweiligen Ebenen an. Die jeweils aktuelle Anzeige der Ebenen erfolgt <u>absteigend nach Maßgabe der definierten Priorität</u> : z.B. (1.) Feuer 2.) Störung 3.) Abschaltung 4.) Sonstige.

Durch Auswahl einer Meldergruppe/eines Melders mit vorliegenden Ereignismeldungen wird die jeweils zugeordnete Laufkarte/weitere Objektunterlagen angezeigt (3). Vorhandene Objektunterlagen können gespeichert und ausgedruckt (4) werden.

Darüber hinaus können die dem Objekt zugeordneten Kameras (5) eingesehen werden. Hierbei gelten die gleichen Ansichtsmodi wie auf der IRAS-Website: 1.) Einzelkamera und 2.) Multikamera-Ansicht.

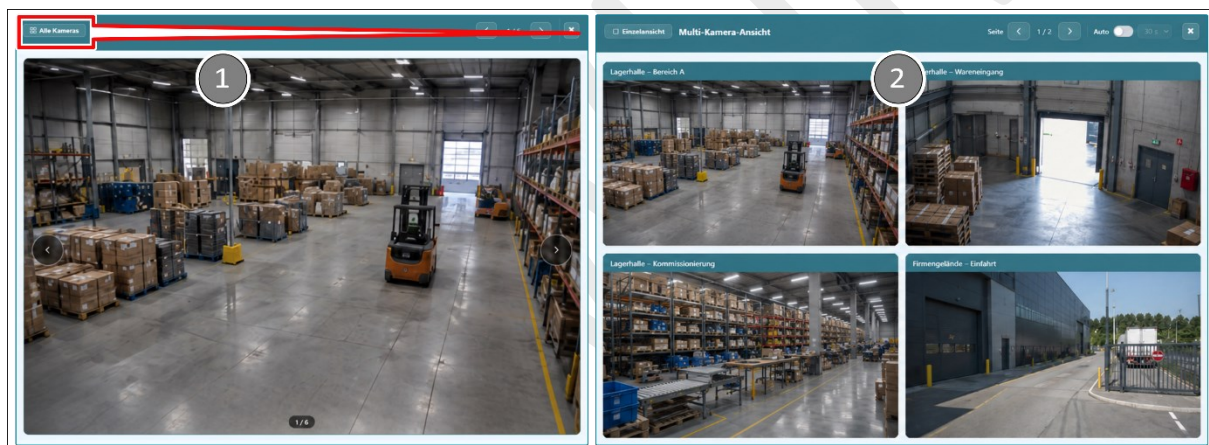


Abbildung 123: IRAS-APP – Kameras (Beispiel)

9.7 Backup und Wiederherstellung

IRAS-SECURE bietet dem Nutzer die Möglichkeit, ein vollständiges Backup aller Projekte und Dateien des Gefahrenmeldesystems vorzunehmen.

Zur Ausführung dieser Funktion muss der jeweilige Nutzer das Lese-/Schreibrecht BACKUP & SYNCHRONISATION besitzen und eine 2-Faktor-Authentifizierung (TOTP) eingerichtet sein.

➔ [Siehe Kapitel 9.4.7 Benutzer verwalten](#) und [9.3.3.2 Zwei-Faktor-Authentifizierung einrichten](#).

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zum Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SICHERUNG.
→ Die Benutzeroberfläche zur Sicherung und Wiederherstellung der System-Konfiguration von IRAS-SECURE wird geöffnet.

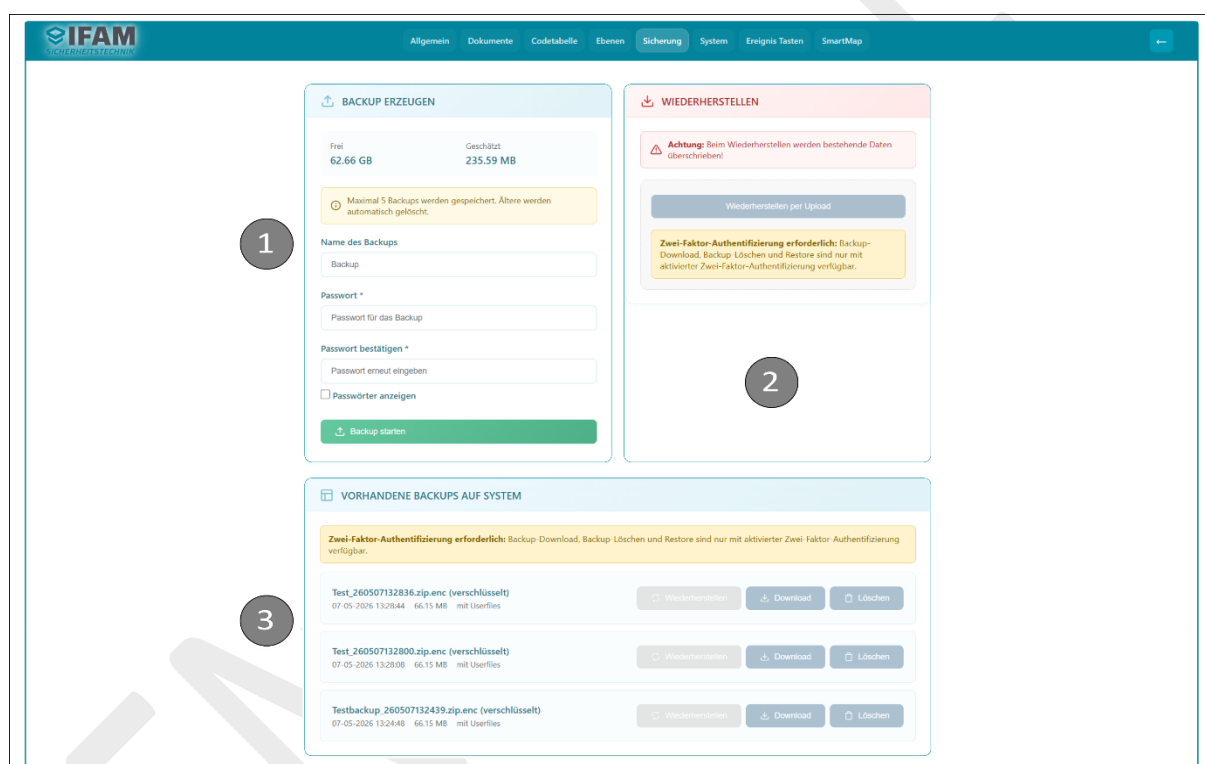


Abbildung 124: IRAS-Website – Sicherung

Sie haben hier die Möglichkeit, 1.) ein **Backup zu erzeugen** und 2.) die **Konfiguration** des IRAS-SECURE-Gefahrenmeldesystems **wiederherzustellen**.

9.7.1 Backup erzeugen

Für die Erstellung eines Backups (1) müssen ein Backup-Name zur eindeutigen Zuordnung und ein Passwort vergeben werden, um sicherzustellen, dass die Wiederherstellung des Systems mit der jeweiligen Sicherung nur von dazu berechtigten Personen ausgeführt werden kann.



Beachten Sie, dass maximal **5 Backups** gleichzeitig im System gespeichert werden können. Wird nach Erreichen dieser Grenze ein weiteres Backup hinzugefügt, wird die jeweils älteste Sicherung automatisch gelöscht. Speichern Sie daher ggf. vor dem Anlegen eines Backups die älteste Version separat ab (Übersicht (3) → DOWNLOAD).

Die neu erstellte Sicherung wird der Übersicht vorhandener Backups **(3)** hinzugefügt. Hier haben Sie auch die Möglichkeit, eine vorhandene Sicherung zu löschen.

9.7.2 System wiederherstellen

Die Wiederherstellung/Zurücksetzen des Systems kann auf zwei verschiedene Arten erfolgen.



Beachten Sie: Wird das Gefahrenmeldesystem mit einem Backup wiederhergestellt, werden alle zu diesem Zeitpunkt vorhandenen Dateien/Konfigurationen überschrieben!

9.7.2.1 Vorhandene Backups

Die Wiederherstellung des Gefahrenmeldesystems kann über ein im System gespeichertes Backup erfolgen.

Wählen Sie hierzu im Feld VORHANDENE BACKUPS AUF SYSTEM **(3)** die gewünschte Version und starten Sie den Vorgang durch Betätigen des Buttons WIEDERHERSTELLEN. Folgen Sie den Anweisungen.

9.7.2.2 Upload (Datei)

Das Wiederherstellen des Gefahrenmeldesystems kann auch über den Upload einer auf einem externen Medium gespeicherten Backup-Datei erfolgen **(2)**. Betätigen Sie die Schaltfläche WIEDERHERSTELLEN PER UPLOAD.

Wählen Sie hierzu die gewünschte Version aus der Übersicht. Folgen Sie den Anweisungen.

9.8 Software-Update

Software-Updates können im gleichnamigen Bereich konfiguriert/vorgenommen werden.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zum Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SYSTEM.
→ Die Benutzeroberfläche zur System-Konfiguration wird geöffnet.
3. Wählen Sie die Option SOFTWARE-UPDATES.

9.8.1 Einstellungen

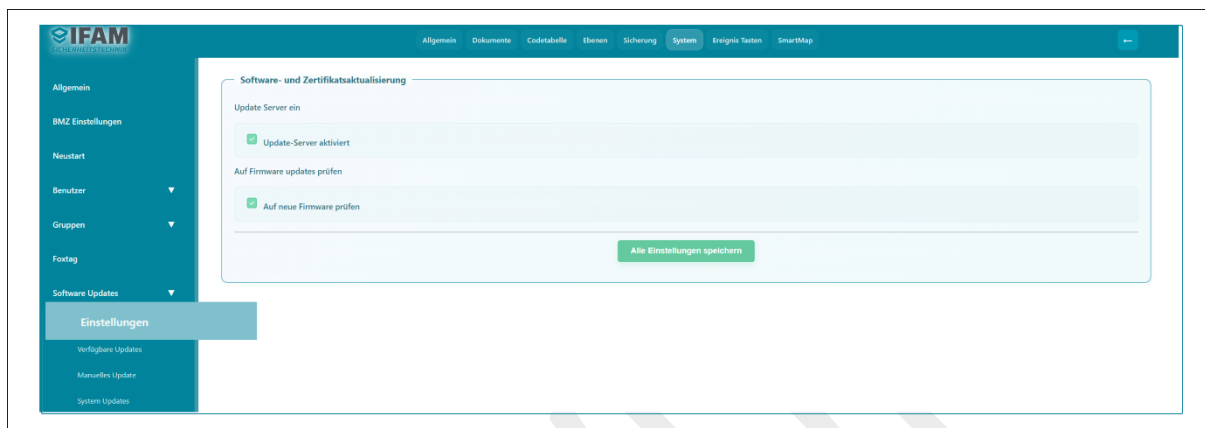


Abbildung 125: IRAS-Website – Update/Einstellungen

Folgende automatische Aktualisierungsoptionen können aktiviert werden:

- UPDATE-SERVER AKTIVIEREN: ...
- AUF NEUE FIRMWARE PRÜFEN: IRAS-SECURE prüft in regelmäßigen Intervallen/beim Start auf neue Firmware-Versionen.

9.8.2 Verfügbare Updates

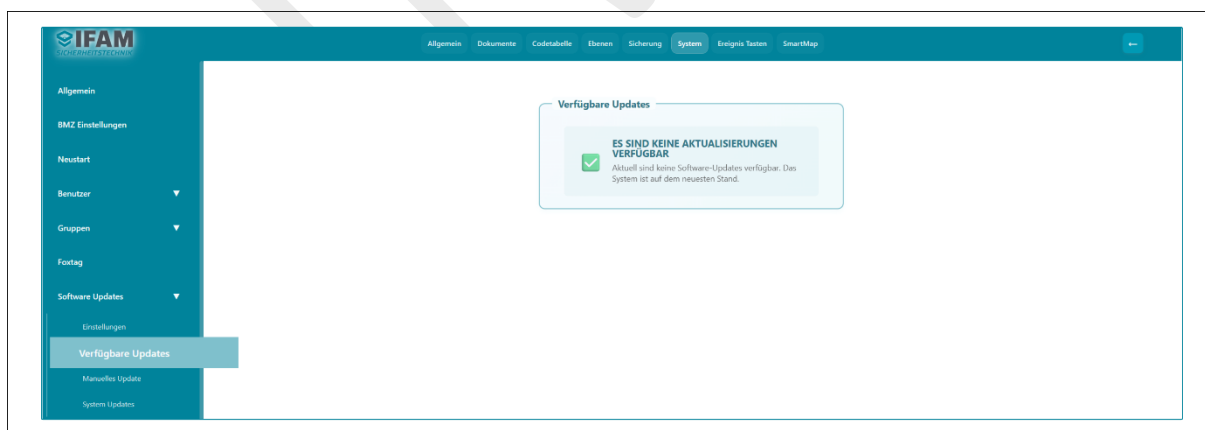


Abbildung 126: IRAS-Website – Verfügbare Updates

Wurden die Optionen zur automatischen Prüfung aktiviert, werden hier ggf. vorhandenen Updates angezeigt.

Wählen Sie entsprechende Aktualisierungen und starten Sie den Vorgang.

...

9.8.3 Manuelles Update

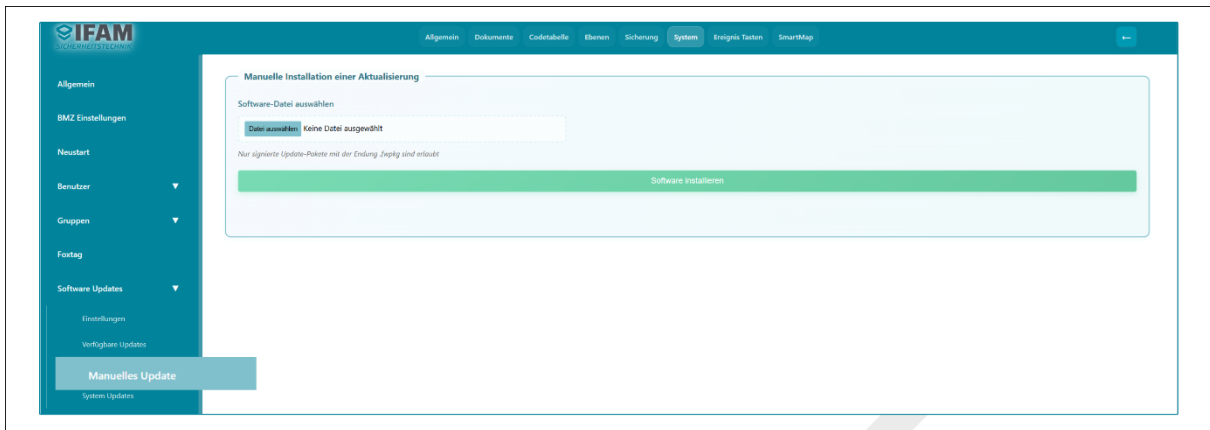


Abbildung 127: IRAS-Website – Manuelles Update

Software-Aktualisierung können, bei vorhandenen Update-Dateien/-Paketen auch manuell vorgenommen werden.

1. Aktivieren Sie die Schaltfläche DATEI AUSWÄHLEN. → Ein Dialog-Feld zur Auswahl der Updatequelle wird geöffnet.
2. Wählen Sie die gewünschten Dateien aus. → Die ausgewählten Dateien werden angezeigt.
Beachten Sie, dass nur signierte Update-Pakete mit der Endung *.fwpkg akzeptiert werden!
3. Aktualisieren Sie das System (PAKET HOCHLADEN/SOFTWARE INSTALLIEREN).

9.8.4 System-Updates

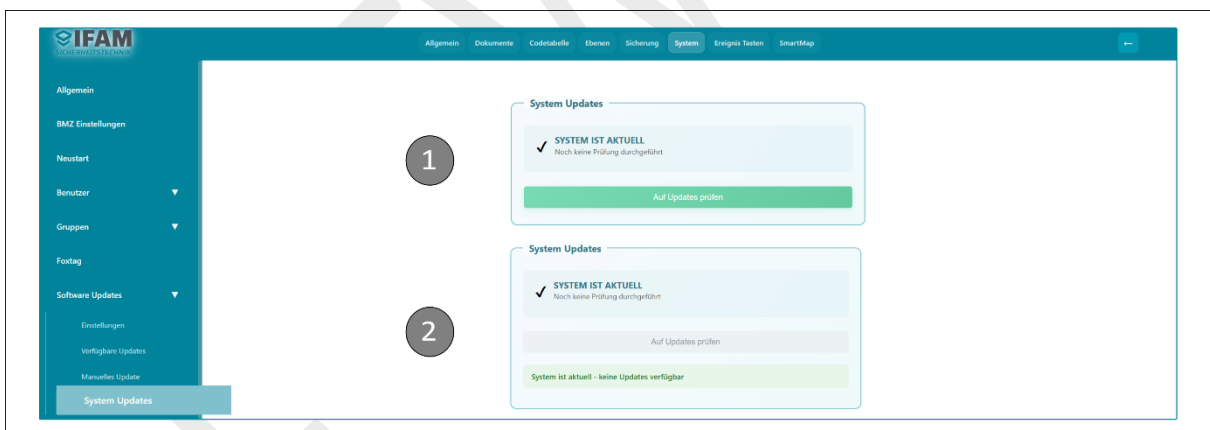


Abbildung 128: IRAS-Website – System-Updates manuell prüfen (Beispiel)

Neben der automatischen Prüfung können Sie auch manuell auf System-Updates prüfen. Aktivieren Sie die Schaltfläche AUF UPDATES PRÜFEN (1). → IRAS-SECURE prüft auf notwendige/vorhandene Aktualisierungen und zeigt das entsprechende Ergebnis an (2) (hier: System auf dem neuesten Stand/aktuell).

9.9 Systeminformation

In der Kategorie SYSTEMINFORMATION können Informationen zum System und Kontaktdaten für Zuständigkeiten hinterlegt werden (Erreichter, Betreiber, Wartung).

1. Wählen Sie auf dem in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zur Systemverwaltung wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche Allgemein.
3. Wählen Sie die Option SYSTEMINFORMATION.

The screenshot displays the IFAM SYSTEMINFORMATION web interface. The top navigation bar includes tabs: Allgemein, Dokumente, Codetabelle, Ebenen, Sicherung, System, Ereignis-Tasten, and SmartMap. The left sidebar lists options: IP-Kamera, OPTIONEN, Wartungsdokument erstellen, Zeit, Bedienung, App Darstellung, and Systeminformation (highlighted). The main content area is divided into six sections:

- Betreiber:** Fields for Straße (Gustav-Weißkopf-Strasse), Stadt (Erfurt), Hausnummer (9), Postleitzahl (99092), Telefonnummer (0361659110), Ansprechpartner (Ursula Mustermann), E-Mail (Info@ifam-erfurt.de), and Firmenname (IFAM GmbH).
- Errichter:** Fields for Straße, Stadt, Hausnummer (5), Postleitzahl, Telefonnummer, Ansprechpartner, E-Mail, and Firmenname.
- System:** Fields for Objektname (Edo Sudhi), Zentralen Typ (FlexEs), Zentralen Version (v1.8.462), Inbetriebnahme (30.02.2024), Abmeldung Alarm bei, Hauptmelderpasswort, Hauptmeldernummer, and Überbrückungszeit bei Netzausfall.
- Wartungsunternehmen:** Fields for Straße (3) and a second empty field.
- Notizen:** A text area containing the text "test 1 2 3".
- Übernehmen:** A green button labeled "Übernehmen".

Abbildung 129: IRAS-Website – Systeminformationen

10 Störungen/Störungsbeseitigung

Das IRAS-SECURE-Gefahrenmeldesystem stellt Software- als auch Hardware-seitig eine Vielzahl an Optionen zur Störungserkennung/-beseitigung zur Verfügung, die im Weiteren beschrieben werden.

Bei Vorliegen einer Störung, nutzen Sie bitte im ersten Schritt stets die nachfolgende Übersicht häufiger Störungen.

10.1 Störungstabelle (häufige Störungen)



Die in den als Reaktion auf Störungen vorgeschlagenen Gegenmaßnahmen enthaltenen Pfadangaben beziehen sich auf die IRAS-Website. Der Ausgangspunkt ist stets die Hauptseite (Dashboard), gefolgt von den Menüeinträgen/Optionen der nachfolgend präsentierten Unterseite.

Beispiel: **SETUP** (Dashboard) → **SYSTEM** → **VERBINDUNG** → **SSL**.

Störung	Ursache	Gegenmaßnahmen
Das IRAS-Gefahrenmeldesystem ist nicht über die Website oder per IRAS-App erreichbar.	Falsche IP-Adresse	Nutzen Sie einen IP-Scanner zum Ermitteln der korrekten IP-Adresse des IRAS-Gefahrenmeldesystem . Ggf. müssen Sie die IP-Adressen anpassen, so dass sich Ihr PC und das IRAS-SECURE-Gefahrenmeldesystem im selben Subnetz befinden. Achten Sie auch auf eine korrekte Subnetzmaske (Netzwerksegmentierung).
	PROXY-Server	Ein im Netzwerk befindlicher Proxy-Server tauscht nutzerspezifische Zertifikate aus und Unterschreibt diese. Vergleichen Sie die lokalen Zertifikate mit den extern gelieferten. Nutzen Sie externe Dienste zur Überprüfung ihrer Zertifikatskette.
	Das IRAS-SECURE-Gefahrenmeldesystem ist aus	Schalten Sie das IRAS-SECURE-Gefahrenmeldesystem ein und verbinden Sie die notwendigen Netzkabel.
		Prüfen Sie die Stromversorgung.
		Prüfen Sie vorhandene Sicherungen.
	HTTPS verwendet	Ändern Sie die URL im Browser von http:// zu https://. Nutzen Sie ggfs. ein „inkognito“ Fenster, damit Browservoreinstellungen gelöscht sind.
	Ungültige/abgelaufene Zertifikate	Fügen Sie bei Ihrem Browser eine Sicherheitsausnahme hinzu und loggen Sie sich mit Ihrem Passwort ein und entfernen Sie den Haken bei „SSL“ und „HTTPS Zertifikat

		verwenden“ unter <u>SETUP→SYSTEM→VERBINDUNG → SSL</u>
Das IRAS-SECURE-Gefahrenmeldesystem startet nicht.	Spannungsversorgung defekt	Überprüfen Sie die Verbindung des IRAS-SECURE-Gefahrenmeldesystem mit dem 230V-Netz und messen Sie ggf. die Spannung. Tauschen Sie das Kabel bei Bedarf aus. Entfernen Sie das Kabel und betreiben Sie das IRAS-SECURE-Gefahrenmeldesystem im Akku-Betrieb. Wenn die Spannung am PC unter 21 V liegt, wird das System sicherheitshalber deaktiviert.
	Akku defekt (bei Nutzung der Erweiterung IRAS-SECURE-USV).	Stecken Sie das Netzkabel ein und Betreiben Sie das IRAS-Gefahrenmeldesystem mit 230 V.
Die Website des IRAS-SECURE-Gefahrenmeldesystem ist leer und enthält keine Elemente.	Browser Cache	Der Browser hat ein altes Cookie gespeichert oder hat einen Cache welcher nicht mehr gültige Daten enthält. Schließen Sie den Browser oder löschen Sie den Cache.
	Updatefehler	Während eines Updates wurde die Spannungsversorgung unterbrochen. Nehmen Sie Kontakt mit dem Service der IFAM GmbH Erfurt auf.
Es kommen keine Push Benachrichtigungen bei Meldungen auf die Mobil Geräte.	Push Filter der Gruppe nicht richtig gesetzt.	Überprüfen Sie unter <u>SETUP →SYSTEM →BENUTZER</u> die Filtereinstellungen für Benachrichtigungen des jeweiligen Nutzers.
	Ausfall des Benachrichtigungsdienstes	Wie einige andere Funktionen auch, ist das IRAS-SECURE-Gefahrenmeldesystem für den Empfang von Benachrichtigungen auf Funktionen des mobilen Betriebssystems angewiesen. Wenn dieser Dienst ausfällt oder kurzfristige Wartungsarbeiten daran durchgeführt werden, kann es zu Störungen oder Verzögerungen bei der Benachrichtigung kommen.
	Push Server nicht erreichbar	Führen Sie die Selbstdiagnose unter <u>SETUP →SYSTEM→DIAGNOSE</u> durch. Wenn der Server nicht erreichbar ist, prüfen sie die Freigabe des Ports 443 und die URL: iras.ifam.com
	Kein mobiles Gerät hat sich bei dem IRAS-	Geben Sie die korrekte Adresse, Benutzername und Passwort in der App ein und speichern Sie diese

	Gefahrenmeldesystem für Push-Nachrichten registriert.	Konfiguration. Dadurch registriert sich dieses Mobile Gerät automatisch bei dem IRAS-Gefahrenmeldesystem für Push-Nachrichten.
Es kommen keine E-Mail-Benachrichtigung bei vorliegenden Meldungen	E-Mail-Filter nicht korrekt eingestellt	Prüfen Sie die Einstellungen der E-Mail-Filter unter <u>SETUP → SYSTEM → E-MAIL</u> , dass das betreffende Objekt benachrichtigt wird. Prüfen Sie die E-Mail-Adressen der Empfänger. Schließen Sie Tippfehler aus. Nutzen Sie die Test-E-Mail um Ihre Einstellungen zu prüfen.
	Provider nutzt APP-ID	Das IRAS-SECURE-Gefahrenmeldesystem bietet aktuell keine Unterstützung für eine APP-ID. Nehmen Sie Kontakt mit Ihrem Anbieter auf um eine Klärung zu erreichen.
	Provider erwartet Zwei-Faktor-Authentifizierung	Das IRAS-SECURE-Gefahrenmeldesystem bietet aktuell keine Unterstützung für eine Zwei-Faktor-Authentifizierung. Nehmen Sie Kontakt mit Ihrem Anbieter auf um eine Klärung zu erreichen. Nutzen Sie App-Passwörter. Diese ermöglichen einen Zugriff mit speziellen Zugangsdaten (google).
	Provider hat Client gesperrt	Es kann vorkommen das der Anbieter, unter bestimmten Voraussetzungen, den E-Mail-Client des IRAS-Gefahrenmeldesystem sperrt (zu viele Emails, Zugriffe unterschiedlicher IPs, usw.). Nehmen Sie Kontakt mit Ihrem Anbieter auf um eine Klärung zu erreichen. Nutzen Sie App-Passwörter. Diese ermöglichen einen Zugriff mit speziellen Zugangsdaten (google).
	Provider hat Sicherheit angepasst	Bitte prüfen sie ob „unsichere Anwendungen“ zugriff auf ihren E-Mail-Dienst haben. Nehmen Sie Kontakt mit Ihrem Anbieter auf um eine Klärung zu erreichen. Nutzen Sie App-Passwörter. Diese ermöglichen einen Zugriff mit speziellen Zugangsdaten (google).
	E-Mail-Einstellungen nicht korrekt	Prüfen Sie ihre E-Mail-Einstellungen unter <u>SETUP → SYSTEM → E-MAIL</u> . Nutzen Sie die Test-E-Mail um Ihre Einstellungen zu prüfen.

	E-Mail-Server nicht erreichbar	Prüfen Sie, dass der unter <u>SETUP → SYSTEM → E-MAIL</u> eingestellte Port für das IRAS-Gefahrenmeldesystem erreichbar ist. Ebenfalls muss ein gültiger DNS eingetragen sein (DHCP) und die URL darf nicht blockiert werden. Nutzen Sie die Test-E-Mail um Ihre Einstellungen zu prüfen.
	Spam Filter	Prüfen Sie Ihren Spam Filter. Nutzen Sie die Test-E-Mail um Ihre Einstellungen zu prüfen.
Die E-Mail wird für konfigurierte Meldungen gesendet, jedoch ohne Anhang.	Laufkarte nicht vorhanden	Das IRAS-SECURE-Gefahrenmeldesystem kann zu der Meldung nicht die entsprechende Laufkarte finden. Prüfen Sie unter <u>SETUP → DOKUMENTE → VERFÜGBARE LAUFKARTEN/MELDEPUNKTE</u> ihre Konfiguration. Prüfen Sie ob die Laufkarten-Dateien vorhanden sind und die Namensvereinbarung einhalten.
	Spam Filter	Der Anhang wird von Ihren E-Mail-Filtern gelöscht. Nutzen Sie die Test-E-Mail um Ihre Einstellungen zu prüfen.
	Benachrichtigungsfilter prüfen	Prüfen Sie die Einstellungen des E-Mail-Filter und ob der Versand von JPG/PDF aktiviert ist.
Das IRAS-SECURE-Gefahrenmeldesystem bekommt ein angekündigtes Software-update nicht	Update-Server nicht erreichbar	Führen Sie die Selbstdiagnose unter <u>SETUP → SYSTEM → DIAGNOSE</u> durch. Achten Sie darauf, dass der Port 443 zur URL iras.ifam.com Zugang hat.
Nach dem Import der Sicherung ist das IRAS-SECURE-Gefahrenmeldesystem nicht mehr erreichbar	Falsche IP-Adresse	Nutzen Sie einen IP-Scanner (DHCP) zum Ermitteln der korrekten IP-Adresse des IRAS-SECURE-Gefahrenmeldesystems. Ggf. müssen Sie die IP-Adressen anpassen, so dass sich Ihr PC und das IRAS-Gefahrenmeldesystem im selben Subnetz befinden.

Bei kommendem Feuer wird in der IRAS-App kein Ton abgespielt.	Fehlende Zuordnung der Meldungen zu dieser Ebene.	Prüfen Sie unter <u>SETUP</u> → <u>CODETABELLE</u> die Zuordnung von Meldungen zu der Ebene Feuer.
	Die App ist nicht korrekt mit dem richtigen IRAS-Gefahrenmeldesystem verbunden.	Geben Sie die korrekte Adresse, Benutzername und Passwort in der App ein und speichern Sie diese Konfiguration. Dadurch registriert sich dieses mobile Gerät automatisch am IRAS-SECURE-Gefahrenmeldesystem für Push-Nachrichten.
	Stummschaltung der Töne am mobilen Endgerät.	Aktivieren Sie die Töne auf Ihrem Endgerät.
	Push-Benachrichtigungen in der App deaktiviert.	Aktivieren Sie die Push-Benachrichtigungen in den Einstellungen der App.

Tabelle 4: Störungsübersicht

10.2 IRAS-Website

10.2.1 Dashboard – Störungsmeldungen

Aktuelle Meldungen werden, auf der Ebene STÖRUNG, auf dem Dashboard angezeigt.

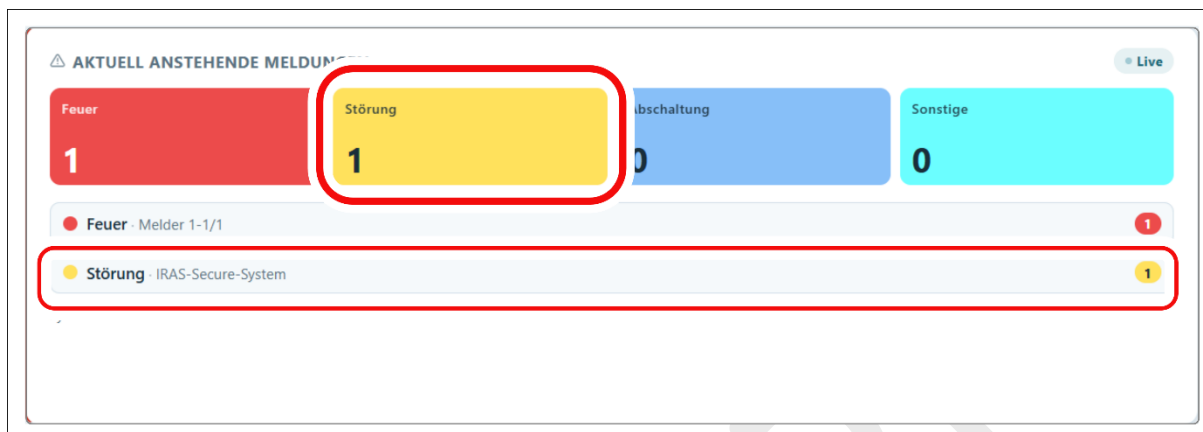


Abbildung 130: IRAS-Website – Dashboard/Störung (Beispiel)

➡ Siehe auch Kapitel 9.3.4.1.2 Aktuell anstehenden Meldungen.

Durch Klick auf die entsprechende Ebene im Bereich AKTUELL ANSTEHENDE MELDUNGEN oder die Statuszeile werden in einer Übersicht alle ggf. anstehenden Störungsmeldungen angezeigt werden.

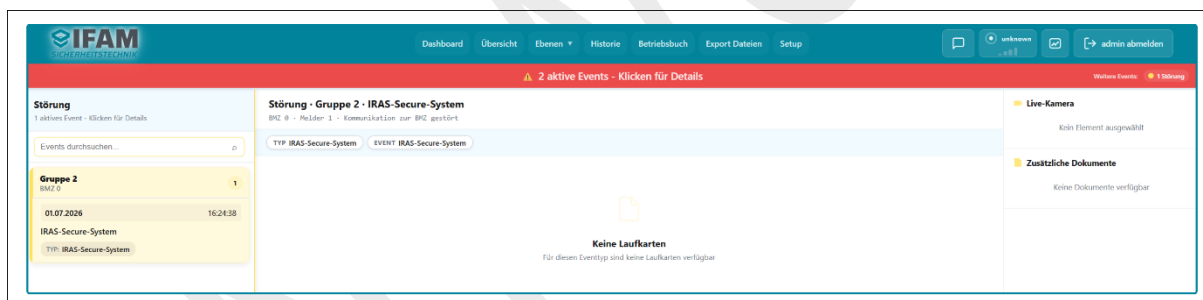


Abbildung 131: IRAS-Website – aktuelle Ereignisse/Störungen (Beispiel)

Durch Auswahl einer Störungsmeldungen werden Details zum Störungsort und ggf. verknüpfte Medien (Laufkarten, zusätzliche Dokumente, Kameras) angezeigt.

10.2.2 Diagnose

Mit Hilfe der Funktion DIAGNOSE werden eine Vielzahl an Optionen zur Unterstützung bei der Suche und Beseitigung von Störungen/Fehlern und für Wartungen zur Verfügung gestellt.

1. Wählen Sie in der Menüzeile die Schaltfläche SETUP.
→ Die Benutzeroberfläche zum Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SYSTEM.
→ Die Benutzeroberfläche der Systemkonfiguration wird geöffnet.
3. Wählen Sie die Option DIAGNOSE.

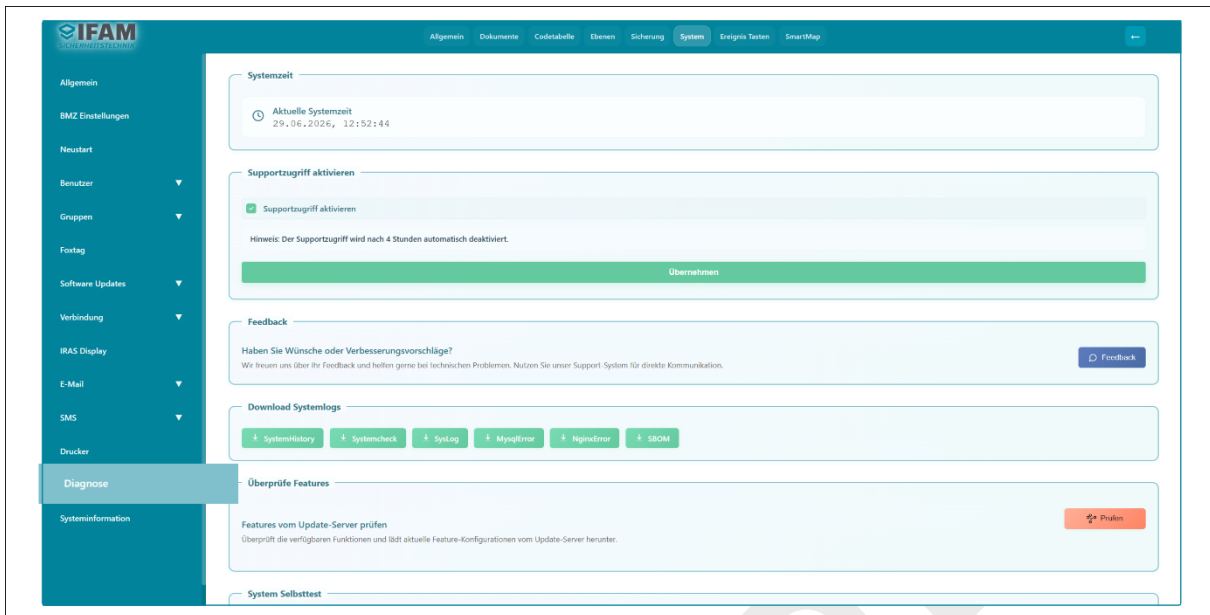


Abbildung 132: IRAS-Website – Diagnose (Beispiel)

10.2.2.1 Supportzugriff aktivieren

Bei auftretenden Störungen/Fehlern kann, nach Absprache, ein Supportzugriff aktiviert werden. Hierbei wird dem Kundendienst der IFAM GmbH Erfurt der Online-Zugriff auf das IRAS-SECURE-Gefahrenmeldesystem ermöglicht. Dieser kann dann u.a. zu Diagnose- und Testzwecken genutzt werden.

Der Supportzugriff kann nur temporär aktiviert werden und wird aus Sicherheitsgründen nach 4 Stunden wieder deaktiviert.

10.2.2.2 Systemlogs

Zur Störungsanalyse können LOG-EINTRÄGE eingesehen werden (z.B. E-Mail, Push, System, Drucker).

Systemlogs können zudem heruntergeladen und eingesehen werden (DOWNLOAD SYSTEM-LOGS). Die Dateien werden im Downloadbereich Ihres Betriebssystems gespeichert.

10.2.2.3 Selbsttest

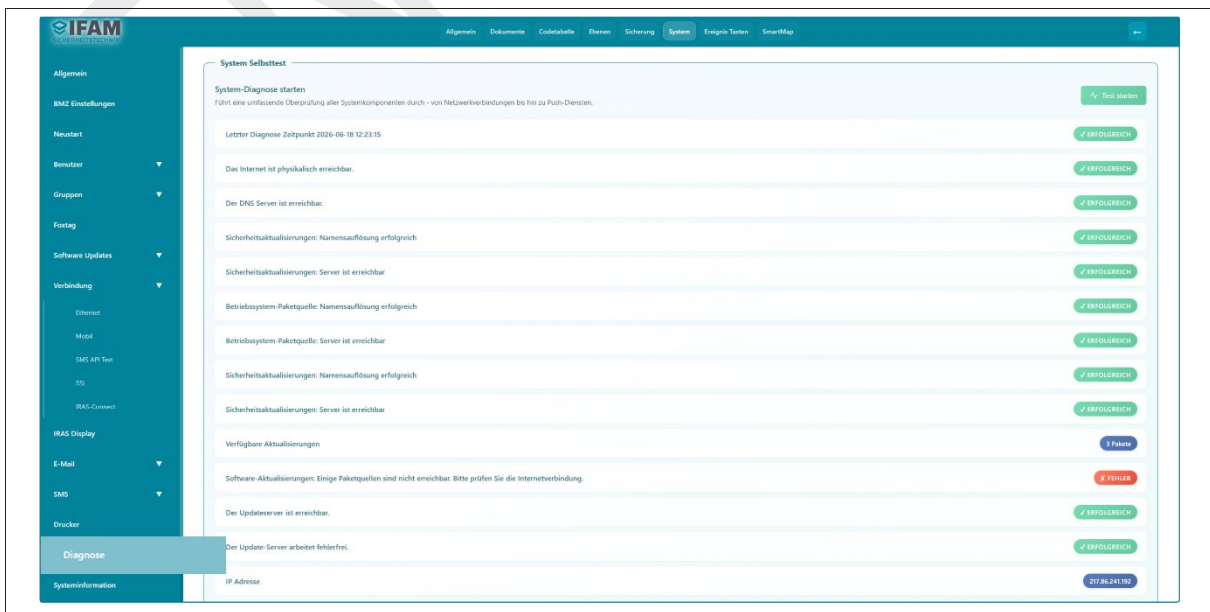


Abbildung 133: IRAS-Website – Selbsttest (Beispiel)

IRAS-SECURE ermöglicht die Ausführung eines SYSTEM-SELBSTTESTS, der der Störungs-Erkennung oder Statusfeststellung dient.

Durch Aktivierung der Schaltfläche TEST STARTEN werden festgelegte Funktionen und Parameter geprüft. Hierbei werden neben allen Systemkomponenten u.a. auch Netzwerkverbindungen, Softaktualisierungen und Push-Dienste einbezogen.

Die Ergebnisse werden in der rechten Spalte als erkannte Parameter (z.B. IP-Adresse) oder als Funktions-Status (z.B. FEHLER/ERFOLGREICH) angezeigt.

Die nachfolgende Tabelle beschreibt ausschließlich rot markierte Ergebnisse (Fehler). Gelbe Warnungen und blaue Informationswerte sind keine fehlgeschlagenen Prüfungen.

Selbsttest-Meldung	Mögliche Ursache	Lösungsansatz
Letzter Diagnosezeitpunkt älter als 7 Tage	Der Selbsttest wurde länger nicht ausgeführt oder konnte nicht abgeschlossen werden.	Selbsttest erneut starten. Bei wiederholtem Fehlschlag Systemprotokoll und verfügbare Speicherkapazität prüfen.
Google konnte anhand der IP nicht erreicht werden	Keine Internetverbindung, fehlerhaftes Standardgateway oder ausgehender ICMP-Verkehr wird blockiert.	Netzwerkkabel, IP-Adresse, Gateway und DNS-Konfiguration prüfen. Firewall-Regeln für ausgehenden Verkehr kontrollieren; ICMP-Sperren nur als Ursache bewerten, wenn die übrigen Internetprüfungen erfolgreich sind.
IRAS-Plus-Connect ist nicht erreichbar.	Keine Verbindung zum primären IRAS-Plus-Connect-Endpunkt oder blockierter VPN-/Firewall-Verkehr.	Internetverbindung und Firewall-Freigaben prüfen. VPN- bzw. IRAS-Plus-Connect-Konfiguration kontrollieren und den Dienststatus beim Betreiber prüfen.
IRAS-Plus-Connect Redundanz Server ist nicht erreichbar.	Keine Verbindung zum redundanten IRAS-Plus-Connect-Endpunkt oder blockierter VPN-/Firewall-Verkehr.	Internetverbindung und Firewall-Freigaben prüfen. Redundanzverbindung und Dienststatus beim Betreiber kontrollieren.
Die DNS-Auflösung für Google ist nicht korrekt	DNS-Server nicht erreichbar oder DNS-Konfiguration fehlerhaft.	Konfigurierte DNS-Server, Gateway und Internetzugang prüfen. Bei statischer Konfiguration korrekte DNS-Adressen eintragen und anschließend Selbsttest wiederholen.
Die DNS-Auflösung für den Updateserver ist nicht korrekt	Der konfigurierte Updateserver kann nicht aufgelöst werden; DNS oder Serveradresse ist fehlerhaft.	DNS-Konfiguration und Updateserver-Adresse prüfen. Bei internem Updateserver dessen Erreichbarkeit und den zugehörigen DNS-Eintrag prüfen.

Selbsttest-Meldung	Mögliche Ursache	Lösungsansatz
Der Apple-Push Dienst konnte nicht erreicht werden. Port 2195 gesperrt?	Ausgehende Verbindung zu Apple Push Notification Service nicht möglich.	Internetzugang und Firewall prüfen. Ausgehenden TCP-Verkehr zu Apple Push Notification Service auf Port 2195 freigeben, sofern Apple-Push verwendet wird.
Der Android-Push Dienst konnte nicht erreicht werden. Port 443 gesperrt?	Ausgehende HTTPS-Verbindung zu Firebase/Google-Push nicht möglich.	Internetzugang, DNS und Firewall prüfen. Ausgehenden TCP-Port 443 zu den Android-Push-Endpunkten freigeben.
Der Windows-Push Dienst konnte nicht erreicht werden. Port 443 gesperrt?	Ausgehende HTTPS-Verbindung zu Windows Push Notification Service nicht möglich.	Internetzugang, DNS und Firewall prüfen. Ausgehenden TCP-Port 443 zu den Windows-Push-Endpunkten freigeben.
Die Kommunikation mit dem Update-Server war nicht möglich	TLS-Zertifikatsprüfung oder HTTPS-Verbindung zum Updateserver fehlgeschlagen.	Systemzeit, DNS, Internetverbindung, Updateserver-URL sowie installierte CA-/Client-Zertifikate prüfen. Zertifikate bei Ablauf oder falscher Zuordnung erneuern.
HTTPS inaktiv	HTTPS ist auf der Box deaktiviert oder der Webserver kann die TLS-Konfiguration nicht laden.	HTTPS in der Systemkonfiguration aktivieren. Webserver-Konfiguration und zugehöriges Serverzertifikat prüfen; anschließend die Oberfläche per HTTPS erneut aufrufen.
Zugriff nicht möglich	Der für den Selbsttest konfigurierte Gegenstellenzugriff bzw. Zertifikatsnachweis ist fehlgeschlagen.	Netzwerkpfad zur Gegenstelle sowie Zertifikate und zugehörige Namen prüfen. Bei weiterem Fehler das Diagnosepaket an den Support übermitteln.
Software-Aktualisierungen: Einige Paketquellen sind nicht erreichbar. Bitte prüfen Sie die Internetverbindung.	Mindestens eine konfigurierte APT-Paketquelle ist nicht erreichbar.	Internet, DNS, Proxy und Firewall prüfen. Danach die zusätzlich ausgegebenen Paketquellen-Einträge für Namensauflösung und Erreichbarkeit auswerten.
Paketquelle: Namensauflösung fehlgeschlagen – der Server konnte nicht gefunden werden.	DNS kann den Host einer APT-Paketquelle nicht auflösen.	DNS-Server und DNS-Sucheinstellungen prüfen. Bei interner Paketquelle deren DNS-Eintrag oder lokale Namensauflösung korrigieren.

Selbsttest-Meldung	Mögliche Ursache	Lösungsansatz
Paketquelle: Server antwortet nicht – möglicherweise blockiert eine Firewall die Verbindung.	Der Host der APT-Paketquelle ist auf Netzwerkebene nicht erreichbar oder ICMP wird gefiltert.	Routing, Gateway, Firewall und Verfügbarkeit der Paketquelle prüfen. Wenn nur diese Prüfung fehlschlägt, aber Updates funktionieren, kann eine ICMP-Sperre die Ursache sein.

Tabelle 5: IRAS-Website - Selbsttest/Fehlermeldungen

10.2.3 Historie

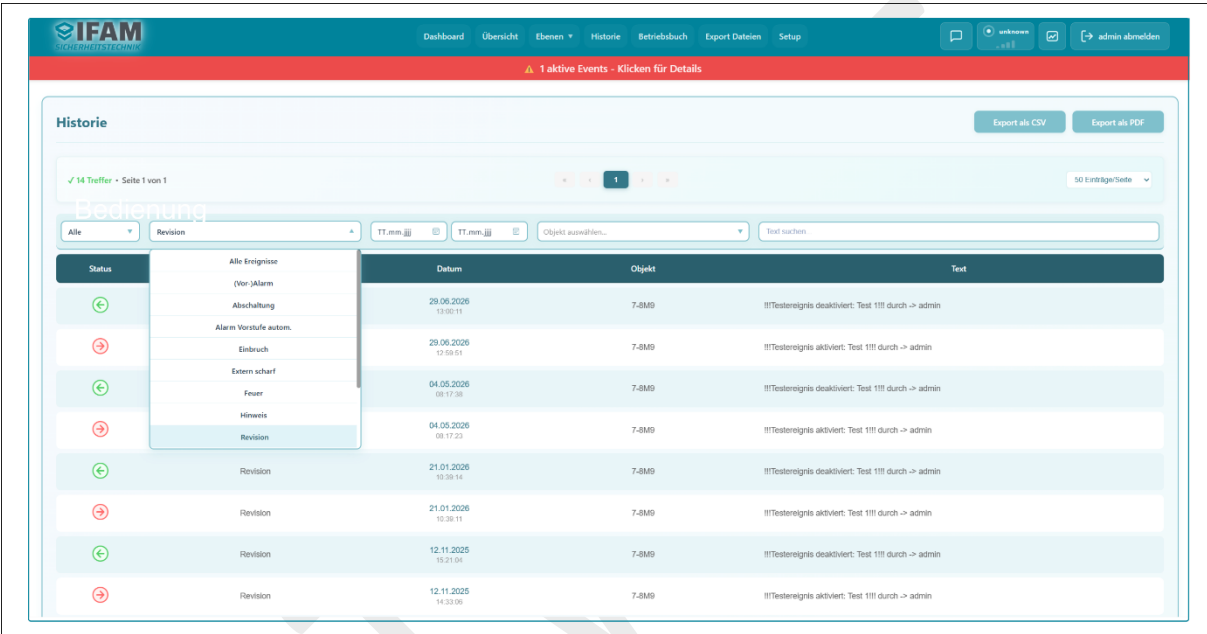


Abbildung 134: IRAS-Website – Störungsbeseitigung/Historie

Die Funktion HISTORIE zur Nachverfolgung/Archivierung aller Ereignis-Meldungen des Gefahrenmeldesystems kann zur Störungs-/Fehlerdiagnose verwendet werden.

Wählen Sie in der Menüzeile die Schaltfläche HISTORIE.
→ Die Benutzeroberfläche HISTORIE, mit einer Darstellung aller Ereignismeldungen, wird geöffnet.

Sie haben hier die Möglichkeit, gezielt nach Meldungen zu Störungen/Fehler, durch eine Filterung zu suchen. Die Einträge können gefiltert werden nach:

- Zeiträumen,
- Ereignistypen,
- Ereignisstatus (kommend/gehend),
- Objekten.

Die Ereignisliste kann als CSV- und PDF-Datei exportiert werden, die im Download-Bereich Ihres Betriebssystems abgelegt wird.

10.2.4 Betriebsbuch (optional)



Das **BETRIEBSBUCH** ist eine Erweiterungsoption von IRAS-SECURE, die in der Standardversion noch nicht enthalten ist.

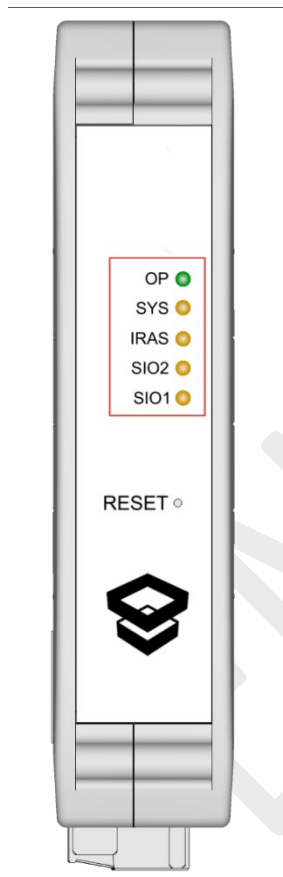
Hier können Eintragungen zu Ereignissen bzw. Meldungen vorgenommen und eingesehen werden, die bei einer Störungs-/Fehlerbehebung und im Rahmen einer Wartung unterstützend verwendet werden können.

Für weitere Informationen wenden Sie sich bitte an den Kundendienst der IFAM GmbH Erfurt.

10.3 Hardware

10.3.1 ADP4000-IRAS – Diagnose-LEDs

Das Auftreten von Störungen wird am *ADP4000-IRAS* durch das Aufleuchten einer oder mehrerer LEDs angezeigt. Die jeweilige LED verweist auf die entsprechende Störung/Störungsstelle.



LED		Beschreibung		
SIO1	gelb	Dual-Ring SIO1	Kommunikationsstörung	
SIO2	gelb	Dual-Ring SIO2	Kommunikationsstörung	
IRAS	gelb	Interne Kommunikation	Kommunikationsstörung	
SYS	gelb	Systemzustand	Störung auf dem <i>ADP4000-IRAS</i> (Fehlfunktion). → Kontaktieren Sie den IFAM-Kundendienst.	
OP	grün	Betriebsstatus	An	Betriebsbereit. Störungsfrei.
			Blinken (lang an – kurz aus)	Störung festgestellt. → Störungsart im <i>Prog4000</i> feststellen. - Konfiguration der Schnittstellen-Parameter prüfen. - Spannung ggf. anpassen.
			Blinken (gleichmäßig)	Bootlader aktiv.

Tabelle 6: ADP4000-IRAS – Diagnose-LEDs/Störungserkennung

10.3.2 ADP4000 – Diagnose-LEDs

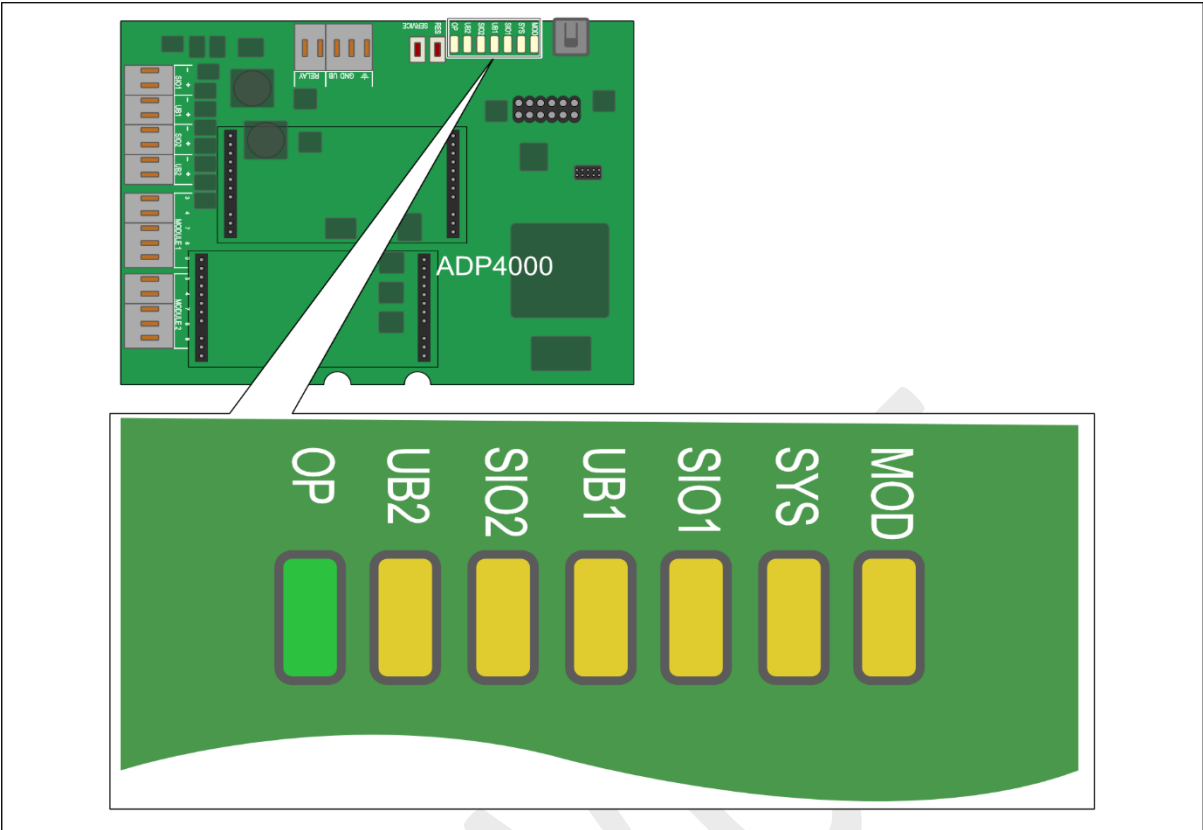


Abbildung 135: ADP4000 – Diagnose-LEDs

Das Auftreten von Störungen wird am ADP4000 durch das Aufleuchten einer oder mehrerer LEDs angezeigt. Die jeweilige LED verweist auf die entsprechende Störung/Störungsstelle.

LED		Beschreibung		
OP	grün	Betriebsstatus	An	Betriebsbereit. Störungsfrei.
			Blinken (lang an – kurz aus)	Störung festgestellt. → Störungsart im <i>Prog4000</i> feststellen. - Konfiguration der Schnittstellen-Parameter prüfen. - Spannung ggf. anpassen.
			Blinken (gleichmäßig)	Bootlader aktiv.
UB2	gelb	Stromversorgung UB2	Störung der Stromversorgung	
SIO2	gelb	Kommunikation SIO2	Kommunikationsstörung	
UB1	gelb	Stromversorgung UB1	Störung der Stromversorgung	
SIO1	gelb	Kommunikation SIO1	Kommunikationsstörung	
Sys	gelb	System	Störung auf dem ADP4000 (Fehlfunktion). → Kontaktieren Sie den IFAM-Kundendienst.	
Mod	gelb	Modulsteckplatz	Verbindung der Schnittstelle zur BMZ gestört. → Physische Verbindung (Kabel) zur BMZ prüfen.	

Tabelle 7: ADP4000 – Diagnose-LEDs/Störungserkennung

10.4 Gefahrenmeldezentrale (GMZ)



Informationen zu Störungsmeldungen entnehmen Sie bitte der [herstellereigenen Dokumentation der Gefahrenmeldeanlage/Gefahrenmelderzentrale](#).

10.5 Prog4000

Störungen können auch mit Hilfe des Konfigurationstools *Prog4000* ermittelt werden.

1. Klicken Sie in der GLOBALEN ÜBERSICHT auf das zu analysierende Gerät.

1. Aktivieren Sie den Button ANALYSIEREN.

→ Der STATUS des Gerätes bzw. des Systems wird angezeigt.



Zeigt an, dass die Geräte korrekt miteinander verbunden wurden/keine Störungen vorliegen.



Zeigt an, dass eine Störung vorliegt. Klicken Sie doppelt auf das Symbol. → Ein Fenster mit Störungsdetails öffnet sich. Beheben Sie die Störung.



Zeigt an, dass eine Meldung/Störungsmeldung für das Gerät vorliegt. Klicken Sie doppelt auf das Symbol. → Ein Fenster mit Informationen/Störungsdetails öffnet sich. Beheben Sie ggf. die Störung.

2. Wurde eine Störung festgestellt, klicken Sie doppelt auf das Störungssymbol.

→ In einem separaten Fenster werden die Störungsdetails angezeigt. Beheben Sie die Störung.



Eine umfassende Beschreibung des Konfigurationstools *Prog4000* finden Sie in der [Konfigurationsanleitung Prog4000](#).

11 Reset

Um IRAS-SECURE, die Gefahrenmeldeanlage (GMA) oder eine einzelne Komponente zurückzusetzen, kann ein Reset ausgeführt werden. Dies kann notwendig werden z.B. im Fall von Störungen, abweichenden, ungewöhnlichen technischen Zuständen, System-Anomalien oder nach Konfigurationsänderungen von z.B. IP-Adresse oder Mobilfunkanbindung.

Die nachfolgenden beschriebenen Optionen setzen das System bzw. die betreffende Komponente auf seinen definierten Ausgangszustand zurück. Vorhandene Konfigurationen bleiben erhalten.

11.1 IRAS-SECURE

IRAS-SECURE kann von der Website aus neu gestartet werden (Reset).

Dieser Vorgang dauert einige Sekunden.

Nach dem Neustart ist der Login erneut vorzunehmen. Hierzu sind die Anmeldedaten der Lieferinformationen zu verwenden.

➞ *Siehe Kapitel 18.1.1 IRAS-SECURE (System) – Lieferinformationen.*

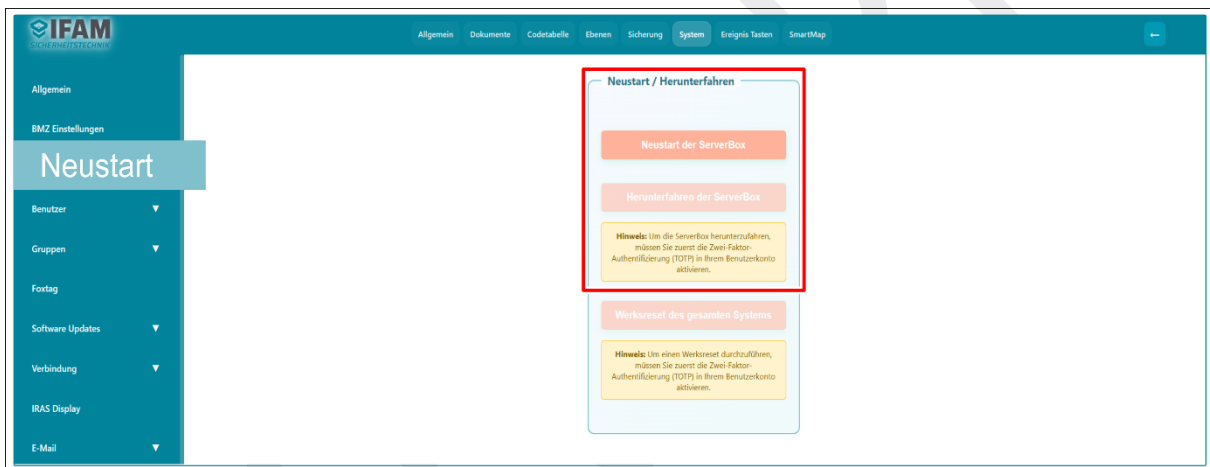


Abbildung 136: IRAS-Website – System-Reset

1. Wählen Sie auf der Menüzeile die Schaltfläche SETUP. → Die Benutzeroberfläche des SETUP-Bereichs wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SYSTEM. → Die Benutzeroberfläche der Systemverwaltung wird geöffnet.
3. Wählen Sie die Option NEUSTART.
4. Aktivieren Sie die Schaltfläche NEUSTART DER SERVERBOX bzw. Herunterfahren der SERVERBOX.



Für das Herunterfahren der Serverbox ist die Aktivierung/Konfiguration einer 2-Faktor-Authentifizierung (TOTP) für den jeweiligen Benutzer erforderlich

➞ *Siehe Kapitel 9.3.3.2 Zwei-Faktor-Authentifizierung einrichten.*

11.2 ADP4000-IRAS



Im Rahmen einer möglichen Störungsbeseitigung kann der **ADP4000-IRAS** neu gestartet werden. Drücken Sie hierfür den Reset-Taster auf der Vorderseite des Gerätes. Nehmen Sie ein geeignetes (spitzes) Werkzeug zu Hilfe.

11.3 Prog4000

11.3.1 Gerätereustart

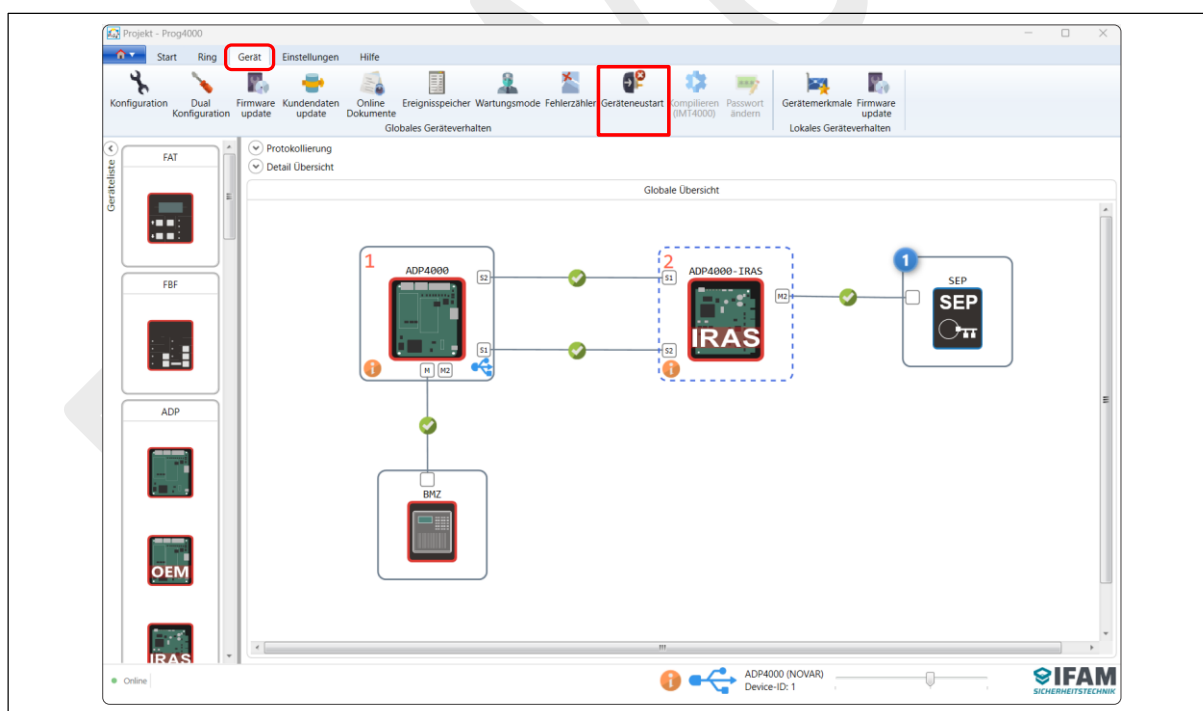


Abbildung 137: Prog4000 – Gerätereustart

1. Öffnen Sie Prog4000 und laden Sie die Gerätetopologie Ihrer Gefahrenmeldeanlage.
2. Markieren Sie das betreffende Gerät (z.B. **ADP4000-IRAS**). → Das Symbol wird blau markiert.
3. Aktivieren Sie auf der Registerkarte **RING** die Option **GERÄTENEUSTART**. → Das Gerät wird neu gestartet.

12 Firmware aktualisieren

12.1 Prog4000

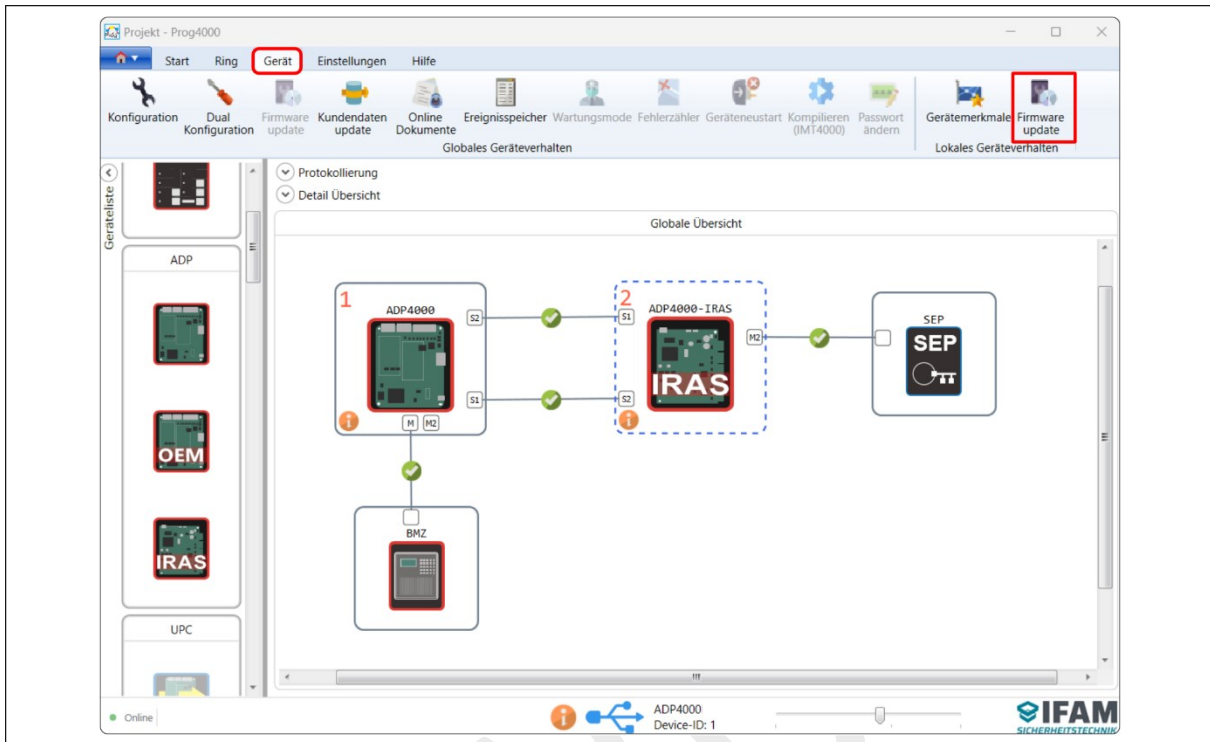


Abbildung 138: Prog4000 – Firmware-Update 1 (Beispiel)

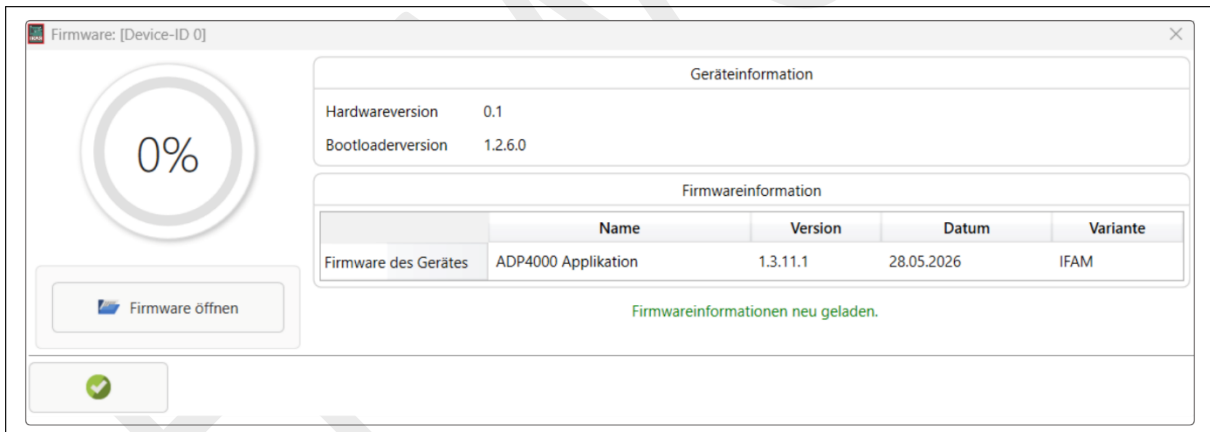


Abbildung 139: Prog4000 – Firmware-Update 2 (Beispiel)

Die Firmware der im Ring enthaltenen Geräte kann mit Hilfe des Konfigurationstools Prog4000 aktualisiert werden. Öffnen Sie hierzu Prog4000 mit der aktuellen Konfiguration des Gerätes/Systems.

Legen Sie ggf. ein neues Projekt mit der gewünschten Konfiguration an.

➡ [Siehe Kapitel 7.3.1 Ring-Komponenten einlesen.](#)

Manuelle Aktualisierung

Voraussetzung:

Das zu aktualisierende Gerät (z.B. ADP4000) muss mit dem PC verbunden sein. Eine aktuelle Firmware-Datei ist verfügbar (Update-Server/lokal).

1. Wählen Sie das zu aktualisierende Gerät (z.B. *ADP4000-IRAS*) aus. → Das Gerätesymbol wird blau umrandet (Abbildung **138**).
2. Betätigen Sie auf der Registerkarte GERÄT die Schaltfläche FIRMWARE UPDATE. → Das Dialog-Fenster zur Firmware-Aktualisierung (Abbildung **34**) öffnet sich. Die aktuell installierte Firmware-Version wird angezeigt (**5**).
3. Betätigen Sie die Schaltfläche FIRMWARE ÖFFNEN (**2**). Wählen Sie die gewünschte Firmware-Datei und starten Sie die Aktualisierung (Schaltfläche INSTALLIEREN) (**3**). → Eine Anzeige (**1**) zeigt den Status der Aktualisierung. Nach Abschluss des Vorgangs kommt der Zeiger zum Stillstand. → Eine gesonderte Meldung (**6**) zeigt das Ergebnis des Vorgangs an.
4. Schließen Sie das Dialog-Fenster FIRMWARE (**4**).



Beim Firmware-Update schaltet die Baugruppe automatisch in den "Bootladermodus". Dieser Zustand wird durch zyklisch wiederholtes 3-fach kurzes Blinken der grünen LED am z.B. *ADP4000-IRAS* angezeigt. In dieser Betriebsart erfolgt keine Kommunikation mit der BMZ und die BMZ zeigt ggf. eine Kommunikationsstörung für diese Schnittstelle an.

13 Wartung

13.1 Allgemeine Empfehlungen

- Nehmen Sie **mindestens einmal jährlich** eine Prüfung des IRAS-SECURE-Gefahrenmeldesystems vor.
- Prüfen Sie Anschlüsse und Kabelbefestigungen auf Unversehrtheit bzw. korrekten Sitz.
- Prüfen Sie insbesondere auf äußere Unversehrtheit und ggf. vorhandene Manipulationen.
- Prüfen Sie die Unversehrtheit der vorhandenen Geräte-Siegel (ADP4000-IRAS und Industrie-PC).
- Achten Sie auf Anomalien und ungewöhnliche Ereignisse, die nicht dem vorgesehenen bzw. erwartbaren Betriebsverhalten von IRAS-SECURE entsprechen.
- Für den Einsatz von IRAS-SECURE in Brandmeldeanlagen (BMA) beachten Sie grundsätzlich die hierfür geltenden Normen und Richtlinien (z. B. DIN 14675-1/-2, DIN VDE 0833-1/-2/-4).
- Dokumentieren Sie Prüfungen ggf. durch entsprechende Einträge im BETRIEBSBUCH (optional).

13.2 IRAS-Secure – Metallgehäuse



- Die Wartung des Gehäuses muss regelmäßig, in Abhängigkeit von den Einsatz- und Umgebungsbedingungen, mindestens einmal jährlich durchgeführt und entsprechend dokumentiert werden! Untenstehende Wartungsmaßnahmen folgen den Empfehlungen des Herstellers.
- Wartungsarbeiten sind durch eine Fachkraft auszuführen.
- Beachten Sie die allgemein geltenden Richtlinien zur Wartung von Betriebsmitteln.

Regelmäßig:

- Prüfen Sie alle Bauteile und Oberflächen auf Beschädigungen.
- Prüfen Sie die Scharniere der Türen auf Leichtgängigkeit. Sprühen Sie sie mit einem wasserfreien Schmiermittel ein.
- Prüfen Sie die Leichtgängigkeit des Schlosses. Sprühen Sie die beweglichen Teile mit einem wasserfreien Schmiermittel ein.
- Prüfen Sie die Andruckkanten der Dichtungen. Bei Beschädigungen in diesem Bereich müssen diese vollständig ersetzt werden.
- Prüfen Sie das Gehäuse auf Korrosion. Beseitigen Sie ggf. vorhandene Schäden.
Kleinflächige Schäden: (z.B. Kratzer, kleinere Korrosionspuren): Schleifen Sie die Oberfläche an der beschädigten Stelle leicht an, beseitigen Sie alle Beschädigungen/Ver-
schmutzungen. Abschließend die bearbeiteten Stellen mit einem geeigneten Ausbesserungslack (alternativ: 2K-PUR Acryllack) verschließen. Der Lack kann mit einem Lackstift, einem Pinsel oder einer Lackspraydose aufgebracht werden.
Großflächige Schäden: Entfernen Sie die Schäden. Oberfläche gleichmäßig abreiben und mit Testbenzin reinigen. Abschließend die gesamte Fläche mit Ausbesserungslack überlackieren (alternativ: 2K-PUR Acryllack).

Weiteres:

- Schützen Sie die Dichtungen vor Anfrieren. Zum Schutz können hierzu u.a. Talkum, Vaseline und Wachse verwendet werden.

14 Außerbetriebnahme

14.1 Werksreset

Mit einem Werksreset kann das IRAS-SECURE-Gefahrenmeldesystem auf seinen Lieferzustand zurückgesetzt werden.

Hierbei werden alle gespeicherten Benutzer-/Betreiber-spezifischen Konfigurationen entfernt, z.B. Benutzerdaten, Netzwerkkonfigurationen, Betriebsbuch-Einträge, Meldungshistorie.

Er muss aus Gründen der Datensicherheit u.a. zwingend bei einer Außerbetriebnahme des Systems oder ggf. bei Betreiber- oder Besitzerwechsel ausgeführt werden.

1. Wählen Sie auf der Menüzeile die Schaltfläche SETUP. → Die Benutzeroberfläche des SETUP-Bereichs wird geöffnet.
2. Wählen Sie in der Menüzeile am oberen Rand die Schaltfläche SYSTEM. → Die Benutzeroberfläche der Systemverwaltung wird geöffnet.
3. Wählen Sie die Option NEUSTART.
4. Aktivieren Sie die Schaltfläche WERKSRESET DES GESAMTEN SYSTEMS.

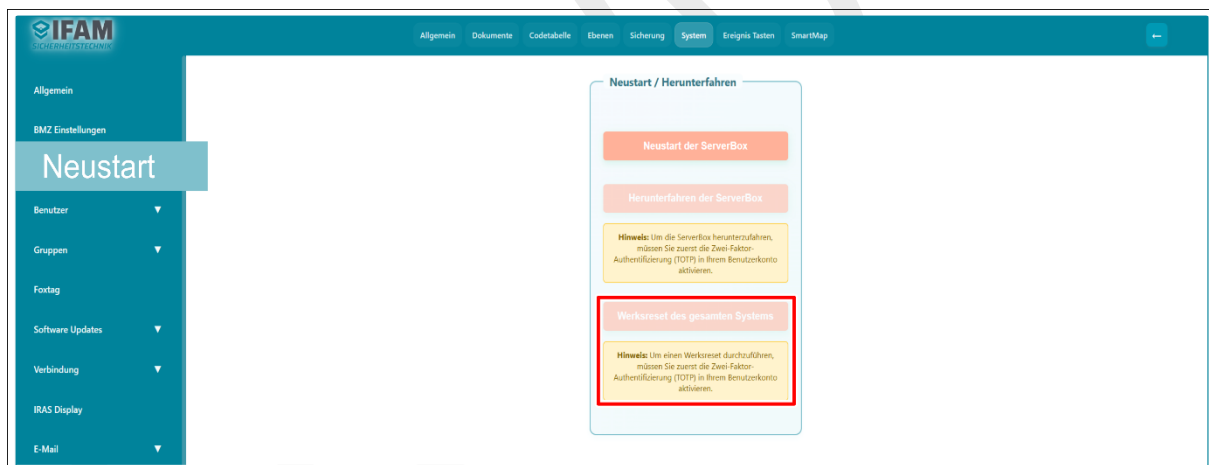


Abbildung 140: IRAS-Website – Werksreset



Für das Ausführen des Werksresets ist die Aktivierung/Konfiguration einer 2-Faktor-Authentifizierung (TOTP) und die Berechtigung des jeweiligen Benutzers erforderlich.

➔ [Siehe Kapitel 9.3.3.2 Zwei-Faktor-Authentifizierung einrichten.](#)

15 Transport und Lagerung

Der Transport und die Lagerung sollten in der Originalverpackung der Geräte durchgeführt werden. Die Verpackung muss vor Beschädigung schützen.

Beachten Sie die im  [Kapitel 17 Technische Daten](#) angegebenen zulässigen Umgebungs- bzw. Lagerbedingungen.

- Der Transport muss stoß- und schlagfrei erfolgen.
- Die Geräte trocken und staubfrei lagern.
- Die Geräte in geschlossenen Räumen (nie im Freien) lagern!
- Mehrere Geräte nicht übereinander stapeln.
- Setzen Sie die Geräte keinen aggressiven Medien aus.
- Schützen Sie die Geräte vor direkter Sonneneinstrahlung.
- Vermeiden Sie mechanische Erschütterungen.

16 Reparatur/Fehlerbehebung

Bei Fehlfunktionen eines Gerätes/des Zubehörs setzen Sie sich mit dem Kundendienst der IFAM GmbH Erfurt in Verbindung.

 [Siehe Kapitel 29 Kontakt und Kundenservice.](#)

Führen Sie keine eigenständigen Reparaturversuche durch!

Beachten Sie die Allgemeinen Geschäftsbedingungen!

Holen Sie ggf. die RMA-Nummer des Gerätes/Systems ein und senden Sie es an die Reparaturabteilung der IFAM GmbH Erfurt.

17 Technische Daten

17.1 IRAS-SECURE

Parameter		Wert	Einheit
Elektrik			
Eingangsspannung		90-264	VAC
Frequenz		47-63	Hz
Wirkungsgrad		88,5	%
Eingangsstrom	Volllast	1,3 (@230 VAC)	A
	Nominal	0,3 (@230 VAC)	A
	USV laden	0,8 (@230 VAC)	A
Empfohlene Vorsicherung		B6 A	-
Umgebungstemperatur (Betrieb)		-5 – 40	°C
Umgebungstemperatur (Lagerung)		-20 – 50	°C
Luftfeuchtigkeit		<95 (nicht kondensierend)	%
Schutzart (Gehäuse)		IP66	

Tabelle 8: Technische Daten – IRAS-SECURE

18 Produktidentifikation

18.1 Hardware

18.1.1 IRAS-SECURE (System) – Lieferinformationen

Informationen zur Geräteidentifikation finden Sie in den IRAS-SECURE-Informationen, die auf der Innenseite der Gehäusetür angebracht sind. ➡ [Siehe Kapitel 4.8 Systemaufbau](#). Die Lieferinformationen enthalten nachfolgende Angaben:

The image shows a digital representation of the IRAS-SECURE information label. It is divided into several sections: Login Information, QR-Code, Hardware Components, Manufacturing Details, and Nameplate. Numbered callouts (1-9) point to specific elements: 1 points to the Nameplate section, 2 points to the Manufacturing Date, 3 points to the Hardware Components section, 4 points to the Software Version, 5 points to the Login Information section, 6 points to the QR-Code, 7 points to the Support Until date, 8 points to the IFAM logo and contact info, and 9 points to the CE mark.

IRAS-SECURE Information	
Login Information	
Hostname:	iras-8d91ed
User:	admin
Password:	qH*YMnme?Huib:92
IP Address:	192.168.254.1
Software Version:	1.0.0.049
QR-Code  IRAS-Connect	
Hardware Components	
PC Label:	KSA7320309
Power Supply Label:	SC2A7T9329
Product Number:	9102.2731
MAC Address:	CC:82:7F:8D:91:EE
LTE IMEI:	860302051727724
USV SN:	2320254072513C0211
Mobil SN:	6005191770
ADP SN:	
Manufacturing Details	
Employee ID:	EMP_b90b0fee
Manufacturing Date:	10.07.2026 11:22
ISO Inspection:	N/A
Order Number:	8025.4910
Quality Inspection:	☒ Passed
Support Until:	10.08.2033
Nameplate	
IRAS-SECURE Product No.: 9102.2731 Device No.: 3425.0169  Date of Manufacture: 07 / 2026  IFAM SICHERHEITSTECHNIK IFAM GmbH Erfurt Gustav - Weisskopf - Strasse 9 99092 Erfurt www.ifam-erfurt.de 	

Abbildung 141: IRAS-Secure – Lieferinformationen (Beispiel)

Pos	Beschreibung
1	System-Informationen – Produkt-/Gerätenummer, Herstellungsdatum
2	Fertigungsdetails
3	Hardware-Informationen – Seriennummern der Komponenten)
4	Software (IRAS-Website) – Versionsnummer
5	Login-Informationen – kundenspezifisch
6	QR-Code – IRAS-Connect
7	Ende des Unterstützungszeitraum
8	Herstellerangaben
9	Entsorgungshinweise

18.1.2 ADP4000-IRAS

Informationen zur Geräteidentifikation finden Sie auf dem Typenschild, das auf der Seitenfläche des Gehäuses angebracht ist.

Das Typenschild enthält nachfolgende Angaben:

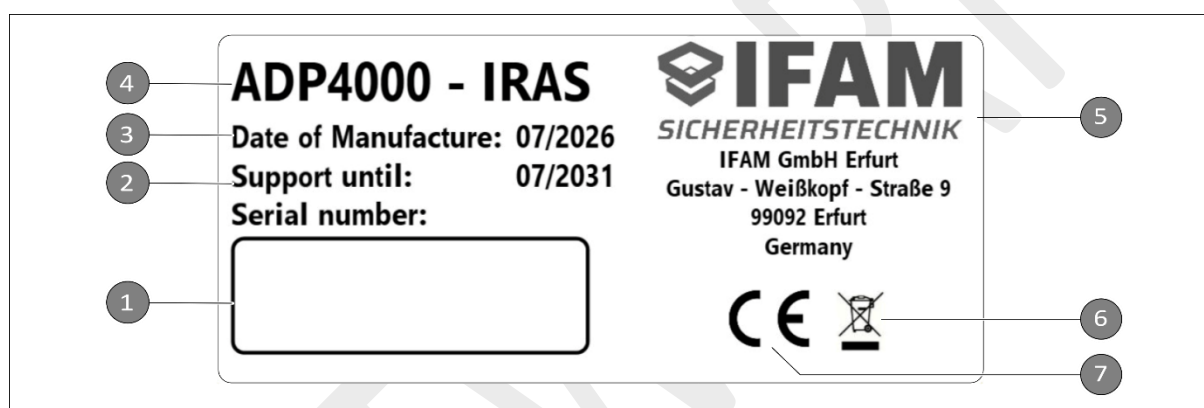


Abbildung 142: ADP4000-IRAS – Typenschild (Beispiel)

Pos	Beschreibung
1	Seriennummer
2	Unterstützungszeitraum/Ende
3	Herstellungsdatum (Monat/Jahr)
4	Gerätetyp/Bezeichnung
5	Herstellerinformation
6	Entsorgungshinweis
7	CE-Konformitätshinweis

18.2 Software

18.2.1 IRAS-Website/System

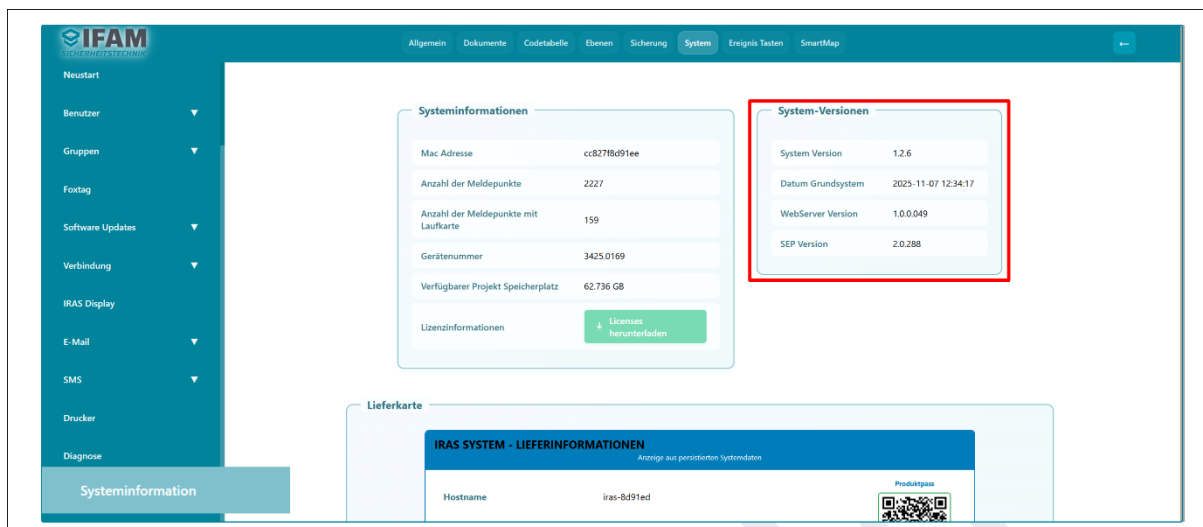


Abbildung 143: IRAS-Website – Systeminformation

Die Kennung/Versionsnummer der IRAS-Website finden Sie in den Lieferinformationen.

➡ [Siehe Kapitel 18.1.1 IRAS-SECURE \(System\) – Lieferinformationen.](#)

Die Versionsangaben zeigen den Stand der Hardware, die Version des Betriebssystems des IRAS-Gefahrenmeldesystems, den Softwarestand des *Webserver*s, sowie der Kommunikationssoftware und viele weitere Kennwerte des Systems.

Diese Lieferinformationen sind auch auf der IRAS-Website abrufbar.

1. Wählen Sie in der Menüleiste den Eintrag SETUP.
2. Wählen Sie in der SYSTEM- Menüleiste den Eintrag SYSTEM.
3. Öffnen Sie die Option SYSTEMINFORMATION.

18.2.2 Prog4000

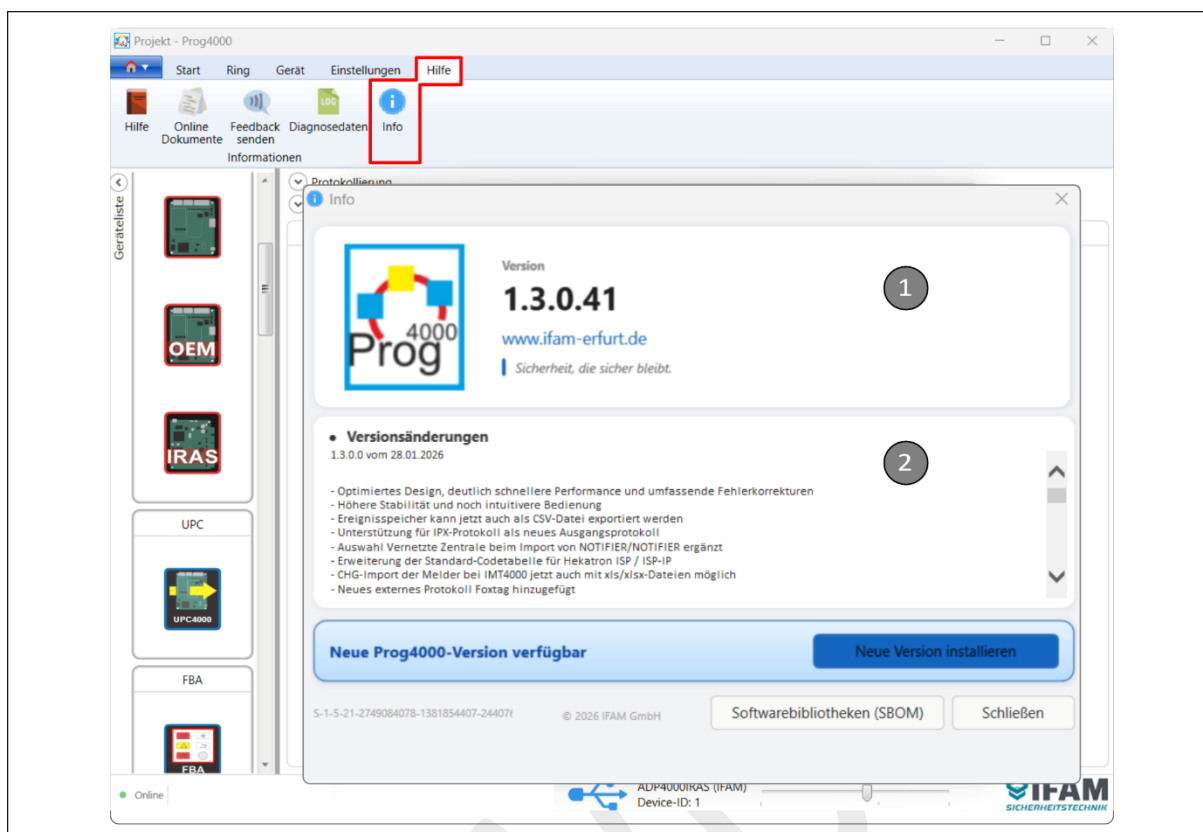


Abbildung 144: Prog4000 – Versionsnummer (Beispiel) - Platzhalter

Die Kennzeichnung der verwendeten Software-Version (1) finden Sie auf der Registerkarte HILFE unter dem Menü-Punkt INFO. Das sich öffnenden Fenster enthält darüber hinaus Informationen über vorgenommene Änderungen (Historie)(2).



Auf der Homepage der IFAM GmbH Erfurt und auf dem Update-Server steht die jeweils **aktuelle Version** des Konfigurationstools zur Verfügung.

18.2.3 IRAS-App

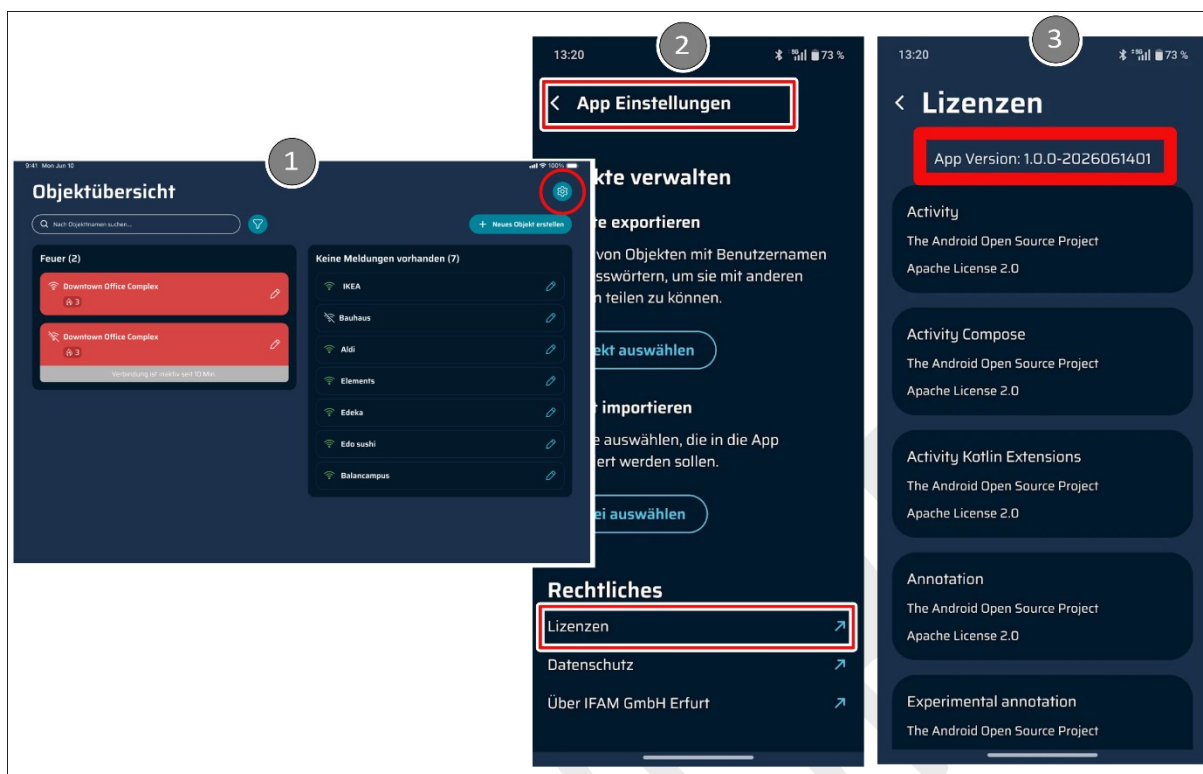


Abbildung 145: IRAS-App – Versionsnummer

18.2.4 Firmware (System4000-Geräte)

Informationen zur verwendeten Firmware-Version der im redundanten Ring enthaltenen System4000-Geräte können im Rahmen der Firmware-Aktualisierung eingesehen werden.

➡ [Siehe Kapitel 12 Firmware aktualisieren.](#)

Folgen Sie den dort beschriebenen Anweisungen.

19 Normen und Richtlinien

Die bei der Entwicklung des *IRAS-SECURE-Gefahrenmeldesystems* berücksichtigten Normen entnehmen Sie bitte der CE-Konformitätserklärung.

20 CE-Konformitätserklärung



Die CE-Konformitätserklärung kann auf der Homepage der IFAM GmbH Erfurt eingesehen werden: www.ifam-erfurt.de/de/service-support/downloads (Bereich IFAM → Konformitätserklärungen).

21 Produktpass

Den digitalen Produktpass zum IRAS-SECURE-Gefahrenmeldesystem können Sie über einen QR-Code auf den Lieferinformationen (auf der Innenseite der Gehäusetür) abrufen (**ab 2027 verfügbar**).

➞ *Siehe Kapitel 18.1.1 IRAS-SECURE (System) – Lieferinformationen.*

Dieses Dokument finden Sie alternativ auch auf der IRAS-Website.

1. Klicken Sie auf der Menüzeile auf den Eintrag SETUP. → Die Unterseite Setup/Dokumente wird geöffnet.
2. Wählen Sie in der Menüzeile den Eintrag SYSTEM. → Die Unterseite Setup/System wird geöffnet.
3. Wählen Sie im Seitenmenü den Eintrag SYSTEMINFORMATION. → Die Unterseite System/Systeminformation wird geöffnet. Scannen Sie im Abschnitt LIEFERKARTE den enthaltenen QR-Code.

22 Produktnummern

Informationen zu Produkt-/bzw. Artikelnummern des IRAS-SECURE-Gefahrenmeldesystems und ihrer möglichen Erweiterungen, die für eine Bestellung nötig sind, finden Sie in den Lieferinformationen sowie auf unserer Homepage im Rahmen der individuellen Produktbeschreibung: www.ifam-erfurt.de/de/produkte/produkte-uebersicht.

23 Unterstützungskonzept (Cybersicherheit)

Die IFAM GmbH Erfurt stellt regelmäßig Informationen zur Produktsicherheit (u.a. zur Cybersicherheit) zur Verfügung.

Dies können, nach Produkten sortiert, Mitteilungen zu Themen wie festgestellte Sicherheitsprobleme und Maßnahmen zu deren Behebung sein.

1. Rufen Sie die Website der Ifam GmbH Erfurt auf (www.ifam-erfurt.de) und navigieren Sie zur Fußzeile.
2. Wählen Sie den Eintrag SICHERHEITSHINWEISE. → Aktuelle Sicherheitsinformationen werden angezeigt (Abbildung 147/2).

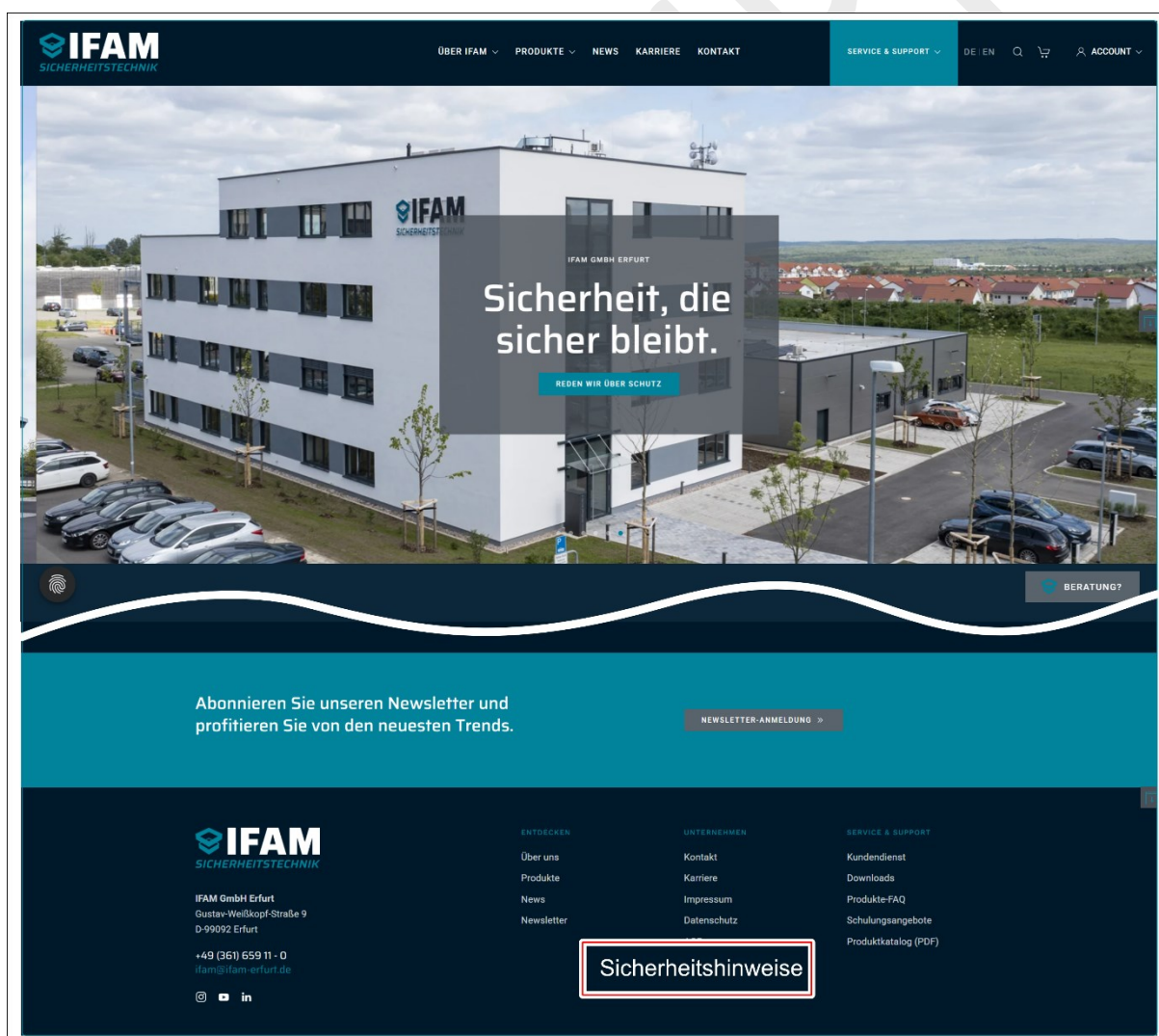


Abbildung 146: IFAM-Website – Sicherheitsinformationen

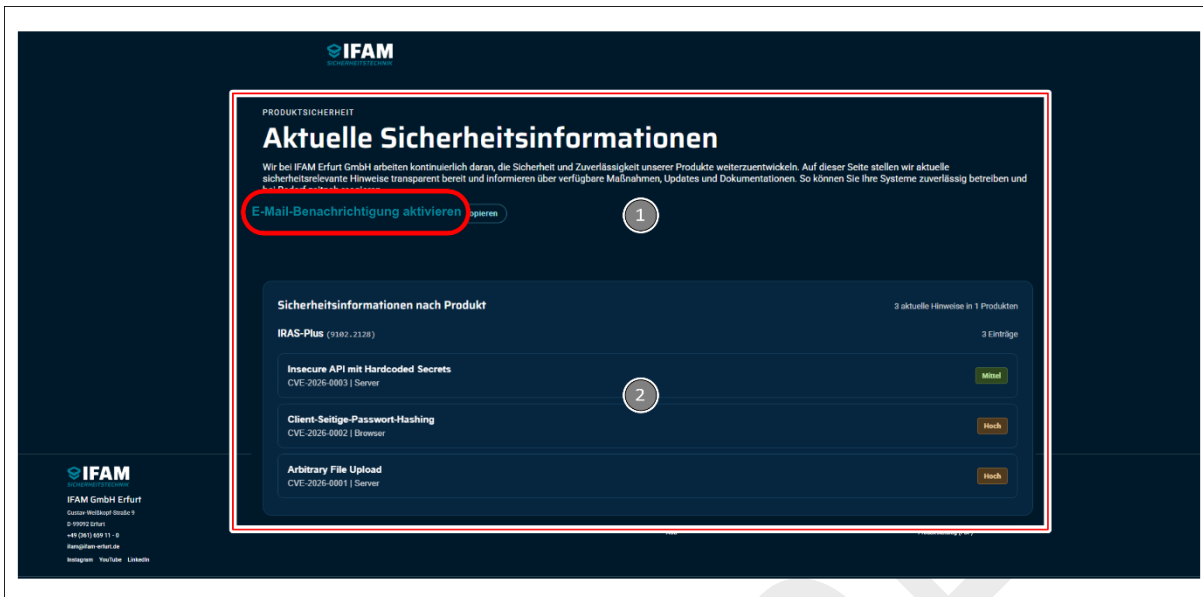


Abbildung 147: IFAM-Website – aktuelle Sicherheitsinformationen

Wählen Sie einen für Sie relevanten Beitrag. → Ein separates Fenster mit Details z.B. zur Art eines aufgetretenen Problems und dessen Lösung wird geöffnet (Abbildung 148).

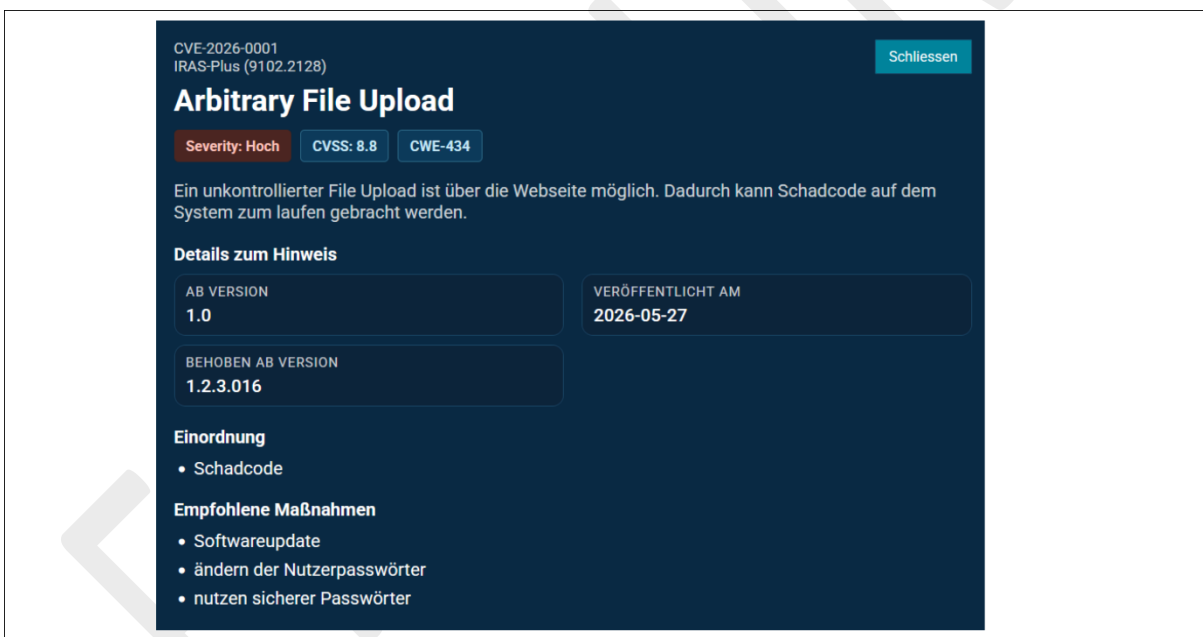
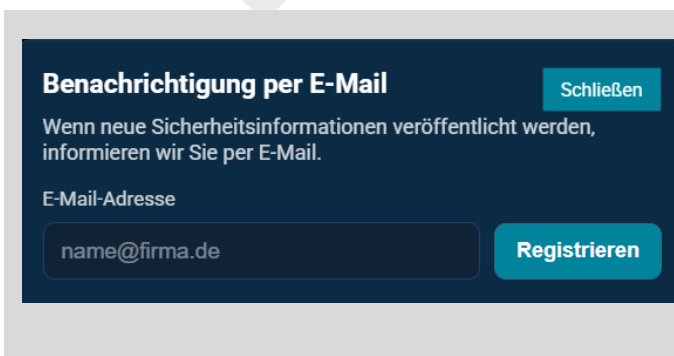


Abbildung 148: IFAM-Website – Sicherheitsinformationen/Details (Beispiel)



Für eine regelmäßige Zustellung von Sicherheitsinformationen bieten wir die Möglichkeit einer automatischen Benachrichtigung an.

Aktivieren Sie hierfür die Option BENACHRICHTIGUNG PER E-MAIL in der Übersichtsdarstellung und hinterlegen Sie Ihre E-Mail-Adresse. (Abbildung 147/1)

24 Datensicherheit

25 Datenschutzerklärung

Während des Betriebs und im Rahmen einer Wartung oder Inspektion erhebt, speichert und verarbeitet das IRAS-Gefahrenmeldesystem unterschiedlichste Daten. Für diese Daten trägt der Betreiber und der Nutzer des IRAS-Gefahrenmeldesystem die Verantwortung gegenüber dem Anlagenbetreiber.



Bitte stellen Sie sicher, dass das IRAS-SECURE-Gefahrenmeldesystem gemäß den geltenden Datenschutzbestimmungen verwendet wird.

Folgende Daten können verarbeitet werden:

Positionsdaten

Diese Daten werden von dem IRAS-Gefahrenmeldesystem nicht erhoben bzw. gespeichert.

Zahlungsinformationen

Diese Daten werden von dem IRAS-Gefahrenmeldesystem nicht erhoben bzw. gespeichert.

Browserdaten

Diese Daten werden von dem IRAS-Gefahrenmeldesystem nicht erhoben bzw. gespeichert.

Log-In Daten

Um den Nutzer im System eindeutig zu identifizieren, muss das IRAS-Gefahrenmeldesystem den Benutzernamen und das zugehörige Passwort speichern. Das Passwort wird verschlüsselt abgelegt.

Des Weiteren wird die IP-Adresse gespeichert um das System vor diversen Angriffsszenarien zu schützen.

Cookies

Cookies dienen der Speicherung technisch notwendiger Informationen. Das IRAS-Gefahrenmeldesystem nutzt die Cookie-Technologie ausschließlich zur Speicherung der SessionID, damit das IRAS-Gefahrenmeldesystem das aktuelle Browserfenster identifizieren kann und Inhalte korrekt angezeigt werden. Wenn Sie Cookies durch Ihren Browser verbieten, kann das IRAS-Gefahrenmeldesystem die Webseiten nicht korrekt darstellen und ein Login ist nicht mehr möglich. Es werden keine Cookies von Drittanbietern gespeichert, verwendet oder ausgewertet. Nach ausloggen des Benutzers ist das erzeugte Cookie ungültig und kann gelöscht werden (Browsereinstellung).

Ereignisdaten

Neben den Daten der Gefahrenmeldezentrale werden auch einzelne Handlungen (Einstellungen und Bedienungen) der Nutzer gespeichert. Diese sind auch für andere Nutzer einsehbar. Es werden Daten wie Login Zeitpunkt, Bedienhandlungen und Konfigurationsänderungen erhoben, gespeichert und angezeigt und mit dem ausführenden Benutzer verknüpft.

E-Mail-Adresse

Für eine Meldung der Ereignisse (Feuer, Störung, usw.) gibt es die Option der Versendung einer E-Mail mit der Laufkarte im Anhang. Dazu benötigt das IRAS-Gefahrenmeldesystem die Zugangsdaten zu einem E-Mail-Provider. Das Passwort wird im Klartext auf dem IRAS-

SECURE-Gefahrenmeldesystem abgelegt, es ist jedoch für keinen Nutzer sichtbar (auch nicht für den Admin nach der Eingabe). Jeder Empfänger einer solchen E-Mail wird in der Datenbank des IRAS-Gefahrenmeldesystems hinterlegt und gespeichert. Eine Auswertung der Daten außerhalb des IRAS-Gefahrenmeldesystems erfolgt nicht und wird auch zu keiner Zeit erfolgen.

Dateizugriff

Es besteht die Möglichkeit, Dateien wie Bilder und Dokumente (PDFs) hochzuladen. Diese können dann als verlinkte Dateien zu Ereignissen von den unterschiedlichen Endgeräten heruntergeladen werden. Dazu gewährt das IRAS-SECURE-Gefahrenmeldesystem, je nach Benutzerberechtigung, Zugriff auf diese hochgeladenen Dateien.

Mobilgeräte

Um eine Push-Benachrichtigung auf dem mobilen Endgerät vorzunehmen ist es notwendig, dass Daten wie eine eindeutige Geräte-ID, der Push-Token für Push-Benachrichtigungen und das verwendete Betriebssystem (Android, Windows, iOS) gespeichert werden. Zur Übermittlung der Push-Benachrichtigung auf das Endgerät, wird der Push-Token mit dem erstellten Text des IRAS-Gefahrenmeldesystems an den Push-Dienst-Betreiber weitergeleitet. Für den Datenschutz ist der Push-Dienst-Betreiber zuständig.

Kontaktdaten und Systeminformationen

Zur Erstellung einer Checkliste werden die vollständigen Kontaktdaten (Name, Straße, Hausnummer, Postleitzahl, Telefonnummer, Faxnummer, Gebäudebezeichnung) von Ansprechpartner und Betreiber benötigt. Diese werden ausschließlich zur Unterstützung der Wartung verwendet. Die Daten werden archiviert und sind auch rückwirkend verfügbar.

Löschen

Die Hauptaufgabe des IRAS-SECURE-Gefahrenmeldesystems besteht in der Aufzeichnung und der Sammlung von Daten. Das Löschen dieser Daten würde evtl. bestehende Vorschriften verletzen und ist daher nur eingeschränkt möglich. Das vollständige Löschen der Daten, kann nur im Rahmen eines Werksresets oder des Entfernens des gesamten Projekts erfolgen.

Update-Server

Wird die Option Update-Server genutzt, werden zur Kontaktaufnahme Daten wie IP-Adresse und Zugriffszeit erhoben und für 62 Tage gespeichert. Zur Steuerung der Updateverfügbarkeit für das individuelle IRAS-Gefahrenmeldesystem, werden Daten wie Mac-Adresse, aktuelle Firmwarestände und das Branding des Systems erhoben und dauerhaft gespeichert. Diese Daten werden ausschließlich zur internen Verarbeitung genutzt und sind notwendig für eine normale Funktion des Systems. Auf diese Daten haben Dritte keinen Zugriff und eine Weitergabe ist ausgeschlossen. Es werden keine personenbezogenen Daten erhoben.

IFAM-Push-Server

Der IFAM-Push-Server dient zur Verteilung sog. Push-Nachrichten auf Mobilgeräte. Dabei stellt der IFAM-Push-Server nur einen Vermittler dar. Dieser empfängt die Nachrichten des IRAS-Gefahrenmeldesystems und sendet diese an den Push-Dienst des Betriebssystemherstellers. Dazu benötigt der IFAM-Push-Server den gerätespezifischen "Token", das Betriebssystem des Gerätes und den Nachrichtentext (z.B.: "Feuer Melder 1-1/1"). Diese Werte werden nicht dauerhaft gespeichert, sondern nur temporär für die verarbeitende Zeit. Zur Kontaktaufnahme werden Daten wie IP-Adresse und Zugriffszeit erhoben und für 62 Tage gespeichert. Es werden keine personenbezogenen Daten erhoben.

Dokumentations-Server

Wird die Option Dokumentations-Server genutzt, werden zur Kontaktaufnahme Daten wie IP-Adresse und Zugriffszeit erhoben und für 62 Tage gespeichert. Zur Steuerung der Dokumentationsverfügbarkeit für das individuelle IRAS-Gefahrenmeldesystem werden Daten wie Mac-Adresse, aktuelle Firmwarestände und das Branding des Systems erhoben und dauerhaft gespeichert. Diese Daten werden ausschließlich zur internen Verarbeitung genutzt und sind notwendig für eine normale Funktion des Systems. Auf diese Daten haben Dritte keinen Zugriff und eine Weitergabe ist ausgeschlossen. Es werden keine personenbezogenen Daten erhoben.

26 Support/Unterstützungszeitraum

Die IFAM GmbH Erfurt gewährleistet für das IRAS-SECURE-Gefahrenmeldesystem technische Unterstützung für den Zeitraum von **7 Jahren ab Lieferdatum**.

Angaben zum für Ihr Gerät zutreffenden Unterstützungszeitraum finden Sie auf den Lieferinformationen an der Innenseite des Gehäuses des IRAS-SECURE-Gefahrenmeldesystems.

➞ *Siehe Kapitel 4.8 Systemaufbau.*

27 Entsorgung



Die im Lieferumfang enthaltenen Geräte, die Verpackung sowie alle mitgelieferten Zubehör- und Anschlussteile gehören nicht in den Hausmüll. Entsorgen Sie die Produktbestandteile getrennt nach den jeweils geltenden nationalen und regionalen Vorschriften:

- Verpackung,
- elektronische/elektrische Bauteile,
- Anschlussteile,
- Akkus/Batterien.

Innerhalb der EU sind die Bestimmungen der Richtlinie 2008/98/EG sowie der Änderungs-Richtlinie 2018/851/EU zu beachten.

Elektro-/Elektronikgeräte

Gemäß der WEEE-Richtlinie 2012/19/EU des Europäischen Parlaments und des Rates vom 4. Juli 2012 sowie dem Gesetz der Bundesrepublik Deutschland über das Inverkehrbringen, die Rücknahme und die umweltfreundliche Entsorgung von Elektro- und Elektronikgeräten vom 20. Oktober 2015 sind Elektro- und Elektronik-Altgeräte der Wiederverwertung zuzuführen und dürfen nicht im Hausmüll entsorgt werden.

Akkus/Batterien

Nutzen Sie die offiziellen Sammelstellen der Kommunen und Entsorgungsunternehmen.

Für eine Entsorgung außerhalb der EU informieren Sie sich bitte über die jeweils geltenden Bestimmungen.

28 Gewährleistung und Garantie

Für die gelieferten Geräte und Komponenten (Hard- und Software) gilt die gesetzlich geregelte Gewährleistungsfrist von 12 Monaten.

Weitere Informationen/Festlegungen enthalten die Verkaufs- und Lieferbedingungen der Firma IFAM GmbH Erfurt bzw. die in den individuellen Verträgen niedergelegten Vereinbarungen.

29 Kontakt und Kundenservice

Bei Fragen zu den Geräten, deren Montage, Installation und Betrieb oder zu weiteren Produkten wenden Sie sich bitte über die untenstehenden Kontaktmöglichkeiten an uns.

IFAM GmbH Erfurt
Gustav-Weißkopf-Straße 9
D-99092 Erfurt

Kundendienst/Technik

Tel. 0049 (361) 659 11-**29** oder -**30** oder -**31**
service@ifam-erfurt.de

Vertrieb

Tel. 0049 (361) 659 11-**13** oder **62**
vertrieb@ifam-erfurt.de

Sie haben die Möglichkeit, von der IRAS-Website aus, mit unserem Kundendienst in Kontakt zu treten. Dort können u.a. Mitteilungen zu Störungen und Anfragen zur technischen Unterstützung versendet werden.

➡ [Siehe Kapitel 9.3.4.1.8 Support und Feedback.](#)

30 Urheberrecht

Alle Rechte an dieser Anleitung und an den ggf. zugehörigen Dokumenten liegen bei der IFAM GmbH Erfurt. Die Unterlagen werden dem Empfänger nur zum persönlichen Gebrauch zur Verfügung gestellt.

Vervielfältigung jeglicher Art (elektronisch oder mechanisch), Übersetzungen in andere Sprachen, auch von Teilen dieser Anleitung, sind nur mit schriftlicher Genehmigung gestattet.

Dritten Personen dürfen Inhalte dieser Anleitung nicht zur Kenntnis gebracht oder zugänglich gemacht werden.

31 Lizenzhinweise

31.1 Pico]OS

Auf den Geräten *ADP4000IRAS* und *IRAS-SECURE-Industrie-PC* wird das Betriebssystem pico]OS verwendet. Dafür gelten die folgenden Lizenzbedingungen:

Copyright (c) 2004-2006, Dennis Kuschel, Swen Moczarski. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR „AS IS“ AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

31.2 Weitere Lizenzen

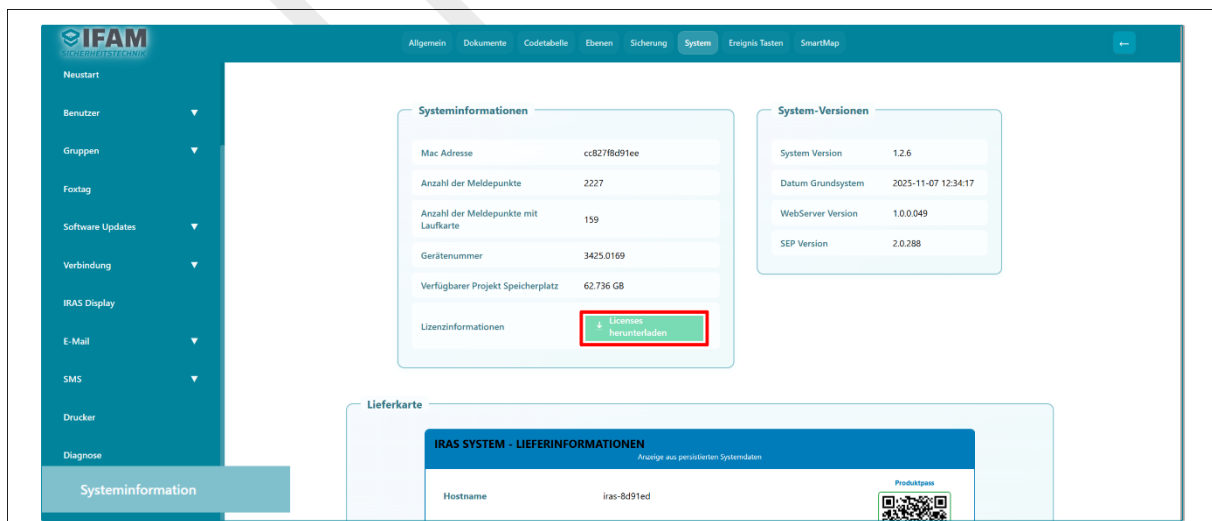


Abbildung 149: IRAS-Website – Lizenzen

IRAS-SECURE stellt Informationen zu weiteren Lizenzen auf der IRAS-Website zum Download bereit.

1. Wählen Sie in der Menüleiste die Option SETUP. → Der Setup-Bereich wird geöffnet.
2. Wählen Sie in der Menüleiste den Eintrag SYSTEM.
3. Wählen Sie den Eintrag SYSTEMINFORMATION.
4. Aktivieren Sie im Bereich LIZENZINFORMATIONEN die Funktion LICENSES HERUNTERLADEN. → Eine Datei **iras sub licenses cache.txt** wird im Downloadbereich abgelegt. Diese enthält Informationen zu allen verwendeten Lizenzen und deren rechtlichen Bestimmungen.

32 Glossar

Terminus	Beschreibung
Browser	Programm zur Darstellung von Webseiten.
Client	Programm oder Dienst, das/der Dokumente von Webservern lädt und anschließend darstellt oder anderweitig auswertet und Funktionen von Webservern nutzbar macht.
Fehler	Nicht korrektes Funktionieren einer Hardware aufgrund eines materiellen Defekts am Gerät oder dessen Zubehör.
Gefahrenmeldeanlage	Klasse von Anlagen/Systemen, die der Feststellung und Meldung von Gefahren dienen (z.B. Brandmeldeanlage, Einbruchmeldeanlage).
Gefahrenmeldezentrale	Klasse von Geräten, die Gefahrenmeldeanlage steuern, Meldungen empfangen, verarbeiten, anzeigen und ggf. weiterleiten (z.B. Brandmelderzentrale, Brandwarnzentrale, Einbruchmeldezentrale).
http	Kommunikationsprotokoll im World Wide Web, bei dem die Daten unverschlüsselt übertragen werden.
HTTPS	Kommunikationsprotokoll im World Wide Web, bei dem die Daten verschlüsselt übertragen werden.
IP-Adresse	Spezifische Geräteadresse in Computernetzen. Sie muss in dem jeweiligen Netz eindeutig sein.
LAN	Computernetzwerk in einem begrenzten Bereich.
Meldepunkt	Definierte Einheit innerhalb einer Gefahrenmeldeanlage, die Ereignisse detektiert (z.B. Feuer, Störung) und Meldungen darüber an eine Melde-Empfangseinheit sendet (z.B. GMZ, FAT, ABT, IRAS-SECURE). Meldepunkte können, je nach Organisationsebene und Funktion, u.a. einzelne Gefahrenmelder (<u>MELDER</u>), aber auch Meldergruppen (<u>GRUPPEN</u>) oder Steuerungsgruppen sein.
Push-Benachrichtigung	Dienst, den die Betriebssystem-Anbieter bereitstellen. Damit können Nachrichten mit diversem Inhalt an die mobilen Geräte versendet werden.
Session	Eine aktive Verbindung eines Clients mit dem Server. Sie wird meist durch einen eindeutigen und nicht replizierbaren Index gekennzeichnet. Sie startet mit dem Login und endet mit dem Logout oder nach Ablauf einer definierten Zeit.
SSL	Technologie zur sicheren Verschlüsselung von Informationen.
Störung	Abweichendes/unkorrektes Verhalten eines Gerätes oder Systems aufgrund einer Dysfunktion (z.B. gestörte Spannungsversorgung, gestörte Datenübertragung).
VPN	VIRTUELLES-PRIVATES-NETZWERK (VPN) bezeichnet eine Technologie, bei der sich Geräte in einem eigenen Netzwerk befinden. Dieses virtuelle Netzwerk ist durch Verschlüsselung vor Zugriffen durch Dritte gesichert.
Webserver/Server	Programm oder Dienst, das/der Dokumente an Webbrowser überträgt.

Tabelle 9: Glossar

33 Abkürzungsverzeichnis

Abkürzung	Bedeutung/Bezug
BMA	Brandmeldeanlage
BMZ	Brandmelderzentrale
GMA	Gefahrenmeldeanlage
GMZ	Gefahrenmeldezentrale

Tabelle 10: Abkürzungsverzeichnis

34 Anhang

34.1 Geräte-/Montagemaße

34.1.1 IRAS-Secure – Montagemaße – Gehäuse/Wandmontage

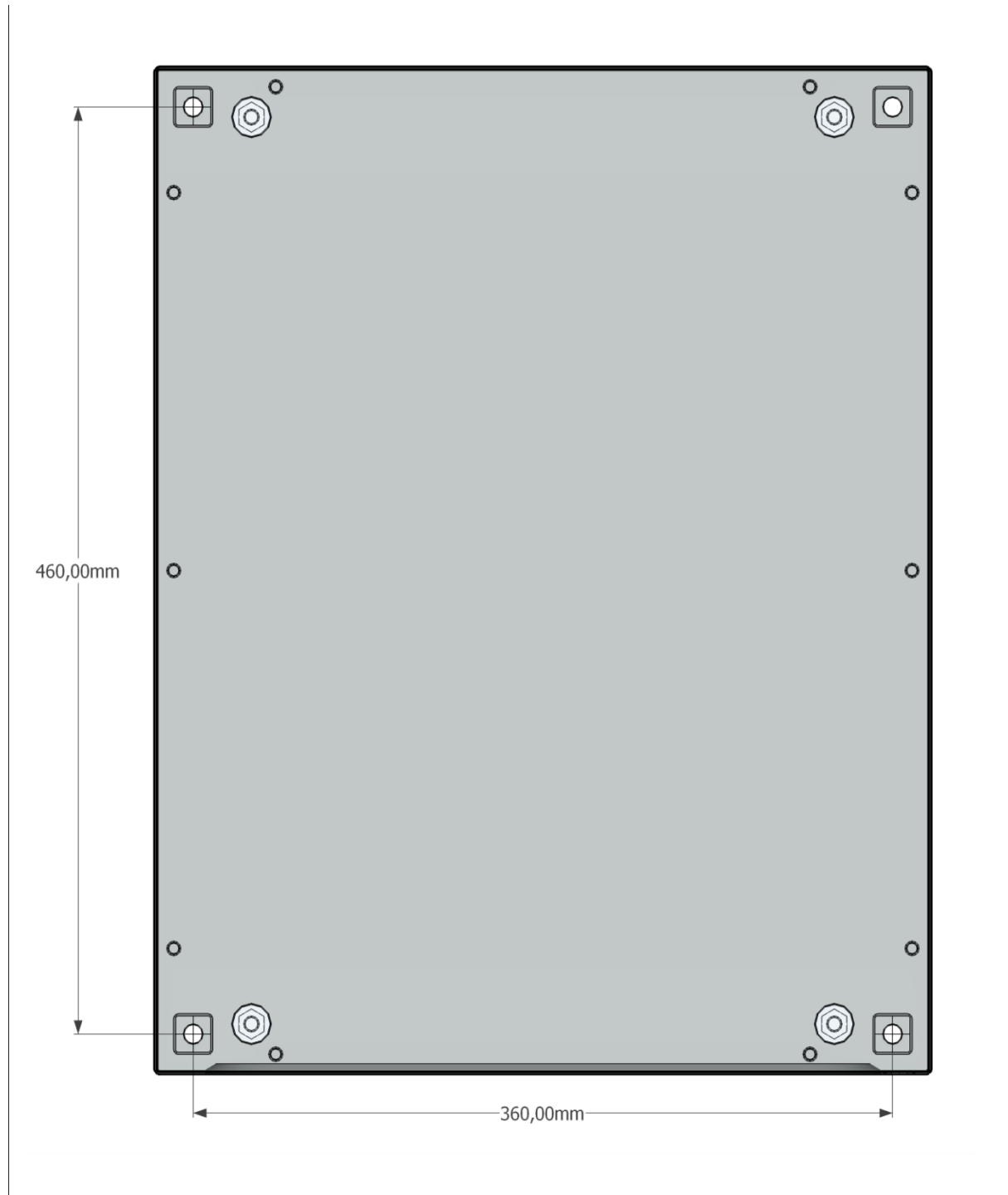


Abbildung 150: IRAS-SECURE – Gehäuse/Wandmontage Maßzeichnung (Vorderansicht)

34.1.2 IRAS-Secure – Gehäuse/Wandhalterung

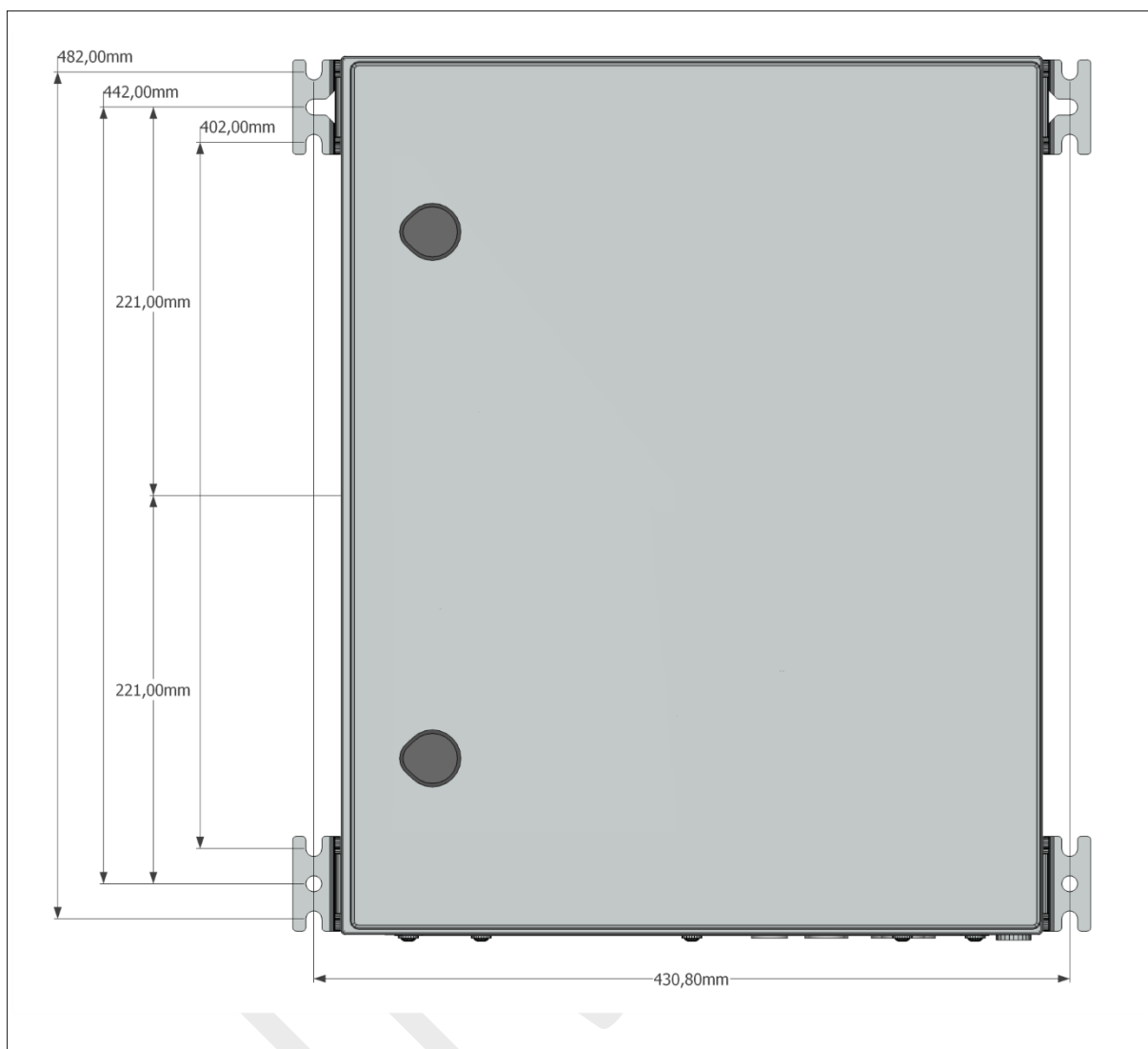


Abbildung 151: IRAS-SECURE – Gehäuse/Wandhalterung, Bemaßung (Vorderansicht)

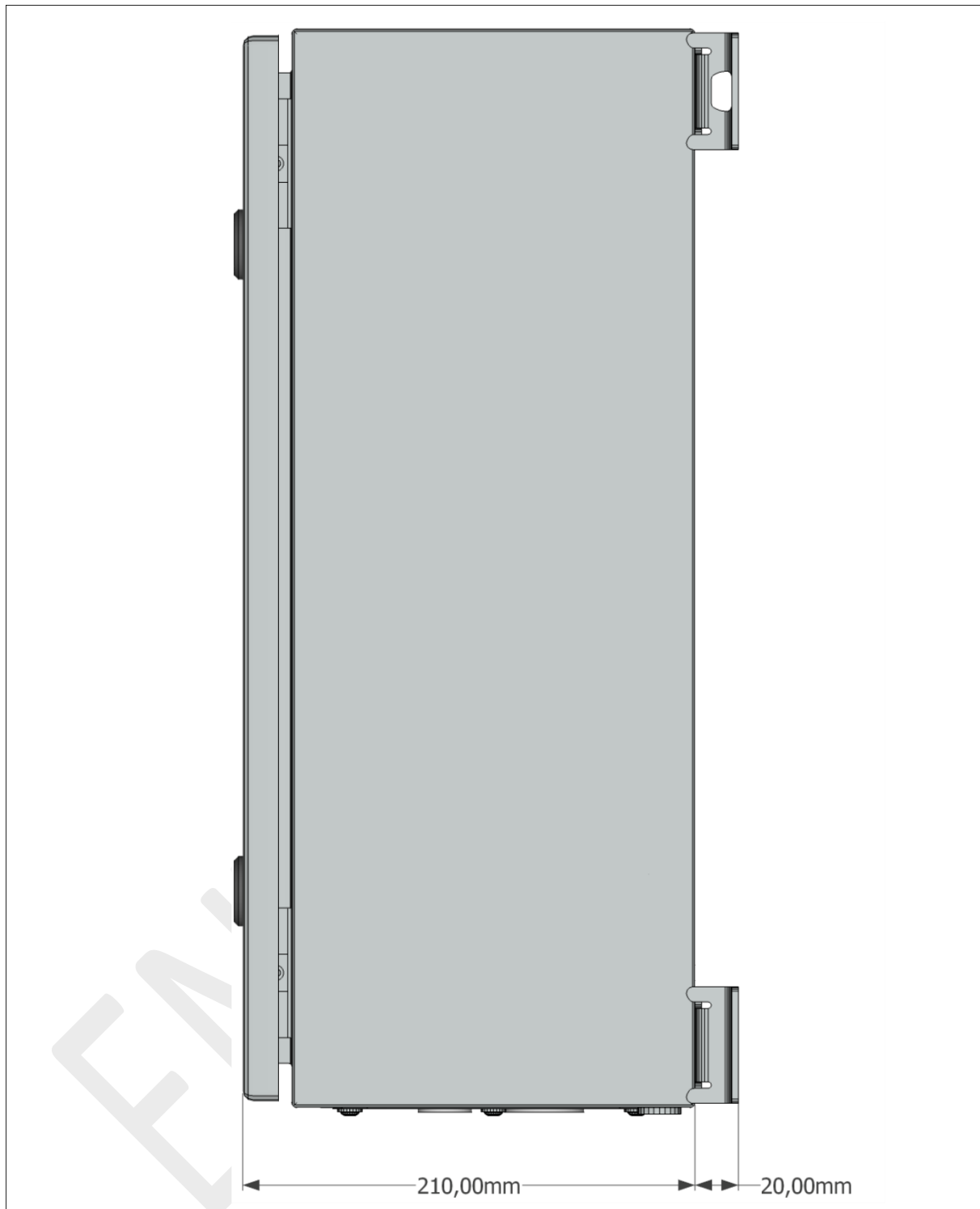


Abbildung 152: IRAS-SECURE – Gehäuse/Wandhalterung, Bemaßung (Seitenansicht)

34.2 CE-Konformitätserklärung

INGENIEURBÜRO FÜR DIE ANWENDUNG
DER MIKROELEKTRONIK IN DER SICHERHEITSTECHNIK

EU-Konformitätserklärung
EC-Declaration of Conformity



IFAM GmbH Erfurt
Gustav-Weißkopf-Straße 9
99092 Erfurt
Tel.: +49 (0) 361 659 11 - 0
Fax: +49 (0) 361 659 11 - 99
ifam@ifam-erfurt.de
www.ifam.com

Dokumenten-Nummer / Document No	DOC 2026-0005
Hersteller / Manufacturer	IFAM GmbH Erfurt
Adresse / Address	Gustav-Weißkopf-Straße 9 99092 Erfurt Germany
erklären, in alleiniger Verantwortung, dass das Produkt / declare, under its sole responsibility that the product	
Produkt-Bezeichnung / Product name	IFAM Remote Access System Plus
Baugruppen-Bezeichnung Assembly Designation	Erläuterung explanation
IRAS-SECURE	IFAM Remote Access System - SECURE
IRAS-SECURE-500	Softwareerweiterung
IRAS-SECURE-Max	Softwareerweiterung
IRAS-SECURE-Mobile	Hard- und Softwareerweiterung
IRAS-SECURE-Druck	Softwareerweiterung
IRAS-SECURE-Drucksystem	Hard- und Softwareerweiterung, mit Sonder-Bedienfeld
IRAS-SECURE-Dienste	Softwareerweiterung
IRAS-SECURE-Display	Softwareerweiterung für 5 Displays
IRAS-SECURE-Betriebsbuch	Softwareerweiterung
IRAS-SECURE-Connect-1-Jahr	Softwareerweiterung
IRAS-SECURE-Connect-5-Jahr	Softwareerweiterung
IRAS-SECURE-Connect-Flat	Softwareerweiterung
IRAS-SECURE-Erkunden	Softwareerweiterung
IRAS-SECURE-EMA-TELENOT	Hard- und Softwareerweiterung
IRAS-SECURE-USV	Hard- und Softwareerweiterung
IRAS-SECURE-Mobile-Redundant	Hard- und Softwareerweiterung
IRAS-SECURE-Display-Lite	Softwareerweiterung
IRAS-SECURE-Display-Control	Hard- und Softwareerweiterung

Geschäftsführer:
Stefan Winter
Amtsgericht Jena HRB 100648
USt-IdNr.: DE 150103499





IFAM GmbH Erfurt
Gustav-Weißkopf-Straße 9
99092 Erfurt
Tel: 0361 65911-0, Fax: -99

Bank-Verbindung:
Deutsche Bank Konto 1309350 BLZ 820 700 24
IBAN: DE 86 8207 0024 0130 9350 00
B.I.C.: DEUTDE33HAN

Abbildung 153: IRAS-SECURE – CE-Konformitätserklärung 1

INGENIEURBÜRO FÜR DIE ANWENDUNG
DER MIKROELEKTRONIK IN DER SICHERHEITSTECHNIK



entspricht bei bestimmungsgemäßer Verwendung den folgenden Produktspezifikationen und -vorschriften den grundlegenden Anforderungen / When used as intended, it complies with the following product specifications and requirements in accordance with the essential requirements

EMC Directive 2014/30/EU

Nr. No	Angewandte Norm(en) Applied standard(s)	Inhalt content
1	DIN EN IEC 61000-6-1:2019-11	Fachgrundnorm Störfestigkeit Wohnbereich
2	DIN EN IEC 61000-6-2:2019-11	Fachgrundnorm Störfestigkeit Industrie
3	DIN EN IEC 61000-6-3:2022-06	Fachgrundnorm Störaussendung Wohnbereich
4	DIN EN IEC 61000-6-4:2020-09	Fachgrundnorm Störaussendung Industrie
5	DIN EN 55032:2022-08	EMV- Anforderungen an die Störaussendung
6	DIN EN 55035:2018-04	Störfestigkeit – Grenzwerte und Prüfverfahren
7	DIN EN 50130-4:2015-04	EMV Störfestigkeit Brand- Einbruch und Hilferuf

Low Voltage Directive 2014/35/EU

8	DIN EN IEC 62368-1:2025-01	Einrichtungen für Audio/Video-, Informations- und Kommunikationstechnik - Teil 1: Sicherheitsanforderungen
---	----------------------------	--

RoHS-Richtlinie 2011/65/EU

9	DIN EN IEC 63000:2019-05	Gefährliche Stoffe in Elektro- und Elektronikgeräten
---	--------------------------	--

IFAM GmbH Erfurt
Gustav-Weißkopf-Strasse 9
99092 Erfurt
Tel.: 0361 65911-0, Fax: -99

Erfurt, 19.08.2026

Stefan Winter

Geschäftsführer / Managing Director

Ort und Datum Name / Unterschrift

Place and date

Name and signature

Geschäftsführer:
Stefan Winter
Amtsgericht Jena HRB 100648
USt-IdNr.: DE 150103499



Bank-Verbindung:
Deutsche Bank Konto 1309350 BLZ 820 700 24
IBAN: DE 86 8207 0024 0130 9350 00
B.I.C.: DEUTDE33HAN

ENTWURF