



*INGENIEURBÜRO FÜR DIE ANWENDUNG  
DER MIKROELEKTRONIK  
IN DER SICHERHEITSTECHNIK*



**Webbasierende Gefahrenmeldungen**

**IRAS-Basic**

**IRAS-Basic-Print**

**IRAS-Plus**

**IRAS-Plus-Mobile**

**IRAS-Wartungsbox**

**IRAS-Sync-Server**

---

<b>Inhalt</b>	<b>Seite</b>
1 Einführung .....	5
2 Fernzugriff auf Brandmeldeanlagen .....	6
2.1 Vorteile dieser Technologie und deren Anwendung.....	6
2.2 Lösungen .....	6
2.2.1 Cloud-basierende Lösungen .....	6
2.2.2 Nicht-Cloud-basierende Lösungen.....	7
2.2.3 Remote-Services .....	7
2.3 Anwendungen.....	8
2.4 Fernzugriff nach DIN VDE 0833-1 .....	8
2.5 Anforderungen an das Bedien-Personal .....	10
2.5.1 Elektrofachkraft GMA.....	10
2.5.2 Eingewiesene Person GMA.....	10
3 Empfehlungen für Betreiber, Errichter und Feuerwehr .....	11
4 IRAS-Basic / IRAS-Basic-Print .....	12
4.1 Die Schnittstelle zur BMZ.....	12
4.2 Die Anbindung der IRAS-Server-Box.....	12
4.3 Die Endgeräte.....	12
4.4 Bestandteile von IRAS-Basic/IRAS-Basic-Print .....	13
4.4.1 Der Redundanzadapter als Gateway .....	13
4.4.2 Das Feuerwehr-Anzeigetableau als Gateway .....	13
4.4.3 Die Prozessor-Baugruppe als Gateway .....	13
4.4.4 Die IRAS-Server-Box .....	13
4.4.5 Das Programm IRAS-Basic/IRAS-Basic-Print.....	14
4.4.6 Die Browser-Darstellung .....	14
4.4.7 Die App-Darstellung.....	14
4.4.8 Die Endgeräte und Betriebssysteme.....	15
4.4.8.1 Tablet-PC und Smartphone.....	15
4.4.8.2 Android-Endgeräte .....	15
4.4.8.3 Apple-Endgeräte .....	15
4.4.8.4 Betriebssysteme.....	15
4.4.8.5 Betriebssystem Android.....	15
4.4.8.6 Betriebssystem iOS.....	15
4.4.8.7 Betriebssystem Windows 10 .....	16
4.4.8.8 Andere Technologien .....	16
4.5 Darstellungen.....	16
4.5.1 Browser-Darstellung .....	16
4.5.2 App .....	16
4.5.3 FAT-Bedieneroberfläche .....	17
4.5.4 FBF-Bedieneroberfläche.....	17
4.5.5 Darstellung der Feuerwehr-Laufkarte .....	17
4.5.6 BMZ-Übersicht .....	18
4.5.7 Ereignisspeicher / Historie .....	18
4.5.8 Wartungsmode / Revision.....	18
4.5.9 USB-Schnittstelle .....	19
4.5.10 Benutzerverwaltung / Berechtigungsstufen .....	19
4.5.11 Nutzung von Kameras .....	19
4.5.12 Objektverwaltung.....	19

4.5.13	Sprachen .....	19
4.5.14	Bilder .....	20
4.6	IRAS-Basic2-App .....	20
4.6.1	IRAS-Basic2 .....	20
4.6.2	Grafische Oberfläche Smart Device – iOS (Apple) .....	20
4.7	Sicherheit IRAS .....	21
4.7.1	Schutz der Kundendaten .....	21
4.7.2	Absicherung der Kommunikation .....	21
4.7.3	Schutz der BMZ-Rückwirkung .....	21
4.8	Zugriffsmöglichkeiten auf die IRAS-Server-Box .....	21
4.8.1	Netz mit fester IP, HTTP .....	21
4.8.2	Router mit fester IP, HTTP .....	22
4.8.3	Router mit fester IP, HTTP mit Portweiterleitung .....	22
4.8.4	Router mit dynamischer IP .....	23
4.8.5	Router mit dynamischer IP und Portweiterleitung .....	23
4.8.6	Router, HTTPS (SSL) .....	24
4.8.7	VPN-Server im lokalen Netz, Fernzugriff über VPN .....	24
4.8.8	VPN-Server im WAN .....	25
4.8.9	Verbindung über Mobilfunknetz, VPN .....	25
4.9	Voraussetzungen .....	26
4.9.1	System .....	26
4.10	Übersicht Leistungsmerkmale IRAS-Basic .....	26
4.11	Lieferumfang IRAS-Basic .....	26
5	IRAS-Plus / IRAS-Plus-Mobile .....	27
5.1	Bestandteile .....	28
5.2	Schnittstellen (Slots) .....	28
5.3	Das App IRAS-Basic2 .....	28
5.4	Übersicht erweiterte Leistungsmerkmale .....	29
5.5	Lieferumfang IRAS-Plus / IRAS-Plus-Mobile .....	29
5.5.1	IRAS-Plus .....	29
5.5.2	IRAS-Plus-Mobile .....	29
5.6	Systemvoraussetzungen .....	30
6	IRAS-Wartungsbox .....	31
6.1	Gerät und Funktionen .....	31
6.2	Projektverwaltung und Dokumente .....	32
6.3	Prüfungen .....	33
6.4	Betriebssysteme .....	33
6.5	Einsatzvorteile .....	34
6.6	Leistungsmerkmale / Bedienkonsole .....	35
6.7	Lieferumfang IRAS-Wartungsbox .....	35
7	IRAS-Sync-Server .....	36
8	Störungs- und Wartungsmanagement .....	37
9	Fazit .....	38
10	Ansprechpartner .....	39

## Sehr geehrte Geschäftspartner, Kunden und Interessenten!

Seit Gründung der Firma IFAM GmbH Erfurt vor mehr als 25 Jahren hat es auf dem Gebiet der Sicherheitstechnik, insbesondere im Bereich Brandmeldetechnik eine Reihe bedeutender gesetzlicher Vorschriften und Richtlinien und damit einhergehend vielfältige technische Veränderungen und Fortschritte gegeben.



Moderne Mikroprozessortechnologien ermöglichen mit Hilfe von seriellen Schnittstellen und komplexen Protokollen neue Möglichkeiten im Hinblick auf den anlagentechnischen Brandschutz. Damit verbunden sind Leistungserweiterungen der Brandmelderzentrale (BMZ) auch für die Schnittstellen der Feuerwehrperipherie und die damit verbundenen Geräte.

Mit der Weiterentwicklung der Informationselektronik und den dadurch zur Verfügung stehenden Endgeräten hat in Sachen Mobilität die Gefahrenmeldung einen neuen Stellenwert erhalten.

In den nachfolgenden Ausführungen möchten wir Sie über das Leistungsvermögen sowie über Lösungsmöglichkeiten einer „Webbasierenden Gefahrenmeldung“ informieren.

Neben den normativen Grundlagen ermöglichen wir Ihnen einen Einblick in unser Produkt „IRAS – IFAM Remote Access System“. Dieses System stellt neue Anwendungen der mobilen Gefahrenmeldung für Betreiber, Errichter und Feuerwehr bereit.

**Ihr IFAM-Team**

## 1 Einführung

Brandmeldeanlagen in der Gesamtheit aller dazu notwendigen Geräte und Systeme zählen mit zu dem wichtigsten Bereich der Gefahrenmeldetechnik und bilden die Grundlage für den anlagentechnischen Brandschutz. Um Menschen, Sachwerte sowie die Umwelt vor Feuer und deren Auswirkungen zu schützen, Kosten zu senken und Risiken zu minimieren, wurde diese Technik unverzichtbar und ist ein fester Bestandteil von Genehmigungsverfahren im Baugewerbe.

Das Herzstück einer solchen Anlage ist die Brandmelderzentrale (BMZ). Sie stellt alle wichtigen Funktionen zur Verfügung, um Feuer frühzeitig, sicher und effizient zu detektieren, Menschen zu warnen, automatisch Maßnahmen einzuleiten und Interventionskräfte über die Brandbekämpfung zu informieren.

Eine ganze Reihe von Geräten steht so dem technischen Leiter eines Unternehmens, Mitarbeitern einer Werkfeuerwehr oder dem Einsatzleiter der Berufsfeuerwehr bereit, um vor Ort über die entsprechende Vorgehensweise zu entscheiden.

Dabei wird ein Sachverhalt deutlich – mögliche Brandbekämpfungsmaßnahmen können erst am Einsatzort entschieden werden, da keine detaillierten Informationen in einer ständig besetzten Stelle oder auf dem Einsatzfahrzeug vorliegen. Wichtige Zeit verstreicht. Einsatztaktik, Maßnahmen zum Selbstschutz und verwendete Löschmittel müssen warten.

Mit der Internet-Technologie und den dazu gehörigen Smart Devices können wichtige Informationen viel schneller, aktueller und umfangreicher an eine hilfeleistende Stelle, gleich ob Leitstand oder mobil im Fahrzeug, weitergeleitet werden. Dabei dient diese Technik nicht als Erstinformation! Zusätzlich zur konventionellen Feuermeldung mittels der Übertragungseinrichtung (ÜE) gelangen so frühzeitig wichtige Informationen an entsprechende Personen und ermöglichen schnelles Handeln, verkürzen Reaktionszeiten und können somit entscheidend für einen erfolgreichen Verlauf der Lösch- und Rettungsmaßnahmen beitragen.

Für Betreiber sind zeitnahe und aktuelle Informationen über den Zustand einer Brandmelderzentrale besonders für den organisatorischen Brandschutz und die sich daraus ergebenden Folgemaßnahmen wichtig, zum Beispiel für das Handeln bestimmter Personen im Alarmfall, bei einer Evakuierung oder die Vorgehensweise einer vor Ort befindlichen Werkfeuerwehr.

Auch Errichter von Brandmeldeanlagen (BMA) nutzen Vorteile einer webbasierenden Gefahrenmeldung. Schon während der Inbetriebnahme, vor allem jedoch ab dem Einschaltzeitpunkt kann der Zustand der BMZ ständig aus der Ferne überwacht werden. Alarmer und Störungen können so genau analysiert werden. Auch im Hinblick auf die nach Norm geforderter Wartung können Smart Devices, wie Tablet-PCs genutzt werden und unterstützen die Organisation sowie die Dokumentation und Nachweisführung.

## 2 Fernzugriff auf Brandmeldeanlagen

### 2.1 Vorteile dieser Technologie und deren Anwendung

Mit der Internet-Technologie und entsprechenden mobilen Endgeräten (Smart Devices) können wichtige Informationen aus Brandmelderzentrale (BMZ) an hilfeleistende Stellen, Technikabteilungen oder mobil direkt an einen zuständigen Service-Techniker weitergeleitet werden. Dabei dient diese Technik nicht als Erstinformationsmittel! Zusätzlich zur konventionellen Alarmmeldung durch die Übertragungseinrichtung (ÜE) gelangen so frühzeitig wichtige Informationen an entsprechende Personen und ermöglichen schnelles Handeln, verkürzen Reaktionszeiten und können somit entscheidend zu einem erfolgreichen Verlauf von Rettungs- und Serviceeinsätze beitragen.

Betreibern von Objekten (Endkunde) stehen zeitnahe und aktuelle Informationen über den Zustand ihrer BMA zur Verfügung. Gerade für den organisatorischen Brandschutz und sich daraus ergebenden Folgemaßnahmen ist diese Form der Informationen von Bedeutung, insbesondere für das Handeln verantwortlicher Personen im Ereignisfall (z. B. stiller Alarm in einem Krankenhaus), bei einer Evakuierung oder die Vorgehensweise einer vor Ort befindlichen Werkfeuerwehr. In Übereinstimmung mit einem Brandschutzkonzept können so zusätzlich Lösungen geschaffen werden, die zur Sicherstellung der Schutzziele beitragen. Auch Errichter von Brandmeldeanlagen (BMA) nutzen Vorteile solcher Lösungen. Alarmer, Störungen und Abschaltungen können so genau analysiert werden. Auch im Hinblick auf die nach Norm geforderte Inspektion/Wartung können Programme für mobile Endgeräte, wie Tablet-PCs genutzt werden und unterstützen die Organisation sowie die Dokumentation und Nachweisführung. Weiterhin übernehmen Programme auch den Zugriff auf die BMA, um umfangreiche Servicemaßnahmen zu unterstützen. Zusätzlich dienen diese Lösungen auch zur Personal- und Kostenoptimierung.

### 2.2 Lösungen

Für die technische Umsetzung der Marktanforderungen wird u. a. die Internet-Technologie genutzt. Hierbei unterscheidet man grundsätzlich den Ort von Kunden-Daten und Anwendungs-Software (Programm). Die Cloud-basierende Lösungen (Cloud-Computing - deutsch: Rechnerwolke) beschreiben die Bereitstellung von IT-Infrastruktur wie beispielsweise Speicherplatz, Rechenleistung oder Anwendungssoftware als Dienstleistung über das Internet. Aber auch herstellereigene Lösungen, die mittels Bluetooth-Standards kommunizieren, finden ihre Anwendung.

#### 2.2.1 Cloud-basierende Lösungen

Die Cloud-basierende Lösung nutzt Kommunikationsserver (COM-Server) professioneller Anbieter, die das Routing (IP) und Authentifizierung (ID) der mobilen Endgeräte, das Übertragungsverfahren (Verschlüsselung, z. B. SSL Zertifikat) sowie das Speichern aller Daten (Verbindungsdaten, Kundendaten) und die dazu notwendigen Schutzmaßnahmen (Firewall) übernehmen. Die Programme (Apps) auf den mobilen Endgeräten nutzen das Leistungsvermögen des jeweiligen Betriebssystems. Der an der BMZ befindliche Client-Server sendet bei einer Zustandsänderung der BMA das entsprechende Ereignis an den COM-Server. Das entsprechend registrierte Endgerät (Client) kommuniziert mit dem COM-Server und erhält bei Zustandsänderungen die aktuelle Information. Bestimmte Ereignisse (Alarmer, Service) können über ein WEB-Portal eingesehen werden. In Abhängigkeit von proprietären Protokollen können Möglichkeiten einer Bedienung (BMZ-Bedienfeld) zur Verfügung gestellt werden.

**Vorteile:** Das Programm wird ausschließlich durch Hersteller auf dem COM-Server aktualisiert. Nötige Zertifikate (z. B. Push-Notifikation) werden am COM-Server bereitgestellt und müssen nicht vom Nutzer kontrolliert werden. Eine Anbindung an das IT-Netzwerkes vor Ort ist nicht erforderlich.

**Nachteil:** Die Sicherheit der Daten und die Verfügbarkeit der Dienste ist vom Anbieter des WEB-Servers abhängig. Die Anzahl der mobilen Endgeräte und Menge der Daten (Speicherbedarf) können begrenzt sein. Die Anwendungen lassen sich bei Hinzunahme oder Tausch von mobilen Endgeräten aufgrund der Authentifizierung nur mit Aufwand portieren. Um die Unabhängigkeit vom IT-Netzwerkes des Kunden zu gewährleisten, sind laufende Kosten für Mobilfunk-Verträge notwendig.

### **2.2.2 Nicht-Cloud-basierende Lösungen**

Die Nicht-Cloud-basierende Lösung benötigt keinen COM-Server im eigentlichen Sinne, da die mobilen Endgeräte eine eigene Kommunikation mit dem an der BMA befindlichen WEB-Server aufbauen. Das Übertragungsverfahren kann mittels Verschlüsselung gesichert werden. Der Programm- und Datenspeicher befindet sich in unmittelbarer Nähe der BMZ und verfügt über entsprechende Schutzmaßnahmen. Die Programme (Apps) auf den mobilen Endgeräten nutzen das Leistungsvermögen des jeweiligen Betriebssystems. Mit den Zugangsdaten des mobilen Endgerätes wird das Abfragen (Polling) des WEB-Clients autorisiert. Nach Zustandsänderung der BMA (Ereignis) empfängt der WEB-Client (Endgerät) die entsprechenden Daten. In Abhängigkeit von proprietären Protokollen können Möglichkeiten einer Bedienung (BMZ-Bedienfeld) zur Verfügung gestellt werden.

**Vorteile:** Das Programm sowie die gespeicherten Daten stehen ausschließlich vor Ort dem Kunden zur Verfügung. Der Kunde hat Rechte eines Administrators und vollen Zugriff auf das System. Durch die Einbindung in das IT-Netzwerk des Kunden entstehen keine laufenden Kosten. Die Größe des Speicherbedarfs sowie die Anzahl der mobilen Endgeräte sind nahezu unbegrenzt.

**Nachteil:** Um Zustandsänderungen den Endgeräten mitzuteilen, muss der Client-Server „immer von außen“ erreichbar sein. Sofern keine andere Anschlussmöglichkeit gewählt wurde (separater DSL-Anschluss, LTE-Router), ist die Abstimmung mit der örtlichen IT-Abteilung zwingend erforderlich. Aktualisierungen entsprechender Software muss dem WEB-Server ermöglicht und können mittels eines automatischen Updates bereitgestellt werden. Das bedeutet, das Netzwerk des Kunden für Zugriffe von außen zu öffnen (Port 80, 443) und erfordert besondere Schutzmaßnahmen durch den Kunden (z. B. Subnetz). Zertifikate sind auf dem WEB-Server hinterlegt.

### **2.2.3 Remote-Services**

Für den Remote-Service sind PC-Programme notwendig, die von entsprechenden Herstellern der BMZ zur Verfügung gestellt werden, um aus der Ferne auf eine BMZ zuzugreifen. Diese Lösungen (Programme) besitzen umfangreiche Leistungsmerkmale (Programmierung der BMZ), die mittels gesonderter Übertragungsverfahren, wie Virtuell Privat Network (VPN) einen direkten Zugriff auf eine BMZ besitzen und somit umfassende Änderungen vornehmen können. Eine ständige Zustandsanzeige im eigentlichen Sinn (Ereignisse der BMZ) ist prinzipiell möglich, spielen aber bei diesen Anwendungen eine untergeordnete Rolle. Die Anschaltung eines Service-PCs via VPN an eine BMZ ermöglicht eine zuverlässige und sichere Verbindung und integriert Teile der BMZ in ein geschlossenes Netzwerk. Neben dem PC-Programm für den Service können auch Möglichkeiten einer Bedienung (BMZ-Bedienfeld) zur Verfügung gestellt werden.

## 2.3 Anwendungen

Es sind unterschiedliche Lösungen am Markt vertreten, die sich verschiedener Technologien bedienen, die über Vor- und Nachteile verfügen und dem entsprechend Risiken mit sich führen. Unter zur Hilfenahme einer Gefährdungsbeurteilung sollte grundsätzlich mit den Verantwortlichen (Betreiber, Errichter, Feuerwehr) eine sachliche Beurteilung der Situation vor Ort in Sachen Brandschutz (Schutzziel) und Netzwerk (IT-Sicherheit) vorgenommen werden, um sich für oder gegen eine Lösung zu entscheiden. Eine weitere Variante sind PC-Programme für den Remote-Service von BMZ-Hersteller. Die unter Punkt 2 genannten Lösungen besitzen ihre Berechtigung am Markt und erfüllen die Anforderungen aktueller Normen, deren wichtigste die DIN VDE 0833-1 darstellt. Die darin beschriebenen Funktionen Fernabfrage, Fernsteuerung, Fernreparatur und Fernparametrierung sind aus fachlicher Sicht nicht ganz unbedenklich und sollten genau geprüft werden. Besonders der Stand der Technik bei Sicherheitsnetzwerken, die Applikationen in Hinblick auf in der DIN VDE 0833-1 geforderten Freigabe und Funktionsprüfungen vor Ort sowie der Fernzugriff auf sicherheitstechnische Einrichtungen (z. B. Gefahrenmeldeanlagen) bedürfen besonderer Aufmerksamkeit bei der Planung, Installation und Wartung. Zielsetzung muss es sein, die Eigenschaften der Lösungen abzuwägen um dann für den Einzelfall die richtige Entscheidung zu treffen. Dabei kommt der Umsetzung, vor allem die Anbindung der BMA an den Fernzugriff und somit an fremde Netzwerke eine besondere Bedeutung zu. Möglichkeiten der Konfiguration wären die Trennung in Kunden- und BMZ-Netzwerk, die Nutzung von proprietären Protokollen und der Verzicht bzw. Limitierung von Open-Source-Komponenten. In Abhängigkeit der Gerätefunktionen müssen die Lösungen rückwirkungsfrei sein und dürfen im Sinne der DIN EN 54-13 den Betrieb der Anlage nicht gefährden.

## 2.4 Fernzugriff nach DIN VDE 0833-1

Nachfolgend wird normativ die Möglichkeit beschrieben, worin der Betreiber unter bestimmten Auflagen Instandhaltungsmaßnahmen aus der Ferne durchführen lassen darf. Die nachfolgenden Anmerkungen sind Auszüge aus der DIN VDE 0833-1.

Quelle: DIN VDE 0833-1, Punkt 5.2.2

Bestimmte Instandhaltungsmaßnahmen und Verbesserungen an einer GMA dürfen somit aus der Ferne vom Instandhalter durchgeführt werden. Diese Tätigkeiten können aus Fernabfrage, Fernsteuerung, Fernreparatur und Fernparametrierung bestehen. Das Vornehmen von Änderungen (Modifikationen) ist hierbei erlaubt, wenn

- die Zugangsberechtigung zwischen dem Betreiber und dem Instandhalter schriftlich festgelegt und jeder Zugang zeitlich begrenzt ist,  
**und**
- jeder Zugang zur GMA mit einem der Anlagenart entsprechend qualifizierten Übertragungsverfahren stattfindet,  
**und**
- eine unmittelbare Freigabe vor Ort durch den Betreiber erfolgt,  
**und**
- jeder Zugang zur GMA in einem anlageeigenen Ereignisspeicher automatisch registriert wird und durch den Betreiber im Betriebsbuch vermerkt wird,  
**und**
- jede Änderung (z.B. Software-Stand, Änderung einer Funktion) im Ereignisspeicher der GMA automatisch registriert und im Betriebsbuch vermerkt wird.

Diese durchzuführenden Tätigkeiten dürfen sein:

a) Fernabfrage

- von Meldungs- und Störungszuständen;
- aktueller Betriebszustände, z. B. Abschaltungen bei BMA;
- des Ereignisspeichers;
- des aktuellen Systemzustandes zur Vorbereitung von Inspektion, Wartung oder Instandsetzung;
- zur Feststellung des Ausbaus, z. B. Peripherielemente, oder von Einstellungen oder der eingesetzten Software-Ausgabestände oder der aktuellen Parameter.



b) Fernsteuerung

- zum Rücksetzen von Meldungs- und Störungszuständen nach dem Überprüfen und dem Beseitigen der Ursache vor Ort;
- zum Abschalten von gestörten Betriebsmitteln, wenn sichergestellt ist, dass derartige Abschaltungen vor Ort zur Anzeige gebracht werden und periodisch innerhalb von 25 h – bis zur Wiedereinschaltung dem Instandhalter gemeldet werden.



c) Fernreparatur

- zur Beseitigung von Software-Systemfehlern, sofern dies eine Verbesserung ist und keine Änderung einer geforderten Funktion beinhaltet. Ist die Fehlerbeseitigung, z. B. wegen fehlerhafter Fernübertragung des Software-Updates, nicht möglich, so muss die bisher bestehende Funktion erhalten bleiben.



d) Fernparametrierung

- zur Änderung einer geforderten Funktion. Ist die Änderung, z. B. wegen fehlerhafter Fernübertragung der Versorgungsdaten, nicht möglich, so muss die bisher bestehende Funktion erhalten bleiben. Nach einer Fernreparatur oder Fernparametrierung muss eine Prüfung nach 4.1.6 und Dokumentation im Betriebsbuch erfolgen.



Unter dem Punkt 4, Regeln für das Planen, Errichten, Erweitern und Ändern von GMA steht in der DIN VDE 0833-1 folgende Regeln:

4.1.6 Nach jeder Erweiterung oder Änderung muss unverzüglich die neue geforderte Funktion der GMA durch eine Prüfung nach 4.1.5 nachgewiesen werden. Diese Prüfung darf sich auf die von der Erweiterung bzw. Änderung betroffenen bzw. beeinflussten Betriebsmittel der vorhandenen Anlage sowie auf die neu hinzugekommenen Betriebsmittel beschränken. Außerdem müssen die Ausführungsunterlagen, insbesondere die Anlagebeschreibung, auf den neuesten Stand gebracht werden.

4.1.5 Vor Inbetriebnahme der GMA ist durch eine Elektrofachkraft GMA eine Abnahmeprüfung durchzuführen. Sie umfasst:

- a) die Sicht- und Funktionsprüfung der in Betrieb gesetzten GMA in allen Teilen;
- b) die Prüfung auf Vollständigkeit der für den Betrieb der GMA erforderlichen Dokumente
- c) das Abnahmeprotokoll mit Unterschrift der für die Abnahmeprüfung Verantwortlichen.

## **2.5 Anforderungen an das Bedien-Personal**

Grundsätzlich sind die Anforderungen an das Bedien-Personal von Gefahrenmeldeanlagen in der DIN VDE 0833-1 beschrieben. In Bezug auf den Fernzugriff sind vom Betreiber (Endkunde) und der Instandhaltungs-/Wartungsfirma jedoch besondere Vereinbarungen zu treffen (siehe Hinweise Punkt 6). Die Aufgabenstellungen des Technikers (Elektrofachkraft, Service) und der vor Ort eingewiesenen Person (z. B. Haustechniker, Hausmeister) sind besondere Beachtung einzuräumen und schriftlich zu fixieren. Das betrifft besonders das Freischalten des Fernzugriffs zur BMA, Prüfung und Dokumentation. Weiterhin muss sichergestellt sein, dass der Fernzugriff auf die BMA einer eindeutigen Identifizierung bzw. Autorisierung des Bedien-Personals unterliegt und Bedien-Vorgänge protokolliert werden müssen.

### **2.5.1 Elektrofachkraft GMA**

Elektrofach ist eine Person, die aufgrund ihrer fachlichen Ausbildung (Nachrichten-, Informations-, Mikroprozessor-, Mess-, Regel- oder der allgemeinen Elektrotechnik), Kenntnisse und Erfahrung die ihm übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann. Darüber hinaus müssen grundlegende interdisziplinäre Erfahrungen über alle zuvor genannten Fachgebiete hinweg und Systemkenntnisse der Gefahrenmeldetechnik seitens der Norm vorhanden sein.

### **2.5.2 Eingewiesene Person GMA**

Eine eingewiesene Person wurde in den Betrieb eine Gefahrenmeldeanlage in bestimmter Weise geschult und kann die ihm übertragenen Aufgaben selbstständig und eigenverantwortlich durchführen, einschließlich aller Dokumentationen. (Mängel ins Betriebsbuch, Meldung an die Fachfirma)

### 3 Empfehlungen für Betreiber, Errichter und Feuerwehr

Vor der Wahl sollte eine Gefährdungsbeurteilung (Risikoanalyse) im Hinblick auf:

- Brandschutzziel,
- IT-Infrastruktur,
- Sicherheit der Kundendaten,
- Anforderungen an die Instandhaltung und Wartung,
- Forderungen der örtlichen Brandschutzbehörde (TAB) durchgeführt werden.

Führt das Ergebnis zum Einsatz einer oben beschriebenen Lösung, sind folgende Sachverhalte zu beachten:

- Erweiterung der BMA nach DIN VDE 0833-2
  - BMZ (Liste Anlageteile, Pos. 6.5.3)
- Erweiterung der BMA im Instandhaltungs-/Wartungsvertrages
  - gesonderte Nutzungsvereinbarung
- Inhalt der Nutzungsvereinbarung für den Fernzugriff
  - Hinweis auf gesicherte Verbindung, qualifizierter Übertragungsweg (DIN EN 50136)
  - Überwachung der ÜW auf Verbindungsausfall
  - Authentifizierung und Speicherung aller Vorgänge (z. B. Person, Datum, Uhrzeit)
  - eingewiesene Fachkraft (vor Ort) festlegen
  - Benennen einer Rückfallebene (Datensicherung, Notfallplan, Backup)
- Nutzung z. B.
  - zur Störungsanzeige, Fehleranalyse und zusätzliche Alarmanzeige
  - zur Vorbereitung der Instandhaltungsarbeiten (z.B. Verschmutzungsgrad)
  - zur Entscheidungsfindung für die Einsatztaktik (Werkfeuerwehr, Feuerwehr)
- Hinweis auf rechtsgültige Normen
  - DIN 14675-1
  - DIN VDE 0833-1
  - DIN EN 50136
  - DIN EN 50710
- Besonderheiten festlegen, z. B.:
  - Abweichung von der Norm (z. B. keine /eingeschränkte Vor-Ort-Freigabe für bedingten rückwirkungs-freien Zugriff auf Grundfunktionen z. B. Reset, Netzstörung, auslesen von Zustandsdaten)
  - Parametrierung nur bei einer eingewiesenen Fachkraft für GMA vor Ort
- Beschreibung
  - Systemvoraussetzungen
  - Benutzerverwaltung/Zugriffsrechte
  - Mögliche Anbindung über örtliche IT
  - Leistungsmerkmale und Dokumentation
- Datenschutzerklärung
  - Wer erhebt die Daten der Anlage
  - Welche Daten werden ausgelesen / gespeichert
  - Wo werden die erhobenen Daten gespeichert
  - Wofür werden die erhobenen Daten genutzt
  - Wie wird die Datenerhebung dokumentiert
- Verwendung von rechtlich bedenklichen Begrifflichkeiten
  - System zur Fernwartung der BMA
  - zur Störmeldeweiterleitung an eine ständig besetzte Stelle nach DIN

## **4 IRAS-Basic / IRAS-Basic-Print**

Die webbasierende Gefahrenmeldung mit der Bezeichnung IRAS-Basic (IFAM Remote Access System) nutzt moderne Kommunikationswege und deren Endgeräte. Alarmer, Störungen, Abschaltungen sowie frei definierbare Kategorien können aus der Gefahrenmeldeanlage (GMA), insbesondere aus der Brandmelderzentrale (BMZ) unabhängig vom Hersteller mit Hilfe einer Browser-Darstellung sowie als Applikation (App) angezeigt werden. Alle Ereignisse werden auf den Endgeräten signalisiert und grafisch aufbereitet dargestellt. Verbunden mit dem jeweiligen Ereignis können Zusatzinformationen an das Endgerät übertragen und angezeigt werden. IRAS-Basic-Print besitzt zusätzlich das Leistungsmerkmal, Feuerwehr-Laufkarten auf im Netzwerk befindliche Drucker (PDF-Print-Format) auszudrucken.

### **4.1 Die Schnittstelle zur BMZ**

Ausgangsbasis ist die Schnittstelle der BMZ für die Feuerwehrperipherie. Hier werden die entsprechenden Daten (BMZ / Meldergruppe / Melder) bereitgestellt. Um diese Informationen in der IRAS-Server-Box verarbeiten zu können, sind Gateways notwendig, die als Protollübersetzer dienen. Diese Aufgaben können die Redundanzbaugruppen (ADP), das Feuerwehr-Anzeigetableau (FAT) oder auch die Prozessorbaugruppe (IMT4CPU) übernehmen.

### **4.2 Die Anbindung der IRAS-Server-Box**

Grundlage der webbasierenden Gefahrenmeldung ist die IRAS-Server-Box. Dieser Industrie-PC empfängt die Daten aus der BMZ über das entsprechende Gateway, verknüpft die Meldungen mit den Objektdaten und stellt diese mittels Web-Server an die dafür autorisierten Endgeräte bereit. Alle kundeneigenen Daten sind auf der IRAS-Server-Box vor Ort im Zuständigkeitsbereich des Kunden! Wichtige Voraussetzung ist hierfür die direkte Erreichbarkeit der IRAS-Server-Box aus dem Internet. Dafür ist der optimale Weg eine separate DSL-Anbindung (DSL-Router / Modem) mit einer festen IP-Zuordnung.

Auch der Weg über das Mobilfunknetz ist möglich. Hier wird an Stelle der DSL-Anbindung ein Mobilfunk-Router an die IRAS-Server-Box angeschlossen. Dabei besteht die Besonderheit, über einen Dienstanbieter die „Endgeräte“ miteinander zu verbinden. Dafür sorgt bei einem Provider das Leistungsmerkmal „geschlossene Benutzergruppe“!

Verfügt ein Objekt über ein umfangreiches WLAN und möchte dieses unter Einbeziehung seiner IT-Infrastruktur zur Gefahrenmeldung nutzen, sollten hohe Ansprüche zur Sicherung seines Netzwerkes im Vordergrund stehen. Die technische Realisierung ist identisch mit dem eines DSL-Anschlusses.

Alle Anschlussvarianten zum Erreichen der IRAS-Server-Box aus dem Internet finden Sie hierzu unter Punkt 7.

### **4.3 Die Endgeräte**

Die Endgeräte (Smart Devices) können Windows Notebooks, Tablet PCs oder auch Smartphones sein. Für alle Geräte steht die Browser-Darstellung zur Verfügung. In Abhängigkeit des Betriebssystems werden Apps (Applikationen) angeboten, die aus dem jeweiligen Store auf die Geräte geladen werden können. Durch sie werden Programme installiert, die dem Nutzer eine moderne Bedienoberfläche und Sonderfunktionen ermöglichen. Derzeit werden die Betriebssysteme iOS und Android unterstützt.

## 4.4 Bestandteile von IRAS-Basic/IRAS-Basic-Print

### 4.4.1 Der Redundanzadapter als Gateway

Der Redundanzadapter, im eigentlichen Sinne zur Bereitstellung von zwei getrennten Leitungswegen (Integrität der Übertragungswege) für das FAT, besitzt die Eigenschaft, das Protokoll der BMZ in ein IFAM-Protokoll zu übersetzen, um Fremdsysteme wie das IRAS mit den notwendigen Informationen zu versorgen. Der ADP der Generationen 3000 und 4000 wird in die Zentrale eingebaut und kann somit die IRAS-Server-Box in unmittelbarer Nähe zur BMZ mit Daten versorgen.



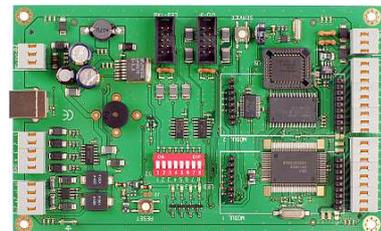
### 4.4.2 Das Feuerwehr-Anzeigetableau als Gateway

Das FAT der Generationen 2000, 3000 und 4000 stellt einen seriellen Anschluss für die Anschaltung von Fremdsystemen bereit. Wie der ADP besitzt das FAT die Eigenschaft, das Protokoll der BMZ in ein IFAM-Protokoll zu übersetzen. Das FAT kann am Standort der Erstinformationsstelle die IRAS-Server-Box mit Daten versorgen.



### 4.4.3 Die Prozessor-Baugruppe als Gateway

Die IMT4CPU ist die Prozessorplatine der IMT4-Baugruppenfamilie und bietet aufgrund der Schnittstellenverfügbarkeit die Anschaltung der IRAS-Server-Box. Ebenso übernimmt sie die Übersetzung des BMZ-Protokolls in das IFAM-Protokoll. Die IMT4CPU kann durch den Einbau in ein separates Gehäuse am Standort der BMZ die IRAS-Server-Box mit Daten versorgen.



### 4.4.4 Die IRAS-Server-Box

Die IRAS-Server-Box ist ein lüfterloser Kleinst-PC auf Linux Basis und verfügt über eine serielle Schnittstelle zur Anschaltung der BMZ über die oben genannten Gateways. Weiterhin ist eine Ethernet-Schnittstelle vorhanden, um ein Netzwerk oder einen entsprechenden DSL-Router anzuschalten. Die vorhandene USB-Schnittstelle ist als Softwareschutz für den Dongle vorgesehen. Das Programm IRAS sowie alle notwendigen Systemprogramme (z. B. WEB-Server) sind installiert. Die Spannungsversorgung kann auf Grund des niedrigen Strombedarfs über die BMZ realisiert werden. Ein Steckernetzteil ist Lieferbestandteil. Die geringen Gehäusemaße gestatten den Einbau in Teile der BMA. Zur Befestigung dient ein Hutschienensystem.



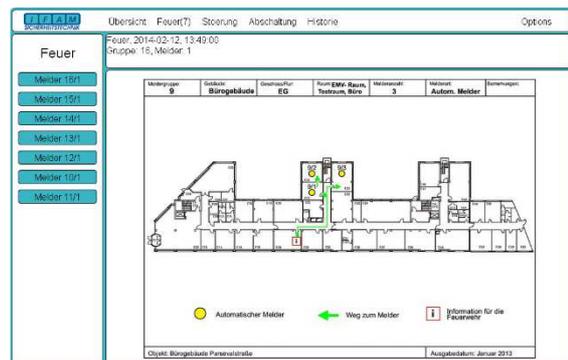
#### 4.4.5 Das Programm IRAS-Basic/IRAS-Basic-Print

Das Programm IRAS wurde speziell für die Weiterleitung von Gefahrenmeldungen auf webfähige Geräte entwickelt. Es übernimmt die Administration des Gesamtsystems und ist somit zuständig für die Verknüpfung von Meldungsdaten (Ereignissen) und den dazugehörigen Objektdaten, Texten und Zusatzinformationen. Es ist verantwortlich für die Kommunikation zwischen den Netzwerken (LAN, GSM, Internet) und übernimmt die Verschlüsselung der Informationen. Ebenfalls Bestandteil von IRAS ist die Speicherung von Informationen in Form von Texten und Grafiken. Das Programm nutzt Zusatzprogramme (z. B. Webserver, Datenbanksystem). Die grafische Ausgabe generiert es in eine Browser-Darstellung als Programmier- und Anzeigebereich.



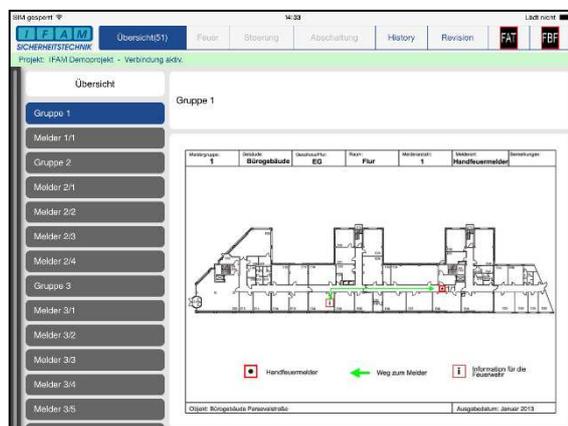
#### 4.4.6 Die Browser-Darstellung

Um Alarme, Störungen usw. anzuzeigen, wird eine Browser-Darstellung angeboten. Diese Darstellungsart besitzt den Vorteil, dass Meldungen auf allen webfähigen Endgeräten angezeigt werden können, ohne Beachtung des jeweiligen Betriebssystems der Smart Devices. Neben den Meldungen besteht die Möglichkeit, alle Ereignisse (Historie) darzustellen. Ein Wartungsmodus „Revision“ unterstützt den Techniker beim Prüfen der BMA. Über die Browser-Darstellung werden alle Einstellungen (Setup) der IRAS-Server-Box durchgeführt und gespeichert. Alle Benutzer werden verwaltet. Als Option ist das FBF als grafische Oberfläche aufrufbar. Die Funktionen des FBF sind konfigurierbar.



#### 4.4.7 Die App-Darstellung

Für die Betriebssysteme iOS (Apple) und Android stehen Applikationen bereit. Die Apps ermöglichen eine benutzerfreundliche Oberfläche. Sie nutzen gezielt Eigenschaften und Funktionen von Smart Devices und gewährleisten die Signalisierung der Meldungen. Darüber hinaus bieten sie nahezu alle Leistungsmerkmale der Browser-Darstellung.



## 4.4.8 Die Endgeräte und Betriebssysteme

### 4.4.8.1 Tablet-PC und Smartphone

Die Endgeräte wie Tablet-PC und Smartphone, beide auch als Smart Device bezeichnet, sind die Empfänger der Gefahrenmeldung. Nach der Installation des Programms auf dem Gerät erhält es unter Beachtung der Verfügbarkeit von Kommunikationsnetzen (z. Bsp. WLAN, UMTS) alle Meldungen.



### 4.4.8.2 Android-Endgeräte

Die Vielzahl am Markt befindlicher Endgeräte bietet ein einheitliches Layout. Die grafische Oberfläche der App wird für das jeweilige Endgerät skaliert und dadurch in gleicher Art und Weise bedienbar.

### 4.4.8.3 Apple-Endgeräte

Zwischen den Applikationen für das iPad und iPhone bestehen durch das Betriebsprogramm bedingte Unterschiede im Layout und somit in der Bedienung.

### 4.4.8.4 Betriebssysteme

Für folgende Betriebssysteme steht die IRAS-Basic App bereit.

### 4.4.8.5 Betriebssystem Android

Android ist das am häufigsten anzutreffenden Betriebssystem für mobile Geräte Stand 2014. Es wird von vielen verschiedenen Herstellern für Smart Devices genutzt. Nach der Installation der App muss diese auf dem Endgerät im Standby bleiben (Hintergrundprozess), um die entsprechenden Gefahrenmeldungen zu erhalten.



### 4.4.8.6 Betriebssystem iOS

Das Betriebssystem iOS des Herstellers Apple weist Besonderheiten auf. Hier braucht die App nicht dauerhaft im Hintergrund aktiv bleiben. Alle Ereignisse werden als Push Notifications an das mobile Gerät übermittelt. Das Gerät signalisiert aus dem Standby. Das Betriebssystem macht ebenfalls eine Anpassung der Bedienoberfläche am Smartphone notwendig. Hier findet keine einfache Skalierung Layouts statt. Die IRAS-Server-Box benötigt den Zugang zum APN-Server.



#### 4.4.8.7 Betriebssystem Windows 10

Das Betriebssystem Windows 10 des Herstellers Microsoft besitzt neben den betriebssystembedingten Eigenschaften (z. B. erweiterte Wischfunktionen) auch die Möglichkeit, die Applikation auf dem Windows 10-PC darzustellen und zu bedienen.



#### 4.4.8.8 Andere Technologien

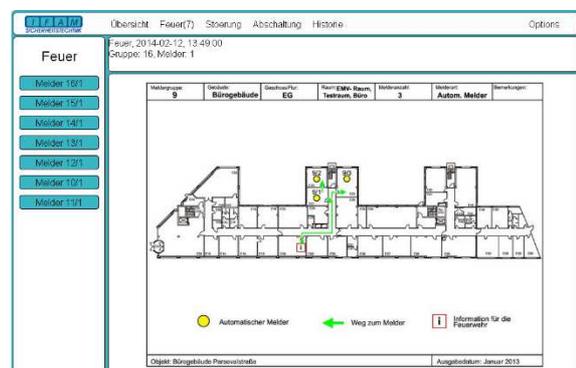
Endgeräte, die nicht über die o.g. Technologien verfügen, können ebenfalls Empfänger der Gefahrenmeldung sein. Dazu ist es nur erforderlich, die entsprechende IP-Adresse der IRAS-Server-Box in den Internet-Browser einzugeben. Nutzer, deren Endgeräte nicht über die oben genannten Betriebssysteme verfügen, sollten bestehende Applikationen anderer Anbieter zwecks möglicher Emulationen überprüfen.

z. Bsp. BlackBerry, Store – BlackBerry app world, ab Version 10.2 (mit Einschränkungen)

### 4.5 Darstellungen

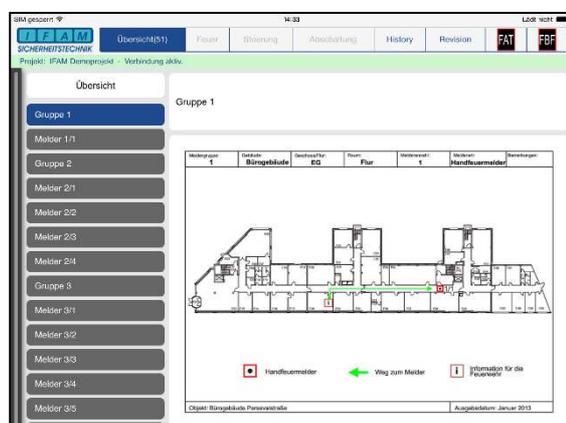
#### 4.5.1 Browser-Darstellung

Ansichtsformat, in der das Programm IRAS-Basic alle Daten wie Texte, Bilder, Grafiken, bzw. Bilder von IP-Kameras zur Signalisierung, Programmierung und Bedienung bereitstellt. Die Browser-Darstellung erlaubt die Nutzung aller webfähigen Endgeräte im lokalen Netzwerk oder über das Internet.



#### 4.5.2 App

Das App ermöglicht die anwenderfreundliche Nutzung von IRAS auf dem Smart Devices. Um diese Art der Darstellung nutzen zu können, ist die Installation der App „IRAS-Basic“ notwendig.



### 4.5.3 FAT-Bedieneroberfläche

Diese Bedienoberfläche zeigt in Form und Funktion das Feuerwehr-Anzeigetableau (FAT) in Anlehnung an die DIN 14662. Alle Ereignisse wie Alarm (Feuer), Störung, Abschaltung usw. werden mittels LED sowie im Display angezeigt. Cursor-Tasten erlauben das Blättern bei mehr als 2 Alarmen. Es besteht keine Rückwirkung auf die BMZ. Mit Hilfe der Taste „Summer ab“ lässt sich der Signalton am FAT der Feuerwehr ausschalten.



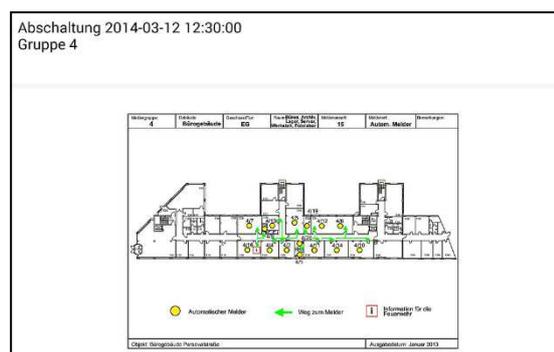
### 4.5.4 FBF-Bedieneroberfläche

Diese Bedienoberfläche zeigt in Form und Funktion das Feuerwehr-Bedienfeld (FBF) in Anlehnung an die DIN 14661. Alle Tastenfunktionen besitzen nach der entsprechenden Programmierung (Freigabe im Setup) Rückwirkung auf die BMZ. Für die Nutzung dieser Funktionen sind konkrete Vereinbarungen zwischen Betreiber, Wartungsfirma und Feuerwehr erforderlich. (siehe hierzu DIN VDE 0833-1) Zusätzlich lassen sich weitere Tasten und Funktionen in Abstimmung mit dem Hersteller der BMZ integrieren.



### 4.5.5 Darstellung der Feuerwehr-Laufkarte

Mit den Meldungen von Ereignissen können weitere Informationen an mobile Endgeräte übertragen werden. Die häufigste Anwendung ist die Anzeige der Feuerwehr-Laufkarte nach DIN 14675. Passend zum ausgelösten Meldebereich wird der Angriffsweg für Brandbekämpfungsmaßnahmen in JPEG- und PDF-Format angezeigt. Weitere Informationen wie Feuerwehrpläne nach DIN 14095, Objektpläne, Gebäude- oder Geländegrafiken können ebenfalls eingebunden werden.



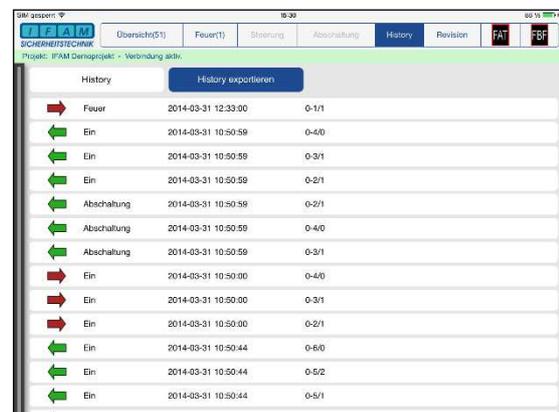
## 4.5.6 BMZ-Übersicht

Die BMZ-Übersicht beschreibt alle angeschalteten Brandmelderzentralen und deren in der IRAS-Server-Box konfigurierten Meldergruppen und Melder. Hier kann auch ohne eine Gefahrenmeldung Einblick in das Gesamtsystem genommen werden.



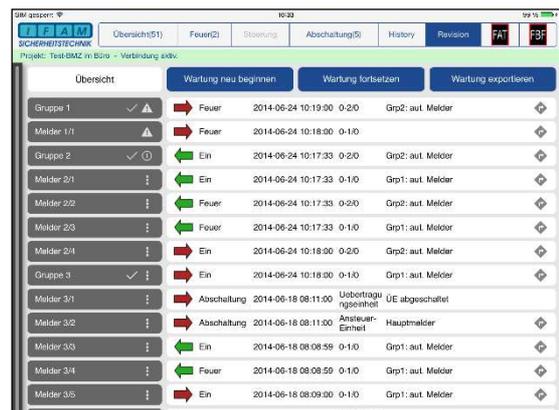
## 4.5.7 Ereignisspeicher / Historie

Der Ereignisspeicher registriert alle kommenden und gehenden Meldungen der BMZ. Alle Einträge werden mit einem Zeitstempel versehen.



## 4.5.8 Wartungsmode / Revision

Nach DIN 14675 unterliegen Brandmelderzentralen einer wiederkehrenden Wartung. Der Umfang dieser Tätigkeit richtet sich nach dem Ausbau der BMZ und der damit verbundenen Größe des Objektes. Um diesen Prüfvorgang zu erleichtern, unterstützt IRAS die Speicherung und Dokumentation der Ereignisse. Zu Beginn der Prüfung wird hierfür der Wartungsmode aktiviert, welcher alle Prüfdaten chronologisch protokolliert und speichert. Zur jeweiligen Prüfung werden Auslösung und Standort kontrolliert und auf dem mobilen Endgerät angezeigt. Zusatzinformationen, wie z. Bsp. fehlerhafte Feuerwehr-Laufkarten, Nichtbegehbarkeit der Räume sowie freie Texteingaben zum Standort lassen sich zum ausgelösten Ereignis hinterlegen. Zum Schluss der Revision wird der Wartungsmode beendet und die Daten können als Datei abgespeichert werden. Über ein E-Mail-Programm lassen sich die gespeicherten Daten zum Ausdruck versenden.



## 4.5.9 USB-Schnittstelle

Die USB-Schnittstelle wird zur Erweiterung der Speicherkapazität genutzt. Hierfür eingesetzte USB-Speicher (z. B. USB-Sticks) erlauben die variable Anpassung an die Größe des jeweiligen Objektes und gestatten eine nahezu unbegrenzte Anzahl von Informationen.

## 4.5.10 Benutzerverwaltung / Berechtigungsstufen

Es sind drei verschiedene Benutzer mit verschiedenen Berechtigungen in der ESPA 4.4.4 konfigurierbar.

<i>Username</i>	<i>Berechtigung für...</i>
admin	Anzeige, Bedienung/ Revision und Setup
operator	Anzeige und Bedienung/ Revision
user	Anzeige

## 4.5.11 Nutzung von Kameras

Das Programm IRAS verknüpft Ereignisse mit IP-Kameras. Durch eine entsprechende Alarmierung und die damit verbundene Aktivierungsmöglichkeit kann mit Hilfe der verknüpften Kamera Einblick in den Meldebereich genommen werden. Mittels betätigen des Kamera-Symbols öffnet sich das Kamera-Bild und gestattet die Sicht auf sensible Bereiche, wie z. Bsp. Reinsträume, Labore oder OP-Säle.



## 4.5.12 Objektverwaltung

Mit Hilfe der Objektverwaltung können Gefahrenmeldungen von einer bestimmten Anzahl von Brandmeldeanlagen auf mobilen Endgeräten abgebildet werden. Durch Ein- bzw. Ausschalten der Projekte wird eine umfassende oder gezielte Überwachung möglich. Bei IRAS-Basic lassen sich bis maximal 25 Objekte in die Überwachungsmaßnahmen einbeziehen. Bei IRAS professional ist diese Anzahl nicht begrenzt.



## 4.5.13 Sprachen

Die App-Darstellung ist in deutscher und englischer Version verfügbar. Werden weitere Sprachversionen gewünscht, kann nach Bereitstellung der entsprechend übersetzten Texte / Schlüsselworte jede andere Sprache implementiert werden.

## 4.5.14 Bilder

Zusätzlich zu Textinformationen besteht die Möglichkeit, Bilder dem jeweiligen Prüfvorgang anzuhängen und so Zustände der BMA zu dokumentieren.

## 4.6 IRAS-Basic2-App

### 4.6.1 IRAS-Basic2



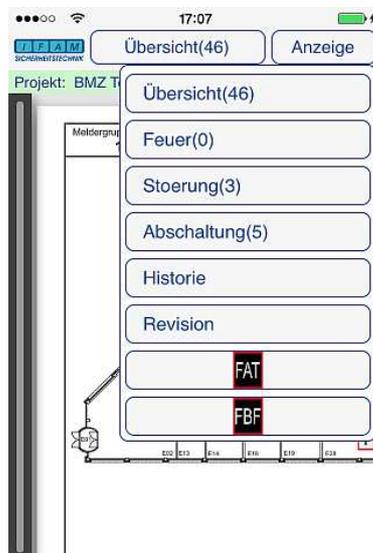
Das Programm IRAS bietet die Möglichkeit, mit dem oben beschriebenen Leistungsumfang bis zu 25 verschiedene Brandmeldeanlagen zu verwalten. Die Erreichbarkeit der IRAS-Server-Box aus dem Internet ist dabei Grundvoraussetzung. In Abhängigkeit der genannten Betriebssysteme und durch die Nutzung von Diensten wird der Zugriff von mobilen Endgeräten auf die IRAS-Server-Box ermöglicht. Neben der Push Notification kann ebenfalls das Port Forwarding in den Kommunikationsverfahren nötig sein. Die Kundendaten liegen auf der IRAS-Server-Box vor Ort.

### 4.6.2 Grafische Oberfläche Smart Device – iOS (Apple)

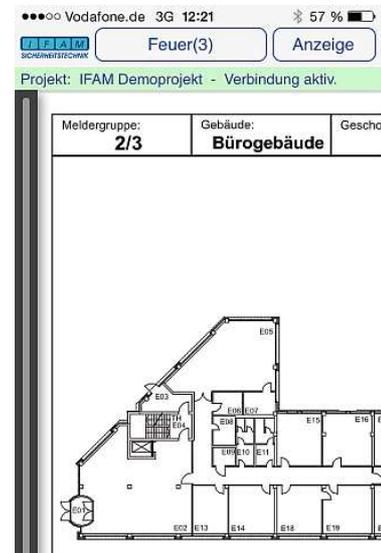
Die grafische Oberfläche wurde durch das Betriebsprogramm bedingt angepasst. Um alle Leistungsmerkmale der App nutzen zu können, wurden Unterschiede zwischen iPhone- und iPad-Bedienung (Apple) erforderlich.



z. Bsp. Übersicht



Auswahl



Feuer

## 4.7 Sicherheit IRAS

### 4.7.1 Schutz der Kundendaten

Alle Zugriffe auf die Kundendaten sind passwortgeschützt. Es existiert ein Rechtesystem, mit dem die Zugriffs- und Konfigurationsmöglichkeiten je nach Bedarf weiter eingeschränkt werden können. Alle Daten werden direkt zwischen der IRAS-Server-Box und dem Endgerät ausgetauscht. Es ist kein weiterer Teilnehmer in der Speicherung der Kundendaten involviert.

### 4.7.2 Absicherung der Kommunikation

Es kann zwischen unverschlüsseltem (HTTP) und SSL-verschlüsseltem (HTTPS) Kommunikationsbetrieb gewählt werden. Es kann je nach Installation abgewogen werden, ob der erhöhte Aufwand für die Verwaltung der Verschlüsselungszertifikate notwendig ist.

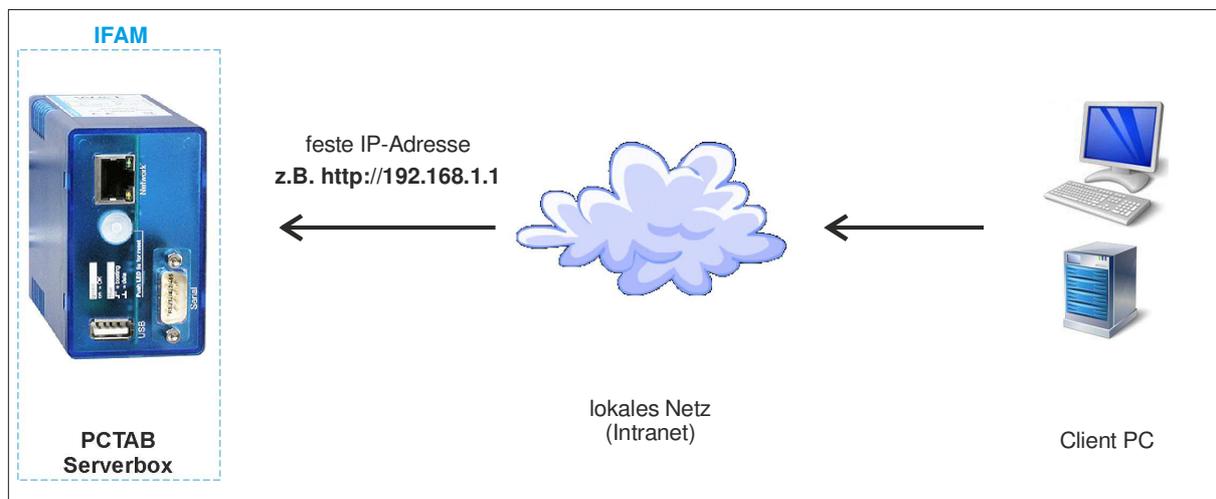
### 4.7.3 Schutz der BMZ-Rückwirkung

Da durch die FBF-Funktionalitäten auf die BMZ zurückgewirkt werden kann, besteht die Möglichkeit, dass fehlerhafte oder unbefugte Zugriffe auf die BMZ deren Funktion und Sicherheit beeinträchtigen. IRAS bietet daher die Möglichkeit die FBF Funktionalität gesondert einzuschränken oder sogar komplett zu deaktivieren.

## 4.8 Zugriffsmöglichkeiten auf die IRAS-Server-Box

Diese Rubrik gibt eine praktische Übersicht über die Zugriffsmöglichkeiten vom Netzwerk bzw. Internet auf die IRAS-Server-Box. Die Einsatzvielfalt reicht von der einfachen Anschaltung im lokalen Netz über die DSL-Router-Ankopplung bis zum gesicherten VPN-Tunnel. Je nach örtlichen Gegebenheiten (Anschlussmöglichkeiten) sowie unter Beachtung des erforderlichen Aufwandes für die Anbindung kann die entsprechende Variante realisiert werden.

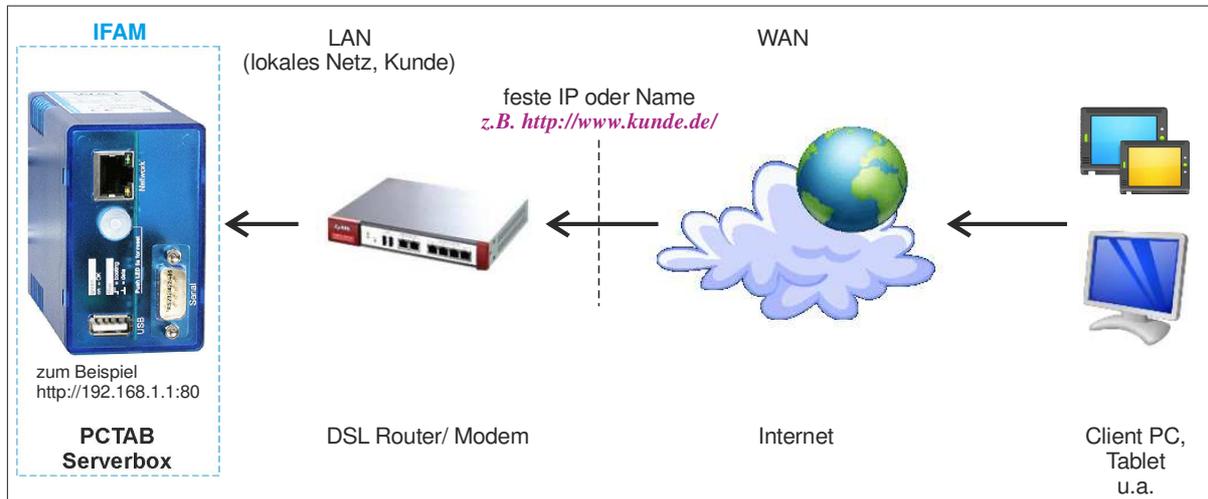
### 4.8.1 Netz mit fester IP, HTTP



Diese Variante zeigt die einfachste Möglichkeit des Zugriffs auf die IRAS-Server-Box. Diese befindet sich im lokalen Netz und ist mit einer festen IP-Adresse im Intranet erreichbar. Es wird

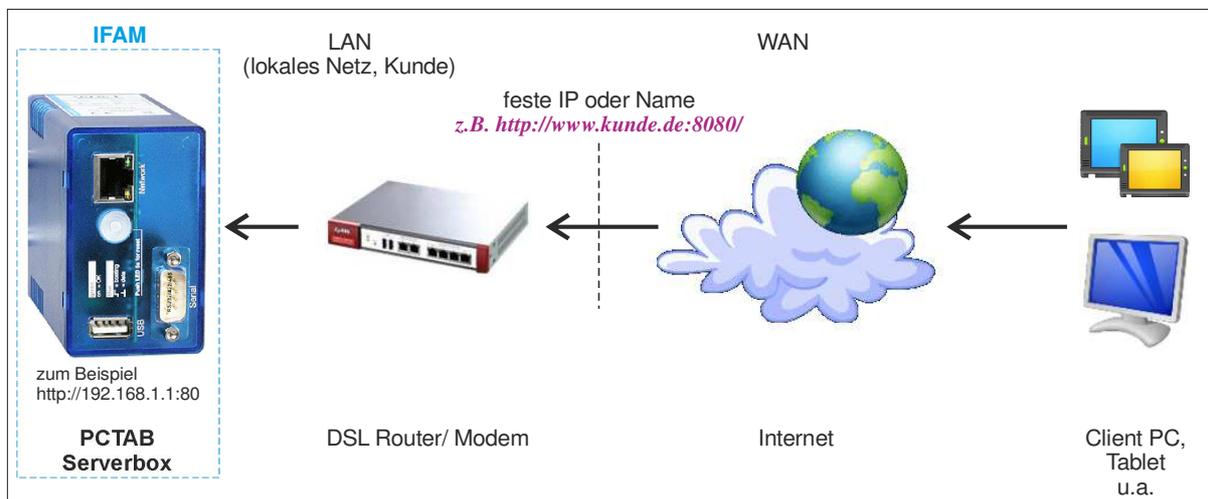
der Standard Port 80 des Webb-Browsers benutzt. Die IRAS-Server-Box benötigt den Zugang zum APN-Server.

#### 4.8.2 Router mit fester IP, HTTP



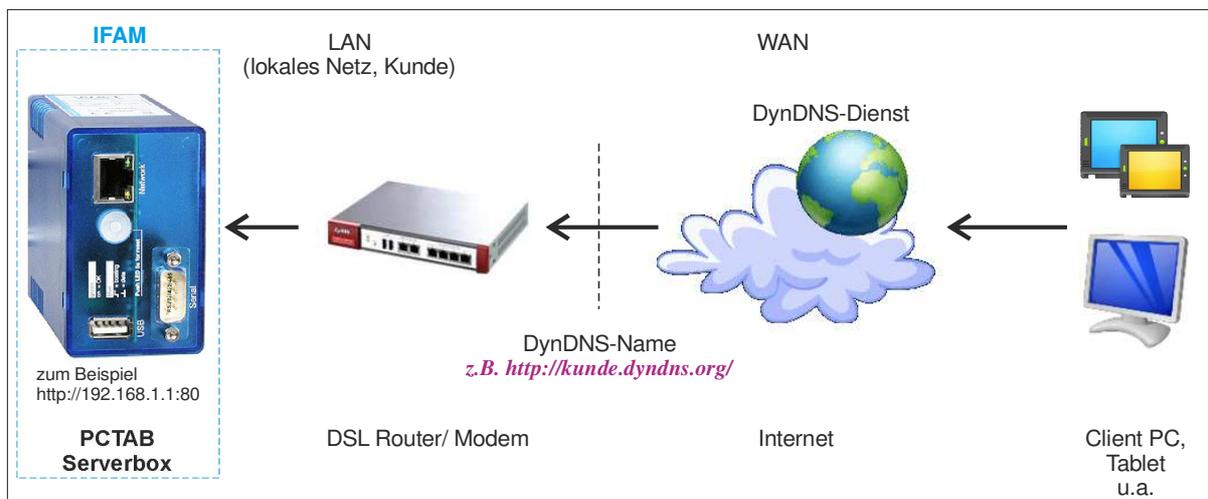
Diese Variante zeigt eine einfache Möglichkeit des Zugriffs auf die IRAS-Server-Box. Voraussetzung ist die Erreichbarkeit vom Internet über einen festen Namen oder eine IP-Adresse. Der Router / Modem leitet alle Anfragen von außen an die IRAS-Server-Box weiter.

#### 4.8.3 Router mit fester IP, HTTP mit Portweiterleitung



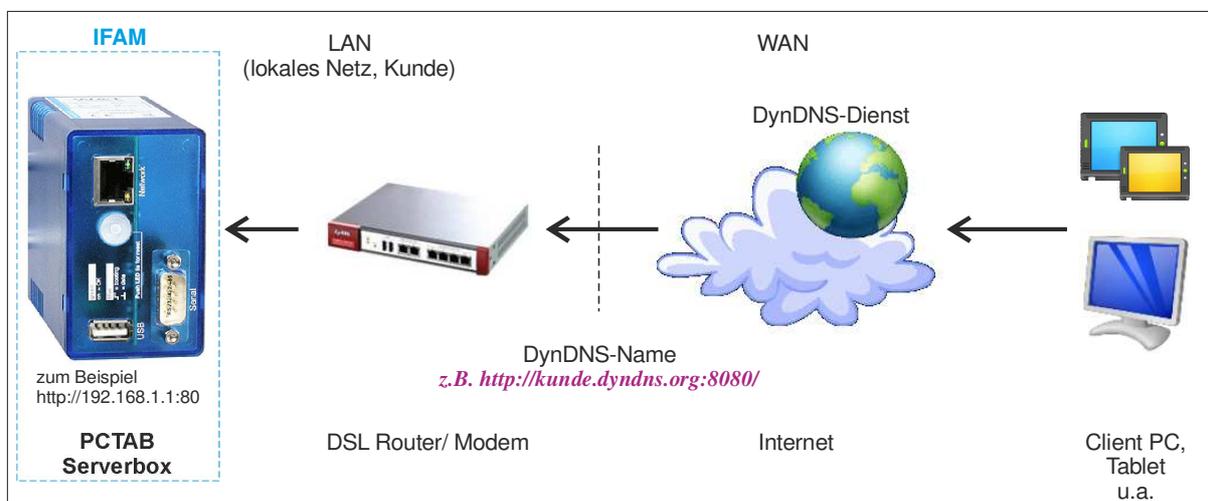
Falls der Standard Port (Port 80/ TCP) schon von einer anderen (kundenspezifischen) Anwendung benutzt wird oder auch aus Sicherheitsgründen kann jeder beliebige andere Port für den Zugriff bis zum DSL-Router eingestellt werden (hier z.B. Port 8080). Der Router muss dann eine Portweiterleitung zum Port 80 auf die IRAS-Server-Box gewährleisten.

#### 4.8.4 Router mit dynamischer IP



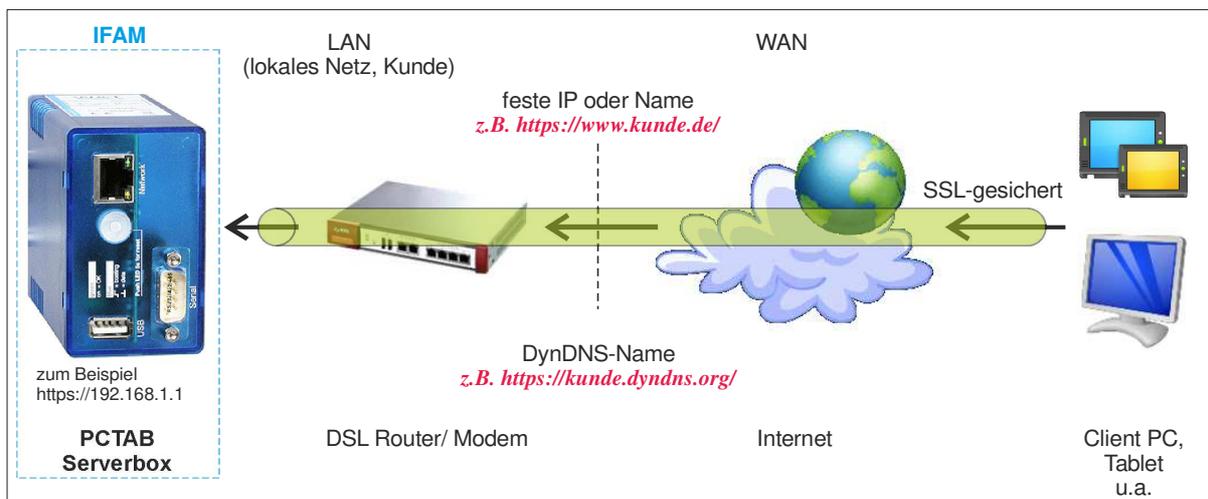
In diesem Fall ist der Zugang auch bei einer dynamischen IP-Adresse möglich. Im Allgemeinen wechselt z.B. die IP-Adresse des Routers alle 24 Stunden. Durch Nutzung eines DynDNS-Dienstes kann hier trotzdem unter Verwendung eines festen Namens der Zugang ermöglicht werden. Der Router / Modem leitet alle Anfragen von außen an die IRAS-Server-Box weiter.

#### 4.8.5 Router mit dynamischer IP und Portweiterleitung



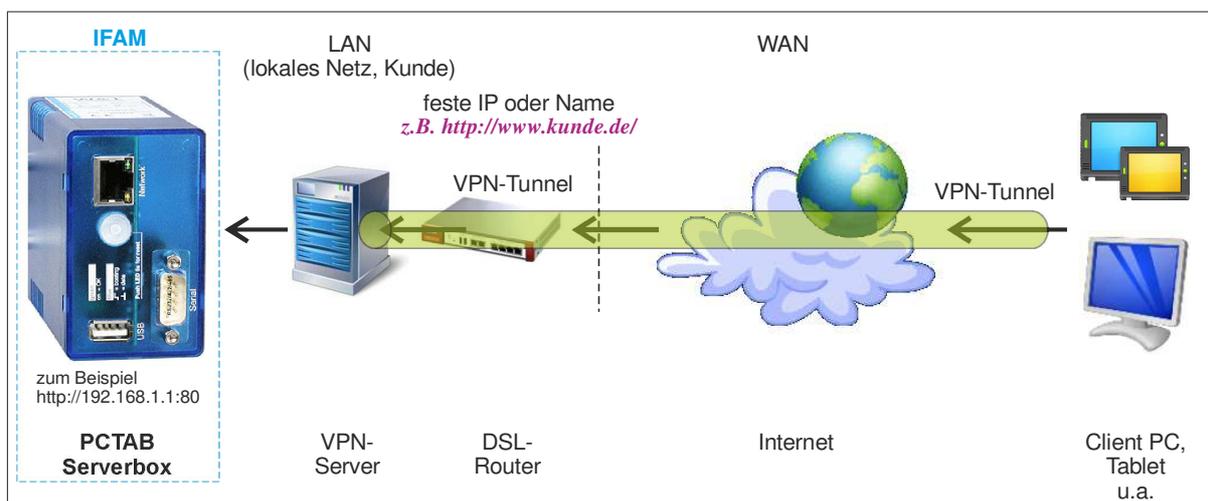
Falls der Standard Port (Port 80) schon von einer anderen (kundenspezifischen) Anwendung benutzt wird oder auch aus Sicherheitsgründen kann jeder beliebige andere Port für den Zugriff bis zum DSL-Router eingestellt werden (hier z.B. Port 8080). Der Router muss dann eine Portweiterleitung zum Port 80 der IRAS-Server-Box gewährleisten.

#### 4.8.6 Router, HTTPS (SSL)



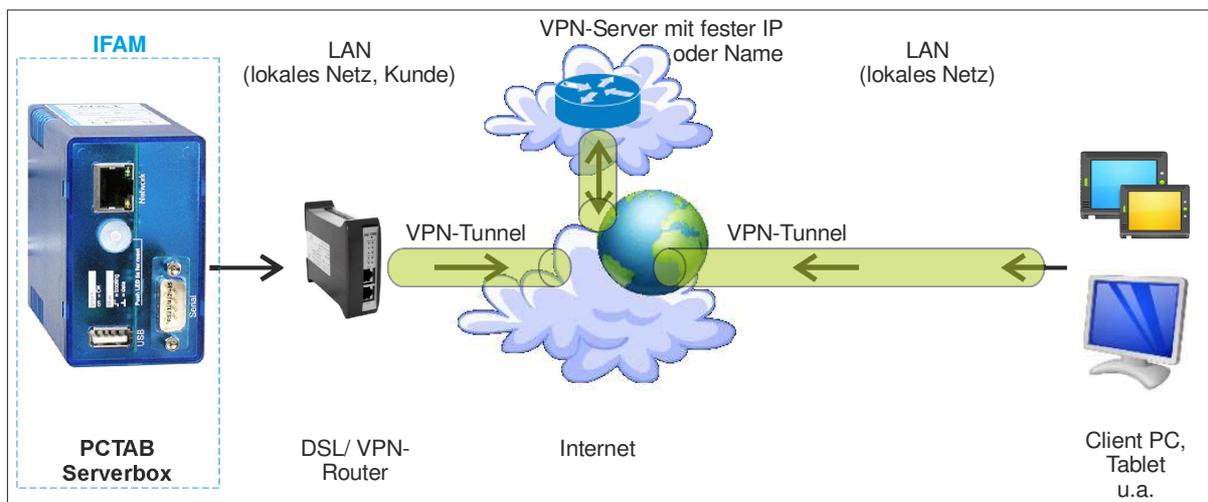
Diese Variante zeigt eine Möglichkeit des sicheren Zugriffs auf die IRAS-Server-Box. Im Unterschied zur Variante 4.8.5 wird die Verbindung zwischen dem Client-Browser und der IRAS-Server-Box (End-to-End) verschlüsselt. Der Router muss dann eine Portweiterleitung zum Port 80 auf die IRAS-Server-Box gewährleisten. Dies gilt bei einer dynamischen IP-Adresse ebenso wie bei einer festen IP-Adresse ebenso für die Varianten 4.8.2, 4.8.3, 4.8.4 und 4.8.5.

#### 4.8.7 VPN-Server im lokalen Netz, Fernzugriff über VPN



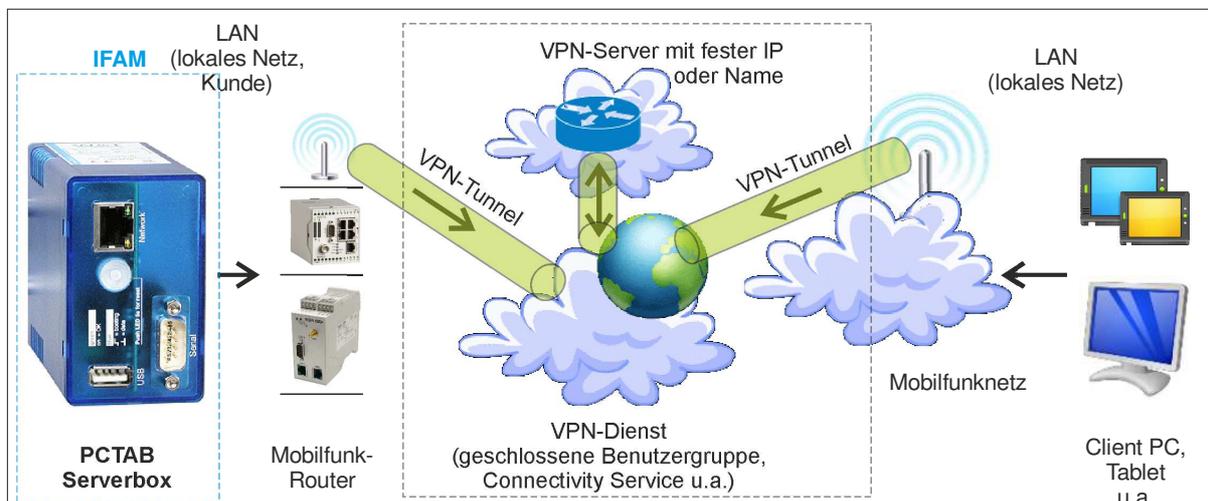
Bei Tunnelung über ein virtuelles privates Netz (VPN) ist der Zugriff vom Client-Browser auf die IRAS-Server-Box prinzipiell wie in Variante 4.8.1 möglich. Es entsteht nur ein erhöhter Aufwand für die Einrichtung bzw. Realisierung eines VPN-Tunnels. Es sind VPN-fähige Endgeräte nötig. Der VPN-Tunnel wird standardmäßig meist verschlüsselt. Auch hier ist die Erreichbarkeit vom Internet über einen festen Namen oder eine IP-Adresse erforderlich, um den VPN-Tunnel aufbauen zu können. Um die Funktionen von IRAS zu nutzen, muss die VPN-Verbindung am Endgerät aktiviert werden. Danach verhält sich das System wie unter Punkt 4.8.1.

#### 4.8.8 VPN-Server im WAN



Diese Variante umgeht die Probleme der Erreichbarkeit der Serverseite. Beide Seiten (IRAS-Server-Box über DSL/ VPN-Router sowie der Benutzer) nehmen Verbindung zu einem gemeinsam bekannten VPN-Server auf (dritter Teilnehmer) auf. Dort wird die Verbindung virtuell zwischen IRAS-Server-Box und Benutzer hergestellt- sie befinden sich in einem gemeinsamen virtuellen Netz. Der Austausch von Daten (Browser - Webserver) erfolgt dann wie im lokalen Netz.

#### 4.8.9 Verbindung über Mobilfunknetz, VPN



Mit dieser Variante ist eine völlige Unabhängigkeit von der IT-Infrastruktur beim Kunden gegeben. Es wird ein UMTS-Router eingesetzt, welcher über das Mobilfunknetz die Anbindung sowie den Zugriff des Client-Nutzers (Browser) wie in einem lokalen Netz erlaubt. Auch hier werden wieder die VPN-Technik sowie eine geschlossene Benutzergruppe (z. B. „mdex“) benutzt. Beide Seiten (IRAS-Server-Box über UMTS-Router sowie der Benutzer) nehmen Verbindung zu einem gemeinsam bekannten VPN-Server auf (dritter Teilnehmer).

## 4.9 Voraussetzungen

### 4.9.1 System

- Serielle Schnittstelle der BMZ (FW-Peripherie)
- Protokollinhalte (z. B. Meldergruppe / Melder, Texte)
- Netzwerkzugang (LAN)
- Internetzugang (DSL), bei Bedarf
- Mobilfunkzugang (GSM) mit Mobilfunkdienst (geschlossene Benutzergruppe), bei Bedarf
- Erreichbarkeit der IRAS-Server-Box aus dem Internet, bei Bedarf

## 4.10 Übersicht Leistungsmerkmale IRAS-Basic

- Programm- und Datenspeicherung auf kundeneigener IRAS-Server-Box
- Stromversorgung für die IRAS-Server-Box über BMZ oder separates Steckernetzteil oder Power over Ethernet
- Anschaltung über FAT, ADP oder IMT4CPU
- Visualisierung über App und Browser
- FAT-Darstellung
- FBF-Darstellung mit FBF-Funktionalität (programmierbar)
- Administration über Browser durch Betreiber oder Wartungsfirma (Berechtigung usw.)
- Anzeige von BMZ-Nr., Meldergruppe, Melder in der Übersicht
- Meldungen je nach konfigurierter Codetabelle (Feuer, Störung, Abschaltung, Technische Alarmer u.a.) oder freier Anzeigemodus
- Darstellung der Feuerwehr-Laufkarten (PDF, JPG)
- Darstellung von zusätzlichen Objektinformationen (Text, PDF, JPG)
- App-Download über Playstore (Android) bzw. Appstore (iOS)
- Benachrichtigung mittels Notification (bei Verwendung der App)
- Anzeige kommender und gehender Ereignisse im Ereignisspeicher
- Verknüpfung mit vorhandenen IP-Netzwerkcameras möglich
- Revisionsmode zur Wartungsunterstützung mit Terminierung, Standortkontrolle, Wohnungshinweisen, Dokumentenversand und Langzeitspeicher
- Objektdaten im Offline-Modus verfügbar
- Integrierte Objektverwaltung

## 4.11 Lieferumfang IRAS-Basic

- IRAS-Server-Box inklusive Software und Dokumentation

Optional:

- ADP4000 / FAT4000 als Gateway
- IMT4CPU (als Gateway) / Gehäuse / Netzteil
- UMTS-Router\*

\* Achtung! Für eine volle Funktionalität ist der Mobilfunkdienst „Geschlossene Benutzergruppe“ bzw. VPN notwendig.

## 5 IRAS-Plus / IRAS-Plus-Mobile

IRAS-Plus ist eine Weiterentwicklung sowie ein eigenständiges Produkt und beinhaltet alle Merkmale von IRAS-Basic. Durch einen leistungsfähigen PC, der über eine wesentlich höhere Performant verfügt, als die IRAS-Server-Box, können erweiterte Anwendungen für Betreiber und Errichter ermöglicht werden und ist somit für besondere Einsätze konzipiert. Die Anbindung an Brandmelderzentralen ist gleich IRAS-Basic. Ebenfalls sind die bewerten Betriebssysteme iOS, Android und windows10 verfügbar.

Die dazu verwendete IRAS-Plus-IRAS-Server-Box ist ein PC im Kleinformat und ermöglicht den Abruf von Gefahrenmeldungen über ein TCP/IP Netzwerk. Sie übernimmt Meldungen von Gefahrenmeldeanlagen über die serielle Schnittstelle (RS232) und stellt diese Ereignisse mittels eines in der IRAS-Plus-IRAS-Server-Box laufenden Programms sowie den integrierten Webserver für den externen Zugriff über das Netzwerk bereit.



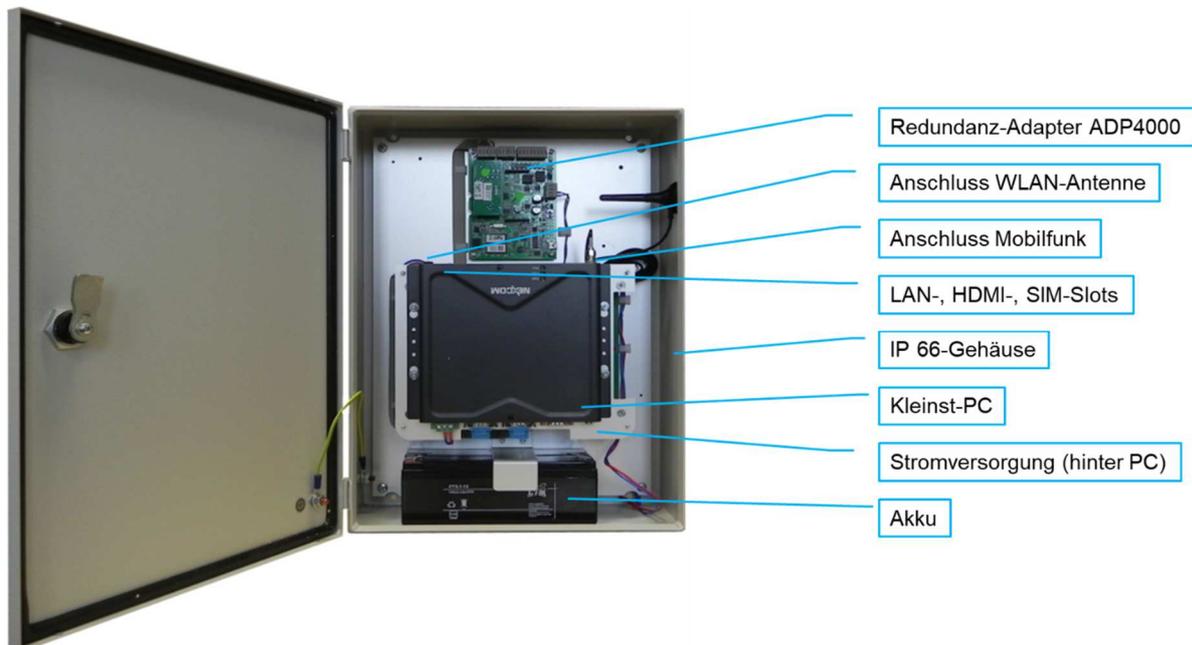
Ein Netzteil mit Akku der IRAS-Plus-IRAS-Server-Box ermöglicht das Versenden von Informationen auch bei Spannungsausfall. Der Akku hat eine Kapazität von ca. 5 Stunden. Zur Visualisierung der Meldungen werden bei der Konfiguration Bilder und Grafiken in der IRAS-Plus-IRAS-Server-Box gespeichert. Mittels Aufrufes der Webseite über einen Browser oder einer speziellen Applikation für mobil Geräte, können alle Meldungen aus der Brandmelderzentrale visualisiert werden. Zusätzlich gibt es die Funktion der Wartung Live-Bilder von IP-Basierten Webcams, können ebenfalls in die Visualisierung eingebunden werden.

Besteht zusätzlich ein Zugang aus dem Internet zur IRAS-Plus-IRAS-Server-Box, können die Meldungen optional auf allen webfähigen Endgeräten dargestellt werden. Für mobile Geräte wie Smartphones oder Tablet-PCs gibt es passende Apps, welche die Bedienung erleichtern und umfangreiche Funktionen bieten.

Die lüfterlose IRAS-Plus-IRAS-Server-Box kann durch die geringen Abmessungen und den geringen Stromverbrauch bei einer Versorgungsspannung von 24V kann auch direkt aus der Gefahrenmeldeanlage mit Strom versorgt werden.

Die Administration des Systems (Installation, Konfiguration) erfolgt über die Netzwerkschnittstelle mittels Webbrowser. Die Administration und eine eingeschränkte Nutzung ist dadurch plattformunabhängig und bedarf keiner weiteren Software, die installiert werden muss. Die Festinstallation vereint die Eigenschaften von IRAS-Basic mit der IRAS-Wartungsbox. Eine wesentliche Eigenschaft ist der Einsatz für Sonderanwendungen, insbesondere bei großen Objekten. Zusätzlich kann ein Mobilfunk-Modul verbaut werden.

## 5.1 Bestandteile



## 5.2 Schnittstellen (Slots)

Serielle Schnittstelle COM2	- dient zur Kommunikation mit dem Netzteil
LAN	- Administration, Webserver, Push-Meldungen, Updates
USB	- Anschluss für einen Massenspeicher
WLAN	- Kunden-WLAN oder Steuerung der Box
HDMI	- Monitoranschluss (Service)
SIM	- Mobilfunkkarte

## 5.3 Das App IRAS-Basic2

Um die neuen Funktionen dem Nutzer zur Verfügung zu stellen, ist der Download einer neuen IRAS-Basic-Applikation „IRAS-Basic2“ notwendig. Das Grundprinzip auf den mobilen Endgeräten ist gleich, verfügt aber über einen erweiterten Bedienkomfort.



## 5.4 Übersicht erweiterte Leistungsmerkmale

- Liste wiederkehrender Prüfungen (Dokument)
- Projektverwaltung
- Export/Import von Projekten
- Projektsicherung auf USB
- Dokumentenverwaltung, Auswahl der Standardansicht
- Darstellung von ausgelösten Ereignissen (Melder, Bereiche, Anfahrten) durch gif-Dateiformat
- Übernahme der Wartungsliste aus vorhandenen Projekten
- FW-Laufkarte kann auch nur noch aus einer PDF bestehen, das JPEG kann dynamisch erzeugt werden
- für PS-Drucker kein Hochladen von Postscript (PS) Dateien mehr notwendig
- Auslösung Testereignis
- selektieren von Grund- und Vorinformation zu bestehenden Meldergruppen (Zusammenfassung für Anfahrtswege)

## 5.5 Lieferumfang IRAS-Plus / IRAS-Plus-Mobile

### 5.5.1 IRAS-Plus

- IRAS-Plus-IRAS-Server-Box inklusive Software und Dokumentation
- ADP4000 als Gateway
- WLAN-Modul inklusive Antenne
- Netzteil inklusive Akkus
- IP66-Gehäuse

Optional:

- FAT4000 als Gateway
- ohne Netzteil, Akkus und Gehäuse

### 5.5.2 IRAS-Plus-Mobile

- IRAS-Plus-IRAS-Server-Box inklusive Software und Dokumentation
- ADP4000 als Gateway
- **Mobilfunkmodul inklusive Antenne (ohne Datenkarte\*)**
- WLAN-Modul inklusive Antenne
- Netzteil inklusive Akkus
- IP66-Gehäuse

Optional:

- FAT4000 als Gateway
- ohne Netzteil, Akkus und Gehäuse

\* Achtung! Für eine volle Funktionalität ist der Mobilfunkdienst „Geschlossene Benutzergruppe“ bzw. VPN notwendig.

## 5.6 Systemvoraussetzungen

- Serielle Schnittstelle der BMZ (FW-Peripherie)
- Protokollinhalte (z. B. Meldergruppe / Melder, Texte)
- Netzwerkzugang (LAN)
- Internetzugang (DSL), bei Bedarf
- Mobilfunkzugang (GSM) mit Mobilfunkdienst (geschlossene Benutzergruppe) \*
- Erreichbarkeit der IRAS-Server-Box aus dem Internet

\* Achtung! Nur bei IRAS-Plus-Mobile

## 6 IRAS-Wartungsbox

Die IRAS-Wartungsbox (IRAS-WB) dient zur Unterstützung und Optimierung der Inspektion bzw. Wartung. Mit Hilfe der IRAS-WB ist es möglich, die Ereignisse einer Prüfung in der Box abzuspeichern, zusätzliche Informationen zu hinterlegen, die gewonnenen Daten zu bearbeiten und zu versenden. Zusätzlich lassen sich Bedienvorgänge an der Brandmelderzentrale (BMZ) realisieren, sofern das Protokoll der BMZ dieses Leistungsmerkmal unterstützt. Diese Bedienvorgänge (Rückwirkungen auf die BMZ) erlauben Steuerungen wie z. B. Abschaltungen, die das Prüfen von Meldergruppen und Meldern im Objekt vereinfachen. Dabei wird der Status der BMZ, besonders im Hinblick auf „FEUER“, ständig überwacht und angezeigt. Die durch die Prüfungen erzeugten Daten können als Dokumente den Stand der Wartung visuell wiedergeben, um so eine Nachweisführung im Sinne der DIN 14675 zu gewährleisten.

Die IRAS-Wartungsbox kann prinzipiell an jede BMZ angeschaltet werden. Voraussetzung dafür ist die Feuerwehrperipherie der Systeme 2000\*, 3000\* oder 4000. Die benötigte serielle Schnittstelle wird über den Redundanz-Adapter ADP4000 oder über ein FAT bereitgestellt. Rückwirkungsfunktionen sind vom Protokoll zwischen BMZ und Feuerwehrperipherie abhängig und vor einer Nutzung abzustimmen. Die IRAS-WB verfügt standardmäßig über einen leistungsfähigen Kleinst-PC, vorbereitet für die Kommunikation durch WLAN- und Mobilfunknetze, um eine komfortable und unabhängig vom Standort betriebene Anzeige und Überwachung zu ermöglichen. Über eine vorhandene USB-Schnittstelle können die Anlagendaten der BMZ importiert oder die Revisionsdaten exportiert werden. Die Projekte werden im Vorfeld einer Revision in der IRAS-WB konfiguriert. Im Zusammenspiel mit dem System4000 ist danach eine automatische Identifizierung zwischen Projekt und BMZ möglich. Die Revision wird durch ein Tablet-PC, Smartphone über die IRAS-WB gestartet, ggf. bestimmte Steuerfunktionen zur BMZ eingeschaltet. Während der Revision ist es über eine Applikation auf Tablet-PCs möglich, den Verlauf sowie weitere Informationen zu kontrollieren und wichtige Hinweise zur Wartung hinzuzufügen. Bei einer Unterbrechung oder nach Abschluss der Revision stehen über Export-Funktionen die Wartungsdaten zur Verfügung. Die Applikation erzeugt eine Übersicht über den Stand der Wartung sowie eine Kommentarliste. Die Revision wird durch eine Benutzeroberfläche verwaltet und gestattet nur autorisierten Personen den Zugriff auf Daten aus der BMZ. Für eine komfortable Bedienung stehen Applikationen (App, IRAS-Basic) in den gängigsten App-Stores zur Verfügung.

\*eingeschränkte Bedienung

### 6.1 Gerät und Funktionen

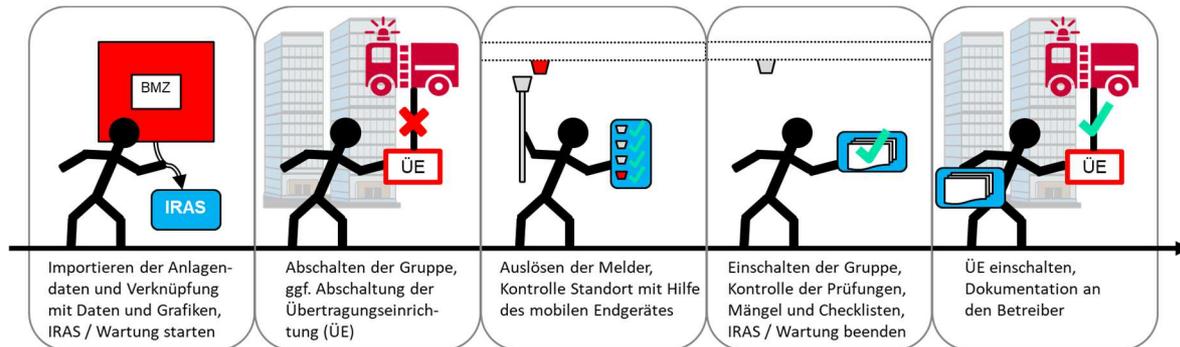




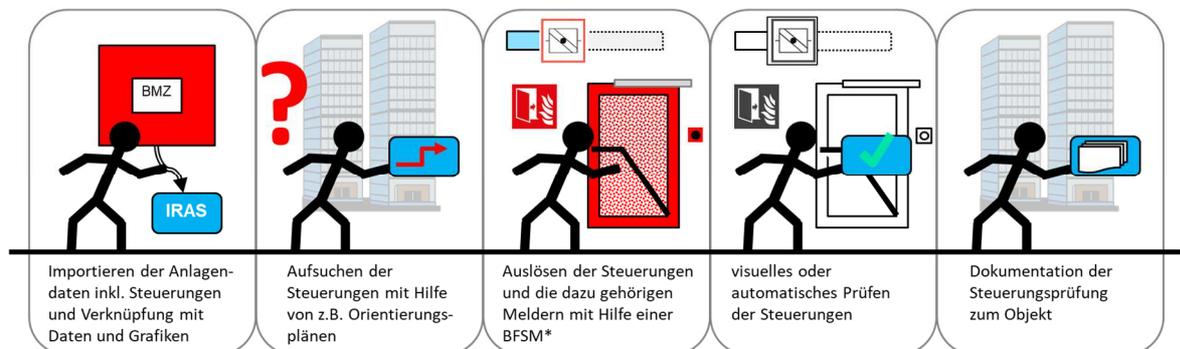
## 6.3 Prüfungen

Grundsätzlich unterscheidet IRAS automatische und nichtautomatische Prüfungen für die Durchführung und Dokumentation.

Automatische Prüfungen umfassen Vorgänge, die aufgrund von Rückmeldungen aus der BMZ selbst einen Prüfeintrag in die Dokumente gestatten und somit die Prüfung vereinfachen, beschleunigen und authentifizieren. (z.B. Melderprüfungen, Steuerungsprüfungen)



Nichtautomatische Prüfungen umfassen Vorgänge, die teilautomatisiert oder nur durch manuelle Einträge in die Prüfungsunterlagen übernommen werden. (z.B. Prüfung der Handfeuerlöscher, Brandschutztüren)



## 6.4 Betriebssysteme



## 6.5 Einsatzvorteile

### Optimierung bestimmter Wartungsabläufe

- Kontrolle ausgelöster Melder vor Ort
- Kontrolle der zugehörigen Laufkarte
- Sprachansage am mobilen Endgerät
- Erstellung der Dokumentation
- Zusatzinformationen (Mängel- und Prüflisten)
- Ab- und Zuschaltungen zu prüfender Meldergruppen (abhängig vom Protokoll der BMZ)
- Datenzugriff ohne externe Server
- Nutzung vorhandener Infrastruktur beim Kunden
- Feuerinformation als Echtzeit-Anzeige
- Import der Anlagendaten
- Export der Wartungsdaten
- Automatisches Erkennen durch Service-Schnittstelle (System4000)
- Mehrere Prüfungen im Objekt gleichzeitig

### Effizienter Personaleinsatz

- Ein-Mann-Revision
- Kontrolle der geprüften Daten wird vereinfacht
- Wartungsstand ablesbar (Online-Modus notwendig)
- Unterstützung / Prüfung bei Erstinstallation / Einschalthilfe

## 6.6 Leistungsmerkmale / Bedienkonsole

- Anlegen von Wartungsdatenbanken
  - Erzeugen von Dokumenten und Übersichten
  - Einblenden von „Alarmen“
  - Sprachansage
  - Alarmton
  - Projektverwaltung
  - Durchführen und Unterbrechen der Wartung
  - Steuerung in Abhängigkeit des Protokolls der BMZ
  - rote LED „Netz / Akku“
  - gelbe LED „Störung“
  - grüne LED „Status“
  - LED „Power“
  - LAN-/USB-/SIM-/ADP-FAT-Slot
- Spannungsversorgung:
- 230 V / DC
  - 2 x 12 V Akkus

## 6.7 Lieferumfang IRAS-Wartungsbox

- IRAS-Wartungsbox inkl. Netzteil
- Produkt-Nummer: 9102.2075
- Dokumentation
- 2 Akkus
- Netzkabel
- Kunststoffkoffer IP65
- UMTS-Modul (ohne SIM-Karte)
- WLAN-Modul
- Servicekabel (2,5 m)
- WLAN-Antenne
- UMTS-Antenne (Kabel 2,5 m)



Optional (Aufpreis):

- IRAS-WB Anschaltbox passiv (9102.2144)



- IRAS-WB Anschaltbox aktiv, mit ADP4000 (9102.2145)



## 7 IRAS-Sync-Server

Synchronisation für IRAS-Wartungsboxen

Diese browserbasierende Applikation zur Synchronisation von IRAS-Wartungsboxen (IRAS-WB) ermöglicht den Einblick in den Prüfstatus von Projekten, das Anlegen und Erweitern von Prüfungen und die Verarbeitung von Dokumenten. Der IRAS-Sync-Server stellt einen Speicherplatz zur Verfügung, welcher durch die IRAS-WB verwendet werden kann. Die Synchronisation wird durch das Zielsystem eingeleitet. Beide Teilnehmer benötigen dafür einen Zugang zum Internet.

Leistungsmerkmale:

- Synchronisation von IRAS-Wartungsboxen
- Aktualisierung des Datenstandes
- Hinzufügen von neuen Projekten (z. B. für Neukunden)
- Bearbeiten von Projekten (z. B. Erweiterungen, FW-Laufkarten)
- Speichern von Projektendaten (als Backup)
- Druck von Wartungsdokumenten
- Administration von beliebig vielen IRAS-WB
- mit USB-Massenspeicher erweiterbar
- verwaltbare Meldepunkte

Schnittstellen:

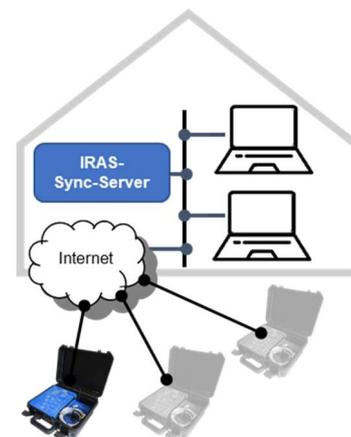
- 1 x USB 2.0,
- Ethernet 100Mbps

Systemvoraussetzung:

LAN-Zugang mit von außen erreichbarer Internetadresse!

Lieferumfang:

- PC, Netzteil, Akku, Gehäuse
- Dokumentation



## 8 Störungs- und Wartungsmanagement

Die Foxtag GmbH und IFAM GmbH Erfurt verbinden Ihre Lösungen zum Wartungsmanagement von Sicherheits- und brandschutztechnischen Anlagen. Dies ermöglicht Serviceunternehmen eine Software zu nutzen, die den kompletten Serviceprozess von Planung bis Protokoll abbildet, für alle Brandschutzanlagen verwendbar ist und zudem für Brandmeldeanlagen die besonders effiziente „Ein-Mann-Wartung“ ermöglicht.

Die Foxtag-Lösung ermöglicht Serviceunternehmen eine Software zu nutzen, die den kompletten Serviceprozess von Planung bis Protokoll abbildet, für alle Brandschutzanlagen verwendbar ist und zudem für Brandmeldeanlagen die besonders effiziente „Ein-Mann-Wartung“ ermöglicht.

IFAM bietet mit der IRAS-Wartungsbox ein System zur Wartung von Brandmeldeanlagen an, welches eine personalschonende „Ein-Mann-Wartung“ von Brandmeldeanlagen ermöglicht. Dabei wird bei der Wartung die von der Brandmelderzentrale (BMZ) registrierte Auslösung von Meldern bei vorhandener Internetverbindung in der App dem Prüfer angezeigt und als Prüfergebnis gespeichert.

Technisch funktioniert die gemeinsame Nutzung von Foxtag und der IRAS-Wartungsbox wie folgt: Die IRAS-Wartungsbox wird an die Brandmelderzentrale (BMZ) angeschlossen über die serielle Schnittstelle des Redundanzadapters ADP4000. Grundsätzliche Voraussetzung dafür ist die Feuerperipherie der Systeme 3000 oder 4000. Die Durchführung der Revision und deren Dokumentation erfolgen über die Foxtag-App. Dabei werden die bei der Wartung erzeugten Melderauslösungen in der BMZ mitgeschrieben und von der IRAS-Wartungsbox über eine Schnittstelle an Foxtag übergeben und in der Foxtag-App angezeigt und als geprüft gespeichert. Dabei wird auch der Status der BMZ, besonders im Hinblick auf „FEUER“ ständig überwacht. In Abhängigkeit des Protokolls der BMZ bleibt die Anlage außerdem bedienbar!

Foxtag bietet eine optimale Kombination für die Instandhaltung von technischen Anlagen

- Planen von Wartungs- und Serviceterminen
- Zugriff auf die komplette Wartungs- und Störungshistorie
- umfangreiche Anpassungsmöglichkeiten aller Berichte und erfassten Daten
- Verwaltung von Störungstypen für unterschiedliche Anlagen und Gewerke
- Übernahme der Wartungsdaten aus der BMZ durch IRAS



Für die Nutzung der FOXTAG-Applikation ist ein separater Zugang mit der FOXTAG GmbH zu vereinbaren. Die Verbindung zwischen IRAS und FOXTAG stellt sicher, dass die Daten der Melderprüfungen und Prüfung von Steuerungen automatisch in die FOXTAG-Dokumentation übernommen werden und damit eine manipulationsarme Prüfliste dem Betreiber zur Verfügung gestellt werden kann. Die Digitalisierung der Prüfung unterstützt die Ein-Mann-Wartung!

Die Lösung ist seit Ende März 2020 verfügbar und kann auf Wunsch nach einer telefonischen Live-Demo 30 Tage kostenlos getestet werden.

## 9 Fazit

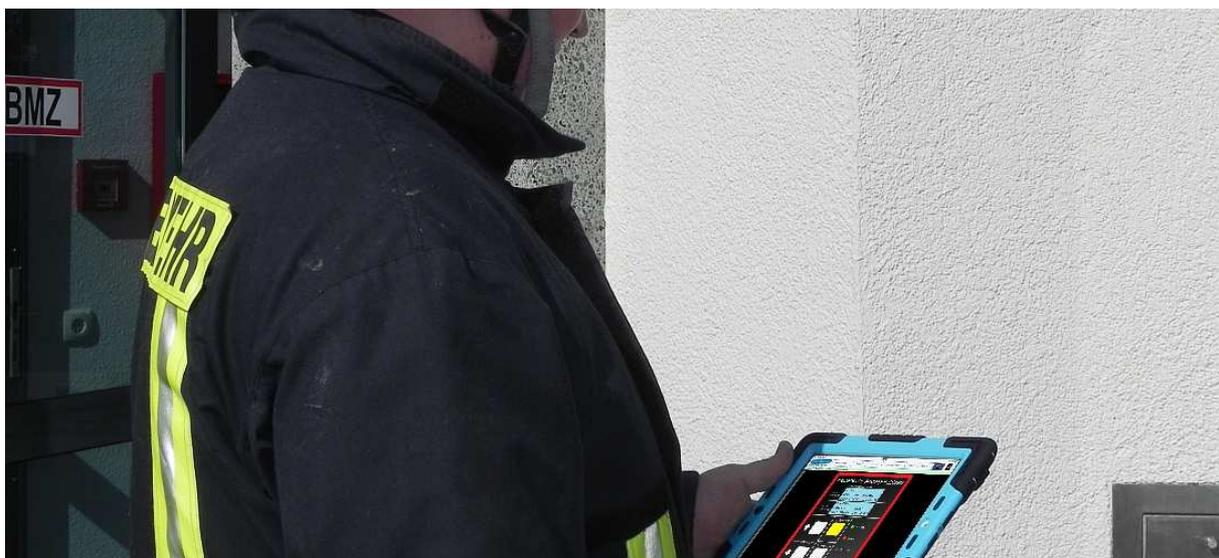
Die webbasierende Gefahrenmeldung IRAS ist für viele Anwendungen eine sinnvolle Ergänzung zu den bestehenden Geräten und Systemen. Ein Ersatz für die konventionelle Übertragung der Alarme stellt sie nicht dar. Besonders für Betreiber und Errichter besitzt IRAS einen hohen Mehrwert und unterstützt die Überwachung der BMZ sowie die Alarmierung im Gefahrenfall. Das Wartungstool erleichtert die Revision der Techniker vor Ort.

IRAS ist für mobile Empfangsgeräte mit Hilfe moderner Übertragungsverfahren ein Alarmierungssystem ohne vollumfängliche Rückwirkung des Bedienfeldes einer BMZ. Nur in Absprache und unter Hinzunahme der Einverständniserklärungen aller Beteiligten (Betreiber, Errichter, Brandschutzbehörde) sollte die FBF-Funktionalitäten freigegeben werden.

Gleichwohl viele Berufsfeuerwehren die Sammelmeldung der detaillierten Information vorziehen, werden für Objekte mit hohem Gefahrenpotential derartige Möglichkeiten neue Wege der Einsatztaktik zur Brandbekämpfung öffnen. Gerade im Bezug auf den Einsatz von Werkfeuerwehren und die damit verbundene Alarmorganisation kann IRAS eine Vielzahl an wichtigen Informationen übernehmen.

Betreiber besitzen nun eine Ergänzung zur herkömmlichen Alarmübertragung und können besonders im Bereich „Organisatorischer Brandschutz“ noch besser eingreifend tätig werden. Das macht Maßnahmen transparent, minimiert Risiken und senkt Kosten.

Für Errichter ist IRAS ein Wartungs- und Kontroll-System. Schon ab einer Inbetriebnahme können mit Einverständnis des Betreibers so Störquellen oder Schwachstellen frühzeitig festgestellt werden. Es hilft bei der Wartung ausgelöste Melder zu kontrollieren und zu protokollieren. Langzeitspeicherung erlaubt den direkten Vergleich zwischen den Wartungsgängen, erinnert an versäumte Bereiche und gestattet eine neue Ausrichtung des „Organisatorischen Brandschutzes“.



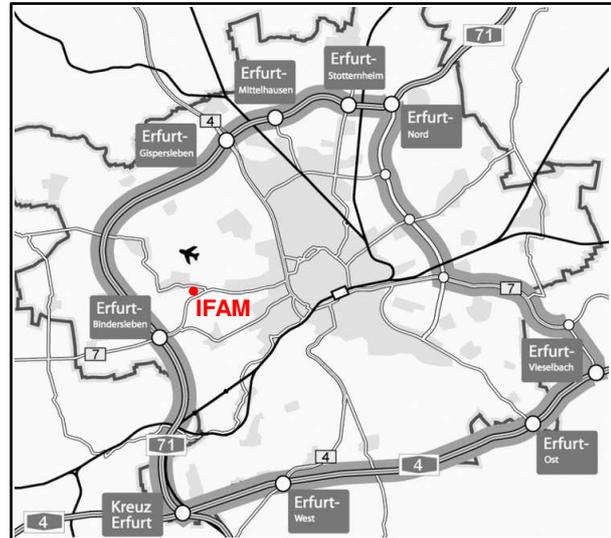
## 10 Ansprechpartner

IFAM GmbH Erfurt  
Ingenieurbüro für die Anwendung der  
Mikroelektronik in der  
Sicherheitstechnik

Parsevalstraße 2  
D-99092 Erfurt

Tel.: +49 (0) 361 / 65 911 - 0  
Fax: +49 (0) 361 / 64 62 139

ifam@ifam-erfurt.de  
www.ifam-erfurt.de  
www.ifam.eu



Vertriebsleitung  
Herr Thomas Popp  
Tel.: 0361 / 659 11 - 13  
vertrieb@ifam-erfurt.de

Vertrieb  
Frau Stefanie Lang  
Tel.: 0361 / 659 11 - 62  
vertrieb@ifam-erfurt.de

Technik-Hotline  
Herr Rainer Deutsch  
Tel.: 0361 / 659 11 - 30  
service@ifam-erfurt.de

Marketing  
Herr Uwe Hoffmann  
Tel.: 0361 / 659 11 - 25  
marketing@ifam-erfurt.de



IFAM GmbH Erfurt

INGENIEURBÜRO FÜR DIE ANWENDUNG  
DER MIKROELEKTRONIK IN DER SICHERHEITSTECHNIK

Parsevalstraße 2  
D-99092 Erfurt

Tel.: +49 (0) 361 / 65 911 – 0

Fax: +49 (0) 361 / 64 62 139

[ifam@ifam-erfurt.de](mailto:ifam@ifam-erfurt.de)

[www.ifam.eu](http://www.ifam.eu)



08/2021 – Technische Änderungen vorbehalten!