Netzwerkanforderungen Safe Fire House Brandwarnsystem

Netzwerkanforderungen — Safe Fire House Brandwarnanlage

Gültig für die PoE-Zentrale, PoE-Repeater und das PoE-Display

---

Vor Inbetriebnahme der Komponenten die Betriebsanleitung lesen

Diese Anleitung ist Teil des Produktes. Die Nichtbeachtung der Vorgaben dieser Anleitung kann eine Beeinträchtigung der Funktion oder die Beschädigung des Gerätes, anderer Sachwerte sowie Personenschäden zur Folge haben.

- Vor jeder Inbetriebnahme sind die entsprechenden Kapitel dieser Anleitung zu lesen und die enthaltenen Sicherheitshinweise zu beachten.
- Die Anleitung ist an jeden nachfolgenden Benutzer zu übergeben.
- Fragen und Hinweise bitte als Serviceticket stellen. Einen Link dazu finden Sie am Ende dieser Anleitung.

Urheberrecht

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

---

1. Einleitung

1.1 Rollenverteilung und Haftung

Die Dexa Solutions GmbH nimmt im Projekt die Rolle des Systemintegrators ein. Wir konzipieren den Lösungsansatz und setzen ihn nach Ihren Vorgaben um. Dabei kommen verschiedene technische Komponenten von namhaften Hard- und Softwareanbietern sowie eigens entwickelte Hard- und Software zum Einsatz. Wir sind nicht Hersteller aller zum Einsatz kommenden Komponenten und übernehmen daher nicht die Produkthaftung der Fremdhersteller, außer für von uns durchgeführte Modifikationen. Diese obliegt weiterhin, genau wie die Gewährleistung und Garantie, dem Hersteller der jeweiligen Komponente. Auf Seiten der Software haften wir in vollem Umfang für die eigens entwickelten Softwareteile, naturgemäß jedoch nicht für die Softwareteile von Drittanbietern.

Unsere Anlage orientiert sich an ausgewählten technischen Anforderungen der VDE 0833-1 (allgemeiner Teil). Es werden teilweise VdS- bzw. EN 54-zertifizierte Rauchmelder eingesetzt, teilweise nicht zertifizierte Rauchsensoren. Die Anlage erfüllt daher ausdrücklich nicht die Anforderungen an bauordnungsrechtlich

geforderte Brandmeldeanlagen nach VDE 0833-2/DIN 14675, wie sie insbesondere in Sonderbauten (z. B. Schulen, Krankenhäuser, Beherbergungsbetriebe) verlangt werden.

In Fahrzeugen sowie in Gebäuden oder Räumen, für die keine bauordnungsrechtliche Pflicht zur Installation einer Brandmeldeanlage nach VDE 0833-2/DIN 14675 besteht, kann die Anlage eingesetzt werden. Sofern die Integration in ein Brandschutzkonzept erfolgt, kann die Anlage als ergänzende technische Maßnahme zur Verbesserung der Früherkennung und Alarmierung berücksichtigt werden, ohne eine bauordnungsrechtlich geforderte Brandmeldeanlage zu ersetzen.

Als Kunde stellen Sie Teile Ihrer IT-Infrastruktur, zum Beispiel einen Netzwerkanschluss mit Internetzugang, WLAN oder Eingangsschnittstellen zu Alarmsystemen bzw. Gebäudetechnik oder Brandmeldeanlage zur Verfügung. Diese muss am Tag der Inbetriebnahme gemäß der abgesprochenen Anforderungen vorbereitet sein. Für das nachhaltige Funktionieren dieser Infrastruktur tragen Sie als Kunde die Verantwortung. Für ein langfristiges Funktionieren können wir, etwa wenn Sie künftig Änderungen vornehmen, keine Haftung übernehmen.

Manche Alarmsysteme, wie zum Beispiel Alamos, werden lokal durch den Kunden gehostet. Hier trägt dieser die Verantwortung für das Funktionieren der bereitgestellten Schnittstelle. Andere Systeme, wie zum Beispiel Divera 24/7, sind Cloud-basiert. Hier wird die Schnittstelle direkt vom Hersteller betrieben. Wir können für den Fall, dass dieser Änderungen vornimmt und dadurch Funktionseinschränkungen auftreten, keine Haftung übernehmen. Unsere Systeme sind aber darauf ausgelegt, in diesem unwahrscheinlichen Fall nachträglich mit nur geringem Aufwand, z. B. per Fernwartung, angepasst zu werden. Die Zusage zur Anbindung von individuellen und wunschgemäßen Schnittstellen, die durch uns noch nicht entwickelt sind, erfolgt unverbindlich und im Rahmen der Verhältnismäßigkeit. Dies gilt ebenso für den Einsatz von besonderen Hardwarekomponenten.

Damit die Zusammenarbeit gelingt und der Verbau der Innenraumüberwachungssysteme zu einem nachweislichen Erfolg wird, endet jede Inbetriebnahme mit einem umfangreichen Funktionstest, der dokumentiert wird. Darüber hinaus kann jeder Melder bzw. Sensor zu jeder Zeit eigenständig getestet und somit die Funktionssicherheit überprüft werden. Den Einsatzkräften wird dies ausdrücklich als Probealarm angezeigt, sodass es nicht zu Missverständnissen kommt.

Sofern der Anschluss an eine vorhandene Brandmeldeanlage gewünscht ist, wird dieser in der Regel durch das Schalten eines potenzialfreien Eingangskontaktes realisiert. Dieser muss Ihrerseits, bzw. durch den Servicetechniker der Wartungsfirma der Brandmeldeanlage, bereitgestellt werden. In der Nähe des Kontaktes muss im fünf Meter Abstand eine 230V-Steckdose vorhanden sein. Für den Anschluss unseres Schaltaktors an Ihre Brandmeldeanlage gelten die gültigen Aufschaltbedingungen Ihrer zuständigen Brandschutzbehörde. Diese geben in der Regel vor, dass Sie nur nach DIN 14675 bzw. EN 54 zertifizierte Komponenten, also Teile anderer Brandmeldeanlagen, anschließen dürfen. Naturgemäß ist dies bei unserem System nicht der Fall, da es für die Überwachung von Innenräumen der Fahrzeuge kein technisches Regelwerk gibt. In den allermeisten Fällen lässt sich ein Anschluss unseres Systems an Ihre BMA aber trotzdem realisieren, da fast alle behördlichen Aufschaltbedingungen eine Öffnungsklausel haben, die besagt, dass die zuständige Behörde im Rahmen Ihrer Genehmigung von den vorangestellten Anforderungen abweichen kann. Sie müssen daher, sofern Ihre Brandmeldeanlage bei einer Feuerwehr-Leitstelle aufgeschaltet ist, vor der Inbetriebnahme eine entsprechende Genehmigung einholen. Die Verantwortung hierfür liegt beim Auftraggeber.

1.2 Hinweise zum Datenschutz

Bitte beachten Sie die folgenden Informationen bezüglich des Datenschutzes in Verbindung mit der Fernwartungsfunktion sowie unseres Online-Service-Logbuchs, die in unserem System enthalten ist:

1. Zweck der Fernwartung: Die Fernwartungsfunktion ermöglicht es unserem technischen Support-Team, auf Ihr System zuzugreifen, um Wartungs- und Supportdienste zu erbringen, Updates durchzuführen und Probleme zu diagnostizieren und zu beheben. Dies geschieht auf freiwilliger Basis. Die Fernwartungsfunktion ist standardmäßig immer aktiv. Wünschen Sie dies nicht, müssen Sie uns darauf schriftlich hinweisen.

2. Datenschutz und Sicherheit: Wir nehmen den Schutz Ihrer Daten ernst und ergreifen angemessene technische und organisatorische Maßnahmen nach Art. 32 DSGVO, um sicherzustellen, dass Ihre Daten während der Fernwartung sicher und geschützt bleiben. Jeglicher Zugriff auf Ihr System erfolgt unter Einhaltung geltender Datenschutzgesetze und unserer IT-Sicherheitsregeln. Der Fernwartungszugriff erfolgt ausschließlich über verschlüsselte, mehrfach authentifizierte Verbindungen.

3. Datenerhebung und -verarbeitung: Während der Fernwartung sowie im Rahmen des zentralen Service-Logbuchs werden technische Informationen, Fehlerprotokolle sowie Standort- und Anlagendaten (Bezeichnung des Standortes, Anschrift der Anlage, technische Kennwerte) verarbeitet. Namen, Privatanschriften oder Telefonnummern natürlicher Personen werden hierbei nicht erhoben. Für den Versand von Serviceberichten und Test-Meldungen sowie ggf. Alarm-Meldungen werden die E-Mail-Adressen der jeweiligen Empfänger verarbeitet; hierbei handelt es sich um personenbezogene Daten, deren Verarbeitung nach den Vorgaben der Datenschutz-Grundverordnung (DSGVO) erfolgt. Der E-Mail-Versand erfolgt über einen Auftragsverarbeiter mit Datenverarbeitung in der Europäischen Union auf Grundlage eines Auftragsverarbeitungsvertrags nach Art. 28 DSGVO. Die vorgenannten Daten werden ausschließlich für Support-, Überwachungs- und Produktverbesserungszwecke verwendet und nicht an sonstige Dritte weitergegeben, es sei denn, dies ist gesetzlich vorgeschrieben oder wird von Ihnen autorisiert.

4. Zentrales Service-Logbuch: Zusätzlich zu den oben genannten Informationen möchten wir darauf hinweisen, dass Anlagendaten in ein zentrales Service-Logbuch geschrieben werden. Diese Daten dienen der Überwachung und Optimierung der Systemleistung und -zuverlässigkeit und werden gemäß den geltenden Datenschutzbestimmungen verarbeitet.

5. Weitere Informationen und Ihre Rechte: Die vorstehend beschriebene Verarbeitung im Rahmen von Fernwartung und Service-Logbuch erfolgt in Übereinstimmung mit der Datenschutz-Grundverordnung (DSGVO). Die für Ihr System maßgeblichen Rechtsgrundlagen, Speicherdauern und eingesetzten Auftragsverarbeiter sowie Ihre Betroffenenrechte (u. a. Auskunft, Berichtigung, Löschung, Einschränkung und Widerspruch) ergeben sich aus den mit Ihnen getroffenen vertraglichen Datenschutzvereinbarungen, insbesondere dem Auftragsverarbeitungsvertrag nach Art. 28 DSGVO. Bei Fragen zum Datenschutz wenden Sie sich bitte an unseren Ansprechpartner für den Datenschutz über die am Ende dieser Anleitung genannten Kontaktdaten.

---

2. Hinweis zur Verbindung

Die Zentrale und der Repeater müssen sich im gleichen Netzwerksegment befinden und über einen Internetzugang verfügen.

Die Rauchmelder und Sensoren kommunizieren per Funk (868 MHz) mit Zentrale und Repeater und stellen keine Anforderung an Ihr Netzwerk.

2.1 Netzwerkanforderungen für Einzelstandort

- **Anschluss:** RJ45 mit PoE
- **PoE-Protokoll:** 802.3af (PoE) / 802.3at (PoE+)
- **Übertragungsrate:** 10/100/1000 Mbps

2.2 Zusätzliche Netzwerkanforderungen für Multistandort

Wenn das System standortübergreifend eingesetzt werden soll, bedarf es einer Vernetzung der Standorte im selben Netzwerk. Dies kann über VPN-Systeme wie WireGuard, ZeroTier, IPSec o. ä. erfolgen. Alternativ auch über ein VXLAN / VLAN. Hierfür sind folgende Anforderungen zwingend erforderlich:

- **Netzwerktyp:** Die Kommunikation zwischen den Standorten erfolgt über Multicast. Die genutzte Multicast-Gruppe 224.0.0.120 liegt im link-lokalen Bereich (224.0.0.0/24) und wird nicht geroutet. Eine standortübergreifende Kopplung muss daher als **Layer-2-Verbindung (Bridge über das VPN)** ausgeführt werden; ein reines Layer-3-Routing der Multicast-Pakete ist für diese Gruppe nicht möglich.
- **Kommunikationsart:** Multicast
- **Architektur:** Am besten gleicher IP-Adressbereich, gleiches Subnetz.

Die Multicast-Gruppe, über die kommuniziert wird, ist 224.0.0.120. Es ist sinnvoll, den gesamten Multicast-(udp)-Verkehr zwischen den Repeatern und der Zentrale zu erlauben. Zusätzlich werden hierfür die Ports 9292 (tcp), 43439 (tcp) und 43438 (udp) genutzt. Die gesamte Kommunikation läuft im VPN-Netzwerk ab. Freigaben in das Internet sind für die Verbindung zwischen Zentrale und Repeater nicht notwendig, außer Sie nutzen ZeroTier als Relay-Dienst.

Der Multicast-Verkehr kann über folgenden Befehl (Linux) eingesehen werden:

```
tcpdump -i eth0 -n 'udp and dst 224.0.0.120'
```

Bitte eth0 ggf. durch das verwendete Interface ersetzen.

Achten Sie bei der Gestaltung der Netzwerkarchitektur in Ihren VPN-Routern oder Firewalls auf sauberes Bridging der Interfaces, sodass keine Loops entstehen. Multicast-Pakete gehen „wild" über alle Interfaces, je nach Routing und Bridging. Lassen sich Loops nicht vermeiden, aktivieren Sie Beschränkungen wie z. B. das Spanning Tree Protocol (STP) und Multicast-Begrenzungen (z. B. bei ZeroTier).

Falls Sie Fragen zur Umsetzung haben, sprechen Sie uns an. Gerne bieten wir Ihnen die Vernetzung Ihrer Standorte als zusätzliche Leistung in einem Vorprojekt an.

2.3 Einsatz hinter einer Firewall

Beim Betrieb der PoE-Zentrale hinter einer Firewall ist zu beachten, dass die Endpunkte gemäß folgender Tabelle sowie die genannten Ports erreichbar sind. Es wird hier anhand von Divera 24/7 lediglich ein Beispiel für eine Alarmschnittstelle gegeben. Für die Erreichbarkeit weiterer Alarmdienste und Schnittstellen sind die Dokumentationen der jeweiligen Anbieter zu konsultieren. Bitte sprechen Sie uns an, falls Sie Unterstützung benötigen.

Bitte stellen Sie sicher, dass alle genannten Ziele, Ports und Protokolle in Ihrer Firewall freigegeben sind, um eine reibungslose Funktionalität der PoE-Zentrale und angeschlossener Geräte zu gewährleisten.

Unser System benötigt keine eingehenden Portfreigaben in Ihrer Firewall!

Verbindung	Protokoll/Port	Ziel	Zweck
PoE-Zentrale ? PoE-Repeater	Multicast (udp/43438), tcp/9292, tcp/43439	local network	Kommunikation zwischen Zentrale und Repeatern

Verbindung	Protokoll/Port	Ziel	Zweck
PoE-Zentrale ? Mailserver	SMTP (tcp/465, implizites TLS)	**`smtp.dexa.gmbh`**	Versand von Statusmails
PoE-Zentrale ? Service-Plattform	HTTPS (tcp/443)	**`hooks.airtable.com`**	Überwachung der Komponenten und Schnittstellen (Statusmeldungen)
PoE-Zentrale ? Telemetrie	FTP (tcp/21)	**`wrk01.dexa.gmbh`**	Upload von Telemetriedaten (Heartbeat)
PoE-Zentrale ? Service-Connector	HTTPS (tcp/443), STUN (udp/3478)	**`controlplane.tailscale.com`**, **`login.tailscale.com`**, **`*.tailscale.com`**	Fernwartung (Koordination und Relay)
	WireGuard (udp/41641)	direkte Peer-Verbindung (ausgehend)	Fernwartung (direkter Tunnel)
PoE-Zentrale ? Internet-Erreichbarkeit	ICMP (Echo/Ping)	**`8.8.8.8`**	Konnektivitätsprüfung (WatchDog)
PoE-Zentrale ? Zeitserver	NTP (udp/123)	**`0-3.de.pool.ntp.org`**	Synchronisation von Datum und Uhrzeit
PoE-Zentrale ? DNS-Server	udp/53, tcp/53	interner DNS-Server (local network)	DNS-Namensauflösung
PoE-Zentrale ? Alarmierungsschnittstellen (Beispiele)	HTTPS (tcp/443)	**`app.divera247.com`** (Beispiel)	Alarmierung (Beispiel Divera 24/7)
	HTTP/HTTPS, lokal (Port gemäß Ihrer Installation)	localhost bzw. local network	Beispiel Alamos (lokal beim Kunden gehostet)
PoE-Display ? PoE-Zentrale	HTTP	local network	Lokale Kommunikation mit dem Frontend

Hinweis zur Internet-Erreichbarkeit: Die Zentrale prüft ihre Internetverbindung per ICMP-Echo (Ping) an **`8.8.8.8`**. Sollte ausgehender ICMP-Verkehr in Ihrer Firewall nicht zulässig sein, kann diese Prüfung auf Wunsch deaktiviert werden. Bitte sprechen Sie uns in diesem Fall an.

Hinweis zum Zeitserver: **`0-3.de.pool.ntp.org`** verweist auf einen öffentlichen Zeitserver-Pool mit wechselnden IP-Adressen. Erlauben Sie hierfür den ausgehenden NTP-Verkehr (udp/123) oder hinterlegen Sie einen festen Zeitserver.

---

3. Weitere Informationen und Technische Daten

- Weitere Informationen finden Sie in unserer Knowledge Base: https://docs.dexa.gmbh/books/faq

---

4. Kontaktdaten und Serviceticket

- Ein Serviceticket können Sie durch Scannen des QR-Codes auf Ihrer PoE-Zentrale/PoE-Repeater erstellen.
- Alternativ finden Sie unser Ticketsystem auch hier: https://dexa.gmbh/serviceticket

Dexa Solutions GmbH
Möhnestraße 2
59519 Möhnesee

Telefon: +49 2924 496 937 0
E-Mail: info@dexa.gmbh

Kontakt als QR Code für Ihr Mobiltelefon: