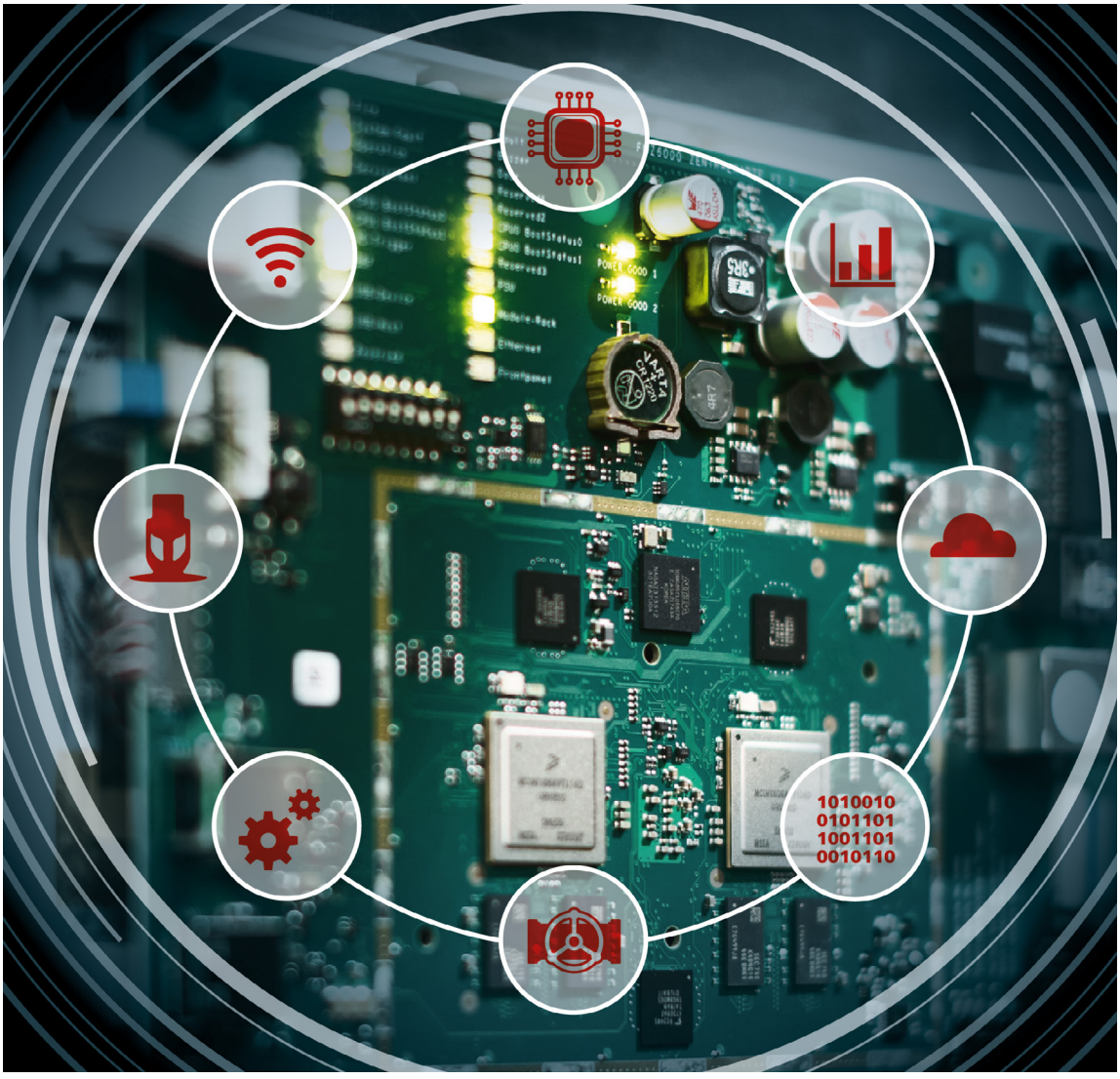
BUNDESVERBAND TECHNISCHER BRANDSCHUTZ e. V.

BRANDSCHUTZWISSEN

Merkblatt

Sichere Ferndienste für Zugriffe auf automatische Löschanlagen (Remote Services) - Rahmenbedingungen und Grenzen

Für Überwachung und Bedienung, präventive Wartungskonzepte oder auch Kompensation von Personalmangel werden klassische Brandmelde- und Löschanlagen zunehmend mit Technologien ausgestattet, die es erlauben detaillierte Informationen zum Zustand der Anlagen und deren Veränderungstrends zu gewinnen. Dienstleistungen mit Fernzugriffen erlangen dabei größere Bedeutung und stellen neue Herausforderungen an die handelnden Personen bzw. auch Organisationen dar.
Dieses Grundsatzpapier fasst den aktuellen Stand der Technik und der Richtlinienarbeit zusammen um den handelnden Personen und deren Organisation einen möglichst rechtssicheren Betrieb zu ermöglichen.



Inhalt

Vorwort

Auch wenn sich die grundsätzlichen Mechanismen im Brandschutz aufgrund physikalischer Gesetzmäßigkeiten nicht ändern, werden doch zunehmend Brandmelde- und Löschanlagen mit Sensoriken und Netzwerktechnologien ausgestattet, die es erlauben detaillierte Informationen zum Zustand der Anlagen und deren Veränderungstrends zu gewinnen.

Im Rahmen der allgemeinen Verfügbarkeit IT-basierter Dienste werden Brandschutzanlagen zunehmend auch mit anderen Gebäudemanagementsystemen vernetzt. Dies geschieht aus den unterschiedlichsten Motiven heraus. Sei es, dass Überwachung und Bedienung an zentralen Stellen beim Betreiber zusammengefasst werden sollen, präventive Instandhaltungskonzepte Verschleißdaten benötigen oder einfach nur der Mangel an Personal durch automatisierte Lösungen kompensiert werden soll. Die fortschreitende Einführung einer vernetzten Planung, den Bau und die Bewirtschaftung von Gebäuden im Rahmen des Building Information Modeling führt letztlich zum digitalen Zwilling und wird diesen Trend zusätzlich verstärken. Alle diese Technologien sind Quelle bisher unbekannter Sicherheitsrisiken und stellen neue Herausforderungen an die handelnden Personen bzw. auch Organisationen dar.

Dieses Grundsatzpapier fasst den aktuellen Stand der Technik und der Richtlinienarbeit zusammen. Es richtet sich an Hersteller von Geräten und Systemen der Brandschutztechnik, Errichter, Betreiber und Anbieter für Remote Services. Dabei werden die spezifischen Kriterien von Sicherheits-, Brandmelde- und Löschanlagen separat betrachtet. Hierbei steht nicht die Technik im Vordergrund, sondern vielmehr die Anforderungen an die handelnden Personen und deren Organisation, um einen möglichst rechtssicheren Betrieb zu erzielen.

Das Grundsatzpapier bietet einen Handlungsrahmen für das Angebot entsprechender Dienstleistungen. Darüber hinaus bietet es eine entsprechende Argumentationsbasis in Kundengesprächen und zeigt die Grenzen des Einsatzes von sicheren Ferndiensten auf.

Erstmals mit Erscheinen der DIN EN 50710 wird die Bereitstellung von sicheren Ferndiensten für Brandsicherheitsanlagen und Sicherheitsanlagen definiert. Diese umfasst Dienstleistungen, die über Kommunikationsnetze bereitgestellt werden, um den Betrieb, die Instandhaltung oder die Unterstützung von Geräten oder Systemen aus der Ferne zu ermöglichen. Die hier vorliegende Überarbeitung des ersten Merkblattes, aus dem August 2022, würdigt den Terminus der oben genannten Richtlinie.

Die hier beschriebenen Normen- und Richtlinienverweise haben keinen Anspruch auf Vollständigkeit! Sie entsprechen dem Normenstand bei Drucklegung dieses Dokumentes und können sich im Laufe der Zeit ändern, ohne dass die Änderungen in diesem Dokument berücksichtigt werden!

Im Interesse der Lesbarkeit dieses Merkblattes wird auf geschlechtsbezogene Formulierungen verzichtet. Selbstverständlich sind immer Frauen, Männer und Diverse gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

1. Anwendungsbereich

In diesem Dokument wird auf in Gebäuden installierte
- Brandmeldeanlagen,
- elektrische Steuereinrichtungen für Löschanlagen,
- elektrische Steuer- und Regeleinrichtungen für Sauerstoffreduzierungsanlagen sowie

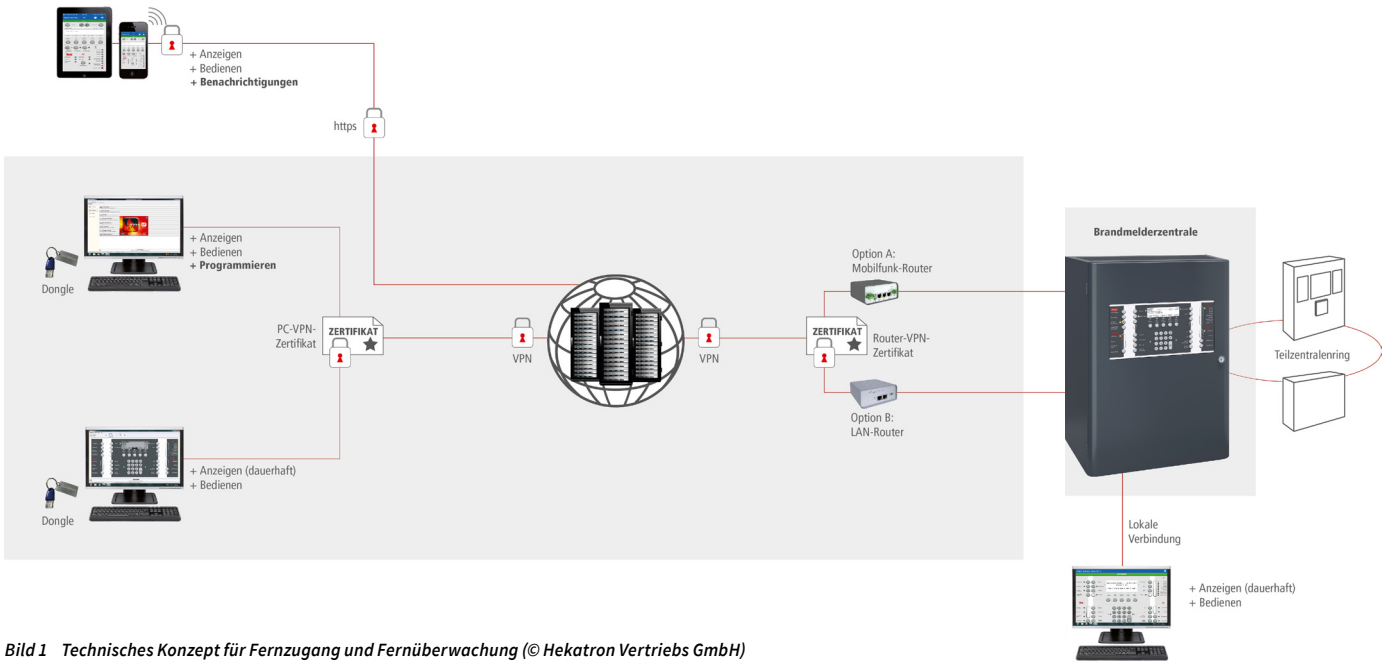


Bild 1 Technisches Konzept für Fernzugang und Fernüberwachung (© Hekatron Vertriebs GmbH)

- Überwachungseinrichtungen der technischen Funktion einer Löschanlage

Bezug genommen.

Diese, in Gebäuden installierten Anlagen, werden in der Regel täglich durch speziell qualifiziertes Personal betreut und erfordern typische Arbeitsschritte wie Inbetriebnahme, Softwarekonfiguration, Parameteranpassungen, Software- oder Firmware-Updates, Auslesen von Daten oder Instandhaltungsarbeiten, für welche Hinweise gegeben werden. Aufgrund ihrer Eigenarten können nicht ohne weiteres zugängliche Anlagen (z.B. Off-Shore Windgeneratoren) erheblichen Abweichungen unterliegen und werden daher hier nicht behandelt.

Nicht zu den Remote Services werden Techniken gezählt, welche eine Bedienoberfläche zum zentralen lokalen Zugriff oder eine lokale Visualisierung über eine direkte Verbindung innerhalb des lokalen Netzwerkes eine Brandschutzlösung bereitstellen, ohne eine Verbindung zu einem öffentlichen Kommunikationsnetz zu besitzen. Diese sind Bestandteil des jeweiligen Systems am Standort und dienen der, teilweise auch systemweiten, lokalen Bedienung.

2. Begriffe

- **BIM** Building Information Modeling
  Softwarebasierte Methode für die Planung, den Bau und den Betrieb von Gebäuden. Alle Daten der eingesetzten Komponenten werden dabei digital modelliert und dienen im Verlauf der Nutzung der Zustandserfassung.

- **OEM** Original Equipment Manufacturer = Erstausrüster

- **Ransomware** von englisch ransom für „Lösegeld“ und ware Schadprogramme, mit deren Hilfe Daten auf einem Computersystem verschlüsselt werden, um für die Freigabe ein Lösegeld zu erzielen.

- **SLA** Service Level Agreement
  Dienstgütevereinbarung zwischen allen für die bestimmungsgemäße Funktion einer Löschanlage und ihrer Remote Services erforderlichen Akteure. Definiert sowohl in welcher Qualität Dienstleistungen erbracht werden müssen, als auch welche Reaktionszeit und Ausfallrate von jedem einzelnen Dienstleister erbracht werden müssen.

- **BSI Standard** Standards und Richtlinien, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland entwickelt wurden. Diese Standards dienen dazu, die Informationssicherheit in Organisationen zu fördern und zu gewährleisten. Sie bieten Rahmenbedingungen und Empfehlungen für den Umgang mit IT-Sicherheit, Risikomanagement und den Schutz von Daten.

- **NIS-2** Richtlinie der Europäischen Union zur Verbesserung der Cybersicherheit in den Mitgliedstaaten. Sie legt Sicherheitsanforderungen für Unternehmen und Organisationen fest, die als kritisch für die Gesellschaft und Wirtschaft angesehen werden. In Deutschland wird diese Richtlinie durch das NIS2 Umsetzungsgesetz (NIS2UmsuCG) in anwendbares Recht überführt.

- **CRA** Cyber Resilience Act
  Verordnung zur Verbesserung der Cybersicherheit für Hardware und Software, die in der EU auf den Markt gebracht werden. Der Cyber Resilience Act sieht vor, in den Phasen Design, Entwicklung und Produktion sowie während des Inverkehrbringens und der Nutzung risikoangemessene Cybersecurity-Maßnahmen zu etablieren. Darüber müssen Hersteller Sicherheitslücken über einen wesentlichen Teil des Produktlebenszyklus schließen und Betreiber über behobene Schwachstellen und Cybersicherheitsvorfälle informiert werden.

3. Risiken

Ein wichtiger Aspekt beim Einsatz von sogenannten „Smart Devices“ in der Umgebung traditioneller Löschanlagen ist die Cyber Sicherheit. Dieser muß besondere Aufmerksamkeit gewidmet werden.

Angriffe auf Systeme durch Datenlecks, Fehlern in Serversoftwaren mit mehr oder weniger freiem Zugang zu den daran angeschlossenen Netzwerken oder gar Ransomware, häufen sich und steigen exponentiell an. Diese können zu umfangreichen Ausfällen wichtiger Infrastruktur führen.

In Verbindung mit einer automatischen Löschanlage sind alle möglichen Angriffsszenarien denkbar. So könnte z.B. deren Wirkweise unbemerkt aus der Ferne verändert werden. Dadurch würde ein bestimmungsgemäßer Betrieb beeinträchtigt, im schlechtesten Fall sogar Menschenleben gefährdet.

Traditionelle Löschanlagen unterliegen einem geringen Aufwand der Systempflege. Nur selten ist es erforderlich, ein einmal eingerichtetes System einer Instandsetzung zu unterziehen. Regelmäßige Inspektionen und Wartungen sorgen dafür, dass Löschsysteme über Jahrzehnte funktionsfähig bleiben.

Die Vernetzung unserer Umwelt verändert dieses Bild ganz grundsätzlich! Nicht nur stellt sie eine Herausforderung an die Entwicklung der Technik dar. Sie erfordert vielmehr eine kontinuierliche Überprüfung aller technischen Einrichtungen in der Wirkkette zwischen der Löschanlage und einem Client-Rechner. Es muss zu jedem denkbaren Zeitpunkt möglich sein, alle eingesetzten Systeme zu erreichen und Fehlerbehebungen auszuführen, auch wenn diese noch nicht aktiv zu einem Problem geführt haben. Das Einspielen von Software zur Fehlerbehebung, Firmwareupdates oder Zertifikatsupdates in jedem Gerät der Wirkkette spätestens bei jeder Instandhaltungsmaßnahme ist durch die Anforderungen der NIS-2 und des CRA Pflicht und im Umfang zu berücksichtigen. Je nach Schwere des von einem Fehler ausgehenden Risikos muss eine solche Behebung einem Betreiber auch außerhalb von Instandhaltungsverträgen angeboten werden.

Dazu braucht es feste Vereinbarungen zwischen dem Errichter und dem Betreiber, welche nicht nur die SLA regeln, sondern auch Informationsketten und Zugänglichkeiten zu den Systemen. In aller Regel ist eine Zusammenarbeit mehrerer Fakultäten, wie z.B. dem Errichter der Löschanlage, der IT des Betreibers aber u.U. auch Cloud-Service-Dienstleister erforderlich. Das gilt sowohl für die Errichtung des Systems, als auch der konstanten Betriebserhaltung über die gesamte Lebenszeit.

Die stetige Aus- bzw. Weiterbildung der beauftragten Mitarbeiter beschränkt sich nicht nur mehr auf die Funktionalität der Löschanlage, sondern auch sonst der Unternehmens-IT vorbehaltenen Informationen zu Kommunikationstechniken. Aktualität der eingesetzten Werkzeuge, Firmwaren und Softwarelizenzen, sowie deren regelmäßiger Updates, sind eine wichtige Grundvoraussetzung für die Sicherheit des Gesamtsystems. Insgesamt kann das Verhalten der Mitarbeiter eine nahezu genau so große Schwachstelle für die Anlagensicherheit darstellen. Entsprechende Unterweisungen und methodische Festlegungen sind daher bereits bei der Einführung der Technik zu berücksichtigen.

4. Rollen, Qualifikationen und Verantwortung

Um die im vorhergehenden Abschnitt beschriebenen Risiken signifikant zu reduzieren, müssen neben den Anforderungen an die Technik, die z.B. in der ISO 27000 Familie zusammengefasst sind, auch organisatorische Voraussetzungen vorhanden sein.

Für den Brandschutz liefert die DIN EN 50710 einen roten Faden an Aufgaben und Verantwortlichkeiten von der Vertragsgestaltung bis zum Abschluss eines durchgeführten Remote Service Einsatzes. Dabei unterscheidet die Norm zwischen Brandmeldeanlagen und automatischen Löschanlagen.

Unterschiedliche hohe Anforderungen, allerdings hier mit Fokus auf die Remote Service Komponenten, kennen auch die DIN EN IEC 62443 und die VdS 3836. Die Normenreihe IEC 62443 beschreibt in Summe fünf Sicherheitslevel, welche die Widerstandsfähigkeit gegen verschiedene Angreiferklassen definieren:

- **Security Level 0:**
  Keine besondere Anforderung oder Schutz erforderlich
- **Security Level 1:**
  Schutz vor unbeabsichtigtem oder zufälligem Missbrauch
- **Security Level 2:**
  Schutz vor vorsätzlichem Missbrauch mit einfachen Mitteln mit geringen Ressourcen, allgemeinen Fähigkeiten und geringer Motivation
- **Security Level 3:**
  Schutz vor vorsätzlichem Missbrauch mit anspruchsvollen Mitteln mit moderaten Ressourcen, IACS-spezifischen Kenntnissen und moderater Motivation
- **Security Level 4:**
  Schutz vor vorsätzlichem Missbrauch unter Einsatz anspruchsvoller Mittel mit umfangreichen Ressourcen, IACS-spezifischen Kenntnissen und hoher Motivation

Die Klassen der VdS3836 sind entsprechend zu den Security Levels der IEC 62443 in Bezug gesetzt:

- Klasse A orientiert sich an Security Level 1
- Klasse B orientiert sich an Security Level 2
- Klasse C orientiert sich an Security Level 3

Damit die sicheren Komponenten auch in einer qualitativ hochwertigen Umgebung betrieben werden, stehen unter anderem folgende weitere Normen zur Verfügung:

- DIN EN 50518 Alarmempfangsstellen
- DIN EN 50600 Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren
- DIN EN16763 Dienstleistungen für Brandsicherheitsanlagen und Sicherheitsanlagen.

4.1.1. Klärung der Verantwortung vor der Installation und Inbetriebnahme (Vorrausetzungen)

Vor der Einrichtung von sicheren Ferndiensten fordert die EN 50710 entsprechende Risikobeurteilungen durchzuführen. Dabei wird festgelegt, welche Remoteservices aufgrund der örtlichen Gegebenheiten, der Anwendung und der IT-Infrastruktur möglich sind. Hinweise für die Durchführung einer adäquaten Risikoanalyse gibt die DIN EN 31010. Praxisnahe Beispiele finden sich im BSI-Standard.

Die Verantwortlichkeiten und die abgestimmten Remoteservices müssen zwischen der Organisation, die die Ferndienste anbietet und dem Kunden, vertraglich festgehalten werden. Die vertraglichen Vereinbarungen müssen folgende Angaben enthalten:

- das spezifische Brandmelde- und/oder Löschsystem und dessen Installationsort
- den Umfang der zu erbringenden Dienstleistungen, die aus der Ferne durchzuführenden Operationen oder Tests, einschließlich des Zeitpunkts und der Umstände, sowie der möglicher weiteren Maßnahmen
- die juristische Person, welche für den für den Ferndienst genutzten Server verantwortlich ist
- Festlegungen wo und wie System- und Standortdaten gehandhabt und gespeichert werden
- der Prozess der Kundenautorisierung, der für jeden Vorgang erforderlich ist, und wie die Mitteilung an den Kunden erfolgt und nachgewiesen wird
- die Verwendung und Handhabung von Berechtigungsnachweisen
- die Art und Weise, wie ein Prüf-Pfad für alle Fernbedienungsaktionen geführt wird, sowie der Aufbewahrungsfrist
- alle vom Versicherer des Kunden geforderten Bedingungen
- alle Bedingungen, die ggf. von Polizei, Feuerwehr und anderen hilfeleistenden Stellen verlangt werden
- Vereinbarungen zur zeitlichen Begrenzung aktiver Fernsitzungen in Bezug auf die Lese-, Steuer- und Schreibfunktionen
- die Nutzung und Handhabung von automatisierten Verbindungen/ Sitzungen
- die Grenze der Verantwortung des Ferndienstleisters

4.1.2. Qualifikationen

4.1.3. Grundsätzliche Anforderungen an einen Remote-Zugriff

Anders als bei ausschließlich lesenden Zugriffen, darf ein Remote-Zugriff zum Zwecke der Bedienung, Parametrierung oder ähnlichen, nicht ohne eine vorherige Information durch den Remote Dienstleiter erfolgen. Vor Einleiten einer Ferndienstleistung sind der Kunde, der Diensteanbieter (falls nicht identisch mit dem Anbieter der Ferndienste), die ständig besetze Stelle und ggf. weitere Behörden (abhängig von der Risikobewertung) über die durchzuführenden Arbeiten zu informieren.

Das Ausführen von Tests durch einen Remote Zugriff ist generell möglich. Fernoperationen dürfen nicht durchgeführt werden, wenn ein Alarmzustand vorliegt und müssen abgebrochen werden, wenn während der Arbeiten ein Alarmzustand auftritt. Eine Bedienung der Brandmeldeanlage aus der Ferne darf nur durchgeführt werden, wenn diese zuvor vor Ort explizit freigegeben wurde.

Wenn durch den Remote Zugriff Beeinträchtigungen der Funktion der Brandmeldeanlage bzw. Löschanlage zu erwarten sind, muss eine verantwortliche Person beim Kunden darüber informiert werden. Nach einem Remote Zugriff muss zeitnah eine Funktionsprüfung der Anlage durch diese verantwortliche Person erfolgen. Vor Beendigung des Ferndienstes muss sichergestellt werden, dass das System voll funktionsfähig ist. Nicht aus der Ferne behebbare Fehler sind schnellstmöglich vor Ort zu beheben. Hier sind ggf. anwendbare Fristen bis zur Behebung zu berücksichtigen (z.B. VdS-Richtlinien).

Das System zur Autorisierung des Zugangs muss dem Stand der Technik entsprechen und eindeutig sein, d.h. es darf nur ein einziges System zur Verwaltung der Benutzerberechtigung verwendet werden. Die Verbindung zum Fernzugangsserver muss über sichere Mittel erfolgen. In den Räumen eines Ferndienstleisters muss Unbefugten die Sicht auf angezeigte Informationen verwehrt werden. Zugänge zu Softwareanwendungen müssen verriegelt werden, wenn das verwendete Fernzugangsterminal unbeaufsichtigt ist. Nach einer für max. 30 Minuten inaktiven Fernbedienungssitzung, muss die Sitzung beendet werden. Erfolgt die Steuerung durch ein Gerät, das sich nicht am selben Ort wie der Fernzugangsserver befindet, muss der Zugang zu diesem Gerät das gleiche Sicherheitsniveau wie der Fernzugangsserver besitzen.

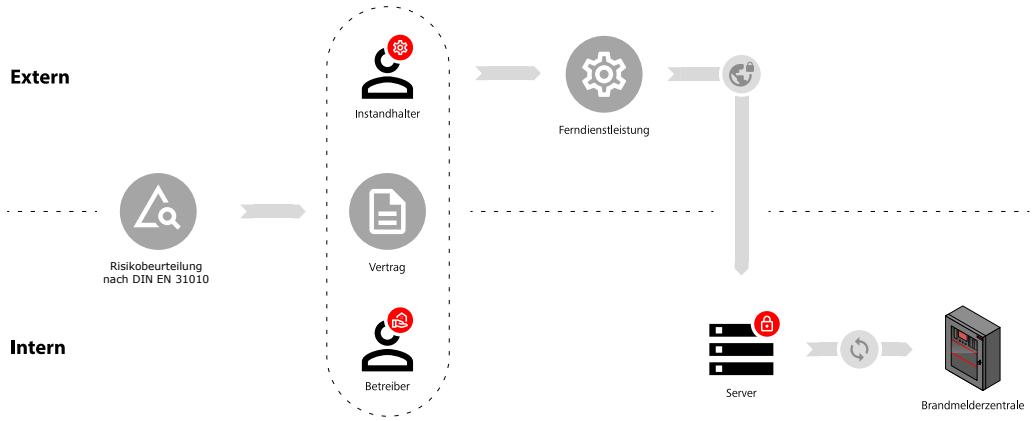


Bild 2 Aufgaben und Verantwortung vor Installation und Inbetriebnahme

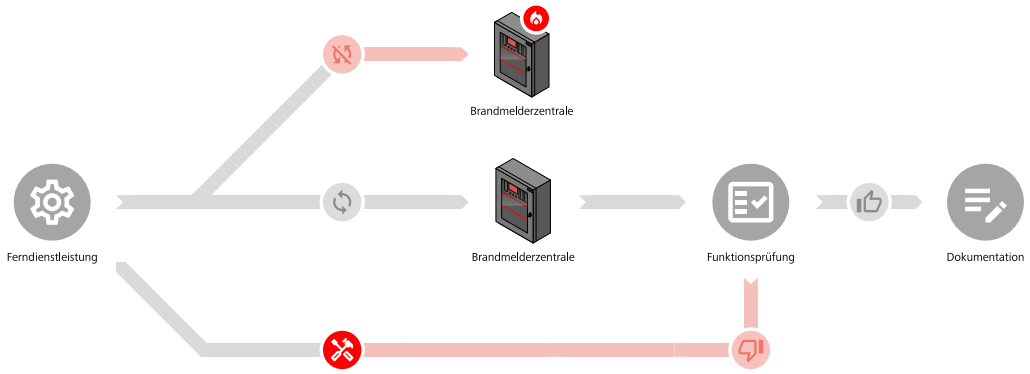


Bild 3 Grundsätzliche Anforderungen an einen Remotezugriff

4.1.4. Anforderungen an das Personal vor Ort

Grundsätzlich darf nur eingewiesenes Personal Zugang zum Server für den Ferndienst, sowie zur Remote-Service-Anwendung haben. Neben der in der Ferne wirkenden Person, muss auch vor Ort Personal an der Anlage verfügbar sein, welches:

a) über die erforderlichen Ortskennnisse verfügt,
b) auf das spezifische System ausgebildet ist und für Löschanlagen zusätzlich benannt und qualifiziert ist,
c) im Besitz der vollständigen Dokumentation ist, die den Sollzustand abbildet,
d) ausreichend Kenntnisse zur Zielfunktion der Anlage hat, um einschätzen zu können ob die Sollfunktion erreicht wird,
e) Nebenbedingungen sicher überprüfen kann (z.B. Gasdichtigkeit, Brandschutzabschottungen, etc.),
f) mit allen den relevanten Werkzeugen und Hilfsmitteln ausgestattet ist,
g) mit den Normen und technischen Spezifikationen der Löschanlage, für die die Dienstleistung erbracht werden soll, und insbesondere mit denen, die sich auf die Systemleistung beziehen, vertraut ist.

Der Mitarbeiter vor Ort kann durch einen beratenden Partner im Hintergrund unterstützt werden. Dieser Partner kann die Daten bis in die Ziel-Geräte hineinspielen, was vom Mitarbeiter vor Ort aktiv initiiert werden muss. Für lesenden Zugriff auf die Brandschutzanlage ist in der DIN EN 50710 keine besondere Anforderung an das Personal vor Ort definiert.

Allerdings muss nach der VdS 3836 jede Art der automatischen Übermittlung von Ereignisdaten bei Inbetriebnahme und nach jedem Softwareupdate durch einen autorisierten Benutzer explizit freigegeben werden.

Für notwendige Überprüfungen oder Verifikationen der Brandschutzanlage vor Ort, die durch eine Bedienung oder Parameteränderung per Remote Service notwendig sein können, fordert die DIN EN 50710, dass das berechtigte Personal vor Ort eindeutig festgelegt und qualifiziert ist. In der Praxis bedeutet dieses, dass es sich um Personal eines Errichters handeln muss, da nur dieser den Betriebsbereitschaftszustand und eine erfolgreiche Parametrierung ggf. durch weitere Tests bewerten kann. Ein Blick auf das Bedienfeld, in welchem kein Fehler angezeigt wird, ist hier nicht ausreichend!

Anders ausgedrückt darf der Remote Service immer genau so weit in das System eingreifen, wie es das Personal vor Ort auch selber hätte tun dürfen bzw. die korrekte Durchführung des Eingriffs überprüfen kann.

Eine erteilte Autorisierung muss Personal welches keinen Zugang mehr benötigt umgehend entzogen werden. Das gilt für alle Beteiligten ob beim Betreiber, beim Errichter oder auch beim Dienstleister.

Der Betreiber hat das beauftragte Personal regelmäßig zu seinen Aufgaben, den Umgang mit der Technik, sowie zu Gebrauch und Handhabung von Zugangsdaten zu schulen.

5. Phasen für den Aufbau und Betrieb

5.1.1. Planung

Nur vom Hersteller (OEM) geprüfte und freigegebene Technik darf zum Zugriff auf die Systeme verwendet werden. Der Hersteller stellt die grundsätzliche Eignung, die regelmäßige Prüfung und ggf. Adaption der Technik sicher. Sonstige, fremde Schnittstellenzugriffe sind verboten.

Im Sinne größtmöglicher Transparenz soll der Hersteller hierbei eine Übersicht aller Daten und anlagenspezifischen Parameter bereitstellen, welche übertragen werden können. Zusätzlich Informationen wo und wie Anlagen- und Objektdaten gehandhabt und gespeichert werden, sowie zu Gebrauch und Handhabung von Zugangsdaten. Übertragungen dürfen nur nach expliziter Freigabe durch den Betreiber erfolgen.

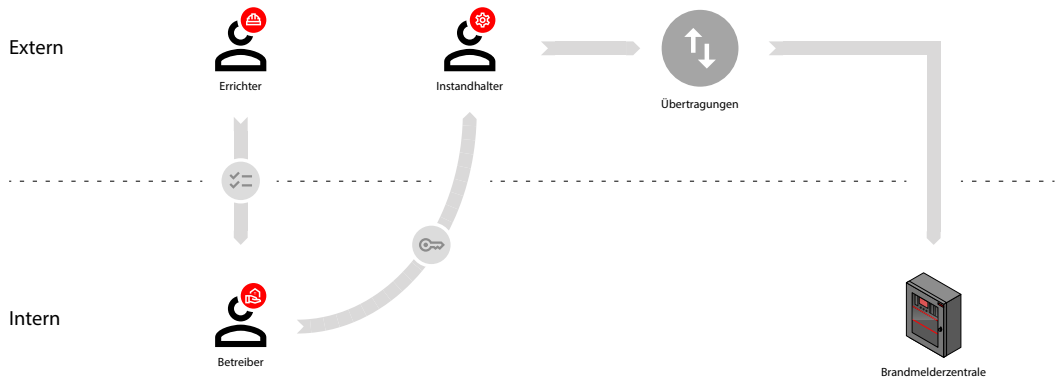


Bild 4 Freigabeszenario bei Fernzugang

Die Grundfunktionalität der Löschanlage darf nicht durch ablaufende Zertifikate, fehlende Internetanbindung oder Lizenzvereinbarungen etc. eingeschränkt werden. Hier ist das Prinzip zur Rückwirkungsfreiheit durchgängig anzuwenden.

Bestimmte Instandhaltungsmaßnahmen dürfen aus der Ferne vom Instandhalter durchgeführt werden. Dabei dürfen auch Änderungen vorgenommen werden, wenn:

- die Zugangsberechtigung zwischen dem Betreiber und dem Instandhalter schriftlich festgelegt ist,
- jeder Zugang zeitlich begrenzt ist und
- jeder Zugang mit einem der Anlagenart entsprechend qualifizierten Übertragungsverfahren stattfindet

Die Sicherheit der Übertragungsverfahren werden durch den Hersteller definiert und sind in der Regel Gegenstand der Systemanerkennung. Für ein System darf nur eine solche Technik ausgewählt werden. Die Ferndienstprozesse, Techniken und Kommunikationspfade müssen sicher und zuverlässig sein. Dies erfordert jeweils ein geeignetes Konzept und Entwurf, Dokumentation sowie umfassende Prüfungen vor der Freigabe.

Es wird empfohlen, den Aufbau einer Kommunikation mit dem Remote-System von innen nach außen zu gestalten. Das heißt, auf Veranlassung einer autorisierten Person am Ort des Löschsystems, meldet sich die Brandmelde- oder Löschsteuerzentrale bei einem zentralen Server, auf welchen auch der Errichter zugreifen kann und diesem Zugriff gestattet. In diesem Fall kann das System von der Kundeninfrastruktur entkoppelt werden, wodurch selbige nicht mehr funktionsrelevant ist. Ein solcher Aufbau reduziert ebenfalls die Zahl möglicher Angriffspunkte bzw. Szenarien.

Wesentliche Anforderungen zum IT-Grundschutz (BSI-Bro20/333), eines entsprechenden Notfallmanagements (BSI-Standard) sowie zur sicheren Bereitstellung von Web-Angeboten (Isi-Web) und Zugriffe auf die interne Netzwerkinfrastruktur (Isi-Fern) sind während der Planung zu berücksichtigen.

Zusammenfassung der Wesentlichen Prozesse und Methoden:

- ☐ Objektspezifische Risikoanalysen
- ☐ Ermittlung kritischer Strukturpunkte und Kernprozesse
- ☐ Vereinbarung der zu erbringenden Dienstleistungen und deren Abgrenzungen
- ☐ Vereinbarung von Verantwortlichkeiten
- ☐ Vereinbarung von Dokumentations- und Datensicherungsmethoden
- ☐ Festlegung von Rollen- und Berechtigungskonzepten
- ☐ Aus- und Weiterbildungsplan Mitarbeiter
- ☐ Vereinbarung zum Verfahren der Ein- und Ausleitung von Zugriffsprozeduren
- ☐ Bereitstellung einer Übersicht der übertragenen Daten und deren Zweck
- ☐ Vereinbarung von Service Level Agreements für die kontinuierliche Pflege des Gesamtsystems

5.1.2. Inbetriebnahme

Voraussetzung für eine Inbetriebnahme ist ein fertig montiertes, verkabeltes und dokumentiertes System. Typische Aufgaben während einer Inbetriebnahme, auch über Ferndienstleistungen, können sein:

- Konfiguration
- Parametrierung (einmessen)
- Funktionsprüfung
- Fehlerbehebung.

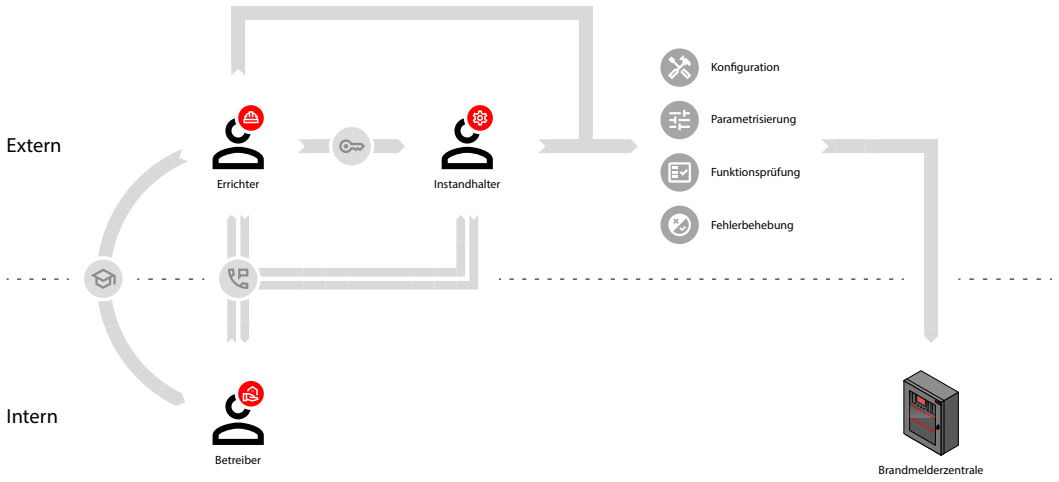


Bild 5 Aufgaben und Verantwortung während der Inbetriebnahme

Vor Beginn jeglicher Schreibfunktionen und jeglicher Überprüfungen der Anlage, ist eine Freigabe durch den Betreiber erforderlich. Alle erforderlichen Autorisierungen und Verifizierungen im Objekt müssen von einer benannten und qualifizierten Person durchgeführt werden, die in der Verwendung der installierten Anlage geschult wurde.

Nach der Ausführung von Schreibfunktionen, z.B. bei einer Konfigurationsänderung oder einer Firmware-Anpassung, Fernreparatur oder Fernparametrierung, müssen die betroffenen Funktionen der BMA und der Löschanlage im Rahmen einer Wiederinbetriebnahme geprüft werden. Diese soll im sinnvollen Ermessen erfolgen. Die Verantwortung verbleibt beim Errichter des Systems.

Generell muss der Mitarbeiter vor Ort angemessene Funktionsprüfungen und Verifizierungen vornehmen um die Funktionalität der Technik zu bestätigen, bevor visuelle oder akustische Informationen oder Zustände zurückgesetzt werden. Sämtliche Aktivitäten sind im Betriebsbuch der Anlage zu dokumentieren.

Sind Änderungen erforderlich, die dazu führen können, dass die Anlage nicht mehr funktionsfähig ist, wie z. B. eine Aktualisierung der Firmware oder eine Neukonfiguration der Anlage, müssen die folgenden Anforderungen gelten:

- Bevor die Fernverbindung hergestellt wird, müssen geeignete Kompensationsmaßnahmen getroffen werden, die so lange in Kraft bleiben, bis der Vorgang abgeschlossen und überprüft ist;
- eine Überprüfung der ordnungsgemäßen Funktion muss im Objekt durchgeführt werden, bevor die Anlage wieder in den Normalbetrieb überführt wird
- wenn die Datenübertragung nicht vollständig abgeschlossen werden kann, muss die Anlage mit den vorhergehenden Daten vollumfänglich in Funktion bleiben und der vorherige Zustand wiederhergestellt werden.

Fazit:
Für Betreiber bietet eine, durch einen Ferndienstleister unterstützte, Inbetriebnahme die Möglichkeit eines effizienteren Einsatzes des Personals. Durch das Wissen um den Zustand der Anlage und die sich ergebenden Analysemöglichkeiten, können externe Spezialisten eine schnellere Inbetriebnahme, eine sicherere Anlagenfunktionalität und die Unterstützung des Personals vor Ort mit spezialisiertem Know-How gewährleisten.

Zusammenfassung der Voraussetzungen für eine Unterstützung während einer Inbetriebnahme:

- ☐ Betriebsfertig installierte und dokumentierte Anlage
- ☐ Ortspersonal mit detaillierten Kenntnissen, Qualifikationen und Autorisierungen
- ☐ Rückfallprozedere bei Fehlern der Fernübertragung
- ☐ Freigabeprozedere vor Durchführung einer Tätigkeit
- ☐ Funktionsprüfungen und Verifizierungen nach Änderungen
- ☐ Umfassende Dokumentation im Betriebsbuch der Anlage

5.1.3. Betrieb

Eine Kernaufgabe im Betrieb von Brandmelde- und Löschanlagen liegt in der

- aktiven Störungsweiterleitung, mit detaillierten Informationen zur Störungsursache an den Betreiber zur Veranlassung von Abstellmaßnahmen
- der Fernabfrage von Zuständen,
- der Fernsteuerung oder
- Fernreparatur

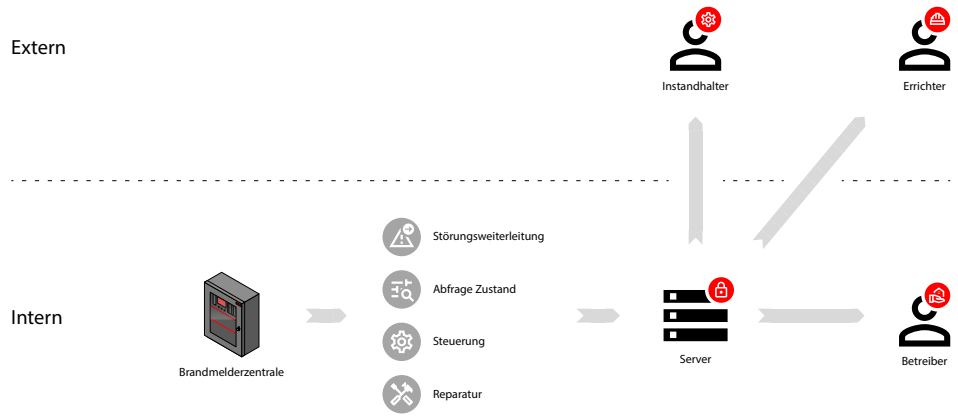


Bild 6 Kernaufgaben und Verantwortung im Betrieb

Eine solche Übertragung ersetzt jedoch nicht die Feuerwehraufschaltung und die dafür erforderliche Übertragungseinrichtung nach EN 50518. Ebenso ergibt sich durch die Erlangung von Informationen keine Handlungsverantwortung des Errichters im Alarmfalle.

Eine Auslösung einer Löschanlage ist selbstverständlich zu keiner Zeit zulässig! Ebensowenig darf eine Blockierung einer Feuerlöschanlage nicht aus der Ferne erfolgen. Alle Aktivitäten werden im Protokoll der Anlage vollständig dokumentiert und nicht löschbar aufbewahrt.

Die vom Betreiber vorgehaltene Kommunikations- und Übertragungstechnik muss, genau wie die Brandschutztechnik, kontinuierlich auf dem Stand der Technik gehalten werden und entsprechenden Update-Verfahren unterzogen werden. Hierfür sind zwischen dem Dienstleister und dem Betreiber entsprechende detaillierte Vereinbarungen abzuschließen und der jeweilige Verantwortungsübergang zu beschreiben. Diese Vereinbarung sollte schriftlich erfolgen und auch die Beschreibung der Schnittstelle, an welcher Stelle die Verantwortung beginnt oder endet, beinhalten.

Wenn das nicht möglich oder nicht prüfbar ist, muss die Fernwirktechnik isoliert ausser Funktion gehen. Die Funktion der Löschanlage ist von höchster Priorität und darf zu keiner Zeit beeinträchtigt werden.

Die für die Zwecke von Ferndienstleistungen installierten Geräte und Anlagen müssen selbst Gegenstand von Prüfungen, sowohl vor der Inbetriebnahme, als auch als Teil der vorbeugenden und fehlerbeseitigenden Instandhaltung sein und regelmäßig dem Stand der Technik folgend sowie nach den Empfehlungen des Herstellers aktualisiert werden.

Fazit:
Für Betreiber wie auch den Errichter bietet eine Fernunterstützung die Möglichkeit bessere Informationen zur Störungsursache und deren Behebung zu erhalten. Ggf. ist es möglich das Ortspersonal bei der Behebung einfacher Fehler anzuleiten. Für komplexere Themen ist in jedem Fall die Entsendung spezialisierter Techniker und die Beistellung passender Ersatzteile ein wesentlicher Baustein für eine effiziente Fehlerbehebung.

Zusammenfassung der Wesentlichen Prozesse und Methoden:

- ☐ Separate Übertragung zu Feuerwehr und hilfeleistenden Stellen vorhalten
- ☐ Bei Überprüfung und Update der Brandschutztechnik ist auch die Kommunikations- und Fernwirktechnik insgesamt zu berücksichtigen
- ☐ Die Funktion der Anlage muss auch ohne Fernwirktechnik sichergestellt sein
- ☐ Umfassende Dokumentation im Betriebsbuch der Anlage

5.1.4. Betriebserhaltung

5.1.5. Instandhaltung

Zur Instandhaltung zählen Inspektions- sowie auch Wartungsaufgaben. Für deren Unterstützung bietet sich die Abfrage von Betriebs- und Verschleißdaten förmlich an, um daraus Trendanalysen zur Vorbereitung möglicher Arbeiten abzuleiten, erforderliche Ersatz- oder Verschleißteile zu beschaffen und auch geeignete Mitarbeiter zu entsenden.

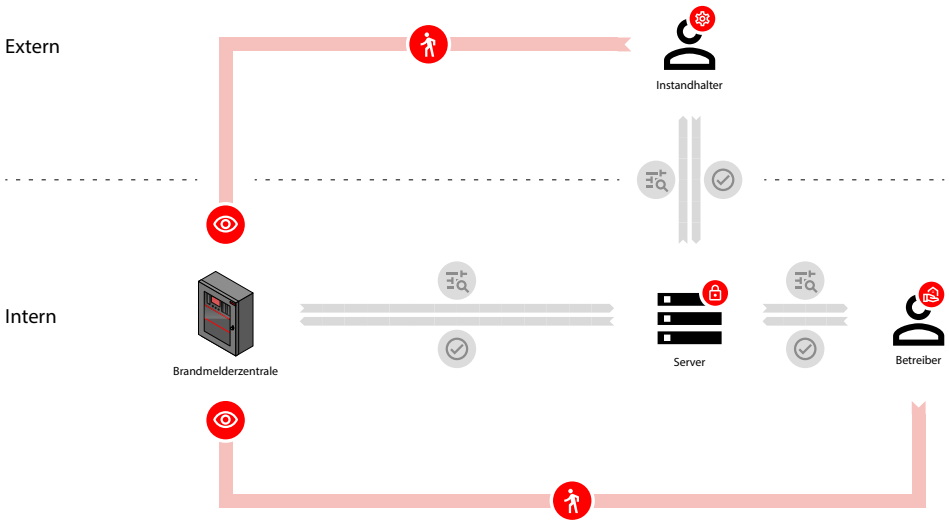


Bild 7 Abfrage von Zustandsdaten für die Instandhaltung

Die Möglichkeit der Abfrage der Betriebsdaten ersetzt nicht die vor Ort vorgeschriebenen Arbeiten. Ebenso dürfen die vorgeschriebenen Betreiberaufgaben wie z.B. Begehungen zur Prüfung der Raumnutzung und Anlagenzustand nicht ausgesetzt werden. Ein Ersatz der Person vor Ort durch Kameras ist nicht ausreichend aussagekräftig.

Ein Remote Funktionstest zur Überprüfung der Anlage im Rahmen einer Inspektion oder Instandsetzung, stellt weder eine Bewertung der kundeneigenen IT-Maßnahmen dar, noch lässt sich eine in die Zukunft gerichtete Aussage zur dauerhaften Funktion ableiten. Vielmehr stellt die Prüfung eine Stichprobe zum aktuellen Zeitpunkt dar.

5.1.6. Instandsetzung

Eine Instandsetzung wird traditionell initiiert aus einer Störung im Betrieb oder ist das Ergebnis der Inspektions- oder Wartungsarbeiten.

Eine eingesetzte Fernwirktechnik kann, wie auch bei einer Inbetriebnahme helfen, Fehler schnell zu identifizieren und eine Reparatur entsprechend effizient auszuführen. Sie ersetzt aber nicht die persönliche Anwesenheit von Personal.

Vorteil: Techniken für Fehleranalysen sind heute derart effizient, dass bereits beim ersten Einsatz die Fehlerbehebung erfolgreich ist. Sie ermöglichen dadurch eine kürzest mögliche Rückkehr in Normalbetrieb und verhindert Mehrfachaufwendungen für Reisen und Behebungsversuche.

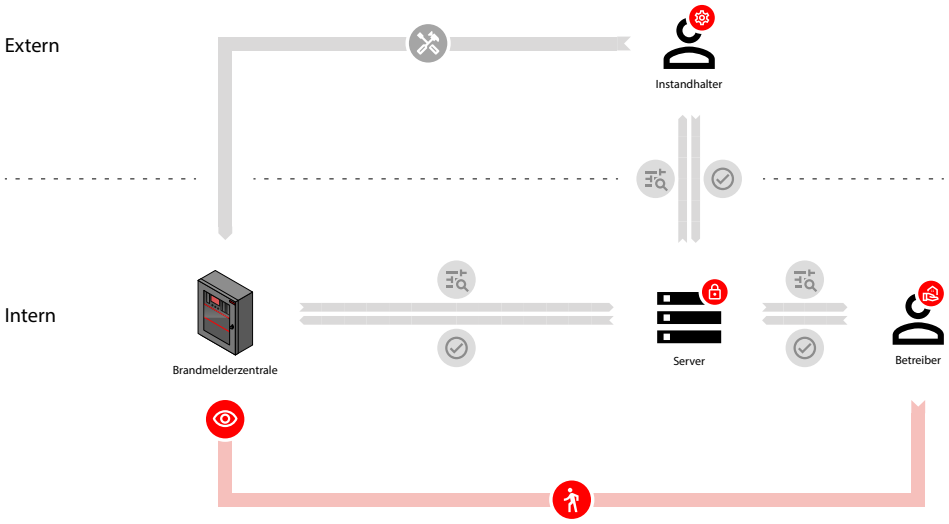


Bild 8 Aufgabenteilung und Informationsfluss für die Instandhaltung

Vor Beginn jeglicher Schreibfunktionen und jeglicher Überprüfungen der Anlage, ist eine Freigabe durch den Betreiber erforderlich. Alle erforderlichen Autorisierungen und Verifizierungen im Objekt müssen von einer benannten und qualifizierten Person durchgeführt werden, die in der Verwendung der installierten Anlage geschult wurde.

Nach der Ausführung von Schreibfunktionen, z.B. bei einer Konfigurationsänderung oder einer Firmware-Anpassung, Fernreparatur oder Fernparametrierung, müssen die betroffenen Funktionen der BMA und der Löschanlage im Rahmen einer Wiederinbetriebnahme geprüft werden. Diese soll im sinnvollen Ermessen erfolgen. Die Verantwortung verbleibt beim Errichter des Systems.

Wenn die Datenübertragung nicht vollständig abgeschlossen werden kann, muss die Anlage mit den vorhergehenden Daten vollumfänglich in Funktion bleiben.

Generell muss der lokale Mitarbeiter angemessene Funktionsprüfungen und Verifizierungen vornehmen um die Funktionalität der Technik zu bestätigen, bevor visuelle oder akustische Informationen oder Zustände zurückgesetzt werden. Sämtliche Aktivitäten sind im Betriebsbuch der Anlage zu dokumentieren.

Zusammenfassung der Wesentlichen Prozesse und Methoden:

- ☐ Ortspersonal mit detaillierten Kenntnissen, Qualifikationen und Autorisierungen
- ☐ Rückfallprozedere bei Fehlern der Fernübertragung
- ☐ Freigabeprozedere vor Durchführung einer Tätigkeit
- ☐ Funktionsprüfungen und Verifizierungen nach Änderungen
- ☐ Umfassende Dokumentation im Betriebsbuch der Anlage

5.1.7. Firmware- und Softwareupdate

Es gelten die identischen Personalanforderungen, sowie Anforderungen zur Autorisierung der Arbeitsgänge, wie bereits unter 7.1.2. Inbetriebnahme beschrieben.

Wenn die Datenübertragung eines Firmware- oder Software-Updates nicht vollständig abgeschlossen werden kann, bei einem Verbindungsverlust oder einer anderen Übertragungsstörung, die den Download unterbricht, muss die Anlage mit der jeweils vorhergehenden Version der Firm- oder Software vollumfänglich in Funktion bleiben bzw. muss die letzte voll funktionsfähige Version wiederhergestellt werden und die Brandmelde- bzw. die Löschanlage wie vor dem fehlgeschlagenen Download funktionieren. Hierfür müssen Funktionen verfügbar sein, die feststellbar machen, dass die Aktualisierung nicht sicher stattgefunden hat.

6. Dokumentation

Bei Durchführung von Instandhaltungsmaßnahmen aus der Ferne muß:

- jeder Zugang zur Brandmelde- oder Löschanlage in einem anlageeigenen Ereignisspeicher automatisch registriert wird und durch den Betreiber im Betriebsbuch vermerkt,
- jede durchgeführte Änderung des Firmware-, Software- oder Konfigurations-Standes der Anlage in einem anlageeigenen Ereignisspeicher automatisch registriert und
- die Informationen zu den Sitzungen (Anmeldung, Abmeldung, Benutzer, Vorgänge) im Ferndienstserver mit Zeitstempeln protokolliert werden.

Nach der Ausführung von Schreibfunktionen müssen die betroffenen Funktionen der Brandmelde- oder Löschanlage geprüft werden. Zusätzlich muss die Dokumentation auf den neuesten Stand gebracht werden.

Quellen

- **VdS 3836** Cyber-Sicherheit für Systeme und Komponenten
- **DIN EN 50710** Anforderungen an die Bereitstellung von sicheren Ferndiensten für Brandsicherheitsanlagen und Sicherheitsanlagen
- **IEC 62443** Industrial communication networks – Network and system security
- **ISO 27000 ff** Information security management systems
- **DIN EN 50518** Alarmempfangsstelle
- **DIN EN 50600** Informationstechnik - Einrichtungen und Infrastrukturen von Rechenzentren
- **DIN EN16763** Dienstleistungen für Brandsicherheitsanlagen und Sicherheitsanlagen
- **DIN EN 31010** Risikomanagement - Verfahren zur Risikobeurteilung
- **VDE 0833** Gefahrenmeldeanlagen für Brand, Einbruch und Überfall
- **BSI-Bro20/333** Wesentliche Anforderungen zum IT-Grundschutz des Bundesamt für Sicherheit in der Informationstechnik
- **BSI-Standard 200-4** IT-Notfallmanagement des Bundesamt für Sicherheit in der Informationstechnik
- **Isi-Web** Sichere Bereitstellung von Web-Angeboten
- **Isi-Fern** Zugriffe auf die interne Netzwerkinfrastruktur
- **NIS-2** Richtlinie EU 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau
- **CRA** Verordnung EU 2022/0272 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen

Bildnachweis

- Bild 1 Hekatron Vertriebs GmbH
- Bild 2 bis 8 bvfa

Der bvfa + Impressum

Der bvfa - Bundesverband Technischer Brandschutz e. V. ist der in Deutschland maßgebliche Verband für vorbeugenden und abwehrenden technischen Brandschutz. Der Verband wurde 1972 gegründet und hat seinen Sitz in Würzburg. In dem Verband sind die führenden deutschen Anbieter von stationärer und mobiler Brandschutztechnik sowie von Systemen des baulichen Brandschutzes vertreten. Die im Verband engagierten Unternehmen haben sich das Ziel gesetzt, den technischen Brandschutz in Deutschland voranzubringen, denn er dient der Sicherheit von Menschen, Sachwerten und Umwelt. Der bvfa arbeitet eng mit Behörden, Gesetzgebern, Normungsinstituten, Sachversicherern, Berufsgenossenschaften und befreundeten Verbänden zusammen. Die aus dieser intensiven Zusammenarbeit resultierenden Ergebnisse und Erkenntnisse zu den wichtigen Themen der Branche werden in aktuelle Informationen umgesetzt.

bvfa-ST-2024-03 (04)

Dieses Merkblatt wurde von der Fachgruppe Ansteuerung im bvfa erstellt.

Veröffentlicht: 09/2024

Impressum

Verantwortlich für den Inhalt:
bvfa, Geschäftsstelle Würzburg.
Geschäftsführer: Dr. Wolfram Krause
Koellikerstraße 13, D-97070 Würzburg
Telefon +49 931 35292-25, Fax +49 931 35292-29

info@bvfa.de | **www.bvfa.de**