ZVEI
Die Elektroindustrie

ZVEI | MERKBLATT

82021:2015-10

Vernetzte Sicherheitstechnik (Security und Safety)

Schnittstellenübersicht und Ausblick auf die IP-Vernetzung

Arbeitsgemeinschaft Errichter und Planer

ZVEI:
Errichter und Planer

Impressum

Merkblatt
Vernetzte Sicherheitstechnik (Security und Safety)
Schnittstellenübersicht und Ausblick auf die IP-Vernetzung

Allgemeine Hinweise für Planungs- und Installationsunternehmen

Herausgeber:
ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Arbeitsgemeinschaft Errichter und Planer
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: 069 6302-245
Fax: 069 6302-1245
E-Mail: krapp@zvei.org
www.zvei.org

Verantwortlich:
Peter Krapp
Geschäftsführer Fachverband Sicherheit
und Arge Errichter und Planer

Das Merkblatt entstand durch die Fachgruppe Vernetzte Sicherheit
der Arge Errichter und Planer.

Oktober 2015

Bildnachweis:

Andrey Prokhorov / iStock U1
Einige Elemente: freepik+fotolia 76
Einige Elemente: freepik+fotolia 94
Einige Elemente: freepik+fotolia 175
Wolke: fotolia 176
Einige Elemente: freepik+fotolia 177

Inhalt

0.1 Vorwort 11
0.1.1 Besondere Anforderungen in Gefahrenmeldeanlagen 11
0.1.2 Unterschiedliche Ausprägungen der Vernetzung bei Safety und Security 12

0.2 Zielsetzung und Aufgabenstellung 13

1. Nutzen und Risiken IP-vernetzter Gefahrenmeldeanlagen 14

1.1 Mehrwert durch IP-Vernetzung 14

1.2 Sicherheitsaspekte IP-vernetzter Gefahrenmeldeanlagen 14
1.2.1 Organisatorische Sicherheitsaspekte 15
1.2.2 Technische Sicherheitsaspekte 15
1.2.3 Netzwerk und Netzwerkprotokolle 16
1.2.4 Fernzugriff und Wartung 16
1.2.5 Geräte und Updates 16
1.2.6 Konfiguration und Komplexität 17
1.2.7 Mögliche Übertragungswege und Feldebenen bei Sicherheitstechnischen Anlagen 17
1.2.7.1 Übersicht der möglichen Übertragungswege 17
1.2.7.2 Feldebenen 18
1.2.7.3 Zulässige Übertragungswege nach der VdS 2311: 2010-11 (04) – Pos. 9.4.2 20
1.2.7.4 Zweiter Übertragungsweg bei IP-Netzen nach der VdS 2311-S1: 2013-08 (01) – Pos. 9.4.7.2 20
1.2.7.5 IP-Übertragung ohne Ersatzweg nach der VdS 2311-S1: 2013-08 (01) – Pos. 9.4.7.3 21
1.2.7.6 Zulässige Übertragungsdauer für Meldungen aus Überfall- und Einbruchmeldeanlagen, sowie aus Brandmeldeanlagen entspr. der DIN EN 50136-1 (VDE 0830-5-1) – Ausgabe August 2012 – Teil 1 21
1.2.7.7 Einweg-Übertragung (analog zu SP4 gemäß DIN EN 50136-1) zur Anschaltung an IP-Netze 23
1.2.7.8 Zweiwege-Übertragung (analog zu DP4 gemäß DIN EN 50136-1) zur Anschaltung an IP-Netze 23
1.2.7.9 Videoüberwachungsanlagen (VÜA) 24
1.2.7.9.1 Zeitliche Anforderungen an die Videoübertragung – Pos. 4.3 - nach der DIN EN 62676-1-2 (VDE 0830-7-5-12) – Ausgabe November 2014 – Teil 1-2 24
1.2.7.9.2 Speicherung von Bilddaten – Pos. 6.1.3.3 - nach der DIN EN 62676-1-1 (VDE 0830-7-5-11) – Ausgabe November 2014 - Teil 1-1 25
1.2.10 Mögliche Rückfallebenen vom Gebäudemanagementsystem-Sicherheitstechnik in Verbindung mit sicherheitstechnischen Anlagen 26

2. ZVEI-Definition – Vernetzte Sicherheit 27

2.1 Beispiele für die Vernetzung von sicherheitstechnischen Gewerken 28

3. Bestehende Normen und Richtlinien in Verbindung mit der „Vernetzten Sicherheit“ 29

3.1 Überfall- und Einbruchmeldeanlagen (ÜMA/EMA) 29
3.1.1 Normen auf deutscher und europäischer Ebene 29
3.1.2 VdS-Richtlinien 29

3.2 Zutrittskontrollanlagen 30
3.2.1 Normen auf deutscher und europäischer Ebene **30**
3.2.2 VdS-Richtlinien **30**
3.2.3 BSI-Richtlinien (Bundesamt für Sicherheit in der Informationstechnik) **30**

3.3 **Videoüberwachungsanlagen 31**
3.3.1 Normen auf deutscher und europäischer Ebene0 **31**
3.3.2 VdS – Richtlinien Planung und Einbau **32**
3.3.3 VdS - Verfahren zur Zertifizierung von Errichterfirmen **32**
3.3.4 VdS-Richtlinien für Produkte **32**
3.3.5 Polizei **32**
3.3.6 Bundesamt für Sicherheit in der Informationstechnik **32**
3.3.7 Arbeitskreis Maschinen- und Elektrotechnik (AMEV) **32**
3.3.8 Deutsche Gesetzliche Unfall Versicherung (DGUV) Vorschrift 25 **33**

3.4 Brandmeldeanlagen 33
3.4.1 Normen auf deutscher und europäischer Ebene **33**
3.4.2 VdS **33**

3.5 Sprachalarmanlagen/Elektroakustische Notfallwarnsysteme (SAA/ENS) 34
3.5.1 Normen auf deutscher und europäischer Ebene **34**

3.6 Rauch- und Wärmeabzugsanlagen 33
3.6.1 Normen auf deutscher und europäischer Ebene **33**
3.6.2 Internationale Normen **33**

3.7 Sicherheitsbeleuchtung- und Fluchtwegbeleuchtung 35
3.7.1 Normen auf deutscher und europäischer Ebene **35**
3.7.2 Sonstige **36**

3.8 Bezugsquellen für Normen, Richtlinien, Bestimmungen und Vorschriften 37

4. Gewerke der „Vernetzten Sicherheit“ 38

4.1 Security 38

4.1.1 **Überfall-und Einbruchmeldeanlagen (ÜMA/EMA) 38**
4.1.1.1 Funktionale Beschreibung **38**
4.1.1.2 Definition der Überfallmeldeanlagen (ÜMA) **38**
4.1.1.3 Definition der Einbruchmeldeanlagen (EMA) **38**
4.1.1.4 Aufbau, Aufgaben und Funktionen **38**
4.1.1.5 Beispielhafte Konfiguration einer Überfall- und Einbruchmeldeanlage (ÜMA/EMA) **39**
4.1.1.6 Überfall- und Einbruchmeldeanlagen (ÜMA/EMA) – Kernaussagen und Nutzen **40**
4.1.1.7 Klassifizierung **41**
4.1.1.8 Bundeseinheitliche Richtlinie für Überfall- und Einbruchmeldeanlagen (ÜMA/EMA) mit Anschluss an die Polizei (ÜEA-Richtlinie) **41**
4.1.1.8.1 Zur ÜEA-Richtlinie gehören insgesamt 11 Anlagen **42**
4.1.1.9 Bildübertragung **42**

4.1.1.10 **Einbruchmeldeanlagen (EMA) nach der Norm DIN VDE 0833-3, Grad 1 - 2 - 3 - 4. 42**
Einbruchmeldeanlagen werden nach DIN VDE 0833-3 je nach Risiko und Gefährdung in verschiedene Schutzgrade eingeteilt.
4.1.1.10.1 Übersicht der beispielhaften Konzepte Einbruchmeldeanlagen (EMA) nach der Norm DIN VDE 0833-3, Grad 1-2-3-4 **43**
Die folgende Tabelle enthält die für den jeweiligen Grad die von der Norm mindestens geforderten Eigenschaften.
4.1.1.10.1.1 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 1 **46**
4.1.1.10.1.2 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 2 **47**
4.1.1.10.1.3 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 3 **48**
4.1.1.10.1.4 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 4 **49**

4.1.1.11 **Einbruchmeldeanlagen nach BSI (Verschlusssachen) 50**
4.1.1.11.1 Einbruchmeldeanlagen nach BSI (Verschlusssachen) und nach der Norm DIN VDE 0833-1 und DIN VDE 0833-3, Grad 4 **50**
4.1.1.11.1.1 Beispielhaftes Konzept für eine Einbruchmeldeanlage (Verschlusssachen) nach BSI 7510 **51**
4.1.1.11.1.2 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach BSI (Verschlusssachen) und nach der Norm DIN VDE 0833-1 und DIN VDE 0833-3, Grad 4 **52**

4.1.1.12 **Überfallmeldeanlagen (ÜMA) nach der Norm DIN VDE 0833-3, Grad 1/DGUV Vorschrift 25 (UVV-Kassen) – nur für Geldinstitute 53**
4.1.1.12.1 Übersicht beispielhafter Konzepte für Überfallmeldeanlagen (ÜEA) nach nach der Norm DIN VDE 0833-3, Grad 1/DGUV Vorschrift 25 (UVV-Kassen) - nur für Geldinstitute **54**
4.1.1.12.2 Beispielhaftes Konzept für eine Überfallmeldeanlage nach der Norm DIN VDE 0833-3, Grad 3 **56**
4.1.1.12.3 Beispielhaftes Konzept für eine Überfallmeldeanlage nach der DGUV-Vorschrift 25 DGUV Vorschrift 25 (UVV-Kassen) - nur für Geldinstitute **57**

4.1.1.13 **Einbruchmeldeanlagen (EMA) nach der VdS, Klasse A-B-C-SG 3 und 4-SG 5 und 6 58**
4.1.1.13.1 Übersicht der beispielhafter Konzepte für Einbruchmeldeanlagen (EMA) nach der VdS, Klasse A-B-C-SG 3 und 4-/ SG 5 – und – 6 **59**
4.1.1.13.1.1 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse A **62**
4.1.1.13.1.2 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse B **63**
4.1.1.13.1.3 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse C-SG 3 und 4 **64**
4.1.1.13.1.4 Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse C-SG 5 und 6 **65**
4.1.1.14 Beispielhaftes Planungsschema für Überfall- und Einbruchmeldeanlagen (ÜMA-EMA) **66**
4.1.1.15 Beispielhafte Funktionen und Anschaltungen einer Überfall- und Einbruchmeldeanlage (ÜMA-EMA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle **68**

4.1.2	**Zutrittskontrollanlagen**	**72**
4.1.2.1	Funktionale Beschreibung	**72**
4.1.2.2	Definition Zutrittskontrollanlage	**73**
4.1.2.3	Aufbau eines elektronischen Zutrittskontrollsystems	**73**
4.1.2.3.1	Beispielhafte Prinzipgrafik für Zutrittskontrollanlagen	**76**
4.1.2.4	Identitätsmerkmalsträger	**78**
4.1.2.5	Biometrie	**79**
4.1.2.6	Beispielhaftes Planungsschema für Zutrittskontrollanlagen	**80**
4.1.2.7	Beispielhafte Funktionen und Anschaltungen einer Zutrittskontrollanlage an ein Gebäudemagementsystem (GMS) und an eine Sicherheits-Leitstelle	**84**
4.1.3	**Videoüberwachungsanlagen (VÜA) für Sicherheitsanwendungen**	**93**
4.1.3.1	Funktionale Beschreibung	**93**
4.1.3.2	Definition – Videoüberwachung	**93**
4.1.3.3	Definition Fern-Videoüberwachung	**93**
4.1.3.4	Aktivitätenverwaltung	**93**
4.1.3.5	Schnittstellen zu anderen Systemen	**94**
4.1.3.6	Digitale Videoüberwachungsanlagen (VÜA)	**95**
4.1.3.7	Beispiele für funktionelle Schnittstellen zu anderen Gewerken	**96**
4.1.3.8	**Videoinformationsanlage (VIA)**	**97**
4.1.3.8.1	Videoüberwachungsanlagen (VÜA) nach der Norm DIN EN 63676-1-1	**98**
4.1.3.8.2	Übersicht der beispielhaften Konzepte für Videoüberwachungsanlagen nach der Norm DIN EN 63676-1-1-Grad 1 bis 4	**99**
4.1.3.8.2.1	Beispielhaftes Konzept für eine Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 1	**101**
4.1.3.8.2.2	Beispielhaftes Konzept für eine Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 2	**101**
4.1.3.8.2.3	Beispielhaftes Konzept für eine Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 3	**102**
4.1.3.8.2.4	Beispielhaftes Konzept für eine Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 4	**103**
4.1.3.9	Beispielhaftes Planungsschema für Videoüberwachungsanlagen (VÜA)	**104**
4.1.3.10	Beispielhafte Funktionen und Anschaltungen einer Videoüberwachungsanlage (VÜA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle	**106**
4.2	**Safety**	**112**
4.2.1	**Brandmeldeanlagen (BMA)**	**112**
4.2.1.1	Funktionale Beschreibung	**112**
4.2.1.2	Aufbau, Aufgaben und Funktionen von Brandmeldeanlagen	**112**
4.2.1.3	Beispielhafte Konfiguration einer Brandmeldeanlage (BMA)	**113**
4.2.1.4	Mögliche Ansteuerungen aus einer Brandmelderzentrale nach der VDI 6010 – Ausgabe Mai 2011	**114**
4.2.1.5	Brandmeldeanlagen – Kernaussagen und Nutzen	**116**
4.2.1.6	Aufschaltebedingungen für Brandmeldeanlagen	**117**
4.2.1.7	Brandmeldeanlagen (BMA) und Brandschutzeinrichtungen nach der Norm DIN VDE 0833, DIN 14675 und der VdS 2095	**117**
4.2.1.7.1	**Übersicht der beispielhaften Konzepte für Brandmeldeanlagen (BMA) und Brandschutzeinrichtungen** Beispielhafte Konzepte für Brandmeldeanlagen (BMA) nach der Norm DIN VDE 0833-1-und-2; DIN 14675; VdS 2095 Beispielhafte Konzepte für Brandschutzeinrichtungen nach der Norm DIN VDE 0833 - Teile 1-und-2; DIN 14675; VdS 2095	**118**
4.2.1.7.1.1	Beispielhaftes Konzept für eine Brandmeldeanlage nach der Norm DIN VDE 0833, Teile 1 und 2 und DIN 14675	**120**
4.2.1.7.1.2	Beispielhaftes Konzept für eine Brandmeldeanlage nach der Norm DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095	**121**
4.2.1.7.1.3	Beispielhaftes Konzept für eine Brandschutzeinrichtung nach DIN – Brandmeldeanlage mit Löschanlage nach der Norm DIN VDE 0833, Teile 1 und 2 und DIN 14675	**122**
4.2.1.7.1.4	Beispielhaftes Konzept für eine Brandschutzeinrichtung nach VdS - Brandmeldeanlage mit Feuerlöschanlagenansteuerung nach DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095	**123**
4.2.1.8	Beispielhaftes Planungsschema für Brandmeldeanlagen (BMA)	**124**
4.2.1.9	Beispielhafte Funktionen und Anschaltungen einer Brandmeldeanlage (BMA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle	**126**
4.2.2	**Sprachalarmanlagen / Elektroakustische Notfallwarnsysteme (SAA/ENS)**	**130**
4.2.2.1	Funktionale Beschreibung	**130**
4.2.2.1.1	Definition Sprachalarmanlage (SAA)	**130**
4.2.2.1.2	Definition Elektroakustische Notfallwarnsysteme (ENS)	**131**
4.2.2.4	Konzepte Sprachalarmanlagen (SAA)/Elektroakustische Notfallwarnsysteme (ENS)	**132**
4.2.2.4.1	Übersicht der Konzepte für Sprachalarmanlagen (SAA) im Brandfall nach der Norm DIN VDE 0833 - Teil 4/Elektroakustische Notfallwarnsysteme (ENS) nach der Norm DIN EN 50849	**133**
4.2.2.4.1.1	Beispielhaftes Konzept für Sprachalarmanlagen (SAA) im Brandfall nach der Norm DIN VDE 0833 - Teil 4	**135**
4.2.2.4.1.2	Beispielhaftes Konzept für Elektroakustische Notfallwarnsysteme (ENS) nach der Norm DIN EN 50849	**136**
4.2.2.5	Beispielhaftes Planungsschema für Sprachalarmanlagen (SAA)	**137**
4.2.3	**Rauch- und Wärmeabzugsanlagen (RWA)**	**138**
4.2.3.1	Funktionale Beschreibung	**138**
4.2.3.1.1	Abwehrender Brandschutz	**138**
4.2.3.1.2	Vorbeugender Brandschutz	**138**
4.2.3.2	Wirkungsweise eines natürlichen Rauch- und Wärmeabzugs	**140**
4.2.3.2.1	Prinzip der Verdünnung	**140**
4.2.3.2.2	Prinzip der Schichtenbildung	**141**
4.2.3.3	Natürlicher Rauchabzug	**141**

4.2.3.4	Planung und Auslegung	**141**
4.2.3.5	RWA-Systeme	**142**
4.2.3.5.1	Situation in Deutschland	**143**
4.2.3.5.2	Berechnung der Öffnungsfläche eines Fensters	**143**
4.2.3.5.3	Berechnung der Rauchabzugsfläche eines NRWG	**143**
4.2.3.5.4	Aa (aerodynamische Fläche) = B Lichte • H Lichte • C v0	**144**
4.2.3.5.5	Um die aerodynamische Wirksamkeit sicherzustellen, muss eine Zuluft vorhanden sein	**145**
4.2.3.5.5.1	Berechnung der Zuluftfläche	**145**
4.2.3.5.5.2	Berechnung der Rauchableitungsfläche (geometrische Öffnung)	**146**
4.2.3.5.5.3	Berechnung der Lüftungsfläche	**147**
4.2.3.6	Beispielhaftes Planungsschema für Rauch- und Wärmeabzugsanlagen (RWA)	**148**
4.2.3.7	Beispielhafte Funktionen und Anschaltungen einer Rauchwärmeabzugsanlage (RWA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle	**150**
4.3	**Sicherheits- und Fluchtwegbeleuchtung**	**152**
4.3.1	Funktionale Beschreibung	**152**
4.3.2	Aufbau von Sicherheits- und Fluchtwegbeleuchtungsanlagen	**153**
4.3.3	Wartung und Prüfung	**153**
4.3.4	Beispielhaftes Planungsschema für eine Sicherheits- und Fluchtwegbeleuchtungsanlage	**154**
4.3.5	Beispielhaftes Funktionsschema einer Sicherheits- und Fluchtwegbeleuchtungsanlage	**156**
4.3.6	Beispielhafte Steuerungsmatrix für eine Sicherheits- und Fluchtwegbeleuchtungsanlage	**158**
4.4	**Gebäudemanagementsystem für Sicherheitstechnik**	**160**
4.4.1	Funktionale Beschreibung	**160**
4.4.2	Aufgaben und Funktionen von Gebäudemanagementsystemen (GMS)	**162**
4.4.2.1	Informationsbe- und -verarbeitung anhand eines genau zu definierenden Maßnahmenplanes	**163**
4.4.2.2	Informationsbe- und verarbeitung anhand eines genau zu definierenden Maßnahmenplanes für die nachfolgenden Anlagen	**163**
4.4.2.3	Bearbeitung von Meldungen und Steuerungen, u. a. aus den gebäudetechnischen Anlagen	**164**
4.4.2.4	Organisatorische Aufgaben	**164**
4.4.3	Technische Anforderungen	**165**
4.4.4	IT-Sicherheitsprogramme für Gefahrenmeldeanlagen und Gebäudemanagementsysteme	**166**
4.4.4.1	Zugriffskontrolle	**166**
4.4.4.2	Manipulationsschutz und Sicherung der Vertraulichkeit	**166**
4.4.4.3	Schutzmechanismen gegen Datenverlust	**166**
4.4.4.4	Kontroll- und Revisionsmaßnahmen	**166**
4.4.5	Planung von Gebäudemanagementsystemen	**167**
4.4.5.1	Zieldefinition	**167**
4.4.5.2	Pflichtenheft	**167**
4.4.5.3	Rahmenbedingungen	**168**
4.4.5.4	Ausschreibung	**168**
4.4.5.5	Auswahl	**168**
4.4.5.6	Projektüberwachung	**168**
4.4.5.7	Schnittstellen bei Gebäudemanagementsystemen (GMS)	**168**
4.4.5.7.1	Den bidirektionalen Datenaustausch zwischen Subsystem und GMS	**169**
4.4.5.8	Forderungen an die Ausfallsicherheit von Gebäudemanagementsystemen (GMS)	**170**
4.4.6	Beispielhaftes Planungsschema Gebäudemanagementsysteme-Sicherheitstechnik	**171**
4.5	**Notruf- und Serviceleitstelle (NSL) und Alarmprovider (AP) nach VdS 3138**	**175**
4.5.1	Funktion	**176**
4.5.2	Technische Ausstattung	**177**
4.5.3	Meldungsübertragung	**177**
4.5.4	Meldebearbeitung	**179**
4.5.5	Betrieb der Notruf- und Service-Leitstelle	**179**
4.5.6	Internetzugang zur Notruf- und Serviceleitstelle	**180**
5.	**Ausblick**	**181**
6.	**Literaturverzeichnis**	**182**
7.	**Übersicht der Mitglieder der ZVEI-Fachgruppe Vernetzte Sicherheit**	**183**

0.1 Vorwort

Die Vernetzung von Gefahrenmeldeanlagen und anderen Sicherheitssystemen untereinander und mit Gewerken der Gebäudetechnik nimmt immer mehr zu. Dadurch werden die Systeme in die Lage versetzt, Informationen auszutauschen und gegenseitig nutzbar zu machen. Alle angeschlossenen Gewerke können von zentraler Stelle aus überwacht und gesteuert werden. Insgesamt profitieren die Anwender von einer verbesserten Funktionalität, höherer Energieeffizienz und geringerem Kostenaufwand.

Beispiele für die Vernetzung von Sicherheitssystemen sind die Aufschaltung von Videobildern zur Alarmverifizierung bei einem Brand oder die Anbindung von Tür- und Fensterkontakten zur bedarfsgerechten Steuerung der Raumtemperatur. Kosteneffiziente und vom Markt immer stärker geforderte Funktionalitäten wie Ferninspektion und Fernwartung werden durch die IP-Vernetzung und den Zugriff von außen erleichtert.

Wurden zur Vernetzung vor wenigen Jahren noch überwiegend einfache analoge Zwei-Draht-Schnittstellen oder proprietäre, herstellerspezifische Kopplungen verwendet, kommen heute standardisierte digitale Übertragungsverfahren und Protokolle zum Einsatz.

Nach einer Umfrage der Arbeitsgemeinschaft Errichter und Planer (Arge) vom November 2013 geben die Umfrageteilnehmer an, dass insbesondere eine durchgehende IP-Vernetzung von Sicherheitssystemen und Gebäudeautomation noch nicht sehr verbreitet ist. Als Gründe werden vor allem eine fehlende, auf herstellerunabhängigen Standards basierende IP-fähige Angebotspalette der Hersteller sowie einheitlich anwendbare Standards und Normen genannt.

Definition: Eine Gefahrenmeldeanlage (GMA) nach DIN VDE 0833 ist eine Anlage, die Gefahren für Sachwerte und Leben durch Einbruch, Überfall und Feuer zuverlässig erkennt und meldet. Diese Funktion setzt die Überwachung der Übertragungswege und die Erfassung von Störungen und Sabotage voraus. Ebenso ist ein Ausfall zu vermeiden.

0.1.1 Besondere Anforderungen in Gefahrenmeldeanlagen

Sicherheitssysteme schützen Leib und Leben von Personen sowie Sachwerte. Dazu zählen u. a. Gefahrenmeldeanlagen nach DIN VDE 0833, die vor Brand, Einbruch und Überfall schützen, aber auch Videoüberwachungsanlagen, Rauch- und Wärmeabzugsanlagen (RWA) oder Zutrittskontrollsysteme.

An diese Systeme werden hohe Anforderungen bezüglich Übertragungssicherheit, Verfügbarkeit und Zuverlässigkeit gestellt, die in zahlreichen Gesetzen, Normen und Richtlinien geregelt sind (vgl. Kap. 3). Ihre sicherheitsrelevanten Funktionen – wie die Gefahrendetektion, die Internalarmierung sowie die Alarmierung von Polizei, Feuerwehr oder Leitstellen und das Steuern nachgeordneter Systeme im Gefahrenfall – dürfen durch eine Vernetzung unter keinen Umständen beeinträchtigt werden.

Dabei müssen Datenschutzaspekte genauso berücksichtigt werden wie der Schutz durch Sabotage von außen, beispielsweise durch Cyber-Angriffe oder Computerviren. Jedoch wächst mit einer steigenden Anzahl von Schnittstellen und möglichen Zugriffen von außen auch das Risiko von Rückwirkungen auf sicherheitsrelevante Kernfunktionen der vernetzten Systeme. Denkbar sind beispielsweise Angriffe auf einzelne Geräte (Code-Injection, Ausnutzung von Schwachstellen in der Firmware oder Wartungszugängen) oder auf das IP-Netz insgesamt (Denial-of-Service-Attacken).

In allen Bereichen, in denen Daten erhoben werden, sind die Aspekte des Datenschutzes in Einklang mit den entsprechenden Gesetzen zu berücksichtigen. Dieser Teil wird jedoch aufgrund des Umfangs und der dazu notwendigen juristischen Fachkenntnisse in diesem Merkblatt nicht behandelt.

Durch die Abschaltung analoger und ISDN-Telefonleitungen wird die Weiterleitung von Alarmen aus Gefahrenmeldeanlagen verstärkt über IP-Netze erfolgen.

0.1.2 Unterschiedliche Ausprägungen der Vernetzung bei Safety und Security

Am weitesten gediehen ist die Nutzung von IP-Vernetzungen in Videoüberwachungssystemen (VÜA). Durch den Wandel von analogen zu digitalen Kameras und Speichersystemen sowie der notwendigen Übertragung großer Datenmengen sind IP-Netze notwendig und es werden dabei auch IP-Netze der Betreiber genutzt. Die im November 2014 neu erschienene Normenreihe DIN EN 62676 legt dazu detaillierte Anforderungen an Netzwerke und die Videoübertragung fest.
Auch die Vernetzung von Unterzentralen innerhalb verschiedener Safety- und Security-Gewerke erfolgt verstärkt über IP-Netze, allerdings in der Regel zwischen Geräten eines Herstellers und über separate Netzwerkverbindungen.

Auch für andere Gewerke der Sicherheitstechnik existieren bereits heute Regelungen zur Vernetzung und zu den Schnittstellen solcher Systeme, die sich allerding über verschiedene Normen und Richtlinien verteilen (vgl. Kap. 3).

Wünschenswert ist daher eine zusammenhängende Dokumentation, welche die Vernetzung und die Schnittstellen von Sicherheitssystemen aufführt und die normativen Grundlagen skizziert.

Thomas Urban (VdS)
„Gefahrenmeldeanlagen sollen Gefahren melden und dadurch Leben, Gesundheit und Schachwerte erhalten. Durch eine zweckmäßige Vernetzung von GMA kann diese Aufgabe wirkungsvoller realisiert werden.
Beispielsweise kann eine Gefahrenmeldung mit zugehörigen Videosequenzen verknüpft werden. Dadurch ist eine zielgerichtete Reaktion der hilfeleistenden Stellen möglich. Dabei kommt der Interoperabilität der unterschiedlichen Systeme eine entscheidende Rolle zu. Nur wenn die Gefahrenmeldungen und alle Metadaten verknüpft und verarbeitet werden können, sind die vielfältigen Möglichkeiten der Vernetzung auszuschöpfen. Das Denken in technischen Sparten und unterschiedliche „Sprachen" zwischen den Komponenten verschiedener GMA ist sicherlich der Grund, dass das Ausschöpfen mit kleinerer Geschwindigkeit geschieht als möglich. Hier ist insbesondere eine Anwendung übergreifende Standardisierung erforderlich, die die Vernetzung auf funktionaler und technischer Ebene zulässt. Ich wünsche mir, dass sich diese Entwicklung beschleunigt."

0.2 Zielsetzung und Aufgabenstellung

Das vorliegende Merkblatt richtet sich an Planer und Errichter sowie an Betreiber und Planungs- und Bauabteilungen privatwirtschaftlicher Unternehmen und öffentlicher Stellen. Es gibt einen Überblick über vorhandene Normen und Richtlinien und beschreibt allgemeine Anforderungen an Systeme, Übertragungswege und Schnittstellen zur zuverlässigen Vernetzung von Sicherheitssystemen untereinander und mit der Gebäudetechnik.

Dazu werden die erforderlichen Ausstattungsebenen von Sicherheitssystemen aus dem Safety- und Security-Bereich dargestellt und es wird beschrieben, welche Systeme sinnvoll miteinander vernetzt werden können. Beispielhafte Schnittstellen werden funktional beschreiben und in eine übersichtliche Matrix-Darstellung gebracht.

In der vorliegenden Version wird die Vernetzung folgender Systeme behandelt:

- **Safety:**
  Brandmeldeanlagen, Sprachalarmanlagen, Rauch- und Wärmeabzugsanlagen
- **Security:**
  Überfall- und Einbruchmeldeanlagen, Zutrittskontrollanlagen, Videoüberwachung
- Sicherheits- und Fluchtwegbeleuchtung
- Gebäudemanagementsysteme für Sicherheitstechnik
- Sicherheits-Leitstelle

Bei der in der Sicherheitstechnik gebräuchlichen Unterscheidung zwischen „Safety"- und „Security"-System handelt es sich um eine idealtypische Unterscheidung. Insofern existieren auch mögliche „Mischformen". Wird beispielsweise ein Videosystem (üblicherweise Security-Gewerk) zur Branderkennung verwendet, erfüllt es in diesem Zusammenhang eine Safety-Funktion, da es zum Schutz von Menschenleben dient, mit allen Anforderungen an Übertragungssicherheit und Verfügbarkeit.
Darüber hinaus wird alternativ z. B. im Bereich der IT-Sicherheit „Safety" als Ausfallsicherheit und „Security" als Schutz vor unerlaubten Zugriffen beschrieben.

Die Vernetzung von Sicherheitssystemen mit Gewerken der Gebäudetechnik soll in einer zukünftigen Merkblatt-Ausgabe ergänzt werden. Die Auswahl der betrachteten Sicherheitssysteme geschah nach bestem Wissen und Gewissen und richtete sich in erster Linie nach dem Wissen und der Erfahrung der Mitglieder der Fachgruppe „Vernetzte Sicherheit"'.

Das Merkblatt ist ausdrücklich offen für die Berücksichtigung weiterer sicherheitsrelevanter Systeme und soll eine erste Orientierungshilfe zur Vernetzung von Sicherheitsanlagen geben. Die Erkenntnisse und Vorschläge sollen von der interessierten Fachöffentlichkeit diskutiert werden, um möglichen Handlungsbedarf bei Forschung, Normung, Standardisierung und Anwendung zu identifizieren.

Hinweis: Das Merkblatt ist nicht als Planungshilfe, Checkliste oder Ähnliches zu benutzen. Die dargestellten Beispiele sind allgemein gehalten und ohne Anpassung nicht auf konkrete Projekte anwendbar. Die Planung, Errichtung und der Betrieb von Sicherheitsanlagen sowie eine gesetzes- und richtlinienkonforme Umsetzung kann nur mit fachkundigem Personal und Dienstleistern individuell am jeweiligen Objekt geklärt werden.

1. Nutzen und Risiken IP-vernetzter Gefahrenmeldeanlagen

1.1 Mehrwert durch IP-Vernetzung

Generell bietet die bereits heute praktizierte Vernetzung von Gefahrenmeldeanlagen – beispielsweise über serielle Verbindungen – zahlreiche Vorteile. Informationen aus allen angeschlossenen Gewerken sind zentral verfügbar und verbessern die Lagebeurteilung im Gefahrenfall sowie das Einleiten von Maßnahmen. Beispiele sind die Überprüfung eines Brandalarms mit Hilfe von Videobildern, die im Brandfall automatisch eingespielt werden oder die automatische Steuerung von Aufzügen im Brandfall.

Eine IP-Vernetzung erhöht die Funktionalität und die Wirtschaftlichkeit nochmals deutlich und verschafft den Anwendern einen wesentlich größeren Handlungsspielraum. IP-Netze können viel mehr Daten wesentlich schneller übertragen als herkömmliche Datenleitungen. Dadurch wird das Verarbeiten und Auswerten umfangreicher Informationen mit hoher Qualität in viel kürzerer Zeit möglich. So lassen sich beispielsweise hochauflösende Videobilder dazu nutzen, bei einem unbefugten Zutritt Personen auch aus großer Entfernung zu identifizieren. Die große Datenvielfalt auch mit Tönen, Bildern und Sprache erlaubt eine bessere Alarmverifizierung und eine schnellere Überprüfung der Systeme.

Die hochstandardisierten IP-Netze erleichtern zudem die Anbindung entfernter Liegenschaften. Selbst weltweit verteilte Außenstellen können zentral gesteuert und überwacht werden. Ferninspektion und Fernwartung werden dadurch in vielen Fällen erst möglich. Dabei schalten sich Servicetechniker von Hersteller oder Wartungsfirma aus der Ferne auf die Anlagen auf. Service-Einsätze vor Ort werden vermieden bzw. effizienter. Die Verfügbarkeit der Gefahrenmeldeanlagen erhöht sich, da die Systeme weniger oft zu Wartungszwecken abgeschaltet werden müssen.

Die Nutzung standardisierter IT-Netzwerkkomponenten und bereits bestehender Netze bis hin zum Internet erhöht die Wirtschaftlichkeit und ermöglicht eine flexible Konfiguration. Die Nutzung von Standardsoft- und Hardware erleichtert eine umfassende Dokumentation und erhöht Transparenz und damit die Sicherheit. So kann mit Web-Browsern ein einfaches und standardisiertes Benutzer-Interface geschaffen werden. Eine aufwändige und pflegeintensive Softwareintegration ist nötig.

Der Mehrwert der IP-Vernetzung kommt allerdings erst dann zum Tragen, wenn grundlegende Sicherheitsvorkehrungen getroffen werden. Durch die Nutzung von Standard-IT-Komponenten und bei Zugangsmöglichkeiten von außen entstehen nämlich neue Risiken.

1.2 Sicherheitsaspekte IP-vernetzter Gefahrenmeldeanlagen

Generell gilt, dass eine Umstellung auf netzwerkverbundene Komponenten das existierende Sicherheits- und Verfügbarkeitsniveau nicht reduzieren darf. Daher muss eine Manipulation oder Beeinträchtigung der Verfügbarkeit der Komponenten über das Netzwerk ausgeschlossen werden. Dies muss bei Planung, Umsetzung und Betrieb berücksichtigt werden, denn neben gezielten Angriffen durch eine Ausnutzung von Fehlern oder Schwachstellen in den Implementierungen können auch ungezielte Angriffe erfolgen, die beispielsweise durch eine Überlastung des Netzwerks entstehen.

Target Hack
Zwischen dem 27. November und 15. Dezember 2013 wurden der amerikanischen Einzelhandelskette Target insgesamt über 100 Millionen Kundendaten, darunter Kundenkarten- und Kreditkartennummern, Kartenprüfcodes, PIN, Post- und Mailadressen, Telefonnummern und weitere Daten durch Hacker entwendeten.
Die kopierten Informationen wurden zum Identitätsdiebstahl oder Betrug genutzt. Der Einbruch in das Datennetz von Target geschah durch einen unzureichend abgesicherten Wartungszugang eines Dienstleisters für Klimatechnik, der mit dem Geschäftsnetz von Target verbunden war.

1.2.1 Organisatorische Sicherheitsaspekte

Durch den Einsatz standardisierter Netzwerk-Technik können auch Produkte zu Einsatz kommen, die nicht ausschließlich für den Einsatz in Gefahrenmeldeanlagen konzipiert werden, wie handelsübliche Switche oder Router. Die Verantwortung für die Konfiguration und langfristige Administration dieser Netzwerkkomponenten muss im Vorfeld geklärt und für die gesamte Lebensdauer der Gefahrenmeldeanlage aufrechterhalten werden. Im Allgemeinen liegt die Lebensdauer von Geräten der klassischen IT weit unterhalb der von Gebäudeleittechnik und damit vernetzter Systeme. Das Auftreten defekter Netzwerkgeräte oder Änderungen an der Netzwerkinfrastruktur sind deshalb vorzusehen und können auch Auswirkungen auf die Gefahrenmeldeanlage haben. Änderungen am Netzwerk müssen mit dem Planer oder Errichter sowie dem Betreiber abgestimmt werden. Ebenso können Wartungszyklen für Updates an den Netzwerkkomponenten die Verfügbarkeit der Gefahrenmeldeanlage beeinflussen. Es sollte daher ein Prozessansatz benutzt werden, der die beschriebenen Fälle für den gesamten Lebenszyklus eines Produkts oder eines Systems abdeckt. Dabei müssen Hersteller, Planer/Errichter und Betreiber zusammen arbeiten und gemeinsam Gegenmaßnahmen ergreifen.

Bis zu einer Milliarde US-Dollar von 100 Finanzinstituten durch Cybergang „Carbanak" weltweit gestohlen
In den Jahren 2013 und 2014 wurden Banken und andere Finanzinstitute in mindestens 25 Ländern angegriffen. Im Durchschnitt dauerte jeder Banküberfall von der Infizierung des ersten Computers im Unternehmensnetzwerk der Bank durch gezielte Spear-Phishing-Attacken bis zum eigentlichen Diebstahl zwischen zwei und vier Monate an. Die Angreifer brachten dafür die Überwachungskameras bzw. deren Steuercomputer sowie Arbeitsplatzrechner von Mitarbeitern unter ihre Kontrolle und konnten dadurch alle Vorgänge in der Bank beobachten und die Aktivitäten der Angestellten imitieren, um Geld zu überweisen oder bar auszuzahlen. Die größten Summen betrugen dabei bis zu 8,8 Millionen Euro pro Überfall.

1.2.2 Technische Sicherheitsaspekte

Je nach Anwendungsgebiet und in Abhängigkeit einer Risikobetrachtung muss man verschiedene gestaffelte Ansätze zur Absicherung zu einem sogenannten Defense-in-Depth-Ansatz kombinieren. Ein starker Perimeterschutz allein – beispielsweise durch Firewalls - deckt nicht alle Angriffswege ab und kann deswegen überwunden werden.

1.2.3 Netzwerk und Netzwerkprotokolle

Es ist davon auszugehen, dass vernetzte Gefahrenmeldeanlagen mit der allgemeinen Netzwerkinfrastruktur der Gebäudeleittechnik zusammen betrieben werden und dass komplett eigenständige Netzwerke nur bei besonders hohen Schutzforderungen zum Einsatz kommen. Eine vollständige Trennung (sog. Airgap) ist technisch nur schwer möglich und würde viele der Vorteile einer Vernetzung wieder zunichtemachen. Das bedeutet aber auch, dass das Netzwerk als potentiell kompromittiert angesehen werden muss, über das die vernetzte Gefahrenmeldeanlage angegriffen werden kann. Dies ist als ein Haupteinfallsweg anzusehen und deshalb ist die Absicherung des Netzwerks besonders wichtig. Diese kann über physikalische oder logische Netzwerksegmentierung erfolgen.

Zusätzlich sollten sichere Netzwerkprotokolle eingesetzt werden, was jedoch komplex und aufwändig ist. Es ist empfehlenswert, dafür einheitliche, bereits existierende und offengelegte Standards mit nachgewiesenen Schutzfunktionalitäten zu verwenden, wobei die korrekte Implementierung sehr genau geprüft werden sollte.

1.2.4 Fernzugriff und Fernwartung

Einer der großen Vorteile der Vernetzung ist die Möglichkeit, aus der Ferne Diagnose und Wartung der vernetzten Gefahrenmeldeanlage durchzuführen. Dazu müssen gezielt Schutzmechanismen außer Kraft gesetzt werden, um eine Verbindung von der Anlage zu der Stelle, die die Fernwartung durchführt, zu erlauben. Hierbei ist sicherzustellen, dass der Zugriff zeitlich und auf das zu wartende System beschränkt bleibt. Aus Dokumentationsgründen sollten alle diese Zugriffe auch protokolliert werden. Zusätzlich sollten Anforderungen an das Sicherheitsniveau der zugreifenden Stelle gestellt werden.

1.2.5 Geräte und Updates

Selbst in kleinsten Sensoren mit Netzwerkanbindung kommen heutzutage oft Standardbetriebssysteme zum Einsatz. Diese Geräte erben auch die Schwachstellen dieser Betriebssysteme. Deshalb ist es wichtig, dass diese Geräte oder auch Bedienterminals über nachträgliche Updatemechanismen verfügen, mit denen im Falle des Bekanntwerden neuer Schwachstellen diese gepatcht werden können. Hersteller sollten den Umgang mit Schwachstellen offensiv, d. h. über Benachrichtigung der Errichter oder Betreiber sowie dem Bereitstellen von Updates auch über längere Zeiträume betreiben. Die Gefährdungslage sollte permanent abgeschätzt und verfügbare Sicherheitsupdates kurzfristig ausgerollt werden. Bis diese Sicherheitsupdates verfügbar sind, müssen wirksame Maßnahmen gegen die Ausnutzung offener Schwachstellen ergriffen werden.

Die Updatemechanismen selbst sind ebenfalls ein Angriffsweg und müssen beispielsweise durch Verschlüsseln der Firmware oder zusätzlichen Hardwareschutz gegen Manipulation geschützt werden.

Viele Endgeräte wie Bedienterminals sind frei zugänglich und müssen gegen physikalische Manipulation oder unberechtigtes Auslesen von Informationen beispielsweise von Passworten geschützt werden.

Eine besondere Herausforderung stellen Computer der Leitzentrale dar, da auch diese oft mit Standardbetriebssystemen ausgestattet und somit für Angriffe empfänglich sind. Diese Angriffe sind identisch mit denen auf Standard-IT-Systeme und können – sofern die Rechner eine Internetverbindung erlauben - durch diese beispielsweise über Phishing-Emails oder Drive-By-Angriffe oder auch über andere für das Bedienpersonal zugängliche Schnittstellen des Rechners (USB, CD/DVD-ROM) kompromittiert werden. Sollte keine Verbindung zum Internet eingerichtet sein, so ist sicherzustellen, dass trotzdem aktueller Virenschutz oder andere Härtungsmaßnahmen installiert sind.

1.2.6 Konfiguration und Komplexität

Verglichen mit vielen Anlagen, bei denen heutzutage oft noch Zweidraht-Verkabelung eingesetzt wird, stellt ein vernetztes System einen Evolutionssprung dar. Damit steigen die Anforderungen an den Errichter enorm, denn mit der gestiegenen Komplexität gibt es viel mehr Konfigurationsmöglichkeiten und damit die zunehmende Gefahr fehlerhafter Einstellungen.

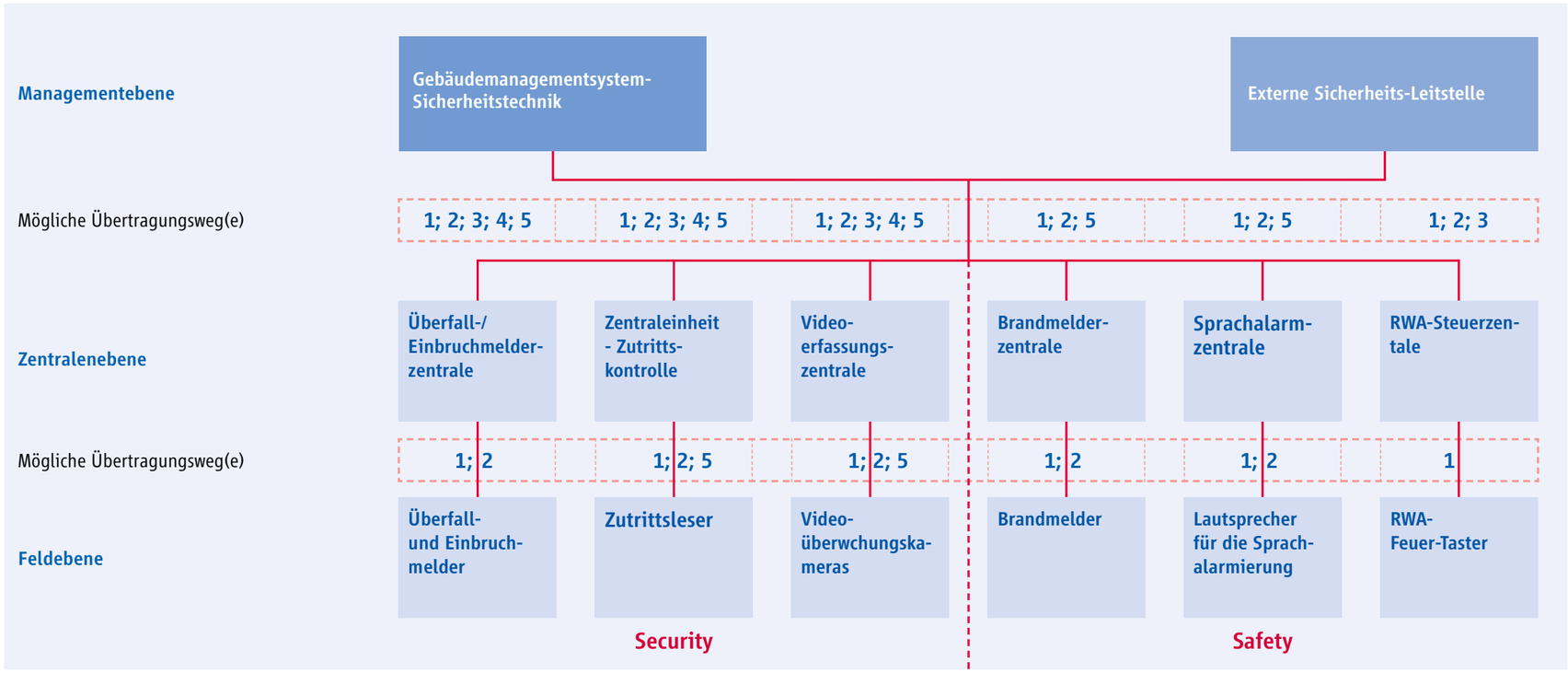
Dasselbe gilt auch für die Gerätehersteller, die zusätzliche Software programmieren müssen. Moderne Entwicklungsprozesse unterstützen zwar gezielt bei der Programmierung sicherer Software, trotzdem treten Schwachstellen nach wie vor auf.
In der Praxis ist ein entsprechendes Management von Schwachstellen und Sicherheitsupdates durch alle Beteiligten erforderlich.

1.2.7 Mögliche Übertragungswege und Feldebenen bei Sicherheitstechnischen Anlagen

1.2.7.1 Übersicht der möglichen Übertragungswege

1. **Drahtgebunden** (auf Drahtbruch – und – Kurzschluss überwacht)
2. **Separate Sicherheits-Netzwerke der Anbieter** (bei sehr hohen Sicherheitsanforderungen)
3. **Bestehende Telekommunikationsnetze (TK-Netze)** der Telekommunikationsanbieter
4. **Funk** (Gegenseitige Überwachung von Sender und Empfänger, damit bemerkt wird, wenn der Sender oder der Empfänger ausfällt – Übertragungsweg gestört)
5. **Mitnutzung der IT-Netze der Betreiber** (z. Z. schon bei Videoüberwachungsanlagen (VÜA) und Zutrittskontrollanlagen)
6. **WLAN** Bisher gibt es hier keine normative Beschreibung für sicherheitstechnische Anwendungen.

1.2.7.2 Mögliche Übertragungswege und Feldebenen bei Sicherheitstechnischen Anlagen



1.2.7.3 **Zulässige Übertragungswege nach der VdS 2311:2010-11 (04) - Pos. 9.4.2**

Für Fernalarm verwendete Übertragungswege müssen den Anforderungen der Richtlinien für Übertragungswege, VdS 2471, entsprechen und im Verzeichnis Übertragungswege in Alarmübertragungsanlagen, VdS 2532 aufgelistet sein.

Hinweis 1:
Die ausschließliche Verwendung von ÜE mit „Funk-Übertragungswegen" ist nur in EMA der Klasse A zulässig.

Hinweis 2:
Übertragungswege in IP-Netzen müssen nicht im Verzeichnis Übertragungswege in Alarmübertragungsanlagen, VdS 2532 gelistet sein.

1.2.7.4 **Zweiter Übertragungsweg bei IP-Netzen nach der VdS 2311-S1:2013-08 (01) – Pos. 9.4.7.2**

Bei der Verwendung des IP-Netzes zur Übertragung von Gefahrenmeldungen ist ein zusätzlicher Übertragungsweg erforderlich. Hierfür müssen ausschließlich VdS-anerkannte Übertragungswege verwendet werden (z. B. bedarfsgesteuerte Verbindung über ISDN Netz- B-Kanal oder Funknetz entsprechend Tabelle 5.17). Es muss sichergestellt sein, dass der zweite Übertragungsweg im Bereich des gesicherten Objektes nicht aus dem als Hauptübertragungsweg genutzten IP-Netz gebildet wird. In diesem Fall ist eine separate Trassenführung (gemäß Abschnitt 9.4.6.1) nicht erforderlich (siehe auch Bilder 9.02 bis 9.05).

Hinweis 1:
Bei EMA der Klassen B und C ist der zweite Übertragungsweg als fester Bestandteil des IP-Übertragungsnetzes immer erforderlich. Eine Abweichung von dieser Anforderung ist nicht möglich (unzulässige Abweichung entsprechend Anhang G).

Bei Ausfall (Unterbrechung von 20 Sekunden oder länger) einer stehenden IP-Verbindung muss bei scharfgeschalteter EMA und/oder bei vorhandenen Überfallmeldern grundsätzlich eine sofortige Intervention durch die hilfeleistende Stelle erfolgen. Alternativ kann auf eine unmittelbare Intervention verzichtet werden, wenn folgende Ersatzmaßnahmen realisiert werden:

- Unmittelbar nach Erkennen des Ausfalls muss eine Meldung an die angeschlossene NSL über den Ersatzweg erfolgen.
- Danach erfolgen mindestens alle 10 Minuten weitere Meldungen über den Ersatzweg (Funktionsüberwachung), bis die stehende IP-Verbindung wieder zur Verfügung steht.

Bei Ausbleiben dieser Meldungen muss sofort interveniert werden.

Hinweis 2:
Bei wiederholt auftretenden netzbedingten Ausfällen der stehenden IP-Verbindung (Kurzzeitunterbrechungen) kann in Abstimmung mit dem Versicherer die Meldung des Ausfalls der IP-Verbindung für eine begrenzte Zeit um bis zu 180 Sekunden verzögert an die angeschlossene NSL übertragen werden.

Die vereinbarten Maßnahmen sind entsprechend Abschnitt 5.4.3 von der angeschlossenen NSL im Alarmdienst- und Interventionsattest VdS 2529 zu dokumentieren.

1.2.7.5 **IP-Übertragung ohne Ersatzweg nach der VdS 2311-S1: 2013-08 (01) – Pos. 9.4.7.3**

Bei der Verwendung von bedarfsgesteuerten IP-Übertragungswegen kann auf einen zusätzlichen Übertragungsweg verzichtet werden, wenn

- bei einem Ausfall der Energieversorgung der dauernd uneingeschränkte Betrieb der ÜE sowie der innerhalb des gesicherten Objekts vorhandenen Kommunikationsgeräte, die Bestandteil des Übertragungsweges sind, für mindestens 12 h sichergestellt ist
- die ÜE über eine Sabotage- und Blockadefreischaltung verfügt, so dass sie absoluten Betriebsvorrang vor anderen Geräten hat.

Hinweis:
Aus technischen Gründen kann für die Realisierung einer bedarfsgesteuerten IP-Verbindung auch eine stehende IP-Verbindung benutzt werden, die mit 5- bzw. 25- stündlicher Funktionsüberwachung betrieben wird.

1.2.7.6 **Zulässige Übertragungsdauer für Meldungen aus Überfall- und Einbruchmeldeanlagen, sowie aus Brandmeldeanlagen entspr. der DIN EN 50136-1 (VDE 0830-5-1) – Ausgabe August 2012**

Alarmanlagen – Alarmübertragungsanlagen und Einrichtungen – Teil 1: Allgemeine Anforderungen an Alarmübertragungsanlagen

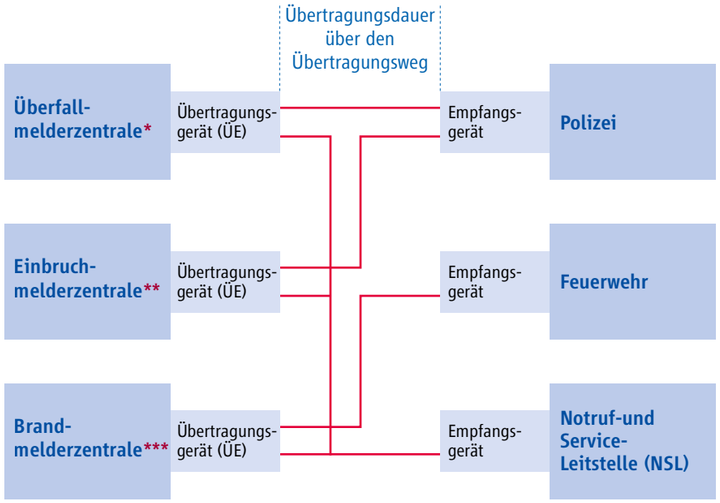
6.3.2 Übertragungsdauer nach der DIN EN 50136-1 (VDE 0850-5-1) von der Alarmübertragungsanlage (AÜA) zur Empfangseinrichtung bei der Polizei - Feuerwehr - Notruf- und Service-Leitstelle

Tabelle 2 Übertragungsdauer

Übertragungsdauer	SP1	SP2	SP3	SP4	SP5	SP6	DP1	DP2	DP3	DP4
Arithmetisches Mittel aller Übertragungen	120 s	60 s	20 s	20 s	10 s	10 s	60 s	20 s	20 s	10 s
95 Perzentil aller Übertragungen	240 s	90 s	30 s	30 s	15 s	15 s	90 s	30 s	30 s	15 s
Maximal akzeptierte Übertragungsdauer	480 s	120 s	60 s	60 s	30 s	30 s	120 s	60 s	60 s	30 s

Erläuterung zu Pos. 1.2.7.6 – Prinzipdarstellung

Übertragung von Meldungen von der Alarmübertragungsanlage (AÜA) zur Empfangseinrichtung bei der Polizei – der Feuerwehr – der Notruf- und Service-Leitstelle



* Überfall-Sekundäralarm und Störungsalarm zur Notruf- und Service-Leitstelle (NSL)

** Einbruchmeldealarm zur Alarmvorprüfung an die Notruf- und Service-Leitstelle (NSL); ebenso der Störungsalarm

*** Brandmelde-Sekundäralarm und Störungsalarm zur Notruf- und Service-Leitstelle (NSL)

1.2.7.7 Einweg-Übertragung (analog zu SP4 gemäß DIN EN 50136-1) zur Anschaltung an IP-Netze

Meldungszeit:	Eine Störung der Funktion des Übertragungsweges muss innerhalb von 180 s erkannt und angezeigt werden. Die Kontrolle des Übertragungsweges erfolgt durch den zyklischen Austausch von Datentelegrammen zwischen ÜZ und ÜE.
Routinemeldung:	Mindestens alle 25 h
Verfügbarkeit in irgendeiner 7-Tages-Periode:	Mindestens 97 %
Übertragungsdauer:	Maximal 60 s; arithmetisches Mittel 20 s

1.2.7.8 Zweiwege-Übertragung (analog zu DP4 gemäß DIN EN 50136-1) zur Anschaltung an IP-Netze

Meldungszeit Erstweg:	Eine Störung der Funktion des Übertragungsweges muss innerhalb von 90 s erkannt und angezeigt werden. Die Kontrolle des Übertragungsweges erfolgt durch den zyklischen Austausch von Datentelegrammen zwischen ÜZ und ÜE.
Meldungszeit Zweitweg bei ungestörtem Erstweg:	Eine Störung der Funktion des Übertragungsweges muss innerhalb von 5 h erkannt und angezeigt werden.
Meldungszeit Zweitweg bei gestörtem Erstweg:	Eine Störung der Funktion des Übertragungsweges muss innerhalb von 90 s erkannt und angezeigt werden. Die Kontrolle des Übertragungsweges erfolgt durch den zyklischen Austausch von Datentelegrammen zwischen ÜZ und ÜE.
Umschaltzeit vom gestörten Erstweg auf Zweitweg	Maximal 90 s
Routinemeldung:	Für Erstweg und Zweitweg mindestens alle 25 h
Verfügbarkeit in irgendeiner 7-Tages-Periode:	Mindestens 99,8 %
Übertragungsdauer:	Maximal 30 s; arithmetisches Mittel 10 s

1.2.7.9 **Videoüberwachungsanlagen (VÜA)**

1.2.7.9.1 **Zeitliche Anforderungen an die Videoübertragung – Pos. 4.3 - nach der DIN EN 62676-1-2 (VDE 0830-7-5-12) – Ausgabe November 2014**

Videoüberwachungsanlagen für Sicherheitsanwendungen – Teil 1-2: Systemanforderungen – Allgemeine Anforderungen an die Videoübertragung

4.3.1 Allgemeines
Videoübertragungsgeräte und deren Verbindungen müssen als Teil der VÜA nach den festgelegten Systemanforderungen ausgeführt sein.

4.3.2 Verbindungszeit
Maßgeblich ist die Verbindungszeit, die für die Initiierung der Übertragung eines Videodatenstroms von einer Quelle zu einem Empfänger erforderlich ist. Diese Zeit muss besonders bei Systemen berücksichtigt werden, bei denen Kamera Touren, ein sequentielles Aufschalten von Kameras oder virtuelle Wächterrundgänge durchgeführt werden sollen. Die initiale Verbindungszeit muss sehr viel kürzer sein als die Verweilzeit der Kamerasequenz.

Tabelle 2 Verbindungen – Zeitliche Anforderungen

Videoübertragungsgeräte dürfen höchstens eine initiale Verbindungszeit für jede neue Anforderung eines Videodatenstroms haben von	Klasse 1	Klasse 2	Klasse 3	Klasse 4
	2.000 ms	1.000 ms	500 ms	250 ms

1.2.7.9.2 **Speicherung von Bilddaten – Pos. 6.1.3.3 - nach der DIN EN 62676-1-1 (VDE 0830-7-5-11) – Ausgabe November 2014**

Videoüberwachungsanlagen für Sicherheitsanwendungen –
Teil 1-1: Systemanforderungen – Allgemeines

Für den Fall, dass in der **VÜA** Speicher- oder Aufzeichnungsfunktionen verfügbar sind, gelten die folgenden in **Tabelle 1** angegebenen Anforderungen.

Die meisten Systeme verändern die Videobilder, bevor diese gespeichert werden (Umwandlung zwischen analogem und digitalem Format, Änderungen der Auflösung, Kompression, Markierung mit Wasserzeichen oder Verschlüsselung). In der Dokumentation müssen alle Prozesse, die Informationsverlust verursachen könnten, klar angegeben werden.

Falls keine redundante Speicherung zur Verfügung steht, müssen die Bilder auf dem Speichermedium so gespeichert werden, dass die Daten mit Hilfe alternativer Einrichtungen angezeigt und kopiert werden können.

Tabelle 1 Speicherung

Die VÜA muss über folgende Funktionen verfügen	Sicherungsgrad			
	1	2	3	4
Datensicherung und/oder redundante Aufzeichnung			●	●
Betrieb eines ausfallsicheren Speichers (z. B. RAID 5 oder fortlaufende Datenspiegelung) oder automatische Umschaltung von einem Speichermedium auf ein anderes im Fall eines Speicherausfalls				●
Reaktion auf ein Ansteuersignal mit einer maximalen Latenzzeit von		1 s	500 ms	250 ms
Wiedergabe eines gespeicherten Bildes aus dem Speicher mit einer maximalen Zeit nach dem Vorfall oder der aktuellen Aufzeichnung von			2 ms	1 ms

1.2.10 Rückfallebenen

Die Rückfallebene bezeichnet ein sekundäres System, das die Funktion des primären Systems übernehmen kann, wenn dieses ausfällt oder gestört ist.

Dieses kann zum Beispiel eine lokale Bedieneinheit an einer Brandmeldeanlage sein, die eine Bedienung der Brandmeldeanlage auch beim Ausfall eines Managementsystems ermöglicht.

Häufig bietet die Rückfallebene nicht alle Funktionen des primären Systems und bietet auch nicht den Bedienkomfort des primären Systems.

So können z. B. beim Ausfall eines Managementsystems die lokalen Bedieneinheiten der angeschlossenen Subsysteme als Rückfallebene dienen. Damit bleiben alle Systeme bedienbar. Allerdings gehen die systemübergreifenden Funktionen verloren. Auch könnte es sein, dass eine Ortsdarstellung nicht mehr in einem grafischen Plan, sondern nur noch als textliche Information angegeben werden.

Wichtig ist, dass die Bediener des Gesamtsystems auch mit der Bedienung der Rückfallebene vertraut sind.

Mögliche Rückfallebenen vom Gebäudemanagementsystem-Sicherheitstechnik in Verbindung mit sicherheitstechnischen Anlagen

Gebäudemanagementsystem-Sicherheitstechnik zur/zum	Abgesetztes Bedienfeld	Tür-Terminal	Sprechstelle zur Alarmierung	Sicherheits-Leitstelle für wesentliche sicherheitsrelevante Funktionen	Redundanzsystem
Überfall- und Einbruchmeldeanlagen	●			●	
Zutrittskontrollanlagen		●		●	
Videoüberwachungsanlagen (VÜA)				●	Nur bei sehr hohen Sicherheits-Anforderungen
Brandmeldeanlagen (BMA)	●			●	
Sprachalarmanlagen (SAA)/ Elektrokustischen Notfallwarnsystemen (ENS)			●	●	
Gebäudemanagementsystem-Sicherheitstechnik				●	Nur bei sehr hohen Sicherheits-Anforderungen

2. ZVEI-Definition – Vernetzte Sicherheit

Eine Vernetzung sicherheitsrelevanter Anlagen untereinander und mit der Gebäudetechnik macht nur dann Sinn, wenn dadurch entsprechende Vorteile wie ein Sicherheitsgewinn, erweiterte Funktionalitäten oder eine höhere Wirtschaftlichkeit erzielt werden.

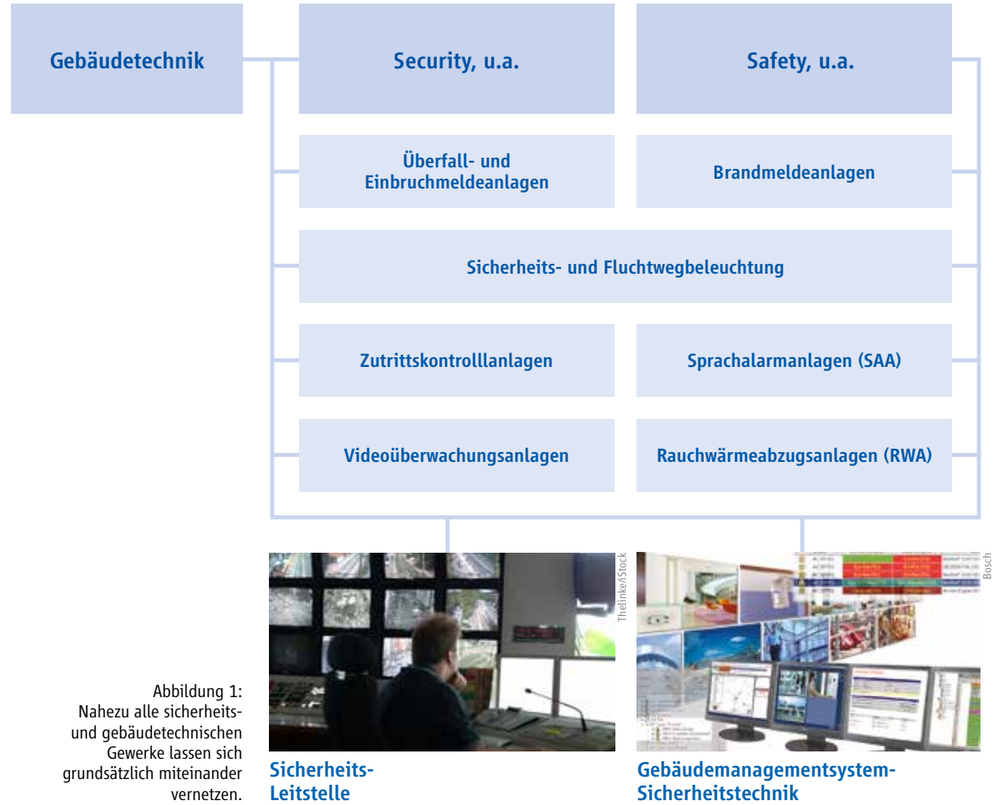


Abbildung 1:
Nahezu alle sicherheits- und gebäudetechnischen Gewerke lassen sich grundsätzlich miteinander vernetzen.

TheImke/iStock

Sicherheits-Leitstelle

Bosch

Gebäudemanagementsystem-Sicherheitstechnik

Grundsätzlich sind jedoch alle sicherheitstechnischen und gebäudetechnischen Gewerke untereinander und mit einer Leitstelle bzw. einem Gebäudemanagementsystem vernetzbar. Einige Beispiele für sicherheitstechnische Gewerke finden sich in Abb. 1. Die große Gruppe gebäudetechnischer Systeme wie Heizung, Klimatisierung oder Lüftung ist nur allgemein als „Gebäudetechnik“ dargestellt, da die Vernetzung mit diesen Systemen in einer späteren Ausgabe ergänzt wird. Das vorliegende Merkblatt behandelt ausschließlich die Vernetzung sicherheitstechnischer Gewerke untereinander und mit einer Sicherheitsleitstelle bzw. einem Gebäudemanagementsystem - Sicherheitstechnik.

Die Vernetzung sicherheits- und gebäudetechnischer Systeme kann auf unterschiedliche Weise erfolgen, beispielsweise drahtgebunden, drahtlos, seriell, parallel oder auf IP-Basis. Die Nutzung standardisierte IP-Netze wird in Zukunft deutlich zunehmen.

Vernetzte Gefahrenmanagementsysteme sind bereits heute Realität. Die Vernetzung läuft dabei im Wesentlichen über serielle oder parallele Datenleitungen. In den Fällen, bei denen eine IP-Vernetzung vorgenommen wird, erfolgt diese meist herstellerspezifisch und in separaten Netzwerken zwischen Zentralen, Unterzentralen und Visualisierungen, während Melder, Leser oder Handtaster über separate serielle Datenleitungen angebunden sind.

2.1 Beispiele für die Vernetzung von sicherheitstechnischen Gewerken:

- Bei einem Brandalarm erfolgt die Meldung zur Feuerwehr sowie parallel als Sekundäralarm an den Gebäude-Leitstand bzw. zu einer externen Sicherheits-Leitstelle.
- Sprachalarmsysteme oder andere akustische Alarmierungskomponenten werden aktiviert, um die sofortige Räumung des Gebäudes zu unterstützen.
- Die Brandfallsteuerung von Aufzügen wird aktiviert.
- Eine „videobasierte Branddetektion“ in Sonderbereichen wie z. B. Containern, Reifenlager, Müllverbrennungsanlagen, Kraftwerke.
- Vernetzung von Überfall- und Einbruchmeldeanlagen mit Zutrittskontroll- und Videoüberwachungssystemen, um die Detektionswahrscheinlichkeit von unerlaubten Zutrittsversuchen zu erhöhen.
- Zutrittskontrollanlagen mit Videoüberwachungssystemen, wenn sich z. B. der Empfang eines Unternehmens nicht im Erdgeschoss eines Unternehmens befindet oder um Tor- und Schrankenanlagen im Lieferantenbereich zu überwachen.

3. Bestehende Normen und Richtlinien in Verbindung mit der „Vernetzten Sicherheit“

Bereits heute existieren für die Gewerke der Sicherheitstechnik zahlreiche Regelungen zur Vernetzung und zu den Schnittstellen solcher Systeme, die sich allerdings über viele Normen und Richtlinien der unterschiedlichsten Regelsetzer verteilen. Die wichtigsten sind – ohne Anspruch auf Vollständigkeit – untenstehend zusammengefasst: Die Auflistung soll Betreibern, Planern, Errichtern und anderen an Bau und Betrieb von sicherheitstechnischen Anlagen als erste Orientierungshilfe dienen. Sie ist weder vollständig noch ist sie als Checkliste, Planungshilfe oder ähnliches zu betrachten.

Über diese Auflistung hinaus existieren zahlreiche weitere Gesetze, Normen, Richtlinien und andere Vorschriften sowie je nach Objekt behördliche Auflagen zu Planung, Bau und Betrieb von sicherheitstechnischen Anlagen. Welche wie zu beachten sind, liegt allein in der Verantwortung des Bauherren bzw. Betreibers und der beteiligten Dienstleistungsunternehmen. Ihre Anwendung und Umsetzung kann nur individuell am jeweiligen Objekt geklärt werden. Die Normen, Richtlinien und Vorschriften sind jeweils in ihrer aktuellen Fassung gültig.

3.1 Überfall- und Einbruchmeldeanlagen (ÜMA/EMA)

3.1.1 Normen auf deutscher und europäischer Ebene

DIN VDE 0833-1 (VDE 0833-1) „Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 1: Allgemeine Festlegungen“

DIN VDE 0833-3 (VDE 0833-3) „Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 3: Festlegungen für Einbruch- und Überfallmeldeanlagen“

DIN EN 50136-2 - 08/2014 „Alarmübertragungsanlagen (AÜA) und -einrichtungen“ Teil 2 Anforderungen an Übertragungseinrichtungen (ÜE)

DIN EN 50136-3 - 08/2014 „Alarmübertragungsanlagen (AÜA) und -einrichtungen“ Teil 3 Anforderungen an Übertragungszentralen (ÜZ)

3.1.2 VdS – Richtlinien

VdS 2311 „VdS-Richtlinien für Einbruchmeldeanlagen – Planung und Einbau“

VdS 2311-S1 „Einbruchmeldeanlagen, Planung und Einbau, Ergänzung S1“

VdS 2463 „Übertragungsgeräte für Gefahrenmeldungen (ÜG), Anforderungen“

VdS 2465 „Übertragungsprotokoll für Gefahrenmeldeanlagen“

VdS 2465-S2 „Übertragungsprotokoll für Gefahrenmeldungen, Ergänzung S2: Protokollerweiterung zur Anschaltung an Netze der Protokollfamilie TCP“

VdS 2465-S3 „Übertragungsprotokoll für Gefahrenmeldeanlagen, Ergänzung S3: Protokollerweiterung zur Anschaltung von Videoüberwachungsanlagen an Gefahrenmeldeanlagen“

VdS 2471 „Übertragungswege in Alarmübertragungsanlagen, Anforderungen und Prüfmethoden“

VdS 2472 „Sicherungsrichtlinien für Banken, Sparkassen und sonstige Zahlstellen“

3.2 Zutrittskontrollanlagen

3.2.1 Normen auf deutscher und europäischer Ebene

EN 50133-1 / DIN VDE 0830 Teil 8-1 „Zutrittskontrollanlagen für Sicherungsanwendungen, Teil 1 Systemanforderungen“

Dokument wurde ersetzt durch:
DIN EN 60839-11-1; VDE 0830-8-11-1
DIN EN 60839-11-1 Berichtigung 1; VDE 0830-8-11-1 Berichtigung 1

EN 50133-2-1 / DIN VDE 0830 Teil 8-2-1 „Zutrittskontrollanlagen für Sicherungsanwendungen, Teil 2 - 1: Allgemeine Anforderungen an Anlagenteile“

EN 50133-7 / DIN VDE 0830 Teil 8-7 „Zutrittskontrollanlagen für Sicherungsanwendungen, Teil 7: Anwendungsregeln“

Nachfolgedokument als Entwurf aus 08-2013: DIN EN 60839-11-1; VDE 0830-8-11-2

3.2.2 VdS-Richtlinien

VdS 2353 „Richtlinien für die Anerkennung von Errichterfirmen für Zutrittskontrollanlagen“

VdS 2358 „Richtlinien für Zutrittskontrollanlagen, Teil 1: Anforderungen“

VdS 2367 „Richtlinien für Zutrittskontrollanlagen, Teil 3: Planung und Einbau“

VdS 3436 „Betriebsbuch für Zutrittskontrollanlagen“

3.2.3 BSI-Richtlinien (Bundesamt für Sicherheit in der Informationstechnik)

TL 03402 (BSI 7550) „Anforderungen an Zutrittskontrollanlagen“

TL 03403 (BSI 7551) „Zutrittskontrollanlagen – Richtlinien für die Projektierung und Ausführung“

TL 03424 „Ergänzung zu BSI TL elektronische Schließsysteme, Zutrittskontrollanlagen, Anforderungen für elektronische Schlüssel“

TR 03126-5 „Elektronischer Mitarbeiterausweis“

TL 03405 „Elektronische Schließzylinder“

3.3 Videoüberwachungsanlagen

3.3.1 Normen auf deutscher und europäischer Ebene

DIN EN 50132-1 (VDE 0830-7-1) „Alarmanlagen – CCTV – Überwachungsanlagen für Sicherheitsanwendungen – Systemanforderungen“[1]

DIN EN 62676-1-1 (VDE 0830-7-5-11) „Videoüberwachungsanlagen für Sicherheitsanwendungen – Systemanforderungen – Allgemeines“

DIN EN 62676-1-2 (VDE 0830-7-5-12) „Videoüberwachungsanlagen für Sicherungsanwendungen - Teil 1-2: Systemanforderungen - Allgemeine Anforderungen an die Videoübertragung“

DIN EN 62676-2-1 (VDE 0830-7-5-21) „Videoübertragungsprotokolle - Allgemeine Anforderungen“

DIN EN 62676-2-2 (VDE 0830-7-5-22) „Videoübertragungsprotokolle - IP-Interoperabilität auf Basis von HTTP- und REST-Diensten“

DIN EN 62676-2-3 (VDE 0830-7-5-23) „Videoübertragungsprotokolle - IP-Interoperabilität auf Basis von Webservices“

DIN EN 50132-5-1 (VDE 0830-7-5-1) „Alarmanlagen – CCTV – Überwachungsanlagen für Sicherheitsanwendungen – Videoübertragung – Allgemeine Leistungsanforderungen an die Videoübertragung“

DIN EN 50132-5-2 (VDE 0830-7-5-2) „Alarmanlagen – CCTV – Überwachungsanlagen für Sicherheitsanwendungen – IP Video Übertragung Protokolle“

DIN EN 50132-5-3 (VDE 0830-7-5-3) „Alarmanlagen – CCTV – Überwachungsanlagen für Sicherheitsanwendungen – Videoübertragung – Analoge und digitale Videoübertragung“

DIN EN 50132-7 (VDE 0830-7-7) „Alarmanlagen – CCTV – Überwachungsanlagen für Sicherheitsanwendungen – Anwendungsregeln“

Norm – Entwurf DIN EN ISO 22311 „Sicherheit und Schutz des Gemeinwesens - Videoüberwachung – Datenschnittstellen“ (ISO 22311:2012) Deutsche Fassung FprEN ISO 22311

[1] 11/2014 zurückgezogen. Gemäß DIN EN 62676-1-1 besteht eine Übergangsfrist bis 02.12.2016. Nachfolgedokument ab 11/2014 ist DIN EN 62676-1-1.

3.3.2 **VdS – Richtlinien Planung und Einbau**

VdS 2366 „Videoüberwachungsanlagen – Planung und Einbau“

VdS 3425 „VdS - Betriebsbuch für VÜA“

VdS 3426 „Installationsattest für eine Videoüberwachungsanlage (VÜA)“

VdS 2833 „Schutzmaßnahmen gegen Überspannung für GMA und Feuerlöschanlagensteuerungen“

VdS 2135 „Grafische Symbole für Gefahrenmeldeanlagen“

VdS 3517 „Testbild für Videoüberwachungsanlagen (VÜA)“[2]

3.3.3 **VdS - Verfahren zur Zertifizierung von Errichterfirmen**

VdS 3442 „Richtlinien für die Anerkennung von Errichterfirmen für Videoüberwachungsanlagen (VÜA) – Verfahrensrichtlinien“

3.3.4 **VdS – Richtlinien für Produkte**

VdS 2364 Entwurf „Videoüberwachungsanlagen-Systemanforderungen Kategorie I“

3.3.5 **Polizei**

Arbeitsgruppe des Hessischen Landeskriminalamtes 03/2013 „Handlungsempfehlung für die Errichtung und den Betrieb von Videoüberwachungsanlagen im öffentlichen Raum“[3]

3.3.6 **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

Bei VS-Objekten sind Videoanlagen nur mit ausdrücklicher Genehmigung einbaubar

3.3.7 **Arbeitskreis Maschinen- und Elektrotechnik (AMEV)**

Instand GMA 2012

Vertragsmuster für Instandhaltung von Gefahrenmeldeanlagen (Brand, Einbruch, Überfall, Video, ZUKO und Geländeüberwachung) in öffentlichen Gebäuden (AMEV Instand GMA 2012). Gemäß Erlass gültig für alle Bundesländer ab 05.07.2012, hierdurch wird der „AMEV Instand GMA 2005“ ungültig.

[2] Hinweis: Mit dem Testbild können wesentliche Forderungen an das von der VÜA erzeugte Bild verifiziert werden. Es dient als praktisches Hilfsmittel vor Ort.

[3] gilt für ganz Deutschland

3.3.8 **Deutsche Gesetzliche Unfall Versicherung (DGUV)**

Die Berufsgenossenschaftlichen Vorschriften, Richtlinien, Informationen und Grundsätze werden heute bereits durch die DGUV verwaltet und veröffentlicht. Diese Umstellung hat auch eine Änderung der Kurzbezeichnung zur Folge.

DGUV Vorschrift 25 (früher BGV C9 (VBG 120)) Unfallverhütungsvorschrift „Kassen“ (Geldinstitute)
Durchführungsanweisung zur UVV Kassen

DGUV Vorschrift 20 (früher BGV C3 (VBG 105)) Unfallverhütungsvorschrift Spielhallen, Spielcasinos und Automatensäle von Spielbanken.
Durchführungsanweisung zur UVV Spielhallen, Spielcasinos und Automatensäle von Spielbanken.

3.4 Brandmeldeanlagen

3.4.1 **Normen auf deutscher und europäischer Ebene**

DIN VDE 0833-1 (VDE 0833-1) „Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 1: Allgemeine Festlegungen“

DIN VDE 0833-2 (VDE 0833-2) „Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 2: Festlegungen für Brandmeldeanlagen“

DIN 14674 „Brandmeldeanlagen – Anlagenübergreifende Vernetzung“
Anhang A (informativ) Auswahl des Übertragungsweges

DIN EN 50136-2 - 08/2014 „Alarmübertragungsanlagen (AÜA) und -einrichtungen“
Teil 2 Anforderungen an Übertragungseinrichtungen (ÜE)

DIN EN 50136-3 - 08/2014 „Alarmübertragungsanlagen (AÜA) und - einrichtungen“
Teil 3 Anforderungen an Übertragungszentralen (ÜZ

DIN EN 54-21 „Brandmeldeanlagen - Teil 21: Übertragungseinrichtungen für Brand- und Störungsmeldungen“ - Anhang B (normativ) „Überprüfung der Leistungsanforderungen für Übertragungsanlagen für Brand- und Störungsmeldungen“

3.4.2 **VdS**

VdS 2095 „VdS-Richtlinien für automatische Brandmeldeanlagen - Planung und Einbau“

VdS 2878 „VdS-Merkblatt zur Vernetzung (Zusammenschaltung) von Brandmelde-Alt- und Neuanlagen“

3.5 Sprachalarmanlagen / Elektroakustische Notfallwarnsysteme (SAA/ENS)

3.5.1 Normen auf deutscher und europäischer Ebene

Entwurf - DIN EN 50849 (VDE 0828-1) „Elektroakustische Notfallwarnsysteme“; Deutsche Fassung prEN 50849

DIN VDE 0833-4 (VDE 0833-4) „Gefahrenmeldeanlagen für Brand, Einbruch und Überfall – Teil 4: Festlegungen für Anlagen zur Sprachalarmierung im Brandfall“

ZVEI Merkblatt „Elektroakustische Alarmierungseinrichtungen – Erläuterungen und Ergänzungen zu Normen, rechtlichen Grundlagen und technischen Regeln“, Stand: Dezember 2010

3.6 Rauch- und Wärmeabzugsanlagen (RWA)

3.6.1 Normen auf deutscher und europäischer Ebene

DIN 18232 „Rauch- und Wärmefreihaltung“, Normenreihe Teile 1-8

DIN 18232-2 „Rauch- und Wärmefreihaltung - Teil 2: Natürliche Rauchabzugsanlagen (NRA); Bemessung, Anforderungen und Einbau“

DIN EN 12101 „Rauch- und Wärmefreihaltung“, Normenreihe Teile 1 bis 10

Normentwurf DIN EN 12101-2 „Rauch- und Wärmefreihaltung - Teil 2 Anforderungen und Prüfmethoden für Natürliche Rauch- und Wärmeabzugsgeräte (NRWG)“, Deutsche Fassung FprEN 12101-2:2014

Normentwurf DIN EN 12101-9 „Rauch- und Wärmefreihaltung - Teil 9: Steuerungstafeln“, Deutsche Fassung prEN 12101-9

DIN EN 12101-10 „Rauch- und Wärmefreihaltung - Teil 10: Energieversorgung“, Deutsche Fassung EN 12101-10

3.6.2 Internationale Normen

ISO 21927 „Rauch- und Wärmefreihaltung“, Normenreihe Teile 1 bis 10

ISO 21927-2 „Rauch- und Wärmefreihaltung - Teil 2: Festlegungen für natürliche Rauch- und Wärmeabzugsgeräte“

ISO 21927-9 „Rauch- und Wärmefreihaltung - Teil 9: Festlegung der Steuerungstafeln“

ISO 21927-10 „Rauch- und Wärmefreihaltung - Teil 10: Festlegung der Energieversorgungseinheit“

3.7 Sicherheits- und Fluchtwegbeleuchtung

3.7.1 Normen auf deutscher und europäischer Ebene

DIN EN 60598-1 „Leuchten - Teil 1: Allgemeine Anforderungen und Prüfungen“

DIN EN 60598-2-22 „Leuchten - Teil 2-22: Besondere Anforderungen - Leuchten für Notbeleuchtung“

DIN EN 1838 „Angewandte Lichttechnik – Notbeleuchtung“

DIN EN 61547 „Einrichtungen für allgemeine Beleuchtungszwecke - EMV-Störfestigkeitsanforderungen“

DIN 4844-1 „Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Teil 1: Erkennungsweiten und farb- und photometrische Anforderungen“

DIN 4844-2 „Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Teil 2: Registrierte Sicherheitszeichen“

DIN EN ISO 7010 „Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Registrierte Sicherheitszeichen“

DIN ISO 3864-1 „Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Teil 1: Gestaltungsgrundlagen für Sicherheitszeichen und Sicherheitsmarkierungen“

DIN ISO 3864-2 Berichtigung 1 „Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Teil 2: Gestaltungsgrundlagen für Sicherheitsschilder zur Anwendung auf Produkten“

DIN ISO 3864-3 „Graphische Symbole - Sicherheitsfarben und Sicherheitszeichen - Teil 3: Gestaltungsgrundlagen für graphische Symbole zur Anwendung in Sicherheitszeichen“

DIN EN 50172 „Sicherheitsbeleuchtungsanlagen“

DIN EN 50272-2 „Sicherheitsanforderungen an Batterien und Batterieanlagen“

DIN EN 62034 „Automatische Prüfsysteme für batteriebetriebene Sicherheitsbeleuchtung für Rettungswege“

DIN VDE 0100-559 „Errichten von Niederspannungsanlagen - Teil 5-559: Auswahl und Errichtung elektrischer Betriebsmittel - Leuchten und Beleuchtungsanlagen“

DIN VDE 0100-560 „Errichten von Niederspannungsanlagen - Teil 5-56: Auswahl und Errichtung elektrischer Betriebsmittel - Einrichtungen für Sicherheitszwecke“

DIN VDE 0100-710 „Medizinisch genutzte Bereiche“

DIN VDE 0100-714 „Errichten von Niederspannungsanlagen - Teil 7-714: Anforderungen für Betriebsstätten, Räume und Anlagen besonderer Art - Beleuchtungsanlagen im Freien“

DIN VDE 0100-715 „Errichten von Niederspannungsanlagen - Teil 7-715: Anforderungen für Betriebsstätten, Räume und Anlagen besonderer Art – Kleinspannungsbeleuchtungsanlagen“

DIN V VDE V0108-100 „Sicherheitsbeleuchtungsanlagen“

3.7.2 Sonstige

ASR A2-3 „Fluchtwege und Notausgänge, Flucht- und Rettungsplan“

ASR A3.4/3 „Sicherheitsbeleuchtung, Optische Sicherheitsleitsysteme“

Arbeitsstättenverordnung

3.8 Bezugsquellen für Normen, Richtlinien, Bestimmungen und Vorschriften

Abkürzung	Institution / Adresse NoRiBeVo* zu beziehen über	PLZ/Ort	Telefon / Fax / Internet
Beuth	Beuth Verlag GmbH Am DIN-Platz, Burggrafenstraße 6	10787 Berlin	030 2601-0 030 2601-1260 www.beuth.de
VDE	VDE Verlag GmbH Bismarkstraße 33	10625 Berlin	030 348001-0 030 348001-9088 www.vde-verlag.de
VdS	VdS Schadensverhütung **NoRiBeVo** zu beziehen über: VdS Schadensverhütung Verlag Amsterdamer Straße 174	 50737 Köln	 0221 7766-0 0211 7766341 vds.de/de/bildungszentrum-verlag/
LKA-ÜEA	Landeskriminalämter – jeweils die zuständigem Landeskriminalämter der Länder **NoRiBeVo** zu beziehen über: Polizeitechnisches Institut Münster Zum roten Berge 18-24	 48165 Münster	 02501 806-256 02501 806-239
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte Kurt-Georg-Kiesinger-Allee 3	53175 Bonn	0228 993073 0228 993075207 www.bfarm.de/DE/Home/home_node.html
DGUV	Unfallverhütungsvorschriften Berufsgenossenschaftliche Vorschriften und Regelwerk – Regional unterschiedliche Ansprechstellen **NoRiBeVo** zu beziehen über: Carl Heymanns Verlag KG Luxemburger Straße 449	 50939 Köln	 0221 94373-0 0221 94373-603 www.carl-heymanns.de/index.php?id=2
BSI	Bundesamt für Sicherheit in der Informationstechnik – Referat III 2.1 Postfach 20 03 63	53133 Bonn	0228 9995820 0228 9995825400 www.bsi.bund.de/DE/Home/home_node.html
ProPK	Kommission Polizeiliche Kriminalprävention der Länder und des Bundes - Zentrale Geschäftsstelle Hölderlinstraße 5 **NoRiBeVo** zu beziehen über: Hessisches Landeskriminalamt HSG 16 - Zentralstelle Öffentlichkeitsarbeit Hölderlinstraße 5	70372 Stuttgart 65187 Wiesbaden	 0611 83-8119 0611 83-8115 www.polizei.hessen.de/Dienststellen/Hessisches-Landeskriminalamt/
ZVEI	Zentralverband Elektrotechnik und Elektroindustrie e.V. **NoRiBeVo** zu beziehen über: ZVEI Versand Verlagsprodukte Lyoner Straße 9	 60528 Frankfurt/M.	 069 6302-200 069 6302-317 www.zvei.org/Seiten/Startseite.aspx
DIBt	Deutsches Institut für Bautechnik – DIBt Kolonnenstraße 30 B	10829 Berlin	030 78730-0 / 030 78730-320 / www.dibt.de/

NoRiBeVo* = Normen Richtlinien Bestimmungen Vorschriften

Achtung:
einige Ausgaben der Normen, Richtlinien, Bestimmungen, Vorschriften können auch, soweit vorhanden, über den Beuth Verlag GmbH, 10772 Berlin, bezogen werden!

Verlagsanschriften für Normen, Richtlinien, Bestimmungen und Vorschriften (NoRiBeVo*) – Stand: August 2015

4. Gewerke der „Vernetzten Sicherheit“

4.1 Security

4.1.1 Überfall- und Einbruchmeldeanlagen (ÜMA/EMA)

4.1.1.1 Funktionale Beschreibung

Überfall- und Einbruchmeldeanlagen sind Gefahrenmeldeanlagen nach DIN VDE 0833, an die besondere Anforderungen an Verfügbarkeit, Zuverlässigkeit der Meldungsübertragung sowie Stör- und Sabotagesicherheit gestellt werden.

4.1.1.2 Definition der Überfallmeldeanlagen (ÜMA)

Überfallmeldeanlagen sind nach DIN VDE 0833-1 Gefahrenmeldeanlagen, die Personen zum direkten Hilferuf bei Überfällen dienen – in der Regel direkt zur Polizei. Parallel kann dieser Alarm als Sekundäralarm von einer externen Sicherheitsleitstelle entgegengenommen werden.

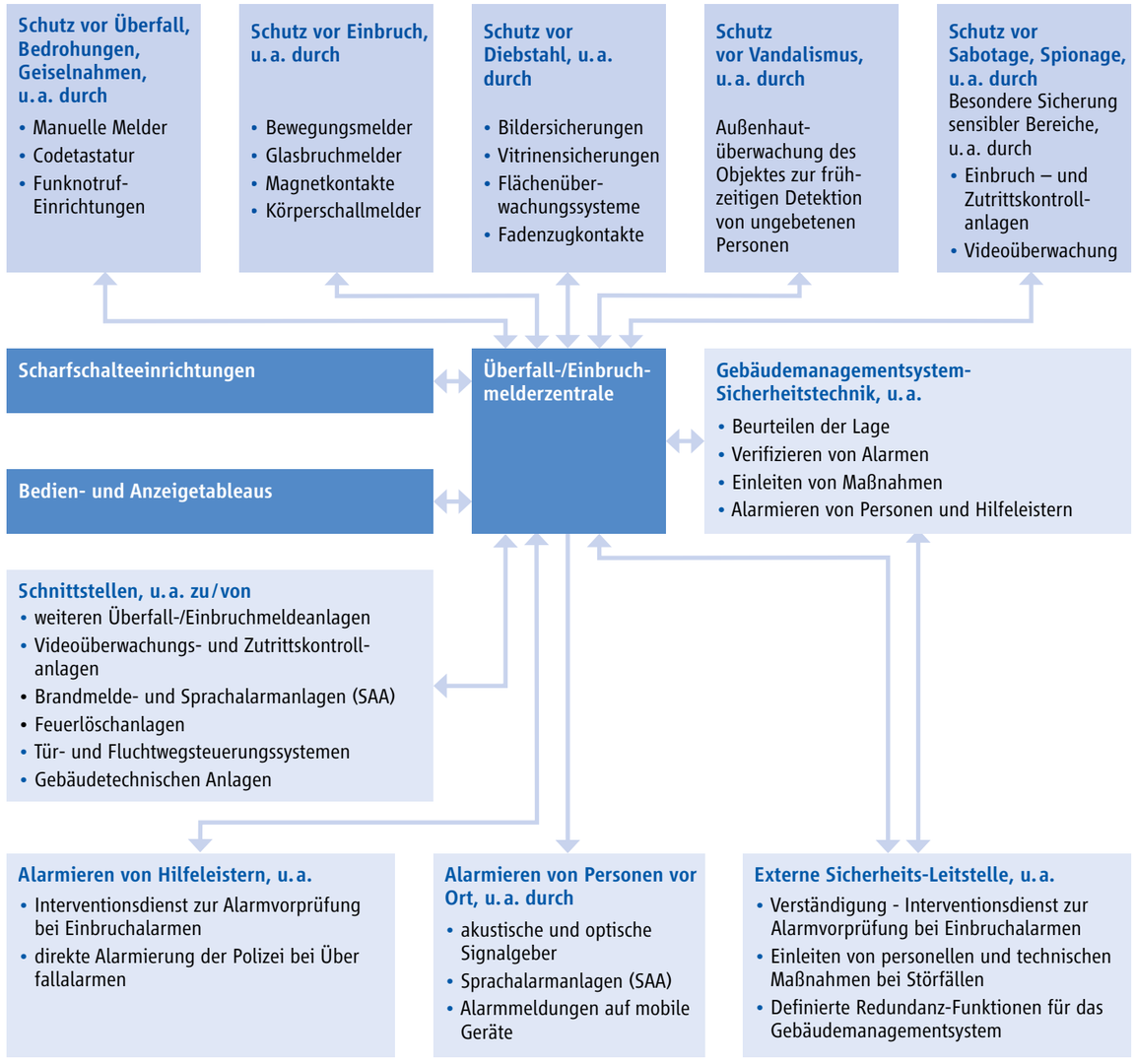
4.1.1.3 Definition der Einbruchmeldeanlagen (EMA)

Einbruchmeldeanlagen sind nach DIN VDE 0833-1 Gefahrenmeldeanlagen, die dem automatischen Überwachen von Gegenständen auf unbefugte Wegnahme sowie von Flächen und Raumen auf unbefugtes Eindringen dienen. Ein Alarm kann direkt von der Polizei oder von einer Hilfe leistenden Stelle, wie z. B. eine externe Sicherheitsleitstelle entgegengenommen werden. Es erfolgt eine sofortige Einleitung der erforderlichen Hilfsmaßnahmen und gegebenenfalls Interventionsmaßnahmen durch die Polizei oder einen Sicherheitsdienstleister vor Ort.

4.1.1.4 Aufbau, Aufgaben und Funktionen

ÜMA/EMA bestehen aus manuellen und automatischen Einbruch- und Überfallmeldern, einer Steuereinheit („Überfall- und Einbruchmelderzentrale“) mit Energie- und Notstromversorgung und der Übertragungseinrichtung zu einer Polizei und/oder zu einer privaten Sicherheitsleitstelle. Zur Weiterleitung der Signale an die Zentrale sind die Melder einzeln oder in Gruppen an Meldelinien angeschlossen. Diese werden als Stich- und/oder Ringleitungen zur Einbruchmelderzentrale geführt.
Über Scharfschalteeinrichtungen werden die Sicherungsbereiche der Einbruchmeldeanlage scharfgeschaltet. In diesem Zustand werden die Einbruchmeldungen über die Übertragungseinrichtung zu einer privaten Sicherheitsleitstelle weitergeleitet. Weitere Aufgaben der Überfall- und Einbruchmelderzentrale sind die Funktions- und Sabotageüberwachung der gesamten Anlage einschließlich Anzeige eventueller Fehler.

4.1.1.5 **Beispielhafte Konfiguration einer Überfall- und Einbruchmeldeanlage (ÜMA/EMA)**



4.1.1.6 Überfall- und Einbruchmeldeanlagen (ÜMA/EMA) – Kernaussagen und Nutzen

Beispielhafte Schutzziele – Schutz vor
- Überfall/Bedrohung/Geiselnahme
- Einbruch
- Diebstahl
- Vandalismus
- Sabotage/Spionage

Überfall und Bedrohung, u. a.
- Auslösen eines stillen Alarms (z. B. an die Polizei) mittels Überfallmelder (z. B. Geldscheinkontakt oder Fußschiene) oder durch Eingeben eines Überfallcodes (z. B. bei Überfall beim Betreten eines Gebäudes)

Einbruch und Vandalismus, u. a.
- Überwachung im Außenbereich des Objektes/Freilandsicherung (Lichtschranken etc.), Videosensorik; Überwachung der Außenhaut des Gebäudes: Glasbruchmelder, Magnetkontakte, Riegelkontakte
- Schwerpunktmäßige Überwachung der Innenräume: Bewegungsmelder
- Objektsicherung (z. B. Geldausgabeautomaten): Körperschallmelder

Diebstahl (besonders im Tagbetrieb bei Anwesenheit von Personen), **u. a.**
- Überwachung auf Wegnahme oder Annäherung:
- Bildersicherung: kapazitive und mechanische Melder
- Vitrinensicherung: kapazitive und seismische Melder

Schnelle und sichere Alarmierung der Polizei und anderer Hilfeleister, u. a.
- Alarmierung der Polizei über gesicherte Übertragungswege
- sofortige Einleitung von vereinbarten Maßnahmen durch eine externe Sicherheits-Leitstelle (z. B. bei unplanmäßiger Unscharfschaltung oder fehlender Scharfschaltung der Einbruchmeldeanlage)
- Alarmierung von Personen vor Ort bei Einbruch/Diebstahl durch akustische und optische Signalgeber

Funktionssicherheit des Notrufmeldesystems, u. a. durch
- fachgerechte Planung und Projektierung
- Systemkomponenten (Zentrale und Melder)
- Zwangsläufigkeit beim Scharfschalten des Notrufmeldesystems (z. B. über Blockschloss)

IST: Einsatz von flexibler „Sicherheits-Netzwerk-Technologie" – zukünftig: Mitnutzung von IT-Netzwerken
- Lokalisierung von Ereignisorten durch Einzelmelderidentifizierung
- Notruf-, Brand- und technische Meldungen (z.B. aus der Haustechnik) in einem System und über „ein" Leitungsnetz
- Problemlose Einbindung von Video- und Zutrittskontrollsystemen

4.1.1.7 Klassifizierung

In der ÜEA-Richtlinie wird je nach den Sicherungsanforderungen in verschiedene Schutzgrade bzw. VdS-Klassen unterteilt. Je höher die Anforderungen, desto größer sind die Anforderungen an Überwindungsschutz, Sabotagesicherheit und Funktionsüberwachung.

Polizei		Klasse (Grad) nach	Klasse (Grad) nach	VdS-Klasse
Pfk	ÜEA-Rili	DIN EN 50131-1	DIN VDE 0833-3	
---	---	1	1	---
A[1)]	---	2	2	A[1)]
B[2)]	B[2)]	3	3[2)]	B[2)]
C[3)]	C[3)]	4	4[3)]	C[3)]

Zusammenstellung der Schutzgrade bzw. -klassen nach der ÜEA-Richtlinie 3.

--- Keine Entsprechung. Solche Anlagen sind gemäß den Polizeirichtlinien nicht zulässig (Grad 1 gemäß Pfk bzw. Grad 1 und 2 gemäß ÜEA-Richtlinie).

1) Es sind grundsätzlich für den Grad 2 zertifizierte Melder einzusetzen.

2) Es sind grundsätzlich für den Grad 3 zertifizierte Melder einzusetzen. Wenn durch geeignete Planung und Errichtung sichergestellt ist, dass dem Risikopotenzial entsprochen wird, ist auch der Einsatz von Meldern zulässig, welche die Anforderungen der VdS Klasse B erfüllen. Hierbei sind jedoch Maßnahmen vorzusehen, die das Umgehen der Melder von innerhalb des Sicherungsbereiches erschweren.

3) Es sind grundsätzlich für den Grad 4 zertifizierte Melder einzusetzen. Wenn durch geeignete Planung und Errichtung sichergestellt ist, dass dem Risikopotenzial entsprochen wird, ist auch der Einsatz von Meldern des Grades 3 bzw. Meldern, welche die Anforderungen der VdS Klasse C erfüllen, zulässig.

4.1.1.8 Bundeseinheitliche Richtlinie für Überfall- und Einbruchmeldeanlagen (ÜMA-EMA) mit Anschluss an die Polizei (ÜEA-Richtlinie)

Die Aufschaltung von ÜEA zur Polizei dient in Deutschland im Rahmen eines umfassenden Sicherungskonzeptes dazu, bei entsprechenden Gefahrenlagen die Polizei direkt zu alarmieren, um polizeiliche Maßnahmen einleiten zu können. Hierbei soll auch die präventive Wirkung durch nachhaltige Verringerung des Tatanreizes berücksichtigt werden.

Die „Bundeseinheitliche Richtlinie für Überfall- und Einbruchmeldeanlagen mit Anschluss an die Polizei (ÜEA) - kurz: ÜEA-Richtlinie" enthält hierfür die entsprechenden Anforderungen. Sie beschreibt Planung, Errichtung, Erweiterung, Änderung, Betrieb und Instandhaltung von Überfall- und Einbruchmeldeanlagen (ÜEA) und legt die dafür notwendigen Mindestanforderungen fest mit dem Ziel, eine zuverlässige Meldungsgabe zu erreichen. Sie nennt die Voraussetzungen, unter denen ein Anschluss genehmigt oder abgeschaltet werden kann und regelt das Genehmigungsverfahren. Die zuständige Polizeibehörde/-dienststelle sollte bereits in der Planungsphase bzw. bei der Erarbeitung des Sicherungskonzeptes zur Beratung herangezogen werden.

4.1.1.8.1 **Zur ÜEA-Richtlinie gehören insgesamt elf Anlagen:**

1. Begriffe und Definitionen
2. Aufbau einer ÜEA
3. Antrag zur Errichtung, Erweiterung, Änderung einer ÜEA
4. Antrag für die Abnahme einer ÜEA mit Abnahmeprotokoll und Anlagenbeschreibung
5. Projektierungs- und Installationshinweise für Überfall- und Einbruchmeldeanlagen
6. Anforderungen an die Bildübertragung und Bildsteuerung
7. Voraussetzung für ein Fachunternehmen und dessen Pflichten
8. Merkblatt für den Betreiber von ÜEA
9. Überprüfung von ÜEA
10. Anforderungen an Alarmempfangsstellen bei der Polizei, AS-Pol
11. Länderspezifische Zusatzregelungen

Die Anlagenbeschreibung in Anhang 4 wurde von ZVEI und BHE in einem verbändeübergreifenden Ansatz gemeinsam mit der Polizei in zahlreichen technischen und redaktionellen Details überarbeitet.
Die Anlagenbeschreibung hat nun den aktuellen Stand 01.03.2014.

4.1.1.9 **Bildübertragung**

Es sind nach Alarmauslösung in einigen Bundesländern auch Bildübertragungen zur Polizei möglich. Werden diese im Rahmen der ÜEA-Richtlinie vorgenommen, gelten die Anforderungen nach Anlage 6. Es sind jedoch auch Bildübertragungen aus Notruf- und Serviceleitstellen (NSL) an die Polizei möglich.

4.1.1.10 **Einbruchmeldeanlagen (EMA) nach der Norm DIN VDE 0833-3, Grad 1 - 2 - 3 - 4**

Einbruchmeldeanlagen werden nach der VDE 0833-3 je nach Risiko und Gefährdung in verschiedene Schutzgrade eingeteilt.

Die folgende Tabelle enthält die für den jeweiligen Grad die von der Norm mindestens geforderten Eigenschaften:

- Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 1
- Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 2
- Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 3
- Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 4

Anschaltung der EMA-Zentraleinheit an

Gebäudemanagementsystem-Sicherheitstechnik

Externe Sicherheits-Leitstelle

Nachfolgende Übertragungswege sind bei der (IP-) Vernetzung erforderlich:

- EMA-Sensorik zur EMA-Zentraleinheit
- EMA-Zentraleinheit zum Gebäudemanagementsystem-Sicherheitstechnik
- EMA-Zentraleinheit zur externen Sicherheits-Leitstelle
- Gebäudemanagementsystem-Sicherheitstechnik zur externen Sicherheits-Leitstelle

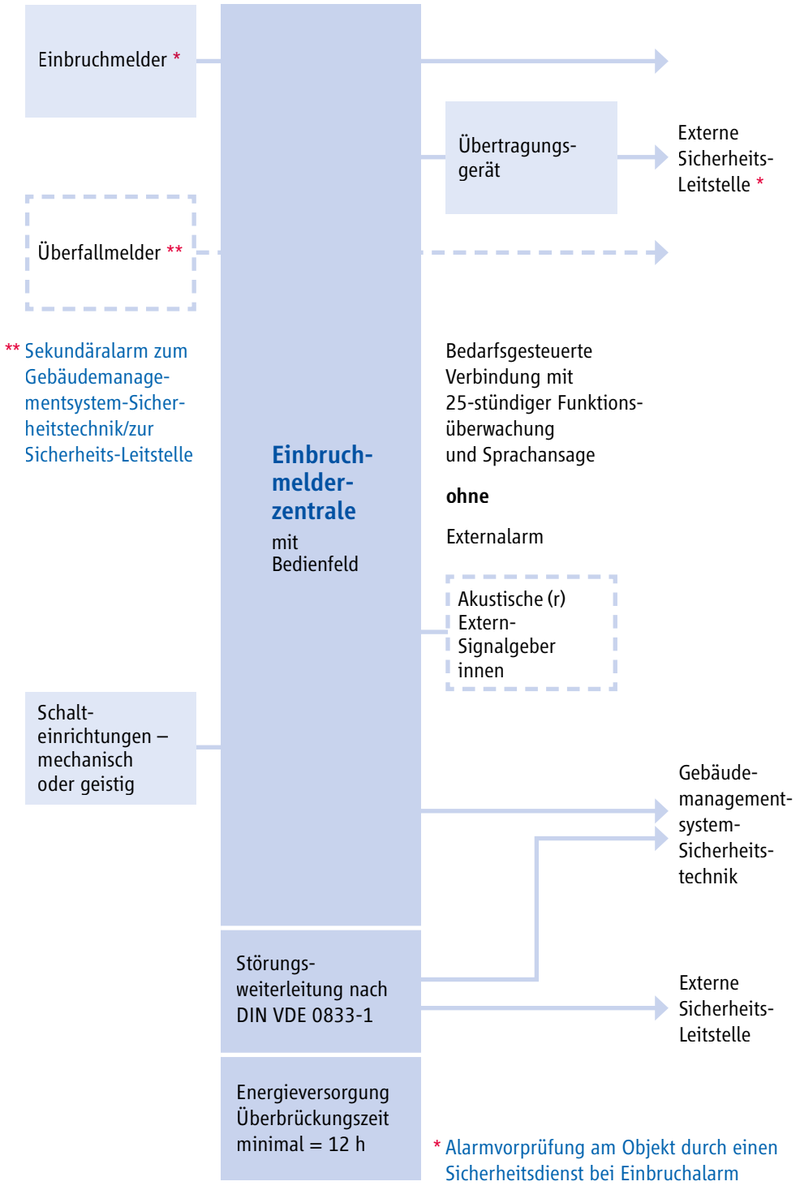
4.1.1.10.1 **Übersicht der beispielhaften Konzepte für Einbruchmeldeanlagen (EMA) nach der Norm DIN VDE 0833-3, Grad 1 - 2 - 3 - 4**

	DIN VDE 0833-3, Grad 1	DIN VDE 0833-3, Grad 2	DIN VDE 0833-3, Grad 3	DIN VDE 0833-3, Grad 4
Die Einbruchmeldeanlage entspricht der Norm DIN VDE 0833-3, Grad 1, 2, 3, 4	●	●	●	●
Die verwendeten Anlageteile müssen mindestens VdS Klasse A anerkannt sein.	●			
Die verwendeten Anlageteile müssen mindestens VdS Klasse B anerkannt sein.		●		
Ab Grad 3 wird unterschieden in außenhaut- und fallen-/schwerpunktmäßiger Überwachung. Die verwendeten Anlageteile müssen mindestens VdS Klasse B anerkannt sein.			●	
Ab Grad 3 wird unterschieden in außenhaut- und fallen-/schwerpunktmäßiger Überwachung. Die verwendeten Anlageteile müssen mindestens VdS Klasse C anerkannt sein.				●
Bei Überfall- und Einbruchmeldeanlagen, die nicht auf die Polizei aufgeschaltet werden, ist der „Bundeseinheitliche Pflichtenkatalog für Errichterfirmen von Überfall-Einbruchmeldeanlagen“ (LKA-Richtlinien) in der jeweils aktuellen Fassung zu beachten.		●	●	●
Die Einbruchmeldeanlage hat die Aufgabe, über Melder Gefahren zu erkennen, über eine Zentrale auszuwerten und zu signalisieren bzw. weiterzumelden, z. B. an eine externe Sicherheits-Leitstelle, um von dort eine Alarmvorprüfung am Objekt durch einen Sicherheitsdienst zu veranlassen, bevor die Polizei gerufen wird.	●	●	●	●
An der Zentrale angeschlossene Melder (z. B. Überfallmelder) sind permanent aktiv oder werden über mechanische oder geistige Schalteinrichtungen aktiviert. Die Übertragung des Überfall-Sekundäralarms an die externe Sicherheits-Leitstelle ist möglich.	●	●	●	●
Bei Verwendung von mechanischen Schalteinrichtungen sind Schlösser mit Profilzylinder nach DIN18252, Klasse P2, wie folgt vorzusehen:				
mindestens 300 Variationsmöglichkeiten	●			
mindestens 3.000 Variationsmöglichkeiten		●		
Bei Verwendung von mechanischen Schalteinrichtungen sind Schlösser mit Profilzylinder nach DIN18252, Klasse P3, mit mechanischem Bohr- und Ziehschutz wie folgt vorzusehen:				
mindestens 15.000 Variationsmöglichkeiten			●	
mindestens 100.000 Variationsmöglichkeiten				●

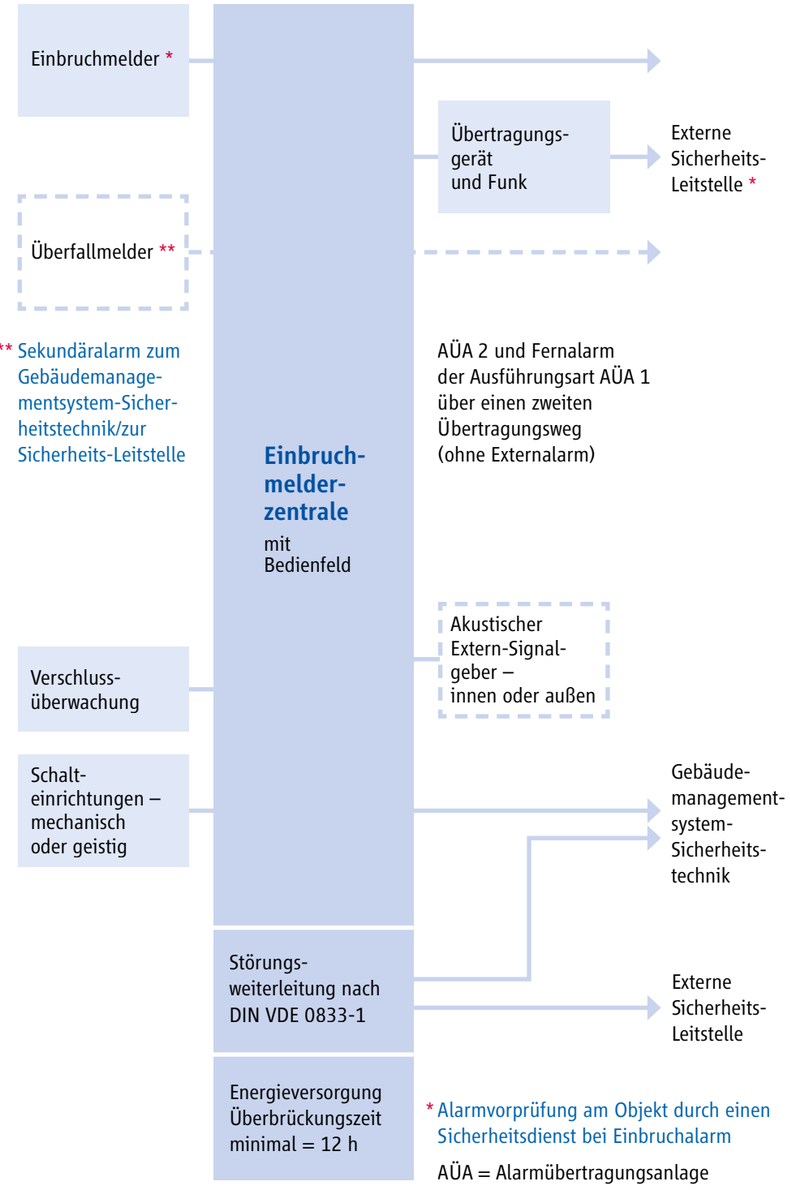
	DIN VDE 0833-3, Grad 1	DIN VDE 0833-3, Grad 2	DIN VDE 0833-3, Grad 3	DIN VDE 0833-3, Grad 4
Bei Verwendung von mechanischen Schalteinrichtungen sind Schlösser mit Profilzylinder nach DIN18252, Klasse P3, mit mechanischem Bohr- und Ziehschutz wie folgt vorzusehen: mindestens 15.000 Variationsmöglichkeiten mindestens 100.000 Variationsmöglichkeiten Geistige Schalteinrichtungen müssen über mindestens:				
1.000 Einstellmöglichkeiten verfügen.	●			
10.000 Einstellmöglichkeiten verfügen.		●		
100.000 Einstellmöglichkeiten verfügen.			●	
1.000.000 Einstellmöglichkeiten verfügen.				●
Zugänge mit Schalteinrichtungen sind auf Öffnen zu überwachen.	●			
Zwangsläufiges Scharfschalten mit Verschlussüberwachung ist erforderlich.		●	●	●
Es können Melder zur Erfassung von Technik-Meldungen angeschlossen werden. Die Auslösung dieser Melder muss von Überfall-/ Einbruchmeldungen unterschieden werden und darf nicht zu einem Externalarm führen.	●	●	●	●
Deckelkontakte von Extern-Signalgebern und der Schalteinrichtung müssen im scharfgeschalteten Zustand auf unbefugtes Öffnen überwacht werden.	●	●		
Die Deckelkontakte von Extern-Signalgebern, Schalteinrichtungen sowie alle Anlagenteile werden ständig überwacht (Sabotagemeldergruppe).			●	●
Die Zentrale ist im Sicherungsbereich an einer für unberechtigte Personen schwer einsehbaren Stelle zu montieren.	●	●		
Die Zentrale ist im Sicherungsbereich an einer für unberechtigte Personen schwer einsehbaren Stelle zu montieren und muss sich im Überwachungsbereich eines Bewegungsmelders oder im Zentralen-Umschrank befinden.			●	●
Bei Fernalarm über eine bedarfsgesteuerte Verbindung mit einer Übertragungseinrichtung kann auf einen Externalarm verzichtet werden.	●			
Der Fernalarm erfolgt über bedarfsgesteuerte Verbindung mit Übertragungsgerät. Bei erfolgloser Übertragung muss der Externalarm mit akustischem Externsignalgeber innen oder außen erfolgen.		●		
Der Fernalarm erfolgt über bedarfsgesteuerte Verbindung mit Übertragungsgerät. Bei erfolgloser Übertragung sollte der Fernalarm über den Ersatzweg "Funk" erfolgen. Bei Ausfall beider Übertragungswege muss Externalarm erfolgen.			●	●

	DIN VDE 0833-3, Grad 1	DIN VDE 0833-3, Grad 2	DIN VDE 0833-3, Grad 3	DIN VDE 0833-3, Grad 4
Zur Hilfeleistung und zur Entgegennahme von Störungsmeldungen nach DIN VDE 0833-1 wird eine, über ein Übertragungsgerät angeschlossene, ständig besetzte Stelle, d. h. eine externe Sicherheits-Leitstelle empfohlen.	●	●		
Zur Hilfeleistung und zur Entgegennahme von Störungsmeldungen nach DIN VDE 0833-1 wird eine, über ein Übertragungsgerät angeschlossene, ständig besetzte Stelle, d. h. eine externe Sicherheits-Leitstelle und/oder Polizei empfohlen.			●	
Zur Alarmweiterleitung wird ein Anschluss an die Polizei empfohlen.				●
Zur Hilfeleistung und zur Entgegennahme von Störungsmeldungen nach DIN VDE 0833-1 wird eine, über ein Übertragungsgerät angeschlossene, ständig besetzte Stelle, d. h. eine externe Sicherheits-Leitstelle empfohlen.				●
Zusätzlich kann der Betreiber • durch im Haus befindliche Signalgeber auf einen Alarm aufmerksam gemacht werden und/oder • durch Klartextmeldungen auf Handy, Pager usw. bestimmte Personen alarmieren lassen.	●	●		
Der Einsatz von akustischem Externalarm wird nicht empfohlen.	●			
Der alleinige Einsatz von Externalarm zur Alarmierung der Öffentlichkeit ist nicht zulässig.		●	●	●
Begehung/Instandhaltung/Inspektion: EMA müssen nach DIN VDE 0833-3 (VDE 0833-3) instand gehalten werden. Die Instandhaltung muss durch eine Elektrofachkraft erfolgen.	●	●	●	●
• Begehung • Inspektion • Wartung • Instandsetzungsbeginn	1 x jährlich 1 x jährlich 1 x jährlich Keine Anforderung	1 x jährlich 1 x jährlich 1 x jährlich innerhalb 40 h	2x jährlich 2x jährlich 1 x jährlich innerhalb 24 h	4 x jährlich 4 x jährlich 1 x jährlich innerhalb 12 h

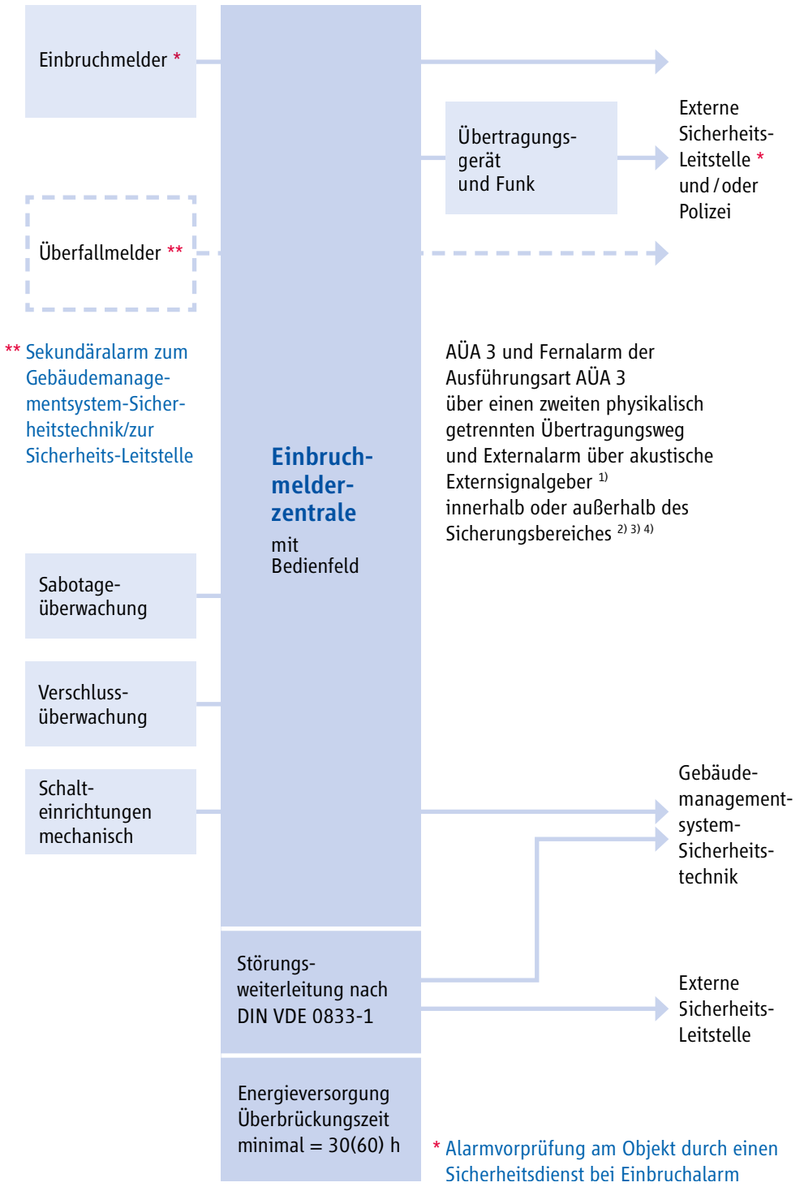
4.1.1.10.1.1 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach der Norm DIN VDE 0833-3, Grad 1**



4.1.1.10.1.2 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach DIN VDE 0833-3, Grad 2**



4.1.1.10.1.3 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach DIN VDE 0833-3, Grad 3**



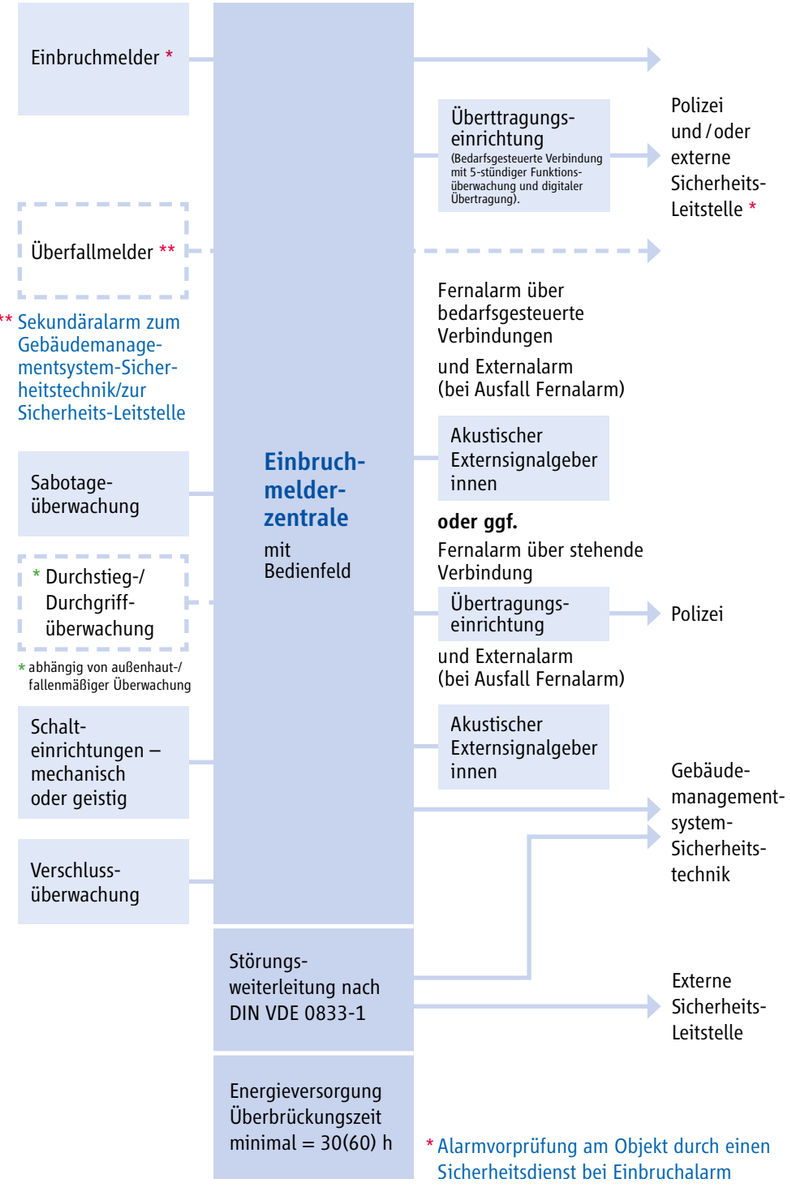
[1] Entweder zwei akustische Externsignalgeber ohne eigene EV (ferngespeiste Signalgeber) oder ein akustischer Externsignalgeber mit eigener EV.

[2] Zusätzliche optische Externsignalgeber dürfen vorgesehen werden.

[3] Überfallalarm darf grundsätzlich nur als Fernalarm ausgegeben werden. Ist auf ausdrücklichen Betreiberwunsch dennoch Extern-/Internalarm vorgesehen, ist der Betreiber vom Errichter über die damit verbundenen Risiken aufzuklären. Das ist zu dokumentieren.

[4] Wenn alle Übertragungswege gestört sind, darf ein sofortiger akustischer Externalarm erfolgen.

4.1.1.10.1.4 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach DIN VDE 0833-3, Grad 4**



4.1.1.11 **Einbruchmeldeanlagen nach BSI (Verschlusssachen)**

Die Einbruchmeldeanlage und die verwendeten Anlagenteile müssen den Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen.

Die Einbruchmeldeanlage hat die Aufgabe, über Melder Gefahren zu erkennen, über eine Zentrale auszuwerten und zu signalisieren bzw. weiterzumelden, z. B. an eine externe Sicherheits-Leitstelle, um von dort eine Alarmvorprüfung am Objekt durch einen Sicherheitsdienst zu veranlassen, bevor die Polizei gerufen wird.

An der Zentrale angeschlossene Melder (z. B. Überfallmelder) sind permanent aktiv oder werden über elektromechanische und geistige Schalteinrichtungen aktiviert. Die Übertragung des Überfall-Sekundäralarms an die externe Sicherheits-Leitstelle ist möglich. Zwangsläufiges Scharfschalten mit Verschlussüberwachung ist erforderlich.

Die Deckelkontakte von Schalteinrichtungen sowie allen Anlagenteilen werden ständig gegen Zugriff überwacht. Magnetkontakte müssen gegen Beeinflussung durch Fremdmagnetfelder geschützt sein, oder auf derartige Einwirkungen überwacht werden. Eine eventuell erforderliche Absicherung gegen Durchdringen ist mit entsprechenden technischen Maßnahmen sicherzustellen.

Die EMA wird über ein Digitales Meldesystem mit Codierung auf eine Leitstelle der Polizei aufgeschaltet. Störungsmeldungen werden an eine ständig besetzte Stelle weitergeleitet.

4.1.1.11.1 **Einbruchmeldeanlagen nach BSI (Verschlusssachen) und nach der Norm DIN VDE 0833-1 und DIN VDE 0833-3, Grad 4**

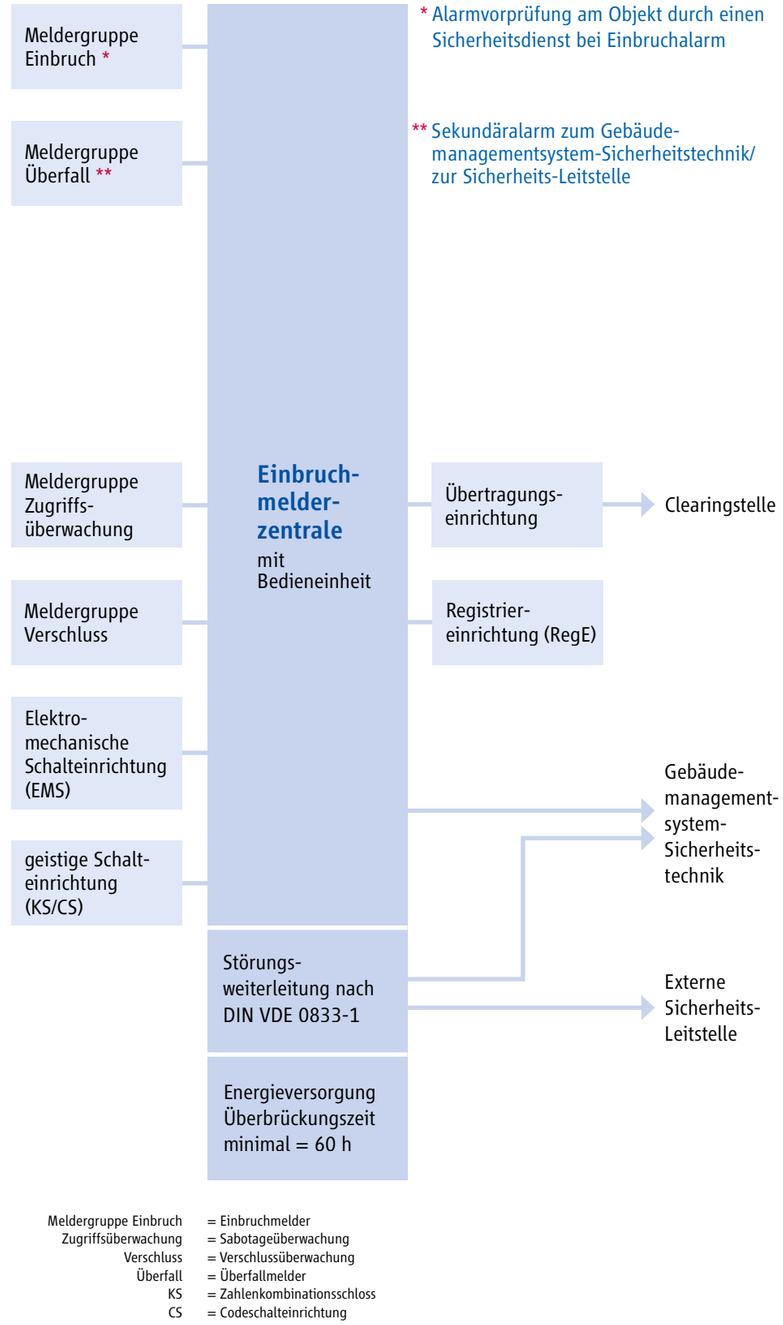
Soll die EMA zusätzlich den Anforderungen der DIN VDE 0833-1 und der DIN VDE 0833-3, Grad 4 genügen, gilt folgendes zusätzlich:

Gemäß VdS 2833 sind ggf. Überspannungs- und Blitzschutzmaßnahmen zu berücksichtigen.

EMA müssen gemäß obenstehender Normen instandgehalten werden. Die Instandhaltung muss durch einen VdS-Errichter erfolgen. Inspektionsrhythmus 4 x jährlich, Wartungsrhythmus 1 x jährlich, Begehung 4 x jährlich.

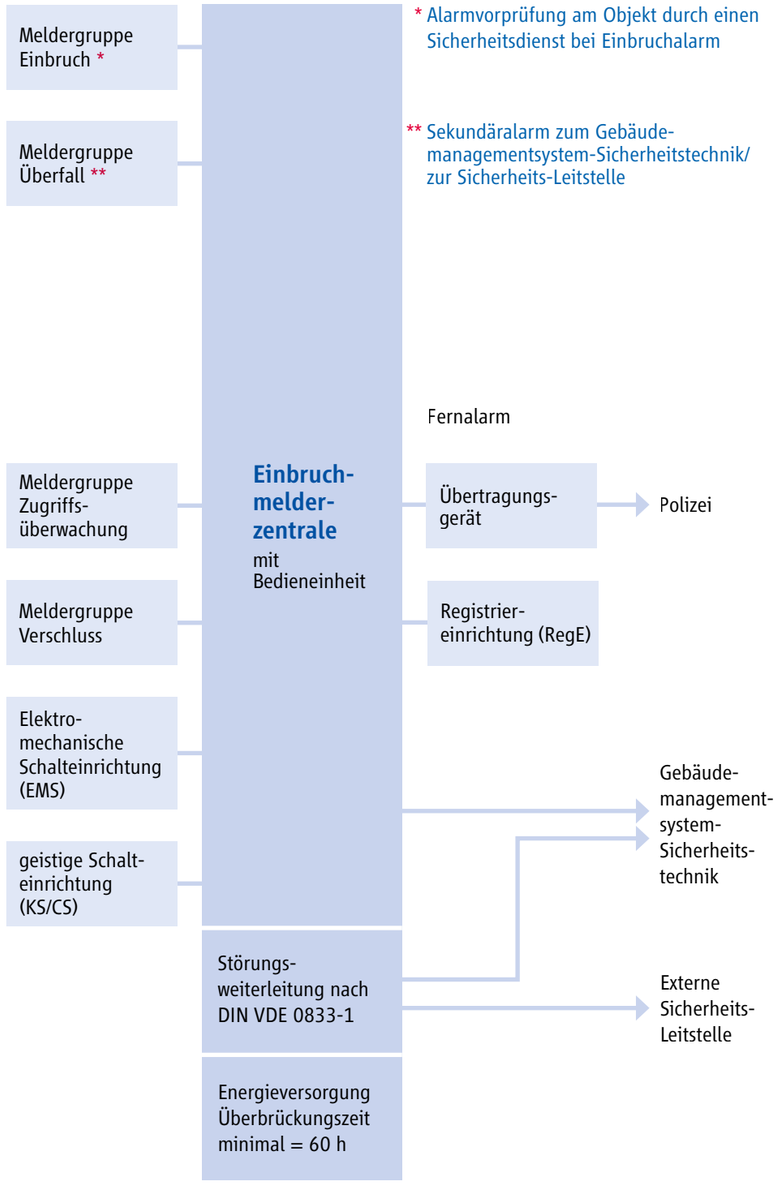
Bei Aufschaltung zur Polizei gilt zusätzlich der „Anhang A" (Aufschaltung zur Polizei).

4.1.1.11.1.1 **Beispielhaftes Konzept für eine Einbruchmeldeanlage (Verschlusssachen) nach BSI 7510**



Meldergruppe Einbruch = Einbruchmelder
Zugriffsüberwachung = Sabotageüberwachung
Verschluss = Verschlussüberwachung
Überfall = Überfallmelder
KS = Zahlenkombinationsschloss
CS = Codeschalteinrichtung

4.1.1.11.1.2 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach BSI (Verschlusssachen) und nach der Norm DIN VDE 0833-1 und DIN VDE 0833-3, Grad 4**



Meldergruppe Einbruch = Einbruchmelder
Zugriffsüberwachung = Sabotageüberwachung
Verschluss = Verschlussüberwachung
Überfall = Überfallmelder
KS = Zahlenkombinationsschloss
CS = Codeschalteinrichtung

4.1.1.12 **Überfallmeldeanlagen nach der Norm DIN VDE 0833-3, Grad 3/Überfallmeldeanlagen UVV Kassen nach DGUV-Vorschrift 25 - nur für Geldinstitute**

- Überfallmeldeanlage (ÜMA) nach Norm DIN VDE 0833-3, Grad 3
- Überfallmeldeanlage DGUV-Vorschrift 25 - nur für Geldinstitute -

Anschaltung der ÜMA-Zentraleinheit an

Gebäudemanagementsystem-Sicherheitstechnik

Externe Sicherheits-Leitstelle

Nachfolgende Übertragungswege sind bei der (IP-)Vernetzung erforderlich:

- ÜMA-Sensorik zur ÜMA-Zentraleinheit
- ÜMA-Zentraleinheit zur Clearingstelle - danach zur Polizei-Leitstelle
- ÜMA-Zentraleinheit zur Gebäudemanagementsystem-Sicherheitstechnik
- ÜMA-Zentraleinheit zur „Externen Sicherheits-Leitstelle“
- Gebäudemanagementsystem-Sicherheitstechnik zur „Externen Sicherheits-Leitstelle“

4.1.1.12.1 **Übersicht beispielhafter Konzepte für Überfallmeldeanlagen (ÜEA) nach nach der Norm DIN VDE 0833-3, Grad 1/DGUV Vorschrift 25 (UVV-Kassen) - nur für Geldinstitute**

	DIN VDE 0833-3, Grad 3	DGUV Vorschrift 25 (UVV-Kassen) - nur für Geldinstitute
Die Überfallmeldeanlage entspricht der Norm DIN VDE 0833-3, Grad 3.	●	
Die Überfallmeldeanlage wird nach der DGUV-Vorschrift 25 (UVV-Kassen) in der jeweils gültigen Fassung konzipiert.		●
Die verwendeten Anlageteile müssen VdS-Klasse B anerkannt sein.	●	
Die DIN VDE 0833-1 und VDE 0833-3 sind zu berücksichtigen.		●
Die Überfallmeldeanlage hat die Aufgabe, über Überfallmelder ausgelöste Meldungen zu erkennen, über eine Zentrale auszuwerten und zu signalisieren bzw. weiterzumelden. Die Übertragung des Überfall-Sekundäralarms an die externe Sicherheits-Leitstelle ist möglich.	●	
Die Überfallmeldeanlage nach DGUV Vorschrift 25 (UVV-Kassen) – nur für Geldinstitute hat die Aufgabe, durch Überfallmelder ausgelöste Meldungen zu erkennen, über eine Zentrale auszuwerten und zu signalisieren bzw. weiterzumelden. Die Übertragung des Überfall-Sekundäralarms an die externe Sicherheits-Leitstelle ist möglich.		●
An die Zentrale angeschlossene Überfallmelder sind permanent aktiv (nicht abschaltbare Melder).	●	●
Jeder Arbeitsplatz mit Bargeldverkehr (auch BBA/AKT, KBA/GAA) muss mit einem Auslöser der Überfallmeldeanlage ausgerüstet sein. Die Abkürzungen sind am Ende der Tabelle in der Legende erklärt.		●
Empfehlung: Zusätzliche Überfallmelder sollten an geeigneten Stellen, z. B. Sozialraum, vorhanden sein.		●
Öffentlich zugängliche Bereiche des Geldinstituts müssen mit einer optischen Raumüberwachung ausgerüstet sein.		●
Bei Geldinstituten oder auf Verlangen der Polizei sollte die Überfallmeldeanlage durch eine optische Raumüberwachung ergänzt werden.	●	
Die Deckelkontakte von allen Anlagenteilen werden ständig überwacht (z. B. Sabotagemeldergruppe bzw. Überfallmeldergruppe).	●	●
Zur Alarmweiterleitung wird ein Anschluss an die Polizei empfohlen.	●	●
Ist ein Anschluss zur Polizei nicht möglich, wird zur Hilfeleistung eine externe Sicherheits-Leitstelle empfohlen.	●	●
Zur Entgegennahme von Störungsmeldungen und ggf. Sabotagemeldungen wird eine über ein Übertragungsgerät angeschlossene, ständig besetzte Stelle z. B. eine externe Sicherheits-Leitstelle empfohlen.	●	●

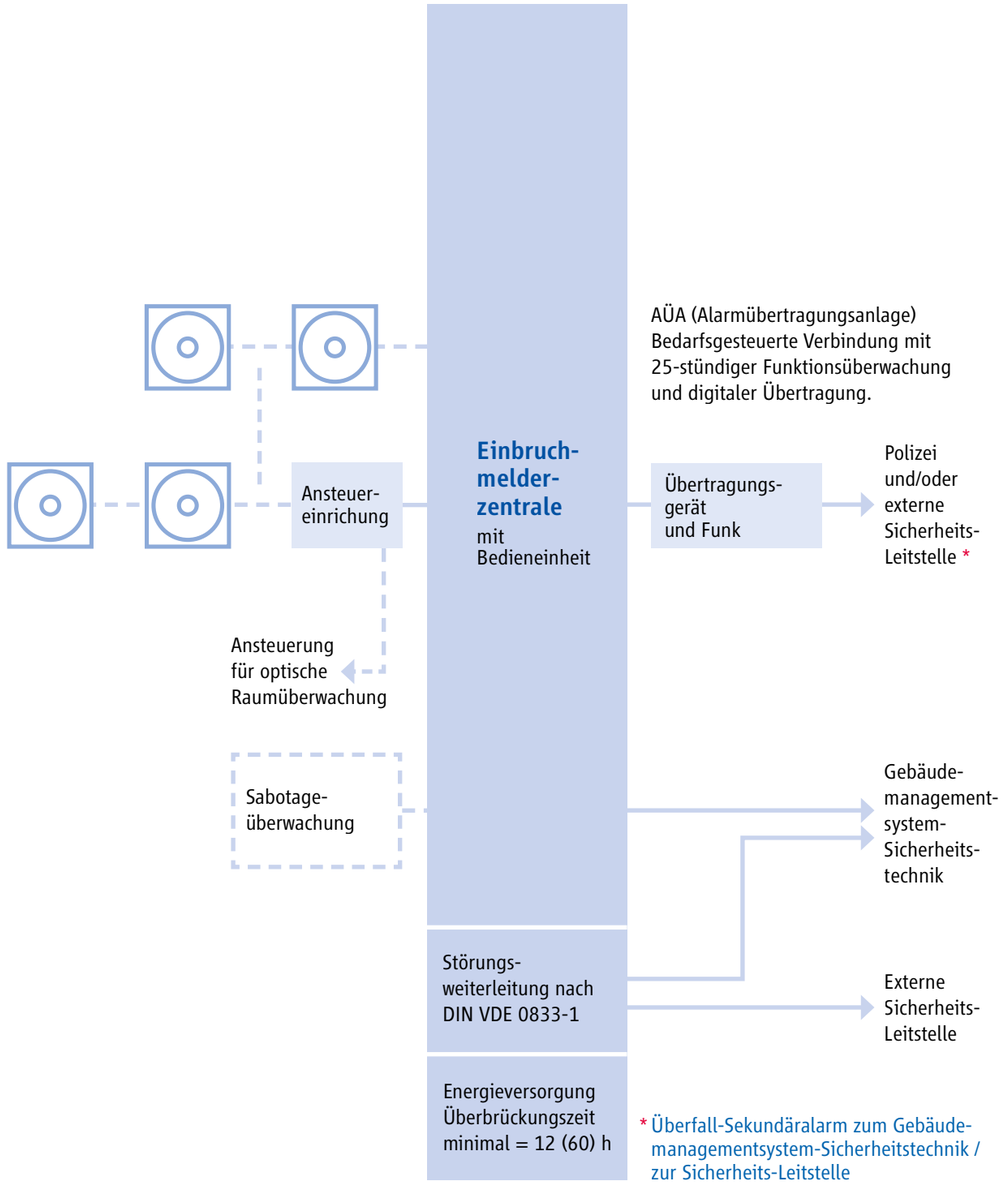
	DIN VDE 0833-3, Grad 3	DGUV Vorschrift 25 (UVV-Kassen) - nur für Geldinstitute
Die Zentrale ist in einem nicht allgemein zugängigen Bereich so zu installieren, dass sie für Nicht-Berechtigte nicht unmittelbar erkennbar ist.	●	●
Der Einsatz von Externsignalgebern zur Alarmierung der anonymen Öffentlichkeit wird nicht empfohlen.	●	●
Bei automatischer Störungsweiterleitung an eine ständig besetzte Stelle, z. B. eine externe Sicherheits-Leitstelle, darf die Überbrückungszeit der Energieversorgung von 60 h auf 12 h reduziert werden.	●	●
Zusätzlich kann der Betreiber • durch im Haus befindliche optische Signalgeber auf einen Alarm aufmerksam gemacht werden und/oder • durch Klartextmeldungen auf Handy, Pager usw. bestimmte Personen alarmieren lassen.	●	●
Instandhaltung: ÜMA müssen gemäß DIN VDE 0833-3, Grad 3 durch einen Facherrichter instandgehalten werden	●	●
• Inspektionsrhythmus: • Wartungsrhythmus:	4 x jährlich 1 x jährlich	1 x jährlich

Beschäftigtenbediente Banknotenautomaten **(BBA)** sind Geldausgabeautomaten, die nicht vom Kunden, sondern von Mitarbeitern des Kreditinstituts bedient werden.

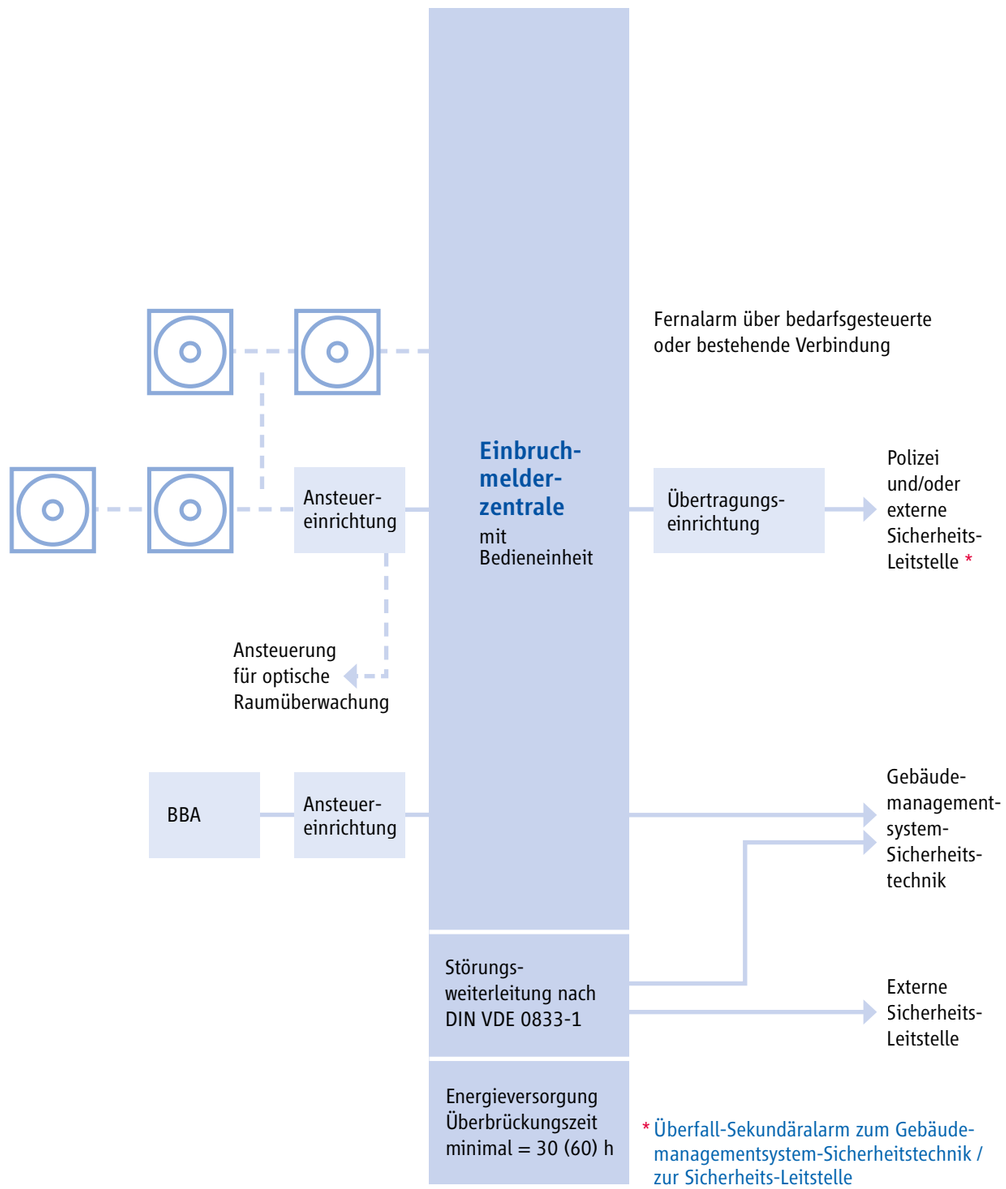
Kundenbedienter Banknotenautomat **(KBA)**, frühere Bezeichnung war Geldausgabeautomat **(GAA)**.

Automatischer Kassentresor **(AKT)**

4.1.1.12.2 **Beispielhaftes Konzept für eine Überfallmeldeanlage nach der Norm DIN VDE 0833-3, Grad 3**



4.1.1.12.3 **Beispielhaftes Konzept für eine Überfallmeldeanlage nach DGUV Vorschrift 25 (UVV Kassen) – nur für Geldinstitute**



4.1.1.13 **Einbruchmeldeanlagen (EMA) nach der VdS, Klasse A-B-C-SG 3 und 4; SG 5 und 6**

- Einbruchmeldeanlage (EMA) nach VdS, Klasse A
- Einbruchmeldeanlage (EMA) nach VdS, Klasse B
- Einbruchmeldeanlage (EMA) nach VdS, Klasse C – SG 3 und - 4
- Einbruchmeldeanlage (EMA) nach VdS, Klasse C – SG 5 (z. B. Geldinstitute) und – SG 6 (z. B. Juweliere)
- Einbruchmeldeanlage (EMA) nach BSI (Verschlusssachen) nach BSI 7510

Anschaltung der EMA-Zentraleinheit an

Gebäudemanagementsystem-Sicherheitstechnik

Externe Sicherheits-Leitstelle

Nachfolgende Übertragungswege sind bei der (IP-) Vernetzung erforderlich:

- EMA-Sensorik zur EMA-Zentraleinheit
- EMA-Zentraleinheit zum Gebäudemanagementsystem-Sicherheitstechnik
- EMA-Zentraleinheit zur „Externen Sicherheits-Leitstelle“
- Gebäudemanagementsystem-Sicherheitstechnik zur „Externen Sicherheits-Leitstelle“

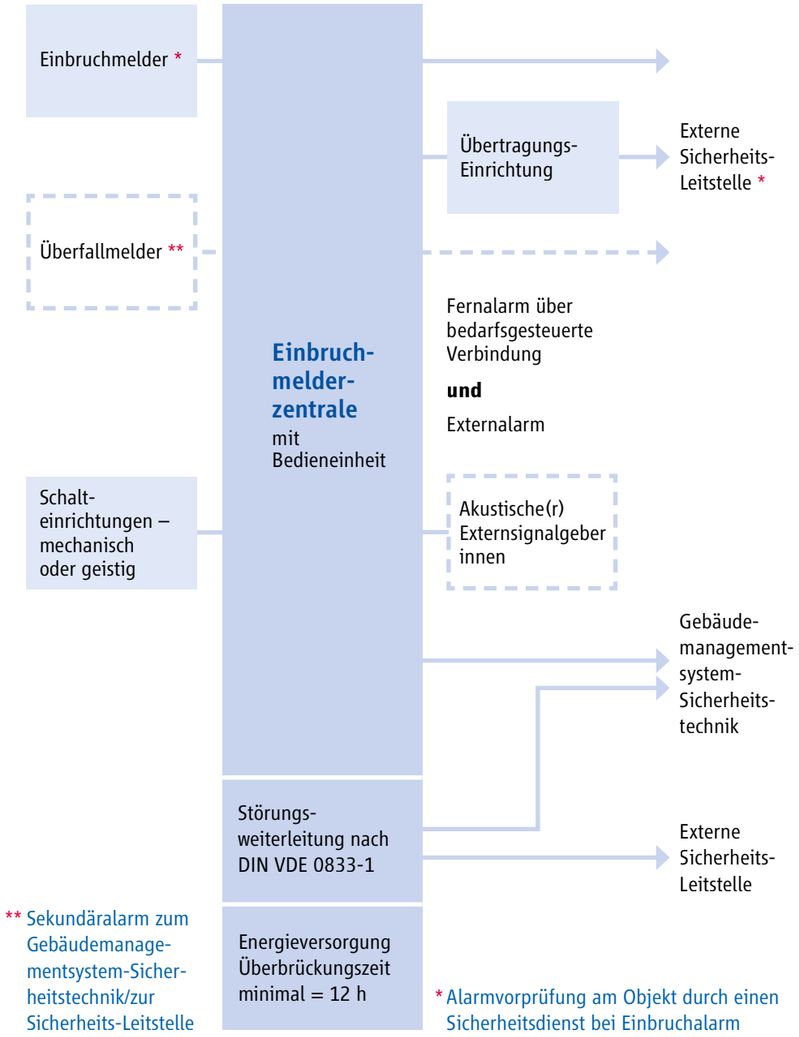
4.1.1.13.1 **Übersicht der beispielhaften Konzepte für Einbruchmeldeanlagen (EMA) nach der VdS-Klasse A-B-C-SG 3 und 4 / SG 5 und 6**

	VdS – Klasse A	VdS – Klasse B	VdS – Klasse C SG 3+4	VdS – Klasse C SG 5+6
Die Einbruchmeldeanlage entspricht den Richtlinien von VdS Schadenverhütung, VdS Klasse A, SH 1 bis SH 3.	●			
Die Einbruchmeldeanlage entspricht den Richtlinien der VdS Schadenverhütung, VdS Klasse B, SH 1 bis SH 3 und SG 1 und SG 2.		●		
Die Einbruchmeldeanlage entspricht den Richtlinien der VdS Schadenverhütung VdS Klasse C, SG 3 und SG 4.			●	
Die Einbruchmeldeanlage entspricht den Richtlinien der VdS Schadenverhütung VdS Klasse C, SG 5 und SG 6.				●
Bei der Aufschaltung zur Polizei gelten zusätzlich die Aufschaltebedingungen der Polizei.			●	●
Der „Bundeseinheitliche Pflichtenkatalog“ für Errichterfirmen von Überfall- und Einbruchmeldeanlagen (LKA-Richtlinien) in der jeweiligen Fassung ist zu beachten	●	●	●	●
Die verwendeten Anlagenteile müssen mindestens VdS Klasse A anerkannt sein.	●			
Die verwendeten Anlagenteile müssen mindestens VdS Klasse B anerkannt sein.		●		
Die verwendeten Anlagenteile müssen mindestens VdS Klasse C anerkannt sein.			●	●
Die Einbruchmeldeanlage hat die Aufgabe, über Melder Gefahren zu erkennen, über eine Zentrale auszuwerten und zu signalisieren bzw. weiterzumelden, z. B. an eine externe Sicherheits-Leitstelle, um von dort eine Alarmvorprüfung am Objekt durch einen Sicherheitsdienst zu veranlassen, bevor die Polizei gerufen wird.	●	●	●	●
An der Zentrale angeschlossene Melder (z. B. Überfallmelder) sind permanent aktiv oder werden über mechanische oder geistige Schalteinrichtungen aktiviert. Die Übertragung des Überfall-Sekundäralarms an die externe Sicherheits-Leitstelle ist möglich.	●	●	●	●
Zwangsläufiges Scharfschalten mit Verschlussüberwachung ist erforderlich.	●	●	●	●
Es können Melder zur Erfassung von Technik-Meldungen angeschlossen werden. Die Auslösung dieser Melder muss von Überfall-/ Einbruchmeldungen unterschieden werden und darf nicht zu einem Externalarm führen.	●	●	●	●

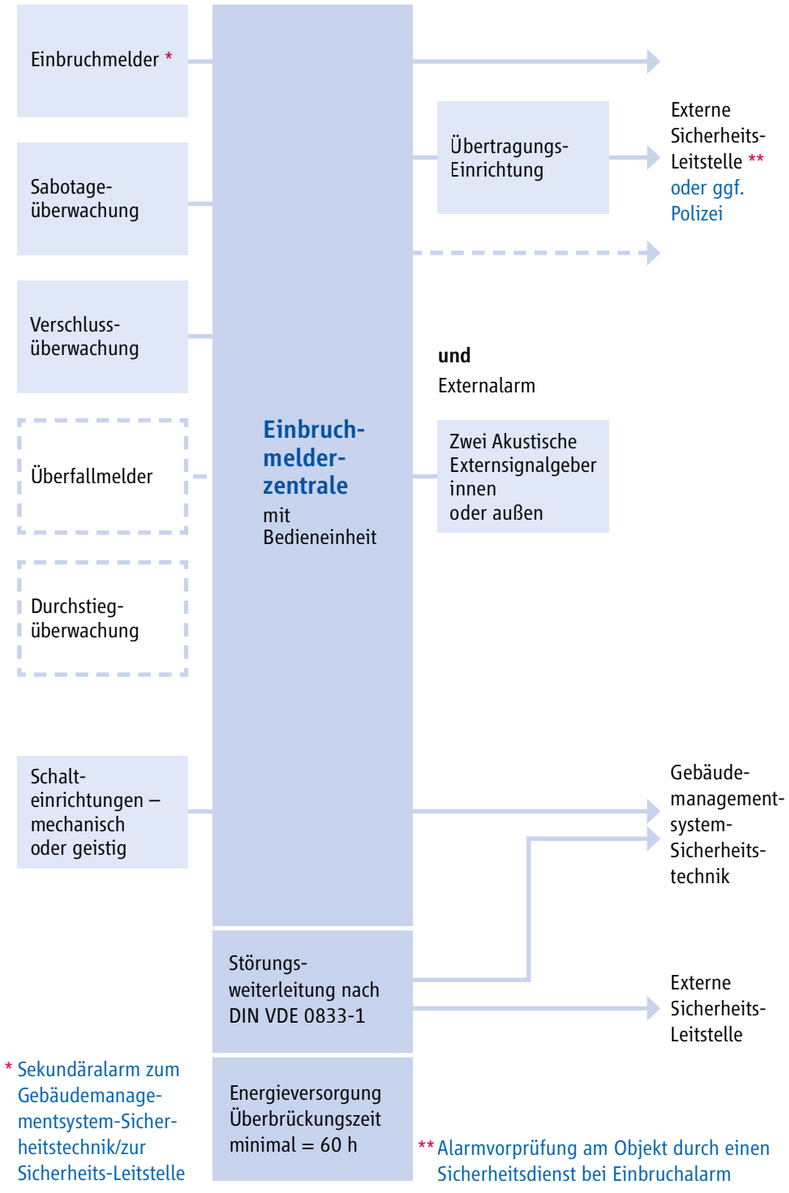
	VdS – Klasse A	VdS – Klasse B	VdS – Klasse C SG 3+4	VdS – Klasse C SG 5+6
Die Deckelkontakte der Anlagenteile werden ständig überwacht (Sabotagemeldergruppe).		●	●	●
Die Zentrale ist im Sicherungsbereich an einer für unberechtigte Personen schwer einsehbaren Stelle zu montieren.	●			
Die Zentrale ist im Sicherungsbereich an einer für unberechtigte Personen schwer einsehbaren Stelle zu montieren und muss sich im Überwachungsbereich eines Bewegungsmelders oder im Zentralenumschrank befinden.		●	●	●
Der Fernalarm erfolgt über eine bedarfsgesteuerte Verbindung mit 25-sekündiger Funktionsüberwachung und Externalarm mit einem akustischem Signalgeber innerhalb des Sicherungsbereiches.	●			
• über eine bedarfsgesteuerte Verbindung mit 20-sekündiger Funktionsüberwachung und Externalarm mit einem akustischen Signalgeber innerhalb des Sicherungsbereiches und bei IP-Übertragung über eine bedarfsgesteuerte Verbindung mit 25-Std. Funktionsüberwachung			●	●
oder				
• über eine bedarfsgesteuerte Verbindung mit 25-sekündiger Funktionsüberwachung und Externalarm mit zwei akustischen Signalgebern innerhalb oder außerhalb des Sicherungsbereiches		●		
oder				
• über eine bedarfsgesteuerte Verbindung mit 25-Std. Funktionsüberwachung und Ersatzweg über bedarfsgesteuerte Verbindung mit 25-Std. Funktionsüberwachung, ohne Externalarm.	●	●		
oder				
• über eine bedarfsgesteuerte Verbindung mit 5-stündiger Funktionsüberwachung und Ersatzweg über bedarfsgesteuerte Verbindung mit 25-Std. Funktionsüberwachung und Externalarm mit zwei akustischen Signalgebern innerhalb oder außerhalb des Sicherungsbereiches.		●	●	●
Zur direkten Hilfeleistung sollte die Alarmübertragung zur Polizei erfolgen.			●	
Zur direkten Hilfeleistung sollte die Alarmübertragung zur Polizei erfolgen. Zusätzlich wird die Bildübertragung zur Polizei bzw. zu einer externen Sicherheits-Leitstelle empfohlen.				●
Für die nach DIN VDE 0833-1 geforderte automatische Störungsweiterleitung an eine ständig besetzte Stelle wird die Aufschaltung auf eine externe Sicherheits-Leitstelle empfohlen.			●	●

	VdS – Klasse A	VdS – Klasse B	VdS – Klasse C SG 3+4	VdS – Klasse C SG 5+6
Akustische Signalgeber außerhalb des Sicherungsbereiches sollten nur in Ausnahmefällen, z. B. abgelegenes Objekt, Defizite in der Übertragungssicherheit, eingesetzt werden.		●		
Zur Entgegennahme von Fernalarmen und für die nach VDE 0833-1 geforderte automatische Störungsweiterleitung an eine ständig besetzte Stelle wird die Nutzung einer externen Sicherheits-Leitstelle empfohlen.	●	●	●	●
Zusätzlich kann der Betreiber • durch im Haus befindliche Signalgeber auf einen Alarm aufmerksam gemacht werden	●	●	●	●
und/oder				
• durch Klartextmeldungen auf Handy, Pager usw. bestimmte Personen alarmieren lassen.	●	●	●	●
Gemäß DIN VDE 0845-1 bzw. VdS 2833 sind ggf. Überspannungs- und Blitzschutzmaßnahmen zu berücksichtigen.	●	●	●	●
Instandhaltung: Einbruchmeldeanlagen müssen gemäß VdS-Richtlinie 2311 instandgehalten werden. Die Instandhaltung muss durch einen VdS-Errichter erfolgen.				
• Inspektionsrhythmus: • Wartungszyklus:	1x jährlich 1x jährlich	2x jährlich 1x jährlich	4x jährlich 1x jährlich	4x jährlich 1x jährlich

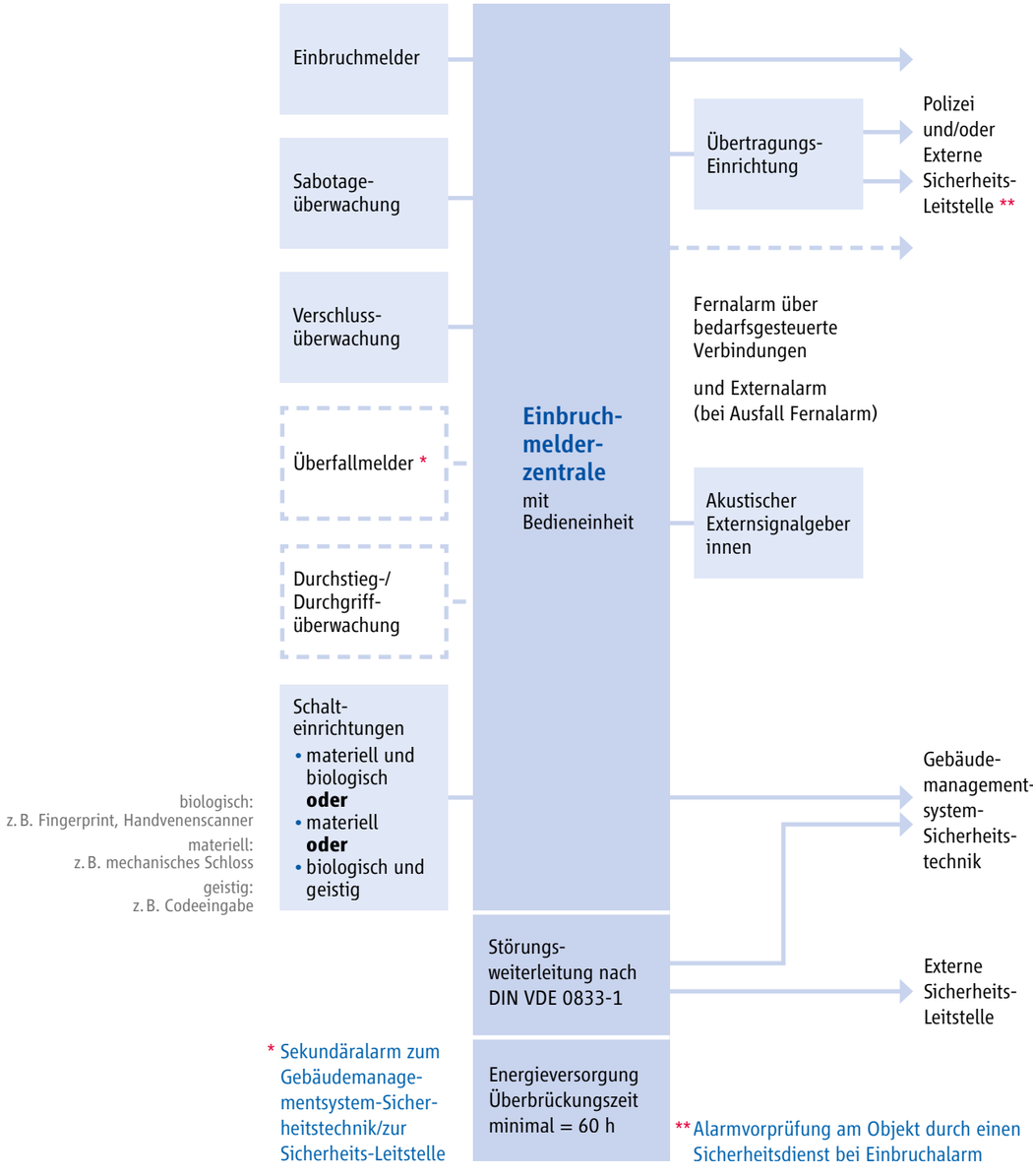
4.1.1.13.1.1 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse A**



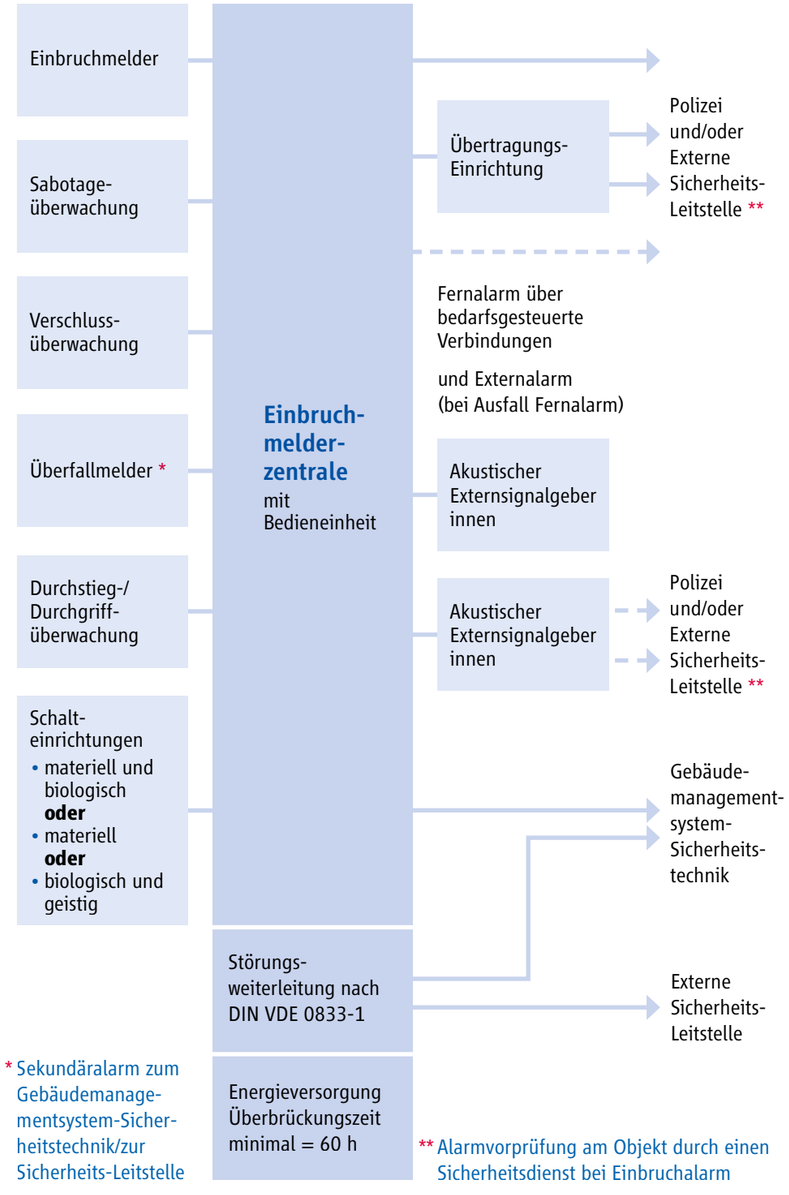
4.1.1.13.1.2 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse B**



4.1.1.13.1.3 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse C – SG 3 und - 4**



4.1.1.13.1.4 **Beispielhaftes Konzept für eine Einbruchmeldeanlage nach VdS, Klasse C – SG 5 (z.B. Geldinstitute) und – SG 6 (z.B. Juweliere)**



4.1.1.14 **Beispielhaftes Planungsschema für Überfall- und Einbruchmeldeanlagen (ÜMA-EMA)**

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Aufgabenstellung	Individuell durch den Auftraggeber, z. B. durch den Fachplaner, die Bauabteilung oder den Betreiber
Beispielhafte Schutzziele des Auftraggebers	Schutz u. a. vor • Überfall • Einbruch • Vandalismus • Sabotage • Spionage
Erfassungsebene – Auswahl der Sensorik (Melder) (abhängig von den Schutzzielen)	Mögliche in Betracht kommende Melder, u. a. • Manuelle Melder • Bewegungsmelder • Körperschall- und Glasbruchmelder • Magnetkontakte • Körperschall- und Glasbruchmelder • Lichtschranken • Flächenüberwachungssysteme und Fadenzugkontakte • Komponenten der Störmeldeüberwachung • Funknotruf-Einrichtungen
Übertragungsweg von der Erfassungsebene zur Zentralenebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze - des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Zentralenebene	Auswahl der passenden Überfall- und Einbruchmelderzentrale mit den dazu passenden Zentralenkomponenten, wie z. B. der • Energieversorgung • Batterien • Anzeigetableaus • Internen und externen Signalgeber • Scharfschalteinrichtungen • Übertragungssysteme
Schnittstellen zu anderen Gefahrenmeldeanlagen und zum Gebäudemanagementsystem-Sicherheitstechnik	Möglich sind Schnittstellen u.a. zu/zum • Videoüberwachungsanlagen • Zutrittskontrollanlagen • Brandmeldeanlagen • Sprachalarmanlagen (SAA) • Gebäudemanagementsystem-Sicherheitstechnik

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Übertragungsweg von der Zentralenebene zum Gebäudemanagementsystem	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Gebäudemanagementsystem-Sicherheitstechnik	Auslegung entsprechend der vorgenannten definierten Anforderungen. Klärung des Alarmpfades bei Systemausfall oder Überlastung des Gebäudemanagementsystems.
Übertragungsweg vom Gebäudemanagementsystem zur Sicherheitsleitstelle	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Sicherheitsleitstelle	Auslegung entsprechend der vorgenannten definierten Anforderungen

4.1.1.15 **Beispielhafte Funktionen und Anschaltungen einer Überfall- und Einbruchmeldeanlage (ÜMA-EMA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle**

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an die ÜMA-EMA-Zentrale	an die Polizei	an GMS	a.d. Sicherheits-Leitstelle
1.	**Anschaltung, u.a. von**							
1.1	1 ..... n Scharfschalteinrichtungen	●	●		●		●	Scharfschalte-Überwachung
1.2	**Überfall-Alarme**							
1.2.1	1 ..... n Überfall-Meldergruppen mit manuellen Meldern	●	●		●	●	●	als Sekundäralarm zur Alarmvorprüfung
1.2.2	1 .... n Übertragungseinrichtungen zur Polizei				●	●	●	
1.3	**Meldergruppen zur Alarmierung**							
1.3.1	1 ..... n Meldergruppen Funknotruf durch Personen im Bereich des Unternehmensgeländes	●	●		●		●	als Alarm zur Alarmvorprüfung
1.3.2	1 .....n Meldergruppen zur Verschlussüberwachung von Fenster und Türen	●	●		●		●	
1.3.3	1 ..... n Meldergruppen zur Außenhautüberwachung	●	●		●		●	
1.3.4	1 ..... n Meldergruppen für Durchstieg-/Durchgriff und Öffnungsmeldungen der Fenster und Türen	●	●		●		●	
1.3.5	1 ..... n Meldergruppen aus fallenmäßiger Überwachung	●	●		●		●	
1.3.6	1 ..... n Meldergruppen zur Flächenüberwachung von Außenwänden, Fußböden und Türen	●	●		●		●	
1.3.7	1 ..... n Meldergruppen zur Fallenmäßigen/Schwerpunktmäßigen Überwachung	●	●		●		●	
1.3.8	1 ..... n Meldergruppen Wegnahmesicherung Geldautomaten	●	●		●		●	
1.3.9	1 ..... n Meldergruppen zur Störmeldeüberwachung		●		●		●	●
1.4	**Peripherie-Komponenten**							
1.4.1	1 .... n Abgesetzte Bedientableaus				●			
1.4.2	1 .... n interne Signalgeber (optisch – akustisch)				●			
1.4.3	1 .... n externe Signalgeber (optisch – akustisch)				●			
1.4.4	1 .... n Alarmierung an eine oder mehrere interne oder externe hilfeleistende Stellen		●		●		●	als Sekundäralarm zur Alarmvorprüfung
1.5	**Fernservice-/Remote-Service-Anschluss**			●	●		●	
2.	**Funktionen von abgesetzten Bedientableaus, u.a.**				●		●	
2.1	Entgegennahme und Bestätigung von Meldungen				●		●	
2.2	Abfragen von Systemzuständen (Anlagenspezifisch)				●		●	
2.3	Einleiten von Steuerungen (Anlagenspezifisch)				●		●	
2.4	Meldergruppen – Abschaltungen (Anlagenspezifisch)				●		●	
3.	**Überwachungsfunktionen, u.a.**		●		●		●	
3.1	Batterieüberwachung		●		●		●	
3.2	Ringleitungsüberwachung		●		●		●	
3.3	Meldergruppenüberwachung		●		●		●	
3.4	Einzelmelderüberwachung		●		●		●	
3.5	Prozessorüberwachung		●		●		●	
3.6	Speicherüberwachung		●		●		●	
3.7	Scharf-/Unscharfüberwachung		●		●		●	
3.8	Sabotageüberwachung		●		●		●	
3.9	Kurzschluss-/Drahtbruchüberwachung		●		●		●	

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an die ÜMA-EMA-Zentrale	an die Polizei	an GMS	a.d. Sicherheits-Leitstelle
4.	**Anschaltung von Schnittstellen zum/zur/zu, u. a. an**							
4.1	weiteren vernetzten Überfall-/Einbruchmeldeanlagen				●		●	
4.2	Videoüberwachungsanlagen				●		●	
4.3	Zutrittskontrollanlagen				●		●	
4.4	Steuereinrichtungen für Parkplatz-/Tiefgaragen-Zufahrten				●		●	
4.5	elektroakustischen Alarmierungseinrichtungen, z. B. Sprachalarmanlagen				●		●	
4.6	Pager/Handy/Personensuchanlagen				●		●	
4.7	übergeordneten Gebäudemanagementsystemen				●		●	●
4.8	Ersatzweg zu einer redundanten Leitstelle				●		●	●
5.	**Service- und Instandhaltungsintervalle nach DIN VDE 0833**							
5.1	**Grad 1**							
5.1.1	Inspektion/Jahr - 1x				●		●	
5.1.2	Wartung/Jahr - 1x				●		●	
5.1.3	Instandsetzungsbeginn - keine Anordnung				●		●	
5.2	**Grad 2**							
5.2.1	Inspektion/Jahr - 1x				●		●	
5.2.2	Wartung/Jahr - 1x				●		●	
5.2.3	Instandsetzungsbeginn - innerhalb 48 h				●		●	
5.3	**Grad 3**							
5.3.1	Inspektion/Jahr - 1x				●		●	
5.3.2	Wartung/Jahr - 1x				●		●	
5.3.3	Instandsetzungsbeginn - innerhalb 24 h				●		●	
5.4	**Grad 4**							
5.4.1	Inspektion/Jahr - 1x				●		●	
5.4.2	Wartung/Jahr - 1x				●		●	
5.4.3	Instandsetzungsbeginn - innerhalb von 12 h				●		●	

4.1.2 Zutrittskontrollanlagen

4.1.2.1 Funktionale Beschreibung

Zutrittskontrollanlagen schützen Waren, Werte, Daten und wertvolle Arbeitsausstattung. Sie erschweren und verhindern Diebstahl, Sabotage sowie ungewünschten Wissenstransfer. Zutrittskontrollanlagen verhindern das unbefugte Betreten von Räumen, Gebäuden und Arealen, schließen also Nichtberechtigte aus und schränken Berechtigte so wenig wie möglich in ihrer Bewegungsfreiheit ein. Zutrittskontrollanlagen erhöhen die Arbeits-, Betriebs- und Prozesssicherheit. Sie steuern den Zutritt über ein vom Betreiber festgelegtes Regelwerk, damit nur berechtigte Personen Zutritt zu den für sie freigegebenen Bereichen und in den für sie festgelegten Zeitenräumen in Gebäuden oder geschützten Arealen erhalten. Zutrittskontrollanlagen vervollständigen Einbruchmeldesysteme in ihrer Funktionsweise optimal, da sie während des laufenden Geschäftsbetriebes eine differenzierte Tagüberwachung gewährleisten.

4.1.2.2 Definition Zutrittskontrollanlage

Eine Zutrittskontrollanlage umfasst sowohl alle baulichen und organisatorischen Gegebenheiten als auch die apparativen Teile, die für die Steuerung des Zutritts erforderlich sind einschließlich der für den Betrieb der Zutrittskontrollanlage notwendigen Software.

4.1.2.3 Aufbau einer Zutrittskontrollanlage

Zutrittskontrollanlagen für Sicherungsanwendungen sind häufig dezentral gesteuert und aufgebaut. Hierbei kann schematisch von einem 3-Ebenen-Konzept ausgegangen werden, in dem übergeordnete Zutrittskontrollzentrale, Zutrittskontrollzentralen und die Erfassungsebene mit den weiteren elektronischen und elektromechanischen Komponenten zusammenwirken, die an den Zutrittspunkten angesteuert oder deren Signale aufgenommen werden. Diese Ebenen sollten hinsichtlich der geforderten Sicherheit aufeinander abgestimmt sein.

In der übergeordneten Zutrittskontrollzentrale (Verwaltungsebene) werden Stammdaten angelegt, Zutrittsberechtigungen vergeben, Bewegungsdaten ausgewertet, Alarme verarbeitet, die Zutrittskontrollzentralen mit System- und Zutrittsberechtigungsdaten versorgt und über Schnittstellen der Datenaustausch mit Gefahrenmanagementsystemen und weiteren Anlagen realisiert. Die dezentral verteilten und in gesicherten Bereichen installierten Zutrittskontrollzentralen (Kontroll- und Steuerungsebene) stellen die Entscheidungsintelligenz für die angeschlossenen Zutrittspunkte dar. In der Zutrittskontrollzentrale erfolgt die Prüfung auf Berechtigung, die Steuerung und Überwachung der Zutrittsleser, der Kontakte und Zutrittskontrollstellglieder (Überwachung von Türen), die Speicherung aller Ereignisdaten sowie die Strom- und Notstromversorgung aller angeschlossenen Komponenten. Die Zutrittsleser an den Zutrittspunkten (Eingabeeinheit) bilden die Erfassungsebene. Hier werden die auf den Identifikationsmerkmalsträgern (z. B. Ausweis) hinterlegten Informationen (Identifikations- oder Erkennungsmerkmal) erfasst, an die Zutrittskontrollzentrale weitergeleitet und das Ergebnis einer Buchung angezeigt. Die Eingabeeinheit befindet sich im ungesicherten Bereich an der Grenze zwischen zwei Raumzonen mit unterschiedlichen Zutrittsberechtigungen und sollte über Sabotagekontakte verfügen. Zutrittsleser können unterschiedlich ausgeführt sein, so können neben einem Ausweismedium auch PIN-Code und biometrische Merkmale zur weiteren Bearbeitung erfasst werden.

Je nach Sicherheitsanforderung wird am Zutrittspunkt eine Verschlüsselung der Informationsübertragung zwischen Eingabeeinheit und Identifikationsmerkmalsträger mit AES oder vergleichbar hochwertigen Verfahren gefordert. Es kann die Prüfung von 2 Merkmalen erforderlich sein (z. B. Ausweismedium und PIN, Ausweismedium und biometrisches Merkmal oder PIN und biometrisches Merkmal).

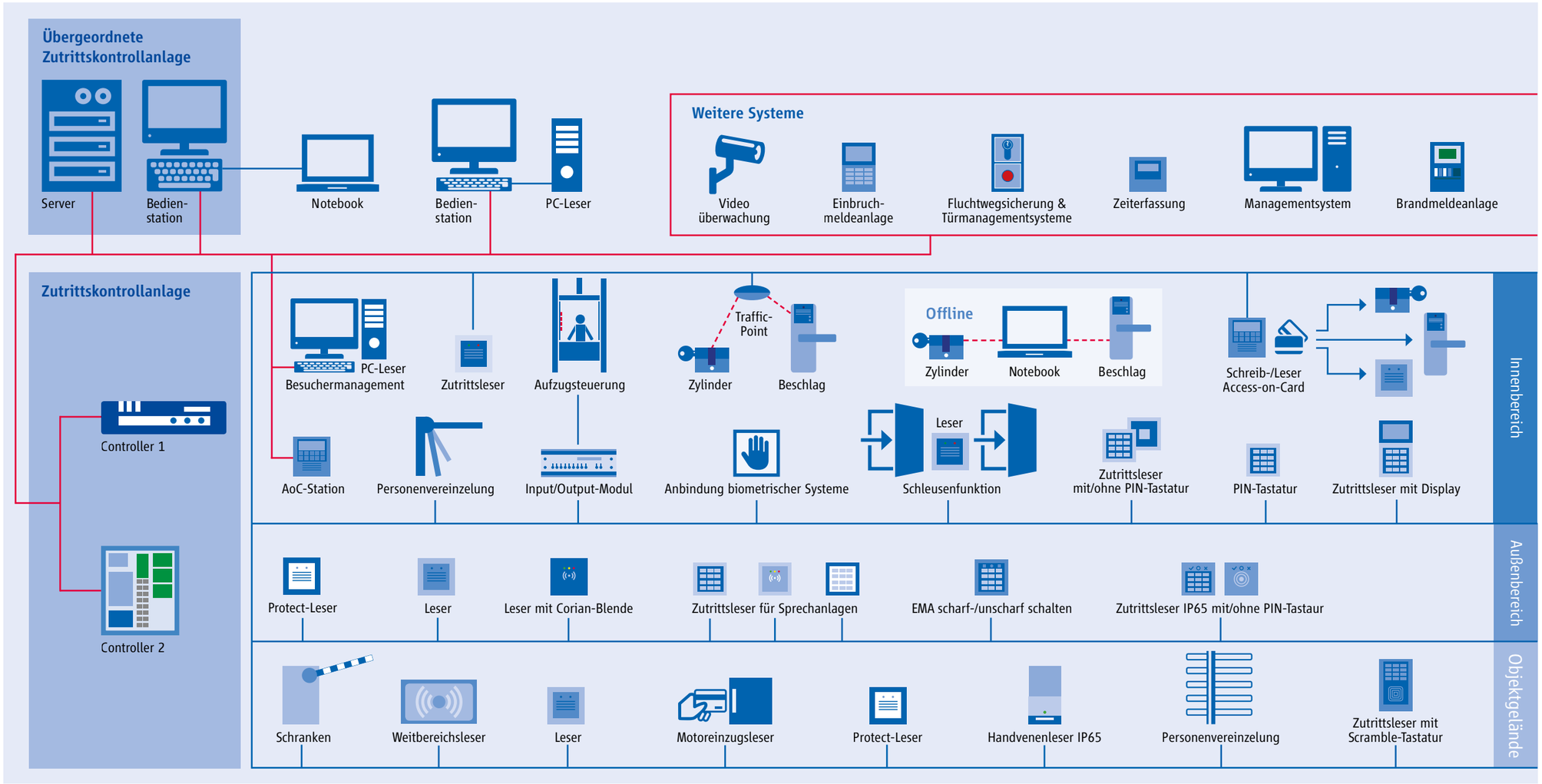
In Zutrittskontrollanlagen können Zutrittspunkte mit unterschiedlichen Sicherheitsanforderungen integriert werden. Eine Sicherheitseinstufung ermittelt für jeden Zutrittspunkt ein entsprechendes Schutzniveau. Die Systemleistungsmerkmale werden entsprechend der Schutzgrade ausgerichtet.

Bei der Planung und Realisierung von elektronischen Zutrittsanlagen werden häufig nicht alle vorhandenen Türen in die Planung einbezogen und mit elektronischen Komponenten der Berechtigungsprüfung und Überwachung des Türstatus ausgestattet. Gründe hierfür sind z. B., dass der finanzielle Aufwand für die Ausstattung aller Türen oft nicht im Verhältnis zum erreichten Nutzen steht, dass aufgrund der Gebäudestruktur nicht jede Tür erreicht werden kann, dass die Installation gerade im Bereich der Nachrüstung sehr aufwändig und kostenintensiv ist und dass Türen wie z. B. Brandschutztüren baulich zum Teil nicht verändert werden dürfen. Dies hat zur Konsequenz, dass für die Durchsetzung von verschiedenen Zutrittsberechtigungen häufig auch zwei Medien – das Ausweismedium und der Schlüssel – erforderlich sind. Ein Lösungsansatz, um die Schlüsselverwaltung zu optimieren und Änderungen von Zutrittsberechtigungen dabei schnellstmöglich umzusetzen, ist die Verwendung von Offline-Komponenten (z. B. elektronische Türbeschläge, Offline-Wandleser und elektronische Schließzylinder), die sich in eine Zutrittsanlage integrieren lassen. Somit können viel begangene Türen mit geringerem Sicherheitsanspruch ohne mechanischen Schlüssel unter Verwendung des vorhandenen Ausweismediums in ein durchgängiges Berechtigungskonzept integriert werden. Auf dem Markt werden heute unterschiedliche Offline-Komponenten für den Einsatz angeboten. Grundsätzlich gilt, dass keine der auszustattenden Türen eine kabelseitige Anbindung benötigt und die Komponenten mit Ausweismedien bedient werden können.

Der elektronische Türbeschlag und der elektronische Schließzylinder arbeiten mit integrierten Batterien, deren Lebenszyklus im Durchschnitt mit 30.000 - 50.000 Buchungen je nach Anbieter und Leseverfahren angegeben wird. Die Komponenten verfügen über einen Buchungsspeicher, der bei Bedarf ausgelesen werden kann. Eine Dauertüröffnung sollte durch spezielle Berechtigungen möglich sein. Eine Öffnung von innen ist bei jeweils einseitiger elektronischer Buchung immer möglich. Bei der Montage erfolgt keine Beschädigung/Änderung des Türblattes, demzufolge ist je nach Hersteller auch der Einsatz an Brand- und Rauchschutztüren sowie an Türen in Fluchtwegen möglich. Die einzusetzenden Komponenten sollten bei entsprechender Anforderung für den Einsatz an Brand- und Rauchschutztüren nach DIN/EN 18273 sowie für den Einsatz an Fluchttüren nach DIN EN 179/DIN EN 1125 zertifiziert sein. Die Auswahl der jeweils einzusetzenden Komponente hängt von der gewünschten Funktion und den Umgebungsbedingungen ab.

In Objekten mit definierten Sicherheitsanforderungen werden oftmals verschiedene Sicherheitssysteme installiert und bauliche Maßnahmen im Rahmen des Brandschutzes umgesetzt. Sicherheitsanlagen beeinflussen sich gegenseitig und es können durch Integration und Verknüpfung Synergien durch die Wechselwirkungen erzielt werden. Anlagen, die Schnittpunkte mit einem Zutrittssystem haben, sind Einbruchmeldeanlagen (Scharfschaltung durch Ausweismedium der Zutrittskontrollanlage), Brandmeldeanlagen (Türsteuerung im Brandfall), Gefahrenmanagementsysteme (einheitliche Alarmbearbeitung für alle Subsysteme) sowie Flucht- und Rettungswegsysteme (Zutrittsprüfung auch bei Fluchttüren für den Normalbetrieb möglich).

4.1.2.3.1 **Beispielhafte Prinzipgrafik für Zutrittskontrollanlagen**



LAN (Local Area Network)
RS 485 max. 1.200 Meter (serielle Kommunikation)

Funk

4.1.2.4 Identifikationsmerkmalsträger

Identifikationsmerkmalsträger sind definitionsgemäß physische Objekte (z. B. Ausweiskarten, Schlüsselanhänger o. ä.), die die Identifikationsmerkmale enthalten, ggf. können auch Personen Identifikationsmerkmalträger sein. Ein Identifikationsmerkmal ist eine mit technischen Mitteln auswertbare Information (Codierung), persönliche Identifikationsnummer (PIN) oder personenspezifisches Merkmal/Eigenschaft (biometrisches Merkmal), die eine eindeutige Identifizierung eines Identifikationsmerkmalträgers erlaubt.

Von entscheidender Bedeutung für die Sicherheit von mediengebundenen Systemen ist die Übertragung der Ausweisdaten vom Ausweismedium über die Luftschnittstelle zum Terminal oder Ausweisleser. Für viele bisher häufig in Zutrittskontrollanlagen eingesetzten passiv berührungslosen Leseverfahren erfolgte eine Kompromittierung der Sicherheitsfunktionen. Durch Veröffentlichung von Berichtsergebnissen in diversen Medien und bei Vorhandensein spezieller Ausstattung besteht die Möglichkeit, dass Unbefugte Daten von einem Ausweismedium auf ein anderes Ausweismedium kopieren können. Das bedeutet, dass bei den klassischen Kartentypen Kopien nicht erkannt werden können und sich z. B. die Türen auch für die Fälschungen öffnen. Dadurch ist die Sicherheit verschiedener bisher verwendeter Leseverfahren gegen Angriffe von außen zukünftig nicht mehr einwandfrei gewährleistet.

Die Technische Leitlinie des BSI - TL 03402 definiert als Mindestanforderungen an das bei Zutrittskontrollsystemen zu verwendende Leseverfahren:

- das verwendete RFID-System soll der Norm ISO/IEC 14443 „Proximity integrated circuit cards“ entsprechen
- es muss ein Authentifizierungsverfahren nach dem Challenge/Response-Prinzip gemäß der Norm ISO/IEC 9798-2 „Entity authentication“ (unilateral oder mutual authentication) aufweisen
- der Datenaustausch zwischen Eingabeeinheit und IMT muss verschlüsselt erfolgen

Gemäß den Richtlinien des BSI müssen Informationen auf Identifikationsmerkmalträgern, die Informationsübertragung und die Authentifikation gegenüber der Zutrittskontrollanlage mindestens mit 3-DES, für neue Anlagen mit AES oder vergleichbar hochwertigen Verfahren, geschützt sein.

Aus heutiger Sicht sind Leseverfahren, die unter anderem eine Verschlüsselung nach dem AES Verfahren (Advanced Encryption Standard) und darüber hinaus weitere Sicherheitsfeatures bieten, als sicher zu bezeichnen. Diese Technologien verfügen jeweils über höchste Sicherheit bei Datenspeicherung und Datenübertragung. Es handelt sich um flexible Prozessorchips mit einem großen Datenspeicher (2,4 bzw. 8 kByte) Die Übertragungsentfernung beträgt aufgrund der durch die Sicherheitsmechanismen erhöhten Kommunikation zwischen Ausweismedium und Lesemodul bei beiden Leseverfahren ca. 4 cm je nach Komponenteneinsatz.

4.1.2.5 Biometrie

Biometrische Komponenten in einer Zutrittskontrollanlage müssen so sicher ausgeführt sein, dass eine Nachbildung von biometrischen Merkmalen nicht zu einer Zutrittsberechtigung führt. Zur Erkennung können die Verifikation (1:1-Vergleich) oder die Identifikation (1:n-Vergleich) genutzt werden. In der Zutrittskontrolle können biometrische Merkmale, wie der Fingerabdruck, die Iris- oder Netzhaut, der Handflächenabdruck, das Handvenenmuster oder Gesichtsmerkmale zur Erkennung herangezogen werden. In den heutigen am Markt verfügbaren Zutrittskontrollanlagen haben sich die Systeme der Fingerabdruck- und Handvenenerkennung durchgesetzt.
Die Handvenenerkennung gilt heute als hochsicheres Verfahren bei der biometrischen Erkennung in der Zutrittskontrolle.

4.1.2.6 **Beispielhaftes Planungsschema für Zutrittskontrollanlagen**

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Aufgabenstellung	Individuell durch den Auftraggeber, z. B. durch den Fachplaner, die Bauabteilung oder den Betreiber. Bei der Festlegung der Türausstattung muss unbedingt der Nutzer mit einbezogen werden, da Zutrittskontrollanlagen nur mit Kenntnis der Personenflüsse (Mitarbeiter, Lieferanten, Besucher) sinnvoll geplant werden können.
Schutzziele des Auftraggebers können sein	• generell Schutz am Tag vor äußeren und inneren Angriffen • Schutz von Waren, Werten, Daten und wertvoller Arbeitsausstattung • Schutz vor Diebstahl, Sabotage, Vandalismus und ungewünschten Wissenstransfer • Schutz vor unbefugtem Betreten von Räumen, Gebäuden und Arealen (Zutrittskontrolle schließt Nichtberechtigte aus) Bei Erfüllung der Schutzziele muss beachtet werden, dass Berechtigte so wenig wie möglich in ihrer Bewegungsfreiheit eingeschränkt werden. Weitere mögliche Einsatzziele: • Personenflüsse steuern und regulieren nach räumlicher und zeitlicher Vorgabe • Erhöhung der Arbeits-, Betriebs-, und Prozesssicherheit • Protokollierung und Auswertung aller Ereignisse an Türen • wirtschaftliche „Schließanlagenverwaltung" durch Ersatz des Schlüssels durch Transponder/Ausweis
Erfassungsebene (Zutrittskontroll-Leser)	Auswahl abhängig von Standort, Umgebungsbedingungen und Schutzgrad des jeweiligen Zutrittspunktes Beispiele für Auswahlkriterien: • Leser für Außenbereich (IP65) mit oder ohne PIN, für Einbau in Sprechanlagen oder Metallumgebungen (z. B. Säulen oder Fassaden) • Weitbereichsleser für Tiefgaragen- und Parkplatzeinfahrten • Leser für Innenbereich mit oder ohne PIN, zum Einbau in Schalterprogramme, für Einbau in Sprechanlagen oder Metallumgebungen (z. B. Aufzugskabine oder Drehsperren) • Türbeschläge und Schließzylinder zur Ablösung der mechanischen Schließanlage • Handvenenleser zur biometrischen Erfassung an besonders schutzwürdigen Bereichen
Türausstattung im Rahmen der Zutrittskontrolle	• Prüfung der baulichen Rahmenbedingungen: Brandschutz, Fluchtwegkonzept • Prüfung der Anforderungen auf Verschluss/Verriegelung und Türstatusüberwachung • Prüfung auf Schnittpunkte zu anderen Systemen (Einbruchmeldeanlage, Fluchtwegsteuerung etc.)

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Identifikationsmerkmalsträger (Ausweise)	Auswahl der Medien abhängig von Umgebungsbedingungen und weiteren Funktionen. Beispiele für Auswahlkriterien: • Art und Form des Mediums: Ausweis, Schlüsselanhänger (diverse Formen verfügbar), Armbandtransponder, selbstklebendes Label • Ausweis mit Druck Firmenlogo und /oder Personalisierung als Dienstausweis • Anforderungen an Maße (z. B. Schlüsseltresor) mechanische Festigkeit, Kratzfestigkeit, Temperaturstabilität, Wasserdichtheit, Lebensdauer und UV-Beständigkeit • Schlüsselanhänger aus glasfaserverstärktem Polyamid, Polcarbonat, Aluminium oder ABS Kunststoff mit massivem Edelstahlrahmen, gravierbar oder bedruckbar • Klärung des zu verwendenden Leseverfahrens (Stand der Technik beachten) • Klärung der erforderlichen Chipeigenschaften: Speicherplatz, Leseentfernung und Lesequalität (ggf. externer Kondensator erforderlich) • Klärung der Antennenqualität: Spulentechnologie, Antennenquerschnitt, Antennenform und -platzierung im Medium • Einhaltung der ISO-Normen : ISO 7810 (Ausweise), ISO 14443 und ISO 15693 (kontaktlose Chipkarten) • Art der Verschlüsselung (3DES, AES) • Art der Sicherheit: Schlüsselmanagement, Lizenzkarten o. ä.
Übertragungsweg von der Erfassungsebene zur Steuerungsebene (Zutrittskontrollzentrale)	Mögliche Varianten, u. a. • eigenes Leitungsnetz • eigenes Funknetz (bei Funkanbindung von Offline-Komponenten) • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege • Klärung der Anforderungen nach Datenverschlüsselung auf den Übertragungswege (AES)
Steuerungsebene (Zutrittskontrollzentrale)	Klärung der dezentralen Standorte, Beachtung der Unterbringung in gesicherten Bereichen (z. B. Technik- oder IT-Räume), Ausführung in 19" oder als Wandgehäuse, Prüfung auf Anforderung nach Notstromversorgung der angeschlossenen Türen, Auswahl nach Art und Anzahl der zu versorgenden Zutrittspunkte sowie der auszuführenden Ansteuerungen und aufzunehmenden Eingangssignale
Übertragungsweg von der Steuerungsebene zur Zentralenebene (übergeordnete Zutrittskontrollzentrale)	Mögliche Varianten, u. a. • eigenes IP-Netz • Mitnutzung des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege • Klärung der Anforderungen nach Datenverschlüsselung der Übertragungswege (z. B. SSH, SSL)

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Zentralenebene (übergeordnete Zutrittskontrollzentrale)	• Auswahl der Software nach Vorgaben des Nutzers zu Betriebssystem, Datenbank, Web-Servern, Virtualisierung und Browserfähigkeit • Auswahl nach Anzahl der Stammsätze, Anzahl sowie Ausführung der geplanten Hardwarekomponenten, • Auswahl nach verfügbaren Systemfunktionen, wie z. B. Besucherverwaltung, Mandantenfähigkeit, Datenimport/-export, Schleusen- und Aufzugssteuerung, Raumzonenwechselkontrolle und Zonenbilanzierung, Scharf-/Unscharfschaltung von Einbruchmeldeanlagen • Auswahl nach erforderlichen Datenbank-, File-, und Socket-Schnittstellen sowie ggf. zertifizierten Applikationsschnittstellen • Klärung des Hardwarekonzeptes für Server und Bedienplatzrechner
Schnittstellen zu anderen Gefahrenmeldeanlagen und zum Gebäudemanagementsystem	Möglich sind Schnittstellen u. a. zu/zum • Überfall-/Einbruchmeldeanlage • Videoüberwachungssystem • Brandmeldeanlage • Flucht- und Rettungswegsystem • Gebäudemanagementsystem-Sicherheitstechnik mögliche Schnittstellen zu weiteren Systemen: • Personaldatenverwaltungssystem • Zeiterfassungssystem • Besucherverwaltungssystem • Kantinendatensystem • Sprechanlage • Parkplatzverwaltungssystem Die Rückwirkungsfreiheit ist zu gewährleisten
Übertragungsweg von der Zentralenebene zum Gebäudemanagementsystem	Mögliche Varianten, u. a. • eigenes Leitungsnetz • eigenes Funknetz (bei Funkanbindung von Offline-Komponenten) • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege Die Rückwirkungsfreiheit ist zu gewährleisten
Gebäudemanagementsystem	• Auslegung entsprechend der vorgenannten definierten Anforderungen • Klärung erforderlich, welche Zustände von welchen Komponenten, welche Alarme mit welchen Prioritäten, welche Störungsmeldungen an GMS übertragen werden sollen, welche Rückgriffe und Fernsteuerungen aus dem GMS erfolgen sollen etc.

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Übertragungsweg vom Gebäudemanagementsystem zur Sicherheitsleitstelle und zur Ausfallebene	Mögliche Varianten, u. a. • eigenes Leitungsnetz • eigenes Funknetz (bei Funkanbindung von Offline-Komponenten) • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege Die Rückwirkungsfreiheit ist zu gewährleisten
Sicherheitsleitstelle	• Auslegung entsprechend der vorgenannten definierten Anforderungen • Klärung erforderlich, welche Zustände von welchen Komponenten, welche Alarme mit welchen Prioritäten, welche Störungsmeldungen an Sicherheitsleitstelle übertragen werden sollen, welche Rückgriffe und Fernsteuerungen aus der Sicherheitsleitstelle erfolgen sollen etc.

4.1.2.7 **Beispielhafte Funktionen und Anschaltungen einer Zutrittskontrollanlage an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle**

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an Zutritskontroll-Zentrale	an die Polizei	an GMS	an die Sicherheits-Leitstelle
1.	**Anforderungen an die Zutrittsleser, u.a.**							
1.1	**Leservarianten in Abhängigkeit zu den Sicherheitsanforderungen**							
1.1.1	Zutrittsleser ohne PIN (AP/UP, Schalterdosenformat, IP65, zum Einbau in Sprechanlage, zum Einbau in Metallumgebungen)		●		●		●	
1.1.2	Zutrittsleser mit PIN (AP/UP, IP65, zum Einbau in Sprechanlage, zum Einbau in Metall-umgebungen)		●		●		●	
1.1.3	Zutrittsleser mit PIN und Display		●		●		●	
1.1.4	Zutrittsleser mit Scramble-PIN		●		●		●	
1.1.5	Fingerprint-Leser		●		●		●	
1.1.6	Handvenen-Leser		●		●		●	
1.2	**Leservarianten für weitere Funktionen**							
1.2.1	Schreib-Leser für die Vergabe von Offline-Berechtigungen		●	●	●		●	
1.2.2	Motoreinzugsleser		●	●	●		●	
1.2.3	Weitbereichsleser		●	●	●		●	
1.2.4	Türbeschlag offline		●					
1.2.5	elektronischer Schließzylinder offline		●					
1.2.6	Wandleser offline		●					
2.	**Buchungs- und Erkennungsfunktionen, u.a.**							
2.1	**Buchungsfunktionen**							
2.1.1	Zutritt berechtigt		●		●		●	
2.1.2	Zutrittsversuch unberechtigt	●	●		●		●	
2.1.3	ungültiger PIN	●	●		●		●	
2.1.4	Bedrohungsalarm	●	●		●		●	●
2.1.5	automatischer Ausweiseinzug		●		●		●	
2.1.6	Dauerfreigabe		●		●		●	
2.1.7	Aufzugssteuerung		●		●			
2.1.8	Scharf-/Unscharfschaltung		●		●		●	
2.2	**Zutrittspunktmeldungen**							
2.2.1	Türöffnung		●		●			
2.2.2	Türoffenzeitüberschreitung	●	●		●		●	
2.2.3	Sabotage Leser	●	●		●		●	●
2.2.4	Einbruch / Durchbruch	●	●		●		●	●
2.2.5	Sabotage Stellglied (Türöffner, Schloß)	●	●		●		●	●
2.2.6	Störung Stellglied (Türöffner, Schloß)	●	●	●	●		●	
2.2.7	Fluchtwegsystem ausgelöst	●	●		●		●	●
2.2.8	Leser offline	●	●	●	●		●	

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an Zutritskontroll-Zentrale	an die Polizei	an GMS	an die Sicherheits-Leitstelle
3.	**Anforderungen an das Zentralsystem, u.a.**							
3.1	räumliche Zutrittsberechtigungen				●			
3.2	Bildung von Raumzonen				●			
3.3	Zeitmodelle mit Zutrittskalender				●			
3.4	Steuerungsfunktionen für Schleusen				●			
3.5	Steuerungsfunktionen für Aufzüge				●			
3.6	Steuerungsfunktionen für Scharf-/Unscharfschaltung EMA	●			●		●	
3.7	Überwachung und Anzeige der Zutrittspunkte (Tableau)	●			●		●	
3.8	Raumzonenwechselkontrolle				●			
3.9	zeitliche Zutrittswiederholkontrolle				●			
3.10	Raumzonenbilanzierung				●			
3.11	mehrere Ausweise pro Person verwaltbar				●			
3.12	4-Augen-Prinzip				●			
3.13	Personenkontrolle /-auslosung				●			
3.14	Videoverifikation				●		●	
3.15	Aufenthaltsdauerüberwachung	●			●		●	
3.16	Doppelbenutzungskontrolle				●		●	
3.17	Routing				●			
3.18	Besucherverwaltung				●			
3.19	Wächterrundgang				●			
3.20	Schließplanverwaltung				●			
3.21	Verwaltung von Offline-Komponenten				●			
3.22	Datenimport und -export				●			
3.23	Speicherung aller Ereignisse		●		●			
3.24	Logbuchfunktion für alle Ereignisse mit Filter		●		●			

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an Zutritskontroll-Zentrale	an die Polizei	an GMS	an die Sicherheits-Leitstelle
4.	**Datenverwaltung**							
4.1	**Personenverwaltung**							
4.1.1	Anlegen von Benutzern und Zugriffsrechten				●			
4.1.2	Anlegen, ändern und löschen von Personendaten				●			
4.1.3	Vergabe, ändern und löschen von Abteilungen				●			
4.1.4	Anlegen, ändern und löschen von Ausweisen							
4.1.5	Vergabe, ändern und löschen von Zutrittsprofilen				●			
4.1.6	Vergabe, ändern und löschen von Vorrangschaltungen				●			
4.1.7	Anlegen, ändern und löschen von Suchkriterien				●			
4.1.8	Vergabe, ändern und löschen von Personen- und Ausweissperren				●			
4.1.9	Personaldaten manuell oder zyklisch im- oder exportieren				●			
4.2	**Besucherverwaltung**							
4.1.1	Anlegen, ändern, löschen und voranmelden von Besuchern				●			
4.1.2	Übersicht über aktuelle Besuche und Voranmledungen				●			
					●			
4.3	**Auswertungen, u.a.**							
4.3.1	Zutritte Personen an Türen			●	●			
4.3.2	Ereignisliste der Leser			●	●			
4.3.3	Übersicht Zutrittsberechtigungen			●	●			
4.3.4	Zutrittsberechtigungen für Personen			●	●			
4.3.5	Zutrittsberechtigungen für Zutrittspunkte			●	●			
4.3.6	Zuordnungen von Ausweisen zu Personen			●	●			
4.3.7	gesperrte Ausweise			●	●			
4.3.8	Anwesenheitsliste (nur bei Ein- und Ausgangsbuchung)			●	●			
4.3.9	Systemdaten			●	●			
4.3.10	dynamische Listen nach Anforderung			●	●			
5.	**Protokollierung, u.a. von**							
5.1	Zutrittsbuchungen		●		●			
5.2	Zutrittsversuchen	●	●		●			
5.3	Alarmmeldungen	●	●		●		●	●
5.4	Bewegungsmeldungen		●		●			
5.5	Störungsmeldungen	●	●		●		●	

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an Zutritskontroll-Zentrale	an die Polizei	an GMS	an die Sicherheits-Leitstelle
6.	**Überwachungsfunktionen, u.a**							
6.1	Ausfall der Energieversorgung (Netz – Ausfall / Batterie)	●	●		●		●	
6.2	Ausfall Server	●	●		●		●	●
6.3	Ausfall der Zutrittskontrollzentrale	●	●		●		●	
6.4	Ausfall Zutrittsleser		●		●		●	
6.5	Überwachung von Zutrittspunkten		●		●		●	
6.6	Aufenthaltsdauer der Personen		●		●		●	
6.7	Zutrittsversuche mit einem ungültigen oder gesperrten Identifikationsmittel	●	●		●		●	
6.8	Zutrittsversuche außerhalb der gültigen Raum- oder Zeitzone		●		●		●	
6.9	Aussperrungen aufgrund der Doppelbenutzungskontrolle		●		●		●	
6.10	Überschreiten der erlaubten Türoffenzeiten	●	●		●		●	
6.11	Einbruch	●	●		●		●	●
6.12	Rücksetzsignale		●		●			
6.13	Quittiersignale		●		●			
6.14	Rückmeldungen		●		●			
6.15	Zustandsmeldungen		●		●			
6.16	Sabotagemeldungen		●		●		●	
6.17	System-Störmeldungen		●		●		●	
7.	**Anschaltung von Schnittstellen zum / zur / zu, u.a. an**							
7.1	Überfall-/Einbruchmeldeanlagen				●		●	
7.2	Videoüberwachungsanlagen				●		●	
7.3	Brandmeldeanlagen				●		●	
7.4	Flucht- und Rettungswegsystem				●		●	
7.5	Gebäudemanagementsystem-Sicherheitstechnik				●		●	
7.6	Personaldatenverwaltungssystem				●			
7.7	Zeiterfassungssystem				●			
7.8	Besucherverwaltungssystem				●			
7.9	Kantinendatensystem				●			
7.10	Sprechanlage				●			
7.11	Parkplatzverwaltungssystem				●			
7.12	Ersatzweg zu einer redundanten Leitstelle				●		●	●
8.	**Fernservice- / Remote-Service-Funktionen**							
8.1	Inspektions-Schaltungen				●		●	
8.2	Update-Service				●			

Hinweise zur Inspektion und Instandhaltung von Zutrittskontrollanlagen geben unter anderem folgende Normen bzw. Richtlinien:

BSI 03403
Eine regelmäßige Wartung der ZKA (mind. einmal im Jahr) ist mit einem fachkundigen Unternehmen zu vereinbaren. Die Wartung ist durch den Auftragnehmer in einem Betriebsbuch zu bestätigen.

VdS 2367
Die Inspektionen sind bei ZKA der Klasse C mindestens viermal jährlich und bei ZKA der Klasse B mindestens zweimal jährlich in etwa gleichen Zeitabständen durchzuführen. Mindestens einmal jährlich ist, ggf. in Zusammenhang mit einer Inspektion, eine Wartung der ZKA durchzuführen.

EN 50133-7 und EN-60839-11-2
Um sicherzustellen, dass die EZKA fortlaufend richtig arbeitet, soll sie in vereinbarten Zeitabständen inspiziert und gewartet werden. Ein Instandhaltungsvertragsabkommen soll mit einem fachkundigen Unternehmen für Inspektion und Wartung getroffen werden. Inspektions- und Wartungsabläufe sollen vom Hersteller oder Errichter geliefert und dokumentiert werden. Inspektion und Wartung sollen nach diesen Abläufen durchgeführt werden und die Prüfung der Funktion der Zutrittspunkte beinhalten.

ZKA Zutrittskontrollanlage
EZKA Elektronisches Zutrittskontrollsystem / Elektronische Zutrittskontrollanlage

4.1.3 Videoüberwachungsanlagen (VÜA) für Sicherheitsanwendungen

4.1.3.1 Funktionale Beschreibung

Videotechnik kann in vielen Bereichen eingesetzt werden. Beispiele dafür sind Verkehrsregelung, Produktionskontrolle, Produktvermessung oder Objektüberwachung. Im Rahmen eines Sicherheitskonzeptes hat sich die Videoüberwachungstechnik zu einem effektiven Mittel der Schadenverhütung entwickelt. Potenziellen Tätern soll durch wirksame und sichtbare Maßnahmen der Anreiz zu Einbruch, Überfall oder Brandstiftung genommen, der Schaden gering gehalten und die Voraussetzungen für das polizeiliche Handeln (z. B. Gefahrenabwehr, Fahndung) verbessert werden. Die Anforderungen an Videoüberwachungssysteme der Kategorie II beschreiben, wie Systemlösungen zu einem wirksamen Gesamtkonzept zusammengeschlossen werden können.

4.1.3.2 Definition - Videoüberwachung

Unter Videoüberwachung versteht man die Beobachtung von Objekten, Personen oder Geländestrecken mittels Videokamera und Monitor. In der einfachsten Form der Videoüberwachung werden lediglich Videokamera und Monitor verbunden. Je nach Aufgabenstellung wird es jedoch notwendig sein, weitere Komponenten in das Videoüberwachungssystem mit einzubinden.

4.1.3.3 Definition Fern-Videoüberwachung

Um aus einer Vielzahl von Meldungen die richtige/angemessene Maßnahme vor Ort abzuleiten, haben Sicherheits-Leitstellen unterschiedliche Strategien entwickelt. Hierzu zählen:

- die Verknüpfung der Meldungen aus einem Objekt
- das Beobachten von Folgemeldungen
- das **„Hineinhören"** in ein Objekt, welches in Deutschland nur bei einem Aufzugsnotruf oder einem Zutrittswunsch nach einer Alarmauslösung üblich ist.
- das **„Hineinsehen"** in Objekte, z. B. zur Alarmverifikation

4.1.3.4 Aktivitätenverwaltung

Die Aktivitätenverwaltung umfasst alle Aktivitäten, die durch Ereignisse oder Benutzeraktionen angestoßen werden. Ein Ereignis ist ein Vorkommnis in der realen Welt, z. B. ein Brand (ein brennendes Haus), ein Einbruch (eine aufgebrochene Tür) oder eine andere definierte Situation (eine sich bewegende Person). Das Ereignis kann mit einer Bedrohung für das Leben oder Eigentum von Personen einhergehen oder auch ein auf die VÜA gerichtetes Vorkommnis sein, z. B. die Sabotage einer Systemkomponente.

Das Ereignis kann eine Alarmprozedur in der VÜA auslösen. Der Auslöser kann das Ergebnis einer Bildverarbeitung (z. B. Videoinhaltsanalyse oder Videobewegungsmelder), ein Signal eines Sensors (z. B. Rauch- oder Bewegungserkennung) oder der Empfang von Daten von einem anderen System, z. B. ein APNR-System (Automatic Number Plate Recognition (Nummernschilderkennung) sein. Wird die Alarmprozedur ausgelöst, führt die VÜA die in der Leistungsbeschreibung festgelegten Aufgaben aus. Meistens bestehen diese Aufgaben aus Reaktionen auf die erkannten Gefahren.

Diese Alarmreaktion kann interne Aktivitäten (z. B. absichtliche Änderung der Kameraposition, um die Ansicht, Aufzeichnung oder Bilddarstellung zu ändern) sowie Benachrichtigungen an ein externes System (z. B. Zutrittskontrollsystem oder Alarmempfangszentrale) einschließen. Eine typische Aufgabe einer Alarmprozedur besteht auch darin, einen Bediener zu alarmieren, so dass dieser wiederum andere Aktivitäten starten kann. Die von einem Bediener durchgeführten Aktionen sind in der Leistungsbeschreibung festgelegt.

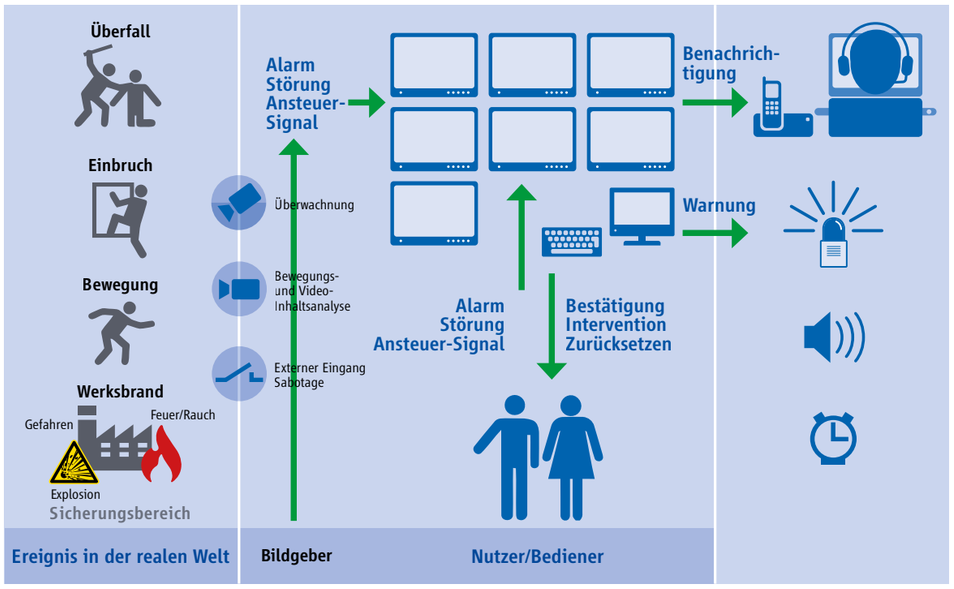


Bild Grafik veranschaulicht ereignisgesteuerte Aktivitäten

4.1.3.5 Schnittstellen zu anderen Systemen

Wenn Schnittstellen zu anderen Systemen vorhanden sind, müssen Befehls- und Datenformate für beide Systeme im Einzelnen festgelegt werden. Systemschnittstellen ermöglichen den gegenseitigen und bequemen Zugriff auf Funktionen und Daten. Eine VÜA kann Schnittstellen mit anderen Systemen haben, wie z. B.

- andere Sicherungssysteme (z. B. andere VÜA, Einbruch- und Überfallsysteme, Zutrittskontrollsysteme oder Brandmeldesysteme);
- Sicherheitsverwaltungssysteme (z. B. Alarmverwaltungssysteme, Alarmempfangszentralen oder Videoempfangszentralen);
- andere Systeme außerhalb der Sicherungstechnik (z. B. Gebäudemanagementsysteme, Geldautomaten, Kassensysteme oder Systeme zur automatischen Nummernschilderkennung).

Die Schnittstellen zwischen den Systemen können Datenübertragungen, die gegenseitige Systemsteuerung, gemeinsame Datenbanken und Benutzerschnittstellen oder andere Arten der Systemintegration verwalten.

Im Allgemeinen kann zwischen zwei Arten der Übertragung unterschieden werden: Entweder ist der physische Übertragungsweg Teil der VÜA oder er wird von einem Dritten als externe Verbindung zur Verfügung gestellt.

4.1.3.6 Digitale Videoüberwachungsanlagen (VÜA)

Digitale VÜA werden heutzutage überwiegend IP basiert aufgebaut. Diese werden häufig auch IP-basierte Videoüberwachung oder IP-Videoüberwachung genannt und ermöglichen die Videoüberwachung und -aufzeichnung von einer beliebigen Position im Netzwerk aus. Dies kann beispielsweise das LAN (Local Area Network) oder ein WAN (Wide Area Network) wie das Internet sein. Im LAN-Bereich wird entweder eine drahtgebundene oder drahtlose Netzwerkinfrastruktur für die Übertragung digitaler Video-, Audio- und anderer Daten genutzt.

Als drahtgebundene Variante kommt Ethernet laut dem IEEE-802.3-Standard zum Tragen und als drahtlose Lösung Wireless LAN (WLAN) nach dem IEEE-802.11-Standard. Im ersten Fall kann durch die Verwendung der Power over Ethernet-Technologie (PoE) die Stromversorgung der Netzwerk-Videoprodukte über das Netzwerk erfolgen.

Die zentralen Komponenten eines Netzwerk-Videosystems sind die Netzwerk-Kameras, die Video-Encoder (für die Anbindung von analogen Kameras), das Netzwerk, der Server, das Speichermedium und die Videoverwaltungssoftware. Da Netzwerk-Kameras und Video-Encoder computerbasierte Geräte sind, bieten sie Funktionalität, die mit einer analogen CCTV-Kamera nicht erzielt werden kann.

Bei den anderen Komponenten wie Netzwerk, Speicher und Server handelt es sich vielfach um Standard-IT-Equipment. Die Möglichkeit zur Verwendung gängiger Standardprodukte ist einer der Hauptvorteile von Netzwerk-Video. Zu den anderen Komponenten eines Netzwerk-Videosystems gehören Zubehörteile, wie z. B. Kameragehäuse, PoE-Midspans und -Splitter.

Das digitale Netzwerk-Videoüberwachungssystem bietet zahlreiche Vorteile und Spezialfunktionen, mit denen ein analoges Videoüberwachungssystem nicht aufwarten kann. Zu den Vorteilen gehören der Fernzugriff, die hohe Bildqualität, die Ereignisverwaltung, intelligente Videofunktionen, einfache Integrationsmöglichkeiten und eine bessere Skalierbarkeit, Flexibilität und Kosteneffizienz.

4.1.3.7 **Beispiele für funktionale Schnittstellen zu anderen Gewerken.**

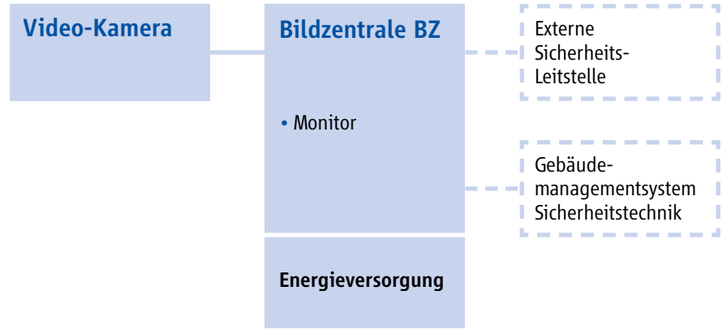
Gewerk	Funktionalität
Brandmeldeanlagen	• Videobasierte Raucherkennung • Videobasierte Branderkennung mittels Wärmebildkamera zur Visualisierung des auslösenden Ereignisses
Einbruchmeldeanlagen	• Optische Verifikation eines auslösenden Ereignisses • Bewegungsmelderfunktion zur Unterstützung bestimmter Bereiche • Sabotageerkennung an der Kamera (verdrehen/abdecken/erschüttern, etc.)
Perimeter/Freigelände	• Personen oder Objekte durch eine Video Content Analyse (VCA) z. B. bei Zaunabsicherungen zu detektieren
Point of Sale	• Kassenanbindung
Zutrittskontrolle/Schlüsselverwaltung/Intercom	• Bildvergleich mit dem Karteninhaber • Fernsteuerung von Zu- und Abgängen (Tore, Schranken) • Biometrie • KfZ-Nummernschilderkennung
Videoempfangssystem	• Aufzeichnungen mittels objektspezifischer Daten einfach finden
Aufzugsnotruf	• Optische Verifikation von Aufzugsnotrufen
Fluchtwegsteuerung	• Optische Überwachung zum Fluchtwegen

Diese Auflistung hat kein Recht auf Vollständigkeit. Sie beschreibt lediglich mögliche Schnittstellen zu anderen Gewerken. Teilweise wird eine Zusatzsoftware benötigt, diese kann entweder auf der Kamera oder aber auf einem separaten Server betrieben werden. Gesetzliche Auflagen sind dabei zu beachten!

4.1.3.8 **Videoinformationsanlage (VIA)**

Die Videoinformationsanlage (VIA) entspricht keiner einschlägigen Norm oder VdS-Richtlinie. Sie hat die Aufgabe, Kamerabilder auf einem Monitor anzuzeigen. Für sicherheitsrelevante Anwendungen sind solche Anlagen ungeeignet.

Schutzziel und Positionierung werden mit dem Betreiber festgelegt. Leitungen sind grundsätzlich betriebssicher und möglichst unauffällig zu verlegen. Die Positionierung der Kameras sollte an die örtlichen Gegebenheiten sowie an die Lichtverhältnisse angepasst, stabil und erschütterungsfrei befestigt werden. Bei Ausfall der Kamera bzw. bei sonstigen Störungen der Zentrale wird die automatische Meldung an eine ständig besetzte Stelle empfohlen. Ebenso sollten Überspannungs- und Blitzschutzmaßnahmen vorgesehen werden.



4.1.3.8.1 **Videoüberwachungsanlagen (VÜA) nach der Norm DIN EN 63676-1-1**

- Videoüberwachungsanlage nach DIN EN 63676-1-1 – Grad 1
- Videoüberwachungsanlage nach DIN EN 63676-1-1 – Grad 2
- Videoüberwachungsanlage nach DIN EN 63676-1-1 – Grad 3
- Videoüberwachungsanlage nach DIN EN 63676-1-1 – Grad 4

Anschaltung der Video-Zentraleinheit an

Gebäudemanagementsystem-Sicherheitstechnik

Externe Sicherheits-Leitstelle

Nachfolgende Übertragungswege sind für die jeweiligen Videoüberwachungsanlagen erforderlich:

- Video-Kameras / Video-Sensorik zur Video-Zentraleinheit
- Video-Kameras / Video-Sensorik zur Video-Managementsystem
- Video-Zentraleinheit zum Gebäudemanagementsystem-Sicherheitstechnik
- Video-Zentraleinheit zur „Externen Sicherheits-Leitstelle“
- Gebäudemanagementsystem-Sicherheitstechnik zur „Externen Sicherheits-Leitstelle“

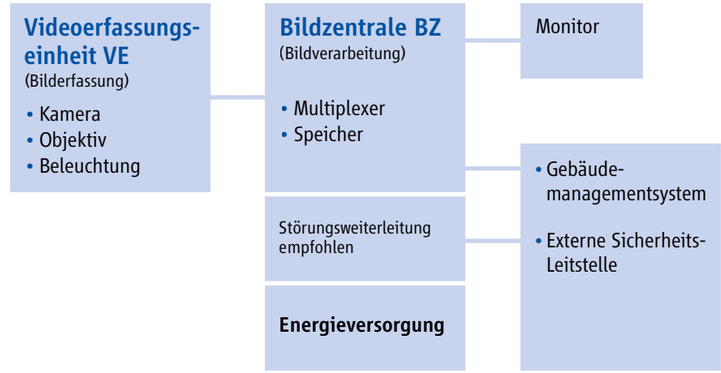
4.1.3.8.2 **Übersicht der beispielhaften Konzepte für Videoüberwachungsanlagen nach der Norm DIN EN 63676-1-1-Grad 1 - 2 - 3 - 4**

	DIN EN 63676-1-1 - Grad 1	DIN EN 63676-1-1 - Grad 2	DIN EN 63676-1-1 - Grad 3	DIN EN 63676-1-1 - Grad 4
Die Videoüberwachungsanlage VÜA entspricht der DIN EN 63676-1-1 Grad 1 (geringes Risiko).	●			
Die Videoüberwachungsanlage VÜA entspricht der DIN EN 63676-1-1 - Grad 2 (geringes bis mittleres Risiko).		●		
Die Videoüberwachungsanlage VÜA entspricht der DIN EN 63676-1-1 - Grad 3 (mittleres bis hohes Risiko).			●	
Die Videoüberwachungsanlage VÜA entspricht der DIN EN 63676-1-1 - Grad 4 (hohes Risiko).				●
Hinweis: Es ist der „Bundeseinheitliche Pflichtenkatalog für Errichterfirmen von VÜA“ (LKA-Richtlinie) zu beachten.	●	●	●	●
VÜA hat die Aufgabe, über Video-erfassungseinheiten VE erfasste Bilder an der Bildzentrale BZ oder auf einem zentralen Gebäudemanagementsystem-Sicherheitstechnik oder in einer Externen Sicherheits-Leitstelle zu verarbeiten und darzustellen.	●	●	●	●
Die Positionierung der VE sollte an die Schutzziele, die örtlichen Gegebenheiten sowie an die Lichtverhältnisse angepasst werden. Sie sind stabil und erschütterungs-frei zu befestigen.	●			
Basierend auf den Schutzzielen sind die Aufgaben zu definieren (z. B. Diebstahl-erkennung, Beweissicherung; Fahndungs-hilfe, Täterabschreckung)		●	●	●
Leitungen sind grundsätzlich betriebssicher und möglichst unauffällig zu verlegen	●	●	●	●
Nach Alarmauslösung muss die Aufzeich-nung mit einer maximalen Verzögerungs-zeit von 1 s starten.		●		
Nach Alarmauslösung muss die Aufzeich-nung mit einer maximalen Verzögerungs-zeit von 500 ms starten			●	
Nach Alarmauslösung muss die Aufzeich-nung mit einer maximalen Verzögerungs-zeit von 250 ms starten.				●
Die VÜA muss in der Lage sein, eine Datensicherung durchzuführen.			●	
Die VÜA muss in der Lage sein, eine Datensicherung durchzuführen und einen ausfallsicheren Speicher zu verwenden.				●
Der Übertragungsweg von der BZ zur BEZ sollte alle 24 h einer Testmeldung (Routineruf) unterzogen werden.		●	●	
Die anlageninternen Übertragungswege müssen alle 10 s auf Verfügbarkeit über-prüft werden. Der Übertragungsweg von der BZ zur BEZ sollte alle 24 h einer Testmeldung (Routineruf) unterzogen werden.				●

	DIN EN 63676-1-1 - Grad 1	DIN EN 63676-1-1 - Grad 2	DIN EN 63676-1-1 - Grad 3	DIN EN 63676-1-1 - Grad 4
Die anlageninternen Übertragungswege müssen alle 30 s auf Verfügbarkeit überprüft werden.			●	
Die VÜA ist in der Lage, ein gespeichertes Bild innerhalb 2 s aus dem Speicher wiederzugeben.		●	●	
Die VÜA ist in der Lage, ein gespeichertes Bild innerhalb 1 s aus dem Speicher wiederzugeben.				●
Die Positionierung der VE muss an die Schutzziele, die örtlichen Gegebenheiten sowie an die Lichtverhältnisse angepasst werden. Sie sind stabil und erschütterungsfrei zu befestigen.		●	●	●
Zur Übertragung von Störungsmeldungen wird eine über bedarfsgesteuerte Verbindung empfohlen, die diese Meldungen an eine ständig besetzte Stelle, z. B. an ein zentrales Gebäudemanagementsystem-Sicherheitstechnik oder eine „Externe Sicherheits-Leitstelle“, weiterleitet.	●	●		
Zur Übertragung von Störungsmeldungen wird eine bedarfsgesteuerte Verbindung empfohlen, die diese Meldungen an eine ständig besetzte Stelle, z. B. an ein zentrales Gebäudemanagementsystem-Sicherheitstechnik oder eine „Externe Sicherheits-Leitstelle“ innerhalb der empfohlenen Übertragungszeiten realisieren kann.			● von 180 s empfohlen	● von 30 s empfohlen
Es ist sicherzustellen, dass gespeicherte Daten bei Ausfall der Energieversorgung nicht verloren gehen.	●	●	●	●
Gemäß DIN VDE 0845-1 sind ggf. Überspannungs- und Blitzschutzmaßnahmen zu berücksichtigen.	●	●	●	●
Instandhaltung: VÜA müssen gemäß DIN EN 50132-7* nach einem vom Anlagenplaner oder Lieferanten festgelegten Zeitplan regelmäßig durch Fachkräfte instand gehalten werden. Die Ergebnisse der wiederkehrenden Prüfungen sollten aufgezeichnet und mit vorherigen Prüfungen verglichen werden.	●	●	●	●

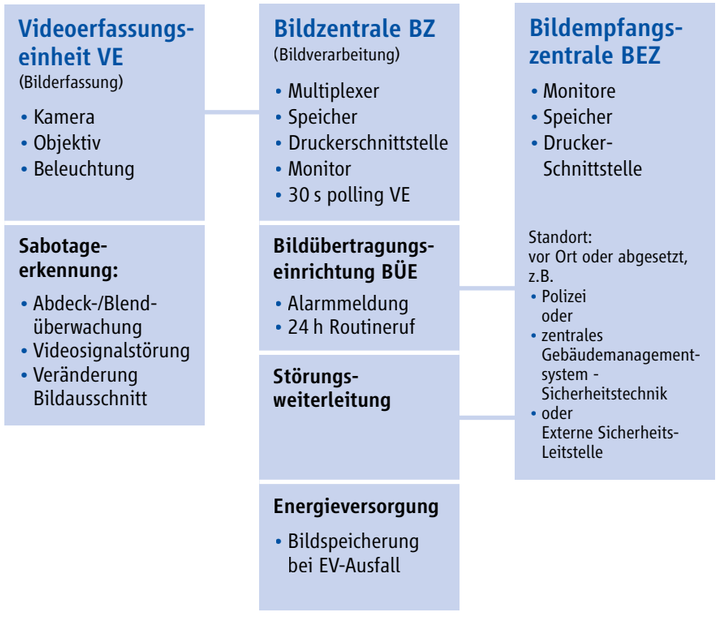
VÜA - Videoüberwachungsanlage
VE - Videoerfassungseinheit
BZ - Bildzentrale
BEZ - Bildeempfangszentrale

4.1.3.8.2.1 **Beispielhafte Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 1**

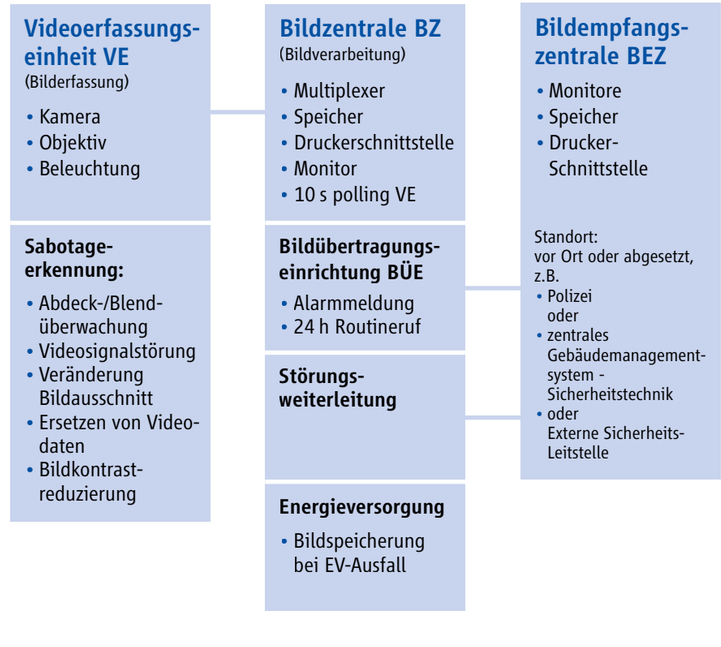


4.1.3.8.2.2 **Beispielhafte Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 2**

4.1.3.8.2.3 **Beispielhafte Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 3**



4.1.3.8.2.4 **Beispielhafte Videoüberwachungsanlage nach der Norm DIN EN 63676-1-1 – Grad 4**



4.1.3.9 Beispielhaftes Planungsschema für Videoüberwachungsanlagen (VÜA)

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Aufgabenstellung	Individuell durch den Auftraggeber, z. B. durch den Fachplaner, die Bauabteilung oder den Betreiber
Beispielhafte Schutzziele des Auftraggebers	Schutz, u. a. vor • Einbruch • Diebstahl • unberechtigtem Zutritt • Vandalismus-Schäden • Sabotage/Spionage
Erfassungsebene – Auswahl der Kameras, mit oder ohne Video-Sensor (abhängig von den Schutzzielen)	Mögliche in Betracht kommende Kameras, u. a. • Autodome-Kameras • Feststehende HD-Dome-IP-Kameras • Feststehende HD/MP IP-Kameras • Thermokamera • IP-Kameras zur Kennzeichenerfassung
Übertragungsweg von der Erfassungsebene zur Zentralenebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze in Abhängigkeit von der Auslastung - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Zentralenebene	Auswahl der passenden Videozentrale mit den dazu passenden Zentralenkomponenten, wie z. B. • Videomanagementsystem • in Verbindung mit dem Gebäudemanagement-system – Sicherheitstechnik (Bereich Video) • Videoaufzeichnungsgeräte • der Energieversorgung • den Batterien • den Anzeigemonitoren • dem/den Übertragungssystem(en)
Schnittstellen zu anderen Gefahrenmeldeanlagen und zum Gebäude-managementsystem	Möglich sind Schnittstellen u.a. zu/zum • Zutrittskontrollanlagen • Brandmeldeanlagen • Sprachalarmanlagen (SAA) • Gebäudemanagementsystem-Sicherheits-technik

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Übertragungsweg von der Zentralenebene zum Gebäudemanagementsystem	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungs-netze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Aus-fall eines der Übertragungswege
Gebäudemanagementsystem–Sicherheits-technik	Auslegung entsprechend der vorgenannten definierten Anforderungen
Übertragungsweg vom Gebäude-managementsystem zur Sicherheitsleitstelle und zur Ausfallebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungs-netze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Aus-fall eines der Übertragungswege
Sicherheitsleitstelle	Auslegung entsprechend der vorgenannten definierten Anforderungen

4.1.3.10 **Beispielhafte Funktionen und Anschaltungen einer Videoüberwachungsanlage (VÜA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle**

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an die Video-Zentrale	an die Polizei	an GMS	a.d. Sicherheits-Leitstelle
1.	**Kamera–Varianten in der Abhängigkeit zu den Sicherheitsanforderungen** (Farbe - Infrarot - Universal), u. a.							
1.1	**Innen, u.a**							
1.1.1	• Feststehende Kameras	●	●	●	●		●	●
1.1.2	• Schwenk-Neige-Kopf-Kameras	●	●	●	●		●	●
1.2	**Außen-Kameras, u.a.**							
1.2.1	• Feststehende Kameras	●	●	●	●		●	●
1.2.2	• Schwenk-Neige-Kopf-Kameras	●	●	●	●		●	●
1.3	**Arten von Kameras, u.a.**							
1.3.1	• Universalkameras	●	●	●	●		●	●
1.3.2	• Dome-Kameras	●	●	●	●		●	●
1.3.3	• Verdeckte (Diskret-) Kameras in sensiblen und öffentlichen Außenbereichen	●	●	●	●		●	●
1.3.4	• Kameras für die Fluchttürenüberwachung	●	●	●	●		●	●
1.3.5	• Kameras in Bereichen, in denen IR-Licht erforderlich ist	●	●	●	●		●	●
1.3.6	• IP-Kameras (Netzwerkkameras)	●	●	●	●		●	●
1.4	**Videoüberwachungsvarianten, u.a. die**							
1.4.1	• Videokameras überwachen permanent		●		●		●	●
1.4.2	• Videokameras werden im Inneren des Gebäudes durch Bewegungsmelder ausgelöst	●			●		●	●
1.4.3	• IR-taugliche Videokameras werden mit nach geschalteten Videosensor bei Bewegungen ausgelöst	●			●		●	●
1.4.4	• Kameras mit Kontakttriggerung und/passiver Infrarotmelder		●		●		●	●
	Hinweis: In Abhängigkeit von dem jeweiligen Hersteller gibt es für fast alle Kameratypen eine Alarm- und Servicefunktion zu implementieren.							

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an die Video-Zentrale	an die Polizei	an GMS	a.d. Sicherheits-Leitstelle
2.	**Anforderungen an die Videozentrale, u.a.**							
2.1	**Technische Kriterien, u.a.**							
2.1.1	• Maßnahmendurchführung anhand eines genau definierten Maßnahmenplanes				●		●	
2.1.2	• Server-gesteuert				●		●	
2.1.3	• Mehrplatzsystem				●		●	
2.1.4	• hohe Bedienerfreundlichkeit				●		●	
2.1.5	• einfache Parametrierung (Set up)				●		●	
2.1.6	• Anschaltung aller Videosender mit Videokameras - Anzahl 1 ... x aus den Permanent-Kameras. - Erfassen wesentlicher Phasen eines Überfalls /einer Straftat generell - (permanente) Bildspeicherung				●		●	
2.1.7	• Bewegungsmelder gesteuerten Kameras				●		●	
2.1.8	• Diskretkameras				●		●	
2.1.9	• Videosensorik				●		●	
2.1.10	• Bildalarmbearbeitung-/Verifizierung und Einleitung der vereinbarten Maßnahmen				●		●	
2.1.11	• Einleitung von Maßnahmen im Alarmfall				●		●	
2.1.12	• Speicherung der eingehenden Bilder im digitalern Bildarchiv (Aufbewahrungszeit-raum-Tage/Wochen/Monate)				●		●	
2.1.13	• Ausdruck / Datensicherung von Einzelbildern bei Bedarf				●		●	
2.1.14	• Ablagemöglichkeit von Vergleichsbildern				●		●	
2.1.15	• Livebild – Darstellungen aus den einzelnen Überwachungsbereichen				●		●	
2.1.16	• Möglichkeit der Alarmsimulationen (über analoges Modem / ISDN und / oder Netzwerk)				●		●	
2.1.17	• Übertragung der Bilddaten im Alarmfall (über analoges Modem / ISDN und / oder Netzwerk)				●		●	
2.1.18	• Anzeige der Bilddaten entfernter Stationen				●		●	
2.1.19	• Umfangreiche Statistikfunktionen, u.a. Suche nach Logbuch-Einträgen				●		●	
2.1.20	• Arbeitsfluss – Überwachung				●		●	

Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an die Video-Zentrale	an die Polizei	an GMS	a.d. Sicherheits-Leitstelle
3.	**Schnittstellen zu ein übergeordnetes Gebäudemanagementsystem-Sicherheitstechnik, u.a. an, zu, durch**							
3.1	• Einbruch-/Überfallmeldesystemen				●		●	
3.2	• Perimeterschutz-/Freilandschutz							
3.3	• Weiteren Videoüberwachungsanlagen				●		●	
3.4	• Brandmeldesystemen				●		●	
3.5	• Sprachalarmanlagen (SAA)							
4.7	• Sprinkleranlagen							
4.8	• Gaslöschanlagen							
3.6	• Zutrittskontroll-/Zeiterfassungssystemen				●		●	
3.7	• Fluchtwegsteuerungssystemen				●		●	
3.8	• Türsteuerungs- und Überwachungseinrichtung							
3.9	• akustischen Alarmierungseinrichtungen				●		●	
3.10	• Pager, Handy, Personensuchanlagen, BOS				●		●	
3.11	• Gebäudemanagementsystem-Sicherheitstechnik				●		●	
3.12	• Lüftungs- und Klimatechnische Anlagen							
3.13	• Aufzugs- und Fahrtreppenanlagen							
3.14	• Steuereinrichtungen für Parkplatz-/Tiefgaragen-Zufahrten				●		●	
3.15	• Ersatzweg zu einer redundanten Leitstelle				●		●	●
4.	**Fernservice-/RemoteService-Anschluss**			●	●		●	
4.1	• Inspektions-Schaltungen				●		●	●
5.	**Überwachungsfunktionen, u.a.**							
5.1	• Störung Video – Zentrale		●		●		●	●
5.2	• Videosignal - Ausfall		●		●		●	●
5.3	• Störung Videosender- / Empfänger 1 ... n		●		●		●	●
5.4	• Störung Videosensorik 1 ... n		●		●		●	●
5.5	• Störung Kamera 1 .... n		●		●		●	●
5.6	• Systemkomponenten-Ausfall		●		●		●	●
5.7	• Prozessorausfall		●		●		●	●
5.8	• Speicherüberwachung		●		●		●	●
5.9	• Drahtbruch/Kurzschluss		●		●		●	●
5.10	• Sabotageüberwachung		●		●		●	●
5.11	• Vandalismusüberwachung		●		●		●	●
6.	**Service- und Instandhaltungsintervalle**							
6.1	• **DIN EN 50132-7 - Instandhaltung**				●		●	
6.1.1	Für die Grade 1 bis 4: Inspektionsrhythmus 2x jährlich							
6.1.2	Wartungsrhythmus 1x jährlich							
6.2	• **VdS 2366 - ABC Instandhaltung, Wartung und Inspektion**				●		●	
6.2.1	Inspektionsrhythmus in Abhängigkeit der Klassen A bis C zwischen 1x und 4x jährlich							
6.2.2	Wartungsrhythmus 1x jährlich							

4.2 Safety

4.2.1 Brandmeldeanlagen (BMA)

4.2.1.1 Funktionale Beschreibung

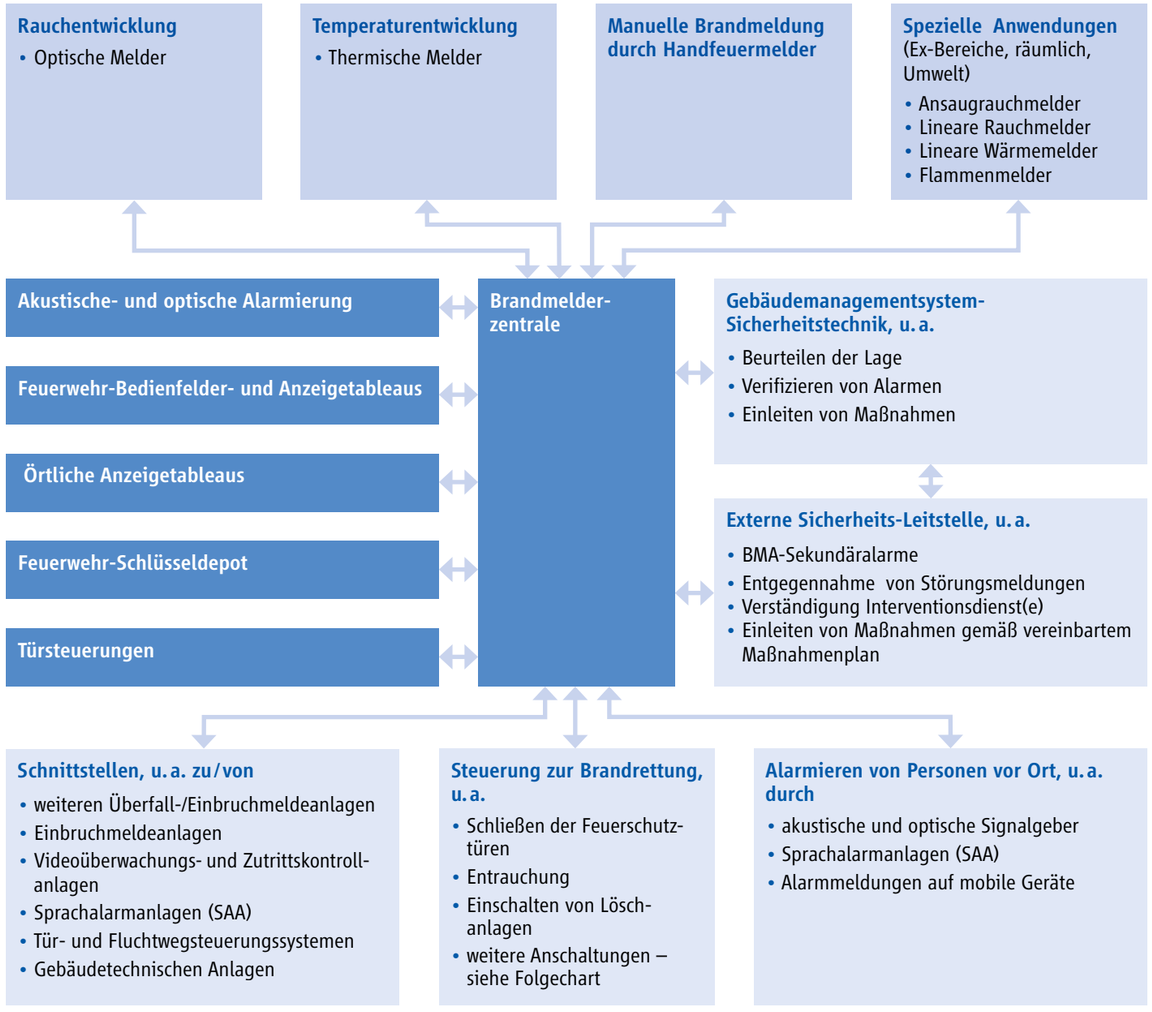
Brandmeldeanlagen haben die primäre Aufgabe, Entstehungsbrände frühzeitig zu entdecken, potentiell gefährdete Personen zu warnen und einen Alarm an die Feuerwehr weiterzuleiten. Neben der automatischen Entdeckung von Entstehungsbränden besteht auch die Möglichkeit, mit Hilfe von Handfeuermeldern einen Alarm manuell über die Brandmeldeanlage an die Feuerwehr oder eine andere hilfeleistende Stelle weiterzuleiten.

4.2.1.2 Aufbau, Aufgaben und Funktionen von Brandmeldeanlagen

Brandmeldeanlagen bestehen aus den Brandmeldern, der Brandmelderzentrale mit Energieversorgung einschließlich Notstromversorgung, der Übertragungseinrichtung, Alarmgebern zur Intern-Alarmierung und den Steuereinrichtungen, z. B. zum Schließen von Brandschutztüren, zum Öffnen von Rauch- und Wärmeabzügen, Ansteuerung von Löschanlagen oder zum Abschalten von Maschinen.

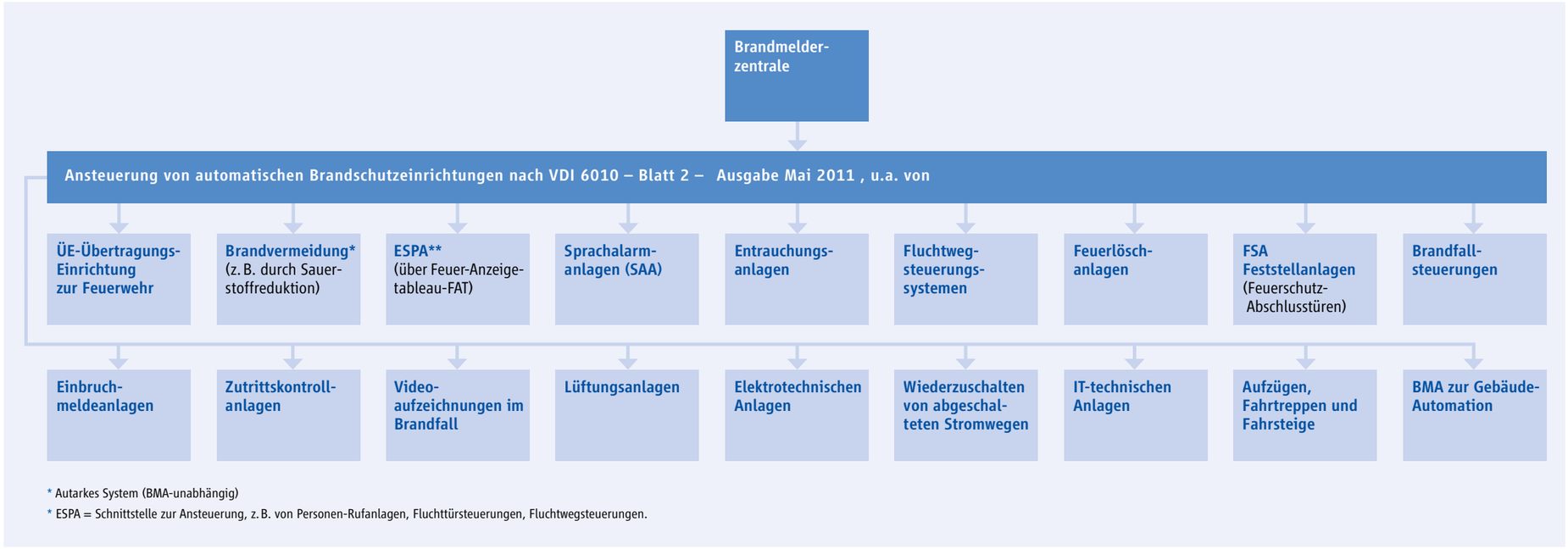
Automatische Brandmelder haben die Aufgabe, bei der Entstehung eines Brandes auftretende Brandkenngrößen wie sichtbaren oder unsichtbaren Rauch, Wärme oder Flammen, zu detektieren und an die Brandmelderzentrale zu melden. Hinzu kommen die Handfeuermelder, die zur manuellen Alarmauslösung eingesetzt werden. Zur Weiterleitung der Signale sind die Melder einzeln oder in Gruppen über Stich- und/oder Ringleitungen an die Brandmelderzentrale angeschlossen.

4.2.1.3 Beispielhafte Konfiguration einer Brandmeldeanlage (BMA)



4.2.1.4 **Mögliche Ansteuerungen aus einer Brandmelderzentrale nach der VDI 6010 – Ausgabe Mai 2011**

Sicherheitstechnische Einrichtungen – Ansteuerung von automatischen Brandschutzeinrichtungen – Kapitel 5 Steuerungsaufgaben



* Autarkes System (BMA-unabhängig)
* ESPA = Schnittstelle zur Ansteuerung, z. B. von Personen-Rufanlagen, Fluchttürsteuerungen, Fluchtwegsteuerungen.

4.2.1.5 Brandmeldeanlagen – Kernaussagen und Nutzen

Schutzziele nach der DIN 14675 – Ausgabe April 2012 – Brandmeldeanlagen : Aufbau und Betrieb – Ziff. 5 – 5.1 - u.a. Schutz vor/durch

- Bränden in der Entstehungsphase
- schnelle Information und Alarmierung der betroffenen Menschen
- automatische Ansteuerung von Brandschutz- und Betriebseinrichtungen
- Schnelle Alarmierung der Feuerwehr und/oder anderen hilfeleistenden Stellen
- Eindeutiges lokalisiieren des Gefahrenbereiches und dessen Anzeige

Brandentdeckung und Brandbekämpfung in der Entstehungsphase, u.a.

- autom. Brandmelder für jede mögliche Brandentwicklung und räumliche Situation:
- optische Melder bei Rauchentwicklung (90 % aller Brände)
- thermische Melder bei Temperaturentwicklung und/oder, wenn Rauchdetektion zu
- Fehlalarmen führen würde (z. B. Rauch aus anderen Quellen, z. B. in Lackierwerkstätten)
- Mehrsensormelder mit höchster Detektionssicherheit
- Flammenmelder bei offenen Bränden ohne Rauchentwicklung (z. B. Lager mit Benzin und flüssigen Chemikalien)
- Rauchansaugsysteme, Lineare Rauch- und Wärmemelder z. B. für Klinikräume, Ex-Räume
- genaue Brandlokalisierung und schnelle Hilfe durch Einzelmelder-Identifizierung
- Möglichkeit der Prüfung auf Fehlalarm durch gezielte lokale Voralarmierung

Schnelle Alarmierung und Information der betroffenen Menschen, u.a. durch

- optische und akustische Alarmierung, Sprachdurchsagen mittels Sprachalarmanlagen (SAA)
- die Einbeziehung von Fluchtleitsystemen

Schnelle und sichere Alarmierung der Feuerwehr und anderer Hilfeleister, u.a.

- Alarmierung der Feuerwehr über gesicherte Übertragungswege
- Alarmierung von Personen und Hilfeleistern durch eine externe Sicherheits-Leitstelle
- gute Orientierung der Einsatzkräfte: Entriegeln des Schlüsseldepots, Feuerwehrbedienfeld

Steuerung zur Brandrettung, u.a.

- Schließen der Feuerschutztüren (DIBt), Öffnen der Fluchttüren und Brandschutzklappen
- Einschalten von Rauch- und Wärmeabzugsanlagen, Entrauchung
- Abschalten von Klima- und Lüftungsanlagen, Einschalten von Löschanlagen
- Automatische Aufzugsevakuierung

Einsatz von flexibler Sicherheits-Netzwerk-Technologie

- Brand-, Notruf- und technische Meldungen (z. B. aus der Haustechnik) in einem System und über „ein" Leitungsnetz
- aktive Eigenüberwachung aller Melder

Schnittstellen zu anderen Gefahrenmeldeanlagen, u.a.

- Überfallmeldeanlagen/Einbruchmeldeanlagen
- Zutrittskontrollanlagen
- Videoüberwachungsanlagen in Verbindung mit der videobasierten Branddetektion
- Sprachalarmanlagen
- Gebäudemanagesystem-Sicherheitstechnik

4.2.1.6 Aufschaltebedingungen für Brandmeldeanlagen

Die Technischen Aufschaltbedingungen für Brandmeldeanlagen (TAB) werden in Deutschland von den einzelnen Landkreisen bzw. von den örtlichen Feuerwehren veröffentlicht. Sie enthalten die individuell festgelegten technischen Aufschaltbedingungen, die zwingend erforderlich sind, um Alarme an die Feuerwehr zu übertragen. In den meisten TAB wird eine Realisierung der Brandmeldeanlage nach DIN 14675 gefordert. Die Abnahme der Brandmeldeanlage erfolgt nur bei Einhaltung der jeweiligen TAB. Die Übertragungseinrichtung muss bei dem Konzessionär der Region beantragt werden.

4.2.1.7 Brandmeldeanlagen und Brandschutzeinrichtungen nach der Norm DIN VDE 0833, DIN 14675 und der VdS 2095

- Brandmeldeanlage nach DIN VDE 0833, Teile 1 und 2 und DIN 14675
- Brandmeldeanlage nach DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095
- Brandschutzeinrichtung nach DIN – Brandmeldeanlage mit Löschanlage nach DIN VDE 0833, Teile 1 und 2 und DIN 14675
- Brandschutzeinrichtung nach VdS – Brandmeldeanlage mit Feuerlöschanlagenansteuerung nach DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095

Anschaltung der BMA-Zentraleinheit an

Gebäudemanagementsystem-Sicherheitstechnik

Externe Sicherheits-Leitstelle

Nachfolgende Übertragungswege sind bei der (IP-)Vernetzung erforderlich:

- BMA-Sensorik zur BMA-Zentraleinheit
- BMA-Zentraleinheit zur Clearingstelle vor der Weiterleitung zur Feuerwehr-Leitstelle
- BMA-Zentraleinheit zum Gebäudemanagementsystem-Sicherheitstechnik
- BMA-Zentraleinheit zur „Externen Sicherheits-Leitstelle"
- Gebäudemanagementsystem-Sicherheitstechnik zur „Externen Sicherheits-Leitstelle"

4.2.1.7.1 **Übersicht der beispielhaften Konzepte für Brandmeldeanlagen und Brandschutzeinrichtungen**

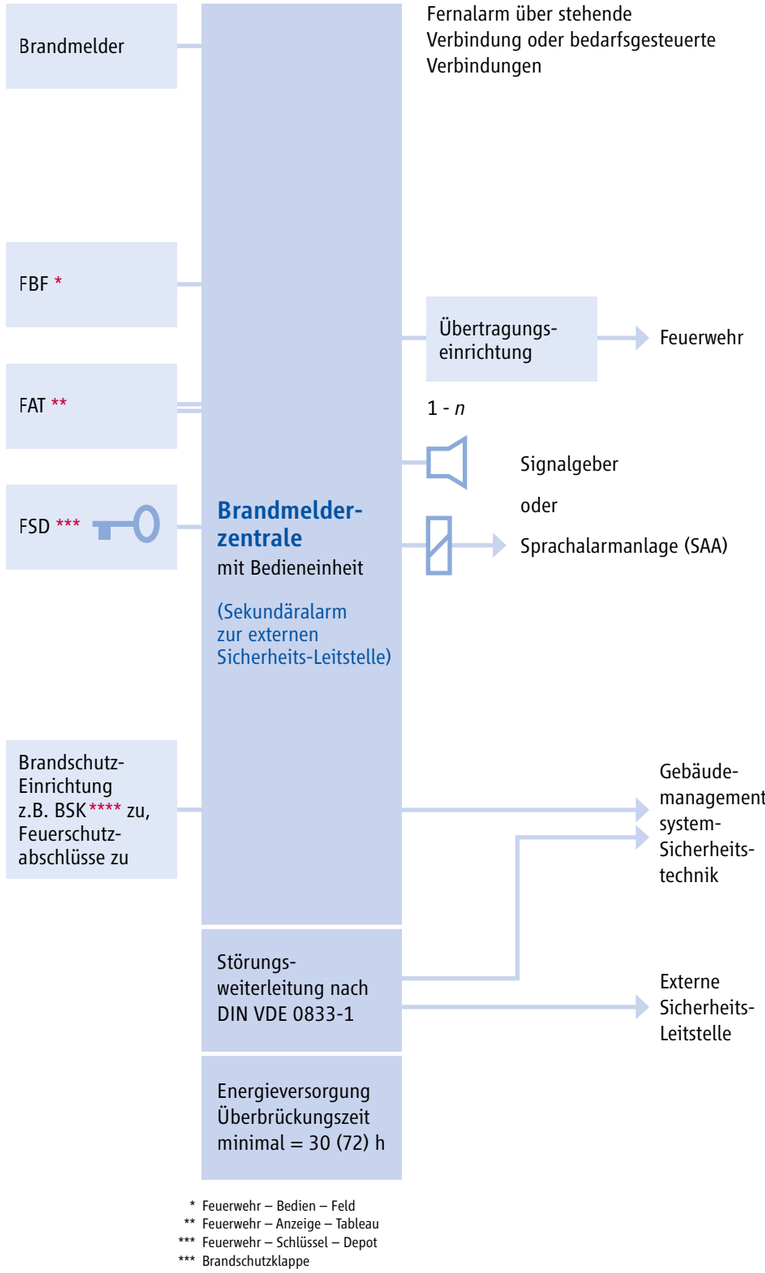
Brandmeldeanlagen (BMA) nach der Norm DIN VDE 0833-1-und-2; DIN 14675; VdS 2095

Brandschutzeinrichtungen nach der Norm DIN VDE 0833 - Teile 1-und-2; DIN 14675; VdS 2095

	BMA nach DIN VDE 0833, Teile 1 und 2 und DIN 14675	BMA nach DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095	Brandschutzeinrichtung nach DIN, BMA mit Löschanlage nach VDE 0833, Teile 1 und 2 und DIN 14675	Brandschutzeinrichtung nach VdS, BMA mit Feuerlöschanlagensteuerung nach DIN VDE 0833, Teile 1 und 2 und DIN 14675 und VdS 2095
Die Brandmeldeanlage entspricht den Normen DIN VDE 0833 Teil 1 und Teil 2, DIN 14675 und ggf. den Richtlinien des Deutschen Institutes für Bautechnik (DIBt).	●			
Die Brandmeldeanlage entspricht den Normen DIN VDE 0833 Teil 1 und Teil 2 sowie DIN 14675, den Richtlinien VdS 2095 und ggf. den Richtlinien des Deutschen Institutes für Bautechnik (DIBt).		●	●	
Die Brandmeldeanlage entspricht den Normen DIN VDE 0833 Teil 1 und Teil 2 sowie DIN 14675, den Richtlinien VdS 2095, VdS 2496 und ggf. den Richtlinien des Deutschen Institutes für Bautechnik (DIBt).				●
Die Brandschutzeinrichtung besteht aus einer Brandmeldeanlage und einer Löschanlage nach DIN und VdS.			●	●
Für Krankenhäuser sollten zusätzlich die Richtlinie VdS 2226 und für Hotel- und Beherbergungsbetriebe die Richtlinie VdS 2082 beachtet werden!	●	●	●	
Entscheidend für den Umfang der BMA ist das Brandschutzkonzept, die Bauauflagen und die Forderungen des Versicherers.	●	●	●	●
Die BMA muss mindestens durch DIN 14675 zertifizierte Fachfirmen geplant, projektiert, installiert, in Betrieb gesetzt, abgenommen und in Stand gehalten werden.	●	●	●	●
Die BMA muss durch DIN 14675 zertifizierte Fachfirmen geplant, projektiert, installiert, in Betrieb gesetzt, abgenommen und in Stand gehalten werden. Ferner muss die Fachfirma die VdS-Errichter-Anerkennung für BMA besitzen.		●	●	●
Das Leitungsnetz muss den Anforderungen der Leitungsanlagen Richtlinie (LAR) entsprechen.	●	●	●	●
Die Brandmeldeanlage hat die Aufgabe, über Brandmelder Gefahren zu erkennen, über eine Zentrale auszuwerten und der Feuerwehr zu signalisieren bzw. weiterzumelden.	●	●	●	●
Sekundäralarme können auf eine externe Sicherheits-Leitstelle aufgeschaltet werden.	●	●	●	●

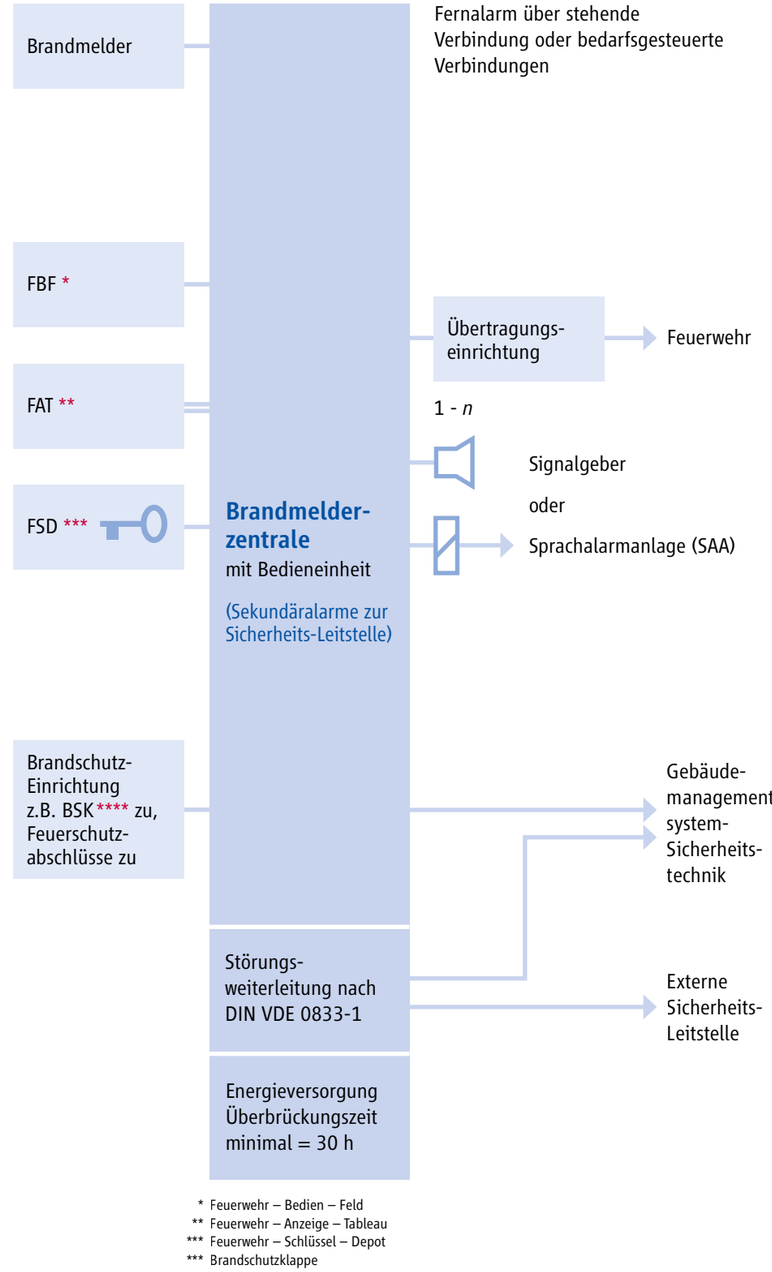
	BMA nach DIN VDE 0833, Teile 1 und 2 und DIN 14675	BMA nach DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095	Brandschutzeinrichtung nach DIN, BMA mit Löschanlage nach VDE 0833, Teile 1 und 2 und DIN 14675	Brandschutzeinrichtung nach VdS, BMA mit Feuerlöschanlagensteuerung nach DIN VDE 0833, Teile 1 und 2 und DIN 14675 und VdS 2095
Die Löschung des Brandes erfolgt von der Löschanlage sofort oder bei Personengefährdung nach Ablauf einer Voralarmierungszeit. Es können weitere Brandmelder außerhalb des Löschbereiches an der BMZ betrieben werden.			●	●
An der Zentrale angeschlossene Brandmelder sind permanent aktiv.	●	●	●	●
Der Betreiber kann einzelne automatische Brandmelder betriebsbedingt (z. B. Schweißarbeiten) abschalten.	●	●	●	●
Es können Handfeuermelder und automatische Brandmelder angeschlossen werden.	●	●	●	●
Über Schnittstellen sind Brandschutzeinrichtungen (z. B. Brandschutzklappen, Löschanlagen, Türfeststellanlagen) anschaltbar.	●	●	●	●
Zur Hilfeleistung wird ein Anschluss über eine Übertragungseinrichtung zur Feuerwehr notwendig.	●	●	●	●
Zur Entgegennahme von Störungsmeldungen nach DIN VDE 0833-1 wird ein Anschluss an eine ständig besetzte Stelle, z. B. eine externe Sicherheits-Leitstelle, empfohlen.	●	●	●	●
Zusätzlich kann der Betreiber durch Klartextmeldungen auf Handy, Pager usw. bestimmte Personen alarmieren lassen.	●	●	●	●
Außerdem muss durch Internalarm (akustische und/oder optische Signalgeber) im Gebäude auf eine Brandmeldung aufmerksam gemacht werden. Diese Alarmierung kann jedoch auch über eine Sprachalarmierungsanlage (SAA) nach DIN VDE 0833-4 durchgeführt werden.	●	●	●	●
Die Technischen Anschlussbedingungen (TAB) der örtlichen Feuerwehr sind zu berücksichtigen.	●	●	●	●
Gemäß DIN VDE 0845-1 bzw. VdS 2833 sind ggf. Überspannungs- und Blitzschutzmaßnahmen zu berücksichtigen.	●	●	●	●
Instandhaltung: BMA müssen nach DIN 14675 instand gehalten werden.	●	●	●	●
Die Instandhaltung muss durch eine nach DIN 14675 zertifizierte Fachfirma erfolgen.	●	●	●	●
• Inspektionsrhythmus • Wartungsrhythmus	4 x jährlich 1 x jährlich	4 x jährlich 1 x jährlich	4 x jährlich 1 x jährlich	4 x jährlich 1 x jährlich

4.2.1.7.1.1 **Beispielhaftes Konzept für eine Brandmeldeanlage nach der Norm DIN VDE 0833, Teile 1 und 2 und DIN 14675**



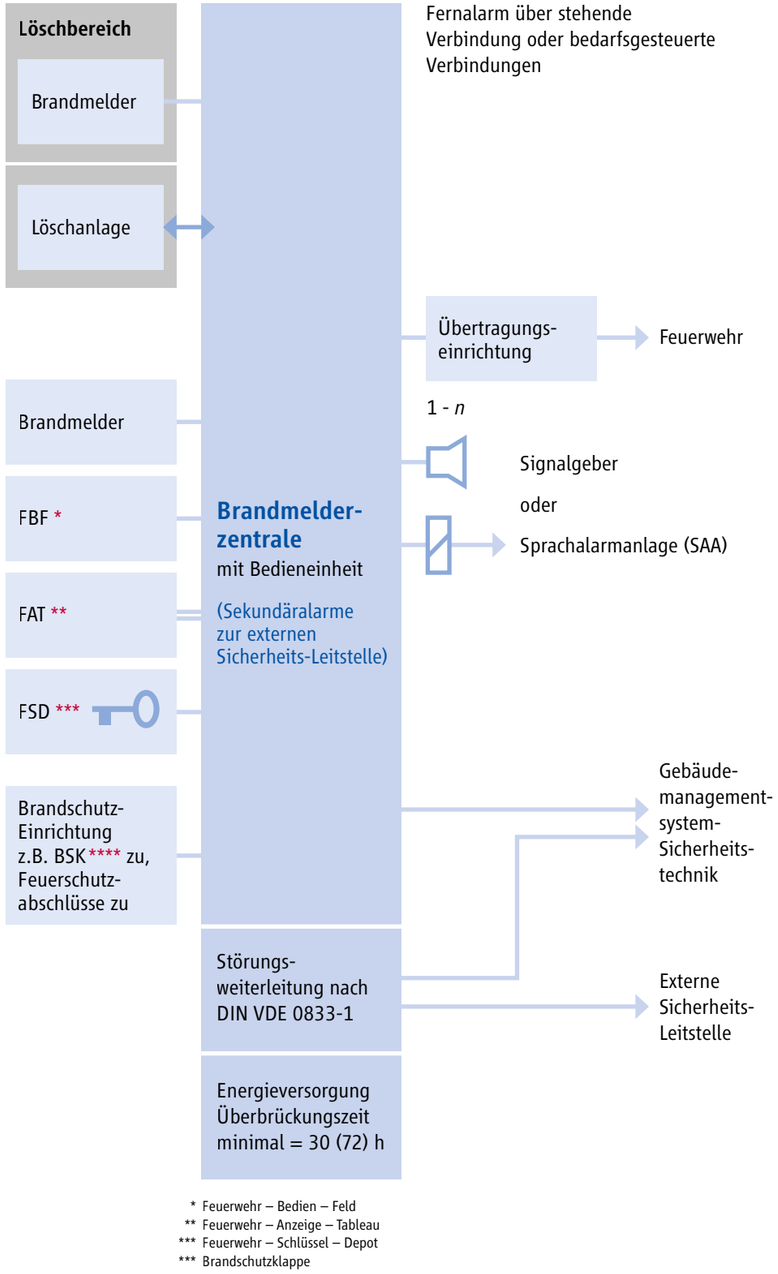
* Feuerwehr – Bedien – Feld
** Feuerwehr – Anzeige – Tableau
*** Feuerwehr – Schlüssel – Depot
*** Brandschutzklappe

4.2.1.7.1.2 **Beispielhaftes Konzept für eine Brandmeldeanlage nach der Norm DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095**



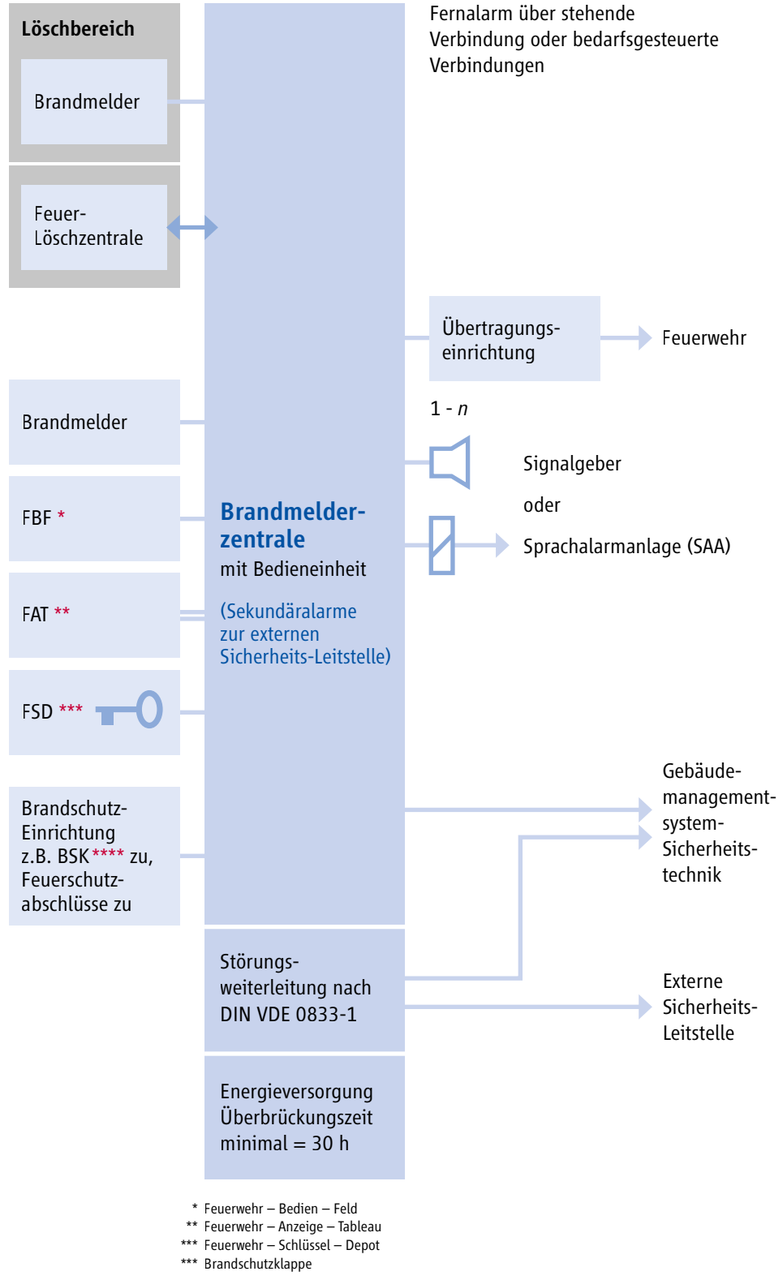
* Feuerwehr – Bedien – Feld
** Feuerwehr – Anzeige – Tableau
*** Feuerwehr – Schlüssel – Depot
*** Brandschutzklappe

4.2.1.7.1.3 **Beispielhaftes Konzept für eine Brandschutzeinrichtung nach DIN - Brandmeldeanlage mit Löschanlage nach der Norm DIN VDE 0833, Teile 1 und 2 und DIN 14675**



* Feuerwehr – Bedien – Feld
** Feuerwehr – Anzeige – Tableau
*** Feuerwehr – Schlüssel – Depot
*** Brandschutzklappe

4.2.1.7.1.4 **Beispielhaftes Konzept für eine Brandschutzeinrichtung nach VdS - Brandmeldeanlage mit Feuerlöschanlagenansteuerung nach der Norm DIN VDE 0833, Teile 1 und 2, DIN 14675 und VdS 2095**



* Feuerwehr – Bedien – Feld
** Feuerwehr – Anzeige – Tableau
*** Feuerwehr – Schlüssel – Depot
*** Brandschutzklappe

4.2.1.8 Beispielhaftes Planungsschema für Brandmeldeanlagen (BMA)

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Aufgabenstellung	individuell durch den Auftraggeber, z. B. durch den/die • Fachplaner • Bauabteilung • Betreiber
BMA-Schutzziele nach der DIN 14675-Ausgabe April 2012 – Brandmeldeanlagen-Aufbau und Betrieb – Ziff. 5 Konzept für BMA – Ziff. 5.1 Schutzziele	Schutz, u. a. vor • Entdecken von Bränden in der Entstehungsphase • schnelle Information und Alarmierung der betroffenen Menschen • Automatische Ansteuerung von Brandschutz- und Betriebseinrichtungen • Schnelle Alarmierung der Feuerwehr und/oder anderer hilfeleistender Stellen • Eindeutiges Lokalisieren des Gefahrenbereiches und dessen Anzeige
Erfassungsebene – Auswahl der Sensorik (Melder) (abhängig von den Schutzzielen)	Mögliche in Betracht kommende Melder, u. a. • Automatische Brandmelder • Handfeuermelder • Ansaugrauchmelder • Feuermelder • Wärmemelder
Übertragungsweg von der Erfassungsebene zur Zentralenebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze - des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Zentralenebene	Auswahl der passenden Brandmelderzentrale mit den dazu passenden Zentralenkomponenten, wie z. B. der • Energieversorgung • Batterien • Anzeigetableaus • Internen und externen Signalgeber • Feuerwehreinrichtungen • Türsteuereinrichtungen • Übertragungsmedien
Schnittstellen zu anderen Gefahrenmeldeanlagen und zum Gebäudemanagementsystem-Sicherheitstechnik	Möglich sind Schnittstellen u.a. zu/zum • Überfall-/Einbruchmeldeanlagen • Zutrittskontrollanlagen • Sprachalarmanlagen • Fluchtwegssteuerung • Gebäudemanagementsystem-Sicherheitstechnik • Rauch- und Wärmeabzugsanlagen
Übertragungsweg von der Zentralenebene zum Gebäudemanagementsystem	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Gebäudemanagementsystem	Auslegung entsprechend der vorgenannten definierten Anforderungen
Übertragungsweg vom Gebäudemanagementsystem zur Sicherheitsleitstelle und zur Rückfallebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Sicherheitsleitstelle	Auslegung entsprechend der vorgenannten definierten Anforderungen

4.2.1.9 **Beispielhafte Funktionen und Anschaltungen einer Brandmeldeanlage (BMA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle**

Pos.	Kriterien	Alarm-Funktion (von Meldern)	Überwachungs-Funktion	Service-Funktion	an/von die BMA-Zentrale	an/für die Feuerwehr	an GMS	a.d. Sicherheits-Leitstelle
1.	**Meldergruppen für**							
1.1	**Automatische Brandmelder**							
1.1.1	Rauchmelder	●	●		●	●	●	●
1.1.2	Wärmemelder	●	●		●	●	●	●
1.1.3	Flammenmelder	●	●		●	●	●	●
1.2	**Sondermelder**							
1.2.1	Ansaugrauchmelder	●	●		●	●	●	●
1.2.2	Lineare Wärmemelder	●	●		●	●	●	●
1.2.3	Lineare Rauchmelder	●	●		●	●	●	●
1.3	**Manuelle Melder**							
1.3.1	Handfeuermelder	●	●		●	●	●	●
	Hinweis: Der Brand-Hauptalarm wird direkt zur Feuerwehr geschaltet - der Sekundäralarm kann zur externen Sicherheits-Leitstelle übertragen werden							
1.8	Eines oder mehrere abgesetzte Feuerwehr-Bedienfelder (FBF) nach DIN 14661				●			
1.9	Abgesetzter Feuerwehr-Anzeigetableaus (FAT) nach DIN 14662				●			
2.	**Feuerwehrtechnische Anforderungen, u.a.**							
2.1	Rundumkennleuchte				●	●		
2.2	Signalgeber zur Gebäude-Identifikation (BEGA- oder Blitzleuchte)							
2.3	Lageplantableau (wenn gefordert)				●	●		
2.4	Etagen - Lageplantableaus (wenn gefordert)				●	●		
2.5	Feuerwehr-Informationsstelle					●		
2.6	Feuerwehr-Laufkarten					●		
2.7	Feuerwehr-Einsatzpläne					●		
3.	**Anschaltung, u. a.**							
3.1	Akustische Signalgeber				●			
3.2	Optische Signalgeber				●			
3.3	Feuerwehr-Schlüsseldepots (FSD)				●			
3.4	Freischaltelement (FSE)	●			●	●		
3.5	Feststellanlagen (autarke Systeme vor Ort)						●	
3.6	Feststellanlagen (angesteuert durch die Brandmelderzentrale)				●			
3.7	Alarmierung an eine oder mehrere interne oder externe Hilfe leistende Stellen				●		●	●
3.8	Übertragungseinrichtung (ÜE) zur Feuerwehr gemäß DIN 14675, Anhang A				●	●		
4.	**Fernservice gemäß DIN VDE 0833-1**							
4.1	Fernabfrage			●	●			
4.2	Fernsteuern			●	●			
4.3	Fernreparatur			●	●			
4.4	Fernparametrierung			●	●			

Pos.	Kriterien	Alarm-Funktion (von Meldern)	Überwachungs-Funktion	Service-Funktion	an/von die BMA-Zentrale	an/für die Feuerwehr	an GMS	a.d. Sicherheits-Leitstelle
5.	**Mögliche Überwachungsfunktionen, u.a.**							
5.1	Netz- und Batterieüberwachung		●		●		●	
5.2	Ring- und Stichleitungsüberwachung		●		●		●	
5.3	Meldergruppenüberwachung		●		●		●	
5.4	Einzelmelderüberwachung		●		●		●	
5.5	Prozessorüberwachung		●		●		●	
5.6	Speicherüberwachung		●		●		●	
5.7	Erdschlussüberwachung		●		●		●	
5.8	System-Störmeldungen generell		●		●		●	
5.9	Rück- und Zustandsmeldungen		●		●		●	
6.	**Mögliche Ansteuerungen aus der Brandmelderzentrale (BMZ), u. a.**							
6.1	Ansteuerung von Sprachalarmanlagen (SAA)				●		●	
6.2	Ansteuerung von Lüftungsanlagen im Brandfall				●		●	
6.3	Abschaltungen der Lüftungsanlagen im Brandfall				●		●	
6.4	Abluftbetrieb der Lüftungsanlagen im Brandfall				●		●	
6.5	Brandfallsteuerungen				●		●	
6.6	Brandschutzklappen				●		●	
6.7	Entrauchungsklappen mit Entlüftungsfunktion				●		●	
6.8	Entrauchungsanlagen				●		●	
6.9	Rauch- und Wärmeabzugsanlagen				●		●	
6.10	Einbruchmeldeanlagen und Videoüberwachungsanlagen				●		●	
6.11	Scharf-/Unscharfschaltung von Sicherungsbereichen im Brandfall				●		●	
6.12	Zutrittskontrollanlagen				●		●	
6.13	Aufzüge und Fahrtreppen				●		●	
6.14	**Ansteuerung von Feuerlöschanlagen (z. B. Gas, Wasser, Schaum, Pulver)**				●		●	
6.15	**Ansteuerung von Gefahren-Informations-systemen**							
6.15.1	Fluchtwegsteuerungen				●		●	
6.15.2	Dynamische Rettungswegbeschilderung				●		●	
6.15.3	Optische Führung durch Blitzleuchten				●		●	
6.15.4	Akustischen Führungen durch Signalgeber				●		●	
6.15.5	Kommunikationsanlagen (TK; SMS; ….)				●		●	
6.16	**Abschaltungen, u.a.**							
6.16.1	Elektroverteiler				●		●	
6.16.2	Niederspannungs- und Mittelspannungsschaltanlagen und Transformatoren				●		●	
6.16.3	Schalt- und Steuerschränke				●		●	
6.16.4	Server-/IT-Schränke, IT-Systemeinheiten oder komplette Rechenzentren				●		●	
6.16.5	Aufzügen und Fahrtreppen				●		●	
6.16.6	Photovoltaik-Anlagen					●	●	
6.16.7	Pumpen und Tankanlagen							
7.	**Service- und Instandhaltungsintervalle sind in den Normen DIN VDE 0833 und DIN 14675 in der jeweils gültigen Ausgabe aufgeführt, u. a.**							
7.1	Inspektion: 1/4-jährlich				●		●	
7.2	Begehung: 1/4-jährlich				●		●	
7.3	Wartung: 1 x-jährlich				●		●	

4.2.2 Sprachalarmanlagen (SAA) /Elektroakustische Notfallwarnsysteme (ENS)

4.2.2.1 Funktionale Beschreibung

4.2.2.1.1 Definition Sprachalarmanlagen (SAA)

SAA generieren gespeicherte oder Live-Durchsagen, die der Alarmierung und der Information der von Brandgefahren betroffenen Personen dienen. Eine SAA im Sinne der Norm DIN VDE 0833-4 Norm muss aus Komponenten bestehen, die den Normen der Reihe DIN EN 54, soweit vorhanden, entsprechen. Das funktionsmäßige Zusammenwirken dieser Komponenten muss sichergestellt sein.

Sprachalarmanlagen sind ein fester Bestandteil der Brandmeldeanlagen. Sie werden im Brandfall automatisch aktiviert. Seit September 2007 ist in Deutschland eine entsprechende Anwendungsnorm in Kraft. Die Systeme übermitteln Durchsagen in hoher Qualität über Lautsprecher, können Personen gezielt warnen und auf eine mögliche Evakuierung vorbereiten. Konventionelle Alarmierungsmittel wie Signalgeber, Hupen oder Sirenen können zwar Aufmerksamkeit wecken, aber nicht über die konkrete Gefahr informieren und notwendige Handlungsanweisungen geben. Dadurch können Menschen in Panik geraten, weil sie nicht wissen, wie sie sich verhalten sollen.

Sprachalarmanlagen vermeiden das Auftreten einer solchen Situation. Mit einer Sprachdurchsage werden klare Anweisungen zum richtigen Verhalten im Brandfall vermittelt. Rettungskräfte können Personen, die sich noch in Gebäuden aufhalten, gezielt über Fluchtwege oder andere Maßnahmen informieren. Alle Komponenten einer Sprachalarmanlage, wie die Zentrale und die verwendeten Lautsprecher, unterliegen Normen und Vorschriften, die eine hohe Qualität garantieren. Die Alarmierungsdurchsagen können bei Bedarf auch in mehreren Sprachen erfolgen. Zudem stehen die Systeme für alltägliche Durchsagen und Musikübertragung zur Verfügung.

4.2.2.1.2 Definition Elektroakustische Notfallwarnsysteme (ENS)

Elektroakustische Notfallwarnsysteme übertragen Signale und Sprachdurchsagen über Lautsprecher. Diese Informationen werden im Notfall durch eine ständig besetzte Stelle ausgelöst. Nach dem Ertönen des Alarmsignals wird eine gespeicherte oder eine Live-Durchsage übertragen. Diese Durchsagen führen sicher über die Fluchtwege aus dem zu evakuierenden Gebäude. In Abhängigkeit von der Gebäudenutzung können sie auch mehrsprachig sein. Optische Anzeigeelemente erleichtern die Orientierung.
Um Paniksituationen aufgrund hoher Personenzahlen auf Fluren und in Treppenhäusern vorzubeugen, empfiehlt sich eine stufenweise Evakuierung. Hierbei werden zuerst besonders gefährdete Gebäudeteile oder -bereiche geräumt. Über Live-Durchsagen mittels Notfallmikrofon können die Rettungskräfte direkt eingreifen, was eine gezielte Räumung erleichtert. Die Betroffenen werden aufgefordert, sich nach den entsprechenden Anweisungen der Rettungskräfte zu verhalten. Elektroakustische Notfallwarnsysteme sind vor allem in öffentlichen Gebäuden sowie an öffentlichen Plätzen mit hohen Besucherzahlen, z. B. auf Flughäfen und Bahnhöfen, in Einkaufszentren, Hotels, Krankenhäusern, Bürogebäuden oder im Sport- und Kulturbereich, im Einsatz.

Alle anderen elektroakustischen Anlagen werden als Beschallungsanlagen bezeichnet. Sie dienen zur Übertragung von Musik und Sprache in geschlossenen Räumen und im Freien. Aufbau und Betrieb unterliegen keinen Normen oder anderen Vorschriften, abgesehen vom Einsatz auf Schiffen, wo eine GL-Zulassung des Germanischen Lloyd erforderlich ist.

4.2.2.4 Sprachalarmanlagen (SAA) / Elektroakustische Notfallwarnsysteme (ENS)

- Sprachalarmierung im Brandfall nach der Norm DIN VDE 0833 - Teil 4
- Elektroakustische Notfallwarnsysteme nach der Norm DIN EN 50849 (Entwurf)

Anschaltung der SAA-/ENS-Zentraleinheit an

Gebäudemanagementsystem-Sicherheitstechnik

Externe Sicherheits-Leitstelle

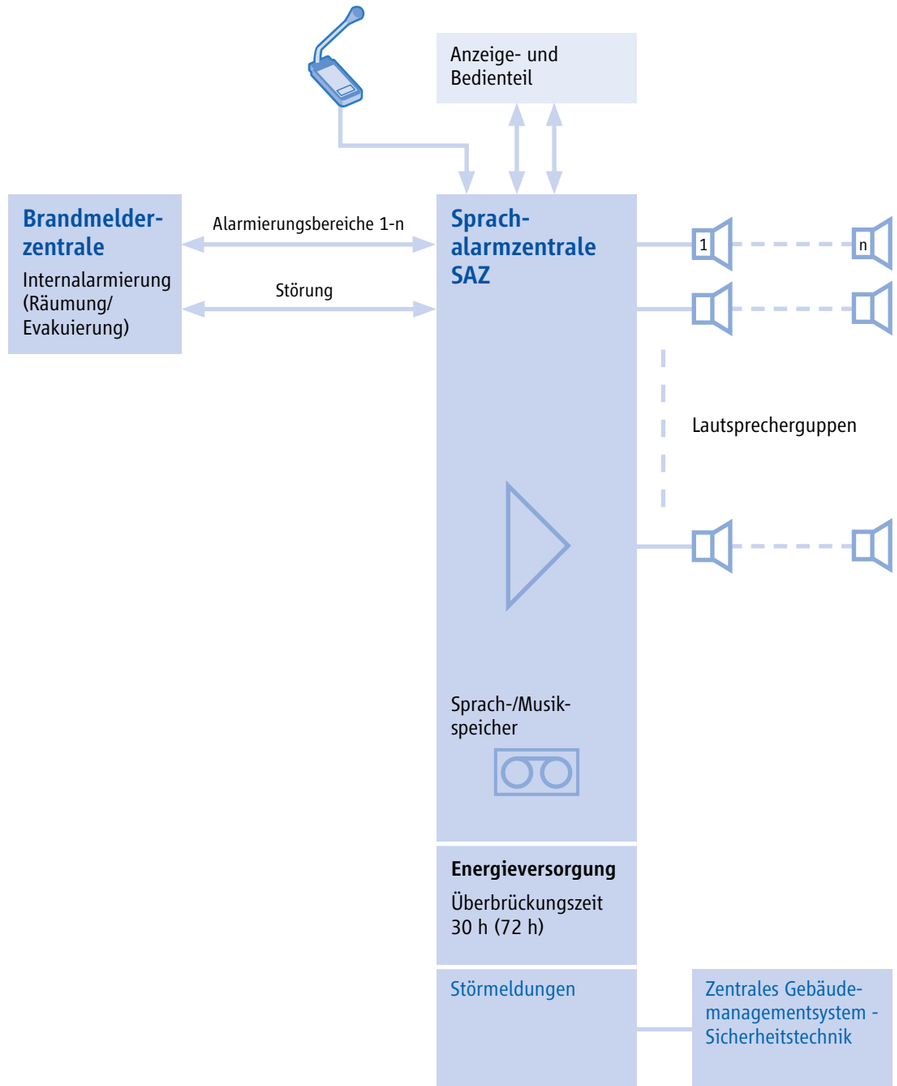
Nachfolgende Übertragungswege sind bei der (IP-)Vernetzung erforderlich:
- Lautsprecherkreise für SAA/ENS zur SAA-/ENS-Zentraleinheit
- SAA-/ENS-Zentraleinheit zum Gebäudemanagementsystem-Sicherheitstechnik
- SAA-/ENS-Zentraleinheit zur Externen Sicherheits-Leitstelle (für Störmeldungen)
- Gebäudemanagementsystem-Sicherheitstechnik - zur Externen Sicherheits-Leitstelle

4.2.2.4.1 Übersicht der Konzepte für Sprachalarmanlagen (SAA) im Brandfall nach der Norm DIN VDE 0833 - Teil 4 / Elektroakustische Notfallwarnsysteme (ENS) nach der Norm DIN EN 50849 (Entwurf)

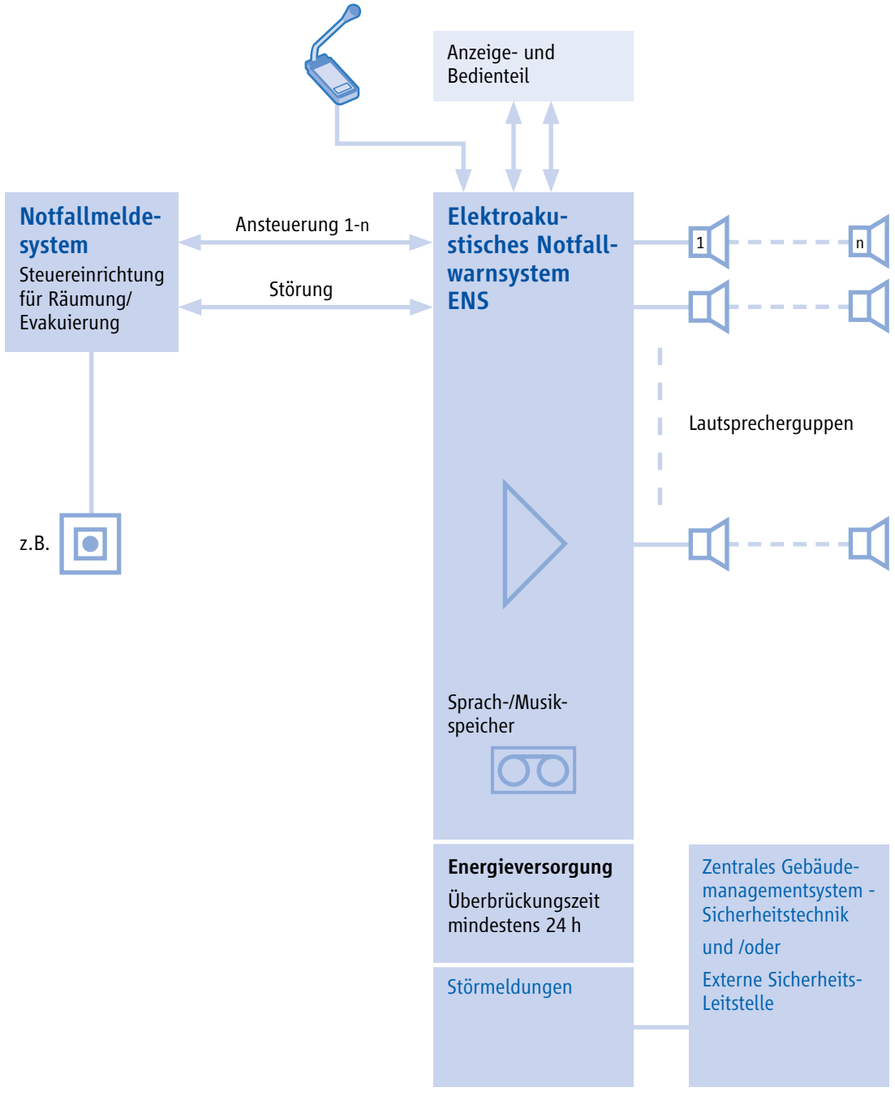
	SAA im Brandfall nach DIN VDE 0833 - Teil 4	ENS nach DIN EN 50849 (Entwurf)
Das Elektroakustische Notfallwarnsystem (ENS) entspricht der DIN EN 50849 (Entwurf).		●
Die Sprachalarmierung im Brandfall (SAA) entspricht der DIN VDE 0833-4.	●	
Elektroakustische Notfallwarnsysteme (ENS) werden in Notfallsituationen eingesetzt, um Personen, die sich in einem Bereich innerhalb oder außerhalb eines Gebäudes aufhalten, zu veranlassen, diesen Bereich schnell und geordnet zu räumen.		●
Die SAA dient der Alarmierung, Information, zur Erteilung von Anweisungen an Beschäftigte und Besucher und/oder der Führung von Personen aus der Gefahrenzone in einem Brandfall.	●	
Mit dem Auftraggeber/Betreiber und mit den zuständigen Stellen muss eine von drei Sicherheitsstufen für die Ausfallsicherheit der Sprachalarmanlage, entsprechend der Gebäudenutzung, festgelegt werden.	●	
Es müssen verständliche Informationen über Maßnahmen verbreitet werden können, die zum Schutz von Menschenleben innerhalb eines oder mehrerer Bereiche vorzunehmen sind.		●
Der Raum für die SAA/ENS muss sauber, trocken und klimatisiert sein und eine geringe Brandlast aufweisen.	●	●
Der Raum in F30-Qualität für die Sprachalarmzentrale (SAZ)/ ENS-Zentrale muss sauber, trocken und klimatisiert sein und eine geringe Brandlast aufweisen.	●	●
Die Ansteuerung der SAA/ENS durch ein Notfallmeldesystem muss über überwachte Übertragungswege erfolgen.	●	●
Die Ansteuerung der SAA durch eine Brandmelderzentrale (BMZ) muss über überwachte Übertragungswege erfolgen.	●	
Die Störungsmeldung der SAA/ENS an das Notfallmeldesystem muss über überwachte Übertragungswege an ein zentrales Gebäudemanagementsystem-Sicherheitstechnik und/oder an eine externe Sicherheits-Leitstelle erfolgen.	●	●
Die Störungsmeldung der SAA an die BMZ muss über überwachte Übertragungswege erfolgen. Zusätzlich kann die Störungsmeldung an ein zentrales Gebäudemanagementsystem-Sicherheitstechnik und/oder an eine externe Sicherheits-Leitstelle erfolgen.	●	
Die Übertragungswege zwischen Lautsprechern, Brandfallmikrofon und Zentrale müssen überwacht werden.	●	●
Leitungen sind grundsätzlich betriebssicher und wenn gefordert in Funktionserhalt F30 zu verlegen.	●	●
Eine Lautsprechergruppe darf einen Bereich von max. 1.600 m² beschallen und dabei einen Brandabschnitt nicht überschreiten.	●	

	SAA im Brandfall nach DIN VDE 0833 - Teil 4	ENS nach DIN EN 50849 (Entwurf)
Der Ausfall eines einzelnen Verstärkers oder Lautsprecher-stromkreises darf nicht zu einem vollständigen Ausfall des Alarmierungsbereiches führen.		●
Wenn ein Brandfallmikrofon für die Feuerwehr vorhanden ist, muss es sich neben der BMZ bzw. am Feuerwehr-Hauptzugang befinden. Es muss an einem für Unbefugte unzugänglichem Ort angeordnet werden.	●	●
Gemäß DIN VDE 0845-1 sind ggf. Überspannungs- und Blitz-schutzmaßnahmen zu berücksichtigen.	●	●
Das Konzept ENS (S2) ersetzt in keinem Fall das Konzept SAA (S4) Sprachalarmierung im Brandfall, da eine ENS nicht der DIN EN 54 entspricht.		●
Instandhaltung ENS müssen gemäß DIN VDE 0833-4 durch eine Elektrofachkraft für GMA nach DIN VDE 0833-1 instandgehalten werden: Inspektionsrhythmus Wartungsrhythmus	●	 2 x jährlich 1 x jährlich
Instandhaltung SAA müssen gemäß DIN VDE 0833-1 durch eine Elektrofachkraft für GMA instand gehalten werden: Inspektionsrhythmus Wartungsrhythmus Begehung	 4 x jährlich 1 x jährlich 4 x jährlich	●

4.2.2.4.1.1 **Beispielhaftes Konzept für Sprachalarmanlagen (SAA) im Brandfall nach der Norm DIN VDE 0833 - Teil 4**



4.2.2.4.1.2 **Beispielhaftes Konzept für Elektroakustische Notfallwarnsysteme (ENS) nach der Norm DIN EN 50849 (Entwurf)**



4.2.2.5 **Beispielhaftes Planungsschema für Sprachalarmanlagen (SAA) nach der Norm DIN VDE 0833-4/Elektroakustische Notfallwarnsysteme nach der Norm DIN EN 50849 (Entwurf)**

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Aufgabenstellung	Individuell durch den Auftraggeber, z. B. durch den Fachplaner, die Bauabteilung oder den Betreiber
Beispielhafte Schutzziele des Auftraggebers nach der VDE 0833-4/2013-10	Mit der Sprachalarmanlage (SAA) müssen mindestens folgende Schutzziele erreicht werden: • Schnelle Information und Alarmierung der betroffenen Menschen • Schnelle Alarmierung des Betriebspersonals
Lautsprecherebene	Mögliche in Betracht kommende Lautsprecher, u. a. • Gehäuse-Lautsprecher • Tonsäulen • Decken-Lautsprecher • Sound-Projektoren • Hornlautsprecher
Übertragungsweg von der Lautsprecher-ebene zur Zentralenebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Sprachalarm-Zentralenebene	Auswahl der passenden Zentraleneinheit mit den dazu passenden Zentralenkomponenten, wie z. B. der • Verstärkereinheiten • Energieversorgung • Basissprechstelle mit den dazugehörigen Mikrofon-Einheiten • Sprechstellentastatur
Schnittstellen zu anderen Gefahren-meldeanlagen und zum Gebäude-managementsystem-Sicherheitstechnik Vom Elektroakustischen Notfallwarnsystem (ENS) besteht in der Regel keine Schnittstelle zur Brandmeldeanlage	Möglich sind Schnittstellen u.a. zu /zum • Überfall-/Einbruchmeldeanlagen • Videoüberwachungsanlagen • Zutrittskontrollanlagen • Brandmeldeanlagen • Gebäudemanagementsystem-Sicherheits-technik
Gebäudemanagementsystem	Auslegung entsprechend der vorgenannten definierten Anforderungen
Übertragungsweg vom Gebäude-managementsystem zur Sicherheitsleitstelle und zur Ausfallebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungs-netze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Sicherheitsleitstelle	Auslegung entsprechend der vorgenannten definierten Anforderungen

4.2.3 Rauch- und Wärmeabzugsanlagen (RWA)

4.2.3.1 Funktionale Beschreibung

Die Erfahrung lehrt: „Alles was brennbar ist, hat schon gebrannt und wird auch wieder brennen." Ein Brand stellt also ein permanentes Risiko dar. Nur ein wirksamer Brandschutz macht dieses Risiko beherrschbar. Dabei werden die Begriffe „abwehrender" und „vorbeugender" Brandschutz unterschieden:

4.2.3.1.1 Abwehrender Brandschutz

Unter dem Begriff „Abwehrender Brandschutz" werden alle Maßnahmen zusammengefasst, die im Falle eines Brandes die Gefahren für Leben, Gesundheit sowie Sachen bekämpfen. Gemeint ist damit die Brandbekämpfung durch die öffentliche oder betriebliche Feuerwehr.

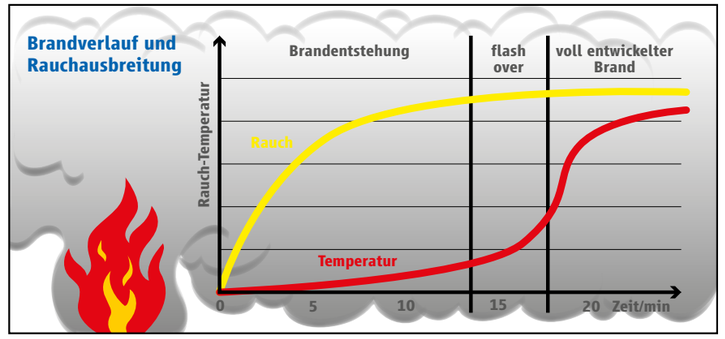
4.2.3.1.2 Vorbeugender Brandschutz

Dieser Bereich umfasst alle Maßnahmen, die den Ausbruch und die Ausbreitung eines Brandes verhindern und Rettungswege frei halten. Ziel ist es, der Ausbreitung im Falle eines Brandes zeitlich solange entgegenzuwirken, dass Personen sich selbst in Sicherheit bringen können und gleichzeitig den Feuerwehren zu ermöglichen, wirksame Rettungs- und Löscharbeiten vornehmen zu können.

Beispiele:
- baulich: Feuerwiderstandsfähige Wände und Decken, bauliche Rettungswege
- anlagentechnisch: Rauchableitung und -abzug, Sprinkleranlage, Brandmeldeanlage
- organisatorisch: Kennzeichnung der Rettungswege und Löschgeräte, Alarmpläne

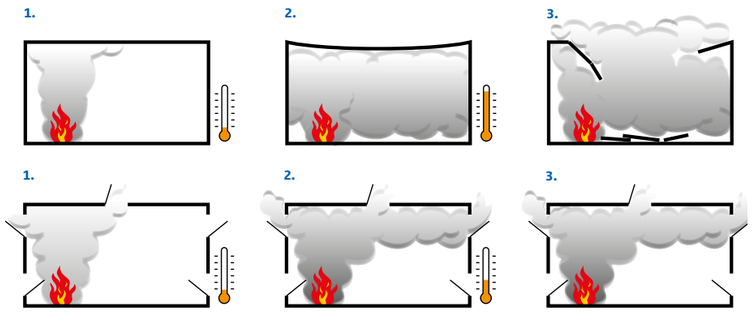
Der Rauch- und Wärmeabzug fällt in den Bereich „Vorbeugender Brandschutz" und kann im Falle eines Brandes Leben retten, da die Fluchtwege raucharm gehalten werden.

Bei einem Brand entstehen erhebliche Mengen an Verbrennungsprodukten wie Rauch- und Brandgasen sowie Wärmeenergie. Die wichtigste Aufgabe einer Rauch- und Wärmeabzugsanlage (RWA) ist es, die entstandenen Verbrennungsprodukte effektiv und schnell aus dem Gebäude abzuführen. Räume und Gebäude ohne RWA werden binnen kürzester Zeit vollständig mit toxisch wirkenden Rauchgasen ausgefüllt. Die Gefahr für Flüchtende und das Rettungspersonal steigt erheblich in diesen Gebäuden, da es durch fehlenden Rauch- und Wärmeabzug zum unkontrollierten Vollbrand kommt und die undurchsichtige Rauchschicht eine aktive und passive Rettung unmöglich macht.



Brandopfer als Folge eines direkten Kontaktes mit dem Feuer treten nur selten auf; fast 90 % aller tödlichen Brandunfälle sind auf Ersticken durch Rauchgase zurückzuführen. „Brandtote sind Rauchtote" – dafür gibt es zwei Gründe:

- Tödlich wirkende Bestandteile im Rauchgas
- Korrosiv wirkende Bestandteile, die Lunge und Atemwege beim Einatmen verätzen



Brandverlauf ohne und mit Rauch- und Wärmeabzugsanlage

Große Rauchgasmengen steigen bedingt durch den thermischen Auftrieb auf und füllen den Raum oder das Gebäude mit Rauch aus. Die hohe Umgebungstemperatur kann im schlimmsten Fall zum Einsturz des Gebäudes führen.

Die Erhaltung der Gebäudekonstruktion ist daher auch eine wesentliche Aufgabe der Rauch und Wärmeabzugsanlage. So können sich flüchtende Personen durch eigene Kraft aus dem Gebäude retten und das Rettungspersonal kann die aktive Rettung – die Evakuierung des Gebäudes – länger durchführen.

Zusammenfassend werden folgende Ziele durch den Einsatz von RWA in Gebäuden erreicht:

Personenschutz: Rauchfreihaltung von Rettungswegen	**Umweltschutz:** Verminderung der Umweltschäden	**Sachwerteschutz:** Erhaltung der Bausubstanz
• Aktive Rettung • Passive Rettung • Lokalisierung des Brandes	• Minimaler Löschmitteleinsatz	• Unterstützung des Löschangriffs • Ventilierung des Brandes • Minimierung der thermischen Belastung • Minimierung der Löschschäden

Um den Rauch und die Wärme aus dem Gebäude abzuführen, gibt es unterschiedliche Möglichkeiten:

- Natürliche Rauchabzugsanlagen (NRA)
- Maschinelle Rauchabzugsanlagen (MRA)

4.2.3.2 Wirkungsweise eines natürlichen Rauch- und Wärmeabzugs

Im Falle eines Brandes werden Öffnungen im oberen Bereich des Gebäudes geöffnet. Durch diese Öffnungen können dann die heißen aufsteigenden Rauchgase bereits in der Entstehungsphase entweichen. Die notwendigen Zuluftöffnungen im unteren Bereich des Gebäudes unterstützen diesen Vorgang durch den Ausgleich des erforderlichen Massenstroms.

Man unterscheidet zwischen zwei Prinzipien:

4.2.3.2.1 Prinzip der Verdünnung

Durch Öffnungen im oberen Teil des Raumes kann der Rauch entweichen. Zufuhr von Luft, z. B. durch Druckbelüftungsgeräte der Feuerwehr, unterstützt den Vorgang.
Die turbulente Luftzufuhr führt zu einer Verteilung, Verdrängung und Verdünnung der Brandgase.

Das sind z. B. Rauchabzüge in notwendigen Treppenhäusern oder eine Rauchableitung in kleineren Brandabschnitten

- Eine Rauchableitung wird meist auch als Kalt-Entrauchung definiert, die nach einem Feuer zur Entfernung des im Gebäude verbliebenen Rauches eingesetzt wird.
- Bei der Rauchableitung handelt es sich z. B. in Deutschland um ein nicht sicherheitsrelevantes Bauprodukt, es wird aus diesem Grund in der Liste C der Bauregelliste aufgeführt.

4.2.3.2.2 Prinzip der Schichtenbildung

Öffnungen zum Rauchabzug und Öffnungen für die Zuluftnachströmung sorgen aufgrund des natürlich wirkenden thermischen Auftriebsprinzips für zwei horizontale Schichten: Eine an der Decke anliegende Schicht heißer Brandgase und eine darunter liegende raucharme Schicht bestehend aus der Umgebungsluft und der nachströmenden kalten Zuluft.

4.2.3.3 Natürlicher Rauchabzug

- Unter Rauchabzug versteht man die Warm-Entrauchung: der Rauch muss schon während eines Feuers aus Flucht- und Rettungswegen abziehen.
- Beim Rauchabzug handelt es sich um das sicherheitsrelevante Bauprodukt „natürliches Rauch- und Wärmeabzugs-Gerät“ (NRWG), das nach EN 12101-2 (DIN EN 12101-2) „Natürliche Rauch- und Wärmeabzugsgeräte“ geprüft sein muss. Gemäß europäischer Norm besteht dieses geregelte Bauprodukt aus
  - einem Fenster mit den dazugehörigen Bestandteilen (Profile, Dichtungen, Beschläge),
  - der Ausfachung (Gläser, Paneele etc.)
  - und dem Antriebssystem mit den dazugehörigen Bestandteilen (Antrieb, Konsolen, Beschläge).

In Deutschland wird das NRWG in der Liste B der Bauregelliste geführt und muss als geprüftes und CE-gekennzeichnetes Bauprodukt eingebaut werden:

- wenn bauordnungsrechtlich eine “Rauch- und Wärmeabzugsanlage“ gefordert ist,
- wenn durch Baubehörden im Brandschutzkonzept im Rahmen einer Baugenehmigung gefordert ist,
- oder wenn das NRWG explizit gefordert wird.

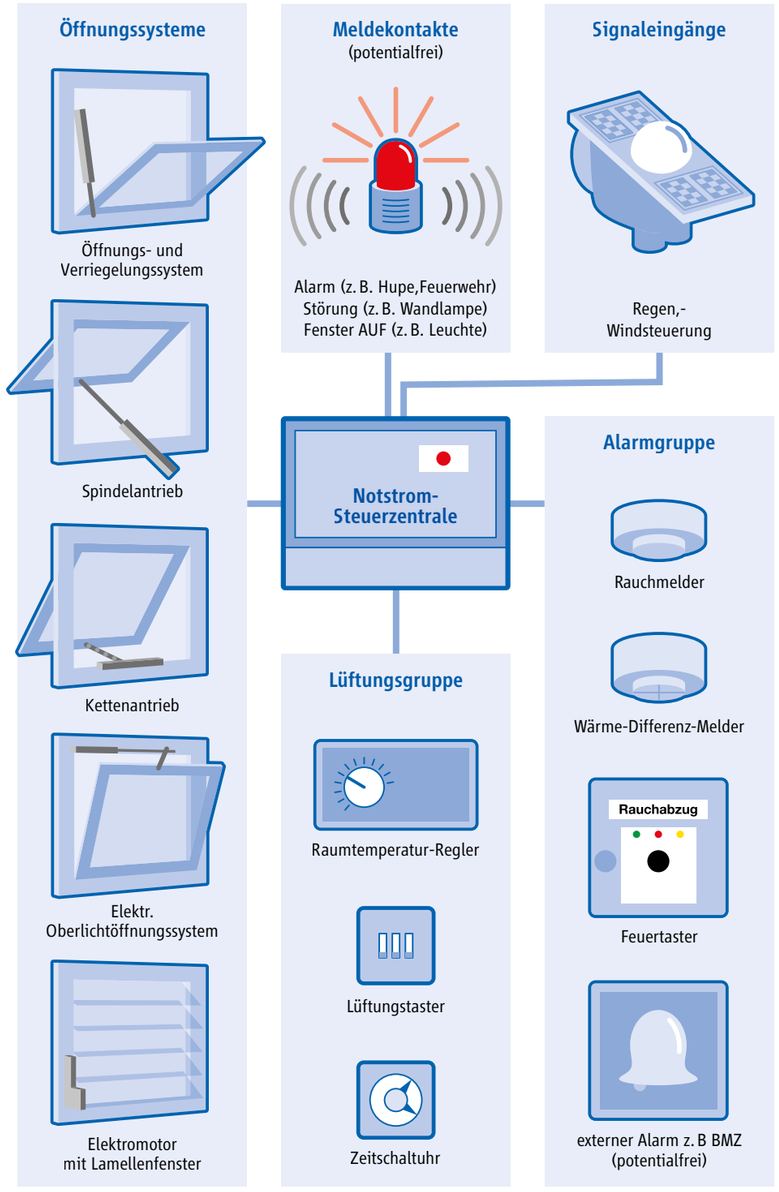
Die Planung und Auslegung der kompletten RWA-Anlage mit Dimensionierung und Einbau von Zuluft und Rauchabzug (NRWG) ist in der DIN 18232-2 „Rauchabzugsanlagen“ geregelt.

4.2.3.4 Planung und Auslegung

Vor allem die Planung und Auslegung von Rauch- und Wärmeabzugsanlagen unterliegen einer Vielzahl von europäischen, nationalen und regionalen Vorgaben. Sie sollte darum immer in Abstimmung mit der örtlichen Brandschutzbehörde stattfinden. Die Anforderungen an eine RWA sind durch einen Brandschutzplaner im Brandschutzkonzept und Brandschutzgutachten eines Bauobjekts definiert.

4.2.3.5 RWA-Systeme

Komponenten einer Rauch- und Wärmeabzugsanlage und Systemaufbau



Für RWA-Anlagen sind folgende Öffnungselemente denkbar:

- elektromotorische Antriebe
- vorgespannte Systeme, die z. B. über einen Elektromagneten gehalten werden
- pneumatische Systeme, z. B. mit Auslösung über CO_2-Patronen
- Pyrotechnisch ausgelöste Öffnung

Das Steuerungssystem einer elektrischen RWA besteht im Wesentlichen aus den Teilkomponenten, welche in der Systemdarstellung unten ersichtlich sind.

Das System deckt zwei große Aufgabenkreise ab: den Alarmfall und den täglichen Lüftungsfall.

4.2.3.5.1 Situation in Deutschland

Ob in einem Objekt eine RWA mit NRWG oder mit Rauchableitungen eingesetzt werden soll, ist im Bauordnungsrecht geregelt und vom jeweiligen Gebäude und dessen Nutzung abhängig.

Rechtsgrundlage sind somit die Bauordnungen, Sonderbauverordnungen und Technischen Regelwerke des Bundes und der Länder.

4.2.3.5.2 Berechnung der Öffnungsfläche eines Fensters

Die Hauptanforderung an ein Fenster ist eine ausreichende Öffnungsfläche für den Abzug von Rauch bzw. für den Luftaustausch bei Lüftungsanwendungen.

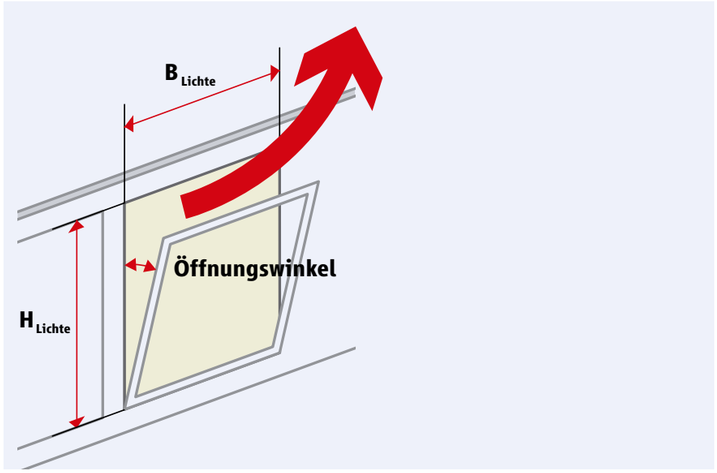
Je nachdem, welche Funktion das Fenster erfüllen soll, werden unterschiedliche Grundlagen zur Berechnung der Öffnungsfläche herangezogen. Bereits bei der Planung sollte die Art der Ermittlung v. a. für RWA-Öffnungsflächen definiert sein.

4.2.3.5.3 Berechnung der Rauchabzugsfläche eines NRWG
(aerodynamisch wirksame Öffnung)

Der erforderliche Öffnungsquerschnitt einer natürlichen Rauch- und Wärmeabzugsanlage für einen Brandabschnitt wird in der Planungsnorm DIN 18232-2 ermittelt.

Zur Berechnung der aerodynamisch wirksamen Öffnungsfläche für das einzelne NRWG muss ein Korrekturfaktor verwendet werden, der entweder aus der Planungsnorm DIN 18232-2 entnommen wird oder experimentell nach EN 12101-2 (DIN EN 12101-2) ermittelt wurde. Der experimentell ermittelte Faktor ist gebunden an das getestete Fensterprofilsystem.

4.2.3.5.4 **Aa (aerodynamische Fläche) = B_{Lichte} • H_{Lichte} • C_{v0}**



C_{v0} = Experimentell nachgewiesener Durchflussbeiwert in Abhängigkeit des Öffnungswinkels.

Da durch Einbauten in der baurechtlich vorgeschriebenen Öffnung in der Wand die Strömung beeinflußt wird, muss diese Veränderung durch einen Beiwert berücksichtigt werden.

Die Ausbreitung und der Abzug von Rauchgasen hängt, besonders in der Brandentstehungsphase, wesentlich von der Raumluftströmung ab. Die Raumluftströmung wiederum wird u. a. von der äußeren Winddruckverteilung an den Abzugs- und Zuluftflächen beeinflusst. Deshalb müssen bei der Entrauchung über die Fassade die Windeinflüsse beachtet werden. Die aerodynamische Wirksamkeit der NRWG wird so je nach Anwendung über zwei verschiedene Korrekturfaktoren berechnet:

- der Korrekturfaktor c_{v0} betrifft die Wirksamkeit eines NRWG ohne Einfluss von Seitenwind
- c_{vw} berücksichtigt den Seitenwind (v. a. bei Dachfenstern)

Somit dürfen alle NRWG, die mit dem Korrekturfaktor c_{v0} ausgelegt sind, nur in solchen Einbausituationen verwendet werden, in denen keine Seitenwindgefährdung gegeben ist. Dies kann beispielsweise durch eine spezielle Einbausituation oder andere technische Maßnahmen wie z. B. eine windrichtungsabhängige Ansteuerung gegeben sein. Wenn NRWG in der Fassade windrichtungsabhängig angesteuert werden, muss die ermittelte Rauchabzugsfläche jeweils in mindestens zwei gegenüberliegenden Außenwänden eines Rauchabschnittes eingebaut werden.

Die DIN 18232-2 bezieht sich hauptsächlich auf NRWG im Dach. Für die Fassade werden aber informative Hinweise gegeben.

4.2.3.5.5 **Um die aerodynamische Wirksamkeit sicherzustellen, muss eine Zuluft vorhanden sein:**

4.2.3.5.5.1 **Berechnung der Zuluftfläche**

Eine wirksame, natürliche Entrauchung erfordert ausreichend dimensionierte Zuluftflächen. Die notwendigen Zuluftöffnungen sorgen für den erforderlichen Ausgleich des Massenstroms und verstärken den Effekt des thermischen Auftriebs (Kamineffekt).

Die Zuluftflächen werden in der Norm DIN 18232-2 beschrieben. Sie müssen vollständig in der raucharmen Schicht liegen und mindestens das 1,5-fache der aerodynamisch wirksamen Abluftfläche betragen. Die Zuluftfläche je Lufteinlass berechnet sich nach DIN 18232-2 wie folgt:

$A_{zu} = a \cdot b \cdot c_z$
(a • b stellt hierbei die lichte Rohbauöffnung der Zuluftvorrichtung dar)

Die Rohbauöffnung (= lichte Öffnung) der Zuluftvorrichtung muss somit mit dem Korrekturfaktor c_z multipliziert werden. Eine Tabelle zu diesem Faktor ist in der Norm zu finden.

Die Oberkante der Zuluftöffnung muss zur Rauchschichtgrenze einen Abstand von mindestens 1 m aufweisen. Im Bereich von Türen oder Fenstern mit maximal 1,25 m Breite kann dieser Abstand auf 0,5 m reduziert werden.

Es ist in jedem Fall darauf zu achten, dass die einströmende Luft nicht direkt in die Rauchgasschicht strömt und dieser Impuls eine Verwirbelung der Rauchgase verursacht.

Als Zuluftöffnungen gelten eigenständige Zuluftvorrichtungen, Tore, Türen oder Fenster, wenn sie entsprechend als Zuluftöffnung für NRA von innen und außen mit Schildern entsprechend DIN 4066 gekennzeichnet sind und zerstörungsfrei (z. B. kein Einschlagen von Fensterscheiben oder Einreißen von Wand- oder Torflächen) von außen geöffnet werden können. Die Zuluftflächen müssen unverzüglich (z. B. automatisch über die RWA-Steuerung, durch die Werkfeuerwehr, durch betriebliche oder organisatorische Vorkehrungen) nach Auslösung des Rauchabzugs geöffnet werden können.

4.2.3.5.5.2 **Berechnung der Rauchableitungsfläche** (geometrische Öffnung)

Da ein Fenster für eine Rauchableitung (z. B. in Treppenräumen oder für kleine Brandabschnitte) kein geregeltes Bauprodukt (kein NRWG) sein muss, gibt es keine europäische bzw. deutsche Norm hierzu.

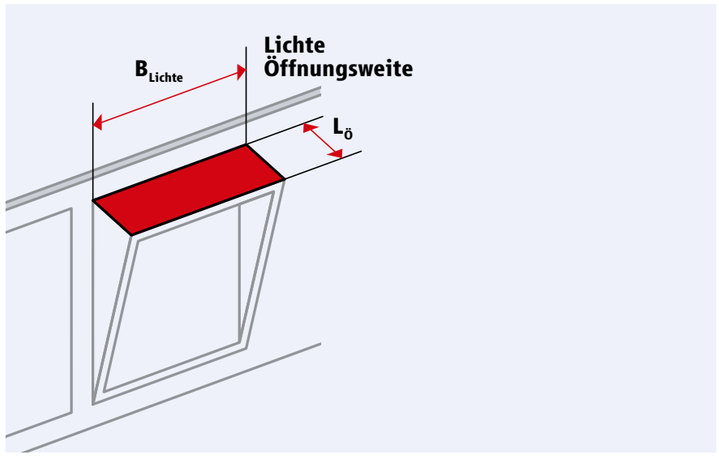
Die geforderte Öffnungsfläche richtet sich nach den Vorgaben aus den nationalen und regionalen Verordnungen (in Deutschland: Landesbauordnungen (LBO) und Sonderbauverordnungen). In der Regel wird eine geometrische Öffnungsfläche gefordert, die sich aus den Fenstermaßen und der Öffnungsweite ergibt (siehe Skizze).

Ob die Öffnungsfläche pro Fenster nur an der Hauptschließkante betrachtet oder ob Seitendreiecke mit einbezogen werden dürfen, hängt von der tatsächlichen Einbausituation und von den definierten Anforderungen und Vorgaben ab (z. B. im Brandschutzkonzept).

Als maximale geometrische Öffnungsfläche darf nur die lichte Fensterfläche angesetzt werden (z. B. bei Öffnungen über 60°).

Eine Zuluft ist in diesem Fall nicht spezifiziert.

A (geometrische Fläche) = Lö • H_{Lichte}



Bei einem Öffnungswinkel größer 60° ist der errechnete Wert „A" mit der maximal lichten Öffnungsfläche des Fensters anzusetzen. Die maximale Fläche kann nur kleiner oder gleich „A" sein!

4.2.3.5.5.3 **Berechnung der Lüftungsfläche**

Entsprechend des Lüftungskonzepts kann die Öffnungsfläche hier auf unterschiedliche Weise berechnet werden:

- Oft wird hier die geometrische Öffnungsfläche verwendet.
- Manchmal werden aber sogar die effektiven Strömungsquerschnitte (je nach Einbausituation) betrachtet. Hier werden entweder wiederum Durchflussfaktoren verwendet oder bei komplexen Anlagen wird eine Strömungssimulation durchgeführt.

4.2.3.6 **Beispielhaftes Planungsschema für Rauch- und Wärmeabzugsanlagen (RWA)**

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Aufgabenstellung	individuell durch den Auftraggeber, z. B. durch den/die • Fachplaner • Bauabteilung • Betreiber
Beispielhafte Schutzziele des Rauch- und Wärmeabzugs	RWA-Schutzziele u. a. • Personenschutz - Rauchfreihaltung von Rettungswegen - Aktive Rettung - Passive Rettung - Lokalisierung des Brandes • Umweltschutz - Verminderung der Umweltschäden - Minimierung der Löschschäden - Minimaler Löschmitteleinsatz • Sachwerteschutz - Erhaltung der Bausubstanz - Unterstützung des Löschangriffs - Ventilierung des Brandes - Minimierung der thermischen Belastung
Erfassungsebene – Auswahl der Sensorik (Melder) (abhängig von den Schutzzielen)	Mögliche in Betracht kommende Melder, u. a. • RWA-Handsteuereinrichtung • BMA-Handfeuermelder • Automatische Melder - Automatische Brandmelder - Thermomelder - Potenzialfreie Kontakte aus der BMA
Übertragungsweg von der Erfassungsebene zur Zentralenebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze - des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Zentralenebene	RWA-Systeme bestehen mindestens aus u. a. • einem Öffnungssystem • einer Notstromsteuerzentrale • zwei Feuertastern (Rauchabzugstastern) • automatische Auslösung, z. B. Rauchmelder (nach DIN 18232 Teil 2 Anhang 4)
Schnittstellen zu anderen Gefahrenmeldeanlagen und zum Gebäudemanagementsystem-Sicherheitstechnik	Möglich sind Schnittstellen u.a. zu/zum • Überfall-/Einbruchmeldeanlagen • Videoüberwachungsanlagen • Zutrittskontrollanlagen • Sprachalarmanlagen • Gebäudemanagementsystem-Sicherheitstechnik
Übertragungsweg von der Zentralenebene zum Gebäudemanagementsystem	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Übertragungsweg vom Gebäudemanagementsystem zur Sicherheitsleitstelle und zur Rückfallebene	Mögliche Varianten, u. a. • Eigenes Leitungsnetz • Mitnutzung - der vorhandenen Schwachstrom-Leitungsnetze des Betreibers - des IP-Netzes des Betreibers • Klärung von möglichen Ersatzwegen bei Ausfall eines der Übertragungswege
Sicherheitsleitstelle	Auslegung entsprechend der vorgenannten definierten Anforderungen

4.2.3.7 **Beispielhafte Funktionen und Anschaltungen einer Rauchwärmeabzugsanlage (RWA) an ein Gebäudemanagementsystem (GMS) und an eine Sicherheits-Leitstelle**

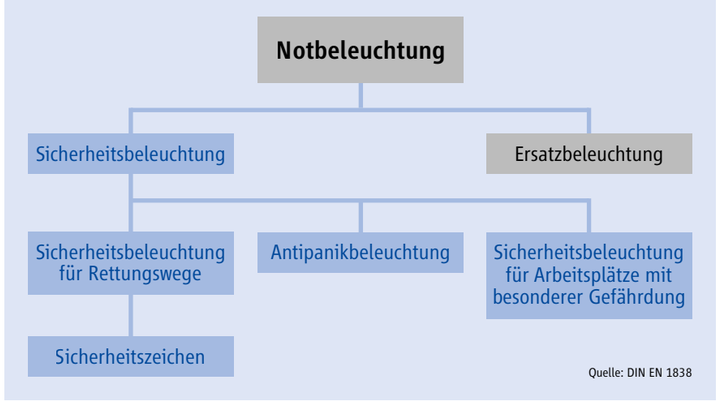
Pos.	Kriterien	Alarm-Funktion	Überwachungs-Funktion	Service-Funktion	an die RWA-Zentrale	an die Feuerwehr	an GMS	a.d. Sicherheits-Leitstelle
1.	**Anschaltung/Ansteuerung, u. a. der**							
1.1	Öffnungssysteme	●	●		●		●	●
1.2	Alarmfunktionen	●			●		●	●
1.3	Lüftungsfunktionen – nur AUF/ZU, ohne STOP							
1.4	Lüftungsfunktionen – nur AUF/ZU und STOP		●		●		●	
1.5	Regen-Wind-Steuerung		●		●		●	
1.6	Rückmeldungen							
1.6.1	Alarm, aktiv nach Alarmauslösung durch Feuertaster oder Rauchmelder oder der Brandmeldezentrale		●		●		●	
1.6.2	Störung, als Sammelstörung für alle erfassbaren Störungen		●		●		●	
1.6.3	Fenster AUF (als Option möglich)		●		●		●	
2.	**Fernservice- und Remotefunktion**			●	●		●	
3.	**Schnittstellen zum/zur/zu, u. a.**							
3.1	Gebäudemanagementsystem-Sicherheitstechnik				●		●	●
3.2	Überfall- und Einbruchmeldeanlagen				●		●	●
3.3	Videoüberwachungsanlagen				●		●	●
3.4	Zutrittskontrollanlagen				●		●	●
3.5	Brandmeldeanlagen				●		●	●
3.6	Sprachalarmanlagen				●		●	●
3.7	Ersatzweg zu einer redundanten Leitstelle				●		●	●
4.	**Service- und Instandhaltungsintervalle** In regelmäßigen Zeitabständen, nach Angaben des Herstellers, mindestens jedoch jährlich, gemäß DIN 18232 Teil 2, müssen RWA sowie ihre Betätigungs- und Steuerelemente, Öffnungsaggregate, Energiezuleitungen und ihr Zubehör auf Funktionsfähigkeit und Betriebsbereitschaft von einer Fachkraft geprüft, gewartet und gegebenenfalls instand gesetzt werden. Die Prüfungen sind in einem Betriebsbuch zu vermerken.				●		●	●

Quelle: FVLR http://www.fvlr.de/rwa_pflegewartung.htm

4.3 Sicherheits- und Fluchtwegbeleuchtung

4.3.1 Funktionale Beschreibung

Die Sicherheitsbeleuchtung soll beim Ausfall der Allgemeinstromversorgung das gefahrlose Verlassen eines Bereiches einer baulichen Anlage gewährleisten. Gemäß DIN EN 1838 werden Sicherheitsbeleuchtung und Ersatzbeleuchtung als Notbeleuchtung bezeichnet.



Anforderungen für eine Sicherheitsbeleuchtung finden sich unter anderem in den Sonderbauverordnungen der Länder, im Arbeitsschutzgesetz und der Arbeitsstättenverordnung sowie in den Technischen Regeln für Arbeitsstätten (ASR).

Die Sicherheitsbeleuchtung für Rettungswege und die Antipanikbeleuchtung sollen für ausreichende Sehbedingungen und Orientierung sorgen, so dass das Gebäude gefahrlos verlassen, Paniksituationen vermieden sowie Brandbekämpfungs- und Sicherheitseinrichtungen leicht aufgefunden und bedient werden können. Die Sicherheitsbeleuchtung für Arbeitsplätze mit besonderer Gefährdung soll die Sicherheit von Personen erhöhen, die sich in einer potentiell gefährlichen Arbeitssituation befinden.

4.3.2 Aufbau von Sicherheits- und Fluchtwegbeleuchtungsanlagen

Sicherheitsbeleuchtungsanlagen bestehen unter anderem aus dem Sicherheitslichtgerät, einer Ersatzstromversorgung, einer Überwachung der Allgemeinstromversorgung, den Rettungszeichen- und Sicherheitsleuchten sowie Steuer- und Meldeeinrichtungen.

Die Ersatzstromversorgung stellt den Betrieb der Sicherheitsbeleuchtung bei Ausfall der Allgemeinstromversorgung sicher. In diesem Fall wird die Sicherheitsbeleuchtung automatisch eingeschaltet (Bereitschaftsbetrieb) oder weiterhin mit Strom versorgt (Dauerbetrieb). Ist eine Brandmeldeanlage vorhanden, erfolgt die Aktivierung der Sicherheitsbeleuchtung im Alarmfall durch diese. Alternativ kann die Ansteuerung auch durch andere Gefahrenmeldeanlagen erfolgen (EMA, Sicherheitsleitstelle).

Ersatzstromversorgungen können entweder über Zentralbatteriesysteme (CPS) oder über Gruppenbatteriesysteme mit Leistungsbegrenzung (LPS) realisiert werden, gegebenenfalls in Kombination mit Notstromaggregaten. In bestimmten Bereichen ist eine Ersatzstromversorgung der Leuchten mit Einzelbatterien zulässig.

Die Leitungsverlegung der Ersatzstromversorgung bis zum Endstromkreis im betreffenden Brandabschnitt hat unter Funktionserhalt (meistens E30) zu erfolgen. Bei bestimmten technischen oder baulichen Voraussetzungen (z. B. Verlegung in Loop-Technik oder Steigschacht in F30-Ausführung) kann auf einen Funktionserhalt der Leitungen verzichtet werden.

4.3.3 Wartung und Prüfung

Eine Sicherheitsbeleuchtungsanlage ist gemäß der DIN VDE 0100-560 und der EN 50171 sowie der EN 50172 täglich, monatlich sowie jährlich zu prüfen und jährlich zu warten.

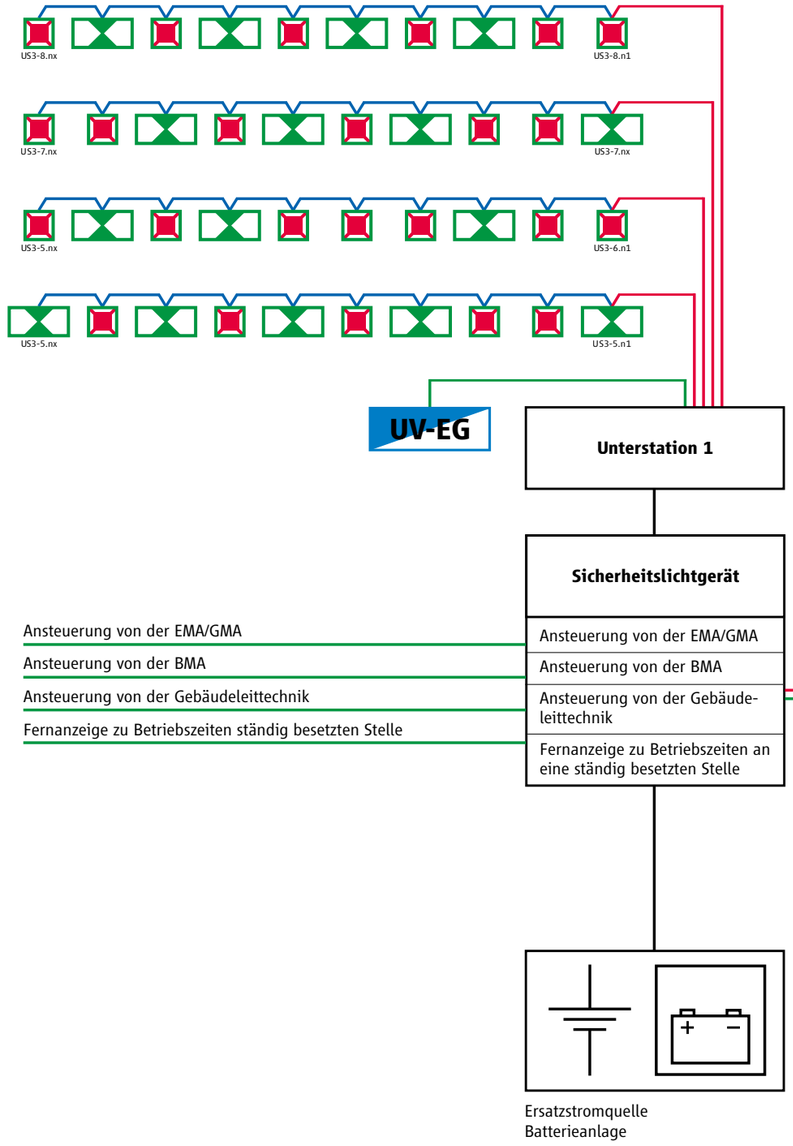
Regelmäßige Wartung der Sicherheitsbeleuchtungsanlagen ist notwendig. Der Betreiber eines Gebäudes muss eine zuständige Person bestimmen, welche die Wartung des Systems überwacht. Diese Person muss ausreichende Befugnisse haben, um die Ausführung der Arbeiten veranlassen zu können, die notwendig sind, um die korrekte Betriebsbereitschaft des Systems sicherzustellen.

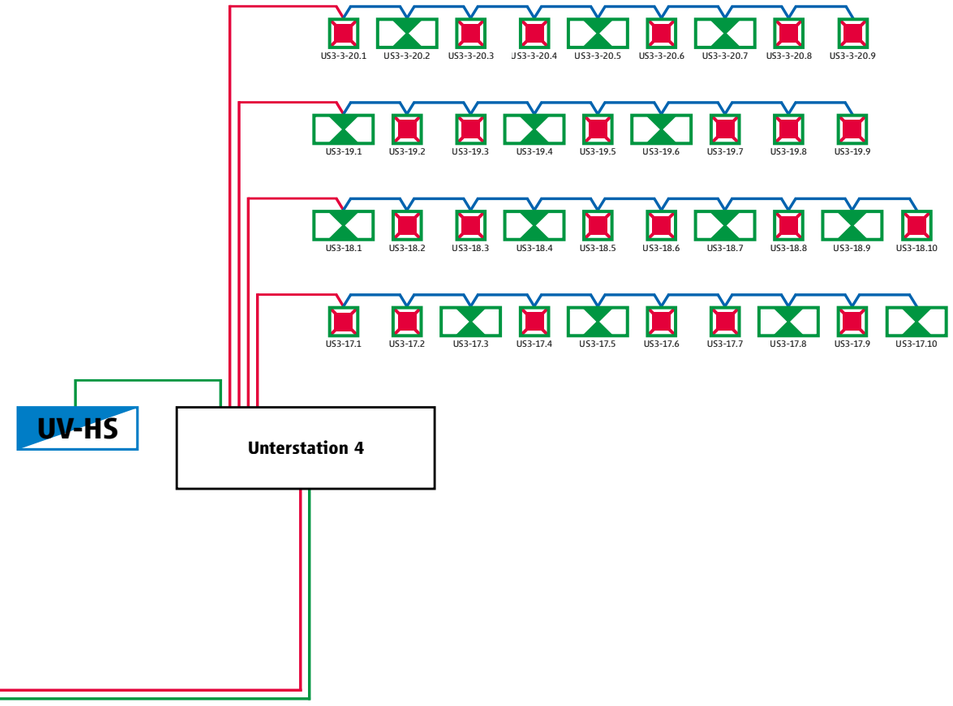
4.3.4 Beispielhaftes Planungsschema für eine Sicherheits- und Fluchtwegbeleuchtungsanlage

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Beispielhafte Aufgabenstellung Projektierung einer Sicherheitsbeleuchtung gemäß den gültigen Normen.	Prüfen behördlicher Auflagen, Bauordnungsrecht der Bundesländer und im Arbeitsschutzrecht des Bundes. Prüfung des Brandschutzkonzeptes sowie der erforderlichen Flucht- und Rettungswegpläne.
Beispielhafte Schutzziele des Auftraggebers Große Räume ohne Tageslichtbeleuchtung, Arbeitsplätze mit erhöhten Unfallgefahren, Versammlungsstätten, Flucht- und Rettungswege, sind mit einer Sicherheitsbeleuchtung auszurüsten, wenn bei Ausfall der allgemeinen Beleuchtung das gefahrlose Verlassen des Gebäudes nicht gewährleistet ist.	Um sicherzustellen, dass die Sicherheitsbeleuchtungsanlage in Übereinstimmung mit der DIN EN 1838 projektiert wird, müssen vor Projektierung der Anlage Flucht- und Rettungswegpläne mit Hinweis auf Feuermelder und Brandschutzeinrichtungen zeigen sowie auf die Lage aller Hindernisse, die die Flucht behindern können. • Um welches Gebäude geht es und welche Vorschriften gelten? • Gibt es eine Risiko- und Gefährdungsanalyse? • Wo befinden sich die notwendigen Flucht- und Rettungswege? • Wo befinden sich die notwendigen Treppenräume? • Wie verlaufen die Flucht- und Rettungswege im Außenbereich bis hin zu den öffentlichen Wegen? • Wo befinden sich Feuerlöscheinrichtungen? • In welche Brandabschnitte ist das Gebäude eingeteilt? • Wie führen wir den Funktionserhalt aus? • Welche Kabel- und Leitungssysteme gibt es? • Welches Anlagensystem und welche Ersatzstromquelle wähle ich? • Einbindung der Allgemeinbeleuchtung oder separate Sicherheitsleuchten? • Welche Leuchten und Leuchtmittel sind geeignet? • Wie hoch sind die Betriebskosten? • Nutzungsdauer?
Erfassungsebene Erkennung von Netzausfällen. Einzelerkennung der in den Sicherheits- und Rettungszeichenleuchten. Brandmeldeanlage und Einbruchmeldeanlage mit Gefahrenmeldeanlage	• Einbau von Netzüberwachungseinrichtungen. • Einbau von Einzelerkennungs- und Überwachungsbausteinen in den Sicherheits- und Rettungszeichenleuchten. • Ansteuerung durch die Brandmeldeanlage über Koppler. • Ansteuerung durch die Einbruch-Gefahrenmeldeanlage über Koppler.
Übertragungsweg von der Erfassungsebene zur Zentralenebene Gebäudevisualisierungen	Einsetzen von Visualisierungsmodulen Die Anlagen sind über ein LON-Netz oder das Internet leicht zu verbinden und von beliebigen Orten aus zu bedienen und zu überwachen.

Planungsebene	Erforderliche Planungsaufgabe in Stichworten
Zentralenebene Visualisierung auf handelsüblichen PCs ohne zusätzliche Software	Durch die Kompatibilität mit Sicherheitsbeleuchtungsanlagen neuer Generationen, die Fehleranalyse über das Internet, den Anschluss an alle gängigen Gebäudevisualisierungen und eine problemlose Erweiterbarkeit ist das flexible System der Standard der Zukunft.
Schnittstellen zum Gebäudemanagementsystem Visualisierung auf handelsüblichen PCs mit zusätzliche Software	Einsetzen eines Hub, Kabelverlegung einer Daten Leitung in Cat-7. Visualisierungssoftware mit dem Gebäudemanagementsystem.
Übertragungsweg von der Zentralenebene zum Gebäudemanagementsystem Weitermeldung von Betriebszuständen und Störmeldungen	Berücksichtigung von Meldemodulen sowie Störmeldungen
Gebäudemanagementsystem Meldungen empfangen, Befehle senden	Berücksichtigung von Meldemodulen sowie Störmeldungen
Übertragungsweg vom Gebäudemanagementsystem zur Sicherheitsleitstelle und zur Ausfallebene Meldungen und Befehle senden	Bereitstellung von potentialfreien Kontakten
Sicherheitsleitstelle Meldungen und Befehle empfangen	Meldetableau
Übertragungsweg von der Sicherheits-Leitstelle zur Ausfallebene Meldungen und Befehle senden	Bereitstellung von potentialfreien Kontakten
Ausfallebene Keine Ausleuchtung von der Sicherheitsbeleuchtung der Flucht- und Rettungswege bzw. keine Kennzeichnung der Flucht- und Rettungswege.	Leuchtmittel in der Sicherheitsbeleuchtung bzw. in den Rettungszeichenleuchten prüfen gegebenenfalls Leuchtmittel auswechseln.

4.3.5 Beispielhaftes Funktionsschema einer Sicherheits- und Fluchtweg-beleuchtungsanlage





Erläuternde Hinweise zur Grafik

Die roten Symbole sind Notleuchten in Bereitschaftsschaltung.

Sicherheitsleuchten dienen zur Beleuchtung der Flucht- und Rettungswege – diese werden erst aktiviert bei:
- Ausfall einer Unterverteilung der Allgemein-Beleuchtung
- Bei einem Brandalarm
- Bei einem Alarm der Einbruchmeldeanlage
- Oder bei der Aktivierung der Alarmierungsanlage.

Notleuchte Leuchte
Die mit oder ohne eigene Stromquelle für Sicherheitszwecke ausgerüstet sein darf und die für Sicherheits- oder Notbeleuchtung eingesetzt wird.

Die Sicherheitsbeleuchtung ist Teil der Notbeleuchtung, der Personen das sichere Verlassen eines Raumes oder Gebäudes ermöglicht, oder der es Personen ermöglicht, vor dem Verlassen einen potentiell gefährlichen Arbeitsablauf zu beenden.

Die grünen Symbole sind Sicherheitsbeleuchtung für Rettungswege (Rettungszeichenleuchten) in Dauerschaltung.

Rettungszeichenleuchten dienen zur Kennzeichnung der Flucht- und Rettungswege; diese werden in Dauerschaltung (Beleuchtung immer eingeschaltet) ausgeführt.

Rettungszeichenleuchte
Leuchte, die zur Kennzeichnung von Rettungswegen eingesetzt wird und hilft, diese zu erkennen.

Die Sicherheitsbeleuchtung für Rettungswege ist Teil der Sicherheitsbeleuchtung, der es ermöglicht, Rettungseinrichtungen eindeutig zu erkennen und sicher zu benutzen, sofern Personen anwesend sind.

4.3.6 Beispielhafte Steuerungsmatrix für eine Sicherheits- und Fluchtwegbeleuchtungsanlage

	Überwachung der Allgemeinen Unterverteilungen						Steuerungen von haustechnischen Anlagen, EMA, GMA, BMA, Gebäudeleittechnik							
Überwachung Einrichtungen / Sicherheitslichtgerät	Überwachung Allgem. Unterverteilung im UG	Bus-Netzwächter Allgemein UV im EG	Bus-Netzwächter Allgemein UV im 1. OG	Bus-Netzwächter Allgemein UV im 2. OG	Bus-Netzwächter Allgemein UV im 3. OG	Bus-Netzwächter Allgemein UV im 4. OG	Einbruchmelde-Anlage Un-Scharfschaltung	Einbruchmelde-Anlage Scharfschaltung	Einbruchmelde-Anlage Alarm Auslösung	Gefahrenmelde-Anlage Alarm Auslösung	Brandmelde-Anlage Alarm Auslösung	Alarmierungs-Anlage Alarm Auslösung	Gebäudeleittechnik / Gebäudemanagementsystem-Sicherheitstechnik	in Betriebszeiten ständig besetzte Stelle
Sicherheitslichtgerät														
DL-Rettungszeichenleuchten Endstromkreise UG	●						●	●	●	●	●	●		
DL-Rettungszeichenleuchten Endstromkreise EG		●					●	●	●	●	●	●		
DL-Rettungszeichenleuchten Endstromkreise 1. OG			●				●	●	●	●	●	●		
DL-Rettungszeichenleuchten Endstromkreise 2. OG				●			●	●	●	●	●	●		
DL-Rettungszeichenleuchten Endstromkreise 3. OG					●		●	●	●	●	●	●		
DL-Rettungszeichenleuchten Endstromkreise 4. OG						●	●	●	●	●	●	●		
DL-Rettungszeichenleuchten Treppenhaus - 01	●	●	●	●	●	●	●	●	●	●	●	●		
DL-Rettungszeichenleuchten Treppenhaus - 02	●	●	●	●	●	●	●	●	●	●	●	●		
BS-Sicherheitsleuchten Endstromkreise UG	●								●	●	●	●		
BS-Sicherheitsleuchten Endstromkreise EG		●							●	●	●	●		
BS-Sicherheitsleuchten Endstromkreise 1. OG			●						●	●	●	●		
BS-Sicherheitsleuchten Endstromkreise 2. OG				●					●	●	●	●		
BS-Sicherheitsleuchtent Endstromkreise 3. OG					●				●	●	●	●		
BS-Sicherheitsleuchten Endstromkreise 4. OG						●			●	●	●	●		
BS-Sicherheitsleuchten Treppenhaus - 01	●	●	●	●	●	●			●	●	●	●		
BS-Sicherheitsleuchten Treppenhaus - 02	●	●	●	●	●	●			●	●	●	●		
BS-Sicherheitsleuchten Außenanlage: Flucht-und Rettungswege Wege bis an öffentliche Straßen	●	●	●	●	●	●			●	●	●	●		
BS-Sicherheitsleuchten Sammelplatz	●	●	●	●	●	●			●	●	●	●		
Sammel-Störmeldung													●	●
Störung Ausfall UV													●	●
Störung Batteriebetrieb													●	●
Störung Tiefentladeschutz													●	●
Bereitschaftslicht Ein													●	●
Anlage Ein/Aus													●	●

● Einschaltbefehl
● Ausschaltbefehl
● Meldung

4.4 Gebäudemanagementsysteme – Sicherheitstechnik

4.4.1 Funktionale Beschreibung

Ein Gebäudemanagementsystem (GMS) besteht aus einem rechnergestützten System, das

- automatisch im Alarmfall detaillierte Informationen in textlicher und grafischer Form für die taktischen Vorgehensweisen über den Alarmort zur Verfügung stellt,
- Alarmhinweise für Interventionskräfte oder an zu benachrichtigende Stellen ausgibt,
- Übersichten über die aktuelle Gefahrensituation zur Verfügung stellt,
- die einlaufenden Meldungen und durchgeführten Aktivitäten protokolliert und archiviert,
- Steuerungsaufgaben über die Kommunikations-, Haustechnik- und Gefahrenmeldeanlagen übernimmt,
- die Bedienung und die Betreuung dieser Anlagen vereinfacht (echte oder abstrakte Bedienfeldemulationen),
- den Betreiber bei seinen dispositiven Sicherheitsaufgaben unterstützt.

Das GMS wird eingesetzt, um Informationen, Alarme und Anweisungen zu empfangen, weiterzuleiten und zu Steuervorgängen zu verknüpfen.

Beispiele:

Gefahrmeldungen und Steuerungen, u. a. aus der

- Überfall- und Einbruchmeldeanlagen (ÜMA-EMA)
- Videoüberwachungsanlagen
- Zutrittskontrollanlagen
- Sicherheits- und Fluchtwegbeleuchtungsanlagen
- Brandmeldeanlagen (BMA)
- Sprachalarmlagen (SAA)
- Entrauchungsanlagen

über gesicherte, bidirektionale Schnittstellen oder potentialfreie Kontakte.

Meldungen und Steuerungen, u. a. aus

- den Gebäudetechnischen Anlagen, u.a.
- Gebäudeautomation
- Gebäudeleittechnik
- Störmeldeeinrichtungen
- Perimeterschutzanlagen
- Elektrotechnik
- Beleuchtungsanlagen
- Aufzugsanlagen
- Heizung
- Sanitär
- Lüftung
- Klima
- Kälte
- Kommunikationsanlagen, u.a.
  - Telefonanlagen
  - Sprechanlagen
  - Betriebsfunkanlagen
  - Personenschutzanlagen
  - Wächterkontrollanlagen

über gesicherte, bidirektionale Schnittstellen oder potentialfreie Kontakte.

Die automatisch erfassten Daten müssen durch das System zum Teil selbsttätig verarbeitet, aber auch im Dialog mit dem Bediener verarbeitet, verteilt und dokumentiert werden können.

Neben der Übernahme von Ereignissen über Datenbus und Kontakte muss auch die Möglichkeit bestehen, mit Unterstützung durch geeignete Formulare an der Datensichtstation sonstige Spezialalarme (Bombendrohung, Geiselnahmen usw.) einzugeben.

Das System muss mit einer leistungsfähigen Dialogsoftware ausgestattet sein und eine individuelle Zugriffsberechtigung durch Passwörter ermöglichen. Jeder einzelne Bedienschritt der windows-ähnlichen Software ist mittels Passwortberechtigung abzusichern.

Alle Bedienvorgänge der Gefahrenmeldezentralen sollen über Maus, Trackball, Touch-Screen oder Tastatur der Workstation durchgeführt werden können.

4.4.2 Aufgaben und Funktionen von Gebäudemanagementsystemen (GMS)

Der praktische Betrieb von Gebäudemanagementsystemen kann in folgende Funktionen eingeteilt werden:

- Entgegennahme von Meldungen und Notrufen
- Veranlassen von Hilfeleistungen
- Fernsteuern von Einrichtungen
- Überwachen von Einrichtungen
- Systempflege und Wartung

Alle Aktionen werden teilweise vollautomatisch vom GMS ausgeführt und in einem umfangreichen Protokoll gespeichert. So können auch nach Monaten Vorfälle an bestimmten Tagen minuziös nachvollzogen werden.

Für Meldungen der Gebäudeleittechnik aus dem Bereich Heizung, Klima und Lüftung werden nur Meldungen bei Überschreiten von Sollwerten an das GMS weitergeleitet, um auch hier gezielt Maßnahmen ergreifen zu können.

Eine wichtige Aufgabe kommt der Pflege der GMS durch den Systembetreuer zu. Hier von besonders betroffen sind:

- Personalveränderungen
- Bauliche Veränderungen
- Wartung des GMS und des Sicherheitsnetzwerkes
- Änderungen der Sicherheitsstrategien
- Revisionen der Subsysteme.

Hierzu sind umfangreiche organisatorische Maßnahmen erforderlich, die vor allem sicherstellen, dass alle Veränderungen dem Systembetreuer zur Verfügung stehen. Dabei muss jedem Verantwortlichen im Betrieb klar sein, welch wichtige Schlüsselposition der GMS-Systembetreuer einnimmt.

Aufgaben des Gebäudemanagementsystems – Sicherheitstechnik, können u. a. sein:

Erfüllung der Anforderungen für die Funktionen und Aufgaben aus der Aufgabenstellung, incl. für Ersatz- und Redundanzfunktionen

4.4.2.1 Informationsbe- und -verarbeitung anhand eines genau zu definierenden Maßnahmenplanes, u. a.

- Empfangen / Anzeige / Bearbeiten von Meldungen und Ereignissen
- Verarbeitung und Darstellung von Aktionsplänen, Lageplänen, Dokumentationen und sonstige Anzeigen-Dokumentationen
- Logbuchfunktionen
- Erstellen von Übersichten
- Durchführung von Steuerungsfunktionen
- Einleiten von Notmaßnahmen
- Veranlassen von sicherheitsrelevanten Belangen
- Dokumentieren
- Archivieren

4.4.2.2 Informationsbe- und verarbeitung anhand eines genau zu definierenden Maßnahmenplanes für die nachfolgenden Anlagen, u. a. aus

- Überfall- und Einbruchmeldeanlagen
- Videoüberwachungsanlagen
- Zutrittskontrollanlagen
- Sicherheits- und Fluchtwegbeleuchtungsanlagen
- Brandmeldeanlagen
- Sprachalarmanlagen
- Entrauchungsanlagen

4.4.2.3 **Bearbeitung von Meldungen und Steuerungen, u.a. aus den gebäudetechnischen Anlagen, u. a.**

- Gebäudeautomation
- Gebäudeleittechnik
- Störmeldeeinrichtungen
- Perimeterschutzanlagen
- Elektrotechnik
- Beleuchtungsanlagen
- Aufzugsanlagen
- Heizung
- Sanitär
- Lüftung
- Klima
- Kälte
- Kommunikationsanlagen, u.a.
  - Telefonanlagen
  - Sprechanlagen
  - Betriebsfunkanlagen
  - Personenschutzanlagen
  - Wächterkontrollanlagen

4.4.2.4 **Organisatorische Aufgaben, u.a.**

- Brandschutz (organisatorisch / personell / elektronisch – mechanisch)
- Zutrittskontrolle (Zutrittsberechtigungen / Ausweiswesen, u. a. für Mitarbeiter-Besucher-Fremdfirmen
- Koppelung mit internen / externen Netzwerken, welche die gleichen Software-Formate haben, sollen ver- / bearbeitet werden können:
  - Maßnahmen der Schließanlagen- und Schlüsselverwaltung
  - Melde- / Berichtswesen für alle relevanten Ereignisse
  - Arbeits- und Umweltschutz (personell / technische / organisatorische Informationen)
  - Dauerlauf von Versuchen / Maschinen schalten zu bestimmten Zeiten
  - Aufgaben der Ersatz- und Redundanzleitstelle bei Überlastung / Störung und Ausfall
  - Kfz- und Parkplatzverwaltung (Mitarbeiter – Besucher – Fremdfirmen)
  - Externe Adressdatenbank für Fremdfirmen und deren Mitarbeiter
  - Mitarbeiter (Personaldaten – Raumdaten – Schnittstelle zur Personalabteilung)
  - Umgang mit betriebsfremden Personen (Besucher / Handwerker / Spediteure / Servicepersonal)
  - Ermittlungen, z. B. für Verlust- / Diebstahl- und Fundmeldungen
  - Erste Hilfe-Maßnahmen
  - Notfallplanung- und Notfallbewältigung (personelle / technische / organisatorische Maßnahmen)
  - Sonstige

4.4.3 **Technische Anforderungen, u. a.**

- Installation in einem eigenen Sicherungsbereich
- Mehrplatz – PC – System; modular erweiterbar
- Kommunikationstechnik
  - Telefon / E-Mail / Internet
  - Betriebs-Bündelfunk
  - Direkt-Notrufleitungen (Feuerwehr / Polizei)
  - Langzeitaufzeichnung (Sprache – Text – Bilder)
- Datentechnik (Netzwerke, Server)
- Klimaanlage
- Notstromversorgung
- Revisionsfunktionen
- Manuelle – und automatische Ersatz- und Redundanzfunktion
- Netzwerkfähig – intern / extern
- Daten – Backup-Sicherung
- Ankoppelung von Daten – Schnittstellen beliebiger Art
- Parametriersoftware
- Serverüberwachung
- Ausfallüberwachung sämtlicher Systeme
- Überwachte ISDN - GSM - UMTS - LTE-Verbindungen
- Funkverbindungen zu mobilen und abgelegenen Objekten
- Redundante Alarmübertragung – ISDN mit D1; D2; GSM; UMTS; LTE; Sonstige
- Sonstige

4.4.4 IT-Sicherheitsprogramme für Gefahrenmeldeanlagen und Gebäudemanagementsysteme

IT-Sicherheitsprogramme sind Programme, die der Sicherheit in der Informationstechnik dienen durch Zugriffskontrolle, Schutzmaßnahmen gegen Manipulation und gegen Aufhebung der Vertraulichkeit von Daten, Schutzmaßnahmen gegen Datenverlust und durch Revisionsmöglichkeiten. Da nur wenige Betriebssysteme integrierte Sicherheit bieten, muss Sicherheitssoftware zusätzlich eingesetzt werden. Die Sicherheits-Software kann folgende Programmfunktionen beinhalten:

4.4.4.1 Zugriffskontrolle

Eine Funktion, die den Zugriff auf das System über eine Reihe von Optionen regelt und kontrolliert:

- Identifizierung und Authentisierung der Benutzer
- Zugriffskontrolle auf Computer-Ressourcen
- Protokollierung und Audit
- Wiederaufbereitung von Speichern

4.4.4.2 Manipulationsschutz und Sicherung der Vertraulichkeit

Diese Funktion vermeidet das Risiko der Manipulation und der Aufhebung der Vertraulichkeit von Daten

- Integritätsprüfung durch Prüfsummen oder elektronische Unterschrift
- Verschlüsselung und Key Management

4.4.4.3 Virenschutzmechanismen gegen Datenverlust

- Backup durch Kopieren der Daten
- Recovery mit Check Point-Techniken
- Virenschutz

Das System kopiert in regelmäßigen Abständen den Speicherinhalt, sodass nach einem Systemabsturz die Verarbeitung lediglich von letzten Check Point an neu aufgenommen werden muss.

4.4.4.4 Kontroll- und Revisionsmaßnahmen

- teilweise integriert in Zugriffskontrollsoftware
- Protokollierung aller für die Sicherheit der DV relevanten Vorgänge

4.4.5 Planung von Gebäudemanagementsystemen

Im Rahmen von Gebäudemanagementsystem (GMS) Projekten gibt es einzelne Projektphasen, die unterschiedliche Inhalte und Verantwortungen aufweisen.

4.4.5.1 Zieldefinition

Die Zieldefinition muss durch den Auftraggeber/Nutzer vorgegeben werden und dient als Grundlage für die Erarbeitung eines Pflichtenheftes. Die Zieldefinition beinhaltet folgende Elemente:

- Umfang der zu integrierenden Sicherheits-, Kommunikations- und Haustechnikanlagen
- Definition der Integration
- Erwartete Verbesserungen gegenüber einer Einzelsystemlösung
- Beschreibung der Arbeitsplätze und Aufgaben der Mitarbeiter an den Arbeitsplätzen.

Aus der Zieldefinition ist ein Pflichtenheft in Zusammenarbeit Nutzer/Planer zu erstellen.

4.4.5.2 Pflichtenheft

Im Rahmen des Pflichtenheftes wird die Vollständigkeit und Klarheit der Zieldefinition überprüft. Folgende Angaben müssen konkretisiert werden:

- Welche Anlagen/Systeme sind im Bestand vorhanden und sind in das Gesamtsystem einzubinden (mit Angabe Softwarestand)?
- Welche Anlagen/Systeme müssen neu angeschafft werden, Fabrikate bzw. Beschreibung der Systeme und der erwarteten Schnittstelle für die Integration?
- Datenpunktumfang
- Funktionale Beschreibung (Alarmpläne, Automatisierungswünsche, Maßnahmenpläne, Grafiken, Bedienungskonzepte etc.)
- Definition der erwarteten Leistungsmerkmale
- Definition der technischen Rahmenbedingungen für die Integration, dazu gehört die Beschreibung der erwarteten physikalischen und logischen Schnittstellen zur Einbindung in die definierte Integration für ein ganzheitliches Managementsystem
- Beschreibung der Betriebsweise von Subsystemen
- Definition von Zeitsynchronisationen, Anlaufverhalten und Synchronisation, Systemüberwachung und sicherheitstechnische Anforderungen
- Definition der rechtlichen Rahmenbedingungen, dazu gehören Themen wie z. B. Lizenzrechte, Offenlegung von Schnittstellen, Unterstützung bei der Neuentwicklung oder Anpassung sowie Inbetriebnahme der Schnittstellen
- Konzeptionelle Lösung (Blockschaltbild) in Bezug auf Vernetzung der anzuschließenden Subsysteme und des Managementsystems.

4.4.5.3 **Rahmenbedingungen**

In den Rahmenbedingungen sind alle auf das Projekt bezogenen sonstigen Bedingungen festzuschreiben. Das Pflichtenheft und die Rahmenbedingungen dienen als Grundlage für Ausschreibungen, Auswahl und Projektüberwachung.

4.4.5.4 **Ausschreibung**

In der Ausschreibung werden die Mengeneinheiten sowie die technischen Anforderungen der anzubietenden Geräte bzw. Anlagenteile definiert und als Mindestanforderung festgeschrieben.

4.4.5.5 **Auswahl**

Bei der Auswahl von Anbietern ist darauf zu achten, dass möglichst standardisierte bzw. zertifizierte Schnittstellen zu den im Projekt einzubindenden Anlagen vorhanden sind. Es ist darauf hinzuweisen, dass die Entwicklung von Schnittstellen Risiko- und Kostenfaktoren darstellen können. Es wird empfohlen, durch Referenzen die angebotenen Leistungen im Hinblick auf die Erfüllung des Pflichtenheftes vor Vergabe zu überprüfen.

4.4.5.6 **Projektüberwachung**

Aufgrund der Komplexität des Gesamtsystems sind frühzeitig Kriterien zur Überprüfung einzelner Schnittstellen und Funktionen festzuschreiben und als Teilsystem bzw. Teilfunktion abzunehmen. Die Gesamtfunktionalität muss dann in der Abnahme aller Systeme geprüft werden.

4.4.5.7 **Schnittstellen bei Gebäudemanagementsystemen (GMS) – Vor und Nachteile**

Die mit dem GMS gekoppelten Subsysteme verfügen heute in vielen Fällen über Rechnerschnittstellen. Wenn das nicht der Fall ist, kann die Anbindung auch über potenzialfreie Kontakte realisiert werden. Es können also drei Arten von Ankopplungen unterschieden werden:

- Bidirektionale Schnittstellen
- Unidirektionale Protokollierungs-Schnittstellen
- Potenzialfreie Kontakte

Am effektivsten ist die Kopplung zweier Systeme über bidirektionale Schnittstellen. Auch hier gibt es zahlreiche Varianten:

- Mit gesichertem Protokoll
- Ohne gesichertem Protokoll
- Normierte Standardprotokolle
- Herstellerspezifische Protokolle

Alle diese Varianten haben ein gemeinsames Merkmal:

4.4.5.7.1 **Den bidirektionalen Datenaustausch zwischen Subsystem und GMS.**

Die Kopplung über unidirektionale Protokollierungs- Schnittstellen wird immer dann genutzt, wenn keine bidirektionale Anbindung bei dem entsprechenden Subsystem vorhanden ist. Auch in den Fällen, wo durch die VdS-Richtlinie eine Einwirkung durch ein GMS nicht zulässig ist, weil dadurch die VdS-Zulassung erlöschen würde (z. B. bei Gefahrenmeldeanlagen), muss auf den Vorteil des Zugriffs auf die volle Funktionalität des Subsystems verzichtet werden. Immerhin kann auch hier das Melden und Dokumentieren von Ereignissen vom GMS genutzt werden.

Diese Schnittstellen sind eigentlich für Protokolldrucker gedacht gewesen. Teilweise existieren aber auch bei Gefahrenmeldeanlagen Schnittstellen, die speziell zur Kopplung an ein übergeordnetes GMS eingerichtet wurden, aber nur unidirektional genutzt werden können.

Schließlich gibt es noch die Möglichkeit, eine Kopplung über potentialfreie Kontakte zu realisieren - eine kostengünstige Lösung zur Auswertung und Steuerung von Toranlagen, Aufzügen, Türkontakten, Lichtsteuerungen usw.

Die Kopplung möglichst vieler Subsysteme mit einem GMS bietet zahlreiche Vorteile:

- Bei einem Feueralarm erfolgt die Anzeige des Melders in der Grafik des GMS und die automatische Ausgabe eines Maßnahmenvorschlags
- auf Tastendruck geht der Alarm für den Löschzug gemeinsam mit einem FAX über den Brandherd raus
- die Tore gehen auf und
- die Evakuierungsanlage wird aktiv
- gespeicherte Lautsprecheransagen fordern zum Verlassen des Gebäudes und der Lifte auf, die automatisch ins Erdgeschoss fahren
- das System überwacht alle Aktivitäten und
- dokumentiert alles sauber im automatisch geführten Einsatzprotokoll.

4.4.5.8 Forderungen an die Ausfallsicherheit von Gebäudemanagementsystemen (GMS)

Von besonderer Bedeutung ist die Ausfallsicherheit von GMS und der angeschlossenen Systemkomponenten bzw. Subsysteme. Zwei Kriterien sind hierbei von Wichtigkeit:

- Für die Ausfallsicherheit aller Systemkomponenten und Subsysteme ist eine ganzheitliche Betrachtungsweise erforderlich. Hier gilt wieder der Grundsatz, dass das schwächste Glied im System den Grad der Ausfallsicherheit bestimmt.
  Wichtig ist, durch ein effizientes Ausfall-Risikomanagement das Ausfallrisiko ständig zu minimieren.
- Alle angeschlossenen Subsysteme müssen bei einem kurzfristigen Ausfall des GMS für sich autark und funktionsfähig bleiben. Denkbare Ausfälle müssen deshalb in regelmäßigen Abständen simuliert und die entsprechenden Verhaltensweisen durch das Leitstellenpersonal geübt werden.

Die Praxis zeigt außerdem, dass ein Großteil der Ausfälle auf kurzfristige Spannungsausfälle oder transiente Störungen im Stromnetz zurückzuführen ist. Eine USV (Unterbrechungsfreie Stromversorgung) schafft hier eine sichere Abhilfe.

4.4.6 Beispielhaftes Planungsschema Gebäudemanagementsysteme – Sicherheitstechnik (1)

Planungsebene	Erforderliche Planungsaufgabe in Stichworten, u.a.
Organisation - Organisationsstruktur des Anwenders	**Organisationsstruktur des Anwenders** • Grundsätzliches Organigramm • Qualifikation des Personals • Wirtschaftlichkeitsberechnung
Struktur des GMS	• Alarmverteilung und Bearbeitung
Schnittstellenübersicht – Zentralenebene	• Art der Schnittstellen • Liste der Informationen zum Managementsystem • Funktionalitäten der Subsysteme > GMS • Funktionalitäten GMS Subsysteme • Funktionsmatrix
Blockdiagramm des GMS und aller Subsysteme	• Gemäß VDI 6010
Hardware - Rechner	• Anzahl der Arbeitsplatzrechner • Beschreibung der Rechneranforderungen • Beschreibung der Server (wenn gefordert)
Netzwerk	• Physikalische Netzwerkschnittstelle • Netzwerktopologie • Angestrebte oder vorhandene Verkabelung
Umweltbedingungen	• Lokationen der Rechner • Raumklima • Lichtverhältnisse • Platzbedarf • EU-Bestimmungen für Bildschirmarbeitsplätze

Beispielhaftes Planungsschema Gebäudemanagementsysteme – Sicherheitstechnik (2)

Planungsebene	Erforderliche Planungsaufgabe in Stichworten, u.a.
Schnittstellen und Protokolle zu Subsystemen	• Physikalische Schnittstellen unter Beachtung der geforderten Funktionalitäten • Verantwortungsbereiche für die Koordination der Protokolle • Einsatz von Schnittstellen-Analyzern bei Meinungsverschiedenheiten • Verkabelung zu den Subsystemen • Art der Verkabelung • Maximale Längen • Art der Steckverbindungen • Verantwortungsbereiche für die Verkabelungen
GMS-Software – Allgemeine Anforderungen	• Betriebssystem • Datenbankschnittstellen • Grafikdaten (z. B. DWG, DXF) • Anforderungen an die Software-Ergonomie • Passwort-Organisation
Grafische Darstellungen	• Alarmvisualisierung • Art der Grafikdarstellung (2D oder 3D) • Melderdarstellung (z. B. nach VdS 2135, BHE oder symbolisiert; Symboldarstellung allgemein mindestens DIN)
Alarmbearbeitung	• Alarmverfolgung • Ereignisprozessverarbeitung (Verknüpfungen) • Behandlung der Prioritäten • Alarmverteilung Tag und Nacht • Parallelbearbeitung
Bedienerschnittstelle (User-Interface)	• Art der Bedienung (z. B. Maus, Trackball, Video-Tracking, Touchscreen) • Anzahl der Bildschirme pro Arbeitsplatz
Maßnahmenkataloge	• Alarmtextmaßnahmen (Form und Aufbereitung) • Verknüpfungen • Schalthandlungen • Steuerungen
Berichte und Protokolle	• Bedienerberichte (Wer hat wann was bedient?, wer war der Bearbeiter?) • Sicherheitsberichte (z. B. alle Ereignisse der letzten 24 Stunden, selektiert nach Subsystemen usw.) • Langzeitprotokoll (Selektion nach Datum, Subsystem oder Meldern) • Statistikfunktionen

Beispielhaftes Planungsschema Gebäudemanagementsysteme – Sicherheitstechnik (3)

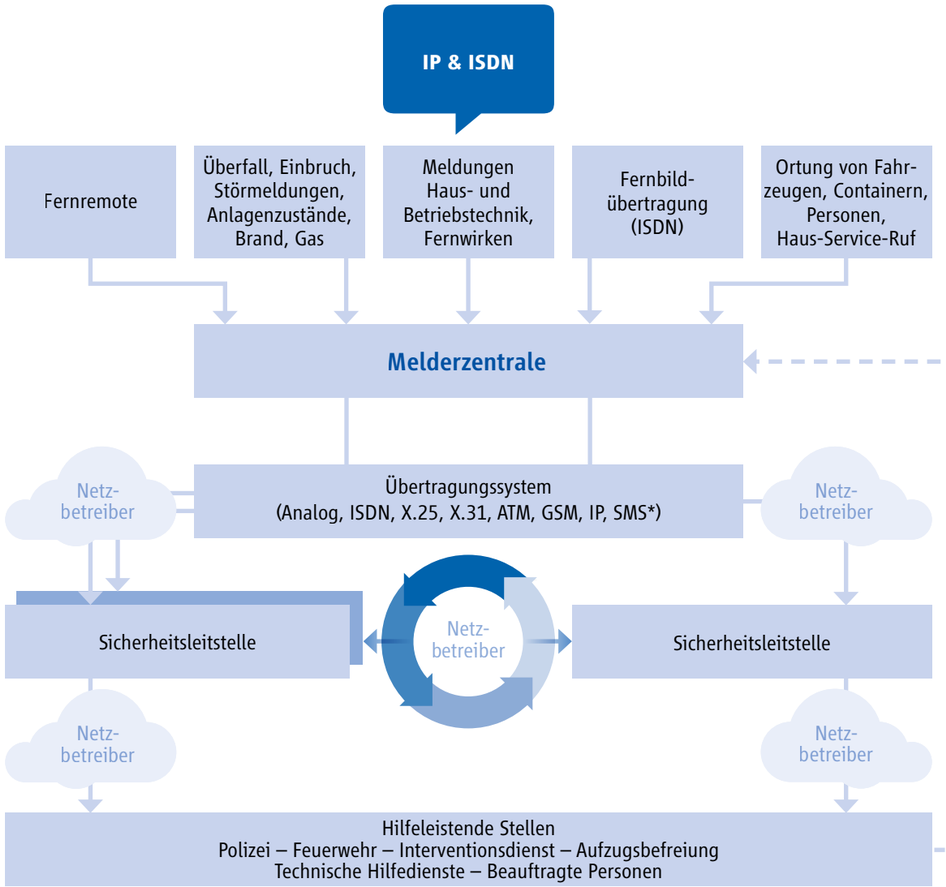
Planungsebene	Erforderliche Planungsaufgabe in Stichworten, u.a.
Druckfunktionen	• Alarmmaßnahmen • Protokolle und Berichte • Drucker im Netzwerk • Grafikdrucke (z. B. FW-Laufkarten) • Statistiken
Projektierung	**Datenpunkte** • Anzahl der Datenpunkte, aufgeschlüsselt nach Subgewerken **Grundrisse** • Anzahl der Grundrisse und Art der Übernahme von Datenpunkten **Übernahme von Grafiken** • Anzahl und Format der Grafiken, die übernommen werden sollen **Erstellen von Maßnahmenkatalogen** • Art und Umfang der Maßnahmenkataloge inkl. der Verknüpfungen
Probebetrieb, Abnahmen und Regelbetrieb	**Probebetrieb** • Genaue Vereinbarungen **Abnahmen** • Einzelabnahmen der Subgewerke inkl. der Abnahmeprotokolle • Gesamtabnahme • Abnahmedokumente • Bedingungen für den Probebetrieb • Dauer des Probebetriebes • Überführung in den Regelbetrieb
Mögliche Dokumentationen vom Bieter – Software-Dokumentationen	• Bedienerhandbuch (oder Online-Dokumentation, z. B. auf CD-ROM) • Software-Struktur-Dokumentation • Dokumentation der Updates (Änderungsdienste)
Mögliche Dokumentationen vom Bieter – Hardware-Dokumentationen	• Blockdiagramme • Installations- und Anschlusspläne • Handbücher • Änderungsdienste
Mögliche Schulungen und Einweisungen vom Bieter – Schulung für den Systemadministrator	• Trainingsphasen • Trainingsumfang
Mögliche Schulungen und Einweisungen vom Bieter – Schulung für das Bedienpersonal	• Leistungsumfang • Trainingsphasen

Beispielhaftes Planungsschema Gebäudemanagementsysteme – Sicherheitstechnik (3)

Planungsebene	Erforderliche Planungsaufgabe in Stichworten, u.a.
Termine – Projektplan (vom Bieter abzufordern)	• Pert- oder Gant-Diagramme • Projektkalender • Ressourcenplan • Meilensteine (Einzelabnahmen, Probebetrieb, Abnahme usw.)
Garantie	• Garantieumfang • Garantiebedingungen • Beginn der Garantie
Projektmanagement / Anbieterprofil – Vorstellung des Anbieters	• Firmenprofil • Referenzinstallationen • Beschreibung der Konfigurationen von Referenzen • Qualifikationsprofil der Mitarbeiter • Erfahrungen in der Abwicklung von GMS-Projekten
Qualitätssicherung des Anbieters	• Zertifizierung nach ISO 9001

4.5 Notruf- und Serviceleitstelle (NSL) und Alarmprovider (AP) nach VdS 3138

Eine Notruf- und Serviceleitstelle überwacht, empfängt und verarbeitet Alarme, Meldungen, Signale und Daten und leitet sie an eine hilfeleistende Stelle weiter. Die Übertragung erfolgt von unterschiedlichen technischen Anlagen wie z. B. Gefahrenmeldeanlagen, haus- und betriebstechnischen Einrichtungen, Personennotrufanlagen, Zutrittskontrollen, Videoüberwachung, usw., die über gemietete Stromwege von Telekommunikationsprovidern bedarfsgesteuert (ISDN, analog, GSM) bzw. per virtueller Standleitung (TCP/UDP, X.25, X.31) signalisiert werden. Sämtliche Ereignisse werden normengerecht dokumentiert.

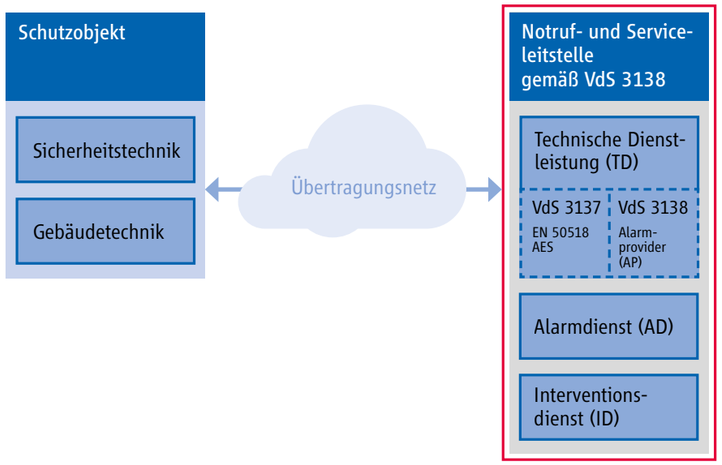


* Die Verfügbarkeit der einzelnen Verbindungsarten ist mit dem jeweiligen Telekommunikationsanbieter abzuklären.

Zur Anerkennung einer Notruf- und Serviceleitstelle (NSL) ist die Zertifizierung nach VdS 3138 erforderlich. Des Weiteren muss der Empfang von Ereignissen über eine Alarmempfangsstelle (AES) erfolgen. Die Anforderungen einer NSL müssen folgende Sicherungskette beinhalten:

- Technische Dienstleistung (TD)
  - Alarmempfangsstelle (AES) gemäß VdS 3137 und DIN EN 50518
  - Alarmprovider (AP) gemäß VdS 3138
- Alarmdienst (AD)
- Interventionsdienst (ID)

Die Architektur kann in einem zentralisierten oder modularen Aufbau erfolgen. Die Dienstleistungen bei einer modularen Architektur können durch Kooperationspartner abgedeckt werden.



Die DIN EN 50518 für Alarmempfangsstellen ist in drei Teile unterteilt:

- Teil 1 Örtliche und bauliche Anforderungen
- Teil 2 Technische Anforderungen
- Teil 3 Abläufe und Anforderungen an den Betrieb

4.5.1 Funktion

Das in einer NSL eingesetzte qualifizierte Fachpersonal (siehe auch VdS-Anerkennung), das rund um die Uhr tätig ist, sorgt unverzüglich dafür, dass die erforderlichen Maßnahmen zur Hilfeleistung bzw. zur Behebung von Störungen oder Schäden sowie zur Gefahrenabwehr durchgeführt werden. Die differenzierte Übertragung unterschiedlicher Kriterien aus den Gefahren- bzw. Störungs-Meldeanlagen in den Schutzobjekten lassen zeitlich und räumlich angepasste Reaktionsabläufe zu.

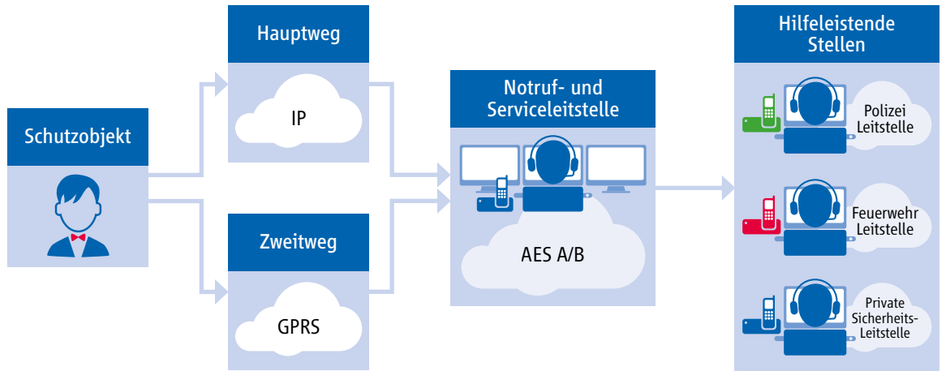
4.5.2 Technische Ausstattung

Das Gefahrenmanagementsystem (GMS) dient zur zentralen Verwaltung eines Schutzobjektes. Im Datensatz des Schutzobjekts werden die objektspezifischen Stammdaten einer Aufschaltung hinterlegt. Sämtliche Meldungseingänge werden chronologisch erfasst. Durch den hinterlegten elektronischen Maßnahmenplan kann für jede Meldung ein separater Aktionsplan hinterlegt werden, sodass unterschiedliche hilfeleistende Stellen benachrichtigt werden können. Für Alarmmeldungen von Brand- und Notrufanlagen werden automatisierte Weiterleitungen zu Behördenleitstellen (Polizei, Feuerwehr) hinterlegt.

Wichtige Leitstellentechnik, wie z. B. Alarmempfangseinrichtungen zur Entgegennahme von Alarmen, Meldungen und Signalen sind redundant aufgebaut, sodass auch bei technischen Störungen oder Wartungen ein uneingeschränkter Meldungsempfang stattfindet. Zur zusätzlichen Sicherheit sind die Systeme mit einer Unterbrechungsfreien Stromversorgung (USV) und einem Überspannungsschutz ausgestattet. Jede Peripherie der Notruf- und Serviceleitstelle ist systemüberwacht. Das heißt, dass durch ein permanentes Monitoring bei technischen Störungen sofort Gegenmaßnahmen eingeleitet werden können. Durch die bestehende Redundanz ist eine uneingeschränkte Verfügbarkeit des Systems weiterhin möglich.

4.5.3 Meldungsübertragung

Entsprechend einer Risikobewertung kommen zur Übertragung von Meldungen unterschiedliche Übertragungsverfahren zum Einsatz:



Ein Höchstmaß an Sicherheit wird durch die verschlüsselte IP-Übertragung mittels virtueller Standleitung erzielt. Ein permanentes Polling zwischen dem Übertragungsgerät des Schutzobjektes (Endgerät) und der Alarmempfangseinrichtung der Notruf- und Serviceleitstelle überwacht den Status der virtuellen Standleitung. Bei einer auftretenden Störung wird die Unterbrechung sofort der Notruf- und Serviceleitstelle signalisiert.

Zustands-/Störungsmeldungen, Übertragungen von Grenzwerten und Steuerbefehlen, sowie Gefahrenmeldungen aus Objekten mit geringem Risiko können über bedarfsgesteuerte Verbindungen übertragen werden. Voraussetzung ist die Meldungsübertragung über verschiedene Trassen, sofern zwei Übertragungswege erforderlich sind.

Eine weitere Möglichkeit besteht in der Signalisierung per SMS über eigene SMSC. Eine vereinbarte SMS-Sequenz wird an die Notruf- und Serviceleitstelle übertragen. Durch das Gefahrenmanagementsystem wird die SMS-Sequenz ausgewertet und dem Schutzobjekt zugeordnet.

Für sämtliche Übertragungsverfahren müssen entsprechende Alarmempfangseinrichtungen in der Notruf- und Serviceleitstelle vorhanden sein. Die übertragenen Informationen werden dort entgegengenommen und ausgewertet. Zur Erreichung einer möglichst hohen Übertragungssicherheit erfolgt zwischen Übertragungseinrichtung und Alarmempfangseinrichtung ein Datenaustausch, bei dem die Übertragungseinrichtung des Schutzobjektes identifiziert und das Datentelegramm revisionssicher überprüft wird. Erst nach erfolgreicher Überprüfung erfolgt die Quittierung der Meldung.

Die einzelnen Klassifizierungen eines Schutzobjektes sind in der DIN EN 50136-2 erläutert. Unterschieden wird zwischen Single Path und Dual Path Übertragungen. Die Einstufung erfolgt vom Sachversicherer bzw. der zuständigen Behörde.

Je nach Klassifizierung des Schutzobjektes erfolgt die Meldungsweiterleitung an hilfeleistende Stellen über bedarfsgesteuerte Verbindungen bzw. mittels virtueller Standleitung. Eine Zwei-Wege-Übertragung (Dual Path Verfahren) ist hierbei erforderlich.

Hinweis:
Bis Ende 2018 stellen alle Telekommunikationsanbieter von ISDN Stück für Stück auf die IP-Übertragung um; somit entfallen auch Stück für Stück die zuvor genannten Übertragungsverfahren. Ebenfalls werden die derzeit bestehenden Normen und Richtlinien entsprechend angepasst.

4.5.4 Meldebearbeitung

Grundsätzlich werden analoge und digitale Informationen einer Übertragungseinrichtung in der Notruf- und Serviceleitstelle übernommen, verarbeitet, überwacht und weitergeleitet. Mittels eines zertifizierten Gefahrenmanagementsystems gemäß VdS 3534 erfolgt die Verarbeitung der Daten. Im Wesentlichen sind neben dem Namen und der Anschrift eines Schutzobjektes ebenfalls weitere spezifische Daten wie z. B. Anfahrtsbeschreibungen, Einsatzmaßnahmen, Meldungsart, Ansprechpartner und hilfeleistende Stellen gespeichert. Anhand dieser Daten wird die Hilfeleistung bzw. die Störungsbeseitigung organisiert. Durch die 24/7 besetzte Notruf- und Serviceleitstelle besteht die Möglichkeit stets Kontakt zwischen dem Einsatzpersonal und der Notruf- und Serviceleitstelle aufzubauen. Sämtliche Vorgänge werden lückenlos durch die NSL-Fachkräfte protokolliert. Die Aufzeichnungen werden mindestens ein Jahr in einem Dokumentenarchivierungssystem aufbewahrt.

4.5.5 Betrieb der Notruf- und Serviceleitstelle

Eine Notruf- und Serviceleitstelle hat aufgrund der Aufgaben und der dort installierten Sicherheitseinrichtungen und gespeicherten Anschlussnehmerdaten ein hohes eigenes Sicherheitsbedürfnis. Es muss daher gewährleistet sein, dass unbefugtes Eindringen sowohl durch bauliche Erschwernisse, wie hohe mechanische Festigkeit von Wänden und Türen, einbruch- und durchschusshemmende Glasflächen, als auch durch elektronische Überwachungseinrichtungen und organisatorische Maßnahmen, wie Zutrittskontrolle, Personalschleusen u. ä., verhindert wird. Betreibt die Notruf- und Serviceleitstelle eine eigene Alarmempfangsstelle (AES), sind zusätzlich die Anforderungen der DIN EN 50518-1 (örtliche und bauliche Anforderungen) zu beachten.

Um jedes Störungsrisiko zu vermeiden, legen risikobewusste Notruf- und Serviceleitstellen ihren Leitstellenbetrieb komplett redundant aus. Sämtliche Peripheriegeräte des Gefahrenmanagementsystems sind komplett gedoppelt bis hin zur Unterbringung an verschiedenen Orten.

In das Leistungskonzept einer Notruf- und Serviceleitstelle kann eine breite Palette von Dienstleistungen unterschiedlicher Art integriert werden:

Priorität haben dabei Gefahrenmeldungen, bei denen häufig eine unmittelbare und weitgehende Bedrohung/Gefahr vorliegt, wie bei Überfall, Einbruch oder Brand. Bei Brandmeldeanlagen ist die direkte Alarmübertragung zur Feuerwehr erforderlich. Ein Sekundäralarm aus einer Brandmeldeanlage kann zusätzlich an eine Notruf- und Service-Leitstelle erfolgen.

Aber auch Überwachungsfunktionen an betriebstechnischen Einrichtungen und sich selbst steuernden Anlagen und Systemen in der Produktion und Verwaltung oder die Überwachung haustechnischer Einrichtungen wie Klima, Heizung und Lüftung dienen dem rechtzeitigen Erkennen von Störungen, deren Folgen mittelbar ebenfalls Menschenleben und Sachwerte erheblich gefährden können.

Die wesentliche Aufgabe der Notruf- und Serviceleitstelle liegt somit in der sinnvollen Kombination der unterschiedlichen Dienste, sodass Erfassung, Übertragung, Entgegennahme und Verfolgung von Meldungen mit dem entsprechenden Qualitätsfaktor wahrgenommen werden. Für die Qualität einer Notruf- und Serviceleitstelle ist neben der technischen Kompetenz die Qualität der NSL-Fachkräfte (Leitstellenmitarbeiter) ausschlaggebend. Vollzeitmitarbeiter, langjährige Berufserfahrung, permanente Refresh-Schulungen wie die Ausbildung zur VdS-anerkannten NSL-Fachkraft, sowie spezielle Personalauswahlverfahren sind wesentliche Bewertungsparameter. Aber auch die Personalorganisation im Hinblick auf maximal Acht-Stunden-Schichten und vorhandene Konzepte zur Anpassung erkennbarer und unvorhersehbarer Meldungsspitzen sind ein Qualitäts-Indikator. Ein zyklisches Sicherheitsscreening sowie eine Sicherheitsüberprüfung sind sicherzustellen. Des Weiteren muss eine behördliche Sicherheitsüberprüfung erfolgen.

Die Ausstattung einer Notruf- und Serviceleitstelle ist in der VdS 3138 beschrieben. Des Weiteren sind die Festlegungen der DIN EN 50518-3 zu beachten.

4.5.6 Internetzugang zur Notruf- und Serviceleitstelle

Kunden einer Notruf- und Serviceleitstelle haben die Möglichkeit, über einen speziell gesicherten Internetzugang für ihre aufgeschalteten Objekte, Alarm- und Ereignisprotokolle abzurufen sowie Maßnahmenpläne (Schließzeiten und festgelegte Kontaktpersonen im Ereignisfall) einzusehen und zu ändern. Des Weiteren können Mitteilungen an die Notruf- und Serviceleitstelle versendet werden.

Aufgrund der meist nicht ausreichenden Datensicherheit im Internet und der nicht eindeutigen Authentifizierungsmöglichkeit des Benutzers, ist für diese hochsensiblen Daten ein besonders hoher Sicherheitsstandard zwingend erforderlich. Um dies zu gewährleisten, ist ein spezielles technisches duales Prüfkonzept sinnvoll. In erster Linie sollte das SSL-Verfahren (Secure Socket Layer) zur Verschlüsselung und Identitätsüberprüfung im Internet, wie es auch bei Onlinebanking angewandt wird, angewendet werden. Zusätzlich ist ein Telefonanschluss über das ISDN- bzw. GSM-Netz erforderlich. Per zusätzlicher Authentifizierung mittels Rückruf nach dem Internet-Login wird der Kunde auf einer vorher hinterlegten Telefonnummer zurückgerufen. Per MFV-Verfahren legitimiert sich der Anwender mit einer PIN.

Das Gefahrenmanagementsystem ist durch eine Firewall vor nicht autorisierten und nicht authentifizierten Anfragen geschützt. Der Internet-Server und das Gefahrenmanagementsystem arbeiten autark und aus Sicherheitsgründen strikt voneinander getrennt.

5. Ausblick

Wie dieses Merkblatt zeigt, bietet die IP-Vernetzung von Gefahrenmelde- und anderen sicherheitstechnischen Anlagen zahlreiche Vorteile. Die Systeme können Informationen austauschen und nutzbar machen. Der Anwender profitiert von zusätzlichen Funktionen und einer höheren Wirtschaftlichkeit, beispielsweise durch eine zentrale Steuerung aller Gewerke inklusive Ferninspektion und Fernwartung.

Noch einen Schritt weiter geht die Vernetzung von sicherheitstechnischen Systemen mit Anlagen der Gebäudetechnik wie z. B. Anlagen der Elektrotechnik, Heizung, Kälte, Klima und Lüftung oder Kommunikations- und Beleuchtungsanlagen.
Durch die erheblich breitere Datenbasis stehen eine Vielzahl zusätzlicher Informationen zur Verfügung, die unter anderem zur Steigerung der Energieeffizienz nutzbar sind. So lassen sich beispielsweise Informationen einer Einbruchmeldeanlage über den Zustand von Türen und Fenstern zur bedarfsgerechten und damit energiesparenden Klimatisierung nutzen.

Die Weiterentwicklung des ZVEI-Schnittstellenmerkblatts „Vernetzte Sicherheit“ wird daher im Zeichen der Vernetzung von Sicherheitstechnik und der Gebäudetechnik stehen.

6. Literaturverzeichnis

[1] „Vernetzung von Sicherheitssystemen ist tägliche Praxis“, www.zvei.org/Verband/Fachverbaende/ArgeErrichterundPlaner/Seiten/Vernetzung-von-Sicherheitssystemen-ist-taegliche-Praxis.aspx, ZVEI (2014)

[2] ZVEI-Merkblatt 33010:2014-02 „ZVEI-Merkblatt für die Interaktion mobiler Endgeräte mit Brandmelderzentralen über IP-Netze“, ZVEI (2014)

Das Merkblatt kann kostenfrei unter www.zvei.org/Verband/Publikationen/Seiten/Integration-mobiler-Endgeraete-mit-Brandmelderzentralen-ueber-IP-Netze.aspx heruntergeladen werden.

[3] [ÜEA] „Bundeseinheitlichen Richtlinie für Überfall- und Einbruchmeldeanlagen mit Anschluss an die Polizei (ÜEA)“, Anlage 5 „Projektierungs- und Installationshinweise“, Seite 4 (2013).

Die ÜEA-Richtlinie ist auf den Internetseiten der Polizeien in den Bundesländern verfügbar, ggf. mit länderspezifischen Zusätzen, siehe z. B. www.polizei.nrw.de/artikel__77.html

7. Übersicht der Mitglieder der ZVEI-Fachgruppe Vernetzte Sicherheit

Folgende Mitglieder der Fachgruppe Vernetzte Sicherheit in der ZVEI-Arbeitsgemeinschaft Errichter und Planer waren ehrenamtlich an der Erstellung dieses Merkblatts beteiligt:

1	Klemens Barde	ASE
2	Manfred Bulle	Honeywell Security Deutschland
3	Stefan Flauder	Atral-Secal
4	Thomas Förster	TIB Technoplan
5	Alexandra Hahn	Bosch Sicherheitssysteme
6	Rene Kiefer	Siemens AG Building Technologies
7	Joachim Klinner	Dehn & Söhne
8	Christian Kühn	Schlentzek & Kühn
9	Joachim Ledermann	Wago Kontakttechnik
10	Hans-Jürgen Leonhardt	Bosch Sicherheitssysteme
11	Lukas Linke	ZVEI
12	Jochen Sauer	Axis Communications
13	Artur Schmidt	Securiton
14	Klemens Siebers	Airlt Systems
15	Alexander Spatz	Honeywell Security Deutschland
16	Karl-Erich Storck	Karl-Erich Storck Betriebssicherheitstechnik
17	Norbert Stühmer	Bosch Sicherheitssysteme
18	Rene Tepaß	Novar
19	Wolfgang Unger	Novar
20	Jens Wiesner	Bundesamt für Sicherheit in der Informationstechnik

Besonderer Dank gebührt Norbert Stühmer, ohne dessen Engagement und großen persönlichen Einsatz dieses Merkblatt kaum zu realisieren gewesen wäre.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main

Telefon: 069 6302-0
Fax: 069 6302-317
E-Mail: zvei@zvei.org
www.zvei.org