



Gefahrenmanagementsysteme

Anforderungen und Prüfmethode

Herausgeber und Verlag: VdS Schadenverhütung GmbH

Amsterdamer Str. 172-174
50735 Köln

Telefon: (0221) 77 66 0; Fax: (0221) 77 66 341

Copyright by VdS Schadenverhütung GmbH. Alle Rechte vorbehalten.

VdS-Richtlinien für rechnergestützte Informationssysteme

Gefahrenmanagementsysteme

Anforderungen und Prüfmethode

Das vorliegende Dokument ist nur verbindlich, sofern dessen Verwendung im Einzelfall vereinbart wird; ansonsten ist die Berücksichtigung dieses Dokuments unverbindlich. Die Vereinbarung zur Verwendung dieses Dokuments ist rein fakultativ. Dritte können im Einzelfall auch andere Anforderungen nach eigenem Ermessen akzeptieren, die diesem Dokument nicht entsprechen.

INHALT

1	Allgemeines	5
1.1	Geltungsbereich	5
1.2	Gültigkeit	5
2	Normative Verweisungen	5
3	Begriffe und Abkürzungen	6
3.1	Begriffe	6
3.2	Abkürzungen	8
4	Aufbau	9
4.1	Aufbau eines GMS	9
4.2	Schnittstellen des GMS	10
5	Anforderungen an die Funktion	11
5.1	Allgemeines	11
5.2	Alarmempfang	11
5.3	Störungen	11
5.4	Überwachung der Verbindung zu Subsystemen	12
5.5	Informationsfluss	12
5.6	Reporting	14
5.7	Stammdaten und Änderungen	14
5.8	Zeitsynchronisierung	15
5.9	Bedieneranmeldung	15
5.10	Anforderungen externer Regelwerke – optional	15
6	Dokumentationspflicht des Herstellers	15
6.1	Mindestanforderungen Hard- und Software	16
6.2	Installationsanleitung	16
6.3	Bedienungsanleitung	16
7	Softwaredokumentation	16
7.1	Versionsschema	16
7.2	Entwicklungsdokumentation	17
7.3	Prozessbeschreibung	17
7.4	Programmdokumentation	18
7.5	Quellcode	18
7.6	Entwicklungswerkzeuge	19
7.7	Ablaufüberwachung	19

8	Prüfmethoden.....	19
Anhang A	Auftrag zur Anerkennung von Gefahrenmanagementsystemen auf Grundlage der VdS 3534	20
Anhang B	Checkliste zur Vorbereitung der Prüfung nach VdS 3534.....	21

1 Allgemeines

1.1 Geltungsbereich

Diese Richtlinien enthalten Anforderungen an Gefahrenmanagementsysteme (GMS) für Übernahme, Eingabe, Erzeugung, Speicherung, Weiterleitung, Verarbeitung und Anzeige von Meldungen und Daten sowie für die Steuerung von verschiedenen Systemen von einer oder mehreren Anlagen. Die Steuerung von Anlagen ist nur dort zulässig, wo sie nicht durch andere Richtlinien und Normen untersagt ist.

Diese Richtlinien gelten nur dann für den Eingriff und die Steuerung von Anlagen des anlagentechnischen Brandschutzes, wenn dies in den mitgeltenden (gewerkspezifischen) Anwendungsregeln definiert ist.

Diese Softwarekomponenten werden auf einem oder mehreren Rechnersystemen mit Bedien- und Visualisierungselementen ausgeführt. Die Rechnersysteme und ihre Betriebssysteme sind nicht notwendigerweise Bestandteil des GMS, können dies aber sein.

Diese Richtlinien enthalten die Mindestanforderungen an Gefahrenmanagementsysteme. Diese können über zusätzliche Funktionen verfügen, die die Mindestanforderungen nicht beeinflussen dürfen.

GMS können über entsprechende Einrichtungen automatische oder vom Bediener manuell ausgelöste Befehle aussenden. Diese Richtlinien enthalten keine Anforderungen an Systeme, die zum Eingreifen in Produktionsanlagen, chemischen Anlagen oder sonstige industrielle Prozesse vorgesehen sind.

1.2 Gültigkeit

Diese Richtlinien gelten ab dem 01.03.2018. Sie ersetzen die Ausgabe 2013-03 (01).

2 Normative Verweisungen

Diese Richtlinien enthalten datierte und undatierte Verweise auf andere Regelwerke. Die Verweise erfolgen in den entsprechenden Abschnitten, die Titel werden im Folgenden aufgeführt. Änderungen oder Ergänzungen datierter Regelwerke gelten nur, wenn sie durch Änderung dieser Richtlinien bekannt gegeben werden. Von undatierten Regelwerken gilt die jeweils letzte Fassung.

- **DIN EN 50518-1** Alarmempfangsstelle (AES) – Teil 1: Örtliche und bauliche Anforderungen
- **DIN EN 50518-2** Alarmempfangsstelle (AES) – Teil 2: Technische Anforderungen
- **DIN EN 50518-3** Alarmempfangsstelle (AES) – Teil 3: Abläufe und Anforderungen an den Betrieb
- **VdS 2227** Richtlinien für Einbruchmeldeanlagen, Allgemeine Anforderungen und Prüfmethode

3 Begriffe und Abkürzungen

3.1 Begriffe

Die allgemeinen Begriffe sind in den Richtlinien für Einbruchmeldeanlagen, Allgemeine Anforderungen und Prüfmethode, VdS 2227 zusammengefasst.

3.1.1 Gefahrenmanagementsystem (GMS)

Ein Softwaresystem zur Übernahme, Eingabe, Erzeugung, Speicherung, Weiterleitung, Verarbeitung und Anzeige von Meldungen und Daten sowie zur Steuerung von verschiedenen Systemen von einer oder mehreren Anlagen.

3.1.2 Alarmer

Darunter versteht man alle Arten von Alarmen, wie Überfall, Einbruch, Zutrittskontrolle, Personenhilferuf usw.

Alle Arten von Systemen dürfen zusätzlich zu den Alarmmeldungen auch andere Arten von Meldungen senden, z. B. Störungsmeldungen und Zustandsmeldungen. Diese Meldungen werden in Übereinstimmung mit diesen Richtlinien auch als Alarmmeldung betrachtet. Der Begriff „Alarm“ wird in dem gesamten Schriftstück in diesem weiten Sinn benutzt.

3.1.3 Bediener

Personen, welche das GMS und dessen Benutzeroberfläche verwenden.

3.1.4 Betreiber

Natürliche oder juristische Person, die für die Inbetriebnahme und Konfiguration sowie den organisatorischen und technischen Betrieb eines Gefahrenmanagementsystems die juristische Verantwortung trägt.

3.1.5 Ereignis

Vorkommnis auf einem Objekt, welches durch eine Meldung, eine Überwachung oder durch einen Bediener ausgelöst wird.

3.1.6 Fehlerhafte Daten

Daten, die der Spezifikation des jeweiligen Datenfeldes, Telegramms etc. entsprechen, aber inhaltlich nicht korrekt sind.

3.1.7 Hersteller (des GMS)

Natürliche oder juristische Person, die das GMS herstellt und/oder in Verkehr bringt.

3.1.8 Identifikationsmerkmal eines Ereignisses

Ein Datenumfang (Auslöser, Bezeichnung, Status etc.), der das Ereignis eines Objektes eindeutig im Datenbestand des GMS festlegt.

3.1.9 Identifikationsmerkmal eines GMS-Bedieners

Ein Datenumfang (Name, Personalnummer etc.), der einen Bediener eindeutig im Datenbestand des GMS festlegt.

3.1.10 Identifikationsmerkmal eines Objektes

Ein Datenumfang (Name, Identnummer etc.), der ein Objekt eindeutig im Datenbestand des GMS festlegt.

3.1.11 Log E(n) (Eventlog, n = 1 bis 4)

Definiert eine Stelle im Informationsfluss, an der eine definierte Menge an Daten gespeichert werden muss.

3.1.12 Log S1 (Stammdatenlog)

Weist die Änderungen an den Stammdaten aus.

3.1.13 Meldung

Information, die im GMS zu verarbeiten ist.

3.1.14 Objekt

Instanz (Örtlichkeit, Person oder Sache), welcher Ereignisse zugeordnet werden.

3.1.15 Rohdaten

Über die S_{GMS} Schnittstelle an das GMS übertragene Daten von Alarmen, ggf. ohne vorhandenen Protokollrahmen.

3.1.16 S_{GMS}

Schnittstelle zur Anschaltung von Subsystemen an das Gefahrenmanagementsystem.

3.1.17 Signal

Physikalische Darstellung einer Information (Quelle: VdS 2227 : 2002-05)

3.1.18 Stammdaten

Im GMS hinterlegte Daten, die für die Bearbeitung und Verarbeitung von Meldungen im GMS relevant werden können.

Beispiele: Objektdaten und Bedienerprofile etc.

3.1.19 Störung des GMS

Zustand, in dem eine Funktionalität zur Erfüllung einer definierten Anforderung an das GMS beeinträchtigt ist.

3.1.20 Subsysteme

Über die Schnittstelle S_{GMS} angeschlossene Systeme, die Alarme an das GMS senden oder vom GMS empfangen (z. B. Empfangseinrichtungen, Gefahrenmeldeanlagen, Videosysteme etc.).

3.1.21 Ungültige Daten

Daten, die nicht der Spezifikation des jeweiligen Datenfeldes, Telegramms etc. entsprechen.

3.1.22 Unterstützende Hardware

Die für den Betrieb des Gefahrenmanagementsystems notwendige Hardware (z. B. Rechnersysteme, Drucker etc.).

3.1.23 Unterstützende Software

Die für den Betrieb des Gefahrenmanagementsystems notwendige Software (z. B. Betriebssystem, Datenbanksystem etc.).

3.1.24 Zeitstempel

Ein Wert, der einem Ereignis einen eindeutigen Zeitpunkt zuordnet.

3.2 Abkürzungen

GMS Gefahrenmanagementsystem

GUI Graphical User Interface (grafische Benutzeroberfläche)

UTC Universal Time Coordinated, die Koordinierte Weltzeit

4 Aufbau

4.1 Aufbau eines GMS

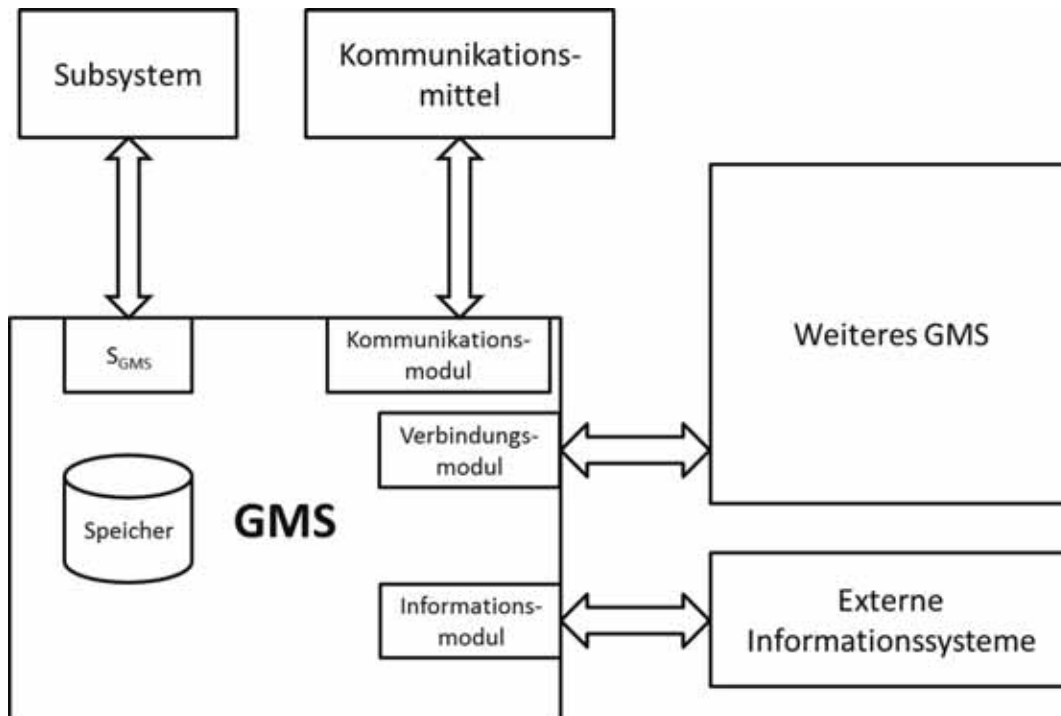


Bild 4-1: Beispielaufbau eines GMS mit seinen funktionellen Komponenten

Bilderläuterung zu Bild 4-1: Die exemplarisch dargestellten funktionellen Komponenten inkl. ihrer Schnittstellen zum GMS können wie folgt beschrieben werden.

S_{GMS}	Schnittstelle zur Anschaltung von Subsystemen (z. B. konventionelle Alarmempfangseinrichtungen, Alarmzentralen, Videoempfangseinrichtungen, Gebäudeleittechnik, Empfangseinrichtungen usw. mit ihren dedizierten Protokollen) an das Managementsystem. Über die Schnittstelle S_{GMS} werden Alarme an das GMS übertragen und umgekehrt.
Verbindungsmodul	Dieses Funktionsmodul dient der Vernetzung mehrerer GMS im lokalen Netz oder weltweit über das Internet oder vergleichbare Übertragungsnetze.
Kommunikationsmodul	Diese Schnittstelle erlaubt den Anschluss zusätzlicher Kommunikationsmittel an das GMS, z. B. Faxgeräte.
Informationsmodul	Diese Schnittstelle erlaubt den Anschluss an Informationen liefernde externe Systeme, z. B. Web-Dienste.
Speicher	Der oder die physikalischen Speicher des GMS, in dem oder in denen Daten des GMS abgelegt sind.
Subsystem	Über die Schnittstelle S_{GMS} angeschlossenes System, das Alarme an das GMS sendet oder vom GMS empfängt.

4.2 Schnittstellen des GMS

4.2.1 Schnittstellen

4.2.1.1 Anforderung

Für folgende Schnittstellen ergeben sich aus dem weiteren Verlauf der Richtlinien Anforderungen:

- Schnittstelle S_{GMS}
- Schnittstelle zu weiteren GMS
- Bedienerchnittstelle
- Schnittstelle zu weiteren Kommunikationsmitteln
- Schnittstelle zu weiteren Informationssystemen

Ein GMS kann über weitere Schnittstellen verfügen. Keine Schnittstelle darf die Funktion der anderen Schnittstellen beeinflussen.

4.2.1.2 Prüfung

Anhand der Dokumentation des GMS und am zur Verfügung gestellten Prüfaufbau wird von VdS überprüft, welche Schnittstellen vorhanden sind und festgelegt, welche Prüfungen durchzuführen sind.

4.2.2 Definition der Schnittstellen

4.2.2.1 Anforderung

Die von einem GMS verwendeten technischen Schnittstellen und Bedienerchnittstellen müssen definiert sein.

4.2.2.2 Prüfung

Anhand der Dokumentation des GMS wird nachvollzogen, ob alle verwendeten Schnittstellen definiert sind. Werden standardisierte Schnittstellen, die durch öffentlich zugängliche Dokumente definiert sind, verwendet, reicht zum Erfüllen der Anforderung der Verweis auf diese Dokumente.

4.2.3 Umgang mit ungültigen Daten

4.2.3.1 Anforderung

Um den zuverlässigen Betrieb des GMS sicherzustellen, müssen die Schnittstellen so ausgeführt sein, dass Störungen im Programmablauf durch ungültige Daten verhindert werden.

4.2.3.2 Prüfung

Anhand der Dokumentation wird nachvollzogen, ob die Software über einen Schutz vor ungültigen Daten verfügt.

5 Anforderungen an die Funktion

5.1 Allgemeines

Nachfolgend werden die Mindestanforderungen an die Funktion eines GMS beschrieben. Weitere Funktionen sind zulässig, sofern die Mindestanforderungen erfüllt werden.

5.2 Alarmempfang

Schnittstellen, über die Alarmpfeile empfangen werden, sind Schnittstellen S_{GMS} im Sinne dieser Richtlinien. Ergänzende Informationen (z. B. Videosignale) können auch über eine andere Schnittstelle vom GMS empfangen werden. Eine vorhandene physikalische Schnittstelle kann dabei als S_{GMS} und als Informationsmodul verwendet werden.

Werden Alarmsignale an das GMS gesendet, die nur von einem Bediener des GMS ausgewertet werden können (z. B. Sprachmeldungen), müssen die Informationsinhalte des Alarms ebenfalls gespeichert werden.

5.3 Störungen

Das GMS muss seine ordnungsgemäße Funktion sowie die Funktion der verwendeten Hard- und Softwarekomponenten laufend überwachen.

5.3.1 Erkennung

Folgende Störungen müssen erkannt werden:

- Störungen oder Ausfall von Teilen der GMS-Software
- Manuelle Eingabe ungültiger Daten
- Empfang von Daten, die nicht durch das GMS interpretiert oder korrekt verarbeitet werden können

Weitere Störungen wie z. B.

- Störung oder Ausfall unterstützender Hardware,
- Störungen oder Ausfall unterstützender Software,

die vom GMS erkannt werden können, sind vom Hersteller des GMS zu dokumentieren, sofern sie in die Zertifizierung einfließen sollen.

5.3.2 Vermeidung

Manuelle Eingaben fehlerhafter oder ungültiger Daten müssen durch inhaltliche Überprüfung vermieden werden. Dies gilt für Eingabefelder, bei denen eine solche Überprüfung logisch möglich ist.

5.3.3 Behandlung

Bei einer erkannten Störung muss mindestens eine eindeutige Meldung erfolgen und die Störung im Log E4 zu speichern.

Der Hersteller des GMS hat zu dokumentieren, wie der Betreiber sicherstellen kann, dass die Meldung von einem Bediener empfangen und bearbeitet werden kann.

5.4 Überwachung der Verbindung zu Subsystemen

Alle von der Zertifizierung umfassten Subsysteme sind auf fehlerfrei funktionierende Verbindungen hin zu überprüfen, sofern das Subsystem eine entsprechende Funktion zur Verfügung stellt.

Subsysteme, die keine entsprechende Funktion zur Verfügung stellen, sind vom Hersteller des GMS zu dokumentieren.

Bei Erkennen des Verbindungsausfalls muss im GMS eine Meldung erzeugt und gespeichert werden, die das betroffene Subsystem eindeutig kennzeichnet.

5.5 Informationsfluss

5.5.1 Protokollierung

Der Informationsfluss des GMS gemäß Bild 5-1 umfasst:

- die Anlage und Pflege der Stammdaten und
- die Behandlung von Ereignissen.

Hierbei kann zwischen der automatischen Verarbeitung durch das GMS und der Bearbeitung durch die Bediener unterschieden werden. Ein Wechsel von automatischer Verarbeitung zur manuellen Bearbeitung und umgekehrt ist möglich. Durch die Behandlung von Ereignissen dürfen keine Informationen verloren gehen oder verfälscht werden.

Um eine herstellerübergreifende, vereinheitlichte Betrachtung des Informationsflusses zu erreichen, muss das GMS festgelegte Standard-Logs generieren können. Die Logs sind in Stammdaten-Logs (S-Logs) und Ereignisdaten-Logs (E-Logs) zu unterscheiden.

Gemäß der folgenden Darstellung, beschreiben die Log-Definitionen in diesem Kapitel nicht den Aufbau der GMS-Datenstrukturen, sondern den Mindest-Informationsumfang.

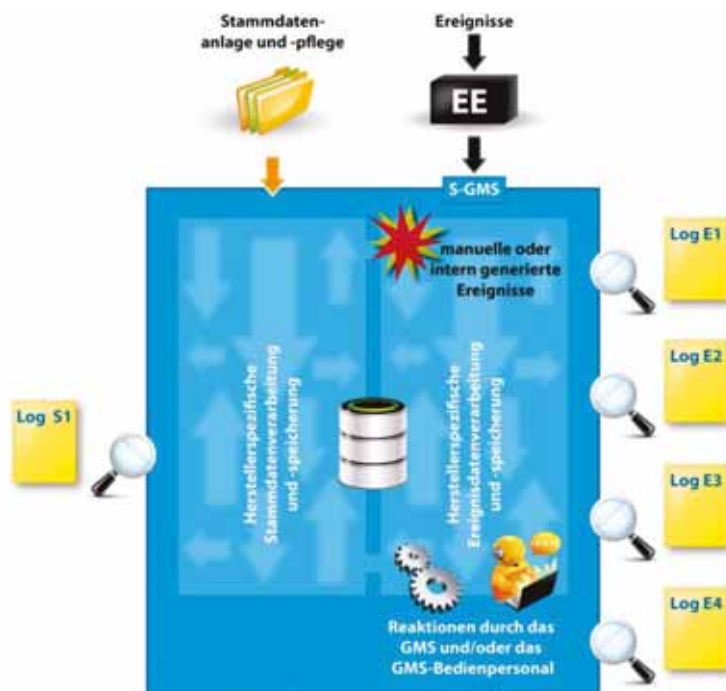


Bild 5-1: Informationsfluss

Stammdaten-Log (Log S1)

Log S1	Stammdatenänderung
Datenumfang	siehe Kapitel 5.7 Stammdaten

Ereignisdaten-Log (Log Ex)

Log E1	Über die S_{GMS} empfangene, unbearbeitete Rohdaten
Datenumfang	Log E1-ID Zeitstempel des GMS ($T_{S_{GMS}}$) empfangener, unbearbeiteter Rohdaten

Log E2	Darstellung der Rohdaten im spezifischen Format des GMS-Herstellers. Dabei können mehrere Log E1-Datensätze zusammengefasst werden oder aus einem Log E1-Datensatz mehrere Log E2-Datensätze generiert werden.
Datenumfang	Log E2-ID Bezug zu Log E1-ID('s) Zeitstempel des GMS ($T_{LOG E2}$) Rohdaten im spezifischen Format des Herstellers

Log E3	<p>Ergebnis der Zusammenführung der Log E2-Datensätze mit eindeutigen Objektidentifikationen und den dazugehörigen Ereignisidentifikationen aus den Stammdaten im GMS.</p> <p>Dabei können mehrere Log E2-Datensätze zusammengefasst werden oder aus einem Log E2-Datensatz mehrere Log E3-Datensätze generiert werden.</p> <p>Log E2-Datensätze, bei denen z. B. wegen fehlender oder fehlerhafter Stammdaten kein Bezug zu einem Objekt und/oder einem Objekt-Ereignis hergestellt werden kann, müssen trotzdem im Log E3 enthalten sein.</p> <p>Interne Ereignisse, die vom GMS (Beispiel: Ereignis aufgrund einer fehlenden Routinemeldung) oder vom Bediener generiert werden.</p>
Datenumfang	Log E3-ID Bezug zu Log E2-ID(s) Zeitstempel des GMS ($T_{LOG E3}$) Identifikationsmerkmal des Objektes Identifikationsmerkmal des Ereignisses

Log E4	<p>Aktion und Reaktion durch das GMS und/oder der Bediener im Rahmen der Behandlung der Log E3-Datensätze.</p> <p>Dabei können mehrere Log E3-Datensätze zusammengefasst werden oder aus einem Log E3-Datensatz mehrere Log E4-Datensätze generiert werden.</p>
Datenumfang	Log E4-ID Bezug zu Log E3-ID(s) Zeitstempel des GMS Informationen zu Reaktionen seitens des GMS und/oder des GMS-Bedienpersonals

Gründe für die vorzeitige Beendigung des Informationsflusses (z. B. durch Informationen im Telegramm) müssen in den Stammdaten, der Dokumentation des GMS oder in den Systemeinstellungen des GMS hinterlegt sein.

5.5.2 Zeitstempel

Das GMS muss die geforderten Zeitstempel generieren und für Auswertungen bereithalten.

Die Zeitstempel der Logs müssen den Zeitpunkt wiedergeben, an dem der jeweils geloggte Vorgang abgeschlossen wurde. Diese müssen in UTC mit einer Auflösungsgenauigkeit von mindestens einer Sekunde wiedergegeben werden können. Zusätzliches Loggen der lokalen Zeit ist möglich. In diesem Fall muss die UTC Zeitangabe klar gekennzeichnet sein.

Das GMS muss die Zeitstempel T_{RX} und $T_{Reaktion}$ in Anlehnung an die EN 50518-2 erfassen und für Auswertungen bereithalten. Als T_{RX} ist der Zeitpunkt des Meldungseingangs an der S_{GMS} zu verwenden. Für Ereignisse, die nicht durch einen Meldungseingang an der S_{GMS} ausgelöst werden, ist der Zeitpunkt der Generierung des Ereignisses als T_{RX} zu verwenden. Als $T_{Reaktion}$ ist der Zeitpunkt des Beginns der Be- oder Verarbeitung zu verwenden.

5.5.3 Manipulation von Daten

Die Daten, aus denen die Logs generiert werden, dürfen nur mittels der vom GMS vorgesehenen Funktionen geändert werden. Es muss erkennbar sein, falls diese Daten nachträglich geändert wurden.

Bemerkung: Unter dem Ändern von Daten ist das Hinzufügen, Verändern oder Löschen zu verstehen.

5.6 Reporting

Das Reporting eines GMS muss als Minimalfunktionalität die Ausgabe der Ereignisdaten und der Stammdaten ermöglichen.

Chronologische Ereignisliste

- Ausgabe der durch die GMS-Verarbeitungsprozesse generierten Ereignisse mit Zeitstempel, Objektbezug und Ereignisbezug.

Protokollierung eines Alarmereignisses

- Ausgabe von Alarmzeitpunkt, Objektbezug und Ereignisbezug. Dokumentation der Reaktionen durch das GMS und/oder des GMS-Bedienpersonals auf Basis der generierten bzw. im Rahmen der Bearbeitung erfassten Informationen (z. B. Alarmbericht, Einsatzzeiten).
- Ausgabe der Stammdaten eines Objektes.

5.7 Stammdaten und Änderungen

Stammdaten zu Subsystemen, Objekten und Abläufen müssen mit Hilfe geeigneter User-Interfaces erfassbar sein.

Alle Einträge und Änderungen müssen so erfasst werden, dass der Zeitpunkt und die ändernde Instanz (Bediener oder Automatismus) erkennbar sind.

Der Zustand der Stammdaten muss für jeden Zeitpunkt innerhalb des vorgehaltenen Zeitraums rückwirkend rekonstruierbar sein. Die Änderung der Stammdaten muss im Log S1 dokumentiert werden.

Bemerkung: Der Zeitraum in dem die Daten vorgehalten werden müssen, muss durch eine externe Vorgabe (z. B. Kundenvorgabe, externe Regelwerke) bestimmt werden.

5.8 Zeitsynchronisierung

Alle Komponenten, die einen Zeitstempel vergeben, verwenden eine auf UTC bezogene Zeit. Die Synchronisierung kann durch das GMS selbst erfolgen oder vom Betreiber des GMS bereitgestellt werden.

Das Fehlen der Synchronisation über mehr als 70 min muss im GMS als Störung behandelt werden.

Tritt bei der Synchronisierung der GMS-Zeit mit der UTC bezogenen Zeit eine Differenz von mehr als 7 s auf, muss dieses als Störung behandelt werden.

Bei Komponenten mit einem GUI für die Alarmbearbeitung muss die durch das GMS verwendete lokale Zeit stets abrufbar sein.

5.9 Bedieneranmeldung

Das GMS darf eine Bedienung erst nach erfolgreicher Identifizierung (Anmeldung) des Bedieners erlauben. Die Identifizierung muss durch ein gesichertes Anmeldeverfahren mittels eines Identifikationsmerkmals des GMS-Bedieners wie z. B. ein Passwort oder biometrische Merkmale erfolgen. Die Identifizierung muss im Log E 4 ersichtlich sein.

Nach der Identifizierung sind dem Bediener vom GMS die entsprechenden Berechtigungen zuzuteilen. Änderungen am Bedienerprofil müssen im Log S1 ersichtlich sein. Die Abmeldung des Bedieners muss im Log E 4 ersichtlich sein.

5.10 Anforderungen externer Regelwerke – optional

Aus externen Regelwerken können sich Anforderungen an das GMS ergeben, die im Rahmen eines Prüf- und Zertifizierungsverfahren geprüft und zertifiziert werden können. Beispiele dafür sind die Normen der Reihe EN 50518, EN 50136-1 und EN 50136-3.

Der Hersteller des GMS dokumentiert vor Beginn der Prüfungen aus welchem externen Regelwerk er zusätzliche Anforderungen erfüllt. Basierend auf einem von der Zertifizierungsstelle von VdS Schadenverhütung GmbH erstellten Prüfplan wird die Übereinstimmung der Angaben während der Prüfung geprüft.

Bei positivem Ausgang der Prüfung wird die Übereinstimmung der dokumentierten und geprüften Angaben des Herstellers ins Zertifikat aufgenommen.

6 Dokumentationspflicht des Herstellers

Der Hersteller eines GMS muss zum Zeitpunkt der Auslieferung des GMS die im Folgenden beschriebenen Dokumentationen bereitstellen. Es muss ein Verfahren beschrieben werden, wie der Hersteller diese Dokumentation aktualisiert oder ergänzt.

Die einzelnen Elemente der Dokumentation müssen nicht als getrennte Dokumente vorliegen, sondern können sinnvoll zusammengefasst werden (z. B. Installations- und Bedienungsanleitung).

6.1 Mindestanforderungen Hard- und Software

Folgende Punkte eines GMS müssen dokumentiert sein und dem Betreiber des GMS zur Verfügung gestellt werden:

- Mindestanforderungen an die unterstützende Hardware.
- Name, Hersteller, Version(en) von unterstützenden Softwareprodukten wie z. B. Betriebssystem(e) mit Version und Service-Pack, Datenbank und Textverarbeitungsprogramm sofern benötigt.
- Modulversionen des GMS, die gemeinsam betrieben werden dürfen.
- Name, Hersteller, Versionen von Systemen (z. B. Empfangseinrichtungen), die über die S_{GMS} angeschlossen werden können. Dabei kann auch auf bereits existierende Spezifikationen und Standards verwiesen werden.
- Hinweise zur Verwendung von Fremdsoftware in der gleichen Software-Umgebung.
- Hinweise zum kontinuierlichen Betrieb des GMS. Mindestens enthalten sein sollten Hinweise zur Datensicherung (Backup), zu Wiederanlauf, zu Systemchecks und zu Redundanz.

6.2 Installationsanleitung

Die Übergabe einer Installationsanleitung und das Inbetriebnahmeprotokoll können zwischen dem Hersteller und dem Betreiber des GMS individuell vereinbart werden.

6.3 Bedienungsanleitung

Eine Bedienungsanleitung beschreibt die Bedienung des GMS und beinhaltet mindestens:

- Versionstand des GMS bzw. der Module, auf die sie sich bezieht
- Beschreibung der Funktionen des GMS und ihrer Benutzung

7 Softwaredokumentation

Die Dokumentation der Software sollte gewährleisten, dass Konstruktion und Programmierschritte zurückverfolgt werden können. Weiterhin sollte die Dokumentation vollständig, korrekt und konsistent sein. Es wird darauf hingewiesen, dass die Prüfung gemäß den zu Grunde liegenden Anforderungen keine Verifikation der Software ist, und nicht sicherstellen kann, dass Software oder Dokumentation fehlerfrei sind.

Die Dokumentation muss dem Betreiber und Anwender nicht zur Verfügung gestellt werden. Es handelt sich um ein internes Dokument des Herstellers des GMS.

7.1 Versionsschema

7.1.1 Anforderung

Ein festes Versionsschema ist vom Hersteller vorzugeben und einzuhalten. Es muss eine Differenzierung bezüglich Umfang und Auswirkung von Modifikationen an den Programmen anhand dieses Schemas festgelegt sein. Dabei muss eine Unterscheidung verschiedener Programmversionen eindeutig möglich sein. Diese sollen mindestens die Änderungen am GMS enthalten.

7.1.2 Prüfung

Es wird überprüft, ob ein festes Versionsschema eingehalten wird. Üblicherweise wird dies durch die Verwendung von Versionierungstools erreicht. Der Hersteller kann jedoch auch ein eigenes Konzept zur Versionierung verwenden. Es muss sich eine Versionshistorie darstellen lassen, welche die wesentlichen Änderungen zu den Vorgängerversionen mindestens stichwortartig beschreibt.

7.2 Entwicklungsdokumentation

7.2.1 Allgemeines

Der Hersteller muss eine Dokumentation vorhalten und pflegen, die einen Überblick über die Funktionalität der Software ermöglicht. Diese Dokumentation muss ausreichend detailliert sein, damit die Übereinstimmung mit den Anforderungen dieser Richtlinien geprüft werden kann.

Die Dokumentation der Software ist grundsätzlich an kein vordefiniertes Format bzw. an keinen vordefinierten strukturellen Aufbau gebunden.

7.2.2 Prüfung

Es wird überprüft, ob die Dokumentation die geforderten Inhalte aufweist.

Die Prüfung erfolgt durch Einsichtnahme in die Dokumentation. Die Dokumente, die die vorgenannten Informationen enthalten, werden bestimmt und festgehalten. Die Ergebnisse werden im Prüfbericht aufgeführt.

Anmerkung: Die in der Entwicklungsumgebung vorgehaltenen Informationen sind ebenfalls Teil der Dokumentation.

7.3 Prozessbeschreibung

7.3.1 Anforderungen

Durch eine Prozessbeschreibung lässt sich die prinzipielle Arbeitsweise des GMS vom auslösenden Ereignis bis zum Ereignisende nachvollziehen. Insbesondere die Generierung der Daten für die Logs E1 bis E4 muss daraus hervorgehen.

Möglich sind grafische Darstellungen (z. B. Sequenzdiagramme, Flow-Charts) oder Beschreibungen in Textform. Dabei sollten die am Prozess beteiligten Softwaremodule kenntlich gemacht werden.

7.3.2 Prüfung

Anhand je eines Beispiels für einen

- automatisierten Verarbeitungsprozess
- Bearbeitungsprozess (durch einen Bediener)

wird geprüft, ob der Ablauf innerhalb des GMS vom Eintreffen der Rohdaten an der S_{GMS} bis zum Abschluss deren Ver- bzw. Bearbeitung anhand der Prozessbeschreibung nachvollziehbar dargestellt ist.

7.4 Programmdokumentation

7.4.1 Anforderungen

Das GMS muss über eine detaillierte Programmdokumentation verfügen.

Diese muss der Prüfstelle nicht eingereicht werden. Sie ist jedoch zur Einsicht in einer Weise bereitzustellen, welche die Rechte des Herstellers auf Vertraulichkeit wahrt. In der Programmdokumentation müssen Beschreibungen aller Programmmodule, so wie sie im Quellcode des Programms implementiert sind, mit jeweils nachstehenden Angaben vorhanden sein:

- a) Name des Moduls
- b) Datum und/oder Versionsreferenz
- c) eine Beschreibung der auszuführenden Aufgaben

Ein Überblick über die zur Erfüllung dieser Richtlinien notwendige Programmarchitektur muss ebenfalls enthalten sein. Die Programmarchitektur soll die oben beschriebenen Programmmodule und deren Wechselwirkung darstellen.

7.4.2 Prüfung

Es wird geprüft, ob eine Dokumentation vorliegt, die die Beschreibungen aller Programmmodule enthält. Jede dieser Beschreibungen sollte mindestens die unter Abschnitt 7.4.1 a) bis c) aufgeführten Inhalte aufweisen.

Anmerkung 1: Es ist nicht erforderlich, dass die Beschreibungen in einem separaten Dokument erfolgen; sie können auch in einem anderen Dokument integriert sein, z. B. in den Quellcode-Header-Dateien oder in einem Metadaten-System.

Es wird anhand von mindestens drei Stichproben überprüft, ob einem Programmmodul ein Name oder eine andere, eindeutig Bezeichnung, eine Versionsnummer und eine Beschreibung zugeordnet sind. Die Dokumente/Absätze, die die geforderten Informationen enthalten, sowie die Art der Beschreibung werden bestimmt und festgehalten. Die Ergebnisse werden im Prüfbericht aufgeführt.

Anmerkung 2: Als Nachweis kann auch ein Ausdruck oder eine Bildschirmkopie des Dokuments/Absatzes gelten.

7.5 Quellcode

7.5.1 Anforderungen

Der Quellcode sollte einschließlich aller globalen und lokalen Variablen, Konstanten und Labels ausreichend Kommentare enthalten. Er muss der Prüfstelle nicht eingereicht werden. Eine Bereitstellung zur Einsichtnahme bei der Vor-Ort Prüfung ist ausreichend.

7.5.2 Prüfung

Anhand von Stichproben wird eine Konsistenzprüfung zwischen Modulbeschreibungen und Quellcode durchgeführt (z. B. wird überprüft, ob ein Quellcode für jedes beschriebene Modul existiert und mit der Beschreibung des jeweiligen Moduls übereinstimmt). Es wird überprüft, ob der Quellcode für einen mit der Programmiersprache vertrauten Softwareentwickler nachvollziehbar gestaltet und angemessen kommentiert ist.

Anmerkung: Der Quellcode sollte mindestens an den nicht sofort erschließbaren Stellen ausreichend kommentiert sein, so dass er nachvollziehbar ist und somit eine mögliche Wartung erleichtert.

7.6 Entwicklungswerkzeuge

7.6.1 Anforderungen

Die Dokumentation muss bezüglich der Entwicklungswerkzeuge mindestens Einzelheiten (Name, Hersteller/Anbieter, Versionsnummer) zu den bei der Programmerstellung verwendeten Software-Werkzeugen (z. B. Entwicklungsumgebung, Assembler usw.) enthalten.

7.6.2 Prüfung

Es wird überprüft, ob die Dokumentation ausreichende Informationen über die Entwicklungs-Werkzeuge bereithält, die für die Entwicklung dieser Software genutzt wurden. Sollten für unterschiedliche Module verschiedene Versionsnummern von Entwicklungswerkzeugen benötigt werden, ist dies ebenfalls zu dokumentieren. Die Quellen, welche die vorgenannten Informationen enthalten, werden bestimmt und festgehalten. Die Ergebnisse werden im Prüfbericht aufgeführt.

7.7 Ablaufüberwachung

7.7.1 Anforderung

Der Hersteller dokumentiert, welche Module auf welcher Art und Weise innerhalb des GMS überwacht werden. Durch die Dokumentation muss sich die prinzipielle Arbeitsweise des Überwachungskonzeptes des GMS nachvollziehen lassen. Insbesondere die Sicherstellung der unter Kapitel 5 genannten Funktionen muss daraus hervorgehen.

Möglich sind grafische Darstellungen (z. B. Sequenzdiagramme, Flow-Charts, etc.) oder Beschreibungen in Textform. Dabei sollten die am Prozess beteiligten Softwaremodule kenntlich gemacht werden.

7.7.2 Prüfung

Anhand der unter 7.3.2 verwendeten Beispiele wird die Dokumentation der Ablaufüberwachung von zwei beteiligten Modulen geprüft.


8 Prüfmethoden

Diese Richtlinien enthalten Anforderungen und teilweise auch Prüfmethoden, die zum Nachweis der Einhaltung der Anforderungen geeignet sind.

Der Nachweis für die Einhaltung von Anforderungen, der nicht durch Prüfmethoden beschrieben ist, erfolgt durch eine Begutachtung des Produktes oder der Dokumentation durch einen kompetenten Prüfer. Durch geeignete Funktions- und Dokumentationsprüfungen werden dabei objektive Nachweise erbracht, die zum Nachweis der Einhaltung der Anforderungen dienen.

Vor der eigentlichen Prüfung reicht der Hersteller des GMS die unter Punkt 6 und 7 dieser Richtlinien genannten Dokumentationen zur Vorprüfung ein. Anhand der Dokumentationen und des vom Hersteller beauftragten Zertifizierungsumfanges wird dann ein geeigneter Prüfplan erstellt, in dem die notwendigen Prüfungen festgelegt sind.

Anhang A Auftrag zur Anerkennung von Gefahrenmanagementsystemen auf Grundlage der VdS 3534

Auftrag zur Anerkennung von Gefahrenmanagementsystemen auf Grundlage der VdS 3534 durch die Zertifizierungsstelle von VdS Schadenverhütung, Amsterdamer Straße 174, 50735 Köln		
<input type="checkbox"/> Erstauftrag zur Anerkennung <input type="checkbox"/> Verlängerungsauftrag zur Anerkennung		Nr. S 7 <input type="text"/>
(Bitte vollständig ausfüllen!)		
1 Auftraggeber		
1.1	Firmenname	<input type="text"/>
1.2	Vertretungsberechtigt (bei Kapital- und Personengesellschaften)	<input type="text"/>
1.3	USt.IdNr.	<input type="text"/>
1.4	Straße/Haus-Nr.	<input type="text"/>
1.5	Land/PLZ/Ort	<input type="text"/>
1.6	Tel.-Nr./Fax-Nr.	<input type="text"/>
1.7	E-Mail-Adresse	<input type="text"/>
1.8	Internetadresse	<input type="text"/> <input type="checkbox"/> nicht vorhanden
1.9	Kontaktperson	<input type="text"/>
2 System für das die Anerkennung/Prüfung beauftragt wird		
2.1	Systembezeichnung	<input type="text"/>
2.2	Verwendung in (Anlagentyp und ggf. Klasse, z.B. EMA Klasse A)	<input type="text"/>
2.3	Anerkennungs-/ Prüfgrundlage(n)	<input type="text"/>
2.4	<input type="checkbox"/> Neben der deutschsprachigen Ausfertigung des Prüfberichtes wird eine englischsprachige Fassung gewünscht	
2.5	<input type="checkbox"/> Neben der deutschsprachigen Ausfertigung des Zertifikates über die Anerkennung wird eine englischsprachige Fassung gewünscht	
3 Fertigungsstätte des Systems		
	Auftraggeber ist mit Fertigungsstätte identisch <input type="checkbox"/> Ja (Punkt 3 entfällt) <input type="checkbox"/> Nein (Bitte Punkt 3.1-3.5 ausfüllen)	
3.1	Firmenname	<input type="text"/>
3.2	Straße/Haus-Nr.	<input type="text"/>
3.3	Land/PLZ/Ort	<input type="text"/>
3.4	Tel.-Nr./Fax-Nr.	<input type="text"/>
3.5	E-Mail-Adresse	<input type="text"/>
4 Der Auftraggeber erklärt,		
	die Richtlinien VdS 2344 „Verfahren über die Prüfung, Anerkennung, Zertifizierung und Konformitätsbewertung von Geräten, Bauteilen und Systemen der Brandschutz- und Sicherheitstechnik“ (insbesondere Abschnitte 7.4, 7.5, 7.6), die Richtlinien VdS 2841 „Durchführung von Produktüberwachungen“, die zugehörigen Gebührentabellen und die Allgemeinen Geschäftsbedingungen, VdS 3177, habe(n) ich (wir) zur Kenntnis genommen und erkenne(n) sie als Vertragsbestandteil an. Abweichend von den Richtlinien VdS 2344 beträgt die Laufzeit der Anerkennung drei Jahre ab Ausstellungsdatum und erfordert kein QM-System. Ersatzregelungen für Hersteller ohne QM-System werden nicht herangezogen. Die Produktüberwachung erfolgt jährlich durch Dokumentationsprüfung, ggf. mittels Audit vor Ort (VdS 2841, Abs. 1.3, Modul 1).	
	Der Auftraggeber erklärt ferner sein Einverständnis, dass die Prüfung des Gefahrenmanagementsystems ganz oder teilweise an dem in Punkt 3 genannten Ort stattfindet, an dem ein entsprechendes Gefahrenmanagementsystem zu Prüfzwecken aufgebaut ist und bestätigt, dass für den Prüfer Zugriff auf Quellcodes, Dokumentation, Einstellungen und Konfigurationen besteht.	
	<input type="checkbox"/> Wir willigen ein, dass VdS Schadenverhütung GmbH im Rahmen des Anerkennungsverfahrens Daten erhebt, verarbeitet, nutzt, in einem Verzeichnis führt und die Anerkennung als Errichterunternehmen Dritten mitteilt.	
	Datum	Stempel und Unterschrift des Bevollmächtigten

Anhang B **Checkliste zur Vorbereitung der Prüfung nach VdS 3534**

Sehr geehrte Kundin, sehr geehrter Kunde,

Sie möchten Ihr Gefahrenmanagementsystem nach den VdS-Richtlinien 3534 anerkennen lassen. Um Zeitaufwand und Kosten der Prüfung im Rahmen zu halten, bitten wir Sie, diese Liste zur Vorbereitung der Prüfung auszufüllen und uns zusammen mit der Dokumentation zukommen zu lassen. Die Formulierungen in der Spalte „geforderte Information“ sind teilweise gekürzt zusammengefasst. Es gelten die Formulierungen in den Richtlinien.

Die Liste kann Ihnen als roter Faden durch die Anforderungen der Richtlinien VdS 3534 dienen.

Stellen Sie uns bitte die Dokumentation, soweit möglich, im Vorfeld des Vor-Ort-Termins zur Verfügung. Nachweise zur Erfüllung der Anforderungen, die nur direkt vor Ort am GMS oder am Entwicklungssystem geführt werden können, bitten wir in der rechten Spalte zu kennzeichnen.

Es wird darauf hingewiesen, dass die Prüfung gemäß den zu Grunde liegenden Anforderungen keine Verifikation der Software ist, und nicht sicherstellen kann, dass Software oder Dokumentation fehlerfrei sind.

Bei Fragen wenden Sie sich bitte an das Labor für Software.

Auftragsnummer (falls schon bekannt)		
Auftraggeber	Firma / Name	
	Straße u. Nr.	
	Land, PLZ, Ort	
Produkt, in dem die Software verwendet wird (Verkaufsbezeichnung)		
Stand/Version/Release des GMS (Werden anstatt einer übergeordneten Gesamtversionierung die Teilsysteme des GMS separat versioniert, ggf. eine Liste beifügen)		

A. Anforderungen an die Funktion (VdS 3534, Abschnitt 5)			
Bezug zu den Richtlinien	geforderte Information	Information ist zu finden in Dokument (ggf. Angabe von Kapitel/Seite) bzw. Der Nachweis kann geführt werden durch/anhand/...	[X], wenn Nachweis vor Ort geführt werden kann
5.2	Alarmempfang: Von Alarmsignalen an das GMS, die nur von einem Bediener ausgewertet werden können (z. B. Sprachmeldungen), müssen die Informationsinhalte des Alarms ebenfalls gespeichert werden.		
5.3	Störungen: Das GMS muss seine ordnungsgemäße Funktion sowie die Funktion der verwendeten Hard- und Softwarekomponenten laufend überwachen.		
5.3.1	Erkennung von: Störungen oder Ausfall von Teilen der GMS-Software.		
	Erkennung von: Manuelle Eingabe ungültiger Daten.		
	Erkennung von: Empfang von Daten, die nicht durch das GMS interpretiert oder korrekt verarbeitet werden können.		
5.3.1	Erkennung von: Störung oder Ausfall unterstützender Hardware		
	Erkennung von: Störungen oder Ausfall unterstützender Software		
	Weitere „Störungserkennungen“ des GMS können hier (oder mit Verweis separat) aufgeführt werden, sofern sie in die Zertifizierung mit einfließen sollen		
5.3.2	Störungsvermeidung: Inhaltliche Überprüfung manueller Eingaben in Eingabefeldern auf ungültige oder fehlerhafter Daten (sofern eine solche Überprüfung logisch möglich ist)		
5.3.3	Störungsbehandlung: Bei einer erkannten Störung muss mindestens eine eindeutige Meldung erfolgen und die Störung ist im Log E4 zu speichern. Es ist zu dokumentieren, wie der Betreiber sicherstellen kann, dass die Meldung von einem Bediener empfangen und bearbeitet werden kann.		

A. Anforderungen an die Funktion (VdS 3534, Abschnitt 5)			
Bezug zu den Richtlinien	geforderte Information	Information ist zu finden in Dokument (ggf. Angabe von Kapitel/Seite) bzw. Der Nachweis kann geführt werden durch/anhand/...	[X], wenn Nachweis vor Ort geführt werden kann
5.4	Überwachung der von der Zertifizierung umfassten Subsysteme. Meldung im GMS bei Verbindungsausfall zum Subsystem. Das Fehlen einer Überwachung ist vom Hersteller zu dokumentieren.		
5.5.1	Protokollierung: Alle Logfiles werden geführt bzw. der protokollierte Informationsfluss ist in Form der Standard-Logfiles S1 und E1-E4 darstellbar.		
5.5.2	Zeitstempel (UTC, Auflösung mind. 1.Sek, T_{RX} und $T_{Reaktion}$ in Anlehnung an die EN 50518-2)		
5.5.3	Manipulation der Protokolldaten muss erkennbar sein		
5.6	Reporting enthält den geforderten Mindestumfang		
5.7	Stammdaten müssen mit Hilfe geeigneter User-Interfaces erfassbar sein. Bei Änderungen sind Zeitpunkt und die ändernde Instanz erkennbar. Stammdatenänderungen werden in Log S1 dokumentiert. Rückwirkende Rekonstruierbarkeit.		
5.8	Zeitsynchronisierung der Komponenten durch GMS oder Betreiber. Störungsmeldung bei Fehlen der Synchronisation ab 70+ min und bei Abweichung der GMS Zeit zu UTC von mehr als 7s. Lokale Zeit bei vorhandenen GUI-Komponenten stets abrufbar.		
5.9	Bedieneranmeldung: Identifizierung muss durch ein gesichertes Anmeldeverfahren erfolgen.		
5.10	Anforderungen externer Regelwerke – optional.		

B. Dokumentationspflicht (VdS 3534, Abschnitt 6)			
Bezug zu den Richtlinien	geforderte Information	Information ist zu finden in Dokument (ggf. Angabe von Kapitel/Seite)	[X], wenn Nachweis vor Ort geführt werden kann
6.1	Folgende Informationen sind in für den Betreiber zur Verfügung stehenden Dokumenten vorhanden:		
	Die Mindestanforderungen an die unterstützende Hardware.		
	Name, Hersteller, Version(en) von unterstützenden Softwareprodukten wie z. B. Betriebssystem(e) mit Version und Service-Pack, Datenbank und Textverarbeitungsprogramm sofern benötigt.		
	Modulversionen des GMS, die gemeinsam betrieben werden dürfen.		
	Name, Hersteller, Versionen von Systemen (z. B. Empfangseinrichtungen), die über die S _{GMS} angeschlossen werden können.		
6.1	Hinweise zur Verwendung von Fremdsoftware in der gleichen Software-Umgebung.		
	Hinweise zum kontinuierlichen Betrieb des GMS. Mindestens enthalten sein sollten Hinweise zur Datensicherung (Backup), zu Wiederanlauf, zu Systemchecks und zu Redundanz.		
6.2	Installationsanleitung/Übergabeprotokoll		
6.3	Bedienungsanleitung		

C. Softwaredokumentation (VdS 3534, Abschnitt 7)			
Bezug zu den Richtlinien	geforderte Information	Information ist zu finden in Dokument (ggf. Angabe von Kapitel/Seite)	[X], wenn Nachweis vor Ort geführt werden kann
7.1	Nachweis der Verwendung eines festen Versionsschemas.		
7.2	Eine Entwicklungsdokumentation wird vorgehalten und gepflegt.		
7.3	Eine Prozessbeschreibung anhand von mind. 2 Beispielen.		
7.4	Programmdokumentation (Beschreibung der Programmmodule und deren Aufgaben; Darstellung der Programmarchitektur)		
7.5	Quellcode (Sind „ausreichend“ erklärende Kommentare vorhanden? Sind Beschreibungen konsistent zum Quellcode?)		
7.6	Angaben zu den verwendeten Entwicklungswerkzeugen.		
7.7	Ablaufüberwachung/Überwachungskonzept		

Bitte beachten Sie:

Diese Checkliste basiert auf den Richtlinien "VdS 3534 – Gefahrenmanagementsysteme". Sie dient zur Unterstützung beim Zusammentragen der geforderten Dokumente und Informationen sowie bei der Vorbereitung. Sie ersetzt nicht die genauen Anforderungen der Richtlinien. Die Liste erhebt keinen Anspruch auf Vollständigkeit.