

Technische Richtlinie der Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

Geräte für die digitale Funkalarmierung

Stand: Januar 2026

Herausgeber:

Ausschuss für Informations- und Kommunikationswesen (AIuK) des Arbeitskreises V
„Feuerwehrangelegenheiten, Rettungswesen, Katastrophenschutz, Zivilverteidigung“
der Arbeitsgemeinschaft der Innenministerien der Länder

Redaktion:

Ausschuss für Informations- und Kommunikationswesen und Zentralprüfstelle für drahtlose Fernmeldegerä-
te bei der Landesfeuerwehrschule Baden-Württemberg

Normative Verweise:

DIN 66003, Ausgabe:1999-02
Informationstechnik - 7-Bit-Code

ISO/IEC 646, Ausgabe:1991-12
Informationstechnik; ISO 7-bit codierter Zeichensatz für Informationsaustausch

DIN EN 55022, Ausgabe: 2011-10 entsprechend **VDE 0878-22** 2016-08
Einrichtungen der Informationstechnik - Funkstöreeigenschaften - Grenzwerte und Messverfahren

DIN EN 60721-3-0, Ausgabe: 2021-08
Klassifizierung von Umweltbedingungen; Teil 3: Klassen von Umwelteinflußgrößen und deren Grenzwerte;
Einführung (IEC 60721-3-0:1984 + A1:1987); Deutsche Fassung EN 60721-3-0:1993

E - DIN 40046-721-3, Ausgabe:2004-11
Leitfaden für die Korrelation und Umsetzung der Klassen von Umgebungsbedingungen nach IEC 60721- 3
in Prüfverfahren nach IEC 60068 - Ortsfester Einsatz, wettergeschützt (IEC/TR 60721)

DIN EN 300113, Ausgabe: 2020-06
Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Mobiler Landfunkdienst
- Funkgeräte, die für die Übertragung von Daten (und/oder Sprache) mit konstanter oder nicht konstanter
Hüllkurvenmodulation ausgelegt sind und einen Antennenstecker haben

DIN VDE 0877-3, Ausgabe:1980-04 (EN 55016-2-6 2007-08)
Das Messen von Funkstörungen; Das Messen von Funkstörleistungen auf Leitungen [VDE-Bestimmung]

DIN EN 60529, Ausgabe: 2014-09
Schutzarten durch Gehäuse (IP-Code) (IEC 60529:1989 + A1:1999); Deutsche Fassung EN 60529:1991
+ A1:2000

DIN EN 300341-1, Ausgabe:2001-06
Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Mobiler Landfunkdienst
(RP02); Funkgeräte mit eingebauter Antenne, die Signale zur Initialisierung einer spezifischen Antwort im
Empfänger senden - Teil 1: Technische Kennwerte und Messverfahren (Anerkennung der englischen Fas-
sung EN 300341-1 V 1.3.1 (2000-12) als Deutsche Norm)

DIN EN 300341-2, Ausgabe:2001-06
Elektromagnetische Verträglichkeit und Funkspektrumangelegenheiten (ERM) - Mobiler Landfunkdienst
(RP 02); Funkgeräte mit eingebauter Antenne, die Signale zur Initialisierung einer spezifischen Antwort im
Empfänger senden - Teil 2: Harmonisierte EN nach Artikel 3.2 der R&TTE-Richtlinie (Anerkennung der
englischen Fassung EN 300341-2 V 1.1.1 (2000-12) als Deutsche Norm)

RED 2014/53/EU

Safety

EN 62368-1:2020 + A11:2020

EMC

ETSI EN 301489-1 V2.2.3 (2019-11)

ETSI EN 301489-2 V2.1.1 (2019-04)

ETSI EN 301489-17 V3.2.4 (2020-09)

Radio

ETSI EN 300390 V2.1.1 (2016-03)

ETSI EN 300328 V2.2.2 (2019-07)

Ersatz für BAPT 222 TE 20, Ausgabe 1996-10

DIN EN 60068 Umgebungseinflüsse

Teil 2-6 Ausgabe 10-2008	Schwingbeanspruchung
Teil 2-7 Ausgabe 03-1995	gleichförmige Beschleunigung
Teil 2-31 Ausgabe 04-2009	Schockbeanspruchung

(EU) 2016/679 Datenschutz-Grundverordnung (DSGVO)

Inhaltsverzeichnis

Vorbemerkung	9
0. Regelungsgegenstand.....	9
1. Interoperabilität.....	9
2. Rufsystem.....	10
2.1. Übertragungscode auf dem Funkweg.....	10
2.1.1. Präambel.....	10
2.1.2. Codewortgruppe.....	10
2.1.3. Codewortarten.....	10
2.1.3.1. Synchronwort.....	11
2.1.3.2. Adresswort.....	11
2.1.3.3. Nachrichtenwort.....	11
2.1.3.4. Füllwort.....	11
2.1.4. Erzeugung der Prüfbits.....	12
2.1.5. Nachrichtenformat für Alphanumerik-Empfänger.....	12
3. Funknetzorganisation	13
4. Rufarten.....	15
4.1. Einzelruf.....	15
4.2. Sammelruf.....	15
4.3. Gruppenruf.....	15
5. Verschlüsselung	15
5.1. Einheitliches Verschlüsselungsverfahren.....	15
5.2. Schlüsselmanagement	15
5.3. Einführung des einheitlichen Verschlüsselungsverfahrens.....	15
6. Verteilung der möglichen Adresskodierungen pro Frequenz auf Bund und Länder.....	16
Teil A: DIGITALE ALARMGEBER.....	17
A.1. Aufgabe	17
A.2. Baustufen.....	17
A.2.1. Baustufe I.....	17
A.2.2. Baustufe II.....	17
A.2.3. Baustufe III	17
A.3. Technische Forderungen	18
A.3.1. Elektromagnetische Verträglichke	18
A.3.2. Stromversorgung.....	18
A.4. Konstruktive Forderungen.....	18
A.4.1. Typenschild.....	18
A.4.2. Aufbau.....	18
A.4.2.1. Beanspruchung.....	18
A.4.2.2. Betriebsbedingungen	18

A.5.	Anschaltung (Schnittstelle DAG-DAU).....	19
A.6.	Technische Unterlagen	19
Teil B: DIGITALE ALARMUMSETZER		20
B.1.	Aufgabe	20
B.2.	Baustufen.....	20
B.2.1.	Baustufe I.....	20
B.2.2.	Baustufe II.....	20
B.3.	Technische Forderungen	20
B.3.1.	Allgemeines	20
B.3.1.1.	Frequenzbereich.....	21
B.3.1.2.	Verträglichkeit.....	21
B.3.2.	Sender	21
B.3.2.1.	Sendeleistung.....	21
B.3.2.2.	Nachbarkanalleistung.....	21
B.3.2.3.	Nebenaussendungen.....	21
B.3.2.4.	Intermodulationsdämpfung	21
B.3.2.5.	Modulator.....	21
B.3.2.6.	Sendefrequenz.....	21
B.3.3.	Empfänger.....	22
B.3.3.1.	Empfindlichkeit	22
B.3.4.	Stromversorgung.....	22
B.4.	Konstruktive Forderungen.....	22
B.4.1.	Gestaltung	22
B.4.2.	Typenschild.....	22
B.4.3.	Aufbau.....	22
B.4.4.	Beanspruchung.....	22
B.4.4.1.	Schutzart	23
B.4.4.2.	Betriebsbedingungen	23
B.4.4.2.1.	Normale Betriebsbedingungen.....	23
B.4.4.2.2.	Extreme Betriebsbedingungen	23
B.4.4.3.	Mechanische Beanspruchung.....	23
B.5.	Anschaltung.....	23
B.6.	Technische Unterlagen	23
B.7.	Voraussetzungen für die Prüfung nach dieser Richtlinie	23
Teil C: DIGITALE MELDEEMPFÄNGER		24
C.1.	Aufgabe	24
C.2.	Verwendungsarten.....	24
C.3.	Technische Forderungen	24
C.3.1.	Allgemeines	25
C.3.2.	Referenzsignal.....	25
C.3.2.1.	Definition.....	25
C.3.2.2.	Verfahren zur Bestimmung des Referenzsignals.....	25
C.3.2.3.	Grenzwerte.....	26

C.3.3.	Empfindlichkeit.....	26
C.3.3.1.	Allgemeines	26
C.3.3.2.	Statische Empfindlichkeit	26
C.3.3.2.1.	Empfindlichkeit im Freifeld.....	26
C.3.3.2.1.1.	Definition	26
C.3.3.2.1.2.	Messverfahren.....	26
C.3.3.2.1.3.	Grenzwerte.....	27
C.3.3.3.	Empfindlichkeit beim Tragen am Körper	27
C.3.3.3.1.	Definition	27
C.3.3.3.2.	Messverfahren	28
C.3.3.3.3.	Grenzwert.....	28
C.3.4.	Gleichkanalunterdrückung	29
C.3.4.1.	Definition	29
C.3.4.2.	Messverfahren.....	29
C.3.4.3.	Grenzwert.....	29
C.3.5.	Nachbarkanaldämpfung	30
C.3.5.1.	Definition.....	30
C.3.5.2.	Messverfahren.....	30
C.3.5.3.	Grenzwerte.....	30
C.3.6.	Nebenempfangsdämpfung.....	30
C.3.6.1.	Definition.....	30
C.3.6.2.	Messverfahren.....	30
C.3.6.3.	Grenzwerte.....	31
C.3.7.	Intermodulationsdämpfung	31
C.3.7.1.	Definition.....	31
C.3.7.2.	Messverfahren.....	31
C.3.7.3.	Grenzwert.....	32
C.3.8.	Verhalten gegenüber hohen Nutzfeldstärken	32
C.4.	Funktionale Forderungen.....	32
C.4.1.	Allgemeines	32
C.4.2.	Adresskodierung	32
C.4.3.	Nachrichtenspeicherung.....	33
C.4.4.	Rufsignalisierung	33
C.4.4.1.	Rufanzeige	33
C.4.4.2.	Akustischer Alarm	33
C.4.4.3.	Speicheralarm	34
C.4.4.4.	Stiller Alarm (Option).....	34
C.4.5.	Dekodierungsanforderungen.....	34
C.4.5.1.	Allgemeines	34
C.4.5.2.	Fehlererkennung und -korrektur	34
C.4.5.3.	Wiedergewinnung der Synchronität.....	34
C.4.5.3.1.	Definition.....	34
C.4.5.3.2.	Messverfahren.....	34
C.4.5.3.3.	Grenzwert.....	35
C.4.5.4.	Ende einer Nachricht	35

C.4.5.5.	Rufwiederholung	35
C.4.6.	Nachrichtenanzeige	35
C.4.7.	Maximale Nachrichtenlänge je Alarmruf.....	36
C.4.8.	Funkversorgungsanzeige.....	36
C.5.	Konstruktive Forderungen.....	36
C.5.1.	Aufbau.....	36
C.5.1.1.	Gehäuse.....	36
C.5.1.2.	Typenschild	36
C.5.1.3.	Beleuchtung	36
C.5.2.	Beanspruchung.....	37
C.5.2.1.	Schutzart	37
C.5.2.2.	Schockbeanspruchung	38
C.5.2.3.	Schwingbeanspruchung	38
C.5.2.4.	Klimatische Beanspruchung	38
C.5.2.4.1.	<i>Normale Beanspruchung</i>	38
C.5.2.4.2.	<i>Extreme Beanspruchung</i>	38
C.6.	Stromversorgung	38
C.6.1.	Akkubetrieb.....	38
C.6.2.	Betrieb mit Heimzusatz.....	39
C.7.	Technische Unterlagen	39
Teil D:	DIGITALE SIRENENSTEUEREMPFÄNGER	40
D.1.	Aufgabe	40
D.2.	Technische Forderungen	40
D.2.1.	Sabotageschutz.....	40
D.2.2.	Empfangssignal.....	40
D.2.3.	Empfänger.....	40
D.2.3.1.	Empfindlichkeit	40
D.2.4.	Auswertung	41
D.2.5.	Stromversorgung.....	41
D.3.	Konstruktive Forderungen.....	42
D.3.1.	Gestaltung	42
D.3.2.	Typenschild.....	42
D.3.3.	Aufbau.....	42
D.3.4.	Beanspruchung.....	42
D.3.4.1.	Schutzart	42
D.3.4.2.	Betriebsbedingungen	42
D.3.4.2.1.	Normale Betriebsbedingungen.....	42
D.3.4.2.2.	Extreme Betriebsbedingungen	42
D.3.4.2.3.	Mechanische Beanspruchung.....	42
D.4.	Technische Unterlagen	43
Teil E –	Verschlüsselungsverfahren für die digitale Funkalarmierung.....	44
E.1.	Einleitung	44

E.2.	Leistungsmerkmale	44
E.3.	Verfahrensbeschreibung	44
E.3.1.	AES-256	44
E.3.1.1.	Verschlüsselung	45
E.3.1.2.	Entschlüsselung	45
E.3.2.	Daten-Authentisierung AES-CMAC (128 Bit)	46
E.3.3.	Erzeugung von abgeleiteten Schlüsseln	46
E.3.4.	Schlüsselmanagement	46
E.3.4.1.	Schlüsselindex	46
E.3.4.2.	Dynamische Schlüsselwahl	46
E.3.5.	Header der Geheimnachricht	46
E.3.5.1.	Initialisierungsvektor (IV)	47
E.3.5.2.	Schlüsselindex	47
E.3.5.3.	Header-Prüfsumme	47
E.3.5.4.	Meldungsintegrität	47
E.3.5.5.	Zusammenfassung Header	48
E.3.6.	Verschlüsselungs-Algorithmus AES-256 im Counter Mode (CTR)	48
E.3.6.1.	Initialisierung des Zählerblocks	48
E.3.6.2.	Erzeugung von abgeleiteten Schlüsseln	48
E.3.6.3.	Verschlüsselung / Entschlüsselung	49
E.3.6.4.	Störanfälligkeit	49
E.4.	POCSAG Geheimnachricht	50
E.4.1.	Textformat - NUMERIK	50
E.4.2.	Verschleierung der Meldungslänge (Padding)	50
E.5.	Beispiel Verschlüsselung	50
E.5.1.	Abgeleitete Schlüssel	50
E.5.2.	Geheimtext	51
E.5.3.	Prüfsumme MAC	52
E.5.4.	Header	52
E.5.5.	Geheimnachricht NUMERIK	52
E.6.	Optionen	52
E.6.1.	Base64-Codierung der Nachricht und Alphanummerische Übertragung	52
E.6.2.	Geheimnachricht Option BASE64	53
E.7.	Prüfung der Endgeräte auf Einhaltung des Verfahrens	53
E.7.1.	Setzen der korrekten Zeit	53
E.7.2.	Entschlüsselung von Meldungen	53
E.7.3.	Textlänge	53
E.7.4.	Dynamische Schlüsselwahl	53
E.7.5.	Zeitauthentifizierung	54
E.7.6.	Meldungsintegrität	54
E.7.7.	Erkennung von unverschlüsselten Nachrichten	54
E.7.8.	Steuerkommandos	54

Vorbemerkung

Ziel dieser Richtlinie ist die Sicherstellung der technischen Interoperabilität von POCSAG-Netzen und Endgeräten u. a. durch die verbindliche Festlegung eines einheitlichen Verschlüsselungsstandards. Sie legt einen Mindeststandard fest. Dieser wird ständig weiterentwickelt.

0. Regelungsgegenstand

Diese Technische Richtlinie BOS legt die technischen Einzelheiten für die POCSAG-Alarmierung fest.

Diese Richtlinie beschreibt die („Luft-“) Schnittstelle zwischen den Digitalen Alarmumsetzern (DAU) und den Digitalen Meldeempfängern (DME) bzw. Digitalen Sirenensteuerempfängern (DSE). Durch das beschriebene Übertragungsprotokoll und die vorgegebenen Leistungsmerkmale soll sichergestellt werden, dass in einem Alarmierungsnetz die DME bzw. DSE unabhängig vom Fabrikat des Herstellers der Netzkomponenten uneingeschränkt betrieben werden können (Interoperabilität). Im Sinne dieser zwingend erforderlichen Interoperabilität zwischen Alarmierungsinfrastruktur (DAG/DAU) und Endgeräten (DME/DSE) sind proprietäre, nicht öffentlich zugängliche, lizenzpflichtige sowie von dieser Richtlinie abweichende Verfahren und Verschlüsselungen nicht zulässig.

Die Richtlinie beschreibt nicht die notwendigen Steuerinformationen, die zwischen den DAU mit oder ohne angeschlossenen Digitalen Alarmgeber (DAG) ausgetauscht werden müssen, um eine Weitergabe der Alarmrufe zu erreichen. Bei der Erweiterung eines bestehenden Alarmierungssystems (= Funkverkehrs-kreis / gleiche Frequenz) sind die zusätzlichen DAU entsprechend einzustellen.

Im Unterschied zu Alarmumsetzern in analoger Technik ist das Sendeempfangsgerät integrierter Bestandteil des digitalen Alarmumsetzers, eine Beschreibung in einer besonderen Technischen Richtlinie ist somit nicht erforderlich. Bei der Alarmierungsstelle sind daher ein DAG und ein abgesetzter DAU notwendig. Ebenso kann der DAU bedarfsweise auch die Funktion der ortsfesten Empfangsfunkanlage für Sirenensteuerung übernehmen.

1. Interoperabilität

Für den Meldungstext/Alarmierungsnachricht muss die Interoperabilität sichergestellt werden. Das bedeutet konkret:

- Alle übertragenen Daten müssen richtig gelesen und verarbeitet werden können.
- Endgeräte und Netze können direkt zusammenarbeiten, ohne Speziallösungen.
- Die Kommunikation funktioniert standardisiert, vorhersehbar und zuverlässig.

Dies hat zur Folge, dass

- alle Verfahren zur Datenübertragung und deren Bedeutung offengelegt werden müssen.
- eine Verschlüsselung der RIC nicht stattfindet.

Entsprechend dem European Interoperability Framework (EIF) dürfen nur Verfahren und Zusatzfunktionen zum Einsatz kommen, die öffentlich dokumentiert sind. Zusatzfunktionen sind Funktionen, die über den Regelungsgehalt der TR BOS hinausgehen. Sie sind nicht öffentlich dokumentiert und dürfen nur verwendet werden, wenn auch Komponenten ohne Nutzung dieser Funktionen interoperabel betrieben werden können. Sofern Zusatzfunktionen lizenzpflichtig sind, dürfen die Lizenzen nur unter fairen, vernünftigen und nicht-diskriminierenden Bedingungen (FRAND) angeboten werden. Die Entscheidung zur Verwendung von Zusatzfunktionen obliegt den nutzenden Organisationen des jeweiligen Alarmierungsnetzes im Benehmen mit den Netzbetreibern. Bei neuen Projekten sind lizenzfreie Lösungen anzuwenden, sofern verfügbar.

2.1.3.1. Synchronwort

Das Synchronwort ist wie folgend dargestellt aufgebaut:

Bit Nr.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit:	0	1	1	1	1	1	0	0	1	1	0	1	0	0	1	0
Bit Nr.	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Bit:	0	0	0	1	0	1	0	1	1	1	0	1	1	0	0	0

2.1.3.2. Adresswort

Das Adresswort ist wie folgend dargestellt aufgebaut:

Bit Nr.	1	2 bis 19	20	21	22 bis 31	32
Bit	0	Adressbits	Funktionsbits		Prüfbits	Schlussbit

Das Bit Nr. 1 eines Adresswortes besteht immer aus einer Null. Dadurch unterscheidet es sich von einem Nachrichtenwort.

Die Bit Nr. 2 bis Nr. 19 sind Adressbits, die den 18 Bits des einem Empfänger zugeordneten Adresscodes entsprechen.

Die Bits Nr. 20 und 21 stellen die Funktionsbits dar. Die Bits Nr. 22 bis Nr. 31 sind Prüfbits.

Das Schlussbit Nr. 32 wird nur gesetzt, um eine gerade Parität über alle Bit von Nr. 1 bis Nr. 32 zu erhalten.

2.1.3.3. Nachrichtenwort

Das Nachrichtenwort ist wie folgend dargestellt aufgebaut:

Bit Nr.	1	2 bis 21	22 bis 31	32
Bit	1	Nachrichtenbits	Prüfbits	Schlussbit

Nachrichtenwörter können in jedem Rahmen übertragen werden. Sie folgen direkt auf das zugeordnete Adresswort. Die Nachrichtenwörter bestehen aus 20 Nachrichtenbits, nämlich den Bits Nr. 2 bis Nr. 21. Darauf folgen die Prüfbits, die entsprechend 2.1.4 gebildet werden.

2.1.3.4. Füllwort

Das Füllwort (Idleword) ist wie folgend dargestellt aufgebaut:

Bit Nr.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bit	0	1	1	1	1	0	1	0	1	0	0	0	1	0	0	1
Bit Nr.	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32
Bit	1	1	0	0	0	0	0	1	1	0	0	1	0	1	1	1

Wenn kein Nachrichten- oder Adresswort vorhanden ist, wird stattdessen ein Füllwort übertragen. Das Füllwort stellt ein gültiges Adresswort dar, das den Meldeempfängern nicht zugeordnet werden darf.

2.1.4. Erzeugung der Prüfbits

Jedes Codewort besteht aus 21 Informationsbits (Bit Nr. 1 bis Nr. 21), die zu den Koeffizienten eines Polynoms mit Gliedern von X^{30} bis X^{10} korrespondieren. Dieses Polynom wird geteilt (Modulo 2) durch das Generatorpolynom $X^{10} + X^9 + X^8 + X^6 + X^5 + X^3 + X^0$. Die Prüfbits entsprechen den Koeffizienten der Glieder von X^9 bis X^0 im nach der Division verbleibenden Restpolynom. Zu den 31 Bits wird ein 32. Bit hinzugefügt, das der Prüfung der geraden Parität des gesamten Codewortes dient.

2.1.5. Nachrichtenformat für Alphanumerik-Empfänger

Bei Alphanumerik-Empfängern werden die Bits jedes Zeichens mit Bit Nr. 1 (d. h. dem LSB-Bit) beginnend in aufsteigender Reihenfolge übertragen. Die Zeichen werden in derselben Reihenfolge übertragen, in der sie gelesen werden sollen. Die vollständige Nachricht wird in aufeinander folgenden 20 Bit-Blöcke (Nachrichtenbits) unterteilt, die in aufeinander folgenden Nachrichtenwörtern übertragen werden.

Jeder nicht verwendete Teil des letzten Codewortes einer Nachricht wird mit den nicht druckbaren Zeichen EOT (04Hex) aufgefüllt. Nicht genutzte Teile des letzten Codewortes mit Länge kleiner 7 Bit werden auch mit Bits der logischen Bedeutung 0 aufgefüllt.

Die Kodierung der Nachricht erfolgt entsprechend der folgenden Tabelle nach DIN 66003, deutsche Referenz-Version (abgeleitet von ISO/IEC 646):

Bit Nr. 7	0	0	0	0	1	1	1	1
Bit Nr. 6	0	0	1	1	0	0	1	1
Bit Nr. 5	0	1	0	1	0	1	0	1
Bit Nr. 4 3 2 1	Zeichen							
0 0 0 0	0	NUL	TC (DLE)	0	§	P	'	p
0 0 0 1	1	TC (SOH)	DC	!	1	A	Q	a q
0 0 1 0	2	TC (STX)	DC	"	2	B	R	b r
0 0 1 1	3	TC (ETX)	DC	#	3	C	S	c s
0 1 0 0	4	TC (EOT)	DC	\$	4	D	T	d t
0 1 0 1	5	TC (ENQ)	TC (NAK)	%	5	E	U	e u
0 1 1 0	6	TC (ACK)	TC (SYN)	&	6	F	V	f v
0 1 1 1	7	BEL	TC (ETB)	'	7	G	W	g w
1 0 0 0	8	FE (BS)	CAN	(8	H	X	h x
1 0 0 1	9	FE (HT)	BM)	9	I	Y	i y
1 0 1 0	10	FE (LF)	SUB	÷	:	J	Z	j z
1 0 1 1	11	FE (VT)	ESC	+	;	K	Ä	k ä
1 1 0 0	12	FE (FF)	IS (FS)	,	<	L	Ö	l ö
1 1 0 1	13	FE (CR)	IS (GS)	-	=	M	Ü	m ü
1 1 1 0	14	SO	IS (RS)	.	>	N		n ß
1 1 1 1	15	SI	IS (US)	/	?	O	-	o Del

Anmerkung: 20Hex ist ein Leerzeichen

3. Funknetzorganisation

Das gesamte Versorgungsgebiet muss in weniger als einer Minute versorgt werden können. Dies kann entweder durch die Systemarchitektur (Anzahl der DAU) oder durch bestimmte Lenkung der System- und Alarminformationen geschehen. Die Systemsteuerung ist für die sequentielle und/oder synchrone Aussendung von Alarmtelegrammen auszulegen. Um eine Funkversorgungsanzeige zu ermöglichen, ist das gesamte Funknetz in 1- bis 10-minütigen Intervallen auf zu tasten.

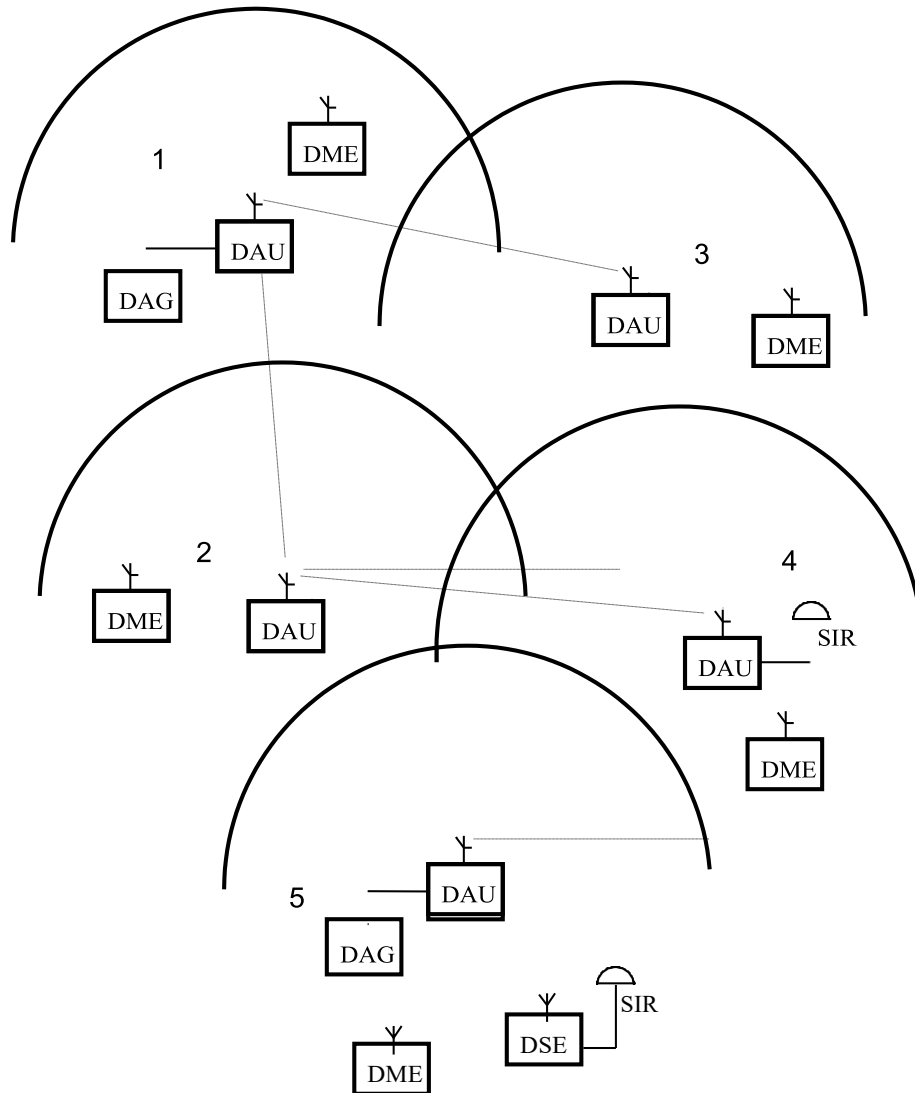
Nur wenige DAG in Baustufe II und III sollen Zugriff auf das gesamte Versorgungsgebiet haben. Eine Änderung der Funknetzorganisation durch Systemsteuerbefehle darf nur von einer Stelle (Master- DAG) aus erfolgen. Für Alarmierungsstellen mit DAG der Baustufe I genügt die Aussendung nur über den DAU, an dem sie jeweils angeschlossen sind.

Über eine Übertragungsleitung erhält der DAU bei der Alarmierungsstelle vom DAG Adressen und Informationen für die DME und strahlt diese über die Antenne ab.

Im Versorgungsgebiet wird der digitale Meldeempfänger die Alarmrufe je nach Standort einmal oder mehrmals empfangen. Deswegen muss dort automatisch erkannt werden, ob der Alarmruf bereits empfangen wurde oder ob er neu ist. Es sollen nur neue Meldungen angezeigt bzw. gespeichert werden.

Der Empfang von Alarmrufen von DAU anderer Systeme bzw. Funkverkehrskreise auf der gleichen Frequenz sowie beliebig modulierte HF-Träger bis zu 30 Sekunden Dauer dürfen zu einer entsprechenden Verzögerung bei der Wiederaussendung, nicht jedoch zu einem Abbruch des Alarmierungsablaufs führen.

Beispiel einer einfachen Netzkonfiguration:



○ Empfangsbereich für Meldeempfänger

— Sichere Verbindung zwischen den DAU

- DAG = Digitaler Alarmgeber
- DAU = Digitaler Alarmumsetzer
- DME = Digitaler Meldeempfänger
- DSE = Digitaler Sirenensteuerempfänger
- SIR = Sirene

4. Rufarten

4.1. Einzelruf

Ein Empfänger wird mittels einer individuellen Rufadresse gerufen. Anwendertypisch werden aus einsatztaktischen Gründen auch mehrere Empfänger mit der jeweils gleichen Rufadresse betrieben und somit gleichzeitig gerufen ("Schleife").

4.2. Sammelruf

Mehrere Empfänger werden mittels sequentieller Aussendung mehrerer Einzelrufe nacheinander gerufen.

4.3. Gruppenruf

Mehrere Empfänger mit individueller 1. Rufadresse haben die gleiche 2. Adresskodierung und können deshalb durch einen besonderen Gruppenruf gleichzeitig gerufen werden.

5. Verschlüsselung

Bei der Übertragung schützenswerter Daten gemäß Datenschutz-Grundverordnung (DSGVO – Verordnung EU 2016/679) in Alarmierungsnachrichten sind gemäß Artikel 5 Abs. 1 f DSGVO geeignete Sicherungsmaßnahmen zu beachten. Dazu ist eine sichere Kryptierung der Nachrichteninhalte, insbesondere personenbezogener Daten wie die postalische Adresse des Einsatzortes, vom Alarmgeber bis zum digitalen Meldeempfänger zwingend erforderlich.

5.1. Einheitliches Verschlüsselungsverfahren

Zur Gewährleistung der Interoperabilität aller verwendeten Komponenten in einem Alarmierungsnetz ist künftig die Nutzung des in Teil E beschriebenen Verschlüsselungsverfahrens vorzusehen.

5.2. Schlüsselmanagement

Die Sicherheit eines Verschlüsselungsverfahrens hängt maßgeblich von der Qualität des Schlüsselmanagements ab. Die Verschlüsselung erfolgt nach dem in Teil E beschriebenen Verfahren. Es ist zu gewährleisten, dass innerhalb eines Alarmierungsnetzes die Verteilung, Speicherung und Nutzung der Schlüssel so erfolgt, dass jeweils nur berechnete Stellen und/oder Personen einen geschützten Zugriff auf die Daten haben. Außerdem sind Regelungen bzw. Mechanismen zum Schlüsselwechsel und zur Sperrung bzw. Vernichtung von Schlüsseln zu treffen, die nicht mehr benötigt werden oder im Verdacht stehen, kompromittiert worden zu sein. Durch ein Schlüsselmanagementsystem kann beispielsweise eine zentrale, rechte-/rollenbasierte und in sich verschlüsselte Verwaltungsumgebung errichtet werden, die den Schutz der Kryptomittel gewährleistet.

5.3. Einführung des einheitlichen Verschlüsselungsverfahrens

Ab 1. Januar 2027 muss in allen neuen Geräten die unter Teil E beschriebene Verschlüsselung umgesetzt werden.

Sofern eine Verschlüsselung bei der Übertragung von Alarmmeldungen erforderlich ist (siehe Ziffer 5.), obliegt die Einführung der Verschlüsselung nach Ziffer 5.1 und Teil E den jeweiligen Betreibern der Alarmierungsnetze. Gegebenenfalls kann – abhängig vom Schutzbedarf der übertragenen Informationen – auch eine teilweise Verschlüsselung, beispielsweise nur für bestimmte Nutzergruppen oder RICs erfolgen. Den Schutzbedarf ermitteln die Netzbetreiber in Abstimmung mit den Nutzern. Sofern keine anderen

gesetzlichen Verpflichtungen gelten, soll eine Umstellung bestehender Systeme bis spätestens 31. Dezember 2028 durchgeführt werden.

6. Verteilung der möglichen Adresskodierungen pro Frequenz auf Bund und Länder

Gesamtkontingent: 2.096.000 Adressen

Anwender	von (Anfangsadresse)	bis (Endadresse)	Anzahl
Bund	0 000 008	0 031 999	31.992
Baden-Württemberg	0 032 000	0 287 999	256.000
Bayern	0 288 000	0 543 999	256.000
Berlin	0 544 000	0 575 999	32.000
Bremen	0 576 000	0 607 999	32.000
Hamburg	0 608 000	0 639 999	32.000
Hessen	0 640 000	0 863 999	224.000
Niedersachsen	0 864 000	1 119 999	256.000
Nordrhein-Westfalen	1 120 000	1 375 999	256.000
Rheinland-Pfalz	1 376 000	1 599 999	224.000
Saarland	1 600 000	1 663 999	64.000
Schleswig-Holstein	1 664 000	1 727 999	64.000
Brandenburg	1 728 000	1 791 999	64.000
Mecklenburg-Vorpommern	1 792 000	1 855 999	64.000
Sachsen	1 856 000	1 919 999	64.000
Sachsen-Anhalt	1 920 000	1 983 999	64.000
Thüringen	1 984 000 #	2 047 999 #	63.998

Aus technischen Gründen ausgenommen: 2 007 665 und 2 045 057

Die Adressen von 0 000 000 bis 0 000 007 und 2 048 000 bis 2 095 999 sind nicht belegt.

Da der jeweils erste Rahmen einer Codewortgruppe für die Adressierung der DAU reserviert ist und die Rahmennummer in der Adresse enthalten ist, sind alle Adressen, die der Gleichung

Adresscodierung = $n * 8$ (worin n = ganze positive Zahl) entsprechen, für die DAU reserviert.

Teil A: DIGITALE ALARMGEBER

A.1. Aufgabe

Digitale Alarmgeber (DAG) setzen die eingegebenen Informationen:

- Rufadresse (Adresscode des Empfängers)
- Nachrichteninhalte (Rufinformation)

für den auszusendenden Alarmruf in ein Datentelegramm um. Über eine Datenleitung sind sie mit dem abgesetzten Digitalen Alarmumsetzer (DAU) verbunden. Die Schnittstelle ist in **A 5** beschrieben.

A.2. Baustufen

A.2.1. Baustufe I

Digitale Alarmgeber der Baustufe I (DAG I) sind Geräte für die Aussendung von 10 bis 20 fest eingestellten Alarmrufen mit verschiedenen Adressen. Jeder Adresse kann eine der vier Funktionsadressen für die Auslösung des akustischen Alarms bei DME gemäß C 4.4.2 zugeordnet werden. Aufbau und Bedienung sollen möglichst einfach gehalten sein.

A.2.2. Baustufe II

Digitale Alarmgeber der Baustufe II (DAG II) sind Geräte für die Aussendung einer beliebigen Zahl von Adressen. Jeder der Adressen kann eine der vier Funktionsadressen für die Auslösung des akustischen Alarms beim DME zugeordnet werden. Zusätzlich muss die Eingabe eines freien Textes möglich sein. Dieser dient auch der Veränderung der Systemwerte (Befehle an die DAU usw.), der Steuerung der regelmäßigen Aussendungen für die Funkversorgungsanzeige und der Aufnahme von Meldungen der DAU (Störungsmeldungen usw.).

Der DAG II besteht aus einer alphanumerischen Tastatur mit Funktionstasten, einem Display und einem Protokolldrucker.

A.2.3. Baustufe III

Digitale Alarmgeber der Baustufe III (DAG III) stellen grundsätzlich eine softwareseitige Realisierung des Alarmgebers mit eigener Hardware dar. Sie müssen mindestens über folgende Möglichkeiten verfügen:

- Alarmprogramm mit Bedienerführung (Adresse/Zielgruppe, Alarmstichwort, Alarmzeit, evtl. Zusatzinformationen)
- Aufnahme von Meldungen der DAU (Störungsmeldungen usw.)

Passwortgeschützt müssen sein:

- Eingabe der Systemwerte (Übertragungsprozedur, Organisation der DAU)
- Versorgung der Meldeempfänger-Datei (Adresse, Rufzone, Name)
- Veränderung der Standard-Alarmstichworte

Digitale Alarmgeber der Baustufe III können auch in das Einsatzleitsystem oder die IT-Umgebung einer Leitstelle integriert werden. In diesem Fall entfallen die Prüfanforderungen für die Hardware des DAG III.

Es wird empfohlen, für diesen Fall eine hiervon unabhängige Rückfallebene vorzuhalten.

A.3. Technische Forderungen

A.3.1. Elektromagnetische Verträglichke

Bei der Emission nach DIN EN 55022 ist Störgrad "B" einzuhalten. Der Nachweis ist durch Prüfzeugnisse zu erbringen.

A.3.2. Stromversorgung

A 3.2.1 Der DAG I muss mit der Nennspannung 12 V = (10,7 bis 15,6 V) betrieben werden können. Ein Schutz gegen überlagerte Störspannung bis 0,5 V (Spitzenspannung) ist vorzusehen.

Auf Wunsch der Anwender ist der Alarmgeber auch mit Netzteil für 230 V, 50 Hz zu liefern¹.

A 3.2.2 DAG II und DAG III können auch für Netzstromversorgung 230 V~, 50 Hz, oder für Nennspannung 12 V = (10,7 bis 15,6 V) ausgelegt sein. Auf Wunsch der Anwender ist eine geeignete gepufferte Stromversorgungseinheit mit Akku und mindestens 15-minütiger Überbrückungszeit anzubieten.

A.4. Konstruktive Forderungen

A.4.1. Typenschild

Zur genauen Kennzeichnung (außer DAG III) ist an geeigneter Stelle ein sichtbares Typenschild anzubringen. Die Verwendung von Klebefolie ist dann zugelassen, wenn eine dauerhafte Verbindung zum Gerät erreicht wird und ein Abziehen nicht ohne Zerstörung derselben möglich ist.

Das Typenschild muss folgende Angaben enthalten:

- Bezeichnung
- Firmenzeichen/-namen
- Fertigungsnummer
- Herstellungsjahr
- BOS-Prüfnummer
- Konformitätserklärung (CE-Kennzeichnung)

Bei DAG III müssen diese Angaben den Betriebsunterlagen entnommen werden können.

A.4.2. Aufbau

A.4.2.1. Beanspruchung

Der DAG wird ortsfest in Innenräumen eingesetzt. Bei der Klassifizierung der Umweltbedingungen wird gemäßigtes Klima zugrunde gelegt. Bezogen auf DIN EN 60721-3-0 wird gemäß E - DIN 40046-721-3 folgende Klasse der mechanischen Umweltbedingung festgelegt: 3 M 1. Unter diesen Umweltbedingungen muss die einwandfreie Funktion des DAG gewährleistet sein.

A.4.2.2. Betriebsbedingungen

Der DAG muss im Temperaturbereich von 0 °C bis + 40 °C funktionsfähig bleiben, das gilt auch für Softwarelösungen nach A 2.3

¹ Die elektr. Sicherheit im Sinne der gültigen Technischen Regeln ist nicht Gegenstand einer Zulassung nach TR BOS.
TR BOS: „Geräte für die digitale Funkalarmierung“

A.5. Anschaltung (Schnittstelle DAG-DAU)

Die Verbindung DAG-DAU erfolgt nach den Anforderungen des Beschaffers.

A.6. Technische Unterlagen

Jedem Alarmgeber ist außer der Bedienungsanleitung eine ausführliche Beschreibung beizufügen, beides in deutscher Sprache.

Teil B: DIGITALE ALARMUMSETZER

B.1. Aufgabe

Digitale Alarmumsetzer (DAU) sind Geräte mit Mehrfach-Nutzen für die digitale Funkalarmierung und enthalten ein Simplex-Sendeempfangsgerät für HF-DFSK-Modulation. Sie empfangen Informationen über Trägerwellen oder über eine Drahtverbindung von einem Digitalen Alarmgeber (DAG) oder einem Einsatzleitreechner mit vergleichbarem Datenausgang. Sie müssen der DIN EN 300113 entsprechen und von einem akkreditierten Prüflabor zugelassen sein.

B.2. Baustufen

B.2.1. Baustufe I

Alarmumsetzer der Baustufe I bestehen aus der Prozessorsteuerung, einem Sendeempfangsgerät für HF-DFSK-Modulation und der Stromversorgung mit Anschluss für die USV. Der Prozessor erhält die auszusendende Information vom DAG (s. A 5) oder vom eigenen Empfänger.

B.2.2. Baustufe II

Alarmumsetzer der Baustufe II enthalten zusätzlich zu den Merkmalen der Baustufe I eine Steuerung für drei Relais-Schaltausgänge zur Sirenenauslösung. Die binäre Funkcodenummer zur Steuerung dieser Kontakte setzt sich aus dem Adresscode und zwei Funktionsbits zusammen.

$$\begin{array}{rcccl} \text{Funkcodenummer} & = & \text{Adresscode} & + & \text{Funktionsbits} \\ 20 \text{ Bit} & & 18 \text{ Bit} & & 2 \text{ Bit} \end{array}$$

Die Funktionsadressen A, B, C und D sind wie folgt durch die Funktionsbits definiert:

Funktionsadresse	Funktionsbit 20, 21	Ausgang
A	00	Kontakt für 1-2 s schließen
B	01	Kontakt für 60 s im 12 s Takt schließen und öffnen
C	10	Kontakt für 60 s im 2 s Takt schließen und öffnen
D	11	Kontakt für 60 s schließen

Kontaktbelastbarkeit: mind. 24 V, 1 A, potentialfrei

Außerdem muss der Zustand eines Meldeeingangs (externer potentialfreier Kontakt) bei der zyklischen Systemüberwachung abgefragt und signalisiert werden.

B.3. Technische Forderungen

B.3.1. Allgemeines

Die folgenden Werte sind Mindestforderungen. Ihr Unter- bzw. Überschreiten im Sinne einer Verbesserung ist anzustreben. Bei den in der EN 301489 zur elektromagnetischen Kompatibilität angegebenen Spannungswerten wird im Messverfahren davon ausgegangen, dass die Ausgangsimpedanz des Messsenders gleich der Nennimpedanz des Empfängereingangs ist.

B.3.1.1. Frequenzbereich

Im Frequenzbereich 165 bis 174 MHz muss die Sende-/Empfangsfrequenz ohne Öffnen des Gehäuses eingestellt werden können; die Schaltbandbreite soll mindestens 1 MHz betragen. Die Veränderung der Frequenz muss am Aufstellort möglich sein.

Kanalraaster ist 20 kHz; eine nachträgliche Anpassung an ein anderes Kanalraaster, z. B. 12,5 kHz, muss möglich sein.

B.3.1.2. Verträglichkeit

Vom Alarmumsetzer darf keine störende Beeinflussung auf andere Funkempfänger ausgehen. Bei der Emission nach DIN EN 55022 ist Störgrad B einzuhalten. Der Nachweis ist durch entsprechende Prüfzeugnisse zu erbringen.

B.3.2. Sender

B.3.2.1. Sendeleistung

Die Sendeleistung muss von 6 bis 15 Watt an 50 Ohm einstellbar sein. Der eingestellte Wert muss bei normalen Betriebsbedingungen (s. B 4.4.2.1) auf $\pm 1,5$ dB, bei extremen Betriebsbedingungen (s. B 4.4.2.2) auf $+2/-3$ dB eingehalten werden. Dauernde Fehlanpassungen zwischen Leerlauf und Kurzschluss dürfen nicht zu einer schädlichen Überlastung der Senderendstufe führen.

B.3.2.2. Nachbarkanalleistung

Das Verhältnis der Nachbarkanalleistung zur Trägerleistung muss bei allen vom Prüfling verwendeten Ausstrahlungen größer als 70 dB sein.

B.3.2.3. Nebenaussendungen

Im Frequenzbereich von 30 bis 1000 MHz dürfen die Nebenaussendungen nicht größer als 250 nW sein.

B.3.2.4. Intermodulationsdämpfung

Die Intermodulationsschwingung 3. Ordnung muss um mindestens 40 dB gegenüber dem Nutzträger gedämpft sein.

B.3.2.5. Modulator

Zur Modulation des Trägers wird eine Frequenzumtastmodulation (HF-DFSK) mit einem Hub von ± 4 kHz (bei 20-kHz-Kanalraaster) angewendet.

Logischer Pegel: 0	Ablage: + 4 kHz (+0%, -10%)	bezogen auf Nennfrequenz
Logischer Pegel: 1	Ablage: - 4 kHz (-0%, +10%)	bezogen auf Nennfrequenz.

B.3.2.6. Sendefrequenz

Die Abweichung von der Nennfrequenz darf unter allen Bedingungen maximal 800 Hz betragen. Anzustreben ist eine Abweichung von maximal 350 Hz.

B.3.3. Empfänger

B.3.3.1. Empfindlichkeit

Die Empfindlichkeit (= maximaler Eingangsspannungsbedarf, damit 9 von 10 Alarmrufen richtig empfangen werden): $< 2\mu\text{V}$ (EMK)

B 3.3.2	Gleichkanalunterdrückung:	> -8 dB	
B 3.3.3	Nachbarkanalämpfung:	> 70 dB	
B 3.3.4	Nebenempfangsdämpfung:	> 70 dB	
B 3.3.5	Intermodulationsdämpfung:	> 70 dB	
B 3.3.6	Blocking (+ / - 1 bis 10 MHz):		> 90 dB μV
B 3.3.7	Störleistung 30 bis 1000 MHz		< 2 nW

B.3.4. Stromversorgung

Der Alarmumsetzer wird mit einer Versorgungsspannung von $230\text{ V} \pm 10\%$ betrieben². Es muss ein Akku mit Tiefentladeschutz angeschlossen werden. Dessen Kapazität ist anzugeben bzw. so zu bemessen, dass Netzausfälle mindestens bis zu 12 Stunden überbrückt werden (Verhältnis Sende- zu Empfangsbetrieb = 1 min: 19 min). Netz- und Akkubetrieb sind auf der Frontplatte anzuzeigen und müssen bei der zyklischen Systemüberwachung unterscheidbar signalisiert werden.

B.4. Konstruktive Forderungen

B.4.1. Gestaltung

Der Alarmumsetzer ist als 19"-Gehäuse bzw. Wandschrank mit Baugruppen-Einschüben auszuführen. Anzeige- und Bedienelemente (unverwechselbar) sind möglichst auf der Frontplatte anzuordnen.

B.4.2. Typenschild

Am Alarmumsetzer muss ein Typenschild mit folgenden Angaben dauerhaft angebracht sein:

- Gerätebezeichnung
- Zulassungszeichen
- BOS- Prüfnummer
- Fertigungsnummer
- Herstellungsjahr
- Firmenname/-zeichen.
- Konformitätserklärung (CE- Kennzeichnung)

Zusätzlich soll die Fertigungsnummer im Geräteinnern eingeprägt sein.

B.4.3. Aufbau

Der mechanische und elektrische Aufbau des Geräts soll ein problemloses Auswechseln der Bauteile und Baugruppen erlauben.

B.4.4. Beanspruchung

Der Alarmumsetzer muss den Einflüssen standhalten, denen er in ungeheizten Räumen ausgesetzt ist, ohne dass dadurch die Betriebsdaten eingeschränkt oder bleibende Schäden verursacht werden. Für die relative Luftfeuchte sind nach DIN EN 60721 die Anforderungen nach Kennbuchstabe E einzuhalten.

² Die elektr. Sicherheit im Sinne der gültigen Technischen Regeln ist nicht Gegenstand einer Zulassung nach TR BOS.
TR BOS: „Geräte für die digitale Funkalarmierung“

B.4.4.1. Schutzart

Nach EN 60529 muss das Gerät mindestens die Forderungen für die Schutzart IP 42 erfüllen. Diese Forderung entfällt, wenn der DAU in ein Rack eingebaut ist, welches die Schutzart IP 42 erfüllt. Ortsspezifisch höhere Anforderungen sind zwischen Anwender und Hersteller besonders zu vereinbaren.

B.4.4.2. Betriebsbedingungen

B.4.4.2.1. Normale Betriebsbedingungen

Soweit nicht besonders angegeben, müssen die geforderten Daten bei Umgebungstemperaturen von -10°C bis $+40^{\circ}\text{C}$ und bei Spannungsschwankungen des 230 V-Netzes von $\pm 10\%$ eingehalten werden.

B.4.4.2.2. Extreme Betriebsbedingungen

Bei extremen Temperaturen über die normalen Betriebsbedingungen hinaus bis -25°C und bis $+55^{\circ}\text{C}$ und bei Spannungsschwankungen des 230 V-Netzes von $\pm 15\%$ muss weiterhin Sende- und Empfangsbetrieb möglich sein.

B.4.4.3. Mechanische Beanspruchung

Der DAU wird ortsfest und wettergeschützt eingesetzt. Bei der Klassifizierung der Umweltbedingungen wird gemäßigtes Klima zugrunde gelegt. Bezogen auf DIN EN 60721-3-0 werden die mechanischen Umweltbedingungen festgelegt als: 3 M 1. Unter diesen Umweltbedingungen muss die einwandfreie Funktion des DAU gewährleistet sein.

B.5. Anschaltung

Zur Anschaltung wird auf Teil A Ziffer 5 verwiesen.

B.6. Technische Unterlagen

Auf besondere Anforderung anwendereigener Werkstätten sind folgende Unterlagen in deutscher Sprache bereitzustellen:

- Bedienungsanweisung
- Vollständiges Datenblatt
- Blockschaltbild mit Frequenzangaben
- Ausführliche Funktionsbeschreibung
- Gesamtschaltplan
- Baugruppenschaltpläne mit Positionsangaben, Halbleiter-Sockelangaben und Steckerbezeichnungen
- Stromlaufplan mit allen für eine ordnungsgemäße Überprüfung und Einstellung notwendigen Angaben (Spannungs- und Stromwerte, Pegel, Impulsdiagramme und Angaben zu den jeweils verwendeten Messgeräten)
- Austausch- und Verschleißteilliste mit Bestellangaben
- Wartungsvorschrift mit Angabe der durchzuführenden Messungen und Einstellungen in der richtigen Reihenfolge
- Programmiersoftware soweit erforderlich

B.7. Voraussetzungen für die Prüfung nach dieser Richtlinie

Erfolgt die Verbindung zwischen den DAU nicht nach dem unter A beschriebenen Protokoll, sind der Prüfstelle der Telegrammaufbau und das Übertragungsverfahren offenzulegen und nach Vorgabe der Prüfstelle die benötigten Messmittel beizustellen.

Teil C: DIGITALE MELDEEMPFÄNGER

C.1. Aufgabe

Digitale Meldeempfänger (DME) sind Einkanal-Empfangsgeräte mit integrierter Antenne zur Alarmierung von Einsatzkräften. Sie müssen der DIN EN 300341 entsprechen.

Die hier beschriebenen Anforderungen sind weitgehend an der Richtlinie BNetzA-BAPT 222 TE 20 (Ersatz für FTZ- Richtlinie 171 TR 1, "Cityruf Funkrufempfänger", orientiert, damit entsprechend kostengünstige Meldeempfänger angeboten werden.

BOS-spezifische Unterschiede sind:

- Anderer Frequenzbereich
- Die Adressen werden nicht im Rahmen "0" ausgesendet, weil dieser den Steuerinformationen vorbehalten ist.
- Eine Meldung kann eine Steuerinformation enthalten, die nicht für den Meldeempfänger bestimmt ist.

Jede empfangene Meldung enthält also:

- Präambel
- Synchronwort
- Adresse
- Meldung
- ggf. Steuerinformation

Der gesamte Übertragungscode (FUNKSchnittstelle –„Luft“) ist im Teil „Allgemeines“ beschrieben.

C.2. Verwendungsarten

Es sind digitale Meldeempfänger (DME) für folgende Rufklassen zu unterscheiden:

- Nur-Ton (DME I):
Übermittlung von akustischen Signalen
- Alphanumerik (DME II):
Übermittlung und gleichzeitige Anzeige von mindestens 16 alphanumerischen Zeichen
- mit synthetischer Sprachwiedergabe: (DME III)
Übermittlung und gleichzeitige Wiedergabe der übermittelten Zeichen als Sprache. Die synthetische Spracherzeugung muss so erfolgen, dass ein verständlicher Text entsteht. Dabei muss es möglich sein, allgemein übliche Abkürzungen sowie Unterschiede zwischen Schreibweise und Aussprache in einem Speicher von wenigstens 3.000 Zeichen abzulegen. Diese werden bei Übermittlung der entsprechenden Zeichenfolge automatisch ausgegeben (z.B. für BAB „Bundesautobahn“ oder die richtige Aussprache fremdsprachiger Worte z.B. „Saint Marie aux Mines – Straße“).
- mit Rückmeldemöglichkeit über andere Kommunikationsnetze: (DME IV)
Die Meldeempfänger haben die Möglichkeit, über andere Netze (z.B. Mobilfunknetze) Rückmeldungen zu geben.

Die Definition der Rufarten ist im Teil „Allgemeines“ zu finden.

C.3. Technische Forderungen

C.3.1. Allgemeines

Für die durchzuführenden Messungen gelten, wenn nicht anders vermerkt, die in BAPT 222 TE 20 angegebenen Prüfbedingungen bedarfsweise und sinngemäß. Es ist zwischen normalen und extremen Prüfbedingungen zu unterscheiden.

Ein **Nutzsignal** ist eine HF-Trägerwelle mit der Nennfrequenz, die mit Prüfmodulation moduliert ist.

Prüfmodulation ist eine Bitfolge aus der Präambel und einer oder mehreren Codewortgruppen.

Pegel ist ein auf eine Bezugsgröße bezogenes logarithmisches Größenverhältnis. Die zueinander in Beziehung gesetzten Größen können sowohl Energie- als auch Feldgrößen sein (VDE 0877, Abschnitt 3.18).

Bei DME IV sind die nachfolgenden Messungen C 3.2 bis C 3.8 bei ausgeschaltetem und eingeschaltetem Sender der zusätzlichen Kommunikationsmöglichkeit (z.B. über GSM) durchzuführen und zu dokumentieren.

Soll im Betriebszustand der Sender der zusätzlichen Kommunikationsmöglichkeit (z.B. über GSM) dauerhaft in Betrieb sein (nicht nur kurzzeitig nach einer Alarmierung) müssen die Grenzwerte C 3.2 bis C 3.8 im Sendebetrieb eingehalten werden.

C.3.2. Referenzsignal

C.3.2.1. Definition

Das Referenzsignal wird für Referenzmessungen definiert. Das Referenzsignal ist ein Nutzsignal mit Prüfmodulation mit dem Pegel, bei dem 80% aller Nur-Ton-Rufe erfolgreich sind.

C.3.2.2. Verfahren zur Bestimmung des Referenzsignals

Das Referenzsignal wird nach dem nachfolgend beschriebenen Verfahren bestimmt (Frontrichtung nach Herstellerangabe):

- a) Auf den Empfänger wird ein Nutzsignal mit Prüfmodulation gegeben. Störsignale wirken nicht auf den Empfänger ein.
- b) Der Pegel des Signals wird so eingestellt, dass weniger als 10% der Nur-Ton-Rufe erfolgreich sind.
- c) Das Signal wird ständig wiederholt ausgesendet, wobei jedes Mal beobachtet wird, ob ein Nur-Ton-Ruf erfolgreich ist oder nicht.

Der Pegel des Signals

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist, oder
- wird um 1 dB erhöht, wenn ein Nur-Ton-Ruf nicht erfolgreich ist.

Dieses Verfahren wird solange fortgesetzt, bis drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind. Der zugehörige Pegel wird notiert.

- d) Der Pegel wird um 1 dB verringert und der neue Pegel ebenfalls notiert. Anschließend wird das Nutzsignal mit Prüfmodulation (C 3.1) 20mal ausgesendet.

Der Pegel des Signals

- bleibt unverändert, wenn ein Nur- Ton-Ruf erfolgreich ist,
- wird um 1 dB erhöht und der neue Pegel notiert, wenn ein Nur- Ton-Ruf nicht erfolgreich ist, oder
- wird um 1 dB verringert und der neue Pegel notiert, wenn drei aufeinander folgende Nur- Ton-Rufe erfolgreich sind

e) Das Referenzsignal ist der arithmetische Mittelwert der unter d) und e) notierten Pegelwerte des Nutzsymbols mit Prüfmodulation.

Der Pegel ist zu notieren.

C.3.2.3. Grenzwerte

Der Pegel des Referenzsignals darf unter extremen Prüfbedingungen gegenüber normalen Prüfbedingungen maximal 6 dB größer sein.

C.3.3. Empfindlichkeit

C.3.3.1. Allgemeines

Die Empfindlichkeit des Empfängers ist die Mindestfeldstärke, bei der ein Nutzsymbols mit bestimmter Erfolgsrate empfangen wird.

Es sind verschiedene Empfindlichkeiten zu unterscheiden:

Die Empfindlichkeit im Freifeld und die Empfindlichkeit bei Körpertrageweise sind Forderungen aus der Sicht der BOS, um eine bestimmte Mindestversorgung planen zu können. Einflüsse, die durch Fadingeffekte im Betrieb auftreten, sind weitestgehend durch bekannte code-spezifische Eigenschaften und funktionale Anforderungen zu berücksichtigen. Aus diesem Grund wird ein Grenzwert für die dynamische Empfindlichkeit in dieser Richtlinie nicht gefordert.

C.3.3.2. Statische Empfindlichkeit

C.3.3.2.1. Empfindlichkeit im Freifeld

C.3.3.2.1.1. Definition

Unter Empfindlichkeit im Freifeld ist eine mittlere Empfindlichkeit eines frei aufgestellten Empfängers zu verstehen.

C.3.3.2.1.2. Messverfahren

Der Messaufbau erfolgt nach DIN EN 300341. Der Empfänger wird in der Mitte des Messplatzes in 1,5 m Höhe, gemessen von der Oberkante des Empfängers, an einer nichtleitenden Vorrichtung befestigt. Die Messung wird in der Position begonnen, in der die Empfängerebene senkrecht zur Achse Sendeantenne - Empfänger steht. Die Empfängerbezugsebene ist vom Hersteller zu definieren.

Es werden insgesamt 8 Messungen durchgeführt, dabei wird der Empfänger um jeweils 45 Grad gegenüber der Sendeantenne gedreht. Von den gemessenen 8 Feldstärkewerten E_n in $\mu\text{V/m}$ wird der folgende Wert

$$E_{Fr} = \sqrt{\frac{8}{\frac{1}{E_1^2} + \dots + \frac{1}{E_8^2}}} \quad \text{gebildet.}$$

E_{Fr} ist der Wert der statischen Empfindlichkeit im Freifeld. Jeder der 8 Feldstärkewerte E_n wird wie folgt ermittelt:

- Auf den Empfänger wird ein Nutzsignal mit Prüfmodulation gegeben (576 Bit Präambel und 544 Bit Codewortgruppe. Die Codewortgruppe enthält die Adresse des Empfängers mit beliebiger Funktionsadresse). Störsignale wirken nicht auf den Empfänger ein.
- Der Pegel des Signals wird so eingestellt, dass weniger als 10% der Nur- Ton-Rufe erfolgreich sind.
- Das Signal wird ständig wiederholt ausgesendet, wobei jedes Mal beobachtet wird, ob ein Nur-Ton-Ruf erfolgreich ist oder nicht.
- Der Pegel des Signals
 - bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist. oder
 - wird um 1 dB erhöht, wenn ein Nur- Ton-Ruf nicht erfolgreich ist.

Dieses Verfahren wird solange fortgesetzt, bis drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind. Der zugehörige Pegel wird notiert.

- Der Pegel wird um 1 dB verringert und der neue Pegel ebenfalls notiert. Anschließend wird das Nutzsignal mit Prüfmodulation 20-mal ausgesendet.

Der Pegel des Signals

- bleibt unverändert, wenn ein Nur- Ton-Ruf erfolgreich ist.
- wird um 1 dB erhöht und der neue Pegel notiert, wenn ein Nur- Ton-Ruf nicht erfolgreich ist, oder
- wird um 1 dB verringert und der neue Pegel notiert, wenn drei aufeinander folgende Nur- Ton-Rufe erfolgreich sind.

- Der Feldstärkewert E_n ist der arithmetische Mittelwert der unter d) und e) notierten Pegelwerte.

Die zuvor beschriebene Messung kann auch ersatzweise in einer geeigneten Streifenleitung erfolgen.

C.3.3.2.1.3. Grenzwerte

Gefordert wird für den Wert der statischen Empfindlichkeit im Freifeld $E_{Fr} < 28 \mu\text{V/m}$ (entspricht 29 dB über $1 \mu\text{V/m}$), anzustreben sind $20 \mu\text{V/m}$ (entspricht 26 dB über $1 \mu\text{V/m}$). Der Grenzwert muss auch bei Frequenzablagen von $\pm 800 \text{ Hz}$ von der Sollfrequenz eingehalten werden.

C.3.3.3. Empfindlichkeit beim Tragen am Körper

C.3.3.3.1. Definition

Unter Empfindlichkeit beim Tragen am Körper ist die mittlere Empfindlichkeit eines Empfängers an einer dem menschlichen Körper nachempfundenen Salzsäule zu verstehen.

C.3.3.3.2. Messverfahren

Der Empfänger wird in der Mitte des Messplatzes in 1,5 m Höhe, gemessen von der Oberkante des Empfängers, an einer dem menschlichen Körper nachempfundenen Salzsäule befestigt. Die Salzsäule ist ein mit Salzwasser (1,49 g NaCl pro Liter; Temperatur zwischen + 15 ° C und + 35

° C) gefüllter Kunststoffbehälter, der folgende Abmessungen hat: Höhe: 1700 ± 100 mm

Innendurchmesser: 300 ± 5 mm

Wandstärke: 5 ± 0,5 mm

Die Messung wird in der Position begonnen, in der die Empfängerebene senkrecht zur Achse Sendeantenne - Empfänger steht. Die Empfängerbezugsebene ist vom Hersteller zu definieren. Es werden insgesamt 8 Messungen durchgeführt, dabei wird die Salzsäule mit dem daran befestigten Empfänger um jeweils 45° gegenüber der Sendeantenne gedreht. Von den gemessenen 8 Feldstärkewerten E_N in $\mu\text{V}/\text{m}$ wird der folgende Wert

$$E_{Fr} = \sqrt{\frac{8}{\frac{1}{E_1^2} + \dots + \frac{1}{E_8^2}}} \quad \text{gebildet.}$$

E_k ist der Wert der statischen Empfindlichkeit beim Tragen am Körper. Jeder der 8 Feldstärkewerte E_k wird wie folgt ermittelt:

- Auf den Empfänger wird ein Nutzsinal mit Prüfmodulation gegeben. Störsignale wirken nicht auf den Empfänger ein.
- Pegel des Signals wird so eingestellt, dass weniger als 10 % der Nur- Ton-Rufe erfolgreich sind.
- Das Signal wird ständig wiederholt ausgesendet, wobei jedes Mal beobachtet wird, ob ein Nur-Ton-Ruf erfolgreich ist oder nicht.
- Der Pegel des Signals
 - bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist, oder
 - wird um 1 dB erhöht, wenn ein Nur- Ton-Ruf nicht erfolgreich ist.

Dieses Verfahren wird solange fortgesetzt, bis drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind. Der zugehörige Pegel wird notiert.

- Der Pegel wird um 1 dB verringert und der neue Pegel ebenfalls notiert. Anschließend wird das Nutzsinal mit Prüfmodulation 20-mal ausgesendet.

Der Pegel des Signals

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist,
- wird um 1 dB erhöht und der neue Pegel notiert, wenn ein Nur- Ton-Ruf nicht erfolgreich ist, oder
- wird um 1 dB verringert und der neue Pegel notiert, wenn drei aufeinander folgende Nur- Ton-Rufe erfolgreich sind.

- Der Feldstärkewert E_k ist der arithmetische Mittelwert der unter d) und e) notierten Pegelwerte.

C.3.3.3.3. Grenzwert

Gefordert wird für den Wert der statischen Empfindlichkeit beim Tragen am Körper $E_k < 14 \mu\text{V}/\text{m}$ (entspricht 23 dB über 1 $\mu\text{V}/\text{m}$). Anzustreben sind 10 $\mu\text{V}/\text{m}$ (entspricht 20 dB über 1 $\mu\text{V}/\text{m}$).

C.3.4. Gleichkanalunterdrückung

C.3.4.1. Definition

Die Gleichkanalunterdrückung ist ein Maß für die Fähigkeit des Empfängers, ein Nutzsignal mit bestimmter Erfolgsrate zu empfangen, ohne dass die aus dem Vorhandensein eines modulierten Störsignals sich ergebende Beeinträchtigung zunimmt. Beide Signale müssen dabei auf der Sollfrequenz des Empfängers liegen.

C.3.4.2. Messverfahren

Die Aufstellung des Prüflings erfolgt unter den Bedingungen, unter denen das Referenzsignal ermittelt wurde. Dann wird nach dem nachfolgend beschriebenen Verfahren das minimale Pegelverhältnis Störsignal/Nutzsignal bestimmt, bei dem die Anrufsicherheit auf 80% absinkt.

- a) Auf den Empfänger werden
 - ein Nutzsignal mit Prüfmodulation mit einer Feldstärke, die 3 dB über dem Referenzsignal liegt, und
 - ein mit einem Ton von 400 Hz und einem Frequenzhub von $\pm 2,4$ kHz moduliertes Störsignal, das von der Sollfrequenz des Empfängers maximal ± 3 kHz abweicht, gegeben.
- b) Der Pegel des Störsignals wird so eingestellt, dass weniger als 10% der Nur-Ton-Rufe erfolgreich sind.
- c) Das Nutzsignal mit Prüfmodulation wird ständig wiederholt ausgesendet, wobei jedes Mal beobachtet wird, ob ein Nur-Ton-Ruf erfolgreich ist oder nicht.
- d) Der Pegel des Störsignals
 - bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist, oder
 - wird um 2 dB verringert, wenn ein Nur-Ton-Ruf nicht erfolgreich ist.

Dieses Verfahren wird solange fortgesetzt, bis drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind. Der zugehörige Pegel wird notiert.

- e) Der Pegel des Störsignals wird um 1 dB erhöht und der neue Pegel ebenfalls notiert. Anschließend wird das Nutzsignal mit Prüfmodulation 20-mal ausgesendet.

Der Pegel des Störsignals

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist,
 - wird um 1 dB verringert und der neue Pegel notiert, wenn ein Nur-Ton-Ruf nicht erfolgreich ist, oder
 - wird um 1 dB erhöht und der neue Pegel notiert, wenn drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind.
- f) Der arithmetische Mittelwert der unter d) und e) notierten Pegelwerte ist der Pegelwert des Störsignals, bei dem die Anrufsicherheit auf 80% absinkt.

C.3.4.3. Grenzwert

Das maximale Pegelverhältnis Störsignal/Nutzsignal muss unter normalen und extremen Prüfbedingungen - 8 dB sein.

C.3.5. Nachbarkanaldämpfung

C.3.5.1. Definition

Die Nachbarkanaldämpfung ist das Maß für die Fähigkeit des Empfängers, ein Nutzsignal mit bestimmter Erfolgsrate zu empfangen, wenn im benachbarten Kanal ein Störsignal vorhanden ist.

C.3.5.2. Messverfahren

Es wird nach dem folgenden Verfahren das minimale Pegelverhältnis Störsignal/Nutzsignal bestimmt, bei dem die Anrufsicherheit auf 80% absinkt.

- a) Auf den Empfänger werden
 - ein Nutzsignal mit Prüfmodulation mit einer Feldstärke, die 3 dB über dem Referenzsignal liegt, und
 - ein mit einem Ton von 400 Hz und einem Frequenzhub von $\pm 2,4$ kHz moduliertes Störsignal, das unmittelbar im Kanal über und anschließend unter dem des Nutzsignals liegt, gegeben.
- b) Der Pegel des Störsignals wird so eingestellt, dass weniger als 10% der Nur- Ton-Rufe erfolgreich sind.

C.3.5.3. Grenzwerte

Das minimale Pegelverhältnis Störsignal/Nutzsignal muss

- | | |
|--------------------------------|--------------------------------------|
| unter normalen Prüfbedingungen | <input type="checkbox"/> 60 dB und |
| unter extremen Prüfbedingungen | <input type="checkbox"/> 55 dB sein. |

C.3.6. Nebenempfangsdämpfung

C.3.6.1. Definition

Die Nebenempfangsdämpfung ist das Maß für die Fähigkeit des Empfängers, ein Nutzsignal mit bestimmter Anrufsicherheit zu empfangen, wenn auf irgendeiner Frequenz ein Störsignal vorhanden ist.

C.3.6.2. Messverfahren

Es wird nach dem nachfolgend beschriebenen Verfahren das minimale Pegelverhältnis Störsignal/ Nutzsignal bestimmt, bei dem die Anrufsicherheit auf 80% absinkt. Das Störsignal weist mehr als den doppelten Kanalabstand von der Empfangsfrequenz auf und wird zwischen 100 kHz bis 1000 MHz durchgestimmt. Der Empfängerhersteller hat zur rechnerischen Ermittlung kritischer Nebenempfangsstellen einen detaillierten Plan der Empfängerschaltung, insbesondere der Frequenzaufbereitung, abzuliefern.

- a) Auf den Empfänger werden
 - ein Nutzsignal mit Prüfmodulation mit einer Feldstärke, die 3 dB über dem Referenzsignal liegt, und
 - ein mit einem Ton von 400 Hz und einem Frequenzhub von $\pm 2,4$ kHz moduliertes Störsignal gegeben.
- b) Der Pegel des Störsignals wird so eingestellt, dass weniger als 10% der Nur- Ton-Rufe erfolgreich sind.
- c) Das Nutzsignal mit Prüfmodulation wird ständig wiederholt ausgesendet, wobei jedes Mal beobachtet wird, ob ein Nur- Ton-Ruf erfolgreich ist oder nicht.

d) Der Pegel des Störsignals

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist, oder
- wird um 2 dB verringert, wenn ein Nur- Ton-Ruf nicht erfolgreich ist.

Dieses Verfahren wird solange fortgesetzt, bis drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind. Der zugehörige Pegel wird notiert. Anschließend wird das Nutzsignal mit Prüfmodulation (C 3.1) 20-mal ausgesendet.

e) Der Pegel des Störsignals

- bleibt unverändert, wenn ein Nur- Ton-Ruf erfolgreich ist,
- wird um 1 dB verringert und der neue Pegel notiert, wenn ein Nur- Ton-Ruf nicht erfolgreich ist, oder
- wird um 1 dB erhöht und der neue Pegel notiert, wenn drei aufeinander folgende Nur- Ton-Rufe erfolgreich sind.

f) Der arithmetische Mittelwert der unter d) und e) notierten Pegelwerte ist der Pegelwert des Störsignals, bei dem die Anrufsicherheit auf 80 % absinkt.

C.3.6.3. Grenzwerte

Das minimale Pegelverhältnis Störsignal/Nutzsignal muss für Spiegelfrequenzen, die außerhalb der unten genannten Frequenzbereiche liegen, 50 dB und für sonstige Frequenzen 60 dB sein.

Für Nebenempfangsstellen in den Frequenzbereichen 47 bis 68 MHz, 87 bis 108 MHz, 174 bis 230 MHz soll ein Pegelverhältnis Störsignal/Nutzsignal 70 dB erreicht werden.

C.3.7. Intermodulationsdämpfung

C.3.7.1. Definition

Die Intermodulationsdämpfung ist das Maß für die Fähigkeit eines Empfängers, ein Nutzsignal mit bestimmter Erfolgsrate zu empfangen, wenn gleichzeitig durch Mischung von zwei oder mehreren Signalen auf anderen Frequenzen als der Sollfrequenz des Empfängers eine Störung erzeugt wird.

C.3.7.2. Messverfahren

Es wird nach dem nachfolgend beschriebenen Verfahren das minimale Pegelverhältnis Störsignal/ Nutzsignal bestimmt, bei dem die Anrufsicherheit auf 80 % absinkt.

a) Auf den Empfänger werden

- ein Nutzsignal mit Prüfmodulation (C 3.1) mit einer Feldstärke, die 3 dB über dem Referenzsignal liegt,
- ein unmoduliertes Störsignal, das in einem Kanalabstand einmal unter und bei einer zweiten Messung über der Sollfrequenz des Empfängers mit einer maximalen Abweichung von ± 3 kHz liegt, und
- ein mit einem Ton von 400 Hz und einem Frequenzhub von $\pm 2,4$ kHz moduliertes Störsignal, dessen Frequenz einmal um den doppelten Kanalabstand unter und bei einer zweiten Messung über der Sollfrequenz liegt, gegeben.

Die Pegel der beiden Störsignale werden gleich groß gehalten.

Die Messung wird anschließend vom doppelten bis zum 4-fachen und/oder bis zum 8-fachen Kanalabstand durchgeführt.

- b) Der Pegel der Störsignale wird so eingestellt, dass weniger als 10% der Nur-Ton-Rufe erfolgreich sind.
- c) Das Nutzsignal mit Prüfmodulation wird ständig wiederholt ausgesendet, wobei jedes Mal beobachtet wird, ob ein Nur-Ton-Ruf erfolgreich ist oder nicht.

d) Der Pegel der Störsignale

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist, oder
- wird um 2 dB verringert, wenn ein Nur-Ton-Ruf nicht erfolgreich ist.

Dieses Verfahren wird solange fortgesetzt, bis drei aufeinander folgende Nur- Ton-Rufe erfolgreich sind. Der zugehörige Pegel wird notiert.

- e) Der Pegel der Störsignale wird um 1 dB erhöht und der neue Pegel ebenfalls notiert. Anschließend wird das Nutzsignal mit Prüfmodulation 20-mal ausgesendet.

Der Pegel der Störsignale

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist,
- wird um 1 dB verringert und der neue Pegel notiert, wenn ein Nur- Ton-Ruf nicht erfolgreich ist, oder
- wird um 1 dB erhöht und der neue Pegel notiert, wenn drei aufeinander folgende Nur- Ton-Rufe erfolgreich sind.

- f) Der arithmetische Mittelwert der unter d) und e) notierten Pegelwerte ist der Pegelwert des Störsignals, bei dem die Anrufsicherheit auf 80 % absinkt.

C.3.7.3. Grenzwert

Das minimale Pegelverhältnis Störsignal/Nutzsignal muss bei jeder Messung 50 dB (anzustreben sind 55 dB) sein.

C.3.8. Verhalten gegenüber hohen Nutzfeldstärken

Die Anrufsicherheit darf bei Feldstärken zwischen 10 bis 70 dB über dem Referenzsignal einen Wert von 99 % nicht unterschreiten.

C.4. Funktionale Forderungen

C.4.1. Allgemeines

Das hochfrequente Nutzsignal besitzt die im Teil „Allgemeines“ beschriebenen Eigenschaften. Der Empfänger muss dieses Signal in geeigneter Weise demodulieren, dekodieren und weiterverarbeiten können.

C.4.2. Adresskodierung

Die binäre Funkcodenummer ist die Information, die auf dem Funkweg übertragen werden muss, um einen oder beim Gruppenruf mehrere Empfänger gleichzeitig anzusprechen.

Die Funkcodenummer setzt sich, wie nachfolgend dargestellt, aus dem Adresscode und zwei Funktionsbits zusammen.

$$\begin{array}{rcccl}
 \text{Funkcodenummer} = & \text{Adresscode} & + & \text{Funktionsbits} & \\
 & \text{(RIC = Radio Instruction Code)} & & & \\
 & 20 \text{ Bit} & & 18 \text{ Bit} & 2 \text{ Bit}
 \end{array}$$

Damit besitzt der Code je Kanalfrequenz ein Adresscodekontingent von 2.096.000. Im Abschnitt „Allgemeines“ sind die Blöcke der nutzbaren Adressen für Bund und Länder festgelegt.

Die Funktionsadressen A, B, C und D sind wie folgt durch die Funktionsbits definiert:

Funktionsadresse	Funktionsbits	Bedeutung	Sprachausgabe
A	0 0	Probealarm	Probealarm
B	0 1	Alarm/Einsatz	Einsatzalarm
C	1 0	Einsatzbereitschaft herstellen	Einsatzbereitschaft
D	1 1	Alarmierungsstelle anrufen	Rückruf

Der Empfänger muss mindestens zwei Adresscodes auswerten. Der 1. Adresscode wird zur individuellen Adressierung (Einzelruf, Sammelruf) verwendet. Der 2. Adresscode kann in einer Gruppe von Empfängern zur zusätzlichen Realisierung des Leistungsmerkmals „Gruppenruf“ genutzt werden. Der Adresscode muss auch nachträglich durch den Anwender veränderbar sein.

C.4.3. Nachrichtenspeicherung

Der Meldeempfänger muss in der Lage sein, Alarmrufe zu speichern und durch einfache Bedienung wiederzugeben. Nur-Ton-Empfänger müssen mindestens vier verschiedene Alarmrufe, alphanumerische Empfänger müssen diese zusätzlich mindestens mit maximaler Nachrichtenlänge speichern können (s. Abschnitt C 4.7).

C.4.4. Rufsignalisierung

C.4.4.1. Rufanzeige

Nachfolgend werden die Anforderungen beschrieben, die von einem Empfänger erfüllt werden müssen, um dem Benutzer einen eingegangenen Alarmruf zu signalisieren. Auf den eingegangenen Ruf soll (neben der optischen Anzeige beim Alphanumerik-Empfänger) aufmerksam gemacht werden. Es sind drei verschiedene Alarme zu unterscheiden:

- a) Akustischer Alarm (s. C.4.4.2)
- b) Speicheralarm (s. C 4.4.3)
- c) Stiller Alarm (s. C 4.4.4)

Der Empfänger muss auf die Alarme a) und b) wahlweise durch den Benutzer einstellbar sein. Der Alarm c) ist optional möglich und kann entweder anstelle b) oder zusätzlich angeboten werden.

C.4.4.2. Akustischer Alarm

Beim akustischen Alarm werden ankommende Alarmrufe durch ein akustisches Signal angezeigt und gespeichert. Zusätzlich oder anstelle des akustischen Alarmsignals kann auch eine Sprachausgabe entsprechend der Funktionsart ertönen (vgl. C 4.2). Die verschiedenen Funktionsadressen (s. C 4.2) müssen durch unterschiedliche akustische Signale angezeigt werden. Für die Dauer der Rufanzeige (= 8 Sekunden) sind die nachfolgend beschriebenen Tonfolgen ständig zu wiederholen. Der Alarmton sollte anfangs einen relativen Schalldruckpegel von 75 dB(A) im Abstand von 30 cm erzeugen, der sich zum Ende hin auf mindestens 80 dB(A) steigert. Der akustische Alarm muss durch Tastendruck einfach zu beenden sein.

Funktionsadresse A (Funktionsbits <20, 21> = <0 0> Tonfolge:
7/8 s Ein, 1/8 s Aus

Funktionsadresse B (Funktionsbits <20, 21> = <0 1> Tonfolge:

1/8 s Ein, 1/8 s Aus, 5/8 s Ein, 1/8 s Aus.

Funktionsadresse C (Funktionsbits <20, 21> = <1 0>

Tonfolge: 1/8 s Ein, 1/8 s Aus, 1/8 s Ein, 1/8 s Aus, 1/8 s Ein, 3/8 s Aus.

Funktionsadresse D (Funktionsbits <20, 21> = <1 1> Tonfolge:

4mal (1/8 s Ein, 1/8 s Aus), 1 s Aus.

C.4.4.3. Speicheralarm

Beim Speicheralarm werden ankommende Alarmrufe ohne oder mit sehr reduzierter akustischer Signalisierung gespeichert.

C.4.4.4. Stiller Alarm (Option)

Beim Stillen Alarm werden ankommende Alarmrufe nur durch einen Vibrator im Empfänger signalisiert und die Nachricht gespeichert.

C.4.5. Dekodierungsanforderungen

C.4.5.1. Allgemeines

Durch geeignete Maßnahmen ist sicherzustellen, dass die Wahrscheinlichkeit der falschen Dekodierung von Adress- und Codewörtern unter schlechten Empfangsbedingungen auf ein Minimum reduziert wird.

C.4.5.2. Fehlererkennung und -korrektur

Der Empfänger muss die Fehlererkennungsmöglichkeiten der redundanten Pfadkonfiguration (RPC) nutzen. Es muss bei Datenwörtern eine Fehlerkorrektur von einem Bit vorgesehen werden. Fehlerkorrekturen sollten im Empfänger intern erfolgen. Wenn eine fehlerbehaftete und nicht korrigierbare Nachricht erkannt worden ist und diese nicht als Ende einer Nachricht (s. C 4.5.4) angesehen wird, dann müssen die betroffenen Teile in der Anzeige geeignet markiert werden.

C.4.5.3. Wiedergewinnung der Synchronität

C.4.5.3.1. Definition

Die Wiedergewinnung der Synchronität ist die Fähigkeit des Empfängers, nach einer kurzzeitigen Unterbrechung des Empfangs (z. B. durch Abschattungen) die erforderliche Synchronität zum gesendeten Signal wiederherzustellen.

C.4.5.3.2. Messverfahren

Es wird nach dem nachfolgend beschriebenen Verfahren der Pegel des Nutzsignals bestimmt, bei dem die Anrufssicherheit 80 % beträgt:

- a) Auf den Empfänger wird ein Nutzsignal mit Prüfmodulation gegeben. Während der 2. bis einschließlich 5. Codewortgruppe ist der Pegel des Nutzsignals mindestens 40 dB unterhalb des Pegels des Referenzsignals gemäß C 3.2 abzusenken (=Austastung des Nutzsignals). Störsignale wirken nicht auf den Empfänger ein.
- b) Der Pegel des Signals wird so eingestellt, dass weniger als 10 % der Nur-Ton-Rufe erfolgreich sind.

c) Das Signal wird ständig wiederholt ausgesendet, wobei jedes Mal beobachtet wird, ob ein Nur-Ton-Ruf erfolgreich ist oder nicht.

d) Der Pegel des Signals

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist, oder
- wird um 1 dB erhöht, wenn ein Nur-Ton-Ruf nicht erfolgreich ist. Dieses Verfahren wird solange fortgesetzt, bis drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind.

Der zugehörige Pegel wird notiert.

e) Der Pegel wird um 1 dB verringert und der neue Pegel ebenfalls notiert. Anschließend wird das Nutzsignal mit Prüfmodulation 20mal ausgesendet.

Der Pegel des Signals

- bleibt unverändert, wenn ein Nur-Ton-Ruf erfolgreich ist,
- wird um 1 dB erhöht und der neue Pegel notiert, wenn ein Nur-Ton-Ruf nicht erfolgreich ist, oder
- wird um 1 dB verringert und der neue Pegel notiert, wenn drei aufeinander folgende Nur-Ton-Rufe erfolgreich sind.

f) Der Pegel des Nutzsignals, bei dem die Anrufsicherheit 80 % beträgt, ist der arithmetische Mittelwert der unter d) und e) notierten Pegelwerte des Nutzsignals mit Prüfmodulation.

C.4.5.3.3. Grenzwert

Das Pegelverhältnis Nutzsignal zu Referenzsignal darf 3 dB nicht überschreiten.

C.4.5.4. Ende einer Nachricht

Eine Nachricht ist beendet, wenn ein Adresscode oder ein Füllwort oder maximal zwei aufeinander folgende nicht korrigierbare Codewörter empfangen werden. Spätestens dann muss signalisiert werden. Alle zuvor dekodierten Codewörter der Nachricht müssen angezeigt werden.

C.4.5.5. Rufwiederholung

Systembedingte Rufwiederholungen über verschiedene Alarmumsetzer führen bei den Meldeempfängern zu Mehrfachempfang gleicher Alarmrufe. Deswegen dürfen innerhalb einer bis 4 min programmierbaren Stummschaltzeit (beginnend mit dem ersten empfangenen Alarmruf) gleiche Alarmrufe nur eine Rufanzeige bewirken. Dabei gilt:

- Nur-Ton-Rufe sind nur dann gleich, wenn sie die gleiche Funktionsadresse haben.
- Alphanumerische Alarmrufe sind nur dann gleich, wenn sie in der Funktionsadresse und im Nachrichteninhalt übereinstimmen.

Bei schlechten Empfangsbedingungen soll der Mehrfachempfang zur Korrektur fehlerhaft empfangener Teile der Nachricht genutzt werden.

C.4.6. Nachrichtenanzeige

Der Alphanumerik-Empfänger muss die in DIN 66003, deutsche Referenz-Version, aufgeführten Zeichen anzeigen können (s. Allg. Teil, 2.1.6). Zusätzlich muss die Funktionsadresse des Alarmrufs angezeigt werden. Es wird die gleichzeitige Anzeige von mindestens 16 Zeichen gefordert.

C.4.7. Maximale Nachrichtenlänge je Alarmruf

Der Alphanumerik-Empfänger muss Alarmrufe mit einer Nachrichtenlänge von mindestens 80 Zeichen speichern und zeilenweise anzeigen.

C.4.8. Funkversorgungsanzeige

Am Meldeempfänger soll erkennbar sein, ob eine nutzbare Funkversorgung vorhanden ist. Dazu wird vom Alarmgeber, wenn sonst keine Alarmrufe zu übertragen sind, periodisch zwischen 1 und 4 min. eine Präambel und ggf. eine Prüfadresse oder ersatzweise eine Codewortgruppe mit Füllwörtern gesendet. Erhält der Meldeempfänger diese Aussendung nicht, so sollte nach Ablauf einer intern programmierbaren Zeit ein kurzer Ton zu hören sein, bei alphanumerischen Empfängern zusätzlich ein Symbol im Anzeigefeld dauernd erscheinen, und so auf die Nicht-Erreichbarkeit hingewiesen werden. Dieser Hinweiston muss sich deutlich von den Signalen in C 4.4.2 unterscheiden.

C.5. Konstruktive Forderungen

C.5.1. Aufbau

C.5.1.1. Gehäuse

Das Gehäuse muss aus schlagfestem Kunststoff bestehen, der bis mindestens +70 ° C formbeständig ist. Es muss eine Einrichtung zur sicheren Mitnahme (stabiler Clip zur Befestigung an der Kleidung) vorhanden sein. Das Akku- bzw. Batteriefach muss vom sonstigen Geräteinnern abgetrennt sein. Für die Kontakte zum Akku und zum Heimzusatz durch federnde Elemente ist rostfreier Stahl oder Werkstoff mit gleichwertigen Eigenschaften zu verwenden.

Alle notwendigen Bedienelemente sollten an der Frontseite des Meldeempfängers angeordnet und so ausgeführt sein, dass sie auch bei rauer Behandlung nicht beschädigt oder unbeabsichtigt verstellt werden können. Sie sind eindeutig mit Symbolen oder in deutscher Sprache zu beschriften.

C.5.1.2. Typenschild

Auf der Rückseite ist ein Typenschild anzubringen. Die Verwendung von Klebefolie ist nur dann zulässig, wenn eine dauerhafte Verbindung zum Gerät erreicht wird und ein Abziehen nicht ohne Zerstörung derselben möglich ist.

Das Typenschild muss folgende Angaben enthalten:

- Bezeichnung
- Firmenzeichen
- Fabriknummer
- Herstellungsjahr
- Konformitätserklärung (CE-Kennzeichen)
- BOS- Prüfnummer
- Empfangsfrequenz
- Adresscode

Ein Teil der Angaben kann auch auf einem Schild im Akkufach untergebracht sein.

C.5.1.3. Beleuchtung

Bei Empfängern mit LC-Display sollte eine Beleuchtung vorhanden sein.

C.5.2. Beanspruchung

C.5.2.1. Schutzart

Die Meldeempfänger müssen der Schutzart IP 52 nach EN 60529 entsprechen und gegen Körperschweiß unempfindlich sein.

C.5.2.2. Schockbeanspruchung

Die mechanische Schockbehandlung für die Prüfung ist nach DIN EN 60068 2-7 und 2-31 vorzunehmen. Es gelten folgende Bestimmungen:

Schärfegrad:	50 g
Schockdauer:	11 ms
Schockform:	Halbsinus
Art der Beanspruchung:	Es sind in beiden Richtungen der drei senkrecht zueinanderstehenden Achsen je drei aufeinander folgende Schocks (insgesamt 18 Schocks) durchzuführen.

C.5.2.3. Schwingbeanspruchung

Die Schwingbeanspruchung ist nach DIN EN 60068 2-6 vorzunehmen. Es gelten folgende Bestimmungen:

Dauer:	Je drei Minuten in den Richtungen der drei senkrecht zueinanderstehenden Achsen
Hub:	$\pm 0,2$ mm
Frequenzbereich:	0 bis 30 Hz, 30 bis 0 Hz während drei Minuten zu durchlaufen.

C.5.2.4. Klimatische Beanspruchung

C.5.2.4.1. Normale Beanspruchung

Der Meldeempfänger muss die geforderten Eigenschaften, Daten und deren Toleranzen im Temperaturbereich 0 °C bis +40 °C bei Luftfeuchten von 20 bis 75 % relative Feuchte erfüllen.

C.5.2.4.2. Extreme Beanspruchung

Der Meldeempfänger muss funktionsfähig bleiben im Temperaturbereich -10 °C bis +55 °C und bei Luftfeuchten von 20 % bis 95 % rel. Feuchte.

C.6. Stromversorgung

C.6.1. Akkubetrieb

Die Stromversorgung soll aus einem Akku (Form möglichst R 6 nach IEC) bestehen.

Das Auswechseln des Akkus muss ohne Werkzeug möglich sein. Auffällige und eindeutige Hinweise müssen die Wahrscheinlichkeit eines falschen Einlegens verringern. Der Empfänger darf keinen mechanischen oder elektrischen Schaden durch falsches Einsetzen des Akkus erleiden.

Der Akku muss eine Empfangsbereitschaft von mindestens 200 Stunden gestatten und am Ende dieser Zeit die Signalisierung noch wenigstens eines Alarmrufes ermöglichen. Die Betriebszeit muss erreicht werden bei Umgebungstemperaturen von - 10 °C bis + 40 °C und auch nach 300 Ladezyklen. Deswegen muss die Nennkapazität des Akkus mindestens dem 1,2fachen der benötigten Gesamtkapazität entsprechen.

Auf das Ende der Betriebszeit ist bei DME II mit alphanumerischer Anzeige etwa 1 Tag vorher durch ein Symbol im Anzeigefeld hinzuweisen. Bei Nur-Ton-Empfängern (DME I) und Empfängern mit Sprachansage (DME III) wird der ausreichende Ladezustand durch einen kurzen Ton beim Einschalten signalisiert, sinkt die verbleibende Akkukapazität unter 33 %, ist dies akustisch anzuzeigen.

In Ausnahmefällen muss der Akku durch eine handelsübliche Trockenbatterie ersetzt werden können. Ist dies nicht möglich, so muss der Empfänger mit einem Ersatzakku ausgeliefert werden.

C.6.2. Betrieb mit Heimzusatz

Der Heimzusatz enthält ein Ladeteil für den im Meldeempfänger eingebauten Akku mit Ladekontrollanzeige und einen Anschluss für externe Signaleinrichtungen sowie für eine Hilfsantenne.

Für das eingebaute Ladeteil gilt:

Die Ladung muss bei Netzspannung $230\text{ V} \pm 10\%$ und 50 Hz und mit einer Ladestrombegrenzung erfolgen³. Während der Ladung muss der Meldeempfänger empfangsbereit bleiben (Pufferbetrieb). Die Ladung muss nach Einschieben des Meldeempfängers in den Heimzusatz beginnen und auch bei vollständig entladenerm Akku nach 12 Stunden beendet sein. Der Ladestrom ist durch eine gelbe Kontrolllampe (beschriftet „LADEN“ oder Symbol) anzuzeigen. Eine Entladung des Akkus über die Ladeschaltung (z. B. bei Netzausfall) darf nicht erfolgen. Puffer-Dauerbetrieb darf nicht zu einer Schädigung des Akkus führen.

Ein Alarmruf mit akustischer Signalisierung im Meldeempfänger muss im Heimzusatz zum Schließen eines potentialfreien Kontakts führen. Durch Betätigen der Löschtaste wird der Kontakt wieder geöffnet.

Kontaktbelastbarkeit: 1 A, mind. 30 V; Anschluss: Schraubklemme mit Drahtschutz oder Diodenbuchse DIN 41 524, Kontakt zwischen Stift 1 und 3. Die Halteschaltung darf ihren Strom nur der Netzversorgung entnehmen. Der Anruf kann auch zusätzlich optisch mit einer roten Leuchtdiode (beschriftet: „ANRUF“ oder Symbol) signalisiert werden.

Über eine BNC-Buchse muss der Anschluss einer Hilfsantenne möglich sein.

Die Verfügbarkeit eines Heimzusatzes ist nicht Voraussetzung für die Erteilung einer Prüfnummer.

C.7. Technische Unterlagen

Jedem Meldeempfänger ist eine Betriebsanleitung in deutscher Sprache beizufügen. Auf besondere Anforderung sind bereitzustellen:

- Ausführliche Funktionsbeschreibung
- Vollständiges Datenblatt
- Blockschaltbild mit Frequenzangaben
- Gesamtschaltplan mit Positionsangaben und Angabe der Spannungs- und Stromwerte an den Prüfpunkten.
- Austausch- und Verschleißteillisten mit Bestellangaben
- Programmiersoftware soweit erforderlich

³ Die elektr. Sicherheit im Sinne der gültigen Technischen Regeln ist nicht Gegenstand einer Zulassung nach TR BOS.

Teil D: DIGITALE SIRENENSTEUEREMPFÄNGER

D.1. Aufgabe

Digitale Sirenensteuerempfänger (DSE) sind ortsfeste Empfangsfunkanlagen für Fernsteuer- und Fernwirkzwecke in Systemen mit digitaler Funkalarmierung und enthalten einen Einkanal-Empfänger für HF-DFSK-Modulation. Sie empfangen Alarmrufe und steuern damit Kontakte.

Sollen DSE mit einer Quittierungseinrichtung (z.B. über GSM) ausgestattet werden, müssen die Forderungen 2.3.1 bis 2.3.7 ebenfalls erfüllt werden.

D.2. Technische Forderungen

D.2.1. Sabotageschutz

Es ist durch ein passwortgeschütztes Authentifizierungsverfahren technisch sicherzustellen, dass eine Auslösung des Sirenenprogramms nur beim Empfangen des RIC sowie der zugehörigen Funktionsadresse erfolgt.

D.2.2. Empfangssignal

Der Einkanal-Empfänger muss auf einer Frequenz im Bereich von 165 bis 174 MHz zu betreiben sein. Kanalraster ist 20 kHz, eine nachträgliche Anpassung an ein anderes Raster, z.B. 12,5 kHz, muss möglich sein. Zur Modulation des Trägers wird eine Frequenzumtastmodulation (HF-DFSK) mit einem Hub von + - 4 kHz (bei 20-kHz-Raster) angewendet.

Logischer Pegel:	0	->	Ablage:	+ 4 kHz bezogen auf Nennfrequenz	Logischer Pegel:
	1	->	Ablage:	- 4 kHz bezogen auf Nennfrequenz.	

Die Abweichung von der Nennfrequenz darf auch unter extremen Bedingungen maximal \square 1 kHz betragen.

D.2.3. Empfänger

Bei den in EMK angegebenen Spannungswerten wird bei der Messung davon ausgegangen, dass die Ausgangsimpedanz des Messendes gleich der Nennimpedanz des Empfängereingangs ist.

Die folgenden Werte sind Mindestforderungen. Ihr Unter- bzw. Überschreiten im Sinne einer Verbesserung ist anzustreben.

D.2.3.1. Empfindlichkeit

Die Empfindlichkeit (= maximaler Eingangsspannungsbedarf, damit 9 von 10 Alarmrufe richtig empfangen werden):

< 2 μ V (EMK)

Nachfolgende Messungen sind analog C durchzuführen:

D 2.3.2	Gleichkanalunterdrückung	\square - 8 dB
D 2.3.3	Nachbarkanaldämpfung	> 80 dB
D 2.3.4	Nebenempfangsdämpfung	> 80 dB
D 2.3.5	Intermodulationsdämpfung	> 70 dB
D 2.3.6	Blocking (+/- 1 ... 10 MHz):	> 90 dB μ V
D 2.3.7	Störleistung (30 bis 1.000 MHz)	< 2 nW

D.2.4. Auswertung

Die binäre Funkcodenummer, auf die der DSE ansprechen muss, setzt sich aus dem Adresscode und zwei Funktionsbits zusammen.

$$\begin{array}{rcccl} \text{Funkcodenummer} & = & \text{Adresscode} & + & \text{Funktionsbits} \\ 20 \text{ Bit} & & 18 \text{ Bit} & & 2 \text{ Bit} \end{array}$$

Der Adresscode, optional auch weitere, muss am Aufstellungsort im Geräteinnern veränderbar sein. Die Funktionsadressen A, B, C und D sind durch die Funktionsbits definiert.

Die Sirenensteuereinheit für das Feuersignalsignal enthält einen Auswerter für die Funktionsadresse B, der einen Programmsteuerteil für das Feuersignalsignal (Ton - Pause - Ton - Pause - Ton, jeweils 12 + - 1 s Dauer) startet. Der Empfang der gleichen Funkcodenummer innerhalb der nächsten 2 min nach Programmstart darf nicht zu einem weiteren Sirenenablauf führen. Der Empfang einer weiteren davon abweichenden Funkcodenummer soll gespeichert werden und im Anschluss das entsprechende Programm starten.

Der Programmsteuerteil muss auch durch einen externen Kontakt, Schließzeit 0,5 bis 1 s, für jeweils einen Programmablauf auszulösen sein. Dieser Eingang zum Start der Sirene am Aufstellungsort muss gegen Fehl-auslösung durch Überspannungsspitzen auf den angeschlossenen Leitungen geschützt sein. Ein Dauerkontaktschluss darf nicht zu einem weiteren Programmablauf führen.

Der Auswerter darf auch mit der Funktionsadresse A den Sirenenkontakt-Ausgang für 1 bis 2 s schließen (Kurzanlauf zur Funktionsprobe).

Optional kann der Auswerter auch mit den zusätzlichen Funktionsadressen C und D spezielle Alarmprogramme auslösen.

Funktionsadresse	Funktionsbit 20, 21	Ausgang
A	00	Kontakt für 1-2 s schließen
B	01	Kontakt für 60 s im 12 s Takt schließen und öffnen
C	10	Kontakt für 60 s im 2 s Takt schließen und öffnen
D	11	Kontakt für 60 s schließen

Kontaktbelastbarkeit: 250 V, 1 A, potentialfrei

D.2.5. Stromversorgung

Der digitale Sirenensteuerempfänger wird mit einer Versorgungsspannung von 230 V \pm 10 % betrieben⁴. Bei der Steuerung netzunabhängiger Sirenen muss ein Akku mit Tiefentladeschutz anschließbar sein, der Netzausfälle bis zu 24 Stunden, auch bei extremen Betriebsbedingungen, überbrücken kann.

⁴ Die elektr. Sicherheit im Sinne der gültigen Technischen Regeln ist nicht Gegenstand einer Zulassung nach TR BOS.

D.3. Konstruktive Forderungen

D.3.1. Gestaltung

Der Digitale Sirenensteuerempfänger ist als Wandgehäuse auszuführen. Es wird eine weitgehende Störeinstrahlungsfestigkeit gegenüber hochfrequenten (\square 10 V/m) und magnetischen Feldern gefordert.

D.3.2. Typenschild

Am Digitalen Sirenensteuerempfänger muss ein Typenschild mit folgenden Angaben dauerhaft angebracht sein:

- Gerätebezeichnung
- Konformitätserklärung (CE- Zeichen)
- BOS- Prüfnummer
- Fertigungsnummer
- Herstellungsjahr
- Firmenname /-zeichen

D.3.3. Aufbau

Der mechanische und elektrische Aufbau des Geräts soll ein problemloses Auswechseln der Bauteile und Baugruppen erlauben. Frequenzbestimmende Baustufen und Bauteile müssen künstlich gealtert sein.

D.3.4. Beanspruchung

Der Digitale Sirenensteuerempfänger muss den Einflüssen standhalten, denen er in ungeheizten Räumen ausgesetzt ist, ohne dass dadurch die Betriebsdaten eingeschränkt oder bleibende Schäden verursacht werden. Für die relative Luftfeuchte sind nach DIN EN 60721 die Anforderungen nach Kennbuchstabe "E" einzuhalten.

D.3.4.1. Schutzart

Nach EN 60529, muss das Gerät mindestens die Forderungen für die Schutzart IP 54 erfüllen. Ortsspezifisch höhere Anforderungen sind zwischen Anwender und Hersteller besonders zu vereinbaren.

D.3.4.2. Betriebsbedingungen

D.3.4.2.1. Normale Betriebsbedingungen

Soweit nicht besonders angegeben müssen die geforderten Daten bei Umgebungstemperaturen von $- 10^{\circ} \text{C}$ bis $+ 40^{\circ} \text{C}$ und bei Spannungsschwankungen des 230 V-Netzes von \square 10 % eingehalten werden.

D.3.4.2.2. Extreme Betriebsbedingungen

Bei extremen Temperaturen über die normalen Betriebsbedingungen hinaus bis $- 25^{\circ} \text{C}$ und bis $+ 55^{\circ} \text{C}$ sowie Schwankungen der Netzspannung von \square 15 % muss weiterhin Empfangsbetrieb möglich sein. Für tiefere Außentemperaturen bis $- 40^{\circ} \text{C}$ kann ein besonders isoliertes und evtl. mit Heizung ausgestattetes Übergehäuse verwendet werden.

D.3.4.2.3. Mechanische Beanspruchung

Der DSE wird ortsfest wettergeschützt eingesetzt. Bei der Klassifizierung der Umweltbedingungen wird

gemäßigtes Klima zugrunde gelegt. Bezogen auf DIN EN 60721-3-0 wird gemäß E - DIN 40046-721-3 folgende Klasse der mechanischen Umweltbedingung festgelegt: 3 M 1. Unter diesen Umweltbedingungen muss die einwandfreie Funktion des DSE gewährleistet sein.

D.4. Technische Unterlagen

Auf besondere Anforderung sind folgende Unterlagen bereitzustellen:

- Bedienungsanweisung
- Vollständiges Datenblatt
- Blockschaltbild mit Frequenzangaben
- Ausführliche Funktionsbeschreibung
- Gesamtschaltplan
- Baugruppenschaltpläne mit Positionsangaben, Halbleiter-Sockelangaben und Steckerbezeichnungen
- Programmablaufplan für die Fehlersuche
- Stromlaufplan mit allen für eine ordnungsgemäße Überprüfung und Einstellung notwendigen Angaben (Spannungs- und Stromwerte, Pegel, Impulsdigramme und Angaben zu den jeweils verwendeten Messgeräten)
- Austausch- und Verschleißteilliste mit Bestellangaben
- Wartungsvorschrift mit Angabe der durchzuführenden Messungen und Einstellungen in der richtigen Reihenfolge
- Programmiersoftware soweit erforderlich

Teil E – Verschlüsselungsverfahren für die digitale Funkalarmierung

E.1. Einleitung

Dieser Anhang soll sicherstellen, dass die Verschlüsselung der Endgeräte (DME, DSE, etc.) vom Hersteller unabhängig in einem beliebigen Netz betrieben werden können.

Er definiert ein offenes lizenzfreies Verfahren, um neben der Nur-Ton- und Alphanummerischen Alarmierung auch eine einheitliche verschlüsselte Text-Alarmierung zu gewährleisten.

E.2. Leistungsmerkmale

Das im Folgenden beschriebene kryptografische Verfahren zeichnet sich durch folgende Leistungsmerkmale aus:

- Verschlüsselung AES-256
- Daten-Authentisierung AES-CMAC (128 Bit)
- Verschlüsselung und Daten-Authentisierung mit getrennten Schlüsseln
- Sichere Zeitauthentifizierung der Nachricht
- Meldungsintegrität (Text und Zeit) Verschleierung der Meldungslänge (Padding)
- Overhead durch Verschlüsselung 80 Bit (4 Codeworte)
- Dynamische Schlüsselwahl mit Schlüsselindex erlaubt die Auswahl von 256 verschiedenen Schlüsseln, Empfehlung:
 - o 4 individuelle Schlüssel pro RIC
 - o zusätzlich 252 allgemeine Schlüssel
- Erkennung unverschlüsselter Nachrichten möglich
- Vereinbarkeit mit der DSGVO
- Vereinbarkeit mit dem Cyber Resilience Act (Verordnung EU 2024/2847 des europäischen Parlaments und des Rates)

E.3. Verfahrensbeschreibung

E.3.1. AES-256

Der Advanced Encryption Standard mit 256 Bit Schlüssellänge (AES-256) ist ein symmetrisches Block-Verschlüsselungsverfahren mit einer Blockgröße von 128 Bit.

Es wird eine symmetrische Verschlüsselung verwendet, bei dieser nutzen Sender und Empfänger denselben, geheimen Schlüssel, um eine Nachricht sowohl zu ver- als auch zu entschlüsseln.

Im Counter-Modus (CTR) wird der AES-Blockchiffre in einen Stromchiffre umgewandelt.

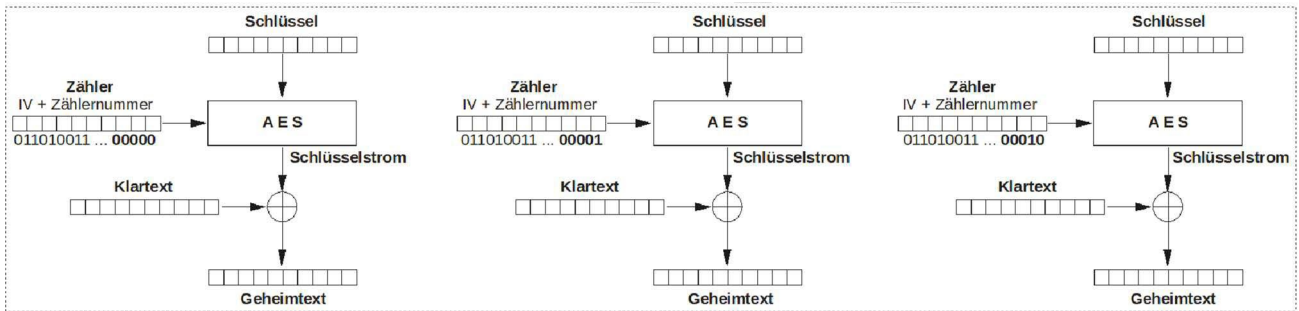
Dabei wird ein Zähler mit dem Schlüssel verarbeitet. Das Ergebnis (Stromschlüssel) wird dann per XOR-Operation mit dem Klartext kombiniert, um den Geheimtext zu erzeugen.

Zur Erzeugung weiterer Zwischenschlüssel wird der Zähler inkrementiert.

Der Zählerblock darf bei Verwendung desselben Schlüssels nicht mehr als einmal vorkommen.

AES und der Counter-Modus werden in der BSI TR-02102-1 Abschnitt 3.1 ausdrücklich empfohlen.

E.3.1.1. Verschlüsselung



Initialisierung des Zählers

Ein Initialisierungsvektor (IV) und eine eindeutige Zählernummer werden kombiniert, um den Startblock zu bilden.

Verschlüsselung des Zählers

Der Startblock wird durch den AES-Algorithmus mit dem geheimen Schlüssel verschlüsselt.

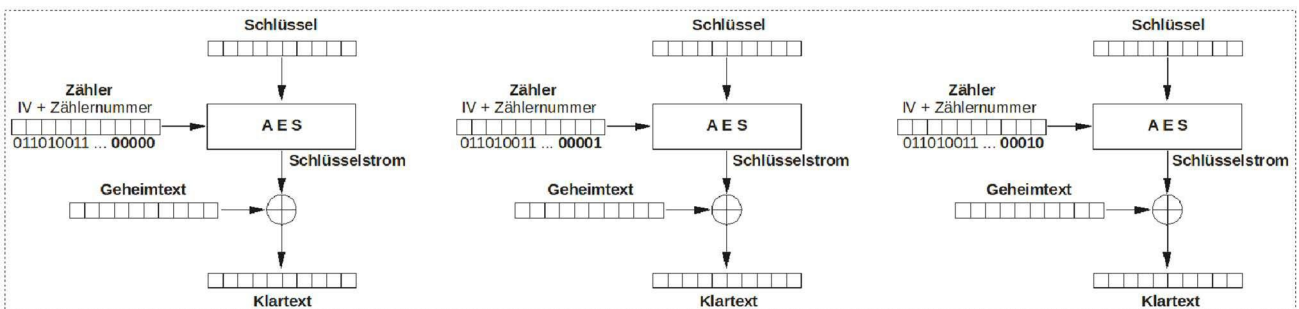
XOR mit Klartext

Das Ergebnis der Zählerverschlüsselung (Stromschlüssel) wird mit dem jeweiligen Klartext XOR verknüpft, um den Geheimtext zu erzeugen.

Inkrementieren des Zählers

Der Zähler wird für den nächsten Block hochgezählt, die Verschlüsselung des Zählers und die XOR-Verknüpfung mit dem Klartext so oft wiederholt, bis alle Klartextblöcke verschlüsselt sind.

E.3.1.2. Entschlüsselung



Initialisierung des Zählers

Für die Entschlüsselung muss der identische Startblock (IV und Zählernummer) verwendet werden, wie bei der Verschlüsselung.

Verschlüsselung des Zählers

Der Startblock wird mit dem identischen Schlüssel wie bei der Verschlüsselung verschlüsselt.

XOR mit Geheimtext

Das Ergebnis der Zählerverschlüsselung (Stromschlüssel) wird mit dem jeweiligen Geheimtext XOR verknüpft, um den Klartext zurückzugewinnen.

Inkrementieren des Zählers

Der Zähler wird für den nächsten Block hochgezählt, die Verschlüsselung des Zählers und die XOR-Verknüpfung mit dem Geheimtext so oft wiederholt, bis alle Klartextblöcke zurückgewonnen sind.

E.3.2. Daten-Authentisierung AES-CMAC (128 Bit)

Um die Integrität einer Meldung überprüfen zu können, wird über die zu schützenden Daten (Meldung) mit einem geheimen Schlüssel unter Verwendung der AES-256 Verschlüsselung eine Prüfsumme MAC (Message Authentication Code) gemäß RFC 4493 berechnet. Jede kleine Veränderung der Daten liefert eine komplett andere Prüfsumme.

Die Prüfsumme MAC schützt die Meldung vor Manipulation.

Die Erzeugung einer gültigen Prüfsumme MAC über einen veränderten (manipulierte Meldung) oder neuen Text (Falschmeldung) ist nur mit Hilfe des geheimen Schlüssels möglich.

E.3.3. Erzeugung von abgeleiteten Schlüsseln

Zur Verschlüsselung und Daten-Authentisierung müssen unterschiedliche Schlüssel eingesetzt werden (vgl. BSI TR-02102-1 Abschnitt B.1.1, "NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication" Abschnitt 5.2).

Um begrenzt vorhandenen Speicherplatz zu sparen, werden aus einem 256 Bit Key zwei Schlüssel in Anlehnung an das HKDF-Verfahren gemäß RFC 5869 abgeleitet.

Der Unterschied zum Verfahren gemäß dem RFC besteht lediglich darin, dass statt HMAC-SHA256 wiederum AES-CMAC eingesetzt wird.

E.3.4. Schlüsselmanagement

Über den Schlüsselindex sind 256 unterschiedliche Schlüssel dynamisch anwählbar.

Damit können beispielsweise jedem RIC vier individuelle Schlüssel zugewiesen werden.

Darüber hinaus gibt es 252 allgemeine Schlüssel, welche RIC-unabhängig genutzt werden können. Aus individuellem Schlüssel und Allgemeinem Schlüssel werden durch eine Berechnung abgeleitete Schlüssel erzeugt, den tatsächlich verwendeten 256Bit AES-Schlüssel und CMAC-Schlüssel.

E.3.4.1. Schlüsselindex

Die bei der Verschlüsselung verwendete Schlüsselnummer (Schlüsselindex) muss bei der Entschlüsselung bekannt sein.

E.3.4.2. Dynamische Schlüsselwahl

Der verwendete Schlüsselindex wird als Bestandteil der Geheimnachricht zur Entschlüsselung im Initialvektor übermittelt.

Der Schlüsselindex kann von Geheimnachricht zu Geheimnachricht variiert werden (dynamische Schlüsselwahl).

E.3.5. Header der Geheimnachricht

Zur Entschlüsselung müssen der verwendete Schlüsselindex und der Initialisierungsvektor bekannt sein. Mindestens diese Informationen müssen zusätzlich zu dem Geheimtext in einem Header mit übergeben werden und zur Entschlüsselung fehlerfrei empfangen werden.

E.3.5.1. Initialisierungsvektor (IV)

Der Initialisierungsvektor wird aus einem Zeitstempel gebildet. Der Zeitstempel hat eine Länge von 32 Bit im Sekunden Raster. Den Basiswert bildet die Systemzeit (00:00:00 01.01.2025 UTC).

Durch UTC finden in der Alarmmeldung keine Zeitsprünge durch Normalzeit-/Sommerzeit- Umstellung statt.

Dieser Initialisierungsvektor liefert gleichzeitig das Kriterium für die Zeitauthentifizierung. Die Entschlüsselung der Geheimnachricht ist auch bei fehlgeschlagener Zeitauthentifizierung (unbekannte oder abweichende Uhrzeit) möglich.

E.3.5.2. Schlüsselindex

Der verwendete Schlüsselindex hat eine Länge von 8 Bit.

E.3.5.3. Header-Prüfsumme

Zur Absicherung, ob es sich um gültige Werte zur Startblockbildung handelt, ist eine Prüfsumme über Initialisierungsvektor und Schlüsselindex vorgesehen. Diese wird ebenfalls Teil des Headers.

Die Prüfsumme hat eine Länge von 8 Bit: CRC-8 Polynom ($x^8 + x^2 + x^1 + 1$) Startwert bei der Berechnung ist der Wert 0x00.

Diese Prüfsumme ist Teil vom dritten Header-Codewort. Auch bei Empfangsfehlern in der Prüfsumme bleibt der Geheimtext entschlüsselbar.

Stimmt die CRC-8 Prüfsummenberechnung bei der Entschlüsselung nicht mit der im Header der Geheimnachricht übergebenen und fehlerfrei empfangenen CRC-8 Prüfsumme überein, so ist dieses als Kriterium zur Erkennung unverschlüsselter Nachrichten (Fallback) zu verwenden.

E.3.5.4. Meldungsintegrität

Zur Prüfung, ob der Text vollständig und unverändert vorliegt, wird mit dem abgeleiteten, geheimen CMAC-Schlüssel über den verschlüsselten Text (Chiffre) unter Verwendung des AES-CMAC Algorithmus eine Prüfsumme MAC (Message Authentication Code) gebildet.

Auch die Alarmzeit geht in die Prüfsummen-Berechnung ein.

Die höchstwertigen 32 Bit dieses Ergebnisses sind ebenfalls Teil des Headers der Geheimnachricht.

Zur Prüfung der Meldungsintegrität wird die Prüfsumme MAC über den verschlüsselten Text gebildet und mit der Information aus dem Header der Geheimnachricht verglichen.

Empfangsfehler (fehlerhafte Zeichen und unvollständige Texte) führen zwangsläufig zu einem Fehler bei der Meldungsintegritätsprüfung. Der Geheimtext bleibt aber auch bei Empfangsfehlern entschlüsselbar.

Die Prüfsumme MAC berechnet sich wie folgt:

MAC = AES-CMAC (CMAC-Schlüssel, Geheimtext)

Der Geheimtext wird als Stream der verschlüsselten Codeworte CWG1 || CWG2 || CWG3 || .. CWGn Byteweise übergeben.

Geheimtext = CWG1 || CWG2 || CWG3 ||.. CWGn mit n= Anzahl der Geheimtext Codeworte

E.3.5.5. Zusammenfassung Header

Es ergibt sich folgender Header-Aufbau:

Headerlänge gesamt:	80 Bit
Initialisierungsvektor (Zeitstempel):	32 Bit im Sekunden Raster, Basis Systemzeit (00:00:00 01.01.2025 UTC), niederwertigstes Byte zuerst (Little Endian)
Schlüsselindex:	8 Bit (Wertebereich 0..255)
Header-Prüfsumme:	8 Bit CRC-8 Polynom: $x^8 + x^2 + x^1 + 1$, Startwert:0x00
Prüfsumme MAC:	32 Bit (von 128Bit AES-CMAC)

E.3.6. Verschlüsselungs-Algorithmus AES-256 im Counter Mode (CTR)

- Verfahren: AES-256
- Schlüssellänge: 256 Bit
- Blockgröße: 128 Bit

E.3.6.1. Initialisierung des Zählerblocks

Der Zählerblock wird gebildet aus den ersten 40 Bit des Headers (Zeitstempel, Schlüsselindex) der Geheimnachricht und dem eindeutigen Zählerstartwert = Null (88 Bit) aufgefüllt, um die erforderliche Länge der Blockgröße des Verschlüsselungsverfahrens (also 128 Bit) zu erhalten.

Durch den sekundengenauen Zeitstempel ist sichergestellt, dass sich der Zählerblock niemals wiederholen wird. Jeder Zählerblock darf pro Schlüssel nur einmal verwendet werden.

E.3.6.2. Erzeugung von abgeleiteten Schlüsseln

Die Berechnung von abgeleiteten Schlüsseln erfolgt zweistufig in Anlehnung an RFC 5869

- Ermittlung eines zufälligen Schlüssels PRK (Pseudo Random Key)
- Berechnung von abgeleiteten Schlüsseln unter Verwendung des PRK

Aus einem geheimen Ausgangsschlüssel und einer Zusatzinformation wird ein Pseudozufalls- Schlüssel PRK als Zwischenschlüssel abgeleitet. Unter Verwendung dieses Zwischenschlüssels werden die beiden benötigten abgeleiteten Schlüssel (AES-Schlüssel, CMAC-Schlüssel) gebildet.

Als Zusatzinformation wird der Zeitstempel und Schlüsselindex verwendet. Durch den sekundengenauen Zeitstempel ist sichergestellt, dass sich eine Zusatzinformation niemals wiederholen wird. Es handelt sich um einen Quasi-Zufallswert.

Die Zusatzinformation (256 Bit) wird gebildet aus den ersten beiden Header-Codeworten CWH1 und CWH2 der Geheimnachricht, aufgefüllt mit 27 Null-Bytes:

Zusatzinformation = CWH1 || CWH2 || 0x0000000000000000000000000000

Die PRK-Bildung erfolgt durch eine mehrstufige AES-CMAC Berechnung:

PRK_hi = AES-CMAC (geheimer Schlüssel, Zusatzinformation)

PRK_lo = AES-CMAC (geheimer Schlüssel, PRK-hi || 0x00)

PRK = PRK_hi || PRK_lo

Die Berechnung der abgeleiteten Schlüssel erfolgt mehrstufig durch AES256-CMAC Berechnung:

AES-Schlüssel_hi = AES-CMAC (PRK, 0x01)

AES-Schlüssel_lo = AES-CMAC (PRK, AES-Schlüssel_hi || 0x02)

CMAC-Schlüssel_hi = AES-CMAC (PRK, AES-Schlüssel_lo || 0x03)

CMAC-Schlüssel_lo = AES-CMAC (PRK, CMAC-Schlüssel_hi || 0x04)

AES-Schlüssel = AES-Schlüssel_hi || AES-Schlüssel_lo

CMAC-Schlüssel = CMAC-Schlüssel_hi || CMAC-Schlüssel_lo

E.3.6.3. Verschlüsselung / Entschlüsselung

Aus dem Zählerblock wird mit dem durch den Schlüsselindex angezeigten Schlüssel ein 128 Bit großer Stromschlüsselblock errechnet.

Alle Zeichen einer Nachricht werden im 7 Bit ASCII Format (Bitreihenfolge LSB first) in Blöcke von 40 Bit (Payload von 2 POCSAG Nachrichten Codeworten) aufgeteilt (Kompression).

Der Nachricht sind abschließend so viele "0"-Bit anzufügen (Padding), dass sich die Bit-Anzahl als Vielfaches von 40 Bit ergibt.

Nachricht N = "Text der Nachricht"

Kompression M = N1 || N2 || N3 .. || Nn mit n = Anzahl der Zeichen der Nachricht
N = Klartextzeichen (7 Bit, LSB first)

Klartext (Payload) K = M || (m * 02) mit m=40 – MODULO(d,40)
d = Anzahl der Zeichen der Kompression M

Jeder 40 Bit-Block des Klartextes wird durch XOR mit dem Stromschlüsselblock zum Geheimtext, bzw. umgekehrt. Der erste 40 Bit-Block nutzt dazu die 40 höchstwertigsten Bits des Stromschlüsselblock (Bit127..88), alle folgenden 40 Bit-Blöcke die jeweils niederwertigeren 40 Bit des Stromschlüsselblock (Bit 87..48, 47..8, 7..96Folgeblock,95..56, ...)

Geheimtext = Klartext XOR Stromschlüsselblock

Klartext = Geheimtext XOR Stromschlüsselblock

Zur Erzeugung weiterer Schlüsselstromblöcke wird der Zählerblock hochgezählt.

E.3.6.4. Störanfälligkeit

Empfangsfehler im Geheimtext führen zum Fehler bei der Meldungsintegritätsprüfung. Der Geheimtext bleibt aber auch bei Empfangsfehlern entschlüsselbar und lesbar, sofern der Zählerblock im Header der Geheimnachricht (die ersten beiden Codeworte) fehlerfrei oder korrigierbar (max. 2 Bitfehler) ist.

Die Lesbarkeit durch Empfangsfehler im Geheimtext wird gegenüber einer unverschlüsselten Nachricht nicht verschlechtert (keine Fehlerfortpflanzung).

Die Entschlüsselung der Geheimnachricht bleibt auch bei fehlgeschlagener Zeitauthentifizierung (unbekannte oder abweichende Uhrzeit) möglich.

Fehler bei der Meldungsintegritätsprüfung oder der Zeitauthentifizierung sind dem Nutzer anzuzeigen.

Input = 3b777579cbbf0c8df6c9202894b563303
 CMAC-Schlüssel_hi = AES-CMAC (PRK, Input)
 = 1a6220a89cffa76f327bda8e4cb4c9ec

 Input = 1a6220a89cffa76f327bda8e4cb4c9ec04
 CMAC-Schlüssel_lo = AES-CMAC (PRK, Input)
 = 19013556e2753eb1f23f7744b603b0e5

 AES-Schlüssel = AES-Schlüssel_hi || AES-Schlüssel_lo
 = eedeaba836d9eb1584d6e4e11765c20f3b777579cbbf0c8df6c9202894b5633

 CMAC-Schlüssel = CMAC-Schlüssel_hi || CMAC-Schlüssel_lo
 = 1a6220a89cffa76f327bda8e4cb4c9ec19013556e2753eb1f23f7744b603b0e5

E.5.2. Geheimtext

123450A Probealarm, Leitstelle nicht anrufen

Der Nachrichtentext besteht im Beispiel aus 35 Zeichen mit je 7Bit = 245Bit

Dem Text sind so viele NULL-Bit anzufügen (Padding), dass sich die Bit-Anzahl als Vielfaches von 40 Bit ergibt (gerade Anzahl von Codeworten, sonst kann der CMAC nicht mit Standardfunktionen gebildet werden).

Im Beispiel sind die 35 Zeichen (245Bit) mit 35 NULL-Bit auf 280 Bit zu füllen.

Es ergibt sich folgendes POCSAG Telegramm (mit Nachrichten Codeworten Klartext):

7A89C197 7A89C197 7A89C197 7A89C197 0788E483 854FE82D D1D3801B E6E1A742 FB66874F
 919A76AA ACBE70C8 AF4CDBE5 9BA60983 9DCBC6D7 E2CB879B A86ED543 BD76762D
 CDD80769 80000769 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197
 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197

Payload (Klartext) 280 Bit (20 Datenbit je Codewort)

0a9fd a3a70 cdc34 f6cd0 2334e 597ce 5e99b 374c1 3b978 c5970 50dda 7aece 9bb00

Schlüsselstrom

AES Schlüssel	eedeaba836d9eb1584d6e4e11765c20f3b777579cbbf0c8df6c9202894b5633	Zähler
0	d5fa1f01010000000000000000000000	
Schlüsselstrom 0	307d22c8181de78b1182a75112f3aed8	
Zähler 1	d5fa1f01010000000000000000000001	
Schlüsselstrom 1	c790166c13618592e181fdecbf1a7d192	
Zähler 2	d5fa1f01010000000000000000000002	
Schlüsselstrom 2	9c85deb5db7caa84d44bdd0517dd1799	
Schlüsselstrom = (Schlüsselstrom 0) (Schlüsselstrom 1) (Schlüsselstrom 2)		

307d22c8181de78b1182a75112f3aed8 c790166c13618592e181fdecbf1a7d192
 9c85deb5db7caa84d44bdd0517dd1799

Chiffprat (verschlüsselter Payload Text) 280Bit

Chiffprat = Payload (Klartext) XOR Schlüsselstrom

```
0a9fda3a70 cdc34f6cd0 2334e597ce 5e99b374c1 3b978c5970 50dda7aece 9bb0000000
XOR
307d22c818 1de78b1182 a75112f3ae d8c790166c 13618592e1 81fdcbf1a7 d1929c85de
=
3ae2f8f268 d024c47d52 8465f76460 865e2362ad 28f609cb91 d1206c5f69 4a229c85de
```

E.5.3. Prüfsumme MAC

Die Prüfsumme MAC wird über das Chiffprat (verschlüsselter Payload Text) gebildet

Chiffprat 280Bit (=35Byte) für Prüfsumme MAC:

```
3ae2f8f268 d024c47d52 8465f76460 865e2362ad 28f609cb91 d1206c5f69 4a229c85de CMAC
Schlüssel 1a6220a89cfa76f327bda8e4cb4c9ec19013556e2753eb1f23f7744b603b0e5
```

E.5.4. Header

```
IV (Zeitstempel) 07.08.2025 10:30:45 d5fa1f01
Schlüsselindex Schlüssel 2 01
Prüfsumme CRC-8 über d5fa1f0101 e8 Prüf-summe MAC (32Bit) 81256a9a
ergibt folgenden Header (80Bit): d5fa1 f0101 e8812 56a9a
```

Payload gesamte Geheimnachricht, Header und Geheimtext (360Bit):

```
d5fa1 f0101 e8812 56a9a 3ae2f 8f268 d024c 47d52 8465f 76460 865e2 362ad 28f60 9cb91 d1206 c5f69
4a229 c85de
```

E.5.5. Geheimnachricht NUMERIK

NUMERIK Geheimnachricht (360Bit) = 90 NUMERIK Zeichen:

```
U*[58[080871184*6595 574[1[461U04232]U*4126*[]626016*74 645U41[6093-
98U84063*[692544931*U7
```

POCSAG Telegramm (Codeworte Geheimnachricht):

```
7A89C197 7A89C197 7A89C197 7A89C197 0788E483 EAFD0A21 F8080B34 F44092B5 AB54D086
9D717B10 C7934491 E8126149 A3EA95EF C232FA4B BB2306F2 C32F1231 9B156AA3 947B0061
CE5C8FCA E8903378 E2FB4A27 A5114925 E42EF68D 7A89C197
7A89C197 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197 7A89C197
```

E.6. Optionen

E.6.1. Base64-Codierung der Nachricht und Alphanummerische Übertragung

Um dieses Verschlüsselungsverfahren auch in Netzsystemen (Leitstelle, Zubringerstrecke, DAG) anwenden zu können, die das NUMERIK Format nicht unterstützen, kann alternativ die gesamte Geheimnachricht durch Base64 Codierung als alphanumerische 7 Bit ASCII Nachricht erzeugt werden. Durch Anwendung der Option BASE64 verlängert sich jede Geheimnachricht um ca. 17%. Geheimnachricht_Base64 = BASE64 (Header || Geheimtext)

E.6.2. Geheimnachricht Option BASE64

Um die Geheimnachricht nicht im NUMERIK Format zu beschreiben, wird der Payload der Geheimnachricht in 6Bit-Worte zerlegt, die dann als BASE64 Zeichen dargestellt werden. Das ggf. erforderliche Padding (Auffüllen mit NULL-Bits) ist zu beachten.

Payload Header und Geheimtext:

d5fa1 f0101 e8812 56a9a 3ae2f 8f268 d024c 47d52 8465f 76460 865e2 362ad 28f60 9cb91 d1206 c5f69
4a229 c85de

Payload Header und Geheimtext (6-Bit Worte):

35 1f 28 1f 00 10 07 28 20 12 15 2a 26 23 2b 22 3e 0f 09 28 34 02 13 04 1f 15 0a 04 19 1f 1d 24 18
08 19 1e 08 36 0a 2d 0a 0f 18 09 32 39 07 11 08 06 31 1f 1a 14 28 22 27 08 17 1e

Payload Header und Geheimtext (BASE64 Zeichen, binär):

31 66 6f 66 41 51 48 6f 67 53 56 71 6d 6a 72 69 2b 50 4a 6f 30 43 54 45 66 56 4b 45 5a 66 64 6b
59 49 5a 65 49 32 4b 74 4b 50 59 4a 79 35 48 52 49 47 78 66 61 55 6f 69 6e 49 58 65

BASE64 Geheimnachricht:

1fofAQHogSVqmjri+PJo0CTEfVKEZfdkYIZeI2KtKPYJy5HRIGxfaUoinIXe

POCSAG Codeworte Geheimnachricht BASE64:

7A89C197 7A89C197 7A89C197 7A89C197 0788E483 C667EC36 D9C18F61 A27DF3B9 BCAD64AB
BDB568E2 9E5EA630 8AA7DB36 86C25348 E8B36B36 BA68A90F D664F119 DCD92B8B B69C9023
CDA4BE05 E90B3154 D4CFA90C C252CDE3 9E23D8B8 9C3ABFD9 EE5BB9BE 92369EA6 7A89C197
7A89C197 7A89C197 7A89C197 7A89C197 7A89C197

E.7. Prüfung der Endgeräte auf Einhaltung des Verfahrens

Nachfolgende Prüfungen müssen aus Interoperabilitätsgründen geprüft und dokumentiert werden:

E.7.1. Setzen der korrekten Zeit

Es wird mit dem Zeitzetzbefehl getestet, dass die Zeit im Melder gesetzt werden kann. Die Zeit muss vor- und zurückgesetzt werden können.

E.7.2. Entschlüsselung von Meldungen

Es wird getestet, dass ein beliebiger RIC und beliebige Schlüssel programmiert werden. Eine verschlüsselte Nachricht mit der Meldungslänge von 240 Zeichen muss im korrekten Zeichensatz entschlüsselt und im Display dargestellt werden.

E.7.3. Textlänge

Die vom Hersteller angegebene maximale Textlänge einer Geheimnachricht ist zu testen.

E.7.4. Dynamische Schlüsselwahl

Es wird eine Nachricht gesendet mit verschiedenen Schlüsselindizes. Dabei müssen alle möglichen Indizes den korrekten Schlüssel anwenden und die Nachricht richtig entschlüsseln.

E.7.5. Zeitauthentifizierung

Es wird getestet, dass eine Geheimnachricht bei falscher Zeit bzw. nicht gestellter DME Uhr

- verworfen wird, bzw.
- dem Nutzer der Zeitauthentifizierungs-Fehler mitgeteilt und Klartext trotzdem angezeigt wird
- oder ein Alarm ohne Text erfolgt

E.7.6. Meldungsintegrität

Es wird getestet, ob eine Geheimnachricht bei falscher Prüfsumme MAC

- verworfen wird, bzw.
- dem Nutzer der Meldungsintegritäts-Fehler mitgeteilt und Klartext trotzdem angezeigt wird
- oder ein Alarm ohne Text erfolgt

Die vom Hersteller angegebene maximale Textlänge einer Geheimnachricht wird getestet.

E.7.7. Erkennung von unverschlüsselten Nachrichten

Es wird getestet, ob eine Klartextnachricht auf einem zu verschlüsselndem RIC

- verworfen wird
- ein Alarm ohne Text erfolgt
- ein Hinweis auf „unverschlüsselt“ mitgeteilt und Klartext trotzdem angezeigt wird.

E.7.8. Steuerkommandos

Es wird getestet, ob folgende Steuerkommandos auf einem Fernwartungs-RIC ausgeführt werden:

- #ZEIT=HHmddMMyy#ZEIT=HHmddMMyy DME Uhr stellen
- SPERR=DME_PASSWORT DME sperren mit 16-stelligem Passwort
- ENTSPERR=DME_PASSWORT DME freigeben mit 16-stellige