



Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben

LEITFADEN

ZUR NUTZUNG VON TETRA-FREMDNETZEN

Version 1.1

**Bundesanstalt
für den Digitalfunk der Behörden und
Organisationen mit Sicherheitsaufgaben (BDBOS)**

Fehrbelliner Platz 3, 10707 Berlin
Postanschrift: 11014 Berlin

Inhaltsverzeichnis

1	Einleitung.....	4
2	Ziel.....	4
3	Abgrenzung.....	5
4	Definition Fremdnetz.....	5
5	Nutzung von Fremdnetzen.....	5
5.1	Nutzungsvereinbarung.....	5
5.2	Datenschutz.....	5
5.3	Anforderungen an TETRA-Fremdnetze.....	6
5.3.1	Kapazität und Versorgungsgüte im Objekt.....	6
5.3.2	Verfügbarkeit.....	6
5.3.3	Redundanz im Fremdnetz.....	6
5.4	Art der Fremdnetznutzung.....	7
5.4.1	Dienste und Priorisierungen.....	7
5.4.2	Handlungsempfehlungen.....	8
5.5	Anforderungen an die Sicherheit.....	9
5.5.1	Sicherheit des BOS-Netzes und der BOS-Endgeräte.....	9
5.5.2	Sicherheit des Fremdnetzes.....	11
5.6	Anforderungen der BOS.....	11
5.6.1	Taktisch-betriebliche Anforderungen der BOS.....	11
5.6.2	Zusammenarbeitsgruppen.....	11
5.7	Schnittstellen, Verantwortlichkeiten und Zuständigkeiten.....	12
5.7.1	Parametrierung Endgeräte.....	12
5.7.2	Parametrierung TETRA-Fremdnetz.....	13
6	Anlagen.....	14

6.1	Checkliste.....	14
6.2	Mitgeltende Dokumente	14
7	Abkürzungsverzeichnis.....	15

1 Einleitung

Dieses Dokument dient als Leitfaden zur Nutzung von TETRA-Fremdnetzen durch BOS-Endgeräte. Im Hoheitsgebiet der Bundesrepublik Deutschland werden zahlreiche private Funksysteme im TETRA-Standard auf zivilen Frequenzen für die betriebsinterne Kommunikation oder im Rahmen betrieblicher Prozesse (Datenverkehr) betrieben. Die in diesem Leitfaden beschriebenen Festlegungen beschränken sich auf Fremdnetze auf dem Hoheitsgebiet der Bundesrepublik Deutschland. Die Zuteilung der TETRA-Netzkennung erfolgt durch die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA).

2 Ziel

Die Möglichkeit zur Nutzung einer zusätzlichen funktechnisch vorhandenen Infrastruktur nach TETRA-Standard durch Endgeräte der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) erweitert die Kommunikationsmöglichkeiten der BOS.

Diese TETRA-Funknetze sind insbesondere in den unter 5.4 genannten Anlagen oder Objekten vorhanden. Die Notwendigkeit der Nutzung durch die BOS ergibt sich aufgrund:

- der besonderen Relevanz im Einsatzfall aufgrund anlagenspezifischer Charakteristika (hohes Gefährdungspotential oder Personenaufkommen) oder
- eines erhöhten Kommunikationsbedarfs im Rahmen polizeilicher Bedarfe oder
- der organisatorischen Zuordnung und originären Aufgabenwahrnehmung der Werkfeuerwehren oder
- aufgrund baugenehmigungsrechtlicher Auflagen.

Auf dem Werksgelände oder in den Objekten ist i. d. R. bereits ein eigenständiges Funksystem im TETRA-Standard installiert, welches für die betriebsinterne Kommunikation genutzt wird. Dieses Funksystem wird auf einer zivilen Frequenz mit einem eigenen Netzkenner betrieben und verfügt über die hierfür erforderliche Frequenzzuteilung der Bundesnetzagentur.

In Abgrenzung hierzu stellt die Errichtung einer Objektversorgungsanlage zur Erfüllung baugenehmigungsrechtlicher Auflagen einen Sonderfall dar.

3 Abgrenzung

Die Nutzung eines fremden Netzes im Ausland wird in diesem Leitfaden nicht betrachtet.

4 Definition Fremdnetz

Die innerhalb der BDBOS und im AK Betrieb abgestimmte Definition lautet:

"Fremdnetz im Sinne des Digitalfunks ist jedes direkt oder indirekt angebundene IT-Netz, durch dessen Anbindung der sichere Betrieb und die sichere Nutzung des Digitalfunks beeinträchtigt werden kann und dessen Konfigurations-, Daten- und Sicherheitsmanagement sich nicht in der direkten Betriebs- und Überwachungshoheit der BDBOS und/oder der BOS befindet."

5 Nutzung von Fremdnetzen

5.1 Nutzungsvereinbarung

Die Rahmenbedingungen der konkreten Nutzung eines TETRA-Fremdnetzes im Sinne dieses Leitfadens werden auf Basis einer einzelvertraglichen Nutzungsvereinbarung zwischen der Betreiberin des Fremdnetzes und dem Nutzer (BOS) vereinbart. Wer für das jeweilige Bundesland als Vertragspartner in die Vereinbarung eintritt, ergibt sich aus landesspezifischen Regelungen. Eine Muster-Nutzungsvereinbarung ist als Anlage beigefügt.

5.2 Datenschutz

Seit dem 25. Mai 2018 ist die Verordnung (EU) 2016/679 (Datenschutz-Grundverordnung – DSGVO) in Kraft gesetzt und anzuwenden, gleiches gilt auch für das neue Bundesdatenschutzgesetz (BDSG).

Zwischen der Betreiberin des zivilen TETRA-Funknetzes und den Nutzern (BOS) ist eine Nutzungsvereinbarung zu schließen (siehe 5.1), in der auch die datenschutzrechtlichen Belange berücksichtigt sind.

5.3 Anforderungen an TETRA-Fremdnetze

5.3.1 Kapazität und Versorgungsgüte im Objekt

Die Kapazität des TETRA-Fremdnetzes deckt hauptsächlich den internen Kommunikationsbedarf der Betreiberin ab und ist entsprechend dimensioniert. Insofern ist vorab in jedem Fall zu prüfen, ob und inwieweit im TETRA-Fremdnetz notwendige Reserven für die zusätzlichen BOS-Teilnehmer und deren Kommunikationsbedarf vorhanden ist. Im Einzelfall können zusätzliche Lizenzen oder technische Systemerweiterungen erforderlich werden.

Darüber hinaus kann grundsätzlich nicht davon ausgegangen werden, dass bei einem Bestandsobjekt alle Bereiche des Objektes, die für BOS-Belange notwendige Versorgung aufweisen. Teilbereiche des Objektes, die aus Sicht der BOS zwingend eine Funkversorgung benötigen, sind im Einzelfall mit der Betreiberin abzustimmen¹.

5.3.2 Verfügbarkeit

Der Betrieb des TETRA-Fremdnetzes auf der Basis der internen betrieblichen Anforderungen und der zusätzliche Bedarf der BOS sind mit der Betreiberin abzustimmen. Dies gilt insbesondere für turnusmäßige Intervalle, in denen das TETRA-Funknetz nicht zur Verfügung steht. Die geplanten Ausfallzeiten (Servicelevel) sind in der Nutzungsvereinbarung zu benennen. Für den Fall eines ungeplanten Ausfalls sind geeignete Kommunikationsbeziehungen festzulegen, über die eine gegenseitige Information gewährleistet werden kann.

5.3.3 Redundanz im Fremdnetz

Es ist mit der Betreiberin des Fremdnetzes zu klären, ob und welche vorbeugenden Maßnahmen bei einem Ausfall einzelner Teile oder des gesamten Netzes getroffen wurden (Redundanz). Sofern keine Redundanzen vorgehalten werden, ist dies bei den Einsatzvorbereitungen der BOS zu berücksichtigen. Die Einsatzkräfte sind regelmäßig und in geeigneter Weise nach landesspezifischen Standards zu unterweisen und auf die Besonderheiten ist hinzuweisen.

¹ Die fachliche Einbindung der Brandschutzdienststellen wird empfohlen.

5.4 Art der Fremdnetznutzung

Auf der Grundlage einer bundesweiten Abfrage zur Nutzung von TETRA-Fremdnetzen ist zwischen der Dienstenutzung des BOS DF in TETRA-Fremdnetzen und der Dienstenutzung des DF in "fremden" IP-Datennetzen zu unterscheiden.

Beschränkt sich die Dienstenutzung im DF BOS in TETRA-Fremdnetzen bisher auf die bidirektionale Sprachkommunikation, ist die Dienstenutzung im DF in „fremden“ IP-Datennetzen wesentlich umfassender. Die Dienstenutzung im DF in diesen Netzen dient in der Regel der Leitstellenkommunikation oder dem Bereitstellen von Informationen zur Lageaufbereitung. Bei diesen „fremden“ IP-Datennetzen handelt es sich grundsätzlich um Landesnetze oder um Netze, die im Auftrag des Landes oder der BOS betrieben werden.

Bei den TETRA-Fremdnetzen können folgende Netzanwendungen differenziert werden:

- Funknetz des öffentlichen Personennahverkehrs (ÖPNV),
- Funknetz eines Industrieunternehmens,
- Funknetz eines Industrieunternehmens mit anerkannter Werkfeuerwehr (BOS) oder Betriebsfeuerwehr,
- Funknetz einer öffentlich-rechtlichen Einrichtung (IT-K-Dienstanbieter),
- mobiles/stationäres Funknetz eines Dienstleisters.

5.4.1 Dienste und Priorisierungen

Zur Einstufung der Dienste bzgl. ihrer taktischen Wichtigkeit für den BOS-Einsatz sind, soweit technisch umsetzbar, folgende Prioritätsstufen maßgebend:

Prio 1	Die Dienstenutzung ist für die taktische Einsatzbewältigung oder aus Gründen der Eigensicherung in TETRA-Fremdnetzen unerlässlich.
Prio 2	Die Dienstenutzung ist für die taktische Einsatzbewältigung in TETRA-Fremdnetzen wünschenswert, aber nicht zwingend erforderlich.
Prio 3	Die Dienstenutzung hat für die taktische Einsatzbewältigung in TETRA-Fremdnetzen grundsätzlich keine Relevanz.

Diese Prioritäten implizieren keine Bevorrechteungen im Fremdnetz!

Folgende Dienste werden für die Dienstenutzung des DF in TETRA-Fremdnetzen aus taktischer Sicht betrachtet und bzgl. ihrer Wichtigkeit für den BOS-Einsatz priorisiert:

Prio 1	Notruf im Digitalfunk, Notrufbegleitdaten (GPS) und Gruppenruf.
Prio 2	Leitstellenruf, Einzelruf, SDS und Verschlüsselung (E2EE).
Prio 3	Durchsageruf, Katastrophenruf, Telefonie, Kurzdatendienst (SDS - Alarmierung, Flash-SDS, taktischer Status) und Datendienste (Multislot Packet Data).

Die Dienste nach Prio 3 haben für die taktische Einsatzbewältigung in TETRA-Fremdnetzen grundsätzlich keine Relevanz und werden somit auf die technisch-betrieblichen Maßnahmen zur Vermeidung dieser Dienstenutzung in TETRA-Fremdnetzen reduziert bzw. stehen im Fremdnetz nicht zur Verfügung.

5.4.2 Handlungsempfehlungen

Nachfolgend genannte Handlungsempfehlungen sind im Fremdnetz zu gewährleisten:

Dienst	Empfehlung
Gruppenruf	Die E2EE ist, sofern technisch möglich, zwingend zu nutzen ² .
Notruf/ Notrufbegleitdaten	Das BOS-Notrufziel im BOS-Digitalfunknetz wird nicht erreicht. Das Notrufziel und die Rahmenbedingungen des Notrufs im Fremdnetz sind mit der Betreiberin des Fremdnetzes zu vereinbaren. Die Notrufbegleitdaten werden ggf. nicht übermittelt, sie sind im Netz der Betreiberin möglicherweise nicht zustellbar. Sofern es das Fremdnetz zulässt, sind die Ziele mit der Betreiberin des Fremdnetzes zu vereinbaren.
SDS	Auf die Nutzung von Kurzdatendiensten ist im Hinblick auf die mögliche Gefährdung durch Schadsoftware grundsätzlich zu verzichten ³ .

² Ob die Ende-zu-Ende Verschlüsselung (E2EE) durch das Fremdnetz unterstützt wird, ist mit der Betreiberin zu klären (siehe Checkliste).

³ Empfehlung der AG Sicherheit vom 16.08.2018.

Dienst	Empfehlung
	Die Sicherheitsrisiken sind im Einzelfall zu bewerten und durch technisch-organisatorische Maßnahmen abzusichern.
Schulung	Schulung der Einsatzkräfte: - Umschalten der Endgeräte auf das Fremdnetz und zurück zum BOS Digitalfunknetz, - Nutzung der E2EE (erstrangig), - Kommunikationsregeln für Netze, welche die E2EE nicht unterstützen (siehe SDS), - Kommunikation unter BOS-Teilnehmern und ggf. Kommunikation mit Teilnehmern aus dem Fremdnetz (ohne E2EE), - Notruf und Notrufbegleitdaten, - Sensibilisierung auf potentielle Sicherheitsrisiken.

Für den Einzelruf gelten die gleichen Vorgaben wie für den Gruppenruf.

5.5 Anforderungen an die Sicherheit

Bezüglich der Nutzung von BOS-Funkgeräten in TETRA-Fremdnetzen ist zu beachten, dass eine potentielle Lösung den sicheren Betrieb des Digitalfunks BOS nicht beeinträchtigen darf. Unter dem sicheren Betrieb ist hierbei insbesondere die anforderungsgerechte Verfügbarkeit der Digitalfunkdienste sowie die Gewährleistung der angemessenen Vertraulichkeit und Integrität der über den Digitalfunk BOS transportierten und ggf. in den Endgeräten vorgehaltenen Informationen zu verstehen. Eine detaillierte Betrachtung der sicherheitsrelevanten Funktionen der TETRA Luftschnittstelle ist der Anlage „Sicherheitsrelevante Funktionen auf der TETRA Luftschnittstelle bei Fremdnetznutzung“ zu entnehmen. Der Umgang mit Sicherheitsvorfällen im Fremdnetz ist in der Nutzungsvereinbarung zu regeln.

5.5.1 Sicherheit des BOS-Netzes und der BOS-Endgeräte

Der Digitalfunk BOS ist ein Kommunikationsmedium für alle BOS in Deutschland, welches auch in Katastrophen- und Krisenzeiten funktionsfähig zur Verfügung stehen muss.

Die von Bund und Ländern betriebene Informationstechnik ist im Rahmen der Regeln des Bundesamtes für die Sicherheit in der Informationstechnik (BSI) zur Informationssicherheit und unter Beachtung der gesetzlichen Bestimmungen zum Datenschutz sowie Geheim- und Sabotageschutz einzusetzen.

Die Erfüllung dieser Anforderungen gewährleistet den Schutz der Informationen zum Digitalfunk BOS als auch von Informationen die über den Digitalfunk BOS übermittelt werden durch Anwendung der:

- BSI-Standards (in der jeweils gültigen Fassung),
- Datenschutzgesetze von Bund und Ländern,
- Sicherheitsüberprüfungsgesetze von Bund und Ländern.

Aufgrund der bestehenden Anforderungen aus dem Geheim- und Sabotageschutz sowie dem Datenschutz wird die Kommunikation im Digitalfunk für alle BOS in Deutschland verschlüsselt betrieben.

Das BOS Digitalfunknetz bietet hierzu verschiedene Sicherheitsfunktionen, die im Wesentlichen aus den folgenden Optionen bestehen:

- Funkschnittstellenverschlüsselung,
- Authentisierung.

Die Funkschnittstellenverschlüsselung (TEA2) ist ein standardisiertes Verfahren nach ETSI, welches einen abschnittweisen Schutz im TETRA Netz vor Abhören bietet. Dieses Verfahren sichert die Funkschnittstelle zwischen Basisstation und Funkgerät ab.

Die Funkschnittstellenverschlüsselung der Sicherheitsklasse 2 kann wahlweise mit oder ohne Authentisierung genutzt werden. Für die Funkschnittstellenverschlüsselung der Klasse 3 ist eine Authentisierung erforderlich. Der für eine Authentisierung erforderliche Authentisierungsschlüssel und die erforderlichen Algorithmen sind auf der BOS Sicherheitskarte, im Endgerät und in der Systemtechnik implementiert. Im Digitalfunk BOS wird im TMO-Betrieb die Sicherheitsklasse 3 verwendet.

Als zusätzlicher Schutz wird im Digitalfunk BOS neben der Funkschnittstellenverschlüsselung auch eine Ende-zu-Ende Verschlüsselung nach Spezifikationen des BSI eingesetzt. Diese

Ende-zu-Ende Verschlüsselung ist auf der gesamten Kommunikationsstrecke zwischen den beteiligten Endgeräten wirksam und auch an den Leitstellenschnittstellen verfügbar. Zur Umsetzung dieser Verschlüsselungsmethode verfügt jeder Funkteilnehmer über eine BSI-Sicherheitskarte und jede Leitstelle über eine Mehrkanalkryptokomponente (MKK).

5.5.2 Sicherheit des Fremdnetzes

Die Sicherheit des Fremdnetzes unterliegt den individuellen Anforderungen des Bedarfsträgers, allgemeingültige Anforderungen sind nicht eingrenzbar.

Allgemein ist davon auszugehen, dass zumindest

- BSI Grundschutz, mindestens Umsetzung der Basisanforderung oder
- Zertifizierung nach ISO 27001 oder
- vergleichbare Schutzmaßnahmen

angewendet werden sollten.

5.6 Anforderungen der BOS

Die Anforderungen der BOS leiten sich aus deren einsatztaktischem Bedarf ab, die polizeilichen und die nichtpolizeilichen Anforderungen sind nicht identisch. Der objektspezifische Bedarf ist individuell zu bestimmen und zwischen Betreiber und den BOS individuell abzustimmen.

5.6.1 Taktisch-betriebliche Anforderungen der BOS

Die taktisch-betrieblichen Anforderungen der BOS leiten sich aus den zu erwartenden Szenarien im jeweiligen Objekt ab. Für Standardeinsätze reichen i. d. R. eine Kommunikationsgruppe pro BOS, größere Ereignisse wie bspw. Brände erfordern ein größeres Rufgruppenkontingent. Der Bedarf ist zwischen den BOS und der Betreiberin abzustimmen und in der Nutzungsvereinbarung verbindlich zu vereinbaren. Die zu nutzenden Dienste sind in diesem Leitfaden unter 5.4.1 aufgeführt.

5.6.2 Zusammenarbeitsgruppen

Die Parametrierung gemeinsamer Kommunikationsgruppen (Zusammenarbeitsgruppen) für Endgeräte der BOS und Endgeräte des TETRA-Fremdnetzes unterliegt engen Vorgaben. Es ist

davon auszugehen, dass die Endgeräte des TETRA-Fremdnetzes die Ende-zu-Ende Verschlüsselung (E2EE) nicht unterstützen. Insofern erfolgt die Nutzung gemeinsamer Kommunikationsgruppen unverschlüsselt bzw. die Ende-zu-Ende Verschlüsselung (E2EE) der BOS-Endgeräte muss für den konkreten Einsatzfall manuell temporär deaktiviert werden. Die Einsatzkräfte sind hierüber in geeigneter Weise zu informieren.

5.7 Schnittstellen, Verantwortlichkeiten und Zuständigkeiten

Das TETRA-Fremdnetz und das BOS-Digitalfunknetz werden physisch nicht miteinander verbunden. Eine Schnittstelle im Sinne dieses Leitfadens meint somit die Vereinbarungen zwischen der Betreiberin des TETRA-Fremdnetzes und den örtlich zuständigen BOS, um die geforderte Funktionalität anzubieten. Die geforderte Funktionalität ist die Möglichkeit zur Kommunikation mit Endgeräten der BOS im jeweiligen TETRA-Fremdnetz. Die hierbei zu beachtenden Punkte sind in der Checkliste Fremdnetze zusammengefasst (siehe 6.1).

Die Abgrenzung der Verantwortlichkeiten ergibt sich aus der Zuständigkeit und den Eigentumsverhältnissen. Das TETRA-Fremdnetz befindet sich im privaten Eigentum eines Unternehmens oder im öffentlich-rechtlichen Eigentum einer Gebietskörperschaft. Das BOS-Digitalfunknetz ist ein bundesweites Netz für alle BOS von Bund und Ländern und wird durch die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) gemeinsam mit den Ländern betrieben.

5.7.1 Parametrierung Endgeräte

Grundsätzlich behalten die Vorgaben aus dem NBHB, Kapitel 8.3.6.3 Parameter der Endgeräte ihre Gültigkeit. Darüber hinaus sind Ergänzungen für den BOS-Nutzerkreis des Fremdnetzes notwendig, bspw.:

- Netzkenner und Bezeichnung des Fremdnetzes,
- Notrufziel im Fremdnetz,
- Notrufdatenziele im Fremdnetz (Notrufstatus und GPS),
- Datenziele (Status und GPS),
- Autorisierte ISSI (z. B. Alarmierung, Nutzung von GPS),
- Gruppen im Fremdnetz,
- Verschlüsselungsalgorithmus,

- Migrationsmethode (temporäre ISSI oder ISSI der BSI-Karte),
- Ende-zu -Ende-Verschlüsselung,
- Frequenzen.

Die Einschaltprozedur und der Wechsel der Endgeräte in das BOS-Netz erfolgen immer verschlüsselt. Die Einschaltprozedur und der Wechsel der Endgeräte in das Fremdnetz kann verschlüsselt oder unverschlüsselt erfolgen⁴.

5.7.2 Parametrierung TETRA-Fremdnetz

Der Netzkenner des TETRA-Funknetzes der Betreiberin und die den BOS hierin zugeordneten Rufgruppen sind in den Endgeräten der BOS zu hinterlegen. Für die BOS werden im Fremdnetz der Betreiberin folgende Konfigurationen vorgenommen:

- Einrichten ISSI-Block,
- Einrichten der Funkteilnehmer der BOS,
- Einrichten [xy] Rufgruppen für BOS,
- Einrichten der Priorisierung von Funkteilnehmern und Rufgruppen der BOS,
- Zuweisung eines Gastzugangs im Fremdnetz.

Die landesindividuellen Bedarfe der BOS innerhalb des TETRA-Fremdnetzes hinsichtlich der notwendigen Parameter sind mit dem jeweiligen Fremdnetzbetreiber abzustimmen.

⁴ Siehe AK Taktik Beschluss 07/003, Schreiben der BDBOS xx-500 303-6#56 vom 18.01.2016

6 Anlagen

6.1 Checkliste

Die Checkliste ergänzt den Leitfaden und dient als Begleitdokument bei der Planung und Umsetzung der Nutzung von Fremdnetzen.

6.2 Mitgeltende Dokumente

	Dokument	Version/Datum
1.	Muster-Nutzungsvereinbarung Fremdnetze für Sende- und Empfangsanlagen im TETRA-Standard	Version 1.1 vom 24.02.2021
2.	Leitfaden zur Planung und Realisierung von Objektversorgungen (L-OV)	Version 3.3 vom 20.05.2019
3.	Checkliste Fremdnetze	Version 1.1 vom 24.02.2021
4.	Benutzerdefinierter Grundsatzbaustein Digitalfunkendgeräte, SYS.3.b5 Digitalfunkendgeräte	siehe BDBOS-Internetseite (CUG)
5.	Umsetzungshinweise zum benutzerdefinierten Baustein SYS.3.b5 Digitalfunkendgeräte	siehe BDBOS-Internetseite (CUG)

7 Abkürzungsverzeichnis

BNetzA	- Bundesnetzagentur
BOS	- Behörden und Organisationen mit Sicherheitsaufgaben
BOStrab	- Verordnung über den und Betrieb der Straßenbahnen (Straßenbahn-Bau- und Betriebsordnung - BOStrab)
E2EE	- Ende-zu-Ende-Verschlüsselung
MBO	- Musterbauordnung
MKK	- Mehrkanalkryptokomponente
NBHB	- Nutzungs- und Betriebshandbuch
RABT	- Richtlinien für die Ausstattung und den Betrieb von Straßentunneln

8 Historie

Datum	Version	Autor	Kommentar	Status
19.11.2019	1.0	K 2	Version zur Freigabe im AK Betrieb	Freigabe AK Betrieb am 23.02.2021
24.02.2021	1.1	NBHB-Re- daktion	Redaktionelle Anpassungen im Dokument sowie an der „Checkliste Fremdnetze“ und an der „Muster-Nutzungsvereinbarung Fremdnetze für Sende- und Empfangsanlagen im TETRA-Standard“	Freigabe K 2