

DIN 43863-4

ICS 35.240.99; 91.140.50

Einsprüche bis 2006-12-31

Entwurf**Zählerdatenkommunikation –
IP-Telemetrie**Meter data communication –
IP-TelemetryCommunication des données de compteurs –
Télémétrie IP**Anwendungswarnvermerk**

Dieser Norm-Entwurf wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfes besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise als Datei per E-Mail an dke@din.de in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (Hausanschrift: Stresemannallee 15, 60596 Frankfurt am Main).

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevante Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen.

Gesamtumfang 32 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Inhalt

	Seite
Vorwort	4
1 Einleitung.....	4
2 Anwendungsbereich.....	4
3 Referenzierte Normen und Dokumente	5
4 Begriffe, Aufgaben, Funktionsanforderungen	5
5 Einteilung und Komponenten	7
6 Steuerungsprotokoll (IPT-C)	7
6.1 Aufgaben	7
6.2 Spezielle Nachrichten des Steuerungsprotokolls.....	7
7 Transportprotokoll (IPT-T).....	7
7.1 Aufgaben	7
7.2 Anforderungen an den Transportkanal	7
7.3 Zustandsautomat.....	8
7.3.1 Anmeldung	9
7.3.2 Link-Betrieb	9
7.3.3 Push-Betrieb.....	9
7.4 Verschlüsselung / Verschleierung.....	10
7.4.1 Kein Schutz	10
7.4.2 Verschleierung	10
7.5 Spezielle Nachrichten des Transportprotokolls.....	11
8 Applikation (IPT-A)	11
8.1 Aufgaben	11
8.2 Spezielle Nachrichten der Applikation.....	11
9 Kodierung	11
10 Kommandos	12
10.1 Aufgaben	12
10.2 Struktur.....	12
10.3 Kommandogruppe genereller Kommandos	14
10.3.1 Unknown-Command-Response	14
10.4 Kommandogruppe zu IPT-C	15
10.4.1 Public-Login-Request.....	15
10.4.2 Public-Login-Response	15
10.4.3 Scrambled-Login-Request	16
10.4.4 Scrambled-Login-Response.....	17
10.4.5 Logout-Request.....	17
10.4.6 Logout-Response	17
10.4.7 Maintenance-Request	18

	Seite
10.4.8 Maintenance-Response	18
10.5 Kommandogruppe zu IPT-T	19
10.5.1 Push-Channel-Open-Request	19
10.5.2 Push-Channel-Open-Response	19
10.5.3 Push-Channel-Close-Request	19
10.5.4 Push-Channel-Close-Response	20
10.5.5 Push-Data-Transfer-Request	20
10.5.6 Push-Data-Transfer-Response	21
10.5.7 Connection-Open-Request	21
10.5.8 Connection-Open-Response	22
10.5.9 Connection-Close-Request	22
10.5.10 Connection-Close-Response	22
10.6 Kommandogruppe zu IPT-A	23
10.6.1 Network-Status-Request	23
10.6.2 Network-Status-Response	23
10.6.3 Protocol-Version-Request	24
10.6.4 Protocol-Version-Response	24
10.6.5 Device-Firmware-Request	24
10.6.6 Device-Firmware-Response	25
10.6.7 Device-Identifier-Request	25
10.6.8 Device-Identifier-Response	25
10.6.9 IP-Statistic-Request	25
10.6.10 IP-Statistic-Response	26
10.6.11 Push-Data-Echo-Request	26
10.6.12 Push-Data-Echo-Response	26
10.6.13 Traceroute-Request	27
10.6.14 Traceroute-Response	28
10.6.15 Device-Authentication-Request	28
10.6.16 Device-Authentication-Response	28
10.6.17 Device-Time-Request	28
10.6.18 Device-Time-Response	29
10.6.19 Push-Target-Namelist-Request	29
10.6.20 Push-Target-Namelist-Response	29
11 Watchdog	30
11.1 Aufgaben	30
11.2 Struktur	30
11.2.1 Watchdog Request	30
11.2.2 Watchdog Response	30
Anhang A	31

Vorwort

Für diesen Norm-Entwurf ist das nationale Arbeitsgremium K 461 „Elektrizitätszähler“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE (<http://www.dke.de>) zuständig.

1 Einleitung

Die zunehmende Bedeutung und die gute Verfügbarkeit der neuen, auf dem Internet Protokoll (IP) basierenden Kommunikationsnetze, (Internet, Intranet, etc.) wecken den Bedarf, diese auch für die Belange der klassischen Zählerdatenkommunikation zu nutzen. Eine wesentliche Anforderung besteht darin, von konkreten Anwendungsprotokollen unabhängig zu sein und damit die Verwendung etablierter sowie künftiger Protokolle und Dienste gleichermaßen zu erlauben.

Hierzu wird ein standardisierter und allgemeingültiger Mechanismus benötigt, der dies gewährleistet.

Um diesen allgemeinen Ansatz zu unterstreichen verwendet die vorliegende Spezifikation den Titel „IP-Telemetrie“ und verzichtet bewusst auf die Bindung an bestimmte Kommunikationsprotokolle und Applikationen.

2 Anwendungsbereich

Die Spezifikation zur IP-Telemetrie hat ihren Ursprung in Produkten zur Zählwertbeschaffung für die Messung elektrischer Energieverbrauche; sie lässt sich auch als generische Lösung für viele vergleichbare Anwendungsfälle in der Automatisierungstechnik einsetzen und ist damit allgemein im Bereich der Maschine-zu-Maschine, M2M, Schnittstellen nutzbar.

Die Spezifikation zur IP-Telemetrie beschreibt das Protokoll zur Lösung dieser Aufgabe unter Verwendung möglichst abstrakter Begriffe, so dass einerseits Hersteller ihre Produkte zur Erfüllung dieser Spezifikation möglichst frei gestalten können und andererseits deren Einordnung in das umgebende Normenwerk erleichtert wird.

Für den konkreten Transport von Nachrichten setzt die Spezifikation IP-Telemetrie gesicherte und mit Mechanismen zur Fehlererkennung ausgestattete, verbindungsorientierte Transportkanäle voraus. Als Beispiel für einen derart vorliegenden Anwendungsfall kann das Transmission Control Protocol (TCP) angesehen werden. Ergänzend sei explizit festgestellt, dass IP-Telemetrie auch jede andere im Grundverhalten mit gleicher Qualität ausgestattete Verbindung als Transportmedium nutzen kann.

Der Einsatz von IP-Telemetrie über ungesicherte und / oder verbindungslose Kommunikationsstrecken ist nicht vorgesehen.

Damit kann das Einsatzumfeld von IP-Telemetrie wie folgt skizziert werden:

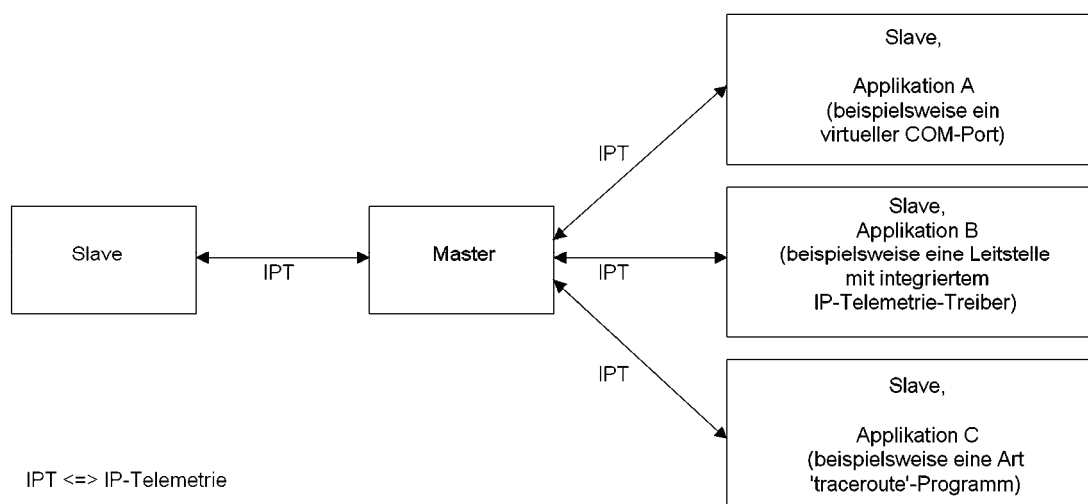


Bild 1 – Einsatzumfeld zu IP-Telemetrie

3 Referenzierte Normen und Dokumente

Tabelle 1 – Liste der verwendeten Normen und Dokumente

Kurzbezeichnung	Stand	Titel / Hinweis
ISO/IEC 8859-15	1999-03	Informationstechnik – 8-Bit-Einzelbyte-codierte Schriftzeichensätze Teil 15: Lateinisches Alphabet Nr. 9
RFC 2396	1998-08	Uniform Resource Identifies (URI): Generic Syntax Network Working Group Updates: 1808, 1738 Category: Standards Track http://www.ietf.org/rfc/rfc2396.txt

4 Begriffe, Aufgaben, Funktionsanforderungen

4.1

Applikation

unter Applikation werden sowohl Anwendungsfälle subsumiert, die die Spezifikation IP-Telemetrie zum Transport serieller Datenströme unter Einsatz bekannter Protokolle nutzen, als auch Einsatzgebiete erfasst, die die speziellen Mechanismen der Spezifikation IP-Telemetrie zum direkten, an Datenblöcken orientierten, Versand verwenden

4.2

Device

der Begriff Device wird in diesem Dokument aus funktionaler Sicht betrachtet. Je nach konkreter Aktion kann der Begriff damit sowohl den Slave wie auch den Master benennen

4.3

direkter Kommunikationspartner

als direkter Kommunikationspartner soll der jeweilige Gegenüber des Master oder Slave benannt werden.

Zwei direkte Kommunikationspartner bilden damit eine Punkt-zu-Punkt-Verbindung. Sie sind jeweils die beiden Endstellen dieser Verbindung

4.4

Internet

als Internet sei „das Internet“ im Sinne des auf dem Internet Protokoll basierenden, weltweiten Rechnerverbunds bezeichnet.

Soweit nicht anders ausgeführt, betreffen Bezüge auf das Internet immer auch lokale Rechnerverbünde, die gleichermaßen das Internet Protokoll anwenden und im allgemeinen Sinne daher als „ein Internet“ bezeichnet werden müssen

4.5

Link-Betrieb

„Link-Betrieb“ bezeichnet eine Betriebsart, bei der zwischen den beiden direkten Kommunikationspartner eine bidirektionale Verbindung erstellt wird, über die beide direkte Kommunikationspartner, quasi wie über eine Standleitung, im Fullduplex-Modus Bytes senden können.

Der Link-Betrieb wird mit dem Anmeldeprozess durch den Slave am Master eingerichtet und hat für die Dauer dieser Beziehung bestand

4.6

M2M

mit „Machine to Machine“, kurz M2M, sollen technische Kommunikationsprozesse zwischen Maschinen bezeichnet werden, die automatisiert über beliebige Kommunikationsnetze ablaufen können

4.7

Master

zum Einsatz dieser Spezifikation wird eine als zentrale Anlaufstelle fungierende Komponente benötigt, die mit Master bezeichnet werden soll.

Der (oder die) Slaves stellen mit der Aufnahme ihres Betriebszustands eine Verbindung über das Transportprotokoll zum Master her. Der dazu benötigte Verbindungsaufbau verwendet das Steuerungsprotokoll

4.8

Transportkanal

diese Spezifikation ordnet dem Begriff Transportkanal eine bidirektionale, gesicherte und mit Funktionen zur Fehlererkennung ausgestattete verbindungsorientierte Kommunikationsstrecke¹⁾ zu.

Der Transportkanal²⁾ bietet aus Sicht der IP-Telemetrie keinerlei Strukturen für die von IP-Telemetrie durch ihn zu übertragenden Daten an. Er bietet quasi die Funktion eines „Rohrs“ („Pipe“) an, durch das von den jeweiligen direkten Kommunikationspartnern einzelne Bytes übertragen werden.

Zur Erkennung von Störungen durch „abgerissene“ Transportkanäle werden mit IP-Telemetrie entsprechende Timeouts und damit Rahmenanforderungen an die für IP-Telemetrie nutzbaren Transportkanäle definiert

4.9

Transportprotokoll

Der Begriff Transportprotokoll wird für den Teil der Spezifikation verwendet, der die Schnittstelle zwischen der Anwendungsseite (der „Applikation“) und dem jeweils darunter verwendeten Kommunikationsnetz beschreibt.

Das Transportprotokoll spezifiziert den Mechanismus zum transparenten, seriellen Datentransport über das jeweils darunter verwendete Kommunikationsnetz

4.10

Push-Betrieb

„Push-Betrieb“ bezeichnet eine Betriebsart, bei der einer der beiden direkten Kommunikationspartner einen singulären Datenblock an sein Gegenüber sendet. Es handelt sich dabei um eine unidirektionale Aktion.

Der Push-Betrieb ist damit über die zum Zeitpunkt der Versendung bekannte Größe des Datenblocks durch eindeutige Start- wie Ende-Bedingungen gekennzeichnet

4.11

Slave

die Endgeräte, die mittels IP-Telemetrie eine Verbindung zu einer Applikation benötigen, werden als Slave bezeichnet.

Sie stellen mit Aufnahme ihrer Betriebsbereitschaft zunächst eine Verbindung zum Master her, wobei es danach die Aufgabe des Master ist, die seitens der Endgeräte angebotene Verbindung zu einer konkreten Applikation weiterzureichen

4.12

Steuerungsprotokoll

der Begriff Steuerungsprotokoll wird für den Teil der Spezifikation verwendet, der die Mechanismen zum Auf- und Abbau von Transportkanälen sowie die Prozesse zu Anmeldung und zum Umgang mit Störungen beschreibt

¹⁾ Applikationshinweis:

Für den Einsatz dieser Norm in Verbindung mit Transportkanälen über öffentliche Netze (beispielsweise das Internet), wird zum Schutz vor Manipulation und Gewährleistung der Privatsphäre empfohlen, gesicherte Transportkanäle (VPN-Tunnel oder vergleichbar) zu verwenden.

²⁾ Applikationshinweis:

Bei Einsatz von paketorientierten Transportkanälen sollte die Implementierung im Rahmen der jeweils konkret definierten Latenzzeit Pakete optimaler Größe bilden.

5 Einteilung und Komponenten

Die Spezifikation IP-Telemetrie ist in die Bereiche Applikation, Steuerungsprotokoll und Transportprotokoll einzuteilen.

Die Kodierung der definierten Nachrichtenstruktur erfolgt gemäß Abschnitt 9.

Zum Einsatz der Spezifikation IP-Telemetrie werden mindestens ein Master und ein Slave benötigt. Hierbei wird bewusst auf die Verwendung der Begriffe Client und Server verzichtet, da Client und Server stets aus dem Blickwinkel der Applikation definiert werden müssen, das Werkzeug IP-Telemetrie aber hingegen diese Blickrichtung offen lassen soll. Letztlich können sowohl der Master als auch der Slave aus der Perspektive der Applikation gesehen die Funktionen Client oder Server wahrnehmen.

6 Steuerungsprotokoll (IPT-C)

6.1 Aufgaben

Das Steuerungsprotokoll definiert die zum Betrieb des Werkzeugs IP-Telemetrie benötigten Prozesse und deren Umsetzung durch das Transportprotokoll. Alle durch das Steuerungsprotokoll bedienten Aufgaben werden über spezielle Nachrichten, siehe 6.2, eingeleitet.

Konkret werden folgende Aufgaben spezifiziert:

- An- / Abmeldung von Slaves an den Master.
- Aktivierung / Deaktivierung des Link-Betriebs.
- Verpackung von Datenblöcken zum Versand an den direkten Kommunikationspartner im Sinne des Push-Betriebs.

6.2 Spezielle Nachrichten des Steuerungsprotokolls

Siehe 10.4.

7 Transportprotokoll (IPT-T)

7.1 Aufgaben

Das Transportprotokoll legt die Struktur der Nachrichten fest.

Um die beiden Betriebsarten „Push-Betrieb“ und „Link-Betrieb“ sowie die betriebsbedingt benötigten Elemente eindeutig über einen vom Prinzip her zunächst unstrukturierten Verbindungsweg, den Transportkanal, transportieren zu können, definiert das Transportprotokoll einen bedarfsgerechten Rahmen.

Für die Erkennung von Störungen durch „abgerissene“ Transportkanäle werden Timeouts (siehe Fußnote 3) festgelegt. Damit diese Timeouts im ordnungsgemäßen Betriebsfall nicht greifen, legt das Transportprotokoll bestimmte Rahmenbedingungen für die aus Sicht von IP-Telemetrie nutzbaren Transportkanäle fest.

Nachrichten werden grundsätzlich ohne zusätzliche Datensicherungselemente transportiert, da die Einsatzszenarien des Werkzeugs IP-Telemetrie stets gesicherte und mit Fehlererkennungsfunktionen ausgestattet unterlagerte Transportwege vorsehen.

Zum Schutz der zu übertragenden Daten vor unberechtigttem Abhören bietet das Transportprotokoll verschiedene Sicherungsstufen.

7.2 Anforderungen an den Transportkanal

Die für IP-Telemetrie nutzbaren Transportkanäle müssen folgenden Randbedingungen zur Datenübertragung zwischen den beiden direkten Kommunikationspartnern genügen:

- Bidirektionale Datenübertragung.
- Verbindungsorientierte Datenübertragung.
- Gesicherte Datenübertragung mit Funktionen zur Fehlererkennung und Fehlerbehebung.
- Datenübertragung innerhalb einer eindeutig definierten Latenzzeit, die aus der konkret verwendeten Applikation resultiert und per Parametrierung das jeweils aktuelle Verhalten des IP-Telemetrie-Transportkanals festlegt.³⁾
- Zeitnahe Meldung von nicht zu behebenden Fehlern an die Transportprotokollschicht. Als zeitnah wird eine Reaktionszeit bezeichnet, die aus dem konkret verwendeten Transportkanal resultiert und per Parametrierung in die Applikation IP-Telemetrie übernommen werden muss. Kann der konkret gewählte Transportkanal die Anforderung der zeitnahen Meldung von nicht zu behebenden Fehlern nicht garantieren, so ist die Watchdog-Funktion (siehe Abschnitt 11) mit passend gesetzten Parametern zur Erkennung derartiger Betriebszustände einzusetzen.

7.3 Zustandsautomat

Das Transportprotokoll zur IP-Telemetrie kennt folgende Zustände:

- Nicht angemeldet.
- Link-Betrieb.
- Push-Betrieb.

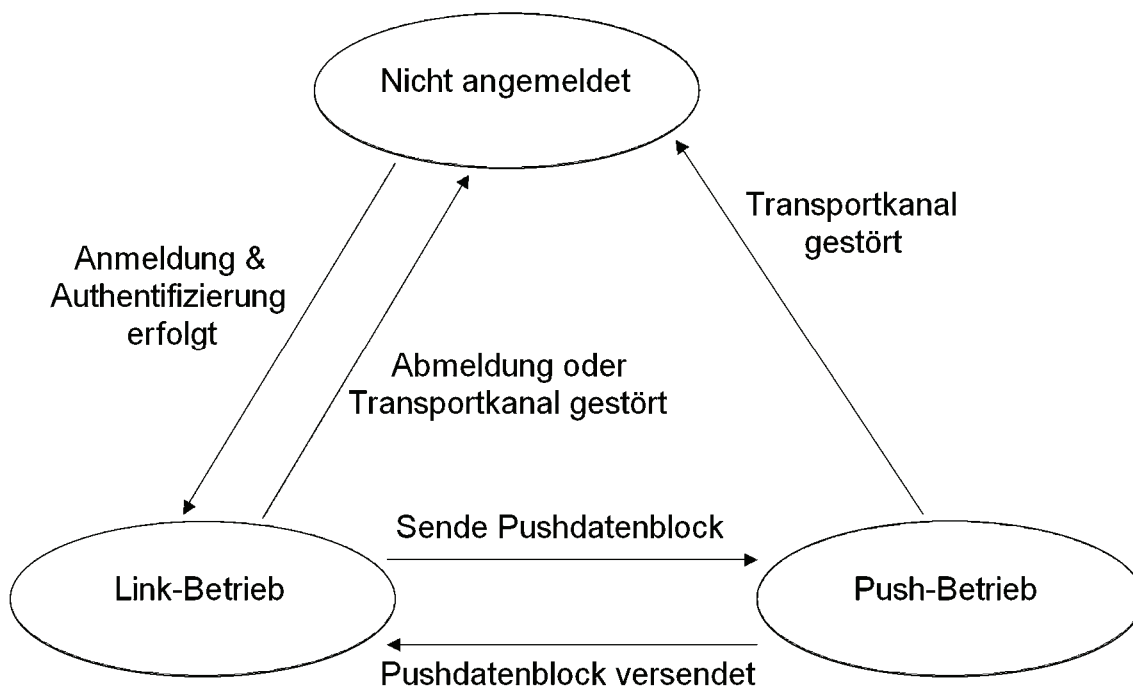


Bild 2 – IPT-Zustandsautomat

Das System startet grundsätzlich im Zustand „nicht angemeldet“ und geht mit der Anmeldung des Slave beim Master in den Zustand „Link-Betrieb“. Im Zustand „nicht angemeldet“ befindet sich das Transportprotokoll im ungeschützten Zustand (siehe 7.4).

Wechselt das System in den Zustand „nicht angemeldet“, so werden alle zu diesem Zeitpunkt noch geöffneten Push-Channels (siehe 10.5.1) automatisch geschlossen.

³⁾ Der zur Überwachung der tatsächlich im Transportkanal auftretenden zeitlichen Latenzen verwendete Grenzwert muss per Parametrierung in Sekundenschritten festgelegt werden können. Der Wert ist im Betrieb durch die Implementation des Transportkanals zu überwachen. Greift das Timeout, ist der Transportkanal zu schließen und eine bestehende Verbindung in den Zustand „nicht angemeldet“ zu wechseln.

Für die quasi gleichzeitige Nutzung von Link- und Push-Betrieb definiert IP-Telemetrie einen per Escape-Sequence einzuleitenden Signalisierungsmechanismus.

Tritt andererseits die Escape-Sequence im Nachrichtenstrom des Link-Betriebs auf, ist diese selber durch Einfügen einer weiteren Escape-Sequence zu maskieren.

7.3.1 Anmeldung

Mit der Anmeldung werden folgende Merkmale festgelegt:

- Authentifizierung des Slave beim Master.
- Auswahl der im Transportprotokoll zu verwendenden Sicherungsstufe (siehe 7.4).
- Festlegung von Betriebsparametern.

7.3.2 Link-Betrieb

7.3.2.1 Aufgaben

Der Link-Betrieb arbeitet Byte für Byte. Jedes zu versendende Byte wird innerhalb der an den Transportkanal geforderten Latenzzeiten an den Empfänger weitergeleitet. Je nach verwendeter Sicherheitsstufe erfolgt die Übertragung in geschützter oder ungeschützter Form (siehe 7.4). Tritt ein Escape-Zeichen im Rohdatenstrom (siehe 7.4, Bild 3) auf, wird dieses auf der Senderseite zweimal gesendet und auf der Empfängerseite wieder entsprechend zurück gewandelt.

Zusätzlich werden vom Link-Betrieb folgende Merkmale geboten:

- Übertragung von Kommandos (siehe Abschnitt 10).
- Übertragung von Watchdog-Ereignissen (siehe Abschnitt 11).

Zur Einleitung von Kommandos oder Watchdog-Ereignissen wird das Escape-Zeichen (siehe Abschnitt 9) verwendet.

7.3.2.2 Struktur der Nachrichten

Zur Strukturierung der Nachrichten im Link-Betrieb verwendet IP-Telemetrie folgenden Rahmen, wobei jede Nachricht, die per Transportprotokoll über einen Transportkanal versendet wird, der nachstehend definierten Struktur folgen muss:

IptLinkMessage ::= *StreamOfUnsigned8*

7.3.3 Push-Betrieb

7.3.3.1 Aufgaben

Der Push-Betrieb erlaubt die Versendung von Datenblöcken an ein sogenanntes Push-Target.

Der Push-Betrieb wird durch ein spezielles Kommando (siehe 10.4) eingeleitet.

7.3.3.2 Struktur der Nachrichten

Zur Strukturierung der Nachrichten im Push-Betrieb verwendet IP-Telemetrie folgenden Rahmen, wobei jede Nachricht, die per Transportprotokoll über einen Transportkanal versendet wird, der nachstehend definierten Struktur folgen muss:

Siehe 10.4.

7.4 Verschlüsselung / Verschleierung

IP-Telemetrie bietet verschiedene Stufen zur Verschlüsselung/Verschleierung der zu übertragenden Datenströme. Die Auswahl des jeweils für einen Transportkanal anzuwendenden Verfahrens erfolgt per Steuerprotokoll auf dem Wege der Anmeldeprozedur.

Derzeit werden folgende Varianten definiert:

- Kein Schutz.
- Verschleierung.

7.4.1 Kein Schutz

In dieser Betriebsart werden die Bytes unverändert durch das Transportprotokoll in den Transportkanal gegeben.

7.4.2 Verschleierung

In dieser Betriebsart wird eine einfache Umkodierung der zu übertragenden Bytes durch das Transportprotokoll erstellt und in den Transportkanal gegeben. Ziel dieser Vorgehensweise ist ein rudimentärer Schutz gegen Ausspähung mit einfachen Mitteln.

Jedes einzelne Byte wird dabei umkodiert, der Grundmechanismus arbeitet wie folgt:

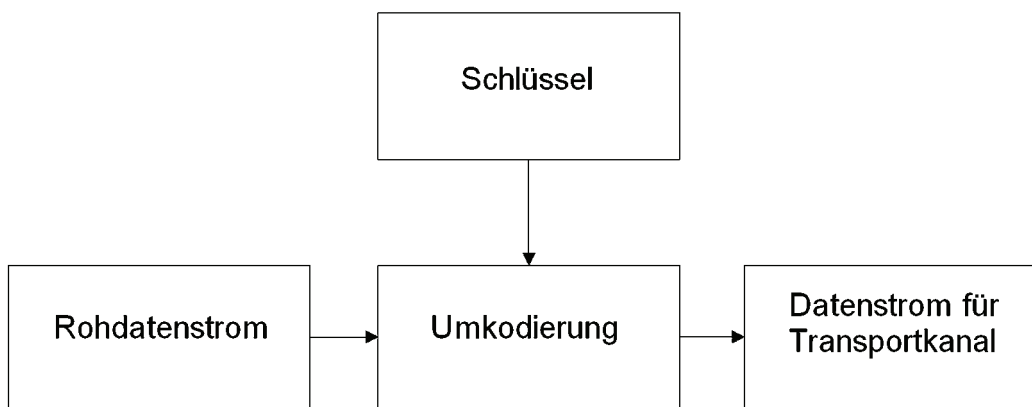


Bild 3 – Grundmechanismus zur Verschleierung

7.4.2.1 Algorithmus zur Verschleierung

Der Algorithmus basiert auf einer einfachen X-OR-Verknüpfung des Rohdatenstroms mit dem Schlüssel.

Je nach Zustand des Protokollautomaten wird entweder ein vordefinierter Schlüssel oder ein per Zufall vom Slave erzeugter Schlüssel verwendet. In beiden Fällen wird die feste Schlüssellänge von 32 Bytes verwendet.

Der Mechanismus arbeitet wie folgt:

- Das erste Byte aus dem Rohdatenstrom wird mit dem ersten Byte des Schlüssels mittels X-OR in das über den Transportkanal zu übertragende Byte umkodiert.
- Analog wird das zweite Byte aus dem Rohdatenstrom mit dem zweiten Byte des Schlüssels umkodiert und transportiert.
- Dieser Ablauf wiederholt sich, bis alle Zeichen aus dem Schlüssel verwendet wurden, danach wird der Prozess mit dem ersten Byte des Schlüssels fortgesetzt und wiederholt sich über alle Bytes des Rohdatenstroms.