Zentralamt für
Mobilfunk
Referat C 2

Anlage 1 zur
FTZ 171 TR 60
Datum 01.08.90

Berechtigungskarte als Prozessorkarte

Inhaltsübersicht

Inhaltsverzeichnis

A Multifunktionale Telekommunikations-Chipkarte

A 1 Einleitung

Der Einsatz einer Multifunktions-Chipkarte bei der Deutschen Bundespost (DBP) soll die Verwendung einer Chipkarte für mehrere Dienste der DBP ermöglichen.

Deshalb sollen diese Spezifikationen allen Entwicklungen von Chipkarten zur Einführung bei der DBP zugrundegelegt werden.

Aufgrund des derzeitigen Marktangebotes (Juli 1987) wird die zunächst zum Einsatz kommende Chipkarte aller Voraussicht nach folgende Struktur haben:

- 8 bit CPU
- 128 Byte RAM
- 2Kbyte EEPROM
- 3Kbyte ROM (maskiert)

Bei der Erstellung der Spezifkationen wurden die zur Zeit geltenden Internationalen Normungsunterlagen berücksichtigt, sowie das nationale DIN-Blockübertragungsprotokoll (im August 1987 von einer Expertengruppe spezifiziert) miteinbezogen.

A 2 Elektrische und physikalische Eigenschaften der Chipkarte

Die Chipkarte muß in den physikalischen und elektrischen Eigenschaften den hierfür spezifizierten internationalen Normen entsprechen. Hierbei ist zu beachten, daß die speziell für Identifikationskarten mit integriertem Chip definierten ISO-Normen sich auf den allgemein für Identifikationskarten gültigen ISO-Normen (z.B. ISO 7810, etc) stützen.

A 2.1 Physikalische Eigenschaften

Die physikalischen Eigenschaften für Chipkarten legt ISO 7816-1 fest.

Die Chipkarte muß dieser Norm mit dem Status "Draft International Standard" (ISO 7816-1 Stand: 29.10.1987) entsprechen. Weitergehende Forderungen werden festgelegt.

ISO 7816-1 gilt für Chipkarten nach Einfügen des Chip-Moduls in die Karte. Sie definiert u.a. folgende physikalische Eigenschaften:

- Beständigkeit gegenüber UV- und Röntgenstrahlen,
- Oberflächenbeschaffenheit der Kontakte,
- mechanische Belastbarkeit der Kontakte und der Karte,
- elektrischer Widerstand der Kontakte,
- elektromagnetische Felder und elektrostatische Aufladung,
- Hitzebeständigkeit.

Die Einhaltung der o.g. Punkte wird nach den im Anhang zur ISO 7816-1 (sowie Arbeitspapier der SC 17/WG 4 für die Teile 1 und 2 von ISO 7816) vorgeschlagenen Meßmethoden geprüft.

A 2.2 Abmessungen und Lage der Kontakte

Es gelten die in ISO 7816-2 (Stand 29.10.87) definierten Abmessungen und Lage der Kontakte (Mittellage) der in Identifikationskarten implantierten Chip-Module.

Neben der Dimensionierung der einzelnen Kontakte ist die Lage der acht genormten Kontakte in Abhängigkeit vom oberen und linken Rand der Karte definiert. Außerdem ist die Nummerierung und die Bezeichnung der Kontakte festgelegt.

Die Chipkarte der Deutschen Bundespost hat die erste Kontaktlage, die in Figur 2 auf Seite 2 dieser Norm definiert ist.

Die Kontakte liegen auf der Vorderseite der Karte. D.h. die Bezugskanten für die Bemessung der Lage der Kontakte sind

C = obere Kante und
A = linke Kante .

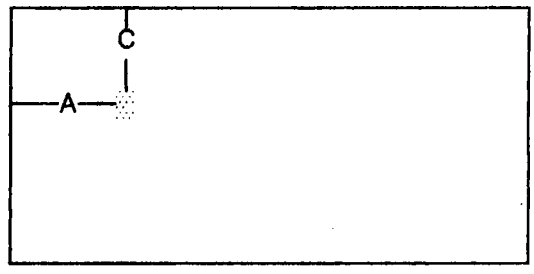


Bild A 2.1: Lage eines Kontaktes ( )

Die Einhaltung der Lage der Kontakte wird nach der im Anhang A zur ISO/DIS 7816-2 (Stand 29.10.87) vorgeschlagenen Meßmethode geprüft.

A 2.3 Elektrische Eigenschaften der Kontakte

Die nachfolgende Beschreibung der elektrischen Signale und elektrischen Eigenschaften der Kontakte wurde auf der Grundlage des ISO DIS 7816-3 (Bearbeitungsstand: 04.03.88) erstellt.

Dieser Teil 3 hat derzeit den Status "Draft International Standard".

Solange die Chipkarte kontaktiert und/oder aktiviert ist, dürfen auf den Kontakten keine Spannungen auftreten, die außerhalb der nachfolgend festgelegten Toleranzen liegen.

A 2.3.1 Elektrische Funktion der Kontakte

Von den in ISO 7816 Teil 2 definierten Kontakten sollen für die Chipkarte fünf Kontakte verwendet werden. Sie sollen folgende Funktionen haben:

I/O : Schaltung, über die serielle Daten vom oder zum in der Karte integrierten Chip transferiert werden,

GND : Null Volt als Referenz-Spannung (0 V),

CLK : Clock- oder Timing-Signal,

RST : Reset-Signal des in der Karte implantierten Chip,

VCC : Versorgungsspannungskontakt.

Anmerkung: Die restlichen drei Kontakte werden nicht belegt. D.h. diese Kontakte (insbesondere Vpp, da dieser Kontakt im FuTel-Netz C für die Speicherkarte benutzt wird) sind kartenseitig mit dem implantierten Chip elektrisch nicht verbunden.

A 2.3.2 Festlegung

Alle Messungen werden relativ zu GND und in einem Temperaturbereich von 0 °C bis 50 °C durchgeführt.

```
XXXXXXXXXXXXXXXXXXXXXXXX FUTEL NETZ-C XXXXXXXXXXXXXXXXXXXXXXXX
X                                                              X
X  Im Netz C gilt ein Temperaturbereich von -20°C bis +55°C.   X
X                                                              X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

Die Stromrichtung in die Karte wird als positiv definiert. Als Status LOW gilt 0 V, Status HIGH entspricht Vcc.

Weiter wird definiert:

V-IH :	Eingangsspannung (high level)
V-IL :	Eingangsspannung (low level)
I-CC :	Versorgungsstrom
I-IH :	Eingangsstrom (high level)
I-IL :	Eingangsstrom (low level)
V-OH :	Ausgangsspannung (high level)
V-OL :	Ausgangsspannung (low level)
I-OH :	Ausgangsstrom (high level)
I-OL :	Ausgangsstrom (low level)
C-IN :	Eingangskapazität
C-OUT :	Ausgangskapazität
V-CC :	Versorgungsspannung am Kontakt Vcc
t-R :	Zeit (Ansteigdauer) zwischen 10 % und 90 % der Signalamplitude
t-F :	Zeit (Falldauer) zwischen 90 % und 10 % der Signalamplitude

Die Bezeichnungen beziehen sich auf die nachfolgend beschriebenen bzw. sämtliche Kontakte.

A 2.3.3 I/O

Über diesen Kontakt werden serielle Daten vom Endgerät zur Karte gesendet oder von ihr empfangen.

Elektrische Eigenschaften :

Symbol	Bedingungen	MIN	MAX	Einheit
V-IH	entweder I-IH max. = ± 500 uA oder I-IH max. = ± 20 uA	2 0.7 * Vcc	Vcc Vcc + 0.3	V V
V-IL	I-IL max. = - 1 mA	- 0.3	0.8	V
V-OH (1*)	entweder I-OH max. = - 100 uA oder I-OH max. = ± 20 uA	2.4 3.8	Vcc Vcc	V V
V-OL	I-OL max. = 1 mA	0	0.4	V
C-IN, C-OUT			30	pF
t-R, t-F			1	us

(1*) Im Endgerät ist ein Pull up Widerstand (Wert: 20 kOhm) einzusetzen, der zwischen I/O und V-CC gelegt wird.

Werden keine Daten vom Endgerät oder der Chipkarte gesendet, so befinden sich beide Seiten im Empfangsmodus. Hierbei muß die I/O-Leitung im Status HIGH gehalten werden.

Endgerät und Chipkarte dürfen nicht gleichzeitig im Zustand 'Senden' sein, da dann der logische Zustand auf der I/O-Leitung undefiniert ist.

Anmerkung: Die I/O-Leitung hat zwei logische Zustände (gemäß ISO 1177):

- Status HIGH: a) Chipkarte und Endgerät sind im Empfangsmodus oder

  b) der Sender legt diesen Status zur Übertragung einer logischen '1 ' an.

- Status LOW: Der Sender legt diesen Status zum Übertragen einer logischen '0 'an.

A 2.3.4 CLK

Die aktuelle Clockfrequenz, die vom Endgerät am Kontakt CLK angelegt wird, ist definiert als fi (initial frequency) oder fs (subsequent frequency). Für die Telekommunikations-Chipkarte gilt folgende Vereinbarung :

fi = 2.4576 MHz bei 4800 bit/s
fs = 4.9152 MHz bei 9600 bit/s

mit

fi = initial frequency (Bei Answer to Reset)
fs = subsequent frequency (Betriebsfrequenz für die Kommunikation)

Anmerkung:

Für manche Anwendungen gilt:

fi = fs = 4,9152 MHz ± 10%

Da die Baudrate starr mit der Clockfrequenz gekoppelt sein muß, verändert sich die Baudrate im gleichen Verhältnis wie die Clockfrequenz.

Beispiel:

Bei einer Clockfrequenz von

4,9152 MHz - 10%

muß die Baudrate

9600 Baud - 10%

betragen.

XXXXXXXXXXXXXXXXXXXXXXXX FUTEL NETZ-C XXXXXXXXXXXXXXXXXXXXXXXX
X X
X Im Netz C gilt fi = fs = 4,9152 MHz ± 10%. X
X X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Elektrische Eigenschaften :

Symbol	Bedingungen	MIN	MAX	Einheit
V-IH	I-IH max. = ± 200 uA	2.4	Vcc + 0.3	V
	I-IH max. = ± 20 uA	0.7 * Vcc	Vcc + 0.3	V
	I-IH max. = ± 10 uA	Vcc - 0.7	Vcc + 0.3	V
V-IL	I-IL max. = ± 200 uA	- 0.3	0.5	V
C-IN			30	pF
t-R, t-F		9 % der Periodendauer mit einem Maximum von 0.5 us		

Duty cycle : zwischen 45 % und 55 % der Periodendauer

A 2.3.5 RST

Elektrische Eigenschaften :

Symbol	Bedingungen	MIN	MAX	Einheit
V-IH	I-IH max. = ± 200 uA	4	Vcc + 0.3	V
	I-IH max. = ± 10 uA	Vcc - 0.7	Vcc + 0.3	V
V-IL	I-IL max. = ± 200 uA	- 0.3	0.6	V

A 2.3.6 VCC

Am Kontakt VCC liegt die Spannung

$$Vcc = 5\ V \pm 5\ \%\ an.$$

Die Stromaufnahme der Chipkarte (Icc) darf 100 mA (abweichend von ISO 7816 (300 mA)) nicht überschreiten. Der Spannungsverlauf am Kontakt VPP muß gleich dem Spannungsverlauf am Kontakt VCC sein.

A 2.3.7 Aktivieren der Kontakte

Die elektrischen Signale dürfen nicht eher aktiviert werden, bis alle Kontakte der Kontaktierungseinheit korrekt positioniert und kontaktiert sind.

Eine Kontaktierungseinheit ist inaktiv, wenn alle Kontakte zwischen 0 V und 0,4 V relativ zu GND liegen und wenn der Strom kleiner als 1 mA ist.

Das Aktivieren der Kontakte geschieht nach folgendem Ablauf :

1. Schritt:
   - Spannung an RST ist im Status LOW.
   - Spannung an I/O ist im Status LOW.
   - Spannung an CLK ist im Status LOW.
   - V-CC wird eingeschaltet.

2. Schritt:
   - I/O des Endgerätes geht in den Status HIGH (Empfangsmodus). V-CC und I/O können auch gleichzeitig auf HIGH gehen, wenn sichergestellt ist, daß die Spannung an I/O gegenüber der Spannung an VCC nicht voreilt.

3. Schritt:
   - CLK wird zum Zeitpunkt T0 (siehe A 2.4.1) mit einem gültigen und stabilen Clock-Signal versorgt.

Für die Aktivierung der Kontakte muß der 2. Schritt abgeschlossen sein, bevor der 3. Schritt erfolgen kann.

A 2.3.8 Deaktivieren der Kontakte

Wenn ein letzter Befehl bearbeitet wurde oder wenn eine Transaktion abgebrochen wurde, müssen die Kontakte elektrisch deaktiviert werden.

Dies geschieht nach folgender Reihenfolge:
1. Schritt: Status LOW an RST,
2. Schritt: Status LOW an CLK,
3. Schritt: Status LOW an I/O,
4. Schritt: Versorgungsspannung an VCC abschalten.

Zwischen dem ersten und dem zweiten Schritt muß ein zeitlicher Abstand von mindestens 20 Clockzyklen liegen.

A 2.4 Reset der Karte

Nach Beendigung des Aktivierens der Kontakte (siehe A 2.3.7) ist die Chipkarte nach ISO 7816-3 bereit, den Reset-Vorgang auszuführen:

Nachdem das Clock-Signal zur Zeit T0 an den Kontakt CLK angelegt worden ist, muß innerhalb der Zeit t2 (200 Clock Zyklen des Clock-Signals an CLK) I/O in den Zustand HIGH gesetzt werden.

Eine Karte mit internem Reset beginnt den Reset bereits nach einigen Clock Zyklen. Bei einem internen Reset beginnt die Antwort der Karte am I/O-Kontakt zwischen 400 und 40.000 Clock Zyklen nach Anlegen des Clock Signals an CLK (Zeit t1 nach T0).

Bei einer Karte mit Reset aktiv LOW wird RST für mindestens 40.000 Clock Zyklen nach Anlegen des Clock Signals an CLK im Status LOW gehalten (Zeit t3 nach T0). Wurde keine Antwort während der letzten 40.000 Clock Zyklen erhalten (also kein interner Reset), wird RST in den Status HIGH gesetzt (zur Zeit T1). Die Antwort der Karte am I/O-Kontakt beginnt dann zwischen 400 und 40.000 Clock Zyklen nach Ansteigen der Flanke des Signals am RST-Kontakt (Wechsel von Status LOW nach Status HIGH zur Zeit T1).

Wird nach 40.000 Clock Zyklen nachdem RST im Status HIGH ist (Zeit t3 nach T1) keine Antwort von der Karte empfangen, wird RST wieder in den Status LOW gebracht (zur Zeit T2) und die Kontakte werden deaktiviert.

Anmerkung:

Die Kontaktierungseinheit kann daraufhin von den Kontakten gelöst und wieder auf sie aufgesetzt werden, um nun noch einen weiteren Reset-Versuch (siehe A 2.3.7) vorzunehmen.

A 2.4.1 Timing des Chipkarten-Reset

(IR = interner Reset)
(AL = Reset mit aktiv LOW)

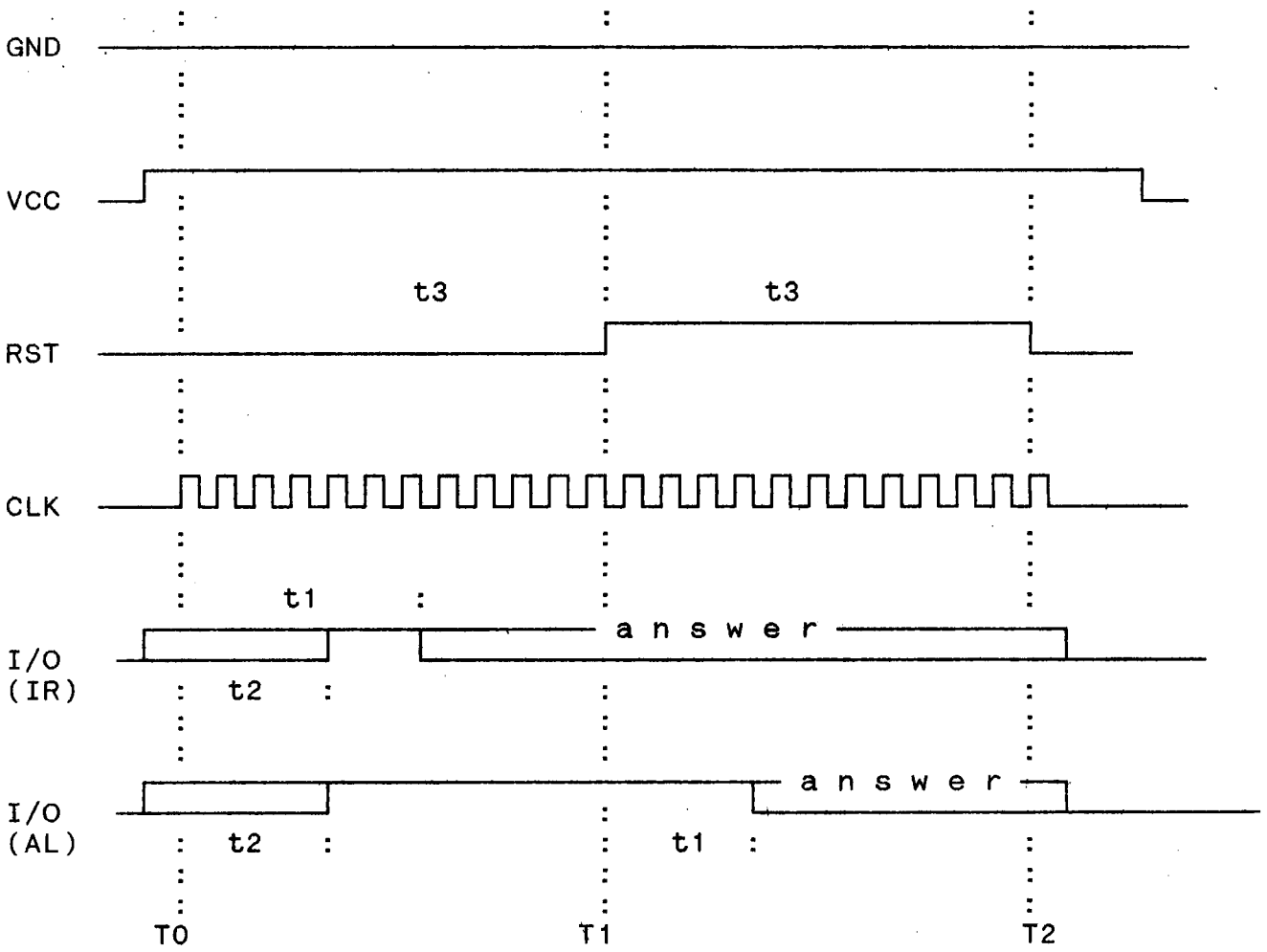


Bild A 2.2: Timing des Chipkarten-Reset

A 2.4.2 Antwort der Chipkarte

Nach einem Reset sendet die Chipkarte eine Bytesequenz als Antwort. Diese Antwort ist der Answer to Reset (ATR). Der ATR und die Behandlung beim ATR ist im Abschnitt D beschrieben.

Der zeitliche Abstand zwischen den Startflanken zweier aufeinanderfolgender Byte muß 12 etu betragen.

*) etu = elementary time unit
Zeiteinheit für ein Bit.

A 3 Datenkommunikation

Dieses Kapitel beschreibt die Grundzüge der Kommunikation mit Chipkarten. Zum einen wird ein Kommunikationsmodell zur Erklärung der an der Kommunikation beteiligten Komponenten vorgestellt. Dieses Modell ist ein allgemeines Modell und kann somit auf andere mögliche Konfigurationen angewandt werden.

Desweiteren werden die für die Kommunikation benutzten Kommunikationsprotokolle aufgezeigt. Diese orientieren sich am OSI-Referenz-Modell. Die einzelnen Protokolle werden in eigenständigen Kapiteln bzw. im Anhang eingehend beschrieben.

Der letzte Teil dieses Kapitels enthält die für die Kommunikation mit Chipkarten getroffenen Vereinbarungen und Definitionen.

A 3.1 Kommunikationsmodell

(siehe Abschnitt D, Punkt 1)

A 3.2 Kommunikationsprotokolle

(siehe Abschnitt D)

A 3.3 Definitionen und Vereinbarungen

Die Kommunikation zwischen ICC und der Anwendungsseite erfolgt nach dem Master / Slave Prinzip. Für den Betrieb mit Chipkarten gilt in der Regel, daß die Chipkarte als Slave, und die Anwendung auf der Seite des CEG's als Master fungiert.

Der Master stellt Anforderung an den Slave. Dieser muß die Anforderung bearbeiten und gibt eine Antwortmeldung an den Master.

- Die Anforderung an den Slave wird in der Anwendungsschicht KOMMANDO genannt.
- Die Antwortmeldung an den Master wird in der Anwendungsschicht ANTWORT genannt.

A 4 Applikationsprotokoll

Das Applikationsprotokoll ist das Protokoll für die Anwendung (Schicht 7 OSI-Referenzmodell). Dieses Protokoll ist ein End-to-End-Protokoll zwischen einem Anwendungsprozeß (Btx, NETZ-C etc.) und der Anwendung auf einer Chipkarte (z.B. Fernmeldedienstkarte).

Der Austausch von Informationen zwischen dem Anwendungsprozeß und der Chipkarte geschieht durch abwechselnde Übertragung von Kommando und Antwort mit oder ohne spezifische Anwenderdaten.

Kommandos und Antworten sind APDUs (Application Protocol Data Units), die folgendes Format haben:

APDU (Application Protocol Data Unit)							
Steuerfeld		Datenlänge	Datenblock				
SFLD		DLNG	D-01	D-02	D-03	.....	D-nn
1 Byte	1 Byte	1 o.3 Byte	1 Byte	1 Byte	1 Byte	....	1 Byte

D-nn = Datenbyte n

Bild A 4.1: Format der APDUs (Application Protocol Data Units)

A 4.1 Steuerfeld des Applikationsprotokolls (SFLD)

Bei einem Kommando enthält das Steuerfeld der APDU ein Kommando für die entsprechende Applikation. Es besteht aus zwei Bytes. Das erste Byte enthält das Ident-bit (I=0) und die Befehlsklasse (CLA). Das zweite Byte enthält den Befehl (INS).

STEUERFELD			
I	Bef.Kl. (CLA)	Befehl (INS)	
b8	b1	b8	b1

Bild A 4.2: Steuerfeld APDU bei einem Kommando

Bei einer Antwort enthält das Steuerfeld den Status der Chipkarte. Es besteht aus zwei Bytes. Das erste Byte enthält ebenfalls das Ident-bit (I=1) und den allgemeinen Chipkarten-Returncode (CCRC). Das zweite Byte steht der Applikation für einen frei definierbaren Returncode (APRC) zur Verfügung.

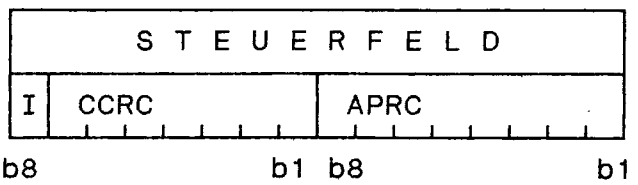
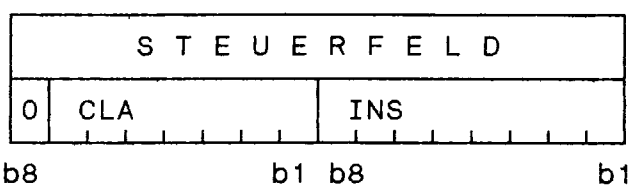


Bild A 4.3: Steuerfeld APDU bei einer Antwort

A 4.1.1 Ident-Bit

Das Ident-bit (I) ist das höchstwertige Bit (bit 8) des ersten Bytes des Steuerfeldes und wird zur Identifizierung eines Kommandos oder einer Antwort benutzt. Bei einem Kommando ist dieses Bit immer '0', bei einer Antwort immer '1'.

(a) Kommando



(b) Antwort

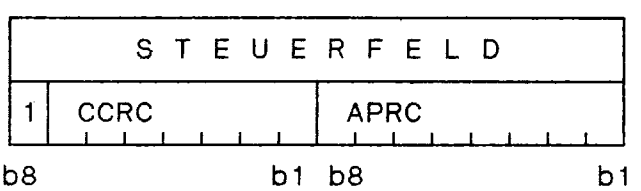


Bild A 4.4: Ident-Bit bei Kommando und Antwort

A 4.1.2 Kommando- und Antwortfeld

Die Bits b1 bis b7 des ersten Bytes zusammen mit dem zweiten Byte des Steuerfeldes heißen im Falle des Kommandos 'Kommandofeld' und im Falle der Antwort 'Antwortfeld'.

A 4.1.3 Befehlsklasse

Die Befehlsklasse erlaubt die logische Gliederung der einzelnen Befehle. Hierdurch kann zum Beispiel ein Satz von Befehlen, der zu einer Funktion der Chipkarte gehört, zusammengefaßt werden.

Durch die 7-Bit der Befehlsklasse ist die Definition von 128 verschiedene Klassen (Klasse: 0 ... Klasse: 127) möglich.

A 4.1.4 Befehl (INS)

Befehle sind Anweisungen eines Anwendungsprozesses an den Empfänger bestimmte Instruktionen auszuführen. Sie sind nach Befehlsklassen eingeteilt. Innerhalb einer Klasse unterteilen sich die Befehle in allgemeingültige, d.h. applikationsunabhängige Befehle, und solche, denen in jeder Applikation eine andere Bedeutung zukommen kann.

A 4.1.5 Chipkarten-Returncode (CCRC)

Bei einer Antwort enthält Bit 1 bis Bit 7 des ersten Bytes im Steuerfeld der APDU den allgemeinen Chipkarten-Returncode (CCRC).

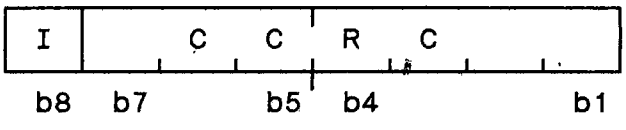


Bild A 4.5: Statusbyte bei einer Antwort

Der CCRC zeigt dem Sender des Kommandos den Status der Chipkarte an.

A 4.1.6 Applikations-Returncode (APRC)

Über den Applikations-Returncode steht dem Anwender die Möglichkeit zur Verfügung, einen innerhalb der Anwendung definierten Status dem Sender eines Kommandos mitzuteilen.

A 4.2 Längenfeld des Applikationsprotokolls (DLNG)

Die Länge des Datenblocks in einer APDU wird in einem Byte angezeigt. Sie wird von 0 bis 254 binär kodiert (b1 = LSB).

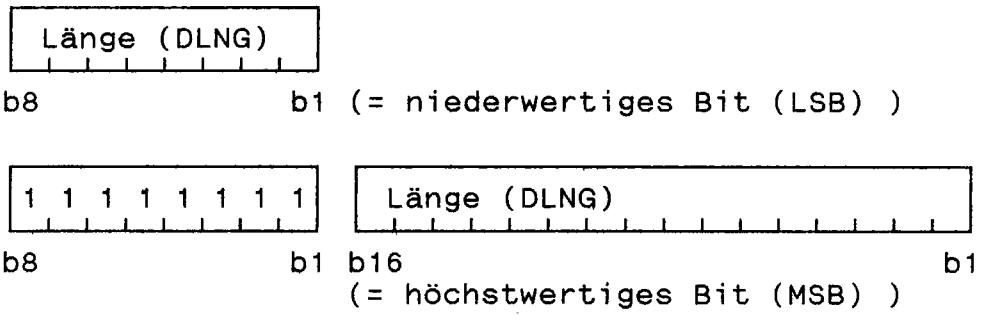


Bild A 4.6: Längenbyte des Applikationsprotokolls

Ein leerer Datenblock hat die Länge 0. Bei der Übertragung von mehr als 254 Byte Schicht-7-Daten wird dieses Längenbyte auf 255 gesetzt. In diesem Fall werden die nächsten zwei Bytes als Längenbyte interpretiert, wodurch eine Längenangabe von 0 bis 65534 möglich wird. Die Längenangabe ist binär kodiert und rechtsbündig angegeben (b1 des 2. Bytes ist LSB).

Byte 2 des DLNG ist das highorder-Byte, Byte 3 ist das loworder-Byte.

```
XXXXXXXXXXXXXXXXXXXXXXXX FUTEL NETZ-C XXXXXXXXXXXXXXXXXXXXXXXX
X                                                              X
X Das Feld DLNG besteht immer aus einem Byte. Signalisiert die X
X Chipkarte die Übertragung von mehr als 254 Datenbyte, so ist X
X die Schicht-7-Fehlerbehandlung (Seite A-21) durchzuführen.   X
X                                                              X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

A 4.3 Datenblock

Der Datenblock beinhaltet die Information, die übertragen werden soll. Die Länge des Datenblocks ist abhängig von DLNG.

```
XXXXXXXXXXXXXXXXXXXXXXXX FUTEL NETZ-C XXXXXXXXXXXXXXXXXXXXXXXX
X                                                              X
X Treten Differenzen zwischen der Länge des Datenblocks und    X
X der in DLNG angegebenen Datenlänge auf, ist die Schicht-7-   X
X Fehlerbehandlung (Seite A-21) durchzuführen.                 X
X                                                              X
X Erfordert die Codierung einer Größe mehr als ein Byte im     X
X Datenblock, so ist im Datenbyte mit der niedrigsten Numerie- X
X rung (z.B. DB-01) das höchstwertige Byte; im Datenbyte mit    X
X der höchsten Numerierung (z.B. DB-nn) das niederwertigste    X
X Byte enthalten.                                              X
X                                                              X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

A 5 Returncodes

Für die Multifunktions-Chipkarte existieren zwei verschiedene Returncodes:

- CCRC für den Status der Chipkarte
- APRC für den Status der selektierten Applikation

Alle Code-Angaben bei den Definitionen der einzelnen Return-Codes sind hexadezimal angegeben. Das für den jeweiligen Return-Code nicht benutzte Halbbyte, bzw. die nicht benutzten Bits, sowie dessen/deren Lage ist/sind durch 'x' dargestellt.

A 5.1 Chip Karten Return Code

Der Chip Card Return Code (CCRC) zeigt den Status der Chipkarte für eine selektierte Applikation an und wird im Steuerfeld der Antwort-APDU (siehe A 4.1) übertragen.

A 5.1.1 Definition der CCRC

Für den CCRC der Multifunktions-Chipkarte gelten folgende Returncodes:

Die nachfolgende Abbildung zeigt die Kodierung des CCRC im Steuerfeld der Antwort.

Die Bits des CCRC haben folgende Bedeutung:

b8 b1	Bedeutung
1 0 0 0 0 0 0 1	PIN-NOT-OK
1 0 0 0 0 0 1 0	AFBZ = NULL
1 0 0 0 0 1 0 0	APRC valid
1 0 0 0 1 0 0 0	reserviert
1 0 0 1 0 0 0 0	reserviert
1 0 1 0 0 0 0 0	reserviert
1 1 0 0 0 0 0 0	GENERAL ERROR
1 0 0 0 0 0 0 0	IDENT BIT

Kombinationen der einzelnen Bits sind ebenfalls möglich.

Beispiel:

1 0 0 0 0 0 1 1	PIN-NOT-OK , AFBZ NULL

A 5.1.2 Kodierung CCRC

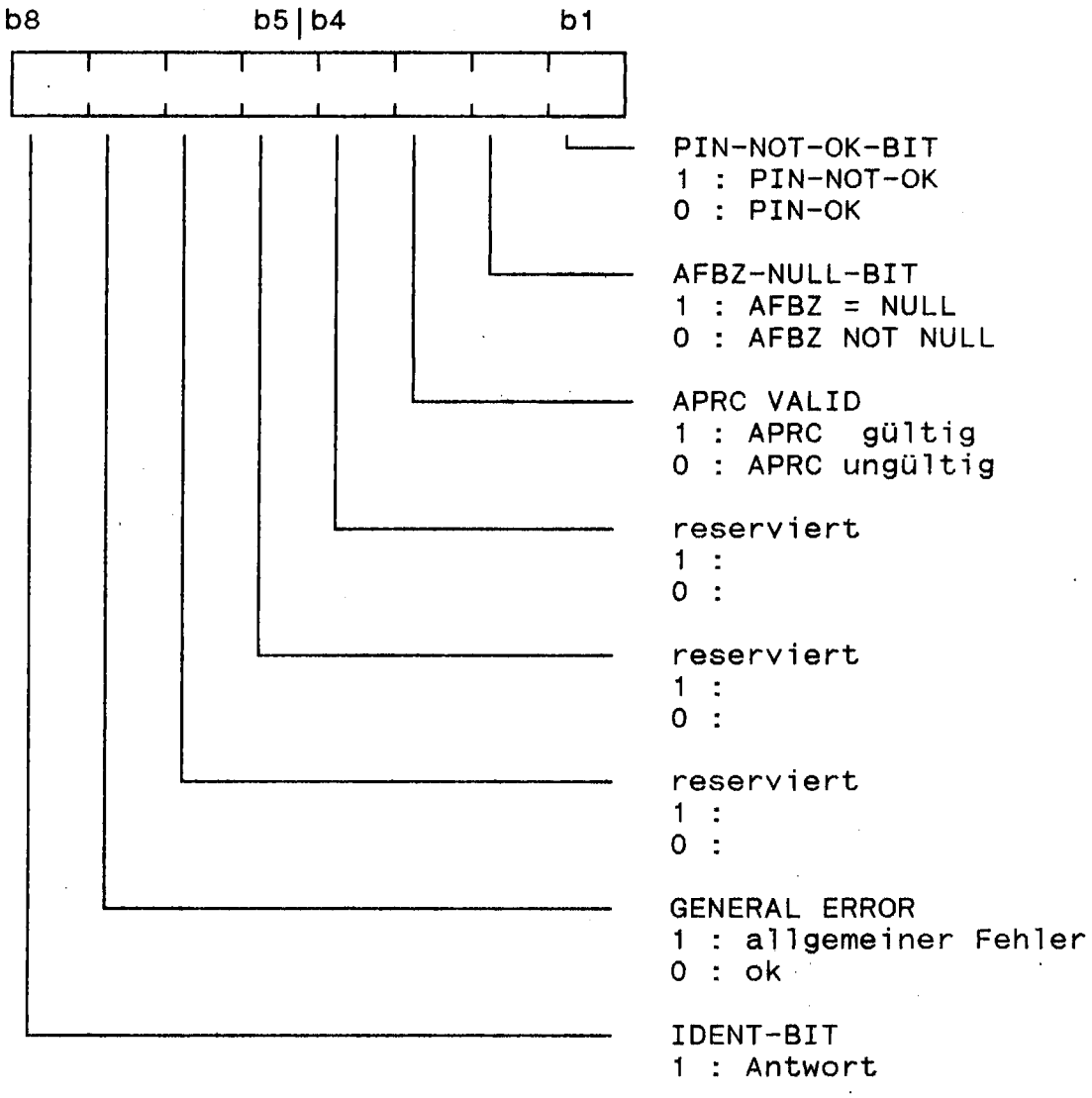


Bild A 5.1: Kodierung CCRC im Statusbyte

XXXXXXXXXXXXXXXXXXXXXXXX **FUTEL NETZ-C** XXXXXXXXXXXXXXXXXXXXXXXX
X X
X Bei der Auswertung der Returncodes müssen müssen grundsätz- X
X lich die nachfolgend dargestellten Prioritäten eingehalten X
X werden. Den nachfolgenden Festlegungen ist zu entnehmen, ob X
X und wie die angegebenen Statusmeldungen auszuwerten sind: X
X X
X 1) Ident-Bit (CCRC, Bit 8) X
X 2) Error-Bit (CCRC, Bit 7) X
X 3) AFBZ-Null-Bit (CCRC, Bit 2) und Applikation-gesperrt-Bit X
X (APRC, Bit 3), falls das APRC-valid-Bit (CCRC, Bit 3) X
X gesetzt ist X
X 4) PIN-NOT-OK-Bit (CCRC, Bit 1) X
X 5) GEBZ-voll-Bit (APRC, Bit 6), falls das APRC-valid-Bit X
X gesetzt ist (nur Applikation Netz C) X
X 6) GEBZ/RUFN-gesperrt-Bit (APRC, Bit 5), falls das APRC- X
X valid-Bit (CCRC, Bit 3) gesetzt ist X
X X
X zu 3): Wird im Returncode angezeigt, daß der AFBZ gleich Null X
X und/oder die Applikation gesperrt ist, so ist einer X
X der beiden Fälle dem Benutzer anzuzeigen. Es dürfen X
X dann keine Funktionen ausgeführt werden, die auf die X
X jeweilige Applikation zugreifen. Tritt dieser Fall für X
X die Applikation Netz C ein darf optional noch auf die X
X Applikation Register ein/aus zugegriffen werden; die X
X Karte ist in diesem Fall zu deaktivieren.
X X
X Das CEG darf seine Menüführung und die Steuerung der Benutzer-X
X eingaben von der Auswertung der Returncodes (Status) der ICC X
X abhängig machen, sofern sich daraus keine Verstöße gegen die X
X FTZ 171 TR 60 ergeben. X
X X
X Das PIN-NOT-OK-BIT wird nur im Zusammenhang mit den Kommandos X
X SL-APPL, CHK-PIN und SET-PIN ausgewertet. X
X X
X Das AFBZ-NULL-BIT wird nur im Zusammenhang mit den Kommandos X
X SL-APPL, CHK-PIN und SET-PIN ausgewertet. X
X X
X Das AFBZ-NULL-BIT und das PIN-NOT-OK-BIT werden zur Steuerung X
X der PIN-Prüfung verwendet. Das Bit PIN-Prüfung (s. A 5.2.1.1 X
X Definition des ASTA) kann nicht zur Endgeräte-Steuerung der X
X PIN-Prüfung genutzt werden. Bei AFBZ-NULL-BIT = 1 ist das X
X PIN-NOT-OK-BIT nicht mehr auszuwerten. X
X X
X Wird ein ungültiger APRC signalisiert (APRC VALID = 0), X
X ist dieser nicht mehr auszuwerten. X
X X
X Wird ein allgemeiner Fehler signalisiert (GENERAL ERROR = 1), X
X ist die Schicht-7-Fehlerbehandlung (Seite A-21) durchzuführen.X
X X
X Das FuTelG setzt das IDENT-BIT immer auf 0, die Chipkarte X
X immer auf 1. Sendet die Chipkarte eine andere Signalisierung, X
X ist die Schicht-7-Fehlerbehandlung durchzuführen. X
X X
X Reservierte Bit sind nicht auszuwerten. X
X X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

A 5.2 Applikations-Returncode (APRC)

Der APRC wird im 2. Byte des Steuerfeldes in einer Antwort von der Chipkarte übertragen. Die Auswertung und Gültigkeit des APRC ist abhängig von den in der selektierten Applikation benutzten Kommandos und wird durch das Bit "APRC VALID" im CCRC angezeigt.

Der APRC hat eine Länge von einem Byte. Das niederwertige Halbbyte (ASTA) des APRC ist fest definiert und spiegelt den Status der selektierten Applikation. Das höherwertige Halbbyte (ASTS) ist abhängig von der Applikation und frei definierbar.

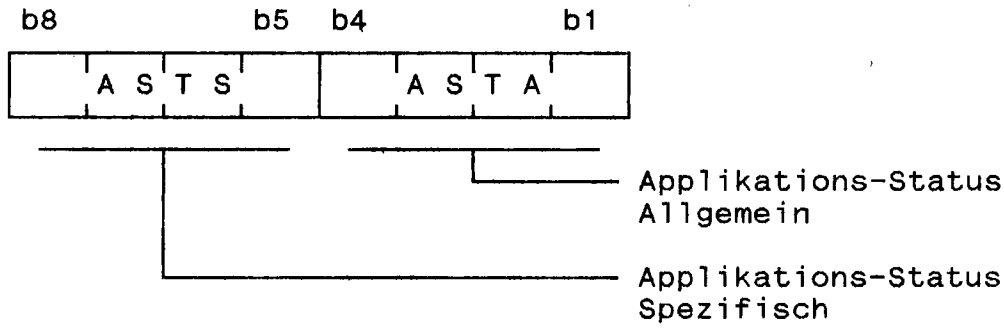


Bild A 5.2: Application Return Code APRC

A 5.2.1 Applikations Status Allgemein

A 5.2.1.1 Definition des ASTA

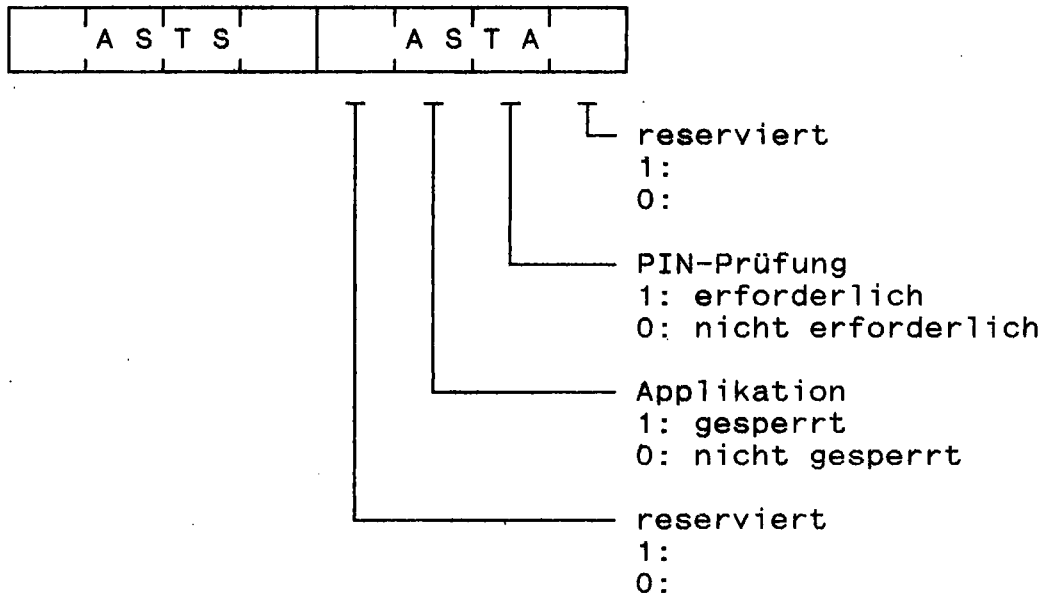
Für den Applikationsstatus ASTA im APRC gelten folgende Returncodes:

Code	Bedeutung
x0	Dadurch wird angezeigt, daß - keine PIN-Prüfung für die selektierte Applikation erforderlich ist, und - die selektierte Applikation nicht gesperrt ist.
x2	PIN-Prüfung: Dadurch wird angezeigt, daß für die selektierte Applikation eine PIN-Prüfung erforderlich ist.
x4	Applikation gesperrt: Dadurch wird angezeigt, daß die selektierte Applikation gesperrt ist.

'x' ASTS (Applikations-Status Spezifisch)

A 5.2.1.2 Kodierung ASTA im APRC

Die untenstehende Abbildung zeigt die Kodierung des ASTA im APRC-Byte.



x	x	x	x	0	0	1	0	PIN-Prüf. erforderlich
x	x	x	x	0	1	0	0	Applikation gesperrt

Kombinationen der einzelnen Bits sind ebenfalls möglich.

Bild A 5.3: Kodierung ASTA im APRC

```
XXXXXXXXXXXXXXXXXXXXXXXXX FUTEL NETZ-C XXXXXXXXXXXXXXXXXXXXXXXXX
X                                                               X
X Das Bit "Applikation" ist nur im Zusammenhang mit dem         X
X Kommando SL-APPL auszuwerten.                                 X
X                                                               X
X Reservierte Bit sind nicht auszuwerten.                       X
X                                                               X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
```

A 5.2.2 Applikations Status Spezifisch

Der Applikations Status Spezifisch (ASTS) ist in den jeweiligen Applikationen beschrieben.

FUTEL NETZ-C

Schicht-7-Fehlerbehandlung

In der Schicht 7 können folgende Fehler auftreten:

- Die Länge des übertragenen Datenblocks entspricht nicht der in DLNG angegebenen Datenlänge.
- Die Länge des übertragenen Datenblocks entspricht nicht den Angaben dieser Spezifikation.
- Die Chipkarte signalisiert im Feld DLNG die Übertragung von mehr als 254 Byte.
- Die Chipkarte signalisiert im CCRC einen allgemeinen Fehler durch Setzen des GENERAL ERROR Bit auf 1.
- Die Chipkarte setzt das IDENT Bit nicht auf 1.

Ergeben sich in einer Antwort der ICC Widersprüche (z.B. Senden des Gebührenstandes trotz gesperrtem Zugriff), so liegt ein Fehlverhalten der Karte vor; es kann in diesen Fällen eine Schicht 7-Fehlerbehandlung eingeleitet werden. Zeigt eine Karte bei der Ausführung von Kommandos innerhalb einer Applikation unterschiedliche Zustände an (z.B. Zugriff frei/gesperrt), obwohl der Status nicht durch ein entsprechendes Kommando geändert wurde, so liegt ein Fehlverhalten der Karte vor und es kann eine Schicht 7-Fehlerbehandlung eingeleitet werden.

Treten einer oder mehrere dieser Fehler auf, ist das zuletzt gesendete Schicht 7-Kommando zu wiederholen. War auch der 3. Versuch noch nicht fehlerfrei, ist die RESET-Fehlerprozedur (siehe Seite E-14) durchzuführen.

Eine Fehlerbehandlung von Antworten auf das Kommando SH-APPL hat zu berücksichtigen, daß die Einträge in den Antworten der Karte zyklisch ausgegeben werden.

A 6 Definition der Kommandos

Ein Kommando wird im Steuerfeld übertragen und besteht aus zwei Bytes. Das erste Byte enthält dabei die Befehlsklasse, das zweite Byte den Code des in dieser Klasse auszuführenden Befehls. Somit könnten bis zu 256 verschiedene Befehle in einer Befehlsklasse definiert werden.

A 6.1 Befehlsklassen (CLA)

Die Befehlsklasse bestimmt den Typ des Befehls. Für eine multifunktionale Chipkarte gelten die folgenden Befehlsklassen:

CNTR	Control
STAT	Status
WRTE	Write
READ	Read
EXEC	Execute
AUTO	Authentication

Nachfolgend werden die definierten Klassen im einzelnen beschrieben.

A 6.1.1 Kodierung der Befehlsklassen

Die nachstehende Tabelle zeigt die Kodierung der definierten Befehlsklassen. Die Code-Werte sind hexadezimal angegeben.

Name	Bedeutung	Code
CNTR	Control Klasse	02
STAT	Status Klasse	03
WRTE	Write Klasse	04
READ	Read Klasse	05
EXEC	Execute Klasse	06
AUTO	Authentifikation Klasse	07

A 6.1.2 Beschreibung der Befehlsklassen

CNTR Control

Diese Klasse wird benutzt für Steuer- und Kontrollkommandos, die die Chipkarte betreffen.

- Auswahl der gewünschten Applikation ("select application")
- Schließen der gewählten Applikation ("close application")
- Anzeigen der Applikationen ("show application")
- Auswahl eines anderen Übertragungsprotokolls
- etc.

STAT Status

Diese Klasse wird benutzt, um Statusinformation von der Chipkarte anzufordern.

- Auskunft über den Zustand (Status) der Chipkarte, z.B. Konsistenz-Check
- etc.

WRTE Write

Diese Befehlsklasse wird benutzt, um Informationen (Daten) auf die Chipkarte zu schreiben. Durch den Befehl wird der Speicherbereich bestimmt, in den die Daten geschrieben werden.

- Schreiben von Daten (Feldern)
- etc.

READ Read

Durch Befehle in dieser Klasse werden Informationen (Daten) aus dem Speicherbereich der Chipkarte gelesen. Durch den Befehl wird der Speicherbereich bestimmt, aus dem die Daten gelesen werden.

- Lesen von Daten (Feldern)
- etc.

EXEC Execute

Durch Befehle in dieser Klasse kann die Ausführung von speziellen Operationen in der Chipkarte veranlaßt werden.

AUTO Authentifikation

Diese Klasse beinhaltet alle die zur Autorisierung notwendigen Befehle des verwendeten Sicherungsverfahren.

A 6.2 Befehle (INS)

Innerhalb der einzelnen Befehlsklassen können allgemeingültige (Standardbefehle) und applikationsabhängige Befehle definiert sein. Diese Befehle unterscheiden sich in der Kodierung.

hex. F0 - FF für allgemeingültige Befehle,
hex. 01 - EF für applikationsabhängige Befehle,
hex. 00 ist für spezielle Befehle reserviert.

A 6.2.1 Definition der Standardbefehle

Für die Chipkarte werden in den einzelnen Klassen folgende Standardbefehle definiert:

Klasse	Befehl	Bedeutung
CNTR	SL-APPL*	Select Application (Applikation auswählen)
	CL-APPL	Close Application (Applikation beenden)
	SH-APPL	Show Application (Applikation(en) anzeigen)
STAT	CHK-KON	Prüfung des Chipkartenstatus
EXEC	CHK-PIN	PIN-Prüfung durchführen
	SET-PIN	Eingabe einer neuen PIN

* (In internationalen Bezeichnungen entspricht 'SL-APPL' dem Befehl 'Select-ADF' .)

A 6.2.2 Kodierung der Standardbefehle

Die nachfolgende Tabelle zeigt die Kodierung der vereinbarten Standardbefehle:

Der Befehlscode hex. '10' ist reserviert und sollte für eventuelle zukünftige Befehlserweiterungen nicht benutzt werden.

Alle Code-Werte sind hexadezimal angegeben.

Kommando Name	Befehls Klasse	Bef. Code	Kommando Daten	Antwort Daten
SL-APPL	CNTR	F1	APP-IDN	------
CL-APPL	CNTR	F2	--	------
SH-APPL	CNTR	F3	--	Länge APP-IDN, APP-IDN, APP-TXT, APP-STS
CHK-KON	STAT	F1	--	------
CHK-PIN	EXEC	F1	PIN	------
SET-PIN	EXEC	F2	PLA, alte PIN, neue PIN	------ ------

A 6.3 Beschreibung und Verwendung der Kommandos und Antworten

Im folgenden werden die für die Multifunktionale Telekommunikations-Chipkarte definierten Standardbefehle beschrieben.

Die Definition und Beschreibung der applikationsabhängigen Kommandos und Antworten erfolgt in den Abschnitten B und C.

Für die Darstellung der Beispiele bzw. Beschreibung der einzelnen Kommandos und Antworten gelten folgende Vereinbarungen:

- Alle Werte (Kodierungen von Kommandoklasse, etc., Datenlänge) in den Beispielen für die einzelnen Kommandos und Antworten sind hexadezimal angegeben..

	Kommando / Antwort
- Steuerfeld	SFLD
- Kommandoklasse, bzw. Chipkarten-Returncode	CLA / CCRC
- Befehl, bzw. Applikations-Returncode	INS / APRC
- Datenlänge	DLNG
- Datenbyte 1	D-01
:	:
- Datenbyte nn	D-nn

- Die einzelnen Bytes werden gemäß dem Byterahmen für die Kommunikation übertragen.

Eventuelle Abweichungen von den hier getroffenen Vereinbarungen sind in den Beschreibungen der einzelnen Kommandos explizit angegeben.

A 6.3.1 Befehlsklasse CNTR

A 6.3.1.1 SL-APPL Select Applikation

Dieses Kommando wird genutzt, um eine gewünschte Applikation in der ICC auszuwählen. Zur eindeutigen Identifikation der Applikation wird ein APP-IDN (Application-Identifier) im Datenblock der APDU übergeben. Der Aufbau des APP-IDN ist unter dem Punkt "Directory" näher beschrieben.

Als Ergebnis wird in der Antwort der CCRC im ersten Byte des Steuerfeldes übergeben.

CEG : Kommando ----------> ICC			
SFLD		DLNG	DATA
CLA	INS		APP-IDN
02	F1	0B	D-01|.....|D-0B

CEG <- Antwort :ICC		
SFLD		DLNG
CCRC	APRC	
xx	xx	00

xxxxxxxxxxxxxxxxxxxxxxxx **FUTEL NETZ-C** xxxxxxxxxxxxxxxxxxxxxxxx
x x
x Im APP-IDN sind für die Applikationen "Netz C" sowie x
x "Rufnummernverzeichnis und Gebührenzähler" als Softwareversionx
x "01" oder die aktuelle, mittels SH-APPL ausgelesene Software- x
x version, einzutragen. x
x x
x Wird eine Applikation ausgewählt, die auf der BK gesperrt x
x bzw. nicht vorhanden ist, ist dies dem Teilnehmer entsprechendx
x zu signalisieren. x
x x
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

A 6.3.1.2 CL-APPL General Close Applikation

Durch dieses Kommando wird die Chipkarte veranlaßt, einen logischen Reset auszuführen.

Die laufende Applikation wird abgeschlossen, und die Chipkarte in den Zustand (Status) vor "Select Application" gesetzt.

Beispiel:

CEG: Kommando -> ICC		
SFLD		DLNG
CLA	INS	
02	F2	00

CEG <- Antwort :ICC		
SFLD		DLNG
CCRC	APRC	
xx	xx	00

XXXXXXXXXXXXXXXXXXXXXXXX **FUTEL NETZ-C** XXXXXXXXXXXXXXXXXXXXXXXX
X X
X Dieser Befehl kann optional von den FuTelG-Herstellern rea- X
X lisiert werden . X
X X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

A 6.3.1.3 SH-APPL Show Application

Mit diesem Kommando wird das 'Directory' der Chipkarte gelesen, das für jede in der Chipkarte implementierte Applikation einen Datensatz enthält (siehe Abschnitt A 7.1.1 "Directory").

Es wird, beginnend beim 1. Datensatz des Directory, jeweils nur ein Datensatz gelesen. Die Chipkarte merkt sich selbst, welcher Satz gelesen wurde und übergibt beim erneuten Aufruf den nächsten Datensatz des Directory.

Als Daten werden die Länge (L) des APP-IDN, der APP-IDN (siehe A 7.1.1.2), die Bezeichnung der Applikation "APP-TXT" (siehe A 7.1.1.3) und der Applikationsstatus "APP-STS" (siehe A 7.1.1.4) im Datenblock der Antwort übergeben.

Das Ende des Directory wird erkannt, wenn der Datenblock der Antwort keine Daten enthält, also die Datenlänge DLNG = 0 ist.

Das Kommando ist in jedem Status ausführbar.

Beispiel: Directory mit zwei aktivierten Applikationen

CEG: Kommando -> ICC		
SFLD		DLNG
CLA 02	INS F3	00

1. Datensatz

CEG <---------- Antwort :ICC			
SFLD		DLNG	DATA
CCRC xx	APRC xx	21	L/APP-IDN/APP-TXT/APP-STS D-01|.....|D-21

CEG: Kommando -> ICC		
SFLD		DLNG
CLA	INS	
02	F3	00

CEG <---------- Antwort :ICC			
SFLD		DLNG	DATA
CCRC	APRC		L/APP-IDN/APP-TXT/APP-STS
xx	xx	21	D-01|.....|D-21

2. Datensatz

CEG: Kommando -> ICC		
SFLD		DLNG
CLA	INS	
02	F3	00

CEG <- Antwort :ICC		
SFLD		DLNG
CCRC	APRC	
xx	xx	00

kein weiterer Datensatz

XXXXXXXXXXXXXXXXXXXXXXXXX **FUTEL NETZ-C** XXXXXXXXXXXXXXXXXXXXXXXXX
X X
X Dieser Befehl kann optional von den FuTelG-Herstellern rea- X
X lisiert werden (s. FTZ 171 TR 60, Abschnitt 7.15). X
X Falls das CEG den APP-STS verarbeitet, werden nur die Bit X
X "PIN-Prüfung" und "Applikation" ausgewertet. X
X X
X Ist das Bit "Applikation" für die Applikation Netz C gesetzt, X
X ist die Bedienung der Applikation Register ein/aus optional. X
X X
X Werden die Daten zum Prüfen und/oder Selektieren einer Appli- X
X kation genutzt und es liegt kein Eintrag für die Applikation X
X Netz C vor, so ist die Karte für die Applikation Netz C abzu- X
X lehnen; die Bedienung der Applikation Register ein/aus ist X
X optional. X
X X
X Werden die Texteinträge angezeigt, so ist eine Konvertierung X
X der nichtdarstellbaren Zeichen (z.B. in Blanks oder Frage- X
X zeichen) vorzunehmen. X
X X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

A 6.3.2 Befehlsklasse STAT

A 6.3.2.1 CHK-KON Prüfung des Chipkartenstatus Konsistenzcheck

Dieses Kommando wird zur Überprüfung des Chipkartenstatus benutzt. Als Ergebnis werden die entsprechenden Bits im CCRC der Antwort gesetzt. In der Antwort werden keine weiteren Datenbytes übertragen.

Das Kommando ist gleichwertig in allen Applikationen und jederzeit ausführbar.

Beispiel:

CEG: Kommando -> ICC		
SFLD		DLNG
CLA 03	INS F1	00

CEG <- Antwort :ICC		
SFLD		DLNG
CCRC xx	APRC xx	00

XXXXXXXXXXXXXXXXXXXXXXXX **FUTEL NETZ-C** XXXXXXXXXXXXXXXXXXXXXXXX
X X
X Dieser Befehl kann optional von den FuTelG-Herstellern rea- X
X lisiert werden. X
X X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

A 6.3.3 Befehlsklasse EXEC

A 6.3.3.1 CHK-PIN PIN-Prüfung

Durch dieses Kommando wird der Chipkarte im Kommando eine am Endgerät eingegebene PIN übergeben. Die Chipkarte vergleicht diese PIN mit der in der Chipkarte für die ausgewählte Applikation gespeicherten PIN.

Stimmen übergebene PIN und gespeicherte PIN überein, so wird dies im CCRC der Antwort angezeigt. Der AFBZ (Applikations-Fehlbedienungszähler) wird auf den für die Applikation vorgegebenen Endwert zurückgesetzt.

Stimmt die übergebene PIN nicht mit der gespeicherten PIN überein, so wird der AFBZ der jeweiligen Applikation um eins dekrementiert und die falsche PIN-Eingabe im CCRC der Antwort aktualisiert. Die Chipkarte bleibt in dem Status "Vor PIN-Prüfung". Weitere PIN-Eingaben dürfen der Chipkarte mit dem Kommando "CHK-PIN" zur Prüfung übergeben werden, bis der AFBZ den Wert NULL erreicht hat.

Erreicht der AFBZ durch das Dekrementieren den Wert NULL, wird dies im CCRC der Antwort angezeigt. In diesem Fall ist eine erneute PIN-Prüfung erst dann möglich, wenn an einem Postserviceterminal der AFBZ auf seinen Endwert zurückgesetzt wird.

Weitere Einzelheiten für die PIN (z.B. Länge, zugelassene Zeichen etc.) sind in den Applikationen festgelegt.

In der Antwort werden keine Daten übertragen.

CEG : Kommando ----------> ICC			
SFLD		DLNG	DATA
CLA 06	INS F1	xx	PIN D-01|.....|D-xx

CEG <---------- Antwort :ICC		
SFLD		DLNG
CCRC xx	APRC xx	00

XXXXXXXXXXXXXXXXXXXXXXXX **FUTEL NETZ-C** XXXXXXXXXXXXXXXXXXXXXXXX
X X
X Siehe FTZ 171 TR 60, Abschnitt 4.7.2.5 X
X X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

A 6.3.3.2 SET-PIN PIN neu setzen

Dieses Kommando ermöglicht für eine gewählte Applikation die Eingabe einer neuen PIN.

Bevor die "neue" PIN als PIN für die jeweilige PIN gespeichert wird, muß zuvor die auch mit diesem Kommando übertragene "alte" PIN geprüft werden. Im positiven Fall wird die "neue" PIN als gültige PIN für die Applikation in der Chipkarte gespeichert. Andernfalls wird der AFBZ für die PIN der selektierten Applikation um eins dekrementiert, und die "alte" PIN bleibt als Applikations-PIN erhalten.

Der Datenblock dieses Kommandos hat folgenden Aufbau:

- PLA PIN-Länge "alte" PIN
- "alte" PIN
- "neue" PIN

PLA ist eine Längenangabe (1 Byte, binär kodiert) für die Anzahl der Bytes der nachfolgenden "alten" PIN.

Die Länge der "neuen" PIN errechnet sich aus:

DLNG Anzahl der Bytes des Datenblocks
- PLA 1 Byte (Länge "alte" PIN)
- "alte" PIN Anzahl Bytes "alte" PIN

Beispiel:

CEG : Kommando ----------> ICC			
SFLD		DLNG	DATA
CLA	INS		PLA, alte PIN, neue PIN
06	F2	xx	D-01|.....|D-xx

CEG <---------- Antwort :ICC		
SFLD		DLNG
CCRC	APRC	
xx	xx	00

XXXXXXXXXXXXXXXXXXXXXXXX **FUTEL NETZ-C** XXXXXXXXXXXXXXXXXXXXXXXX
X X
X Siehe FTZ 171 TR 60, Abschnitt 4.7.2.5 X
X X
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

A 7 Datenfelder

Bei einer Multifunktions-Chipkarte muß gegenüber einer unifunktionalen Chipkarte zwischen Datenbereichen unterschieden werden, die Informationen beinhalten, die die gesamte Chipkarte betreffen, und jenen, die Informationen und Daten enthalten, die spezifisch für die implementierten Applikationen sind.

Diese verschiedenen Datenbereiche werden als globale und applikationsabhängige Datenfelder bezeichnet.

A 7.1 Globale Datenfelder

Für die Multifunktionalität der Chipkarte werden globale (applikationsunabhängige) Datenfelder definiert. Diese sind unabhängig von der Applikation und ohne ein vorhergehendes 'select application' oder aus jeder Applikation gleichwertig auszulesen. Zu diesen Feldern gehören Datenfelder, die die in der Karte realisierten Applikationen beschreiben (Applikations-Directory).

Desweiteren werden Datenfelder zur Speicherung eines Kurzwahlverzeichnisses (Rufnummernspeicher) definiert. Auf dieses Verzeichnis wird applikationsabhängig zugegriffen. Der Aufbau dieses Speicherbereiches ist im Abschnitt C RUFN+GEBZ Applikation beschrieben.

A 7.1.1 Directory

Für jede in der Chipkarte implementierte Applikation wird ein Datensatz, der für die Applikation spezifische Informationen enthält, in der Chipkarte gespeichert. Diese Datensätze bilden das Directory der Multifunktions-Chipkarte.

A 7.1.1.1 Aufbau eines Directory-Datensatzes

Der Datensatz hat für alle implementierten Applikationen die gleiche Struktur und beinhaltet folgende Felder:

- L Längenindikator für APP-IDN
- APP-IDN Application Identifier
- APP-TXT Applikationsbezeichnung
- APP-STS Statusbyte für die Applikation

Der Applikation-Identifier kann für die in einer Multifunktions-Chipkarte implementierten Funktionen verschiedene Längen haben. Die Felder APP-TXT und APP-STS besitzen eine fixe Länge.

Der Längenindikator L für APP-IDN hat eine Länge von 1 Byte und ist binär kodiert.

A 7.1.1.2 Application Identifier (APP-IDN)

Der APP-IDN dient zur eindeutigen Identifizierung der implementierten Applikationen. Für die auf der Fernmeldedienstkarte implementierten Applikationen hat der APP-IDN eine Länge von 11 Byte und ist wie folgt aufgebaut.

Feld	Byte-Nr./ Länge	Kodierung	Werte (dez.)
Branchenhauptschlüssel	01 - 02 02 Byte	ASCII	89
Länderkennzeichen	03 - 04 02 Byte	ASCII	49 (gem. CCITT)
Applikationsnummer -Issuer	05 - 06 05 Byte -02 "	ASCII	01 (gem. CCITT)
-Dienstenr.	07 - 09 -03 "	ASCII	001 ÖKART 002 Btx 003 Netz C 004 RUFN+GEBZ
Softwareversion	10 - 11 02 Byte	ASCII	

Branchenhauptschlüssel : Schlüsselzahl gemäß ISO 7812 zur eindeutigen Kennzeichnung von Branchen.

Länderkennzeichen : Kennzeichnung des registrierenden Landes (gemäß CCITT)

Applikationsnummer: eindeutige Kennzeichnung für den Betreiber der Applikation.

Byte 5 und 6 Issuer
- 01 gemäß CCITT

Byte 7 bis 9 die Nummer des Dienstes
- 001 ÖKART
- 002 Btx
- 003 Netz C
- 004 RUFN+GEBZ

Softwareversion: Versionsnummer der Applikationssoftware

Die nachfolgende Abbildung zeigt die Stellung der einzelnen Felder im APP-IDN.

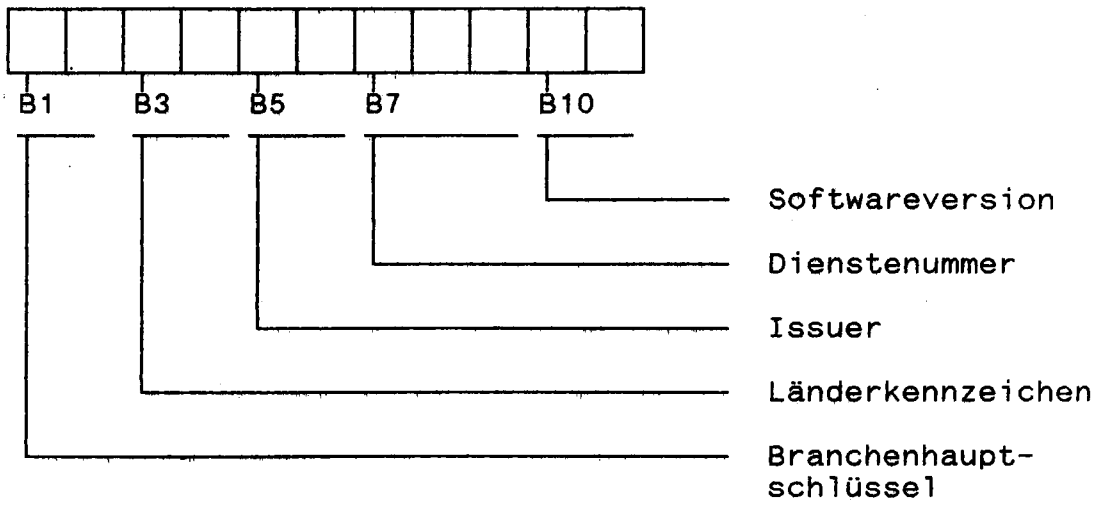


Bild A 7.3 Position der APP-IDN Felder

A 7.1.1.3 Applikationsbezeichnung (APP-TXT)

Inhalt: Name der Applikation
Länge: 20 Byte
Kodierung: ASCII

Z.Zt. sind für die Applikationen folgende Namen festgelegt:
ÖKART
Bildschirmtext
Netz C
Register ein/aus

A 7.1.1.4 Applikationsstatus (APP-STS)

Inhalt: Statusflags für die Applikation
Länge: 1 Byte
Kodierung: Der Aufbau des APP-STS ist der gleiche wie der des Applikation Return Codes. (siehe "Applikations Return Code (APRC)")

A 7.2 Applikationsabhängige Datenfelder

Auf die applikationsabhängigen Datenfelder wird nur zugegriffen, wenn die betreffende Applikation selektiert wurde.

Die Beschreibung der einzelnen spezifischen Datenfelder für die in der Multifunktions-Chipkarte implementierten Applikationen erfolgt im Anhang.

A 8 Zitierte und verwendete Unterlagen

ISO 7810, Identification cards - Physical characteristics.

ISO 7811, Identification cards - Recording technique
Part 1 - Part 5

ISO 7812, Identification cards - Numbering system and registration procedure for issuer identifiers.

ISO 7813, Identification cards - Finacial transaction cards.

ISO 7816-1 Identification cards - Integrated circuit(s) cards with contacts
Part 1: Physical characteristics

ISO 7816-2 Identification cards - Integrated circuit(s) cards with contacts
Part 2: Dimensions and locations of the contacts

ISO 7816-3 Identification cards - Integrated circuit(s) cards with contacts
Part 3: Electronic signals and exchange protocols

DIN 9752 Identifikationskarten, Begriffe und Einteilung

DIN 9781 Identifikationskarten aus Kunststoff oder kunststoff-laminiertem Werkstoff

B Netz-C spezifische Funktionen und Datenfelder

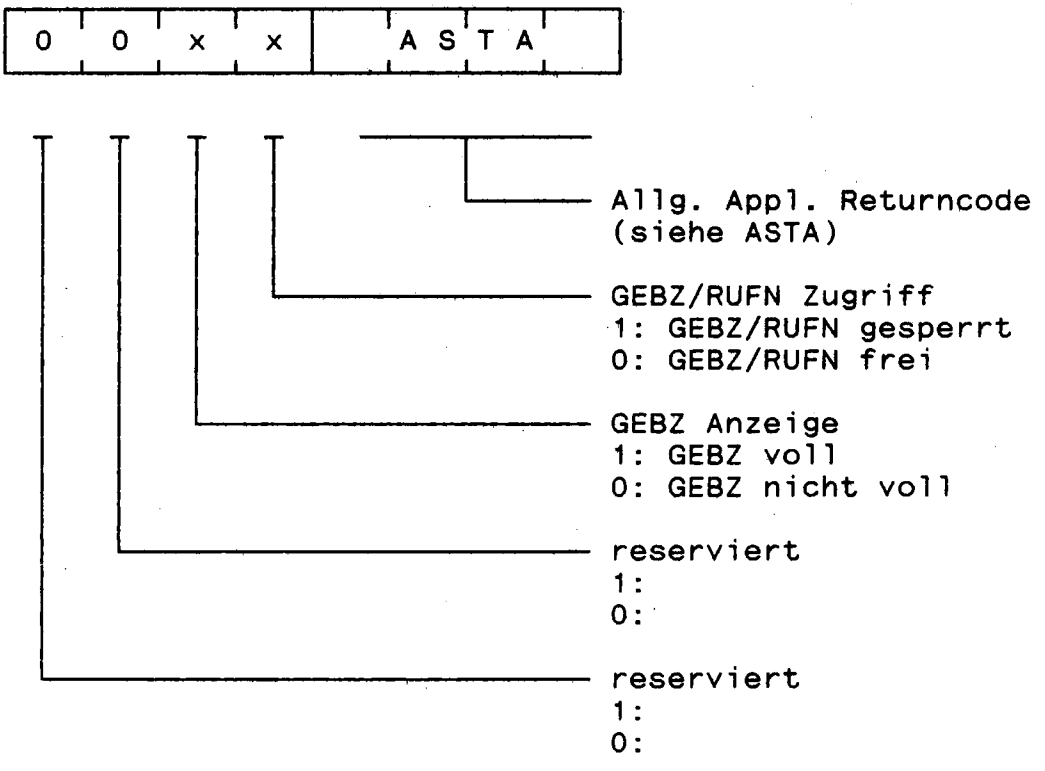
B 1 Applikations Status Spezifisch

Bei der Netz-C Applikation gelten folgende spezielle Returncodes im höherwertigen Halbbyte des APRC-Bytes:

Code	Bedeutung
1x	Gebührenzähler (GEBZ) für LESEN und LÖSCHEN gesperrt; Rufnummernverzeichnis RUFN gesperrt.
2x	Gebührenzähler voll

'x' Allgemeiner Applikationsreturncode ASTA

Die nachstehende Abbildung zeigt den Aufbau und die Kodierung des APRC bei der Netz-C Applikation.



```
0   0   0   1   x   x   x   x GEBZ/RUFN gesperrt
0   0   1   0   x   x   x   x GEBZ voll
```

Kommbinationen der einzelnen Bits sind ebenfalls möglich.

Beispiel:

```
0   0   0   0   x   x   x   x GEBZ/RUFN frei
                              GEBZ nicht voll
0   0   1   1   x   x   x   x GEBZ/RUFN gesperrt
                              GEBZ voll
```

Bild B 1.1 : ASTS NETZ-C-Applikation

Reservierte Bit sind nicht auszuwerten.

B 2 Definition der Netz-C Kommandos

Für die Multifunktions-Chipkarte gelten folgende, ausschließlich für das Netz-C bestimmte Kommandos:

Klasse	Befehl	Bedeutung
READ	RD-EBDT	Einbuchdaten lesen
	RD-RUFN	Satz aus Rufnummernverzeichnis lesen
	RD-GEBZ	Gebührenzähler lesen
WRTE	WT-RUFN	Satz in Rufnummernverzeichnis schreiben
EXEC	EH-GEBZ	Gebührenzähler erhöhen
	CL-GEBZ	Gebührenzähler löschen
AUTO	AUT-1	Autorisierung 1

B 2.1 Kodierung der Netz-C Kommandos

Die nachfolgende Tabelle zeigt die Kodierung der vereinbarten Kommandos für die Netz-C Anwendung:

Alle Code-Werte sind hexadezimal angegeben.

Kommando Name	Befehls Klasse	Bef. Code	Kommando Daten	Antwort Daten	s.auch RL Abschnitt
RD-EBDT	READ	01	--	Einbuchdaten	4.7.3.3
RD-RUFN	READ	02	Satz-Nr.	Rufnummernsatz	7.5
RD-GEBZ	READ	03	--	Gebühren	7.2
WT-RUFN	WRTE	01	Satz-Nr, Rufnr.,Text	--	7.5
EH-GEBZ	EXEC	01	Gebühren	--	5.1.3.3.5 7.2
CL-GEBZ	EXEC	02	--	--	7.2
AUT-1	AUTO	01	Autorisie-rungszahl	Autorisierungs-parameter	4.7.2.2

B 3 Beschreibung der Netz-C Kommandos

Nachfolgend werden die Kommandos und ihre Verwendung bei der Netz-C Applikation beschrieben.

B 3.1 RD-EBDT Einbuchdaten lesen

Mit diesem Kommando werden die Einbuchdaten von der Chipkarte gelesen.

Als Ergebnis werden der APRC und im Datenblock der Antwort die Einbuchdaten übertragen.

Der Aufbau der Einbuchdaten ist im Abschnitt B 4.1 näher beschrieben.

Beispiel:

CEG: Kommando ——> ICC		
SFLD		DLNG
CLA 05	INS 01	00

CEG <---------- Antwort :ICC			
SFLD		DLNG	DATA
CCRC xx	APRC xx	09	Einbuchdaten D-01|.....|D-09

B 3.2 RD-RUFN Rufnummernsatz lesen

Dieses Kommando wird nur ausgeführt, wenn der Zugriff auf das Rufnummernverzeichnis freigegeben ist.

Das Kommando liest einen Satz aus dem Rufnummernverzeichnis. Der zu lesende Satz wird durch die Kurzrufnummer (KRN) im ersten Datenbyte des Kommandos angegeben.

Als Ergebnis werden der APRC und im Datenblock der Antwort der ausgewählte Rufnummernsatz übertragen.

Wird die Kurzrufnummer 0 (Header) gelesen, so wird in der Antwort der APRC und der Header (Informationssatz für das Rufnummernverzeichnis) übertragen.

Ist das Rufnummernverzeichnis gesperrt, wird dies durch den APRC angezeigt. In diesen Fällen wird in der Antwort kein Datenblock übertragen.

Ist unter der ausgewählten Kurzrufnummer kein Rufnummernsatz gespeichert, wird der APRC und im Datenblock der Antwort der gewählte Rufnummernsatz mit der Leerkennung übertragen.

Der Aufbau des Rufnummernverzeichnisses sowie die Kodierung von Header und Rufnummersatz ist in Abschnitt C, Punkt 4.5.1 ff beschrieben.

Beispiel:

CEG : Kommando --> ICC			
SFLD		DLNG	DATA
CLA 05	INS 02	01	KRN D-01

CEG <---------- Antwort :ICC			
SFLD		DLNG	DATA
CCRC xx	APRC xx	18	Rufnummernsatz D-01|.....|D-18

B 3.3 WT-RUFN Rufnummernsatz schreiben

Dieses Kommando wird nur ausgeführt, wenn der Zugriff auf das Rufnummernverzeichnis freigegeben ist.

Mit diesem Kommando können Rufnummern im Rufnummerverzeichnis gespeichert werden. Kurzrufnummer, Rufnummer und Text werden im Datenblock des Kommandos der Chipkarte übergeben.

Rufnummer und Text werden unter dem über die Kurzrufnummer ausgewählten Rufnummernsatz gespeichert. Das diesem Rufnummernsatz entsprechende Bit in der Bitmap des Headers wird auf NULL gesetzt. Ist der ausgewählte Rufnummernsatz bereits belegt, wird dieser mit der übergebenen Rufnummer und dem Text überschrieben.

Zum Löschen eines Rufnummernsatzes ist dieser mit der Leerkennung (Rufnummer und Text) zu übergeben. Der über die Kurzrufnummer ausgewählte Rufnummernsatz wird gelöscht, das dem Rufnummernsatz entsprechende Bit in der Bitmap des Headers auf EINS gesetzt. Ist der ausgewählte Rufnummernsatz bereits mit einer Leerkennung versehen, werden diese Operationen nicht ausgeführt.

Das Ergebnis wird durch den APRC der Antwort angezeigt.

Die Kurzrufnummer 0 ist mit dem Header belegt und kann somit nicht mit einem Rufnummernsatz beschrieben werden (siehe Abschnitt C, Punkt 4.5.1.1)

Der Aufbau des Rufnummernverzeichnisses sowie die Kodierung von Header und Rufnummersatz ist in Abschnitt C, Punkt 4.5.1 ff beschrieben.

Beispiel:

CEG : Kommando ----------> ICC			
SFLD		DLNG	DATA
CLA 04	INS 01	19	KRN,RUFNUMMERNSATZ D-01|.....|D-19

CEG <---------- Antwort :ICC		
SFLD		DLNG
CCRC xx	APRC xx	00

B 3.4 EH-GEBZ Gebührenzähler erhöhen

Mit diesem Kommando wird der Gebührenzähler erhöht. Als Daten werden der Chipkarte die Anzahl der neu angefallenen Einheiten übergeben.

Das Ergebnis wird im APRC der Antwort angezeigt. Im Datenblock der Antwort werden keine weiteren Daten übertragen.

Ist der Gebührenzählerzähler voll, wird dies im APRC angezeigt. Werden auch nach der Meldung "Gebührenzähler voll" noch Einheiten zur Chipkarte übertragen, bleibt der Gebührenzähler auf seinem Endwert stehen. Dieser kann nur durch das Löschen des Gebührenzählers (CL-GEBZ) verlassen werden.

Beispiel:

CEG : Kommando --> ICC

SFLD		DLNG	DATA
CLA 06	INS 01	01	EINH D-01

CEG <---------- Antwort :ICC

SFLD		DLNG
CCRC xx	APRC xx	00

B 3.5 RD-GEBZ Gebührenzähler lesen

Das Kommando wird nur ausgeführt, wenn der Gebührenzähler für 'Lesen' freigegeben ist.

Das Lesen des Gebührenzählers wird durch das Kommando:

- SP-GZRV gesperrt und durch
- FR-GZRV freigegeben.

Das Kommando wird benutzt, um den auf der Chipkarte geführten Gebührenzähler zu lesen. Als Ergebnis wird der APRC und im Datenblock der Antwort die Summe der bisher aufgelaufenden Gebühreneinheiten übertragen.

Beispiel:

CEG: Kommando -> ICC		
SFLD		DLNG
CLA 05	INS 03	 00

CEG <---------- Antwort :ICC			
SFLD		DLNG	DATA
CCRC xx	APRC xx	 03	EINHEITEN D-01|.....|D-03

B 3.6 CL-GEBZ Gebührenzähler löschen

Das Kommando wird nur ausgeführt, wenn der Gebührenzähler für 'Löschen' freigegeben ist.

Das Löschen des Gebührenzählers wird durch das Kommando:

- SP-GZRV gesperrt und durch
- FR-GZRV freigegeben.

Mit diesem Kommando wird der auf der Chipkarte geführte Gebührenzähler für die aufgelaufenen Gebühreneinheiten gelöscht, d.h. auf den Wert NULL gesetzt.

Als Ergebnis wird der APRC übertragen.

Beispiel:

CEG: Kommando -> ICC		
SFLD		DLNG
CLA 06	INS 02	00

CEG <---------- Antwort :ICC		
SFLD		DLNG
CCRC xx	APRC xx	00

B 3.7 AUT-1 Autorisierung 1

Durch dieses Kommando wird die Chipkarte angewiesen, mit der im Datenblock des Kommandos übergebenen Autorisierungszahl (Zufallszahl etc.) eine Autorisierung durchzuführen.

Die Chipkarte ermittelt den Autorisierungsparameter und übergibt diesen im Datenblock der Antwort.

Die Autorisierungszahl und der Autorisierungsparameter sind binär kodiert.

Beispiel:

CEG : Kommando ----------> ICC			
SFLD		DLNG	DATA
CLA 07	INS 01	08	Autorisierungszahl D-01|.....|D-08

CEG <---------- Antwort :ICC			
SFLD		DLNG	DATA
CCRC xx	APRC xx	08	Autorisierungsparam D-01|.....|D-08

B 4 Datenfelder Netz-C

Für die Netz-C Anwendung werden zusätzlich folgende Datenfelder vereinbart:

Feld	Länge	Kodierung	
EBDT (Einbuchdaten)	9 Byte		siehe Aufbau der Einbuchdaten
GEBZ (Geb.-Zähler)	3 Byte	binär	Wertebereich 0 - 16.777.215
PLNG (PIN-Länge)	1 Byte	binär	Wertebereich 4 bis 8
PIN	8 Byte	ASCII	4- bis 8-stellig
AFBZ	1 Byte	binär	Endwert: z.Z. 3

B 4.1 Aufbau der Einbuchdaten

Das Feld Einbuchdaten hat eine Länge von neun Bytes und ist wie folgt aufgebaut:

Feld	Länge	Kodierung	
Rufnummer	24 Bit		
Sicherungscode	16 Bit	binär	
Kartenkennung	3 Bit	"	
Sonderheiten-schlüssel	13 Bit	"	
Wartungs-schlüssel	16 Bit	"	

Die nachfolgende Abbildung zeigt die Stellung der einzelnen Elemente im Datenfeld Einbuchdaten.

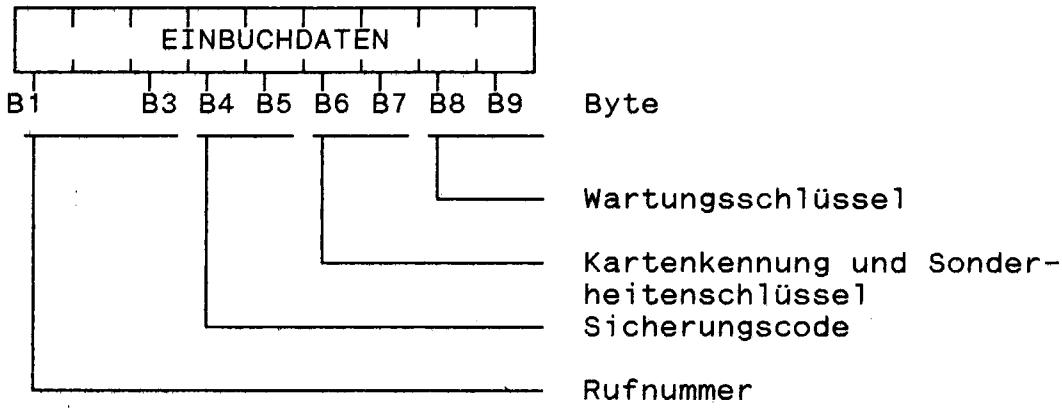


Bild B 4.1: Einbuchdaten

Die Einbuchdaten werden von links nach rechts, also in der Reihenfolge Byte 1 (B1) ... Byte 9 (B9) übertragen.

Nachfolgend werden die einzelnen Elemente der Einbuchdaten beschrieben.

Rufnummer

Die Rufnummer hat eine Länge von 24 Bit (3 Byte) und ist wie nachfolgend beschrieben kodiert.

Feld	Byte-Nr./ Länge		Kodierung	
FuTln-Nationalität	01	03 Bit	binär	Bit 8 - Bit 6
FuTln-Heimat-FuVSt-Nummer	01	05 Bit	binär	Bit 5 - Bit 1
FuTln-Restnummer	02 - 03	16 Bit	binär	

Die nachfolgende Abbildung zeigt die Kodierung der Rufnummer im Datenfeld Einbuchdaten.

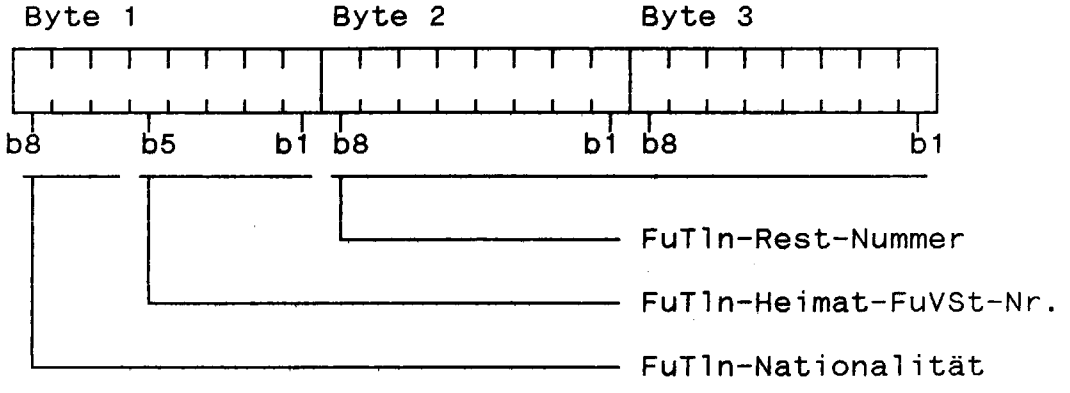


Bild B 4.2: Rufnummer im Datenfeld Einbuchdaten

Sicherungscode

Der Sicherungscode hat eine Länge von 16 Bit (2 Byte).

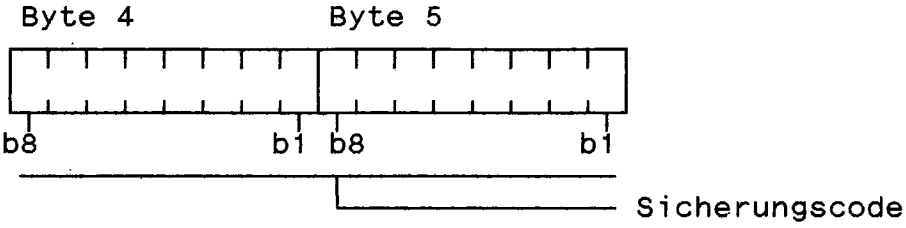


Bild B 4.3: Sicherungscode im Datenfeld Einbuchdaten

Kartenkennung und Sonderheitenschlüssel

Kartenkennung und Sonderheitenschlüssel haben eine Länge von 16 Bit (2 Byte) im Datenfeld Einbuchdaten.

Die nachfolgende Abbildung zeigt die Kodierung der Kartenkennung und des Sonderheitenschlüssels im Datenfeld Einbuchdaten.

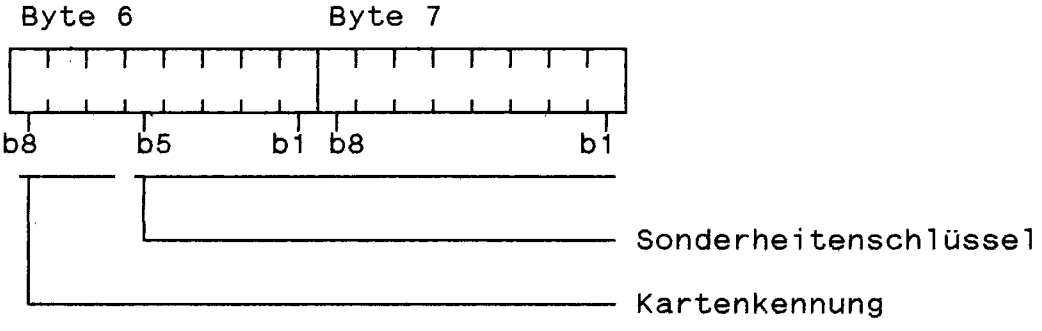


Bild B 4.4: Kartenkennung und Sonderheitenschlüssel im Datenfeld Einbuchdaten

Wartungsschlüssel

Der Wartungsschlüssel hat eine Länge von 16 Bit (2 Byte) im Datenfeld Einbuchdaten und ist binär kodiert.

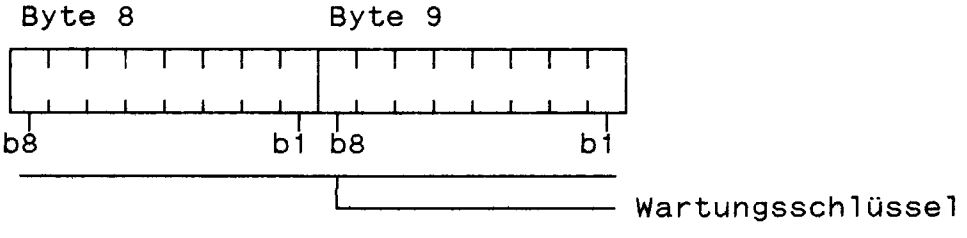


Bild B 4.5: Wartungsschlüssel im Datenfeld Einbuchdaten

B 4.2 Aufbau des Gebührenzählers

Das Feld für den Gebührenzähler hat eine Länge von drei Byte und ist binär kodiert.

Die nachfolgende Abbildung zeigt das Datenfeld Gebührenzähler mit dem Beispielwert für 10 Gebühreneinheiten.

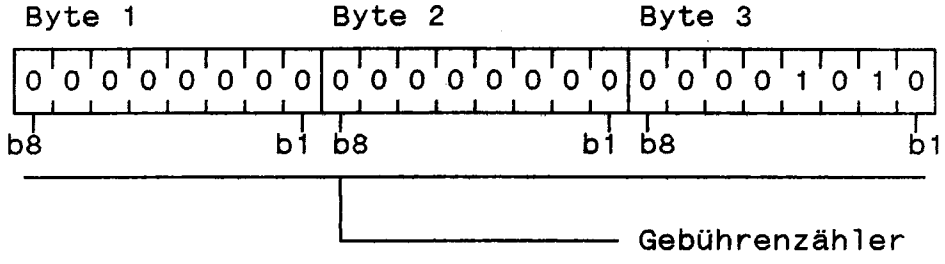


Bild B 4.6: Datenfeld für Gebührenzähler

B 4.3 PIN-Länge (PLNG)

Das Feld beinhaltet die Anzahl der Byte für die PIN. PLNG hat eine Länge von einem Byte und ist binär kodiert. Dieses Feld kann einen Wert von mindestens 4 bis maximal 8 enthalten.

B 4.4 PIN (Persönliche Identifikations-Nummer)

Dieses Feld enthält die Persönliche Identifikations-Nummer PIN des Karteninhabers für die Netz-C Applikation. Die PIN ist eine der PIN-Länge entsprechende 4- bis 8-stellige Zahl.

Die PIN ist in keinem Status auslesbar, kann jedoch durch den Befehl SET-PIN verändert werden.

Wird für diese PIN die System-PIN (SPIN) eingegeben, so hat das zur Folge, daß für die Netz-C Applikation der Status "PIN-Prüfung nicht erforderlich" besteht.

B 4.5 System-PIN (SPIN)

Die SPIN ist eine Konstante und hat den Wert 0000.

Wurde mit dem Kommando "SET-PIN" als "neue" PIN die spezielle System-PIN (SPIN) der selektierten Applikation übertragen, so wird nach erfolgreicher Verifizierung der "alten" PIN die PIN-Prüfung für diese Applikation deaktiviert. Dies bedeutet, daß für die weitere Benutzung dieser Applikation so lange keine PIN-Prüfung erforderlich ist, wie die SPIN als PIN in der Chipkarte gespeichert ist.

Wird innerhalb einer Applikation, für deren Zugang die PIN-Prüfung deaktiviert ist (PIN = SPIN), mit dem Kommando "SET-PIN" eine PIN eingegeben, die ungleich der SPIN ist, so wird diese PIN in das PIN-Feld übernommen und die PIN-Prüfung für diese Applikation aktiviert.

B 4.6 AFBZ (Applikations-Fehlbedienungszähler)

Das Feld Applikations-Fehlbedienungszähler (AFBZ) beinhaltet den Fehlbedienungszähler für die PIN der Applikation.

Der Endwert des AFBZ beträgt z. Zt. 3, was bedeutet, daß der Fehlbedienungszähler nach 3 falschen PIN-Eingaben den Wert Null erreicht hat, wodurch der Zugang zu dieser Applikation "gesperrt" ist. Dies wird durch das AFBZ-NULL-BIT angezeigt.

B 5 Autorisierungszahl und -parameter

Die Autorisierungszahl zur Berechnung des Autorisierungsparameters ist eine 8 Byte (64 Bit) lange Zufallszahl.

Der Autorisierungsparameter für das in dieser Applikation verwendete Sicherungsverfahren hat eine Länge von 8 Byte (64 Bit).

D-01 der Autorisierungszahl bzw. des Autorisierungsparameters (Anlage 1, Abschnitt B 3.7) entspricht Byte 8 der Funkdaten der Zufallszahl bzw. des Autorisierungsparameters (Abschnitt 5.1.3.2.1); D-02 entspricht Byte 7 usw.

B 6 Festlegung der Geräteadressen

Bezüglich der Geräteadressen für den Sender und Empfänger eines Request bzw. Response, die im 1. Byte des Übertragungsblockes (Abschnitt D 7.1.7) übertragen werden, gilt folgende Vereinbarung:

Geräteadresse:	'1 '	Chipkarte
	'3 '	Chipkarten-Endgerät

C RUFN + GEBZ spezifische Funktionen und Datenfelder

C 1 Applikations Status Spezifisch

Bei der RUFN + GEBZ Applikation gelten folgende spezielle Returncodes im höherwertigen Halbbyte des APRC-Bytes:

Code	Bedeutung
1x	Gebührenzähler (GEBZ) für LESEN und LÖSCHEN gesperrt; Rufnummernverzeichnis RUFN gesperrt.

'x' Allgemeiner Applikationsreturncode ASTA

Die nachstehende Abbildung zeigt den Aufbau und die Kodierung des APRC bei der RUFN + GEBZ Applikation.

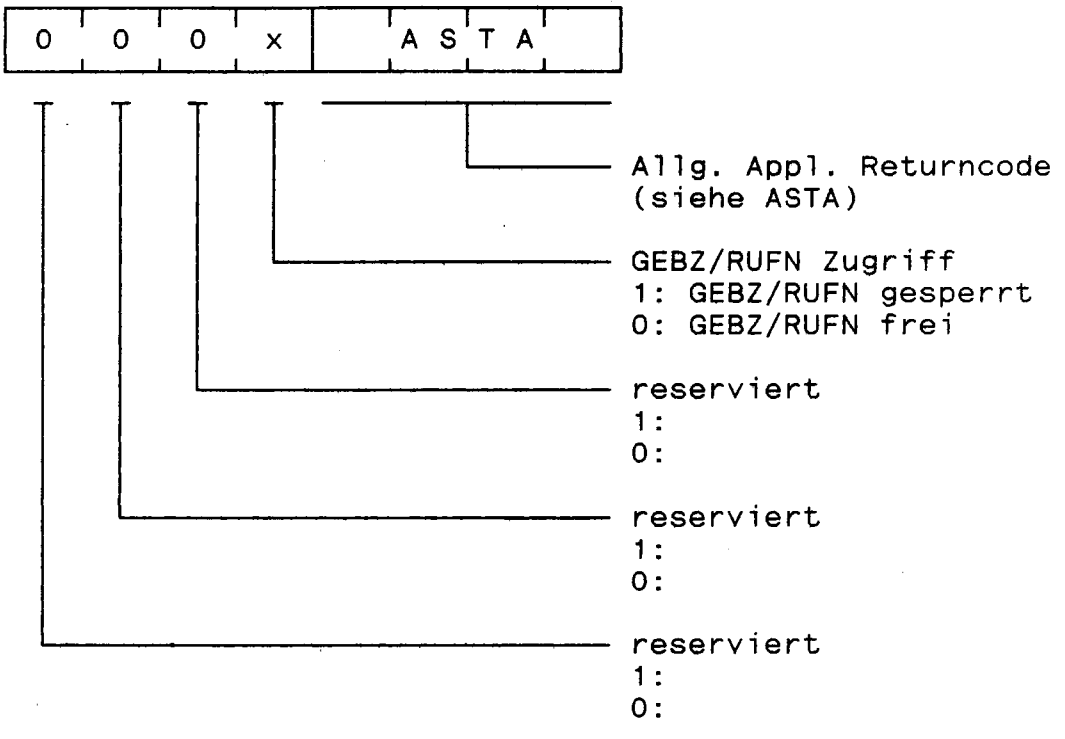


Bild C 1.1: ASTS RUFN+GEBZ Applikation

Reservierte Bit sind nicht auszuwerten.

C 2 Definition der RUFN+GEBZ Kommandos

Für die Multifunktions-Chipkarte gelten folgende, ausschließlich für die RUFN+GEBZ Anwendung bestimmte Befehle:

Klasse	Befehl	Bedeutung
EXEC	SP-GZRV	Gebührenzähler und Rufnummern-verzeichnis sperren.
EXEC	FR-GZRV	Gebührenzähler und Rufnummern-verzeichnis freigeben.

C 2.1 Kodierung der RUFN+GEBZ Kommandos

Die nachfolgende Tabelle zeigt die Kodierung der RUFN+GEBZ Kommandos:

Alle Code-Werte sind hexadezimal angegeben.

Kommando Name	Befehls Klasse	Bef. Code	Kommando Daten	Antwort Daten	s.auch RL Abschnitt
SP-GZRV	EXEC	01	--	APRC	7.2 7.5
FR-GZRV	EXEC	02	--	APRC	7.2 7.5

C 3 Beschreibung der RUFN+GEBZ Kommandos

Nachfolgend werden die Kommandos und ihre Verwendung bei der RUFN+GEBZ Applikation beschrieben.

C 3.1 SP-GZRV Zugriff auf Gebührenzähler und Rufnummernverzeichnis sperren

Mit diesem Kommando wird der Zugriff auf den Gebührenzähler und das Rufnummernverzeichnis gesperrt.

Der Gebührenzähler wird für die Kommandos

- Gebührenzähler lesen (RD-GEBZ) und
- Gebührenzähler löschen (CL-GEBZ)

gesperrt. Das Erhöhen des Gebührenzählers (EH-GEBZ) wird von diesem Kommando nicht geperrt.

Das Rufnummernverzeichnis wird für die Kommandos

- Rufnummernsatz lesen (RD-RUFN) und
- Rufnummernsatz schreiben (WT-RUFN)

gesperrt.

Die mit diesem Kommando gesetzte Sperre gilt für alle auf der Chipkarte implementierten Applikationen.

Als Ergebnis wird der APRC übertragen.

Beispiel:

CEG: Kommando -> ICC

SFLD		DLNG
CLA 06	INS 01	00

CEG <---------- Antwort :ICC

SFLD		DLNG
CCRC xx	APRC xx	00

C 3.2 FR-GZRV Zugriff auf Gebührenzähler und Rufnummernverzeichnis freigeben

Dieses Kommando hebt die durch das Kommando SP-GZRV gesetzten Sperren für den Gebührenzähler sowie für das Rufnummernverzeichnis auf.

Der Gebührenzähler wird für die Kommandos

- Gebührenzähler lesen (RD-GEBZ) und
- Gebührenzähler löschen (CL-GEBZ)

freigegeben.

Das Rufnummernverzeichnis wird für die Kommandos

- Rufnummernsatz lesen (RD-RUFN) und
- Rufnummernsatz schreiben (WT-RUFN)

freigegeben.

Die mit diesem Kommando erfolgte Freigabe gilt für alle auf der Chipkarte implementierten Applikationen.

Als Ergebnis wird der APRC übertragen.

Beispiel:

CEG: Kommando -> ICC		
SFLD		DLNG
CLA 06	INS 02	00

CEG <---------- Antwort :ICC		
SFLD		DLNG
CCRC xx	APRC xx	00

C 4 Datenfelder RUFN+GEBZ

Für die RUFN+GEBZ Anwendung werden folgende Datenfelder definiert:

Feld	Länge	Kodierung	
PLNG (PIN-Länge)	1 Byte	binär	Wertebereich 4 - 8
PIN	xx Byte	ASCII	4- bis 8-stellig
AFBZ	1 Byte	binär	Endwert: z.Z. 3
Rufnummern-speicher - Header	24 Byte	binär bitmap	Byte 1 max. Ruf-nr.-Sätze($0-$B8) Byte 2 - 24 Anzeige freier und bel. Sätze
- Rufnummern satz	24 Byte	BCD ASCII	Rufnummer Byte 1 - 8 Name Byte 9 - 24

C 4.1 PIN-Länge (PLNG)

Das Feld beinhaltet die Anzahl der Byte für die PIN. PLNG hat eine Länge von einem Byte und ist binär kodiert. Dieses Feld kann einen Wert von mindestens 4 und maximal 8 enthalten.

C 4.2 PIN (Persönliche Identifikations-Nummer)

Dieses Feld enthält die Persönliche Identifikations-Nummer PIN des Karteninhabers für die RUFN+GEBZ-Applikation. Die PIN ist eine der PIN-Länge entsprechende 4- bis 8-stellige Zahl.

Die PIN ist in keinem Status auslesbar, kann jedoch geändert werden.

Wird für diese PIN die System-PIN (SPIN) eingegeben, so hat das zur Folge, daß für die RUFN+GEBZ Applikation der Status "PIN-Prüfung nicht erforderlich" besteht.

C 4.3 System-PIN (SPIN)

Die SPIN ist eine Konstante und hat den Wert 0000.

Wurde mit dem Kommando "PIN-SET" als "neue" PIN die spezielle System-PIN (SPIN) der selektierten Applikation übertragen, so wird nach erfolgreicher Verifizierung der "alten" PIN die PIN-Prüfung für diese Applikation deaktiviert. Dies bedeutet, daß für die weitere Benutzung dieser Applikation so lange keine PIN-Prüfung erforderlich ist, wie die SPIN als PIN in der Chipkarte gespeichert ist.

Wird innerhalb einer Applikation, für deren Zugang die PIN-Prüfung deaktiviert ist (PIN = SPIN), mit dem Kommando "PIN-SET" eine PIN eingegeben, die ungleich der SPIN ist, so wird diese PIN in das PIN-Feld übernommen und die PIN-Prüfung für diese Applikation aktiviert.

C 4.4 AFBZ (Applikations-Fehlbedienungszähler)

Das Feld Applikations-Fehlbedienungszähler (AFBZ) beinhaltet den Fehlbedienungszähler für die PIN der Applikation. Der AFBZ hat z.Zt. den Endwert 3. Bei nicht erfolgreicher PIN-Prüfung wird der AFBZ um eins dekrementiert. Erreicht der AFBZ durch das Dekrementieren den Wert NULL, wird dieses im CCRC angezeigt. In diesem Fall ist eine erneute PIN-Prüfung erst dann möglich, wenn der AFBZ an einem Postserviceterminal auf seinen Endwert zurückgesetzt wurde.

Eine erfolgreiche PIN-Prüfung setzt den AFBZ auf seinen Endwert, wenn dieser noch nicht den Wert NULL erreicht hat.

C 4.5 Rufnummernverzeichnis

Die Multifunktions-Chipkarte beinhaltet Datenfelder zur Speicherung von Datensätzen, die Rufnummern mit den zugehörigen optionalen Texten beinhalten. Diese Sätze stellen das Rufnummernverzeichnis der Chipkarte dar.

Die maximale Anzahl der Rufnummersätze, die gespeichert werden können, ist von der Chipkarte abhängig und wird im Header-Satz des Rufnummernverzeichnis angezeigt.

Das Rufnummernverzeichnis enthält mindestens einen Satz, den Header-Satz.

Der Zugriff auf dieses Verzeichnis ist abhängig von der jeweiligen Applikation.

Das Rufnummernverzeichnis kann in der Applikation "RUFN+GEBZ" für Zugriffe (Lesen und Schreiben) gesperrt und freigegeben werden. Die Sperre bzw. die Freigabe gilt dann für alle auf der Chipkarte implementierten Applikationen, die Zugriff auf das Rufnummernverzeichnis haben.

C 4.5.1 Aufbau des Rufnummernverzeichnis

Das Rufnummernverzeichnis besteht aus dem Informationssatz (Header,Rufnummernsatz 0) für das Verzeichnis, und den Rufnummernsätzen zur Speicherung von Rufnummern und Namen.

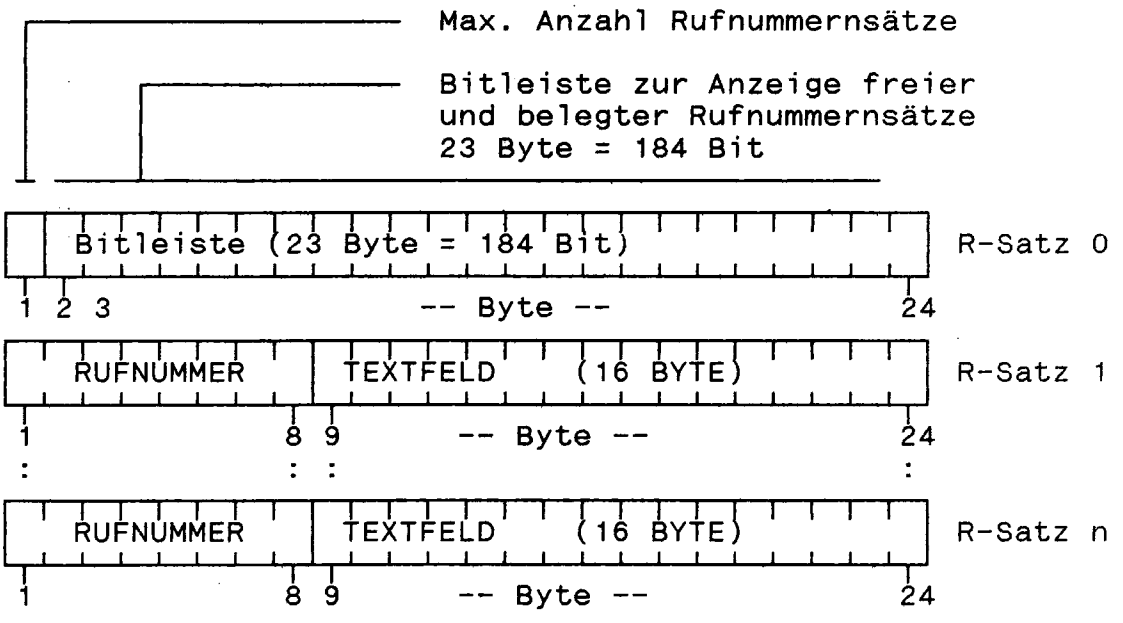


Bild C 4.1: Rufnummernverzeichnis

C 4.5.1.1 Header

Der Header beinhaltet die Information über die Größe und Belegung des Rufnummernverzeichnisses. Dieser Satz ist der 1. Satz des Verzeichnisses und unter der Satznummer 0 (Kurzrufnummer 0) abgelegt.

Der Header hat eine Länge von 24 Byte und ist wie folgt aufgebaut:

Feld	Byte-Nr./	Länge	Kodierung	Inhalt
Max. Anzahl Rufnr.-sätze	01	01 Byte	binär	$00 - $B8
Bitleiste zur Anzeige freier und belegter Rufnr.-Sätze	02 - 24	23 Byte	binär	'1'- Satz frei '0'- Satz belegt

Die nachfolgende Abbildung zeigt die Stellung der Felder im Header-Satz des Rufnummernverzeichnisses:

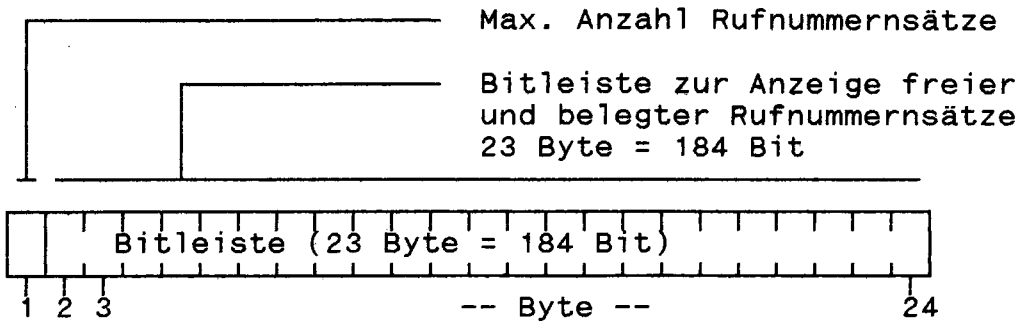
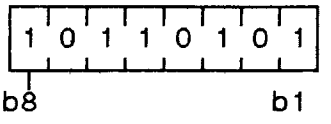


Bild C 4.2: Header

Der 1. Rufnummernsatz wird durch das höchstwertige Bit (Bit: 8) in Byte 2 (Kurzrufnummer 1), der letzte Rufnummernsatz (max: 184) durch das niederwertigste Bit (Bit: 1) in Byte 24 des Header repräsentiert.

Das nachfolgende Beispiel zeigt den Header bei:

- 181 ($B5) max. speicherbaren Rufnr.-Sätzen
- 3 ($03) belegten Rufnummernsätzen



Byte 1: max. 181 Rufnr.-Sätze

Byte 2 bis Byte 24:
Bitmap zur Anzeige der freien und belegten Rufnummernsätze.
- '1' Rufnummernsatz frei
- '0' Rufnummernsatz belegt
- 'X' nicht definiert

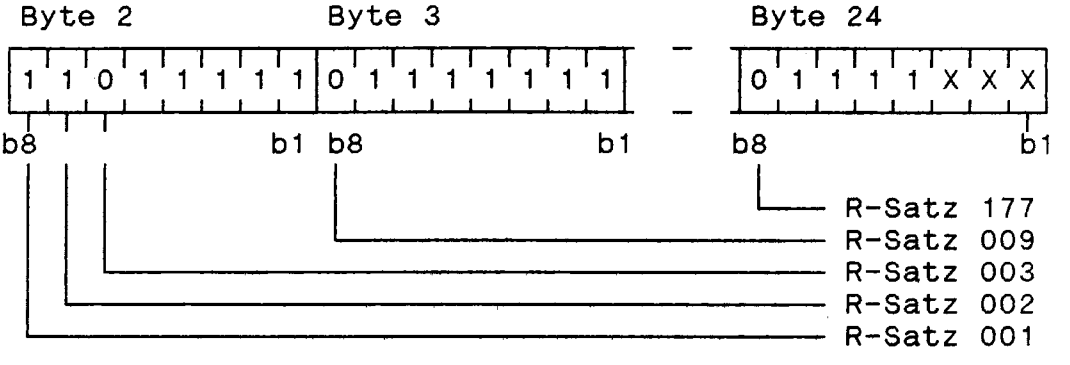


Bild C 4.3: Belegungsbeispiel Header

C 4.5.1.2 Rufnummernsatz

Ein Rufnummernsatz besteht aus der Rufnummer und dem zugehörigen, optionalen Text (Name etc.) für die Rufnummer. Ein Rufnummernsatz hat eine Länge von 24 Byte.

Feld	Byte-Nr./	Länge	Kodierung	Inhalt
Rufnummer	01 - 08	08 Byte	BCD	$FFFFFF0610335205
Text	09 - 24	16 Byte	ASCII	MUSTERMANN

Rufnummer

Die Rufnummer ist rechtsbündig im Feld 'Rufnummer' gespeichert und links mit 'F'(hex) aufgefüllt. Bei einem leeren bzw. gelöschten Rufnummernsatz ist die Rufnummer (Byte 1 bis Byte 8) mit 'F'(hex) besetzt.

Die Rufnummer kann neben den Wahlziffern 0 bis 9 auch aus den in Abschnitt 5.1.3.3.16 angegebenen Wahlziffern mit den entsprechenden Codierungen bestehen. Entspricht ein aus der BK gelesenes Zeichen nicht den Wahlziffern, so ist dieses Zeichen durch das Zeichen "?" darzustellen.

Text

Der Text ist linksbündig im Feld 'Text' gespeichert und rechts mit 'blank' ($20) aufgefüllt. Bei einem leeren bzw. gelöschten Rufnummernsatz ist der Text (Byte 9 bis Byte 24 mit 'blank' ($20) besetzt.

Die der BK übergebenen Daten sind in ASCII nach DIN 66003 zu kodieren, wobei die Deutsche Referenz-Version (mit Umlauten) zu verwenden ist. Es dürfen nur die darstellbaren Zeichen ($20 bis $7E) genutzt werden, wobei nicht der vollständige Zeichensatz verwendet werden muß. Kann ein von der BK gelesenes Zeichen nicht angezeigt werden, so ist dieses Zeichen entweder durch ein äquivalentes Zeichen (a = A, ä = ae) oder durch ein Blank zu ersetzen.

Nachfolgend werden die Stellung der Felder im Rufnummernsatz dargestellt und Beispiele für einen belegten sowie einen leeren Rufnummernsatz gezeigt.

Rufnummernsatz:

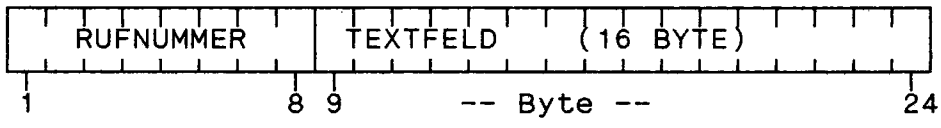


Bild C 4.4: Rufnummernsatz

Rufnummernsatz belegt:

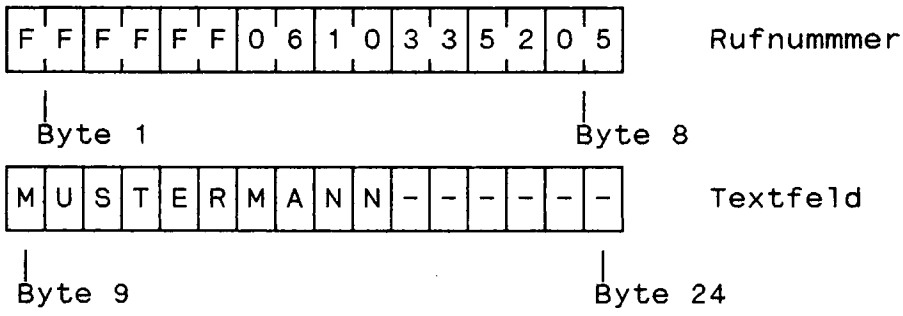


Bild C 4.5: Rufnummernsatz belegt

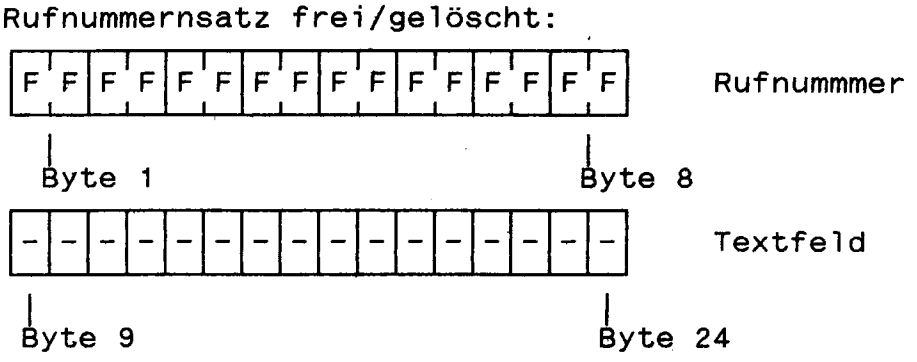


Bild C 4.6: Gelöschter bzw. freier Rufnummernsatz

C 5 Festlegung der Geräteadressen

Für die Geräteadressen des Senders und des Empfängers eines Request bzw. Response, die im 1. Byte des Übertragungsblockes (Schicht 2, Anhang C 4.1.1) übertragen werden, gelten folgende Vereinbarungen:

Geräteadresse:	'1 '	Chipkarte
	'3 '	Chipkarten-Endgerät

D Chipkarten-Blockübertragungsprotokoll

D 1 Allgemeines

D 1.1 Einleitung (gemäß ISO 7816-3)

Diese Norm beschreibt Eigenschaften, Parameter und den Gebrauch von Chipkarten mit Kontakten (ICC, Integrated Circuit Cards). Diese Chipkarten sind Identifikationskarten und werden für den Informationsaustausch, welcher zwischen der Kartenumgebung und dem in der Karte vorhandenen integrierten Schaltkreis (IC) ausgehandelt wird. Als Ergebnis dieses Informationsaustausches liefert die Karte Daten, beispielsweise Berechnungsresultate, oder darin gespeicherte Informationen und/oder modifiziert die in ihr gespeicherten Daten oder Zustände.

D 1.2 Geltungs- und Anwendungsbereich

Diese Norm spezifiziert sowohl elektrische Eigenschaften als auch Kommunikationsprotokolle für die Kommunikation zwischen Chipkarte (ICC) und Chipkartenzugangsgerät (Interface Device ID) dar. Dabei wird den Konfigurationsmöglichkeiten Rechnung getragen, daß das ID entweder als Stand-alone-Gerät über eine in dieser Norm nicht festgelegte Schnittstelle mit einem lokalen Datenendgerät LD (siehe Bild D 1.1) verbunden ist oder in einem LD integriert ist. Die Kombination von ID und LD heißt Chipkarten-Endgerät (CEG). Außerdem berücksichtigt diese Norm, daß ein entferntes, über ein Netz mit dem LD verbundenes Datenendgerät (RD) mit der Chipkarte kommunizieren kann, ohne daß hierbei das LD das End-To-End-Protokoll zwischen Chipkarte und dem RD kennen muß, das heißt, eine Protokollumwandlung vornehmen muß.

Die Kommunikationsprotokolle werden schichtenweise (gemäß OSI-Referenzmodell, siehe Bild D 1.2 für Anwendungen mit lokalen Datenendgeräten und Bild D 1.3 für Anwendungen mit entfernten Datenendgeräten) beschrieben, sodaß eine weitestgehende Unabhängigkeit zwischen Anwendung und der reinen Datenübertragung erzielt wird. Außerdem wird somit auch eine Möglichkeit für ein zukünftiges Einbringen von stabil gewordenen ISO-Normen (auch schichtenweise) geschaffen, die, soweit sie die bis dahin in Betrieb gegangenen Anwendungen nicht betreffen, letztere unangetastet lassen können.

Da es aus der Sicht der Chipkarte unerheblich ist, ob ID und LD separate Geräte oder in einem CEG enthalten sind, wird aus Vereinfachungsgründen im weiteren nur noch von der Kombination aus ID und LD, also dem Chipkarten-Endgerät CEG gesprochen.

Grundsätzlich ist diese Norm auch für kontaktlose Chipkarten verwendbar, wenn das Kapitel D 4 sowie die Abschnitte D 5.1 und D 5.5 aus Kapitel D 5 dahingehend modifiziert werden.

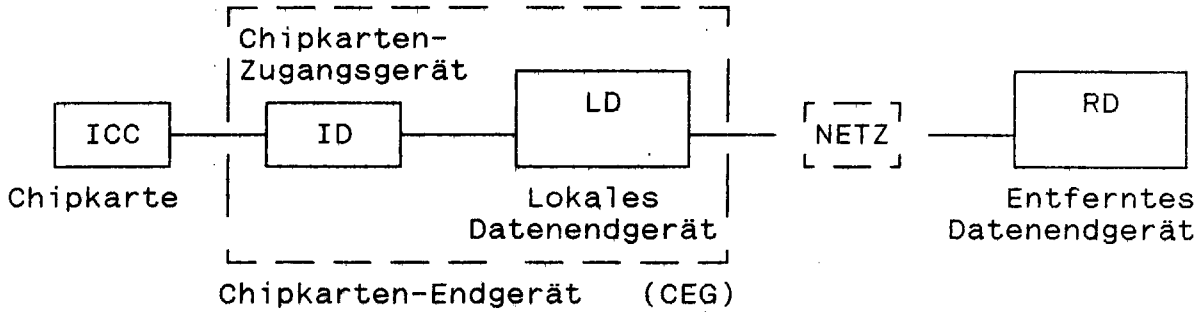


Bild D 1.1: Gerätekonfiguration bei der Kommunikation mit Chipkarten

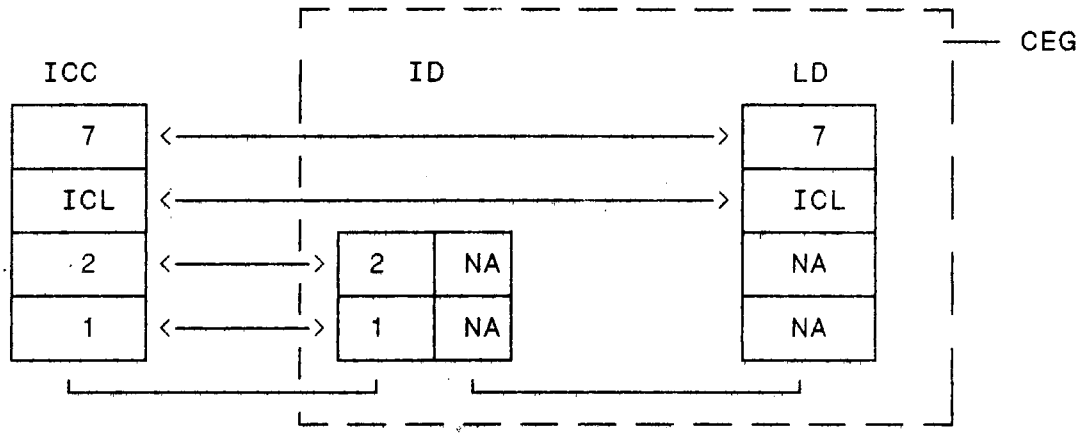


Bild D 1.2: Schichtenarchitektur der Kommunikation zwischen Chipkarte und einem lokalen Endgerät

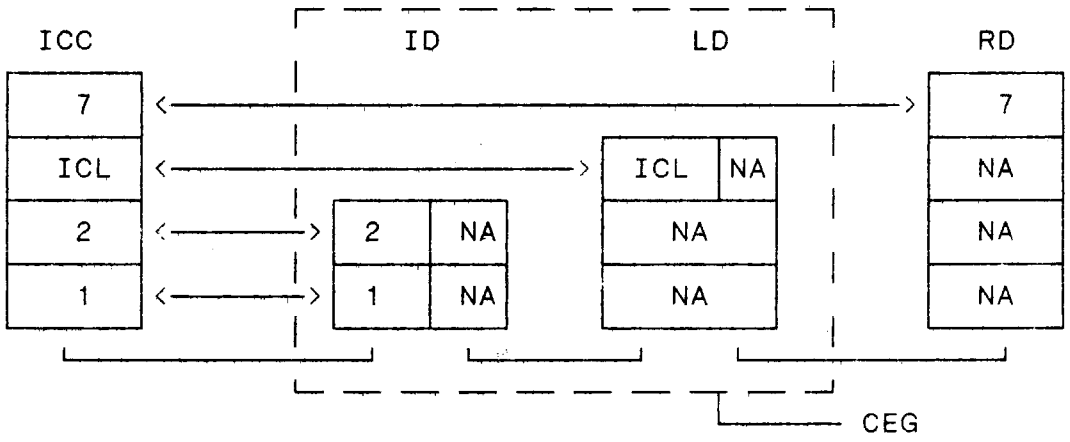


Bild D 1.3: Schichtenarchitektur der Kommunikation zwischen Chipkarte und einem entfernten Endgerät

Anmerkung: NA = nicht Gegenstand dieser Norm (not applicable)
ICL = Interface Control Layer

D 2 Referenznormen (gemäß ISO 7816-3)

D 3 Definitionen (gemäß ISO 7816-3)

Der Begriff Identifikationskarte ist in ISO 7810 definiert.

Chipkarten-Zugangseinrichtung: ein Endgerät oder Kommunikationsgerät, an das eine Chipkarte während ihres Betriebs elektrisch verbunden ist.

D 4 Elektrische Eigenschaften der Kontakte

D 4.1 Elektrische Funktionen (gemäß ISO 7816-3)

D 4.2 Spannungs- und Stromwerte (gemäß ISO 7816-3)

D 4.2.1 Abkürzungen (gemäß ISO 7816-3)

D 4.2.2 I/O (gemäß ISO 7816-3)

D 4.2.3 VPP (gemäß ISO 7816-3)

D 4.2.4 CLK (gemäß ISO 7816-3)

D 4.2.5 RST (gemäß ISO 7816-3)

D 4.2.6 VCC (gemäß ISO 7816-3)

D 5 Betriebliche Eigenschaften für Chipkarten (gemäß ISO 7816-3)

D 5.1 Verbindung und Aktivierung der Kontakte (gemäß ISO 7816-3)

D 5.2 Chipkarten-Reset (gemäß ISO 7816-3)

D 5.3 Answer to Reset (gemäß ISO 7816-3)

ISO-kompatible Abweichungen werden in Kapitel 6 beschrieben.

D 5.4 Informationsaustausch (gemäß ISO 7816-3)

D 5.5 Deaktivierung der Kontakte (gemäß ISO 7816-3)

D 6 Answer to Reset, Bitübertragungsprotokoll (Schicht 1)

Dieses Kapitel beschreibt die Reaktion der Chipkarte (ICC) auf einen physikalischen Karten-Reset durch das Chipkarten-Endgerät (CEG). Der prinzipielle Aufbau der Reaktion und deren Semantik erfolgt nach ISO 7816-3, so daß die Reaktion jeder Chipkarte vom CEG ausgewertet werden kann, die sich nach dieser Norm richtet.

Nach einem Reset wird von der ICC eine Folge von Datenbytes (Characters), der "Answer to Reset", übertragen. Der Answer to Reset (ATR) enthält die Parameter für mindestens ein mögliches Übertragungsprotokoll für die dann folgende Kommunikation.

Der ATR ist folgendermaßen gegliedert:

- Global Characters (immer vorhanden)
  - TS
  - T0
- Global Interface Characters (optional)
  - TA1
  - TB1
  - TC1
  - TD1
- Protocol Specific Interface Characters (optional)
  - TAi (i = 2,3,...,n)
    :
  - TDi
- Historical Characters (optional)
  - T1
    :
  - T15

Unmittelbar auf den ATR folgt:

- Checkbyte für die Answer-to-Reset-Sequenz
  - TCK

Die grundsätzliche Struktur der ATR-Sequenz erlaubt es der ICC dem CEG zu signalisieren, daß sie für die nachfolgende Kommunikation mehrere Übertragungsprotokolle mit unterschiedlichen protokollspezifischen Parametern beherrscht.

Der ATR hat eine maximale Länge von 32 Bytes. Durch das Byte TD1 (T=15) kann dem CEG jedoch signalisiert werden, daß mehr als 32 Byte übertragen werden. Im Falle T=15 in TD1 wird das erste oder einzige in der ICC verfügbare Übertragungsprotokoll in TD2 signalisiert. Die genaue Festlegung ist von der ISO noch nicht verabschiedet worden.

Zusätzliche auf Answer to Reset folgende Byte werden vom CEG ignoriert bzw. wird deren Bedeutung hier nicht festgelegt mit der

Ausnahme, daß das erste oder einzige auf Answer to Reset folgende Byte die Bedeutung des Checkbytes TCK hat (siehe D 6.6). Es obliegt dem CEG, ob TCK ausgewertet oder ignoriert wird.

Falls mehr als insgesamt 33 Byte im Answer to Reset von der ICC gesendet worden sind, gilt dies als Fehler. Das CEG führt in diesem Fall erneut ein Reset durch.

D 6.1 Physikalischer Karten-Reset

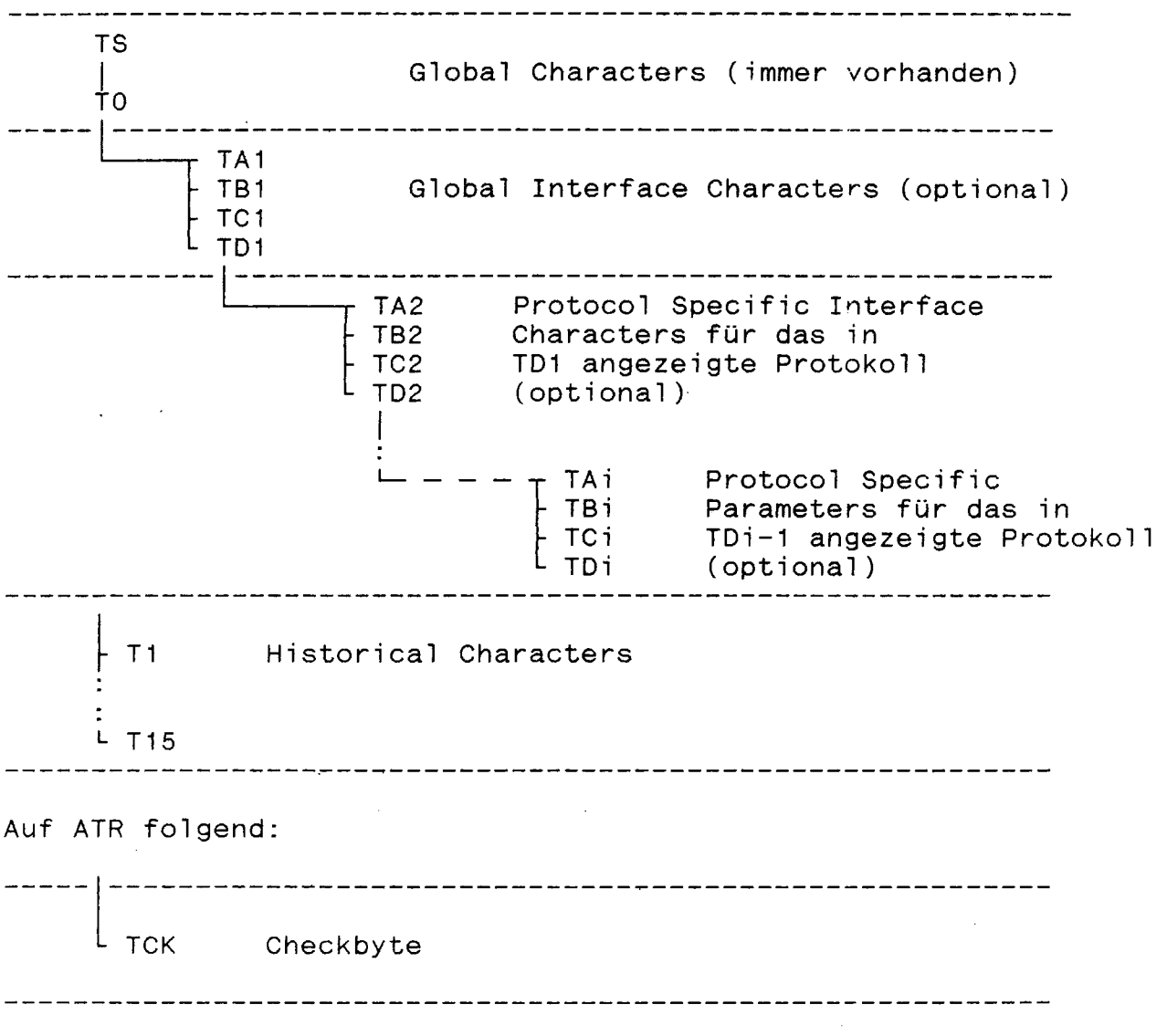


Bild D 6.1: Aufbau der ATR-Sequenz

D 6.2 Global Characters

Byte TS und Byte T0 des ATR werden als Global Characters bezeichnet und von der ICC im ATR immer übertragen. Diese Bytes haben folgende Bedeutung:

- TS Initial Character
- T0 Format Character.

D 6.2.1 TS, Initial Character (gemäß ISO 7816-3)

Dieses Zeichen bestimmt das Datenformat für die Byteübertragung und beinhaltet zwei mögliche Werte für

- Direct conventions : LSB first (Bit 1)
- Inverse conventions : MSB first (Bit 8).

D 6.2.2 T0, Format Character (gemäß ISO 7816-3)

Durch T0 wird angezeigt, welche weiteren Bytes (Global Interface Characters, Historical Characters) im ATR übertragen werden.

Das niederwertige Halbbyte (Bits: b1-b4) bestimmt die Anzahl k der Historical Characters (T1-Tk), die übertragen werden.

Das höherwertige Halbbyte (Bits: b5-b8) gibt an, welche Global Interface Characters TA1-TD1 nachfolgen. In Abhängigkeit des jeweiligen Bit-Wertes wird das entsprechende Byte übertragen oder nicht:

"1" = wird übertragen;
"0" = wird nicht übertragen.

Dabei wird TA1 durch Bit b5, TB1 durch Bit b6, TC1 durch Bit b7 und TD1 durch Bit b8 repräsentiert (siehe Bild D 6.2).

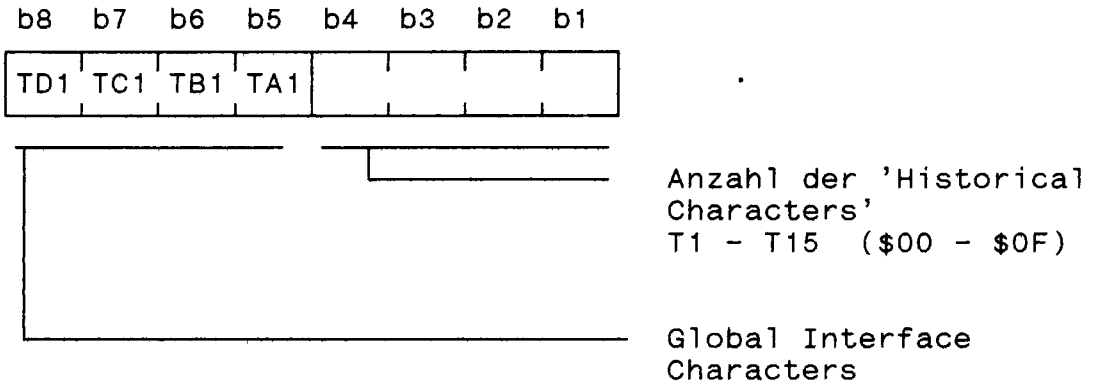


Bild D 6.2: Kodierung von T0

D 6.3 Global Interface Characters

Die Global Interface Characters TA1, TB1, TC1 und TD1 beinhalten die Information für das CEG und werden gemäß ISO 7816-3 benutzt.

D 6.3.1 TA1 (gemäß ISO 7816-3)

D 6.3.2 TB1, Programmierspannung (gemäß ISO 7816-3)

TB1

Legt bei Notwendigkeit einer zusätzlichen Programmierspannung (Vpp) die Höhe von Vpp fest. Es wird eine Programmierspannungsgenauigkeit von 4 % unterstellt.

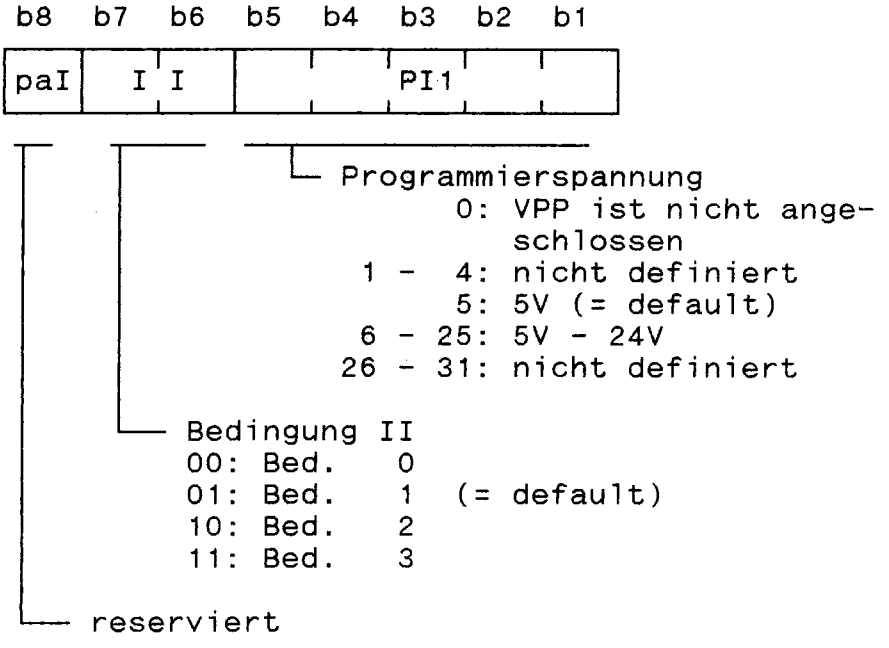


Bild D 6.3: Kodierung von TB1

D 6.3.3 TC1 (gemäß ISO 7816-3)

D 6.3.4 TD1 und TDi (i=2,3,...), Protokoll- und Folgebyteanzeige

TDi b1-b4 (i=1,2,...)

Durch das niederwertige Halbbyte in TDi (i=1,2,...) wird der für die weitere Kommunikation benutzte Protokolltyp T bestimmt. Folgende Festlegungen sind nach ISO 7816-3 getroffen worden:

T = 0	Byte-Übertragungsprotokoll (ISO 7816-3, Kapitel 8)
T = 1	Block-Übertragungsprotokoll (ISO 7816-3, Kapitel 9)
T = 2-3	Reserviert für zukünftige 'full duplex' Anwendungen
T = 4-13	Reserviert für zukünftige Anwendungen (Protokolle)
T = 14	Privat Use Protocol (kein ISO-Standard)

T = 15 reserviert für zukünftige Erweiterungen.

Die auf TDi folgenden protokollspezifischen Parameter TAi+1, TBi+1, TCi+1 beziehen sich auf den in TDi signalisierten Protokolltyp T.

Wird in TDi der gleiche Protokolltyp T wie in TDi-1 angezeigt, so beziehen sich die protokollspezifischen Parameter TAi+1, TBi+1, TCi+1 auch auf den in TDi-1 angezeigten Protokolltyp.

Wenn folgende TDi-Characters unterschiedliche Werte T enthalten, heißt dies, daß die ICC mehrere Protokolle (entsprechend dem Typ nach Wert T) zu bearbeiten fähig ist. Dabei ist zu beachten, daß der Protokolltyp T=0 als erster in der ATR-Sequenz signalisiert werden muß, falls mehrere Protokolle (darunter auch das Protokoll gemäß T=0) von der ICC unterstützt werden.

TDi b5-b8 (i=1,2,...) Das höherwertige Halbbyte in TDi gibt an, welche protokollspezifischen Parameter in TAi+1 (Bit b5), TBi+1 (Bit b6), TCi+1 (Bit b7) und der Interface Character TDi+1 (Bit b8) nachfolgen.

D 6.4 Protocol Specific Interface Characters

Die protokollspezifischen Parameter TAi, TBi, TCi (i=2,3,...) beinhalten Informationen für den in TDi-1 bestimmten Protokolltyp T.

D 6.4.1 Interface Characters für alle Protokolltypen

D 6.4.1.1 TB2 (gemäß ISO 7816-3)

D 6.4.2 Interface Characters für den Protokolltyp T=0

D 6.4.2.1 TC2 (gemäß ISO 7816-3)

D 6.4.3 Interface Characters für den Protokolltyp T=1

D 6.4.3.1 TA2 (gemäß ISO 7816-3)

Falls in TD1 der Protokolltyp T=14 signalisiert wird, hat der Parameter in TA2 keine Bedeutung. TA2 darf in diesem Fall weder gesendet werden, noch hat sein Default-Wert eine Bedeutung.

D 6.4.4 Interface Characters für den Protokolltyp T=14

Die Parameter speziell für den Protokolltyp T=14 werden mittels Interface Characters mit Index i>2 signalisiert.

Wenn nur der Protokolltyp T=14 signalisiert wird, enthalten TD1, TD2 und auf Bedarf weitere folgende TDi mit i>2 den Wert T=14.

Im folgenden bezeichnet:

fo: die Referenzfrequenz für eine Übertragungsrate von 4800 Baud (die Frequenz fo ist definiert mit 2.4576 MHz) und

fs: die Betriebsfrequenz nach Übertragung des Answer to Reset

D 6.4.4.1 TAi (i>2), Betriebsfrequenz

TAi b1-b4 (i>2)	minimale Betriebsfrequenz: fsmin 0 ($0) = Default 1 ($1) = 1 MHz (= Default) 2 ($2) = 2 MHz 3 ($3) = 3 MHz 4 ($4) - 15 ($F) = reserviert
TAi b5-b8 (i>2)	maximale Betriebsfrequenz: fsmax 0 - 3 = reserviert 4 ($4) = 4 MHz 5 ($5) = 5 MHz (= Default) : 15 ($F) = 15 MHz

D 6.4.4.2 TBi (i>2), Übertragungsblockgröße

TBi b1-b8 (i>2)	Maximale Größe des Übertragungsblocks Default-Wert ist dezimal 64

D 6.4.4.3 TCi (i>2), Character Waiting Time

TCi b1-b8 (i>2)	Max. Character Waiting Time CWT Dieses Byte beinhaltet den Parameter CWI zur Bestimmung der max. Character Waiting Time CWT. CWI ist ein Integerwert im Bereich von 1 bis 255. Der Default-Wert für CWI ist 5. CWI=0 ist für zukünftige Benutzung reserviert.

CWT wird bestimmt durch:

$$CWT = CWI \times \frac{fo}{fs} \; ms$$

Beispiel: Im Fall fo=fs kann der Wert für CWT zwischen 1 und 255 msec betragen.

CWT bestimmt den maximalen Zeitabstand für den Empfang bzw. das Senden zweier zusammengehöriger Bytes.

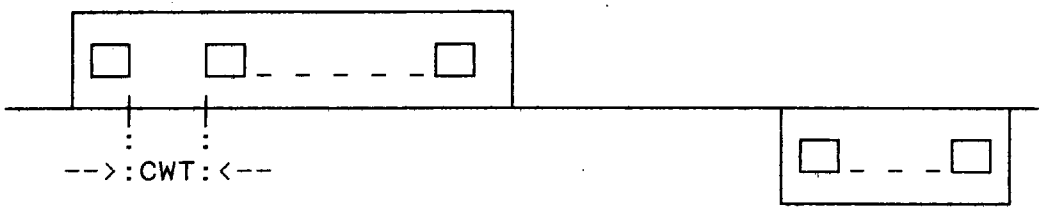


Bild D 6.4: Maximum Character Waiting Time CWT

D 6.4.4.4 TAi+1 (i>2), Block Waiting Time

TAi+1 (i>2) b1-b8

Max. Block Waiting Time BWT
Dieses Byte beinhaltet den Parameter BWI zur Bestimmung der max. Block Waiting Time BWT. BWI ist ein Integerwert im Bereich von 1 bis 255. Der Default-Wert für BWI ist 20. BWI=0 ist für zukünftige Benutzung reserviert.

BWT wird bestimmt durch:

$$BWT = 100 \times BWI \times \frac{fo}{fs} \; ms$$

Beispiel: Im Fall fo=fs kann der Wert für BWT zwischen 100 msec und 25.5 sec betragen.

BWT ist die Zeit, in der nach Empfang eines Requests spätestens mit der Übertragung eines Response begonnen werden muß (maximale Antwortzeit).

BWT ist anwendungsabhängig, und muß größer als die Maximale Character Waiting Time CWT gewählt werden.

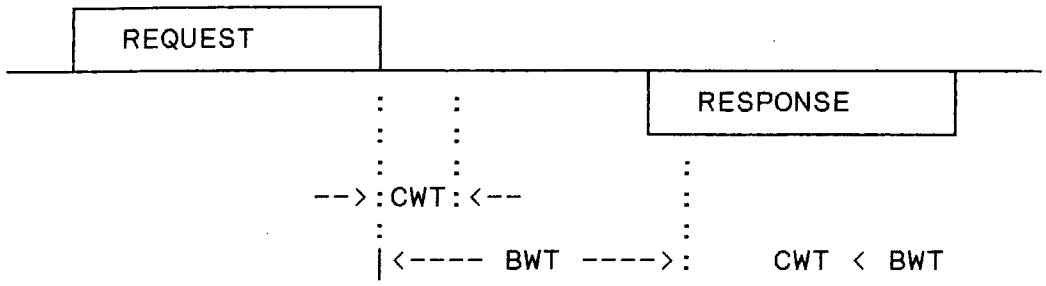


Bild D 6.5: Maximum block waiting time (BWT)

D 6.4.4.5 TBi+1 (i>2), Protokollprofil-Anzeige

TBi+1 (i>2) b1-b8 Mit diesem Byte werden dem CEG Details zum in der ICC implementierten Protokoll angezeigt.

b1 =0: Verwendung der XOR-Checksummenmethode im Schicht-2-Protokoll
=1: Verwendung der CRC-Checksummenmethode im Schicht-2-Protokoll

b2 =0: Verwendung des 12-etu-Byterahmens
=1: Verwendung des 11-etu-Byterahmens

b3 =0: Kein Chaining im ICL-Schicht-Protokoll
=1: Chaining im ICL-Schicht-Protokoll

b4 =0: Keine Kompatibilität zu ISO 7816-3/Kap. 8
=1: Kompatibilität zu ISO 7816-3/Kap. 8

b5 =0: Kein privates Protokoll im ICL-Schicht-Prot.
=1: Privates Protokoll im ICL-Schicht.Protokoll

b6 =0: Keine ICB-Extension im ICL-Schicht-Protokoll
=1: ICB-Extension im ICL-Schicht-Protokoll

b7-b8 reserviert

Die Defaultwerte der Bits dieses Bytes sind sämtlich 0.

D 6.5 Historical Characters

Wird durch ein TDi-Byte angezeigt, daß die Chipkarte ein nationales Protokoll (Protokolltyp T=14) unterstützt, wird das international genormte Länderkennzeichen des Protokoll-Herkunftslandes in den Historical Characters T1 und T2 übertragen (siehe Bild D 6.6).
Falls mehr als 2 Historical Characters gesendet werden, so ist T3 für zukünftige Erweiterungen reserviert und hat defaultmäßig den Wert 00. T3 und eventuell noch weitere empfangene Historical Characters gelten als anwendungsabhängig, so daß deren Auswertung dem CEG überlassen bleibt.

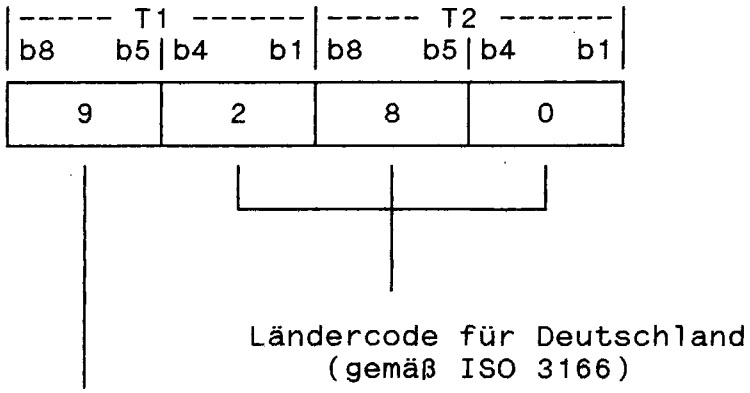


Bild D 6.6: Historical Characters für das nationale Blockübertragungsprotokoll von Deutschland

D 6.6 TCK, Checkbyte für die Answer-to-Reset-Sequenz

Das Checkbyte TCK folgt unmittelbar auf den Answer to Reset und weist denjenigen Wert auf, der bei Anwendung der Operation XOR von T0 bis TCK das Ergebnis 0 liefert.

Wenn die ICC nur das Protokoll T=0 signalisiert, wird TCK nicht gesendet. In allen anderen Fällen ist die Aussendung von TCK obligatorisch.

D 6.7 Fehlerbehandlung bei Answer to Reset

Werden bei Empfang der ATR-Bytes Fehler erkannt, wird vom Chipkarten-Endgerät durch erneutes Aktivieren der Reset-Leitung ein neuer Reset ausgelöst. Die Chipkarte wird als defekt betrachtet, wenn nach drei Versuchen keine korrekte Answer to Reset Information empfangen worden ist.

Bei der Übertragung des Answer to Reset werden folgende Fehler erkannt:

- Parity Error
- Frame Error
- Underrun (Time-Out)
- Overrun

Die genannten Fehler lassen sich durch einen erneuten Reset-Versuch nur dann beheben, wenn sie durch temporäre Störungen verursacht wurden. Andere Ursachen führen nach dreimaligen Reset-Versuch zum Abruch des Chipkartenbetriebes durch das Chipkarten-Endgerät.

D 6.7.1 Parity Error

Wird bei Empfang eines Bytes ein Parity-Fehler erkannt, so wird ein neuer Reset veranlaßt.

D 6.7.2 Frame Error

Wird der vereinbarte Byterahmen gemäß ISO 7816-3 (Start/Stop-Bit, Übertragungsgeschwindigkeit) nicht eingehalten, tritt ein Framing Error auf. Dieser Fehler führt zu einem erneuten Reset.

D 6.7.3 Underrun

Ein Underrun tritt auf, wenn die Chipkarte weniger Bytes gesendet hat als erwartet. Die Anzahl der zu erwarteten Bytes ist durch die gesetzten Bits in den entsprechenden Bytes (T0, TD1 usw.) definiert. Der Fehler führt zu einem Reset.

D 6.7.4 Overrun

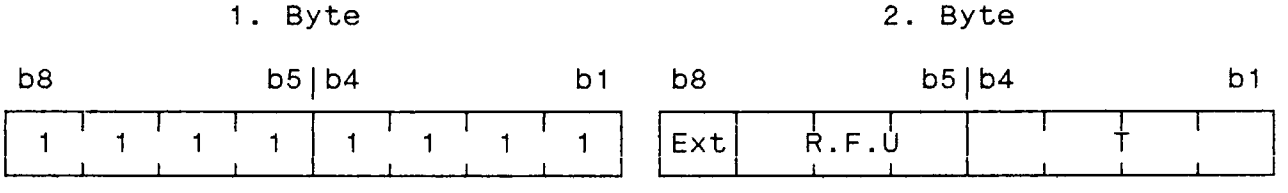
Ein Overrun tritt auf, wenn die Chipkarte mehr Bytes sendet, als erwartet werden. Dieser Fehler führt zu einem Reset.

D 6.8 Protokollauswahl

Wird von der Chipkarte im ATR signalisiert, daß mehr als ein Protokoll implementiert ist (siehe D 6.4), so muß eine Protokollauswahl durch das Chipkarten-Endgerät (CEG) erfolgen.

Nach Empfang der kompletten ATR-Bytesequenz wird vom CEG mit der für ATR gültigen und möglicherweise mittels der globalen Interface Characters geänderten Übertragungsparameter (Byterahmen, Baudrate, Frequenz) ein Protocol Type Select (PTS) Request zur Chipkarte übertragen. Die Chipkarte sendet als Antwort das PTS Request als PTS Respone zum CEG zurück und initialisiert das selektierte Protokoll.

PTS ist wie folgt kodiert:



Ext = Reserviert für zukünftige Erweiterung (0 = Default)
R.F.U = Reserviert für zukünftige Nutzung (000 = Default)
T = Ausgewählter Protocol Type

Bild D 6.7: Protocol Type Select (Request and Respone)

Falls die ICC u.a. T=0 signalisiert hat und nach dem Answer to Reset als erstes Byte nicht FF (hexadezimal) empfängt, unterstellt sie, daß das Protokoll T=0 vom CEG ausgewählt wurde und daß kein PTS Request und PTS Response übetragen werden.

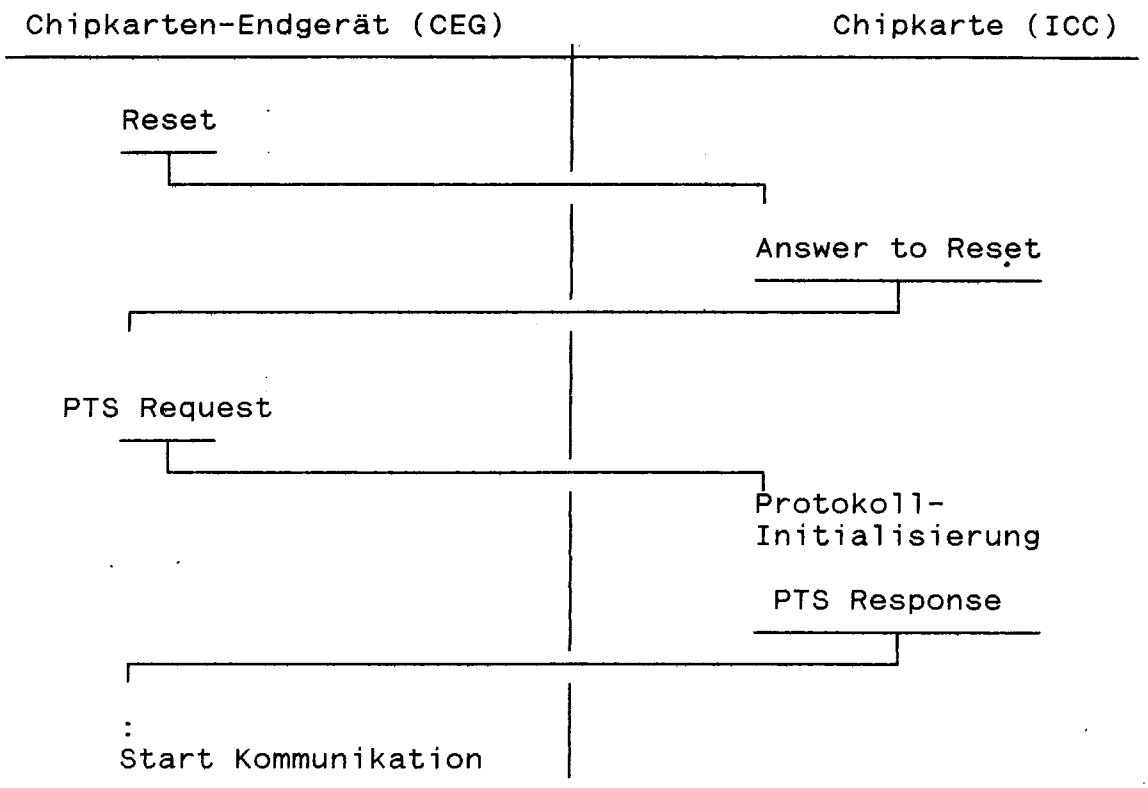


Bild D 6.8: Szenario mit Protokollverhandlung

Wenn die ICC einen fehlerbehafteten PTS Request erhalten hat, sendet sie keinen PTS Response. In diesem Fall führt das CEG einen Reset aus.

Wenn das CEG nach einem ATR einen fehlerbehafteten PTS Response erhalten hat, führt es erneut einen Reset aus.

Zeigt die Chipkarte an, daß sie nur ein Protokoll implementiert hat, beginnt das CEG nach Empfang des ATR und nach Ablauf einer Zeit, die größer als die Zeit CWT (Max. Character Waiting Time) ist, die Kommunikation mit der Chipkarte in dem angezeigten Protokoll.

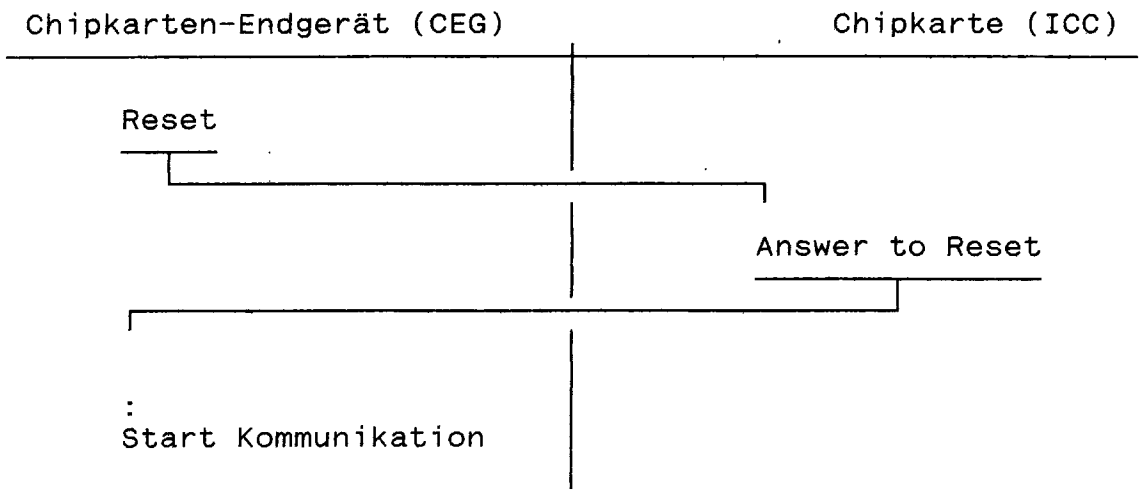


Bild D 6.9: Szenario ohne Protokollverhandlung

D 7 Protokoll in der Sicherungsschicht (Schicht 2) für T=14

D 7.1 Übertragungsblock

Der Austausch von anwendungsbezogenen Informationen zwischen dem Chipkarten-Endgerät und der Chipkarte geschieht durch abwechselnde Übertragung von Blöcken.

Die anwendungsbezogenen Informationen werden mittels des Blockübertragungsprotokolls übertragen. Sie stehen im Informationsfeld des Übertragungsblockes dieses Protokolls.

Ein Übertragungsblock besteht aus drei Teilen und hat folgende Struktur:

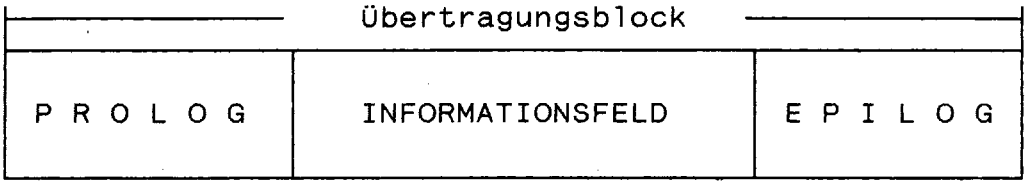


Bild D 7.1: Übertragungsblock

Die einzelnen Komponenten des Übertragungsblocks haben folgende Bedeutung.

D 7.1.1 Prolog

Der Prolog eines Übertragungsblock hat eine Länge von drei Bytes. Er besteht aus dem Adreßfeld für die Geräteadressen (Länge: 1 Byte), dem Steuerfeld (Länge: 1 Byte) und dem Längenfeld für die Anzahl der zu übertragenen Datenbytes (Länge: 1 Byte).

D 7.1.2 Informationsfeld

Das Informationsfeld beinhaltet die Informationen (Daten) die übertragen werden. Die Daten sind für diese Schicht transparent und unabhängig vom Übertragungsprotokoll. Das Informationsfeld hat eine Länge von 0 bis 254 Byte (siehe D 7.1.8).

D 7.1.3 Epilog

Das Epilog-Feld beinhaltet die Kontrollsumme des übertragenen Blocks. Je nachdem, welche Methode zur Generierung der Kontrollsumme verwendet wurde (XOR-Methode oder Polynom-Methode), besteht dieses Feld aus einem bzw. zwei Bytes.

Die nachfolgende Abbildung zeigt die detaillierte Darstellung eines Übertragungsblocks.

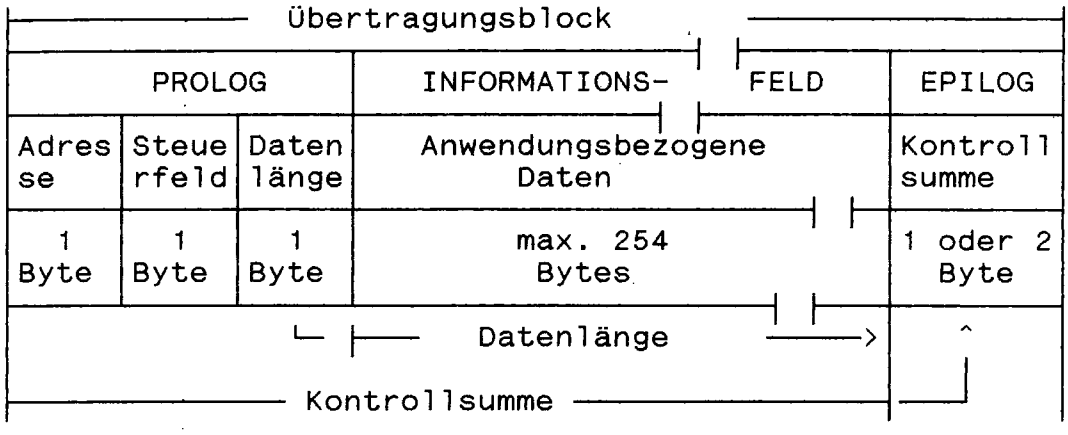


Bild D 7.2: Detaillierte Darstellung eines Übertragungsblockes

Die Bedeutung der einzelnen Felder des Übertragungsblocks wird in den folgenden Abschnitten beschrieben.

D 7.1.4 Anfangserkennung eines Übertragungsblockes

Der Anfang eines Übertragungsblockes wird am Empfang des Startbits und des darauffolgenden kontextabhängigen Bytes (Adreßbyte) erkannt.

D 7.1.5 Endeerkennung eines Übertragungsblockes

Das Ende eines Übertragungsblockes wird am Empfang eines Bytes, das das n-te Byte in Abhängigkeit des empfangenen Längenbytes darstellt, erkannt. Anschließend folgt noch ein oder zwei Byte (abhängig von der Generierung der Kontrollsumme) für die Kontrollsumme (logisches Blockende). Danach muß die Leitung für eine Zeit, die größer ist als die Zeit CWT (max. Character Waiting Time) in Ruhe gehalten werden (physikalisches Blockende).

D 7.1.6 Adreßfeld

Das Adreßfeld hat eine Länge von einem Byte und gibt die Geräteadresse des Senders (Interface Device bzw. Chipkarte) und die des Empfängers (Interface Device bzw. Chipkarte) eines Übertragungsblockes an.

Durch das höherwertige Halbbyte des Adreßbytes wird die Geräteadresse des Senders (source address), durch das niederwertige Halbbyte die Geräteadresse des Empfängers (destination address) spezifiziert.

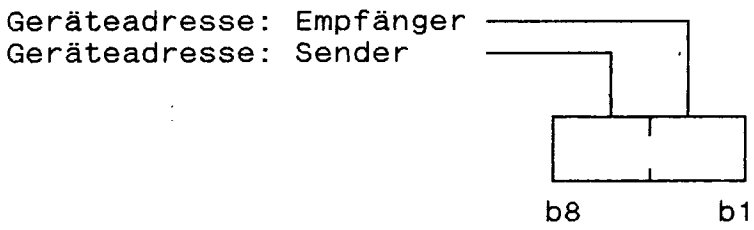


Bild D 7.3: Adreßbyte

Es werden folgende Geräteadressen vereinbart:

- für das Chipkarten-Endgerät: Adresse A = X
- für die Chipkarte: Adresse B = 1

Für das Adreßbyte ergibt sich damit folgendes Format:

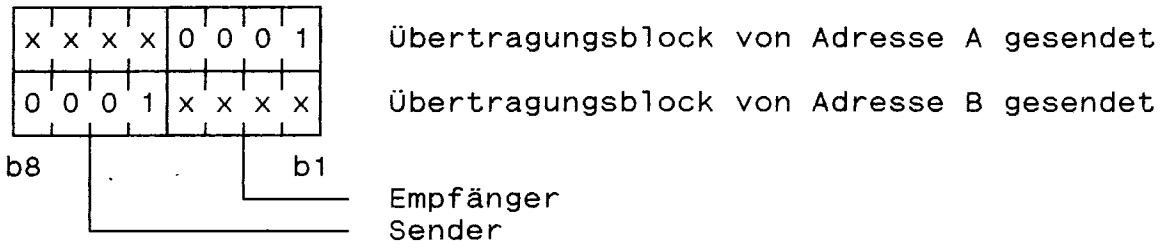


Bild D 7.4: Adressierung Sender/Empfänger

Die Geräteadresse für das mit der Chipkarte (ICC) kommunizierende Endgerät (CEG) wird durch dieses selbst bestimmt. Von der ICC wird diese Adresse bei der Übertragung ihrer Datenblöcke zum CEG als Empfängeradresse in das Adreßbyte übernommen.

Die am Anfang festgelegten Adressen A und B=1 gelten so lange, bis eine gegenseitig bestätigte Änderung der Geräteadressen erfolgt ist. Das Verfahren für die Änderung von Adressen bedarf weiterer Festlegungen.

Vom CEG empfangene Blöcke mit abweichendem A unter Beibehaltung von B=1 werden als ungültige Blöcke behandelt. Vom CEG empfangene Blöcke mit B ungleich 1 werden ignoriert und nicht beantwortet.

D 7.1.7 Steuerfeld

Das Steuerfeld besteht aus einem Byte. Es kodiert einen Befehl des Protokolls der Schicht 2.

Folgende Befehle werden für die Schicht 2 verwendet:

- I-Befehl Informationsbefehl
- REJ-Befehl Wiederholungsaufforderungsbefehl
- RES-Befehl Resynchronisationsbefehl

D 7.1.7.1 I-Befehl

Mit dem I-Befehl werden Nutzer-Daten der ICL-Schicht (ICL bedeutet Interface Control Layer) transparent und blockweise zwischen Chipkarten-Endgerät (CEG) und Chipkarte (ICC) ausgetauscht. Die zu übertragenden Daten befinden sich im Informationsfeld. Werden in einem I-Befehl keine Nutzer-Daten übertragen (Länge 0), so hat der I-Befehl nur Quittungsfunktion.

Der I-Befehl beinhaltet zwei Nummern:

- Sendefolgenummer N(S)
- Empfangsfolgenummer N(R)

Die Verwendung beider Folgenummern setzt sowohl im Chipkarten-Endgerät als auch in der Chipkarte den Betrieb zweier voneinander unabhängiger Zähler voraus:

- Sendefolgezähler V(S)
- Empfangsfolgezähler V(R)

Die Folgenummern- und -zähler haben beide zu Beginn des Protokolls der Schicht 2 den Wert 0 und werden dann von 0 beginnend modulo-8 hochgezählt, d.h. von 0-7 und dann wieder von 0 beginnend.

Vor Beginn der Blockübertragung (nach ATR und eventuell der Protokollvereinbarung) und unmittelbar nach quittiertem RES-Befehl befinden sich V(S) und V(R) sowohl im Chipkarten-Endgerät als auch in der Chipkarte auf dem Wert 0.

Ein auszusendender I-Befehl erhält als N(S) den momentanen Zählerstand von V(S) und als N(R) den momentanen Zählerstand von V(R).

Ist der I-Befehl übertragen worden, wird V(S) beim Sender um 1 erhöht, V(R) bleibt unverändert.

Nach Empfang eines I-Befehls wird dessen N(S) mit V(R) und N(R) mit V(S) verglichen. Nur wenn Nummer und Zähler übereinstimmen und der I-Befehl als fehlerfrei interpretiert worden ist, wird V(R) um 1 erhöht.

Im Punkt D 7.4 werden Beispiele zum Folgezählermechnismus gegeben.

Kodierung des I-Befehls:

b8	b7	b6	b5	b4	b3	b2	b1
N(R)			0	N(S)			0

b2 = low-order Bit von N(S)
b6 = low-order Bit von N(R)

Bild D 7.5

D 7.1.7.2 REJ-Befehl

Mit dem REJ-Befehl wird signalisiert, daß ein fehlerhafter Übertragungsblock empfangen worden ist. Mit dem REJ-Befehl wird die Aussendung des entweder falsch empfangenen oder als nächsten erwarteten I-Befehls gefordert. Das Feld N(R) des REJ-Befehls enthält die Sendefolgenummer N(S) des zu übertragenden I-Befehls. Nach Aussenden des REJ-Befehls wird der Zähler V(S) des REJ-Befehl-Senders nicht erhöht.

Beim Empfang eines REJ-Befehls muß die Nummer N(R) mit dem um 1 verminderten Zählerstand V(S) beim Empfänger des REJ-Befehls übereinstimmen. Der Empfänger eines REJ-Befehls wiederholt daraufhin die Übertragung des I-Befehls, wobei auch die zuvor übertragenen Zählerstände beibehalten werden. Demzufolge wird der Zähler V(S) nach wiederholtem Aussenden des I-Befehls nicht erhöht.

Im Punkt D 7.4 werden Beispiele zur Benutzung von REJ und deren Auswirkung auf die Folgezähler gegeben.

Kodierung des REJ-Befehls:

b8	b7	b6	b5	b4	b3	b2	b1
N(R)			0	1	0	0	1

b6 = low-order Bit von N(R)

Bild D 7.6

D 7.1.7.3 RES-Befehl

Der RES-Befehl dient zur Synchronisation der Datenübertragung in der Schicht 2.

Initiator der Resynchronisation kann sowohl das Chipkarten-Endgerät als auch die Chipkarte sein. Der Sender eines RES-Befehls

(Initiator) setzt, nachdem als Antwort ein RES-Befehl empfangen wurde, die Zähler V(S) und V(R) auf 0. Der Empfang eines RES-Befehls muß mit einem RES-Befehl beantwortet werden. Nachdem der RES-Befehl gesendet worden ist, werden die Zählerstände V(S) und V(R) auf 0 gesetzt.

Initiierung und Beantwortung von RES-Befehlen werden von der Schicht oberhalb Schicht 2 angestoßen.

Kodierung des RES-Befehls:

b8	b7	b6	b5	b4	b3	b2	b1
1	1	1	0	1	1	1	1

Bild D 7.7

D 7.1.8 Längenanzeige

Die Länge des Informationsfeldes eines Übertragungsblocks wird in einem Byte (für Längen von 0 bis 254) angezeigt.

Der Wert 255 des Längenanzeige-Bytes (alle Bits gesetzt) ist für künftige Erweiterungen reserviert.

D 7.1.9 Kontrollsumme

Die Bildung der Kontrollsumme erfolgt für dieses Übertragungsprotokoll nach der XOR-Methode. Das Feld hat demnach eine Länge von einem Byte.

Die Kontrollsumme wird gebildet durch 'exklusiv oder' der einzelnen Bytes des Übertragungsblocks, vom Adreßbyte bis einschließlich des letzten Datenbytes des Informationsfeldes.

Die Verwendung einer anderen Kontrollsummen-Methode, z.B. CRC, wird in einem noch zu definierenden ATR-Parameter für das Protokoll T=14 angezeigt.

D 7.2 Zeitlicher Ablauf in der Schicht 2

Die in diesem Kapitel verbal gehaltene Beschreibung des zeitlichen Ablaufs wird im Kapitel 7.3 durch die formale Beschreibung der Dienste der Schicht 2 und der Zustandsdiagramme sowie der Zustandstabellen ergänzt.

Hinweis:

Im Abschnitt E befindet sich die Beschreibung einer abwärtskompatiblen Untermenge des hier getroffenen Protokolls für einfachere Anwendungen.

D 7.2.1 Fehlerfreier Ablauf

Grundsätzlich kann immer nur ein einziger Übertragungsblock vom Sender zum Empfänger übertragen werden, woraufhin die Rollen des Senders und Empfängers getauscht werden, also die Sendeberechtigung übergeben wird. Das Chipkarten-Endgerät (CEG) hat die Sendeberechtigung am Anfang des Blockübertragungsprotokolls sowie nach einem BWT-Timeout. Das Management der Sendeberechtigung befindet sich oberhalb der Schicht 2. Das heißt, daß in der Schicht kein Wissen darüber besteht, bei welchem Kommunikationspartner sich die Sendeberechtigung befindet.

Das Protokoll wird vom CEG mit einem RES-Befehl oder einem I-Befehl eingeleitet. Im Falle eines RES-Befehls antwortet die Chipkarte mit einem RES-Befehl.

Nachdem die Schicht 2 des CEG von der ICL-Schicht Nutzer-Daten erhalten hat, werden diese an die Chipkarte mit einem I-Befehl gesendet.

Die Schicht 2 der Chipkarte übergibt der ICL-Schicht die empfangenen Nutzer-Daten. Die ICL-Schicht informiert dann die Schicht 2 darüber, ob der Empfang der Nutzer-Daten sofort quittiert werden soll oder übergibt der Schicht 2 Nutzer-Daten zum Aussenden an das CEG.

Die sofortige Quittierung geschieht mittels Aussenden eines I-Befehls ohne Nutzer-Daten (leerer I-Befehl, Längenanzeige 0), der in Abhängigkeit der jeweils vorliegenden Sendeberechtigung in der Schicht oberhalb der Schicht 2 mit einem leeren I-Befehl beantwortet wird.

D 7.2.2 Fehlerhafter Ablauf

D 7.2.2.1 Ungültiger Block (invalid block)

Im weiteren wird die Bezeichnung "ungültiger Block" bzw. "invalid block" benutzt, die einer näheren Erläuterung bedarf.

Ein Block ist ungültig wenn:

- das Steuerfeld einen falschen Inhalt aufweist:
  * Befehl nicht bekannt
  * Zählerstand/-stände falsch

- das Längenfeld einen falschen Wert enthält,

- ein Parity- oder Frame-Error (siehe D 6.7.2) eintritt.

D 7.2.2.2 Fehlerbehandlungen

Fehlerbehandlung 1:

(a) Das Chipkarten-Endgerät (CEG) sendet zu Beginn des Blockübertragungsprotokolls oder zwischendurch einen RES-Befehl und wartet auf den Empfang eines RES-Befehls als Antwort, weswegen der BWT Timer gestartet wird.
(b) BWT Timeout, Empfang eines ungültigen Blocks oder eines REJ-Befehls oder eines I-Befehls
(c) Das CEG wiederholt den RES-Befehl (max. 2 Male). Wenn die insgesamt 3 Versuche nicht zum Empfang eines korrekten RES-Befehls geführt haben, beginnt das CEG die Kommunikation mit der Chipkarte (ICC) erneut durch physikalischen Reset. Es sind eine bestimmte Anzahl von physikalischen Resets festgelegt. Wenn diese Anzahl von Versuchen erreicht ist, sind folgende Reaktionen auf diesen Fehler hin möglich: Auswurf der Karte oder eine entsprechende Fehlermeldung an den Benutzer der Karte.

Fehlerbehandlung 2:

(a) Das CEG bzw. die ICC sendet einen I-Befehl und wartet auf eine Antwort, weswegen ein Timer gestartet wird.
(b) Timeout
(c) Das CEG bzw. die ICC wiederholt den I-Befehl max. 3 bzw. 2 Male. Wenn die insgesamt 4 bzw. 3 Versuche nicht erfolgreich waren, informiert die Schicht 2 die Schicht oberhalb der Schicht 2 über diesen Fehler. Mögliche Reaktionen auf diesen Fehler hin sind physikalischer Reset, Aussenden eines RES-Befehls, Auswurf der Karte oder eine entsprechende Fehlermeldung an den Benutzer der Karte.

Fehlerbehandlung 3:

(a) Das CEG bzw. die ICC sendet einen REJ-Befehl und wartet auf eine Antwort, weswegen ein Timer gestartet wird.
(b) Timeout
(c) Das CEG bzw. die ICC wiederholt den REJ-Befehl max. zweimal bzw. einmal. Wenn die insgesamt 3 bzw. 2 Versuche des CEG bzw. der ICC nicht erfolgreich waren, informiert die Schicht 2 die Schicht oberhalb der Schicht 2 über diesen Fehler. Mögliche Reaktionen auf diesen Fehler hin sind physikalischer Reset, Aussenden eines RES-Befehls, Auswurf der Karte oder eine entsprechende Fehlermeldung an den Benutzer der Karte.

Fehlerbehandlung 4:

(a) In Erwartung eines I-Befehls empfängt das CEG bzw. die ICC einen ungültigen Block.

(b) Das CEG bzw. die ICC sendet einen REJ-Befehl. Wenn nach 3 bzw. 2 REJ-Versuchen kein gültiger Block empfangen wird, informiert die Schicht 2 die Schicht oberhalb der Schicht 2 über diesen Fehler. Mögliche Reaktionen auf diesen Fehler hin sind physikalischer Reset, Aussenden eines RES-Befehls, Auswurf der Karte oder eine entsprechende Fehlermeldung an den Benutzer der Karte.

D 7.3 Formale Beschreibung des Sicherungsschicht-Protokolls

D 7.3.1 Dienste der Schicht 2

D 7.3.1.1 Allgemeine Erläuterungen

Gemäß Modellvorstellung beim OSI-Referenzmodell fordert eine höhere Schicht von der nächst tieferen Dienste an, deren Ausführung bestimmte Protokollereignisse in den tieferen Schichten zur Folge haben. Diese Protokollereignisse sind selbst nicht Bestandteil der Dienst-Definitionen, sind sogar von ihnen total unabhängig, damit ein Austauschen von Protokollen in den tieferen Schichten ohne Änderung der Dienstfestlegungen möglich ist.

Die Inanspruchnahme und das Erbringen von Diensten an der Dienst-Schnittstelle zwischen zwei vertikal benachbarten Schichten (siehe Bild D 7.8) wird durch sogenannte Dienstelemente (im Engl.: service primitives) zum Ausdruck gebracht. Die höhere Schicht fordert Dienste von der tieferen an, währenddessen die tiefere Schicht der höheren Schicht Dienste erbringt. Die Darstellung von fordernden bzw. erbringenden Dienstelementen geschieht durch nach unten bzw. nach oben zeigende Pfeile (siehe Bild D 7.9).

Zu bemerken wäre an dieser Stelle, daß die Beschreibung von Diensten nur in konzeptioneller Weise und für die Schaffung eines besseren Verständnisses der Kommunikationsabläufe Bedeutung haben, nicht aber notwendigerweise identisch in Implementationen umgesetzt werden müssen.

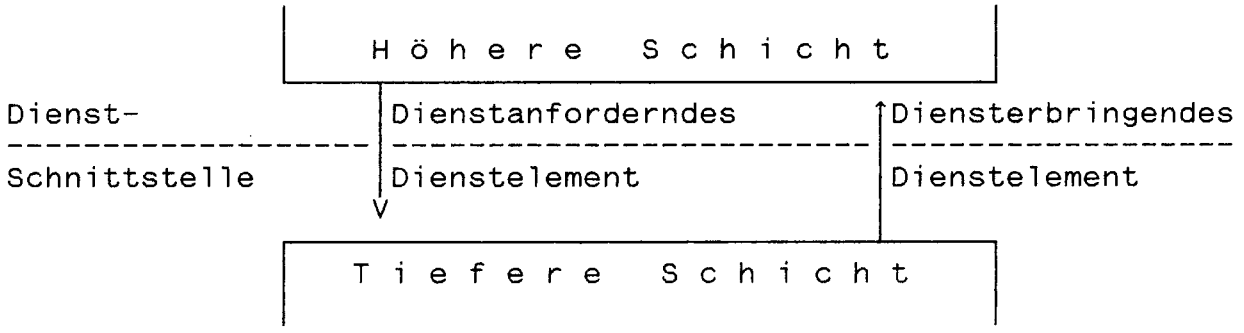


Bild D 7.8: Dienst-Schnittstelle und Dienstelemente

Da die zeitliche Folge von Dienstelementen nicht beliebig sein kann, muß die erlaubte zeitliche Folge, das sogenannte Dienstprotokoll, festgelegt werden. Dies geschieht zumeist in tabellarischer Form.

D 7.3.1.2 Beschreibung der Dienste der Schicht 2

Die hier beschriebenen Dienste sind auf Dienstleistungen der Schicht 2 beschränkt, die mit dem GZS/DBP-Blockübertragungsprotokoll in Zusammenhang stehen. Weitere Dienste in Verbindung mit der Bitübertragung, dem Reset/Answer to Reset sowie der Protokollverhandlung stehen vorerst aus und sind noch zu untersuchen.

D 7.3.1.2.1 Datenübertragungsdienst DL-DATA

Mittels des Dienstes DL-DATA (DL steht für Data Link Layer) vermag die ICL-Schicht der Schicht 2 den Auftrag zu erteilen, Daten transparent zu senden oder empfangene Daten von der Schicht 2 zu erhalten. Hierbei wird vorausgesetzt, daß in der ICL-Schicht das Wissen vorhanden ist, welche Schicht-2-Instanz das Senderecht besitzt. Definitionsgemäß gibt es demnach kein Senderecht-Management in der Schicht 2.

Zwei Dienstelemente erfüllen diese Aufgaben (siehe Bild D 7.9):

(1) DL-DATA request (Parameter: Timer Control ON/OFF)

Mit diesem Dienstelement signalisiert die ICL-Schicht der Schicht 2, daß die mit DL-DATA request gelieferten Daten sofort gesendet werden sollen. Auch wenn die mitgelieferte Datenmenge leer ist, gilt dies als Sende-Auftrag. Er führt in diesem Fall dazu, daß ein leerer I-Befehl gesendet wird. Mit dem Parameter Timer Control ON/OFF wird der Schicht 2 mitgeteilt, daß der erwartete Empfang eines Blocks zeitüberwacht werden soll.

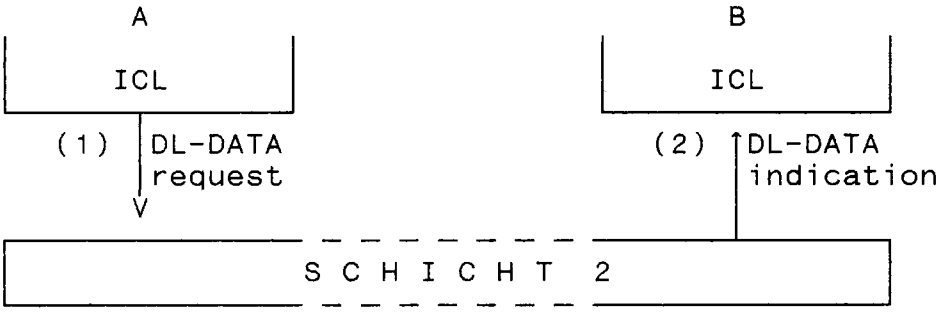


Bild D 7.9: Dienstelemente des Dienstes DL-DATA
(Die Ziffern geben die zeitliche Reihenfolge an)

(2) DL-DATA indication

Mit diesem Dienstelement übergibt die Schicht 2 der ICL-Schicht fehlerfrei empfangene Daten. Auch im Falle, daß ein leerer I-Befehl empfangen wird, zeigt dies die Schicht 2 der ICL-Schicht per DL-DATA indication an.

D 7.3.1.2.2 Resynchronisierungsdienst DL-RESYNCH

Im Protokollablauf der Schicht 2 sind Fehlerfälle denkbar, die mit dem Funktionsumfang der Schicht 2 allein nicht aufzufangen sind. Entweder erlangt die ICL-Schicht Kenntnis von solchen Fällen direkt von der Schicht 2 mittels des Fehlermeldungsdienstes DL-ERROR (siehe D 7.3.1.2.3) oder implizit, z.B. durch Timer-Ablauf in der ICL-Schicht. Die ICL-Schicht fordert somit den Resynchronisierungsdienst von der Schicht 2 an, um

- sich eventuell in der Schicht 2 befindliche Daten zu löschen,
- die Schicht 2 in einen funktionsfähigen Zustand zu bringen: beide Schicht-2-Instanzen befinden sich im Grundzustand, beide Zähler-Paare sind auf 0 gesetzt, die Timer-Steuerung wird abgeschaltet.

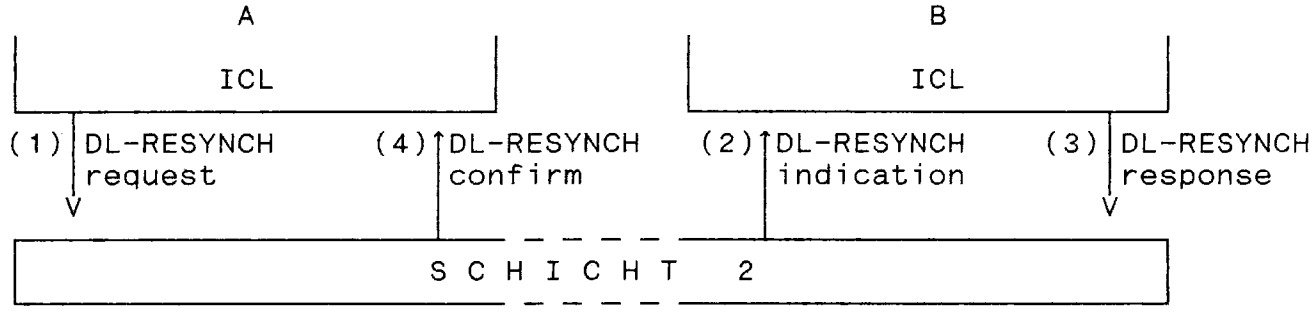


Bild D 7.10: Dienstelemente des Dienstes DL-RESYNCH
(Die Ziffern geben die zeitliche Reihenfolge an)

Vier Dienstelemente erfüllen den Resynchronisierungsauftrag der ICL-Schicht (siehe Bild D 7.10):

- DL-RESYNCH request

  Die ICL-Schicht fordert die Resynchronisierungsdienstleistung von der Schicht 2 an.

- DL-RESYNCH indication

  Die Schicht 2 zeigt der ICL-Schicht an, daß die Kommunikationspartner-Instanz der ICL-Schicht den Resynchronisierungsdienst angefordert hat.

- DL-RESYNCH response

  Die ICL-Schicht quittiert der Schicht 2 die Resynchronisierungsdienstanforderung der Partner-Instanz. Sie weiß nun, daß eventuell sich noch in der Schicht 2 befindliche Daten gelöscht werden und daß die Zähler auf den Anfangszustand zurückgesetzt werden.

- DL-RESYNCH confirm

  Mit diesem Dienstelement bestätigt die Schicht 2 der veranlassenden ICL-Schicht, daß die Resynchronisierungsdienstleistung erbracht wurde und daß auch die Partner-ICL-Schicht-Instanz Kenntnis von dieser Resynchronisierung erlangt hat.

D 7.3.1.2.3 Fehlermeldungsdienst DL-ERROR

Mit dem Dienstelement DL-ERROR indication (siehe Bild D 7.11) meldet die Schicht 2 der ICL-Schicht einen in der Schicht 2 nicht behebbaren Fehlerfall. In der Regel wird die ICL-Schicht, die gerade das Senderecht besitzt, daraufhin mit DL-RESYNCH request reagieren. Auch Kartenauswurf- oder Reset-Anforderung wären mögliche Reaktionen.

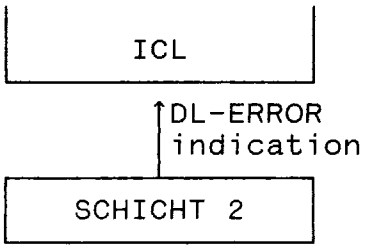
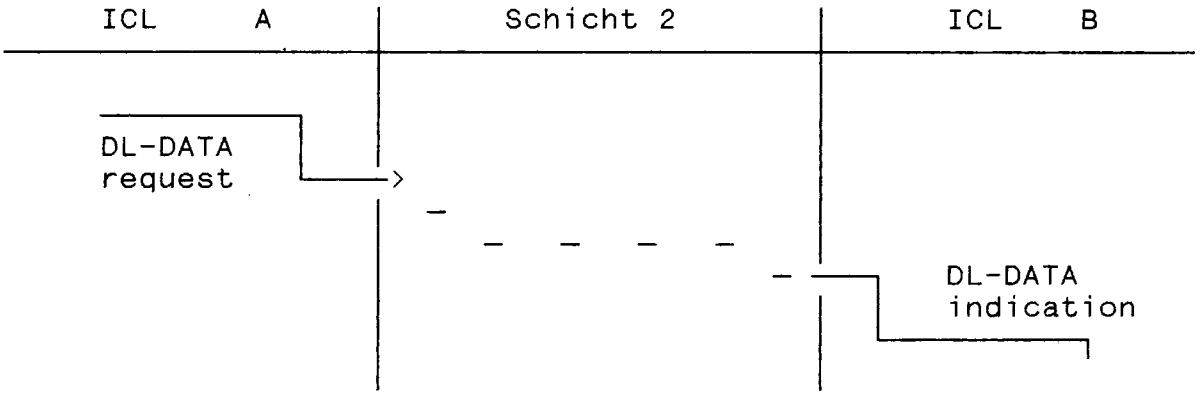


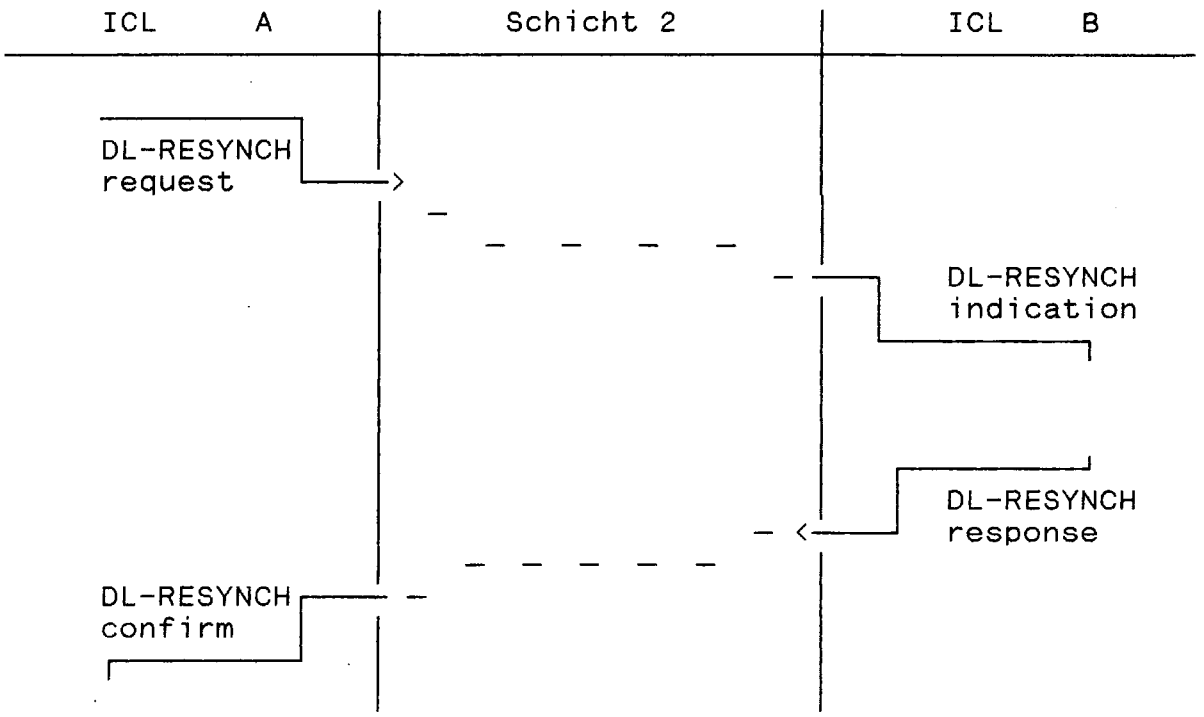
Bild D 7.11: Dienstelement des Dienstes DL-ERROR

D 7.3.1.3 Zeitdiagramme für die Dienste der Schicht 2

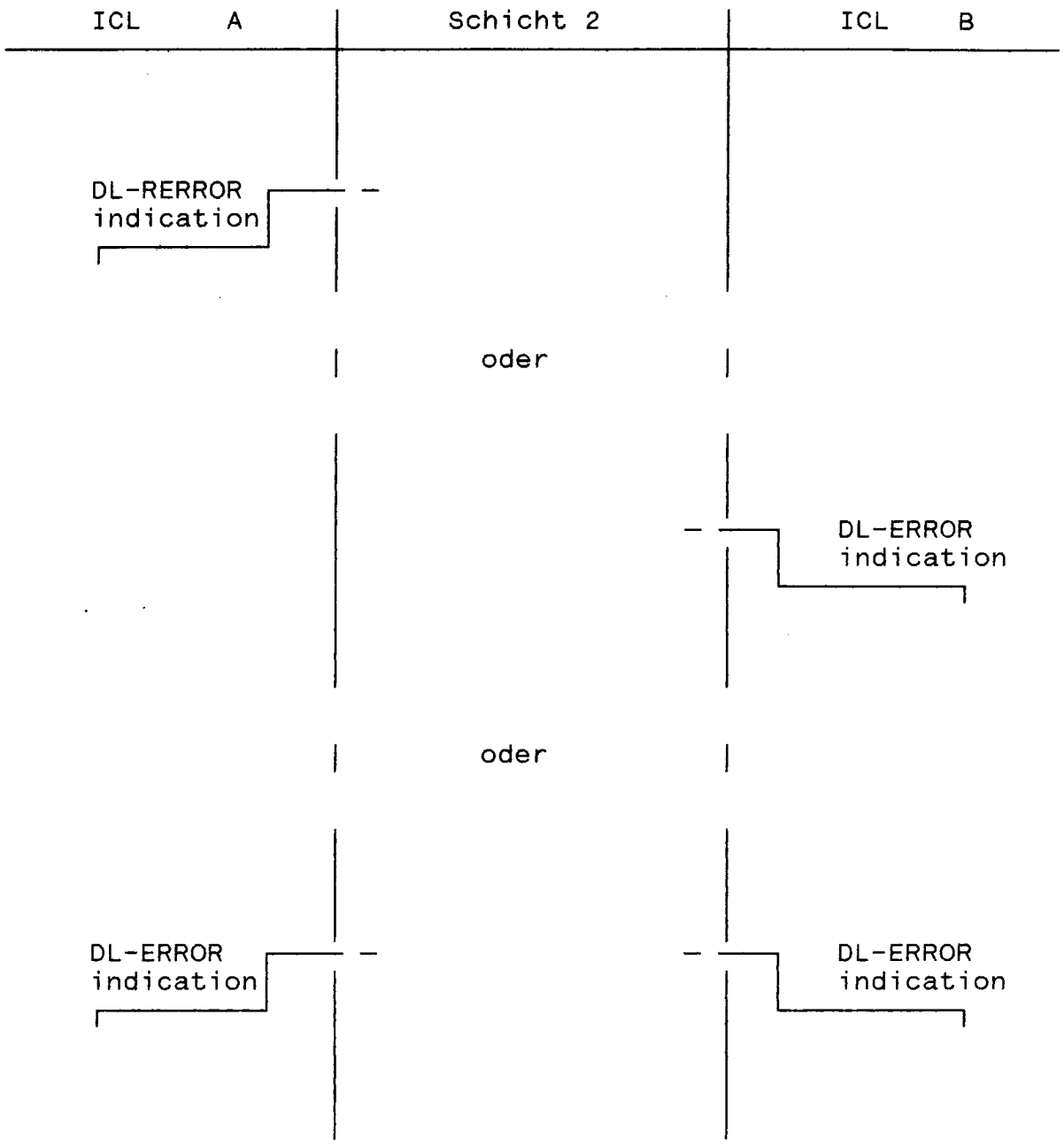
D 7.3.1.3.1 Zeitdiagramm für DL-DATA



D 7.3.1.3.2 Zeitdiagramm für DL-RESYNCH



D 7.3.1.3.3 Zeitdiagramme für DL-ERROR



D 7.3.1.4 Tabelle für das Dienstprotokoll der Schicht 2

darf folgen: \ Auf:		Anfng zust. *)	DL-DATA req	DL-DATA ind	DL-RESYNCH req	DL-RESYNCH ind	DL-RESYNCH resp	DL-RESYNCH conf	DL-ERROR ind
DL-DATA	request	X		X				X	
	indic.	X	X				X		
DL-RE-SYNCH	request	X	X	X	X			X	X
	indic.	X	X	X			X		X
	resp.					X			
	confirm				X				
DL-ERROR	indica-tion	X	X	X	X		X		X

*) "Anfangszustand" bedeutet hier, daß noch kein Dienstelement über die Dienst-Schnittstelle signalisiert wurde.

D 7.3.2 Zustandsdiagramme und -tabellen des Schicht-2-Protokolls

D 7.3.2.1 Allgemeine Erläuterungen

In diesem Kapitel wird das Protokoll mittels der Methoden Zustandsdiagramme und Zustandstabellen formal beschrieben. Bei Zustandsdiagrammen und -tabellen wird das im folgenden beschriebene Modell zugrundegelegt:

Es wird davon ausgegangen, daß ein Protokoll (hier speziell das der Schicht 2) von einer Protokollmaschine ausgeführt wird, die in beiden Kommunikationspartner-Instanzen vorhanden ist.

Die Protokollmaschine befindet sich zu einer Zeit in einem der möglichen, nur endlich vielen Zustände. Zustände werden in den Zustandsdiagrammen durch Kreise oder Ellipsen dargestellt (siehe Bild D 7.12).

Aus einem Zustand geht die Protokollmaschine bei Auftreten eines Ereignisses heraus und gelangt nach Abarbeitung keiner, einer oder mehrerer Aktionen zu dem gleichen oder einem anderen Zustand. Nach Verlassen eines zeitüberwachten Zustands gilt die Timer-Steuerung als abgeschaltet und der Timer als zurückgesetzt.

In der vorliegenden Beschreibung werden der Übersichtlichkeit halber indizierte Zustände benutzt. Wenn in einen nicht indizierten Zustand übergegangen wird, gelten die Indizes (Zähler) als zurückgesetzt.

Zustandsübergänge werden mit Pfeilen dargestellt, deren Richtung vom Ausgangszustand zum Zielzustand zeigt. Ereignisse werden neben dem aus dem Ausgangszustand herausführendem Pfeil angegeben. Verschiedene Ereignisse führen zu verschiedenen Zustandsübergängen. Die Angabe eines Ereignisses kann aus der logischen Verknüpfung mehrerer anderer Ereignisse bestehen.

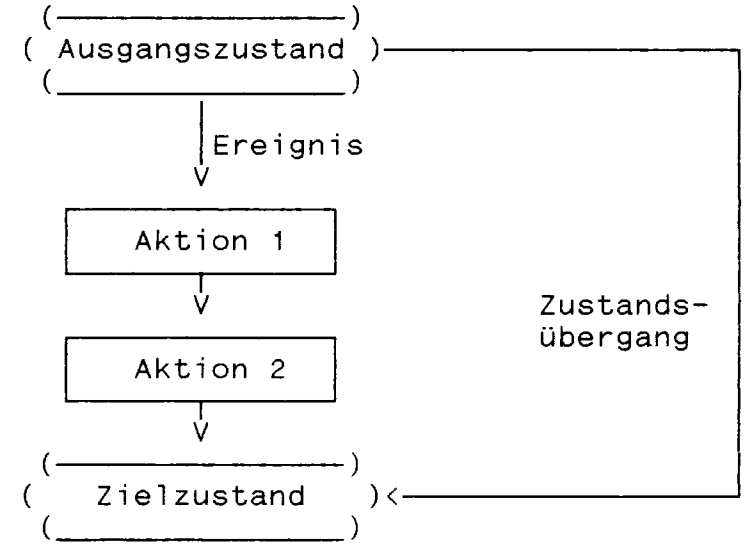


Bild D 7.12: Allgemeines Zustandsdiagramm

Aktionen werden in rechteckigen Kästen dargestellt und befinden sich innerhalb des Zustandsübergangspfeiles. Eine Unterbrechung der Aktionsabarbeitung ist während eines Zustandsübergangs unmöglich.

D 7.3.2.2 Zustände des Schicht-2-Protokolls

D 7.3.2.2.1 Zustände der Protokollmaschine des Chipkarten-Endgeräts (CEG)

DT	Data Send/Receive State in the IC card terminal without timer control
WT	Data Send/Receive State in the IC card terminal with timer control
RWT1	Resynchronisation Waiting State 1 in the IC card terminal
RWT2	Resynchronisation Waiting State 2 in the IC card terminal
ET	General Error State in the IC card terminal
ET(i)	Error State i in the IC card terminal (i=1,2,...,n) (n=3)
EW1T(i)	Error Waiting State 1 (i) in the IC card terminal (i=1,2,...,n), (n=3)
EW2T(i)	Error Waiting State 2 (i) in the IC card terminal (i=1,2,...,n), (n=3)

D 7.3.2.2.2 Zustände der Protokollmaschine der Chipkarte (ICC)

DI	Data Send/Receive State in the ICC without timer control
WI	Data Send/Receive State in the ICC with timer control
RWI1	Resynchronisation Waiting State 1 in the ICC
RWI2	Resynchronisation Waiting State 2 in the ICC
EI	General Error State in the ICC
EI(i)	Error State i in the ICC (i=1,2,...,n) (n=2)
EW1I(i)	Error Waiting State 1 (i) in the ICC (i=1,2,...,n), (n=2)
EW2I(i)	Error Waiting State 2 (i) in the ICC (i=1,2,...,n), (n=2)

D 7.3.2.3 Ereignisse im Schicht-2-Protokoll

Ereignisse können sein:

- die Dienstanforderungs-Dienstelemente der Schicht-2-Dienste:
  - DL-DATA request
  - DL-RESYNCH request
  - DL-RESYNCH response

- der Empfang eines korrekten oder fehlerhaften Befehls, der mit R: vor dem betreffenden Block angegeben wird (R für Receive); es wird davon ausgegangen, daß erst nach S:xxx wieder ein Block empfangen werden kann. Eventuell erkannte, empfangene Blöcke gelten als nicht empfangen.

- Timeout (Ablauf der Zeitüberwachung)

- die Diensterbringungs-Dienstelemente der Schicht-1-Dienste (noch nicht spezifiziert)

D 7.3.2.3 Aktionen im Schicht-2-Protokoll

Aktionen können sein:

- die Diensterbringungs-Dienstelemente der Schicht-2-Dienste:

  * DL-DATA indication
  * DL-RESYNCH indication
  * DL-RESYNCH confirm
  * DL-ERROR indication

- das Aussenden eines Blocks, das mit S: vor dem betreffenden Befehl angegeben wird (S für Send)

- Zählerveränderungen

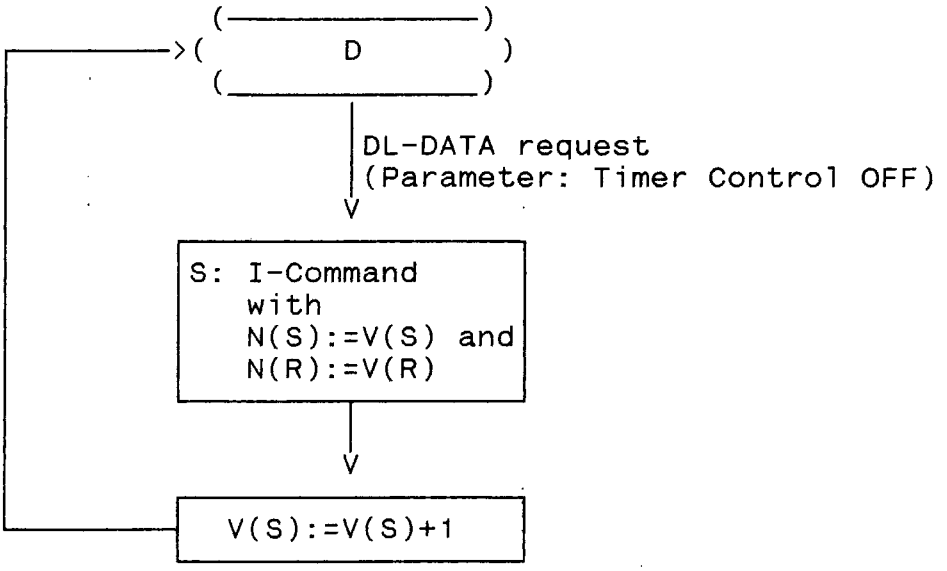
- Start Timer (Einschalten der Zeitüberwachung)

- die Dienstanforderungs-Dienstelemente der Schicht-1-Dienste: (noch nicht spezifiziert)

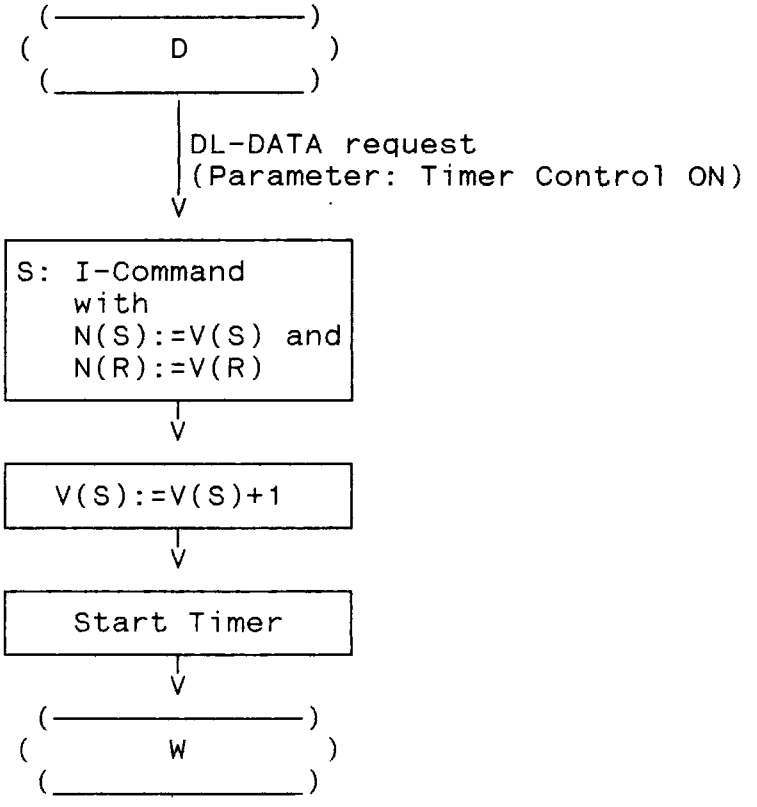
D 7.3.2.4 Zustandsdiagramme

Da die Protokollmaschinen für das CEG und die ICC abgesehen von unterschiedlichen Maxima für den Index i identisch sind, werden die folgenden Diagramme und Tabellen für beide zusammen geliefert, indem die Buchstaben T und I, welche CEG bzw. ICC kennzeichnen, weggelassen. Zum Beispiel steht D für DT bzw. DI sowie RW2 für RWT2 bzw. RWI2.

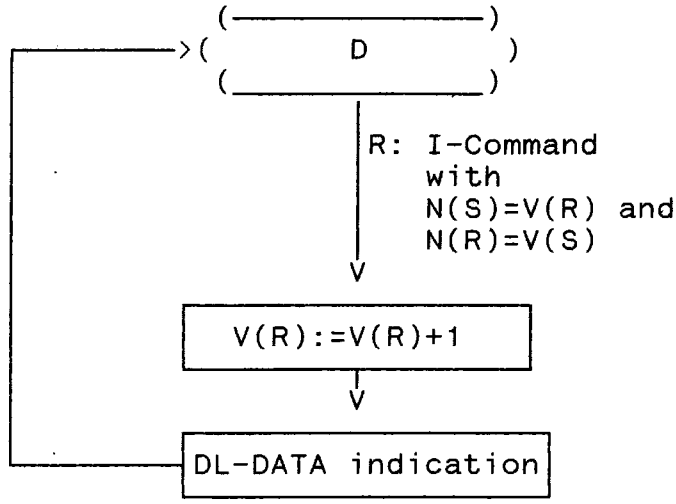
D 7.3.2.4.1 Sendeprotokoll 1 (ohne Zeitüberwachungsanforderung)



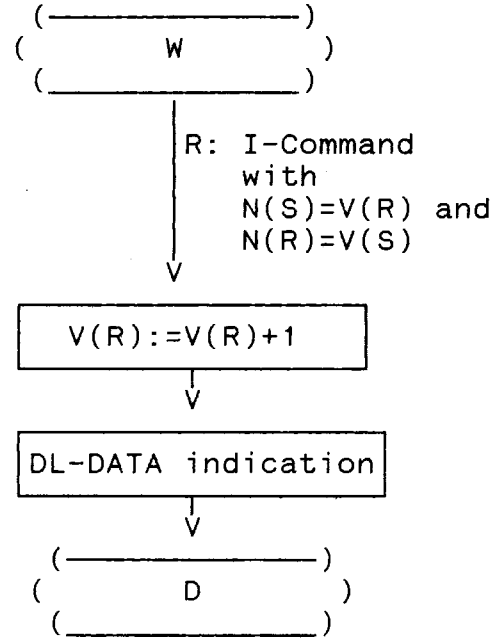
D 7.3.2.4.2 Sendeprotokoll 2 (mit Zeitüberwachungsanforderung)



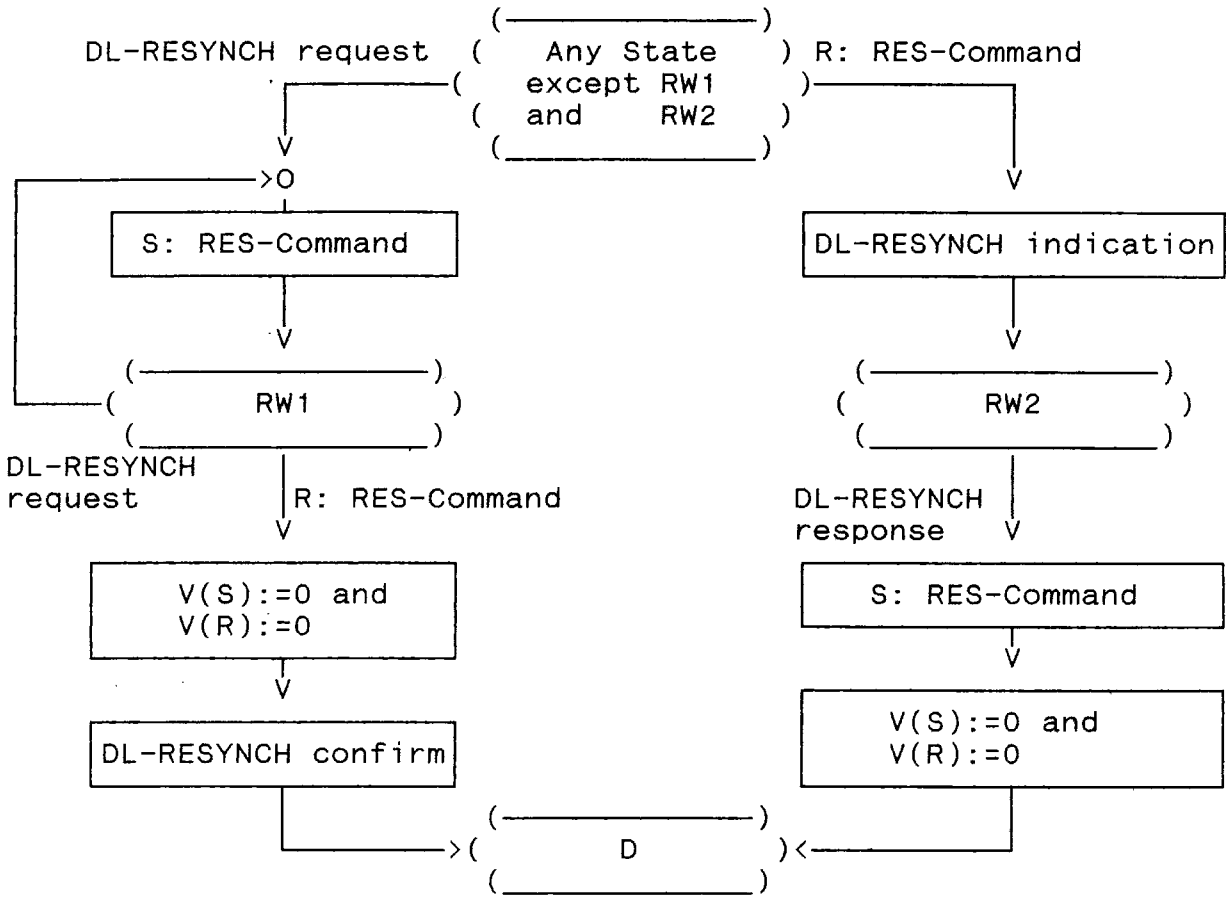
D 7.3.2.4.3 Empfangsprotokoll 1 (ohne Zeitüberwachung)



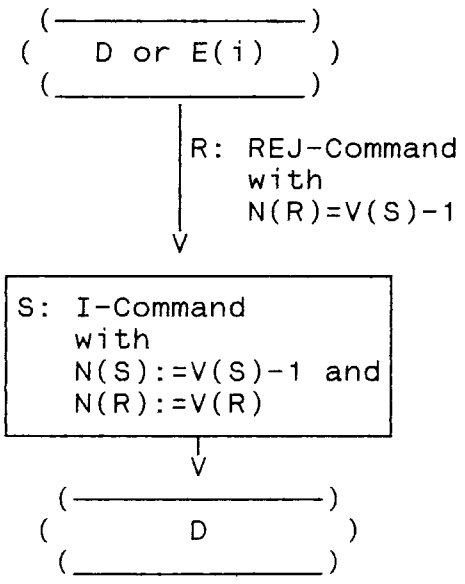
D 7.3.2.4.4 Empfangsprotokoll 2 (mit Zeitüberwachung)



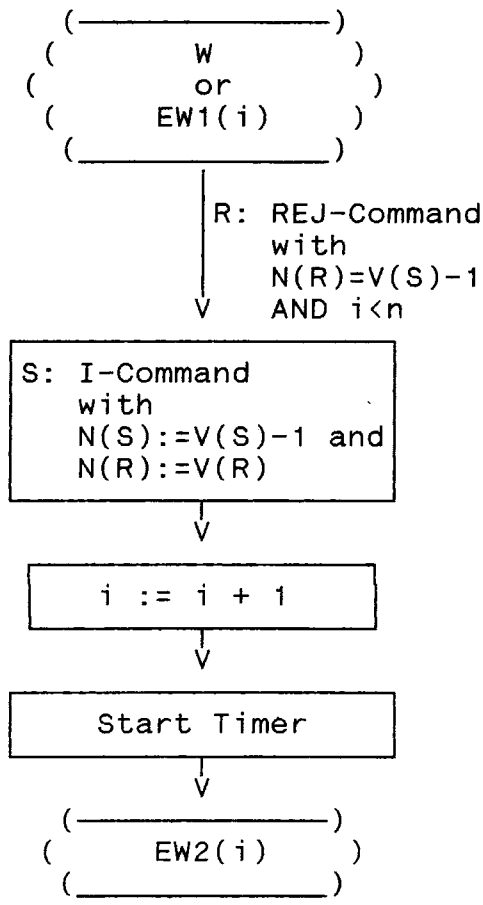
D 7.3.2.4.5 Resynchronisierungsprotokoll



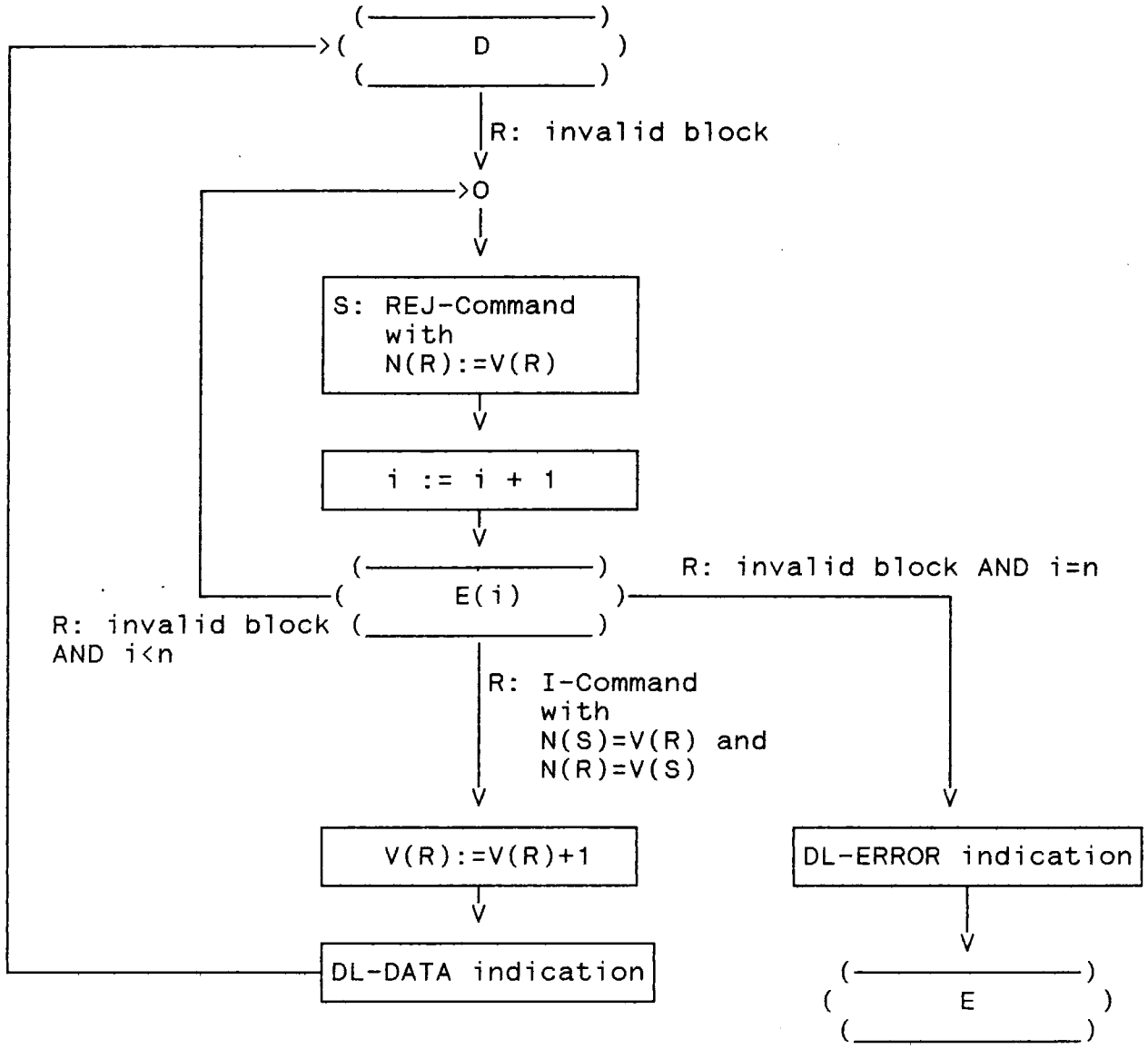
D 7.3.2.4.6 Fehlerbehandlungsprotokoll 1



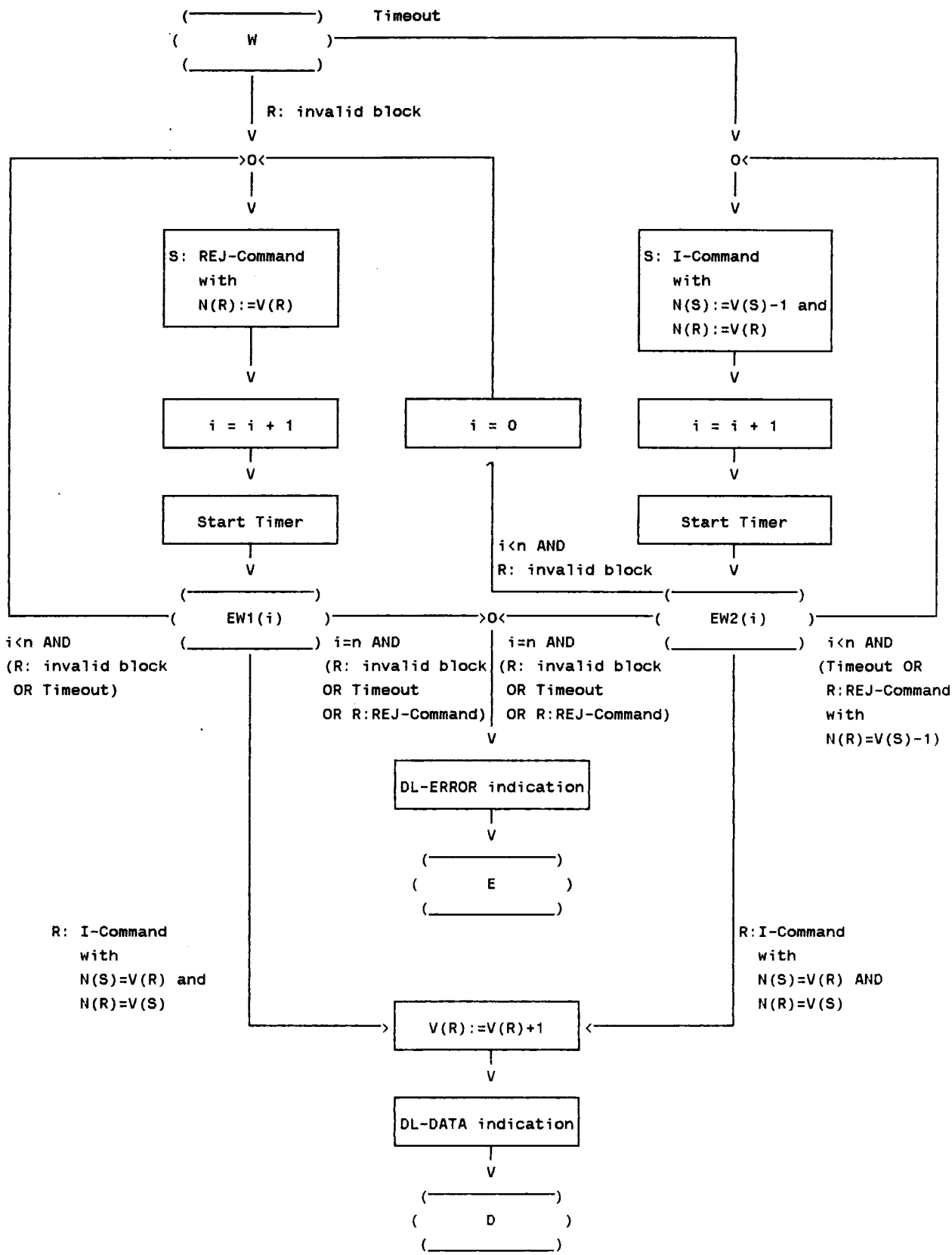
D 7.3.2.4.7 Fehlerbehandlungsprotokoll 2



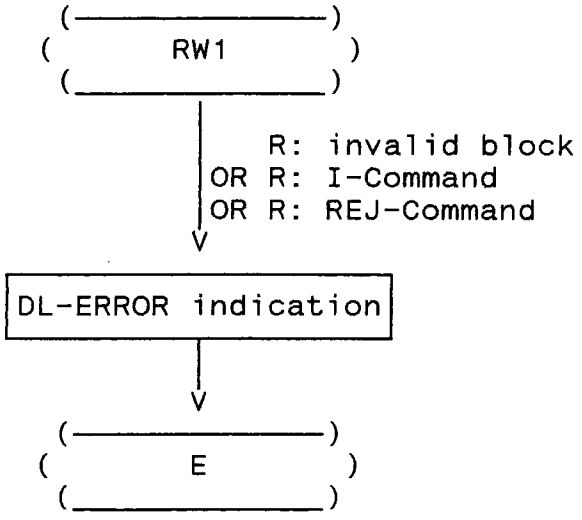
D 7.3.2.4.8 Fehlerbehandlungsprotokoll 3



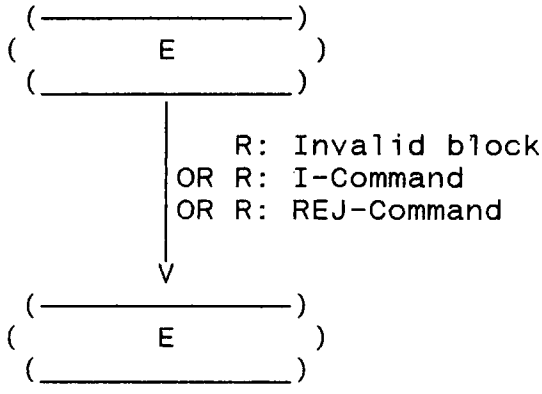
D 7.3.2.4.9 Fehlerbehandlungsprotokoll 4



D 7.3.2.4.10 Fehlerbehandlungsprotokoll 5



D 7.3.2.4.11 Fehlerbehandlungsprotokoll 6



Hinweis:

Im Abschnitt E befindet sich die Beschreibung einer abwärtskompatiblen Untermenge des hier getroffenen Protokolls für einfachere Anwendungen.

D 7.3.2.5 Zustandstabelle für die Protokollmaschine der Schicht 2

Transition	Ausgangszustand	Ereignis	Aktion(en)	Zielzustand
1	D	DL-DATA request (Param. Timer Control OFF)	S:I-Command with N(S):=V(S) and N(R):=V(R) --- V(S):=V(S)+1	D
2	D	DL-DATA request (Param. Timer Control ON)	S:I-Command with N(S):=V(S) and N(R):=V(R) --- V(S):=V(S)+1 --- Start Timer	W
3	D	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	D
4	D	DL-RESYNCH req.	S:RES-Command	RW1
5	D	R:RES-Command	DL-RESYNCH ind.	RW2
6	D	R:REJ-Command with N(R)=V(S)-1	S:I-Command with N(S):=V(S)-1 and N(R):=V(R)	D
7	D	R:invalid block	S:REJ-Command with N(R):=V(R) --- i:=i+1	E(i)
8	W	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	D
9	W	DL-RESYNCH req.	S:RES-Command	RW1
10	W	R:RES-Command	DL-RESYNCH ind.	RW2

Tran-sition	Ausgangs-zustand	Ereignis	Aktion(en)	Ziel-zustand
11	W	R:REJ-Command with N(R)=V(S)-1	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EW2(i)
12	W	R:invalid block	S:REJ-Command with N(R):=V(R) --- i:=i+1 --- Start Timer	EW1(i)
13	W	Timeout	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EW2(i)
14	RW1	R:RES-Command	V(S):=0 and V(R):=0 --- DL-RESYNCH conf.	D
15	RW1	DL-RESYNCH req.	S:RES-Command	RW1
16	RW1	R:invalid block OR R:I-Command OR R:REJ-Command	DL-ERROR indic.	E
17	RW2	DL-RESYNCH res.	S:RES-Command --- V(S):=0 and V(R):=0	D
18	E(i)	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	D
19	E(i)	DL-RESYNCH req.	S:RES-Command	RW1

Tran-sition	Ausgangs-zustand	Ereignis	Aktion(en)	Ziel-zustand
20	E(i)	R:RES-Command	DL-RESYNCH ind.	RW2
21	E(i)	R:REJ-Command with N(R)=V(S)-1	S:I-Command with N(S):=V(S)-1 and N(R):=V(R)	D
22	E(i)	R:invalid block AND i<n	S:REJ-Command with N(R):=V(R) --- i:=i+1	E(i)
23	E(i)	R:invalid block AND i=n	DL-ERROR indic.	E
24	EW1(i)	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	D
25	EW1(i)	DL-RESYNCH req.	S:RES-Command	RW1
26	EW1(i)	R:RES-Command	DL-RESYNCH ind.	RW2
27	EW1(i)	R:REJ-Command with N(R)=V(S)-1 AND i<n	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EW2(i)
28	EW1(i)	(R:invalid bl. OR Timeout) AND i<n	S:REJ-Command with N(R):=V(R) --- i:=i+1 --- Start Timer	EW1(i)
29	EW1(i)	(R:invalid bl. OR Timeout OR R:REJ-Comm.) AND i=n	DL-ERROR indic.	E
30	EW2(i)	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	D

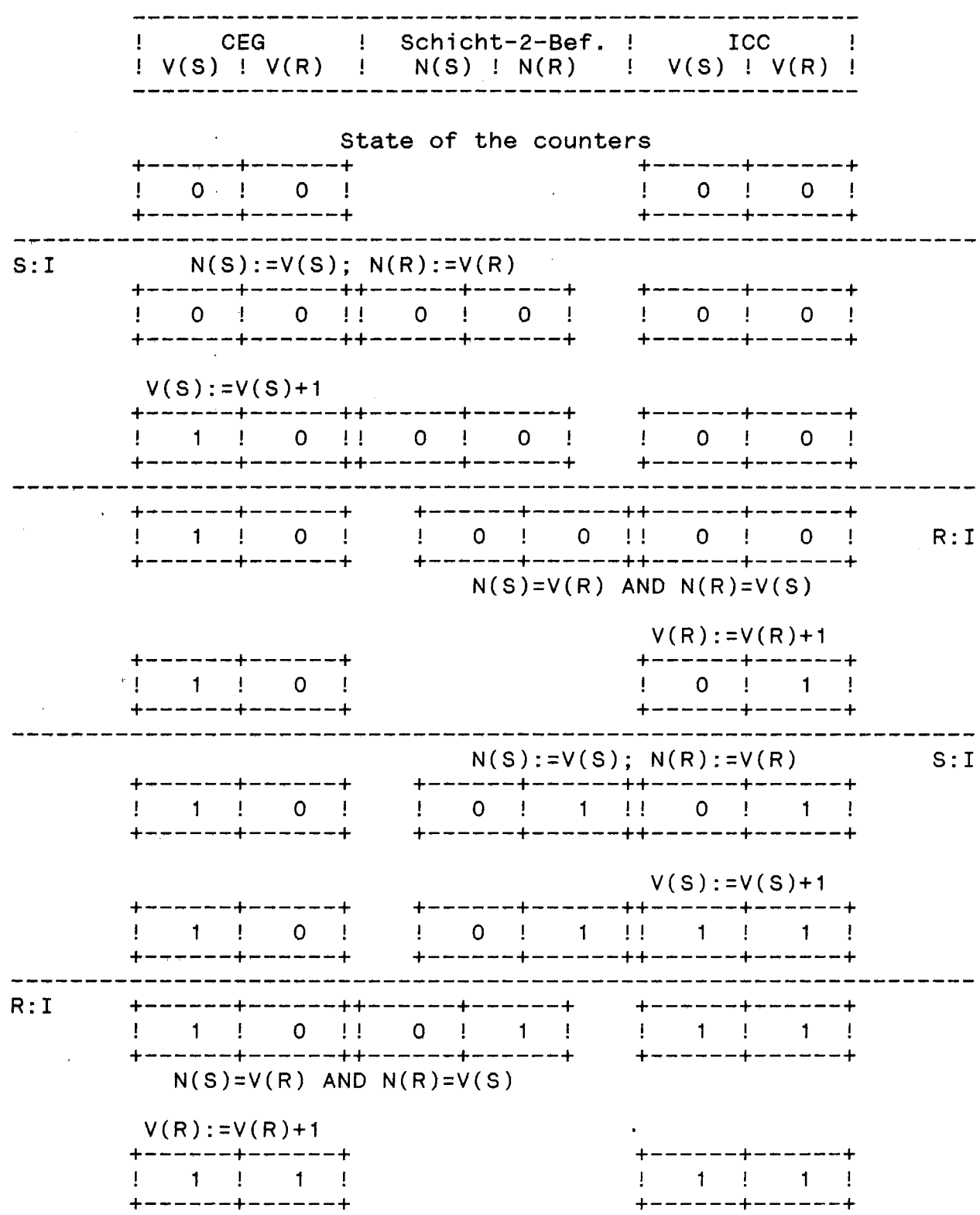
Tran-sition	Ausgangs-zustand	Ereignis	Aktion(en)	Ziel-zustand
31	EW2(i)	DL-RESYNCH req.	S:RES-Command	RW1
32	EW2(i)	R:RES-Command	DL-RESYNCH ind.	RW2
33	EW2(i)	R:REJ-Command with N(R)=V(S)-1 AND i<n	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EW2(i)
34	EW2(i)	Timeout AND i<n	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EW2(i)
35	EW2(i)	R:invalid block AND i<n	S:REJ-Command with N(R):=V(R) --- i:=1 --- Start Timer	EW1(i)
36	EW2(i)	(R:invalid bl. OR Timeout) OR R:REJ-Comm.) AND i=n	DL-ERROR indic.	E
37	E	DL-RESYNCH req.	S:RES-Command	RW1
38	E	R:RES-Command	DL-RESYNCH ind.	RW2
39	E	R:invalid block OR R:I-Command OR R:REJ-Command	(no action)	E

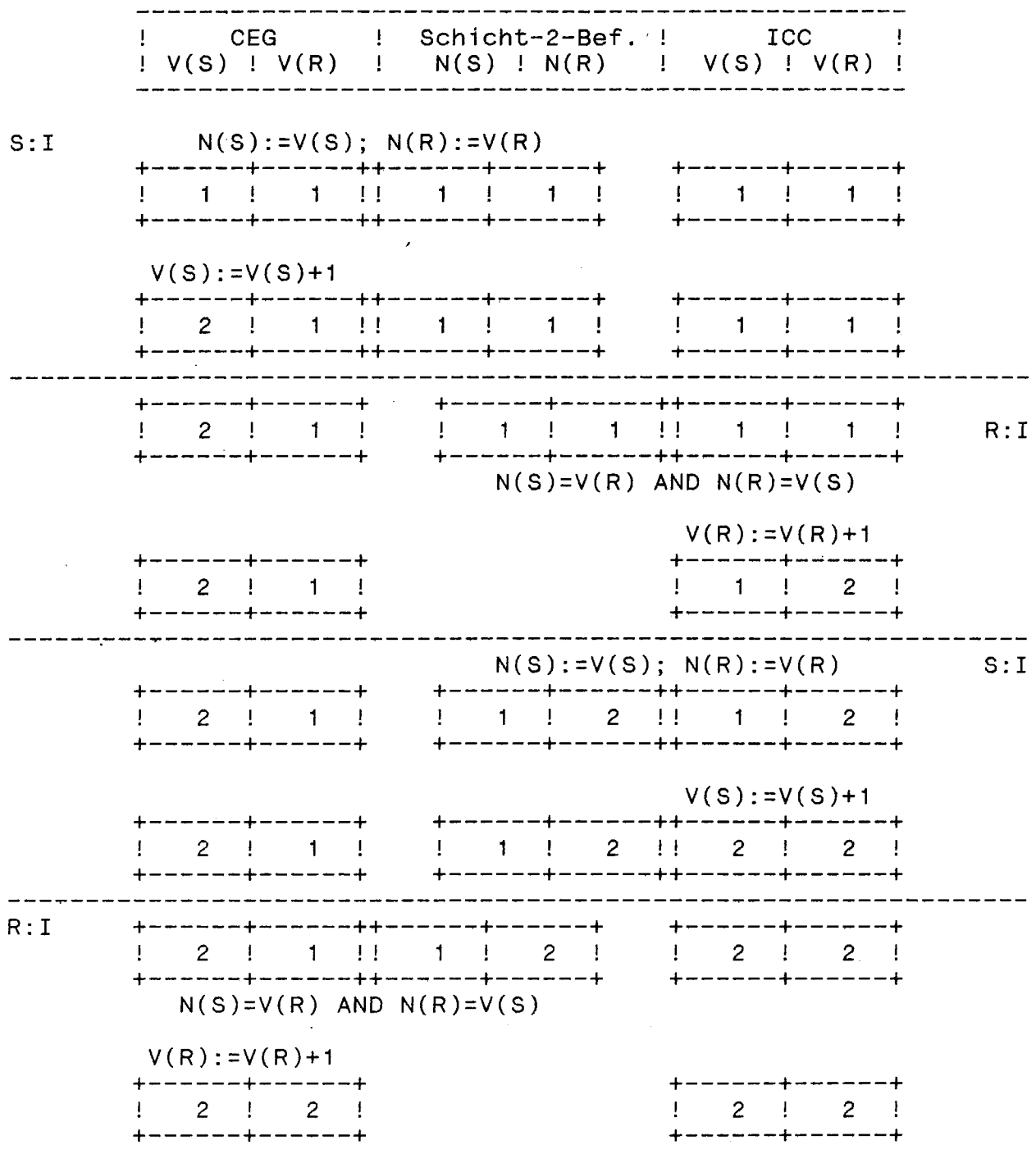
Hinweis:

Im Abschnitt E befindet sich die Beschreibung einer abwärtskompatiblen Untermenge des hier getroffenen Protokolls für einfachere Anwendungen.

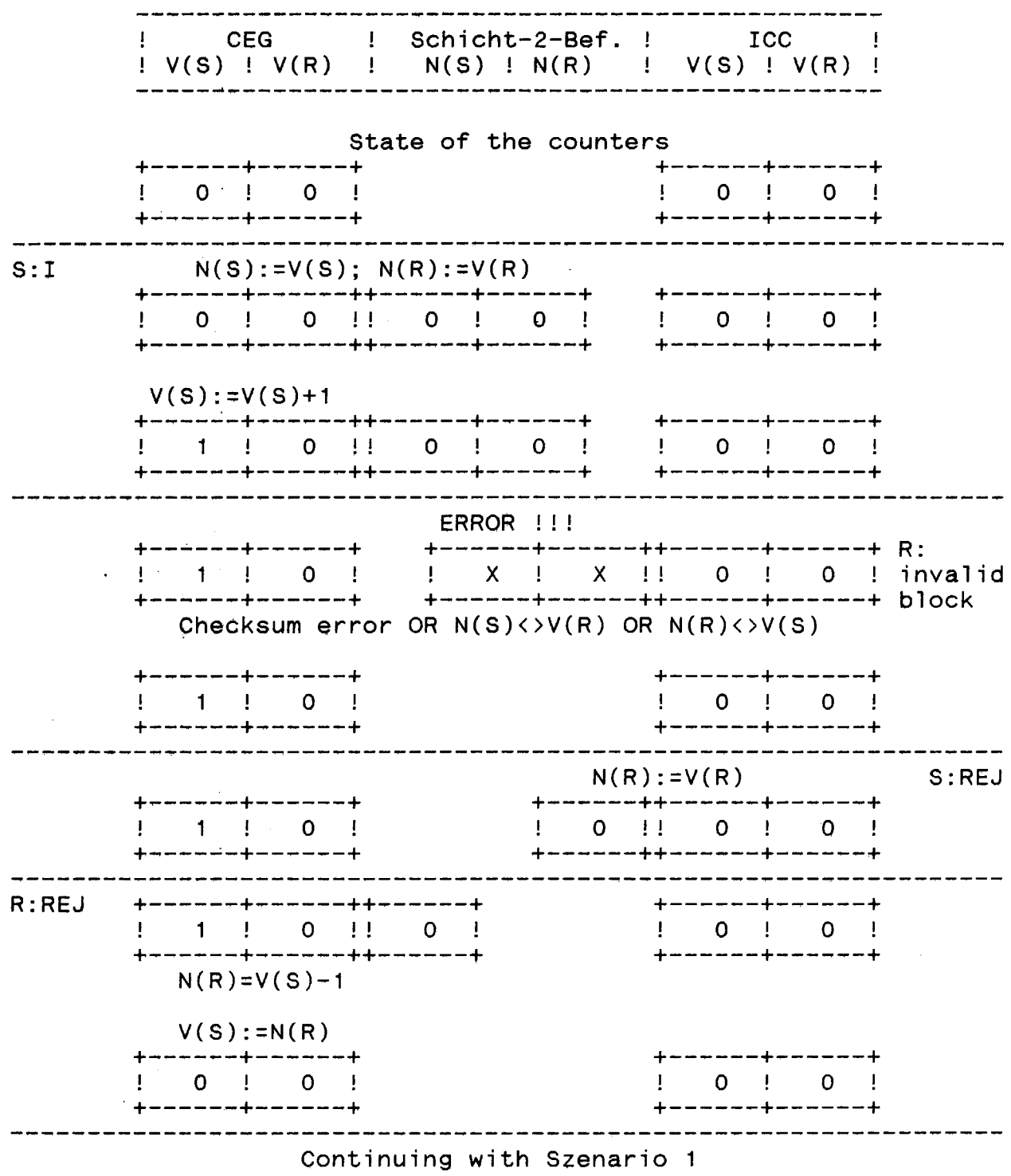
D 7.4 Beispiele zur Verdeutlichung des Folgezählermechanismus

D 7.4.1 Szenario 1: Korrekter Austausch von I-Befehlen

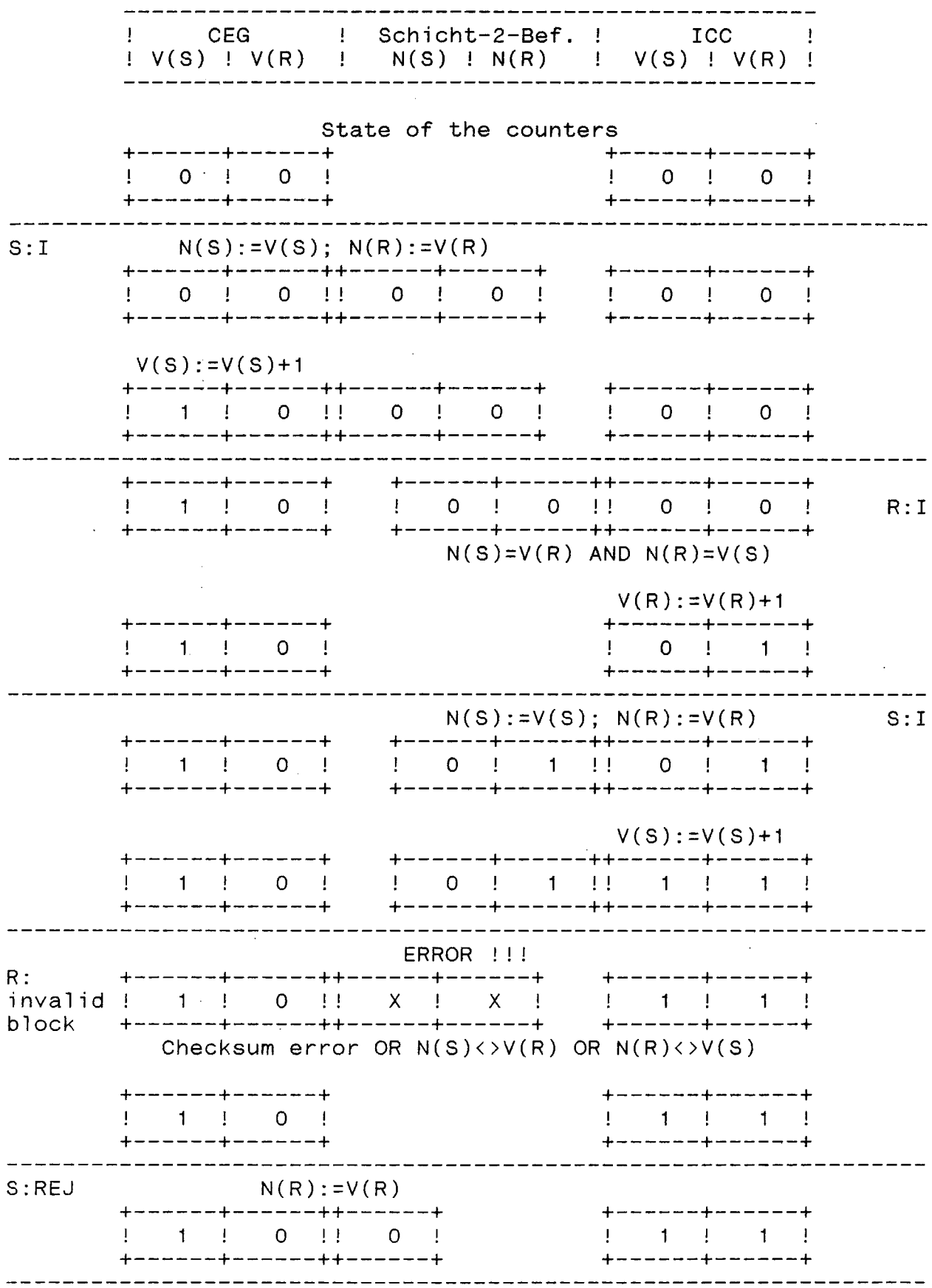


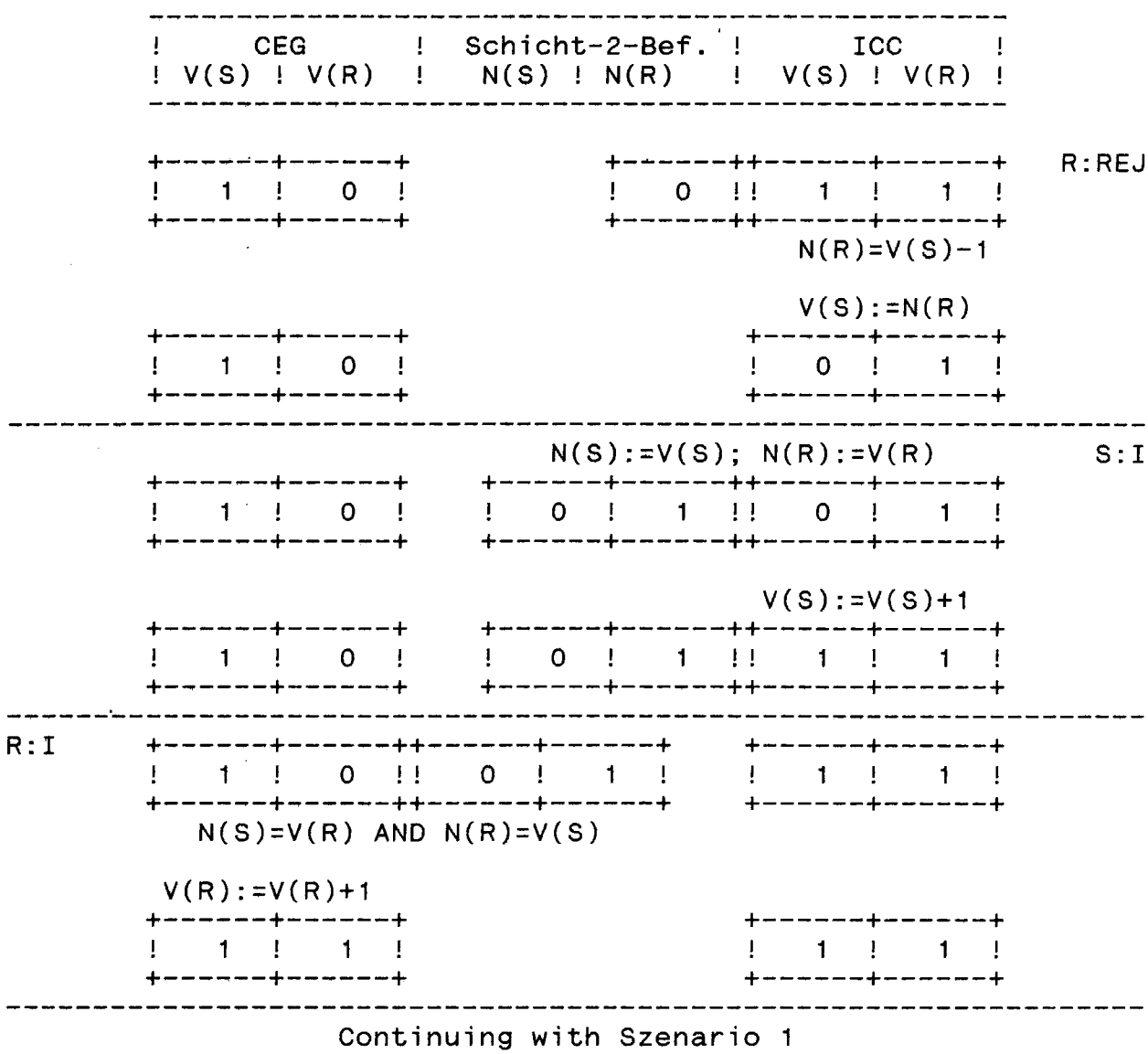

CEG
V(S) V(R)
Schicht-2-Bef.
N(S) N(R)
ICC
V(S) V(R)
S:I
N(S):=V(S); N(R):=V(R)
V(S):=V(S)+1
R:I
N(S)=V(R) AND N(R)=V(S)
V(R):=V(R)+1
S:I
N(S):=V(S); N(R):=V(R)
V(S):=V(S)+1
R:I
N(S)=V(R) AND N(R)=V(S)
V(R):=V(R)+1

D 7.4.2 Szenario 2: Fehler nach Senden eines I-Befehls vom CEG



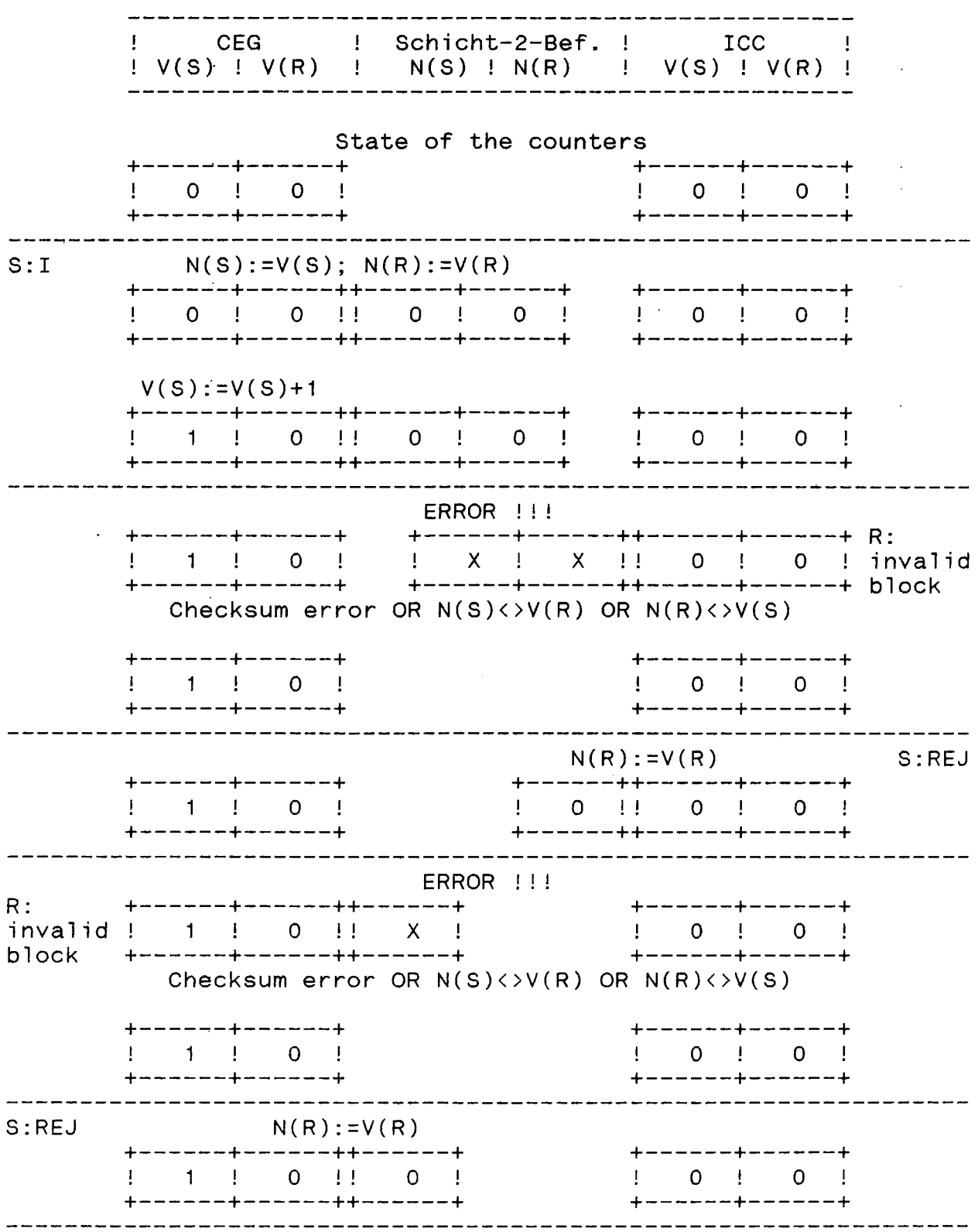
D 7.4.3 Szenario 3: Fehler nach Senden eines I-Befehls vom ICC

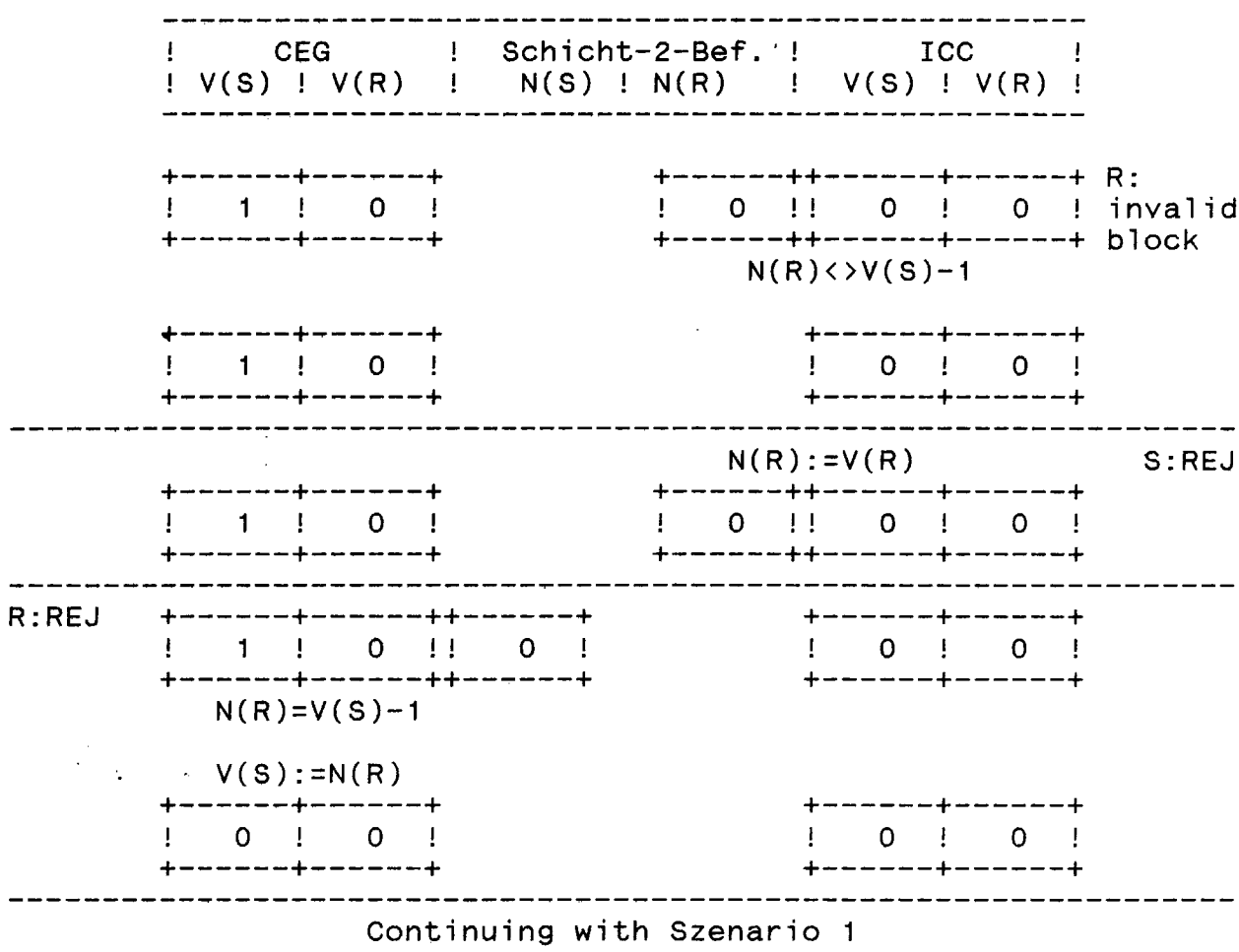




Continuing with Szenario 1

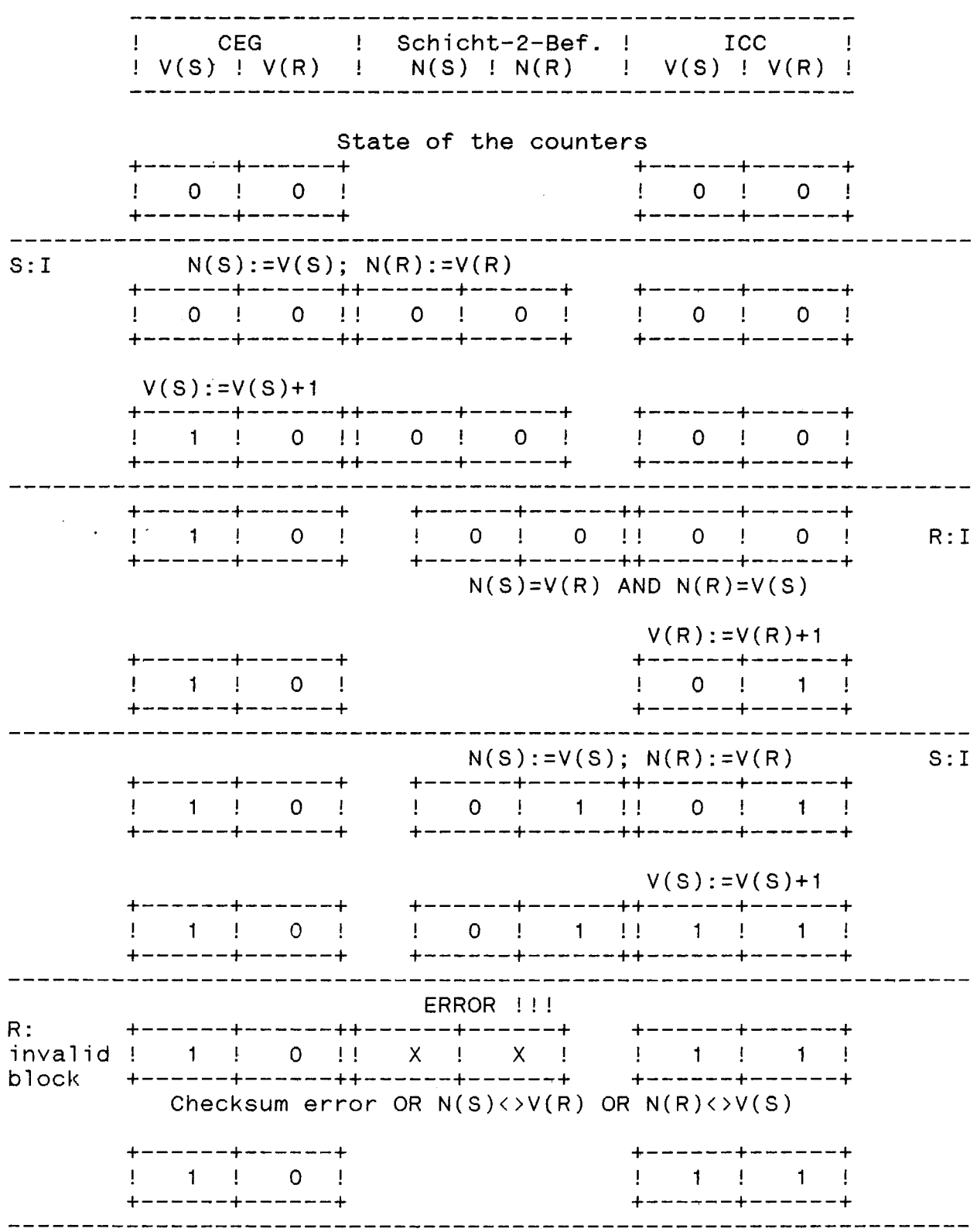
D 7.4.4 Szenario 4: Fehler nach Senden eines I-Befehls vom CEG und nach dem darauffolgenden Senden eines REJ-Befehls vom ICC

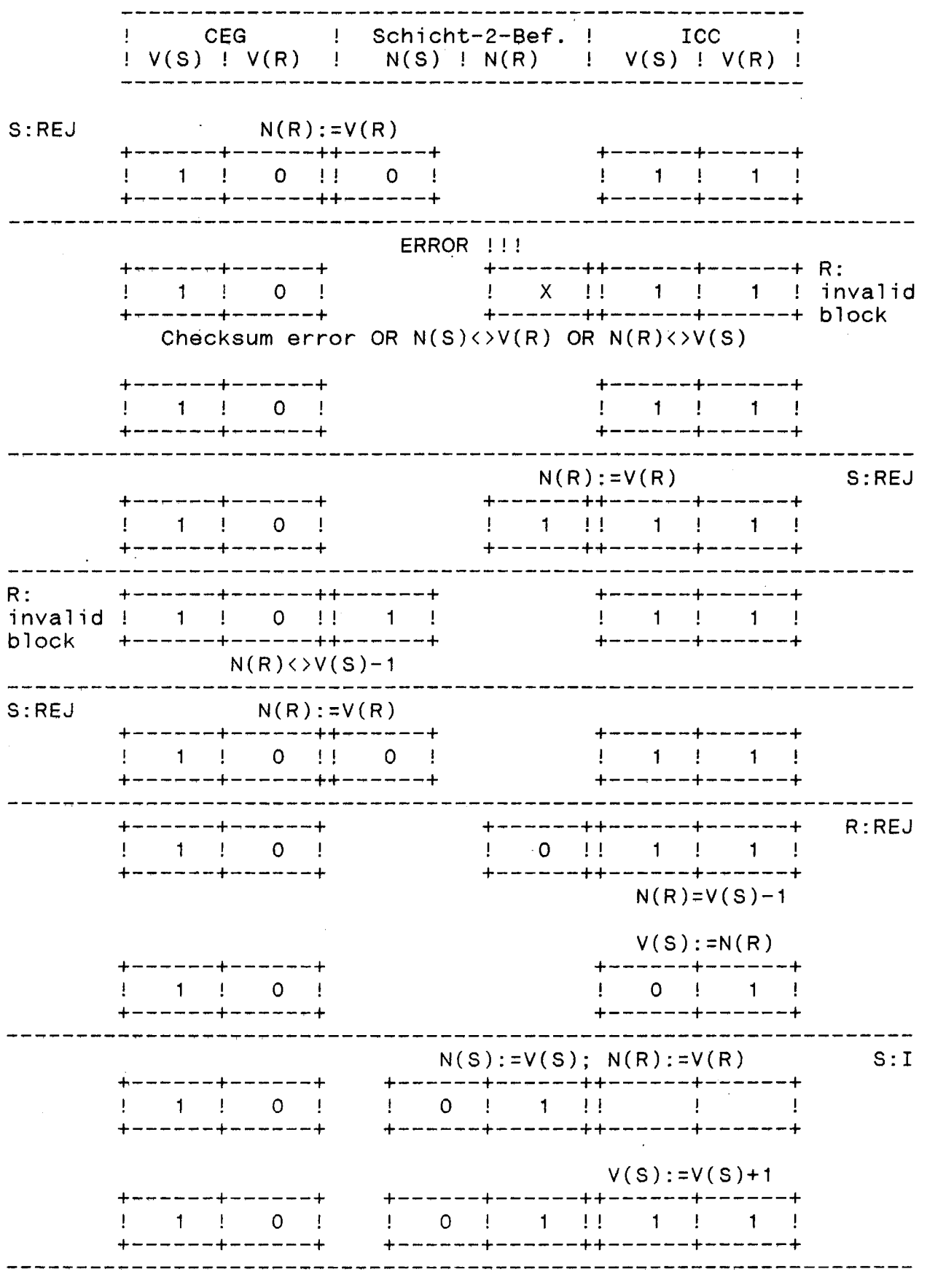


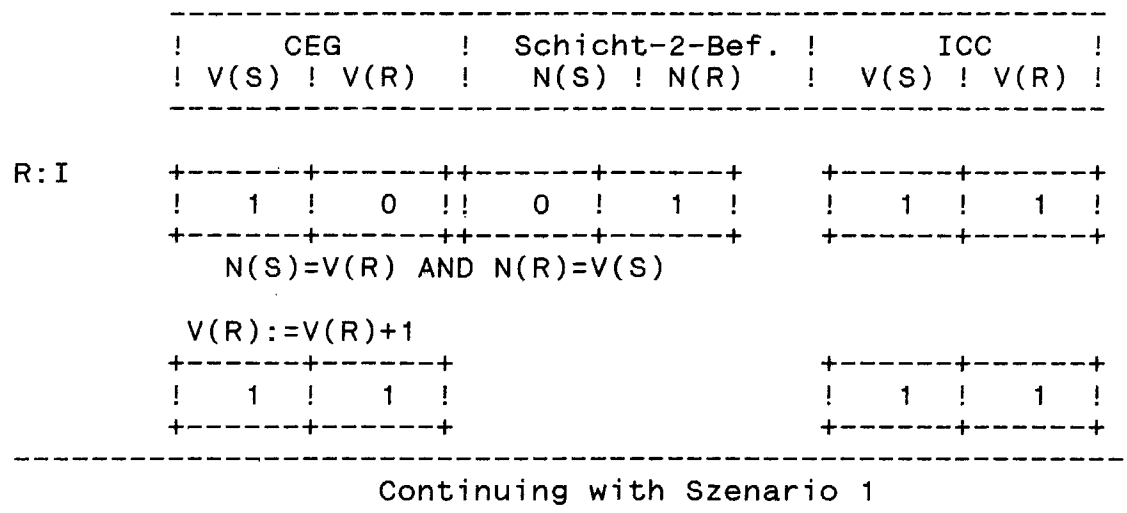


Continuing with Szenario 1

D 7.4.5 Szenario 5: Fehler nach Senden eines I-Befehls vom ICC und nach dem darauffolgenden Senden eines REJ-Befehls vom CEG




CEG
V(S) V(R)
Schicht-2-Bef.
N(S) N(R)
ICC
V(S) V(R)
S:REJ
N(R):=V(R)
1 0 0 1 1
ERROR !!!
1 0 X 1 1
R: invalid block
Checksum error OR N(S)<>V(R) OR N(R)<>V(S)
1 0 1 1
N(R):=V(R)
S:REJ
1 0 1 1 1
R: invalid block
N(R)<>V(S)-1
S:REJ
N(R):=V(R)
1 0 0 1 1
R:REJ
1 0 0 1 1
N(R)=V(S)-1
V(S):=N(R)
1 0 0 1 1
S:I
N(S):=V(S); N(R):=V(R)
1 0 0 1 1
V(S):=V(S)+1
1 0 0 1 1 1 1



Continuing with Szenario 1

D 8 Protokoll im Interface Control Layer (ICL)

Es gibt anwendungsbezogene Funktionen, die einerseits nichts mit der eigentlichen Blockübertragung der Schicht 2 und nichts mit denjenigen anwendungsorientierten Funktionen zu tun haben, welche sich auf die Kommunikation zwischen dem lokalen oder einem entfernten Datenendgerät und der Chipkarte beziehen. Diese Funktionen werden der ICL-Schicht zugeordnet, welche oberhalb der Schicht 2 und unterhalb der Schicht 7 liegt.

Folgende ICL-Anwendungsfunktionen sind definiert worden:

- Chaining (Verketten von Schicht-7-Daten)
- WT-Extension (Wartezeit-Verlängerung)
- Master/Slave-Kennzeichnung
- Off/On-line-Relevanz der Schicht-7-Daten
- Private Use Schicht-7-Protokoll
- Addendum-1 Schicht-7-Protokoll
- Dynamic Buffer Size (Dynamische Pufferverwaltung)
- Confirmation (Quittierung einer ICL-Anforderung)
- Error (Fehleranzeige für ICL-Anwendung)
- Abort/Terminate (Beendigung der ICL-Anwendung)

In der Schicht ICL gibt es Protokollelemente mit oder ohne zusätzlicher Schicht-7-Information. Sie heißen ICL-PDUs (ICL Protocol Data Units).

<table>
<tr><td colspan="3">Prolog</td><td colspan="7">Informationsfeld</td><td>Epilog</td></tr>
<tr><td colspan="3" rowspan="3"></td><td colspan="7">ICL - PDU</td><td rowspan="3"></td></tr>
<tr><td colspan="2">ICL-PCI</td><td colspan="5">Schicht-7-Information</td></tr>
<tr><td colspan="2"></td><td colspan="5">ICL-SDU</td></tr>
<tr><td>A</td><td>C</td><td>L</td><td>ICB1 ...</td><td>I</td><td>CLA</td><td>INS</td><td>DLNG</td><td>Daten..</td><td>CSUM</td></tr>
</table>

A = Adreßfeld, C = Steuerfeld, L = Übertragungsblocklänge
DLNG = Datenblocklänge, CSUM = Checksum (Kontrollsummenfeld)
ICL = ICL-Schicht, PDU = Protocol Data Unit
PCI = Protocol Control Information, SDU = Service Data Unit

Bild D 8.1: Formate

Die rein auf die Steuerung des ICL-Protokolls bezogenen Bytes (Interface Control Bytes, ICB) tragen den Namen ICL-PCI (ICL Protocol Control Information) und stehen am Anfang einer ICL-PDU. Die ICL-PCI bestehen aus einem oder mehreren Bytes. Das erste Byte heißt ICB1, das zweite ICB2, etc.

D 8.1 ICL-Anwendungsfunktionen

D 8.1.1 Chaining

Mit der Chaining-Funktion wird dem Empfänger angezeigt, daß die zur Schicht 7 gehörende Information logisch noch nicht abgeschlossen ist und mit der nächsten ICL-PDU fortgesetzt wird.

Auf jede ICL-PDU mit Schicht-7-Information und mit Chaining-Anzeige wird mit einer ICL-PDU ohne Schicht-7-Information, bei der Chaining- und Confirm-Anzeige kombiniert sind, geantwortet.

Für spezielle Steuerzwecke ist es erlaubt, ICL-PDUs mit Chaining-Anzeige jedoch ohne ICL-SDU zu übertragen.

Der Sender einer verketteten Schicht-7-Information kann das Verketten dadurch unterbrechen, indem er eine ICL-PDU mit Chaining- und zusätzlicher Error-Anzeige sendet. In diesem Fall gilt sämtliche beim Empfänger bisher aufgesammelte, logisch zusammengehörige, jedoch noch nicht abgeschlossene Schicht-7-Information als verworfen. Bestätigt wird diese Löschung mittels einer ICL-PDU mit Chaining-, Error- und Confirm-Anzeige.

Wird irgendeine ICL-PDU mit Schicht-7-Information und Chaining-Anzeige durch eine ICL-PDU mit Error-Anzeige beantwortet, so gilt alle bisher logisch zusammengehörige Schicht-7-Information als verworfen. Die ICL-PDU mit Error-Anzeige wird vom Sender der verketteten Schicht-7-Information durch eine ICL-PDU mit Error- und Confirm-Anzeige beantwortet. Der Empfänger letzterer ICL-PDU quittiert diese auf Schicht 2 mittels eines leeren I-Befehls.

D 8.1.2 Waiting Time Extension

Kann auf einen Request hin nicht innerhalb der maximalen Blockwartezeit BWT ein Response gegeben werden, so kann der Slave mittels einer ICL-PDU mit WT-Extension-Anzeige den Master um Verlängerung der Wartezeit auffordern. Der Master quittiert diese Aufforderung mit einer ICL-PDU mit WT-Extension- und Confirm-Anzeige. Der Master verweitert diese Aufforderung dadurch, daß er eine ICL-PDU mit WT-Extension und Error-Anzeige sendet. Der Slave beantwortet diese negative Quittung mit Error- und Confirm-Anzeige.

D 8.1.3 Master/Slave

Ein ICL-Request wird in der entsprechenden ICL-PDU durch eine Master-Anzeige gekennzeichnet. Ein ICL-Response wird entsprechend durch eine Slave-Anzeige gekennzeichnet.

Will der Master ein Slave werden, so signalisiert er dies durch eine ICL-PDU ohne Schicht-7-Information und mit Slave-Anzeige. Folgt darauf als Antwort eine ICL-PDU mit Master-Anzeige, so wurde der Rollentausch Master/Slave erfolgreich durchgeführt. Letztere ICL-PDU wird durch eine ICL-PDU mit Slave- und Confirm-Anzeige beantwortet, wenn die ICL-PDU des neuen Masters keinen zu

beantwortenden Request enthält.

Folgt dagegen die Beantwortung auf die erstere ICL-PDU des Masters mit Slave-Anzeige durch eine ICL-PDU mit Slave-Anzeige vom Slave, so wurde der Rollentausch nicht vorgenommen.

Will der Slave ein Master werden, so teilt er diesen Wunsch dem Master dadurch mit, daß er in einer Response die Master-Anzeige mitsendet. Der Master wird daraufhin zum Slave mittels des zuvor beschriebenen Verfahrens. Wenn der Master nicht seine Rolle abgeben möchte, enthält der folgende ICL-Request (ICL-PDU) die Master- und die Confirm-Anzeige.

D 8.1.4 Off/On-line-Relevanz der Schicht-7-Daten

Die Off/On-line-Anzeige gibt an, ob die Schicht-7-Information in einer ICL-PDU vom lokalen (Off-line) Chipkarten-Endgerät oder entfernten (On-line) Datenendgerät stammen bzw. dorthin gesendet werden sollen.

D 8.1.5 Private Use Protokoll

Sollen Nutzer-Daten der ICL-Schicht gänzlich anders als in diesem Normvorschlag festgelegt interpretiert werden, so wird dies über die Private-Use-Anzeige signalisiert.

D 8.1.6 ISO 7816-3/Kap.8-Schicht-7-Protokoll

Sollen Nutzer-Daten der ICL-Schicht gemäß ISO 7816-3/Kap.8 interpretiert werden, so wird dies durch die 7816-3/Kap.8-Anzeige signalisiert.

D 8.1.7 Dynamic Buffer Size

Diese Funktion wird nur dazu benutzt, um anzuzeigen, daß eine Puffergröße verfügbar ist, welche kleiner als die in TBi angezeigte Übertragungsblockgröße ist.

Die Chipkarte kann in einer ICL-PDU dem Chipkarten-Endgerät mitteilen, wie groß die augenblickliche Puffergröße in ihrem Speicher ist. Solange die Chipkarte die Dynamic-Buffer-Size-Anzeige gesetzt hat, darf das Chipkarten-Endgerät der Chipkarte keine Übertragungsblöcke zuführen, die größer als die angezeigte Puffergröße sind. Wenn die Dynamic-Buffer-Size-Anzeige nicht gesetzt ist, gelten die ursprünglich bei Kommunikationsbeginn festgelegten Übertragungsblockgrößen.

D 8.1.8 Confirmation

Mit der Confirmation-Anzeige werden ICL-Protokoll-Anforderungen bestätigt. Der genaue Ablauf im Protokoll wird in der jeweiligen Anforderung beschrieben.

D 8.1.9 Error

Die Error-Anzeige wird dazu benutzt, einen logischen Fehler anzuzeigen. Dieser kann dadurch erkannt worden sein, daß eine ICL-PDU unplausibel ist oder der zeitliche Ablauf im ICL-Protokoll nicht eingehalten worden ist oder ein anderer allgemeiner Fehler vorliegt.

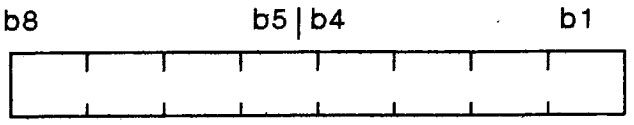
D 8.1.10 Abort/Terminate

Mit dieser Anzeige wird das ICL-Protokoll beendet. Als Terminate wird diese Anzeige interpretiert, wenn sie der Master in einer ICL-PDU ohne Schicht-7-Information als Request verwendet. Daraufhin wird eine ICL-PDU ohne Schicht-7-Information als Response mit Abort/Terminate- und Confirm-Anzeige gesendet.

Als Abort wird diese Anzeige interpretiert, wenn sie der Slave in einer beliebigen ICL-PDU ohne Schicht-7-Information als Response verwendet. Eventuell auftretende ICL-Nutzer-Daten gelten als verworfen.

D 8.2 Kodierung der ICL-Anwendungsfunktionen

D 8.2.1 Interface Control Byte 1 (ICB1)



ON-LINE-BIT
1 : On-line Daten
0 : Off-line Daten

CONFIRM-BIT
1 : Confirmation
0 : keine Bedeutung

MASTER/SLAVE (M/S) BIT
1 : Sender dieses Bits ist Master
0 : Sender dieses Bits ist Slave

WT-EXTENSION-BIT
1 : Request für WT-Extension
0 : keine Forderung nach WT-Extension

ABORT/TERMINATE BIT
1 : Abort/Terminate Request
0 : keine Bedeutung

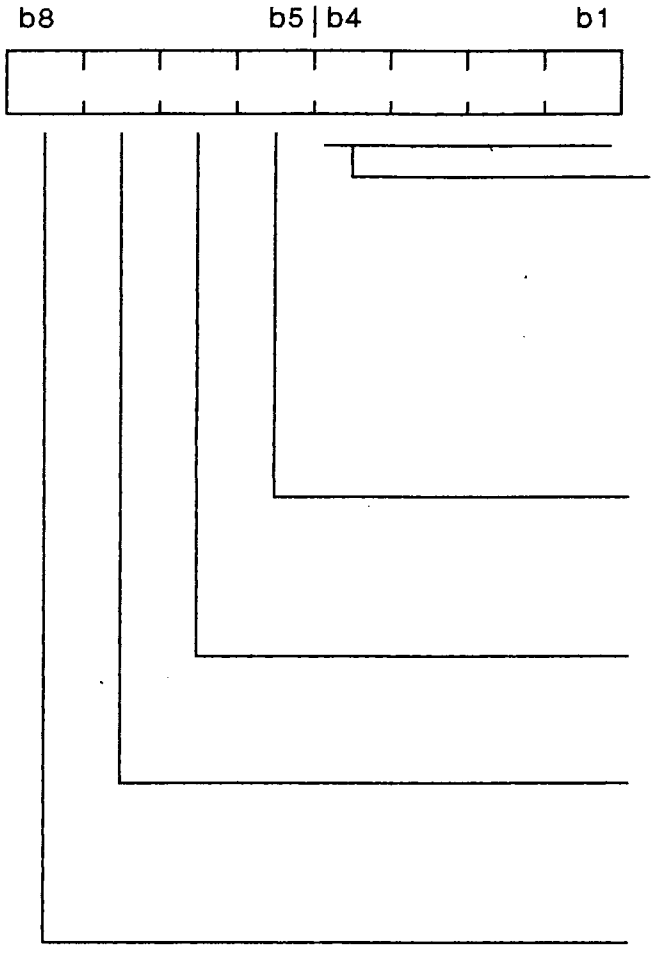
ERROR-BIT
1 : Fehleranzeige
0 : keine Bedeutung

CHAINING-BIT
1 : Weitere ICL-Nutzdaten folgen
0 : keine weiteren ICL-Nutzdaten folgen

ICB - EXTENSION-BIT
1 : ICB2 folgt
0 : kein weiteres ICB folgt

Bild D 8.2

D 8.2.2 Interface Control Byte 2 (ICB2)



BUFFER-SIZE
- b1 low order bit
  b4 high order bit
- Wertebereich: 1-15
- Die Puffergröße wird errechnet aus dem Wert in b4-b1 multipliziert mit dem Faktor 8.

DYNAMIC BUFFER SIZE BIT
1 : Puffergröße in b4-b1
0 : Bit b1-b5 keine Bedeutung

7816-3/Kap.8-BIT
1 : kompatibel mit 7816-3/8
0 : inkompatibel

PRIVATE USE BIT
1: ein Private-Use-Schicht-7-Protokoll wird ausgewertet
0: keine Bedeutung

ICB-EXTENSION-BIT
1 : ein weiteres ICB folgt
0 : kein weiteres ICB folgt

Bild D 8.3

E FuTel-Netz C spezifische Festlegungen

Für das FuTel-Netz C gelten die nachfolgenden Festlegungen, Ergänzungen, Einschränkungen und Änderungen für die genannten Punkte.

E 1 Festlegungen zu Abschnitt D

zu D 2 - D 5

Diese Punkte sind im Abschnitt A spezifiziert (Ausnahme: nachfolgende Anmerkung zu D 5.4).

zu D 5.4

Byterahmen

Durch den Byterahmen wird das Format und die Übertragung der Datenbytes bei Answer to Reset und der nachfolgenden Kommunikation bestimmt.

Das Format gilt gleichermaßen für den ANSWER TO RESET und die nachfolgende Kommunikation und ist wie folgt festgelegt:

1	Startbit	(low)
8	Datenbit	LSB first (bit 0 first)
1	Paritybit	even parity
2	Stopbit	(high)

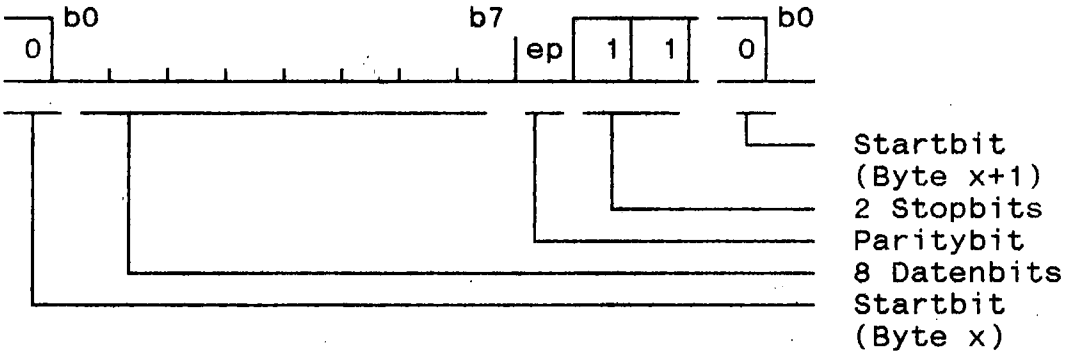


Bild E 1 : Byterahmen

Die Übertragung der Datenbytes (zeitliche Folge) unterscheidet sich bei der Übertragung von Answer to Reset und der Übertragung von Kommando und Antwort der nachfolgenden Kommunikation. Es genügt, ein Stopbit auszuwerten.

ANSWER TO RESET

Der Abstand zwischen 2 Startbits muß genau 12 etu betragen, d.h. auf das letzte Stopbit eines Bytes folgt unmittelbar das Startbit des folgenden Bytes.

Kommunikation

Während der Kommunikation beträgt der zeitliche Abstand zwischen 2 Startbits mindestens 12 etu.

Die Zeit zwischen dem letzten Stopbit eines Bytes und dem Startbit eines folgenden wird durch die max. Character Waiting Time (Byte TC3 im Answer to Reset) bestimmt.

Elemetary time unit

Die elementary time unit (etu) bezeichnet die Zeiteinheit für ein Bit auf I/O.

$$1\ \text{etu} = \frac{fo}{fs * 4800}\ (s)$$

fo = 2,4576 MHz
fs siehe A 2.3.4

zu D 6 Answer to Reset

Die Summe der von der ICC gesendeten Byte, bestehend aus Answer to Reset, Checkbyte und nachfolgenden Byte, beträgt maximal 33 Byte.
Kann die ICC T = 14 nicht verarbeiten, was vom CEG durch die Auswertung des ATR erkannt wird, ist dem Benutzer anzuzeigen, daß die Kommunikation mit der ICC nicht möglich ist.

zu D 6.2 Global Characters

zu D 6.2.1 TS, Initial Character

Dieser Character wird immer von der ICC gesendet, wird jedoch vom CEG nicht ausgewertet, da bei T = 14 immer "direct conventions" gilt.

zu D 6.2.2 T0, Format Character

Dieser Character wird immer von der ICC gesendet. Er muß vom CEG ausgewertet werden, da erkannt werden muß, welche weiteren Character folgen.

zu D 6.3 Global Interface Characters

zu D 6.3.1-3 TA1, TB1, TC1:

Falls diese Characters von der ICC gesendet werden, werden sie vom CEG nicht ausgewertet.

zu D 6.3.4 TD1 und TDi (i=2,3,.....), Protokoll- und Folgebyte-anzeige

Falls diese Characters von der ICC gesendet werden, müssen sie vom CEG ausgewertet werden. Es muß erkannt werden, welche weiteren Characters folgen und auf welchen Protokolltyp sich diese beziehen. TD1 wird immer gesendet.

zu D 6.4 Protocol Specific Interface Characters

zu D 6.4.1 Interface Characters für alle Protokolltypen

zu D 6.4.1.1 TB2

Falls dieser Character von der ICC gesendet wird, wird er vom CEG nicht ausgewertet.

zu D 6.4.2 Interface Characters für den Protokolltyp T=0

zu D 6.4.2.1 TC2

Falls dieser Character von der ICC gesendet wird, wird er vom CEG nicht ausgewertet.

zu D 6.4.3 Interface Characters für den Protokolltyp T=1

zu D 6.4.3.1 TA2

Falls dieser Character von der ICC gesendet wird, wird er vom CEG nicht ausgewertet.

zu D 6.4.4 Interface Characters für den Protokolltyp T=14

zu D 6.4.4.1 TAi (i>2), Betriebsfrequenz

Falls dieser Character von der ICC gesendet wird, wird er vom CEG nicht ausgewertet.

zu D 6.4.4.2 TBi (i>2), Übertragungsblockgröße

Falls dieser Character von der ICC gesendet wird, wird er vom CEG nicht ausgewertet.

zu D 6.4.4.3 TCi (i>2), Character Waiting Time

Falls dieser Character von der ICC gesendet wird, kann er vom CEG ausgewertet werden. Das CEG muß sich auf den im ATR geforderten Wert einstellen. Für CWI = 0 oder > 3 arbeitet das CEG bei der nachfolgenden Übertragung mit CWI = 3. Wird dieser Character nicht von der ICC gesendet, so arbeitet das CEG mit CWI = 3 (Netz C-default).
Wird dieser Character nicht von CEG ausgewertet, so arbeitet das CEG für den Empfang mit CWI = 3. Beim Senden muß der Abstand zwischen 2 Startbit genau 12 etu betragen, d.h. auf das letzte Stopbit eines Bytes folgt unmittelbar das Startbit des folgenden Bytes.

zu D 6.4.4.4 TAi+1 (i>2), Block Waiting Time

Falls dieser Character von der ICC gesendet wird, muß er vom CEG ausgewertet werden. Das CEG muß sich auf den im ATR geforderten Wert einstellen. Für BWI = 0 oder > 8 arbeitet das CEG bei der nachfolgenden Übertragung mit BWI = 8.

Wird dieser Character nicht von der ICC gesendet, so arbeitet das CEG mit BWI = 8 (Netz C-default). Spätestens nach Ablauf der BWT + 10% ist mit dem erneuten Senden des Blocks zu beginnen.

zu D 6.4.4.5 TBi+1 (i>2), Protokollprofil-Anzeige

Falls dieser Character von der ICC gesendet wird, wird er vom CEG nicht ausgewertet.

zu D 6.5 Historical Characters

Falls Historical Characters von der ICC gesendet werden, werden diese vom CEG nicht ausgewertet.

zu D 6.6 TCK, Checkbyte für die Answer to Reset-Sequenz
Dieser Character ist vom CEG auszuwerten. Die Fehlerbehandlung ist entsprechend D 6.7 durchzuführen. TCK weist denjenigen Wert auf, der bei der Anwendung der Operation XOR von TS bis TCK das Ergebnis 0 liefert.

zu D 6.8 Protokollauswahl
Wenn das CEG keinen bzw. einen fehlerhaften PTS Response erhält, wird mittels Fehlermeldung die Reset-Fehlerprozedur (siehe Seite E-14) angestoßen. Als Fehler sind die beim ATR (D 6.7) beschriebenen Fehler zu erkennen. Ein weiterer Fehler liegt vor, wenn der Inhalt des PTS nicht gleich FF0E (hexadezimal) ist.

zu D 7.1.5 Endeerkennung eines Übertragungsblockes
Die Mindestgröße des CEG-Empfangspuffers ist abhängig von den realisierten Schicht 7-Leistungsmerkmalen, d.h. von den längsten zu erwartenden Schicht 7-Antworten.

zu D 7.1.6 Adreßfeld

Sendet das CEG einen Übertragungsblock, so wird das Adressfeld mit $31 belegt.Das CEG wertet das Adressfeld eines empfangenen Übertragungsblocks nicht aus.

zu D 7.1.7.3 RES-Befehl

Der Timer für die Überwachung der maximalen Antwortzeit (BWT) nach dem Senden eines RES-Befehls befindet sich in der ICL-Schicht und ist deshalb in Kapitel D 7.3.2 nicht dargestellt.

zu D 7.2.2.1 Ungültiger Block

Ein Block ist auch ungültig bei einer falschen Ckecksumme; ebenso bei einem falschen Format des REJ- oder RES-Befehls, d.h. das Feld Datenlänge enthält nicht den Wert $00 und/oder das Informationsfeld enthält Daten sowie wenn der zu empfangende Block länger als der Empfangspuffer des CEG ist.

zu D 7.2.2.2 Fehlerbehandlung
Meldet die Schicht 2 einen Fehler an die höhere Schicht, so ist ein RES-Befehl anzustoßen. Werden weitere Fehler gemeldet, so ist der RES-Befehl zu wiederholen. Führt auch der dritte Versuch nicht zum Erfolg ist mittels Fehlermeldung die Reset-

Fehlerprozedur (siehe Seite E-14) anzustoßen.

zu D 7.3.1.4 Tabelle für das Dienstprotokoll der Schicht 2

Da im Netz C immer ein Master-Slave-Verhältnis vorliegt (CEG = Master, ICC = Slave), entfallen sowohl beim CEG als auch bei der ICC Teile der Tabelle.
Die für das Netz C gültigen Tabellen sind nachfolgend dargestellt.

Tabelle für das Dienstprotokoll der Schicht 2 im CEG

darf folgen: / Auf:		Anfng zust.	DL-DATA req	DL-DATA ind	DL-RESYNCH req	DL-RESYNCH ind	DL-RESYNCH resp	DL-RESYNCH conf	DL-ERROR ind
DL-DATA	request	X		X		NA	NA	X	
	indic.		X			NA	NA		
DL-RE-SYNCH	request	X		X	X	NA	NA	X	X
	indic.					NA	NA		
	resp.					NA	NA		
	confirm				X	NA	NA		
DL-ERROR	indica-tion		X		X	NA	NA		

NA: nicht anwendbar

Tabelle für das Dienstprotokoll der Schicht 2 in der ICC

darf folgen: / Auf:		Anfng zust.	DL-DATA req	DL-DATA ind	DL-RESYNCH req	DL-RESYNCH ind	DL-RESYNCH resp	DL-RESYNCH conf	DL-ERROR ind
DL-DATA	request			X	NA			NA	NA
	indic.	X	X		NA		X	NA	NA
DL-RE-SYNCH	request	NA	NA	NA	NA	NA	NA	NA	NA
	indic.	X	X	X	NA		X	NA	NA
	resp.				NA	X		NA	NA
	confirm	NA	NA	NA	NA	NA	NA	NA	NA
DL-ERROR	indica-tion	NA	NA	NA	NA	NA	NA	NA	NA

NA: nicht anwendbar

zu D 7.3.2.5 Zustandstabelle für die Protokollmaschine der Schicht 2

Da im Netz C immer ein Master-Slave-Verhältnis vorliegt (CEG = Master, ICC = Slave), entfallen sowohl beim CEG als auch bei der ICC Teile der Protokollmaschine.

Die sich daraus ergebenden Protokollmaschinen für CEG und ICC sind in den nachfolgenden Tabellen und Bildern zusammengestellt.

Zustandstabelle für die Protokollmaschine der Schicht 2 im CEG

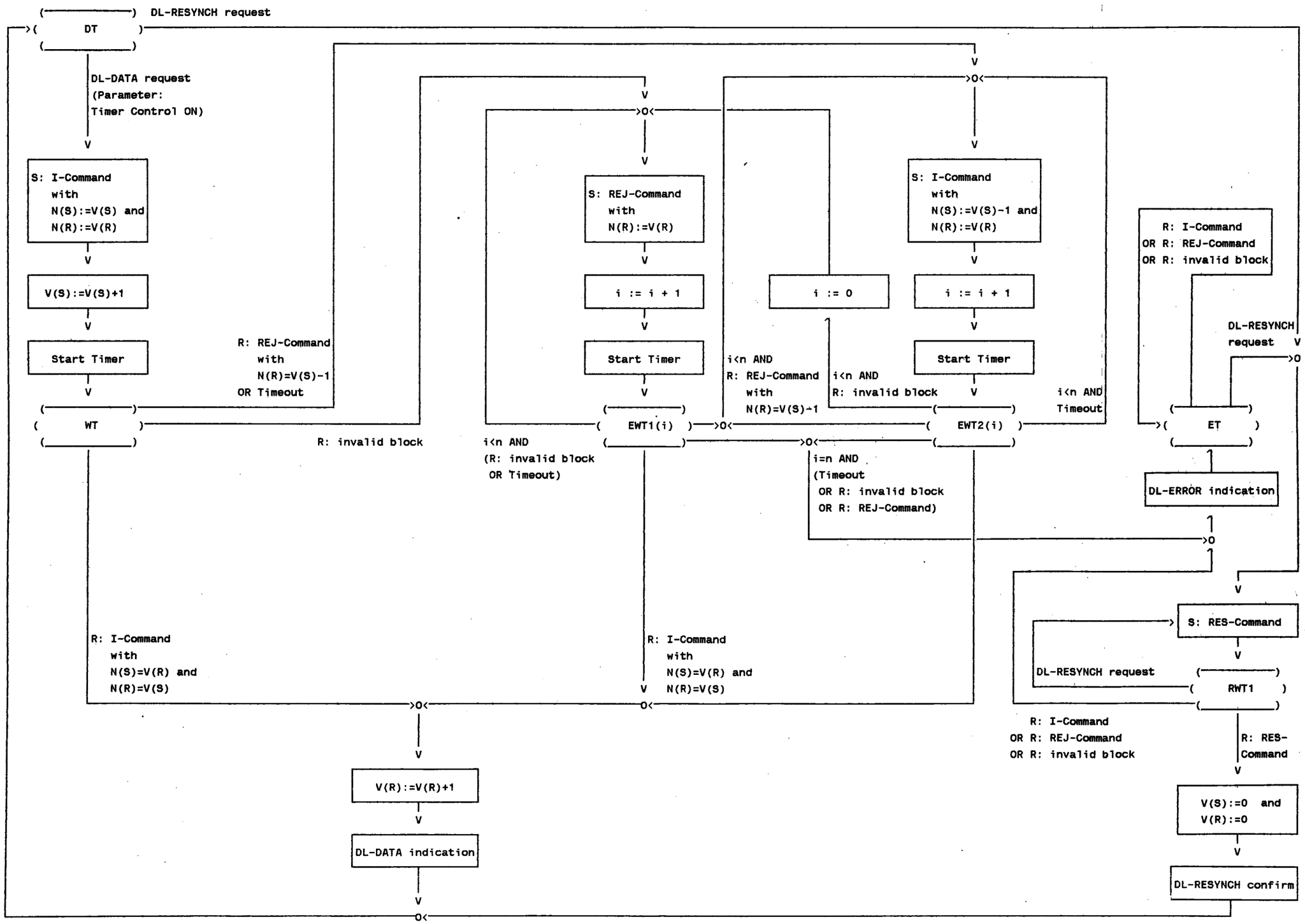
Transition	Ausgangszustand	Ereignis	Aktion(en)	Zielzustand
1 (2)	DT	DL-DATA request (Param. Timer Control ON)	S:I-Command with N(S):=V(S) and N(R):=V(R) V(S):=V(S)+1 Start Timer	WT
2 (4)	DT	DL-RESYNCH req.	S:RES-Command	RWT1
3 (8)	WT	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 DL-DATA indicat.	DT
4 (11)	WT	R:REJ-Command with N(R)=V(S)-1	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) i:=i+1 Start Timer	EWT2(i)
5 (12)	WT	R:invalid block	S:REJ-Command with N(R):=V(R) i:=i+1 Start Timer	EWT1(i)

Transition nach Abschnitt D 7.3.2.5

Tran-sition	Ausgangs-zustand	Ereignis	Aktion(en)	Ziel-zustand
6 (13)	WT	Timeout	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EWT2(i)
7 (14)	RWT1	R:RES-Command	V(S):=0 and V(R):=0 --- DL-RESYNCH conf.	DT
8 (15)	RWT1	DL-RESYNCH req.	S:RES-Command	RWT1
9 (16)	RWT1	R:invalid block OR R:I-Command OR R:REJ-Command	DL-ERROR indic.	ET
10(24)	EWT1(i)	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	DT
11(27)	EWT1(i)	R:REJ-Command with N(R)=V(S)-1 AND i<n	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EWT2(i)
12(28)	EWT1(i)	(R:invalid bl. OR Timeout) AND i<n	S:REJ-Command with N(R):=V(R) --- i:=i+1 --- Start Timer	EWT1(i)
13(29)	EWT1(i)	(R:invalid bl. OR Timeout) OR REJ-Command) AND i=n	DL-ERROR indic.	ET

Tran-sition	Ausgangs-zustand	Ereignis	Aktion(en)	Ziel-zustand
14(30)	EWT2(i)	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	DT
15(33)	EWT2(i)	R:REJ-Command with N(R)=V(S)-1 AND i<n	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EWT2(i)
16(34)	EWT2(i)	Timeout AND i<n	S:I-Command with N(S):=V(S)-1 and N(R):=V(R) --- i:=i+1 --- Start Timer	EWT2(i)
17(35)	EWT2(i)	R:invalid block AND i<n	S:REJ-Command with N(R):=V(R) --- i:=1 --- Start Timer	EWT1(i)
18(36)	EWT2(i)	(R:invalid bl. OR Timeout OR REJ-Command) AND i=n	DL-ERROR indic.	ET
19(37)	ET	DL-RESYNCH req.	S:RES-Command	RWT1
20(39)	ET	R:invalid block OR R:I-Command OR R:REJ-Command	(no action)	ET

Protokollmaschine der Schicht 2 im CEG



Durch das Rücksetzen des Zählers "i" in der Transition 17(35) entsteht eine Endlosschleife in der Schicht 2-Protokollmaschine des CEG, die unter bestimmten Fehlerbedingungen durchlaufen wird. Wird diese Endlosschleife eine längere Zeit durchlaufen, ist eine sinnvolle Kommunikation mit der ICC nicht mehr möglich. Dies muß durch eine der nachfolgend genannten Maßnahmen verhindert werden:

a) eine Timer in einer höheren Ebene überwacht die Schicht 2-Protokollmaschine und veranlaßt ggf. den Abbruch der Endlosschleife;

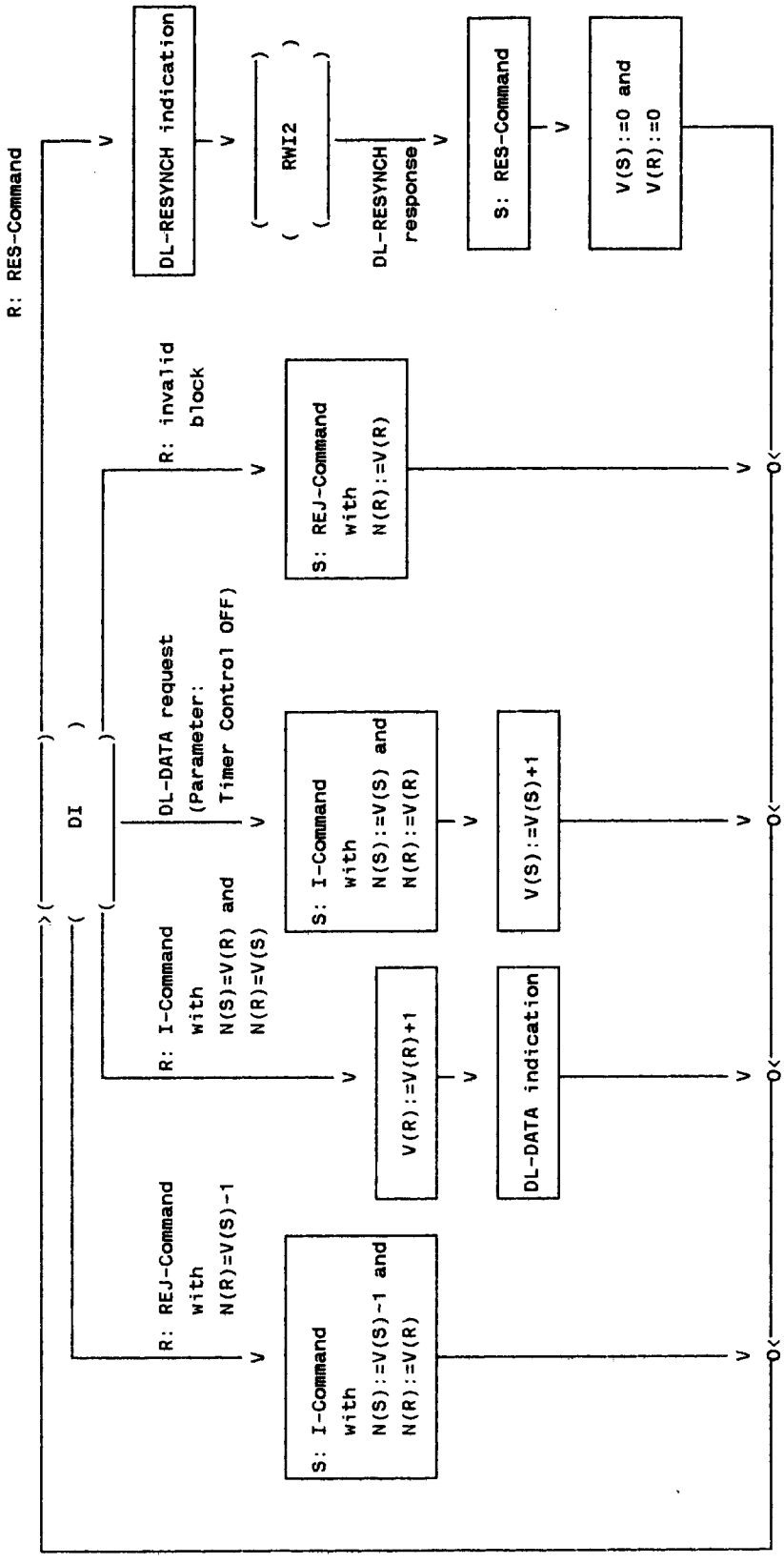
b) der Zähler "i" wird in der Transition 17(35) nicht auf Eins gesetzt, sondern um 1 erhöht. Die Transition 17(35) hat somit der nachfolgenden Darstellung zu entsprechen.

17(35)	EWT2(i)	R:invalid block AND i<n	S:REJ-Command with N(R):=V(R) --- i:=i+1 --- Start Timer	EWT1(i)

Zustandstabelle für die Protokollmaschine der Schicht 2 in der ICC

Transition	Ausgangszustand	Ereignis	Aktion(en)	Zielzustand
1 (1)	DI	DL-DATA request (Param. Timer Control OFF)	S:I-Command with N(S):=V(S) and N(R):=V(R) --- V(S):=V(S)+1	DI
2 (3)	DI	R:I-Command with N(S)=V(R) and N(R)=V(S)	V(R):=V(R)+1 --- DL-DATA indicat.	DI
3 (5)	DI	R:RES-Command	DL-RESYNCH ind.	RWI2
4 (6)	DI	R:REJ-Command with N(R)=V(S)-1	S:I-Command with N(S):=V(S)-1 and N(R):=V(R)	DI
5 (7)	DI	R:invalid block	S:REJ-Command with N(R):=V(R)	DI
6 (17)	RWI2	DL-RESYNCH res.	S:RES-Command --- V(S):=0 and V(R):=0	DI

Protokollmaschine der Schicht 2 in der ICC



zu D 8 Protokoll im Interface Control Layer (ICL)

In den im Netz C verwendeten Befehlen wird immer nur ein ICB-Byte genutzt.

Sendet das CEG einen Übertragungsblock, so wird das ICB1 mit $04 belegt. Das CEG prüft, ob das ICB1 eines empfangenen Übertragungsblocks $00 ist. Hat das ICB1 des empfangenen Übertragungsblocks einen Wert ungleich $00, so ist dieses Schicht 7- Kommando zu wiederholen. Tritt dieser Fehler auch nach dem 3. Versuch noch auf, ist mittels Fehlermeldung die Reset-Fehlerprozedur (siehe Seite E-14) anzustoßen.

E 2 Reset-Fehlerprozedur

Aufgrund von Fehlermeldungen wird durch erneutes Aktivieren der Reset-Leitung (bzw. Deaktivieren und Aktivieren der Karte bei einer Karte mit internem Reset) ein Reset ausgelöst.

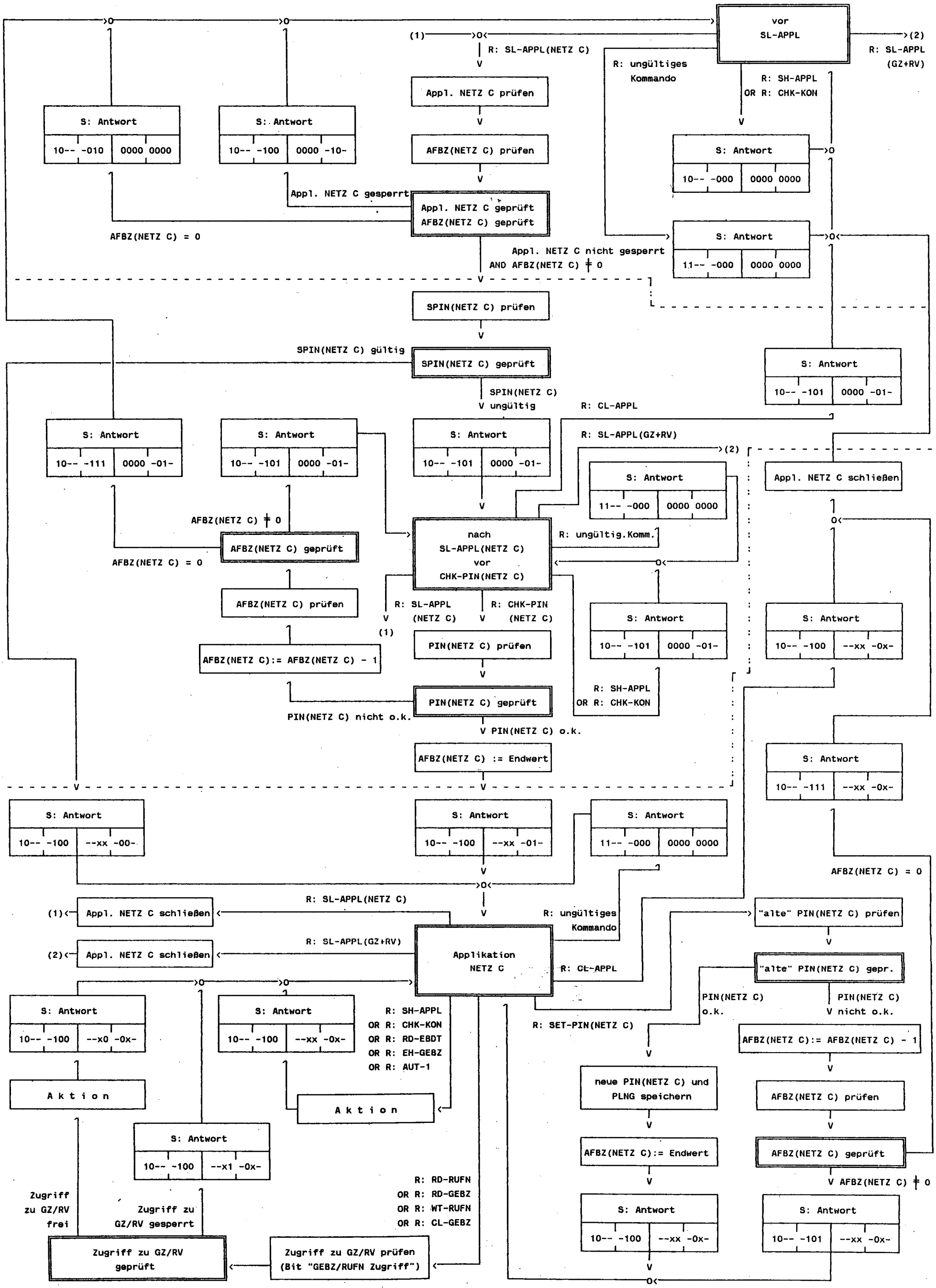
Ursache für Fehlermeldungen können

- ATR,
- Protokollauswahl,
- Schicht 2,
- Schicht ICL und
- Schicht 7

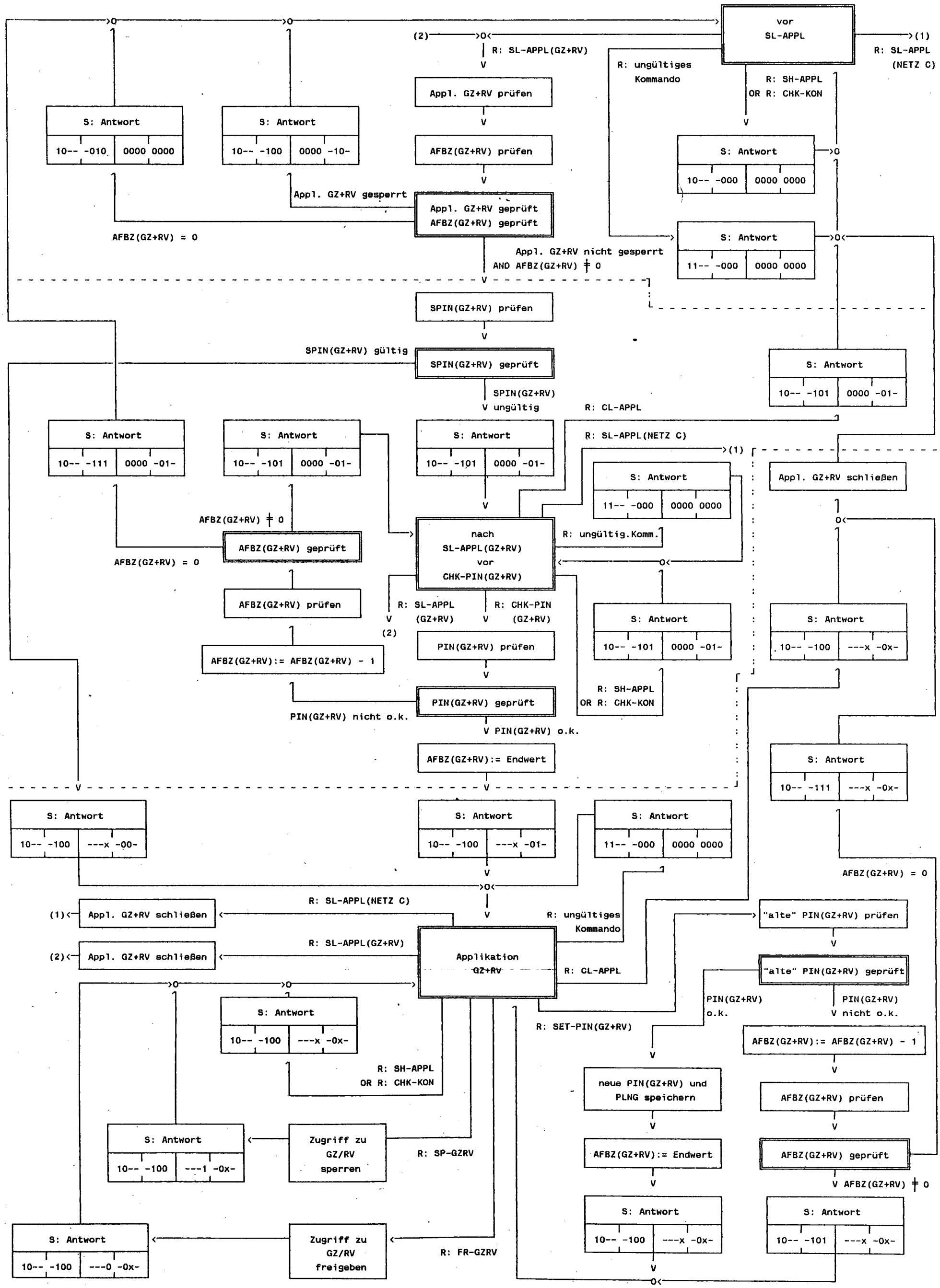
Fehler sein.

Treten nach dem ersten Reset noch weitere Fehlermeldungen auf, die durch eine Fehlerbehandlung in den jeweiligen Ebenen nicht beseitigt werden können, ist der Reset zu wiederholen. Treten auch nach dem 3. Versuch noch Fehlermeldungen auf, ist die Kommunikation mit der Chipkarte abzubrechen, d.h. die ICC ist zu deaktivieren. Ursachen können z.B. verschmutzte Kontakte, defekte Chipkarte oder defektes FuTelG sein. Dem Benutzer ist anzuzeigen, daß die Kommunikation mit der Karte nicht mehr möglich ist.

E 3 ICC-Ablaufdiagramm der Schicht 7 (Teil 1: Applikation NETZ C)



ICC-Ablaufdiagramm der Schicht 7 (Teil 2: Applikation GZ+RV)



E 4 Maximale Bearbeitungszeiten der Prozessorkarte

Die maximale Bearbeitungszeit ist die Zeit zwischen dem Absenden des letzten Stopbit des Request und dem Empfang des ersten Startbit des Response. Die angegebenen Zeiten gelten bei einer Taktfrequenz von 4.9152 MHz.

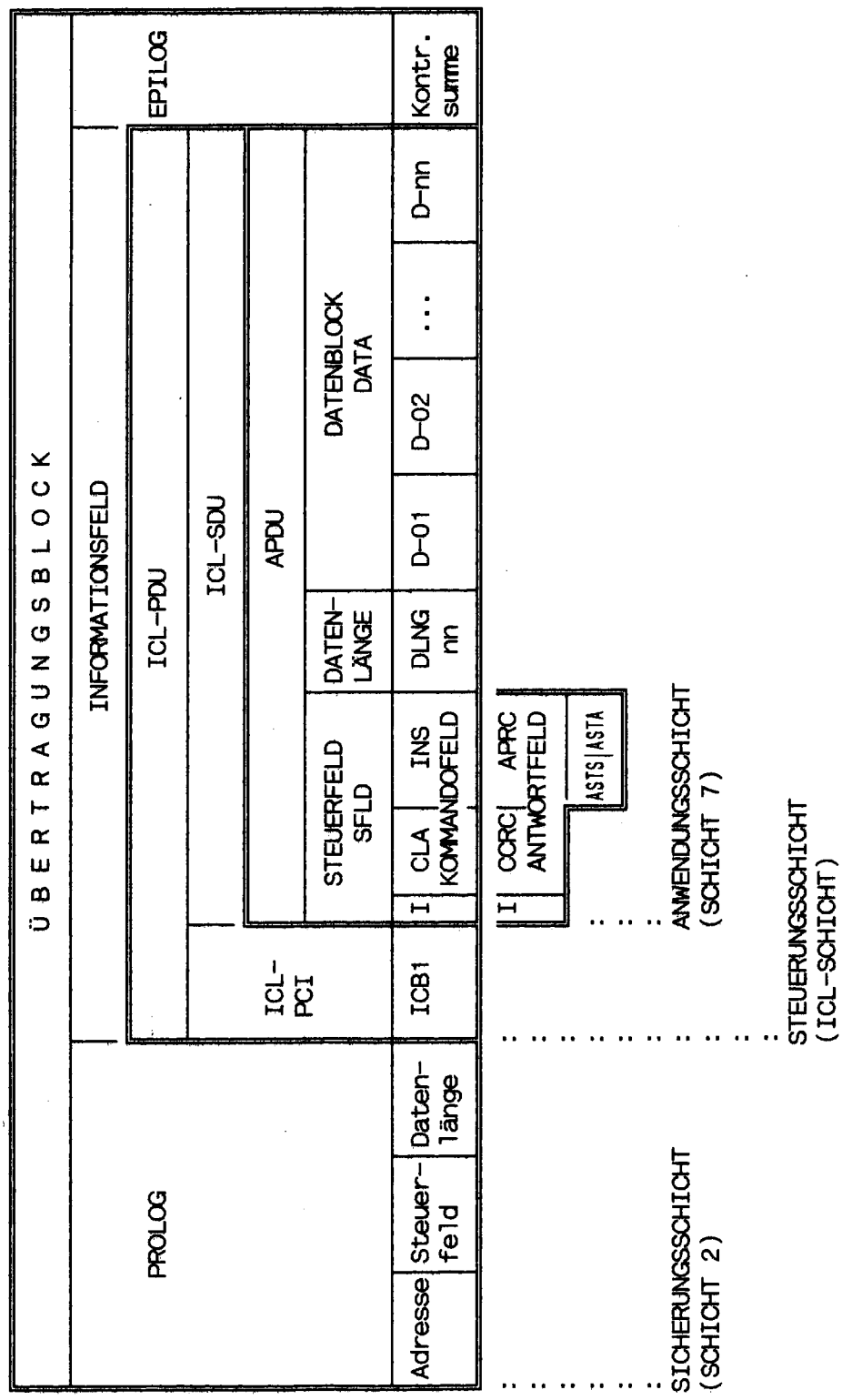
E 4.1 Protocol Select

Wenn die ICC einen korrekten PTS Request erhalten hat, sendet sie den PTS Response nach spätestens 30 ms.

E 4.2 Kommandos

Kommando	maximale Befehlsausführungszeit
SL-APPL	20 ms
CL-APPL	20 ms
SH-APPL	20 ms
CHK-KON	20 ms
CHK-PIN	50 ms
SET-PIN	150 ms
RD-EBDT	20 ms
RD-RUFN	20 ms
RD-GEBZ	20 ms
WT-RUFN	400 ms
EH-GEBZ	400 ms
CL-GEBZ	400 ms
AUT-1	400 ms
SP-GZRV	50 ms
FR-GZRV	50 ms

E 5 Aufbau eines Übertragungsblocks



E 6 Zusammenfassung der Fehlerbehandlung

E 6.1 Allgemeines

Die Schicht 1 besitzt zwei Fehlerzähler, einen für Fehlerursachen aus der Schicht 1 und einen für Fehlerursachen aus der ICL-Schicht und der Schicht 7.

Die Schichten 2 und 7 haben je einen Fehlerzähler; die ICL-Schicht besitzt zwei Fehlerzähler.

Eine erfolglose Fehlerbehandlung in einer Schicht führt zu einer Fehlerbehandlung in einer unteren Schicht.

In einer Schicht wird immer nur der zuletzt aufgetretene Fehler behandelt, d.h. tritt während einer Fehlerbehandlung ein neuer Fehler auf (in der gleichen Schicht), wird nur der neue Fehler behandelt. Die Stände der Fehlerzähler werden dabei übernommen und hochgezählt.

Treten während der Fehlerbehandlung neue Fehler in einer unteren Schicht auf, so sind diese Fehler entsprechend der Schichtenfolge (untere zuerst, obere zuletzt) zu behandeln. Die Stände der Fehlerzähler der oberen Schichten werden beibehalten (Ausnahme: Reset). Die Stände der entsprechenden Fehlerzähler der Schicht 1 werden bei Reset hochgezählt.

E 6.2 Zähler der Fehlerbehandlungen

Schicht	Zähler	Ursachen für Fehlerbehandlung	Maßnahmen der Fehlerbehandlung	Endwert	wird zurückgesetzt durch	Folgemaßnahmen bei Endwert
Schicht 7	Zähler für Resets durch Fehlerbehandlung der Schicht 1 h(S1)	- fehlerhafter ATR - fehlerhaftes TCK - fehlerhafter PTS-response Fehler: - Parity-Fehler - Frame-Error - Underrun/Timeout - Overrun	1. Inkrementierung des Zählers h(S1) 2. Wenn h(S1)<3: Reset, ggf. anschließend Senden des PTS-request	3	- Ziehen der Karte - Ab-/Anschalten des Endgeräts je nach Fehlerursache: - korrekter ATR+TCK - korrekter PTS-response	nach erfolgloser Fehlerbehandlung Benachrichtigung an den Bediener, daß eine erfolgreiche Kommunikation nicht möglich ist
	Zähler für Resets durch Fehlerbehandlung der oberen Schichten h(RES/ICB1/S7)	- erfolglose Fehlerbehandlung der oberen Schichten	1. Inkrementierung des Zählers h(RES/ICB1/S7) 2. Wenn h(RES/ICB1/S7)<4: Reset, anschließend weitere(r) Versuch(e) in den oberen Schichten	4	- Ziehen der Karte - Ab-/Anschalten des Endgeräts - korrekter response (!) auf das Schicht 7-Kommando, dessen Antwort die Fehlerbehandlung zum ersten Mal auslöste	
Schicht 2	Fehlerzähler i* Beachte: i*: Gesamtanzahl der Versuche = 4 i : Anzahl der Wiederholungen gemäß Abschnitt E 1, Protokollmaschine der Schicht 2 im CEG (Endwert = 3)	In Erwartung eines I- oder REJ-Befehls: - Empfang eines ungültigen Blocks - falscher Inhalt des Steuerfeldes - falscher Inhalt des Längenfeldes - falsche Checksumme - falsches Format des REJ-Befehls - Parity-Fehler	1. Inkrementierung des Zählers i* 2. Wenn i*<4: Senden eines REJ-Befehls	4	- Ziehen der Karte - Ab-/Anschalten des Endgeräts - korrekt empfangener I-Befehl - korrekt empfangener RES-Befehl - Reset	Benachrichtigung der ICL-Schicht, die das Senden eines RES-Befehls veranlaßt
		- Empfang eines REJ-Befehls	1. Inkrementierung des Zählers i* 2. Wenn i*<4: Wiederholen des letzten I-Befehls			
		- BWT-Timeout	1. Inkrementierung des Zählers i* 2. Wenn i*<4: Wiederholen des letzten Befehls (I- bzw. REJ-Befehl)			
		In Erwartung eines RES-Befehls: - Empfang eines korrekten RES-Befehls	- Durchführung der Schicht 2-Fehlerbehandlung			
		- kein Empfang eines RES-Befehls (ungültig oder BWT-Timeout)	- Benachrichtigung der ICL-Schicht die das Senden eines RES-Befehls veranlaßt			
ICL-Schicht	Zähler für gesendete RES-Befehle r	- Meldung der Schicht 2 nach erfolgloser Fehlerbehandlung, daß kein korrekter I-Befehl empfangen wurde - Meldung der Schicht 2, daß kein korrekter RES-Befehl empfangen wurde bzw. keine Meldung der Schicht 2	1. Inkrementierung des Zählers r 2. Wenn r<4: Veranlassung des Sendens eines RES-Befehls	4	- Ziehen der Karte - Ab-/Anschalten des Endgeräts - Meldung der Schicht 2, daß der I-Befehl korrekt empfangen wurde, der den RES-Befehl verursachte - Reset	Benachrichtigung der Schicht 7, die einen Reset veranlaßt
	Fehlerzähler j	- ICB1 ≠ $00	1. Inkrementierung des Zählers j 2. Wenn j<3: Wiederholen des letzten Schicht 7-Kommandos	3	- Ziehen der Karte - Ab-/Anschalten des Endgeräts - ICB1 = $00 - Reset	Benachrichtigung der Schicht 7, die einen Reset veranlaßt
Schicht 7	Fehlerzähler k	- GENERAL-ERROR-Bit = 1 - IDENT-Bit = 0 - Länge des übertragenen Datenblocks entspricht nicht der in DLNG angegebenen Datenlänge - Länge des übertragenen Datenblocks entspricht nicht der Spezifikation - Inhalt von DLNG ist größer als $FE	1. Inkrementierung des Zählers k 2. Wenn k<3: Wiederholen des letzten Schicht 7-Kommandos	3	- Ziehen der Karte - Ab-/Anschalten des Endgeräts - korrekte Schicht 7-Antwort, für die zuletzt eine Fehlerbehandlung durchgeführt wurde - Reset	Reset

E 7 Maßnahmen bei gespeicherter PIN und dekrementiertem AFBZ

Für den Zugang zu den Applikationen Netz-C und GZRV kann in bestimmten Fällen für das Kommando CHK-PIN eine im FuTelG gespeicherte PIN verwendet werden. Damit wird ein schneller, erneuter Zugang zu diesen Applikationen nach dem Deaktivieren der Chipkarte (z. B. zwecks Stromersparnis bei eingeschaltetem FuTelG bzw. Fehlerbehandlung nach Abschnitt E 2) oder bei Applikationswechsel ermöglicht, ohne daß der Benutzer die PIN erneut eingeben muß. Dabei wird der in der Karte für die jeweilige Applikation geführte AFBZ, beim erneuten Zugang zu dieser Applikation (unter Verwendung der gespeicherten, richtigen PIN), auf seinen Endwert zurückgesetzt. Dies bedeutet, daß ein durch SET-PIN unter Verwendung einer falschen, alten PIN dekrementierter AFBZ auf seinen Entwert zurückgesetzt wird, ohne daß der Tln eine richtige PIN eingeben mußte.

Durch erneute Durchführung des Kommandos SET-PIN mit einer falschen, alten PIN ist sicherzustellen, daß der AFBZ nach dem Zurücksetzen mittels CHK-PIN wieder auf den Wert gesetzt wird, der zuvor durch die falsche(n) PIN-Eingabe(n) erreicht worden war.

F Abkürzungsverzeichnis

AFBZ	Applikations-Fehlbedienungszähler
APDU	Application Protocol Data Unit
APP-IDN	Applikations-Identifier
APP-STS	Applikations-Status
APP-TXT	Applikations-Text(Bezeichnung)
APRC	Applikations-Returncode
ASTA	Applikations-Status-allgemein
ASTS	Applikations-Status-spezifisch
ATR	Answer to Reset
Btx	Bildschirmtext
BWT	Block Waiting Time
CCITT	Comite Consultatif International Telegraphique et Telephonique
CCRC	Chikarten-Returncode
CEG	Chipkarten Endgerät
CSUM	Checksumme
CWT	Character Waiting Time
DBP	Deutsche Bundespost
DIN	Deutsche-Industrie-Norm
DL	Data Link
DLNG	Datenblocklänge (Schicht-7-Daten)
EDAT	Einbuchdaten
etu	elementary time unit
FBZ	Fehlbedienungszähler
FTZ	Fernmeldetechnisches Zentralamt
FuTel-Netz C	Funktelefon Netz C

FuTelTln	Funktelefon-Teilnehmer
FuVSt	Funkvermittlungsstelle
GEBZ	Gebührenzähler
HDLC	High Level Data Link Control
I-Befehl	Informationsbefehl
ICB	Interface Control Byte
ICC	Integrated Circuit Card
ICL	Interface Control Layer
ICL-PCI	ICL-Protocol-Control-Information
ICL-PDU	ICL-Protocol-Data-Unit
ICL-SDU	ICL-Service-Data-Unit
ICWT	Initial Character Waiting Time
ID	Interface Device
ISO	International Standardisation Organization
ISO/DIS	Draft International Standard
ISO/DP	Draft Proposal Standard
LAP	Lokaler Anwendungsprozeß
LD	Lokales Datenendgerät
LSB	Last Significant Bit
MSB	Most Significant Bit
NABÜP	Nationales asynchrones Blockübertragungs-Protokoll
ÖKart	Öffentliches Kartentelefon
OSI	Open System Interconnection (Kommunikation offener Systme)
PIN	Personal Identification Number
PLA	PIN-Länge "alte" PIN
PLNG	PIN-Länge
PST	Post Service Terminal
PTS	Protocol Type Select

RAP	Remote Anwendungsprozeß
REJ-Befehl	Wiederholungsaufforderungsbefehl
RES-Befehl	Resynchronisationsbefehl
RUFN	Rufnummernverzeichnis
SFLD	Steuerfeld
SPIN	System-PIN
WT	Waiting Time