Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03109-1

Anlage IV: Feinspezifikation „Drahtgebundene LMN-Schnittstelle“
Teil a: „HDLC für LMN“

Version 1.0, Datum 18.03.2013

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-100

E-Mail: smartmeter@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Abbildungsverzeichnis

1 HDLC – Transportschicht

HDLC wird in Zusammenhang mit dem SMGW vergleichsweise zu TCP genutzt. In Anlehnung an die bei TCP üblichen Port-Nummern wird ein vergleichbarer Protokoll-Selektor in den HDLC-Adressen benutzt.

Das SMGW DARF nur TLS-über-HDLC-Verbindungen aufbauen. Hierzu ist der HDLC-Adress-Zusatz ‚0x11' zu verwenden.

2 HDLC – Verbindungsschicht

Für die Verbindungsschicht wird HDLC nach ISO/IEC 13239 benutzt.

Folgende Detailvorgaben sind anzuwenden:

- HDLC-Frame-Type: 3
- Primary-Station: SMGW
- Secondary-Station: Zähler
  - HDLC-Address-Type: Es werden unterschiedliche Adress-Typen für die Datenrichtungen: SMGW → Messeinrichtung und Messeinrichtung → SMGW benutzt.
  - Datenrichtung SMGW → Zähler:
    Per Broadcast wird der für die Verbindung zu nutzende Adress-Type (2- oder 4-Byte) festgelegt.
  - Datenrichtung Zähler → SMGW:
    Da es in dem System immer nur ein SMGW geben kann, wird der Adress-Type ‚2-Byte' vereinbart.

- Final-Flag:
  - Datenrichtung SMGW → Zähler:
    Das ‚Final-Flag' wird immer auf ‚1' gesetzt. Ein Zähler kann damit über seine Antwort die Fluss-Steuerung realisieren und so verhindern, dass ein SMGW eine Kette von HDLC-Paketen ohne Pausen an ihn richtet.

  - Datenrichtung Zähler → SMGW:
    Das ‚Final-Flag' wird immer auf ‚1' gesetzt. Ein Zähler kann seine Antwort daher immer nur innerhalb eines HDLC-Pakets ablegen.

- CRC: Berechnung gemäß IEC 62056-46
- Baudrate: 921,6 kBit/s
- Datenformat je Byte: 1 Start-Bit, 8 Datenbits, kein Paritätsbit, 1 Stopp-Bit.

- Timing:
  - Maximale Pause zwischen zwei Bytes(Inter-Character-Timeout) innerhalb eines HDLC-Datenpakets: 10 µs

- Maximale Antwortzeit für den Beginn der HDLC-Response auf das Ende des HDLC-Request (maximale Pause zwischen dem Ende des letzten Bytes aus den HDLC-Request bis zum Beginn des ersten Bytes der HDLC-Response): 1 ms

- Maximale Abschaltzeit nach dem Senden eines HDLC-Datenpaketes (Zeitspanne, gerechnet ab dem Ende des letzten Bytes eines HDLC-Datenpaketes bis zum Abschalten des Senders [„Tx-Off“]): max. 50 µs

- Minimale Aufschaltzeit („Guard-Time“) nach dem Empfang eines HDLC-Datenpaketes (Zeitspanne, gerechnet ab dem Ende des letzten Bytes eines HDLC-Datenpaketes bis zum Aufschalten des Senders [„Tx-On“] für das Aussenden des HDLC-Response: min. 100 µs

- Fehlerfall, Ausbleiben der HDLC-Response:
  Bleibt eine HDLC-Response nach Ablauf der unter Timing maximal zulässigen Wartezeit aus, ist nach einer Pausenzeit von 1 ms der nächste Slave (falls es mehr als einen Slave gibt, sonst ist derselbe Slave erneut) auf dem RS 485 Bus anzusprechen. Ob ein HDLC-Slave nach diesem Fehlerfall später erneut – mit demselben oder einem anderen HDLC-Frame – anzusprechen ist, legt die Parametrierung des HDLC-Master (⇔ SMGW) fest.

- Fehlerfall, Inter-Character-Timeout überschritten:
  Erkennt ein Master oder Slave in einem HDLC-Datenpaket eine Pausenzeit, die das Inter-Character-Timeout überschreitet, sind der Telegramm-Empfang zu beenden und die bis zu dem Fehler empfangene Byte-Kette zu verwerfen.

  Tritt dieser Fehler beim Empfang einer HDLC-Response bei dem Master auf, ist nach einer Pausenzeit von 1 ms der nächste Slave (falls es mehr als einen Slave gibt, sonst ist derselbe Slave erneut) auf dem RS 485 Bus anzusprechen

3 HDLC-Adressen

Da HDLC keinen Mechanismus zur Unterscheidung unterschiedlicher, im OSI-Stapel oberhalb angeordneter, Protokolle bietet, wird die Zuordnung der von HDLC angebotenen Adress-Bytes wie folgt festgelegt:

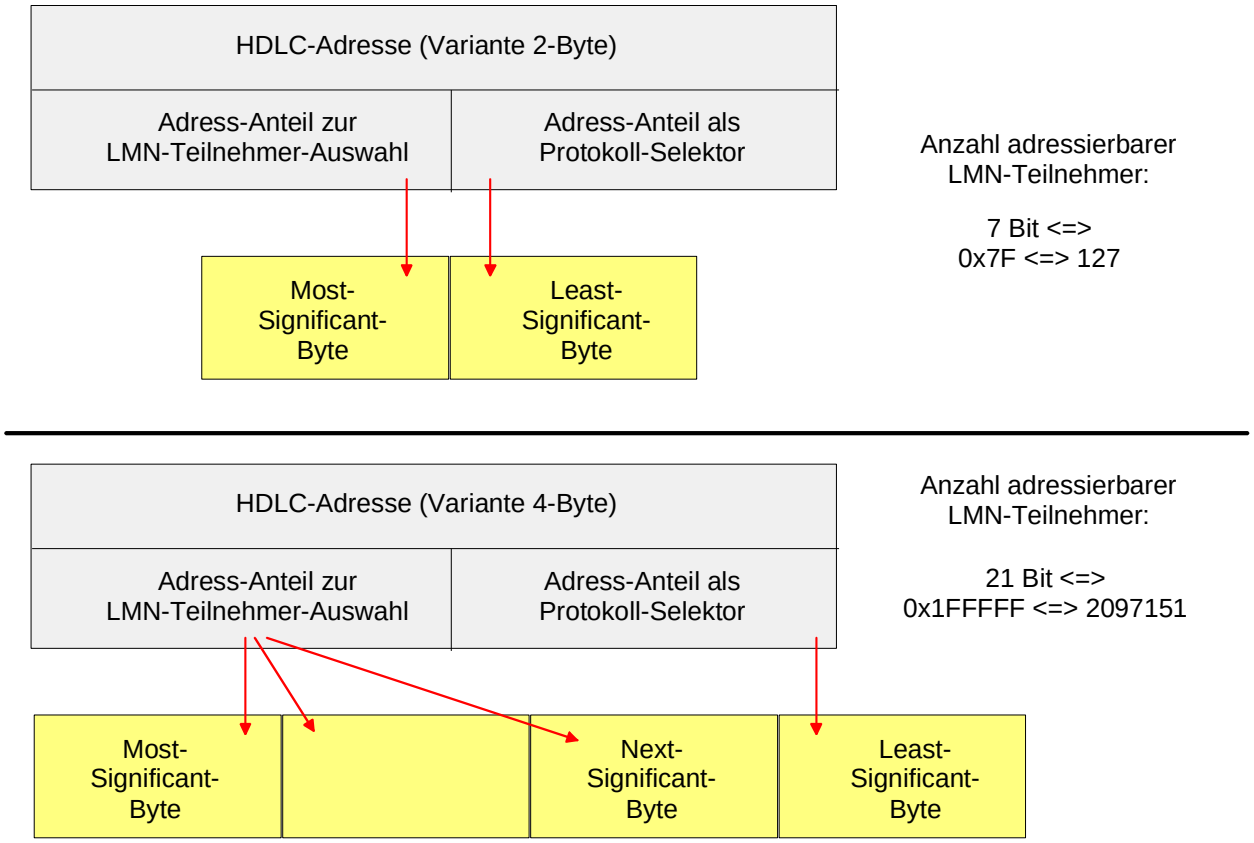

Abbildung 1: Aufteilung der HDLC-Adresse in reinen Adress-Teil und Protokoll-Selektor.

Der für die LMN-Busteilnehmer nutzbare Adressbereich („Adress-Anteil zur LMN-Teilnehmer-Auswahl“) ist wie folgt gegeben:

- Variante 2-Byte:
  - 0x01 ⇔ Fest dem SMGW zugeordnet.
  - 0x02 .. 0x7E ⇔ Nutzbar für LMN-Bus-Teilnehmer.
  - 0x7F ⇔ Broadcast-Adresse für HDLC-Adress-Vergabe.

- Variante 4-Byte:
  - 0x000001 ⇔ Fest dem SMGW zugeordnet.
  - 0x000002..0x1FFFFE ⇔ Nutzbar für LMN-Bus-Teilnehmer.
  - 0x1FFFFF ⇔ Broadcast-Adresse für HDLC-Adress-Vergabe.

4 Vergabe von eindeutigen HDLC-Adressen

4.1 HDLC-Adressen, reiner Adress-Teil

Um zu gewährleisten, dass die von den an ein SMGW angeschlossenen Zählern benutzten HDLC-Adressen einerseits eindeutig und andererseits automatisch vergeben werden, wird folgender Mechanismus festgelegt:

Erkennung neuer LMN-Busteilnehmer:

- Ein SMGW sendet periodisch einen HDLC-Broadcast („UI-Frame“) aus. Der Inhalt des Rundrufs fordert ausgewählte LMN-Busteilnehmer auf, sich selber eine neue HDLC-Adresse zu geben. Die Auswahl des LMN-Busteilnehmers hat dazu nach einem Zufallsverfahren zu erfolgen. Das SMGW formuliert den Rundruf dabei derart, dass die Aufforderung an alle jene LMN-Busteilnehmer geht, die dem SMGW nicht bekannt sind.
- Die vorstehend angesprochenen LMN-Busteilnehmer antworten in Zeitschlitzen („UI-Frame“). Dabei wird der für die Antwort zu benutzende Zeitschlitz ebenfalls per Zufall bestimmt. Jedem Zeitschlitz wird eine „Guard-Time“ vorangestellt. Während dieser Zeit darf kein LMN-Busteilnehmer antworten. Im Anschluss an die „Guard-Time“ folgt das Fenster, innerhalb dessen die Versendung der Antwort beginnen muss. Für das restliche Timing der dabei zu übertragenden HDLC-Pakete gelten die unter Kapitel „2 – Verbindungsschicht“ definierten Zeiten. Der Zeitschlitz besteht damit aus folgenden Elementen:
  - „Guard-Time“: 5 ms +/- 10 %
  - Fenster für HDLC-Response: 5 ms +/- 10 %
- Als Resultat wird es teilweise zu Kollisionen bei den HDLC-Antworten, zur Auswahl identischer HDLC-Adressen durch mehrere LMN-Busteilnehmer aber auch zur Erfassung neuer, dem SMGW bis dahin unbekannter LMN-Busteilnehmer kommen.
- Da der Vorgang periodisch ausgeführt wird, die LMN-Topologie überwiegend statisch und die Anzahl der LMN-Busteilnehmer klein sein wird, wird ein SMGW nach kurzer Zeitspanne alle LMN-Busteilnehmer ‚kennen‘.
- Da der Vorgang periodisch ausgeführt wird, werden neue LMN-Busteilnehmer, die im Zuge späterer Installationen ergänzt werden, ebenfalls automatisch erkannt.
  - Periodizität: Alle 30 +/-1 s ist die Abfrage zur Erkennung neuer LMN-Busteilnehmer vorzunehmen. Dabei sind maximal 50 Zeitschlitze zu erlauben.

Erkennung ‚verstummter‘ (entfernter) LMN-Busteilnehmer:

Ein SMGW sendet periodisch einen HDLC-Broadcast („UI-Frame“) aus. Der Inhalt des Rundrufs fordert ausgewählte LMN-Busteilnehmer auf, sich in einem bestimmten Zeitschlitz zu melden („UI-Frame“). Antwortet einer der aufgeforderten LMN-Busteilnehmer nicht, kann er als ‚verstummt‘ / ‚entfernt‘ gewertet werden. Wird er als ‚verstummt‘ / ‚entfernt‘ gewertet, ist dessen HDLC-Adresse aus der Liste der erkannten HDLC-Adressen im HDLC-Master (⇔ SMGW) zu entfernen.

- Periodizität: Alle 30 +/-1 s ist die Abfrage zur Erkennung
  - ‚verstummter' LMN-Busteilnehmer
  - vorzunehmen. Dabei sind maximal 50
  - Zeitschlitze zu erlauben.

Der Ablauf wird durch folgenden Zustandsautomaten beschrieben:

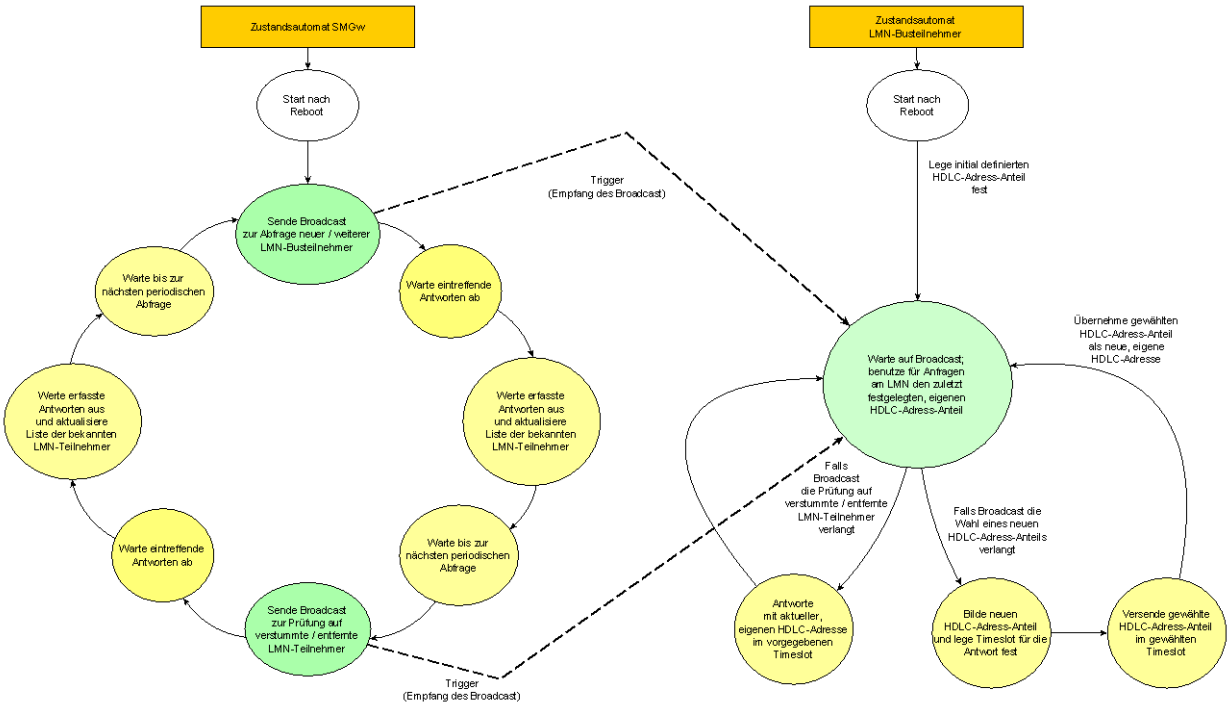

Abbildung 2: Zustandsautomat zur Vergabe der HDLC-Adressen

4.2 HDLC-Adressen, Protokoll-Selektor

Entgegen anderen Verbindungsprotokollen bietet HDLC keinen Protokoll-Selektor. Um dennoch eine Lösung zu verwenden, die künftig auf andere Transportprotokolle ausgedehnt werden kann, wird Folgendes festgelegt:

Destination-Service-Access-Point:

- In der Datenrichtung SMGW → Zähler legt das Least-Significant-Byte den Destination-Service-Access-Point („DST-SAP") fest.
- Der DST-SAP benennt das in der Nutzlast verwendete Protokoll, wobei folgende Varianten derzeit zulässig sind:
  - HDLC-I-Frame (⇔ Unicast), TLS und darin SML/COSEM ⇔ 0x01
  - HDLC-I-Frame (⇔ Unicast), TLS ohne Festlegung des Inhalts ⇔ 0x02
  - HDLC-I-Frame (⇔ Unicast), direkt SML/COSEM ⇔ 0x03
  - HDLC-I-Frame (⇔ Unicast), alle anderen reserviert ⇔ 0x00 sowie 0x04..0xFF
  - HDLC-UI-Frame (⇔ Broadcast), Aufruf zur HDLC-Adressvergabe ⇔ 0x01

- HDLC-UI-Frame (⇔ Broadcast), Aufruf zur HDLC-Adress-Prüfung ⇔ 0x02
- HDLC-UI-Frame (⇔ Broadcast), alle anderen reserviert ⇔ 0x00 sowie 0x03..0x7F

- Das Next-Significant-Byte legt das unterste Byte der eigentlichen Adresse fest. Falls mehr als ein Adress-Byte benötigt werden, folgen die weiteren Adress-Bytes.

Source-Service-Access-Point:

- In der Datenrichtung Zähler → SMGW legt das Least-Significant-Byte den Source-Service-Access-Point („SRC-SAP“) fest.
- Der SRC-SAP signalisiert dem anfragenden SMGW in der Antwort eine Art ‚Antwort-Port‘. Ein LMN-Busteilnehmer hat den SRC-SAP mit Aufbau der HDLC-Verbindung zu wählen und darf den einmal gewählten Inhalt für die Dauer dieser HDLC-Verbindung nicht ändern.
- Kein HDLC-UI-Frame mit Protokoll-Selektor zu einem Protokoll ‚A‘ schließt automatisch alle weiteren, möglicherweise bestehenden HDLC-Verbindungen zu anderen Protokollen. Alle per Protokoll-Selektor definierten HDLC-Verbindungen sind voneinander unabhängig.

4.3 HDLC-Adressen, Adressvergabe (Beispiel)

Die folgenden drei Abbildungen stellen den Ablauf einer eindeutigen und automatischen HDLC-Adressvergabe unter verschiedenen Ausgangssituationen dar. Alle Abläufe **MÜSSEN** vom SMGW unterstützt werden.

Bei gegebener Ausgangssituation, dass noch kein LMN Teilnehmer dem SMWG bekannt ist, stellt sich der Ablauf der HDLC Adressvergabe folgendermaßen dar:

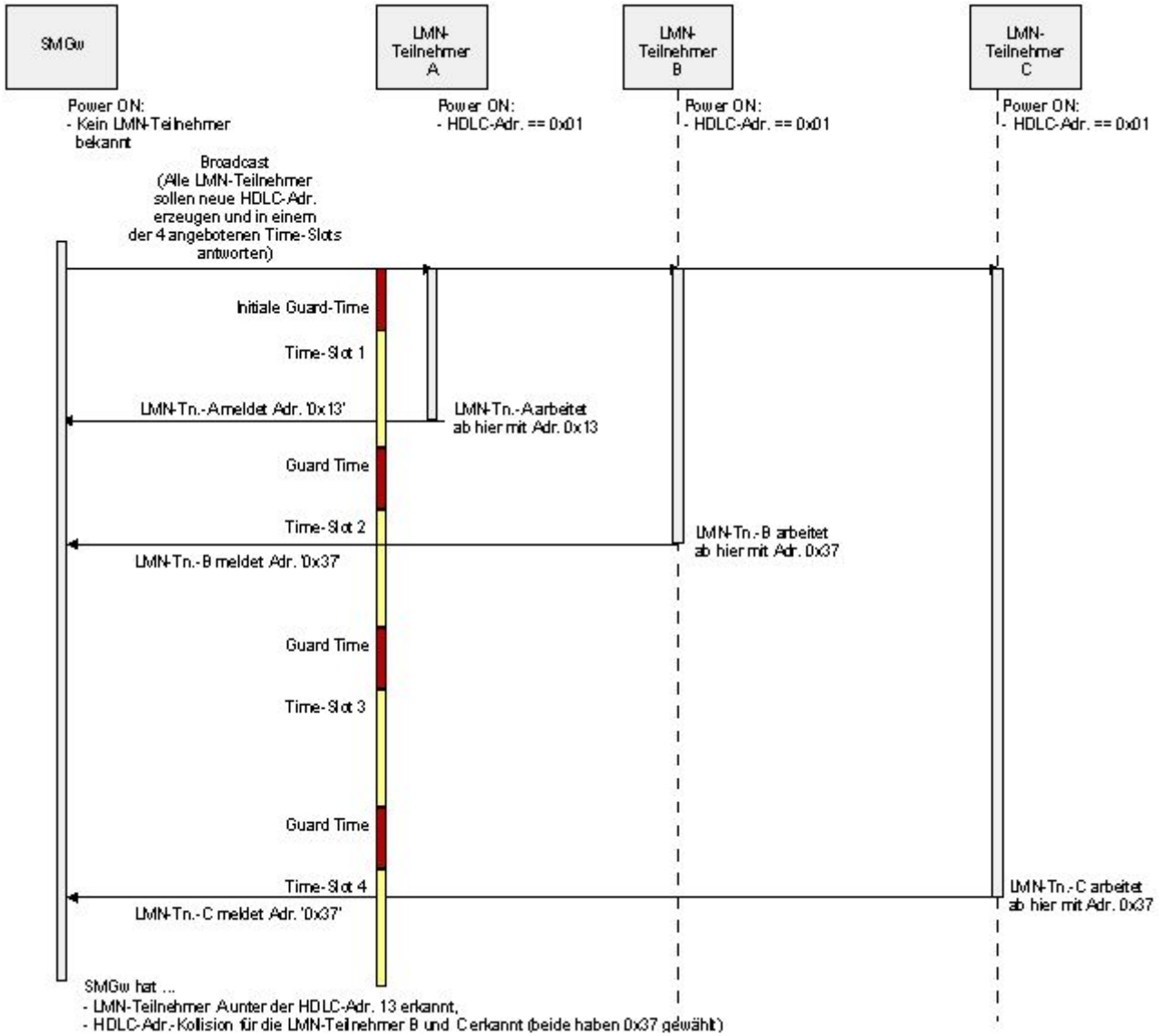

Abbildung 3: HDLC-Adressvergabe – Vorgehen, wenn kein LMN-Teilnehmer dem SMGW bekannt ist

Bei gegebener Ausgangssituation, dass noch nicht alle LMN Teilnehmer dem SMWG bekannt sind, stellt sich der Ablauf der HDLC Adressvergabe folgendermaßen dar:

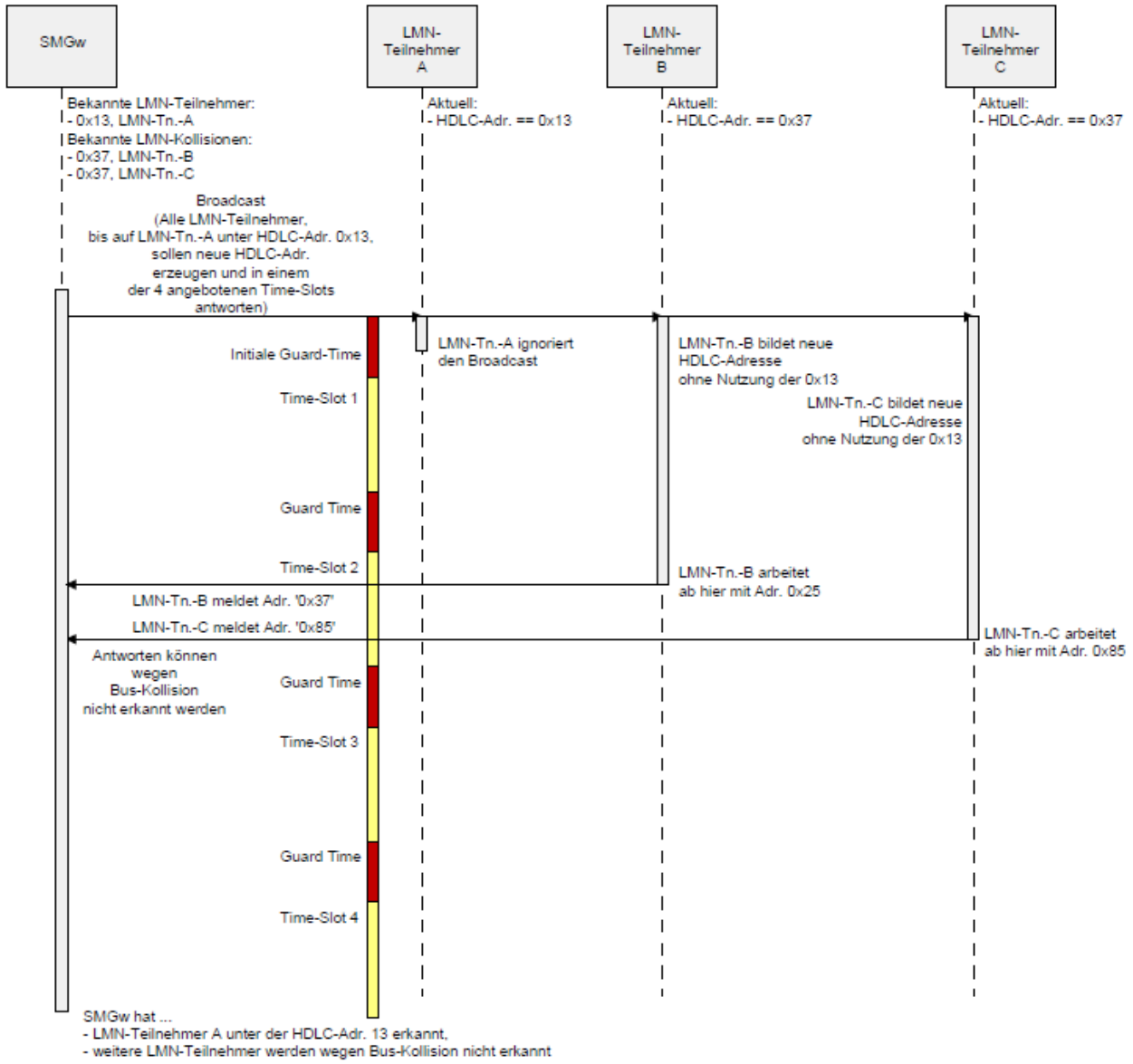

Abbildung 4: HDLC-Adressvergabe – Vorgehen, wenn nicht alle LMN-Tn. dem SMGW bekannt sind; nach Adressen-Kollision

Bei gegebener Ausgangssituation, dass noch nicht alle LMN Teilnehmer dem SMWG bekannt sind, und ein Time-Slot-Kollision auftrat, setzt sich der Ablauf der HDLC Adressvergabe folgendermaßen fort:

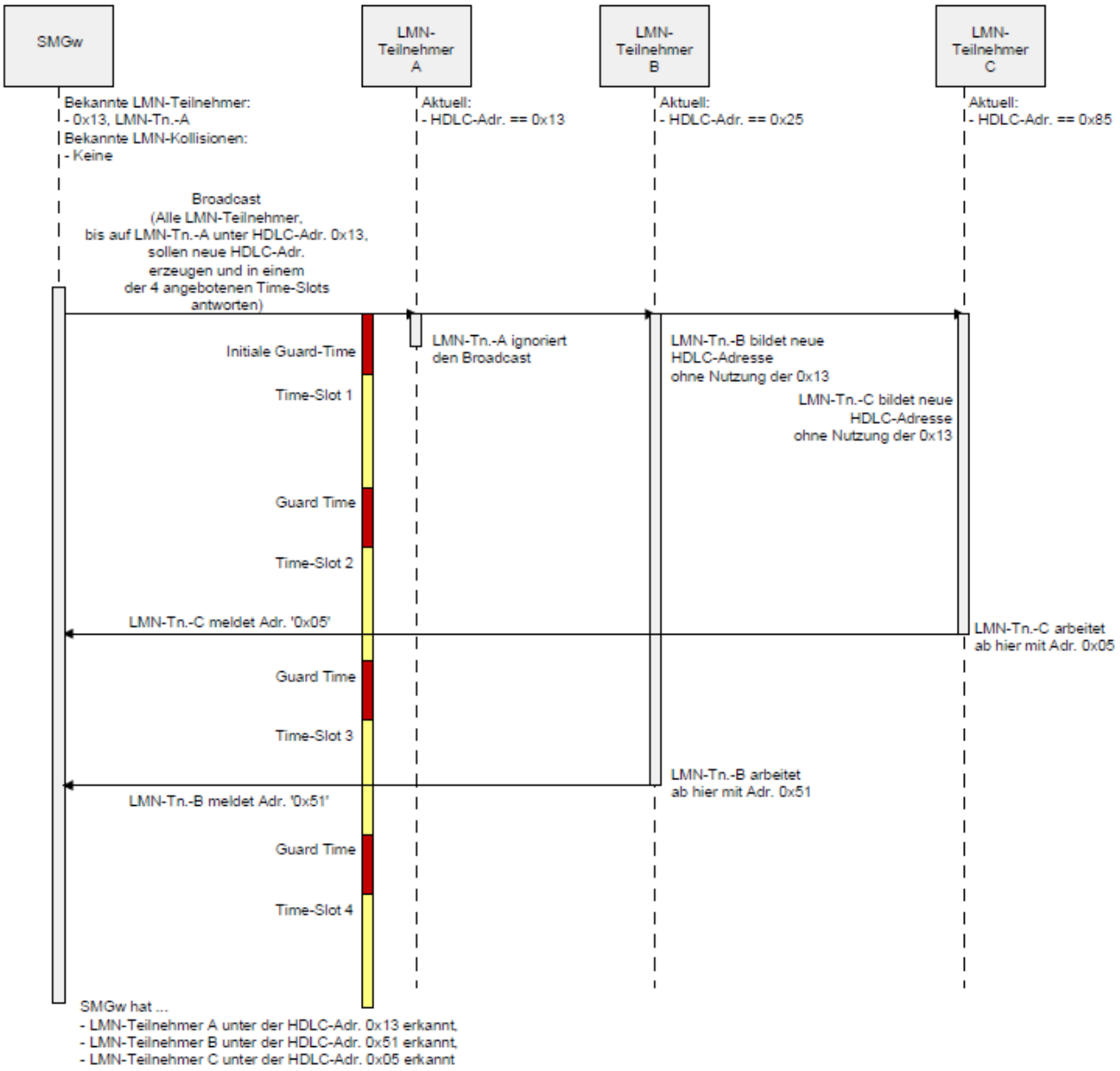

Abbildung 5: HDLC-Adressvergabe – Vorgehen, wenn nicht alle LMN-Tn. dem SMGW bekannt sind; nach Time-Slot-Kollision

4.4 HDLC-Adressen, Adress-Prüfung (Beispiel)

Sollte ein LMN-Teilnehmer nicht mehr am Bus verfügbar sein (z.B. aufgrund eines Defekts), sind grundsätzlich zwei Verfahren denkbar, um dies zu erkennen:

- Eine Möglichkeit besteht darin, einen Teilnehmer aus der Liste der erkannten Geräte herauszunehmen, wenn dieser Teilnehmer auf eine konkrete HDLC-Anfrage nicht antwortet.

- Es wird eine weitere Möglichkeit für den Fall benötigt, bei dem keine HDLC-Verbindung zu einem Teilnehmer aktiv ist. Für diesen Fall bietet sich an, einen vergleichbaren Mechanismus per Broadcast zu nutzen. Das SMGW sendet einen Broadcast, in dem alle dem SMGW bekannten LMN-Teilnehmer aufgelistet sind. Teil dieser Nachricht ist eine Zuordnung auf einen Time-Slot, in dem der LMN-Teilnehmer den Broadcast bestätigen muss. Fehlt nun in der Rückrichtung ein LMN-Teilnehmer, kann das SMGW diesen aus der Liste der ihm bekannten LMN-Teilnehmer streichen (siehe Abbildung 6)

Beide Varianten **MÜSSEN** vorgesehen werden.

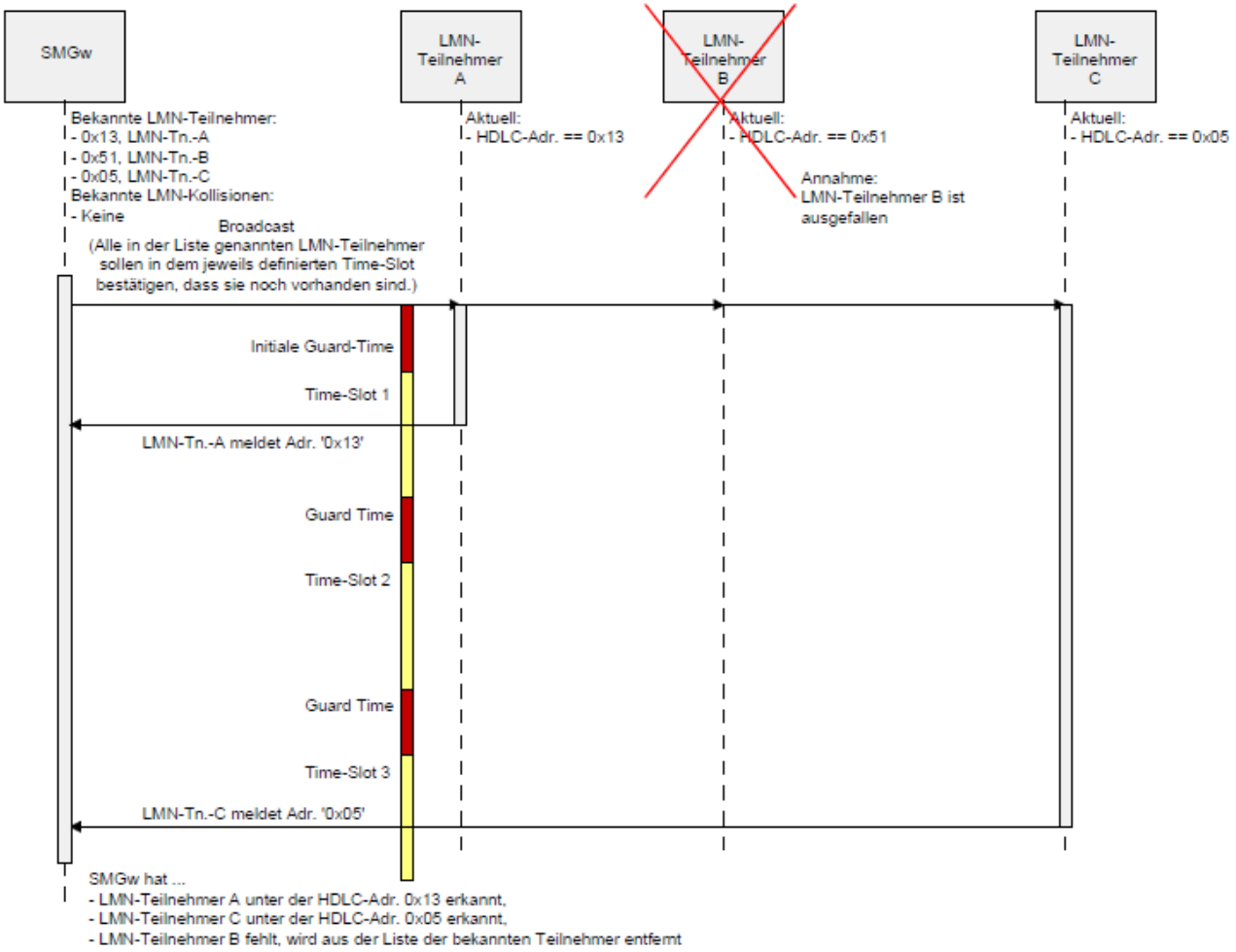

Abbildung 6: HDLC-Adressvergabe – Vorgehen zur Prüfung auf ‚verlorene' Teilnehmer

4.5 HDLC-Adressvergabe, Broadcast zur Auswahl neuer Adressen

Falls ein HDLC-Master keinen einzigen HDLC-Slave als Teilnehmer kennt, sendet er eine leere Payload. Sobald er mindestens einen HDLC-Slave kennt, den er von der HDLC-Adress-Vergabe herausnehmen will, sendet er eine Payload gemäß Tabelle 1. Damit wird die Payload immer in Byte-Ketten zu 32 anwachsen. Die maximal mögliche Anzahl von HDLC-Teilnehmer wird durch die maximale Größe einer Payload begrenzt.

HDLC-Slaves, die in der folgenden HDLC-Payload nicht gelisteten sind, sollen sich eine neue HDLC-Adresse bilden:

Byte-Index	Bedeutung	Feldlänge / Bytes	Kommentar / Hinweis
0	Bekannter Teilnehmer 1	32	Aufbau der Byte-Kette gemäß Tabelle 2; in der Byte-Kette ist das Feld zum Zeitschlitz auf ‚0x00' zu setzen
1 x 32	Bekannter Teilnehmer 2	32	Aufbau der Byte-Kette gemäß Tabelle 2; in der Byte-Kette ist das Feld zum Zeitschlitz auf ‚0x00' zu setzen, diese Zeile entfällt, wenn nur ein Teilnehmer bekannt ist.
2 x 32	Bekannter Teilnehmer 3	32	Aufbau der Byte-Kette gemäß Tabelle 2; in der Byte-Kette ist das Feld zum Zeitschlitz auf ‚0x00' zu setzen, diese Zeile entfällt, wenn nur zwei Teilnehmer bekannt sind.
…	…	32	…

Tabelle 1: HDLC-Adress-Vergabe, Payload für die Auswahl neuer Adressen

Byte-Index	Bedeutung	Feldlänge / Bytes	Kommentar / Hinweis
0	HDLC-Adresse	1	Die HDLC-Adresse des Teilnehmers.
1	Index zum Zeitschlitz	1	Dieses Feld ist in der Nutzungsvariante ‚Auswahl neuer HDLC-Adressen' nicht benötigt und dann auf ‚0x00' zu setzen. In der Nutzungsvariante ‚Prüfung auf vorhandene HDLC-Teilnehmer' wird hier der Zeitschlitz angegeben, in dem der Teilnehmer mit der HDLC-Adresse antworten muss.
2	LMN-Busteilnehmer-Identifikation	30	Als LMN-Busteilnehmer-Identifikation wird die eineindeutige Geräteadresse nach DIN 43863-5 benutzt. Falls nach der Kodierung weniger Bytes benötigt werden, als die Feldlänge anbietet, sind die bis zum Most-Significant-Byte verbleibenden Bytes mit ‚0x00' aufzufüllen.

Tabelle 2: HDLC-Adress-Vergabe, Byte-Kette zur Beschreibung eines HDLC-Slaves.

4.6 HDLC-Adressvergabe, Broadcast zur Prüfung auf vorhandene Teilnehmer

Falls ein HDLC-Master keinen einzigen HDLC-Slave als Teilnehmer kennt, sendet er eine leere Payload.

Sobald er mindestens einen HDLC-Slave kennt, dessen Vorhandensein er prüfen will, sendet er eine Payload gemäß Tabelle 3. Damit wird diese Payload immer in Byte-Ketten zu 32 anwachsen. Die maximal mögliche Anzahl von HDLC-Teilnehmer wird damit durch die maximale Größe einer Payload begrenzt.

HDLC-Slaves, die in der nachfolgend definierten HDLC-Payload gelisteten sind, sollen in dem ebenfalls in der HDLC-Payload genannten Zeitschlitz antworten:

Byte-Index	Bedeutung	Feldlänge / Bytes	Kommentar / Hinweis
0	Bekannter Teilnehmer 1	32	Aufbau der Byte-Kette gemäß Tabelle 2; in der Byte-Kette ist das Feld zum Zeitschlitz auf ‚0x01' zu setzen
1 x 32	Bekannter Teilnehmer 2	32	Aufbau der Byte-Kette gemäß Tabelle 2;in der Byte-Kette ist das Feld zum Zeitschlitz auf ‚0x02' zu setzen; diese Zeile entfällt, wenn nur ein Teilnehmer bekannt ist.
2 x 32	Bekannter Teilnehmer 3	32	Aufbau der Byte-Kette gemäß Tabelle 2; in der Byte-Kette ist das Feld zum Zeitschlitz auf ‚0x03' zu setzen; diese Zeile entfällt, wenn nur zwei Teilnehmer bekannt sind.
…	…	32	…

Tabelle 3 HDLC-Adress-Vergabe, Payload für die Prüfung auf vorhandene Teilnehmer.

4.7 HDLC-Adressvergabe, Antwort auf Broadcast-Anfrage

Ein HDLC-Slave, der gemäß Kapitel 4.5 zur Auswahl einer neuen HDLC-Adresse aufgefordert oder gemäß Kapitel 4.6 zur Prüfung auf Vorhandensein befragt wird, sendet in dem von ihm gewählten / gemäß Auftrag zu benutzenden Zeitschlitz seine Antwort mit einer nach Tabelle 3 definierten HDLC-Payload. In dieser Payload ist in diesem Fall genau ein Eintrag nach Tabelle 2 enthalten.

4.8 TLS über HDLC

Zur Sicherung gemäß TR-03109-1 wird TLS (RFC 5246) benutzt.

Für die Verbindung von TLS über HDLC gelten folgende Regeln:

- Die Default-Buffer-Größe von TLS wird auf die maximal durch HDLC gegebene Fragment-Größe eingeschränkt. Die Einschränkung erfolgt per ‚max_fragment_length' (siehe RFC 6066).
- Die TLS-Rollen werden wie folgt definiert:
    - Das SMGW agiert als TLS-Client;
    - Der Zähler arbeitet in der Rolle TLS-Server.

5 Initialer Austausch von Zertifikaten im LMN

Dieses Kapitel hat normativen Charakter.

Für die Vergabe eines TLS-Zertifikats zur Nutzung zwischen einem Zähler (LMN-Busteilnehmer) und einem führenden System (SMGW) wird nachstehender Ablauf verlangt:

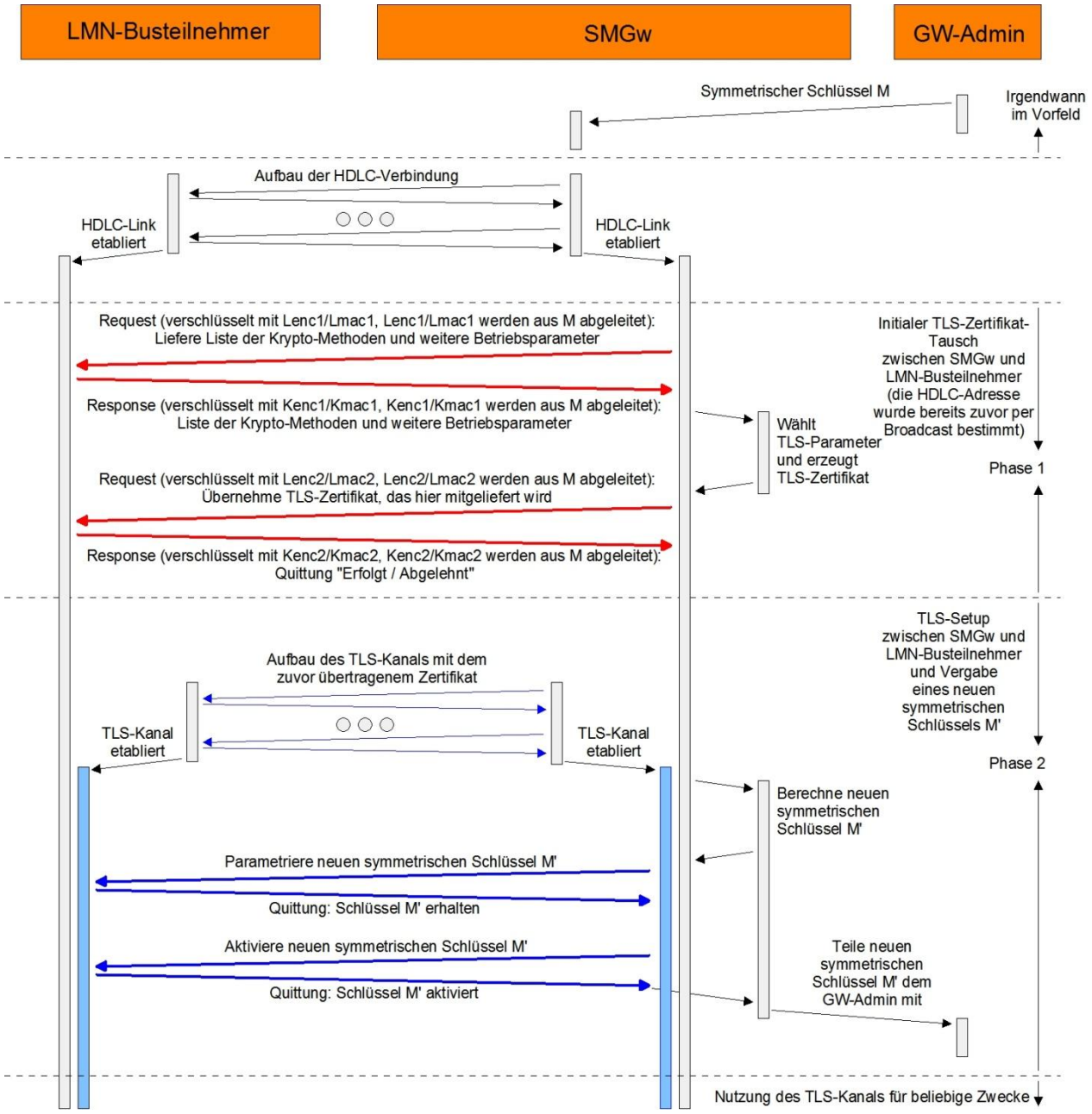

Abbildung 7: TLS über HDLC, Vergabe des TLS-Zertifikats und symmetrischer Schlüssel