

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

OEM-Modul CM200

Verschlüsseln von seriellen Datenübertragungen

Technische Dokumentation



Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 1 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

INHALTSVERZEICHNIS

DOKUMENTE	3
KURZBESCHREIBUNG	3
TECHNISCHE DATEN	3
BLOCKSCHALTBILD	4
SCHNITTSTELLEN	5
BESCHREIBUNG DER SCHNITTSTELLENSIGNALE	6
KONFIGURATION	8
ELEKTRISCHE PARAMETER	8
IDENTIFIKATION.....	8
BAUDRATE.....	8
DATENPROTOKOLL.....	9
USERKEY ANZEIGEN.....	10
USERKEY ÄNDERN.....	10
USERKEY DEFAULT.....	10
SELBSTTEST ZUFALLSGENERATOR	10
KONTINUIERLICHE GENERIERUNG VON ZUFALLSZAHLEN	12
PIN ÄNDERN.....	12
NEUSYNCHRONISATION.....	13
KRYPTIERTE LOOP FÜR SELBSTTEST	13
OFFENE LOOP FÜR SELBSTTEST	14
DEFAULT -WERTE.....	14
STROMSPARMODUS.....	14
FEHLERMELDUNG.....	15
VERSION.....	15
TESTFOLGEN SESSIONKEY	15
TESTFOLGEN ALGORITHMUS.....	16
EINSTELLUNGEN ABFRAGEN.....	17
FEHLERMELDUNGEN	17
VERSCHLÜSSELTE VERBINDUNGSaufNAHME	19
FUNKTION VERSCHLÜSSELN	21
APPLIKATION MODEMÜBERTRAGUNG	21

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 2 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Dokumente

- [1] Datasheet
Flash Microcontroller P89C51RD2
Phillips Semiconductors
- [2] Datasheet
Dual universal asynchronous receiver/transmitter (USART)
User-Guide (SC26C92)
Phillips Semiconductors

Kurzbeschreibung

Viele Industriesysteme beinhalten serielle Kommunikationseinrichtungen für Fernwartung und Ferndiagnose, wobei die Daten offen und somit abhörbar und manipulierbar sind. In modernen Kommunikationssystemen sind Verschlüsselungskomponente deshalb unerlässlich. Das OEM-Modul CM200 beinhaltet ein vollständiges Kryptierverfahren und ist vom Hersteller der Industriesysteme ohne spezifische Kenntnisse auf dem Gebiet der Kryptologie sofort einsetzbar. Das implementierte Kryptierverfahren (Verschlüsselungs-Algorithmus, Schlüsselmanagement und Sicherheitsfunktionen) organisiert automatisch die garantiert sichere Punkt-zu-Punkt-Übertragung der Daten und den Schutz sicherheitsrelevanter Daten auf dem Modul. Die notwendigen Schlüssel für die verschlüsselte Datenübertragung werden automatisch mittels integrierten physikalischen Zufallsgenerators ausgezeichneter Qualität erzeugt. Das Schlüsselmanagement wird vom OEM-Modul verwaltet, so daß vom Anwender kein Handlungsbedarf besteht.

Technische Daten

- Max. Abmessungen 35x45x3,5 (mm)
- 2 Kanäle asynchrones serielles Interface, bidirektional, TTL-Pegel
- Wählbare Baudraten: 1,2; 2,4; 4,8; 9,6; 19,2; 38,4; 57,6; 115,2; 230,4 (Kbit)
- Integrierter physikalischer Zufallsgenerator ausgezeichneter Qualität
- Anschluß aller Signale über Löt pads bis 15 cm Länge
- Stromversorgung bei 5V ca. 60mA

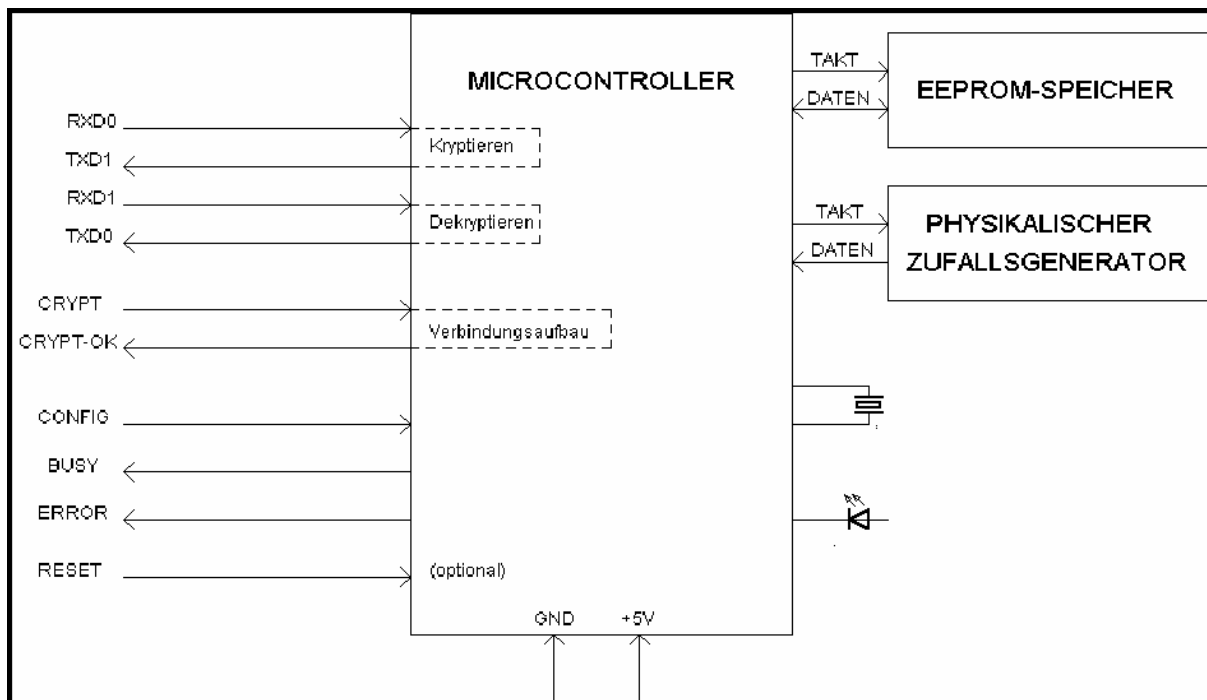
Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 3 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

- Standby-Modus: Reduzierung der Stromaufnahme (< 20mA)
- Betriebstemperatur: -10...+85°C
- Luftfeuchtigkeit: nicht kondensierend

Blockschaltbild

Das Blockschaltbild zeigt die wesentlichsten Komponente des Moduls sowie alle Schnittstellensignale:

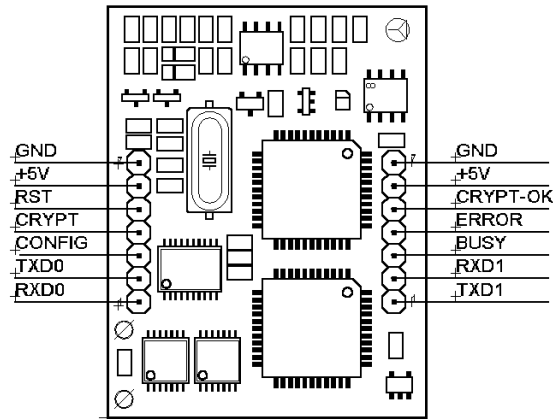


Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 4 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Schnittstellen

Anschlußbelegung des OEM-Moduls CM200 (Top view):



Signalname	Richtung	Aktiv	Funktion
GND	Power		Bezugspotential
+5V	Power		Stromversorgung +5V, 10% Toleranz
RXD0	Input		Asynchrones Empfangssignal vom Steuersystem
TXD0	Output		Asynchrones Sendesignal zum Steuersystem
RXD1	Input		Asynchrones Empfangssignal vom Übertragungssystem
TXD1	Output		Asynchrones Sendesignal zum Übertragungssystem
BUSY	Output	Low	OEM-Modul aktiv, es werden keine Daten vom Steuer- und Übertragungssystem angenommen
ERROR	Output	Low	Fehler in der Verarbeitung oder in der Verbindungsaufnahme
CONFIG	Input	Low	Konfigurationsmodus aktiv, nicht bei kryptierter Verbindung möglich
CRYPT	Input	Low	Aktiviert eine kryptierte Verbindung, nicht im Konfigurationsmodus möglich
CRYPT-OK	Output	Low	Meldet dem Steuersystem, daß eine verschlüsselte Verbindung aufgebaut ist
RST	Input	High	Externer RESET-Eingang, Neustart des OEM-Moduls

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 5 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Beschreibung der Schnittstellensignale

Stromversorgung VCC, GND:

Das Modul wird mit +5V (=VCC) versorgt und benötigt ca. 60 mA im Aktivmodus. Die Störspannung auf der Versorgungsspannung soll den üblichen Richtwerten für digitale Versorgungsspannungen entsprechen ($V_{ssmax.} < 100mV$). Die Toleranz der Versorgungsspannung ist 10% vom Sollwert.

Für alle **RDX/TXD**-Signale gilt:

- Asynchrone serielle Datensignale mit TTL-Pegel
- Datenprotokoll 8 Bit, keine Parität, 1 Stopbit
- Datenübertragung bis 230,4 KBit

BUSY:

Handshake-Signal zwischen Steuersystem und Modul. Ist das BUSY-Signal aktiv (low-activ), können keine Daten angenommen werden (auch nicht vom Übertragungssystem). Eine Ausnahme bildet der Konfigurationsmodus: es können Daten mit dem Steuersystem ausgetauscht werden. Bei der Programmierung des Steuersystems ist das unter Sicherheitsaspekten zu beachten.

ERROR:

Wird dieses Signal durch das Modul aktiv (low-activ) geschaltet, so ist eine verschlüsselte Kommunikation mit einer Übertragungseinrichtung verhindert. Das Signal zeigt einen Fehler der internen Verarbeitung oder eine fehlerhafte Verbindungsaufnahme an und kann nur im Konfigurationsmodus oder durch ein RESET des Moduls zurückgesetzt werden.

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 6 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

CONFIG:

Dieses Signal kann vom Steuersystem aktiviert werden (low-activ). Es können Parameter abgefragt oder verändert werden. Während der Konfiguration ist das BUSY-Signal als Rückmeldung aktiv geschaltet. Ist das Signal CRYPT aktiv, kann nicht in den Konfigurationsmodus geschaltet werden.

CRYPT:

Das Signal kann nur bei deaktivierten Signalen CONFIG und ERROR aktiviert werden. Das Modul versucht mit einer Gegenstelle eine verschlüsselte Verbindung aufzubauen. Ein Fehler während der Authentisierungsphase bewirkt ein Abbruch der Kommunikation und eine Fehlermeldung an das Steuersystem mit dem ERROR-Signal.

CRYPT-OK:

Ist eine kryptierte Verbindung mit einer Gegenstelle erfolgreich aufgebaut, wird als Rückmeldung zum Steuersystem das Signal CRYPT-OK aktiviert (low-activ). Eine Deaktivierung des CRYPT-Signals bewirkt auch ein Rücksetzen des CRYPT-OK-Signals.

RST:

Das Modul besitzt eine eigene Power-ON-Resetlogik. Das Steuersystem kann alternativ ebenfalls ein RESET des Moduls auslösen. Das RESET-Signal ist high-activ und für 100ms zu aktivieren.

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 7 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Elektrische Parameter

Für die elektrischen Parameter der Schnittstellen gelten die Spezifikationen des Herstellers für den Microcontroller P89C51RD2 für folgende Signale:

- Busy, Error, Config, Crypt, Crypt-ok

Durch den UART-Schaltkreis SC26C92 sind folgende Signale spezifiziert:

- RXD0, TXD0, RXD1, TXD1

Die Leitungslängen zwischen Modul und Anwendersystem dürfen maximal 15 cm betragen.

Konfiguration

Für den Konfigurationsmodus sind die Steuersignale wie folgt zu setzen:

Signal „CRYPT“: inaktiv (high)

Signal „CONFIG“: aktiv (low)

Identifikation

Mit dieser Funktion kann die eingestellte Baudrate des Moduls ermittelt werden.

Im Abstand von > 100ms wird die Kennung 0x55 mit einer der möglichen Baudraten gesendet.

Wird ein Zeichen mit 0x55 empfangen, ist die Baudrate festgestellt.

Input: 0x55

RC: 0x55 (Modul gefunden)

Baudrate

Einer der übertragenen Parameter für die Baudraten-Einstellung des Moduls wird gespeichert und nach dem Verlassen des Konfigurationsmodus im Modul aktiviert. Alle Baudraten (außer 230,4 Kbit) sind für eine verschlüsselte Vollduplex-Verbindung geeignet. Weitere Einschränkungen sind in der Beschreibung für die automatische Neusynchronisation ausgewiesen.

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 8 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Input: 0x01, Parameter1, Parameter2

RC: 0x55 oder 0xaa (Programmierfehler)

Baudrate	Parameter1	Parameter2
230.400	0x08	0x00
115.200	0x10	0x00
57.600	0x20	0x00
38.400	0x30	0x00
19.200	0xfd	0x01
9.600	0xfd	0x00 (default)
4.800	0xfa	0x00
2.400	0xf4	0x00
1.200	0xd8	0x00
600	0x40	0x00
....300	0x50	0x00

Datenprotokoll

Das gewünschte Datenprotokoll wird an RXD0 gesendet und im Modul gespeichert.

Hinweis: das neue Datenprotokoll wird erst nach Verlassen der Konfiguration aktualisiert.

Input: 0x18, prot

Prot: 0x00: 8,N,1 (default)

0x01: 8,N,2

0x02: 8,E,1

0x03: 8,E,2

0x04: 8,O,1

0x05: 8,O,2

RC: 0x55 (ok) oder 0xaa (Programmierfehler)

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 9 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Userkey anzeigen

Die Anzeige des Userkeys kann nur nach erfolgreicher PIN-Eingabe erfolgen. Ist die PIN-Eingabe fehlerhaft, wird nur mit dem RC=0xaa quittiert. Jede Funktion mit einer PIN-Eingabe wird ca. 1 Sekunde verzögert bearbeitet.

Input: 0x02, PIN (4)
 RC: 0x55 (ok) oder 0xaa (Falsche PIN)
 Output: Userkey (16), nur bei RC=0x55

Userkey ändern

Nach einer erfolgreichen Authentisierung mit der PIN wird der neue Userkey zum Modul gesendet und mit dem Devicekey verschlüsselt gespeichert. Es wird empfohlen, den Userkey nur als ASCII-Zeichen zu definieren, da sonst in Zusammenarbeit mit dem Serviceadapter SA200 keine fehlerfreie Darstellung auf dem Terminalprogramm garantiert werden kann.

Input: 0x03, PIN (4)
 RC: 0x55 (ok) oder 0xaa (Falsche PIN)
 Input: Userkey (16)
 RC: 0x55 (ok) oder 0xaa (Programmierfehler)

Userkey default

Mit dieser Funktion wird der Userkey mit den Zeichen 16x „0“ (ASCII) im Modul programmiert

Input: 0x04, PIN (4)
 RC: 0x55 (ok) oder 0xaa (falsche PIN oder Programmierfehler)

Selbsttest Zufallsgenerator

In diesem Test werden 10.000 Bits erzeugt und die statistische Verteilung mit der Bewertung eines Halbbyte-Tests (die Anzahl der zufällig erzeugten Halbbytes aus vier aufeinanderfolgenden Bits werden gezählt) geprüft. Die in der Auswertung gezeigte Bewertung (Byte 19) reflektiert sehr

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 10 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

anspruchsvolle Kriterien für einen physikalischen Zufallsgenerator: Bei einem Mittelwert von 156 ist die zulässige Abweichungen 40 für jedes Halbbyte. Statistisch betrachtet können 5% aller erzeugten Tests aus einer positiven Bewertung herausfallen.

Input: 0x05,

RC: 19 Bytes

01. Byte: Anzahl der „1“ bei 10.000 Bit (hex), höherwertiger Teil der Anzahl
02. Byte: Anzahl der „1“ bei 10.000 Bit (hex), niederwertiger Teil der Anzahl
03. Byte: Anzahl Wert „0x00“ (hex)
04. Byte: Anzahl Wert „0x01“ (hex)
05. Byte: Anzahl Wert „0x02“ (hex)
06. Byte: Anzahl Wert „0x03“ (hex)
07. Byte: Anzahl Wert „0x04“ (hex)
08. Byte: Anzahl Wert „0x05“ (hex)
09. Byte: Anzahl Wert „0x06“ (hex)
10. Byte: Anzahl Wert „0x07“ (hex)
11. Byte: Anzahl Wert „0x08“ (hex)
12. Byte: Anzahl Wert „0x09“ (hex)
13. Byte: Anzahl Wert „0x0a“ (hex)
14. Byte: Anzahl Wert „0x0b“ (hex)
15. Byte: Anzahl Wert „0x0c“ (hex)
16. Byte: Anzahl Wert „0x0d“ (hex)
17. Byte: Anzahl Wert „0x0e“ (hex)
18. Byte: Anzahl Wert „0x0f“ (hex)
19. Byte: 0x55 (ok) oder 0xaa (außerhalb der zulässigen Grenzen)

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 11 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Kontinuierliche Generierung von Zufallszahlen

Der zweite Test stellt eine kontinuierliche Generierung von Zufallswerten dar. Die Daten können für statistische Langzeituntersuchungen genutzt werden. Dieser Test kann mit dem Zeichen „ESC“ jederzeit abgebrochen werden.

Input: 0x07

Output: 24 Byte in Blöcken (Hex-Format) im Abstand von ca. 50ms

Abbruch mit 0x1b

PIN ändern

Die 4-stellige PIN ist durch alle ASCII-Zeichen (Buchstaben, Ziffern, Sonderzeichen, alle mit und ohne Shift-Taste, 89 verschiedene) charakterisiert; somit ergeben sich 62,7 Millionen Varianten.

Input: 0x08, alte PIN (4)

RC: 0x55 (ok) oder 0xaa (Falsche PIN, Abbruch)

Input: neue PIN (4)

RC: 0x55 (ok) oder 0xaa (Programmierfehler)

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 12 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Neusynchronisation

Eine automatische Neusynchronisation ist mit Halbduplex-Übertragungen ohne Protokoll (Z-Modem, X-Modem usw.) möglich. Während einer Neusynchronisation (Signal Busy aktiv) werden vom Steuersystem keine Daten akzeptiert. Folgende Parameter organisieren eine automatische Neusynchronisation bei einer verschlüsselten Verbindung:

Input: 0x06, sync
 sync: 0x00 keine automatische Neusynchronisation (default)
 0xff automatische Neusynchronisation aktiviert
 RC: 0x55 (ok) oder 0xaa (Programmierfehler)

Kryptierte Loop für Selbsttest

Voraussetzung für diesen Funktionstest ist eine Brücke zwischen TXD1 und RXD1. Für eine Anwendung in einer Applikation ist diese Funktion nicht geeignet. Sie unterstützt vor allem den Serviceadapter SA200.

Input: 0x09
 RC: 0x55 (ok) oder 0xaa (Fehler Zufallsgenerator)
 Zeichen an RXD0 werden verschlüsselt, über TXD1 nach RXD1 gesendet (Loop)
 und wieder von TXD0 im Klartext zurückgesendet
 Abbruch mit ESC (0x1b)
 RC: 0x55

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 13 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Offene Loop für Selbsttest

Äquivalent zur vorherigen Funktion kann hier eine Loop im Klartext getestet werden.

Input: 0x10
 RC: 0x55 (ok)
 Abbruch mit ESC (0x1b)
 RC: 0x55

Default-Werte

Soll der Fertigungszustand programmiert werden oder ist die PIN vergessen worden, so stellt dieser Befehl default-Werte ein.

Input: 0x11, 0x55, 0xaa
 RC: 0x55 (ok), 0xaa (Programmierfehler)
 Default: Baudrate 9.600 bps
 Userkey (ASCII): 16x „0“
 PIN (ASCII): 4x „0“
 Neusynchronisation: 0x00 (keine)
 Datenprotokoll: 0x00 (8,N,1)

Stromsparmodus

Per Befehl kann die Stromaufnahme auf ca. 40% reduziert werden. Der Normalzustand wird wieder durch ein beliebiges Zeichen an einem der seriellen Eingänge eingestellt. Der Stromsparmodus kann nur im Konfigurationsmodus aktiviert werden.

Input: 0x12
 RC: 0x55 (ok)
 Abbruch Stromsparmodus mit einem beliebigen Zeichen an RXD0 oder RXD1

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 14 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Fehlermeldung

Eine Fehlermeldung wird durch aktives ERROR-Signal vom Modul angezeigt. Dieses Signal kann nur durch ein RESET des Moduls oder durch diese Funktion rückgesetzt werden.

Input: 0x13

RC: Fehlernummer

Fehlernummer: 0x10: CRC-Fehler des EEPROM-Speichers

0x11: Fehler Zufallsgenerator

0x12: Empfangsfehler bei Authentisierung

0x13: Timeout in einer Funktion

Version

Die Firmware-Version ist ein fest programmierter Parameter des μ C und wird per Befehl an TXD0 gesendet.

Input: 0x14

RC: 5 Byte ASCII (z.B. „V 1.0“)

Testfolgen Sessionkey

Zum Verifizieren der Varianz des vom physikalischen Zufallsgenerators erzeugten Sessionkey können beliebig viele Beispiele ausgegeben werden. Diese Funktion ist für eine Zusammenarbeit mit dem Serviceadapter SA200 gedacht

Input: 0x15

RC: formatierter ASCII-Text,

Beispiel:

Physikalischer Zufallsgenerator generiert Sessionkey (16 Byte)
Start und Abbruch mit jeder Taste

F0 95 2A 15 5F 93 A7 98 4E F7 5D C2 85 85 C8 C9

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 15 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Testfolgen Algorithmus

Eine fehlerfreie Implementierung des Algorithmus ist eine wesentliche Voraussetzung für die Vertraulichkeit der übertragenen verschlüsselten Daten. Mit dieser Funktion werden folgende verifizierbare Daten generiert:

- Ein Sessionkey wird mittels physikalischen Zufallsgenerator (128 Bit = 16 Byte) erzeugt
- Expansion des Sessionkey entsprechend Algorithmus-Vorschrift (256 Byte)
- Zustand der S-Boxen nach 256 Zeichen verschlüsseln (256 Byte)

Diese Funktion ist für eine Zusammenarbeit mit dem Serviceadapter SA200 gedacht

Input: 0x16

RC: formatierter ASCII-Text,

Beispiel:

```

Physikalischer Zufallsgenerator generiert Sessionkey (16 Byte)
45 6F D7 40 A6 F3 3D BD DB 0D 9D 46 65 61 8B EF

Expandierter Sessionkey (256 Byte)
44 B5 8E 55 76 EB 54 0B 5D 84 1A 6B DC F8 7F 1C
49 EE 9F F2 AC 5F 43 3E CE F4 C4 8D 82 35 A4 B2
DB A7 6F E8 CD 9E AB BC BE 65 27 80 63 BA 52 0E
FF 12 D9 19 F5 57 56 15 77 92 F0 E1 78 24 20 A5
CA 13 93 59 86 7E 01 B9 2D 36 EC 4B 6C 38 72 3C
67 75 2B C1 BB A1 53 F1 DD 7A 34 17 9C 91 C6 9A
E7 3D C3 66 70 8C 2A 1E 42 05 A2 C5 C8 A6 31 47
46 D6 28 4F F3 73 29 71 8B 06 EF B7 B3 3A 21 E3
89 85 6E DF 69 62 45 2E EA 1F 22 32 40 F6 97 BF
D0 90 04 B1 C0 A3 6A 3B ED 2F B4 AF FA 4C E5 14
64 23 18 95 74 D4 50 61 B0 DA FB FE 98 AD E6 83
37 0F D3 39 5E 5C BD 9B CC E4 D8 0C AE 7D 68 1D
33 96 E0 CF 7C D2 D5 C9 87 81 7B 88 94 4E 11 03
51 25 16 9D 30 C7 0A 08 1B 3F 07 26 B6 DE E9 AA
8F E2 99 8A FD CB 2C 0D D1 A8 60 F9 5B 10 79 41
F7 4D A9 58 FC 02 B8 5A 4A D7 6D C2 09 A0 48 00

SBox nach 256 Zeichen (256 Byte)
EE 0D 93 02 E0 40 D1 9F 43 26 9D D0 09 80 A8 41
D7 B4 54 5C E4 19 81 03 15 B4 1D 45 87 51 C6 27
41 97 6B 6D 2C 5D 5E 80 E0 DE 1C 13 02 9F 49 9B
EA 0C CC 56 80 BE F6 E9 04 0B 2A 66 9B 39 93 72
B8 76 09 B2 CF D8 D6 09 E6 9B ED E0 B8 CE 48 34
DC 41 C1 4B 81 80 E6 23 00 B7 E3 54 89 81 14 DF
85 A1 A9 0F 8F 74 A0 A3 14 C4 DC 9A 25 9B AC 30
12 EE E3 E2 81 E3 73 41 AE 80 DC A3 BB 03 81 49
C9 E3 8D 73 E4 CD 4C C8 25 E5 3F A6 FA 3D 0A FA
0B BF 07 B6 6B 60 68 09 82 3A CB FC 0F 64 F8 3B
DD C3 BA 89 12 47 51 14 4D 83 A1 D1 0B A7 F5 3D
2D 31 54 99 34 54 37 77 FB 5B 59 98 B7 76 67 13
63 8E 5F 2B F7 49 65 CD 9C 4F 8E 96 60 69 96 12
A4 31 D8 F3 8E A0 B5 9D F7 A1 A7 2F CB A5 14 13
F2 1E 5A 48 04 82 7C 48 B5 49 12 72 11 F4 1C 17
27 BC 54 AF 52 CE 85 F9 CE 50 A5 34 97 B1 8D CA

```

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 16 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Einstellungen abfragen

Die Einstellungen für Synchronisation und Datenprotokoll werden an TXD0 gesendet.

Input: 0x17

RC: 2 Byte

- | | | |
|---------------------------|-------|---|
| 1. Byte: Synchronisation: | 0x00 | keine automatische Neusynchronisation |
| | 0xff | automatische Neusynchronisation aktiviert |
| 2. Byte: Datenprotokoll | 0x00: | 8,N,1 |
| | 0x01: | 8,N,2 |
| | 0x02: | 8,E,1 |
| | 0x03: | 8,E,2 |
| | 0x04: | 8,O,1 |
| | 0x05: | 8,O,2 |

Fehlermeldungen

Das Auftreten von Fehlermeldungen bedeutet nicht immer, daß ein technischer Fehler vorliegt.

Nachfolgend werden alle Fehlermeldungen einzeln betrachtet:

- **Prüfsummenfehler** (CRC-Fehler) des EEPROM-Speichers (Fehlernummer 0x10)

Nach einem Power-ON (PON) und nach Beendigung einer verschlüsselten Verbindung wird die Integrität des EEPROM-Speichers (gespeicherte verschlüsselte Parameter wie Userkey und PIN) überprüft. Ist die Kontrolle negativ, wird das Signal „ERROR“ aktiviert. Liegt ein externes RESET-Signal zu kurz (< 100ms) oder undefiniert an, kann der PON-Test zu Fehler führen, obwohl Datenintegrität vorliegt.
- **Fehler Zufallsgenerator** (0x11)

Diese Fehlermeldung wird bei der internen statistischen Kontrolle nach der Generierung von Zufall nach PON und für verschiedene Funktionen (Erzeugung von Sessionkey und Initialvektoren) aktiviert. Es werden Tests auf statistische Gleichverteilung von 0/1-Bits und konstante Bitfolgen bewertet. Ist ein solcher Test negativ, sollte ein aussagekräftiger Test mit

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 17 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

der Funktion „Selbsttest Zufallsgenerator“ mehrfach durchgeführt werden (diese Funktion aktiviert nicht das ERROR-Signal bei negativer Bewertung!). Sind auch diese Tests zu mehr als 5% fehlerhaft, ist das Modul zum Hersteller zu senden.

- **Empfangsfehler** bei Authentisierung (0x12)

Für diesen Fehler können zwei verschiedene Ursachen verantwortlich sein:

- Tritt während einer Verbindungsaufnahme zwischen Sender und Empfänger eine mehrfache Datenverfälschung auf, ist die Authentisierung negativ und wird als aktives ERROR-Signal gemeldet.
- Sind die Userkeys beider Seiten nicht identisch, ist die Authentisierung negativ. Die Kommunikation zur Übertragungseinrichtung wird blockiert und das ERROR-Signal aktiviert.

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 18 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

- **Timeout (0x13)**

Werden bei einer Verbindungsaufnahme die vereinbarten Daten der Authentisierung nicht vollständig übertragen, wird nach einer Wartezeit von ca. 5 Sekunden die Funktion mit Fehlermeldung und aktivem ERROR-Signal abgebrochen.

Verschlüsselte Verbindungsaufnahme

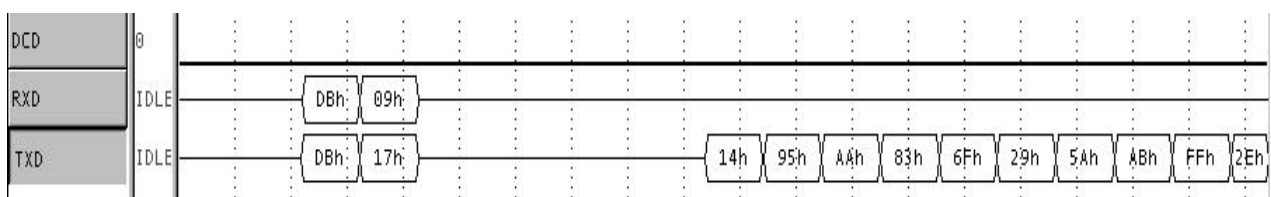
Der Verschlüsselungsmodus wird unter folgenden Voraussetzungen aktiviert:

- Signal „CRYPT“ aktiv (low)
- Signal „CONFIG“ inaktiv (high)
- Signal „ERROR“ inaktiv (high)

Für die verschlüsselte Verbindung wird ein jeweils unidirektionaler Sendekanal in jede Richtung aufgebaut, d.h., für Sende- und Empfangsrichtung existiert ein unidirektionaler Schlüssel. Zur Verhinderung von Replay-Angriffen wird das Challenge-Response-Verfahren eingesetzt.

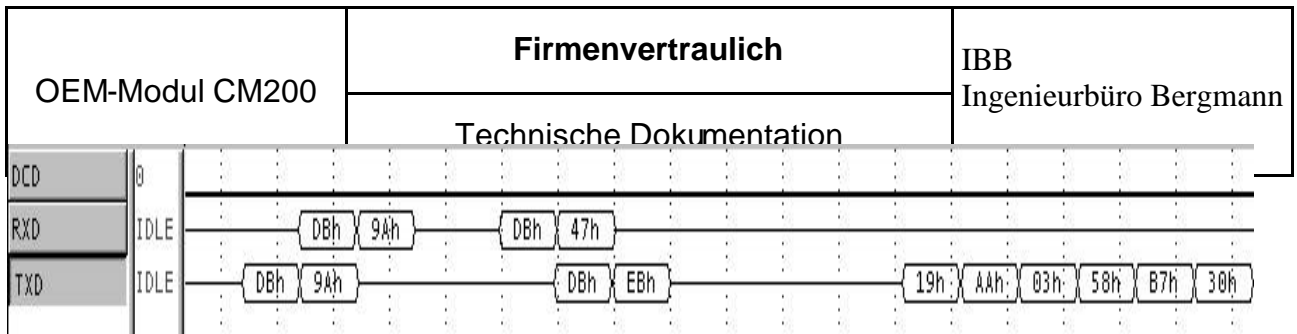
Nach der Aktivierung des CRYPT-Signals auf Sender und Empfängerseite werden von beiden Seiten nacheinander folgende Funktionen ausgeführt:

Zuerst wird ermittelt, welche Seite die Authentisierung beginnt. Hierzu tauschen beide Seiten nach dem Synchronisationszeichen (0xDB) einen Zufallswert aus.



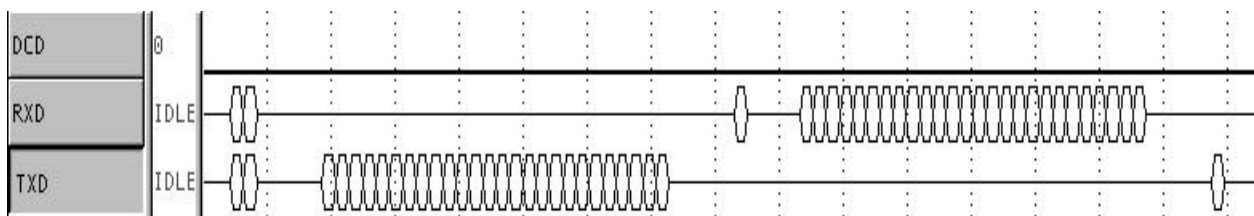
Die Seite mit dem höheren Wert beginnt. Sind beide Werte gleich, werden erneute Zufallswerte ausgetauscht.

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 19 von 22



Anschließend wird der per Zufallsgenerator erzeugte Sessionkey verschlüsselt zur Gegenstelle übertragen:

- Generierung eines unikaten Sessionkeys und Initialvektors mittels Zufallsgenerator, statistische Kontrolle der Zufallsdaten, bei Fehler Abbruch der Verbindung
- Addition von Masterkey, Userkey und Initialvektor → Transportkey
- Berechnung einer CRC-Summe über den Sessionkey
- Verschlüsseln von Sessionkey und CRC-Summe mittels Transportkey
- Übertragen von Initialvektor, verschlüsselten Sessionkey und CRC-Summe zur Gegenstelle
- Einstellen der Verschlüsselungsfunktion in Senderichtung mit erzeugtem Sessionkey
- Warten auf Quittungszeichen und verschlüsselten Sessionkey der Gegenstelle
- Empfang von Initialvektor, verschlüsselten Sessionkey und CRC-Summe der Gegenstelle
- Addition von Masterkey, Userkey und empfangenen Initialvektor
- Entschlüsseln des empfangenen Sessionkeys und CRC-Summe
- Vergleich von übertragener CRC-Summe mit errechneter CRC-Summe
- Anfangseinstellung der Empfangsrichtung mit Sessionkey der Gegenstelle
- Quittungszeichen an die Gegenstelle senden

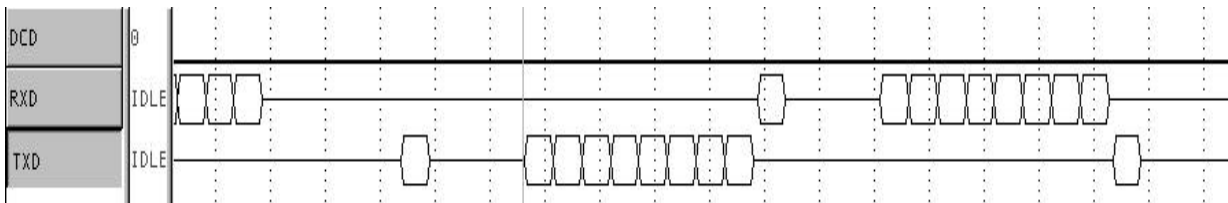


Danach erfolgt das Challenge-Response-Verfahren: eindeutige Authentisierung

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 20 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

- 8 Byte Zufall (Prüffolge) werden mit dem erzeugten Sessionkey verschlüsselt und zur Gegenstelle gesendet
- Die Gegenstelle empfängt, entschlüsselt und verschlüsselt die Prüffolge und sendet diese nach einem Quittungszeichen zurück
- Der Absender der Prüffolge entschlüsselt die empfangene Prüffolge, vergleicht mit der ursprünglichen Prüffolge und sendet ein Quittungszeichen zurück
- Danach wird das Signal Crypt-OK aktiviert, Daten können verschlüsselt übertragen werden
- Bei Fehler wird die Verbindung mit einer Meldung (Signal Error aktiv) beendet



Danach werden alle Daten verschlüsselt übertragen und auf der Gegenstelle automatisch entschlüsselt. Eine Klartext-Übertragung ist nicht möglich. Ebenso können die Übertragungssysteme (Modems) nicht mehr mit Befehlen erreicht werden, da alle Daten verschlüsselt sind. Beendet wird die Funktion Verschlüsselung durch Deaktivierung des „CRYPT“-Signal. Das Signal „CRYPT-OK“ wird danach deaktiviert (high).

Applikation Modemübertragung

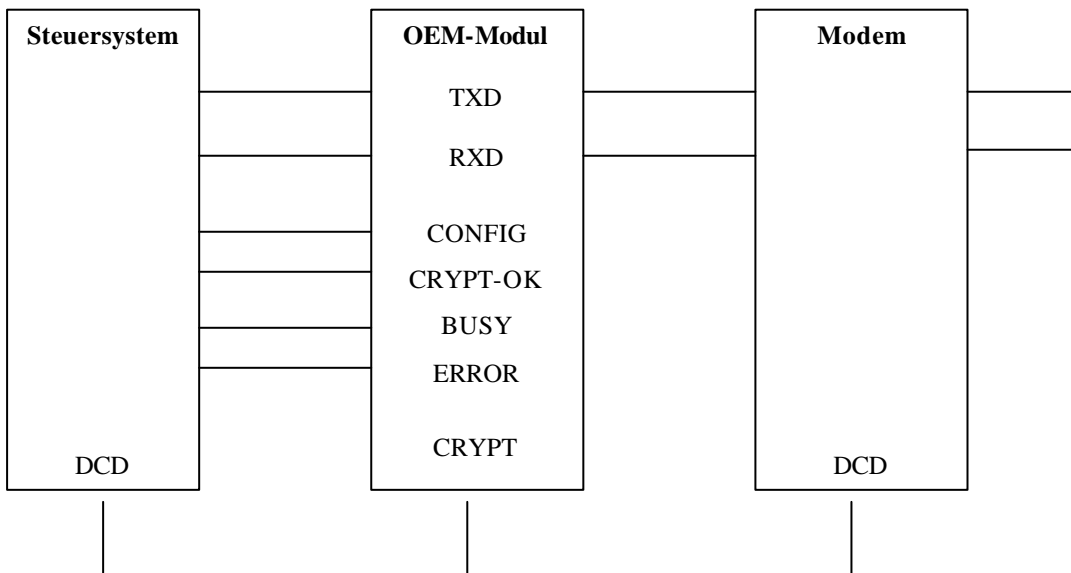
Im Folgenden wird eine mögliche Applikation für eine verschlüsselte Modemübertragung beschrieben. Diese Applikation für Industrieanwendungen mit Datenübertragungen mittels Modem ist typisch für Fernwartung und Fernkonfiguration. Da vor allem auch sicherheitsrelevante Daten wie Paßwörter und Parameter übertragen werden, ist die Integration eines Verschlüsselungsmoduls notwendig.

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 21 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Das folgende Beispiel zeigt eine Lösung, bei der die Umschaltung in die Verschlüsselung unabhängig vom Steuersystem erfolgt. Eine Möglichkeit der automatischen Umschaltung ist mit dem Modem-Signal DCD (Data Carrier Detect) gegeben. Damit wird das Steuersystem entlastet und garantiert, daß bei jedem Verbindungsaufbau eine verschlüsselte Datenübertragung realisiert wird. Es muß darauf geachtet werden, daß auf Sender- und Empfängerseite die Modems mit dem AT-Befehl für eine Generierung des DCD-Signals initialisiert sind (AT&C1, meist eine Standardeinstellung). Erkennt das Steuersystem das nach einem Verbindungsaufbau vom OEM-Modul geschaltete Signal CRYPT-OK, ist eine verschlüsselte Datenübertragung garantiert. Bei Aktivierung der automatischen Neusynchronisation ist die Verknüpfung des Busy-Signals mit dem Modem-Handshake-Signal CTS notwendig, da bei einer Neusynchronisation vom Modul keine Daten akzeptiert werden.

Bei aktivierter Neusynchronisation ist zu beachten, daß die durchschnittliche Übertragungsrate je nach Baudrate sinkt, während in beiden Richtungen keine Daten übertragen werden können. Der Abstand zwischen zwei Neusynchronisationen ist zufällig und beträgt im Mittel 256 Zeichen. Eine automatische Neusynchronisation ist nur bei Halbduplex-Übertragungen möglich.



Blockschaltbild einer typischen Applikation

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 22 von 22

OEM-Modul CM200	Firmenvertraulich	IBB Ingenieurbüro Bergmann
	Technische Dokumentation	

Datum: 20.12.01		
Dateiname: OEM-Modul CM200	Version: 1.0	Seite: 23 von 22