Rechtliche Bestimmungen

Weitere Informationen

Bei Fragen hilft Ihr Fachhändler, bei dem Sie das Gerät erworben haben, gerne weiter.

Weitere Informationen zum Produkt und zur E3/DC GmbH entnehmen Sie bitte der Firmenwebsite.

E3/DC GmbH
Karlstraße 5
D-49074 Osnabrück
Telefon: +49 541 760268-0
Fax: +49 541 760268-19
E-Mail: info@e3dc.com
Website: www.e3dc.com
Kundenportal: https://s10.e3dc.com/s10

Inhaltsverzeichnis

1 Beschreibung

Das S10 ist ein Energiespeichersystem, bestehend aus Wechselrichter, Lithium-Ionen-Akkus und Batteriewandler. Alle Komponenten sind vollständig in einem System integriert.

Im folgendem wird von Hauskraftwerk gesprochen. Damit ist sowohl das S10-E als auch das S10-MINI gemeint.

Die Funktionsweise des Hauskraftwerks erlaubt es, Energie zu speichern und bei Bedarf wieder abzugeben. Dieses geschieht je nach Hausverbrauch vollautomatisch. Dennoch kann es Sinn machen, das Hauskraftwerk in ein übergeordnetes Energiemanagement oder beispielsweise eine Hausautomation einzugliedern.

Um dieser Anforderung gerecht zu werden, hat die E3/DC GmbH ein Fernauslese- und Fernsteuerungsprotokoll, das RSCP (Remote-Storage-Control-Protocol), für die Hauskraftwerke entwickelt.

1.1 Übertragung

Obwohl RSCP dafür ausgelegt ist, über unterschiedlichste Medien übertragen zu werden, wird momentan nur die Kommunikation über TCP/IP über Ethernet unterstützt.

Das Hauskraftwerk öffnet zu diesem Zweck einen TCP-Socket auf **Port 5033**. Zu diesem kann sich ein RSCP-Client aus dem lokalen LAN verbinden.

Die Verbindung ist grundsätzlich per AES verschlüsselt. Mehr dazu im Abschnitt zum Thema Verschlüsselung (s. S. 8f.).

1.2 Service Discovery

Zum einfachen Verbindungsaufbau innerhalb des lokalen LANs versendet das Hauskraftwerk in regelmäßigen Abständen Nachrichten nach dem UPnP-Standard.

2 Protokollbeschreibung

Die Kommunikation zwischen den beiden Teilnehmern erfolgt auf Basis von sogenannten RSCP-Frames.

- Der verbindungsaufbauende Client sendet immer einen RSCP-Frame.
- Der empfangene RSCP-Frame wird vom Hauskraftwerk beantwortet.
- Erst nach Eintreffen der Antwort kann vom Client eine erneute Anfrage gesendet werden.

2.1 Aufbau eines Frames

Ein RSCP-Frame ist immer identisch aufgebaut.

„**MAGIC**“ und „**CTRL**“:

Der RSCP-Frame startet mit den zwei Magic Bytes (0xE3 0xDC), gefolgt von einem 2 Byte breiten Protokoll-Kontrollfeld (CTRL).

„**TIME**“ (Unterfelder „**SECONDS**“ und „**NSECONDS**“):

Im anschließenden Feld TIME wird der Absendezeitpunkt des Frames eingetragen.
TIME ist in zwei Unterfelder geteilt: SECONDS, NSECONDS.
In diesen Unterfeldern wird die lokale Absendezeit des Frames eingetragen, in Sekunden und Nanosekunden seit 01.01.1970 (Unixtime).
Das Feld NSECONDS kann hierbei auf Mikrosekunden gerundet werden.

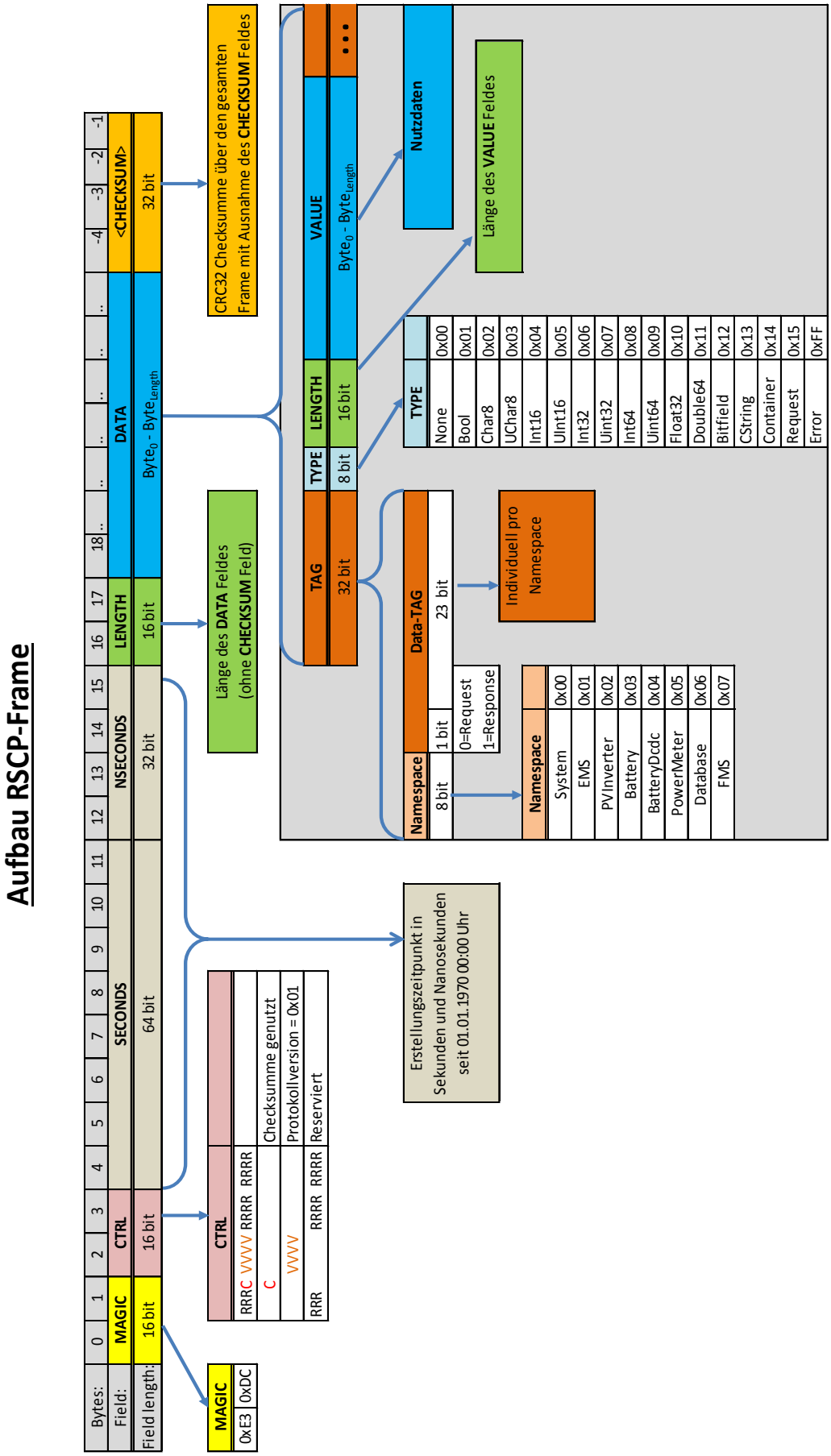
„**LENGTH**“:

Im Folgefeld LENGTH wird die Anzahl der im Frame enthaltenden DATA-Bytes eingetragen, die darauf folgen.

„**CHECKSUM**“ (optional):

Das Feld CHECKSUM am Ende des Frames ist optional und sollte nur bei Verbindungen genutzt werden, die nicht auf tiefer liegenden Schichten abgesichert sind.
So hat beispielsweise TCP/IP ein eigenes CHECKSUM-Feld, so dass die Checksumme von RSCP nicht genutzt werden muss, um Übertragungsfehler abzusichern.
Hinweis:
Wird allerdings vom Sender eine Checksumme benutzt, muss der Empfänger immer auch mit Checksumme antworten!

Die folgende Abbildung bietet einen Überblick über den RSCP-Frame.


Aufbau RSCP-Frame
Bytes:
Field:
Field length:
MAGIC
CTRL
SECONDS
NSECONDS
LENGTH
DATA
<CHECKSUM>
16 bit
64 bit
32 bit
16 bit
Byte0 - ByteLength
32 bit
MAGIC
0xE3 0xDC
CTRL
RRRC VVVV RRRR RRRR
C
Checksumme genutzt
VVVV
Protokollversion = 0x01
RRR RRRR RRRR Reserviert
Erstellungszeitpunkt in Sekunden und Nanosekunden seit 01.01.1970 00:00 Uhr
Länge des DATA Feldes (ohne CHECKSUM Feld)
CRC32 Checksumme über den gesamten Frame mit Ausnahme des CHECKSUM Feldes
TAG
32 bit
TYPE
8 bit
LENGTH
16 bit
VALUE
Byte0 - ByteLength
Nutzdaten
Länge des VALUE Feldes
Namespace
8 bit
Data-TAG
1 bit
23 bit
0=Request
1=Response
Individuell pro Namespace
Namespace
System 0x00
EMS 0x01
PVInverter 0x02
Battery 0x03
BatteryDcdc 0x04
PowerMeter 0x05
Database 0x06
FMS 0x07
TYPE
None 0x00
Bool 0x01
Char8 0x02
UChar8 0x03
Int16 0x04
UInt16 0x05
Int32 0x06
Uint32 0x07
Int64 0x08
Uint64 0x09
Float32 0x10
Double64 0x11
Bitfield 0x12
CString 0x13
Container 0x14
Request 0x15
Error 0xFF

2.2 Das Protokoll-Kontrollfeld CTRL

Mit Hilfe dieses Feldes werden protokollspezifische Eigenschaften zwischen den Kommunikationspartner, vereinbart. Dazu ist dieses Feld bitweise codiert. Die Bedeutung der einzelnen Bits ist der folgenden Tabelle zu entnehmen:

Byte	0								1								Bedeutung:
Bit	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	
	R	R	R	C	V	V	V	V	R	R	R	R	R	R	R	R	
	R	**R**	**R**						**R**	**R**	**R**	**R**	**R**	**R**	**R**	**R**	**Reserviert für zukünfige Erweiterungen**
	0	0	0						0	0	0	0	0	0	0	0	Derzeitiger Zustand für die reservierten Bits
				C													**Checksummen Flag**
				0													Checksumme wird nicht verwendet
				1													Checksumme wird verwendet. Das Feld CRC am Ende des Frames ist ein Pflichtfeld, ansonsten wird der Frame verworfen!
					V	**V**	**V**	**V**									**Versionskennzeichnung**
					0	0	0	1									Version 1.0 (Momentan einzig zugelassener Wert)

2.3 Das Feld TIME

Das Feld TIME enthält den Absendezeitpunkt des Frames seit 01.01.1970, 00:00:00 Uhr.

Damit auch Echtzeitanwendungen über RSCP gesteuert werden können, hat dieses Feld eine Auflösung von 1 Nanosekunde.
Dazu ist das Feld in zwei Unterfelder unterteilt:

- Das erste Feld SECONDS enthält den Zeitstempel des Frames in Sekunden. Dies entspricht dem Unixtime-Zeitstempel. Entgegen den heutigen noch üblichen Implementierungen ist dieses Feld jedoch 64bit breit, um eine Verwendung über den 19. Januar 2038 um 03:14:08 Uhr hinaus zu gewährleisten.
- Das zweite Feld NSECONDS enthält anteilig abgelaufenen Nanosekunden. Dieses Feld ist 32bit breit und darf den Wert 1 000 000 000 nicht überschreiten. Ansonsten wird das Frame als ungültig verworfen.

2.4 Das Feld LENGTH

Dieses Feld enthält die Anzahl der Daten die im Feld DATA übertragen werden und ist 2 Byte breit.

2.5 Das Feld DATA

Das Feld DATA enthält die Nutzdaten des RSCP-Frames. Diese werden TLV-kodiert übertragen. Allerdings wird nicht das Format BER-TLV verwendet, sondern nur der Grundgedanke von TLV.

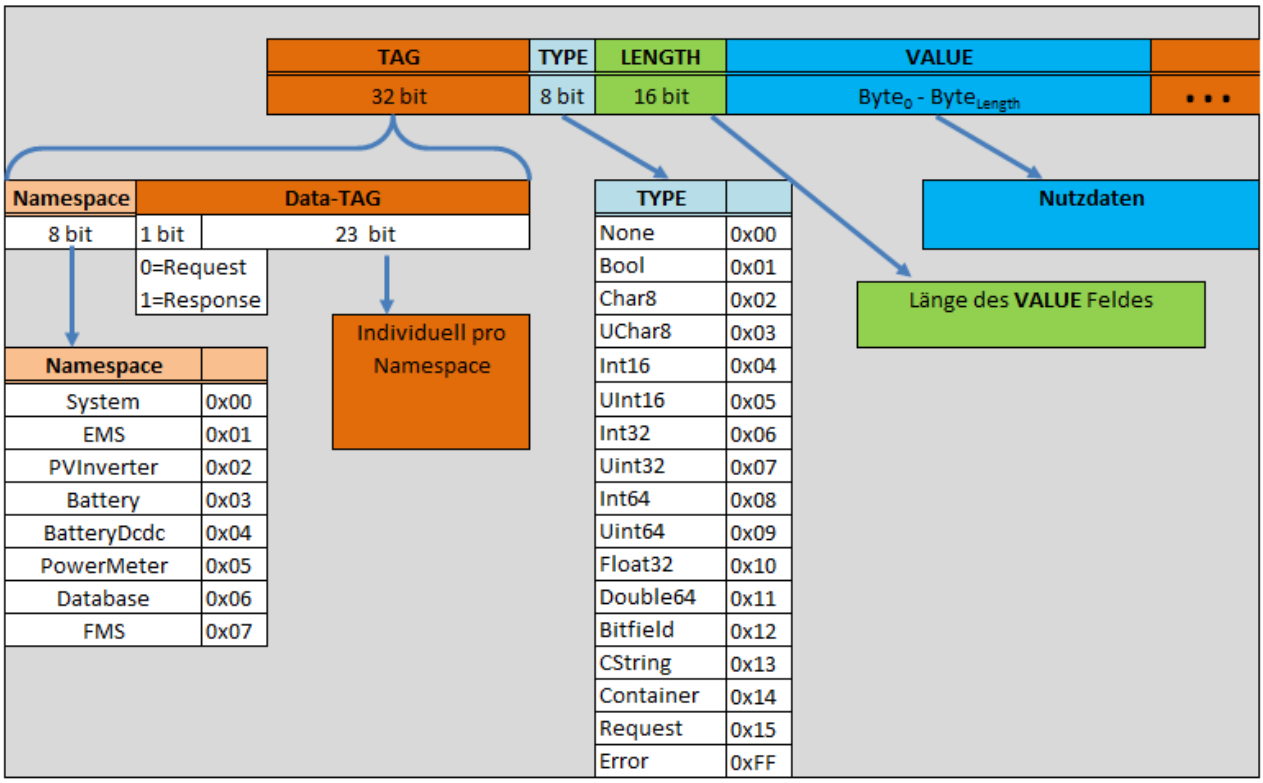
Das TAG-Feld im RSCP-Format ist 32 Bit breit und unterteilt sich in Namespace (8 Bit) und Data-TAG (24 Bit). Diese Unterteilung ermöglicht eine saubere Erstellung und Unterteilung von TAG-Listen.

„**TYPE**“:

Im Unterschied zum TLV Standard wird bei RSCP nun ein TYPE-Feld zwischen TAG und LENGTH eingefügt. Dieses 1 Byte breite Feld definiert, um welchen Datentyp es sich innerhalb des Feldes VALUE-handelt. Dadurch können Analysetools die Daten korrekt darstellen, ohne die konkrete Interpretationsliste vorhalten zu müssen.

„**LENGTH**“:

Das Feld LENGTH innerhalb des DATA-Feldes ist ebenfalls 2 Byte breit. Allerdings können in einem TAG maximal 65.528 Bytes übertragen werden, da das DATA-Feld immer mindestens einen TLV-Header enthält. Die Einschränkung ergibt sich aus dem LENGTH-Feld des RSCP-Frames, das ebenfalls 16 Bit breit ist.
In einem RSCP-Frame können mehrere TLV-Daten übertragen werden, diese werden aneinander gereiht.
Der große Vorteil dieser Übertragungsmethode ist, dass grundsätzlich alle Datenformate übertragen werden können. Die Software, die RSCP unterstützt, muss also nur die Container auswerten, die sie verarbeiten kann. Trifft sie auf ein unbekanntes Kennzeichen, überspringt sie dieses TAG anhand des LENGTH-Feldes und arbeitet den restlichen Teil ab.



„**TAG**“:

Wie bereits erwähnt, ist das Feld TAG beim RSCP-Datenformat logisch in Namespace und Data-TAG unterteilt. Dies vereinfacht die Erstellung von TAG-Listen, da die TAGs einfacher gruppiert werden können. In jedem Namespace kann also wieder von neuem mit der Durchnummerierung begonnen werden.
Die nachfolgende Tabelle enthält die momentan verfügbaren Namespaces.

Beim Data-TAG gibt es zusätzlich noch die Konvention, dass das 24. Bit bei Anfragen ans System eine 0, bei Antworten auf Anfragen eine 1 enthält. Dadurch lassen sich auf schnelle Art und Weise Antworten zu Anfragen zuordnen.

Eine aktuelle Liste mit den gültigen Tags kann von der E3/DC-Webseite heruntergeladen werden.

Namespace	Wert
RSCP	0x00
EMS	0x01
PVI	0x02
BAT	0x03
DCDC	0x04
PM	0x05
DB	0x06
FMS	0x07
SRV	0x08
HA	0x09
INFO	0x0A
EP	0x0B
SYS	0x0C
UM	0x0D
WB	0x0E

3 Verschlüsselung

Da über das RSCP-Protokoll sensible Daten übertragen werden können, ist es beim Einsatz über TCP/IP verschlüsselt.
Zum Einsatz kommt das AES-Verschlüsselungsverfahren im Cipher-Block-Chaining-Modus (CBC) mit 256 Bit Schlüssel- und Blocklänge. Leider bietet die recht populäre Bibliothek openSSL (1) noch keine Unterstützung für AES mit 256 Bit Blocklänge. Hier (2) kann eine freie C++ Klasse heruntergeladen werden, die den 256 Bit CBC-Modus unterstützt.

Das Passwort für den AES-Algorithmus wird erzeugt, indem der vom Benutzer definierte Passwortstring ohne Nullterminierung in ein 32 Byte großes (mit 0xFF aufgefülltes) Feld kopiert wird.

Beispiel:

```
unsigned char ucAesKey[32] = {
        0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
        0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
        0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
        0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
        0xFF, 0xFF, 0xFF, 0xFF
};
ucAesKey[32] = {
        'p',  'a',  's',  's',  'w',  'o',  'r',
        'd', 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
        0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
        0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF,
        0xFF, 0xFF, 0xFF, 0xFF
};
```

Wie das RSCP-Passwort am S10 vom Benutzer geändert werden kann, lesen Sie bitte in der aktuellen Bedienungsanleitung nach.

Der Initialisierungsvektor (IV) ist ebenfalls standardmäßig mit 0xFF initialisiert und 32 Byte groß.

4 Autorisierung

Um einen ungewollten Zugriff auf das S10 eines Kunden zu vermeiden, werden bei einem Verbindungsaufbau zusätzlich noch Benutzer-Berechtigungen abgefragt. Benutzer, die sich an einem S10 per RSCP anmelden möchten, müssen zuvor im E3/DC-Portal angelegt worden ein.

Nach dem Verbindungsaufbau muss das Tag REQ_AUTHENTICATION im ersten Frame übertragen werden. Als Daten werden innerhalb der Subtags AUTHENTICATION_USER und AUTHENTICATION_PASSWORD die Benutzerdaten übertragen.
Nach dem REQ_AUTHENTICATION-Tag können im selben Frame zusätzliche Anfragen mit übertragen werden. Das Benutzerlevel gilt ab sofort.

5 Literaturverzeichnis

1. **The OpenSSL Project.** openssl.org. *openssl.org.* [Online] [Zitat vom: 03. 02. 2015.] https://www.openssl.org/.

2. **Lomont, Chris.** lomont.org. [Online] [Zitat vom: 03. 02. 2015.] http://www.lomont.org/Software/Misc/AES/AES.php.