Protokolle

- IEC60870-5-101
- Modbus Protokoll

IEC60870-5-101

Fernwirktechnik Protokoll IEC60870-5-101

> Diese Seite befindet sich aktuell in Bearbeitung und die aufgeführten Informationen sind evtl. noch unvollständig! {.is-danger}

> Diese Seite beinhaltet eine reine Beschreibung des IEC60870-5-101 Protokolls. Für eine Übersicht der Einstellungen, die am SmartDog oder in den Konfigurationen der Fernwerktechnik-Klassen vorgenommen werden können, siehe hier bzw. hier. {.is-info}

Das Protokoll der Fernwirktechnik IEC60870-5-101 (kurz auch CS101 genannt) kommuniziert über eine serielle Schnittstelle.

Es können zwei Übertragungsmodi verwendet werden:

- Symmetrisch / Balanced
- Unsymmetrisch / Unbalanced {.links-list}

Symmetrische / Balanced Übertragung

Bei einer symmetrischen Verbindung handelt es sich immer um eine Punkt-zu-Punkt (End-to-End) Verbindung. Im Folgenden werden die Begriffe Unterstation für die Station, die in Überwachungsrichtung übertragt (d.h. der SmartDog) und Zentrale für die Station, die in Befehlsrichtung überträgt (d.h. das Gerät des Netzbetreibers) verwendet.

Damit eine aktive Verbindung aufgebaut werden kann, müssen zuerst beide Stationen normiert (initialisiert) werden. Hierbei senden sowohl die Unterstation, als auch die Zentrale kontinuierlich den Befehl "Abfrage des Zustands der Verbindungsschicht" ("request status of link"), welcher von der Gegenstelle mit "Zustand der Verbindungsschicht" ("status of link") beantwortet werden muss. Danach wird der Befehl "Normieren der Verbindungsschicht der Sekundärstation" ("reset of remote link") gesendet, welcher ebenfalls beantwortet werden muss.

Folgende Antworten sind zulässig (FC beschreibt die Nummer des zugehörigen Funktionscodes):

- FC: 0 → positive Bestätigung (`ACK`)
- FC: 1 → negative Bestätigung (`NACK`)
- FC: 14 → Dienst der Verbindungsschicht arbeitet nicht
- FC: 15 → Dienst der Verbindungsschicht nicht vorhanden

Entspricht die Antwort der Gegenstelle keiner positiven Bestätigung, so wird erneut die "Abfrage des Zustands der Verbindungsschicht" gesendet. Wird der Normierungs-Befehl positiv bestätigt, wechselt der Status der Verbindungsschicht auf "verfügbar" und es können weitere Daten übertragen werden.

Bei diesem Verbindungsaufbau werden folgende Daten übertragen:

Übertragungsrichtung	Telegramm-Info[^1]	Beschreibung	Rohdaten (HEX)	Anmerkung
Unterstation → Zentrale	RES: 0, PRM: 1, FC: 9	Abfrage des Zustands der Verbindungsschicht	`10 49 01 00 4a 16`	
Zentrale → Unterstation	RES: 1, PRM: 0, FC: 11	Zustand der Verbindungsschicht	`10 8B 01 00 8C 16`	
Unterstation → Zentrale	RES: 0, PRM: 1, FC: 0	Normieren der Verbindungsschicht der Sekundärstation	`10 40 01 00 41 16`	
Zentrale → Unterstation	RES: 1, PRM: 0, FC: 0	Positive Bestätigung	`10 80 01 00 81 16` bzw. `E5`	Feste Länge bzw. nur ein Byte

Da es bei einer symmetrischen Verbindung keinen expliziten Master und Slave gibt, erfolgt die Normierung auch in die entgegengesetzte Richtung:

Übertragungsrichtung	Telegramm-Info[^1]	Beschreibung	Rohdaten (HEX)	Anmerkung
Zentrale → Unterstation	RES: 1, PRM: 1 FC: 9	Abfrage des Zustands der Verbindungsschicht	`10 C9 01 00 CA 16`	
Unterstation → Zentrale	RES: 0, PRM: 0, FC: 11	Zustand der Verbindungsschicht	`10 0B 01 00 0C 16`	

Übertragungsrichtung	Telegramm-Info[^1]	Beschreibung	Rohdaten (HEX)	Anmerkung
Zentrale → Unterstation	RES: 1, PRM: 1, FC: 0	Normieren der Verbindungsschicht der Sekundärstation	`10 C0 01 00 C1 16`	
Unterstation → Zentrale	RES: 0, PRM: 0, FC: 0	Positive Bestätigung	`10 00 01 00 01 16` bzw. `E5`	Feste Länge bzw. nur ein Byte

Nach erfolgreicher Normierung der beiden Stationen wird die Verbindung aufrecht erhalten, indem nach Ablauf einer vorgegebenen Zeit die "Testfunktion für Verbindungsschicht" gesendet wird.

Übertragungsrichtung	Telegramm-Info[^1]	Beschreibung	Rohdaten (HEX)	Anmerkung
Unterstation → Zentrale	RES: 0, PRM: 1, FCB: 1, FCV: 1, FC: 2	Testfunktion für Verbindungsschicht	`10 72 01 00 73 16`	
Zentrale → Unterstation	RES: 0, PRM: 0, FC: 0	Positive Bestätigung	`10 80 01 00 81 16` bzw. `E5`	Feste Länge bzw. nur ein Byte

[^1]: Für eine genauere Beschreibung der Status-Bits der Telegramme, siehe Telegrammstrukturen

Die hierzu relevanten Informationen können in der Norm DIN EN 60870-5-101 auf Seite 21 ff. gefunden werden:

> Die Abfragen der Norm-Funktionscodes in Primärrichtung (0 bis zu 3 und 9) müssen positiv oder negativ beantwortet werden. Im Fall eines nicht vorhandenen (en: unimplemented) Dienstes muss die Sekundärstation mit dem Funktionscode 15 „Verbindungsschichtdienst nicht vorhanden“ antworten.[^2]

[^2]: DIN EN 60870-5-101, Kaptiel 6.2.1.2, S. 21 ff.

> | Funktionscodes und Dienste in Primärrichtung | Zulässige Funktionscodes und Dienste in Sekundärrichtung |
> |---|---|
> | <0> Normieren der Verbindungsschicht der Sekundärstation | <0> CONFIRM: ACK oder
<1> CONFIRM: NACK |
> | <1> Normieren des Anwenderprozesses | <0> CONFIRM: ACK oder
<1> CONFIRM: NACK |
> | <2> SEND/CONF-Testfunktion für Verbindungsschicht | <0> CONFIRM: ACK oder
<1> CONFIRM: NACK |

Funktionscodes und Dienste in Primärrichtung	Zulässige Funktionscodes und Dienste in Sekundärrichtung
<3> SEND/CONF-Anwenderdaten	<0> CONFIRM: ACK oder <1> CONFIRM: NACK
<4> SEND/NO REPLY-Anwenderdaten	keine Antwort
<9> REQUEST/RESP-Abfrage des Zustands der Verbindungsschicht	<11> RESPOND: Zustand der Verbindungsschicht
[Tabelle 4: Zulässige Kombinationen der Dienste der symmetrischen Verbindungsschicht]	

Unsymmetrische / Unbalanced Übertragung

Bei einer unsymmetrischen Verbindung handelt es sich um ein Master-Slave-System, d.h. es können mehrere Stationen an einen Bus angeschlossen werden, die alle mit dem selben Master kommunizieren.

Die Position des Masters füllt immer das Gerät des Netzbetreibers. Der SmartDog fungiert immer als Slave.

Telegrammstrukturen

Es werden zwei Telegrammstrukturen verwendet: Telegramme mit fester und variabler Länge.

Eine Übersicht des Aufbaus dieser Telegramme kann hier betrachtet werden:

- Dokumentation Beckhoff
- Dokumentation Vinci {.links-list}

Die Norm DIN EN 60870-5-101 definiert den Aufbau der Telegramme in Kapitel 7 auf den Seiten 28 ff.

Telegramm mit fester Länge:

Ein Telegramm mit fester Länge beginnt immer mit dem Start Byte `10 h` und endet immer mit dem Stopp Byte `16 h`. Die Länge beträgt entweder 5 oder 6 Byte, abhängig von der Länge der Adresse der Verbindungsschicht. Die Prüfsumme wird folgendermaßen berechnet: Byte 1 + Byte 2 (+ Byte 3)

Byte \ Bit	7	6	5	4	3	2	1	0
0	Start Byte (`10 h`)							
1	DIR	PRM	FCB ACD	FCV DFC	Functionscode			
(2)	Adresse der Verbindungsschicht LSB (optional*)							
(3)	Adresse der Verbindungsschicht MSB (optional)							
4	Prüfsumme							
5	Stopp Byte (`16 h`)							

Die Adresse der Verbindungsschicht ist bei symmetrischer übertragung optional. Falls diese angegeben wird, so ist sie ein oder zwei Byte lang. Das niedrigstwerige Byte wird zuerst übertragen.

Telegramm mit variabler Länge

Ein Telegramm mit variabler Länge beginnt immer mit dem Start Byte `68 h` und endet immer mit dem Stopp Byte `16 h`. Die Länge ist abhängig von den zu übertragenden Daten. Die Prüfsumme wird aus den Bytes 4 bis N - 2 berechnet.

Byte \ Bit	7	6	5	4	3	2	1	0
0	Start Byte (`68 h`)							
1	Länge Anwenderdaten							

Byte \ Bit	7	6	5	4	3	2	1	0
2	Länge Anwenderdaten (Kopie)							
3	Start Byte (`68` h)							
4	DIR	PRM	FCB ACD	FCV DFC	Funktionscode			
(5)	Adresse der Verbindungsschicht LSB (optional*)							
(6)	Adresse der Verbindungsschicht MSB (optional)							
7	Typkennung							
8	SQ	Anzahl der Informationsobjekte						
9	T	P / N	Übertragungsursache					
(10)	Herkunftsadresse (optional)							
11	Gemeinsame Adresse der ASDU LSB							
(12)	Gemeinsame Adresse der ASDU MSB (optional)							
Beginn Informationsobjekt 1								

Byte \ Bit	7	6	5	4	3	2	1	0
13	Adresse des Informationsobjekts LSB							
(14)	Adresse des Informationsobjekts (optional)							
(15)	Adresse des Informationsobjekts MSB (optional)							
16	Satz von Informationselementen							
(17 bis 24)	Zeitmarke `TODO: CP24Time2a` bzw. `CP56Time2a` (optional)							
Ende Informationsobjekt 1								
Weitere Informationsobjekte								
N - 1	Prüfsumme							
N	Stopp Byte (`16`h)							
[Primärtelegramm]								

Die Länge der Anwenderdaten bezieht sich auf Byte 4 bis inklusive N - 2. Die Werte von Byte 1 und 2 sind identisch.

Die Adresse der Verbindungsschicht ist bei symmetrischen Verbindungen optional. Wird diese verwendet, so ist sie entweder ein oder zwei Byte lang, wobei das niedrigstwertige Byte zuerst übertragen wird.

Auflistungen der Typkennungen und Übertragungsursachen können auf den zugehörigen Wiki-Seiten betrachtet werden.

Die gemeinsame Adresse der ASDU ist anlagenspezifisch und kann im Bereich 1 bis 254 bzw. 1 bis 65534 frei gewählt werden (abhängig davon, ob die Länge 1 oder 2 Byte beträgt). Eine ASDU-Adresse von 255 bzw. 65535 richtet sich an alle Stationen, die sich im selben System befinden. Hierbei antworten die einzelnen Stationen allerdings mit ihrer definierten Adresse. Falls eine gemeinsame Adresse mit einer Länge von 2 Byte verwendet werden soll, wird das niedrigstwertige Byte zuerst übertragen.

Als Adressen der Informationsobjekte können Werte im Bereich 1 bis 255, 1 bis 65535 oder 1 bis 1677215 (abhängig von der Adresslänge) verwendet werden. Die Adresse 0 ist bedeutungslos und wird nur für Telegramme verwendet, die kein Informationsobjekt betreffen. Die Übertragungsreihenfolge ist wiefolgt: niedrigstwertiges, mittleres, höchstwertiges Byte.

Unter Satz von Informationselementen sind die Daten eines Informationsobjektes zu verstehen, dh. z.B. bei einer Einzelmeldung der EIN/AUS-Zustand und die zugehörigen Qualitätsbits (blockiert, ersetzt, aktuell, usw.). Ein genauer Aufbau dieser Informationselemente kann unter Typkennungen gefunden werden.

Als Zeitmarke kann abhängig von der Typkennung des Informationsobjekts entweder CP56Time2a oder CP24Time2a verwendet werden. Hierbei muss sich innrehalb einer Datenpunktliste allerdings auf eine Zeitmarke geeinigt werden, da eine Mischung von CP56Time2a und CP24Time2a laut Norm nicht vorgesehen ist.[^3]

[^3]: DIN EN 60870-5-101, Kapitel 7.3, S. 57

Flags

`TODO: Steuerfeld Link-Layer separat erklären und Primär und Sekundärtelegramm zusammenfassen`

`TODO: Typkennungen und Übertragungsursachen auflisten`

In den oben aufgeführten Telegrammstrukturen werden folgende Flags verwendet:

Name	Beschreibung	Telegrammtyp
RES	Reserviert, immer <0>	Beide
DIR	Physikalische Übertragungsrichtung (nur bei symmetrischer Verbindung) <0> Station B → Station A (idR. Unterstation → Zentrale) <1> Station A → Station B (idR. Zentrale → Unterstation)	Beide

Name	Beschreibung	Telegrammtyp
PRM	Primärnachricht <0> Antwort auf eine empfangene Primärnachricht <1> Senden einer Primärnachricht	Beide
FCB	Telegrammfolgebit Abwechselnd <0> oder <1> für aufeinanderfolgende SEND/CONFIRM oder REQUEST/REPLY-Dienste	Primär
ACD	Zugriffsanforderung (nur bei unsymmetrischer Verbindung) <0> Keine Anforderung <1> Anforderung für Daten der Klasse 1	Sekundär
FCV	Telegrammfolgebit gültig <0> wechselnde Funktiond es FCB ist ungültig <1> wechselnde Funktiond es FCB ist gültig	Primär
DFC	Datenflusssteuerung <0> Weitere Nachrichten werden angenommen <1> Weitere Nachrichten können einen Datenüberlauf verursachen	Sekundär
SQ	Einzel / Folge <0> Datenbereich beinhaltet voneinander unabhänige Informationsobjekte, die jeweils eine Objektadresse besitzen <1> Als Adresse wird die Objektadresse des ersten Informationsobjekt verwendet. Für nachfolgende Objekte wird diese jeweils um eins erhöht.	Primär
T	<0> Keine Prüfung <1> Prüfung	Primär
P / N	<0> Powitive Bestätigung <1> Negative Bestätigung	Sekundär

Quittierung von Sollwert-Befehlen

SollwertStellbefehle (Typkennungen `48`, `49`, `50`, `61`, `62` und `63`) können laut Norm wahlweise mit einer Bestätigung (Confirmation) und Beendigung (Termination) oder nur mit einer Bestätigung (Confirmation) quittiert werden.

Wenn die optionale Beendigung (Termination) verwendet werden soll, muss dies passend in beiden Stationen eingestellt werden, d.h. der Netzbetreiber muss explizit angeben, dass die Beendigung gefordert wird.

Im Idealfall füllt der Netzbetreiber die Angaben zur Kompatibilität[^4] aus.

[^4]: DIN EN 60870-5-101, Kapitel 8, S. 157ff.

> Bayernwerk gibt in den Technischen Anschlussbedingungen an, dass die Beendigung (Termination) NICHT verwendet wird, fordert diese allerdings trotzdem. {.is-info}

Modbus Protokoll

Modbus Grundlagen

emmod20x_modbus-grundlagen.pdf

Modbus Spezifikation

modbus_application_protocol_v1_1b3.pdf

Quelle: https://modbus.org/docs/Modbus_Application_Protocol_V1_1b3.pdf

Modbus TCP

modbus_messaging_implementation_guide_v1_0b.pdf

Quelle: https://modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf

Modbus RTU

modbus_over_serial_line_v1_02.pdf

Quelle: https://modbus.org/docs/Modbus_over_serial_line_V1_02.pdf