Protocol

FA 014-02
The FLAG Protocol
July 1998

1 SCOPE

This document represents what is currently understood as IEC FLAG. For local optical access, IEC FLAG is a fully compatible sub-set of IEC 1107 (see document listed in section 2 for IEC 1107 details). This specification may need to be revised whenever IEC 1107 is revised. Parts of this specification which are not IEC 1107 compliant are marked with an asterisk '*' in the margin. These have been added to make IEC FLAG more accessible via other communications mediums.

IEC FLAG products will use only Mode C as defined in IEC 1107.

2 REFERENCE DOCUMENTS

IEC 1107 : 1996 (Second Edition)

Guide to the FLAG and IEC Meter Communications Specifications (FLAG Association Limited) Revision FAD 001-02.

3 DEFINITIONS

Hand Held Unit (HHU) : Primary station (master), portable device for transferring data to and from tariff devices, or electricity meters.

Local Data Exchange : Data exchange between one or a group of tariff devices and a hand held unit.

Tariff Devices : Fixed data collection unit, normally linked or combined with an electricity meter.

Physical Address: An address which is directly linked to physical address space in the meter.

Logical Address: An address (or identifier) which refers to a specific piece of metering data which is not (necessarily) related to the address space in the meter. The meaning of each address/identifier is application specific.

4 TRANSMISSION CHARACTERISTICS

4.1 Type of Transmission

Asynchronous serial bit (Start - Stop) transmission according to ISO 1177, half-duplex.

4.2 Transmission Speed

Initiation Baud rate	-	300
Standard Baud rates	-	300, 600, 1200, 2400, 4800, 9600
*	-	14,400

Note: The maximum spec may be limited by the communications medium

4.3 Signal Quality

To ISO 7480 (1984) Category P1 for the transmitter
Category PA for the receiver

4.4 Character Format

Character format to ISO 1177
(1 start bit, 7 data bits, 1 parity bit, 1 stop bit)

4.5 Character Code

Character code to ISO 177, international reference version (7 bit ASCII).

4.6 Character Security

With parity bit, even parity to ISO 1177.

5 DATA TRANSMISSION PROTOCOL

5.1 Overview

The data transmission protocol will use mode C operation of IEC 1107. The definitions of the messages and their contents are given in sections 5.4 and 5.5.

The following error conditions apply at all stages of communication.

5.1.1 A COMMS Error can be any one of the following :

1 Character format error (section 4.4)
2 Character security error (section 4.6)
3 Incorrect message framing characters (section 5.5 items 1, 2, 3, 4, 5, 6, 8 and 16)
4 Incorrect BCC (section 5.5 item 7)

5 A data string not bounded by open and closed brackets (section 5.6.1)

5.1.2 A DATA ERROR can be any one of the following :

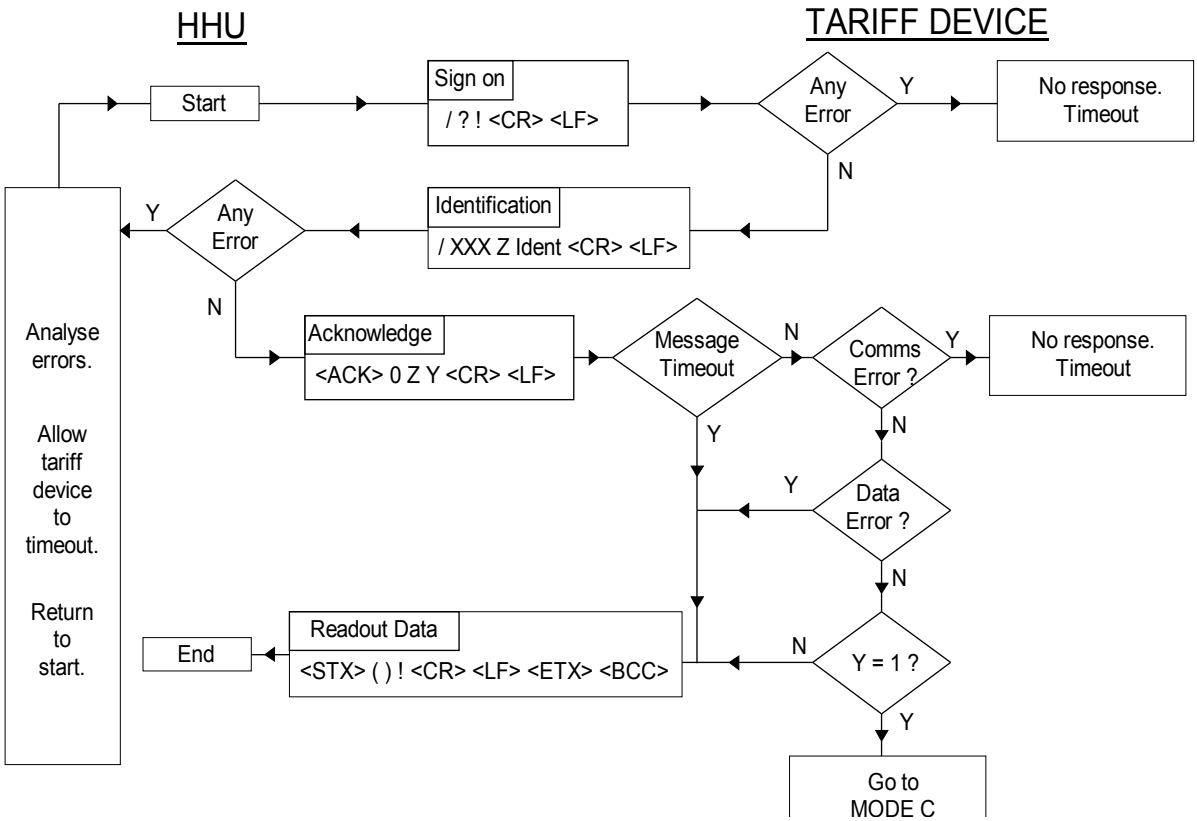
1 Invalid command message identifier (section 5.5 item 17)
2 Invalid command type identifier (section 5.5 item 18)
3 Invalid mode control character (section 5.5 item 10)
4 Invalid baud rate identification (section 5.5 item 12)
5 Invalid data identity (section 5.6.1)
6 Data identity being written to is still password protected (section 6.2)
7 Function being requested is still in time lock out
8 Incorrect protocol procedure character (section 5.5 item 9)
9 The characters in a data string are invalid (section 5.6.1)
10 Data access denied due to restrictions other than 7 and 8 above

5.1.3 A COMMS ERROR takes precedence over a DATA ERROR.

5.2 Establishing Communications

For local optical connection the opening communication exchanges take place at 300 baud. Each product must specify the baud rate to be used for any subsequent data exchange.

The flow chart for establishing communications is shown below.



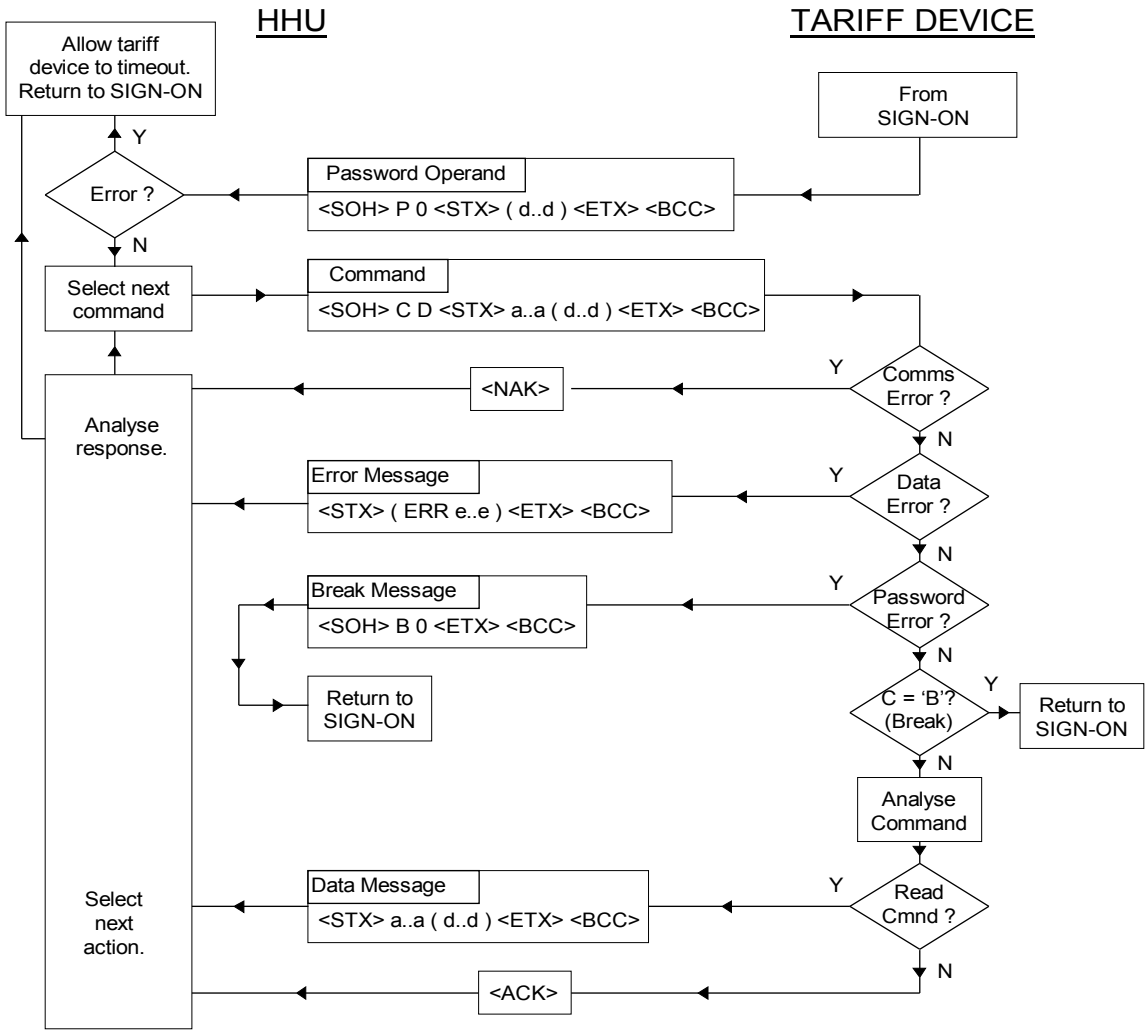
These exchanges will always take place regardless of the function being performed.

The READOUT DATA is not used, but will respond with no data content. This is included in order to comply with the IEC specification.

5.3 Data Exchange

Once communications have been established, all subsequent data exchanges will take place at the baud rate determined by Z in the ACKNOWLEDGEMENT message.

The flow chart for the data exchange is shown below.



The following data exchange function are available:

a Unprotected read. Reading of data is not subject to any security checks.

b Protected read. Reading is only permitted following security checks using a special algorithm.

c Unprotected write. Writing is only permitted following security checks using a special algorithm.

d Protected write. Writing of data is only permitted following security checks using a special algorithm and/or the presence of a physical link

The types of data being used and any restrictions, security measures, lock-outs etc. are manufacturer, product, and application specific.

The command sequence to be executed is pre-determined by a master unit

and downloaded to the HHU and may consist of a mixture of reads and writes.

The HHU analyses the responses received from the tariff device and determines whether to :

a repeat the previous command
b proceed to the next command
c send an exit command
d timeout and return to the start

The tariff device generates a pseudo-random operand for use in the security algorithm. It also analyses the commands received and determines whether to:

a transmit NAK for communication errors
b respond with the data requested
c transmit ACK for commands which require no other response. ACK is not transmitted in response to the EXIT command.
d transmit an error message for data errors
e transmit a BREAK message if the security password response is incorrect

5.4 Message Formats

The contents of each message are defined in section 5.5.

5.4.1 Request Message

/	?	Device Address (optional)	!	CR	LF
		20)			

5.4.2 Identification Message

/	X	X	X	Z	Identification	CR	LF
1)	11)	11)	11)	12)	13)	3)	3)

5.4.3 Acknowledgement to Identification Message

ACK	O	Z	Y	CR	LF
4)	9)	12)	10)	3)	3)

5.4.4 Acknowledgement Message

ACK
4)

5.4.5 Repeat-Request Message

NAK
14)

5.4.6 Command Message

SOH	C	D	STX	Data Set	ETX	BCC
15)	16)	17)	5)	18)	6)	7)

5.4.7 Data Message

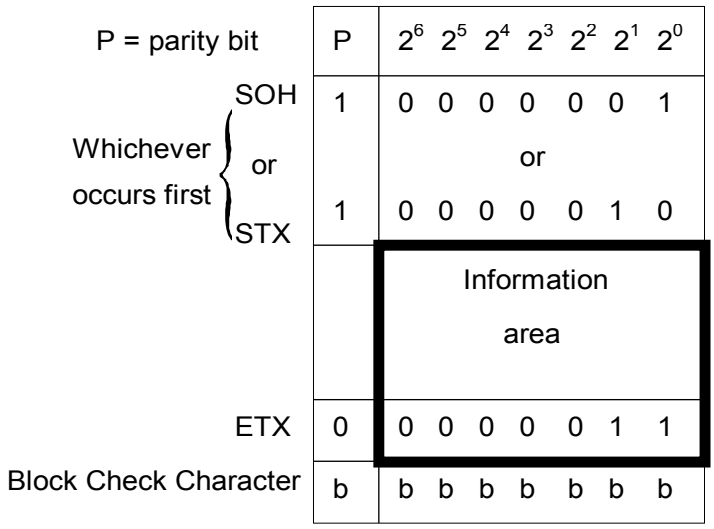
STX	Data Packet	ETX	BCC
5)	19)	6)	7)

5.5 Definitions of Message Contents

1 Start character / (forward oblique, Code 2FH)
2 End character ! (exclamation mark, Code 21H)
3 Completion character (CR, carriage return, Code 0DH, LF, Line feed, Code 0AH)
4 Acknowledge character (ACK, acknowledge, Code 06H)
5 Start of text character (STX, start of text, Code 02H)
6 End character in the block (ETX, end of text, Code 03H)
7 Block check character (BCC). This will be calculated in accordance with ISO 1155 (exclusive-OR). The calculation of the block check character commences with the first occurrence of either SOH or STX and includes all subsequent characters up to and including ETX. This will be transmitted as a single character.

It will be calculated using the seven data bits of each character and the appropriate parity bit set.

Block Check Character Calculation



The block check character is set up over the heavily outlined area.

8 Transmission request command ? (question mark, Code 3FH)

9 Control characters

0 - normal protocol procedure

10 Mode control

0 - Readout fixed data
1 - Read/program mode

11 Manufacturer's identification, this will be the three upper case letters controlled by the FLAG Association. However if the (third) character is lower case, this indicates a “20ms turn-around time” (see Section 5.8.2)

12 Baud rate identification (for Baud rate changeover). The baud rate to be used will be product dependent and must be specified in the technical specification.

Mode C Protocol

0 - 300 baud
1 - 600 baud
2 - 1200 baud
3 - 2400 baud
4 - 4800 baud
5 - 9600 baud
* 6 - 14,400 baud

For local optical links, the request message, the identification message and the acknowledgement are transmitted at the initialising rate of 300 baud. The baud rate of the data message depends on the baud rate determined by the protocol. If Z = 0 in the acknowledgement message all subsequent transmission takes place at 300 baud.

13 Identification. This will consist of up to 16 printable characters. The '/' '!' characters may not be used.

14 Repeat request character (NAK, Code 15H)

15 Start-of-header character (SOH, Code 01H)

16 Command message identifier.
(Signifies the nature of the command message)

P - Password command
W - Write command
R - Read command
B - Break (or Exit) command

Other characters are reserved for future use and are considered invalid for data error purposes.

17 Command type identifier
(Signifies the variant of the command)

Values :

a for password P command

0 data is operand for secure algorithm
1 data is operand for comparison with internally held password
2 data is result of secure algorithm
3-9 not used by IEC FLAG

b for write W command

0 reserved for future use
1 write ASCII 0 coded data
2-9 not used by IEC FLAG
c for read R command

0 reserved for future use
1 read ASCII - coded data
2-9 not used by IEC FLAG
3 read partial block ASCII-coded data
4-9 " " "

d for exit B command
0 complete sign off
1-9 not used by IEC FLAG

18 Data set (see section 5.6 for syntax diagram)

This provides the address and/or data for the command message and the following variations apply:

a The password P command

Only the data packet is present. The length of this packet is fixed and manufacturer specific.

b The write W command

This contains an address (consisting of ASCII Hex characters), which identifies the start location or identifier into which the following data string (consisting of hexadecimal characters) will commence being written.

c The read R command

This contains an address (consisting of ASCII Hex characters), which identifies the start location or identifier from which data will commence being read and a data string which identifies the amount of data to be read. Both strings are of fixed length for a given meter type.

One byte of memory may contain two BCD digits, a bit pattern of two hexadecimal characters or a mixture of both.

d The exit B command

The data set and the preceding STX are omitted.

Note that BDC digits are transmitted as ASCII characters 30 - 39H and hexadecimal characters are transmitted as ASCII characters 30 - 39H, 41 - 46H.

19 Data packet (see section 5.6 for syntax diagram).

The following variations apply :

a In response to a read command
The data packet consists of up to 128 characters bounded by

open and closed brackets. A NULL data packet is only open and closed brackets.

The contents of the data packets must be defined by each manufacturer and product and are interpreted by the HHU and/or master unit.

b An error message

The data string contains the error message. The first two characters must be ER (transmitted as 45H, 52H,) followed by a series of ASCII characters indicating the type of data character condition. This indication is manufacturer specific.

20 Device address, optional field, manufacturer-specific, 32 characters maximum. The characters can be digits (“0” - “9”), upper-case letters (“A” - “Z”) or lower case letters (“a” - “z”) or a space (“ “) characters. Upper and lower case letters and the space character are unique. Leading zeros must not be evaluated. This means that all leading zeros in the transmitted address are ignored and all leading zeros in the tariff device address are ignored (i.e. “10203” = “010203” = “000010203”). When both the transmitted address and the tariff device address contain only zeros, regardless of their respective lengths, the addresses are considered equivalent. A missing address field is considered as a general address (“ / ? ! CR LF”), the tariff device shall respond. The tariff device must be able to evaluate the complete address as sent by an external device even if the internal programmed address is shorter or longer in length.

Note: The device identification number can be used as an address to avoid reading of or writing the wrong devices.

5.6 Syntax Diagram

5.6.1 Data Set

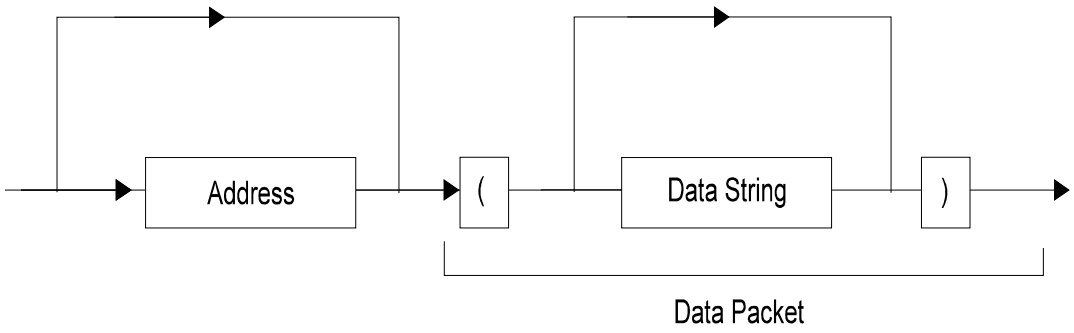
A data set contains, in general, an address and a data packet.

A data packet consists of a data string of a maximum of 128 characters, which may represent one or more values, bounded by open and closed brackets.

The address must only contain ASCII Hex characters (see section 5.5, item 19), and is of a fixed length, specific to manufacturer and product. The address may be a physical address (i.e. mapped to physical memory in the meter) or a logical address (i.e. referring to a series of application specific identifiers).

The data string must only contain hexadecimal characters (see section 5.5,

item 19).



5.6.2 Data Packet

The data packet is a subset of the data set in which the address may be omitted. All other characteristics of the data packet are identical to that in a data set.

5.6.3 Partial Block

Partial block is a reading mode using the R3 command which may be used to retrieve quantities of data greater than 128 bytes with one command. This overcomes the packet size limit in FLAG. Note that Partial Block mode may be used for packets smaller than 128 bytes.

The address and “amount of data” strings are of fixed length and may relate to physical or logical addressing.

Data is returned as a series of Data Sets as defined in 5.6.1 as follows

To Meter <SOH> R3 <STX> Address Amount <ETX> <BCC>

Response: <STX> Data Set <EOT> <BCC>

To Meter: <ACK>

Response: <STX> Data Set <EOT> <BCC>

To Meter: <ACK>

Last Response: <STX> Data Set <ETX> <BCC>

A <NAK> to the meter causes the same block to be repeated. Any other character (including the start of a new command) escapes from partial block mode.

An address is returned with each block from the meter. The value of this address is application specific. If physical addressing is used then the return address will increment in the same way as it would if the packets were addressed individually using R1. This is also the preferred method for logical addressing; that the return address is the same as what it would be if the packet were addressed individually.

For some applications it is not possible or relevant to allow individual addressing of each packet. In this case either the same address as requested can be returned for each packet or the address can be incremented by a given value for each packet.

It is very important that addresses returned by partial block are not the same as other logical addresses in the meter if the meaning is different ie. there must be no ambiguity between addresses, whatever reading/writing mechanism is used.

5.7 End of Transmission

The data exchange is terminated by either:

a receipt of the exit command
b timeout

The exit command does not require any acknowledgement response.

5.8 Reaction and Monitoring Times

5.8.1 Inter-Character Timeout

The maximum time between two characters in any message is 1500 msec.

After this time the receiving device (HHU or tariff device) will timeout and take the appropriate action.

5.8.2 Turn-around Time

Upon receipt of a message the device (HHU or tariff device) will send a response for a minimum of 200 msec. However if a special indication has been given at sign-on (Section 5.5 Item 11) this time will be 20ms.

5.8.3 Inter-message Timeout

The tariff device will timeout if it has not started to receive a message from the HHU within 60 sec. (Note that circumstances may occasionally dictate that the tariff device will timeout earlier).

6 SECURITY

The following security checks are carried out :

6.1 Character Check

Each character is checked for correct start, stop and priority bits and also for frame errors.

6.2 Secure Algorithm

Both the HHU and the tariff device will contain a special algorithm which can encrypt data.

The security algorithm is the subject of a separate specification.

During the initial data exchange (see section 5.3) the tariff device will transmit an operand using the PO command. This will be a pseudo-random number of fixed size hexadecimal characters, dependent on product and manufacturer.

Both the tariff device and HHU will encrypt this number in a manner defined by the security algorithm.

The HHU will transmit its results (fixed size) to the tariff device using the P2 command.

The tariff device will then compare the HHU result with its own result and if the two results are the same then the tariff device will permit increased access privilege.

During any communications session access privileges will revert to default again after :

a Receipt of an EXIT message from the HHU
b An inter-message timeout

The HHU need not send the P2 command immediately after the P0 command but must do so before requiring increased access privilege.

6.3 Password

Some access privilege may be protected by a password in addition to the security algorithm.

This password (fixed length hexadecimal characters) is transmitted as part of a P1 command.

* 7. Modem-Friendly FLAG

FLAG access is enabled remotely via telephone or radio pads by maintaining a fixed baud-rate. Instead of sign-on at 300 baud, the in-station signs on at the manufacturer and product specific baud-rate.

* 8. Water FLAG

FLAG access is enabled via 2-wire or 3-wire inductive pads by maintaining a fixed baud-rate in the same way as Modem-Friendly FLAG. This technology is used primarily with water meters.

R:PILOTDOC\FLAG\GENFLAG.DOC