

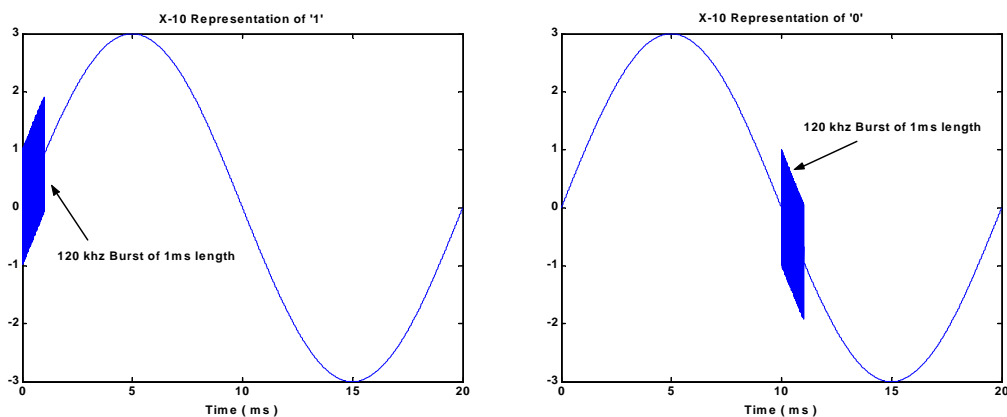
APPENDIX I

X10 Protocol

X-10 Protocol

X-10 system was the first PLC that has been implemented commercially. X-10 was requested by the BSR (British sound Reproduction) to build an electronic, wireless method of remote control for its equipments. This protocol is characterized by the following features:

- It has the advantage of using the power line voltage as a global synchronization signal to simplify the design and help overcoming the line problems. So the key element and the heart of any X-10 device is " zero crossing " detector that globally synchronizes all the devices connected to the same mains. The transmitter waits until it detects the zero crossing point to put its burst and the receiver opens a window around each zero crossing to detect if burst exists or not. So this window is opened 100 times per second for a line frequency of 50 Hz, and 120 times for 60 Hz power networks.
- The use of two zero crossing locations to represent each data bit so the binary 1 is represented by the existence of a burst followed by an absence, and the binary 0 is represented by the absence of a burst followed by a burst existence (similar to manchester coded data), The following figures shows the relative location of the bursts to the power line waveform.

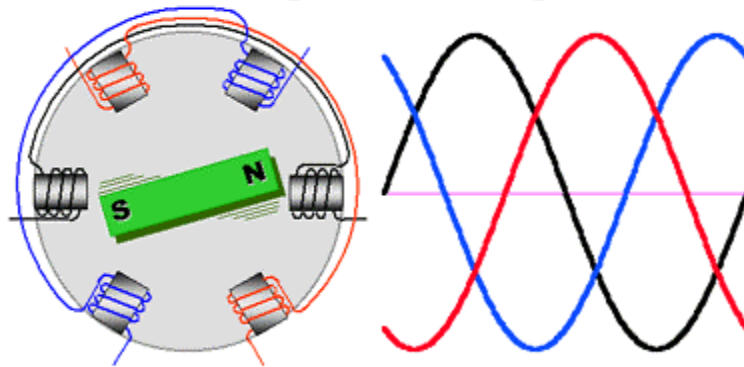


X-10 Burst Location Relative to the Power Signal

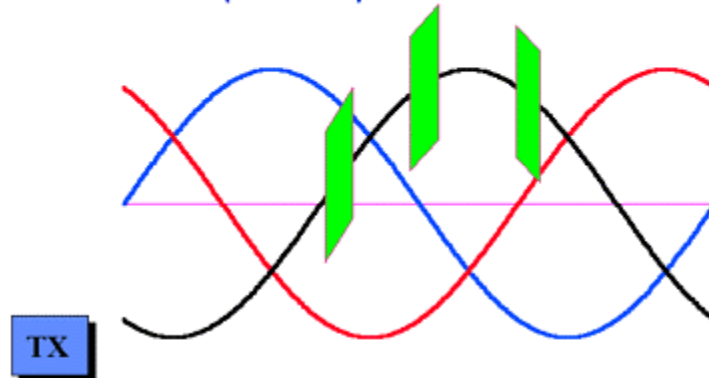
- The burst frequency is chosen to be 120 kHz. This band as shown previously has a relatively low Noise Power Spectral Density profile than the lower frequency bands, although it is still considered as a low frequency. This justifies that its radiation from the wire lines and the reflection effects for typical network lengths of 1 km can be neglected. The burst duration remains for only 1 ms so the average transmitted power is reduced.
- As a general rule in communication systems, data is always sent as packets (Frames), and the receiver must have a way to determine the frame start and end. This process may be called frame synchronization. In X-10, this is accomplished by leaving at least 6 clear zero crossings, then a start code of successive 3 bursts followed by an absence, at the beginning of each frame to indicate its start. Once the Start Code has been transmitted , the first half of the command byte is sent.

- X-10 designers decided to use some form of repetition code, that is to repeat each data frame twice to increase the reliability (Probability to receive a correct packet).
- The power is actually distributed in 3-phase configuration with 120 degrees phase shift among them, and hence if the transmitter and receiver are not connected to the same phase their zero crossing detectors will not be clocked together but will be separated by $\pm 10/3$ ms (for 50 Hz), To overcome this problem each transmitter actually send three bursts each half line cycle instead of one burst just after its zero crossing, This requires an auxiliary timing circuit to determine the locations of the other two bursts The following figure shows the locations of the burst relative to the mains signals .

All Electric Utilities generate electric power in 3 phases.



So instead of sending only one pulse all X-10 transmitters "should" send 3 pulses per half sine wave.



As shown the X-10 protocol is designed primarily for control applications and its raw data rate is very low (50 or 60 bit/s) and its throughput is further reduced by the framing and repetition overheads. This led to several modifications and extinctions to be added to the X-10 to improve its performance and to make it suitable for data transmission. Another disadvantage is its use of the On-Off Keying modulation technique which is sensitive to amplitude variation and impulsive noise types, and so it is expected to be more susceptible to link failure; due to impulsive noise or the periodic line impedance changes.

CEBus Protocol

CEBus PROTOCOL

CEBus is a standard proposed by the Electronic Industries Association

CEBus is an open standard, which provides separate physical layer specification documents for communication on power lines and other media. Data packets are transmitted by the transceiver at about 10 Kilobits per second (Kbps), employing spread spectrum technology. To avoid data collisions, it uses a Carrier Sense Multiple Access/ Collision Detection and Resolution (CSMA/ CDCR). CEBus is an open architecture which explains how to make products communicate through the following media:

- Power line Wires.
- Low voltage twisted pairs,
- Coax, Infrared,
- RF,
- Fiber optics

CEBus based products consist of two components

- A transceiver which implements spread spectrum technology
- A controller to run the protocol

The CEBus standard includes commands such as volume up, fast forward, rewind, pause, skip, and temperature up or down 1 degree. The CEBus Power line Carrier uses Spread Spectrum technology. The CEBus Power line Carrier spreads its signal over a range from 100 Hz to 400 Hz during each bit in the packet transmitted. Instead of frequency hopping or direct sequence spreading. Due to the high noise level of power line channels, data should be transmitted via short frames. The requirement for short frames is met by a physical layer spread spectrum technology. Each frame is transmitted on a raw data rate of 135 kbps. Using forward error correction (FEC) and automatic repeat request (ARQ) transfers data with an effective through put of 19.2 kbps at an error rate of 10^{-9} . CEBus protocol uses a Carrier Sense Multiple Access/Collision Detection and Resolution (CSMA/CDCR) protocol to avoid data collisions

CEBus & OSI Model

◆ Application Layer

- Specifies how service is perceived or experienced by the user.
- Responsible for managing the communication access.

◆ Presentation Layer (Not used by EIA – 600)

- Specifies how the appearance of the service is generated at the user terminal from the telecommunications signal received.
- Provides the services that allow the user to interpret the meaning of the information being transferred.

◆ Session Layer (Not used by EIA – 600)

- Specifies how a specific interaction is setup between user and computer.
- Supports the dialog between cooperating users, binding and unbinding them into and out of a communicating relationship.

◆ Transport Layer (Not used by EIA – 600)

- Defines protocol of very general applicability; provides flow control and error control.
- Provides end – to – end control and information/status interchange with the level of reliability of service needed by the user.

◆ Network Layer

- Sets basic standards for formatting of information once link is established.
- Provides the switching and routing functions needed to establish, maintain and terminate connections and data transfer between user

◆ Physical Layer

- Provides the characteristics to activate, maintain and deactivate the physical links passing the stream of communications symbols.
- Exchanges symbols with the data link layer, encoding and decoding the symbols to and from the medium states.

◆ Data Link Layer

- Makes a transmission channel appear to the Network Layer as an open, and error – free channel.
- Provides the means for establishing and maintaining individual data links.
- Provides for the transfer of information over the physical link with the required synchronization, error control and flow control functions.
- Provides for the encapsulation and de – encapsulation of the message exchanged between itself and the network layer.
- Exchanges symbols and medium status between itself and the physical layer.

CEBus & OSI Model (Data Link)

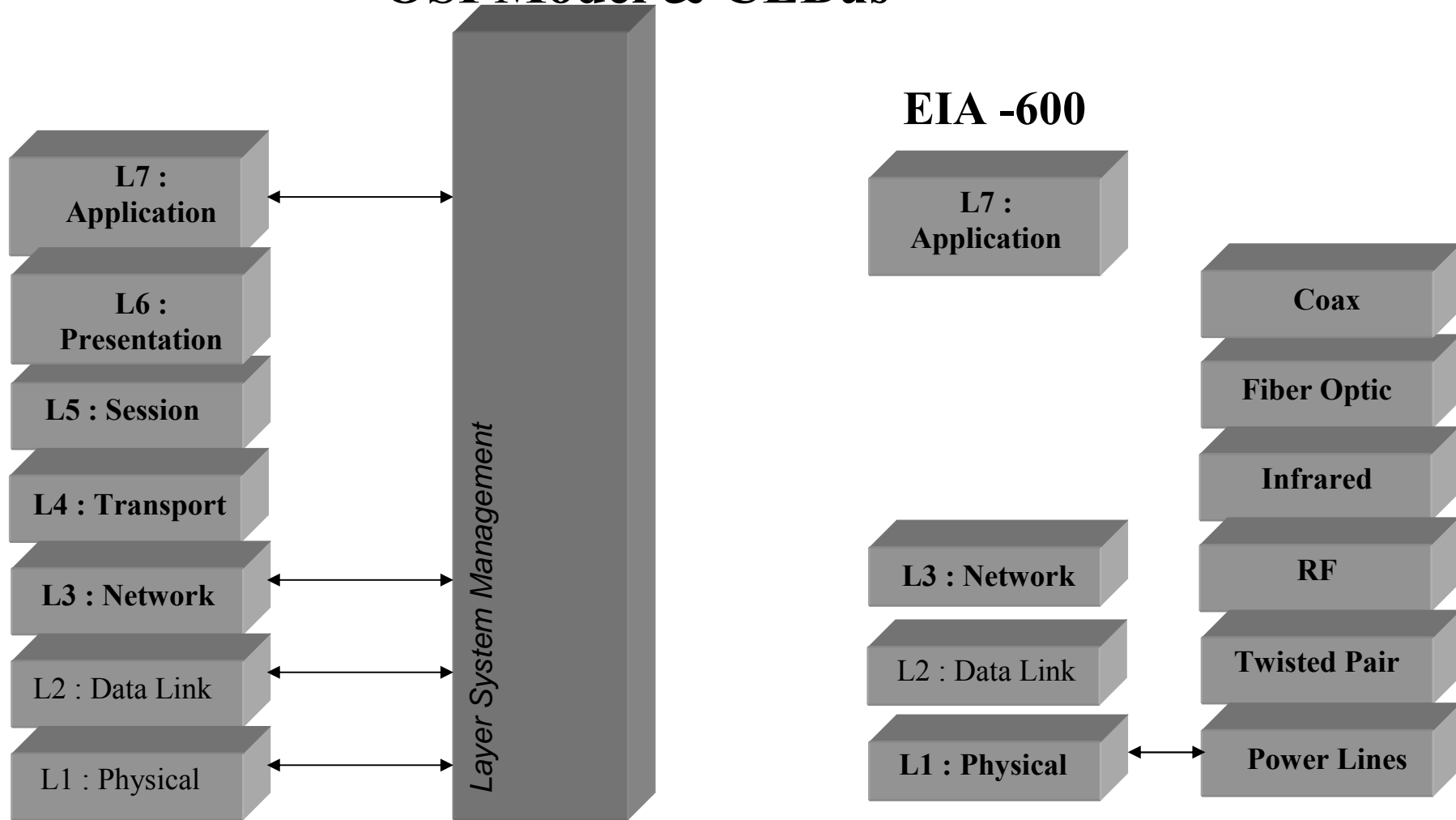
- ◆ Data from the Network Layer is incorporated into a frame within the Data Link Layer
 - The “ frame ” is the form of data which is generated within the Data Link Layer.
- ◆ The contents of the frame are relayed to the Physical Layer for transmission across the channel.
- ◆ Data received from the channel are passed from the Physical Layer to the Data Link Layer to form the received frame
- ◆ Data Link Layer is divided into two sub layers of MAC and LLC
 - Performs the functions of transmitting and receiving Protocol Data Units.

- ◆ The Medium Access Control (LLC) Sub layer
 - Provides the interface to the Network Layer.
 - Administers the transmission and reception of Protocol Data Units.

| OSI Layer | Purpose | Features | Benefits |
|------------------|---|--|--|
| Physical | Electrical Interconnection | <ul style="list-style-type: none"> • Support for various media | <ul style="list-style-type: none"> • Installation • Performance • Reliability |
| Link | Media Access and Framing | <ul style="list-style-type: none"> • Democratic media access • Scheme and priority • Large Packet size | <ul style="list-style-type: none"> • Low latency for critical nodes, uniformly democratic access for all other nodes • Support for discrete, anabas, as well as configuration and diagnostic data with out fragmentation and performance impact |
| Network | Destination Addressing | <ul style="list-style-type: none"> • Support for routers | <ul style="list-style-type: none"> • Size and interconnectivity-support for large networks • Reliability-traffic flattening, seamen ting network into functional clusters, while allowing transparent communication across clusters when needed • Installation ease and reliability • Reliability-oratting additional path between communication nodes |
| Transport | End-To-End Reliability | <ul style="list-style-type: none"> • Unacknowledged service with and without repeat. • Acknowledged service. • Multi cast service with and without acknowledgment from each node and the ability to re-transmit selectively. • Duplicate detection | <ul style="list-style-type: none"> • Optimal communication to a large number of devices, or devices unable to acknowledge. Maintains network reliability in these conditions • Reliable delivery • Performance and reliability |
| Session | Remote Actions | <ul style="list-style-type: none"> • Request/Response | <ul style="list-style-type: none"> • Reliability-to ensure acknowledgement of addition • Reliability-to ensure sender |
| Presentation | Data Interpretation | <ul style="list-style-type: none"> • Standard Data type | <ul style="list-style-type: none"> • Ability to exchange and interpret standard data regardless of applications |
| Application | Sensor/Actuator Appellation compatibility | <ul style="list-style-type: none"> • High level standard object interface definitions • Standard configuration properties | <ul style="list-style-type: none"> • Representation of any sensor, actuator, or controller interface as aggregations of high level objects • Interpret ability with standard sensor interface |

OSI/(CEBus)Model

OSI Model & CEBus



LON Protocol

LON Protocol

Lon works is a local operating network (LON) which makes possible to create a network of intelligent devices that sense, process, communicate, and control a multitude of applications ranging from hand-held instruments to large process control system.

Echelon's implementation of LON technology is available. Echelon has arranged for multiple sourcing of the key elements of Lon works, making it possible to manufacture Lon works compatible products.

The major elements of LONWORKS are:

- LonTalk protocol
- Neuron chips
- LONWORKS transceivers
- Network management and applications software

The LonTalk Protocol

The LonTalk protocol is a collection of services that supports reliable communication among nodes and makes efficient use of the communications medium. Conformance with the LonTalk protocol provides three primary benefits:

- Insulates the developer of LONWORKS-compatible products from the detailed design of reliably moving information throughout a local operating network.
- Provides installers of LONWORKS networks enormous flexibility in selecting and configuring nodes to meet a particular application.
- Ensures the predictability of network behavior under all conditions.

The LonTalk protocol has been designed for applications involving sense, monitor, control and identification functions. This section describes the key features of the LonTalk protocol:

1) Reliability -

The LonTalk protocol supports end-to-end acknowledgments with automatic retries. When this service is used, a node sending a message will expect an acknowledgment from all intended receivers and will automatically retransmit the message unless all intended receivers respond. Alternatively, an IEC developed "heartbeat" timer technique, in which nodes notify the network of their presence at predetermined intervals, assuring reliable communication. Absence of an acknowledgment, or a "heartbeat", can be used to trigger an alarm condition.

2) Variety of communications media -

The LonTalk protocol supports communications on a variety of wired and wireless media, including:

- Twisted pair
- Power line (powered or unpowered)
- Radio frequency
- Coaxial cabling
- Fiber optics

3) Response time –

The LonTalk protocol uses a proprietary collision prediction algorithm that permits a channel to carry its maximum capacity, rather than have its throughput degrade due to excess collisions (as, for example, happens with Ethernet). In addition, collision detection is optionally supported on certain media, including twisted-pair; this further enhances response time in cases where collisions do occur. At the fastest LonTalk data rate of 1.25 million bits/second, the LonTalk protocol supports over 500 transactions per second. For applications that must limit the maximum delay incurred by nodes with high-priority messages, the LonTalk protocol offers an optional priority feature. Using priority, the highest priority node is guaranteed access to the medium as soon as transmission of any message in progress is completed.

4) Low product cost –

Many LON nodes are small, simple devices: light switches, temperature sensors, on-off controls, etc. Such devices cannot tolerate substantial increases in size and cost. The LonTalk protocol has been designed for implementation using a single, low-cost, VLSI chip that can be economically and practically incorporated in these low-cost devices.

5) Interoperability –

A major goal of the LonTalk protocol is to give developers, from the same or different companies, the ability to design products that will be able to interact with one another. The LonTalk protocol provides a common applications framework that ensures interoperability using powerful concepts called network variables and Standard Network Variable Types (SNVTs).

Standard Network Variable Types

The use of Standard Network Variable Types (SNVTs, pronounced "snivets") contributes to the interoperability of LONWORKS products from different manufacturers. Echelon maintains a growing list of over 100 SNVTs for nearly all physical measurement types including the type of variable such as integer or floating point. For example, a SNVT for continuous level is defined as SNVT_lev_contin.

If all manufacturers use this variable type in their application when a network variable for continuous level is defined, any device reading a continuous level can communicate with other devices on the network that may be using the variable as a sensor output to initiate an actuator. As long as a network input variable and a network output variable are defined with the same SNVT when the developer creates the applications, they can be connected together on the network through a process called binding.

Binding is defined at the time of installation using the ICELAN Windows based graphical installation tool. When you install a node, you specify which network variables are to be connected between nodes. This is easily done by highlighting the output network variable on one node and the input network variable on the node or nodes to be connected. ICELAN makes this easy since the important information in each node is presented graphically through a standard Windows interface. Only

network variables of the same SNVT type can be bound together. In other words, a temperature type could not be bound to a pressure type.

LonTalk Protocol Services

The LonTalk protocol design follows the International Standards Organization's Reference Model for Open Systems Interconnection (ISO OSI), which prescribes the structure for open communications protocols. LONWORKS is unique in that it is the only control protocol that implements all seven layers of this model. The LonTalk protocol supports many different types of communications services so that a system can be tailored to meet your requirements. All of these services are selected at the time of node installation with IEC's ICELAN network management software, based on Peak Components. The various services below are briefly described:

- Unacknowledged - Unacknowledged is the most commonly used message service. In this mode, system nodes send out messages on the network whenever the local application determines it appropriate. The node that sent the message does not listen for responses from receiving nodes. This service provides the widest network bandwidth.
- Unacknowledged/Repeated - This service is similar to acknowledged service, but does not receive confirmation of receipt from the receiver. Instead, the message is sent a number of times determined at the time of node installation on a network variable basis.
- Acknowledged - Acknowledged service is used when it is critical that a message be received at its intended destination. The retry time-out is set at the time of installation when the node is installed and when SNVTs are bound between nodes. The network management software (for example, ICELAN) sets all of the timers in the Neuron Chip according to the network design. This service will reduce available bandwidth on the network.
- Priority - You can allocate priority time slots on a channel to improve the response time of critical packets. This ensures that one and only one node is assigned to a particular priority slot. This service reduces communication bandwidth and should be used sparingly.

LonTalk Addressing

To simplify message routing, the LonTalk protocol defines a hierarchical form of addressing using domain, subnet, and node addresses. This form of addressing can be used to address the entire domain, an individual subnet, or an individual node. In addition, multiple dispersed nodes can be addressed using domain and group addresses.

A channel is the physical transport medium for the LonTalk messages. Every node is physically connected to a channel. The communications medium can be twisted pair, power line, radio frequency, coax or fiber optic media.

A domain is a logical collection of nodes on one or more channels. Communications can only take place among nodes in a common domain; therefore, a domain forms a virtual network. Multiple domains can occupy the same channel, so domains may be used to prevent interference between nodes in different networks. The user can choose domains for nodes at the time of installation with ICELAN. For example, two adjacent buildings using nodes with RF transceivers on the same frequency would be on the same channel, but the installer could configure the nodes in each building to be in different domains to prevent interference between the applications. The user assigns the domain ID at the time of installation.

A subnet is a logical collection of up to 127 nodes within a domain. Up to 255 subnets can be defined within a single domain. All nodes in a subnet must be on the same channel, or on channels connected with bridges. Subnets cannot cross routers. If a node is configured to belong to two domains, it must be assigned to a subnet within each of the domains. All nodes within a domain are typically configured in the same subnet except in the following cases: They are located on different channels with intervening routers. Since subnets cannot cross routers, the nodes must be on different subnets. Configuring the nodes in the same subnet would exceed the maximum number (127) of nodes allowed in a subnet. Multiple subnets may be configured on a set of channels connected by bridges to increase the capacity above 127 nodes. For example, a set of channels connected by bridges with two subnets may have up to 254 nodes.

Every node within a subnet is assigned a unique node number within the subnet.

Groups can also be assigned within a domain. A group is a logical collection of nodes within a domain, but the members do not have to share the same channel as with a subnet. A node can be a member of up to 15 groups. Groups are an efficient way to use network bandwidth for one to many network variable and message tag connections. A single domain can contain up to 256 groups.

Each node has a 48-bit unique ID assigned during manufacture. This ID is typically used as a network address only during installation and configuration. It may also be read and used by application programs as a unique product serial number. With 281,474,976,710,656 possible IDs, every node in a LONWORKS network is sure to have a unique address.

The Neuron Chip

The Neuron Chip is the heart of the LONWORKS technology. LONWORKS nodes usually contain a Neuron Chip to process all LonTalk protocol messages, sense inputs and manipulate outputs, implement application-specific functions and store installation-specific parameters. The integral applications processor means that low cost nodes can be designed with as little as one VLSI device. The customer benefits from this technology because manufacturers are integrating it into their sensors and actuators to provide a wide variety of devices for use in networked applications. A stream of new products from a diverse group of manufacturers is now in development to take advantage of LONWORKS technology for present and future applications.

Each Neuron chip has three resident 8-bit processors: two processors dedicated to LonTalk protocol processing, and a third dedicated to the node's application program. Neuron chips are manufactured under license by both Motorola and Toshiba, two of the four largest semiconductor manufacturers in the world.

Neuron chips are programmed in Neuron C, which extends ANSI Standard C to support an object-oriented approach to developing distributed applications. Neuron C provides direct support for LONWORKS objects such as network variables and SNVTs. The language also provides a new statement called the "when" statement that is used to schedule execution of user tasks based on predefined and user-

defined events. In addition, Neuron C provides a syntax for declaring a wide range of I/O objects that are supported by the Neuron Chip application I/O hardware.

All services of Neuron C leverage the run-time support provided by the Neuron firmware. This firmware contains:

- The LonTalk protocol communications software, including network management functions and network variable processing
- An event driven scheduler
- Run-time support for applications I/O objects
- Arithmetic, logical, conversion and other application routine libraries

Compatibility with the OSI Reference Model

The ISO (International Organization for Standardization) developed a standard defining a model for general purpose data communications architecture.

Each of the seven layers of this model is implemented in the LonTalk protocol. Each has a purpose to make the technology robust and provide room to grow the network. The most important benefit of this approach is that each layer performs services for the next higher layer so that details are hidden to the higher layer. Changes can be made in a layer without changing any of the other layers.

Layer #1: Network Physical Layer - Electrical Interconnect

This layer addresses specifics of wiring and connections. The specification of the 78 kbps twisted pair media with 2000 meter range, 64 nodes per network segment, and network isolation characteristics is an example of one physical layer type of media. LONWORKS technology provides many different communications media options including 1.25 Mbps twisted pair, power line, fiber optic, and RF transceivers. This provides you with a wide range of choices for communicating your data.

Layer #2: Data Link Layer - Media Access and Framing

This layer defines the rules of access to the physical layer. For example, this corresponds to the dial tone on the telephone network. Services provided by this layer include:

- Error Detection (CRC)
- Flexible allocation of bandwidth
- Priority access mechanisms
- Graceful behavior under overload (p-persistent CSMA)
- Message collision avoidance
- Optional collision resolution, collision detection

Layer #3: Network Layer - Destination Addressing

This layer specifies the destination of a message on the network. This corresponds to the area and long distance codes on the telephone network. Services provided by this layer include:

- Contains the node address information
- Provides for routing of messages to segment and control network bandwidth usage

This layer provides many important services such as determining which nodes on the network receive various messages. The ability to provide routers to segment the traffic and communicate between different physical media is part of this service.

Layer #4: Transport Layer - End to End Reliability

This layer establishes the type of services required for the node messages depending on the level of reliability required by the application. The services provided are:

- Broadcast addressing
- Unicast addressing
- Multicast addressing
- Repeated service
- Acknowledged service
- Unacknowledged service
- Duplicate packet detection

- Authentication

The level of service required by the application is established when each node is installed on the network. This is all handled by a network management installation tool, such as ICELAN, and the node's design.

Layer #5: Session Layer - Remote Actions

This layer provides the communications to request action from another node. Examples of the services include:

- Acknowledgment of received message
- Application to application communication
- Retry if the correct response is not received from the remote node
- Request to a destination group and receive individual responses from the group
- Request - response message authentication

Layer #6: Presentation Layer - Data Interpretation

This layer provides translation of the network data for the application. Examples of services provided in this layer include:

- Input, output, and configuration variables for the node
- Standard data representations for physical quantities
- Network variable description

The standard data representations are important to assure interoperability between products from different manufacturers.

Layer #7 Application Layer-Application Compatibility

This layer includes services to simplify development of application programs to interface to specific sensors, actuators, and external microprocessors. The services provided in this layer include the following:

- Memory storage for application program

- Built-in real-time operating system
- Device drivers for the I/O hardware on the Neuron Chip
- Standard Network Variable Types (SNVTs)

EOIP Protocol

EOIP Protocol

EOIP Protocol for Data Transmission over the Power Lines

General

This document describes EOIP protocol specification for both the local and remote systems. EOIP protocol for local system is used for exchanging data between tariff device and Hand Held Unit HHU while in the remote system EOIP protocol is used for data exchange between tariff devices and a receiver module.

Compiling Circuit:

Capture Isolated Type

Modulation Scheme and Signal:

Base Band. Direct sequence spread spectrum, chip rate 100 k chip/second. Number of chips per data Bit: 128.

Antipodal signaling (the waveform representing the "Zero" bit is the negative inversion of the waveform representing the "One" bit.)

Band width and emission limits:

Complying with European standard CENELEC A-Band 9KHz. To 95KHz and EN 50065-1,1995

- Single phase line to neutral transmission

1- Protocol: Pure Aloha with transmission times driven by the randomness of the customer consumption.

Packet Construction:

| | | | |
|-----------------------------|--------------|------|-----|
| Acquisition period 1024 bit | Frame 15 bit | Data | CRC |
|-----------------------------|--------------|------|-----|

- Acquisition period to synchronize the receiver (Sliding Correlator Receiver).

- Data is marked using 15 bit frame. The pseudo random generation of selected output from taps order (1,3)
- Data protection and error control coding.
 - The packet is tailed by a CRC (Cyclic Redundancy check) code one of the (CCITT polynomials)
 - The message body consists of the data and CRC fields can be repeated odd number of times. The receiver will then take the majority after using any of the decision techniques Hard decision, or soft decision,

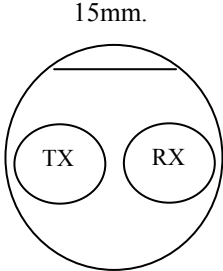
Power line networks are designed primarily to carry 50Hz frequency. Power line network exhibits same bad characteristics from the communication point of view, and so it's considered as a host media for communication signals. The Power line also suffers from severe attenuation that can reach up to 80 dB/Km. Noise types in power lines include:

- 1- Wide Band 1/f noise.
- 2- Impulsive Noise.
- 3- Narrow band interferences.
- 4- Harmonic related Noise.

EOIP Protocol for Data Exchange with Meter

Physical properties

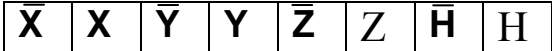
- The distance between the TX- led and the Receiver is: 15 mm. \pm 1mm.
- LED current is 50 mA.



Optical Characteristics

EOIP Protocol for Data Exchange with Meter

- The optical port is used to insure electrical isolation and for ease of operation.
- Wave length: between 800 n m to 1000 n m
- Transmitter
 - Modulation ON – OFF keying 50% \pm 10% duty cycle
 - Carrier frequency 38 KHz \pm 0.5 KHz.
- Manchester coded bytes (every byte carries on 4 bits repeated twice)



Represents the data **XYZH** least first transmission

No Carrier: On condition logic '1'
 Carrier exists: Off condition logic '0'

- Environment lighting condition:
 The optical path is not be affected by surrounding light (light composition comparable with daylight, including fluorescent light)

Transmission Speed

The baud rate used is fixed at 9600 bps

Character Transmission

- Type of transmission:
Asynchronous serial bit (start - stop) transmission half- duplex
- Transmission Speed:
9600 bps
- Character format
(1 start bit, 8 data bits, No parity, 1 stop bit)

The time between the reception of a transmitted character and transmission of the answered character $\{1\text{ms} \leq t \leq 100\text{ms}\}$

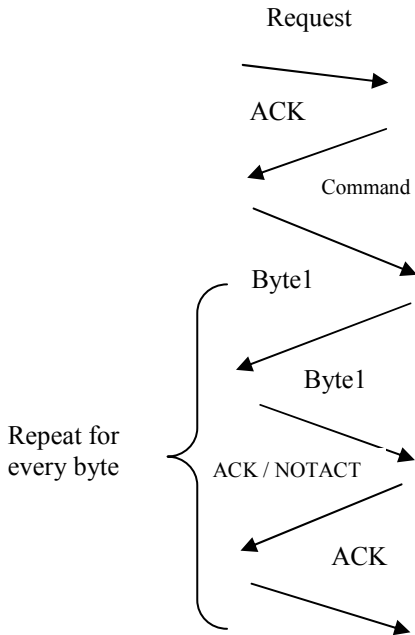
Data Transmission Protocol

- Data packets are transferred into Manchester code.
Two main packets are used:
 - Reading packet
Reading packet consists of 4 bytes in BCD format.
 - Identification packet
Identification packet consists of 6 bytes.

Read

HHU

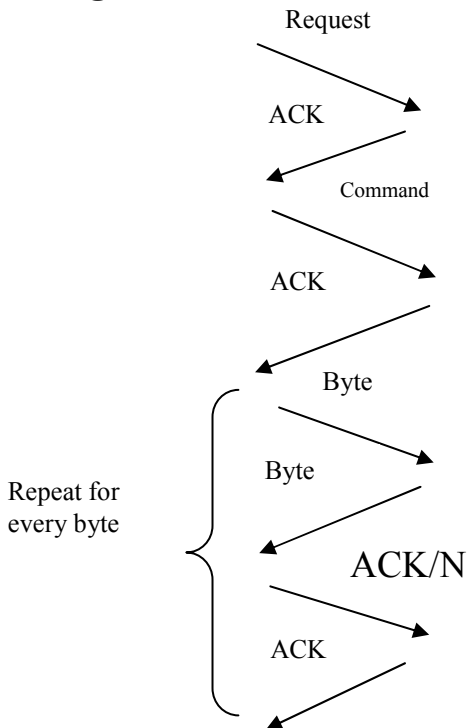
Meter



Write

HHU

Meter



IEC1107 Protocol

IEC 1107 PROTOCOL DATA EXCHANGE FOR METER READING TARIFF AND LOAD CONTROL- DIRECT LOCAL DATA EXCHANGE

Introduction

This international Standard describes a method for direct local data exchange, where the Tariff device is read and programmed using a hand held unit directly connected to the meter.

1-General

1.1 Scope and Object

This international standard presents hardware and protocol specifications for local Systems, while specifications for a remote system falls within the scope of another document. This standard deals with direct local system. In which the hand-held unit (HHU) is connected to one tariff device only at a time. Connection can be permanent or disconnectable through an electrical or optical coupling. The protocol took as its basis the basic reference model for communication between open systems (OSI).

2-Physical Properties

2.1 Electrical Interface

- a) Type of signal: 20ma current loop (ISO 7498 potential separation)
- b) Power Supply: On the tariff device side the interface is passive (ISO 7498). The HHU supplies the necessary power.
- c) Connection: Via terminals or suitable connectors.

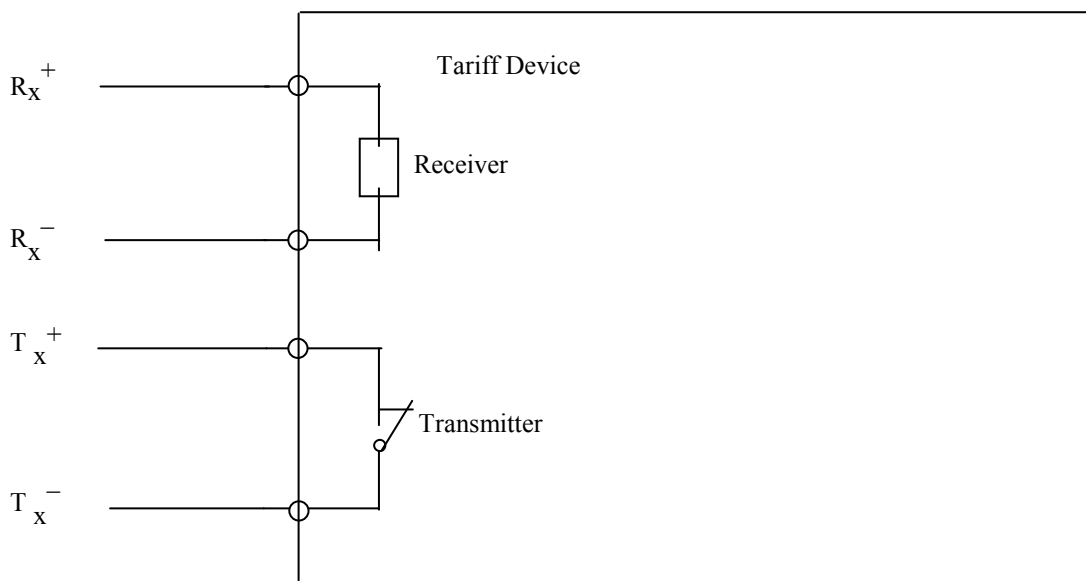


Fig 1)-a) Circuit arrangement in 4-wire configuration

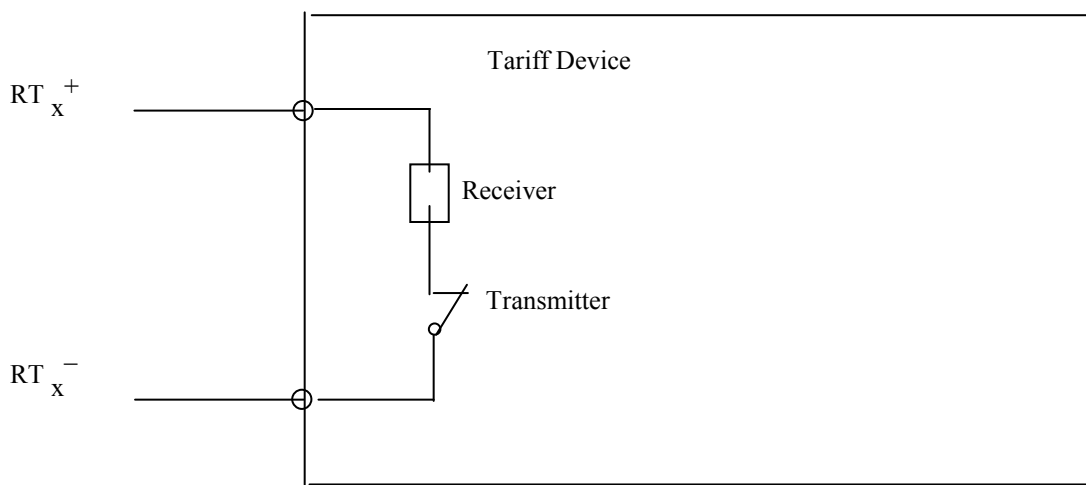
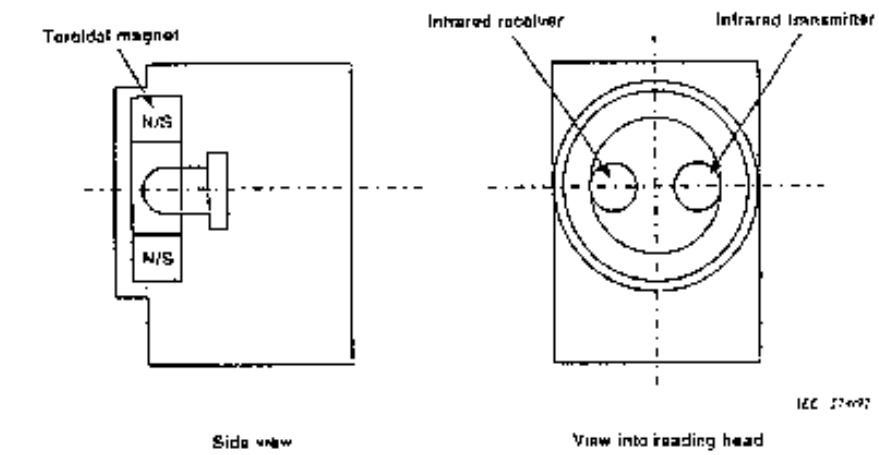


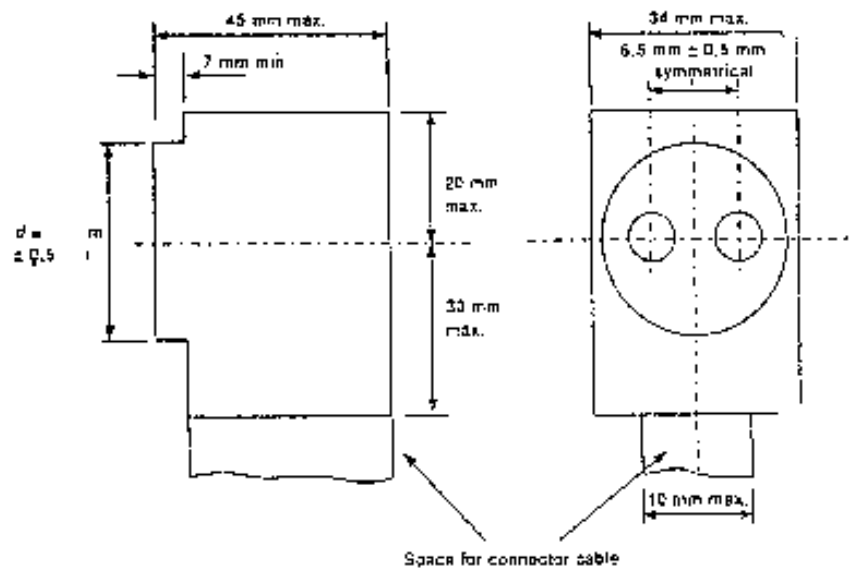
Fig 1)-b) Circuit arrangement in 2-wire configuration

3.2 Optical interface

3.2.1. Construction of the reading head



a) Arrangement of components

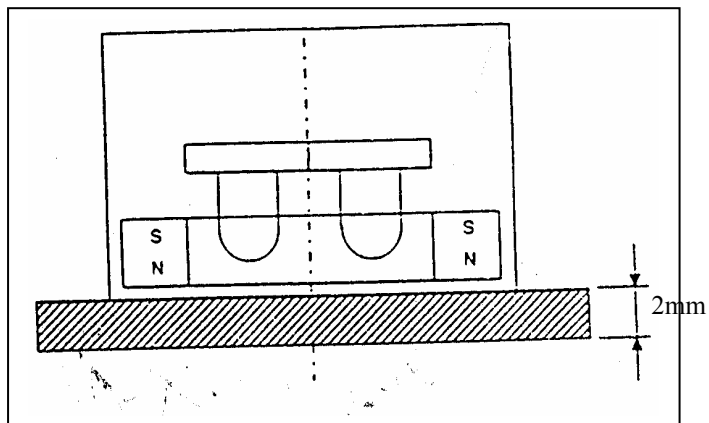


b) Dimensions

Figure 2 - Construction of the reading head

3.2.2 Characteristic Data of the Magnet Cohesion Force

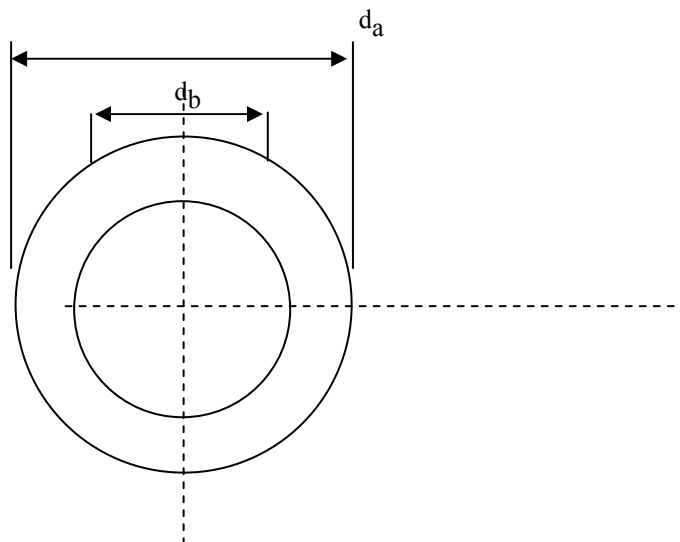
The cohesion F is defined as the perpendicular pulling force as measured when the magnet is positioned on a bright 2 mm thick deep-drawing/steel plate St ". 2, minus the weight of the reading head itself.



Cohesion force $F \geq 5 \text{ N}$ in contact with the steel plate.

$F > 1,5 \text{ N}$ at a distance 012 mm (rom the sieel plat

a) Cohesion force



Optical Characteristics Wavelength

The wavelength of the radiated signal in both directions is between 800 nm and 1000 nm (infrared)

Transmitter

The transmitter in the tariff device as in the reading head generates a signal with a radiation strength $E_{e/t}$ over a defined reference surface (optically active area) at a distance of $\approx 10\text{mm}$ ($\pm 1\text{mm}$) from the surface of the tariff device or the reading head. The following limiting values apply:

ON-condition: $500 < E_{e/t} < 5000 \mu\text{W}/\text{cm}^2$

OFF-condition: $E_{e/t} < 10 \mu\text{W}/\text{cm}^2$

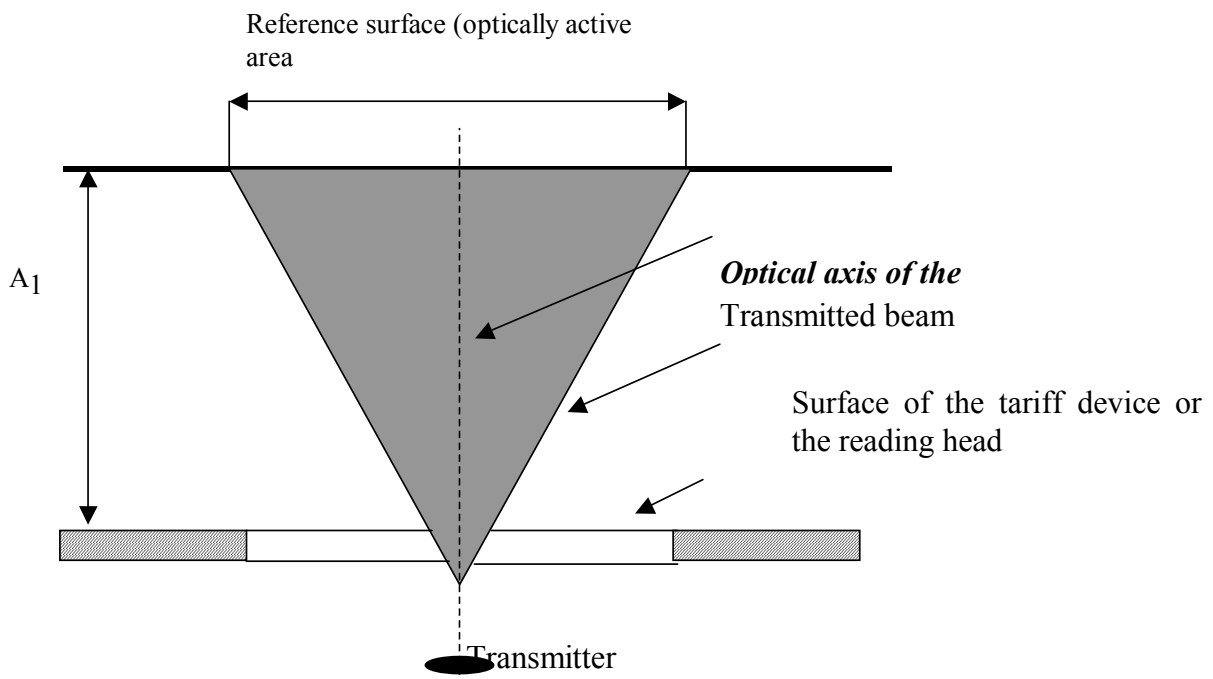


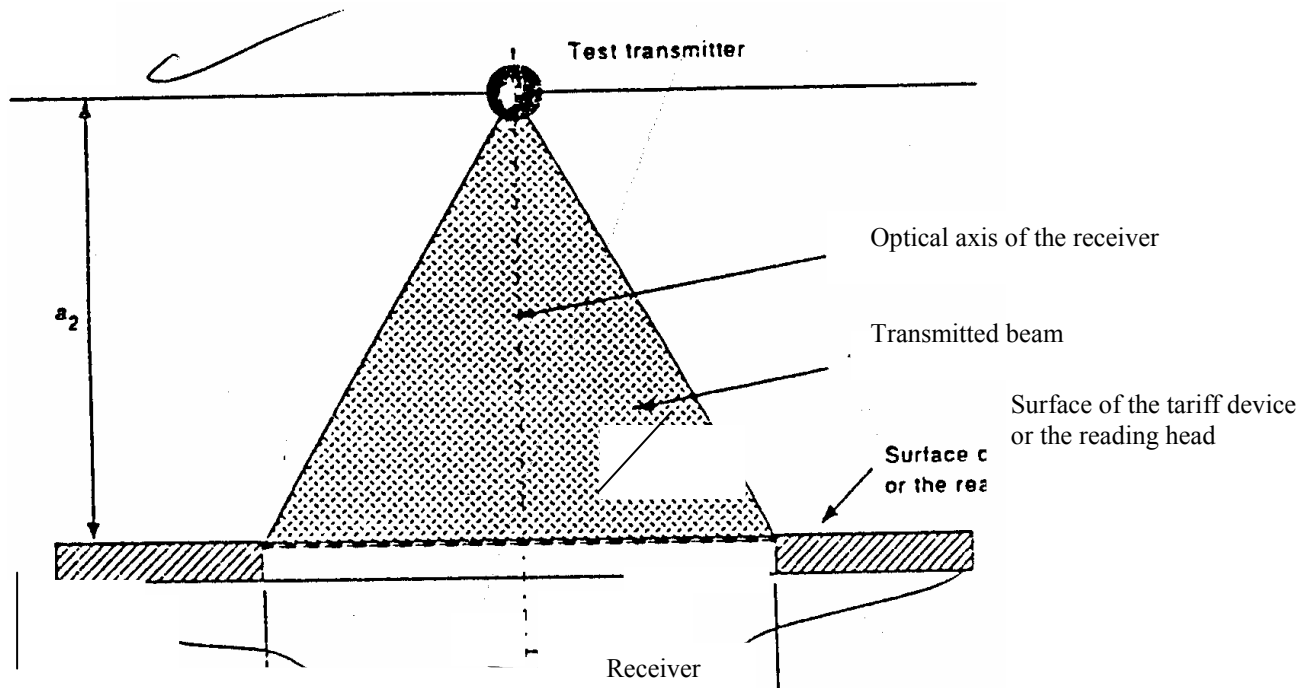
Figure 5-Test arrangement for the transmitter

Receiver

A transmitter which is positioned at a distance $a_2 = 10 \text{ mm}$ on the optical axis from the receiver in the tariff device or the reading head generates a signal with a radiation strength E_e/R Over a defined reference surface (optically active area)

The following limiting values apply:

ON -condition: receiver definitely ON at $E_e/R \geq 200 \mu\text{W}/\text{cm}^2$



ON -condition: receiver definitely OFF at $E_e/R \geq 20 \mu\text{W}$

Signal levels

Off-condition

binary 1

MARK (quiescent state)

light indication off

$< -3 \text{ V}$ (V.28)

-0.5V to $0,4\text{V}$ (TTL)

NOTE TTL levels are inverted with respect to conventional usage.

Transmission speed: At least 2400 baud.

ON-condition

binary 0

SPACE

light indication on

$< +3 \text{ V}$ (V.28)

-2.4V to V_p (TTL)

The following apply 10 command messages.

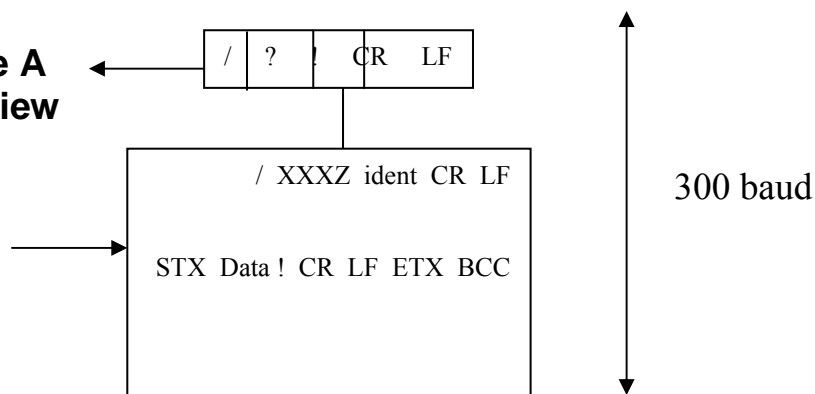
- a) The password command.
The address and unit fields are empty (devoid of any characters)
- b) The write command
Where the value represents a data string The address is the start location to which the data is to be written. The unit field is left empty.
- c) The read command
Where a data string is to be read. the address is the start location from which data is read.
The value represents the number of locations to be read including the start location. The unit field is left empty.
- d) The exit command
No dataset is required when the command identifier is '0'.

20) Error message

This consists of 32 printable characters maximum with exceptions of and It is bounded by front and rear boundary characters, as in the dataset structure. This is manufacturer specific and should be chosen such that it cannot be confused with data.

5.4 Communication modes

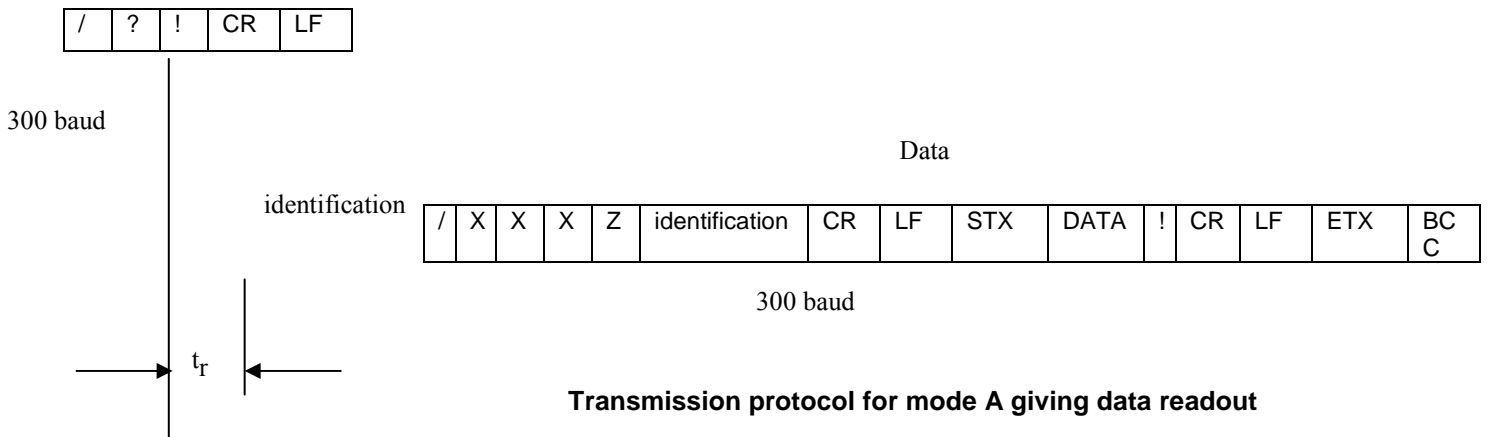
5.4.1 Mode A Overview



Data readout

The tariff device transmits the data message immediately following the identification message.

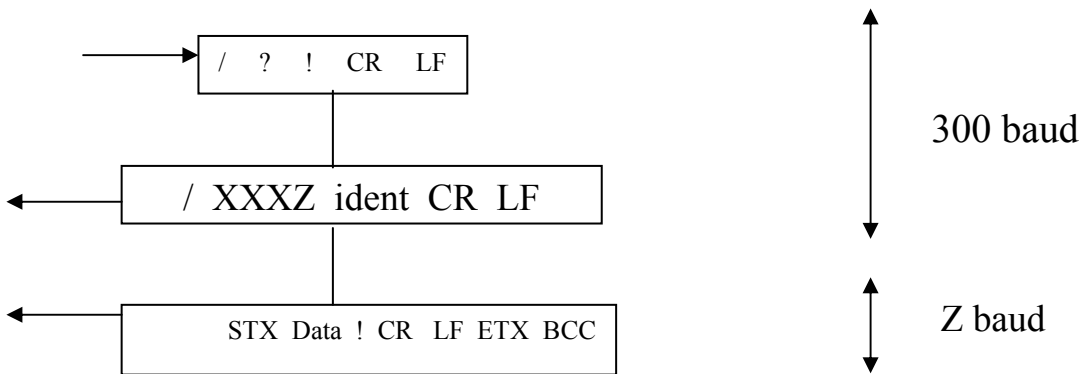
Request



Transmission protocol for mode A giving data readout

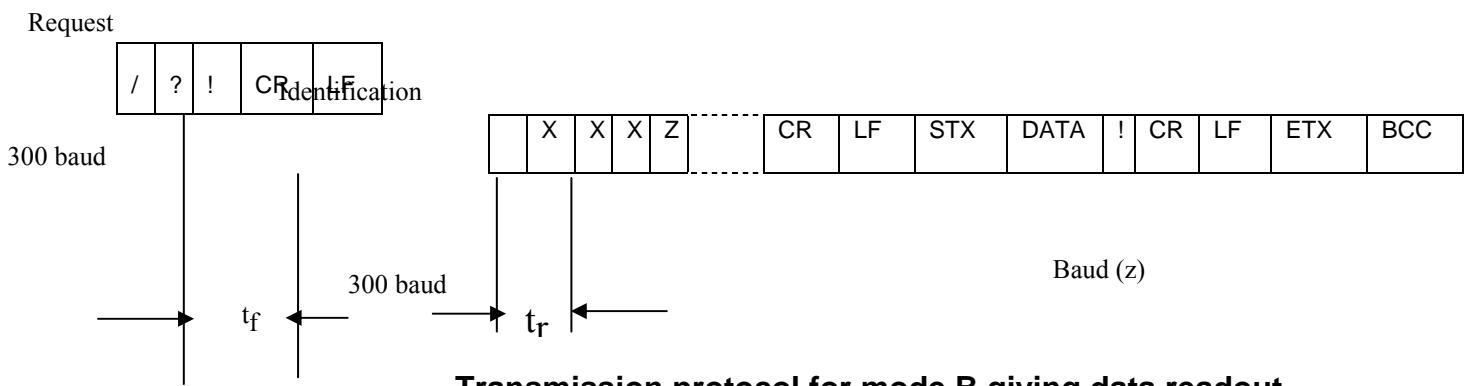
5.4.2 Mode B

Overview



Data readout

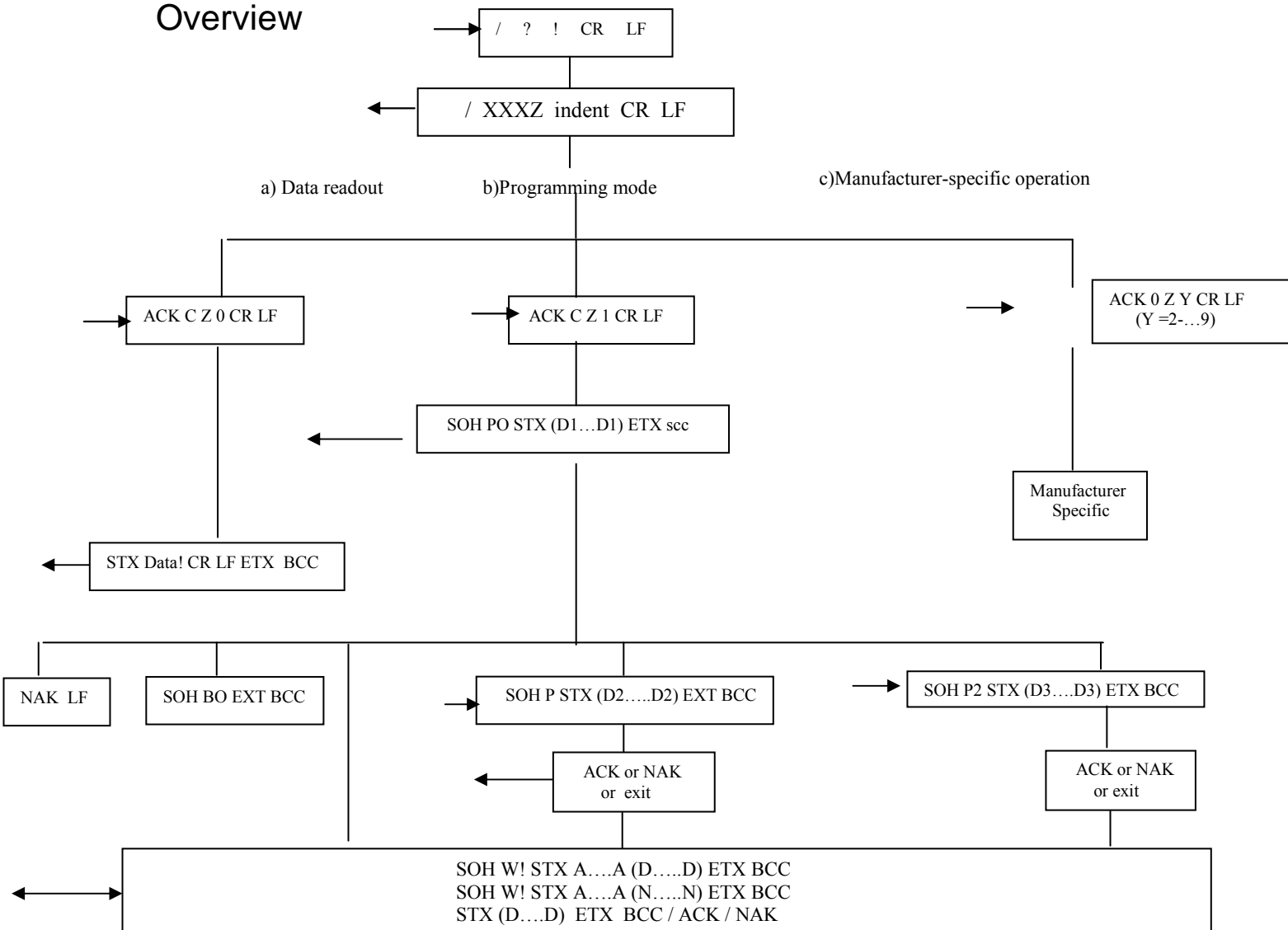
After transmitting the identification message. The tariff device briefly interrupts the transmission. During the interval the tariff device and the HHU switch over to the baud rate prescribed in the identification message. Following this tariff device transmits the data message at the new baud rate.



Transmission protocol for mode B giving data readout

5.4.2 Mode C

Overview



Levels of access - system security

In order to restrict access to the tariff device, different levels of security are defined. An) or a tariff device may use all of these

Access level 1,

Requires only a knowledge of this protocol to gain access.

Access level 2

Requires one or more passwords to be correctly entered.

Access level 3

Requires operation of a scalable button or manipulation of certain data with a secret algorithm to gain access.

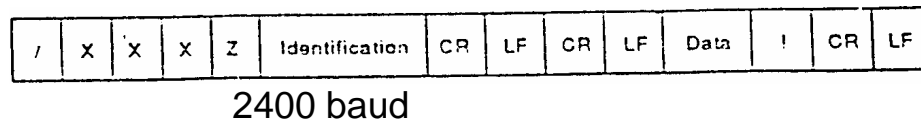
Overview.

Access level 4

Requires physical entry into the case of the tariff device and effecting a physical change / such as making/breaking a link or operation of a switch, before further communication:

Data readout

The tariff device transmits the data message at 2 400 baud immediately following the activation of a push button or other sensor on the tariff device



Transmission protocol for mode D

The time between two characters in a character sequence 's': $t < 15 \text{ ns}$

- Identification number or address: 16 printable characters maximum with the exception of '(".")', '/', and "!". The identification string is the code given to the 'value' and is taken from the identification code 'in the glossary system of the equipment concerned.
- Front boundary character of the value information,
- Rear boundary character of the value information ')".
- Value: 32 printable characters maximum with the exception of '(".")', '"', "/" and "!". For decimal values, only points (not commas) shall be used and shall be counted as characters.
- The separator character " between value and unit is not required if there are no units. e) Unit: 16 printable characters maximum with the exception of '(".")', '/' and "!". Remarks regarding items a) and 1) NOTE 1 - To reduce the quantity of data, the identification code a) or/and the unit information e) and 1) can be dispensed with, providing an unambiguous correlation exists. For example the identification code of the unit, information is not necessary for a sequence of similar values (sequence of historical values) on condition that the evaluation unit can clearly establish the identification code and unit of the succeeding values from the first value of a sequence Remarks regarding item d) NOTE 2 - In programming mode C, the 'value' portion may contain up to 12B characters.

Flag Protocol

FLAG Protocol:-

1 TRANSMISSION CHARACTERISTICS

1.1 Type of Transmission

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

1.2 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

1.3 Signal Quality

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

1.4 Character Format

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

1.5 Character Code

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

1.6 Character Security

With parity bit, even parity to ISO 1177.

2 DATA TRANSMISSION PROTOCOL

2.1 Overview

The data transmission protocol will use mode C operation of IEC 1107.

The following error conditions apply at all stages of communication.

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

- 1 Character format error
- 2 Character security error
- 3 Incorrect message framing characters
- 4 Incorrect BCC
- 5 A data string not bounded by open and closed brackets

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

- 1 Invalid command message identifier
- 2 Invalid command type identifier
- 3 Invalid mode control character**
- 4 Invalid baud rate identification
- 5 Invalid data identity
- 6 Data identity being written to is still password protected
- 7 Function being requested is still in time lock out
- 8 Incorrect protocol procedure character
- 9 The characters in a data string are invalid
- 10 Data access denied

2.1.3 A COMMS ERROR takes precedence over a DATA ERROR.

2.2 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.

2.3 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 following data exchange functions 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

2.4 Message Formats

i) Request Message

| | | | | | |
|---|---|---------------------------|---|----|----|
| / | ? | Device Address (optional) | ! | CR | LF |
|---|---|---------------------------|---|----|----|

ii) Identification Message

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

iii) Acknowledgement to Identification Message

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

iv) Acknowledgement Message

| |
|-----|
| ACK |
| 4) |

v) Repeat-Request Message

| |
|-----|
| NAK |
| 15) |

vi) Command Message

| | | | | | | |
|-----|-----|-----|-----|----------|-----|-----|
| SOH | C | D | STX | Data Set | ETX | BCC |
| 16) | 17) | 18) | 5) | 19) | 6) | 7) |

vii) Data Message

| | | | |
|-----|-------------|-----|-----|
| STX | Data Packet | ETX | BCC |
| 5) | 20) | 6) | 7) |

2.5 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.

- 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"
- 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

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
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.

2.6 Syntax Diagram

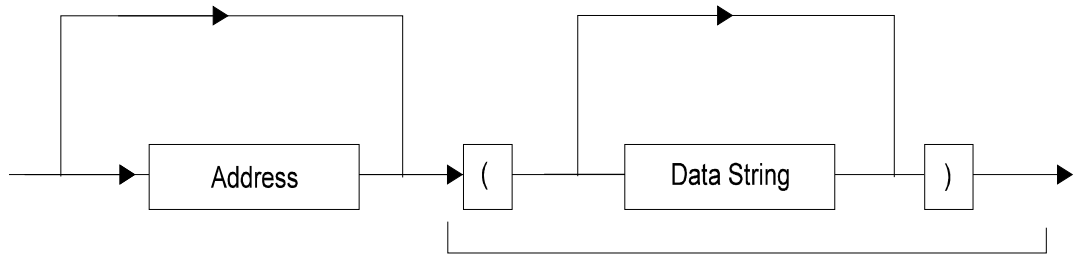
2.6.1 Data Set

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, 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



2.6.2 Data Packet

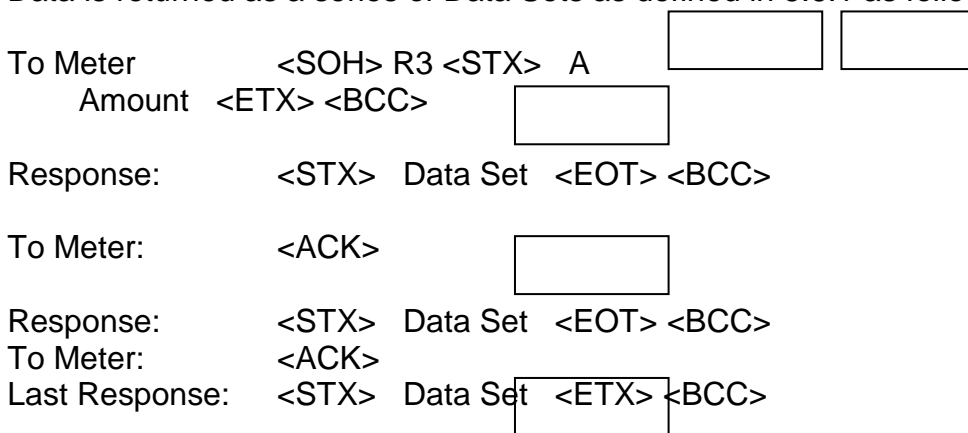
The data packet is a subset of the data set in which the address may be omitted. All other characteristics of the data packet are identical to that in a data set.

2.6.3 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



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.

2.7 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.

2.8 Reaction and Monitoring Times

2.8.1 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.

2.8.2 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 this time will be 20ms.

2.8.3 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).

3 SECURITY

The following security checks are carried out :

3.1 Character Check

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

3.2 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 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.

3.3 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.

*** 4. 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.

* **5. 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.