PUBLICLY AVAILABLE SPECIFICATION

IEC PAS 62030

Pre-Standard

First edition
2004-11

Digital data communications for measurement and control – Fieldbus for use in industrial control systems –

Section 1: MODBUS® Application Protocol Specification V1.1a –

Section 2: Real-Time Publish-Subscribe (RTPS) Wire Protocol Specification Version 1.0

Reference number
IEC/PAS 62030:2004(E)

Publication numbering

As from 1 January 1997 all IEC publications are issued with a designation in the 60000 series. For example, IEC 34-1 is now referred to as IEC 60034-1.

Consolidated editions

The IEC is now publishing consolidated versions of its publications. For example, edition numbers 1.0, 1.1 and 1.2 refer, respectively, to the base publication, the base publication incorporating amendment 1 and the base publication incorporating amendments 1 and 2.

Further information on IEC publications

The technical content of IEC publications is kept under constant review by the IEC, thus ensuring that the content reflects current technology. Information relating to this publication, including its validity, is available in the IEC Catalogue of publications (see below) in addition to new editions, amendments and corrigenda. Information on the subjects under consideration and work in progress undertaken by the technical committee which has prepared this publication, as well as the list of publications issued, is also available from the following:

- **IEC Web Site (www.iec.ch)**
- **Catalogue of IEC publications**

  The on-line catalogue on the IEC web site (www.iec.ch/searchpub) enables you to search by a variety of criteria including text searches, technical committees and date of publication. On-line information is also available on recently issued publications, withdrawn and replaced publications, as well as corrigenda.

- **IEC Just Published**

  This summary of recently issued publications (www.iec.ch/online_news/ justpub) is also available by email. Please contact the Customer Service Centre (see below) for further information.

- **Customer Service Centre**

  If you have any questions regarding this publication or need further assistance, please contact the Customer Service Centre:

Email: custserv@iec.ch
Tel: +41 22 919 02 11
Fax: +41 22 919 03 00

PUBLICLY AVAILABLE SPECIFICATION

IEC PAS 62030

Pre-Standard

First edition
2004-11

Digital data communications for measurement and control – Fieldbus for use in industrial control systems –

Section 1: MODBUS® Application Protocol Specification V1.1a –

Section 2: Real-Time Publish-Subscribe (RTPS) Wire Protocol Specification Version 1.0

International Electrotechnical Commission, 3, rue de Varembé, PO Box 131, CH-1211 Geneva 20, Switzerland
Telephone: +41 22 919 02 11 Telefax: +41 22 919 03 00 E-mail: inmail@iec.ch Web: www.iec.ch

Commission Electrotechnique Internationale
International Electrotechnical Commission
Международная Электротехническая Комиссия

PRICE CODE XG

For price, see current catalogue

CONTENTS

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

DIGITAL DATA COMMUNICATIONS FOR MEASUREMENT AND CONTROL – FIELDBUS FOR USE IN INDUSTRIAL CONTROL SYSTEMS –

Section 1: MODBUS®* Application Protocol Specification V1.1a – Section 2: Real-Time Publish-Subscribe (RTPS) Wire Protocol Specification Version 1.0

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

A PAS is a technical specification not fulfilling the requirements for a standard but made available to the public .

IEC-PAS 62030 has been processed by subcommittee 65C: Digital communications, of IEC technical committee 65: Industrial-process measurement and control.

The text of this PAS is based on the following document:	This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document
Draft PAS	**Report on voting**
65C/341A/NP	65C/347/RVN

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned will transform it into an International Standard.

---

* MODBUS is a trademark of Schneider Automation Inc.

It is foreseen that, at a later date, the content of this PAS will be incorporated in the future new edition of the IEC 61158 series according to its structure.

This PAS shall remain valid for an initial maximum period of three years starting from 2004-11. The validity may be extended for a single three-year period, following which it shall be revised to become another type of normative document or shall be withdrawn.

Overview

This PAS has been divided into two sections. Section 1 deals with MODBUS® Application Protocol Specification V1.1a while Section 2 covers the Real-Time Publish-Subscribe (RTPS) Wire Protocol Specification Version 1.0.

It is intended that the content of this PAS will be incorporated in the future new editions of the various parts of IEC 61158 series according to the structure of this series.

Section 1 – MODBUS® Application Protocol Specification V1.1a

1 MODBUS

1.1 Introduction

1.1.1 Scope of this section

MODBUS is an application layer messaging protocol, positioned at level 7 of the OSI model, that provides client/server communication between devices connected on different types of buses or networks.

The industry's serial de facto standard since 1979, MODBUS continues to enable millions of automation devices to communicate. Today, support for the simple and elegant structure of MODBUS continues to grow. The Internet community can access MODBUS at a reserved system port 502 on the TCP/IP stack.

MODBUS is a request/reply protocol and offers services specified by **function codes**. MODBUS function codes are elements of MODBUS request/reply PDUs. The objective of this PAS is to describe the function codes used within the framework of MODBUS transactions.

MODBUS is an application layer messaging protocol for client/server communication between devices connected on different types of buses or networks.

It is currently implemented using:

- TCP/IP over Ethernet. See Annex A of Section 1: MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE.
- Asynchronous serial transmission over a variety of media (wire : EIA/TIA-232-E, EIA-422-A, EIA/TIA-485-A; fiber, radio, etc.)
- MODBUS PLUS, a high speed token passing network.

NOTE The "Specification" is Clause 1 of this PAS.

NOTE MODBUS Plus is not in this PAS.

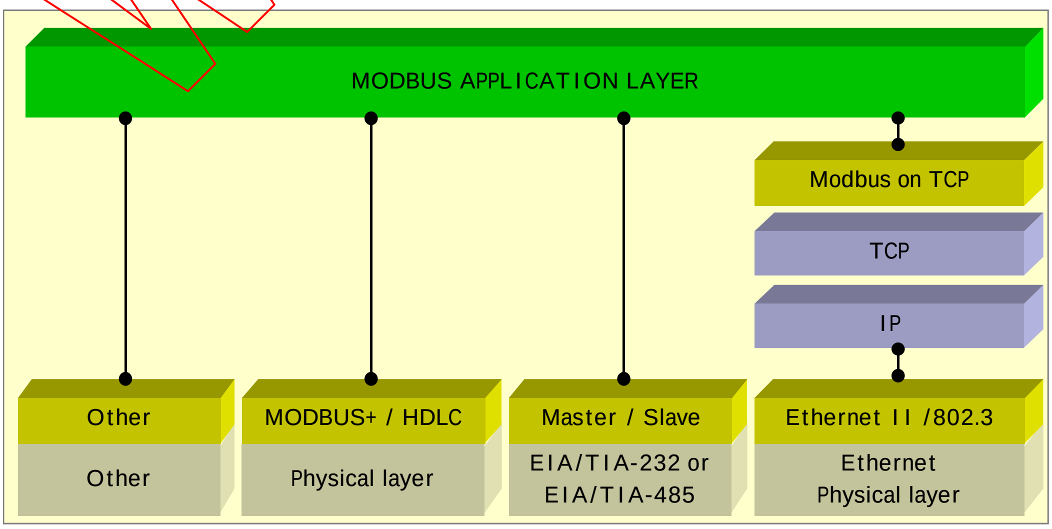

Figure 1 – MODBUS communication stack

This Figure 1 represents conceptually the MODBUS communication stack.

1.1.2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC 61131 (all parts): Programmable controllers

EIA*/TIA**-232-E: *Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary data Interchange*

EIA-422-A: *Electrical Characteristics-Balanced Voltage Digital Interface Circuit*

EIA/TIA-485-A: *Electrical Characteristics of Generators and Receivers for Use in balanced Digital Multipoint Systems*

RFC 791, *Interne Protocol*, Sep81 DARPA

1.2 Abbreviations

ADU Application Data Unit
HDLC High level Data Link Control
HMI Human Machine Interface
IETF Internet Engineering Task Force
I/O Input/Output
IP Internet Protocol
MAC Medium Access Control
MB MODBUS Protocol
MBAP MODBUS Application Protocol
PDU Protocol Data Unit
PLC Programmable Logic Controller
TCP Transport Control Protocol

1.3 Context

The MODBUS protocol allows an easy communication within all types of network architectures.

* EIA: Electronic Industries Alliance.

** TIA: Telecomunication Industry Association.

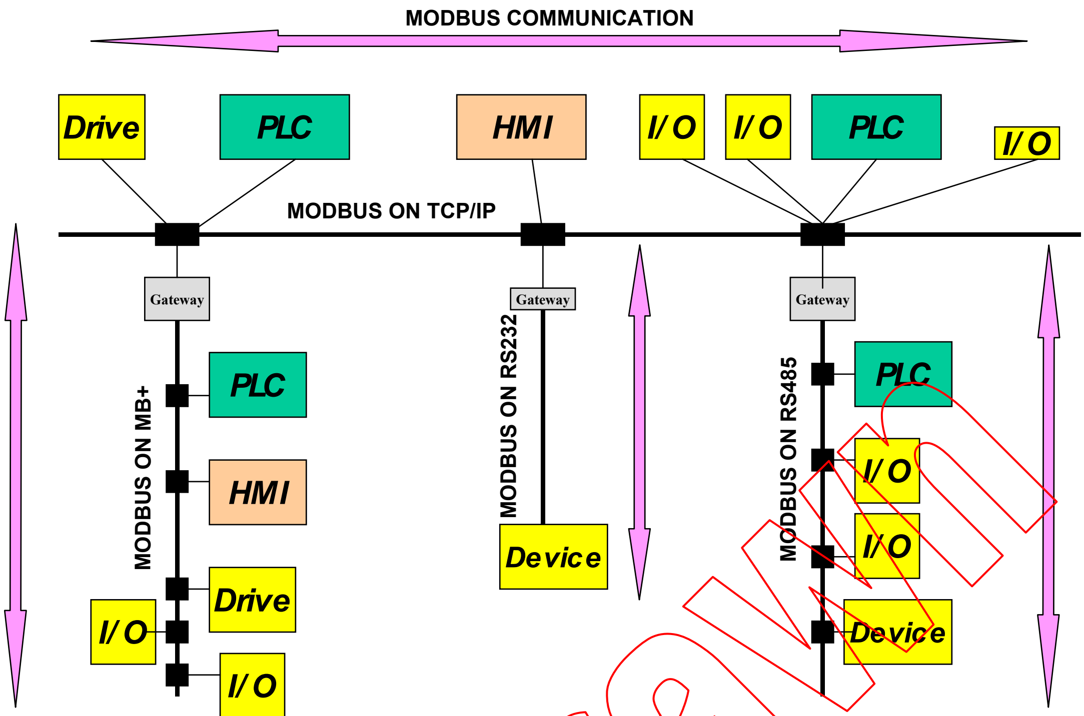

Figure 2 – Example of MODBUS Network Architecture

Every type of devices (PLC, HMI, Control Panel, Driver, Motion control, I/O Device…) can use MODBUS protocol to initiate a remote operation.

The same communication can be done as well on serial line as on an Ethernet TCP/IP networks. Gateways allow a communication between several types of buses or network using the MODBUS protocol.

1.4 General description

1.4.1 Protocol description

The MODBUS protocol defines a simple protocol data unit **(PDU)** independent of the underlying communication layers. The mapping of MODBUS protocol on specific buses or network can introduce some additional fields on the application data unit **(ADU)**.

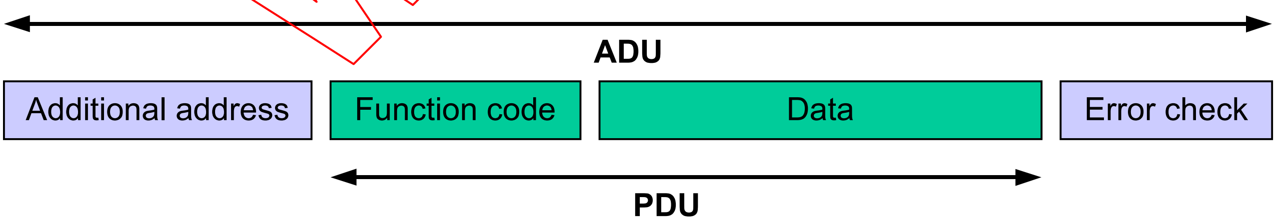

Figure 3 – General MODBUS frame

The MODBUS application data unit is built by the client that initiates a MODBUS transaction. The function indicates to the server what kind of action to perform. The MODBUS application protocol establishes the format of a request initiated by a client.

The function code field of a MODBUS data unit is coded in one byte. Valid codes are in the range of 1 ... 255 decimal (128 – 255 reserved for exception responses). When a message is sent from a Client to a Server device the function code field tells the server what kind of action to perform. Function code "0" is not valid.

Sub-function codes are added to some function codes to define multiple actions.

The data field of messages sent from a client to server devices contains additional information that the server uses to take the action defined by the function code. This can include items like discrete and register addresses, the quantity of items to be handled, and the count of actual data bytes in the field.

The data field may be nonexistent (of zero length) in certain kinds of requests, in this case the server does not require any additional information. The function code alone specifies the action.

If no error occurs related to the MODBUS function requested in a properly received MODBUS ADU the data field of a response from a server to a client contains the data requested. If an error related to the MODBUS function requested occurs, the field contains an exception code that the server application can use to determine the next action to be taken.

For example a client can read the ON / OFF states of a group of discrete outputs or inputs or it can read/write the data contents of a group of registers.

When the server responds to the client, it uses the function code field to indicate either a normal (error-free) response or that some kind of error occurred (called an exception response). For a normal response, the server simply echoes to the request the original function code.

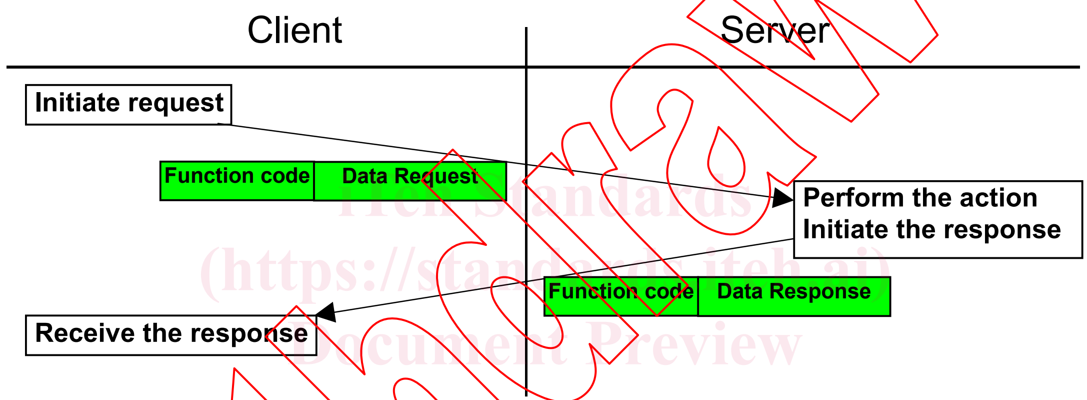

Figure 4 – MODBUS transaction (error free)

For an exception response, the server returns a code that is equivalent to the original function code from the request PDU with its most significant bit set to logic 1.

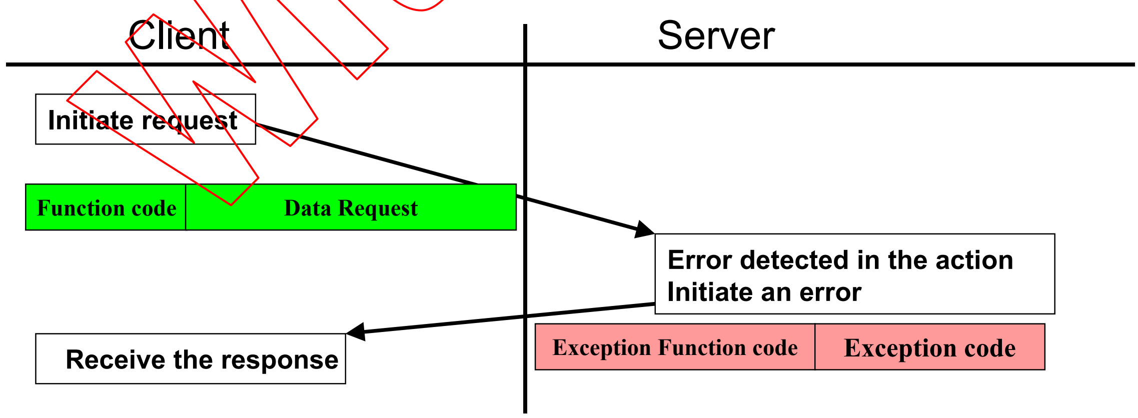

Figure 5 – MODBUS transaction (exception response)

NOTE It is desirable to manage a time out in order not to indefinitely wait for an answer which will perhaps never arrive.

The size of the MODBUS PDU is limited by the size constraint inherited from the first MODBUS implementation on Serial Line network (max. RS485 ADU = 256 bytes).

Therefore:

MODBUS **PDU for serial line communication =** 256 - Server adress (1 byte) - CRC (2 bytes) = **253 bytes**.

Consequently:

RS232 / RS485 **ADU** = 253 bytes + Server adress (1 byte) + CRC (2 bytes) = **256 bytes**.

TCP MODBUS **ADU** = 253 bytes + MBAP (7 bytes) = **260 bytes**.

The MODBUS protocol defines three PDUs. They are :

- MODBUS Request PDU, mb_req_pdu
- MODBUS Response PDU, mb_rsp_pdu
- MODBUS Exception Response PDU, mb_excep_rsp_pdu

The mb_req_pdu is defined as:

mb_req_pdu = {function_code, request_data}, where

function_code = [1 byte] MODBUS function code corresponding to the desired MODBUS function code or requested through the client API,

request_data = [n bytes] This field is function code dependent and usually contains information such as variable references,

variable counts, data offsets, sub-function codes etc.

The mb_rsp_pdu is defined as:

mb_rsp_pdu = {function_code, response_data}, where

function_code = [1 byte] MODBUS function code

response_data = [n bytes] This field is function code dependent and usually contains information such as variable references,

variable counts, data offsets, sub-function codes, etc.

The mb_excep_rsp_pdu is defined as:

mb_excep_rsp_pdu = {function_code, request_data}, where

exception-function_code = [1 byte] MODBUS function code + 0x80

exception_code = [1 byte] MODBUS Exception Code Defined in table "MODBUS Exception Codes" (see 1.7).

1.4.2 Data Encoding

- MODBUS uses a 'big-Endian' representation for addresses and data items. This means that when a numerical quantity larger than a single byte is transmitted, the most significant byte is sent first. So for example

Register size	value			
16 - bits	0x1234	the first byte sent is	0x12	then 0x34

NOTE For more details, see [1] in 1.1.2.

1.4.3 MODBUS data model

MODBUS bases its data model on a series of tables that have distinguishing characteristics. The four primary tables are:

Primary tables	Object type	Type of	Comments
Discretes Input	Single bit	Read-Only	This type of data can be provided by an I/O system.
Coils	Single bit	Read-Write	This type of data can be alterable by an application program.
Input Registers	16-bit word	Read-Only	This type of data can be provided by an I/O system
Holding Registers	16-bit word	Read-Write	This type of data can be alterable by an application program.

The distinctions between inputs and outputs, and between bit-addressable and word-addressable data items, do not imply any application behavior. It is perfectly acceptable, and very common, to regard all four tables as overlaying one another, if this is the most natural interpretation on the target machine in question.

For each of the primary tables, the protocol allows individual selection of 65536 data items, and the operations of read or write of those items are designed to span multiple consecutive data items up to a data size limit which is dependent on the transaction function code.

It's obvious that all the data handled via MODBUS (bits, registers) must be located in device application memory. But physical address in memory should not be confused with data reference. The only requirement is to link data reference with physical address.

MODBUS logical reference number, which are used in MODBUS functions, are unsigned integer indices starting at zero.

- **Implementation examples of MODBUS model**

The examples below show two ways of organizing the data in device. There are different organizations possible, but not all are described in this document. Each device can have its own organization of the data according to its application

Example 1 : Device having 4 separate blocks

The example below shows data organization in a device having digital and analog, inputs and outputs. Each block is separate because data from different blocks have no correlation. Each block is thus accessible with different MODBUS functions.

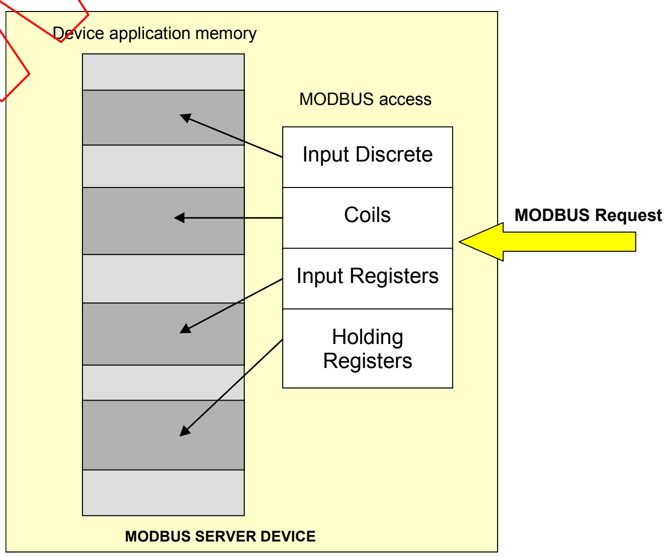

Figure 6 – MODBUS Data Model with separate block