PUBLICLY AVAILABLE SPECIFICATION

Pre-Standard

IEC PAS 62030

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

FOREWORD 5

Section 1 – MODBUS® Application Protocol Specification V1.1a 7
1 MODBUS 7
1.1 Introduction 7
1.1.1 Scope of this section 7
1.1.2 Normative references 8
1.2 Abbreviations 8
1.3 Context 8
1.4 General description 9
1.4.1 Protocol description 9
1.4.2 Data Encoding 11
1.4.3 MODBUS data model 12
1.4.4 MODBUS Addressing model 13
1.4.5 Define MODBUS Transaction 14
1.5 Function Code Categories 16
1.5.1 Public Function Code Definition 17
1.6 Function codes descripitons 17
1.6.1 01 (0x01) Read Coils 17
1.6.2 02 (0x02) Read Discrete Inputs 19
1.6.3 03 (0x03) Read Holding Registers 21
1.6.4 04 (0x04) Read Input Registers 22
1.6.5 05 (0x05) Write Single Coil 23
1.6.6 06 (0x06) Write Single Register 24
1.6.7 07 (0x07) Read Exception Status (Serial Line only) 26
1.6.8 08 (0x08) Diagnostics (Serial Line only) 27
1.6.9 11 (0x0B) Get Comm Event Counter (Serial Line only) 30
1.6.10 12 (0x0C) Get Comm Event Log (Serial Line only) 32
1.6.11 15 (0x0F) Write Multiple Coils 34
1.6.12 16 (0x10) Write Multiple registers 35
1.6.13 17 (0x11) Report Slave ID (Serial Line only) 37
1.6.14 20 / 6 (0x14 / 0x06) Read File Record 37
1.6.15 21 / 6 (0x15 / 0x06) Write File Record 39
1.6.16 22 (0x16) Mask Write Register 41
1.6.17 23 (0x17) Read/Write Multiple registers 43
1.6.18 24 (0x18) Read FIFO Queue 45
1.6.19 43 (0x2B) Encapsulated Interface Transport 46
1.6.20 43 / 13 (0x2B / 0x0D) CANopen General Reference Request and Response PDU 47
1.6.21 43 / 14 (0x2B / 0x0E) Read Device Identification 48
1.7 MODBUS Exception Responses 52

Annex A of Section 1 (informative) MODBUS MESSAGING ON TCP/IP IMPLEMENTATION GUIDE 54
A.1 INTRODUCTION 54
A.1.1 OBJECTIVES 54
A.1.2 CLIENT / SERVER MODEL 54

A.1.3 REFERENCE DOCUMENTS 55
A.2 ABBREVIATIONS 55
A.3 CONTEXT 55
A.3.1 PROTOCOL DESCRIPTION 55
A.3.2 MODBUS FUNCTIONS CODES DESCRIPTION 57
A.4 FUNCTIONAL DESCRIPTION 58
A.4.1 MODBUS COMPONENT ARCHITECTURE MODEL 58
A.4.2 TCP CONNECTION MANAGEMENT 61
A.4.3 USE of TCP/IP STACK 65
A.4.4 COMMUNICATION APPLICATION LAYER 71
A.5 IMPLEMENTATION GUIDELINE 82
A.5.1 OBJECT MODEL DIAGRAM 83
A.5.2 IMPLEMENTATION CLASS DIAGRAM 87
A.5.3 SEQUENCE DIAGRAMS 89
A.5.4 CLASSES AND METHODS DESCRIPTION 92

Annex B of Section 1 (Informative) MODBUS RESERVED FUNCTION CODES, SUBCODES AND MEI TYPES 96

Annex C of Section 1 (Informative) CANOPEN GENERAL REFERENCE COMMAND 96

Section 2 – Real-Time Publish-Subscribe (RTPS) Wire Protocol Specification Version 1.0 97

2 RTPS 97
2.1 Basic Concepts 97
2.1.1 Introduction 97
2.1.2 The RTPS Object Model 98
2.1.3 The Basic RTPS Transport Interface 99
2.1.4 Notational Conventions 100
2.2 Structure Definitions 101
2.2.1 Referring to Objects: the GUID 101
2.2.2 Building Blocks of RTPS Messages 102
2.3 RTPS Message Format 105
2.3.1 Overall Structure of RTPS Messages 105
2.3.2 Submessage Structure 105
2.3.3 How to Interpret a Message 106
2.3.4 Header 107
2.3.5 ACK 108
2.3.6 GAP 109
2.3.7 HEARTBEAT 110
2.3.8 INFO_DST 112
2.3.9 INFO_REPLY 112
2.3.10 INFO_SRC 113
2.3.11 INFO_TS 114
2.3.12 ISSUE 114
2.3.13 PAD 115
2.3.14 VAR 116
2.3.15 Versioning and Extensibility 117
2.4 RTPS and UDP/IPv4 118
2.4.1 Concepts 118
2.4.2 RTPS Packet Addressing 118
2.4.3 Possible Destinations for Specific Submessages 121

2.5 Attributes of Objects and Metatraffic 122
2.5.1 Concept 122
2.5.2 Wire Format of the ParameterSequence 124
2.5.3 ParameterID Definitions 125
2.5.4 Reserved Objects 126
2.5.5 Examples 130
2.6 Publish-Subscribe Protocol 132
2.6.1 Publication and Subscription Objects 132
2.6.2 Representation of User Data 137
2.7 CST Protocol 139
2.7.1 Object Model 139
2.7.2 Structure of the Composite State (CS) 140
2.7.3 CSTWriter 140
2.7.4 CSTReader 145
2.7.5 Overview of Messages used by CST 147
2.8 Discovery with the CST Protocol 149
2.8.1 Overview 149
2.8.2 Managers Keep Track of Their Managees 150
2.8.3 Inter-Manager Protocol 150
2.8.4 The Registration Protocol 151
2.8.5 The Manager-Discovery Protocol 152
2.8.6 The Application Discovery Protocol 152
2.8.7 Services Discovery Protocol 153
Annex A of Section 2 (informative) CDR for RTPS 155
A.1 Primitive Types 155
A.1.1 Semantics 155
A.1.2 Encoding 155
A.1.3 octet 155
A.1.4 boolean 156
A.1.5 unsigned short 156
A.1.6 short 156
A.1.7 unsigned long 156
A.1.8 long 156
A.1.9 unsigned long long 156
A.1.10 long long 156
A.1.11 float157
A.1.12 double 157
A.1.13 char 157
A.1.14 wchar 157
A.2 Constructed Types 157
A.2.1 Alignment 157
A.2.2 Identifiers 157
A.2.3 List of constructed types 157
A.2.4 Struct 158
A.2.5 Enumeration 158
A.2.6 Sequence 158
A.2.7 Array 158
A.2.8 String 158
A.2.9 Wstring 159

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.

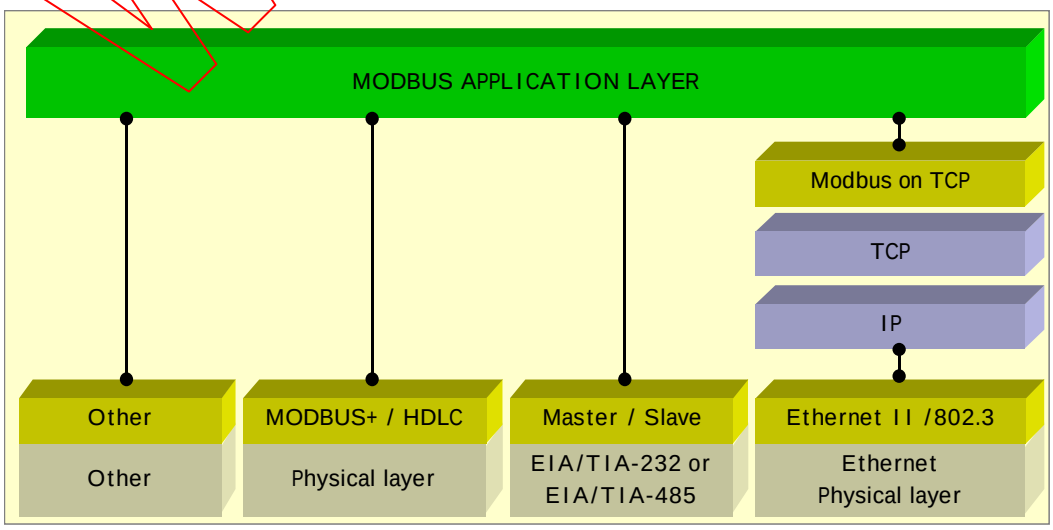

Figure 1 – MODBUS communication stack

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

* EIA: Electronic Industries Alliance.

** TIA: Telecomunication Industry Association.