Practical Troubleshooting and Problem Solving of Modbus Protocols

THIS BOOK WAS DEVELOPED BY IDC TECHNOLOGIES

WHO ARE WE?

IDC Technologies is internationally acknowledged as the premier provider of practical, technical training for engineers and technicians.

We specialize in the fields of electrical systems, industrial data communications, telecommunications, automation and control, mechanical engineering, chemical and civil engineering, and are continually adding to our portfolio of over 100 different workshops. Our instructors are highly respected in their fields of expertise and in the last ten years have trained over 200,000 engineers, scientists and technicians.

With offices conveniently located worldwide, IDC Technologies has an enthusiastic team of professional engineers, technicians and support staff who are committed to providing the highest level of training and consultancy.

TECHNICAL WORKSHOPS

TRAINING THAT WORKS

We deliver engineering and technology training that will maximize your business goals. In today's competitive environment, you require training that will help you and your organization to achieve its goals and produce a large return on investment. With our 'training that works' objective you and your organization will:

- Get job-related skills that you need to achieve your business goals
- Improve the operation and design of your equipment and plant
- Improve your troubleshooting abilities
- Sharpen your competitive edge
- Boost morale and retain valuable staff
- Save time and money

EXPERT INSTRUCTORS

We search the world for good quality instructors who have three outstanding attributes:

1. Expert knowledge and experience – of the course topic
2. Superb training abilities – to ensure the know-how is transferred effectively and quickly to you in a practical, hands-on way
3. Listening skills – they listen carefully to the needs of the participants and want to ensure that you benefit from the experience.

Each and every instructor is evaluated by the delegates and we assess the presentation after every class to ensure that the instructor stays on track in presenting outstanding courses.

HANDS-ON APPROACH TO TRAINING

All IDC Technologies workshops include practical, hands-on sessions where the delegates are given the opportunity to apply in practice the theory they have learnt.

REFERENCE MATERIALS

A fully illustrated workshop book with hundreds of pages of tables, charts, figures and handy hints, plus considerable reference material is provided FREE of charge to each delegate.

ACCREDITATION AND CONTINUING EDUCATION

Satisfactory completion of all IDC workshops satisfies the requirements of the International Association for Continuing Education and Training for the award of 1.4 Continuing Education Units.

IDC workshops also satisfy criteria for Continuing Professional Development according to the requirements of the Institution of Electrical Engineers and Institution of Measurement and Control in the UK, Institution of Engineers in Australia, Institution of Engineers New Zealand, and others.

CERTIFICATE OF ATTENDANCE
Each delegate receives a Certificate of Attendance documenting their experience.

100% MONEY BACK GUARANTEE
IDC Technologies' engineers have put considerable time and experience into ensuring that you gain maximum value from each workshop. If by lunchtime on the first day you decide that the workshop is not appropriate for your requirements, please let us know so that we can arrange a 100% refund of your fee.

ONSITE WORKSHOPS
All IDC Technologies Training Workshops are available on an on-site basis, presented at the venue of your choice, saving delegates travel time and expenses, thus providing your company with even greater savings.

OFFICE LOCATIONS
AUSTRALIA • CANADA • INDIA • IRELAND • MALAYSIA • NEW ZEALAND • POLAND • SINGAPORE • SOUTH AFRICA • UNITED KINGDOM • UNITED STATES

idc@idc-online.com **www.idc-online.com**

Technology Training that Works

Presents

Practical Troubleshooting and Problem Solving of Modbus Protocol

Revision 4.1

Website: www.idc-online.com
E-mail: idc@idc-online.com

IDC Technologies Pty Ltd
PO Box 1093, West Perth, Western Australia 6872
Offices in Australia, New Zealand, Singapore, United Kingdom, Ireland, Malaysia, Poland, United States of America, Canada, South Africa and India

First published 2008

ISBN: 978-1-921007-36-1

Disclaimer

Whilst all reasonable care has been taken to ensure that the descriptions, opinions, programs, listings, software and diagrams are accurate and workable, IDC Technologies do not accept any legal responsibility or liability to any person, organization or other entity for any direct loss, consequential loss or damage, however caused, that may be suffered as a result of the use of this publication or the associated workshop and software.

In case of any uncertainty, we recommend that you contact IDC Technologies for clarification or assistance.

Trademarks

All terms used in this publication that are believed to be registered trademarks or trademarks are listed below:

Acknowledgements

IDC Technologies expresses its sincere thanks to all those engineers and technicians on our training workshops who freely made available their expertise in preparing this manual.

Table of Contents

Preface

The objective of this workshop is to help delegates identify, prevent and fix common industrial data communications problems focusing on the Modbus protocol. The focus is 'outside the box', with the emphasis on practicals that go beyond the typical communications issues and theories. The workshop focus is on providing delegates with the necessary toolkit of skills to solve industrial data communication problems where Modbus is used.

Modbus-based industrial communications systems (based on RS-232/RS-485 and Ethernet) are being installed throughout industry today, from connecting simple instruments to Programmable Logic Controllers to the PCs throughout the plant. Communications problems range from simple wiring problems to intermittent transfer of protocol messages. Whilst the main issues with the Modbus protocol will be covered in this workshop, a clear understanding of the protocols and standards that transport Modbus are required in order to effectively work with Modbus. This includes RS-485/RS-232 and Ethernet (preferably Industrial Ethernet) and TCP/IP.

Modbus, effectively one of the few (arguably, the only) industrial messaging protocols recognized by the Internet world (port 502) has one of the largest installed bases worldwide with more than 7.2 million installed nodes. The Modbus TCP/IP profile has recently been accepted by the International Electro-technical Commission (IEC) as a publicly available specification (IEC PAS 62030) and is now eligible to become part of future editions of the International Standards IEC 61158 and IEC 61784-2. So it enjoys the status of a widely available Open Standard available to everyone and thus the popularity. Whilst detractors will say that the Modbus protocol lacks some of the refinements of the newer offerings on the market; there is no doubt that it is one of the most popular standards available in the industrial world.

The communications system on your plant underpins your entire operation. It is critical that you have the knowledge and tools to quickly identify and fix problems as they occur, to ensure you have a secure system. No compromise is possible here. This workshop distills all the tips and tricks learnt with the benefit of many years of experience. It offers a common approach covering all of the sections with each standard/protocol having the following structure:

- Quick overview of the standard
- Common problems and faults with this standard
- Description of tools used

Each of the typical faults is then discussed in depth with details on how to fix them.

1

Introduction

Objectives

When you have completed study of this chapter you will be able to:

- Describe the modern instrumentation and control system
- List the main industrial communications systems
- Describe the essential components of industrial communications systems

1.1 Introduction

Data communications involves the transfer of information from one point to another. In this book, we are specifically concerned with digital data communication. In this context, 'data' refers to information that is represented by a sequence of zeros and ones, the same sort of data handled by computers. Many communication systems handle analog data; examples being telephone systems, radio and television. Modern instrumentation is almost wholly concerned with the transfer of digital data.

Any communications system requires a transmitter to send information, a receiver to accept it, and a link (the medium) between the two. Types of link include copper wire, optical fiber, radio and microwave.

Some short–distance links use parallel connections, meaning that several wires are required to carry a signal. This type of connection is confined to devices such as local printers. Virtually all modern data communications systems use serial links in which the data is transmitted in sequence over a single circuit.

Digital data is sometimes transferred using a system that is primarily designed for analog communication. A modem, for example, works by using a digital data stream to modulate an analog signal that is sent over a telephone line. Another modem demodulates the signal to reproduce the original digital data at the receiving end. The word 'modem' is derived from *modulator* and *demodulator*.

There should be mutual agreement on how data is to be encoded, that is, the receiver must be able to understand what the transmitter is sending. The rules governing the communication are known as *protocols.*

In the past decade, many standards and protocols have been established, and this allows data communications technology to be used more effectively in the industry. Designers and users are beginning to realize the tremendous economic and productive gains possible with the integration of systems that are already in operation.

Historically, developers of software and hardware platforms have developed protocols that can only be used on their own products. In order to develop more integrated instrumentation and control systems, standardization of these communication protocols was required.

Standards may evolve from the widespread use of one manufacturer's protocol (a *de facto* standard) or may be specifically developed by bodies that represent certain industries. Standards allow manufacturers to develop products that communicate with equipment already in use. For the customer this simplifies the integration of products from different sources.

The industrial communications market is characterized by a lack of standardization. There are, however, a few dominant standards. Modbus has been a *de facto* standard for many years and the tried-and-tested physical standards such as RS-232 and RS-485 have been widely used. The area that has caused a considerable amount of angst (and dare we say - irritation) amongst vendors and users is the choice of an acceptable fieldbus, which would tie together instruments to PLCs and PCs. This effort has resulted in a few dominant, but competing standards such as PROFIBUS, DeviceNet and FOUNDATION Fieldbus being used in various areas of the industry.

The standard that has created an enormous amount of interest in the past few years is Ethernet. Initially it was rejected as being non-deterministic, which means there is no guarantee that a critical message is delivered within a defined time. This problem has been solved with the latest standards in Ethernet and the use of switching technology. The other protocol suite that fits onto Ethernet extremely well is TCP/IP. Being developed specifically for the Internet, it is very popular and widely used.

1.2 Modern instrumentation and control systems

In an instrumentation and control system, data is acquired by measuring instruments and transmitted to a controller, typically a computer. The controller then transmits data (control signals) to the control devices, which act upon a given process.
The integration of systems in a plant allows data to be transferred quickly and effectively between different systems along a data communications link. This eliminates the need for expensive and unwieldy wiring looms and termination points.
Productivity and quality are the principal objectives in the good management of any production activity. Management can be substantially improved by the availability of accurate and timely data. From this, we can surmise that a good instrumentation and control system can facilitate both quality and productivity.
The main purpose of an instrumentation and control system in an industrial environment is to provide the following:

- **Control of the processes and alarms**

  Traditionally, analog controllers operating on standard 4-20 mA loops provide control of parameters such as temperature and flow. The 4-20 mA standard is used by equipment from a wide variety of suppliers, and it is common for equipment from various sources to be mixed in the same control system. Stand-alone controllers and instruments have largely been replaced by integrated systems such as Distributed Control Systems (DCS), described below

- **Control of sequencing, interlocking and alarms**

  Typically, this was provided by relays, timers and other components hardwired into the control panels and motor control centers. The sequence control, interlocking and alarm requirements have largely been replaced by PLCs.

- **An operator interface for display and control**

  Traditionally, several operators are responsible for a portion of the overall process, operating process and manufacturing plants from various local control panels. Modern control systems tend to use a central control room to monitor the entire plant. The control room is equipped with computer-based operator workstations that gather data from the field instrumentation and use it for controlling the processes, monitoring alarms, control sequencing and interlocking.

- **Management information**

  Management information was traditionally provided by taking readings from meters, chart recorders, counters and transducers and from samples taken from the production process. This data is required to monitor the overall performance of a plant or process and to provide the data necessary to manage the process. Data acquisition is now integrated into the overall control system. This eliminates the gathering of information and reduces the time required to correlate and use the information to remove bottlenecks. Good management can achieve substantial productivity gains. The ability of control equipments to fulfill these requirements has depended on major advances that have taken place in the fields of integrated electronics, microprocessors and data communications. The four devices that have made the most significant impact on how plants are controlled are:
    - Distributed Control Systems (DCSs)
    - Programmable Logic Controllers (PLCs)
    - SCADA (Supervisory Control And Data Acquisition) systems
    - Smart Instruments

1.2.5 DCSs

A DCS is a hardware- and software-based (digital) process control and data acquisition system. The DCS is based on a ‘data highway’ (bus) and has a modular, distributed, but integrated architecture. Each module performs a specific dedicated task such as the operator interface/analog or loop control/digital control. There is normally an interface unit situated on the data highway allowing easy connection to other devices such as PLCs and supervisory computer devices.