SCADA: Supervisory Control and Data Acquisition

4th Edition

The Integration Group of The Americas Ex. 1007-Page 1
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001054

SCADA: Supervisory Control and Data Acquisition

4th Edition

By Stuart A. Boyer

Iliad Development Inc.



The Integration Group of The Americas Ex. 1007-Page 2
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001055

Notice

The information presented in this publication is for the general education of the reader. Because neither the author nor the publisher have any control over the use of the information by the reader, both the author and the publisher disclaim any and all liability of any kind arising out of such use. The reader is expected to exercise sound professional judgment in using any of the information presented in a particular application.

Additionally, neither the author nor the publisher have investigated or considered the affect of any patents on the ability of the reader to use any of the information in a particular application. The reader is responsible for reviewing any possible patents that may affect any particular use of the information presented.

Any references to commercial products in the work are cited as examples only. Neither the author nor the publisher endorse any referenced commercial product. Any trademarks or tradenames referenced belong to the respective owner of the mark or name. Neither the author nor the publisher make any representation regarding the availability of any referenced commercial product at any time. The manufacturer's instructions on use of any commercial product must be followed at all times, even if in conflict with the information in this publication.

Copyright © 2010
ISA—International Society of Automation
All rights reserved.

Printed in the United States of America.
10 9 8 7 6 5 4 3 2

ISBN 978-1-936007-09-7

No part of this work may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher.

ISA
67 Alexander Drive, P.O. Box 12277
Research Triangle Park, NC 27709
www.isa.org

Library of Congress Cataloging-in-Publication Data

Boyer, Stuart A.
SCADA: supervisory control and data acquisition / by Stuart A. Boyer.-- 4th ed.
p. cm.
ISBN 978-1-936007-09-7 (pbk.)
1. Management information systems--Programmed instruction. 2. Supervisory control systems--Programmed instruction. 3. Automatic data collection systems--Programmed instruction. I. Title.

T58.6.B675 2010
670.42'75--dc22

2009027094

WB_00001056

TABLE OF CONTENTS

	Preface to the Fourth Edition	**ix**
UNIT 1	**Introduction and Overview**	**3**
1-1	Text Coverage	3
1-2	Purpose	3
1-3.	Audience and Prerequisites	3
1-4.	Study Materials	4
1-5.	Organization and Sequence	4
1-6.	Course Objectives	6
1-7.	Course Length	6
UNIT 2	**SCADA – Purpose, Elements, and Layout**	**9**
2-1.	Purpose of a SCADA System	10
2-2.	Applicable Processes	10
2-3.	Elements of a SCADA System	12
2-4.	SCADA Layout	16
2-5.	A Limited Two-Way System	17
	Unit 2 Exercises	17
UNIT 3	**Historical Development—Analog and Digital**	**21**
3-1.	Analog Signals, Measurement, and Control	21
3-2.	Discrete Signals, Measurement, and Control	22
3-3.	Development from Telemetry	24
3-4.	Dependence on Communication and Computers	25
	Unit 3 Exercises	29
UNIT 4	**Real-Time Systems**	**33**
4-1.	Is SCADA Real-Time?	34
4-2.	Continuous Process Control	36
4-3.	Communications Access and "Master-Slave"	39
4-4.	Determining Scan Interval	40
4-5.	Where to Compute?	43
	Unit 4 Exercises	47
UNIT 5	**Control System Elements: Sensors, Actuators, and Algorithms**	**51**
5-1.	A Forgotten Cost	52
5-2.	Special Considerations	58
5-3.	Standardization	60
5-4.	Maintenance	61
5-5.	Local Controllers	62
5-6.	Controllers in RTUs	65
	Unit 5 Exercises	67
UNIT 6	**Field/RTU Communications**	**71**
6-1.	Three Rules of Communication	71
6-2.	Analog Pneumatic and Hydraulic Signals	73
6-3.	Analog Electronic Controllers	74
6-4.	Digital Electrical Communication	77
6-5.	How Digital Works—Analog to Binary to Digital	78
6-6.	Parallel or Serial?	84

The Integration Group of The Americas Ex. 1007-Page 4
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001057

6-7. Communication Topology 85
6-8. Fieldbus and Similar Standards 86
Unit 6 Exercises 87

UNIT 7 **Remote Terminal Units—RTUs 91**
7-1. What Does an RTU Do? 91
7-2. Communications Interface 92
7-3. Protocol Detailed 93
7-4. Discrete Control 97
7-5. Analog Control 98
7-6. Pulse Control 100
7-7. Serial Control 101
7-8. Monitor Discrete Signals 101
7-9. Monitor Pulse Count Signals 102
7-10. Monitor Serial Signals 104
7-11. Non-RTU Functions 105
7-12. RTU Hardware Choices 105
Unit 7 Exercises 105

UNIT 8 **RTU/MTU Communication 109**
8-1. Communications System Components 109
8-2. Protocol 110
8-3. Modems 113
8-4. Synchronous or Asynchronous? 119
8-5. Telephone Cable or Radio? 119
8-6. Simplex or Duplex? 121
8-7. Turn-On Time 123
8-8. Frequencies: Are They Available? 127
8-9. Path Studies and Seasonal Variations 129
8-10. Solar Variations 130
8-11. Reliability and Maintenance 130
8-12. Satellite Communications 131
8-13. Cell Phones 132
8.14 Internet SCADA 132
Unit 8 Exercises 133

UNIT 9 **Master Terminal Units—MTUs 137**
9-1. Communications Interface 137
9-2. Configuring a Picture of the Process 138
9-3. Some Simple Applications 144
9-4. Data Storage 147
Unit 9 Exercises 148

UNIT 10 **Operator Interface 153**
10-1. Operator Interface on Very Small Systems 154
10-2. Operator Interface on Mid-sized Systems 154
10-3. Operator Interface on Large Systems 156
10-4. Local Security Considerations 156
10-5. Monitor Status Points 156
10-6. Monitoring Alarms 157
10-7. Totalized Values and Trending 161
10-8. Control Interfacing 162
10-9. Reports 163

The Integration Group of The Americas Ex. 1007-Page 5
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001058

Unit 10 Exercises 164

UNIT 11 **Remote Control—What Not to SCADA 167**
11-1. Murphy's Law and Remote Control 167
11-2. Safety Instrumented Systems 168
11-3. Regulatory Requirements 172
Unit 11 Exercises 175

UNIT 12 **Security 179**
12-1. What Is the Risk? 179
12-2. Risk Evaluation Procedures 181
12-3. Risk Mitigation 182
12-4. Document and Follow-Up 185
Unit 12 Exercises 185

UNIT 13 **Applications 189**
13-1. Real Time Revisited 189
13-2. Accounting and Quality of Data 192
13-3. Scanning and Communications 196
13-4. Automatic or Remote Control 199
13-5. Advisory Applications 200
Unit 13 Exercises 201

UNIT 14 **What's Next? 205**
14-1. Communications Technology—Field Data 205
14-2. Communications Technology—RTU/MTU 207
14-3. Reductions in SCADA/Enterprise Communications 207
14-4. More Fully Automatic Applications 208
Unit 14 Exercises 208

UNIT 15 **SCADA Economics 213**
15-1. Costs versus Benefits 213
15-2. The Time Value of Money 214
15-3. Capital Costs 216
15-4. Training and Maintenance Costs 218
15-5. SCADA Operating Costs 219
15-6. Benefits: Reduced Capital Costs 219
15-7. Benefits: Reduced Operating Costs 220
15-8. Benefits: Improved Facility Effectiveness 221
15-9. Tax Implications 221
Unit 15 Exercises 222

APPENDIX A **Suggested Readings and Study Materials 225**

APPENDIX B **Glossary of SCADA Terminology 229**

APPENDIX C **Solutions to All Unit Exercises 237**

Index 255

The Integration Group of The Americas Ex. 1007-Page 6
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001059

Preface to the Fourth Edition

The first three editions of this book were written with the intent that they be an introduction to SCADA. These three editions formed the basis of a series of courses, from one-half day to as much as five days in length. As time went by, we found that more and more class-generated questions could not be answered by a reference to the text. This edition provides a basic description of SCADA while also including some side paths that will clarify why things in modern SCADA are done the way they are.

When Edition One was written, times were simpler, both in terms of technology and in terms of the sophistication of computer hacking. At the time, nearly all SCADA systems were developed on the basis of a Master-Slave communication system, with the communication paths owned by the process owner. Now, communication utilities own most of the data paths. This leads to the potential for people other than the intended recipients to view the information on the system. As SCADA has become easier to design and install, companies have applied it to more and more processes, often without proper consideration for security. When a SCADA system was limited to shutting the valves on a small oil pipeline across a river, not much could go wrong if the system was ordered to close by a teenager from his bedroom computer. Now that international electric power transmission grids are operated by SCADA, millions—and perhaps billions—of dollars of damage may be generated by malicious hacker activity.

For these reasons, the sections dealing with communications and security have been expanded in this Fourth Edition. Since both of these technologies are so large, some references have been included to direct readers to the additional information that cannot be included in this one text.

Comments on this volume

This volume is organized into units, each of which deals with some limited aspect of SCADA. It should be possible to learn much about SCADA concepts without needing to refer to other books. If you engage in system design, you will need to refer to vendor information detailing the specific equipment that you will evaluate for use.

Consideration was given to including a Glossary of Terms early in the book, because there are some terms that are unique to SCADA or that take on a slightly different meaning when used in SCADA systems than they do in other technologies. We have found that this is not an effective way to learn new technical terms; consequently, each technical term that may be

The Integration Group of The Americas Ex. 1007-Page 7
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001060

new is described as it appears. In addition, there is a short Glossary in Appendix B near the end of the text.

Because examples and exercises have been proven to be an effective way to increase the amount of new material that can be learned, there are examples throughout the text and, at the end of each unit, there is a selection of questions (with answers in Appendix C) for the student to use to check his or her understanding of a topic.

The technology called SCADA has developed over the last forty years (since about the mid-1960s). It is a collection of separate technologies, including process instrumentation, various communication methods, and computer applications. Every once in a while, someone figures out a better way to do one or more of the things that are included in SCADA, and we see the entire technology move in a different direction. Even so, it is safe to say that SCADA is a mature technology.

Dedication

I dedicate this book to Linda, who has provided both practical and moral support in its development even though—or perhaps because—neither of us understood at the beginning how much work would be involved.

Stuart A. Boyer, P. Eng.
Life Member ISA,
Life Member APEGGA

The Integration Group of The Americas Ex. 1007-Page 8
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001061

Unit 1: Introduction and Overview

The Integration Group of The Americas Ex. 1007-Page 9
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001062

UNIT 1

Introduction and Overview

Welcome to the ISA's text on SCADA, Supervisory Control And Data Acquisition. This unit provides an overview of the book and the information you will need for independent study.

Learning Objectives—When you have completed this unit you should:

A. Understand the general organization of the material in this course.

B. Know the course objectives.

1-1. Text Coverage

This text provides introductory technical material about SCADA systems. It addresses the basic layout of SCADA systems and the parameters for system selection. Communications and the basic building blocks of SCADA systems are dealt with in some detail. System security methods and the need for security are considered. Applications examples are provided and discussed. Economic evaluations are mentioned.

No recommendations about specific equipment types or methods are provided; however, techniques that will help the reader to make such selections are included.

1-2. Purpose

The purpose of this text is to introduce the student to the basics of SCADA by providing overviews of relevant topics where appropriate and details where necessary. SCADA consists of the elements of several different technologies and it is sometimes difficult to know where to stop when describing some of these technologies. The text will focus on such technologies to the extent that doing so makes SCADA more understandable. This text will also attempt to identify major differences between the SCADA systems of different industries, but because the basics of SCADA are much the same from one industry to another, examples from many industries have been included throughout the text.

1-3. Audience and Prerequisites

This text is designed for those who wish to learn the basics of SCADA by themselves at their own pace. It will be useful to managers, supervisors, engineers, operators, and technicians who contemplate coming in contact

The Integration Group of The Americas Ex. 1007-Page 10
SitePro, Inc. v. WaterBridge Resources LLC, et al.

WB_00001063

with SCADA systems. It will also be useful to students of technical schools and colleges as an introduction to the subject. For any technical people who have a personal interest in the subject, it should serve as a source of overview information about SCADA.

1-4. Study Materials

This text is the only required study material for learning the basics of the subject. For those who want or need to learn additional details about some aspects of the subject, Appendix A provides a comprehensive list of readings and other study material.

1-5. Organization and Sequence

This text is divided into fifteen separate units. Unit 2 is an overview of SCADA that provides some definitions and describes elements and some of the limits of SCADA systems. It will focus the student's attention on those factors that make SCADA what it is.

Unit 3 provides a sketch of the technology and defines it in the context of related technologies. Unit 3 also discusses analog and digital measurement and nomenclature.

Unit 4 considers the effect of time on a SCADA system. Certain functions must be completed before other functions are started. In addition, a definition of Real-Time Systems is discussed and methods of calculating scan times are introduced.

Unit 5 talks about control system elements. Sensors, used to measure what the process or equipment is doing; and actuators, used to make changes to the process, are introduced in this unit. Control algorithms are discussed to the extent needed for an understanding of how they can be used in SCADA.

Unit 6 addresses the specific needs of communication between field sensors/actuators and RTUs.

Unit 7 is about one of the main pieces of hardware unique to SCADA systems, the Remote Terminal Unit (RTU). The necessary functionality of RTUs is described, and several hardware methods to achieve this functionality are presented.

Of course, for a SCADA system to work, the RTUs must also be able to communicate with Master Terminal Units. Unit 8 discusses how this happens and the problems that must be defeated for this to happen. Developments in this form of communication are among the things

The Integration Group of The Americas Ex. 1007-Page 11
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001064

affecting the way SCADA systems are now being designed and built. This is the unit where protocols are detailed.

Master terminal units, the other equipment unique to SCADA, are explained in Unit 9. Their functionality, layouts, and particular requirements are discussed in some detail in this unit.

Unit 10 discusses methods of communication between the system and the human operator. Because SCADA systems are often being integrated into corporate enterprise systems, Unit 10 also discusses some advantages and disadvantages of doing so.

Unit 11 considers whether SCADA is a remote control system or an automatic control system. This unit will also offer some suggestions about system reliability and how the lack of reliability should affect the way you apply the system.

Security is the subject of Unit 12. Early SCADA systems paid scant attention to this aspect of design. Modern systems pay more attention to this feature. Additionally, methods of improving security are being developed that will result in very secure control and monitoring of the process.

Unit 13 provides a list of applications that are being used by companies now. You may come across an application for your company that you had not thought of, or you may feel that your design is complete if you do not find an application that you have not already included.

Unit 14 outlines some of the directions in which SCADA may move in the near future. As technologies improve, these improvements may be harnessed to push or pull SCADA in different directions.

Unit 15 discusses the economics that must be considered when justifying a SCADA project. The concept of present value is introduced.

Appendix A provides a bibliography of books that the author used in developing this text. Referring to these sources will allow additional information to be gathered to the extent that the reader is interested.

Appendix B provides a glossary of terms from SCADA technology—of course, no such list can be complete. Since SCADA development dates from the time NASA was very active in space exploration, their love affair with acronyms has carried over to SCADA.

Appendix C provides solutions to the exercises that form the last part of each unit. It has been found that the learning process is enhanced by applying what has just been learned to solving a problem using this new

The Integration Group of The Americas Ex. 1007-Page 12

WB_00001065

knowledge. The reader is encouraged to work these exercises as he or she goes through the book.

Appendix D, the Index, allows the reader to search for instances of particular words throughout the text.

1-6. Course Objectives

When you have completed this text, you should be able to:

- Converse with SCADA nomenclature
- Describe the typical architecture of a SCADA system
- Identify the limitations of a SCADA system
- Describe the basic technology of each of SCADA's major building blocks
- Recognize when a SCADA system would be beneficial to your operation
- Select the appropriate SCADA technologies for your operational requirements

In addition to these general objectives, each unit contains a specific set of learning objectives to help direct your study in that unit.

1-7. Course Length

The basic idea of this book is that students learn best if they proceed at their own pace; consequently, the amount of time individual students will require to complete this text/course will vary significantly. Most students will complete this course in eighteen hours.

The Integration Group of The Americas Ex. 1007-Page 13
SitePro, Inc. v. WaterBridge Resources, LLC, et al

WB_00001066

Unit 2: SCADA – Purpose, Elements, and Layout

The Integration Group of The Americas Ex. 1007-Page 14
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00720 U.S. Patent No. 9,512,978

WB_00001067

UNIT 2

SCADA – Purpose, Elements, and Layout

SCADA is the technology that enables a user to collect data from one or more distant facilities and to send limited control instructions to those facilities. It is important to note the words "distant" and "limited" in this definition.

SCADA has been developed to monitor and control very large process facilities. SCADA is not normally used to operate a small facility like a factory; although, some factories are large enough to benefit from using SCADA. Control systems like programmable logic controllers (PLC) or distributed control systems (DCS) will do a better job for most factory control and monitoring. An example of a very large process facility is a group of wells that produce and gather the oil and gas from a reservoir beneath fifteen square kilometers (3,700 acres) of farmland or forest. Another example is a transmission system, including wires, switches, and transformers, that moves electrical power across entire states, provinces, or countries.

Note also that the definition does not say, "Control and Data Acquisition." It says "Supervisory Control and Data Acquisition." A good supervisor, one who does not micromanage, gives a target to his workers and lets them get on with the job, monitoring them occasionally. A supervisory control system sends a process target to parts of the system, lets those parts attain the target, and monitors them to ensure that the targets are being reached.

Whenever a definition is written down, it is like a challenge to the reader to think of exceptions. Someone might say, "I know of a factory where SCADA is used to measure a flow rate," or "Our SCADA system does detailed, not supervisory, control." Please accept the definition as given, at least until you finish reading this text. It may be that you will reconsider your argument. It may also be that you will find that your system is not really a SCADA system, but is a large DCS.

This unit discusses some of the purposes that a SCADA system can be put to, introduces the elements that comprise such a system, and illustrates layouts that are common to SCADA systems.

The Integration Group of The Americas Ex. 1007-Page 15
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001068

Learning Objectives—When you have completed this unit you should:

A. **Have a general understanding of what processes SCADA systems may be applied to**

B. **Understand the benefits that you should expect from applying a SCADA system to your process**

C. **Recognize the various elements that make up a SCADA system**

D. **Know why communication paths have such a big influence on the physical layout of a SCADA system**

E. **Be able to lay out a typical SCADA system**

2-1. Purpose of a SCADA System

SCADA allows a human operator, in a location central to a widely distributed process—such as a pipeline system, oil or gas field, hydroelectric generating complex, or irrigation network—to make set point changes on distant process controllers, to open or close valves or switches, to monitor alarms, and to gather measurement information. When the dimensions of the process become very large, hundreds or even thousands of kilometers from one end to the other, one can appreciate the benefits that such a system offers in terms of reducing the cost of routine visits to monitor and control that process. The benefits grow if elements of the process are not only distant, but physically difficult to reach, perhaps requiring a helicopter or other special transportation. Once the benefits of a SCADA system are recognized, improved control methods can be utilized to operate the facility more efficiently and safely than could be done without the system.

2-2. Applicable Processes

SCADA technology is best applied to processes that are spread over large areas; are relatively simple to control and monitor; and require frequent, regular, or immediate intervention. The following examples should help you visualize the range of applicable processes that SCADA is suitable for:

A. Groups of small hydroelectric generating stations which are turned on or off in response to customer demand and are usually located in remote locations. They can be controlled easily by opening or closing valves to feed water to turbines. They need to respond quickly to changes in demand and must be monitored continuously.

WB_00001069

B. Oil or gas production facilities—including wells, gathering pipelines, fluid measurement equipment, and pumps—are usually spread over large areas, require relatively simple controls such as turning motors on and off, need to gather fluid metering information regularly, and must respond quickly to conditions in the rest of the field.

C. Pipelines for gas, oil, chemicals, or water have elements located at various distances from a central control point that can be controlled by opening or closing valves or starting and stopping compressors or pumps, and must be capable of responding quickly to market conditions and leaks of dangerous or environmentally sensitive materials.

D. Electric transmission systems may cover thousands of square kilometers, can be controlled by opening or closing switches, and must respond almost instantly to load changes on the lines.

E. Irrigation systems often cover hundreds of square kilometers, can be controlled by opening and closing simple valves, and require meter data gathering to allow proper billing for the water supplied to customers.

F. At a heavy oil upgrader, controlled by a distributed control system, there are several surface water pumping stations. It is necessary to monitor the water levels as well as to turn the pumps on or off in response to tank levels in the upgrader. The pumps are located far enough away from the control room that it would be very expensive to install dedicated data cables.

These examples are just that—examples. SCADA has been successfully applied to each of these types of processes, as well as many others. The types of control illustrated in these examples may give the mistaken impression that SCADA is not suitable for more complex control. As we will describe later, the complexity of remote control that is possible with SCADA has grown as the technology has matured.

Typical signals gathered from remote locations include status indications, alarms, analog values, and totalized meter values. This seems like a small list of simple options, but a vast range of information can be gathered with this apparently limited menu of available signal types.

Signals sent from the SCADA system's central location to the remote sites are usually limited to discrete binary bit changes or to analog values addressed to a device at the process. An example of a binary bit change could be an instruction to a motor to change from OFF to ON. An example of an analog value is an instruction to a valve controller to change the valve set point from 60% open to 70% open. Given simple signal types like these and a lot of imagination, nearly any control change may be effected.

The Integration Group of The Americas Ex. 1007-Page 17
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001070

2-3. Elements of a SCADA System

Figure 2-1 shows the major elements of a SCADA system. At the center is the operator, who interfaces with the system through some form of input/output (I/O) device. The I/O device in turn communicates with the master terminal unit (MTU). The MTU communicates with one or more remote terminal units (RTUs), each of which communicates with sensors or actuators at the process. In addition to these major elements, the drawing shows several other boxes identified as modems and radio. Each of these elements will be briefly described in this section so that you will be able to follow the discussion, and will be dealt with in more detail later in the units dedicated to MTUs, RTUs, and communications.

The two purposes of a SCADA system are to extend the operator's ability to see what is happening in the process and to extend the operator's ability to make changes to the process. When the process is very small and simple, the operator may be able to directly see what is happening and to reach out to make the needed change with his or her own hand. When the process gets a bit larger, that becomes impossible; however, it may still be practical to have a wire connection from each sensor to a light located near the operator and a wire from a switch near the operator to the motor or valve that the operator needs to adjust to make the process work properly. As the process increases in size even more, the signals to and from the operator start to degrade and the cost of running dedicated wires for each element becomes prohibitive. The operator must still know what is happening in the process and he or she must still be able to make the changes to the process.

The master terminal unit is the system controller. Some industries use the term "host computer," "host controller," or "server," but for the rest of this book we will refer to this device as the MTU. In modern SCADA systems, MTUs are always based on a computer. With appropriate software, the MTU can monitor and control the process even when the operator is not present. It does this by means of a built-in scheduler, programmed to repeat instructions at set intervals. For example, the MTU may be scheduled to request an update from each RTU every six minutes. The operator's I/O, and the SCADA system generally, must be a two-way device. Just as a SCADA system is not just a telemetry system gathering data from the field and presenting it to the operator, the I/O must not be limited to presenting data to the operator. It must also be capable of receiving instructions from the operator and passing them on to the process. Presentation to the operator from the system is normally done by means of graphic or textual information on a CRT or LCD screen. For very simple systems, lights or annunciator windows may suffice for telling the operator about the process. For many systems, audible signals may be used to reinforce certain types of messages in order to ensure that the

The Integration Group of The Americas Ex. 1007-Page 18
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001071

operator is quickly made aware of the situation. Presentation to the system is normally done through a computer keyboard, although pointing devices like touch screens and mice are also popular. For very basic systems, a set of simple electrical switches may suffice.

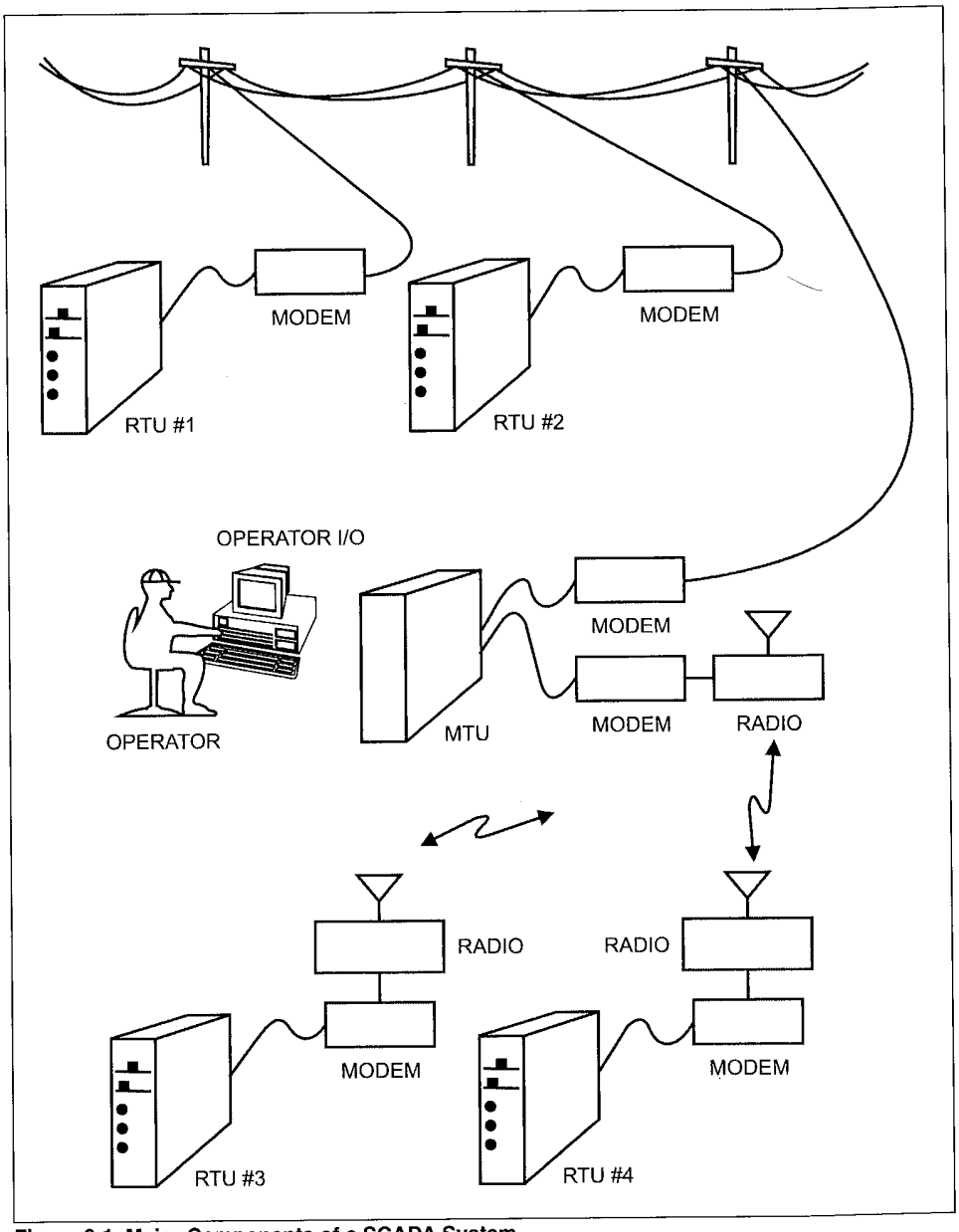


Figure 2-1. Major Components of a SCADA System

Normally, the MTU will have auxiliary devices like printers, backup memories, and audible alarms attached to it. These devices are considered to be part of the MTU. In many applications, the MTU is required to send accounting information to other computers or management information to corporate enterprise systems. These connections may be by dedicated cable between the MTU and the other computers, but newer SCADA systems are more likely to use local area network (LAN) drops for this communication. These other computers are not considered to be a part of the MTU or the SCADA system. In many SCADA systems, the MTU is required to receive information from other computers. This is often how applications programs, operating on other computers and connected to the MTU, provide a form of supervisory control over SCADA. These applications may or may not be on computers that are considered part of the MTU. Detailed descriptions of MTU functions will be found in Unit 9.

In a large process where the operator is located in a comfortable control room, anything outside and far away, such as the process, is considered to be remote. The operator, through the MTU, must communicate with the process; and to facilitate this, SCADA systems provide remote terminal units or RTUs. A SCADA system may have as few as one RTU or as many as several thousand RTUs. An RTU has two major functions. First, it must provide an ability to communicate with the MTU. Second, it must provide an ability to communicate with each of the field sensors and actuators that is connected to it. At one time, RTUs were custom designed electronic panels weighing several hundred pounds and requiring delivery lead times of several months. Now they are normally computer based, flexible, and off-the-shelf.

For the RTU to communicate with the MTU, it must recognize that the MTU wants to talk to it; must decode the message sent by the MTU; must act on the message, perhaps by composing and sending an answer to the MTU; and must shift back to listening for additional messages from the MTU. Acting on the message may be a complex operation. It may require checking the existing position of a particular field device, comparing the existing position to the MTU's required new position, sending an electrical signal to an actuator to move the device to the required position, checking a set of field sensors to ensure that the device has moved to the appropriate position, and then sending a message back to the MTU to confirm that the new condition has been reached. Because of this complexity, modern RTUs are computer based.

The RTU also communicates with sensors that measure field equipment conditions and with actuators that change field equipment conditions (see Figure 2-2). To do this, the RTU must know which language, or protocol, each field device uses. It must know the name, or address, of each field device. If it is to gather information from field devices, it must know

The Integration Group of The Americas Ex. 1007-Page 20
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001073

where to store the information so that it will be able to send the information onward when told to do so by the MTU.

At one time, RTUs did not do much besides that just described. When computers became the preferred frame for RTUs, designers decided to include other functions in the RTU. Now, functions like fluid flow totalizing, interactive valve positioning, control functionality, and pipeline pig sending control may be included in the RTU.

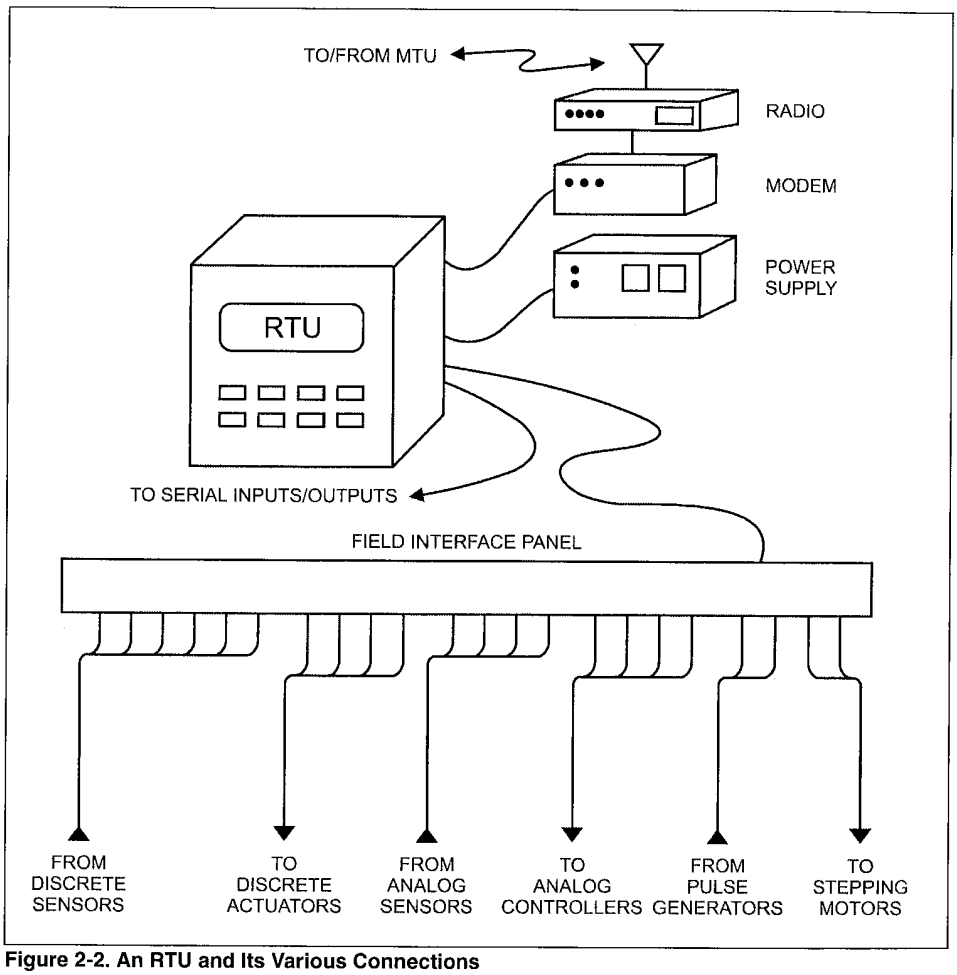


Figure 2-2. An RTU and Its Various Connections

Connections between the RTU and the field devices are most often made with electrical conductors—that is, wires. Usually the RTU supplies the electrical power for both sensors and low power actuators. Depending on the process, reliability requirements may necessitate that an uninterruptible power supply (UPS) be used to ensure that failures of the electric utility do not result in process or safety upsets.

The Integration Group of The Americas Ex. 1007-Page 21
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001074

Just as the MTU scans each RTU, the RTU scans each of the sensors and actuators that are wired to it; however, the RTU's scanning is done at a much higher rate than the scanning done by the MTU.

RTUs will be discussed in some detail in Unit 7.

Communication between the MTU and its RTUs will probably take place over one of two media: radio or land line. The media may be owned by the SCADA system owner or it may be leased from a telephone utility. In either case, because electrical signals deteriorate when transmitted over long distances, a MODEM, which MOdulates the electrical signal onto a carrier wave at the sending end and DEModulates it from the carrier wave at the receiving end, is required.

Some SCADA systems may use both radio and land lines for communication. One of the distinguishing features of SCADA systems is that their processes tend to be simple. For that reason, the amount of data that needs to be moved over a SCADA communication system tends to be small; consequently, the data rate at which SCADA modems need to work is small. Often, 300 bits per second is sufficient. Seldom is more than 1200 bits per second needed.

Details of SCADA communication will be discussed in Unit 8.

Field devices and the wiring connecting them to the RTU form a very important and often overlooked part of the system. As noted earlier, field devices include sensors that tell the system what is happening to the process and actuators that change some of the basics of the process. The purchase, installation, and wiring of these devices forms a large part of both the design and construction costs of a SCADA system.

Details of field devices and their wiring will be discussed in Unit 5.

2-4. SCADA Layout

The layout selected for connecting one MTU, a communications system, and a group of RTUs to form a SCADA system will depend on the shape of the process to be controlled and on whether there is existing communications infrastructure.

In the very simplest of systems, like a water supply well near a small town, for example, the MTU is likely to be put in the town maintenance office; the RTU will be at the pump/well; and the communication equipment, probably a simple dedicated radio, will have equipment at both sites.

The Integration Group of The Americas Ex. 1007-Page 22
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001075

For a more complex system, like an oilfield with free flowing and pumped wells, water injection pumps, and separation facilities, the MTU will probably be located at the field operations office; RTUs will be located at the separation facilities and injection pump stations; and the communications equipment, either a dedicated radio system or a cell phone network, will be distributed throughout the area. If the equipment is a dedicated radio system, it will include a radio at the MTU and at each of the RTUs and may include one or more repeater radios.

A large pipeline facility is likely to have the MTU located at the pipeline corporate office. Sub-MTUs will be located at major operations or maintenance centers along the line. RTUs will be located at pumping or compression stations, as well as at metering stations where product is added to or removed from the pipeline. Communications may be owner supplied, but will probably include some communications utility equipment, including satellite stations, buried optical fiber cable, and copper telephone cable.

2-5. A Limited Two-Way System

Although SCADA is somewhat limited in its ability to control functions within the process, it is its supervisory control functionality that makes SCADA different from a telemetry (one-way data transmission) system. SCADA is a two-way system.

On the other hand, it is the fact that its control ability is limited that makes SCADA different from most other control systems, such as distributed control systems (DCS). Some recent technical articles have projected that as communication achieves higher bandwidth and better reliability, the control systems will become continuous and broader. They will, but then the systems will not be SCADA. They will be very large DCS.

Unit 2 Exercises:

2-1. *What factor makes SCADA different from other control and monitoring systems?*

2-2. *Most SCADA systems have communication systems that operate between the MTU and the RTU(s) at relatively low data rates. How does the system get away with this and how does it affect the selection of communications equipment?*

2-3. *What are the three primary subsystems of a SCADA system? Are there other parts in a SCADA system?*

2-4. *Two communications media are used frequently in SCADA systems. What are they?*

The Integration Group of The Americas Ex. 1007-Page 23
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001076

2-5. *What three characteristics of processes make them potential candidates for SCADA?*

2-6. *In a process, the temperature of a heated liquid, the status of an open/closed ball valve, and the number of cubic meters of gas that have passed through a meter must be gathered. Which of these parameters can be gathered by a SCADA system?*

2-7. *From where do the process sensors receive their electrical energy?*

2-8. *Why is an uninterruptible power supply (UPS) needed at an RTU site?*

The Integration Group of The Americas Ex. 1007-Page 24
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001077

Unit 3: Historical Development Analog and Digital

The Integration Group of The Americas Ex. 1007-Page 25
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001078

UNIT 3

Historical Development—Analog and Digital

When we try to learn a new subject, it is usually helpful to become acquainted with at least a small amount of its history. This enables us to place new information into a familiar context. Knowing something about a subject's history also allows us to understand that subject in terms of its development over time. The better we can relate to the subject, the "friendlier" that subject becomes.

The early days of SCADA coincided with the development of electronics. This was driven largely as a tool in the exploration of space. It turned out to be useful in the control of more mundane processes, but also applied to industrial control. Originally, electronics was an analog technology; but shortly before SCADA needed the complexity that analog would have had difficulty providing, digital technology began to appear. It was embraced at the beginning of SCADA.

Learning Objectives—When you have completed this unit you should:

A. Understand the differences among analog, discrete, and digital signals.

B. Know what precursor technologies contributed to SCADA.

C. Recognize how technical development of radios, instruments, and computers have changed SCADA in the past, and how further changes are likely to change SCADA in the future.

D. Have some appreciation for how old SCADA is as a technology.

3-1. Analog Signals, Measurement, and Control

You will read several times throughout this book that SCADA is a tool that is used to extend the ability of the process operator to learn what is happening in the process and to extend the ability of the process operator to control what is happening in the process. So what would the operator do if he or she were right there at the process?

When processes were very simple and instrumentation had not yet been developed, the operator would stand next to a piece of process equipment, such as a tank, and watch the level of liquid in the tank. As the tank filled up, the operator would either reduce the rate of liquid flow into the tank or increase the rate of liquid flow out of the tank. The technology can be thought of as analog. A full tank is one that is 100% full. An empty tank is

The Integration Group of The Americas Ex. 1007-Page 26
SiteFlo, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001079

one that is 0% full. The tank can be at any percent of fullness between these two limits. With time and experience, the operator would learn that there is a "best level" at which to try to keep the tank. That best level came to be known as the "set point." The operator would manually adjust the level to that point and then could relax for a while.

Soon, his supervisor would notice that an experienced operator was relaxing more than he was adjusting. The supervisor could then assign one experienced operator to control two tanks, as long as they were fairly close together. If a float assembly were now put in each tank so that a rod would rise above the tank top as the liquid level increased in the tank, then the operator could know how high the liquid was without actually needing to see the liquid. He would be looking at an analog of the liquid. If these rods were situated so that the operator could see two or three of them from one spot, he would be getting an analog signal from each of the tanks under his control. The efficiency of the operator had been improved with no reduction in his reliability.

After the first such conceptual success, many more would have followed, with temperature, pressure, and speed as the early parameters measured. In each of these cases, the early instruments had a readout that had an analog basis. Temperature showed as a column of mercury or colored alcohol that increased in height as the temperature increased. Pressure and speed showed as a needle that moved in a clockwise direction as the parameter increased, and moved counter-clockwise as the parameter decreased.

Similarly, controls that the operator had to adjust were originally valves, brakes, and throttles. Some would be recognizable to us, but most had levers as handles instead of wheels. The same range, 0% to 100%, was available and manual operation was the only option. So controls as well as measurements retained the same form for the parameter being manipulated.

3-2. Discrete Signals, Measurement, and Control

A certain class of process signals is simpler than analog signals. They are called discrete signals. They are separate and distinct, although they may be thought of as the 0% or 100% points of an analog signal. Do not confuse digital signals, which can impart as much information as an analog signal, with discrete signals, which describe only the end points. For a valve, two discrete signals would be "closed" or "open." For a motor, two discrete signals would be "off" or "on." For a fire alarm, two discrete signals would be "fire" or "no fire."

The Integration Group of The Americas Ex. 1007-Page 27
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001080

Historically, this type of signal was probably used at least as often as analog. The operator would have responded in the same way to a discrete signal that indicated "Level Alarm High" as he or she would have to an analog signal that indicated "80% Full." Also, the instrument to measure a discrete signal is a bit easier to build and install than the instrument to measure an analog signal.

You would think that with access to both discrete and analog signals, nothing else would be needed to completely measure and control a process. At one time, you would have been correct. Discrete sensors (such as limit switches) were and still are wired into control and safety circuits to start or stop motors when process conditions warrant. Mechanical and pneumatic controllers have been developed to recognize that an analog process parameter is higher or lower than it should be and to increase or decrease an analog control to correct that error. These analog controllers often use cams, wheels, and levers to perform the control algorithm.

Success in the development of electronics, initially analog electronics, encouraged process control vendors to develop electronic control devices. These tended to allow much more flexibility than mechanical units. Now more parameters of control could be adjusted. Repeatability was better, and the fact that these changes, including changes of set point, were now adjustable electrically meant that the operator could make the adjustments remotely. This led to moving the operator to a central location where he or she could monitor many controllers without having to move through the plant. When this became the normal thing to do in a new plant, more and more attention was paid to the comfort of the operator. Control rooms were built with air conditioning, heating, and humidity control. Sometimes this was done to make the operator more comfortable; sometimes it was done to make the control equipment more comfortable.

At about the same time as all of this was happening, the race to the moon, between the United States and the Soviet Union, resulted in the development of several different technologies, two of which (radio communication and digital electronics) are of great interest in SCADA development. In a later unit, we will discuss the effects that improvements in radio communication had on SCADA. For now, it is important for you to know that digital electronics received a major boost during this period. In the late 1960s, geophysical prospecting started adapting digital electronics for recording seismic signals. Shortly after that, oil and gas production equipment started applying digital amplifiers and controllers. In the same way that electronic controllers were more flexible than mechanical or pneumatic controllers, digital controllers, which could be programmed, were much more flexible than analog electronic ones.

The Integration Group of The Americas Ex. 1007-Page 28
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001081

It was important that process control engineers learned about digital signaling. It would have been possible to transmit analog values over long distances, but it would have been much slower than using digital values—and there was no means of ensuring that the analog values had been transmitted without error. As we shall see in Unit 8, digital communication techniques do allow this valuable capability. For this and other reasons, for SCADA systems most of the traffic between the remote terminal units and the master terminal unit is now carried by radio with digital encoding of the data.

3-3. Development from Telemetry

In the first two-thirds of the twentieth century, the engineering development of aircraft and rockets, as well as the investigation of weather and other geophysical phenomena, required that simple pieces of data be gathered from equipment located where it was either difficult or impossible to place observers. For example, in earlier days of experimental aviation, aircraft had space for a pilot but little room left over for design and testing engineers to accompany the flight and monitor the hundreds of sensors installed to evaluate stresses and strains on the airframe and engine. These were the early days of telemetry, a one-way communication system designed to gather information.

Similarly, early rockets did not even have room for a pilot; and, because all early rocket trips ended very suddenly, it would have been difficult in any case to get engineers or technologists to volunteer to ride along to read the instruments! The fact that most of these early trips not only ended suddenly, but much sooner than scheduled, made it doubly necessary to find a way to get the flight information while it was still available.

From the time technology was first applied to predicting weather, scientists realized that large masses of data would be required to make accurate forecasts. But only a very small amount of this data was available where people were generally located. Remote post offices and lighthouses, ships and specially established weather stations could be manned and could transmit the data to a central location, either by telephone, telegraph, or radio. But that only accounted for surface information, and weather is composed of much more than just surface effects. To get a better handle on weather, scientists thought that developing profiles of weather information up through the atmosphere would be helpful. Small balloons were affordable. Small instruments could be mounted on them to measure the parameters of interest and provide the desired information. But how should that information be gathered?

The Integration Group of The Americas Ex. 1007-Page 29
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001082

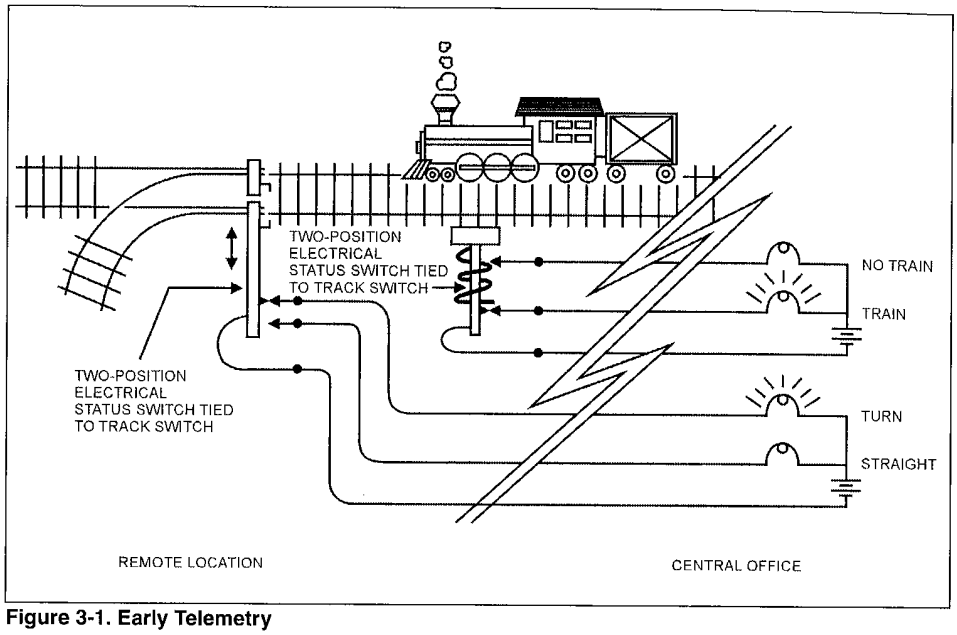


Figure 3-1. Early Telemetry

3-4. Dependence on Communication and Computers

The answer to this question emerged from a communications method that was being used in another industry to alleviate a safety concern. For some time, rail systems had used wire communications to monitor the position of their rolling stock and the status of switches that controlled on which tracks the trains travelled. Figure 3-1 shows how this was accomplished using electric switches, wire, and status lights. Early railroad right-of-ways usually included elevated telegraph wires, in much the same way that modern utility right-of-ways include pipelines, power lines, and communication cables. Very long distances required signal repeaters to be inserted into these telegraph wires at frequent intervals. This communication system, called telemetry, allowed a central office to monitor things that were happening at distant locations and enabled controllers to efficiently and safely schedule the trains. Instructions to manually change the position of the track switches would be sent by telegraph to operators. The system was, of course, limited to fixed facilities where wires could be laid between the source of the signal and the central monitoring office; but, where these conditions applied, telemetry worked well. Systems of this kind are still in use.

At about the same time that the need arose to maintain communications with moving facilities, radio technology was also advancing. As long as one did not expect to get too much information, radio could send it. And as long as the radio did not have to transmit for too long a time, its battery could be small enough to be practical. Thus the technology of radio

The Integration Group of The Americas Ex. 1007-Page 30
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001083

telemetry was born. Figure 3-2 outlines how a temperature sensor and a barometer could be tied to a radio to provide information about temperature versus altitude.

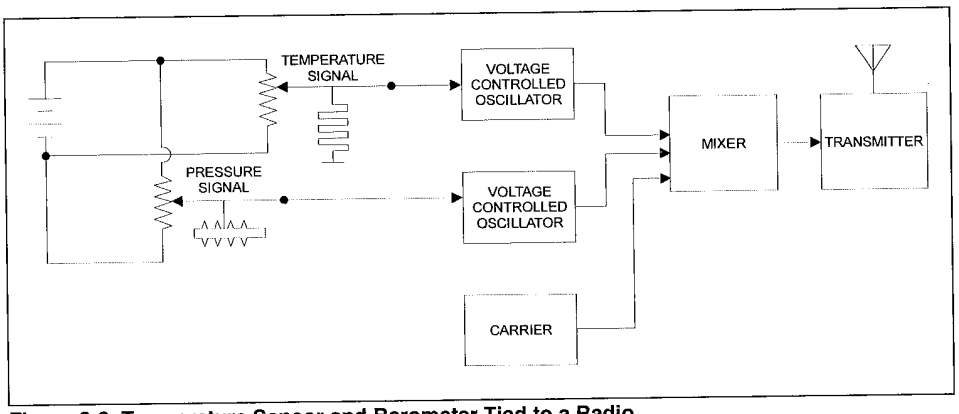


Figure 3-2. Temperature Sensor and Barometer Tied to a Radio

Radio telemetry evolved over time by improving the reliability of the radio system, by increasing the density of the data that could be transmitted, by developing error-detecting and even error-correcting codes, and by miniaturizing the equipment. But throughout this evolution, radio telemetry maintained its one-way nature. Data was gathered from the remote site and transmitted to a central location. No radio signals were sent from the central location to the remote site.

Hardwired telemetry also matured during this period. Rather than concentrating on improving the reliability or the size of the equipment, the railroad engineers who worked with wire telemetry devices developed the concept of two-way communication to allow efficient remote control. This allowed the train track switches not only to be monitored from a distance but also to be adjusted from a distance. Of course, since it was real people that were riding around in these trains, the rail companies had to be very sure that the switches had moved to the correct position before a train was allowed to use the track. To do this, traffic lights near the tracks were hardwired to electric status switches on the track assemblies. Even though this system combined telemetry and remote control, it was still not SCADA because the "Supervisory" nature of the control was not in place.

Electric power utility companies and pipeline transportation companies had facilities that were comparable to those of the rail companies—large capital investments that required little in the way of complex control to operate. A major difference being that the switches and valves that had to be controlled were located at distant, inconvenient spots. Oil and gas production companies seemed to find most of their prizes in very

The Integration Group of The Americas Ex. 1007-Page 31
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001084

inhospitable, poorly developed parts of the world, in which it was difficult to get operating crews to live. All of these industries responded to the same problem with the same solution: They investigated ways of remotely monitoring and controlling simple functions by using wire-transmitted electric signals to reduce the operating costs of their facilities. By the beginning of the 1960s, remote monitoring and supervisory control of several industrial processes was a developing technology, and while in some cases the systems would now qualify as SCADA systems, the term SCADA had not yet been defined.

Scientists and technologists recognized the improvements being made in radio technology for telemetry and applied them to this new two-way remote operation. Radio had transformed the gathering of weather information from a two-dimensional to a three-dimensional technology. When radio was applied to the remote monitoring and control of processes, it transformed this technology from one-dimensional—that is along a railroad, pipeline, or electric transmission line where wires could be installed inexpensively—to two-dimensional. Radio equipment could be located almost anywhere on the surface of the Earth that it was needed.

Often, a combination of wire and radio was the most effective method for gathering and distributing signals. As radio improved, the costs of installation dropped and more facilities could pass the economic feasibility hurdle. Installing buried telephone cable in remote areas can be extremely expensive, but still less expensive than overhead wire, unless the owner already owns an overhead pole system. Radio paths are relatively immune to the intervening countryside as long as a clear line of sight exists between the transmitter and receiver. During the 1960s, radio was used more and more. By the middle of the 1970s, radio became the communication medium of choice for most newly installed telemetry systems to fixed locations, and more and more, for two-way systems.

At the same time that radio was moving into the ascendancy for communication, another electronics technology was developing. Digital computers made their debut in remote monitoring and supervision in the early 1960s. The increased flexibility that they offered was very attractive to the designers of these systems. Early on, non-computerized systems had central stations that had grown in complexity—they required up to several thousand relays. Before the advent of electronic computers, in some cases, these central stations had punched paper-tape programming. So-called mid-sized computers became available about 1965, and the stage was set for an explosion of systems that would allow massive centralizing of control. Large-scale communications, which often required leased long distance telephone lines in combination with privately owned radio systems, provided the paths to a very large number of field facilities.

The Integration Group of The Americas Ex. 1007-Page 32
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001085

Often, the entire complement of a company's field facilities would be tied into one computer that was located hundreds of miles from the operation.

It was at the beginning of the 1970s, that the term SCADA was coined and the word telemetry began to fall out of use in describing two-way systems. Radio became so much better during the 1970s, that it often replaced existing buried cable systems. Ground-dwelling rodents and backhoes couldn't do as much damage to radio signals as they could to buried cable. The stability of radio's frequency control was increased, requiring less maintenance. The reduced complexity of the equipment and the improved industrial design of radio packaging made it possible to service the equipment in the field with less-qualified technicians and less-complicated service equipment.

SCADA technology matured slowly during the late 1970s. Improvements in software resulted in better human-machine interfaces (HMI). Report writers were developed to provide the information that was wanted, when it was wanted. Systems got bigger. As was the case with most industrial technologies, the development of minicomputers had a profound effect on the development of SCADA. For one thing, smaller facilities could now be considered for remote operation. Perhaps the most profound effect, however, was that the minicomputer, which is usually the basis for the host computer or master terminal unit (MTU), became so inexpensive that it was no longer necessary to centralize the system. Of course, centralization could still be done where it made operational sense, but now, operational effectiveness rather than cost could determine where the MTU was located. Industries such as electric utilities and pipelines retained their centralized philosophy, while oil and gas production companies shifted to a more decentralized mode to put the control of the fields back in the hands of field operations specialists.

As systems proliferated, the radio spectrum became more fully utilized. Frequencies became harder and harder to get. As this was happening, other methods of radio communication were being developed, including satellite communications and cellular telephone. Peer-to-peer communications management systems, which could replace Master-Slave communications, were developed. The costs for these communications methods dropped to the point where, with a few modifications to the SCADA system, they became the technology of choice in many systems.

This is where SCADA is today. It is expected that computer and communications improvements will continue to influence the development of the technology. Local area networks (LANs), which are dedicated, high-speed methods for communicating between digital hardware, are the hot communications subject now.

The Integration Group of The Americas Ex. 1007-Page 33
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001086

Unit 3 Exercises:

3-1. *By what decade had two-way remote control and monitoring become a recognized technology?*

3-2. *Name three factors that caused radio to be preferred over land lines for two-way remote control and monitoring.*

3-3. *Flexibility and the ease with which existing systems can be modified are two reasons that electronic computers supplanted built-for-purpose central controllers. What is another reason?*

3-4. *What was the most profound effect of the development of small, inexpensive minicomputers?*

3-5. *What factor do pipelines and electric transmission systems have in common with railroads that drove them to be early users of remote monitoring and control?*

3-6. *What two things about the process operator does SCADA attempt to extend?*

3-7. *Analog signals and discrete signals are two methods for moving data to or from an operator. What is the primary difference between the two?*

The Integration Group of The Americas Ex. 1007-Page 34
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001087

Unit 4: Real-Time Systems

The Integration Group of The Americas Ex. 1007-Page 35
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001088

Unit 4

Real-Time Systems

For a long time—many years—SCADA operated independently of other computer-based systems, and the issue of synchronizing communications among different computers was unimportant. Depending on how you prefer to define "real-time," it may not have been important for SCADA to be "real-time." How should we define real-time? At one time, a sloppy definition like, "A system whose output occurs at the same time as its input is a real-time system," seemed sufficient. This definition had the advantage of simplicity, but a definition like this resulted in systems that worked reliably on slow processes and did not always work on fast systems. It was not quantitative. Most dictionary based definitions talk about "extremely fast," "virtually immediately," or something similar.

Consider the way that computers operate. The central processing unit (CPU) sits waiting for an interrupt request. That interrupt request may be generated by someone striking a keyboard key or by an external switch in a printer advising that the printer has run out of paper or by an alarm that the battery voltage is getting low. The CPU will evaluate the priority of the interrupt request and, if the request is important enough, it will accept the request. The CPU will now operate on the request. It will continue to operate on that request until it has finished that operation—or until another request with higher priority comes along. Most computers have lots of time to do all of the things that are asked of them. If a couple of interrupt requests have to wait for a hundredth of a second, or a tenth of a second, no great harm is done.

But now consider that the interrupt request is from a process sensor, that the request is only milliseconds long, and that it is advising of something urgent. For the system to operate properly, this interrupt request must get through. *The Instrument Engineer's Handbook, Process Control, 3rd Edition,* defines "real-time system" as a system that guarantees a definite maximum time between an interrupt request and the correct execution of the code designed to respond to the interrupt. This kind of a definition allows for real-time systems that are more real-time than others, based on the "definite maximum time" guaranteed. But that is still acceptable if the range of guaranteed times will satisfy the needs of the process. In fact, we shall see later in this unit that certain functions of a SCADA system do not have to respond instantly, but do have to respond within a defined length of time.

The Integration Group of The Americas Ex. 1007-Page 36
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001089

Learning Objectives—When you have completed this unit, you should:

A. Understand the terms that deal with time response.

B. Understand the criteria to be considered when selecting scan interval.

C. Know the factors that affect decisions about where to place calculation or computing elements.

4-1. Is SCADA Real-Time?

Now that we have a workable definition of "real-time," we are in a position to answer this question. As we will consider in detail later in this book, some parts of a SCADA system must respond much faster than other parts but each part has some time constraints that must be met. Let's look at a simple SCADA system from the field end.

First, we have an instrument in contact with the process. It is a differential pressure transmitter. As the flow increases through a meter orifice, the transmitter senses an increase in the differential pressure across the orifice. This happens very quickly. It happens so quickly that for practical purposes, there is no delay. The result of the flow increase is to change the current through a wire pair connecting the sensor to a flow computer. This flow computer has a simple purpose: It solves an algorithm by multiplying the differential pressure signal by several constants and one or two variables that are changing with time to arrive at an answer that can be called "corrected flow rate." If the flow computer can read each of these variable inputs, including differential pressure, and can multiply them by the constants that have been programmed into the flow computer and can produce an output fast enough, then it has done its job. How fast is fast enough? Experiments have shown that with good sensors, significant changes in differential pressure can be measured in the order of milliseconds. So the ability of the computer to sample all of the variables in less than a millisecond should work. Multiplying them by the constants will take only microseconds or less. We can feel comfortable that an electronic flow computer can act as a real-time device for one orifice meter. But could it handle four or five flow calculations at the same time? How about thirty? How about two hundred?

Second, the corrected flow rate will be available as a current coming out of the flow computer. The remote terminal unit (RTU) will sample this variable and will store it in a memory register. The RTU will also sample analog variables from other flowmeters, from level transmitters, or from temperature transmitters; and will sample discrete variables from fire alarms and the like. Each of these variables will be sampled and stored in

The Integration Group of The Americas Ex. 1007-Page 37
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001090

its own memory location. Since we know that RTUs are microcomputer based, we can feel comfortable that an RTU should be capable of handling this workload for three or four transmitters, and do so in such a short time that the flow, level, or temperature of the process would not have changed significantly. It would be able to do this in "real time." Could it do all of this quickly enough for 200 transmitters? 3,000 transmitters?

Third, the RTU must listen for a request from the master terminal unit (MTU), which will periodically tell each of the RTUs in the system to report what it knows. When it receives such an order, the RTU must confirm that the message is indeed for it and not for some other RTU. Then it must put together a message that includes all of the information requested by the MTU—this information must be arranged in a very specific manner. Then, an error-detecting code must be attached to the message that will allow the MTU to determine if any communication errors have occurred as the message travelled from RTU to MTU. The RTU must then turn off its radio receiver, turn on its radio transmitter, and send the message to the MTU. After that, the RTU must turn off its transmitter, turn on its receiver, and wait for the MTU to give it further orders. If it can do this before the MTU gets tired of waiting for an answer, it will have been successful. It can do the job in "real time." We can believe that this is possible for short answers, but if the MTU asks for 50 pieces of data, will it still work? How about 1,500 pieces?

Fourth, the MTU must receive this data; check it to determine if any communication errors have occurred; store the data in predetermined memory locations; and present any alarms, reports, or data screens to the process operator. At the same (apparent) time, it must instruct the next RTU on what to do. This group of activities seems like it could be done in the time available, and if it is, then the MTU has been successful in acting as a "real-time" device.

From this admittedly superficial description of SCADA activity, we can see that even though some of the functions take much longer than others, the definition that we used at the beginning of the unit has been useful in designing a system that will work. The description provides some measures that we could use if we believed that parts of the system were not working in "real time." For example, if it were discovered the MTU was not receiving all of the RTU's response, it might be necessary to shorten the list of requested data points, or it might be necessary to lengthen the time that the MTU was allowed to wait before moving to the next request.

The Integration Group of The Americas Ex. 1007-Page 38
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001091

4-2. Continuous Process Control

Most systems that control continuous processes operate in real-time. Consider Figure 4-1. The controlled variable signal is fed to the input of the control system with no (significant) time delay. The controller acts on this signal as quickly as possible with the control algorithm. The manipulated variable is sent to the process immediately. Time delays exist in the control side of the system, but they are usually kept very short.

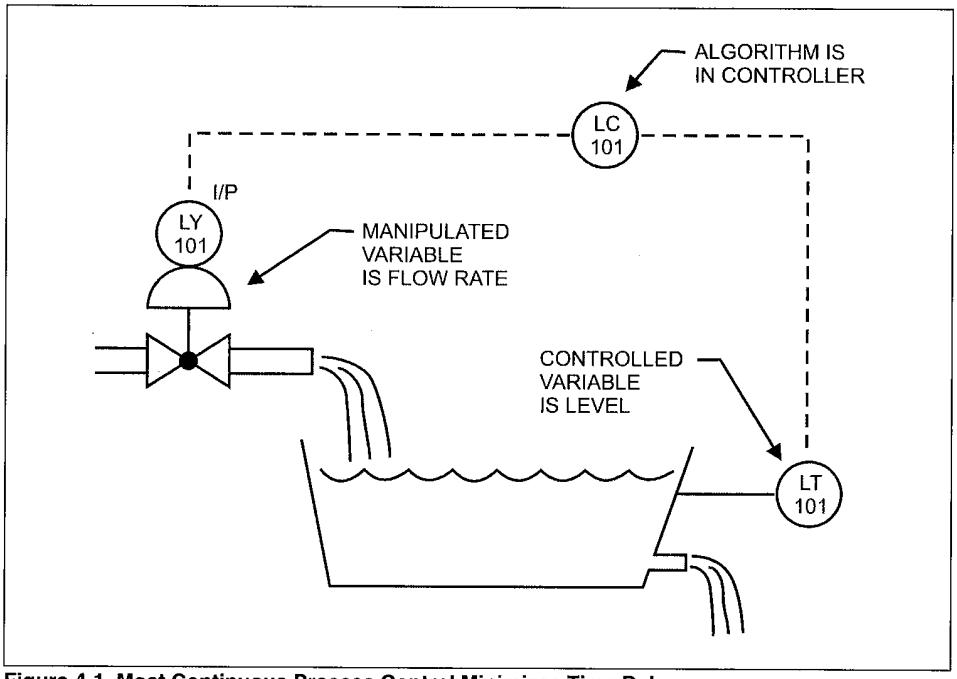


Figure 4-1. Most Continuous Process Control Minimizes Time Delay

Figure 4-2 shows a simple SCADA with the MTU scanning three RTUs. The MTU asks RTU number 1 for information about flow through FE-101, and then it asks each of the other RTUs about flow through their flow elements. The scan interval (sometimes called the "scan period") is the time between one conversation with an RTU and the next conversation with the same RTU. The constraints of the SCADA system and its method of low-speed scanning are going to introduce a time delay. It is the responsibility of the system designer to ensure that the delay is not long enough to introduce a safety or operability problem.

Figure 4-3 plots the delay introduced by a scan of three RTUs. The decision as to whether or not control will be affected by the scan interval can only be made by someone (or some team) that is familiar with the process. At the early stages of the design of a SCADA system, the scan

The Integration Group of The Americas Ex. 1007-Page 39
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001092

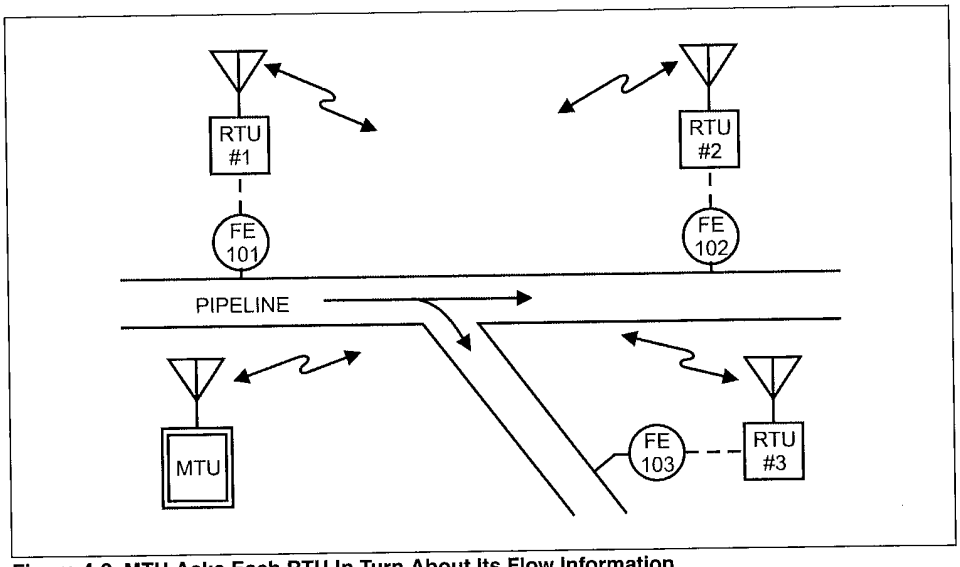


Figure 4-2. MTU Asks Each RTU In Turn About Its Flow Information

interval can be selected to mitigate some of the time delay effects. Section 4-3 will examine the process of tailoring the scan interval to the needs of the process.

In particular, systems for indicating status or for alerting operators to process conditions that are out of limits (alarms) attempt to introduce as little time delay as is "economically feasible." This is an important phrase when considering SCADA. It does not mean "as little time as possible." It means that the operator's time response to the alarm must be considered when determining how quickly the alarm must be presented to the operator. The following three examples will help to clarify this. For each example, a process upset or equipment failure has been recognized. The SCADA system signals the operator that an alarm condition exists. The operator then responds to return the process to normal.

Example 4-1. Out-of-limits condition: A beam pump on an oil well located at site 10-22 has stopped. Such pumps lift oil from the underground reservoir. When the pump stops, the flow of oil stops.

Alarm Signal: "Beam Pump 10-22 Stopped"

Likely response: On the next scheduled visit to this part of the oil field, the field operator will plan to spend enough time at this site to determine the cause of the pump's failure, will write up a description of the failure, and will call in appropriate maintenance personnel to repair it. These pumps

The Integration Group of The Americas Ex. 1007-Page 40
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001093

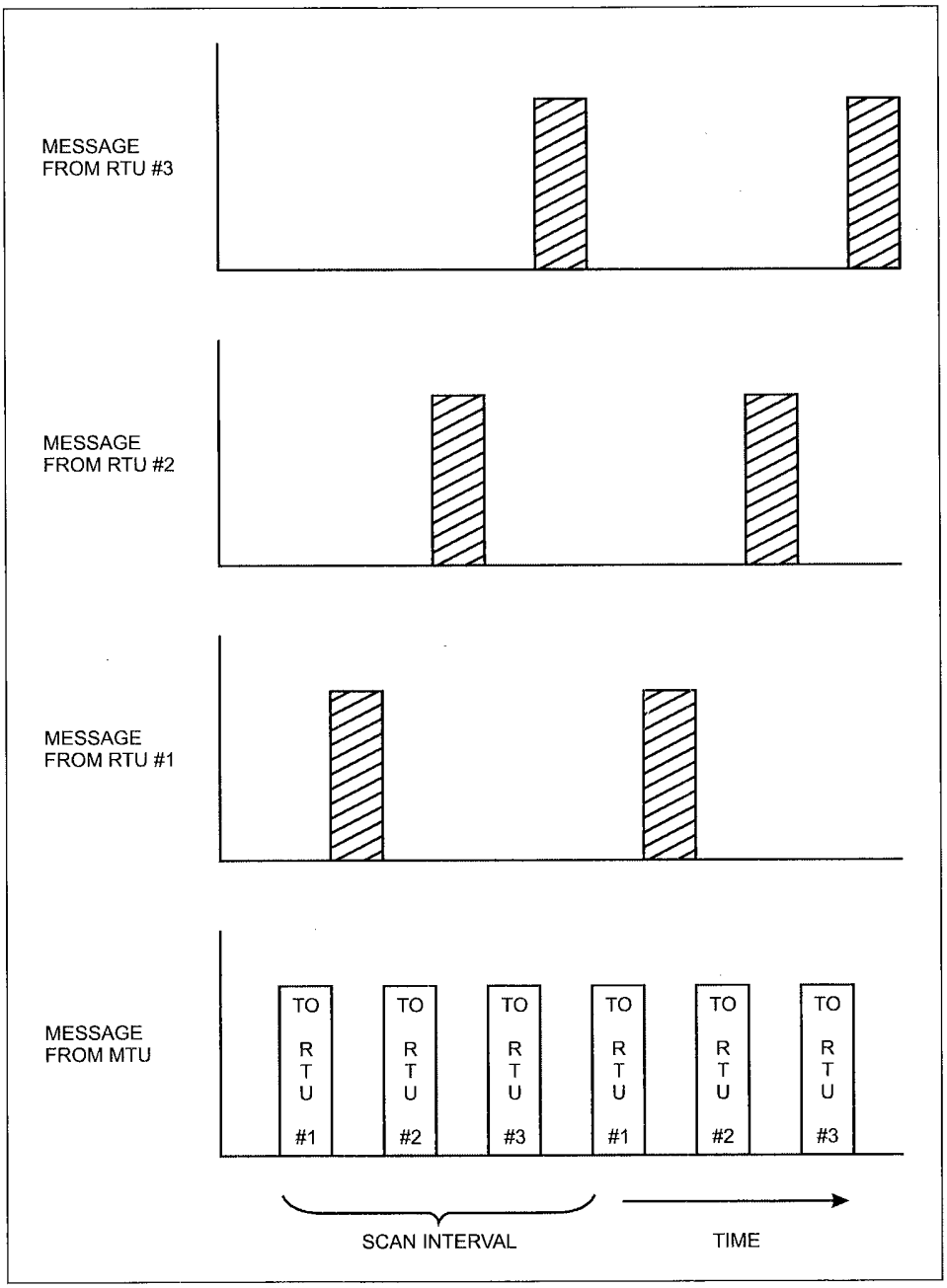


Figure 4-3. Time Delay with SCADA System

produce small amounts of oil per day, and it will probably take two or three days to repair.

The economically feasible time delay for this response is on the order of hours—perhaps as much as twenty-four hours.

The Integration Group of The Americas Ex. 1007-Page 41
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001094

Example 4-2. Out-of-limits condition: An electric submersible pump on an oil well located at site 6-33 has stopped.

Likely response: Electric submersible pumps are expensive, high volume pumps. For this reason, they are installed on high volume wells. Because this well produces a very large amount of oil and downtime is important to the company, a maintenance crew will be dispatched, day or night, as soon as the alarm is received.Alarm signal: "Submersible Pump 6-33 Stopped"

The economically feasible time delay for this response is on the order of minutes, perhaps as much as one hour.

Example 4-3. Out of limits condition: An electric switch between generator number G-510 and the electric transmission system has opened.

Alarm Signal: "Generator G-510 Switch Open"

Likely response: A generator that is presently in the spinning reserve mode will be connected to the transmission grid as soon as possible.

The economically feasible time delay for this response is on the order of seconds—perhaps thirty seconds.

From these three examples, it should be clear that the response time the process requires should be the overriding consideration when determining what is and what is not "real-time." Pragmatically, real-time means that the time delay of the system is not long enough to introduce problems in control. For this reason, much of SCADA is considered to be real-time control even though a recognized time delay is associated with it.

4-3. Communications Access and "Master-Slave"

Electronic machines can talk to each other in several ways. Depending on the purpose of their conversation, the required speed, and the machines' status relative one to the other, different communications access methods may be used. The communications requirements both determine and are controlled by the communications protocol selected. Unit 9 will discuss protocols and communication topology.

For this discussion, you should know that most SCADA systems use a communications plan called "Master-Slave." With a master-slave arrangement, only one of the machines (in this case, the master or MTU) is capable of initiating a conversation. The MTU calls one RTU, gives instructions, asks for information updates, and then tells the RTU to

The Integration Group of The Americas Ex. 1007-Page 42
SitePro, Inc. v. WaterBridge Resources, LLC, et al
WB_00001095

respond. The MTU then listens for an answer. The RTU answers as soon as the MTU has finished speaking. Then the RTU stops talking and starts listening for more instructions. If the MTU has no more instructions for RTU-1, it will call RTU-2 and go through the same procedure. The MTU will go through each RTU, then return to RTU-1 and continue. No RTU can initiate a message. It can only answer a message when specifically instructed to do so by the MTU.

There is a provision for the situation in which one of the RTUs has failed. The MTU will listen for a predetermined time, then, if it "times-out" before it gets a reply from that RTU, it will send its next message to the same RTU. Again, it will wait for that predetermined time. If still no reply, it will send a third and last message to the same RTU. If no reply is forthcoming, it will move on to the next RTU and will continue with its scan. When it does this, it will record the failure of the RTU to reply. This will generate a communications failure alarm. Depending on how the scan program was written, this RTU may be eliminated from further scans until a manual over-ride, which would happen after Maintenance has fixed the RTU, has been input.

As we have seen, the process of talking to each RTU in order and then going back to the first RTU to begin the cycle all over again is called "scanning" or "polling." The length of time between the MTU talking to RTU-1 and the next time it talks to RTU-1 is called the *scan interval.*

4-4. Determining Scan Interval

Control should not be compromised by excessive time delay. There are time constraints imposed by the rate that data (which includes, but is not limited to, process information and control instructions) is sent between the MTU and the RTUs. It therefore follows that there is a "best rate" at which to scan RTUs for data. One of the factors that determines scan interval must be the number of RTUs that have to be scanned. An estimate of the likely numbers of RTUs, made early in the design phase, will probably be sufficient to determine what this number is.

A second factor to be considered is the amount of data that must be passed during each conversation. This will be determined by the size of the facility at each remote site and the amount of independence each remote site is capable of exercising. Depending on these factors, the amount of data to be gathered from each RTU could be as little as one status point or as much as several hundred status and alarm points, several hundred bits of accumulated process data, and several dozen analog points. To communicate, each status or alarm point requires one (usually) or two (less frequently) bits of data. Since each totalized meter value or analog measurement point must be converted into a binary word, each point

The Integration Group of The Americas Ex. 1007-Page 43
SitePro, Inc. v. WaterBridge Resources, LLC, et al
WB_00001096

requires about 16 bits. This will vary with different equipment; however, sixteen is a close enough number for this calculation.

For simplicity, as well as for safety-factor reasons, it is best to select the largest outgoing RTU message when calculating points. Multiply this point count by the total number of RTUs to get the count of all data coming back from all the RTUs. Remember that a conversation is usually a transfer of information in both directions. It is important to include the time taken by the MTU to talk to each of the RTUs. This will include the time taken by the MTU to ask each RTU for data plus the time taken by the MTU to give other instructions to each RTU. Again, at this early design stage, it is best to take the largest outgoing message and multiply by the number of RTUs. This should provide a conservative result, necessary because, as the design progresses, more people will approach with a comment that begins with, "Wouldn't it be nice if we added...," and any extra room you have left in the system will be used up.

The third factor is the data rate. The number of bits per second (bps) that can be transmitted over the communications medium is important in determining scan interval, but at the early design stage, this number may be flexible. Bps numbers may be traded back and forth as the design progresses. At this point in the process of determining scan interval, consider that there are two data rate groupings. The first, which is used in voice grade telephone equipment and many UHF radio–modem communication systems, is between 300 and 2,400 bps. Using 1,200 bps in the calculation will give you a good first estimate. The second data rate grouping applies if a special communication package is being considered. It may be as low as 19,200 or as high as 10 million bps. For systems that are complex enough to require these data rates, there will be a specialist on the design team who can provide a meaningful data rate for this calculation.

The fourth factor in determining scan interval is communications efficiency, which may be thought of as the following ratio: the time spent moving the data of interest divided by the total time spent communicating. Much of the inefficiency is obvious. For example, part of each message must include the address of the RTU, which is data that holds only administrative interest. Some of the inefficiency is not so obvious, however. Error detection codes are frequently used, and these take time. Similarly, radio turn-on time (to allow the power electronics stage of a radio to stabilize) may take more time than the entire message. These factors will be dealt with in more detail in Unit 8, but as a first approximation, use the following numbers for communications efficiency: dedicated telephone line, 70%; radio, 40%; dial-up telephone, 1%.

The Integration Group of The Americas Ex. 1007-Page 44
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR2025-00708

WB_00001097

Example 4-4. Based on the preceding discussion, calculate a scan interval for a SCADA system.

1. It will initially have seven RTUs, but will likely increase eventually to twenty; therefore, the number of RTUs equals twenty.

2. The largest RTU has the following point count:

140 status points	140
30 alarm points	30
10 measurement meters (16 bits each)	160
10 analog points (16 bits each)	160

The MTU will send the following point counts to the RTU:

150 discrete control (valves, motors)	150
6 stepping motors (16 bits each)	96
10 valve controller points (16 bits each)	160
Total	896 bits

3. Data rate is based on the likelihood that UHF radio will be used for communication. Use 1,200 bps.

4. Communications efficiency, based on UHF radio, is 40%.

Therefore, 20 RTUs x 896 bits/RTU = 17,920 bits.

At a data rate of 1,200 bps, this will take 17,920/1200 = 14.9 seconds at 100% efficiency.

At 40% efficiency, this will take 14.9 seconds/.40 = 37.3 seconds

It would be good design practice to round this up to one minute. Having calculated this number, you should now ensure that a one minute delay of data will not adversely affect any of the process functions. If such problems do exist, but only at one or two of the RTUs, the problems may be addressed by scanning each of those RTUs twice on each scan.

Example 4-5. If the scan rate were acceptable for all except RTU number 5 in a system of five RTUs, the scanning program could be set up as follows:

RTU-1, RTU-2, RTU-5, RTU-3, RTU-4, RTU-5, RTU-1...

The Integration Group of The Americas Ex. 1007-Page 45
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001098

As with most quick fix solutions, there are limits to how often you can get away with this before you start to degrade the whole system. By adding one extra RTU scan in a group of 5, you have degraded the scan time by only 20%. If you tried to scan RTU-5 after each RTU, you would nearly double the scan time, which might make the scanning unworkable.

If most of the RTUs show process functions that are marginally good or bad from a timing point of view, one solution would be to increase the communications data rate (in this case from 1,200 bps to 2,400 bps). It is important to realize that doubling the data rate will not reduce the scan period by one half. Communications efficiency is a nonlinear function of data rate. If many problems are identified and the process requires a response time that is orders of magnitude shorter than the problems will allow, it may be necessary to review the communications method. It may be that some functions should be removed from the SCADA system.

Provisions should be made for additions to the amount of data to be transmitted. Most SCADA systems have functions added to them over their lives; few have functions deleted. Unit 11 will address some of the functions that should not be dependent on the communications system. The next section of this unit will discuss options for locating computing or calculating elements.

4-5. Where to Compute?

Have you ever noticed, as you travel on a highway that is well lighted by fluorescent or mercury vapor lights, that the spokes on the hubcaps of the car next to you are visible and are slowly turning—sometimes backward, sometimes forward? This is the "strobe effect," and it happens because the street lights give off a burst of light twice in every $1/60^{th}$ of a second (every $1/50^{th}$ of a second if the power system operates at 50 Hertz). If the spokes of the hubcap are turning so that a spoke is at (or near) the same position that another spoke was $1/120^{th}$ of a second ago, your eyes will be fooled into thinking that they are seeing the same spoke.

Figure 4-4 shows how this works. To clarify the illustration, one of the spokes (the one at the twelve o'clock position in Figure 4-4A) has been smeared by road tar. If we assume a 15-inch-external-diameter tire on a wheel with 6 spokes, the configuration shown in Figure 4-4B will happen $1/120^{th}$ of a second later if the car is going 53.7 MPH, and the configuration in Figure 4-4C will happen $1/120^{th}$ second after that of Figure 4-4B.

Now take off the road tar. Imagine that the car is going 53.7 MPH or 107.4 MPH or any integral multiple of 53.7 MPH. If you could see (or sample) only the relative position of the spokes, you would have no way to tell

The Integration Group of The Americas Ex. 1007-Page 46
SitePro, Inc. v. WaterBridge Resources LLC et al.
WB_00001099

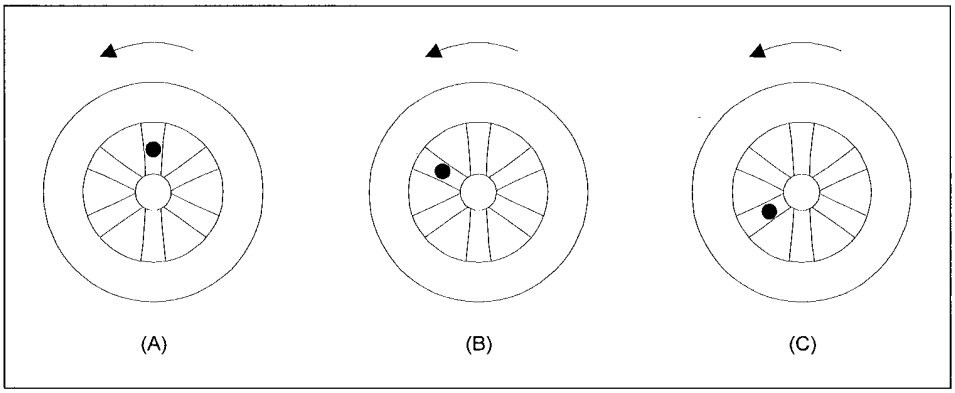


Figure 4-4. Sampling Frequency and "Aliasing"

how fast the car is going. The spokes would not appear to move. If the car were going a bit slower, the hubcap would appear to rotate backward. If the car were moving a bit faster, it would appear to rotate forward slowly.

So, for a case that has the physical constraints we have described, there is something magic about 53.7 MPH and the sampling frequency of 120 samples per second. The "magic" is that for every integral multiple of 53.7 MPH, a spoke (we don't know which one) passes through the top vertical position. Now turn the problem around. Say that we know that the range of speeds is between 0 MPH and 53.7 MPH, and we wish to calculate the minimum frequency of a strobe light so we can unambiguously determine the speed. How could we do it?

Since we know that it takes $1/120^{th}$ of a second for the spoke to advance one position, we must fire the strobe a bit faster than $1/120^{th}$ of a second if we want to sample the situation that exists before the spoke gets there. The frequency must be faster than 120 Hertz because at 120 Hertz, one spoke could masquerade as another. In this example, 120 Hertz is called the "aliasing" frequency. For a similar situation in which the number of spokes doubles to twelve, the aliasing frequency would also double—to 240 Hertz.

"This is all very interesting," you may say, "but what does this have to do with SCADA?" If the highest natural frequency of the process is known, then the aliasing frequency can be calculated. The process parameters can be sampled effectively at frequencies higher than the aliasing frequency, but not at lower frequencies—meaning this simple test can tell if the scan frequency is adequate for sampling. If it is adequate and if the measurement is not too critical, the process can be sampled, the raw data can be scanned, the calculation (or computation) can be done in the MTU, and the result can be sent back to the RTU and processed. On the other hand, those processes that have aliasing frequencies higher than the

The Integration Group of The Americas Ex. 1007-Page 47
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001100

selected scanning frequency must have the computations done before the scanning. These computations must take place in the RTU or some other equipment at the same location as the RTU. The following two examples will illustrate this point.

Example 4-6. Given that a scan interval of one minute is practical, determine where the calculations should be performed to measure the amount of water produced from a well using a tank metering system. Such metering systems are used in irrigation systems to keep track of the amount of water diverted to a field. Water flows into a tank until it is full, then stops. A valve is then opened to start the flow of water from the tank to the field. When the tank becomes empty, the drain valve closes and the tank refills. It takes four minutes to fill the tank and four minutes to drain the tank. Status switches on the valves are monitored by the SCADA system. When the drain valve is closed, the refill valve is open and vice versa.

Question: Can the flow totalizing be done at the MTU?

Answer: Since the scan interval is one minute and the aliasing frequency (the highest cycling frequency in the process) is one cycle in eight minutes, this calculation would be an acceptable one to do at the MTU.

Example 4-7. Assume the same conditions as in Example 4-6, except that only twenty seconds are required to fill the tank and thirty seconds are required to empty it.

Question: Can the flow totalizing be done at the MTU?

Answer: Since the natural frequency of the drain valve (1 cycle divided by 20/60ths of a minute plus 30/60ths of a minute) = (1 / (50/60)) = 60/50 = 1.2 cycles per minute is higher than the scan frequency of 1 cycle per minute, the MTU cannot reliably calculate the flow rate.

Refer to Figure 4-5. Consider that on scan 1, the MTU sees the drain valve closed. On scan 2, the drain valve has opened and closed, but the MTU has no way to tell that it has opened. The MTU will not recognize that the valve has moved until the third cycle. This will result in an error. For this case, it is necessary to do the totalizing at the RTU, and the RTU must sample the position of the drain valve more frequently than 1.2 cycles per minute. That should not be a problem. RTU sampling frequencies of several thousands of cycles per minute are normal.

The Integration Group of The Americas Ex. 1007-Page 48
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR2025-00[illegible]

WB_00001101

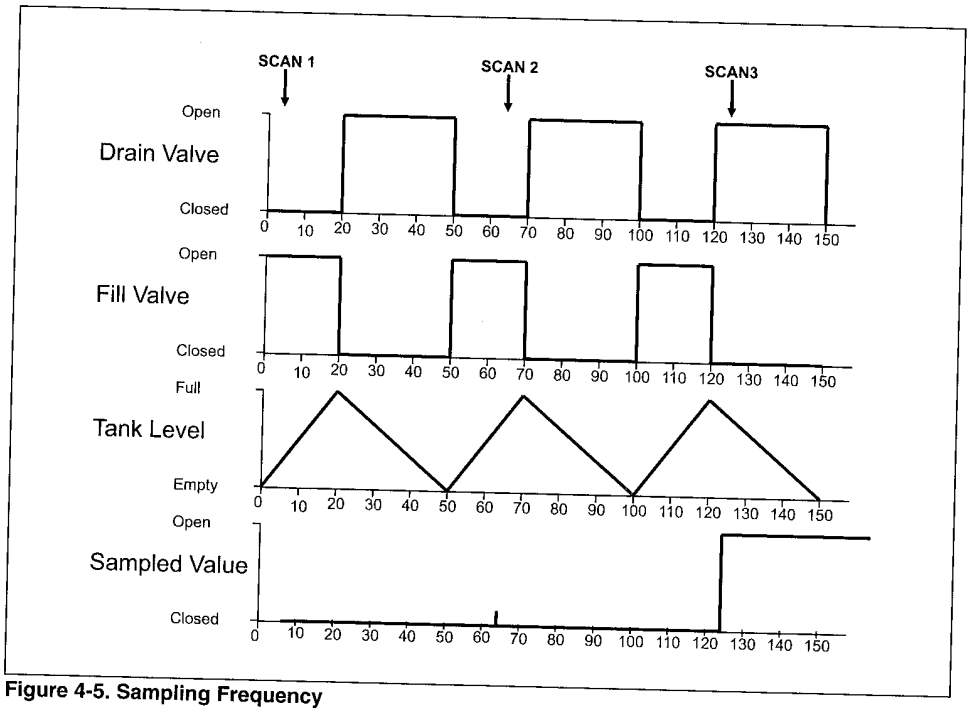


Figure 4-5. Sampling Frequency

Given that some rather simple calculations can be used to determine which computations should be done at the MTU and which should be done at the RTU, there remains the question of which hardware should be used to perform auxiliary calculations at the RTU's location. At one time, it would have been normal to use a dedicated kilowatt-hour meter to measure delivered energy. Because of the enormous reduction in the cost of small computer hardware, it is now feasible to purchase a computer that is powerful enough to complete, in a timely manner, all of the calculations, all of the instructions to actuators, and all of the storage of historical data that may be needed at the site. This means that it is possible to have the computer-based RTU do all of the remote site calculations.

There are several reasons why you do not want to "put all of your eggs in one basket" and do all of the calculations in the RTU. As will be explained in Unit 11, safety-related considerations call for the use of fail-safe logic for safety shutdowns. Regulatory requirements may mandate that meter totalizer logic be located in separate locked enclosures. Small, simple RTUs supported by special-purpose logic modules may be more price competitive than large, complex RTUs that can do all of the logic calculations. Finally, some control calculations require input data from more than one remote site. These control calculations are most logically completed at the MTU. Simple orders can then be sent to the appropriate RTU to effect the controls.

The Integration Group of The Americas Ex. 1007-Page 49
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001102

Unit 4 Exercises:

4-1. *"Real–time" is a relative term. For the following process conditions, determine if the response time is adequate:*

a. *Customer billing for gas through a meter is issued once per month. The scan rate is once per hour.*

b. *Customer billing for gasoline is based on individual fill-ups, each lasting ninety seconds. The scan rate of the meter is once per hour.*

4-2. *An RTU recognizes that a motor that should be running has stopped. It is 2:00 a.m. For this motor failure, overtime is not allowed, so no maintenance crew will be sent to investigate until 9:00 a.m.*

a. *Would a ten-minute scan rate be acceptable?*
b. *Would a one-hour scan rate be acceptable?*
c. *Would a twenty-four-hour scan rate be acceptable?*

4-3. *An RTU in a Master-Slave SCADA system determines that a fire is burning in the chlorine injection building of a water treatment plant. Because this is an extremely serious condition, what can the RTU do to notify the MTU without waiting for the next scan?*

4-4. *Describe one way that the scan rate for a single RTU could be increased beyond the scan rate for the other RTUs.*

4-5. *What is the range of data rates for most SCADA systems?*

4-6. *Name three things that detract from communications efficiency.*

4-7. *In Example 4-4, what would be the scan interval if a dedicated telephone line, not a UHF radio, were the communications medium?*

4-8. *The liquid level in a column gravity separator is observed to cycle with a two-minute period from one maximum level to the next. What would be the effect of sampling this level with the following:*

a. *A two-minute scan rate?*
b. *A thirty-second scan rate?*

The Integration Group of The Americas Ex. 1007-Page 50
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR2025-01103

WB_00001103

Unit 5: Control System Elements Sensors, Actuators, and Algorithms

The Integration Group of The Americas Ex. 1007-Page 51
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,242,078

WB_00001104

Unit 5

Control System Elements: Sensors, Actuators, and Algorithms

The details of any project can easily be overshadowed by its one or two most prominent or obvious highlights. With SCADA projects, for example, the features that attract the eye are the MTU, the communication system, and the RTUs. It may, therefore, come as a surprise to learn that such apparently simple and inexpensive parts as limit switches, valve actuators, analyzers, and their associated wiring may easily represent the largest portion of the capital cost of a SCADA project. This is particularly true if the project involves the modification of an existing process so it interfaces with SCADA.

Control functionality includes measurement, comparison of what the measured value is to what it should be, and correction of some parameter that should result in the measurement value getting closer to the desired value. This series of actions is repeated over and over again, as long as the process is operating. It is important that the controller is updated with fresh information often enough to keep ahead of the changes in the process, and, for this reason, most controllers are located in or near the RTU instead of at the MTU.

The instruments—sensors, actuators, analyzers, and so on—must be able to communicate with the RTU. To do so, they must speak the same language, or protocol. In addition, they must use the same medium. It may be copper wire, optical fiber, or radio signals. These are the factors that we will discuss in Unit 8.

Learning Objectives—When you have completed this unit, you should:

A. **Be aware that the cost of process interface equipment can be significant.**

B. **Recognize that when sensors and actuators are being selected and installed, the special considerations of the process and ambient conditions must be taken into account.**

C. **Be comfortable with the knowledge that sensors provide a representation of what the present conditions of the process are. Actuators provide a means of changing certain of those conditions. Between these two items of equipment, there must be a decision-making logic function, or algorithm, that will manipulate one variable in response to a change in a different, measured variable.**

The Integration Group of The Americas Ex. 1007-Page 52
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001105

5-1. A Forgotten Cost

This unit—indeed, this entire book—will make no attempt to discuss all of the types of sensors and actuators that SCADA systems can use to interface with the process that they control and monitor. Several sensors and actuators will be discussed as examples, but it should be obvious by now that many industries use SCADA. Each of those industries has many measurement and control requirements that are unique. In addition, most of these requirements can be handled in several ways by many different pieces of equipment. Multiplying "many" by "many" by "several" by "many" culminates in a very large result indeed. For most SCADA RTU locations, this same kind of vast arithmetic calculation can be applied to determining the cost of the sensors and actuators associated with the SCADA system.

Rightly or wrongly, the economics of establishing an RTU at a particular location are usually based on taking one or two valuable measurements remotely and making one, two, or sometimes three changes remotely or automatically from a distant control location. It is on these three or four functional benefits that the cost of the installation must be justified. As soon as the feasibility of installing SCADA for these three or four functions is established, the phrase, "Wouldn't it be nice if..." rises to the top of the hit parade. The hurdle has been cleared: The MTU and RTU have been justified. So everything else is free, right?

What is forgotten by the uninitiated is that the sensors, the actuators, and the wiring between them and the RTU also cost money. In fact, these items frequently cost three to four times as much as the RTU, UPS, and communications equipment at a particular site. Figure 5-1 shows the costs of SCADA at a simple RTU site. In the figure, there is only one RTU, one radio, and one power supply at a remote site; however, that site may easily have as many as 250 sensors, actuators, and analyzers.

Many of the things an operator does while visiting a remote site are done without conscious thought. He or she does them by using the enormously versatile sensing and actuating capabilities of the human body. We have been augmenting these capabilities for the past sixty-four million years, ever since the dinosaurs moved over to make room for mammals. Since 1769, when James Watt developed improvements to the steam engine and the Industrial Revolution began, operators have been recognizing parameters that need to be measured and controls that need to be adjusted. Generally speaking, we are very well matched to the measurement and control functions that process operators are required to fulfill because those functions have been established with the operators in mind.

The Integration Group of The Americas Ex. 1007-Page 53
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001106

Item	Cost
RTU cost (includes panel)	6,900
Radio System (includes path study)	1,150
Uninterruptible Power Supply (24 VDC)	2,000
Instrumentation	
Sensors	9,200
Actuators	8,625
Heater Automatic/Remote Ignitor	3,450
Installation/Wiring of Instrumentation	5,000
Engineering	
Design, Configuration, Procurement	10,000
Drafting	4,000
Total Cost	**50,325**

Figure 5-1. The Costs of SCADA at Simple RTU Site (Courtesy of Tartan Engineering Corp. Ltd.)

Specialized tools have developed as industry has grown. When it became important to know not just whether a liquid was "hot" or "cold" but "how hot" and "how cold," thermometers were developed. When enough people had to know the height of liquid in a vessel, sensors that a person could read were built, even when the atmosphere above the liquid was 500°F at a pressure of six atmospheres and consisted of combustible, carcinogenic vapors.

The point is that many years of engineering effort have been invested in perfecting sensors and actuators so a person-operator can interface with the process. When a SCADA system is installed between the operator and the process, some additional engineering effort (and cost) is required. For example, very little extra effort is required to enable an operator to use a thermometer to measure a process within arm's length, but extensive work and equipment will be needed to allow the operator to read a non-contact, infrared-sensing, 4–20 mA output thermal-imaging device on a process several miles away. Similarly, a person needs little support to operate a quarter-turn, hand-operated ball valve actuator, but extensive engineering, planning, and equipment will be needed for that same person to operate a pneumatically controlled, Scotch yoke, spring-opposed, fail-safe ball valve actuator that is located several miles away.

Sensors that are cheap to buy if they are to be read by a human operator are usually more expensive if they are to be read by a machine. The thermometer to be fitted into a thermowell in a process vessel (shown in Figure 5-2) will cost about $50; a temperature transmitter to be fitted into

The Integration Group of The Americas Ex. 1007-Page 54
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001107

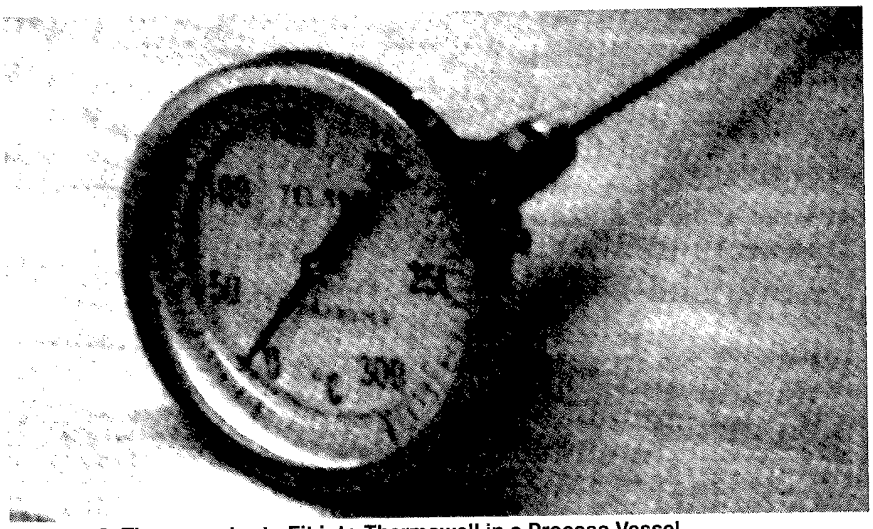


Figure 5-2. Thermometer to Fit into Thermowell in a Process Vessel

the same thermowell and to output a 4–20 mA signal to an RTU (shown in Figure 5-3), $600. The ratio of costs for the local versus the remote measurement of pressure or level is similar.

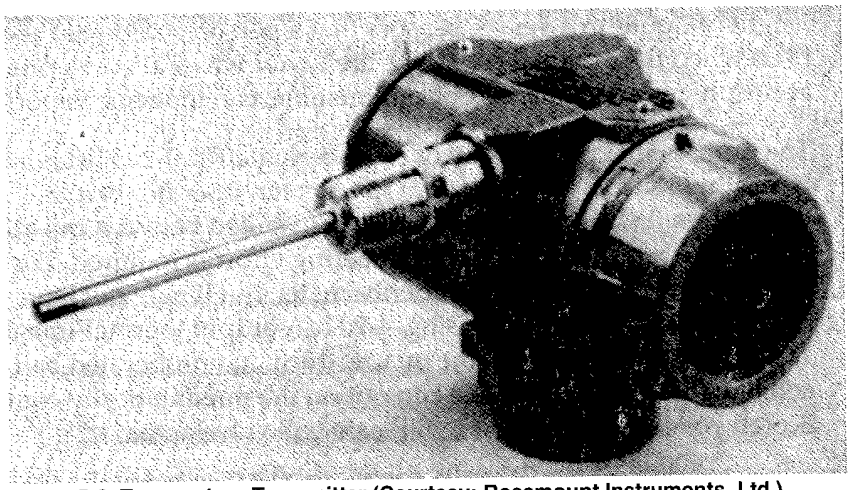


Figure 5-3. Temperature Transmitter (Courtesy: Rosemount Instruments, Ltd.)

Besides purchase cost, there is a cost associated with connecting the sensor or actuator to the RTU. Copper wire is normally used because the signals are usually low-voltage electrical. In many applications, shielding must be added over the copper wire to prevent electromagnetic interference (noise) from corrupting the signal. Some form of physical protection of the copper wire and shield is also necessary; it may take the form of some type of flexible armor that is integral to the structure of the cable. Alternatively,

The Integration Group of The Americas Ex. 1007-Page 55
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001108

the unarmored cable may be fed through rigid pipes called conduit or laid in protective channels called cable tray. Both of these techniques will provide mechanical protection for the cable. To protect the conductors from moisture or corrosive atmospheres, the cable is usually encapsulated in a jacket of fluid-proof, flexible plastic. This jacket will also prevent toxic or flammable fluids from entering and traveling through the cable to areas that must be kept free of these fluids.

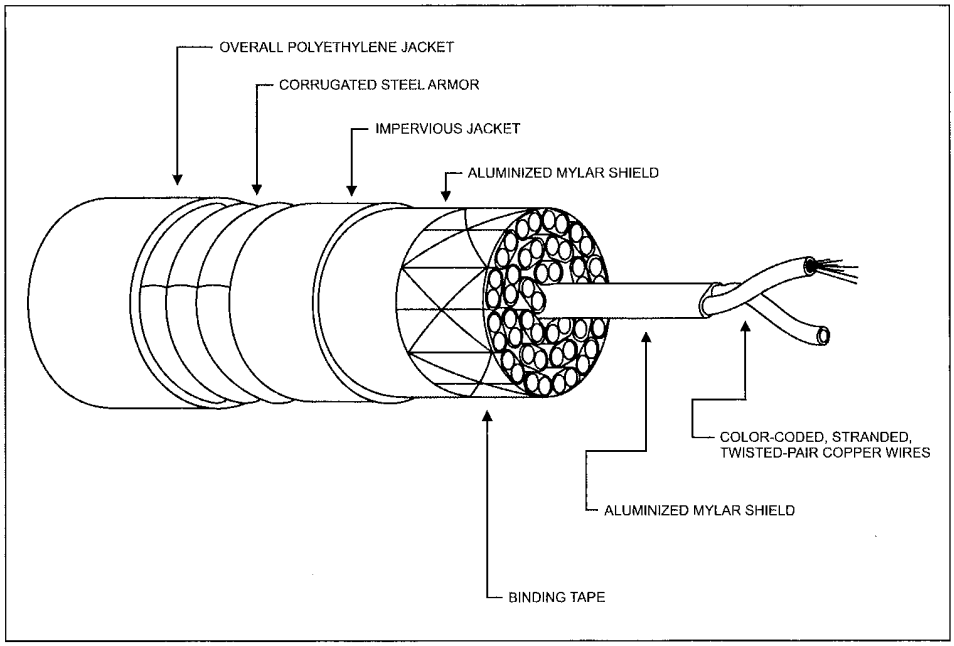


Figure 5-4. Cutaway Drawing of Cable

Figure 5-4 shows a cutaway drawing of such a cable. Many pairs of copper wires, each pair twisted in such a way that the inductance of the wire pair combined with its capacitance will attenuate the frequency most expected to provide noise, can be integrated into this cable. Process instruments are not large enough to allow multi-pair cables to enter their wiring boxes, pass through, and carry on to the next instrument; junction boxes or field termination boxes are used to overcome this limitation. Figure 5-5 shows a large multi-pair cable coming from an RTU to a concentration of instruments; in this case, status switches on ball valves. At a convenient location near the concentration, a junction box (Figure 5-6) with terminal strips is mounted. The wires from the multi-pair cable are terminated in the junction box. Smaller cables, often with only one or two pairs of wires, are run from this junction box to the individual instruments.

In general, it is better to have few rather than many junction boxes because most wiring problems happen at places where a wire connects to a

The Integration Group of The Americas Ex. 1007-Page 56
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001109

terminal. Corrosion, loose connections, and broken wires due to mishandling are the main reason for this.

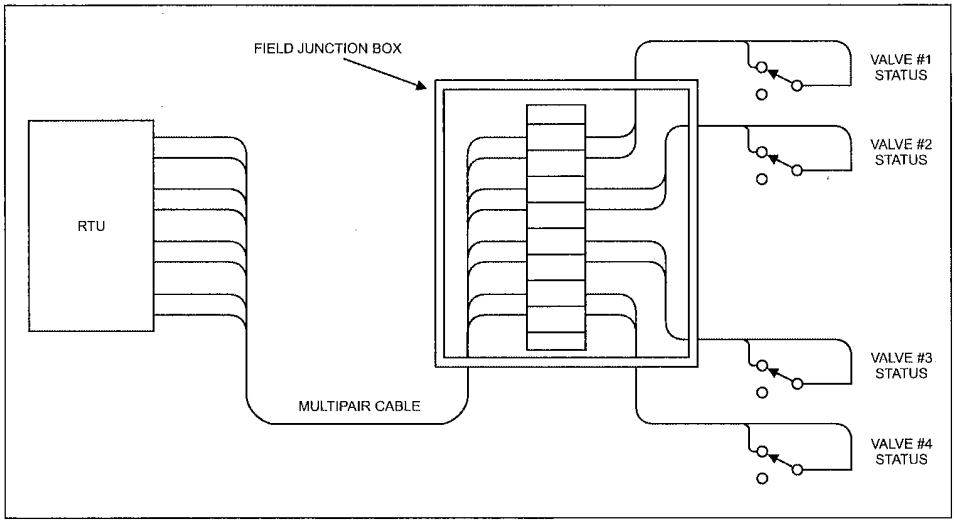


Figure 5-5. Large, Multipair Cable from an RTU

The physical configuration of the process may mean that several of these multi-pair cables will need to connect to the RTU. Often, when this is done, a large junction box, called a marshalling panel, is located at the RTU location (see Figure 5-7). Terminal strips in this box allow all of the wiring to the process instruments to be wired and checked for correctness before the RTU is even delivered to the construction site. The marshalling panel also acts as the platform for power relays, control power fuses or circuit breakers, intrinsically-safe barriers, and special calibration or testing circuitry. If small numbers of special instruments are required, such as flowmeter totalizers, pollution-monitoring electronics, or process moisture analyzers, they are often housed in the marshalling panel. Very often, the marshalling panel even houses a few status lights and manual controls. If local, manually read meter outputs are mandated, they also are usually located here. Figure 5-8 shows the front of a marshalling panel.

All of this technical equipment must be specified. Installation drawings and instructions must be developed. Documentation of the system, individual equipment, licenses, software, and operating instructions must be gathered or written. In short, the engineering of the SCADA field installation must be performed.

Because of the high relative complexity of a SCADA system, the ratio of control engineering cost to total project cost may often be three to five times as high as would be expected for a non-SCADA project. Engineering, development, and documentation costs may reach 50 percent

The Integration Group of The Americas Ex. 1007-Page 57
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001110

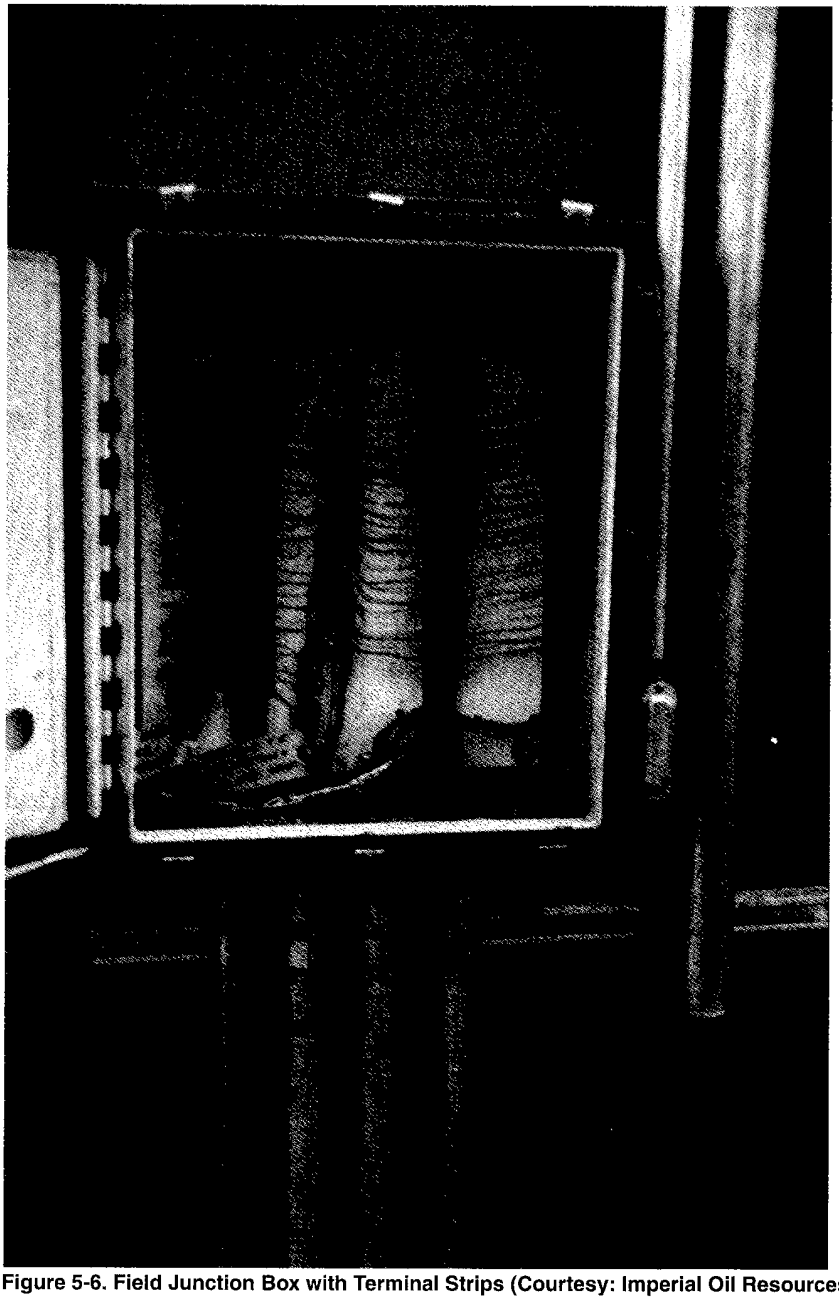


Figure 5-6. Field Junction Box with Terminal Strips (Courtesy: Imperial Oil Resources, Ltd.)

of the total SCADA project cost compared to 10 to 15 percent of the cost of non-automated process projects.

The Integration Group of The Americas Ex. 1007-Page 58
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001111

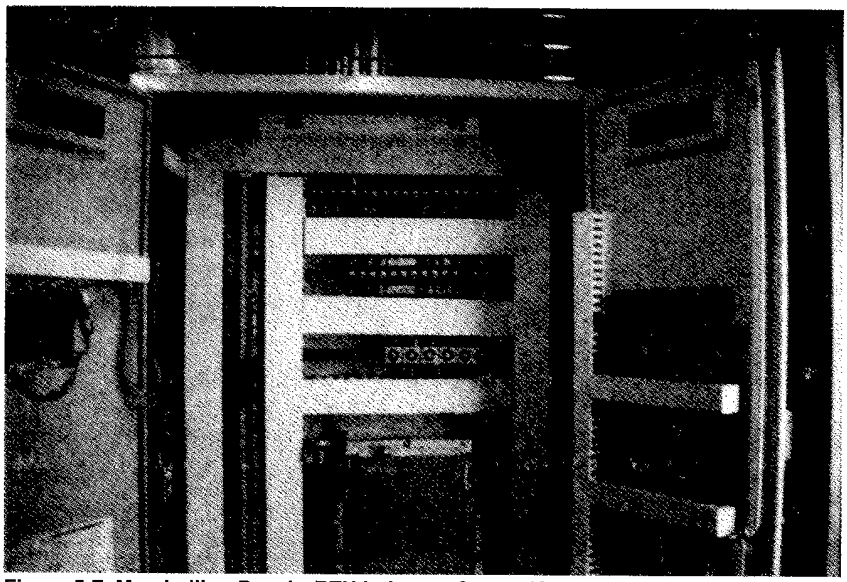


Figure 5-7. Marshalling Panel—RTU in Lower Center (Courtesy: Imperial Oil Resources, Ltd.)

5-2. Special Considerations

Each industry has process considerations that make it, if not unique, then certainly distinct. The production, processing, and transportation of hydrocarbon fluids require that the sensors, actuators, and wiring used in these processes not initiate fires and explosions. Chemical processing may face these same issues, but it will also be concerned with corrosion caused by the process fluids and the pollution of the surrounding atmosphere. Electric power generation and transmission must deal with the issue of isolating instruments from strong electrical fields and high voltages. Food processing has to be concerned about field equipment that comes into contact with the food could contaminate it. Each of these special considerations can be met by equipment if there is enough of a market for suppliers to produce it and if the purchasers are prepared to pay enough. It will cost extra. The extra costs of these specialized control systems will, of course, accrue whether the system has SCADA system or is operated from a control room on the site. Since the field equipment must overcome these particular issues, consideration must be paid to them unless the facility will be operated manually.

As an example, Figure 5-9 shows how a simple device (a cam-operated limit switch) operates. On the left side of the figure, a simple Form C, single-pole, double-throw switch is equipped with a lever that is moved by a cam on a valve shaft. When the shaft moves down, contacts "COM" (common) and "NO" (normally open) close, indicating that the valve is closed. In a clean, non-combustible atmosphere, the housing for this



Figure 5-8. Front View of RTU Marshalling Panel (Courtesy: Imperial Oil Resources, Ltd.)

switch can be designed so support for the working parts is the primary consideration. The materials used can be low-cost cast plastics. The cost will be about $30.

The right side of Figure 5-9 shows a switch that functions in a way similar to the switch shown on the left side; however, in this case, the atmosphere

The Integration Group of The Americas Ex. 1007-Page 60
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001113

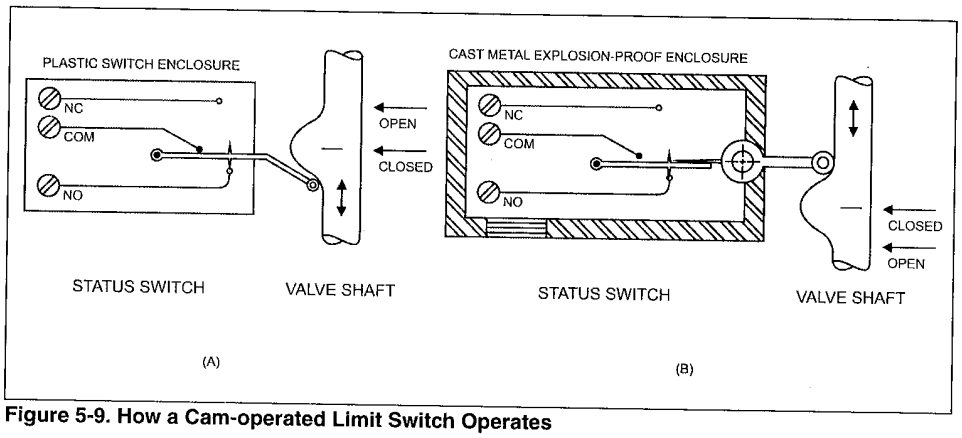


Figure 5-9. How a Cam-operated Limit Switch Operates

is often 20 percent methane. A common way to address this condition is to design an explosion-proof housing for the switch. The housing is not designed to keep the atmosphere away from the contacts; it is designed to be so strong that if a combustible atmosphere does exist and the sparking of the switch contacts ignites the atmosphere inside the housing, the housing will not break up and explode. In addition, the clearance between the moving and mating surfaces must allow the expanding gases to escape and the surfaces must be long enough that the gases will cool as they escape. The gases must be below the ignition temperature of the atmosphere when they get out of the box. The materials for this enclosure will be metal, and the surfaces will be finely machined. The cost will be about $250.

5-3. Standardization

Very few sensors and actuators are so unusual that they are made by only one manufacturer. As market conditions change, the prices of one manufacturer's product relative to another's will vary, and there may be a temptation to switch from one supplier of these process end devices to another. This temptation should be resisted. It is acceptable to change suppliers because the instrument is of inferior quality or because the original is no longer available, but small price savings can easily be overshadowed by the time lost replacing the old instrument and the increased costs of warehousing, training personnel, changes to drawings and other documentation, and calibration procedures. If the SCADA system will be installed in an existing facility, you should consult local maintenance personnel to learn which suppliers have provided good service in the past.

A survey should be made of potential suppliers of sensors and actuators early in the planning stages of a SCADA system. In addition to the fitness of a manufacturer's sensors and actuators for the purpose of the device,

The Integration Group of The Americas Ex. 1007-Page 61
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001114

consideration should be given to the financial stability of the manufacturer and the manufacturer's history of supporting equipment that is no longer marketed. Ideally, spares for each part that forms your SCADA system will be available until you decommission it. An acceptable second-best situation might be that replacement parts for the field devices will continue to be available for at least ten years after the devices cease to be marketed.

The reason that this is more important for sensors and actuators than for MTUs and RTUs is that MTUs and RTUs do not have very many moving parts. They may suffer from a lot of failures when they are first installed (so-called infant mortality), but, unless subjected to long-term overheating, they can be expected to run without trouble for a long time afterward. On the other hand, sensors and actuators do have moving parts that wear out. They are exposed to process chemicals, shifts in ambient temperature, vibration, and a host of other conditions that contribute to failure. The planning for a SCADA project should include provision for maintenance, and those maintenance plans should concentrate on sensors and actuators.

5-4. Maintenance

The maintenance requirements in a SCADA system are not significantly different from those in most other high-technology control systems, the exception being the communications equipment, including radios, modems, and protocol drivers. The calibration, validation, and servicing of those devices require special equipment and manpower training that is not generally available. Depending on the size of your SCADA system and the availability of contract service companies with these particular talents and resources, you may have to make sure your company is able to provide for this maintenance.

As noted earlier in this unit, when you are establishing the proper level of service for your SCADA system, you should do it with the expectation that service requirements (primarily for RTUs and MTUs) will be high initially and then will drop off to a lower plateau (see Figure 5-10). There will be a high initial maintenance level as new equipment goes through its early mortality stage and as loose contacts and pinched wires from the manufacturing and construction phases make themselves known. After this early phase is over, the process interface devices will continue to wear and fail at a higher rate than will the solid-state equipment (see Figure 5-11). To anticipate this, the facility's design should allow ease of access; temporary isolation from the process; and manual monitoring and control while the remote sensors and actuators are being calibrated, replaced, or repaired.

The Integration Group of The Americas Ex. 1007-Page 62
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001115

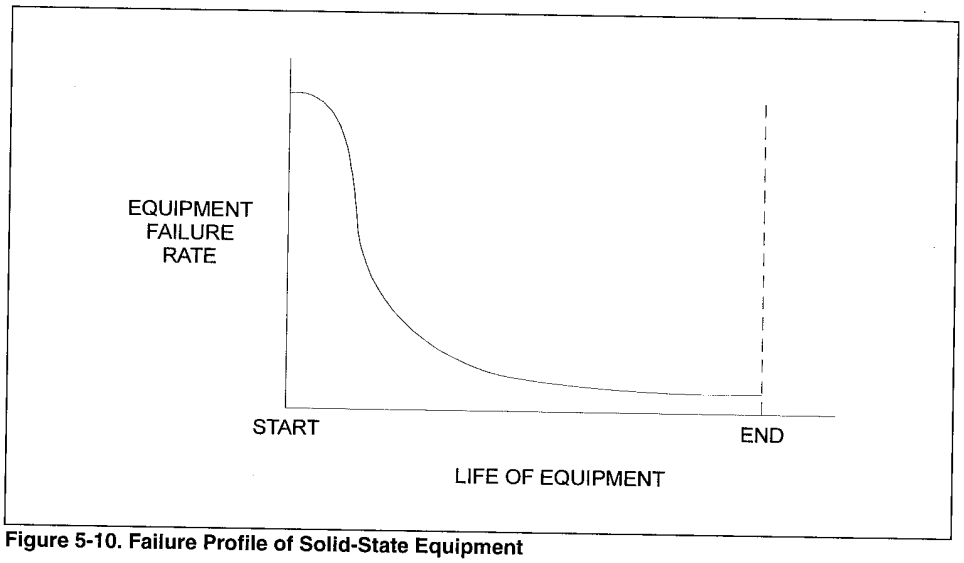


Figure 5-10. Failure Profile of Solid-State Equipment

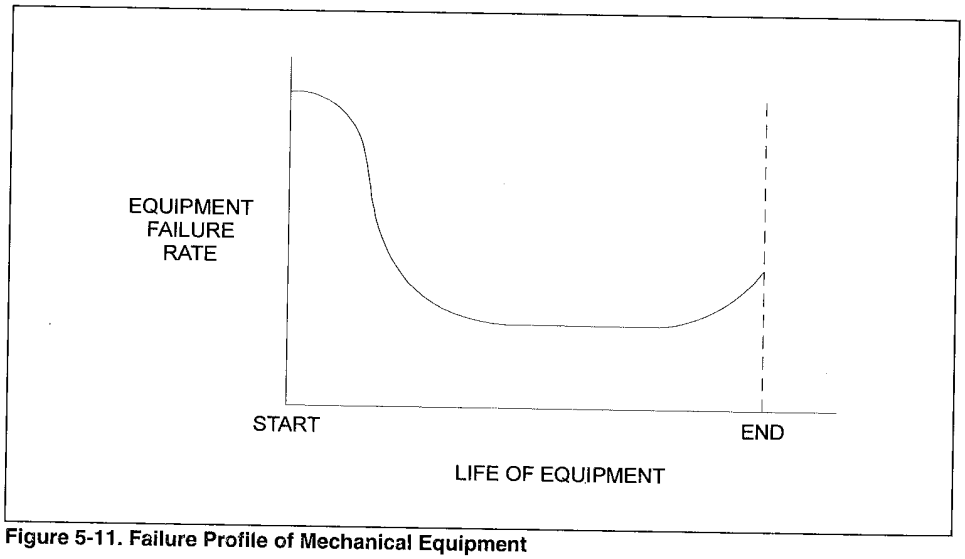


Figure 5-11. Failure Profile of Mechanical Equipment

5-5. Local Controllers

In Unit 4, we considered scan times and aliasing, and determined that there are some (or many) process loops that move too quickly to allow each control decision to be made in the MTU. One way to address this problem is to buy and install a controller dedicated to the fast loop. This controller will be located in the field location. If the process is not potentially explosive and the ambient conditions are not extreme, the controller can be located anywhere that is convenient. An enclosure to keep out rain and bugs is sufficient. If the process is likely to generate

explosive atmospheres and/or the temperature and/or humidity reach extremes, the controller should be located in an atmosphere-conditioned room near the remote terminal unit.

"Controller" is a very general term. Depending on what response is required to a change in the measured variable, the controller may be very simple—or very complex. An example of a very simple controller is illustrated in Figure 5-12. The controller supplies +24VDC to a level switch on the vessel. When the level is below a selected value, the contacts are closed. Current flowing through the contacts energizes a relay in the controller. Energizing this relay causes a set of contacts to supply 120VAC to a solenoid. As long as this solenoid is energized, the instrument air supply will force valve LV-101 to open, allowing more fluid into the vessel. When the level reaches the selected value or above, the 24VDC will be interrupted, the relay will de-energize, and the solenoid will de-energize, disconnecting the instrument air from valve LV-101. When the solenoid de-energizes, it will also vent air from the valve, allowing the valve to close. This is one of the simplest controllers that you can have. It has a very simple algorithm. An *algorithm* is the mathematical description of what the controller does. The algorithm for this type of controller is Z=A. A time graph of how the system works is shown in Figure 5-13.

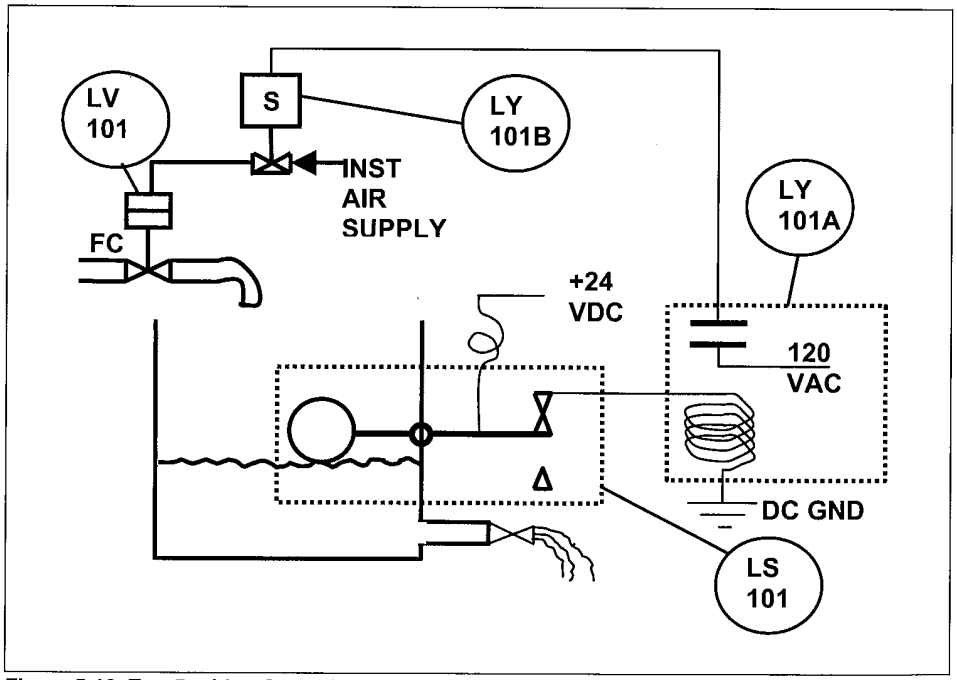


Figure 5-12. Two Position Control

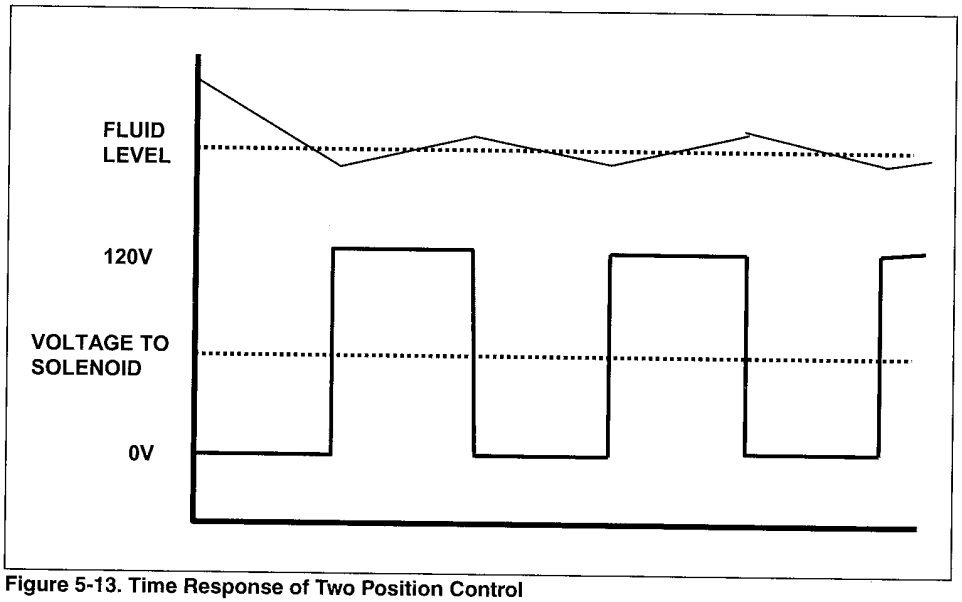


Figure 5-13. Time Response of Two Position Control

This system will work. It will not keep the level of liquid in the vessel very constant. The top of the liquid will go up, then down, then up, etc. But that is all that we required.

If we want to keep the level more constant, we have to use a different controller. Figure 5-14 shows a system that would work. Be aware that the level signal is more complex than in Figure 5-12. It is an analog signal. The signal varies between 4 mA (when the level is very low) and 20 mA (when the level is very high). Not very long ago, most controllers were mechanical or pneumatic. They received analog signals that represented the process value as a position of a mechanical lever or a pressure of instrument air. In those cases, the controller would do all of the calculations as mechanical or pneumatic operations on the input and would output a mechanical or pneumatic signal. Controllers of this type have been largely replaced because of the need for frequent, difficult maintenance. Electrical controllers, with few or no moving parts, are not as subject to wear and vibration.

With a system like this, the controller can recognize a very small increase in level and output a control signal to decrease, by a very small amount, the flow into the vessel. The relative amount that the valve must be closed to keep the level constant is proportional to the relative amount that the level is above its desired value. A proportional controller, with a selectable Proportional factor, would work for this situation. The algorithm for such a situation is shown in Figure 5-15.

The Integration Group of The Americas Ex. 1007-Page 65
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001118

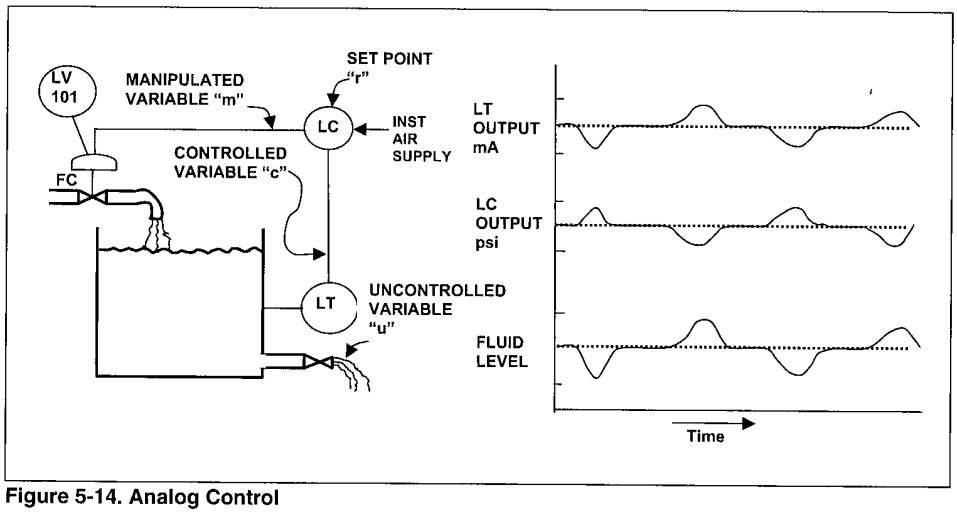


Figure 5-14. Analog Control

If the pressure upstream of the control valve were to change, or if any of several other factors were to change, this algorithm would not respond quickly enough to keep the process stable. Integral and Differential factors would have to be added to the algorithm to address these problems. The mechanical, pneumatic, or electrical parts that would have to be added to the controller would make it more complex, expensive, and difficult to maintain. But it is possible to build a controller that is capable of controlling process level, temperature, or pressure as tightly as necessary. An algorithm for a more general controller, including Proportional, Integral, and Differential factors, is shown in Figure 5-16.

Since we seem able to write a mathematical description for each of these controllers, someone might ask if it would be possible to do the controller function in a computer. The answer is, "Yes." As computers became less and less expensive, they became the basis for building controllers. Just as important, as computers became more and more capable, they were able to handle multiple functions, one after another. One computer is capable of providing the functional equivalent of several older controllers.

5-6. Controllers in RTUs

RTUs are now made from small computers. Shortly after this began, controller algorithms were programmed into the RTU. Flow totalizers, power factor calculators, and logic solvers soon followed. Any function that can be described by a mathematical formula, or algorithm, can be solved by the computer in a sufficiently complex RTU. The signals are gathered from field sensing devices. The algorithms are solved. Control instructions are sent out to valves or other control actuators. This happens

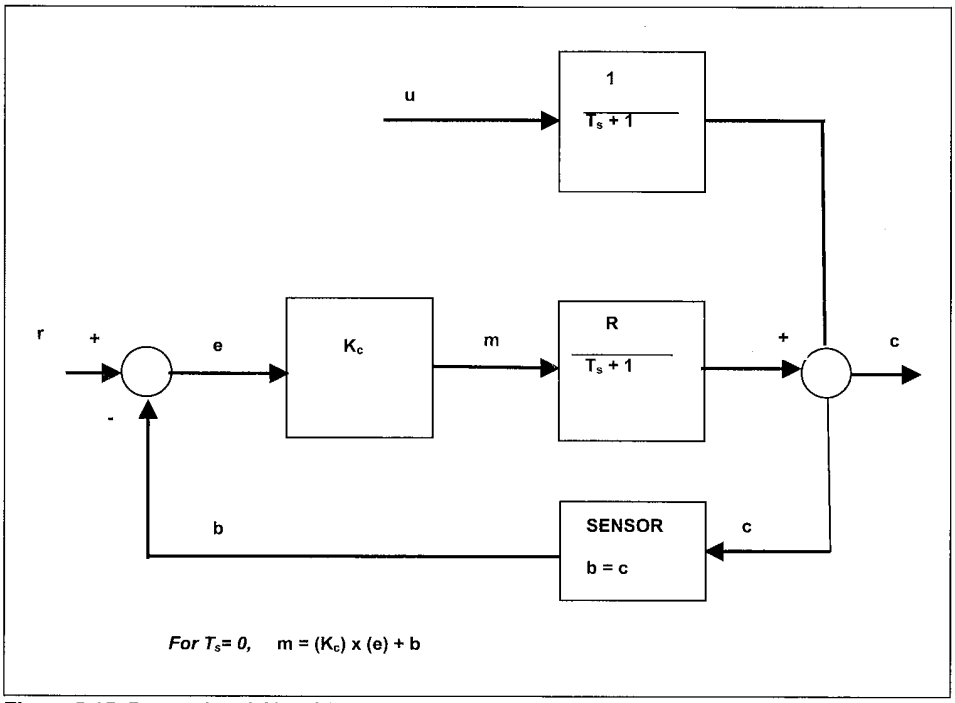


Figure 5-15. Proportional Algorithm

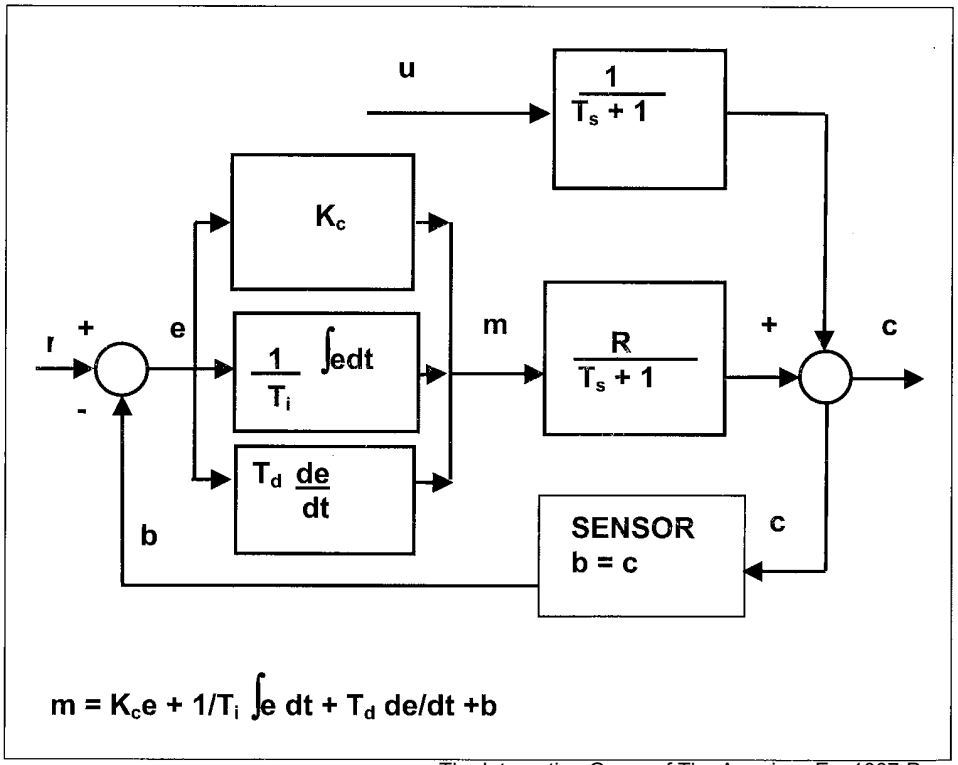


Figure 5-16. General Proportional, Integral and Differential Algorithm

The Integration Group of The Americas Ex. 1007-Page 67
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001120

very fast, in the order of milliseconds or less, and then the RTU does it all again. Scan periods in RTUs are very short.

Certain safety-related functions, like fire or smoke detection and toxic gas concentration, are solved in dedicated hardware. It is not because they have technically difficult algorithms, but because the regulatory agencies that certify them require them to be stand-alone devices.

With sensors measuring the process variables and actuators adjusting process parameters, controllers solving algorithms to control the actuators in response to the measured variables, and the whole system tied together by wiring or some similar communication system, the field process near the RTU can operate according to design.

This unit has concentrated on some of the considerations to be kept in mind when applying sensors and actuators. As used in SCADA, these devices may not be significantly different from the instruments that fulfill similar functions in any highly automated plant in a similar industry; however, they will be different from instruments that are designed to be read directly by a human operator. SCADA sensors and actuators tend to be expensive to buy and to maintain, a fact that should be taken into account when you develop cost estimates for SCADA installations.

Unit 5 Exercises:

5-1. *Why is electric wire the most common medium for moving signals between the RTU and the field devices?*

5-2. *What special feature of oil and gas processing increases the cost of many of the sensors used in those industries?*

5-3. *What is the primary purpose of a marshalling panel? Name three other purposes.*

5-4. *For what are field termination boxes used?*

5-5. *Why are engineering charges higher for SCADA than for most other projects?*

5-6. *Name four factors that would increase the cost of a project if the same type of sensor were purchased from multiple manufacturers.*

5-7. *Why do maintenance costs peak at the beginning of a SCADA project?*

The Integration Group of The Americas Ex. 1007-Page 68
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001121

Unit 6: Field/RTU Communications

The Integration Group of The Americas Ex. 1007-Page 69
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001122

Unit 6

Field/RTU Communications

Before the control algorithm can be solved, the information gathered by the field sensor must be delivered as an input to the controller or RTU. Some communication must happen between the sensor and the RTU. Then, after the algorithm is solved, some communication must happen between the RTU and the actuator. This unit will discuss some of the methods that are used to effect this communication.

Learning Objectives—When you have completed this unit you should:

A. **Understand the differences between analog and digital methods for communicating information.**

B. **Be clear on the way that analog signals can be changed to digital signals and back.**

C. **Know the Three Rules of Communication and how the choice of topologies may affect these rules.**

6-1. Three Rules of Communication

There are three general rules that describe what is needed for communication to be successful between a talker and a listener.

1. Talker and Listener must use the same medium.
2. Talker and Listener must use the same language.
3. Talker must not talk when someone else is talking.

Rule 1: Field communication normally uses twisted copper wire as the medium of communication between RTUs and instruments. It is possible to use optical fiber, and more and more, we are seeing small dedicated radios as the medium of communication. The important point here: If the instrument is going to use twisted copper wire, the RTU must use twisted copper wire. If the instrument is going to use optical fiber, the RTU must use optical fiber. The medium must be the same.

Rule 2: There are several languages that can be used between field instruments and RTUs. Most existing instruments use a language that carries its information in the amount of current in a copper wire loop that connects the instrument and the RTU (see Figure 6-1). The process transmitter measures the variable of interest (e.g., fluid level) and adjusts

The Integration Group of The Americas Ex. 1007-Page 70
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001123

the amount of current flowing through the transmitter according to some formula. The minimum level may result in 4 milliamps of current. The maximum level would then result in 20 mA of current. These minimum and maximum levels are normally adjustable to meet the process requirements. 4 to 20 mA is a normal range for analog process transmitters. In the past, 0 to 50 mA was a standard, but if the wire loop were broken, 0 mA would flow, which meant that there was no clear indication that the loop was still working. With a 4- to 20-mA standard, a broken wire would be recognized as such if 0 mA were flowing. Normally the RTU or a dedicated controller will provide a supply of electrical power to the instrument and the instrument will control the current flowing through the loop.

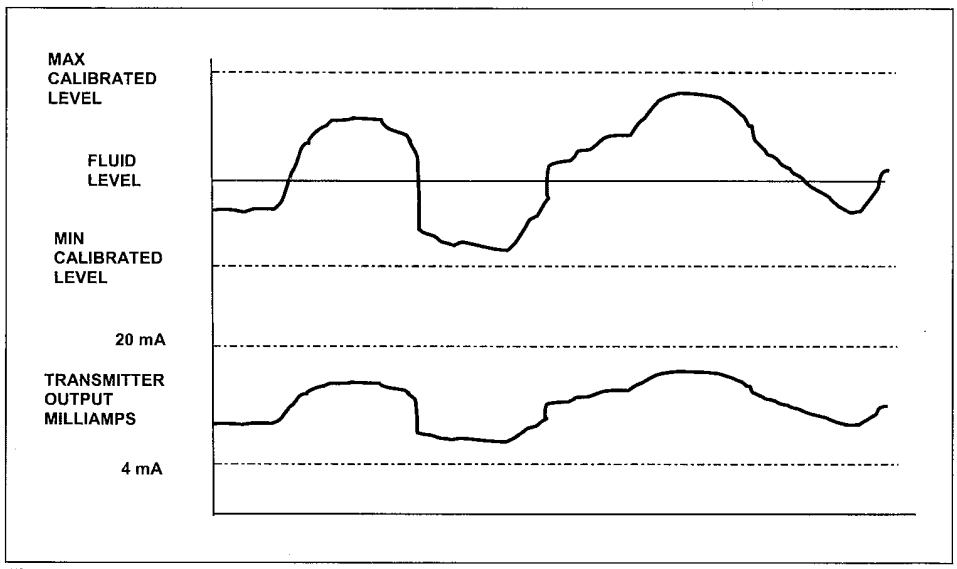


Figure 6-1. 4- to 10-mA Transmitter for Level Measurement

Rule 3: Interference that could occur if the receiver were talking when a message is sent to it is not often much of a problem. It almost never happens that an RTU talks to an analog transmitter. If it does, it uses a separate wire pair or a method of communication different from 4- to 20-mA loop current. The potential problem of one transmitter talking when another transmitter is talking is not an issue because each transmitter that uses 4- to 20-mA loop current is connected to the RTU by its own twisted-pair copper wire medium and feeds into a dedicated input circuit on the RTU.

The signal that goes from the RTU to the field actuator further illustrates the point about speaking the same language. After the RTU has calculated what message it wants to send to a control valve (for example), it outputs

The Integration Group of The Americas Ex. 1007-Page 71
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001124

an electrical signal. Since most valves understand an instrument air pressure language, not an electrical language, a translator is needed between the RTU and the valve. These translators are called transducers in the process control industry (see Figure 6-2 for the rest of this discussion).

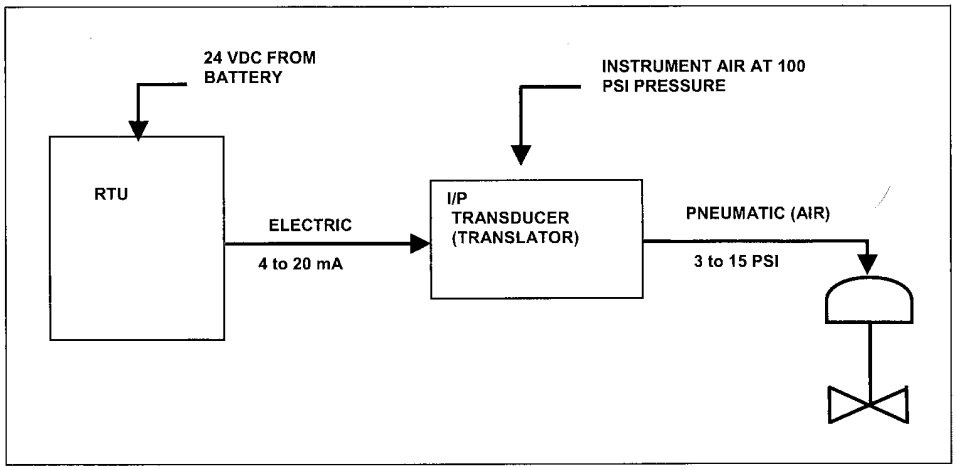


Figure 6-2. Transducer from 4-20 mA Electric to 3-15 psi Pneumatic

The RTU outputs an electrical signal that is a direct current that varies between 4 and 20 mA. It is received by a transducer, sometimes also called an I to P transducer or just an I to P, since it will change the language from electric current (I) to air pressure (P). The I to P receives air from the instrument air compressor at about 100 psi, and outputs 6 psi if it receives 4 mA from the RTU. It outputs 30 psi if it receives 20 mA from the RTU. This air pressure provides power to open or close the valve by an amount proportional to the current output by the RTU. The 6 to 30 psi is one popular air pressure language, but not the only one. Smaller valves may use 3 to 15 psi. Larger valves, requiring more power to open and close, may use 10 to 50 psi.

Very large valve actuators may be powered by hydraulic actuators, in which case, the transducer will convert an electric signal of 4 to 20 mA into a hydraulic signal of 100 to 500 psi to operate the actuator (see Figure 6-3).

6-2. Analog Pneumatic and Hydraulic Signals

Historically, process instruments were first built for reading directly by a human operator. The operator would then communicate to the process by turning a knob or moving a lever. When automatic controllers became available, analog signals were developed to feed directly into the controller. These first controllers were mechanical, and the field signals were either mechanical, pneumatic, or hydraulic. Unless the signal was

The Integration Group of The Americas Ex. 1007-Page 72
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,242,078
WB_00001125

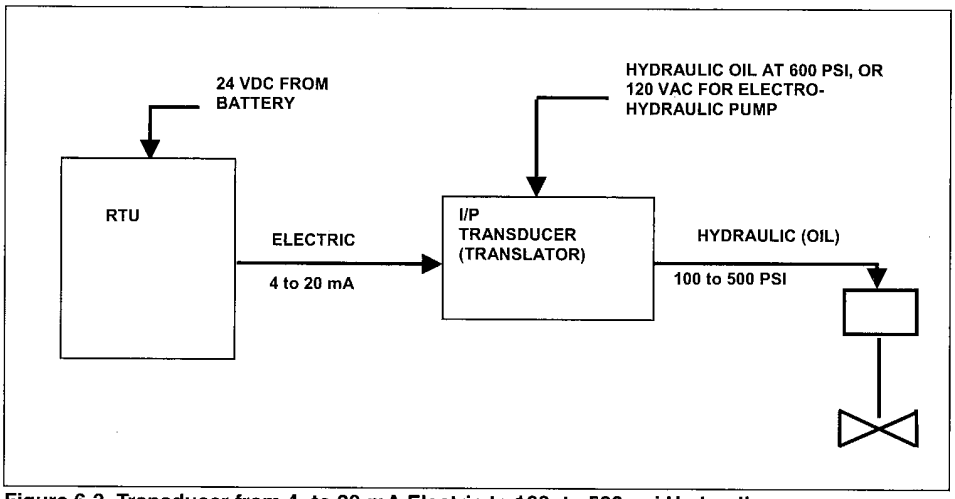


Figure 6-3. Transducer from 4- to 20-mA Electric to 100- to 500-psi Hydraulic

mechanical, the medium that was used to allow the process sensor to pass its pneumatic or hydraulic signal to the controller was metal tubing. One run of metal tubing had to be installed between each sensor and the controller, and one run of metal tubing had to be installed between each controller and the actuator that it controlled. Labor for installing these tubing runs was expensive. The space taken up by many tubing runs became significant. Tubing connections eventually leaked, causing loss of instrument air or hydraulic fluid and the subsequent loss of measurement and control.

Hydraulic systems caused the most problems and had the best reasons to be replaced. Not only did lost hydraulic fluid cost more to replace than instrument air, it also made a big mess.

One of the advantages that pneumatic or hydraulic communication systems have is that in addition to providing the data about the process, they also provide the power needed to move the parts inside the controller that do the calculating. They can provide the power to move the actuator, both against an opposing spring and against the force of the process (see Figure 6-4).

6-3. Analog Electronic Controllers

When pneumatic and hydraulic controllers developed into electronic controllers, the signalling medium between sensors and controllers, and between controllers and actuators, shifted from pressurized fluid inside metal tubing to electric current carried in an electrical conductor.

At the sensor end, there is relatively little power required. The controller or RTU is usually the location where electrical power, in the form of a low

The Integration Group of The Americas Ex. 1007-Page 73
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001126

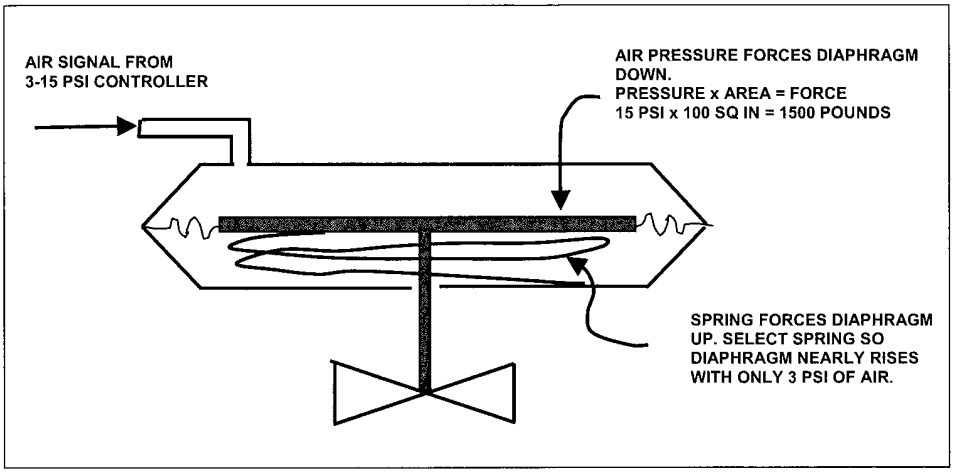


Figure 6-4. Air Signal Can Provide the Power to Move the Valve

voltage, direct current supply, is applied to the circuit (see Figure 6-5). The circuit is a low resistance loop, which means that with no additional control, a high current would flow through the loop. But the sensor is equipped with a variable constant-current device that will limit the current. The device is variable so that when the sensor detects a low process measurement, let us say temperature, it will allow a small amount of current to flow in the loop. When the sensor detects a high temperature, it will allow a large amount of current to flow in the loop. At the controller end of this loop, a precision resistor is connected to ground. If we know the value of the resistor, and we measure the voltage drop across this dropping resistor, we can calculate the current flowing in the loop. The sensor has been calibrated to have a direct relationship between the current and the process measurement, so we know the measurement—temperature in this case.

In all discussions until now in this book, a low process measurement has been translated into a low current. This is not necessary. It may be that 4 mA will be used to represent the highest expected temperature and that 20 mA will be used to represent the lowest expected temperature. The important thing is that both the sensor and the controller must speak the same language (i.e., they must both know what 4 mA means and what 20 mA means).

It also is not necessary that there be a linear relationship between the process measurement and the current output from the sensor. It may be an exponential function, an inverse function, or any kind of function that will produce an effective message. The controller must be programmed to understand what is meant by any value between 4 mA and 20 mA.

The Integration Group of The Americas Ex. 1007-Page 74
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001127

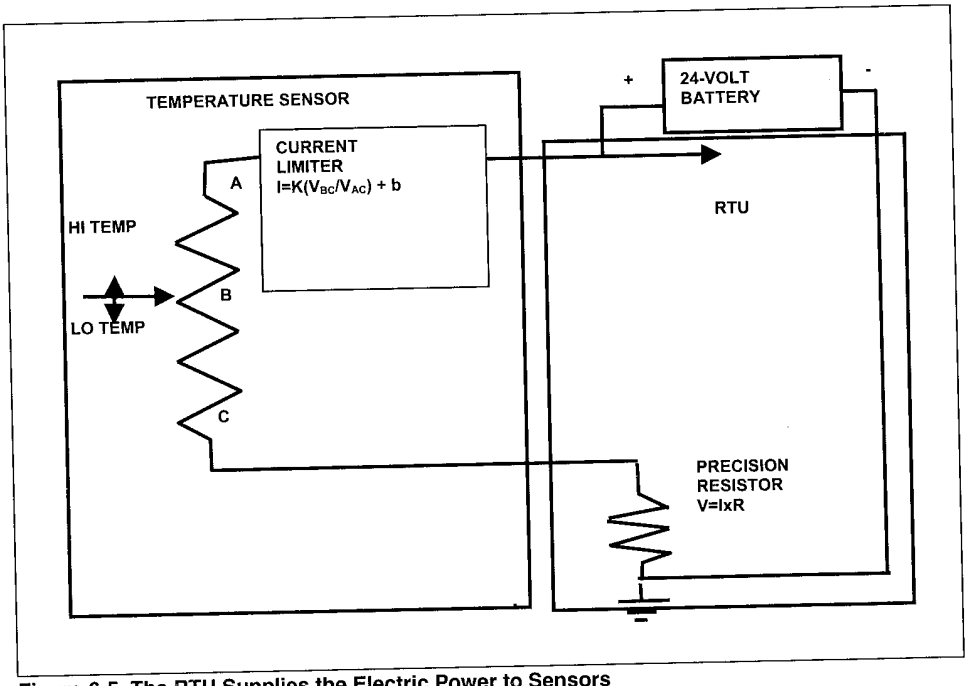


Figure 6-5. The RTU Supplies the Electric Power to Sensors

As mentioned earlier, it may be that the wire between the controller and the sensor has broken or there is a corroded connection where the wire joins either the sensor or the controller. If so, no current will flow, or less than 4 mA will flow. As a standard practice, this condition is treated as a communication failure.

The electricity that is provided by the RTU or the controller is low voltage DC. There are regulations that define low voltage DC, and they usually limit the voltage to 32 volts. In fact, most industrial low voltage systems are nominally 24 volt. Electrical code regulations, which are the basis for cable manufacturing standards, have resulted in standard instrument electrical cables that are used in most industrial applications. These cables are available with conductor sizes from very small, 24 AWG (American Wire Gauge), to large, 14 AWG. Even though we limit the amount of current flowing through the loop, it is necessary that the wire resistance of the loop does not result in too much of the voltage drop happening before the dropping resistor can introduce its voltage drop. Longer loop runs therefore require larger gauge cable. Short runs may be able to use a wire smaller than 24 AWG, but it is difficult to work with wire smaller than 20 or 24 AWG.

There are several advantages to using electrical cable as an analog signal medium in process areas. It is much less expensive than metal tubing, both to buy and to install. It takes up less room in process trays and in the

The Integration Group of The Americas Ex. 1007-Page 75
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00738 U.S. Patent No. 9,249,979

WB_00001128

control rooms or RTU buildings. Once electrical cable has been installed and tested, it is less likely to degrade than metal tubing, which is subject to leakage caused by vibration.

Over the years, several standard signal levels have been accepted. At present, 4- to 20-mA and 10- to 50-mA current loops are the two most commonly applied. Signal levels based on voltage instead of current are more susceptible to noise.

6-4. Digital Electrical Communication

Digital electrical communication is replacing analog electrical communication in new installations. Two main advantages are that more than just the basic process measurement can be made, and that the digital signal is less susceptible to noise than an analog signal.

New technologies that are successful in replacing older technologies often use the same infrastructure as the older technology. Digital Electrical Communication operates with the same voltage levels and sources and can use the same electrical cable systems as analog electrical.

In the same way that automobile manufacturers introduced us to a new technology by building a hybrid between internal combustion engines and electric motors as the driving force, measurement instrument manufacturers got us used to the concept of digital communication in the late 1990s with a hybrid communication system called HART. HART stands for Highway Addressable Remote Transducer. It still uses a current loop to send the main signal, for example, process pressure from the instrument to the controller. In addition, HART allows the instrument to send such things as calibration data, instrument health status, and device identification via a digital signal. In fact, as many as forty data items are available in a HART-enabled instrument.

Note that it must be a HART instrument. Implicit in this is that the instrument is "smart." It is computer based and has been built to have the additional communication capability.

HART operates by superimposing a Bell 202 digital signal over the 4- to 20-mA current signal (see Figure 6-6). Bell 202 is a frequency-shift key system and its standard defines a "one" as a frequency burst of 1200 Hz for $1/1200^{th}$ of a second. It defines a "zero" as a frequency burst of 2200 Hz for $1/1200^{th}$ of a second. This allows as much as 1200 bits per second of digital information to be piggy-backed onto the standard 4- to 20-mA signal without distorting the analog signal.

The developers of HART recognized another very important advantage of the system. Now, the controller could also send messages to the

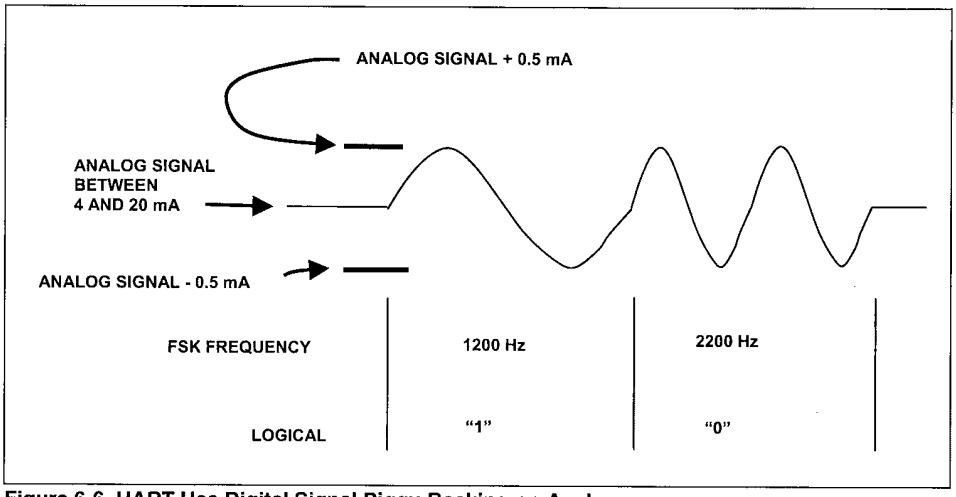


Figure 6-6. HART Has Digital Signal Piggy-Backing on Analog

instrument. The type of message that a controller may want to send to a sensor might be "change the sensor range to 10 to 150 psi" if the controller noticed that the process pressure was getting too close to the maximum of its previous 10 to 100 psi range. With both the controller and the sensor now able to talk, rules had to be put in place to ensure that both do not talk at the same time. HART uses a Master-Slave system to ensure that the sensor (slave) only talks in response to an order from the controller (master).

There are other messages that the controller can send to the sensor to increase its effectiveness. These messages depend on the type of sensor that is being addressed.

HART can also be used to send messages from the effector device such as a valve controller to the RTU. The signals that are piggy-backed on the current signal can include information that shows wear, play, and other factors that can be used to predict equipment life remaining.

6-5. How Digital Works—Analog to Binary to Digital

All data moved between the MTU and the RTUs is binary data. It may have originated as binary data as the status condition of an on-off switch or it may have been converted to binary form from analog form. Figure 6-7 shows the output from a limit switch that may be used to indicate the state of a valve. In Figure 6-7(a), the valve is open and the switch output is a steady +5 VDC. In Figure 6-7(b), the valve is closed and the switch output is a steady 0 VDC. Note that the switch output is 0 VDC at any time that the valve is not completely open. This feature can be used to advantage. If you need to know when the valve is not completely closed,

The Integration Group of The Americas Ex. 1007-Page 77
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001130

you can arrange to have it output +5 VDC at all times except when it is completely closed. The bottom part of Figure 6-7 shows a switch output for a valve that is open, then closed, then open, and so on.

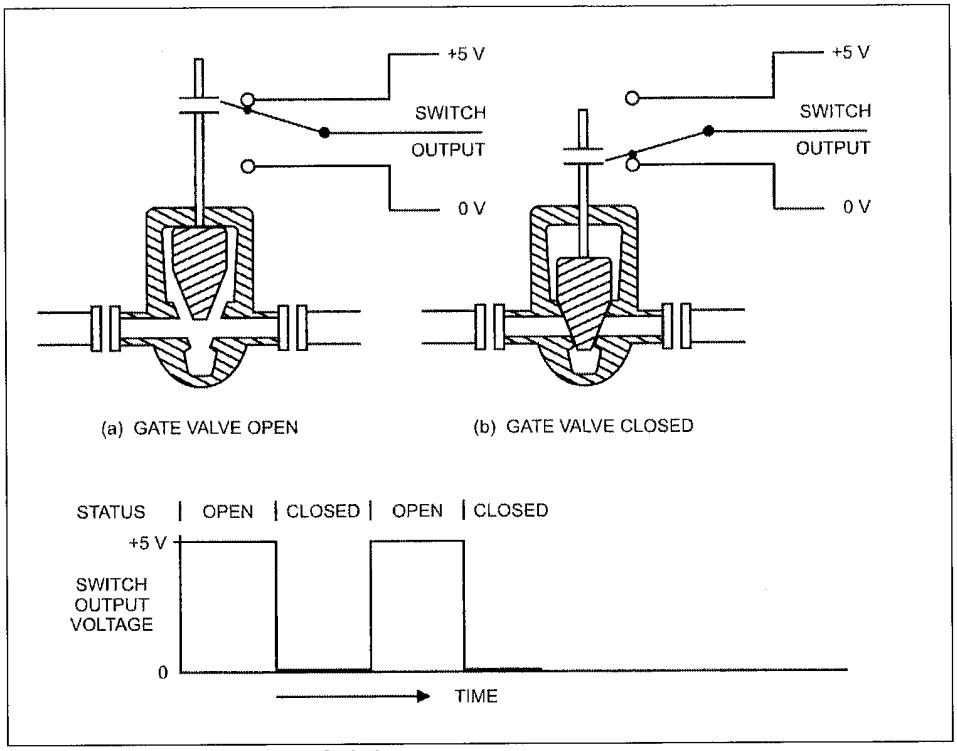


Figure 6-7. Output from a Limit Switch

Figure 6-8 shows how the switch output from a valve is changed to a bit. The word *bit* stands for **b**inary dig**it**. A single-bit register, or flip-flop, is shown in Figure 6-8(a). The valve status switch output is fed to the enable input of the register, and the register binary output signal comes out of the register. A continuous series of pulses, called the clock, is fed into another input of the register. Figure 6-8(b) shows the timing of the logic. Shortly before time = 1, the valve opens and the valve status switch output moves from 0 volts to +5 volts. At time = 1, the clock pulse goes positive (from 0 volts to +5 volts) and this, combined with +5 volts on the enable input of the register, causes the register to output a "1" (see bottom line of Figure 6-8(b).

The valve stays open for several clock periods and closes after time = 3. When it does, the enable signal goes to 0 volts, but this does not change the register output. When the clock goes positive at time = 4, the register output changes to a "0".

The Integration Group of The Americas Ex. 1007-Page 78
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001131

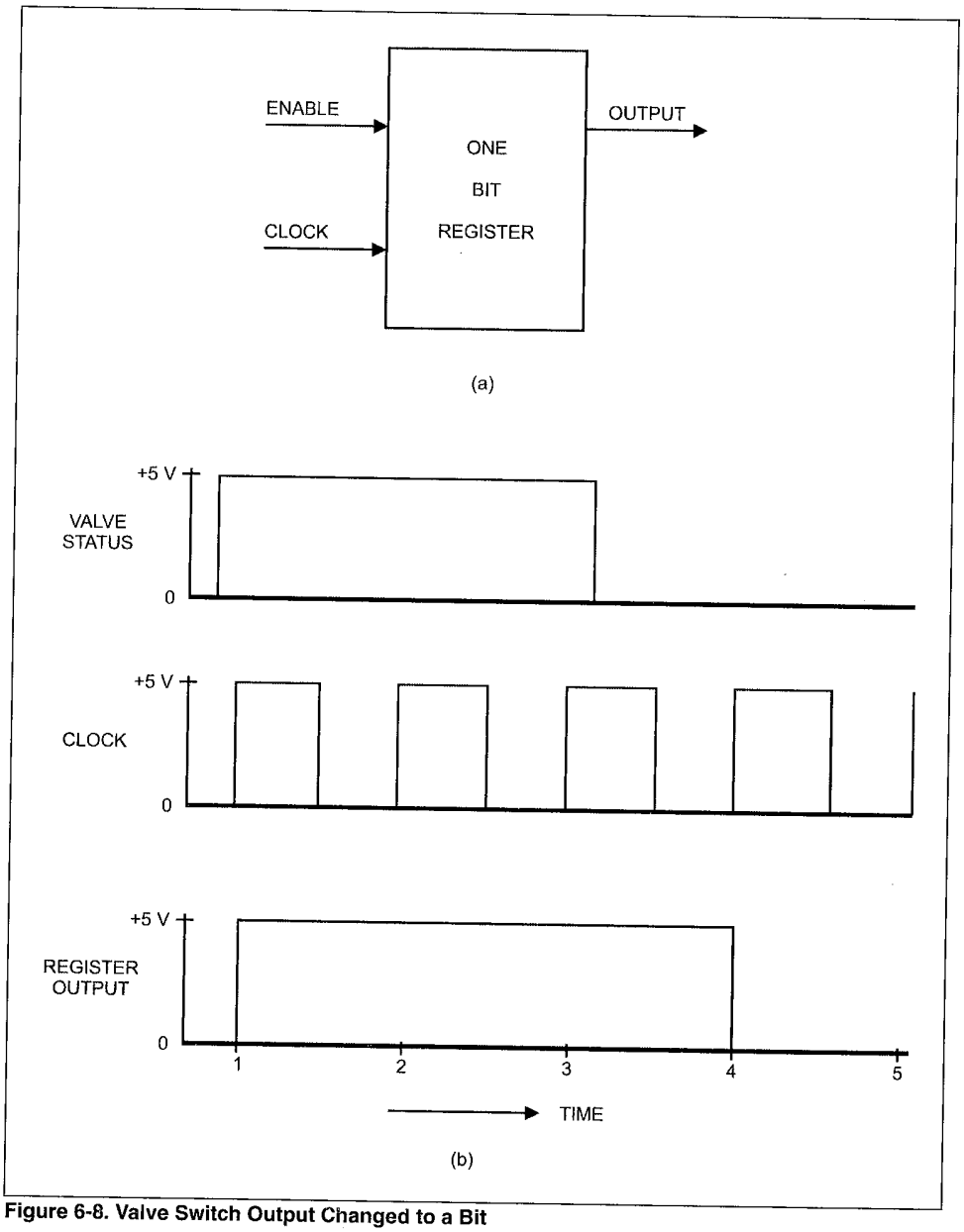


Figure 6-8. Valve Switch Output Changed to a Bit

Figure 6-9 shows how an analog signal is developed to represent a valve position. When the valve stem rises to its fully open position, the transmitter output will be +5.000 volts. When the valve is fully closed, the output will be 0.000 volts. As shown in Figure 6-8, the output is at some value between 0 and 5 volts. Let us assume that it is +3.000 volts.

Instead of going directly to a register, the +3.000 volt analog signal is sent to an analog-to-digital converter (ADC), shown in Figure 6-10, that

The Integration Group of The Americas Ex. 1007-Page 79
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001132

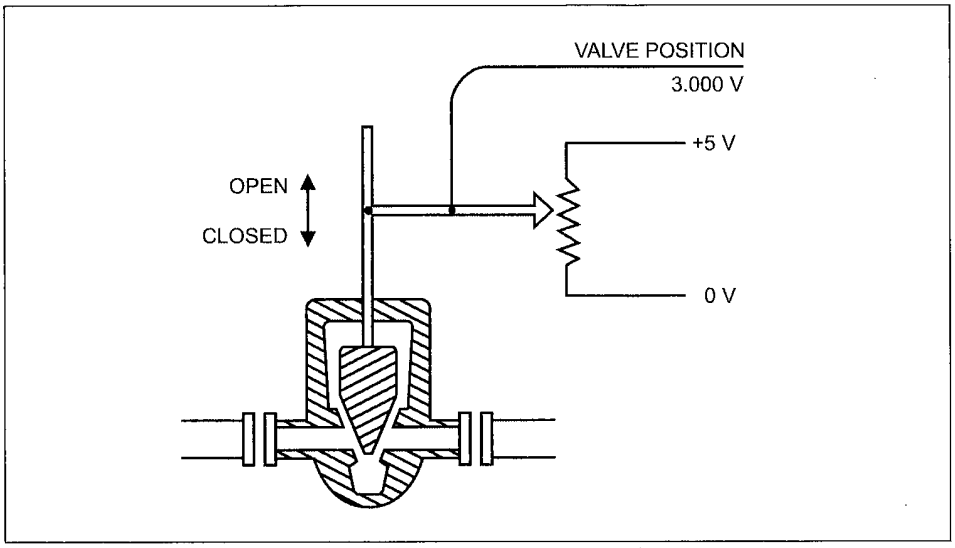


Figure 6-9. Analog Signal Developed to Represent a Valve Position

changes it to a series of binary digits and stores these bits in a register. Usually, there are eight to 16 bits in this kind of register, but for simplicity, only four bits will be used in this example. The largest bit is usually called the most significant bit or MSB; the smallest bit is the least significant bit or LSB. The MSB is one half of the value of the full-scale amount. Each succeeding bit is one half the value of the previous bit.

Starting at the top left of Figure 6-10, the +3.000 volt signal is fed to the first stage of the ADC. The converter tries to subtract 2.500 volts from it. It can (because 3.000 is larger than 2.500) so it outputs a +5 volt signal to the enable input of 2.500 volt bit (MSB) of the register. The next clock pulse forces the register MSB to output a "1". The remainder (3.000 – 2.500 = 0.500 volts) is fed to the second stage. The converter tries to subtract 1.250 volts from it. It cannot (because 0.500 is smaller than 1.250) so it outputs a 0 volt signal to the enable input of the 1.250 volt bit of the register. The next clock pulse forces that register bit to a "0".

The remainder (still 0.500 volts) is fed to the third stage. The converter tries to subtract 0.625 volts from it. It cannot (because 0.500 is smaller than 0.625) so it outputs a 0 volt signal to the enable input of the 0.625 volt bit of the register. The next clock pulse forces that register bit to a "0". The remainder (still 0.500 volts) is fed to the fourth stage. The converter tries to subtract 0.3125 volts from it. It can, so it outputs a +5 volt signal to the enable input of the LSB of the register. The next clock pulse forces that register bit to a "1".

The Integration Group of The Americas Ex. 1007-Page 80
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001133

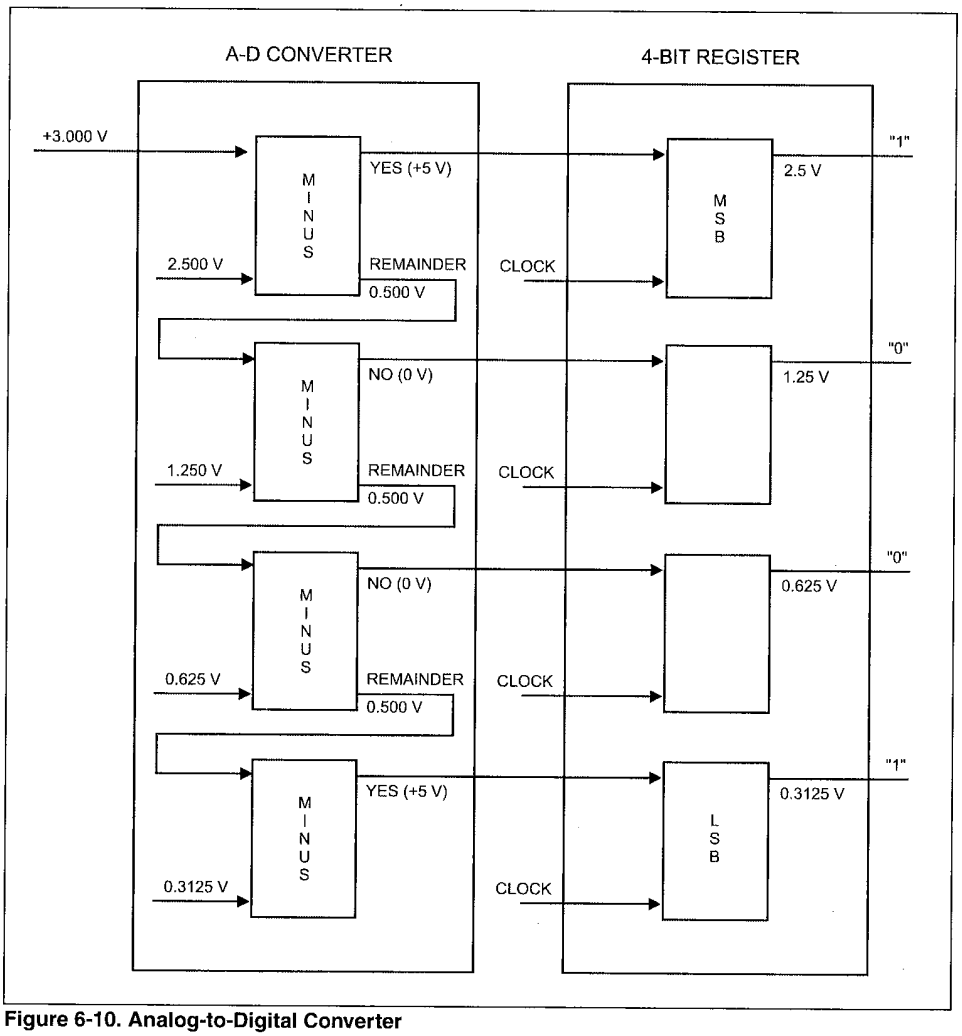


Figure 6-10. Analog-to-Digital Converter

The result is a four-bit binary word that describes the 3.000 volts as follows:

MSB 1 x 2.500 volts	=	2.500 volts
+0 x 1.250 volts	=	0 volts
+0 x 0.625 volts	=	0 volts
+LSB 1 x 0.3125 volts	=	0.3125 volts
		2.8125 volts

Because a four-bit register provides precision of 1 in 2^4, or 1 in 16, this is as close as we can get to 3.000 volts. For some applications, the signal will vary from positive to negative, using up one additional bit. Additional bits would provide additional precision. The accuracy of analog-to-digital

The Integration Group of The Americas Ex. 1007-Page 81
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001134

converters is sometimes defined in terms of plus or minus one-half of the least significant bit (LSB).

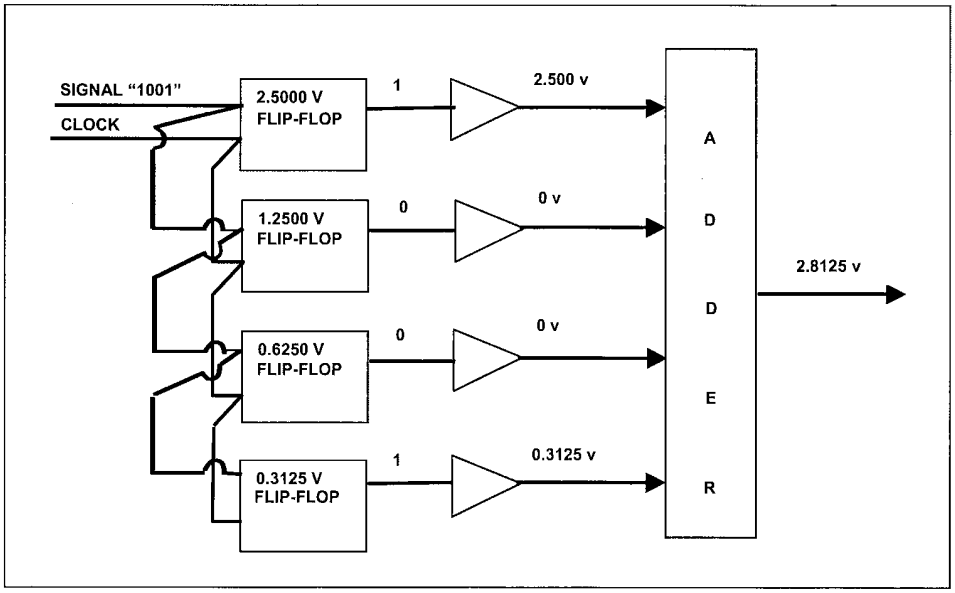


Figure 6-11. Digital-to-Analog (DAC) Converter

Digital-to-analog converters (DACs) are devices that take a digital signal and convert it to an analog value. Figure 6-11 shows how this can be done.

Using the digital value established by the ADC in Figure 6-10, we feed the most significant bit into the enable port of the top flip flop, the second most significant bit into the enable port of the second flip flop, and so on. When the clock pulse triggers each of these flip flops, 5 volts will appear at the output of each flip flop that had a "1" on its input. 0 volts will appear at the output of each flip-flop that had a "0" on its input. The voltage switches each have two inputs. One is a very precise voltage that will either be allowed to pass through the switch or will be blocked. The other input is the switching signal. If it is 5 volts, the precise voltage will pass through. If it is 0 volts, the precise voltage will not pass. The largest voltage is one half of the full scale of the DAC. The second voltage is exactly one half of the first, and so on. The adder block on the right adds each of its inputs and then outputs a result that is the sum of the inputs.

In this case, the output will add 2.500 volts plus 0.3125 volts to output 2.8125 volts.

The Integration Group of The Americas Ex. 1007-Page 82
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00738 U.S. Patent No. 9,243,978
WB_00001135

6-6. Parallel or Serial?

Digital signals can be moved in two ways: parallel or serial. In the last section, the four bits were moved in parallel. By clocking each of the four flip-flops at the same time, we were able to move the data out of these flip-flops and on to another location. This is a very fast way to move information, but it requires a path for each bit of data. Normally our digital words are 16 bits long. Sometimes they are as little as 8 bits long; sometimes as much as 32 bits. Occasionally 64 bits are used, but that is seldom needed in SCADA applications.

Because a separate path is required for each bit when parallel communication is used, this method is only used for very short distances. Because of its speed, it is the preferred method within logic solvers like computers.

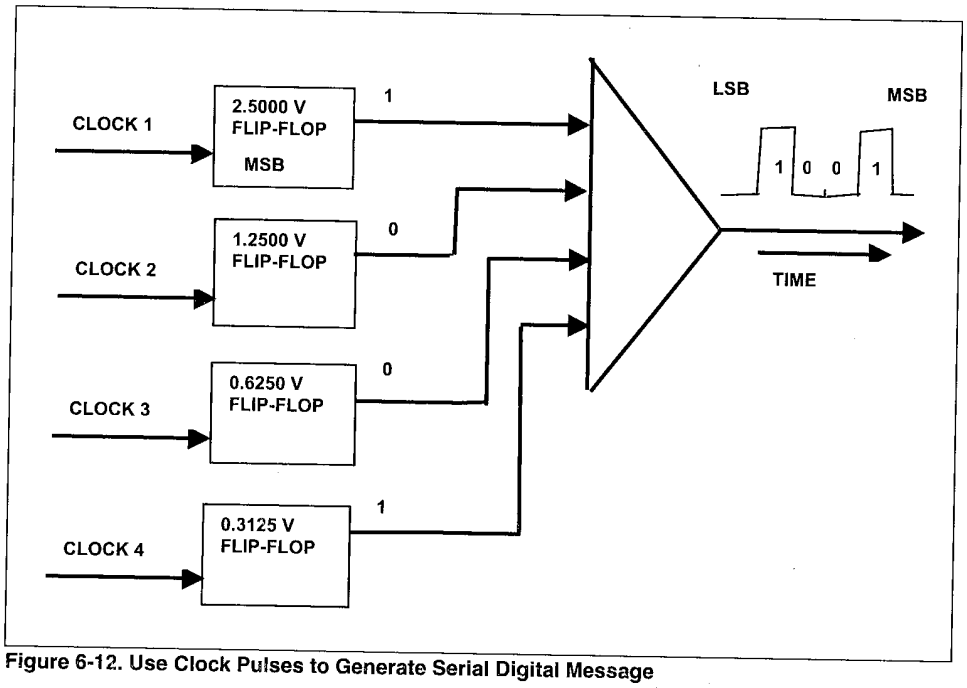


Figure 6-12. Use Clock Pulses to Generate Serial Digital Message

If the distance is more than about three feet (one meter), it is normal to send the data out in serial form (see Figure 6-12). Instead of clocking all four flip-flops with the same clock pulse, we will steer the clock pulses, with the first one going to the MSB flip-flop, the second one going to the next most significant bit flip-flop, and so on. The outputs of all four flip-flops are tied together and the wave form coming out of the flip-flops will appear as shown on the right side of the figure. It is a serial signal that takes longer to move, but requires only one data path. One data path costs

The Integration Group of The Americas Ex. 1007-Page 83
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001136

less to provide than four or eight or sixteen data paths. If we are using copper conductors or optical fiber for the communication medium, using a single data path will provide a cheaper way to build the system. If the communication medium is to be radio, we can do it with just one carrier frequency. There are many cases where multiple carrier frequencies are just not available to a SCADA system. In these cases, the ability to communicate serially means the difference between being able to build a system and not being able to build a system.

6-7. Communication Topology

In this unit, we have learned that often, each instrument is connected to the RTU by its own dedicated wire loop. If you were to draw this layout in a very simple way, you would have something called a "Star" layout, as shown in Figure 6-13(A). Characteristic of this layout, each instrument is connected to the RTU but is not connected to any other instrument. Implicit in this statement is the expectation that no instrument can speak to any other instrument. A condition of having only one path between the instrument and the RTU is that the RTU cannot talk to the instrument if the instrument is talking to the RTU. Remember that the talker, per Rule 3, must not talk when someone else is talking. The way around this problem will be discussed in more detail in Unit 8, when we talk about Master-Slave communication.

Another of the common layouts (topologies) that are used in SCADA communication is called "Bus" and is shown in Figure 6-13(B). In this layout, any one of the instruments is connected to all the other instruments. The RTU is also connected to all the instruments. In effect, they appear to have equal status. They are "peers." This layout allows for any entity to talk directly to any other entity. As you would expect, there are potential problems with two entities talking at the same time, but methods have been developed to prevent that from happening. This topology is much used for instruments that use digital communication methods to talk/listen with RTUs.

The third layout type is called "Ring," as shown in Figure 6-13(C). It suffers from the same problem of instruments talking when they should be listening, and gets around the problem a similar way. One other problem with this topology is that in order for a message to be sent to a non-adjacent station, the message must be passed from station to station until it reaches the correct station. This takes time, but the ring topology can be used successfully in some conditions. We will discuss this in Unit 8 when we consider some problem paths for radio-based communication.

The Integration Group of The Americas Ex. 1007-Page 84
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001137

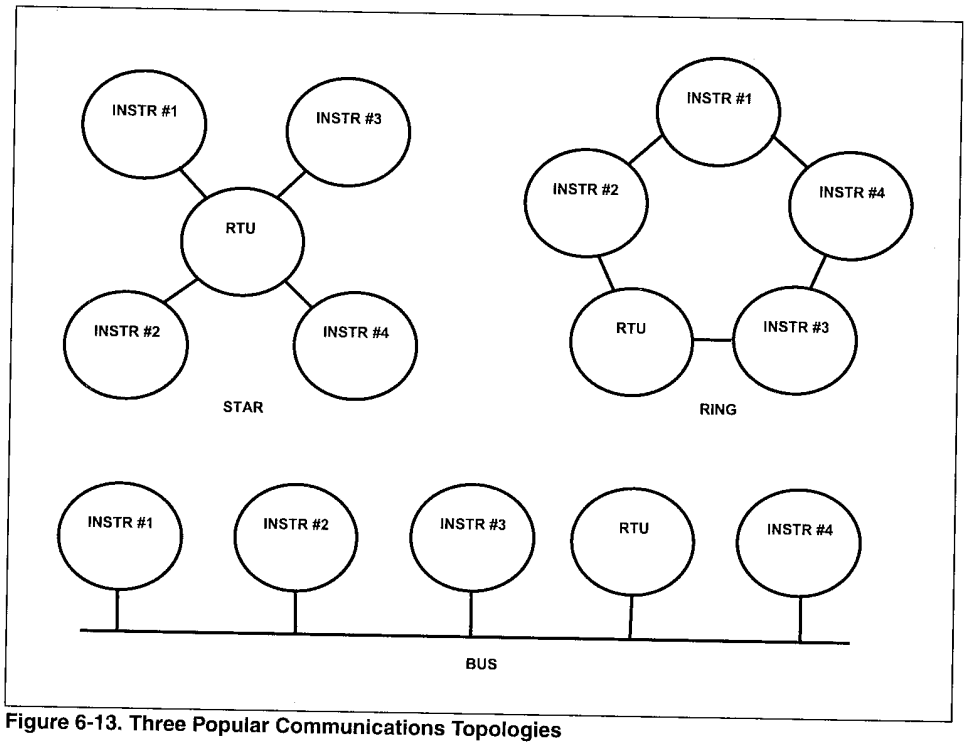


Figure 6-13. Three Popular Communications Topologies

6-8. Fieldbus and Similar Standards

When they became capable of using digital methods instead of analog to communicate to the RTU or controller, process field instruments left behind some of the hurdles that limited the way they could be applied to process control. One of the expansions in their capability was that they could now share a common electrical conductor loop. Another was that they could pack much more information into the messages that they sent to their controller. A third was that they could now receive messages in addition to sending them.

In the mid 1980s, ISA formed a committee to describe in detail the capabilities and limitations of a digital method of communication between field instruments and control equipment. Other organizations, some of them corporate entities, formed groups to do the same thing. Over the next twenty years, work progressed, leading to definitions of Fieldbus, Profibus, and several other bus-based communication standards.

This text cannot describe the details of any of these standards, which are lengthy, and the reader is referred to the detailed descriptions available as IEC (International Electrotechnical Commission) Standard 61158, which includes eight related standards that use digital communication methods to move process field signals to and from instruments and control devices.

The Integration Group of The Americas Ex. 1007-Page 85
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001138

IEC 61158 is a very comprehensive document that describes communication protocols, signal levels, timing, physical cable layout and nearly every other variable that can be considered. IEC 61158 is based on the ISA Fieldbus series of standards.

Unit 6 Exercises:

6-1. *What advantage does a 4- to 20-mA signal standard have over a 0- to 50-mA standard?*

6-2. *In percent, what precision does an eight-bit digital measurement have?*

6-3. *Name at least three reasons why electrical cable is preferred as a medium of analog signals than is metal tubing.*

6-4. *How does an instrument in a star topology system know when to send a message to the RTU?*

6-5. *How can a digital signal be superimposed on an analog signal without affecting the value of the analog signal?*

6-6. *Why should it be possible to transmit data faster using parallel communication than using serial communication?*

6-7. *Profibus is one of the digital standards included in IEC 61158. Name at least one other.*

The Integration Group of The Americas Ex. 1007-Page 86
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001139

Unit 7: Remote Terminal Units—RTUs

The Integration Group of The Americas Ex. 1007-Page 87
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00720 U.S. Patent No. 9,243,475

UNIT 7

Remote Terminal Units—RTUs

A SCADA system is characterized by three element types: RTUs, communications, and MTUs. In Unit 2, we briefly discussed what RTUs and MTUs are and what they do. In this unit, we will go into more detail about how RTUs do the things they do.

Learning Objectives—When you have completed this unit, you should:

A. **Understand what an RTU does, how it does it, and why.**

B. **Know how this element fits into a general SCADA package and how it interfaces with the process and with the communications links.**

C. **Recognize the various hardware types that may be used for an RTU.**

7-1. What Does an RTU Do?

Earlier, we discussed the RTU's functionality in terms of a "black box" that accomplished some poorly defined functions. Figure 7-1 shows, in block form what signals come into the RTU; Figure 7-2 shows what signals leave the RTU. To review them briefly, the RTU gathers information from the field in the form of analog or digital values, alarm and status points, and metered amounts. It converts this data into digital form and keeps the information available in memory until the MTU asks for it. It then codes and transmits the information to the MTU. In addition, when the MTU instructs, the RTU sends signals to open and close valves, or turn switches on and off, outputs analog or digital signals that may represent set points, and outputs pulse trains to move stepping motors. As discussed in Unit 5, the RTU also solves algorithms, allowing it to act as a controller or a pulse totalizer for functions that can not wait for a decision from the MTU. This collection of functions may seem like a limited repertoire, but it is sufficient to accomplish all the control, remote control, and monitoring that needs to be done.

RTUs are now being offered that have the ability to receive and send messages to field devices in serial format, usually RS-232, or Fieldbus. In most cases, this feature does not increase SCADA's capability; however, it does simplify some of the field local data transfer. In the near future, we can expect that serial communication in the form of Fieldbus will be more commonly used than the 4–20 mA analog signals used now. At the time this is written, Fieldbus installations are preferred over 4–20 mA analog

The Integration Group of The Americas Ex. 1007-Page 88
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001141

installations for industrial control applications, and this can be expected to extend into SCADA applications.

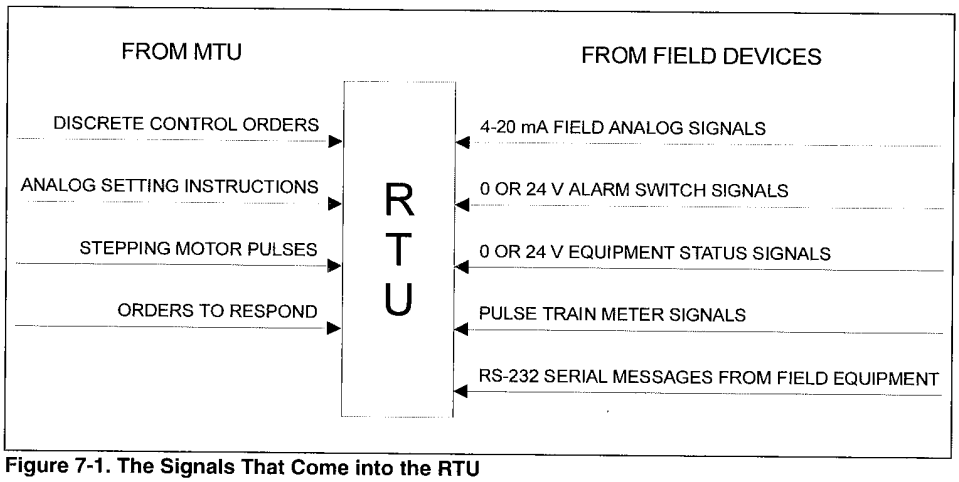


Figure 7-1. The Signals That Come into the RTU

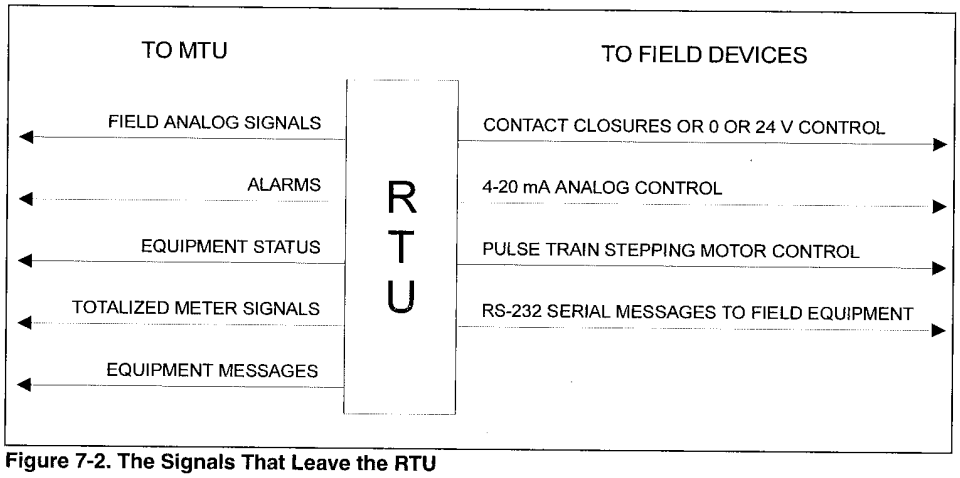


Figure 7-2. The Signals That Leave the RTU

7-2. Communications Interface

Figure 7-3 expands the "black box" description of an RTU. Although some analog-based RTUs are still in use, modern RTUs are essentially microcomputers with special equipment at one end to interface with the long range communications link and with special equipment at the other end to interface with the sensors, actuators, and calculators in the process. While the RTU is in receive mode, part of the communications interface equipment (the modem, which will be discussed in Unit 8) receives a serial signal from the communications medium. This signal is conditioned (converted) to a stream of bits that are either ones or zeros. At this stage,

The Integration Group of The Americas Ex. 1007-Page 89
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001142

the signal is binary, although some analog signals may have been coded into binary for transmission to the RTU. Using rules that were established when the communications protocol was established, another part of the communications interface interprets the string of ones and zeros and passes the information on to the rest of the RTU.

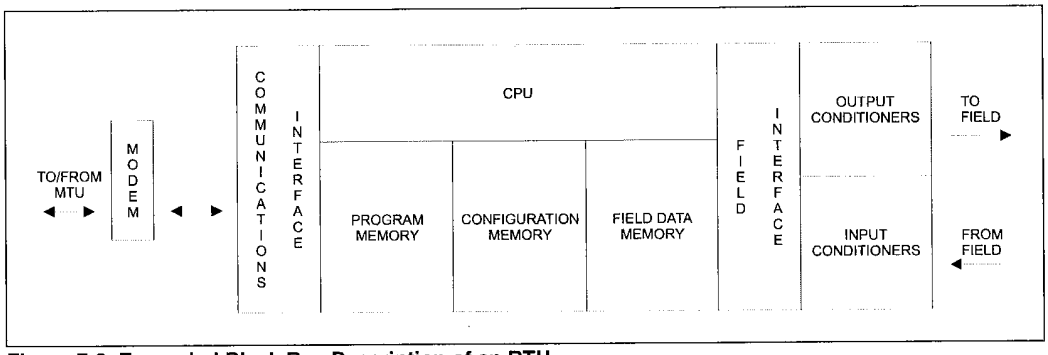


Figure 7-3. Expanded Black Box Description of an RTU

Note that in some cases the interpretation function is accomplished by the modem, and in other cases by the microprocessor that forms the heart of the RTU. When this type of architecture is used, part of the program that translates the ones and zeros into useful information is called a "protocol driver" program. Also, for this architecture, the interrupt feature, which is critical to the operation of an RTU, must execute quickly or there must be a buffer to store the incoming message. If the first bit or bits of a message are not recognized, the message will not be understood. The RTU does not know when a message is going to be sent to it. It must always be in the listening mode (except when it is in the talking mode). However, while it is listening, the RTU will be doing many other things. Early RTUs used electronic circuits that were dedicated to listening continuously for incoming messages, decoding them, storing the message in buffer memory, and passing pertinent information to the rest of the RTU when the RTU demanded it. Modern RTUs accomplish these functions with the protocol driver program run by the RTU's central processor unit (CPU).

7-3. Protocol Detailed

It may be useful to use an example to review how a simple message is received and decoded at the RTU. Recall that the information is received at the modem located at the RTU as a series of ones and zeros modulated onto a carrier frequency. The modem strips off the carrier and makes a series of ones and zeros available to the RTU. For the purposes of this discussion, the protocol will be one based on standard ANSI/IEEE C37.1-1979. It is a protocol that at one time was widely used for SCADA and has all the elements needed for most SCADA communication. One of the

WB_00001143

important points of this discussion is that you learn how much detail is required in a protocol description.

In Figure 7-4 (and all other figures like it in this text), the leftmost bit of information is the first one received. Figure 7-4 shows the three basic fields in the binary message. They are "Message Establishment," "Information," and "Message Termination." For the example shown in the figure, message establishment and message termination have fixed lengths. Information fields may be of different lengths.

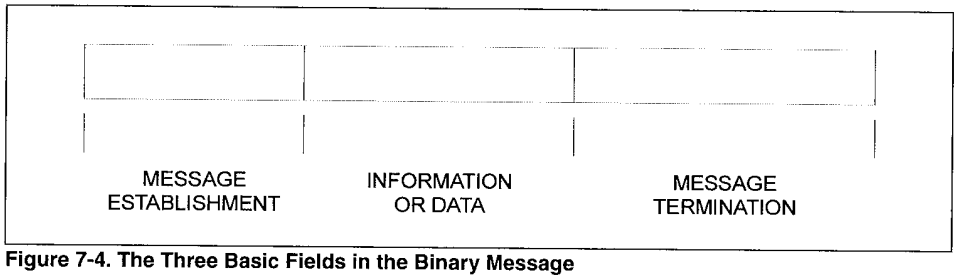


Figure 7-4. The Three Basic Fields in the Binary Message

The "Message Establishment" field has two subfields, as shown in Figure 7-5. The first is called "Sync" (for synchronizing) and is one octet (eight bits) long (00010100). It establishes that an MTU is sending a message to an RTU. In addition to telling all RTUs that a message is coming, this subfield also is used to synchronize the RTU clock to the MTU clock. The second subfield, the "Remote Address," defines to which RTU the message is being sent. It also consists of eight bits. Normally, eight bits would allow two-to-the-eighth-power or 256 RTUs to be addressed, but only 254 of these addresses are valid (0 and 255 are reserved for another use). The address in this figure, 00001011, decodes to RTU number 11. Unless both subfields are recognized by the RTU, the RTU will know that the message is not for it, will ignore the rest of the message, and will reset its message establishment registers to wait for another message. The RTU with the matching address (RTU number 11) will listen for the next stage, which is "Information."

The "Information" field shown in Figure 7-6 consists of several subfields of data that the MTU wants to pass on to the RTU. The first subfield, "Function," defines the type of response that the RTU must make to this message or the type of control message that the MTU is now transmitting. There are eight bits in this subfield, so there are two-to-the-eighth-power or 256 potential responses that could be demanded and/or 256 control message types that could be sent. An example of a control message might be binary number seven, which could mean "Close all of the following valves." An example of a response demand message might be "Send the totalized flow values for fluid meters." With 256 possible options, there

The Integration Group of The Americas Ex. 1007-Page 91
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001144

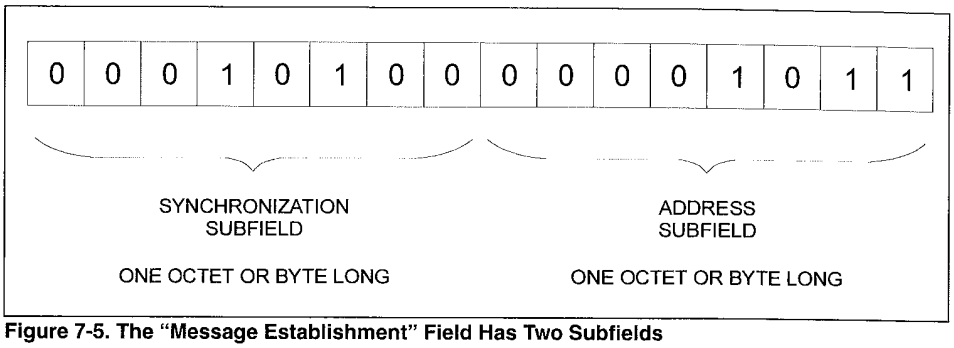


Figure 7-5. The "Message Establishment" Field Has Two Subfields

are more than enough choices to cover all of the needs for any SCADA system, although the functions chosen for one SCADA system may be different from the functions chosen for a different SCADA system.

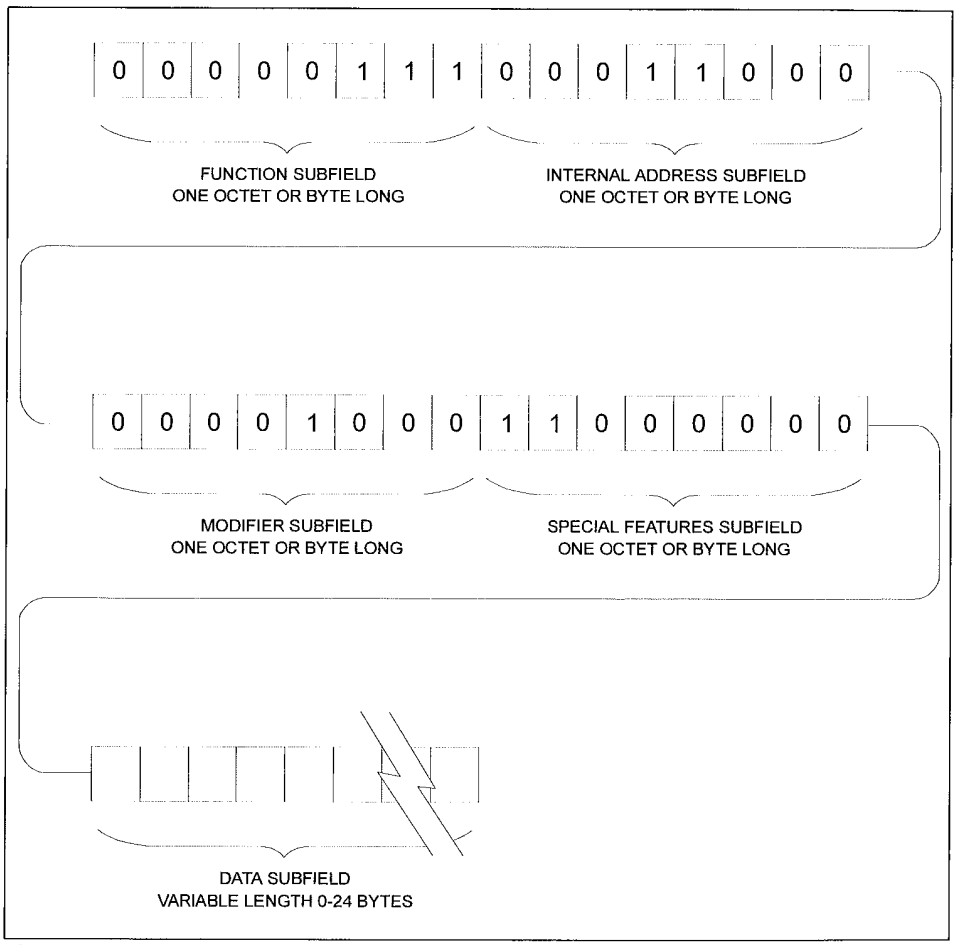


Figure 7-6. Information Field

The fourth subfield, "Special Orders," allows for special instructions to the RTU, including resetting trouble flags, resetting communication error flags, and "Expect a long message at the next command." A 1 in the most-significant-bit position (left side) means that the MTU acknowledges that the RTU has executed a restart and instructs the RTU to reset this flag. A 1 in the second MSB means that the MTU acknowledges that the RTU has detected a communication-related problem and instructs the RTU to reset this flag. The second subfield, "Internal Address," subfield identifies the location within the RTU. For example, this subfield might say "24," meaning that memory register 24 is the location of the FIRST of those flowmeter totals to be sent, or it might mean "The valve identified in memory register 24 is the first in the list of valves to close." The third subfield, "Modifier," defines the number of data units to be transferred. In this example, if the modifier were eight, the MTU would be asking that totals from meters 24 to 31 (24 + 8), inclusive, be sent. Or it might mean "The eight valves including and after the one identified in memory register 24 are the ones to close."

The "Expect a long message at the next command" flag special order deserves some explanation. Most SCADA systems do much more monitoring than they do controlling. For this reason, messages from the MTU to the RTUs are usually shorter than messages from the RTUs to the MTU (in this protocol). The MTU will alert an RTU when it is going to send a long message that includes data subfields to the RTU.

The fifth subfield, "Data," provides for generalized data to be sent from the MTU to the RTU. For a message of the type used up until now in this example, the data subfield would have a length of zero. For other message types, it could be up to 24 octets long.

After the information field is complete, a "Message Terminator" field, which consists of one subfield, is sent (see Figure 7-7). This subfield, called the "Security Code" and consisting of 16 bits, is calculated at the MTU, based on the information sent by the MTU. As the RTU reads the information that it receives, it uses the same algorithm to calculate a 16-bit security code. It compares the security code received to the security code that it has calculated. If there is any difference at all, the RTU will reject the message and will increment its "Communication Error" counter. The security code algorithm will be discussed in Unit 8—RTU-MTU Communication.

When the entire message has been received and confirmed as correct, the RTU, in addition to all of the other things it has been doing, will perform the instructions contained in the message just received. This last message required that a certain group of fluid meter volumes contained in registers 24 to 31 be sent to the MTU. The RTU will now refer to its memory

The Integration Group of The Americas Ex. 1007-Page 93
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR2025-01[illegible]

WB_00001146

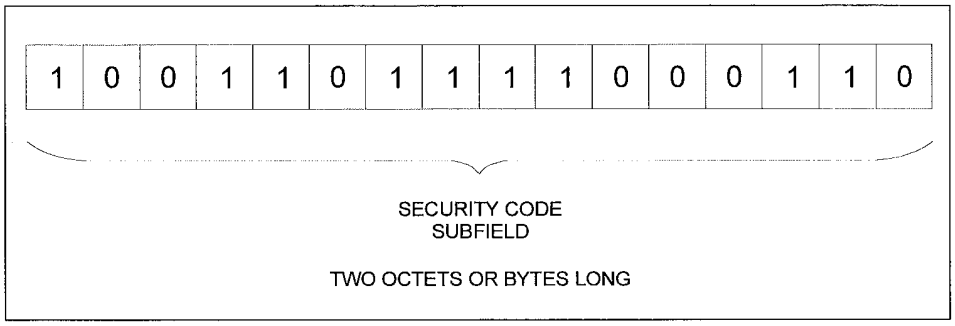


Figure 7-7. Message Terminator Field

registers, pull out the appropriate information, develop a message to the MTU according to similar rules and using the same protocol, and tell the MTU what those registers contain.

7-4. Discrete Control

Some of the messages from the MTU relate to control. They require the RTU to develop and transfer a signal to one of the field devices near its location. In this section, we'll first follow the activities that occur if a message is received by the RTU calling for it to open some two-position valves when the first valve location in memory is memory location 32 and the number of valves is two (see Figure 7-8).

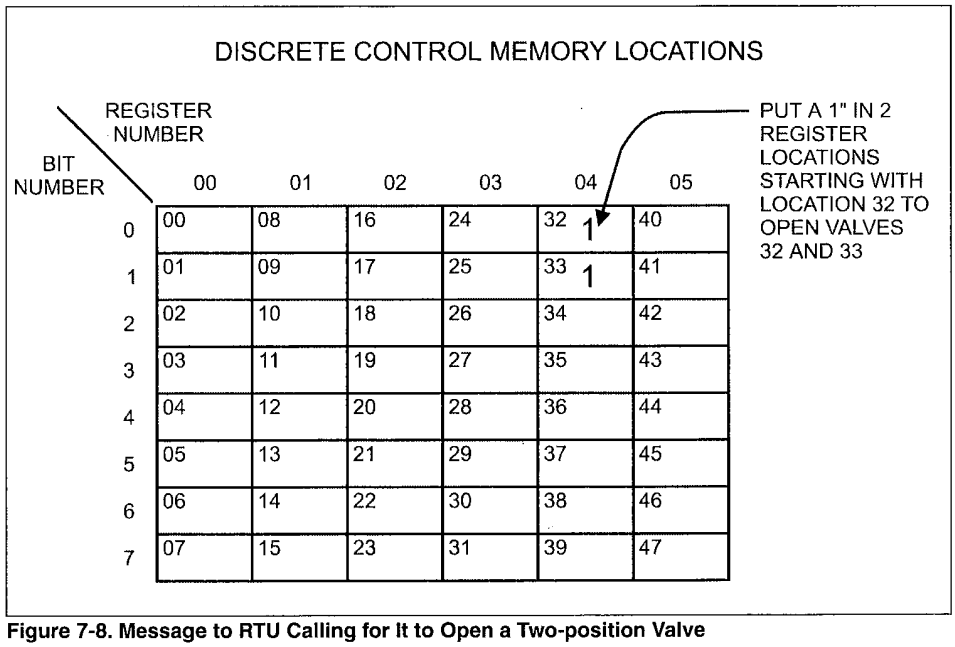


Figure 7-8. Message to RTU Calling for It to Open a Two-position Valve

The RTU will locate the registers that are allocated to controlling discrete valves. Notice that since each register is one octet or eight bits long and each bit is able to define "closed" position by 0 and "open" position by 1, each register can control eight discrete elements. The RTU will locate the first specified register position (position 32 in register 04) and will force it to a 1 state. It will then move to the second position (33) and will force it to a 1 state. A couple of milliseconds later, this register is routinely read (see Figure 7-9.) At this point, because these two registers have a 1 in their specified positions, the RTU will cause two control relay drivers on an output card to latch two relays closed. Each of these relays will drive a solenoid valve that will allow instrument air to open one of the valves. Notice that the latching, either at the relay driver or the relay itself, causes the effect to be "Fail to last position." This means that if the communication system fails after the message has been received to open the valves, the valves will stay open. If it becomes necessary to close them while the SCADA system is out of service, a manual or safety-instrumented system that acts to override the SCADA must be put in place.

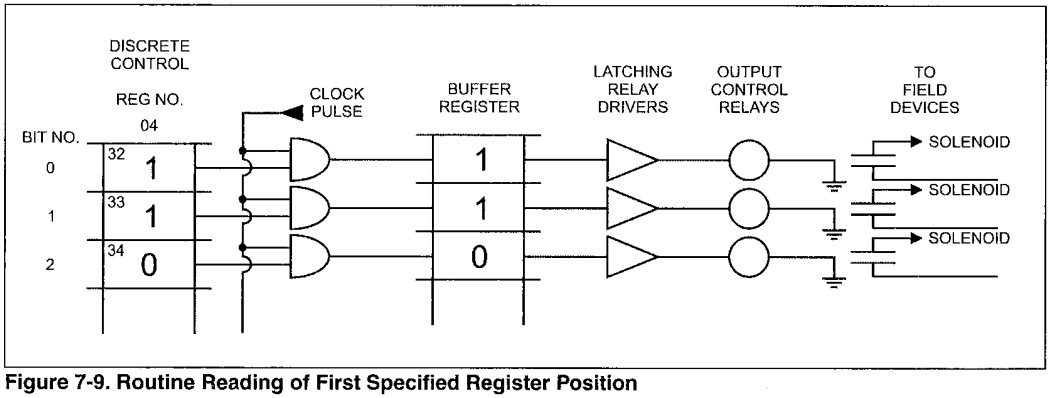


Figure 7-9. Routine Reading of First Specified Register Position

The same procedure would be used to turn a motor on. Instead of energizing a solenoid, the latching relay would close a motor starter. Most discrete binary controls can be effected this way.

7-5. Analog Control

Suppose the MTU instructed the RTU to open a valve, not all the way, but only to 75 percent of fully open. This would be handled by an analog control instruction. For this example, shown in Figure 7-10, the MTU message will call for analog output, register number 22, and set it at 75. In this case it takes more than one bit to define the requirement. Register 22 has eight bits, the same number that register 4 had in the last example. Now, however, more data is required to define the degree of openness of

The Integration Group of The Americas Ex. 1007-Page 95
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001148

the valve. Eight bits will allow one part in 2^8, or one in 256, which is about ½ percent. For many control applications, including this one, ½ percent is all that we need so eight bits of precision is adequate. Applications that need more precise control use part or all of a second eight-bit register. Sixteen bits results in a precision of one in two-to-the-sixteenth-power, or 1 in 65,536. For this example, eight bits of the twenty-second analog register have been set to 11000000, which is 75 percent of 256.

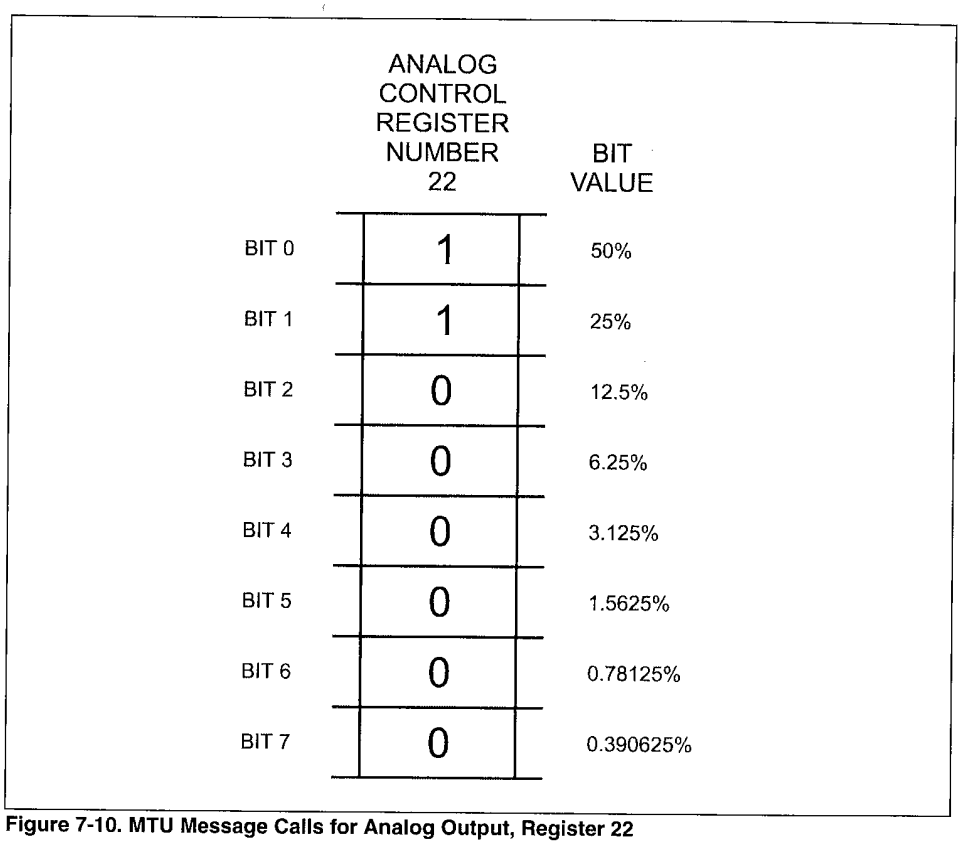


Figure 7-10. MTU Message Calls for Analog Output, Register 22

Now, when the clock strobe pulse comes by and these values are moved to a buffer register, something different will happen. In an analog output card (Figure 7-11) these bits must be reconstituted into an analog signal. For this exercise, assume that 10 volts will cause the valve to go 100 percent open, and 0 volts will cause it to go 0 percent open. The first bit (called bit 0) is the MSB. Because it is a 1, it turns on a voltage source that outputs 5.000 volts. The second bit, because it is also a 1, turns on a voltage source of 2.500 volts. The third bit, because it is a 0, does not turn on a voltage source of 1.250 volts. The fourth also does not turn on the 0.625 volt source, and so on. All of these voltages are added, and the resulting 7.500 volts is fed to a power driver. From here, it may be turned into a 4–20

The Integration Group of The Americas Ex. 1007-Page 96
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001149

mA signal. This would result in 0.75 x (20-4) + 4 =16 mA being sent to a valve so as to position the valve at 75% of full open position.

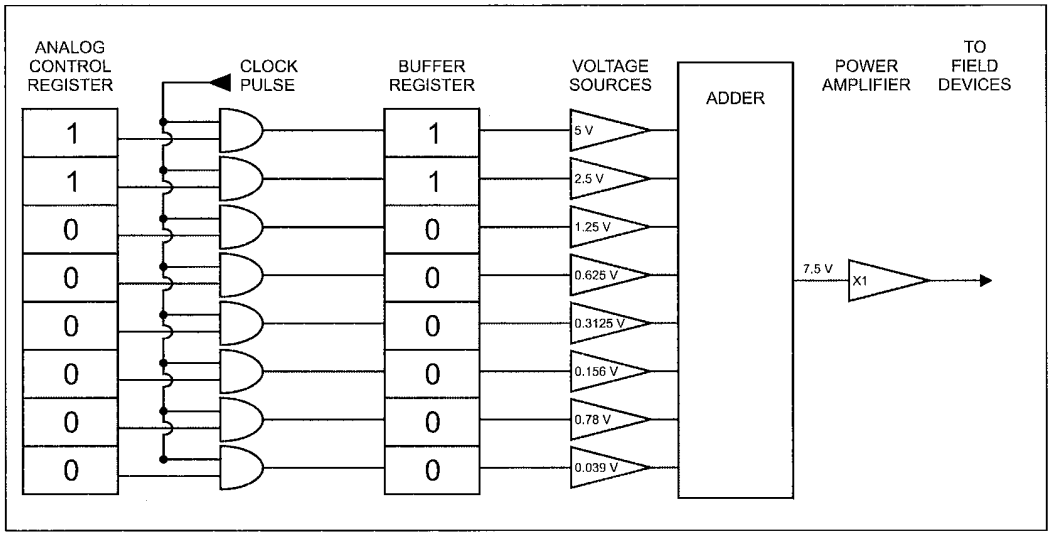


Figure 7-11. Analog Output Card

In fact, the signal would be more likely to act as the remote set point of a PID (proportional/integral/derivative) controller, and the output from the controller would control a valve, a louver, a machine speed, or any number of parameters that could be described by an analog value between 0 and 100 percent.

7-6. Pulse Control

The pulse control method of control is seldom used and will not be discussed in detail here. It allows a stepper motor to be incremented or decremented by a specified number of steps. The 16-bit register may have the zero bit set with a 1 to increment or a 0 to decrement. One of the remaining 15 bits will be set with a 1 for each pulse output that is required. All bits are not clocked out simultaneously from the buffer register; instead, they are clocked out one at a time and arranged to go to the stepper motor one after another (serially).

One of the reasons that this system is not popular is that each instruction to the motor requires knowledge of the motor's present position. In time, errors will accumulate in the supposed present position of the motor. It therefore becomes necessary to intermittently force the motor either to the full open or full closed position to reconfirm its present position. While this is not particularly difficult from a control point of view, it can have some very destabilizing effects on the process.

The Integration Group of The Americas Ex. 1007-Page 97
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00738 U.S. Patent No. 9,242,078

WB_00001150

Feedback position switches are now being applied to eliminate this problem, but the damage done by poor early applications makes this an unpopular method of control.

7-7. Serial Control

Many end devices, such as sensors and actuators, are equipped with serial output and input capability. This capability simplifies the movement of data between instruments and RTU registers. The technique was discussed in Unit 6.

7-8. Monitor Discrete Signals

One of the most common data acquisition functions that a SCADA system can be called upon to perform is the monitoring of discrete status or alarm points. These are sometimes called digital points. Consider Figure 7-12, which is the representation of a discrete alarm: In this case, a high-level switch on a hydroelectric reservoir. The wiper side of the switch, LSH-101, is supplied with +24 VDC from the RTU. When the water level gets high enough to open the switch, the voltage on the return wire will change from +24 VDC to 0 VDC. This new voltage will be recognized by a signal conditioning circuit in the RTU. Here, transients, AC noise, and the effects of switch contact bounce are removed, and the electronics transfers the conditioned signal, in this case a +5-volt level, into discrete input register number 20, bit 7, as a 1. The next time the MTU asks the RTU for the status of discrete input register 20, bit 7, the RTU will look at this bit and report that it is a 1. The MTU will then know that the water level in the reservoir is high.

Of course, if the water level had been low, the 24-volt signal would have continued to reach the signal conditioner, and the output of the signal conditioner would have been 0 volts. This would have been clocked into the register as a 0. A 0 discrete input register 20, bit 7, would be configured to mean that there is not a high level in the reservoir. Note that this does not mean that there is a reservoir low level alarm, just that there is not a high reservoir alarm.

Discrete inputs can inform on the status of a vast range of variables. Levels, pressures, temperatures, flows, valve positions, motor status, and so on, can be monitored using simple switches. By using special logic with relay contact output, it is also possible to get the status of high-radiation monitors, combustible gas alarms, out-of-limits pH analysis, and nearly anything else.

It is often important to monitor a process parameter to get more than a binary amount of information. For example, the actual height of liquid in

The Integration Group of The Americas Ex. 1007-Page 98
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001151

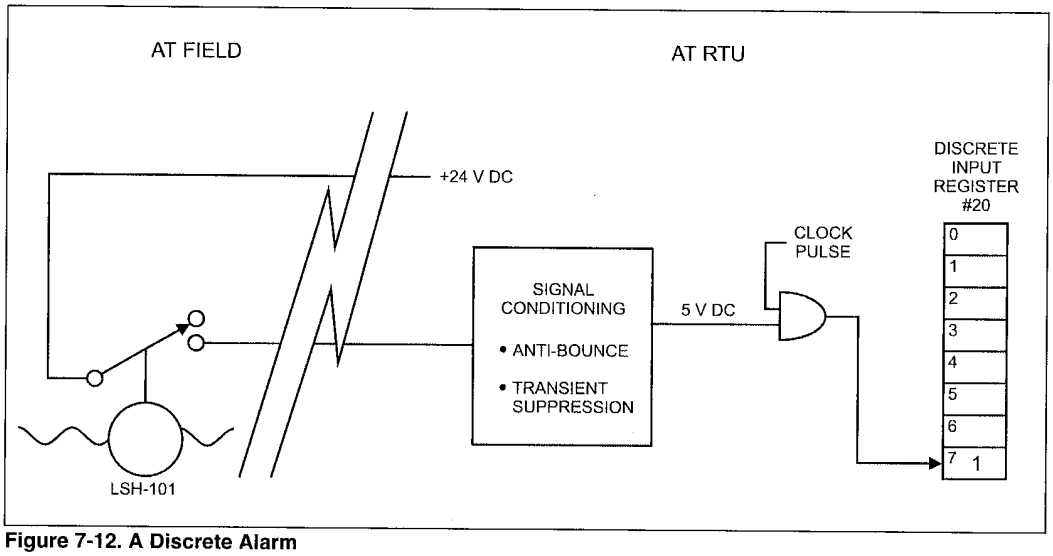


Figure 7-12. A Discrete Alarm

the reservoir, the speed of a motor, or the level of radiation may be needed. In these situations, a sensor is provided that changes the parameter of interest to a more easily monitored quantity, such as current.

In Figure 7-13, the float device on the surface of the reservoir modifies the 24-volt DC signal supplied by the RTU so that, over the range that interests us, the current varies from 4 mA to 20 mA. This current, fed through a 250-ohm resistor, results in a voltage of between 1 volt and 5 volts at the input of the circuit, which does some signal conditioning and then samples and holds the voltage. An analog-to-digital converter (ADC) then operates on the voltage, as has been discussed. The result is an eight-bit word that represents the 1-volt to 5-volts to within about ½ percent. If better accuracy were needed, and it seldom is, up to 16 bits could be employed. This word is clocked into a specific register, and the RTU, when asked, will send the contents of the register to the MTU.

7-9. Monitor Pulse Count Signals

Many sensors or local instruments that originally output their information via odometer-style readouts have been modified to be read by SCADA. Often, the least expensive way is to have the device send a string of pulses or interrupt a current from the RTU by opening and closing a relay contact in such a way that each open-close cycle represents a fixed, known amount. In this way, the RTU can count or accumulate these contact closures and infer from their sum how much the device has measured. Figure 7-14 shows how such a totalizer works. A totalizer may be external or internal to the RTU.

The Integration Group of The Americas Ex. 1007-Page 99
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001152

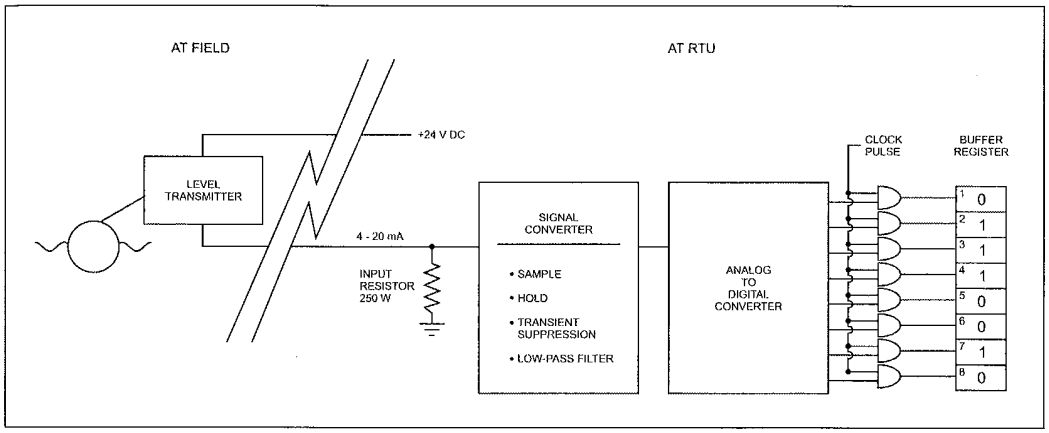


Figure 7-13. Float on the Surface of a Reservoir Modifies 24-volt DC Supplied by the RTU

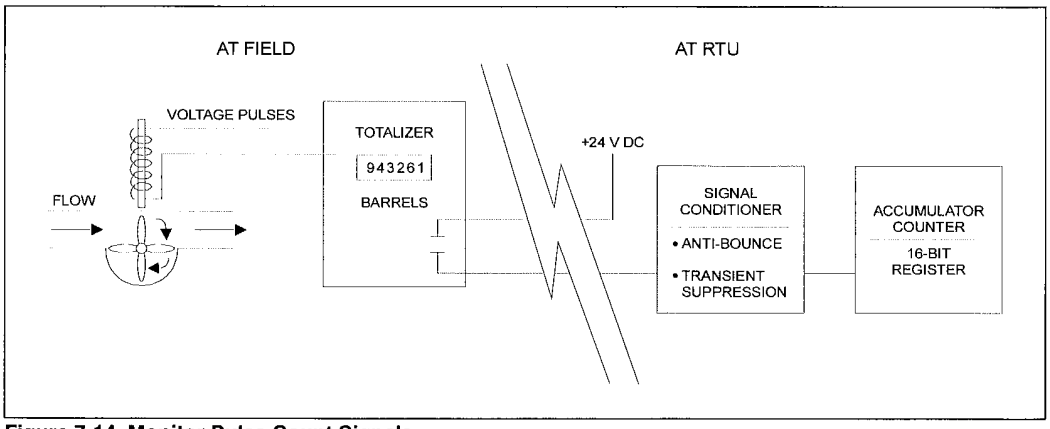


Figure 7-14. Monitor Pulse Count Signals

Here an external totalizer outputs a contact closure for (in this example) each barrel of oil that passes through a turbine meter. This contact closure is energized by the 24-volt DC supply from the RTU, and the intermittent signal is fed into a signal conditioner. The output from the signal conditioner is then passed into a counting circuit that is composed of flip-flops and steering logic. Typically, the counter will have 16 bits and so can count up to two-to-the-sixteenth-power (65,536) engineering units.

To determine what the engineering units should be, this maximum engineering unit count number should be used at the design stage, in conjunction with the scan period and the degree of difficulty of sending an operator to the facility. For this example, the engineering unit represented by one count is one barrel, but it could just as easily be 1/1000 barrel, 1/10 barrel, 1 barrel, or 100 barrels. If an oil well produced 65 barrels of oil per hour and the scan period were one hour, it would be a poor design to have each count represent 1/1000 barrel. There would be cases where there was

The Integration Group of The Americas Ex. 1007-Page 100
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001153

uncertainty, from one scan to the next, whether the well had produced 10/10,000 or (65,536+10)/10,000 of a barrel. It would be better to have each register bit represent 1/100 of a barrel or even 1/10 of a barrel. Then, several hours of power failure and a few consecutive communications errors would still give you enough time to send an operator to the RTU to manually read the total before the counter rolls over to zero and the oil measurement is lost forever.

7-10. Monitor Serial Signals

The serial signal is the last RTU field-input signal-type that we will be discussing in this unit. Like most analog and pulse count inputs, a serial signal is sent to the RTU from an electronic processor of some kind. This will very often be a complex device such as an engine vibration analyzer or a process stream chromatograph. Usually, the signal or signals can be presented in the form of analog signals, but because the signals exist within the electronic processor as digital signals it is easier to move them as serial digital signals.

The physical connection used is often an RS-232 link, as shown in Figure 7-15. Acting as a master, the RTU signals the field device to respond. The device identifies itself and sends a serial message with a very fixed format, essentially telling the RTU all it knows. The RTU stores this data in registers as it comes in. When the MTU scans the RTU, the RTU includes this information with everything else it sends.

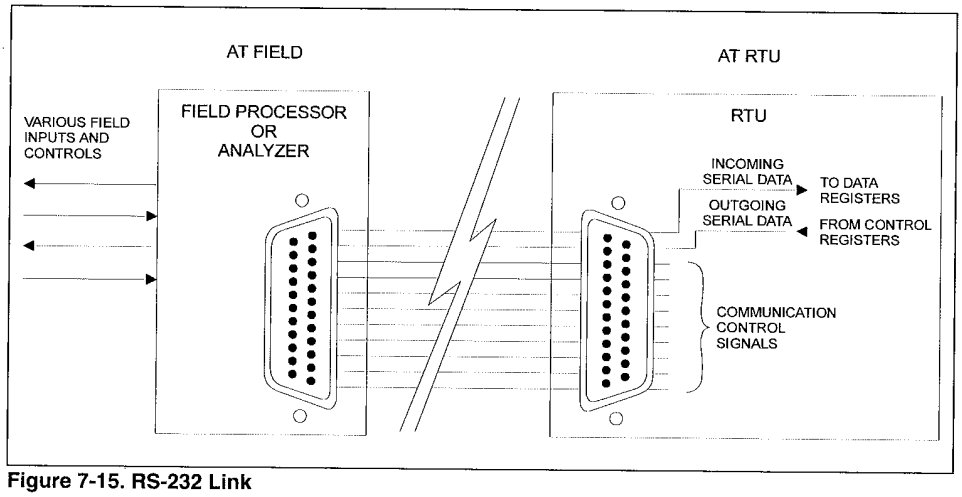


Figure 7-15. RS-232 Link

7-11. Non-RTU Functions

RTU functions are the functions that RTUs perform as RTUs. In addition, some RTUs that have computing capability can be programmed to perform other functions. Before deciding to program such RTUs to do other things, you should ensure that you don't load too much onto the RTU. The potential concerns include overloading the CPU, exposing the equipment to electrical transients, exposing the software to people who are developing new programs, and meeting regulatory requirements involving the stability of data.

7-12. RTU Hardware Choices

Early RTUs were custom designed pieces of hardware that were very expensive ($70,000), had very long delivery (five months), and were very large (five by six feet). They were bid based on extensive specification sheets and no non-RTU functions were included.

Chip-based computers changed all of that. Soon after micro-computers became available, small off-the-shelf RTUs were developed based on these computers. Initially their functionality was limited to discrete inputs/outputs, analog inputs/outputs, and pulse outputs. Serial inputs and pulse inputs followed. Any logic or totalizing that was required had to be done by other equipment.

As it became recognized that there was nearly always a flow totalizer at an RTU site and flow totalizing was the most important function at the site, pressure was applied to the manufacturers of flow totalizers to add a couple of discrete inputs and outputs to their totalizers, as well as some rudimentary communications capability. This led to the first flow totalizer that was also an RTU. Similar additions to programmable logic controllers (PLCs) resulted in PLCs that had RTU functionality. Many RTUs are now flow totalizers or PLCs that have been delivered with additional RTU capability built in.

Unit 7 Exercises:

7-1. *An RTU can gather data in the form of a discrete switch position. This is used for alarm and status monitoring. What three other forms of field data can an RTU gather?*

7-2. *What four forms of signal can an RTU generate to control field equipment?*

7-3. *What is the function of a protocol driver program?*

7-4. *Many protocols divide the binary message into three fields. What are they?*

The Integration Group of The Americas Ex. 1007-Page 102
SitePro, Inc. v. WaterBridge Resources LLC et al.
WB_00001155

7-5. What is the purpose of a security code?

7-6. Communication forms like discrete, analog, and pulse counting are used between field devices and RTUs. Name one other form of communication between the RTU and field devices. Where is it likely to be used?

7-7. Why would you be unlikely to require 16 bits in a register to define a valve position?

7-8. What other electronic devices located in a field position can have RTU functionality built in?

WB_00001156

Unit 8: RTU/MTU Communication

The Integration Group of The Americas Ex. 1007-Page 104
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

Unit 8

RTU/MTU Communication

In Unit 6, we mentioned that long-distance digital communication is always serial because of the cost of additional media that would be needed to transmit it in parallel. In nearly every case, the RTU is located a long way, on the order of miles, from the MTU. This unit will discuss the issues that arise and the solutions that have been applied to allow communication between such widely separated devices.

Learning Objectives—When you have completed this unit, you should:

A. **Know what a modem does and why it is needed.**

B. **Be able to understand the communications terms that relate to remote data acquisition and control.**

C. **Be familiar with radio paths and how they are calculated.**

D. **Know the various radio technologies available for long-distance SCADA communications.**

8-1. Communications System Components

Figure 8-1 illustrates a very simple SCADA system that consists of one MTU and one RTU. Somehow the MTU and the RTU must be equipped to communicate with each other.

In telecommunications parlance, the MTU and the RTU are each called "data terminal equipment" (DTE). They each have the ability to formulate a signal that contains the information that must be sent. They also have the ability to decipher a received signal to extract its information. What they lack is the capacity to interface with the medium.

Figure 8-2 shows equipment interposed between the DTEs and the medium that has that ability to interface. The modems, which can be called "data communication equipment" (DCE), are able to receive information from the DTEs, make the necessary changes to the form of the information, and send it out over the medium to other DCEs, which will receive it and transform it before passing it to another DTE.

The International Organization for Standardization (ISO) has developed the Open Systems Interconnection (OSI) model (see Figure 8-3). It is called the OSI Seven Layer Model and it defines the function of each layer. The

The Integration Group of The Americas Ex. 1007-Page 105
SitePro, Inc. v. WaterBridge Resources, LLC, et al

WB_00001158

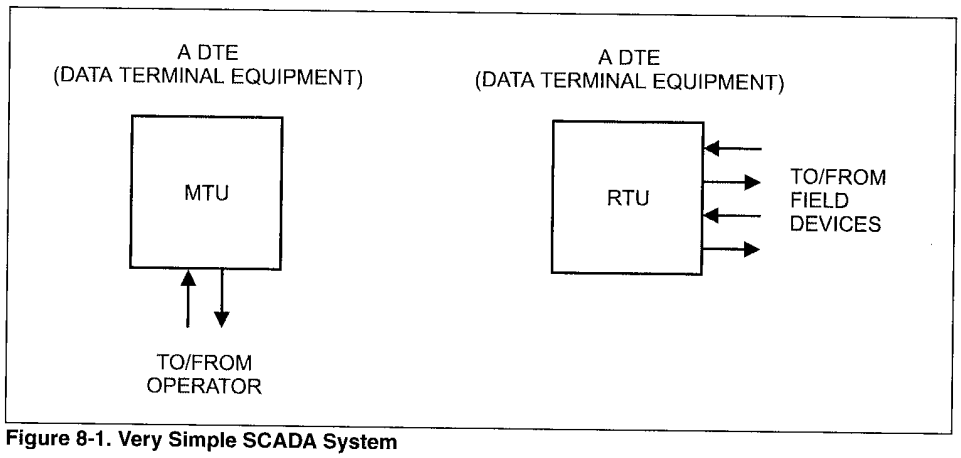


Figure 8-1. Very Simple SCADA System

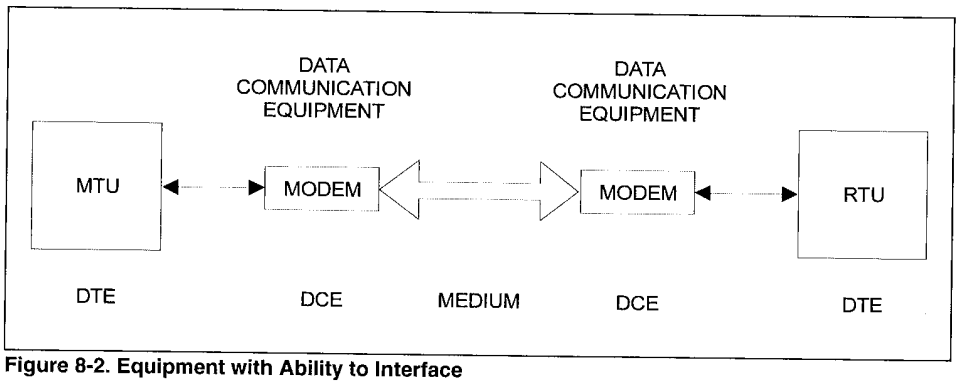


Figure 8-2. Equipment with Ability to Interface

intent is that when the appropriate number of layers is supplied for any two machines, communication between them will be possible.

The uppermost layer and the lower two layers, that is, layers seven, two, and one, are sufficient for most SCADA communications—if they are using Master-Slave communication. Some of the more complex communication methods discussed later in this unit will require more than those three layers. Note that there is not necessarily a direct correspondence between an OSI layer, which defines a function, and a physical piece of hardware. Most of the functionality of layer one and some of the functionality of layer two can be thought of as occurring in the modem. Some of the functionality of layer two can be thought of as occurring in the RTU and the MTU, as does all of the functionality of layer seven.

8-2. Protocol

Protocol was discussed in detail in Section 7-3. It is a set of rules that defines the meaning of a pattern of binary words. It has been established

The Integration Group of The Americas Ex. 1007-Page 106
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001159

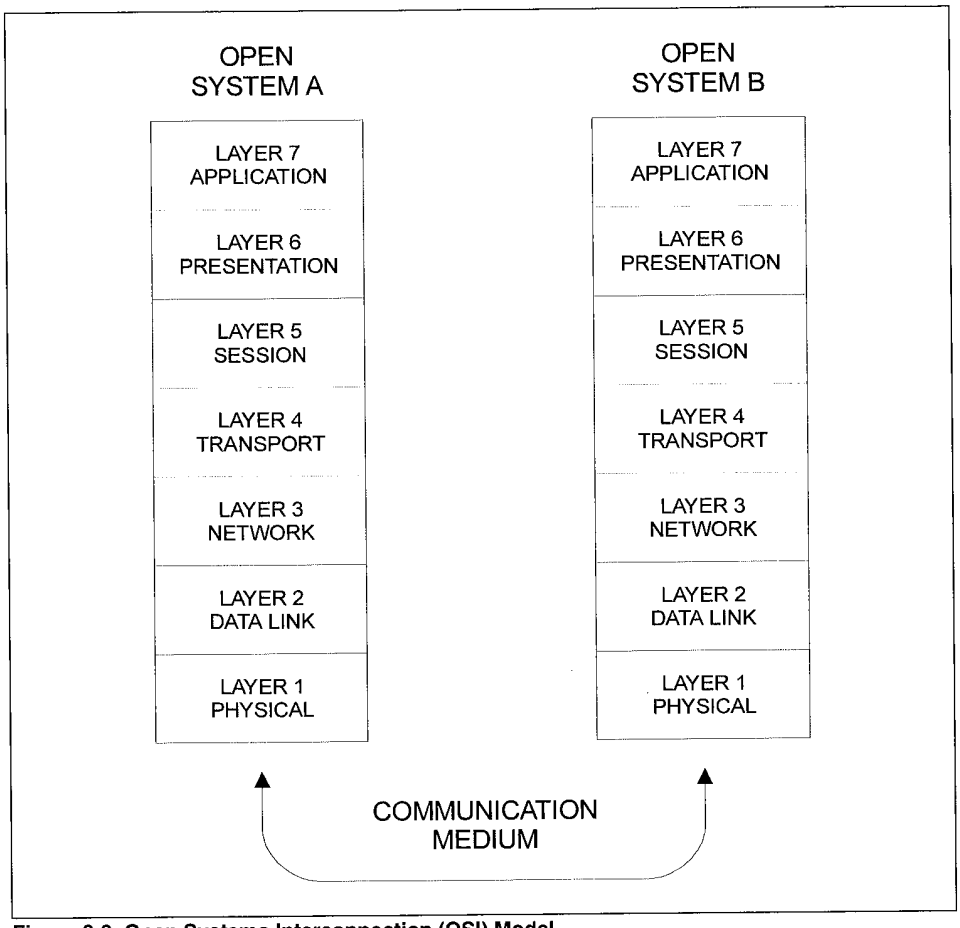


Figure 8-3. Open Systems Interconnection (OSI) Model

that the messages to be sent from the MTU to the RTU are a series of binary digits. But what will the first bit represent? The second? The 247th? Protocol tells us. It supplies the code to create this long series of ones and zeros. The same code, or protocol, allows the receiving station to decode it. Since there are dozens of available protocols, it is important that the SCADA developers ensure that the same protocol is used for all stations that will communicate with each other.

Equipment manufacturers started developing these protocols before any standards organizations became interested. Many equipment manufacturers continued to use their proprietary protocols even after standards organizations had developed open standards, and some developers even built new proprietary protocols after these open standards were available. Some are better for some applications than others. Some are worse for all applications than others. The important thing to know about them (Communication Rule 2) is that one absolutely must have the same protocol at the RTU as at the MTU.

The Integration Group of The Americas Ex. 1007-Page 107
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001160

Figure 8-4 shows the layout of a message sent in a particular protocol based on standard IEEE C37.1. The purpose of each bit is defined. The total length of the transmitted document is included as the sum of all fixed bits plus the number of bits carried in the "data" frame. The "synch" frame signals all potential receivers that a message is coming and provides a reference that can be used for each receiver to synchronize its clock to the clock of the transmitter. The "remote address" frame defines the station to which the message is sent. Eight bits, (one "octet"), allow one of any 254 stations to be identified. The "function" frame defines which of up to 256 message types this will be. An example might be "Turn off all of the following motors." The "internal address" frame describes which sets of registers within the receiving station the message is directed to. The "modifier" modifies the internal address and defines how many data words are included in the message. "Special Orders" contains shorthand messages about MTU and RTU conditions. An example might be "Reset all communication error counters". "Data" is a field of variable length, from 0 to 192 bits. The "CRC" is a 16-bit cyclic redundancy code based on the Bose-Chaudhuri-Hocquenghem (BCH) formula for detecting transmission errors.

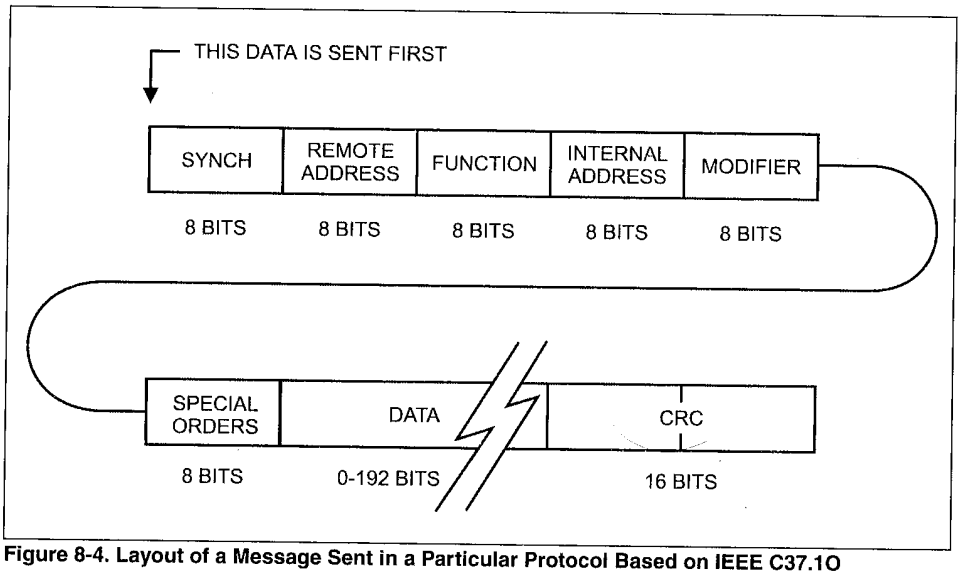


Figure 8-4. Layout of a Message Sent in a Particular Protocol Based on IEEE C37.1O

This is a good place to talk about the CRC. As just mentioned, it is a code word that is calculated according to a formula. As with protocols, several different formulas can be used for the CRC, and one of the variables that controls which formula to use is the number of bits in the message to be checked. The CRC used in Figure 8-4 is called the "(255,239) BCH". 255 is the maximum number of bits in the word that the CRC will guard. 239 is the maximum number of bits—not including the 16-bit CRC itself. As with

The Integration Group of The Americas Ex. 1007-Page 108
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001161

protocols, the same formula must be used by the encoder as by the decoder. One interesting thing about the CRC is that it is practically impossible to regenerate the original message by knowing the CRC, even if you know the formula that was used to generate it. If there was, however, an error in transmitting the message, of one or two or even many bits, the CRC that is generated from the original message will be very different from the CRC that is generated from the received message.

Figure 8-5 explains how the CRC is calculated for an eight-bit word. The procedure appears complicated but is accomplished quickly and easily by digital logic. In fact, dedicated hard wired logic is often used instead of using up valuable computer time. This method starts with 16 bits of ones, but some other methods start with 16 bits of zeros. Some methods that transmit bits from right to left require that the polynomial be transformed left to right and the shifting be done to the right.

When one station, either the MTU or the RTU, must send a message to the other, it activates a part of itself called the protocol driver (Section 7-2) and uses that driver to encode the message into the form shown in Figure 8-4. It arranges the operational data according to protocol rules, and then it adds the 16-bit CRC at the end of the message. Then it checks to ensure that the communications link is clear. If it is, it passes a "request to send" to the next communications component, the modem.

8-3. Modems

The modem is at the lowest two layers of the ISO/OSI seven-layer model. It is the equipment that checks to determine if the communication medium is being used and turns the radio transmitter on. When all is ready, it changes the low-power binary signals as they are fed to it from the MTU or RTU into a form that will travel to the other end of the medium and be received by another modem. As noted earlier, modem is an acronym for "**mo**dulate and **dem**odulate. But what does "modulate" mean? Generally, it means to vary or to change a carrier wave according to a pattern.

Early attempts to send direct-current (DC) signals long distances over wireline demonstrated, not too surprisingly, that resistance reduced the signal amplitude. Attempts to send more and more pulses down the line demonstrated that inductance and capacitance effects also affected the shape of the pulses, and limits on data rates and distances were reached early.

Figure 8-6 shows that a wave form can be separated mathematically into a series of sine waves. Joseph Fourier showed this at about the turn of the eighteenth century. It turns out that sharp-edged wave forms contain

The Integration Group of The Americas Ex. 1007-Page 109
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No.
WB_00001162

PROCEDURE FOR CALCULATING A CYCLIC REDUNDANCY CODE

In this example, we will determine the CRC for an eight-bit data word, 0100 0000.

The CRC we will use is the (225,239) BCH, which has the generator polynomial of ($x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x + 1$). This can be rationalized to a binary word by placing a one in each of the identified bits and a zero in those not identified in the generator polynomial. The result is 1011 0111 1011 0001 1. Note that this is a 17-bit word. The most significant bit is discarded because it will not affect the arithmetic we will use it for. The effect polynomial is, then, the 16-bit word, 0110 1111 0110 0011.

The procedure looks complex but is easily handled by electronic binary logic.

A 16-bit register is filled with all ones. The data word is added to it, and simple shifts and additions are completed as follows.

FLAG	BINARY NUMBER	COMMENTS
	1111 1111 1111 1111	Initiate 16-bit register of all ones.
	0100 0000	First eight bits of the message.
	1011 1111 1111 1111	Sum of the two lines with no carrys, (exclusive OR).
1	0111 1111 1111 1110	Shift all bits one to the left. Note the flag is one.
	0110 1111 0110 0011	Since flag was one, add the polynomial.
	0001 0000 1001 1101	Sum of the two lines with no carrys, (exclusive OR).
0	0010 0001 0011 1010	Shift all bits one to the left. Note the flag is zero.
0	0100 0010 0111 0100	Since flag was zero, shift one bit to the left.
0	1000 0100 1110 1000	Since flag was zero, shift one bit to the left.
1	0000 1001 1101 0000	Since flag was zero, shift one bit to the left.
	0110 1111 0110 0011	Since flag was one, add the polynomial.
	0110 0110 1011 0011	Sum of the two lines with no carrys, (exclusive OR).
0	1100 1101 0110 1001	Shift all bits one to the left.
1	1001 1010 1101 0010	Since flag was zero, shift one bit to the left.
	0110 1111 0110 0011	Since flag was one, add the polynomial.
	1111 0101 1011 0001	Sum of the two lines with no carrys, (exclusive OR).
1	1110 1011 0110 0010	Shift all bits one to the left. If there were additional bits in the word, we would now add the next eight bits as we did the first eight and would go through the same process of adding the polynomial and shifting until we had made eight shifts. We would then add the next eight bits and so on. Since we are doing this example with only an eight-bit word, the process is complete. The CRC is the result after the eighth shift. It will be transmitted after the eight-bit data word, so the total message will be:

0100 0000 1110 1011 0110 0010
| DATA | CRC |

Figure 8-5. How the CRC Is Calculated for an Eight-bit Word

more high frequency waves than rounded edged wave forms do and that inductance will selectively attenuate high frequencies. The inductance of a long wireline will change the shape of a wave form by removing the high frequencies and rounding the wave form, as shown in Figure 8-7.

The Integration Group of The Americas Ex. 1007-Page 110
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00738 U.S. Patent No. 9,342,078

WB_00001163

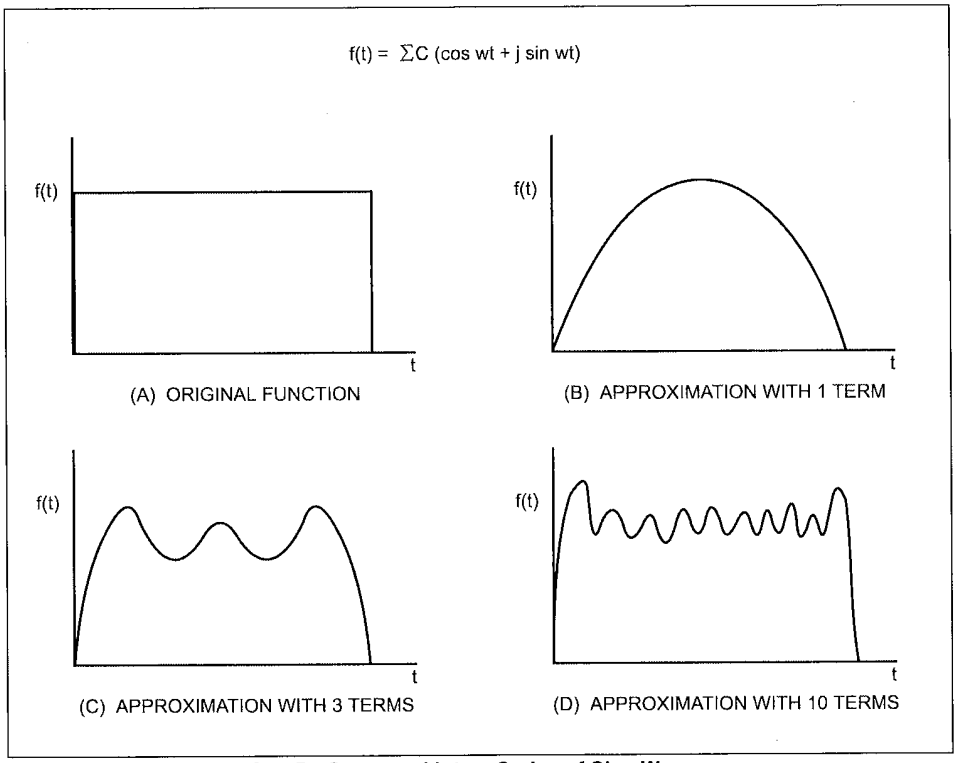


Figure 8-6. Wave Forms Can Be Separated into a Series of Sine Waves

In addition to this "amplitude distortion," the delay time imposed on component frequencies also varies. Some frequencies take longer to get to the other end of a transmission line than other frequencies. This is called "phase distortion." A sine wave, having only one frequency, is immune to both of these forms of distortion. For this reason, a sine wave is usually used as a carrier wave if the message has to travel a long distance.

The communications modulator varies one of three characteristics of the carrier. It may change the amplitude, the frequency, or the phase of the carrier. Amplitude modulation (AM) varies the amplitude of the carrier by multiplying the amplitude of the data by the amplitude of the (unmodulated) carrier. The result is a series of sine waves at the carrier frequency that vary in amplitude at the data rate (see Figure 8-8).

Frequency modulation (FM) varies the frequency of the carrier wave according to the amplitude of the data. Output amplitude is constant. Figure 8-9 shows the effect. Because most atmospheric noise is amplitude related and FM does not receive any data from the signal amplitude, FM signals are not affected by atmospheric noise as much as AM signals are.

Binary digital signals, since they consist of only a zero or a one, can frequency modulate a carrier wave by a method called frequency-shift

The Integration Group of The Americas Ex. 1007-Page 111
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001164

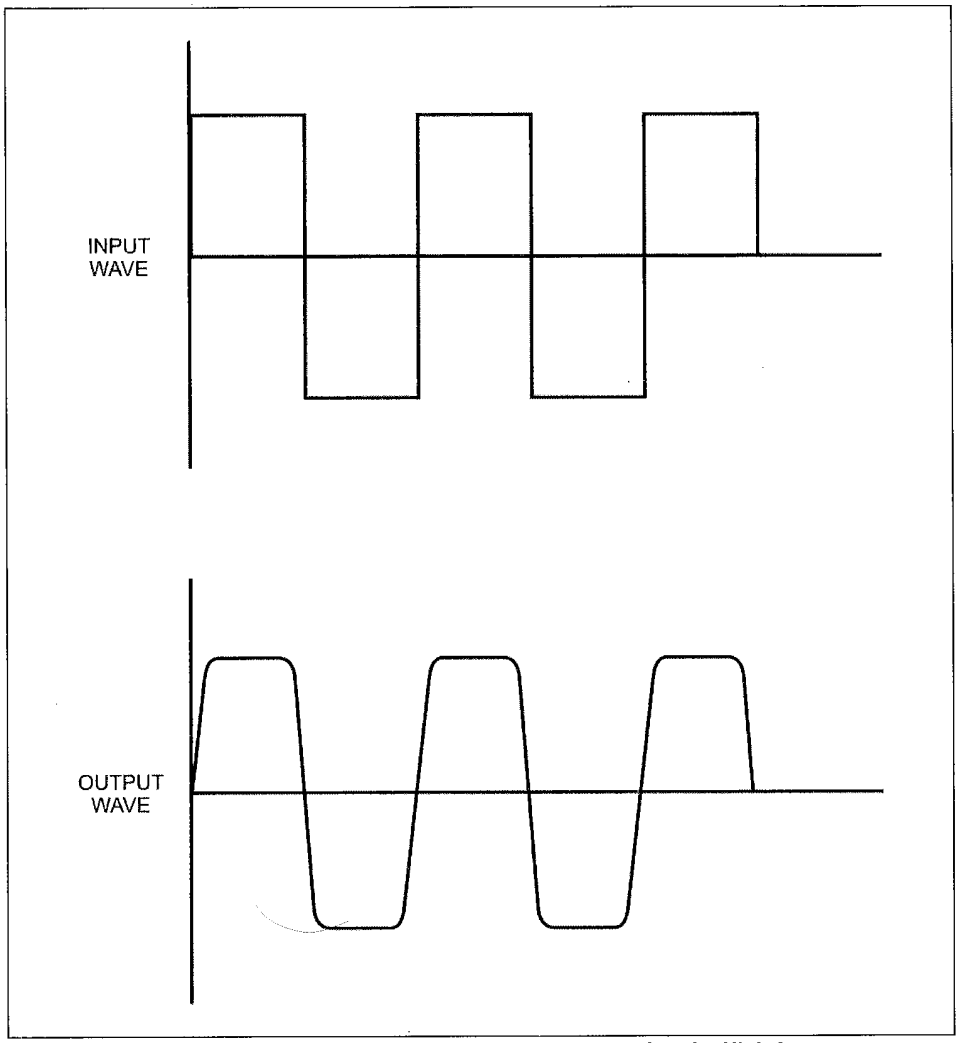


Figure 8-7. Reactance of Long Pair of Wires Selectively Attenuating the High-frequency Components

keying, or FSK, using only two tones on the carrier. This technique allows the carrier to be frequency shifted by (for example) 1200 Hz for a "mark," typically a one, and 2200 Hz for a "space," typically a zero. In fact, these are the frequencies used by the Bell 202 modem, one of the earlier ones.

Notice that although we are changing the frequency of the carrier and could expect that this would result in modulation distortion, the amount of change by adding 2200 Hz to a carrier of perhaps 450,000,000 Hz is insignificant.

Phase Modulation (PM), also called phase-shift keying (PSK), involves changing the phase angle of the carrier wave in response to a change in the

The Integration Group of The Americas Ex. 1007-Page 112
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001165

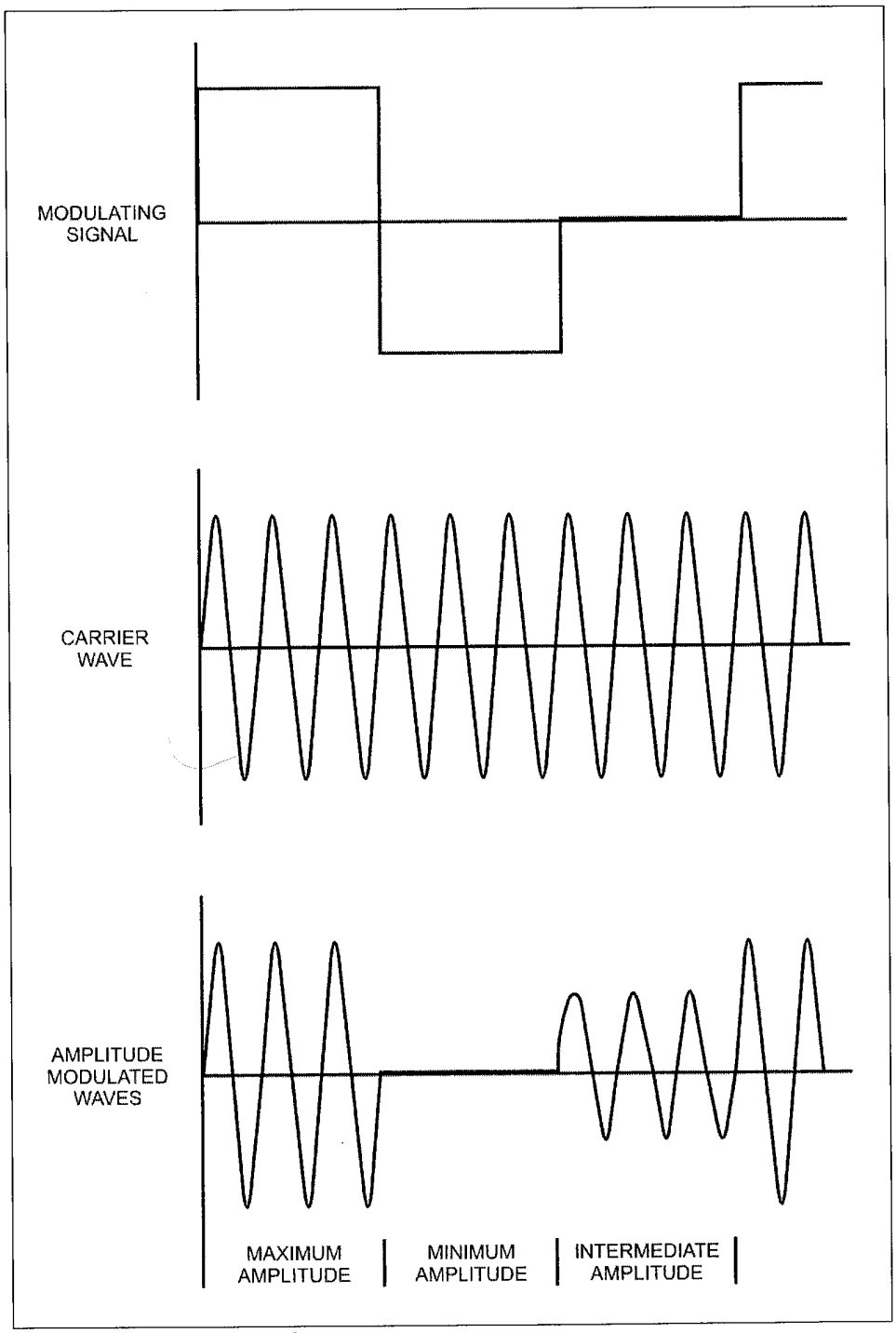


Figure 8-8. Amplitude Modulation

The Integration Group of The Americas Ex. 1007-Page 113
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00739 U.S. Patent No. 9,810,070

WB_00001166

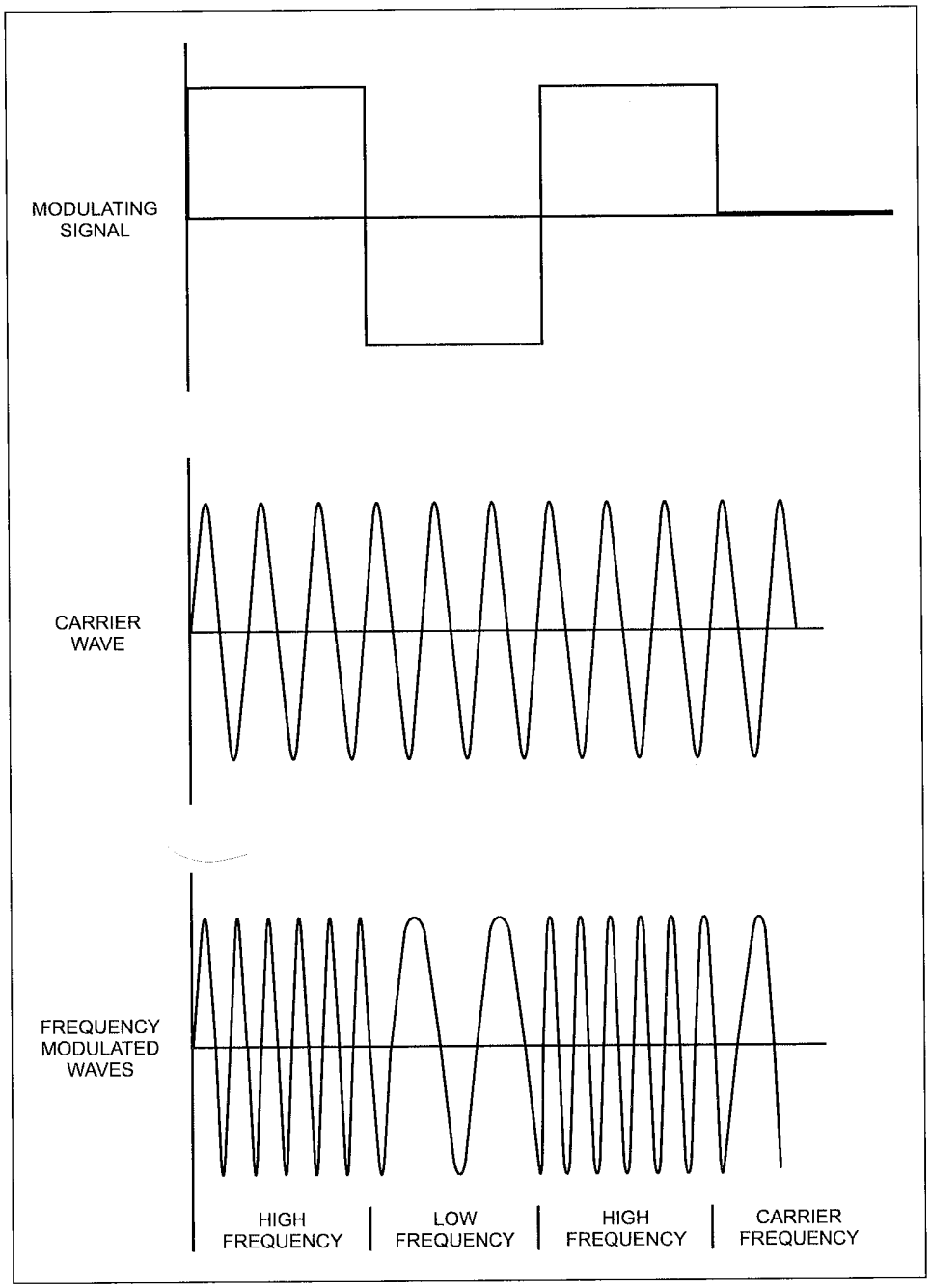


Figure 8-9. Frequency Modulation

amplitude of the data. As the data rate approaches the carrier rate, PM looks more and more like FM, and in fact, FM is sometimes referred to as a special case of PM. Shifting the carrier by +90 degrees or by -90 degrees depending on whether the data bit is a one or a zero is the simplest PSK

WB_00001167

method. To get higher data rates, quadra-phase shifting allows for shifting the carrier by 90 degrees if the data pair is 00, by 180 degrees if the data pair is 01, by 270 degrees if the data pair is 10, and by 360 degrees if the data pair is 11. Other groupings can be used to increase the efficiency or to reduce errors in decoding.

8-4. Synchronous or Asynchronous?

"Synchronous" and "asynchronous" refer to the need for a timing signal to be transmitted with the data. Synchronous modems must transmit a clock pulse that is used to ensure that the receiver is working at the same clock speed as the transmitter. Usually, the transmitted clock is used to synchronize a clock that is working at the receiver. In other cases, the transmitted clock is conditioned and actually becomes the clock signal at the receiver. Both of these methods result in the clock signals at the receiver and transmitter having the same phase and frequency relationship.

Asynchronous modems do not require that the receiver be clock-synchronized with the transmitter. "Start of message" and "End of message" signals are required to advise the asynchronous receiver of the status of a message.

8-5. Telephone Cable or Radio?

In the past, the choice of communications media was determined by two things: data rate and cost. More and more now, consideration is being given to a third, and that is security of data.

In Section 4-4 we developed a method that calculated the scan interval. The method was based on several things, including the data rate, and trade-offs could be made between the data rate and the scan interval. For some SCADA purposes, it is not feasible to get a short enough scan interval unless the data rate is pushed very high, that is, over 5000 bps. When this situation exists, a communication medium with a bandwidth greater than that of a voice grade line is required, such as optical fiber, microwave radio, or one of the more sophisticated UHF (Ultra High Frequency) systems. Dedicated lines of a higher bandwidth than voice grade lines leased from a telephone company are one possibility for such a communications medium. The cost is likely to be fairly high, but for those industries that require high-volume, high-speed data, these choices do exist.

When an acceptable scan interval can be achieved with data rates in the 300 to 4800 bps range, the choice becomes much broader. All of the preceding solutions will meet the technical requirements. Other

WB_00001168

equipment that will do the job are voice-grade telephone line, which is designed to operate from 300 to about 5000 Hz, or inexpensive UHF radios designed for commercial and light industrial applications.

One additional choice of communications media may exist. Nearly all processes that can benefit from SCADA are served by electric utility power. Some power companies are marketing a communications option that will allow high frequency data to be superimposed on the 60 Hz power. Some engineering is required to realize this sharing since the signals must be removed and then re-inserted as the power goes through a transformer, but the data security of such a system can be better than that of radio. The costs will be better than dedicated buried signal cable and may be better than radio for some installations.

Buried telephone cable was at one time the preferred communications medium. The low cost of purchasing and installing it made its use acceptable, but some problems had to be solved first. Problems caused by rodents chewing through the cable were eliminated by putting metal armor around the conductors. Figure 8-10 shows a buried cable construction cutaway. Various materials have been successfully used to keep water out of the cable, but efforts to keep ditchers from digging the cable up have been unsuccessful. The cost of installation dropped when a cable construction technique was developed that allowed direct plowing-in, although solid rock must be blasted to provide a trench. Purchasing right-of-way in which to bury the cable is sometimes very expensive, and the cable signals can be affected by high currents in parallel power transmission lines and by low-frequency magnetic effects from sunspot activity.

For remote areas, where telephone companies do not have an incentive to install their own lines, it may be necessary for the user to pay a high capital cost to get the telephone company to install a line that can be leased. In other areas, the user may have to purchase and install the cable. Optical fiber cable is becoming cost competitive with copper, even for small low-data-rate links. It can be plowed in or installed in the same trench as a new pipeline. Security of data from interception or from sabotage is much better with copper cable or optical fiber than it is with radio. Any cable will have the disadvantage of flexibility in location. When it is in, it stays in. One cannot decide five years later that it would be nice to move it. For many applications, however, this permanence is not a problem.

Occasionally, overhead copper or optical fiber cable may be used if plowing is impractical. It is seldom used unless there is already an overhead line in place.

The Integration Group of The Americas Ex. 1007-Page 116
SitePro, Inc. v. WaterBridge Resources, LLC, et al.

WB_00001169

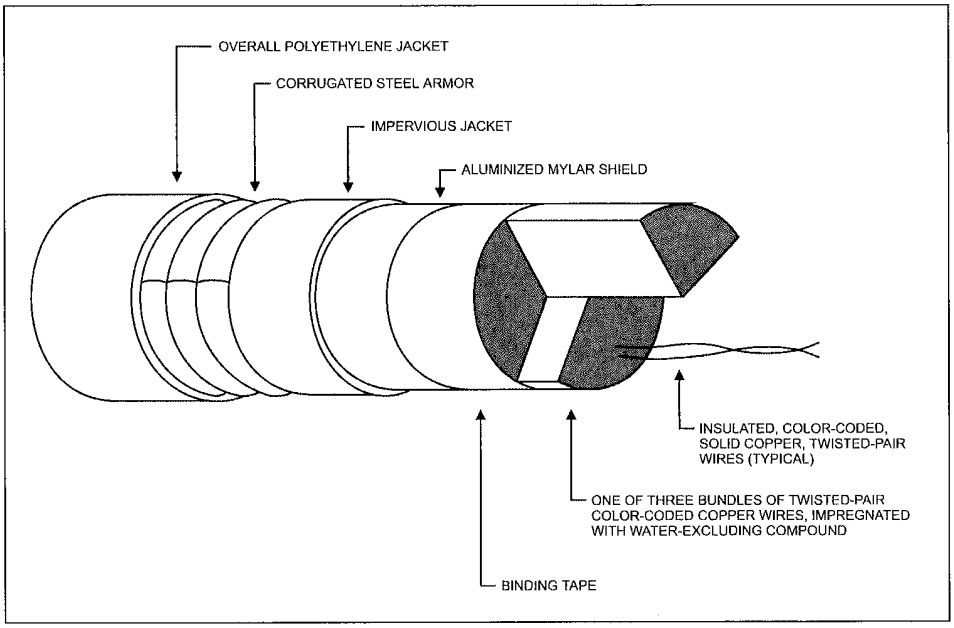


Figure 8-10. Buried Cable Construction Cutaway

Although radio systems are technically more difficult to design and maintain, they usually offer sufficient advantages over land lines to make them the medium of choice. Figure 8-11 shows a factory built RTU, complete with solar power battery charger, weather-proof enclosure and UHF radio system, suitable for mounting near a gas well or pipeline valve location.

8-6. Simplex or Duplex?

Communication can be a one-way pass of information or a two-way exchange. Earlier in this text we determined that for both the supervisory control function and the data acquisition functions to be realized, the information in a SCADA system must be able to move in both directions. The terms used to describe the ability of a communications system to move information are as follows: simplex, half duplex, and duplex—sometimes called full duplex. These terms refer to other communications systems in addition to radio, but to appreciate how radio systems are selected, it is important that you understand what they mean.

Simplex systems, shown in Figure 8-12, allow information to be passed in one direction. Paul Revere used a simplex system when he lit a lamp to indicate "One if by land—two if by sea." He could send information out but could receive no information back. Even the information that his message had been received was not immediately available to him. Amerind (American Indian) smoke signals (when only one fire was used)

The Integration Group of The Americas Ex. 1007-Page 117

WB_00001170

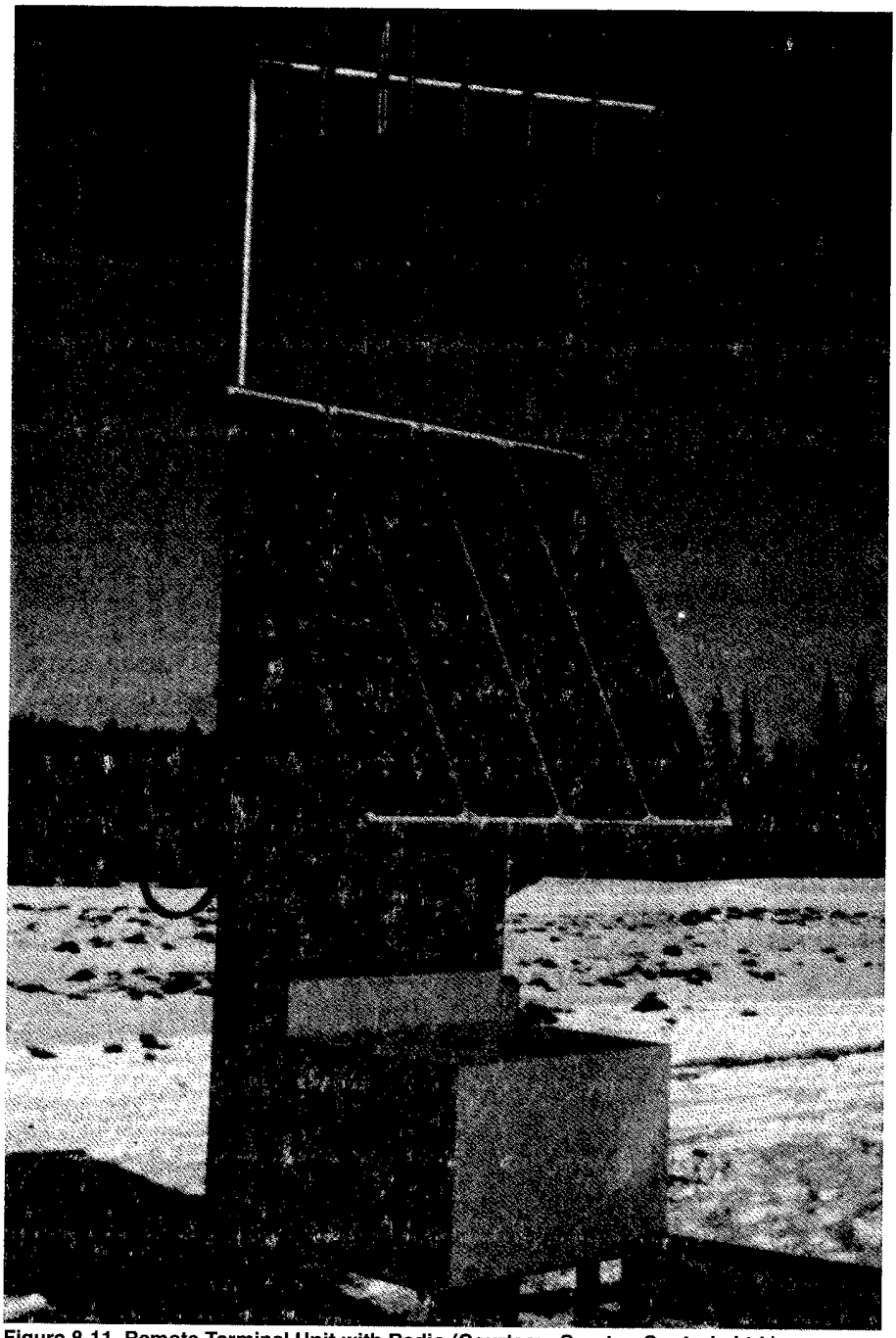


Figure 8-11. Remote Terminal Unit with Radio (Courtesy: Spartan Controls Ltd.)

WB_00001171

were also simplex communications. They sent the information out but did not receive information back. Note that the addition of a second fire could change the system description from simplex to something else.

More recent examples of simplex systems are the various signals sent by telemetry from weather balloons, experimental rockets, and commercial radio and television broadcasts. Since SCADA requires two-way movement of information, it does not use simplex communication.

At the other end of the communications utility spectrum is duplex (or full duplex). Full-duplex communication allows information to be transmitted and received at the same time. Duplex is like having two simplex systems running parallel to each other, but in opposite directions (see Figure 8-13). An early example of duplex is the semaphore, which used a sender and a receiver at each end of the path. Each of the stations could thus both talk and listen simultaneously. More recent technology-based examples of duplex include the telephone. But while full duplex offers an advantage in terms of utility, it comes at the cost of requiring more wires or other equipment than simplex.

Interestingly, a compromise is available. If it is necessary to move information in both directions but not continuously, it is possible to use one pair of wires or one radio frequency with the data going sometimes in one direction, sometimes in the other. This is called half-duplex. As Figure 8-14 shows, some additional switching is necessary. It wouldn't do, for example, to have the transmitter output connected to the receiver input.

SCADA systems are able to use either full duplex or half duplex. The criteria for selection are not exclusively the cost of an extra pair of wires in a land cable or an extra crystal for a radio. They may include the time it takes for a radio transmitter to turn on and stabilize or the availability of an extra radio frequency in a limited spectrum that has great demands on it.

8-7. Turn-On Time

Figure 8-15 illustrates a typical half-duplex SCADA radio system that consists of one MTU and five RTUs. It is possible for the MTU to 1) send a message to its radio to start transmitting, 2) turn the transmitter on and wait until it stabilizes, 3) modulate the transmitter carrier with the message it wants to send to RTU #1, including the RTU identification, 4) turn the radio transmitter off, and then 5) turn its receiver on and wait for RTU #1 to answer.

All the RTUs normally wait with their receivers on. When a message is received, each RTU checks to see if the message is for RTU #1 or some other RTU. If it is not for RTU #1, RTU #1 will ignore the message. If it is for RTU #1, it will be acted on within RTU #1. Then RTU #1 will pass a

The Integration Group of The Americas Ex. 1007 Page 119

WB_00001172

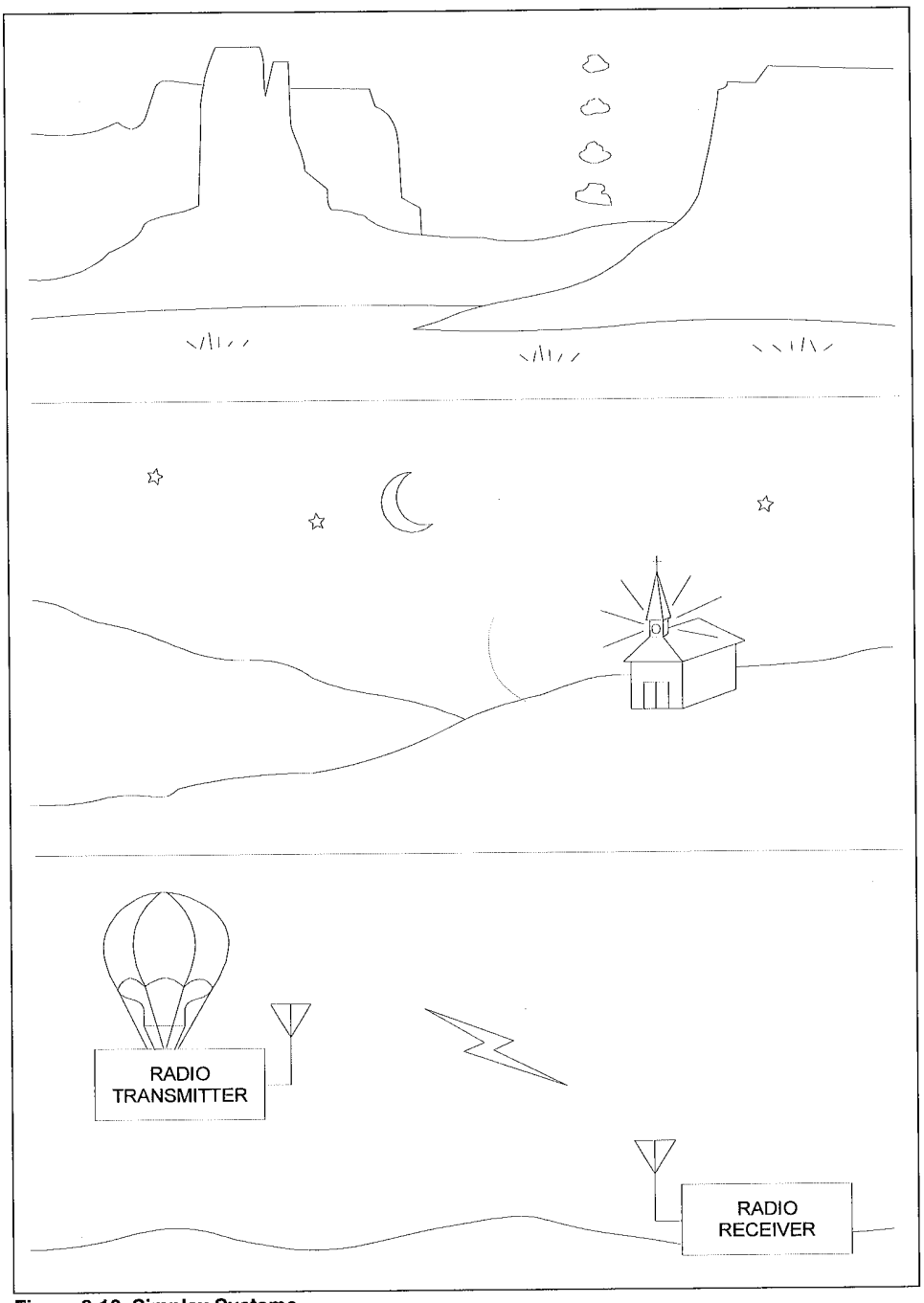


Figure 8-12. Simplex Systems

message back to the MTU by turning its receiver off, turning its transmitter on, waiting until the transmitter stabilizes, modulating the radio transmitter carrier with the message (which includes its own identification), turning its transmitter off, and turning its receiver on.

The Integration Group of The Americas Ex. 1007-Page 120

WB_00001173

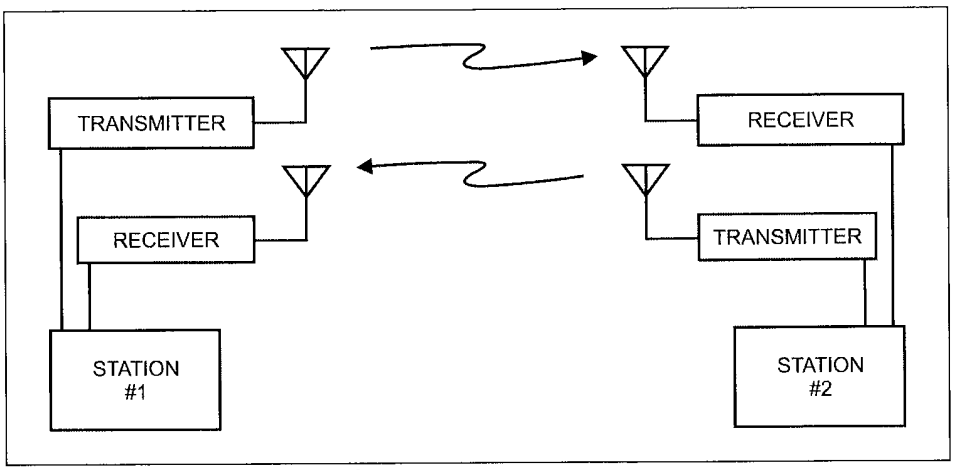


Figure 8-13. Duplex or Full-Duplex System

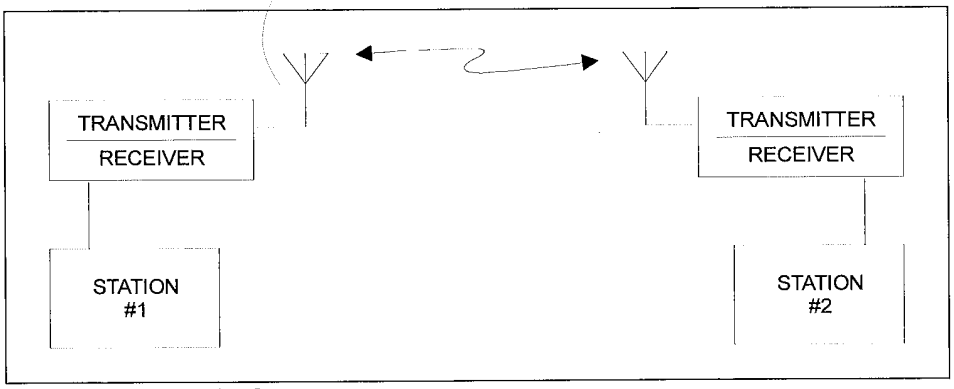


Figure 8-14. Half-Duplex System

During this time, all the other RTUs are recognizing that the message is not for them, so they ignore the message and keep listening for a message for them.

At first glance, the time required for the transmitter to turn-on and stabilize does not look very significant. When a timing chart, as shown in Figure 8-16 is drawn, it is obvious that this time can be significant. More than one-half of the total transaction time can be consumed, but this will vary depending on the message length and the data rates. This time is one of the factors that is used to calculate communication efficiency.

The length of the wait for a radio transmitter to turn on and stabilize is a function of the radio and is generally independent of the data rate. Because of this, attempts to reduce the scan interval should concentrate on the communications equipment. One way to improve the communications equipment is to take advantage of full duplex. If a second frequency is available, the MTU can transmit on one frequency and all of the RTUs can

WB_00001174

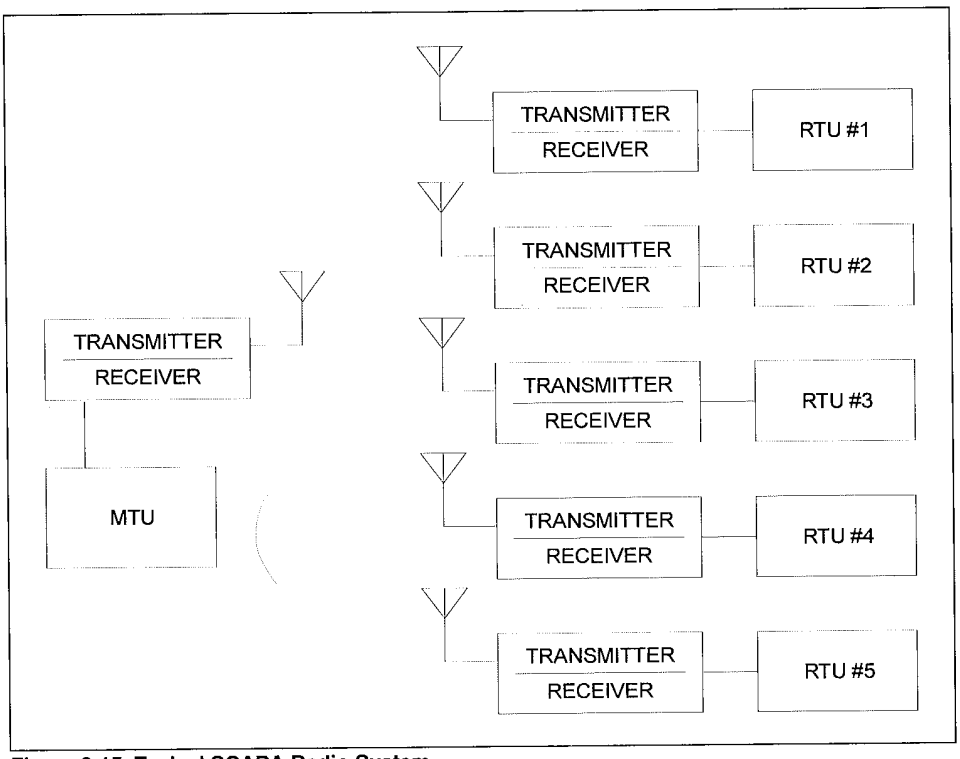


Figure 8-15. Typical SCADA Radio System

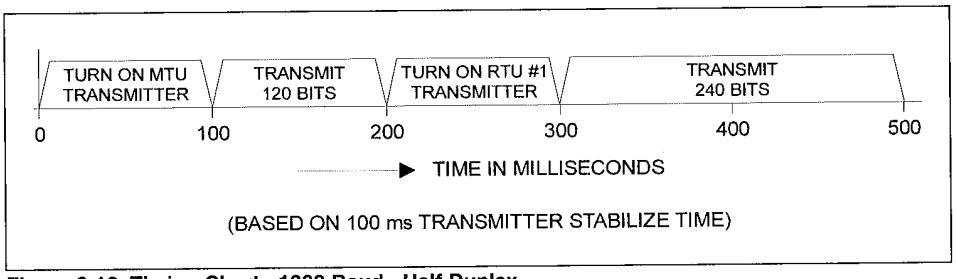


Figure 8-16. Timing Chart - 1200 Baud - Half Duplex

transmit on the other frequency (see Figure 8-17). The implication is that the MTU radio can transmit 100 percent of the time; therefore, it is not necessary to wait for it to stabilize each time a message must be sent from the MTU. Most of the time, only the carrier will be transmitted from the MTU. This technique is often used and results in a shortening of the scan time for a small increase in cost. Note that since all the RTUs are using the same frequency to transmit, only one can transmit at a time. For radio communications, it is seldom justified to have each RTU transmit on a separate frequency.

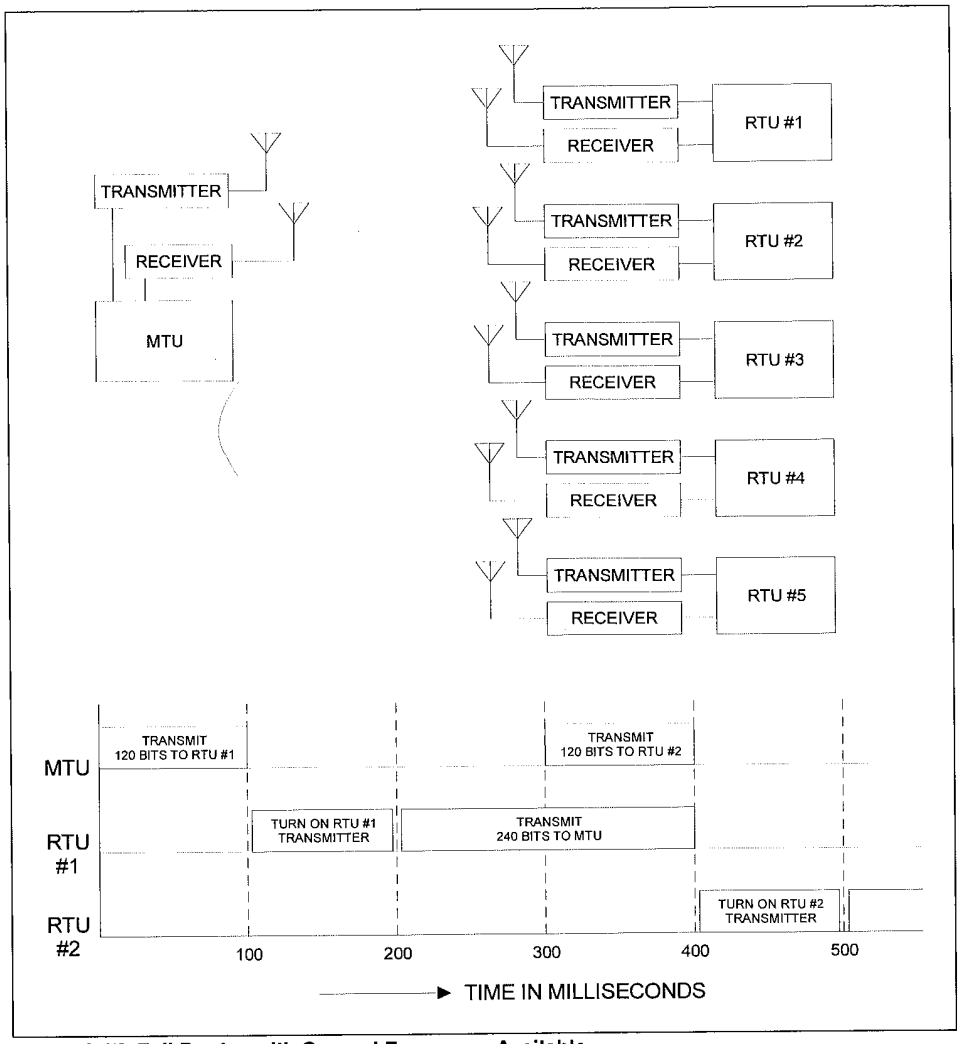


Figure 8-17. Full Duplex with Second Frequency Available

8-8. Frequencies: Are They Available?

We have just shown that by adding one frequency (thereby doubling the requirement for frequencies), we could effect an improvement in the response of a SCADA system. But that improvement was also accompanied by the caution, "If a second frequency is available..."

As with many other things in this world, radio frequencies are commodities that are in demand and are being used up. People think of the number of frequencies as being limitless, but that is also the way people used to think of the dodo, carrier pigeons, and the Atlantic cod. The International Telecommunications Union (ITU), a United Nations agency, organizes World Administrative Radio Conferences to allocate

WB_00001176

bands of frequencies on a worldwide basis. The decisions of these conferences are binding on the member countries and are used to establish national regulations.

Government regulatory agencies carefully evaluate applications to use frequencies and allocate those frequencies if they are available and if the agency is convinced that the applicant really needs them. It is not a foregone conclusion that a license will be issued just because an application is made.

When radio is chosen as the medium for SCADA communications, some limitations automatically exist. One of these is that radio needs not only one frequency but a band of frequencies centered on the one carrier frequency. The width of this band, or bandwidth, is related to the modulation rate (measured in baud) that we wish to use. Depending on the type of modulation, the bandwidth in Hz is about equal to the number of bits per second for single sideband AM, which is about two times the number of bits per second for frequency-shift keying (FSK) modulation and three times the number of bits per second for frequency modulation (FM). Phase-shift modulation can actually move data at a rate higher than the baud rate, but even then a significant amount of bandwidth is required.

In addition to this bandwidth, a guard band of several hundred Hz is added above and below the band being used. This guard band prevents the overlap of frequencies and the resulting interference when (not if) the radio transmitter drifts off the frequency it is calibrated to use. Therefore, to communicate at 1200 bps, a band of frequencies about 3000 Hz wide is required. Interestingly enough, this is just about the same bandwidth needed to communicate analog voice data with acceptable quality. Could it be that 1200 bps has become a standard for this reason?

The other factor that limits how many frequencies (or frequency bands) are available for use is their range. Some people can remember listening to commercial radio at night and being bothered by unfamiliar stations drifting in and out. Sometimes this interference was so strong that it completely obscured the station being listened to. This phenomenon can be described by stating that the signal-to-noise ratio (SNR) has dropped below 1. When listening to the radio for enjoyment, this is a nuisance. When a SCADA RTU is listening to the radio to receive an order to block in a leaking oil pipeline and the SNR drops below 1, it is much more than a nuisance.

Radio waves refract for many reasons, but, generally, higher frequencies refract less than lower frequencies. There is a group of frequencies between 300 MHz and 3000 MHz called ultra-high frequency (UHF). It has

The Integration Group of The Americas Ex. 1007-Page 124
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR 00738 U.S. Patent No. 9,243,870

WB_00001177

the benefits of being limited (nearly) to line of sight and yet it is still technically simple enough to be maintainable in the field. The advantage is based on the need of the licensing agency to ensure that the new station does not interfere with any other licensed stations. The new UHF station will almost never interfere with stations over the horizon. Most SCADA radio operates in the UHF band.

8-9. Path Studies and Seasonal Variations

As radio frequencies get higher, the radio waves act more and more like light. At the UHF band, and even more so for microwave radio (which is sometimes used for high data rate SCADA), the radio path is essentially line-of-sight. One of the implications of this is that the system design must include a "path study." For each link between transmitter and receiver, an evaluation must be made regarding transmitter power, antenna gain, losses as a function of distance, and, very importantly, whether any hills lie between the transmitter and the receiver. The path study uses topographical maps, which may suggest changes of location that will keep antenna heights to a minimum or indicate the need for radio repeater stations. Figure 8-18 shows a simplified path study.

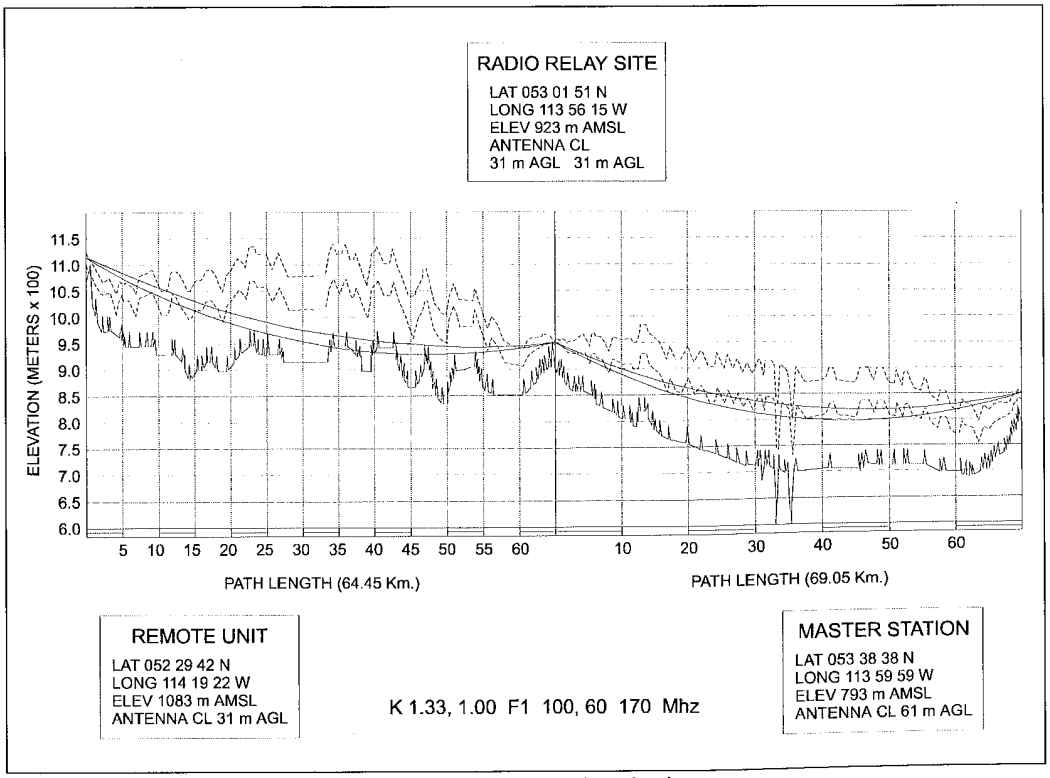


Figure 8-18. Simplified Path Study (Courtesy: ParaDimensions Inc.)

WB_00001178

Sometimes the safety margin for path studies is shaved thin to keep the cost of antenna towers or repeater stations down. There have been cases in which a system worked well during winter months, but when springtime brought leaves to the trees on a hill between the transmitter and the receiver, the signal level dropped down into the noise. Another problem is fast-growing coniferous trees that have needles that are just the right length to act as quarter-wave antennas, absorbing much of the incident radio power.

8-10. Solar Variations

Radio signals propagate through space as electromagnetic waves and are indistinguishable from other electromagnetic waves of the same frequency. One of the reasons that it takes a long time to get a radio license is that the agency responsible must determine whether the applicant will interfere with another receiver on that frequency and must ensure that no other transmitter on that frequency will interfere with the applicant.

But this cannot prevent the most powerful transmitter in the neighborhood from transmitting radio noise periodically. Every eleven years, the sun experiences a major series of storms that are accompanied by sunspots and flares. The effect on radio traffic is very damaging. UHF and microwave are less affected by solar variations than are some of the other bands, but even they may see increased amounts of noise. The best ways to minimize the effects of solar radio activity are to design initially for a high SNR and to keep the equipment maintained and calibrated.

8-11. Reliability and Maintenance

Solid-state electronics have made improvements in radio technology that could not have been imagined thirty years ago. Of course, the first thing that most people think of when such a statement is made is that the equipment is now smaller and uses less power. That, in fact, is true. But what is probably more important is that reliability and maintainability have been improved. Figure 8-19 shows a radio modem designed especially for SCADA applications.

Temperature compensation is now built in. Immunity to vibration and power supply transients is much better. But some maintenance of radio equipment is still required. Antennas loosened by the wind and shifted from their intended target must be realigned. The electric storage cells of uninterruptible power supplies (UPS), which ensure that the radios receive continuous electrical power, must be cleaned and refilled from time to time. Even the radios themselves can be damaged by lightning or can drift off-frequency and thus require checking and repair. But they are much better now than they were.

The Integration Group of The Americas Ex. 1007-Page 126
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001179

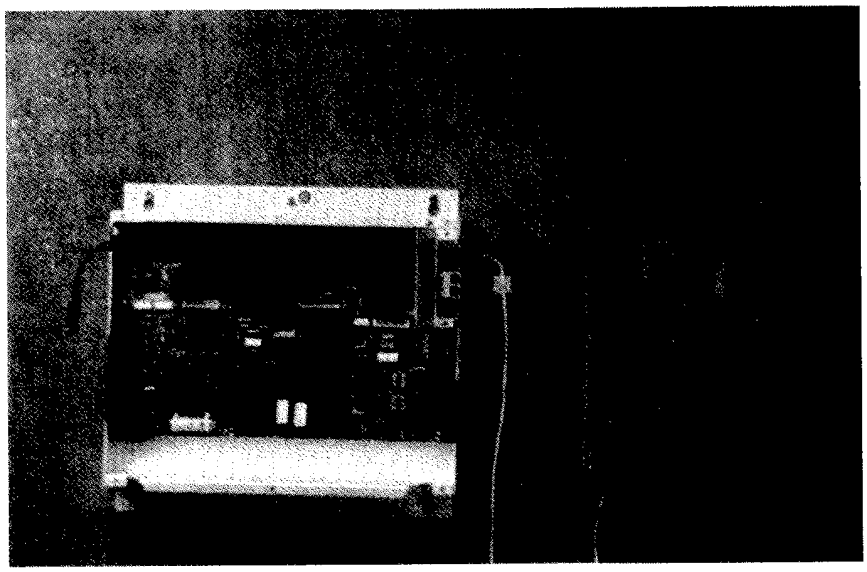


Figure 8-19. RTU with Built-In Modem (Left) and Built-For-Purpose Radio (Right) (Courtesy: Imperial Oil Resources Ltd.)

8-12. Satellite Communications

The use of geosynchronous communications satellites is now at the threshold of affordability for SCADA communications. For most applications, there are less expensive ways to send messages back and forth between MTU and RTUs. For very large systems such as pipelines and electric transmission lines, however, especially in remote, poorly developed areas, such satellites may be the most cost-effective communications method.

The principle is simple. The MTU and each of the RTUs have access to an antenna that is pointed at a satellite that stays over the same spot (hence the term *geosynchronous*). The satellite acts as a radio repeater, receiving data from one station and sending it to all the others. Usually, a capital cost must be paid for the antennas and special radio equipment. There is also a monthly fee for the service. This is much like the tariff charged for any utility communications equipment. The costs are becoming more reasonable as more users share the systems, which, of course, have very high start-up costs.

Another satellite-based system is becoming affordable faster than geosynchronous. Low Earth Orbit (LEO) or Highly Elliptical Orbit (HEO) communication satellites can operate without large expensive station antennae, because the distance between the station and the satellite is relatively small. Hand portable satellite telephones, needing small batteries and simple antennae, can communicate with these satellites for a

The Integration Group of The Americas Ex. 1007-Page 127
SitePro, Inc. v. WaterBridge Resources, LLC, et al.
WB_00001180

much smaller capital cost than they could communicate with geosynchronous satellites, but the method is the same.

8-13. Cell Phones

Cellular telephones are actually miniaturized radio transmitters and receivers. Their range is intentionally very limited because the system design includes cell stations that are close together. This combination allows for more cell phones to use available bandwidth. The shift from first generation cell phone systems to second and third generation has simplified their use as communication devices between RTUs and MTUs. The spread of cell phones outward from major urban areas has increased the likelihood that there will be a cell tower usefully near a process that needs SCADA communication.

Many cell phone companies are taking advantage of the fact that human speech is interposed with intervals during which no one is speaking. Since data for SCADA is not very time critical, it is possible to stuff small packets of SCADA data between sentences with no significant cost to the carrier. That is not to say that the SCADA user will get a free ride, but costs for the service may be low enough that cell phones may be the most cost-effective method of communication. If cellular coverage is almost but not quite good enough for your needs, discuss paying the communication utility to extend the system to meet your needs.

Tariffs for packet data cell service can be reasonable and are often based on the number of bits that are moved. This billing method should be considered when planning a SCADA system that will use cell phones. For example, rather than a straight polling system that requires each RTU to respond to a message from the MTU at frequent regular intervals, a report-by-exception system, requiring the RTU to transmit only when it has something significant to say, would result in a more cost-effective design.

8.14 Internet SCADA

Over the last several years, the concept of contract SCADA has been implemented using the Internet as the communications medium. Some of the products marketed as such are one-way data gathering systems, and as such are not really SCADA but are telemetry systems. As with any publicly accessible medium, the Internet exposes your communications to malicious interference. You must pay extra attention to data security when using such a medium.

The Integration Group of The Americas Ex. 1007-Page 128
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR [illegible]

WB_00001181

Unit 8 Exercises:

8-1. *Why is simplex communication not used for SCADA?*

8-2. *Why is transmitter turn-on time something to be avoided?*

8-3. *What concerns must you address if you plan to use the Internet as a communications device in your SCADA system?*

8-4. *UHF radios have some advantages over lower-frequency equipment; for example, the antennas needed to focus the signal can be made much smaller for UHF. What is one of the disadvantages of UHF?*

8-5. *For low speed SCADA, what two common media are used?*

8-6. *Name three methods for modulating a sine wave.*

8-7. *How many pairs of wire are in a buried telephone line?*

8-8. *As part of the communication procedure, one piece of equipment is responsible for checking to determine if the communications medium is in use. What is that equipment called?*

WB_00001182

Unit 9: Master Terminal Units—MTUs

The Integration Group of The Americas Ex. 1007-Page 130
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

Unit 9

Master Terminal Units—MTUs

At the center of each SCADA system is the device that issues all the commands, gathers all the data, stores some information, passes other information on to associated systems, interfaces with the people who operate the process, and actually seems to be in charge. This device is the master terminal unit (MTU). Some industries call it the "host computer." Sometimes it is called the "SCADA Server."

Learning Objectives—When you have completed this unit, you should:

A. Understand what makes the MTU unique in a SCADA system.

B. Understand the main functions that an MTU performs.

C. Understand the concept of configuring as it applies to MTUs.

9-1. Communications Interface

The MTU must send information to each RTU. It almost always uses the same medium that the RTU uses to send information to it. It also uses the same protocol as the RTU. In these respects, the MTU has the same communications interface capabilities and equipment that we discussed in Unit 7 in connection with RTUs. Most, but not all, SCADA communication happens using master-slave communications. The major difference between the RTU and the MTU is that as a slave, the RTU cannot initiate a conversation; as a master, the MTU can. Its communications are initiated by programs within the MTU that can be triggered by manual instructions from the operator (very unusual) or by other programs within the MTU (normal method). More than 99% of all messages from the MTU are automatically initiated.

The MTU must also communicate to the printers and video screens that form the operator interface. It does this with techniques that are identical to those used by any computer. For this reason, these communications will not be covered in this book. Many MTUs are required to pass data upward to accounting computers, corporate business computers, or computer networks. In some cases, proprietary protocols will be used. In other cases, open products designed especially for inter-computer communications will be used. At this level of communication, peer-to-peer communication is more common than master-slave communication. Nearly all of this type of communication is handled by local area networks (LANs).

The Integration Group of The Americas Ex. 1007-Page 131
SitePro, Inc. v. [illegible]
IPR-[illegible]
WB_00001184

9-2. Configuring a Picture of the Process

For the RTU to do all the things identified in Unit 2, a very detailed description of all of the sensors and actuators connected to the system must be available to the MTU's processor. To ensure it is handled in the most time-effective manner, this description must be arranged in an hierarchical form. Different hierarchical forms may benefit different processes; and frequently, several possible paths through the process description will result in the same action. This statement will be illustrated below in the description of equipment needed to detect a leak in a pipeline and shut in (turn off) the pipeline in response to the detected leak.

To visualize how the process picture can be described to the MTU, consider the very simple process shown in Figure 9-1, which represents a pipeline under the control of an MTU. At the input end of the pipeline, RTU #1 monitors the status of a pump, which may be either on or off. It also allows the pump to be controlled, on or off, and a block valve to be controlled, open or closed, from the MTU. It monitors the position, open or closed, of the block valve and allows the accumulated flow, or totalized flow, of fluid going into the pipeline to be gathered by the MTU. Finally, RTU #1 provides for a low-pressure switch, which will be interpreted as an alarm, to be monitored from the MTU. At RTU #3, the same functions are available, except there are no pumps to monitor or control. At RTU #2, there are only a block valve, which can be controlled and monitored, and the low-pressure alarm to be interfaced to the MTU. This is a very simple but workable SCADA system for monitoring and controlling a pipeline.

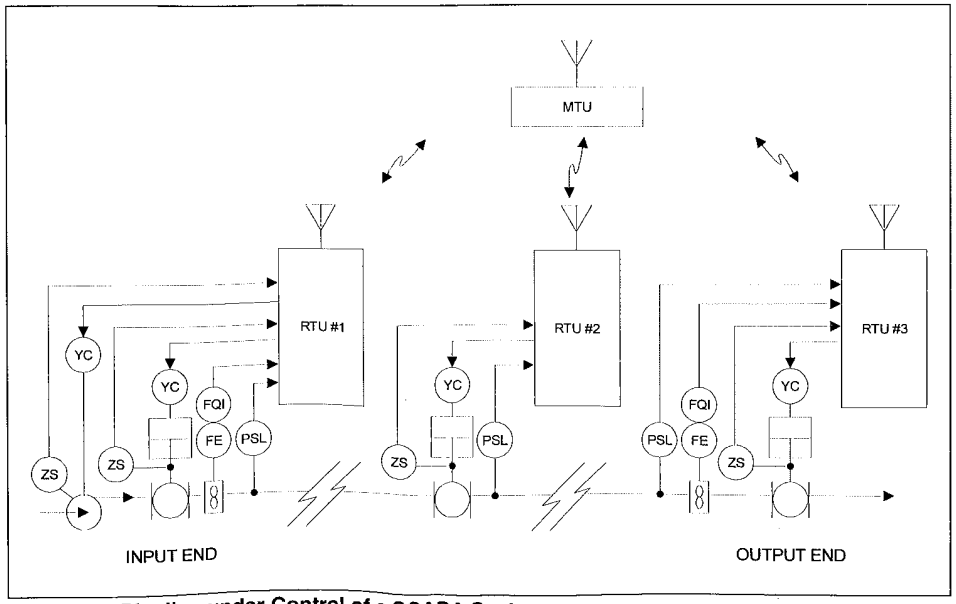


Figure 9-1. Pipeline under Control of a SCADA System

WB_00001185

What this system is required to do is continually measure the fluid going into the pipeline on a twenty-four-hour basis, subtract the fluid going out of the pipeline, and create an alarm at the MTU so the operator will know when there is a problem. The system should also watch the low-pressure alarm switch at each RTU and, if the pipeline is not working properly, create an alarm at the MTU. If the operator acts to shut in the pipeline, the MTU should send a command on a high-priority basis to each RTU that has an associated block valve, ordering the RTU to close its block valve. At the same time, the MTU should order RTU #1 to shut off the pump. It should then check to determine that each block valve did close. If the valve closed, the MTU should advise the operator. If the valve did not close, the MTU should advise the operator and resend the command to the appropriate RTU, telling it, again, to close the valve. If after some predetermined number of tries the valve has not closed, the MTU should advise the operator that the valve refused to close and will now stop trying to close the valve.

In addition to these actions, which happen at shut-in, the MTU should inform the operator whenever it is asked about the status of the pump or block valves. The MTU should allow the operator to remotely open or close any one of the block valves. At shift changes, and on request, the MTU should print out a report that tells how much fluid was inserted into and delivered out of the pipeline during the last shift, in the past twenty-four hours, and in the previous twenty-four-hour period. The MTU should also print, on a separate alarm printer, a description that includes the date and time of every change in an alarm condition as it occurs.

Later in this unit we will look at some of the decisions the MTU must make to fulfill these requirements, but the purpose of this section is to understand how the process is described to the MTU. This describing procedure is called "configuring." It consists of filling in lookup tables that the MTU can use whenever it needs to know what its world looks like.

Many people are familiar with desktop computers that allow different screens or printers to be connected to them. When the computer is being set up, the operator will be asked questions about the make and model of the device that is connected to each of the computer's ports. By answering these questions, the operator is providing a picture of the system to the computer—or "configuring" the system. Thereafter, if the computer is required to output a message on LPT1, it will use the correct protocol to talk to the printer at that port. The principle of configuring an MTU is not much different, but there are many more questions to be answered.

On the physical level, as shown in Figure 9-2, configuring the MTU is very similar to configuring a desktop computer. A video monitor must be described (VGA, EGA, color, etc.) and the report printer must be described

WB_00001186

(driver, paper source, paper layout, etc.) The alarm log printer must be described in a similar way. The connections to the RTUs must be configured. Assuming half-duplex radio communications, the configuration information must include such things as the length of time it takes for the radio transmitter to turn on and stabilize, the data rate, and the protocol. These describe the equipment that is physically connected to the MTU.

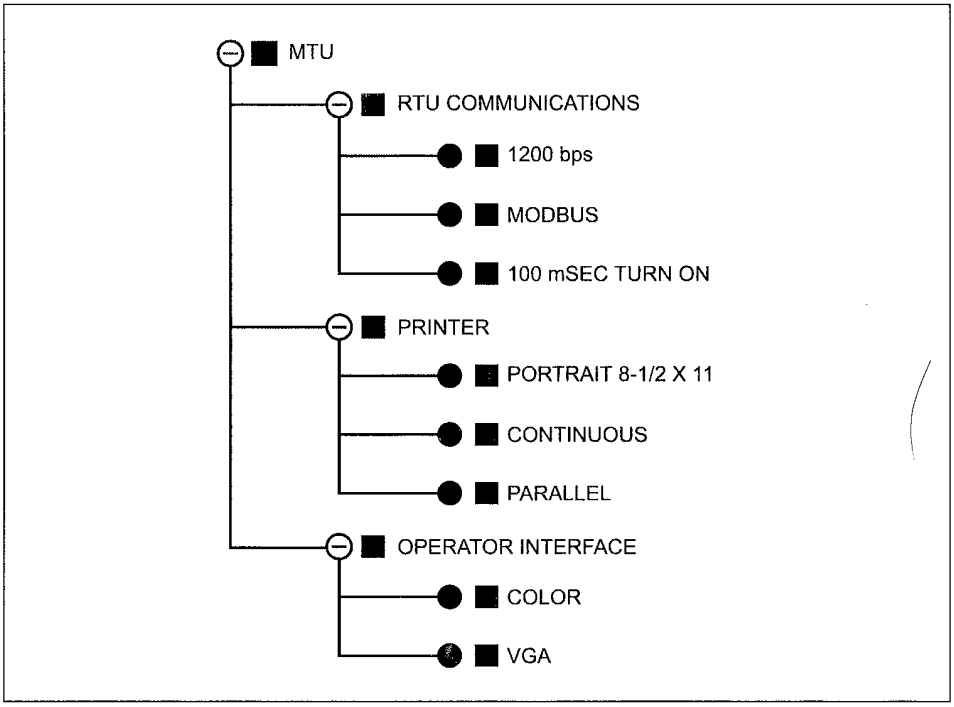


Figure 9-2. Configuring the MTU

Beyond the communications (in this example, radio), more layers must be configured. The MTU must be told how many RTUs there are and what the identification of each of them is. In this example, Figure 9-3 shows that there are three RTUs and that their identification numbers are 1, 2, and 3. Written in binary, this would be 00000001, 00000010, and 00000011. The MTU must also know what is connected to each terminal at each RTU. The configuration of the MTU must, of course, be identical to the configuration of the RTU at this level. Only the RTU with identification number 1 will be considered here.

In Figure 9-4, inputs to and outputs from the RTU have been grouped. At this stage we will define all discrete outputs as being coded 001, all discrete inputs as 010, and all totalizer inputs as 011. If there were any analog inputs, analog outputs, or pulse train outputs, they would also be

WB_00001187

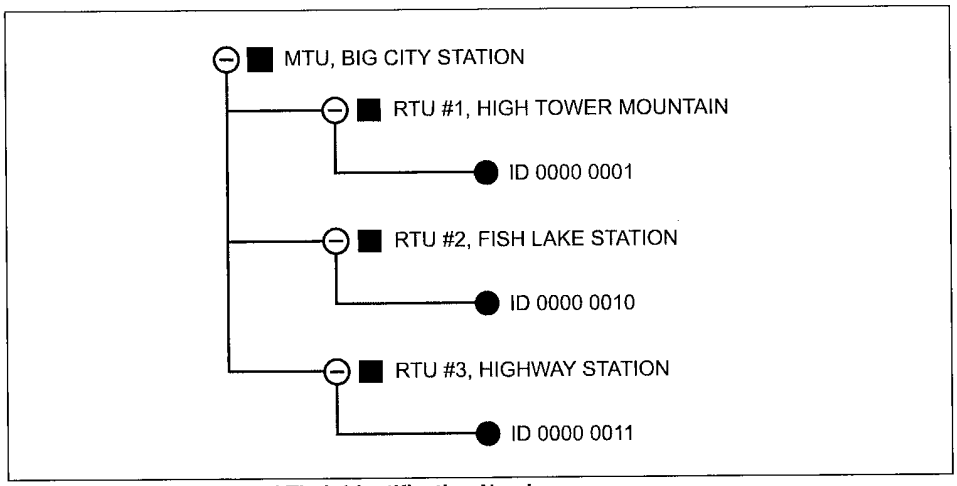


Figure 9-3. Three RTUs and Their Identification Numbers

identified as groups. Note that many of the configuration points within groups are shown as NC (not connected). RTUs are physically constructed as modular devices; thus, even though only one totalizer is needed, the smallest module available may have connections for four. The smallest module available for discrete outputs or discrete inputs may have four, eight, or sixteen. Figures 9-5 and 9-6 show samples of these modules.

With this simple coding system, we have now described essentially everything to which the MTU is connected. For example, to turn *Pump number 4* off, the MTU must deliver a signal through the modem to *RTU #1* that says, "Put 0 in the following register address:"

RTU #1	0001
Discrete Outputs Group	001
Pump #4 Device	0100
TOTAL ADDRESS	00010010100
TOTAL MESSAGE	000100101000

Similarly, to turn the pump on, the MTU must send a signal that says, "Put a 1 in the following register address:"

RTU #1	0001
Discrete Outputs Group	001
Pump #4 Device	0100
TOTAL ADDRESS	00010010100
TOTAL MESSAGE	000100101001

WB_00001188

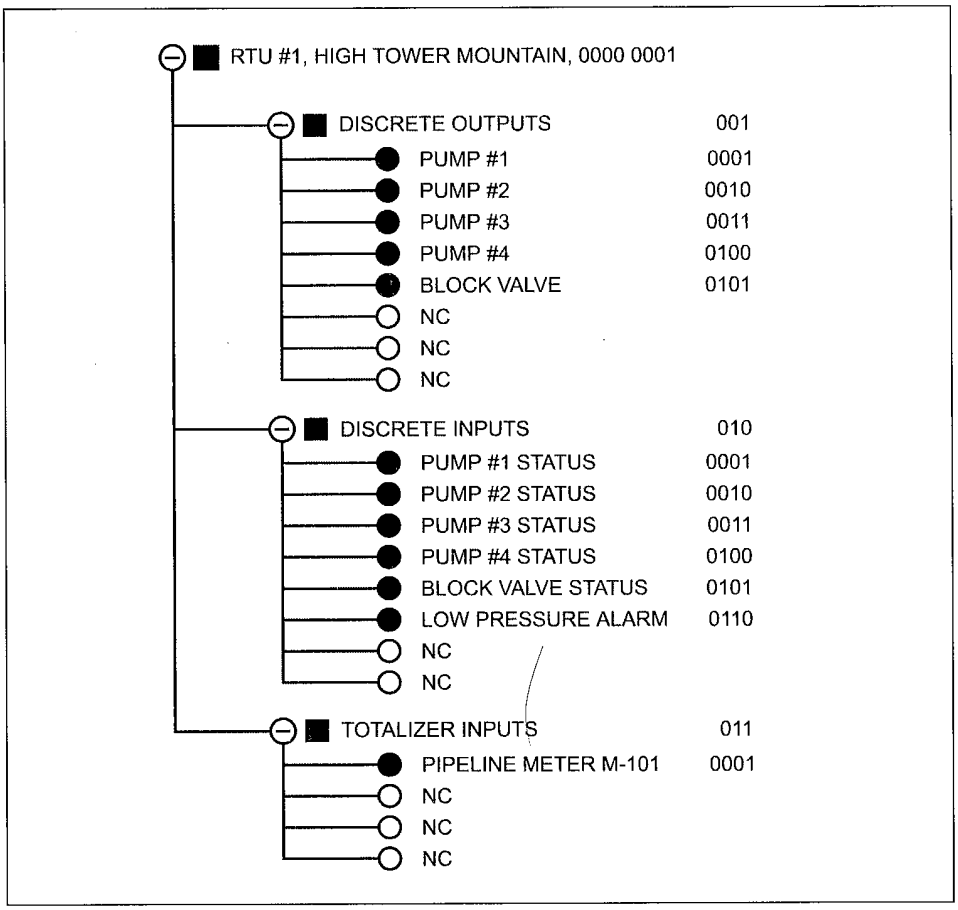


Figure 9-4. Grouped Inputs to and Outputs from the RTU

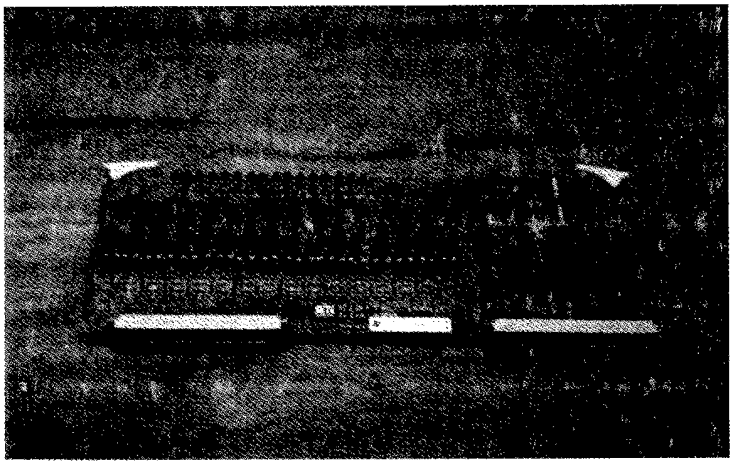


Figure 9-5. 16-Point Discrete Output Card (Courtesy: Imperial Oil Resources Ltd.)

The Integration Group of The Americas Ex. 1007-Page 136
SitePro, Inc. v. WaterBridge Resources LLC, et al.
WB_00001189

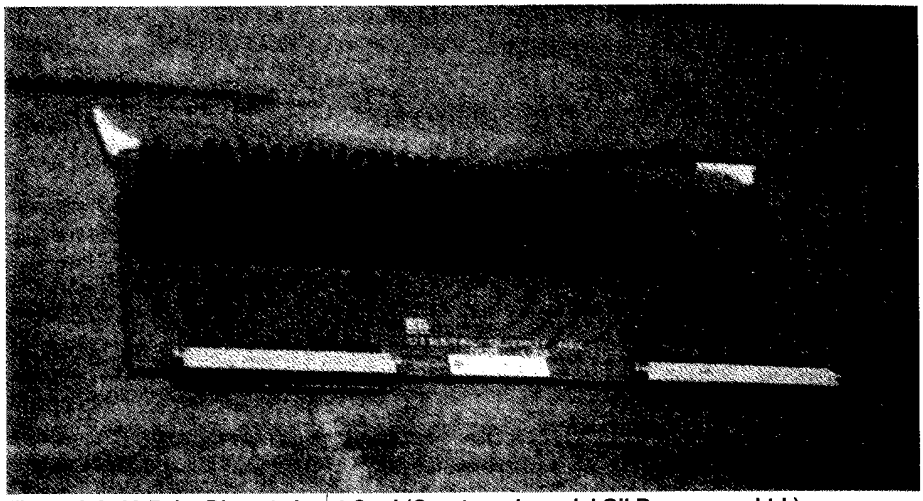


Figure 9-6. 16-Point Discrete Input Card (Courtesy: Imperial Oil Resources, Ltd.)

Similarly, to learn the status of the low-line pressure alarm switch at the middle of the pipeline, the MTU must order RTU #2 to advise the status by sending the following code to RTU #2:

RTU #2	0010
Discrete Inputs Group	010
Position #5 Device	0101
TOTAL ADDRESS	00100100101
TOTAL MESSAGE	001001001011

The MTU has put a 1 after the address to indicate to the RTU that it wants the RTU to send the status of that device. When the RTU sends its reply to the MTU, it will either put a 1 or a 0 in the last position to tell the MTU whether the switch is open or closed.

Notice that one bit, the smallest available quantum of data, is sufficient to open or close a valve, turn a motor on, or read a status switch. This is true only if a great deal of planning has gone into the message and if a great deal of care has gone into configuring the system so that the MTU and the RTUs know exactly where each piece of information exists. Totalizer inputs and analog points, such as valve percent open, are slightly more complex than discrete points. The information in these signal types cannot be contained in one bit.

Usually, an analog or totalizer word has been converted into 16 bits (although it may also be 8, 12, or 32). As long as both the MTU and the RTU are configured the same and the communications protocol can handle the word size, the number of bits doesn't matter. The message sent

WB_00001190

by the MTU to the RTU will describe the register location of the first bit of the word. When the RTU gets this message, it will send the information that is in that location as well as in the following fifteen locations to the MTU.

With this amount of detail, the MTU can be advised of what is happening everywhere in its universe. It can also reach every point that is connected to it to effect changes; however, some clarification is still required. It would be a real nuisance if the operator had to memorize these long codes, which are so easy for a computer to manipulate. An operator input-output interface or human-machine interface must be configured. After it has been configured, when the operator asks about the low-pressure alarm condition at RTU #1, the MTU will know that it is being asked what bit is in register position 0100101 in RTU number 0001; it will know that if it finds a 1 in that register position, the message it should send to the alarm screen is, "Pipeline Inlet Pressure Is Normal."

When all this configuring has been done, the MTU has a complete picture of the process and has the ability to communicate this information to the operators, RTUs, and others.

9-3. Some Simple Applications

Until an application is defined to the MTU, a picture of the process will be useless. Many standard applications apply to most SCADA systems. For example, one application might require that the MTU start a scan of every RTU every 10 minutes. Another application might require that the condition of every alarm point that is read be compared to its condition on the previous scan and, if there is a difference, print the new condition plus the time of the last scan on the alarm log.

These simple modular applications, which the MTU can treat as subroutines, can be combined with one another into useful, more complex applications. In programming parlance: They are equipped with "hooks" that allow them to be connected together.

Example 9-1. Using the SCADA layout and configuration defined earlier in this unit, let's investigate a leak detection application. Several better ways exist to detect leaks, but this method has been used successfully and has the attraction of being simple. It is called the Volume Balance Method.

The principle of this method is that for a non-compressible fluid (liquid) pipeline, what goes in should equal what goes out. If the flow rate out of the pipe is greater than the flow rate into the pipe, there is a measurement error, and perhaps one or more of the meters needs recalibration. If the output is less than the input, there are two possibilities: a measurement

WB_00001191

error or another undesirable and unmeasured output from the pipeline—a leak! The dynamics of the pipeline, particularly flow volume changes due to pressure surges, may cause short-term inequalities that can be filtered out by comparing running average inputs and outputs.

The layout of the application will look like this:

1. Conduct a scan of each RTU every ten minutes (scan).
2. Add the new line input meter reading to the previous four line input meter readings and divide by five (running average filter of input).
3. Add the new line output meter readings to the previous four line output meter readings and divide by five (running average filter of output).
4. Subtract the sum of line output meter readings from the sum of line input meter readings (difference).
5. Divide the difference obtained in Step 4 by the running average input obtained in Step 2 (error ratio).
6. Multiply the quotient obtained in Step 5 by 100 (percentage of error).
7. Compare the number from Step 6 to a number selected by the operator and defined as the "minimum error for alarm."
8. If the percentage of error is less than this operator-selected number, no further action is required. Go back to Step 1.
9. If the percentage of error is greater than this operator-selected number, check that an alarm was generated on the previous scan. If so, no further action is required. Go back to Step 1.
10. If the number from Step 6 is negative, send an alarm to the video screen that says, "Meter error in input meter or output meter! Check calibration." Send the same message with a time stamp to the alarm log. Go back to Step 1.
11. If the number from Step 6 is positive, send an alarm to the video screen that says, "Potential pipeline leak." Send the same message with a time stamp to the alarm log. Go back to Step 1.

Several changes could be made to this application to make it more useful, and many details would need to be added to make the application really work (for example, identifying the register location of the "operator-

WB_00001192

selected minimum alarm percentage error"); however, enough detail was shown in Example 9-1 to give you an idea of how an application works.

Example 9-2. One of the economic benefits of a SCADA system is that it enables an operator to make routine, manually initiated, remote control changes. In this example, we will rough out an application that allows the block valve at the pipeline inlet to be closed. The layout of the application would look like this:

1. If a keyboard entry calling for "Close Pipeline Inlet Block Valve" is made, set a flag (put a 1) in the MTU register reserved for this function.
2. Each time a scan is ordered, check this MTU register and compare what is in it to a register in the MTU that tells what the status of that valve is (1 for closed, 0 for open).
3. If the registers are the same, send a message to the video screen that says, "Pipeline Inlet Block Valve is Already Closed." Go to standby mode.
4. If the registers are different, include an order in this scan that tells the block valve at RTU #1 to close.
5. After the next scan, check that the block valve status at RTU #1 reads "Closed." Go to standby mode.
6. If the status reads "Open," resend the control order on the following scan.
7. After one more scan, check that the valve closed. If it did, send a message to the video screen that says, "Pipeline Inlet Block Valve is now Closed." Go to standby mode.
8. If the valve is still open, send a message to the screen and to the alarm printer that says, "Pipeline Inlet Block Valve Refuses to Close." Go to standby mode.

Example 9-3. You can see that when the SCADA system has determined that there is a "potential pipeline leak," the operator may want to move quickly to close all block valves. Rather than calling for a series of individual applications, each one of which will close and verify one block valve, another application can be developed. The layout of that application could look like this:

WB_00001193

1. If a keyboard entry calling for "Shut In the Pipeline" is made, set a flag (put a 1) in the MTU register reserved for closing the pipeline block valve at RTU #1, turning the pump off at RTU #1, closing the pipeline block valve at RTU #2, and closing the pipeline block valve at RTU #3.

   Each one of the four individual instructions should be accompanied by the same amount of detail as shown in Example 9-2.

2. Instead of waiting for the next regular scan, this order to "Shut In the Pipeline" has sufficiently high priority to initiate a special scan to the RTUs involved in shutting in the pipeline.

3. After ordering the RTUs, the MTU should go back to each of them to check for compliance. After advising the operator that the pipeline is shut in, the MTU should return to the regular scan.

More and more complex applications can be built up using simpler applications as modules or subroutines.

9-4. Data Storage

In the same way that the RTU is required to store certain critical pieces of data, such as meter values, for extended periods of time, MTUs must retain certain high classes of data. Their ability to pass information to the next higher level computer may be inhibited by the failure of machine-to-machine connections. An estimate of the longest time needed to discover and repair such a failure, including an adequate safety margin, should form a basis for calculating how much of the history of these critical data sets must be retained. If the failure will have an effect on the environment or on personal safety, a government regulatory agency will probably establish a minimum length of time that this data must be retained.

Before the capabilities of graphical interface tools existed, there was not much incentive to store large amounts of data. SCADA is an operating tool, so references to what happened four months ago were not seen as being very useful to operators. When graphical tools like trending became available, the situation changed. Operators could call up a trend of nearly any data point plotted against time. Plotting two or more trends provided information about the interdependence of sets of data that was otherwise difficult to visualize. This created demand for MTUs equipped with larger data historians.

The pendulum is swinging in the other direction now that computers have high-speed access to other databases via network communications. Figure 9-7 shows a block diagram of a system that allows an MTU, as well as

WB_00001194

many other subsystems, to store some of its data in a central data store. This capability will cause most of the data that is not critical for the operation (such as historian information) to be stored in the central data store. The data that is vital, such as lookup tables and configuration information, will continue to be stored in the MTU.

Much of the information needed to operate the SCADA system is of no interest to others outside SCADA. It is probably not worth retaining and will be erased after an expiration date is reached.

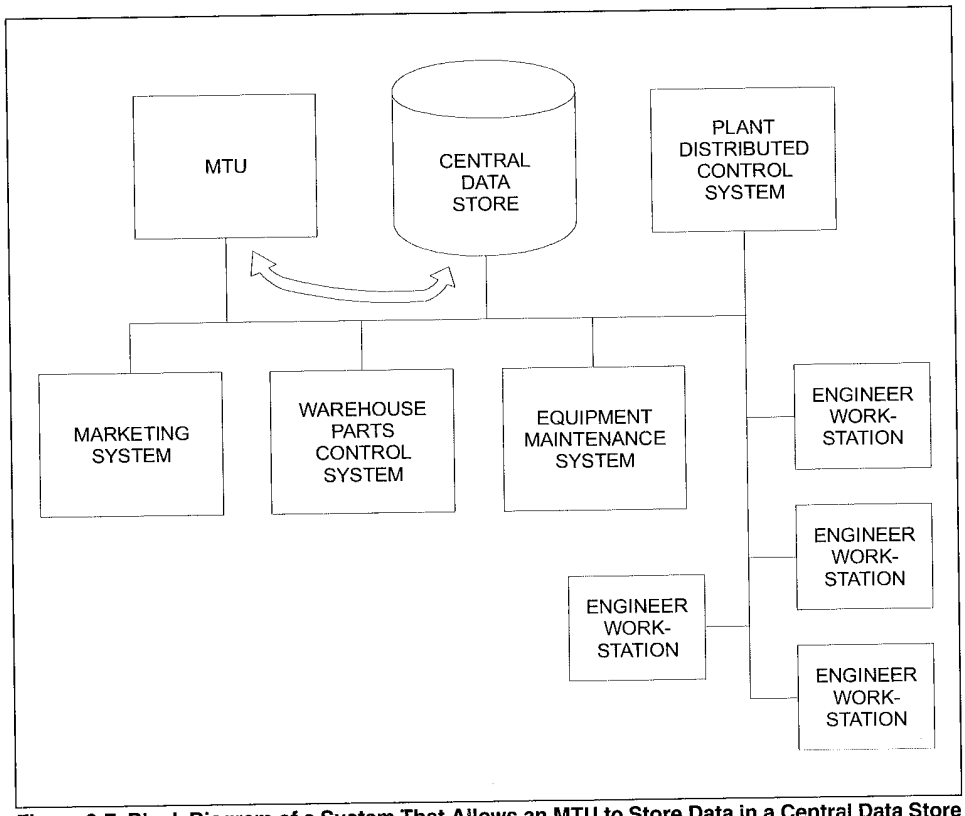


Figure 9-7. Block Diagram of a System That Allows an MTU to Store Data in a Central Data Store

Unit 9 Exercises:

9-1. *An MTU is the only station that can initiate a conversation with another station. This statement describes what kinds of communication?*

9-2. *Only one station has a definition of the entire process in its memory. What is this station called?*

9-3. *Each RTU has a part of that definition. What defines those things about which the RTU must know?*

WB_00001195

9-4. *MTUs communicate to three classes of machines. What are they?*

9-5. *By using groups of simple applications, the MTU can accomplish more complex applications. Examples 9-2 and 9-3 in this unit illustrated this for a pipeline and its block valves, respectively. Develop a similar scenario for an electric power transmission scheme in which the MTU has the ability to interrupt certain loads when demand for power is high.*

9-6. *Inexpensive memory led to more and more information being stored in the MTU. What technology may turn that trend around?*

9-7. *What effect do graphics have on memory demand?*

9-8. *In addition to communicating with other machines, storing information, and interfacing with the operator, what does the MTU do?*

The Integration Group of The Americas Ex. 1007-Page 143

WB_00001196

Unit 10: Operator Interface

Unit 10

Operator Interface

We have learned that of all the applications that the MTU performs, 99% or more happen independently of the operator. Most automatically generated applications, such as scanning and communications checks, are vital, but not process-related applications. They are activities like polling the RTUs in a scheduled scan, checking for communication errors, and the like.

Most of the control applications that SCADA implements are not initiated by the SCADA system, but rather are under the direct control of the human operator. Recall how the pipeline leak detection system in the last unit advised the operator that there was a potential leak in the pipeline, but left it to the human operator to make the final decision to shut in the pipeline.

SCADA is a hands-on operating tool with some automatic capabilities.

The very concept of a hands-on tool implies a requirement for fast, meaningful feedback from the process to the operator, and effective control input methods to the process. This unit will consider the operator interface, also called the human-machine interface (HMI) or the input/output (I/O). The operator interface is the junction from which information travels from the SCADA system to the operator and from the operator to the SCADA system.

The SCADA system should allow for monitoring of the status of equipment like valves and motors. It should receive input from process equipment when out-of-limits conditions exist, and tell the operator that there is an alarm condition. It should be able to present analog values, representing such things as level in tanks, electric current in conductors, speed of compressors, or percentage composition from chromatographs. Totalized values of flow, kilowatt hours, or process cycles should be viewable by the operator. Finally, some mechanism should be provided to receive instructions from the operator to switch certain equipment on and off and to adjust other equipment by incremental amounts.

Learning Objectives—When you have completed this unit you should:

A. Know the various media that are available to convey information from the SCADA system to the operator.

WB_00001198

B. Understand the various ways in which information is presented by the system to the operator.

C. Understand how the SCADA system can be developed to make the presentation of information to the operator most effective.

D. Appreciate how operator instructions to the SCADA system can best be organized.

10-1. Operator Interface on Very Small Systems

Many SCADA systems are installed to operate as little as one pump. The status, alarms, and controls for such a system can be adequately interfaced by a couple of panel lights and a switch. One light will tell the operator if the pump is running or not, a second light will tell if there is a power failure at the site, perhaps a third will tell if the pump station pressure is too high or too low, and the switch will let the operator turn the pump on and off. If the system grows much beyond one or two pumps, hardware operator interfaces are not the best way to go; thus, it will probably make more sense to have a computer screen dedicated to each of the stations and to build software copies of each station's panel lights and switches. With multiple stations, computer screens with graphic representations of the site equipment can provide more flexibility, lower maintenance costs, and lower capital cost than a hardware interface.

Even if the interface is hardwired lights and switches, the master terminal unit will still be a computer. Those changes in status or alarm that the MTU recognizes may be archived, with time and date stamps, for future reference if the design team believes that there would be a benefit to doing so. At least one hardcopy report of process changes, printed at a regular time (usually first thing in the morning), is usually available. A list of time-stamped alarms is also printed on a scheduled basis. These report types can also be printed on demand.

10-2. Operator Interface on Mid-sized Systems

Once the process complexity grows beyond six or eight status and alarm points and three or four controls, it becomes more effective to have information presented to the operator as symbols on a graphic that resembles a process flow drawing. When the design team is designing these graphic interfaces, or "screens," they should resist the urge to make them complex just because they can. The goal should be to have the graphical representation of the process be as simple as possible while still presenting all the information needed to operate the process.

The Integration Group of The Americas Ex. 1007-Page 146

WB_00001199

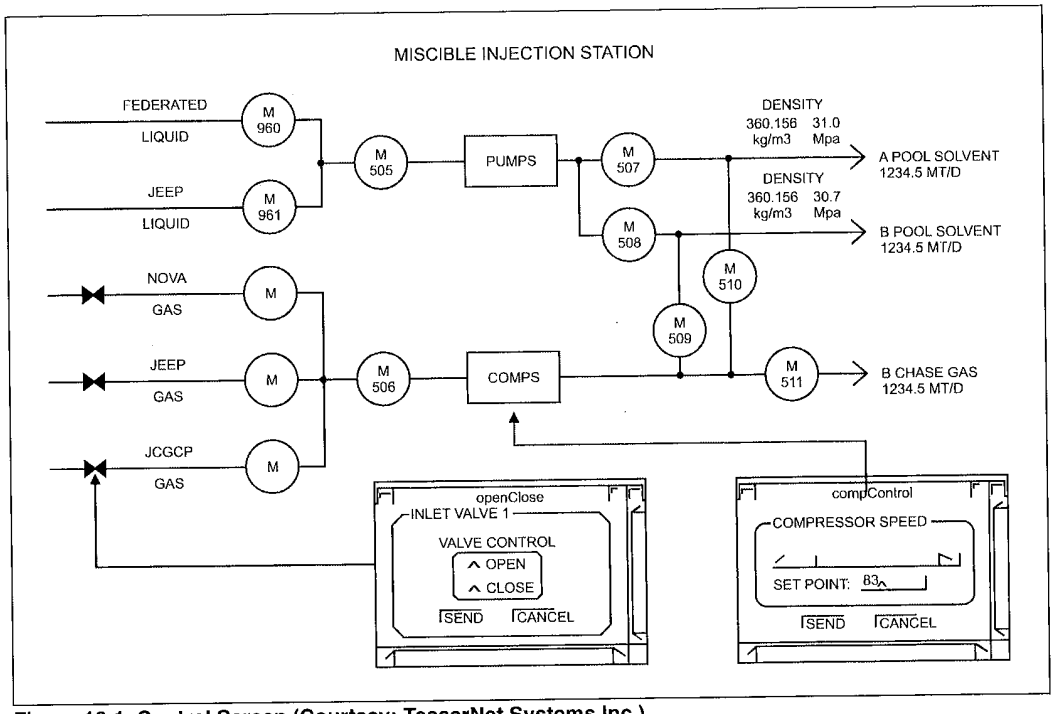


Figure 10-1. Control Screen (Courtesy: TesserNet Systems Inc.)

Figure 10-1 shows an operator interface screen showing the status of three inlet valves (lower left side). It also shows that pop-up controls for each of the controllable valves sit hidden until required and that pop-up controls for the compressors and pumps are available. The valve controls use a mouse to locate the cursor over one of the two choices, "open" or "closed," with a click to select. The compressor and pump speed are controlled by using the mouse to drag the speed set-point indicator to a lower or higher location on the speed indicator. The density and pressure of each of the gas/liquid blends are available, and flow rates (in metric tonnes/day) for three of the fluid streams appear at the upper right. This screen does not directly show alarm conditions, but if the process conditions are out of limits and there is an alarm, the density numbers, pressure numbers, and/or flow rate numbers could be made to blink. Most graphic screens developed today use colors extensively; perhaps too extensively.

If this graphic screen represented most or all of the process, monochrome would be sufficient. If there were three or four times as much process equipment being monitored and controlled by the SCADA system, you would use multiple pages, with an intuitive way to move from one page to any other. If the process were very complex, you could consider several video screens. One or two pieces of video display hardware with graphic screens laid out like this one would be sufficient for a SCADA system of nearly any large size. In addition, another piece of hardware that is

WB_00001200

dedicated to alarm indications and is equipped with a fast way to change the Status/Control Screen for each process section to one that may have an alarm should be provided for a SCADA system of any size. Much of the technology for a SCADA operator interface is shared with a distributed control system (DCS) operator interface.

10-3. Operator Interface on Large Systems

Most large systems could be controlled by an operator interface similar to the one just described for medium-sized systems. One video screen dedicated to alarms and one or two video screens for control/status and totalizer amounts (or some corresponding value in an electrical distribution system) are normally sufficient. Remember that the SCADA system is normally an operationally simple one that will usually be operated by one person, and that safety-related functions will be handled by local-loop, hardwired controllers. This means that fast operator response to upsets is not as important in Supervisory Control as it may be in Direct Process Control.

10-4. Local Security Considerations

When you consider that with a few keystrokes on a standard keyboard or a few mouse clicks on a screen it is possible to shut in an entire oil field, electrical power system, or pipeline, it will be apparent that some security measures should be in place to control who makes those keystrokes or clicks. We will deal, in some detail, with security considerations in Unit 12. For now, you should be aware that keeping unauthorized people away from the controls of the facility is important. Physical security and passwords are the first layers of protection to consider.

10-5. Monitor Status Points

Since SCADA is put into place to extend the operator's view and the operator's control of the process, let us first look at presenting process equipment status to the operator. Very early systems used a narrative list of equipment status that was updated and printed at regular intervals, perhaps every hour. This method did not provide any intuitive aid for the operator. Human beings think in terms of pictures and using a graphic screen similar to Figure 10-2 will help the operator remember how the field device that he or she is checking fits into the overall process.

When there are multiple devices that have similar effects on different process streams, they should be arranged in a similar way. Notice that the six pairs of valves on the left in Figure 10-2 allow produced fluid from each of six wells to be transferred to the Test Separator if the upper valve of the pair is open and the lower valve is closed. If the valve positions are

The Integration Group of The Americas Ex. 1007 Page 448

WB_00001201

dedicated to alarm indications and is equipped with a fast way to change the Status/Control Screen for each process section to one that may have an alarm should be provided for a SCADA system of any size. Much of the technology for a SCADA operator interface is shared with a distributed control system (DCS) operator interface.

10-3. Operator Interface on Large Systems

Most large systems could be controlled by an operator interface similar to the one just described for medium-sized systems. One video screen dedicated to alarms and one or two video screens for control/status and totalizer amounts (or some corresponding value in an electrical distribution system) are normally sufficient. Remember that the SCADA system is normally an operationally simple one that will usually be operated by one person, and that safety-related functions will be handled by local-loop, hardwired controllers. This means that fast operator response to upsets is not as important in Supervisory Control as it may be in Direct Process Control.

10-4. Local Security Considerations

When you consider that with a few keystrokes on a standard keyboard or a few mouse clicks on a screen it is possible to shut in an entire oil field, electrical power system, or pipeline, it will be apparent that some security measures should be in place to control who makes those keystrokes or clicks. We will deal, in some detail, with security considerations in Unit 12. For now, you should be aware that keeping unauthorized people away from the controls of the facility is important. Physical security and passwords are the first layers of protection to consider.

10-5. Monitor Status Points

Since SCADA is put into place to extend the operator's view and the operator's control of the process, let us first look at presenting process equipment status to the operator. Very early systems used a narrative list of equipment status that was updated and printed at regular intervals, perhaps every hour. This method did not provide any intuitive aid for the operator. Human beings think in terms of pictures and using a graphic screen similar to Figure 10-2 will help the operator remember how the field device that he or she is checking fits into the overall process.

When there are multiple devices that have similar effects on different process streams, they should be arranged in a similar way. Notice that the six pairs of valves on the left in Figure 10-2 allow produced fluid from each of six wells to be transferred to the Test Separator if the upper valve of the pair is open and the lower valve is closed. If the valve positions are

The Integration Group of The Americas Ex. 1007-Page 149
SitePro, Inc. v. WaterBridge Resources, LLC, et al

WB_00001202

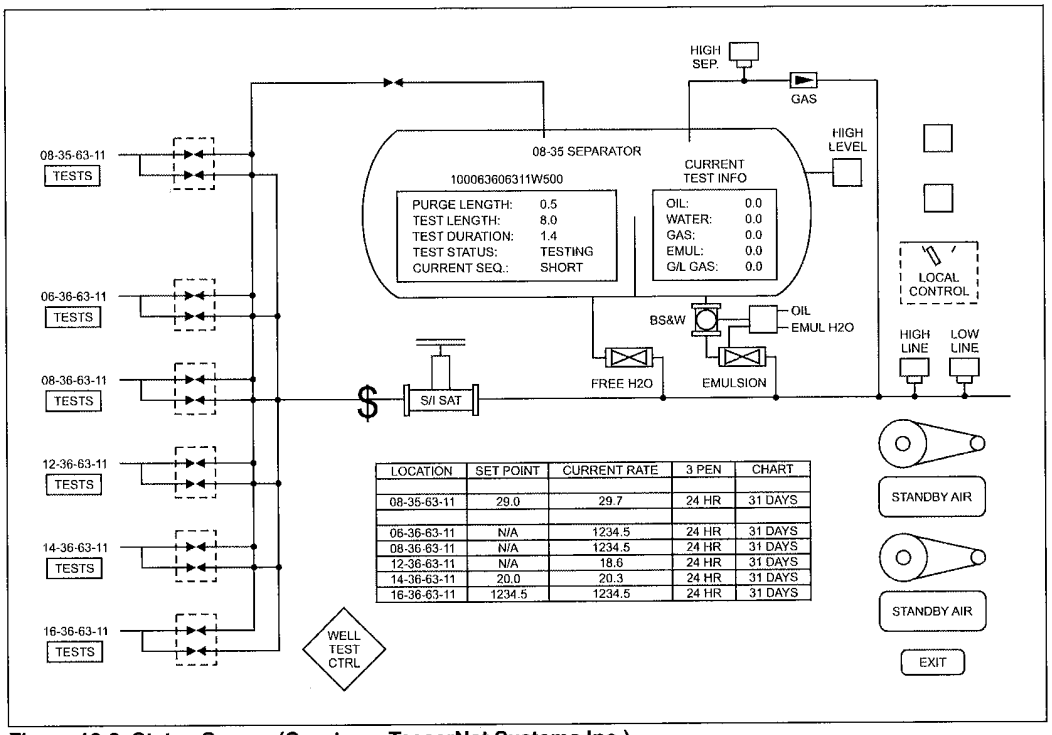


Figure 10-2. Status Screen (Courtesy: TesserNet Systems Inc.)

reversed, the fluid will bypass the separator and go to the pipeline. Borrowing a convention from driving, "Green for Go and Red for Stop," is often used for color-coding open/closed valves. If the valve is open, its symbol on the graphic should be green. If the valve is closed, its symbol should be red. This can be taken one step further, have the valve appear orange on the graphic while it is transitioning from open to closed.

In the lower right of the figure, two air compressors are shown. The color codes used for electrical equipment are not consistent. Some companies use, "Green for Go and Red for Stop," others opt for an electrical standard that is based on "Red for Run and Green for Safe(ly off)." Whichever convention you decide to use, be consistent throughout the company.

10-6. Monitoring Alarms

Two of the economic justifications for installing SCADA are keeping the operation running and restoring it to operation quickly when it does shut down. In Unit 11 we will discuss safety instrumented systems, which act to shut down (or otherwise make safe) a process so as to prevent injury to staff or the public, damage to the process, or negative environmental impact. In Unit 11 we shall make a very strong argument for having these safety systems local. Except for pipeline shutdown due to leaks, safety

The Integration Group of The Americas Ex. 1007-Page 150
SitePro, Inc. v. WaterBridge Resources, LLC, et al
WB_00001203

shutdown logic, which does not depend on the SCADA system, should be hard wired at the remote location to ensure that communication failures do not result in failure to shut down when an unsafe process condition requires shutdown.

When the safety systems do operate and shut down the process, the operator should be advised quickly so the upset condition can be rectified and downtime can be minimized. To this end, the MTU treats alarms in a special way. At the field site and in the RTU, they are treated the same as a status point. They exist as voltage levels on the output of a physical or electronic switch and influence the setting of a register position. Once they arrive at the MTU, they are treated differently. The condition of each point that has been identified as an alarm point is compared to its condition on the previous scan. The upper left portion of Figure 10-3 shows a simple eight-bit register in the MTU that holds the previous condition of eight alarm points. All alarm conditions are off except the ones stored in bits 3 and 4. The lower part of the figure is the register into which the last scan information has been entered. The MTU now does a bit-by-bit comparison to check for differences. When it checks bit 1 and finds that it is the same, it does nothing and moves to the next bit. When it checks bit 2 and finds that a new alarm has been generated, it goes into alarm mode. (More on that later.) When the MTU checks bit 3, it sees no change. Notice that there is an alarm here, but because it is not a change, it is ignored. When the MTU checks bit 4, it sees that the alarm that had been on is now off, and it passes this information on for additional processing. When it checks bits 5 to 8, it sees no change.

What has just been described is a "report-by-exception" mode. A SCADA system might monitor three thousand alarm points. If one hundred of them were in alarm (not an unusual situation) and the operator was advised of every scan, information overload would bring the system (and maybe the operator) to its knees. Report-by-exception alarming tells the operator about alarms only when their status has changed.

In large systems, even that amount of information may be too much. "Alarm storms" can occur inundating the operator with such a large series of report-by-exception alarm indications that he or she is overwhelmed and doesn't know how to respond. Consider the alarm regime of an unmanned oil production platform. Figure 10-4 lists four possible alarm conditions. If the generator has failed, the electrically-driven pumps will not operate, so it is not necessary to advise the operator about each one that has stopped running. The MTU can be programmed to inhibit the "Transfer Pump P-101 Stopped" alarm whenever the "Generator Failed" alarm is on. This is called *alarm override mode*. It can reduce the decision load during process upsets when the operator is busiest. The other two

The Integration Group of The Americas Ex. 1007-Page 151
SitePro, Inc. v. WaterBridge Resources, LLC, et al

WB_00001204

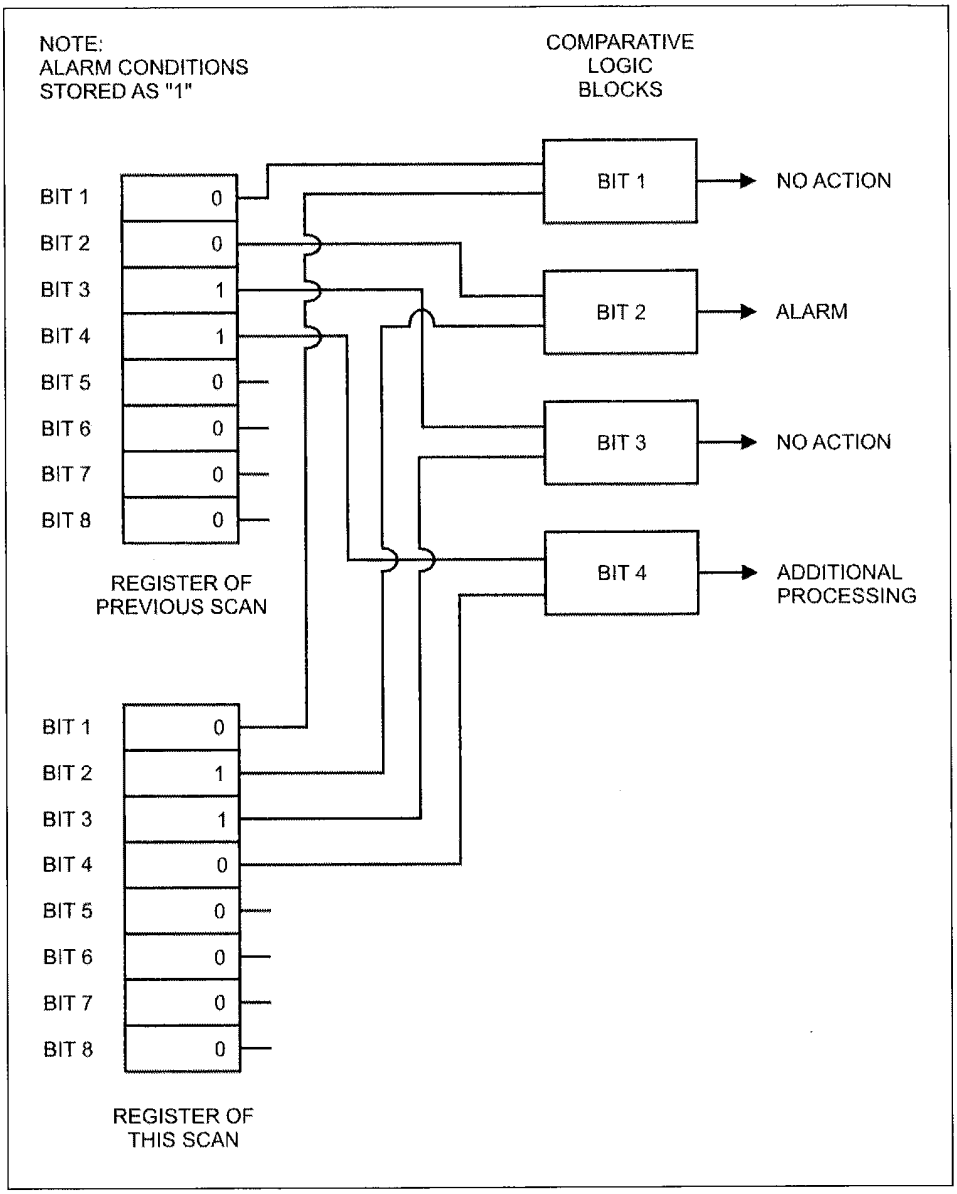


Figure 10-3. Checking for New Alarms

alarms in Figure 10-4 would not be overridden because they would be expected to operate even during a power failure.

Some alarm conditions are more important than others. Some cause no reaction except a comment in the next routine maintenance report. But in most SCADA systems, all changes in alarm status are logged and time and date stamped into an archive. This data is important enough that, often, a copy is made of it at the end of each day and the copy is stored off-site. Note that the time stamp is generated by the MTU based on when the

WB_00001205

Production Platform No. 1
Current Alarm Screen

- Electric Generator Failed
- Transfer Pump P-101 Stopped
- Fire in Generator Module
- Low Generator Fuel Level

Figure 10-4. Four Possible Alarm Conditions for Unmanned Oil Production Platform

change in alarm status was received by the MTU. For systems with long scan intervals, this time may be as much as one-half hour after the event actually happened.

If the alarm is not being overridden, it will be checked by the system for priority. When the system is being configured, each alarm point is assigned a priority. There may be between one and five levels of priority. Figure 10-5 shows that the lowest priority (in this case a priority 3) would result in the alarm being displayed on the dedicated "alarm screen." The second-lowest priority would cause the alerting of the operator, perhaps by a flashing symbol on the screen to refer to the alarm screen for further information. The highest priority would also result in the alarm being displayed on the dedicated alarm screen, but would sound an audible alarm as well, calling the operator to the operator interface station from wherever he or she was in the facility.

Alarm Priority	SCADA System Reaction
1.	Print on "Alarm Screen" Print on "Alarm Log" Flash "Alarm" on any active screen Sound audible alarm
2.	Print on "Alarm Screen" Print on "Alarm Log" Flash "Alarm" on any active screen
3.	Print on "Alarm Screen" Print on "Alarm Log"

Figure 10-5. Effects of Various Priority Alarms

Alarms must be acknowledged by the operator. When they are acknowledged, the special features (flashing and sirens) go away. Generally, a return to normal on a later scan will not cancel the features

The Integration Group of The Americas Ex. 1007-Page 153
SitePro, Inc. v. WaterBridge Resources, LLC, et al

WB_00001206

unless the operator has acknowledged the alarm. Time-stamping the operator acknowledgement into the alarm log is normally done by the MTU. Time-stamping the "Return to Normal" event is also done by the MTU.

An operator interface method that is becoming common is designed to reach operators that are not located at the site of the MTU. For those alarms that are prioritized at or above a selected level, the MTU can initiate a phone call to a telephone list of operators, dialing each name on the list until it is successful in reaching one. The MTU will then play a pre-recorded message that is tied to the type of alarm that has occurred. The operator can communicate with the MTU by using the telephone keypad numbers to indicate that he/she has received the message and acknowledges it. In some cases, the operator may also have limited control functionality using his or her keypad. Security may be a problem, and passwords will be required to assure the MTU that the operator is in fact the person answering the phone. This technique is becoming much more popular with cell phones and laptop computers that are wirelessly connected to the Internet.

10-7. Totalized Values and Trending

Most of the totalized data gathered is presented to the operator on graphic screens in order to contextualize it. Refer to Figure 10-2. The totalized flows of water, oil, gas, and emulsion are presented on the test separator graphic symbol to help the operator recognize that they refer to the present test. Below the separator, the current production rates of the six wells are presented, in tabular form, on the graphic of the production facility through which they produce. Any large SCADA system, whether for oil and gas production, electric transmission or distribution, irrigation, or water and sewer, will have totalized data points widely scattered. Presenting the data tied to their location will be more effective than presenting them as a large table or list.

Trending aids the operator by providing a graphic depiction of progress. By plotting recent history as well as the current reading, the operator can see at a glance if the situation is stable or is getting better or worse. He or she can also see when volumes or levels started to move away from optimal, and knowing this can aid in troubleshooting (see Figure 10-6). You can tell when the trouble began on this process just by glancing at the trend. You can tell how bad the trouble is and you can extrapolate to learn how much time you have to fix it.

Color adds another dimension that improves the "at a glance" ability of operators. Adding a limited number of colors draws the attention of the operator to the things that he or she must concentrate on.

The Integration Group of The Americas Ex. 1007 Page 154

WB_00001207

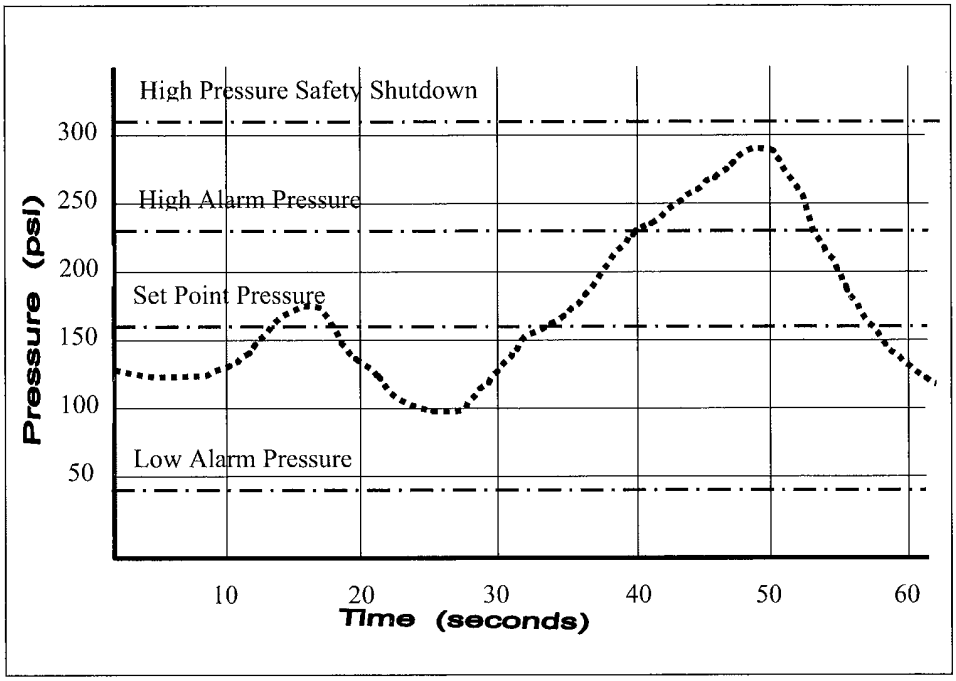


Figure 10-6. Trends Provide Implied Information

10-8. Control Interfacing

Because the available control functions are rather limited, the operator interface screens that allow these changes do not have to be complex. Figure 10-1 shows a simple screen that includes the control functions for an injection compressor and pumping station. Notice that for this application, and, in fact for most control and monitoring screens, all of the points refer to equipment at one location. In this example, most of the control functions can be effected by moving the screen cursor to a spot next to the control function and pressing the ENTER button. In the case of adjustments to the speed, the selected speed could be typed in after the cursor has been moved to near the speed select area, or the speed control could be selected by the mouse and dragged to the preferred speed.

Some control screens include an additional column to advise the operator of the present status of each control function. If this is done, some provision must be made to alert the operator that an order has been given and the system is waiting for the next scan to confirm that the order was implemented. Starting a compressor may require a dozen or more individual actions, each one of which must be accomplished in a definite sequence and only after various conditions have been confirmed. The logic for this detailed control is located at or near the equipment, often in the RTU. It is neither necessary nor advisable to locate it at the MTU. The SCADA operator is interested only in getting the compressor to start.

The Integration Group of The Americas Ex. 1007-Page 155
SitePro, Inc. v. WaterBridge Resources LLC, et al.
WB_00001208

After it is ordered to start, the operator wants to know if it did. If it fails to start, a message should come back telling of the failure. The operator can then send out a maintenance crew to repair the compressor or its control system.

10-9. Reports

Two of the vast number of reports that may be required from a SCADA system are alarm logs and communication reports. These reports may be grouped in several ways. It is common to pre-format the reports rather than have them printed in an ad-hoc form, and to have them grouped by function. Another grouping is those that print automatically at a fixed time and those that print only when asked for, or on demand.

Most companies operating SCADA still require that one dedicated printer be allocated to alarms. This is becoming less of a rule since the reliability of MTU computers and, particularly, their disc memories are much better than before. Alarm data is now archived in a historian, and that historian will probably be stored off-site as will the printed version. Although many days' worth of alarms may never be looked at, they are available if needed and don't take up much storage space. Since the alarm log printer records each alarm, as well as the time of its acknowledgement and return to normal, it is usually busy and noisy. Dedicated alarm log printers are often relegated to closets or other sound-proof rooms near the control room.

There may be need for routinely printed reports that the SCADA operator does not normally see. Daily communication reports, accounting-related information, and reports detailing the need for process maintenance are examples. These reports should also be printed away from the control room.

The final group of reports consists of those that the operator uses to run the facility. Examples include a special alarm report to help analyze a problem or a run report that enables each field operator to carry a hard copy detailing the recent operation of the part of the process that is his or her responsibility. The printer that produces these reports should be in the control room.

As SCADA systems are becoming integrated electronically with the rest of the corporation by local area networks, many of these reports are generated by other computers that are owned by other corporate departments. These reports use data gathered by the SCADA system, but their presentation method will be customized by the end user.

Portable computers, carried by maintenance workers, can be set up to gather and present information needed by the maintenance worker in his

WB_00001209

or her rounds. If these rounds take the worker into potentially combustible areas, the portable computer should be rated for the atmosphere to which it will be exposed.

10-10. Parallel Operator Interface

In its upward spiral, computer technology has now made it possible for multiple screen/keyboard stations to be connected to one computer workstation. Translated into SCADA language, this means that more than one interface can be driven by one MTU.

It is seldom a problem to have more than one operator running a SCADA system. If the load exceeds the ability of one operator, the system can be split into two or three completely separate sub-operations within the SCADA system. Operations that are growing or that are being updated can benefit from having the system engineer or technologist connected to the MTU. But when this is done, each operation uses a separate interface and is enabled by a password or the appropriate authority to avoid interfacing with the action of the operator.

This parallel operation requires that great attention be paid to enabling the various people who can access the MTU to communicate with each other. It also increases the importance of security for the system because now the system interface equipment has several physical locations.

Unit 10 Exercises:

10-1. MTUs can present information to operators in two forms. What are they?

10-2. Why is trending, the graphic representation of a series of data points, so effective?

10-3. What is the advantage of clustering pieces of similar data together for presentation to the operator?

10-4. In what way does the MTU treat an alarm point differently than it treats a status point?

10-5. What is the purpose of an alarm log?

10-6. What is meant by "reporting by exception"?

10-7. What technological tools are making the printing of maintenance reports unnecessary?

10-8. The purpose of SCADA is to extend the view and the reach of the operator. How is success in this purpose going to be economically justified?

WB_00001210

Unit 11: Remote Control— What Not to SCADA

The Integration Group of The Americas Ex. 1007-Page 158
SitePro, Inc. v. WaterBridge Resources, LLC, et al.
WB_00001211

Unit 11

Remote Control—What Not to SCADA

Every technology has applications for which it seems admirably suited, other applications for which it seems only marginally suited, and a group of applications for which it simply should not be used. When a technology is very young, it is often not clear which of those applications should be avoided. As the technology matures, the hard school of experience clearly identifies some of them. In this unit, we will discuss whether some types of control and data acquisition application should not depend on SCADA for their operation.

Learning Objectives—When you have completed this unit you should:

A. Recognize that some process control and data acquisition functionality should not be handled remotely.

B. Anticipate the type and magnitude of problems that can and will assail a SCADA system.

C. Be able to develop solutions to these problems.

11-1. Murphy's Law and Remote Control

Murphy lives! If you want to prove it, butter a slice of bread and drop it on the floor. If your intention is to prove that it will always fall butter-side-down, you will almost certainly note that this is so only about 50 percent of the time. On the other hand, if you drop it accidentally, it always falls butter-side down. In a similar way, a remote control system or a data acquisition system can be counted on to perform flawlessly until that moment when a message absolutely must be sent, or a piece of data essential to the financial continuity of the company is working its way from one end of the system to the other. Then the system will fail.

You can test the system. You can perform all manner of evaluations on each and every individual part of the system. You can run performance checks on the system as a whole. You can consult the experts. How many times has this author been told by maintenance technical specialists, "That system must be absolutely reliable. It hasn't failed since I've been here!" Believe it: If you depend on a remote control or data acquisition system to handle some critical function, it will fail. The more critical the function, the faster and more catastrophically it will fail.

WB_00001212

Over the years, signals that could potentially be placed on a SCADA system have been evaluated to determine which ones could cause a problem. The specific signals needed by individual industries will vary, but the general types of signals are fairly consistent. Two types should not be designed to depend on SCADA: the first are safety instrumented systems and the second are product measurement systems that will be used for billing or paying taxes and thus will require audit trails.

11-2. Safety Instrumented Systems

All processes should be equipped with a safety instrumented system if through failure of some part they may cause injury to a member of the public or a worker, or may cause damage to the equipment or the environment. Safety instrumented systems should be designed to override the normal control systems.

The normal control system, of course, is designed to monitor the operation parameters of the process and to make adjustments as necessary to keep the process within limits. This will ensure that the product meets a predefined specification and that process and related equipment do not leak, burn, explode, or otherwise come into potentially harmful contact with people or the environment. But the normal control system does not always work properly. Sometimes this is a result of mechanical failure. Sometimes the feedstock didn't meet specifications, or the energy source failed. Occasionally, the targets that the operator established for the normal controls to achieve were incorrect. Figure 11-1 lists the three characteristics around which safety instrumented systems are designed.

1. SHOULD BE ABLE TO OVERRIDE NORMAL CONTROL SYSTEM.
2. SHOULD NOT SHARE COMPONENTS WITH NORMAL CONTROLS.
3. SHOULD BE AS SIMPLE AS POSSIBLE.

Figure 11-1. Three Main Design Characteristics of Safety Instrumented Systems

If the safety instrumented system is designed to override the normal control system, it may operate to keep the process safe even when several failures occur simultaneously in the control system. If the safety instrumented system is designed so that its integrity does not depend on the continued operation of those elements of the normal control system, the joint reliability of the two systems will be improved. And, if the safety instrumented system follows the maxim of the U.S. Army, "KISS (Keep It Simple, Stupid!)," with a minimum number of parts, electrical contacts, and instructions, it will invariably work better.

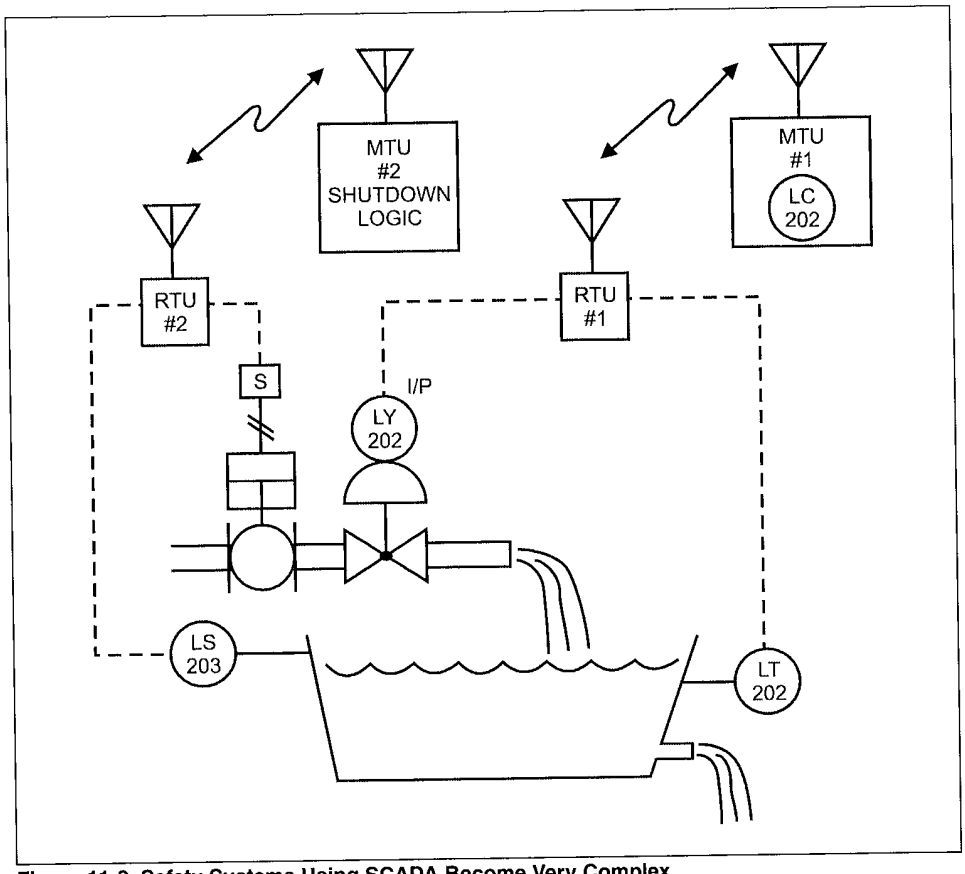


Figure 11-2. Safety Systems Using SCADA Become Very Complex

The last two of these three conditions for safety instrumented systems argue against the inclusion of the SCADA system in the safety instrumented system. With respect to the continued operation of the control system, it would be feasible to tie the sensors and actuators dedicated to the safety instrumented system into the SCADA. It would usually not be feasible to install a second RTU, communications system or MTU just for the safety instrumented system. Figure 11-2 shows how complex the situation could get for even a simple system.

"Keeping it simple" may be a relative concept, but few qualified designers would argue that SCADA is sufficiently simple to qualify as an appropriate element for a safety instrumented system. This is not to say that SCADA cannot be used to enhance the safety of geographically diverse systems. Pipelines are often protected from leaks by measuring inflow and outflow, subtracting the two, and closing block valves along the line if the difference gets too large. What it does say, however, is that the sensing, logic, and actuation features of a safety instrumented system at a local site should not rely on the SCADA system. In fact the design of a

WB_00001214

process that is to be controlled and monitored by a SCADA system should always include an assessment of the result of each conceivable type of failure of the SCADA. These assessments will identify some failures that can be classified as "high risk."

Risk is measured as the product of probability of failure and consequence of failure. If the probability is high and the consequence is negligible, then the risk is not high. Similarly, if the probability approaches zero but the consequence is high, then the risk is not high. But in some conditions, the probability of failure will be reasonably high and the consequences of failure will be serious; such conditions will indicate a high-risk situation. Figure 11-3 shows a matrix of this method for establishing generic risk.

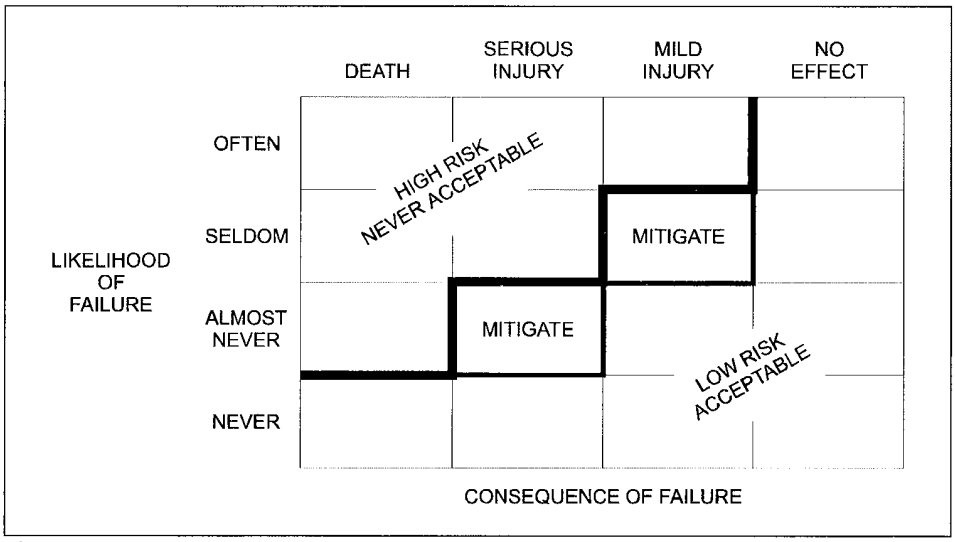


Figure 11-3. Matrix of the Generic Risk Establishment Method

The evaluation of risk is becoming an engineering specialty in its own right. It should be undertaken by people who are familiar with the process, equipment, operating conditions, and evaluation methods. High-risk failures should be guarded against by installing local safety instrumented systems. The International Society of Automation (ISA) has developed a standard, ANSI/ISA-84.01 – *Programmable Electronic Systems for Use in Safety Systems*, which deals with the requirements of safety instrumented systems.

Figure 11-4 shows an example of a SCADA-operated valve with a local loop override. In this case, a high liquid level will cause the valve to close even if the SCADA system tries to keep it open.

The Integration Group of The Americas Ex. 1007-Page 162
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078

WB_00001215

Example 11-1 illustrates one of the few high-risk applications in which SCADA is involved in a safety-related system. Even here, local loop protection may be involved.

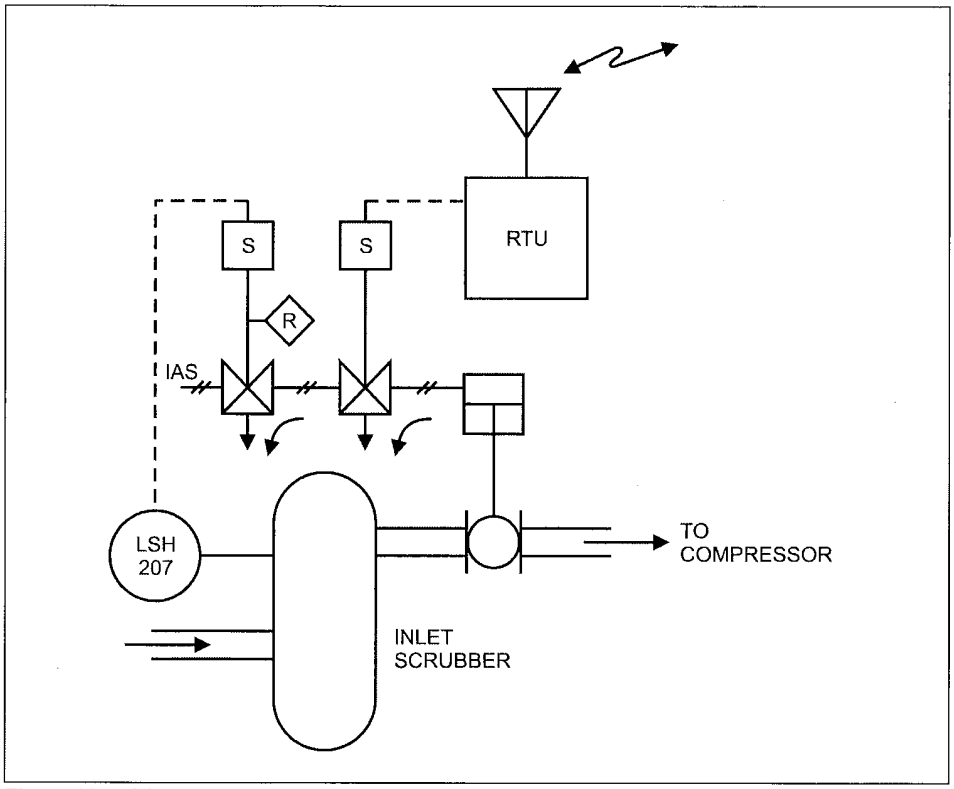


Figure 11-4. SCADA-operated Valve with Local Loop Override

Example 11-1. A SCADA system monitors the inflow and outflow of a liquid hydrocarbon pipeline. Refer to Figure 11-5. At the MTU location, calculations are done to determine if the inflow is equal to or less than the outflow. If more liquid is measured going into the line than going out of it, the MTU will recognize a leak and will send a message to the RTU at each end that will cause a block valve at each of those two locations to close. As an alternative, the MTU may send an alarm message to the operator who will then decide whether to shut in the line by closing the remotely-operated valves.

Murphy has the power to cause the radio at either one of the RTU sites or the MTU site (or all three for that matter) to become unserviceable at just that time. Rather than allow the pump to continue forcing oil into the line, the designer should assume that the MTU will not send a timely shut-down instruction. A local shut-down loop, as shown in Figure 11-6, that is based on low pressure or on the rate of change of pressure drop will not

The Integration Group of The Americas Ex. 1007 Page 163

WB_00001216

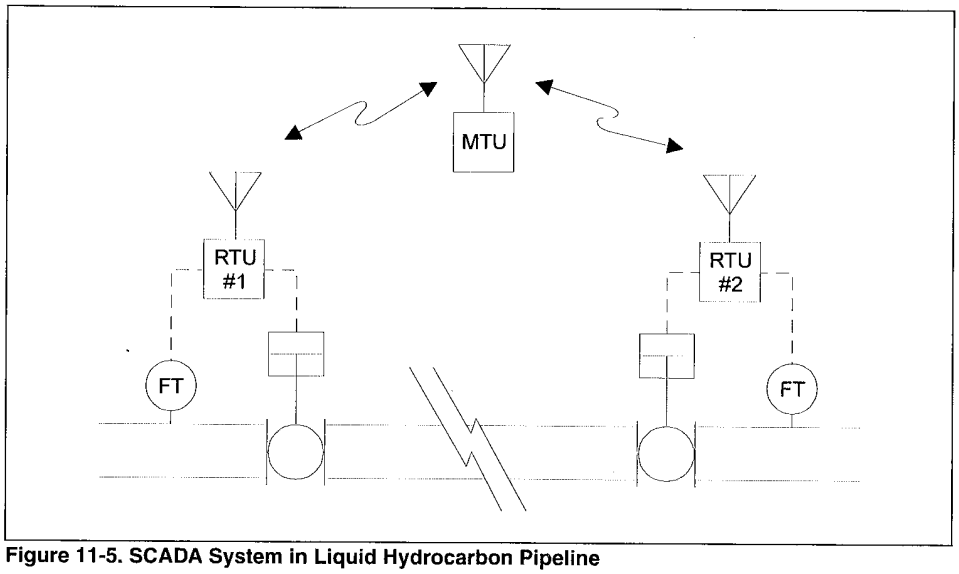


Figure 11-5. SCADA System in Liquid Hydrocarbon Pipeline

detect small leaks as quickly, but will provide protection for large leaks. The large ones are those with the most severe consequences.

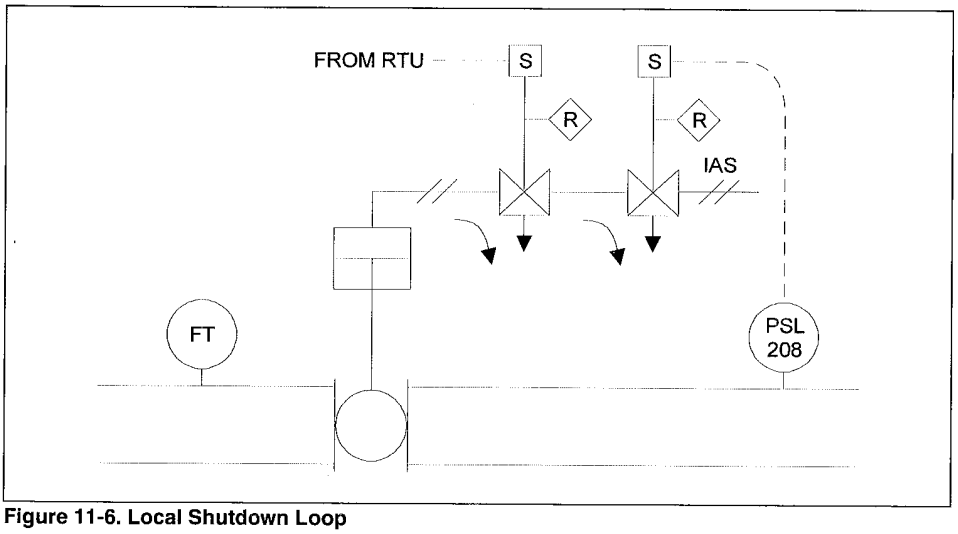


Figure 11-6. Local Shutdown Loop

11-3. Regulatory Requirements

For years we have been told that the computer is bringing on the age of the paperless society. That may be difficult to believe for anyone who is on forty mailing lists for computer-generated junk mail or who stores all of his or her e-mail on paper printouts. But even if we are approaching being

WB_00001217

a paperless society, some authorities still insist that certain data have a "paper trail." Some of these authorities have almost as much power as Murphy. They certainly have enough power to make it worthwhile for system designers to listen. These authorities are the ones who are responsible for ensuring that the measuring of weights, volumes, or other quantities of product is done correctly (both for the purchaser and any taxing authority) and that taxes, royalties, tariffs, and so on are paid in the correct amount.

Most industries follow government regulations requiring that something be measured and the measurement be reported to one or more government agencies. Often, the numbers reported represent large amounts of money that must be paid to the government. Examples of this process include the measurement of oil from a well, which requires that a royalty be paid, or the measurement of irrigation water from a government-owned reservoir, which requires that a fee be paid. Many industries have associates, customers, or suppliers with which they exchange products. The products may represent large cash values. If each of the parties is considered to be "sophisticated," rules will be established between the buyer and seller to govern the method of measuring and billing for the product transfer. Examples of this include electric utilities sending blocks of electric power across their transmission line for a fee or a pipeline company moving batches of clean natural gas through a pipeline for a tariff.

Some industries supply thousands of relatively small amounts of product to the general public. In these cases, the monetary value of each transaction may be small, but there are large numbers of transactions. Governments recognize that the public is "unsophisticated" about measurement and accounting techniques. For this reason, they often enact regulations that the measurement and accounting procedures follow certain forms. Records of each of these types of transactions will be required by at least one party in order to establish a paper trail.

The term "paper trail" comes from the method that auditors use to check that a true accounting has been made. They start with one piece of paper, such as a request for quotation. They then move on to the next piece of paper, which would be the quotations submitted, and on to the next pieces of paper, which may be the evaluation of the quotes, the order itself, the materials receipt, the invoice, the check, and then the final receipt. In following this trail, they can determine whether or not the proper procedures were followed, whether the right amount of material was delivered, whether the right amount of money was paid, and whether the proper people received the money.

WB_00001218

This procedure has proved to work well. It is not going to be supplanted by another method just because SCADA systems are capable of electronically moving some of those data elements that were once moved in triplicate on variously colored pieces of paper. In fact, compromises are currently being reached to allow more than paper records to form part of the "paper" trail. Many of these compromises recognize that electronic data is more ephemeral than data on paper, and they therefore require that a considerable amount of time must pass before this data can be erased from the primary measurement device, even after it has been transmitted to the data collection device. Some of the compromises are of the belt-and-suspenders variety, requiring that a physical printout be made on a daily basis even though the billing numbers are sent electronically.

Allowance may also be made for the fact that computer programs designed to calculate volumes of product or amounts of energy can be changed more easily than the mechanical devices that were formerly used to make the measurements. The security procedures for the devices on which these computer programs reside may be extensive, even including housing them inside locked metal boxes. However, the more likely approach, the controlled access of passwords, is sometimes accepted.

So, the paper trail does not always have to be fashioned out of paper. But some method for supporting an audit is required. Almost certainly, the primary measurement calculations should be done at the RTU location. They should also be stored at that location for some time afterward, perhaps as long as thirty-five days. Figure 11-7 shows a typical printout for a primary measurement calculation.

The regulations that deal with these measurements and how they are managed vary from jurisdiction to jurisdiction and also from industry to industry. You should be aware that such regulations are likely to apply whenever the custody of a material is transferred or some similar transaction occurs. You certainly should plan to acquire the data on your SCADA system, but you should also plan to acquire and maintain backup data by other means.

WB_00001219

NOMINAL OIL AND GAS CO. LTD.

GAS METERING STATION NO 1009
METER POINT NO 1009

DATE OF PRINTOUT 961020

STANDARD FACTORS
—PIPE DIAM. 201.3 mm
—ORIFICE SIZE 100.0 mm
—BASE PRESS. 101.325 kPag
—BASE TEMP. 15.0 °C

DATE YY/MM/DD	TIME HH/MM	DAY RATE km^3/D	CUM TOTAL km^3
96/10/19	23/59	121.62	2431.09
96/10/18	23/58	122.47	2309.47
96/10/18	00/01	121.22	2187.00
96/10/16	23/59	120.14	2065.78
96/10/15	23/59	112.09	1945.64
96/10/14	23/58	109.11	1833.55
96/10/13	23/59	118.77	1724.44

Figure 11-7. Typical Printout for a Primary Measurement Calculation

Unit 11 Exercises:

11-1. *Safety instrumented systems override control systems, are independent of control systems in terms of their elements, and are designed to have few parts. Which two of these characteristics indicate that SCADA should not be used for safety instrumented systems?*

11-2. *The level of liquid in a tank is measured by a displacer that outputs a signal to a valve controller. When the level gets above a pre-selected amount, the controller causes the valve to pinch back, reducing the flow into the tank. Can a signal from this displacer be monitored by the SCADA system?*

11-3. *Should a signal from the displacer in Exercise 11-2 be used for a protective override of the valve actuator?*

11-4. *What is it about communication systems that suggest they should not be used for "Safety Instrumented Systems"?*

11-5. *Electric transmission systems are often equipped with SCADA packages that can develop trends. From these trends, it is possible to predict when parts of a transmission line will become overloaded. Should remote switches be installed to allow the operator to isolate these sections of the line?*

WB_00001220

11-6. What other protection should be in place to protect these lines?

11-7. In addition to safety instrumented systems, what other function should not be dependent on SCADA? Why not?

11-8. Why do some regulatory agencies insist that the algorithm used to calculate fluid volumes be printed out by each flow totalizer once a day?

The Integration Group of The Americas Ex. 1007-Page 168
SitePro, Inc. v. WaterBridge Resources, LLC, et al.
WB_00001221

Unit 12: Security

Unit 12

Security

This unit is about the security of a SCADA system, the equipment and product that a SCADA system controls, and the data that it gathers. One of the things that make SCADA systems different from almost all other industrial control systems is that they exist, at least in part, outside of property owned and controlled by the owner of the process. The media used to transmit data from the field to the control center and from the control center to the field is almost always in the public domain.

One of the first things that must be done about the security of a SCADA system is to analyze if you need to do anything. The owner of the system should assign ownership of system security to one person, referred to here as the Security Owner. The Security Owner should form a team that is qualified and empowered to evaluate risks to the SCADA system and to implement fixes to problems that they identify. The mandate of the security owner should extend beyond the initial evaluation to a regular re-evaluation and follow-up.

Much attention has been focused on cyber security in the last 10 years. This has resulted in recommendations and comprehensive standards being developed.

Learning Objectives—When you have completed this unit you should:

A. **Know how to initiate an evaluation of security risk to your system.**

B. **Recognize the primary weakness points that could be attacked.**

C. **Understand that a team of the proper people will be more effective at solving the security problem than any one individual.**

12-1. What Is the Risk?

When most SCADA systems now in operation were designed and built, they were built with the intent to maximize their speed and effectiveness and to minimize their cost. If security was even on the list of things that the designer considered, it was down near the bottom of the list. If security was considered, it involved putting a lock on the door of the buildings that the RTUs were mounted in and putting a lock on the room where the MTU was located. Since RTUs were usually put in remote, unmanned places and contained neat things like radios and other electronic boxes, they were considered to be prime targets for the theft of equipment. Since

WB_00001223

MTUs had been specifically designed to be easy to operate intuitively, it was recognized that people could maliciously or accidentally make changes in the settings of the process in the field. Even so, no-one thought very much about it, and if they did, they were not very worried.

When airplane hijacking became rampant in the 1970s, it still did not seem likely to affect SCADA. After all, SCADA systems were complex and used radios and coded digital signals, and even the workers that used them on a daily basis did not really understand how they did what they did. It was not until the early 1990s that non-specialists had any understanding of digital communication. The World Wide Web at the beginning of the 1990s and e-mail near the middle of the 1990s started to catch the attention of the masses, and then the cat was out of the bag. Hacking into systems that were connected to telephone wires became popular, just to prove that it could be done.

There were few reports of SCADA systems being turned against their owners, although most companies that know they have been hacked into have little reason to advertise it and more reason to keep it quiet. There was recognition by SCADA users that a potential risk existed, but not much incentive to do anything about it. The al-Qaeda attack on the United States in 2001 resulted in attention being focused on the vulnerability of these systems and a push toward improving their security.

When a company decides to build a SCADA system or recognizes that it has exposure to a SCADA system that is not secure, it should assign the ownership of system security to a person within that company. No effective work is likely to happen if the responsibility is not accepted. The security owner (whatever his or her official title) should know what is expected of him or her and should know what resources are available. The cost of failure, both to the company and to the owner, should be discussed.

The owner should form a team of people consisting of specialists in the process, the control system, cyber security, risk management, and the company's goals and prospects. The team members will undertake to analyze what could go wrong. They should consider the potential for damage to equipment and for loss of product, be it electricity, irrigation water, oil, or gas. They must consider the loss of data, including competitive advantage loss if this data should become known by companies in competition with the owner's company. Damage to the environment, with the attendant loss of corporate reputation and the cost of fines and remediation, must be considered. Personnel injury or death, to both employees and the public, must be a part of this evaluation.

If the team determines that there is no risk to the company, the environment or the public, then the team can be disbanded and the owner

The Integration Group of The Americas Ex. 1007-Page 171
SitePro, Inc. v. WaterBridge Resources, LLC, et al

WB_00001224

reassigned. This situation may exist if the SCADA system controls a benign process like water pumps for a non-competitive organization like a municipal authority, and that process is well designed with local-loop safety shutdowns available and no connection to the Internet.

If there is a risk, that risk must be quantified. Risk is the product of the likelihood of an event multiplied by the consequences of that event. The team should be selected to include members, be they company employees or contractors hired specifically for this assignment, who have the experience to identify all of those things that could go wrong, and to estimate the probability of them going wrong. They should also be capable of estimating how much it will cost to reduce the risks to an acceptable level.

A report should be presented to company management by the security owner, who will retain responsibility for reducing the risks that management decides to address. Team members will be released as decided by the owner.

12-2. Risk Evaluation Procedures

There are several documents useful for such risk evaluation (see the Bibliography for "21 Steps to Improve Cyber Security of SCADA Networks" and "ANSI/ISA-99.02.01-2009 *Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*"). Both of these documents stress the importance of first identifying any connections between the SCADA network and other networks. This is best done by reviewing an existing drawing or drawing a new network diagram of the SCADA system, including all ties to other networks, including corporate networks and public networks. The team should then do a physical check to ensure that the network diagram is correct. The author's experience shows that existing drawings are almost never complete and correct. In most cases, connections exist that are not shown on existing drawings.

Keeping the SCADA system as isolated as possible from other networks is important. Keeping it isolated from the Internet is the most important. Risk to the system is a function of how accessible it is to interference from potential attackers, and the Internet includes an almost limitless number of potential attackers.

A second item to consider during the risk evaluation is whether the SCADA system has security features, their effectiveness, and whether they have been disabled. Early systems generally were provided with no security. Some later systems have rudimentary security: "We haven't had any problems, so we don't need much security." Security features often

WB_00001225

make it difficult to install or modify applications in an existing SCADA system. During such installations, it is convenient to disable them to get the system started. Sometimes, the installer forgets to turn them back on.

The effectiveness of any security system is based on what it was designed to protect against, and what is vulnerable to attack. As you know, new computer viruses are being developed every day and new anti-virus procedures are continually being developed to combat them. Similar escalation occurs in industrial security. Does the existing system include Intrusion Detection to tell you if anyone has tried to get into the system?

A third consideration is the attitude of company management to the issue of cyber security. Are they knowledgeable enough about the potential effects of a security breach? Are they prepared to support the training, equipment, and software replacement that may be necessary to bring security up to an acceptable level? Is there an organization in place to monitor the system continuously and to recommend and follow up on improvements?

The fourth item to look at is the physical security of the SCADA system. Can anyone walk in off the street and get to the MTU console? Are the RTUs in locked, fenced enclosures? Are radio antennas and their feed cables suitably protected? Are power supplies as secure as the rest of the hardware? Is there a system in place to archive data at a secure location and in a timely fashion? Has the control system for the process been designed considering the possibility of SCADA not being available? This point considers the need, for example, of a safety over-ride system to ensure that an unintended pressure increase does not exceed the ability of the piping system to contain the process fluid.

12-3. Risk Mitigation

After confirming that the SCADA network drawing is correct, the team should analyze it for direct or indirect connections to the Internet and for any connections to any other networks.

Challenge the need for every network connection. It is so much easier to move information to and from a SCADA system by using network connections that this has become the default thing to do. In fact, most information can be moved using other methods, albeit not so easily. Consider alternative methods for moving data to and from the SCADA system. Originally, SCADA MTUs were not connected to application computers. Applications were sometimes written inside the MTU computer; sometimes on separate computers. If on separate computers, the resulting supervisory settings were passed to the SCADA operator, who manually directed the SCADA system to its new target. Production

The Integration Group of The Americas Ex. 1007-Page 173
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR2025-01[illegible]

WB_00001226

results were output on printed reports. Information that had to be input into other systems was done by hand or by moving memory media (tapes) from one system to another. This can still be done, and it will obviate the need for a hardwired connection to other systems.

If the team finds connections that cannot be eliminated, then you must ensure that firewalls are installed between the SCADA system and the network that you have been unable to disconnect. Be prepared to accept some throughput reduction, although this may be so small that it will not be noticed.

A SCADA system that is discovered with no security capability should be upgraded. Ensure that any security capability that was provided with the system is turned on. As we have seen, if your system was installed 10 years ago or more, there may have been no attempt to provide cyber security. Purchase and installation of security software from the MTU supplier may be all that is needed to address this weakness. It may be necessary to work with a security software specialist to meet your needs. In some cases, it may be necessary to replace the MTU hardware in order to get software that will be sufficient for your needs. If it is very old, replacement of the master terminal unit may solve problems in addition to the security issues that you have discovered. The costs, both for the hardware and for the reconfiguration, will be high for this solution.

Intrusion detection and alarming is a valuable capability. Data from conventional industrial safety programs that have kept track of near-misses have shown that those facilities that have large numbers of near-misses will also have large numbers of safety incidents. It is the same with cyber security. In order to know if you have security near-misses, you must have the capability to recognize and alarm if someone is trying to break into your SCADA system. If you do not have intrusion detection, get it.

Company management has a responsibility to provide the manpower and funding necessary to protect company resources from theft and vandalism. That does not necessarily mean that company management knows all about the threats that are out there. If no security owner has been assigned, and no team put in place, technical employees in a company have a responsibility to tell the management about what these threats are and how they can be countered. In the absence of dedicated individuals, the people who work on a daily basis with the SCADA system and the information technology specialists for the company are the ones who are best able to communicate these specialist problems and solutions to management for their consideration.

It is only recently that training has been generally available on the subject of cyber security. As a consequence, very few technical specialists have

WB_00001227

received much formal training and there is little feedback about such courses. When you do attend meetings or courses on the subject, document your opinions about them. Ensure that the people in your company who can increase the number of attendees for good cyber security courses learn about those courses that are good—and those that are not.

Before the term "cyber" came into the vocabulary, physical security was recognized as important. It is still important and this form of attack should be included in the items that the team evaluates. Any process that provides a valuable product should be kept operating. Any process that includes expensive equipment should be protected against vandalism and damage. Any feedstock or product that could injure workers or the public or could damage the environment should be kept enclosed in the process piping. It is possible to upset any of these three situations using cyber attacks—but it is also possible to upset them by physically entering and damaging the process equipment.

These attacks can be reduced by installing fences, buildings, locked doors, and security glass windows. Physical intrusion alarms and closed circuit television should be considered at locations where company personnel are not normally situated. This type of protection should also be considered for locations that do not normally have RTUs, such as radio repeater towers, utility power stations. and source water locations.

Master terminal units are normally located in high population density areas. They are more likely to attract attackers, since they are easier to get to. Providing secure, locked rooms for these facilities is important. Keeping the locations of these facilities secret may be just as effective. I know that there are at least five large MTUs for major companies in my city, and although I have a professional interest in them, I know where only one of these MTUs is located. Security training of corporate employees includes recognition that talking about such things as MTU locations will not benefit the company, and may damage it.

The team should evaluate making provision for the operation of the process in the event of loss of the MTU. Often, large SCADA systems have back-up MTUs located at separate locations. Most often, these back-up MTUs are more basic than the primary MTU, because it is recognized that they will not be used often. They may be used during primary MTU upgrades, but the most important reason for their existence is that they are available if the primary one is damaged. Similarly, the archiving of data from the SCADA system should occur at a location other than at the MTU. It may not be necessary to have this archived data in as readily accessible a form as the original data, since it will not be accessed as frequently.

The Integration Group of The Americas Ex. 1007-Page 175

WB_00001228

12-4. Document and Follow-Up

The final product of the cyber security team should be the writing of the documentation and the presentation to company management. The documentation should include all the network drawings, details of the equipment that comprises the system, the results of tests of the system elements, recommendations for improvements, and results of the presentation to management.

After all questions are answered, the team should be disbanded. The security owner should continue to hold his or her position, even if the only thing that the owner is responsible for is the regular re-evaluation of the cyber security of the SCADA system, and providing answers to security-related questions from company management.

Unit 12 Exercises:

12-1. *What are the two divisions of security that can apply to SCADA systems?*

12-2. *After company management has recognized the potential for a problem with the security of the SCADA system and has assigned a security owner and approved a security team, what is the next thing that should happen in the evaluation of the problem?*

12-3. *Why is it important that a security owner be assigned to confirming the adequacy of SCADA system security?*

12-4. *Were old SCADA systems designed with better security than recent ones?*

12-5. *Why would anyone turn off the security features of a SCADA system?*

12-6. *What is the purpose of keeping the owner assigned after the security status report has been presented to management?*

WB_00001229

Unit 13: Applications

Unit 13

Applications

No accumulation of parts or subsystems can be justified unless it serves some useful purpose. This unit will discuss some of the common applications that SCADA systems are built for and how they may be used for either automatic or remote control of the processes. Perhaps more importantly, it will also present features of SCADA systems that allow these applications to be applied so you may evaluate and develop your own applications.

In addition to industry-specific applications, applications that are common to all, or nearly all, SCADA systems will also be discussed. These applications include items such as scanning, communications analyzing, reporting, and the like.

Learning Objectives—When you have completed this unit, you should:

A. Be aware of the broad classes of purposes to which SCADA is applied.

B. Recognize those features that support and those that inhibit the application of SCADA.

13-1. Real Time Revisited

As we learned earlier in this book, real time can be thought of as an event happening in less than the time that is available for it to happen. The time lag associated with transferring information from a field sensor to the RTU (or from the RTU to a field-mounted actuator) is essentially zero. RTU scans are fast. On the other hand, significant time delays are caused by low communication data rates and protocols that encourage regular, scheduled interrogation for each point in the system by the MTU. The time delay required to correct a problem may be as much as two scan periods. See Figure 13-1 for an application that involves the MTU. This inherent potential time delay is not critical for many applications, but for others it can be the determining factor. Some applications, such as the following example, simply will not work when a significant time delay is introduced.

In Figure 13-1, a SCADA system monitors the operation of a bank of compressors and a distribution pipeline to learn if the compressors are running and to keep track of pressure in the line. The gas is injected at specific points into oil wells, and the resultant reduction in the average

WB_00001231

density of the well-bore fluid causes more oil per hour to get to the surface. Each well has a different productivity of oil raised per unit of gas injected. If some of the compressors fail and the pressure of the distribution system starts to drop, some wells will stop producing. These gas-lift systems may be large, covering hundreds of square miles. Restarting a gas-lift well usually requires that an operator visit each well, often for several hours, until it stabilizes.

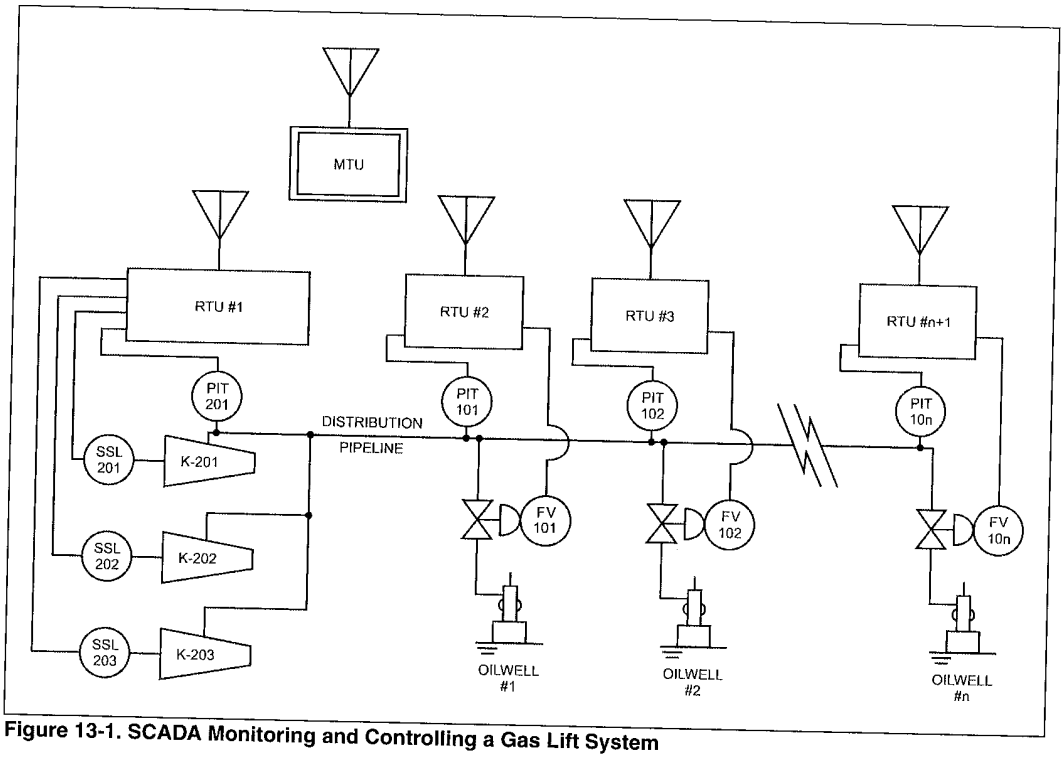


Figure 13-1. SCADA Monitoring and Controlling a Gas Lift System

The distribution system has enough capacity to maintain a working pressure for about 10 or 15 minutes before wells randomly stop producing. To maintain the highest possible production rate, specific wells will be shut in (turned off). The incentive for optimizing the selection of wells to be shut in can be great. It may be that the lowest productivity wells or the wells located closest to the operations center are shut in first.

In Figure 13-1, the MTU scans each RTU every five minutes. In the worst case, a compressor fails just after its RTU is scanned (see Figure 13-2). The RTU at the compressor site learns of the failure quickly, in about one second, but must wait until the next scan, which occurs five minutes later, to pass the data to the MTU. In less than one second after it learned of the compressor failure, the MTU has applied an algorithm to the data and has

WB_00001232

decided which wells should be shut in. It can now start sending instructions to selected wells to turn off, but at this scan rate it will be another five minutes before the last RTU (and well) has received its instructions.

Process calculations can be performed, or actual measurements taken, to determine if this response is fast enough. If necessary, such special provisions as scanning the compressor RTU two times in each regular scan may gain the couple of minutes of response that will make the difference between a workable and a non-workable system. Set up this way, the application would work within the constraints of scan times.

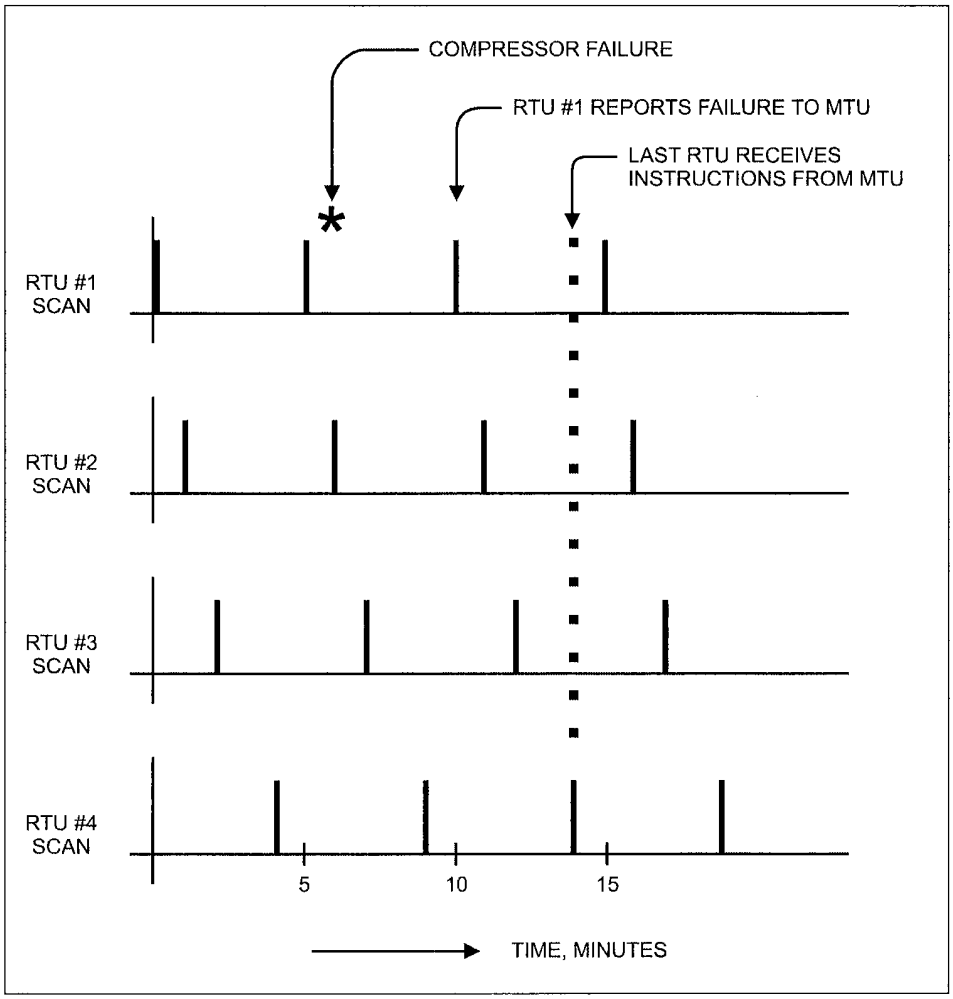


Figure 13-2. Compressor Fails after Its RTU Is Scanned

WB_00001233

On the other hand, an application for generating electricity and performing transmission load-shedding, which is closely analogous to the application just described, would almost certainly not work with the communications speeds described. Permissible scan times on the order of seconds would be required. Constraints like these determine system specifications. In fact, many SCADA systems used by electric utilities provide scan times of one to five seconds.

13-2. Accounting and Quality of Data

The custody transfer of a commodity requires the seller and buyer to mutually agree on several points. These points are usually listed in an agreement—a contract—between the two parties. One of the important points of a contract is the price that will be paid for each unit of the commodity. Another is the number of units that are to be transferred. When one of the parties, usually the buyer, is a member of the public or is otherwise considered to be potentially incapable of protecting itself in the exchange, a regulatory agency may become involved. As a result, we have residential electricity meters that have been calibrated under the authority of a regulatory agency and have been mechanically sealed to prevent tampering (see Figure 13-3). Gasoline pumps are calibrated and sealed in a similar fashion. On the other hand, the contract between two sophisticated parties will not be reviewed by the regulatory agency at all. Each of the two parties to the transaction will provide input to the contract, including details regarding the calibration methods and intervals, correction factors, security of data, and the like.

The transfer of ownership of many industrial commodities occurs at remote locations. Methane moving from a gas transmission pipeline to a city distribution system may be metered fifteen kilometers from the city. Irrigation water may be metered where the aqueduct crosses a state line. Electric power sold from one utility company to another may be metered at the boundary between the two utility jurisdictions.

Note the unit cost of the commodities is not an issue when SCADA is used for custody transfer.

Using SCADA to ascertain the number of units transferred does raise two questions, that is, the accuracy and the security of the measurement.

Accuracy is not always the greatest concern. Most measurements used in custody transfer start by gauging a simple parameter and then adjusting it by applying fixed and variable correction factors. For some measurements, there are few corrections, and their effects are not large. Other measurements require that 10 or more parameters be input to an algorithm to generate the custody transfer amount.

WB_00001234

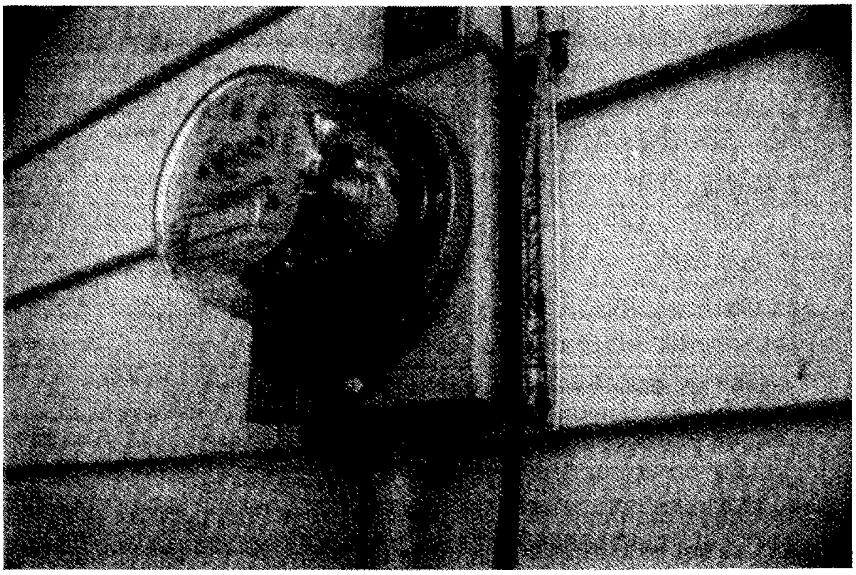


Figure 13-3. Mechanically Sealed Residential Electrical Meters

$$Q_v = F_b F_r Y F_{pb} F_{tb} F_{tf} F_{gr} F_{pv} (h_w P_{f1})^{0.5}$$

where:

F_b = a function of the orifice and meter tube diameter
F_r = a function of the fluid Reynolds number
Y = a function of the compressibility of the fluid
F_{pb} = a function of the legal contract base pressure
F_{tb} = a function of the legal contract base temperature
F_{tf} = a function of the actual fluid temperature
F_{gr} = a function of the fluid density
F_{pv} = a function of the compressibility of the fluid
h_w = the differential pressure across the orifice
P_{f1} = the static pressure at the orifice plate

Figure 13-4. Gas Volumes Measured by Measuring Pressure Drop across the Orifice

Figure 13-4 shows an example in which gas volumes are measured by measuring the pressure drop across the orifice (the static pressure and the temperature may also be measured). In addition, information about the size of the pipe and the orifice, the density and composition of the gas, and several other things may be included in the calculation. To achieve acceptable accuracy, all of these corrections must be made. If the algorithm to incorporate all the corrections is to be run at the measurement point, additional computing power will have to be

WB_00001235

purchased, installed, and maintained at each measurement point. It would make much better financial sense to share the computing power among several metering points and gather the totalized meter reading for each meter point. This is very often done, and, in fact, manufacturers of orifice meter totalizers usually offer a model that can provide this capability for three or more meter runs (see Figure 13-5).

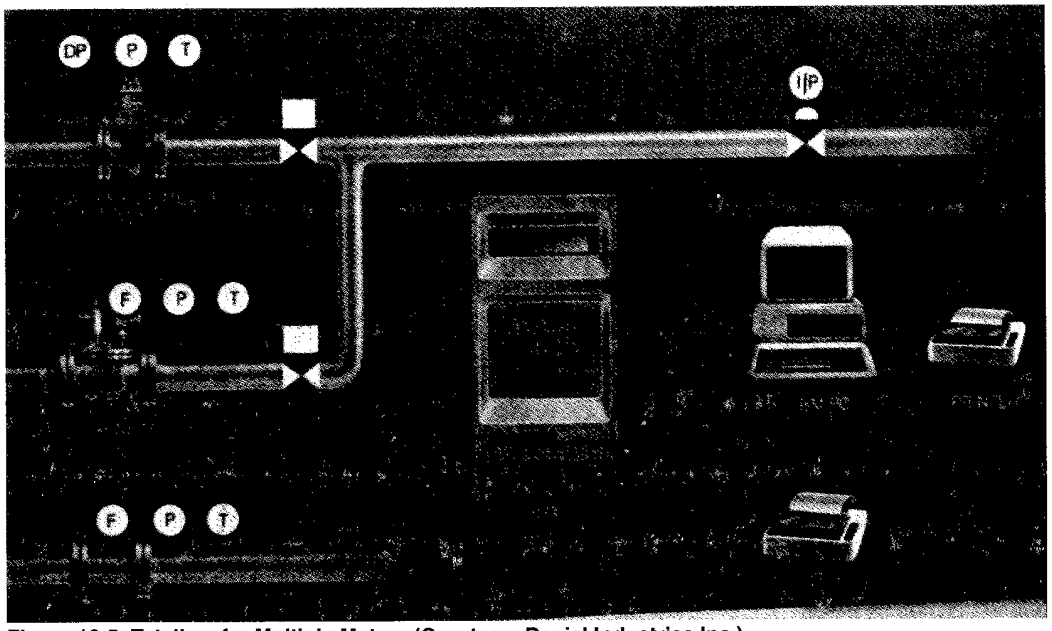


Figure 13-5. Totalizer for Multiple Meters (Courtesy: Daniel Industries Inc.)

The ultimate extension of this philosophy would be to bring the variable value, or values associated with each metered stream, all the way back to the MTU and do the computing there. In earlier systems where this was done, the computing load that was placed on the MTU was severe enough to degrade the overall system. Faster computers may have overcome this problem, but there is a more basic reason for not doing the calculations at the MTU: scan rates. Many of the basic measurement quantities must be integrated over time to arrive at a useful accounting value. In the case of the previous example of the orifice flowmeter, the basic variable measured is differential pressure, which is related to flow rate. To get to the accounting units, which are likely to be mass or volume, it is necessary to integrate flow rate readings over time. The more often the flow rates are read and integrated, the more accurate the flow rate measurement will be. Scan rates from MTUs are often too slow to produce an acceptable accuracy level. Measuring production rates with extra-fast-responding flow rate equipment has shown that oil well production rates can vary

WB_00001236

over as little as 2 or 3 milliseconds. This means MTUs will not be able to scan sufficiently quickly.

In addition, any failure of the communications system or of other equipment would further degrade the accuracy of the data.

If the MTU scan rate and the unreliability of the communications system preclude doing the computation in the MTU, how about doing it in the RTU? Although most SCADA systems use built-for-purpose flow totalizers, some systems do use the RTU to calculate accounting-grade information. Most modern RTUs offer the ability to program in one or more high-level computer languages, so the capability to do the calculations is there. The RTU does scan its inputs frequently enough for most measurement requirements and can handle the computation load associated with a few meter points. However, before using the RTU as a totalizer, you should take into account the maintenance of the meter totalizing function. Built-for-purpose totalizers usually make it easy for a qualified person to change algorithm variables through push-button control. The same changes to an RTU-based totalizer program are likely to be cumbersome and subject to errors.

Security is at least as important as accuracy when handling custody transfer information. The wire and lead seals used on mechanical meters are installed to show whether the meter was tampered with after it was officially calibrated. In some cases, this technique has carried over to the present. Meter totalizers are sometimes required to be enclosed in tamper-proof boxes, complete with wire and lead seals.

In most cases, a software security code known by only a restricted number of people must form part of the access procedure for changing totalizing algorithm variables. In some cases, a hard copy must be printed at stated time intervals to establish to the satisfaction of the accounting departments, what these variables were. Figure 13-6 is an example of such a hard copy printout. In many cases, the current totalized flow must be visually confirmable by an inspector at all times by providing a read-out visible to the inspector at any time.

Even with our current ability to move complex data electronically, the need for a "paper trail" is still with us. This does not mean, however, that the regular billing will wait for a manual confirmation. Most often, the billing is done on the basis of the electronically gathered data. Auditing is usually done on a non-periodic basis to confirm that the electronically generated billing information is correct.

WB_00001237

Meter Log Record

Date: 96.08.15

Tag Number: FT_702, PT_702, TT_702

Description: Dry gas to injection.

Physical Data:
Orifice Size: 101.60 mm Pipe Diameter: 202.4 mm

Base Conditions:
PB = 101.325 kPag TB = 15.00 C

Local Barometric Pressure = 100.00 kPa

Calibration:

FT_702	0-25.0 kPa
PT_702	0-689.5 kPag
TT_702	5-39.0 C

Operating Average: (24 hr)

FT_702	15.0 kPa
PT_702	450.0 kPag
TT_702	25.0 C

CPRIME: (24 hr average)

Fb	3369.42
Fr	1.0004
Y	1.0046
Fpb	1.0023
Ftf	0.9881
Fgr	1.0541
Fpv	1.0081
Fa	1.0000

Total Flow: (24 hr average)
FQI_702 = 166.617 km^3/d

Figure 13-6. Hard-Copy Printout (Courtesy of Crystal Engineering Ltd.)

13-3. Scanning and Communications

The applications concerned with scanning and communications are put in place to monitor and, in some cases, to modify or correct problems associated with these two functions. The scanning of the various RTUs by the MTU is itself an application. A relatively simple program defines the order in which the RTUs will be scanned. This order is usually adjustable or configurable by the SCADA system operator to optimize the operation of the process. Consider a system (see Figure 13-7) that includes a pipeline that carries incompressible fluids and has one meter point measuring fluid flow into the line and six meter points measuring fluid flow out of the line. The algorithm would be "Subtract all output meter readings from all input

WB_00001238

meter readings and alarm if the difference exceeds 5 percent of the sum of the inputs."

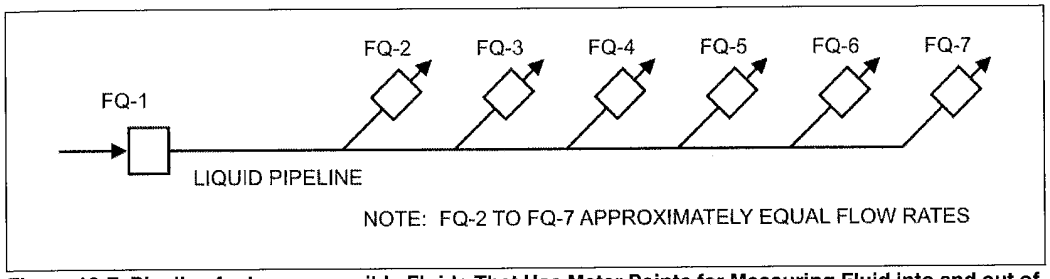


Figure 13-7. Pipeline for Incompressible Fluids That Has Meter Points for Measuring Fluid into and out of the Line

What is not stated in this algorithm is that the readings should all be taken simultaneously. In fact, if the scan period of this system was long and the meters were read at other than the optimal times, a systematic error would be introduced (see Figure 13-8). That error could be reduced, probably to the point of inconsequentiality, by arranging to read half of the outputs, then the input, then the other half of the outputs. A slightly different and more effective strategy, shown in Figure 13-9, would be to scan those RTUs that contributed one half of the pipeline output followed by the RTU that provided the pipeline input, followed in turn by the RTUs that provided the other half of the pipeline output. The scanning application would have to be modified if additional pipeline outputs were added after the system was initially built.

Different types of scans may be needed depending on the process situation. When everything is normal, the best scan is likely to be one that interrogates and provides instructions to an RTU and then waits for a response before moving to the next RTU. In an upset condition where it is very important that the *correct* control actions occur, the best scan would be one that involves having each RTU confirm that it received the correct message before the RTU acts on the message. In an upset situation where the *speed* of the control response becomes more important, a more effective scan may be one that sends out a single instruction to each RTU in rapid succession without waiting for a response.

A communications-related application is frequently used to keep track of failures to communicate and to alert the operator, either by a daily report or by an audible or visible alarm, when the ratio of unsuccessful communication attempts to successful ones exceeds some value. That value is selectable by the operator. As we learned earlier, a message put together by an MTU will include the identification of the RTU to which it is sent as well as a message and an error-detection code. For most classes of message, the RTU is expected to respond to the MTU by indicating that

WB_00001239

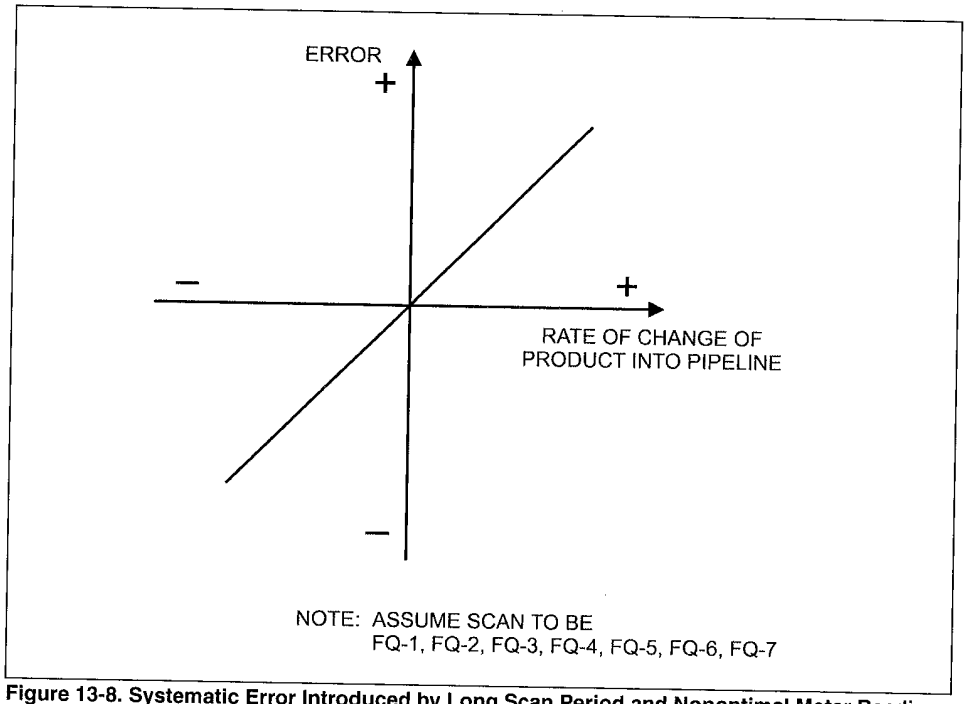


Figure 13-8. Systematic Error Introduced by Long Scan Period and Nonoptimal Meter Reading Times

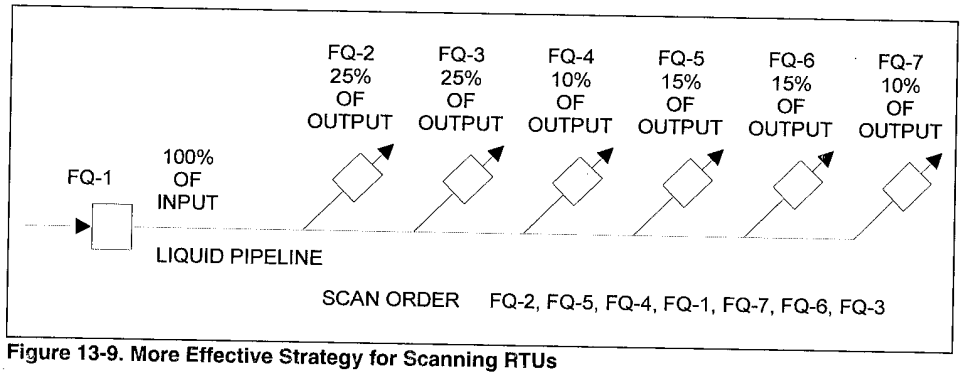


Figure 13-9. More Effective Strategy for Scanning RTUs

it received the message. If the MTU does not receive this response, it will consider this communication attempt to be a failure. It will add one failure to the total number of failures for the RTU, and it will resend the message. After a preselectable number of consecutive failures to one RTU, it will move on to the next RTU in the scan sequence. Usually, the simple failure of one random message will do nothing except appear on a daily communications failure report. The failure of three or four consecutive communication attempts to an RTU will probably trip an alarm to the system operator that maintenance is required on that communications circuit.

WB_00001240

In the absence of such an alarm, an inspection of the daily communication report can often point to circuits that are becoming marginal. Responding to the information in these reports allows many problems to be corrected before they cause lost production or increased operating cost.

A second communications-related application can keep track of the total amount of time per day that the MTU and each RTU spent transmitting. This information would be included in the daily communication report. A comparison of current information to historical averages for each of these units may point to future trouble spots. An evaluation of the absolute values of these data is useful if additions or other changes to the system size are being considered.

A third communications application is called "anti-streaming." It is similar to a watchdog timer. At each transmitter location, the application monitors the length of time that a transmitter is keyed on. If the transmitter stays on longer than required, the anti-streaming application turns it off, usually by removing power to the transmitter. Automatic or manual recovery methods may be used to return it to normal.

13-4. Automatic or Remote Control

Automatic control happens when a system senses that a process variable has changed and modifies a control parameter without bringing a human operator into the decision. An example in an electric power transmission system is the automatic arming of a local load-shedding device to protect a transmission line from overloading only under very specific conditions that could be detected by the SCADA system. Examples of these conditions could include very high ambient temperature combined with high current flow in the line. These combined factors will result in a high temperature in the transmission line, stretching the line to the extent that it may short out to ground. Similar combinations of wind and high current may result in excessive swinging of the line, leading to phase-to-phase (wire-to-wire) shorting.

Some hydroelectric generating companies will monitor the areas surrounding their dammed lakes to check for rainfall. Large amounts of rainfall can be expected to raise the lake levels, and such companies will know how much rainfall their facilities can stand. It is sometimes necessary to partially drain the lake before the surge of new rainwater gets close to the design limits of the dam. This function may be done automatically or manually following a SCADA generated alarm.

Remote control occurs when a decision to modify a control parameter is effected at a significant distance from the process. The operative words in the concepts "automatic" and "remote control" are *human* and *distance*,

WB_00001241

respectively. An automatic control responds with no direct human involvement. A remote control responds from a distance.

Very often, people confuse the terms in the mistaken belief that because SCADA is associated with so much computer hardware, it must be automatic. In fact, most early SCADA systems and a large minority of present ones are not automatic at all. They are very efficient remote control and remote data-gathering systems. Intervention in the form of human decisions is usually required before the data that is gathered can be translated into a control action.

Processes that are spread over dozens or hundreds of square kilometers, but are not technically complex and may be automatically controlled without an increase in risk to the process or to personnel are better candidates for automatic control applications. In the pipeline industry, for example, simple volume-balance leak detection has the potential to automatically block the line and shut down the pumps and/or compressors. Early attempts to use this automatic control were often frustrated, however, by unnecessary shut-ins, with the result that most systems reverted to alarming in the control room so a human being could make the decision. The operator's decision to shut in the pipeline would be executed by remote control. The factors that caused the false alarms were later addressed by better communications and algorithms, and the tide has begun to turn back toward automatic control for these functions.

Starting pumps or compressors in response to sensed or anticipated demands is another potential automatic control application. This also is not a very common application. Many more pump or compressor stations are controlled by local loops and/or by the remote control of human operators than by MTU automatic control. The two analogous processes in electric power transmission also qualify for automatic control through the MTU. Operating switches through the MTU in response to the situation on the entire network has become more common as network complexity increases. Small electric power generators, for example hydro stations or wind turbines, are frequently started or stopped in response to loads. Few other applications lend themselves to true automatic control through the MTU.

13-5. Advisory Applications

If SCADA systems are not often used for automatic control, what kind of control are they used for? As we have seen, almost all control applications in SCADA systems bring the operator into the loop. They do this by gathering data, sometimes in very large amounts, from many locations over a wide geographical area, integrating it, and making it digestible by the operator. They then present it as advice. These advisory applications

WB_00001242

recognize that the operator has a better knowledge of the myriad factors that affect the operation, factors that the MTU simply does not know.

Many pipeline leak detection applications, for example, have the MTU warn the operator that there is probably a leak. If the operator knows that the meters are being calibrated that day, he or she may not make the decision to shut in the line. Increased demands on an electric transmission line may cause the MTU to advise that a particular generating facility be started up. If the operator knows that the facility is undergoing maintenance and is not available, he or she will choose another solution. For reasons such as these, for most control applications the SCADA system is used as an advisory tool rather than as an automatic control tool.

Unit 13 Exercises:

13-1. *Some applications of SCADA require much design and implementation effort to increase the MTU's scanning speed. Why is this important?*

13-2. *Why can it take as much as two scan periods for a field problem to be resolved if the MTU is in the decision path? What can be done to shorten this?*

13-3. *Accounting policies and government regulations sometimes prevent using electronically gathered data, which are not really in the paper trail, from being the basis for billing. What can be done to minimize billing delays?*

13-4. *Two factors determine the total price of a transferred commodity. What are they?*

13-5. *Establishing the number of units of a commodity involves two important issues. What are they?*

13-6. *What broad characteristics make an application attractive to a SCADA solution? One of them is distance; what are the other two?*

13-7. *Applications exist to monitor the communication system. Why would someone want to know the communications system failure rates on a SCADA system?*

WB_00001243

Unit 14: What's Next?

Unit 14

What's Next?

As we have seen, SCADA systems consist of three functional components: communications equipment, remote terminal units (RTUs), and master terminal units (MTUs). It is reasonable to ask what changes we may expect these components to undergo in the near future. Some of the advances identified in this unit are in fact already available as this book goes to press, but we will discuss them in the context of their future potential.

Not surprisingly, communications is the area that is likely to have the largest impact on SCADA in the future. Communications is the glue that holds SCADA together. Changes in communications methods will be seen in the future.

Shifting away from the present drive to integrate SCADA with enterprise systems and with the Internet has enough apparent benefits that we can expect to increasingly see such isolation in future systems.

Increases in the sophistication of MTU based programming will result in more purely automatic, as opposed to manual, remote control applications being built into SCADA.

Learning Objectives—When you have completed this unit, you should:

A. Know how advances in communications technology and security are likely to affect the future of SCADA.

B. Appreciate that advances in reliability and risk management will result in SCADA systems better able to automatically control large processes.

14-1. Communications Technology—Field Data

At the field level, data must be gathered from sensors that measure process variables and data must be moved from the remote terminal units to process actuators. This data has historically been moved, first using pneumatic media, then using analog signals on electric media, then using digital signals on electric media. We are starting to see, and can expect to see more of, digital signals moving on radio communication media.

From its early use, wireless data gathering and actuator commands promised major cost reductions because without the necessity for wire to connect the sensors and actuators to the remote terminal unit, it would be cheaper to install wireless sensors and actuators. It was early recognized

WB_00001245

that interference from other electrical equipment nearby could degrade the data signals. Countermeasures such as multiple transmissions, frequency shifting, and increasing transmitter power were generally successful in beating this "natural" interference.

Security could be difficult against a well-planned cyber attack if all the sensors and actuators were connected to the control system by radio. Certainly encryption techniques are now available that will keep the data secret, but if the purpose of the cyber attack is to disrupt facility control, flooding the RTU sites with a strong radio frequency blanket could be an effective tool. To counter such an attack, "spread-spectrum" techniques have been applied to encrypt the transmission and to confound attempts to interfere with legitimate transmissions. Spread-spectrum communications as a concept has been in existence since the late 1930s, when as the wife of an Austrian arms dealer, the woman who was later to become known as Hedy Lamarr developed the concept of a method of radio control for torpedoes that would not alert the enemy that the communication to steer the torpedo was even taking place. This stealthy communication would also have the advantage of preventing the enemy from jamming the signal or taking over control of the torpedo. This type of spread-spectrum communication is known as "frequency hopping spread spectrum" (FHSS), and works this way: The carrier frequency is shifted in a pseudo-random way. The intended receiver changes its frequency in exactly the same way, using the same code. No one without the code can adjust his or her receiver quickly enough to monitor the transmission. In fact, most receivers will be unable to determine that a transmission is even occurring. Implementation of the concept took until about the early 1960s. It is the basis for the Bluetooth wireless protocol and has been used to connect instruments to RTUs and RTUs to MTUs in SCADA systems.

The second type of spread-spectrum communication is known as "direct sequence spread spectrum" (DSSS). Its basis goes back to Bell Labs researcher Claude Shannon, who proposed in about 1949 adding a pseudo-random sequence of ones and zeros to the digital message. He also determined that by widening the bandwidth, the data rate could be increased for a constant signal-to-noise ratio. This has the effect of making the message resemble random noise to any receiver that cannot subtract the proper sequence of ones and zeros from the message. As long as the signal-to-noise ratio is acceptably high, it is possible to have multiple messages simultaneously being transmitted within the spread spectrum. About 40 years later, Irwin Jacobs of Qualcomm was able to realize the concept in hardware. His code division multiple access (CDMA) uses extremely complex electronics to allow time synchronization between cell stations and hand sets and to arrange that transmitter output be varied so that signal level at the receiver is the same for all hand sets—irrespective of their distance from the base.

WB_00001246

Spread spectrum has at least two advantages over other radio communication methods. First, security, in terms of the difficulty of intercepting or interfering with the message, is attractive when the SCADA system is being used in a process that could be a strategic or commercial target. Present SCADA systems are almost never cyber-encrypted. We can expect that many, perhaps most, future SCADA systems will have this feature.

The second advantage is related to the fact that since the message is encrypted, a lower power transmitter can be used to successfully move the message between two points. This often means that the power output of the transmitter can be low enough that no radio license is required. In areas of dense radio coverage, this can make the difference between being able to use a radio transmitter and not being able to use one. These two advantages can be expected to mean that spread-spectrum radio communication will be used for SCADA much more in the future than it is now.

14-2. Communications Technology—RTU/MTU

The shift away from Master-Slave communication to Report by Exception (Peer to Peer) has been made possible because so much attention has been paid to improving both the communication equipment and the protocols. This Report by Exception technique has changed the way that RTUs and MTUs communicate. The change is ongoing and will result in most new systems being designed as Peer to Peer.

The use of cell phone signals (packet data communication) as the communication medium for SCADA systems has been generally successful. Squeezing the small amount of data needed for a SCADA operation into the spaces between sentences in a voice conversation can be done for a very low cost if the infrastructure is in place near the operation. As cell phone users demand better coverage, this infrastructure is being built, and SCADA users are benefiting. Where it is unlikely that the telephone utility will build towers for conventional cell phone business, they may build for packet data communication if the SCADA system owner is prepared to share in the capital cost of the towers.

14-3. Reductions in SCADA/Enterprise Communications

It is possible to build secure communications systems to allow SCADA and other corporate networks to communicate with each other safely. There are financial incentives to do this, since automatic data transfer should cost less than manually initiated data transfer. However, in the same way as you and I spend money each month to feel better about our

WB_00001247

chances of avoiding a computer virus, it costs money to maintain a secure link between a SCADA system and another system.

Large companies that have information technology specialists may have the resources in both money and trained manpower to support the constantly changing needs of such a link. Most small companies do not have enough of either resource to safely do this. They will become targets, and even though the reports of their failures to maintain security will be hidden, the reports will eventually get out, perhaps encouraging further attacks. Most SCADA systems do not have a real need to be tied directly to another system. The amount of data that must be moved from one to another is small and can be moved using something other than a direct wire connection.

The danger of a cyber attack is particularly high for SCADA systems that have a connection to the Internet. As has been mentioned, because the Internet is essentially infinite in size, the number of potential attackers is very large. The cost of protecting a system against a group of potential attackers increases as the size of the group increases.

Because the costs often outweigh the benefits, in the future, more SCADA systems will be designed to be isolated from other networks.

14-4. More Fully Automatic Applications

Despite my comments in the last section, cyber security techniques have improved the security of SCADA systems in the last decade. The quality of process instrumentation has improved. The cost of such instrumentation, while it has not gone down, has not increased unreasonably. The cost of computer hardware has dropped very noticeably. The effects of all these factors can result in SCADA systems that have more reliable data about the process. Application software has been written to take advantage of this better data. As a result, more and more applications can now be built to be completely automatic, rather than advisory/manual. As experience with this approach indicates which of these applications have less risk and which have more, we should expect to see more automatic applications built as part of many SCADA systems.

Unit 14 Exercises:

14-1. What improvements in radio communication are likely to affect SCADA the most?

14-2. What two methods of spread-spectrum encryption assure that messages cannot be intercepted?

WB_00001248

14-3. *Concern about connecting a SCADA system to another kind of network is based on what?*

14-4. *Name three factors that are increasing the popularity of fully automatic SCADA applications.*

14-5. *What factor contributes to low power requirements in spread-spectrum radios so that they do not require licenses?*

14-6. *Why can the cost of moving data be as low for packet data as used for SCADA communication on cell phone networks?*

WB_00001249

Unit 15: SCADA Economics

The Integration Group of The Americas Ex. 1007-Page 197
SitePro, Inc. v. WaterBridge Resources, LLC, et al.

WB_00001250

Unit 15

SCADA Economics

Several times in this book, we have referred to some aspect of economics. In this unit, we will concentrate on the basic economic and business factors that you should consider when evaluating whether a process can benefit from SCADA. This discussion is about economic principles rather than numbers. The costs of installation, technical support, and maintenance will vary from area to area. To do an actual economic evaluation, you will have to gather local numbers for these costs and benefits.

Learning Objectives—When you have finished this unit, you should:

A. Appreciate the methods used to quantify costs and benefits.

B. Understand the qualitative factors that must be considered to answer the question, "Should we install SCADA on this process?"

15-1. Costs versus Benefits

Reaching economic decisions may appear to be a simple process. Add all the benefits, subtract all the costs, and if the result is positive, do it! In the real world, however, decisions are seldom so straightforward. The design of a SCADA system is an iterative process. Each incremental increase in system benefit (capability) creates a corresponding but nonlinear increase in cost.

If the corporation that will own the system has no existing SCADA infrastructure on which to build, the cost to get started will be high. The MTU is a large part of the cost of the system. If communication links cannot be leased, they are also high-cost items. All of the parts of the system must be supplied before any benefits can accrue.

The commitment and cost to a company to develop in-house expertise can also be high. The large potential costs of one or two bad decisions made during the early stages of system development can exacerbate this cost. Experts in SCADA technology are available to act as consultants, but to ensure success for your job such consultants must be knowledgeable about the factors that are unique to your company and your industry.

The benefits identified first tend naturally to be the more valuable. For example, it may be that the cost of an all-weather road to a station can be deferred if remote monitoring and control is provided. Perhaps an

WB_00001251

operating license will be contingent on the inclusion of remote shut-in capability, in which case the capital project could not be built without SCADA.

15-2. The Time Value of Money

Often, our first way of thinking about costs and benefits has them all happening at the same time. This is an easy way to think about it, but it can lead to the wrong answers. The story is told of the island of Manhattan being bought from the Manhattan Indians for trade goods worth about $24. Most people who hear the story feel that the purchasers got the better of the locals, and even robbed them. It may be interesting to do a quick time-value analysis.

Example 15-1. Assume that the purchase of Manhattan took place in 1626; the $24 was invested at 7.2 percent, compounded; and the investors paid no tax on their interest. There is a rule that says that an amount of money will double when the product of interest rate and the time in years that the money is invested equals 72. It is called, logically, "the rule of 72." At 7.2 percent, the investment would double every ten years (7.2 x 10 = 72).

In 1626 the investment is worth $24.

In 1636 the investment is worth $48.

In 1646 the investment is worth $96.

In 1656 the investment is worth $192.

The general formula for calculating present value of money invested in the past is

$$\text{Present Value (PV)} = \text{Principal} \times (1+\text{interest})^{(\text{Now} - \text{Investment Year})}$$

In 1656, the PV = $24x $(1.072)^{1656-1626}$ = $193.22

In 1726, the PV = $24x $(1.072)^{(1726-1626)}$ = $25,100.92

In 1826, the PV = $24x $(1.072)^{(1826-1626)}$ = $26,252,357.00

In 1926, the PV = $24x $(1.072)^{(1926-1626)}$ = $27,456,000,000.00

In 2009, the PV = $24x $(1.072)^{(2009-1626)}$ = $9,000,000,000,000.00

Perhaps the deal was not so unfair after all. What we have calculated here is the present value of the investment at 7.2 percent interest, which is sometimes written PV7.2.

WB_00001252

When doing economic calculations, you should use the interest rates that are available to your company for investing its money. You should use a selection of these values to check whether an investment decision is sensitive to various rates. If your company could get 10 percent interest on an investment, you would calculate PV10, but you should also check PV7 and PV13 to see how sensitive your project is to a 3 percent change in the interest rate.

In the same way that you can calculate the present value of an investment made in the past, you can determine the present value of a cost that must be paid out in the future.

Example 15-2. As part of our proposed SCADA system, we know we will have to pay $200,000 to plow optical fiber cable to three RTU sites. This payment will have to be made two years from now. We can get 10 percent interest for our money. (Ignore tax.) What is the present value cost of the optical fiber cable installation? (Hint: The present value of a future cost can be thought of as the amount of money that must be invested now in order to yield the cost in the future.)

We will use the common interest formula, $A = P \times (1+i)^t$, where

A = Accumulated amount

P = Principal

i = Interest rate/unit time (in decimal form)

t = Time (in number of units)

We know that the accumulated amount is $200,000, the interest rate is 0.10 per year, and the time is two years. Transpose the equation to yield the following:

$$P = A / (1+i)^t$$

$$P = \$200{,}000 / (1+0.10)^2$$

$$P = \$165{,}000$$

This is the amount of money that we have to put into the budget now at 10 percent interest in order to have $200,000 at the time we need it to plow in the cable.

The present value of a benefit that will be gained by having a SCADA system can be calculated in a similar manner.

WB_00001253

Example 15-3. The operations engineer for an electric power company estimates that the improved utilization of facilities made possible by a SCADA system will make it unnecessary to buy $300,000 worth of electric power every year from a neighboring power grid. The deferral of this power purchase will be possible for eight years from now. The interest rate is 12 percent per year. (Ignore tax.) It will take two years to build the SCADA system. What is the PV12 of this benefit?

For Year 1, SCADA system is not built. No benefit.

For Year 2, SCADA system is not built. No benefit.

For Year 3, $300,000 benefit, averaged halfway through the year.

$$PV = A / (1+i)^t$$

$$PV = \$300{,}000 / (1.12)^{2.5}$$

$$PV = \$225{,}983.$$

For Year 4, $\$300{,}000 / (1.12)^{3.5}$

$$PV = \$201{,}771$$

For Year 5, PV = $180,152

For Year 6, PV = $160, 850

For Year 7, PV = $143, 616

For Year 8, PV = $128, 229

The total PV12 is the sum of all of these annual amounts: PV12 = $1,040,601

In the same way that the value of benefits received in the future must be discounted by a number related to interest, the future value of some of these values must be increased by a number related to inflation. Labor rates, for example, can be projected to rise over time in some more or less predictable manner. The cost of a commodity can be projected to increase or decrease in response to demographic demand, natural supply, and several other factors. The SCADA designer is not usually expected to originate these numbers, but he or she should be aware that they will have an effect on the economic decisions.

15-3. Capital Costs

Capital costs are the first ones considered when the word "costs" is mentioned. Indeed, they are usually significant and are usually easy to quantify. These costs normally include engineering and installation labor, the services of technical specialists, warehousing, and transportation, in

WB_00001254

addition to the costs for the hardware devices that are conventionally thought of when the term costs is used.

Table 15-1 is a list of those items that may be included as capital items for a SCADA project.

Location	Capital Items
Central	Design/construction engineering Master terminal unit (MTU) Control room c/w heat, light, air conditioning, and ventilation Security (programmable door locks) Furniture Uninterruptible power supply (UPS) Communications equipment (may include radios, modems, antennae, and towers)
Remote	Design/construction engineering Remote terminal units (RTUs) Marshaling/termination panels Uninterruptible power supplies (UPSs) Communications equipment (may include radios, modems, antennae, and towers) Special sensors and actuators Purchase land for RTUs and repeater stations Interconnection of RTU to sensors and actuators Building in which to house RTU/UPS/communications equipment Light, heat, air conditioning, ventilation
Between Central and Remote	May include capital contribution to utility for leased communications lines May include radio repeater stations (if owned radio) May include purchase and installation costs (if owned copper or optical fiber cable)

Table 15-1. Capital Items

Some items are closely related to these but quantify as "capital-related expense items." The things that might qualify include the removal of existing equipment to make room for new equipment, certain refurbishments of existing buildings or equipment, and custom-designed computer software. Different jurisdictions allow placing different things into the expense category. Check your local laws before you get too creative.

WB_00001255

15-4. Training and Maintenance Costs

For some reason, training and maintenance costs are frequently neglected during the economic evaluation. It is true that training costs are not very high, but they do exist. The failure to include training in the planning stage will likely lead to a failure to schedule operators' and technicians' time for that training. To have an existing group of operators provide the manpower to configure the system, you must address the issue of training for them and any related adjustments to their schedules very early in the project. The costs for the instructor and the training aids should be negotiated before the system is selected. The costs for the time lost while operators learn the system are real and should be included in the cost-benefit analysis.

Maintenance technicians will have to be trained in the equipment that they will become responsible for because it will be unfamiliar to them. Their maintenance duties will begin later than the configuration duties of the operators. For this reason, their training may be deferred. On the other hand, if the maintenance technicians will be actively involved in the installation, their training may be scheduled earlier. It will be most effective if it is provided just before it is to be applied.

The best location for the training courses will depend on the number of people who must be trained and the cost of travel to the facility. Regularly scheduled, in-house courses may work best if only a few people are to be trained. Having one instructor travel to the site will be more cost-effective than having ten workers travel to another site. Offsetting the travel costs, however, is the value of such intangibles as having your people meet valuable sources of technical information such as the manufacturers' technical specialists or the status that goes with a factory trip. Moreover, the trainees' learning effectiveness will be reduced if they are interrupted by operations problems, as they may be if the training occurs at their normal work location.

Maintenance costs are high enough that they should be included in the economic evaluation. It is not the MTU and RTUs that are responsible for most of these costs, although they and the communications equipment will provide their share at the beginning. Over the life of the SCADA system, most of the maintenance costs will be for the calibration, repair, and replacement of mundane items such as flow-measuring equipment, limit switches, analyzers, and actuators. The wire terminations that join all these components into one system are also a major source of maintenance cost. Each of the process variables that, in a manually operated facility, could be monitored by eye or by a simple sensor will have to be monitored by a more complex sensor. Each remotely operated valve requires an actuator. All these devices that have moving parts will wear out or break.

The Integration Group of The Americas Ex. 1007-Page 203

WB_00001256

The point is that because there are so many of them, the maintenance load will be significant. Software upgrades will also contribute to maintenance costs.

As we have seen, properly designed and manufactured electronic equipment that has no moving parts can be expected to suffer high "infant mortality;" that is, it will fail near the beginning of its life and then, after repair, settle down to be a low-maintenance item. This is the reason that most industrial electronic equipment is delivered only after an extended "burn in" period. Early failures are more easily accepted if they happen at the factory and statistically, a factory burn in will push many of the failures into the factory. With proper attention to voltage transients and over-temperature protection, RTU equipment can last more than thirty years. However, improvements in technology may make it advantageous for an RTU to be replaced before it stops working.

Anticipating this infant mortality, you may plan to have most of the maintenance base load handled by company technicians and the initial extra load handled by people contracted specifically for that purpose. Warranties may meet both these needs. You may also want to contract some (or all) of the specialty work, such as radio or optical fiber system maintenance. These costs should be included in the economic calculations for the project.

15-5. SCADA Operating Costs

Besides system maintenance costs, the size of your operating costs will vary with the size of the system. For all but the largest systems, energy costs and consumables in the form of report paper and backup media are negligible. The cost of manpower in the form of operating staff may be the largest non-maintenance cost. The size of this operating staff will depend on the system's size and complexity as well as its operating philosophy. Some simple irrigation systems may operate essentially unmanned, with only one operator checking in once or twice during a single eight-hour shift. Large systems in electric utility transmission or generating service may require six or more operators per shift with two or three shifts per day.

For systems that use leased telecommunications services, the cost of such leasing must be factored into the economics during the economic planning phase. These costs may represent the largest operating cost.

15-6. Benefits: Reduced Capital Costs

Finally, after discussing all of the increased costs that are attributable to the SCADA system, we now consider some of the benefits. One potential

WB_00001257

benefit of SCADA that should be evaluated is the reduction in capital costs of the entire facility, including process and SCADA, which SCADA makes possible. Opportunities to capture these reduced capital costs should be vigorously pursued. For many processes, they will simply not exist. For others, the value of these reduced capital costs can easily offset the entire capital cost of the SCADA system. The process of identifying opportunities for capital cost reduction should be performed by a multi-disciplinary team that includes operations, maintenance, and construction people.

Table 15-2 lists some examples of cost reduction projects with the order-of-magnitude capital cost savings they make possible.

Industry	Item	Dollar Savings
Offshore	Eliminate living quarters on platform.	$10,000,000
Irrigation	Eliminate all-weather road to metering site.	$1,000,000
Electric transmission	Eliminate all-weather road to switching site.	$1,000,000
Gas pipeline	Eliminate living quarters at compressor station.	$2,000,000

Table 15-2. Capital Cost Savings

15-7. Benefits: Reduced Operating Costs

This category includes the largest number of items. Most are of small value relative to the capital costs we reviewed just now. When added up, however, they often provide sufficient incentive to justify the installation of SCADA. A multi-disciplinary team with a strong background in operations will be the most effective at identifying and quantifying them.

The time spent by operations people, either traveling to or from a site or spent ineffectively on site, represents a large amount of value. The benefits SCADA offers in reducing this time cost will be enjoyed most by widely scattered locations that have only a few process measurements and/or controls at each site. That is why SCADA has made such inroads in this type of facility. But, besides savings in salaries, the operations team specialists will also identify other related benefits from SCADA. It may reduce the capital and maintenance costs of vehicles, overtime paid for off-shift call-outs, road maintenance costs, and a host of other things that may apply only to the industry or facility being evaluated.

WB_00001258

A properly instrumented facility with SCADA capabilities can have its protective systems set to shut down equipment earlier than would a non-SCADA facility. It can do this because Operations knows that the shutdown will be recognized quickly by the SCADA system, the maintenance people can be immediately sent out to the facility, and there will be less downtime as a result. The benefits of this are two-fold: the facility may be safer and more environmentally benign, and long-term machine maintenance costs will probably be lower with faster shut-downs. In addition, the record keeping on machine failures and maintenance costs can be more effective on SCADA equipped processes, leading to reduced preventive maintenance expenses.

15-8. Benefits: Improved Facility Effectiveness

Large amounts of capital are spent on facilities that depend on SCADA. Hydroelectric or wind-powered generating stations, offshore oil platforms, and gas compression stations all have capital costs in the millions or hundreds of millions of dollars. This money has been spent with the understanding that SCADA will provide a return while it is operating. Maximizing the amount of time that a facility runs is one of the largest benefits a SCADA system can provide.

An oil well in an onshore field may be visited once a day. If it stops producing five minutes after the operator leaves, it may be twenty-four hours before the failure is discovered. A compressor station's failure could be inferred by a reduced pressure or throughput at the next manned site, but it may be a long time before these values deteriorate enough to be noticeable. The continuous monitoring available through SCADA can identify such failures immediately, thus making it possible to minimize their impact.

These are the modes of facility effectiveness that SCADA systems can address. Working together, operations, maintenance, and design engineering teams will find many more. Quantifying them and then converting the benefits into present value form will make it possible to bring them into the economic equation.

15-9. Tax Implications

For most of the examples noted in this unit, we ignored taxes when we did the calculations. One of the reasons for this was that it simplifies the calculations. The other is that methods for calculating taxes vary from one country to another and from one industry to another within each country.

When you do the calculations for a real project, however, you cannot ignore the role of taxes in the economics of a decision. Because it is such a

WB_00001259

broad field (and because it has very little to do with SCADA), we will not discuss taxes beyond this statement: Ensure that each benefit and each cost in the economic evaluation has had the appropriate tax treatment applied to it. To do this, you will need the services of a person who is a specialist in the local tax rules for the industry in question. Many operating companies develop and maintain comprehensive economic models into which the costs and benefits can be fed in order to determine after-tax credits. This makes it easy to do quick, first pass tests of potential SCADA projects without a great deal of effort.

Unit 15 Exercises:

15-1. *What two basic factors make up the economic equation?*

15-2. *Why should the time value of money be a significant factor?*

15-3. *Why is a taxation specialist needed for SCADA economics?*

15-4. *What is meant by the present value of a cost to do something in the future?*

15-5. *The benefits associated with reduced project capital cost should be taken into account early. Why?*

15-6. *What group of people will be best able to identify potential operating savings?*

15-7. *In addition to direct costs for training, what other aspect of training is important?*

15-8. *How can SCADA improve facility effectiveness?*

WB_00001260

Appendix A: Suggested Readings and Study Materials

APPENDIX A

Suggested Readings and Study Materials

Process Instrumentation

Lipták, Béla (ed.) *Instrument Engineers' Handbook: Process Measurement and Analysis, Fourth Edition, Vol. 1.* New York: CRC Press, 2003.

Whitt, Michael *Successful Instrumentation and Control Systems Design.* Research Triangle Park: International Society of Automation (ISA), 2004.

Communication

Clarke, Gordon and Reynders, Deon *Practical Modern SCADA Protocols.* Oxford: Elsevier Press, 2004.

Strock, O. J. *Introduction to Telemetry.* Research Triangle Park: International Society of Automation (ISA), 1987.

Thompson, Larry *Industrial Data Communications, Fourth Edition.* Research Triangle Park: International Society of Automation (ISA), 2007.

Cyber Security

Schneier, Bruce *Applied Cryptography, Second Edition.* New York: John Wiley and Sons, 1996.

ANSI/ISA-99.-02.-01 – 2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. American National Standards Institute (ANSI) / International Society of Automation (ISA), 2009.

The Integration Group of The Americas Ex. 1007-Page 209

WB_00001262

Appendix B: Glossary of SCADA Terminology

The Integration Group of The Americas Ex. 1007-Page 210
SitePro, Inc. v. WaterBridge Resources, LLC, et al.
WB_00001263

Appendix B

Glossary of SCADA Terminology

The definitions presented in this appendix are taken from four sources. The first is ISA's Standard on Process Instrumentation Terminology, ANSI/ISA-51.1-1979 (R1993). This ISA standard contains many terms beyond the field of process instrumentation, as well as many notes and amplifying figures that illuminate the terminology. The serious student of process control should have a copy of this standard for routine reference. The terms in this glossary that are defined based on the ISA standard are followed by a "T".

Other terms have been defined using ISA's *Automation, Systems, and Instrumentation Dictionary, 4th Edition* (2003). This reference guide contains definitions of more than eleven thousand terms and abbreviations and is the only comprehensive dictionary of measurement and control terms. The words that are defined here based on this document are followed by a "D".

Some terms have been defined using the *Compact Oxford English Dictionary*. These terms are identified by an "O".

The last group of terms have been defined based on their context within this book or based on definitions from *Webster's Dictionary, Third Edition.* These terms are identified by a "W".

actuator (D) – A fluid powered or electric powered device that supplies force and motion to a valve closure member.

A/D Converter (W) – Also **ADC** – a device which converts continuous signals to discrete digital signals.

advisory (W) – A software application that advises a human operator to make changes to the setting of a process controller

algorithm (D) – (1) A prescribed set of well-defined rules or processes for solving a mathematical problem in a finite number of steps. (2) An equation that will provide a solution to a regularly occurring process problem.

aliasing (D) – A particular problem in data sampling where the data is not sampled enough times per cycle, and the sampled data cannot be reconstructed to adequately represent the process.

AM – Amplitude Modulation, a method of imposing information on a carrier waveform by changing the carrier's amplitude.

WB_00001264

analog (T) – Referring to a variable which may be continuously observed and controlled.

asynchronous (W) – An asynchronous signal does not require a clock signal; a synchronous signal sends a clock signal (or the means for making a clock signal) from the transmitter to the receiver.

baud (D) – A unit of signaling speed that is equal to the number of code elements per second.

binary (W) – A numeral system that represents numerical values using combinations of two symbols, normally "0" and "1".

bit (W) – A Binary digIT taking the value of either "0" or "1". It is the basic unit of electronic information storage.

bps (W) – Bits per second; bit transmission rate in digital communication.

carrier wave (W) – A (usually) sinusoidal waveform that can be modulated with an input signal to carry information.

CCITT (T) – Consultative Committee on International Telephony and Telegraphy.

CPU – Central Processing Unit

CRC – Cyclic Redundancy Check

CRT – Cathode Ray Tube; now largely replaced in SCADA applications by LCDs.

cyber security (W) – The technology of protecting computers and their communication from unwanted intrusion.

D/A Converter (W) – Also **DAC** – A device for converting a digital signal to an analog signal.

decimal (W)– A positional decimal system represents numerical values using 10 symbols, from 0 to 9.

demodulation (W) – The act of extracting the original information from a modulated carrier waveform.

discrete (W) – Consisting of distinct parts. In SCADA, a signal that is either a "1" or a "0".

displacer (D) – A device for inferring liquid level by means of measuring buoyant force on a cylindrical element partially submerged in the liquid.

WB_00001265

duplex (full; see also half duplex) (D) – A method of operation for a communication circuit where each end can simultaneously transmit and receive.

EPROM (T) – Erasable Programmable Read Only Memory.

flip-flop (D) – A bi-stable electronic device that can store one bit of data.

FM (W) – A method of modulation in which the frequency of the carrier wave is adjusted in response to the signal being sent.

FSK (W) – Frequency-Shift Keying. A modulation scheme in which digital information is transmitted through discrete frequency changes of the carrier.

geosynchronous (W) – For an Earth satellite, moving in orbit at such a speed as to appear fixed above a point on the equator.

half duplex (W) – A method of operation for a communication circuit where each end can either transmit or receive, but not simultaneously.

hexadecimal (W) – A numerical system that uses 4 binary digits to represent 16 symbols, 0 to 9 and A to F.

HEO – Highly elliptical orbit. Referring to an Earth satellite that has an orbit that brings the satellite close to the Earth at some point. Less power is required to communicate when two objects are close together.

I/O (D) – Input/Output. General term for the equipment used to communicate between the computer and the operator.

ISO – International Organization for Standardization.

iterative (D) – Referring to "repeatedly executing a series of operations until some condition is satisfied."

LAN – Local Area Network

LCD – Liquid Crystal Display. A type of graphical screen commonly used to communicate between a computer and an operator.

LEO – Low Earth Orbit. Referring to Earth satellites. An orbital path that allows satellite/Earth station communication with less power because they are close together. Low earth orbits may be circular and not elliptical. Low earth orbits will be subject to more atmospheric friction and will, therefore, have shorter lives or will require more fuel to retain their orbits.

LSB – Least Significant Bit (of a string of binary bits).

WB_00001266

medium (W) – The physical material or method of transmission between devices that are communicating.

modulation (T) – The process whereby some characteristic of a carrier wave is varied in accordance with a string of data.

MSB – Most Significant Bit (of a string of binary bits).

MTU – Master Terminal Unit. In SCADA, the device that interfaces with the operator, provides long-term storage of data, and handles communication to and from the Remote Terminal Units.

orifice meter (W) – A device that measures the pressure drop of a fluid across a know cross sectional restriction to calculate flow rate.

OSI – Open Systems Interconnection. A nonproprietary standard model that attempts to standardize end-to-end computer communication.

parallel (W) – A method of moving digital information via multiple data paths by using one wire or other medium for each bit of data in the digital word. See "serial."

protocol (D)– A set of rules and formats that determines the communication behavior of an entity.

PSK – Phase-Shift Keying. A modulation method that transfers information by changing the phase of the carrier wave rather than the amplitude or frequency.

real time (D)– In SCADA, pertaining to the performing of a computation during the actual time that the related physical process transpires so the results of the computation can be used to guide the physical process.

refraction (W) – The bending of a ray of light, electromagnetic wave, or sound when it passes from one medium to another medium whose speed of propagation differs from the first.

register (D) – In data processing, the specific location of data in memory.

Reynolds number (W) – A unitless number that represents turbulence. Less than 2000 means laminar flow. More than 4000 means turbulent flow.

risk (W) – The product of the likelihood of an event multiplied by the consequences of the event.

RTU – Remote Terminal Unit. In SCADA, the device that is located away from the central control area. It communicates between the Master Terminal Unit and the field end devices and provides local short-term memory.

WB_00001267

SCADA – Supervisory Control And Data Acquisition.

Scan (D) – To sample, in a predetermined manner, each of a number of variables.

sensor (W) – An element that receives information about the process and converts it to a form that is usable by the control system.

serial (O) – The method of transferring data over a single data path as a single sequence of bits. See "parallel."

simplex (D) – A method of data transmission whereby data can be transferred in one direction only.

SIS (W) – Safety Instrumented System. A system that overrides the control system to return the process to a safe condition.

supervisory control (T) – Control in which the loops operate independently and are subject to intermittent corrective action.

synchronous (W) – Digital communication in which a common timing signal is established, which allows for very high data transmission rates. See asynchronous.

telemetry (O) – Transmitting the readings of a distant measuring instrument, most often by radio.

totalizer (W) – A device that receives pulses or other basic signals and applies an algorithm to them to determine the amount of product that has been measured. It often outputs its results in engineering units.

UPS (D) – Uninterruptible Power Supply. An electric battery-based system for providing continuous power to critical equipment.

UHF – Ultra High Frequency. Radio frequency between 300 MHz and 3000 MHz.

VDU (D) – Video Display Unit. Any device for visually presenting computer information to a person. May be CRT or LCD.

WB_00001268

Appendix C: Solutions to All Unit Exercises

The Integration Group of The Americas Ex. 1007 Page 910

WB_00001269

Appendix C

Solutions to All Unit Exercises

Unit 2

2-1. SCADA is different from other control and monitoring systems in that the distance between the process and the central control area is normally much greater in a SCADA system. SCADA is different from other remote control and monitoring systems because with SCADA, only supervisory control is applied from the central control area. Targets and set points are provided to controllers located near the process.

2-2. SCADA RTUs and MTUs can operate with low data rate communication systems because most of the decisions are made at the RTU. Only supervisory instructions such as set points need to be sent from the MTU to the RTUs. Only condensed answers to limited queries need to be sent from the RTU to the MTU. Those SCADA systems that do operate at low data rates have a wide selection of communications media from which to choose. The option of using complex, higher-speed media is there, but cheaper, more available media can also be used.

2-3. The three primary subsystems are the MTU and its related equipment, the RTUs, and the communications equipment. Other parts of a SCADA system—primarily process instruments—are those that can be found in any control system.

2-4. Land lines, in the form of copper or optical fiber, are one medium of communication; the other is radio in any of its many forms.

2-5. Processes are potential candidates for SCADA if they (1) cover a large amount of space, measured in kilometers or square kilometers, (2) can be controlled by relatively simple instructions and monitoring, and (3) require frequent, regular, or fast response in order to operate well.

2-6. All of the data types mentioned can be gathered on a SCADA system by selecting end devices properly and configuring the system properly.

2-7. In almost all cases, the RTU provides electric power to the sensor, which modifies the power in some way. The sensor most commonly used controls the current between 4 and 20 mA, but it may also cause the supplied power to resemble a pulse train or to be turned

The Integration Group of The Americas Ex. 1007-Page 217
SitePro, Inc. v. WaterBridge Resources, LLC, et al
IPR-00738-U.S. Patent No. 9,342,078
WB_00001270

on and off, as in the case of a switch. In a few cases, such as thermocouples and turbine meters, the sensor itself supplies the electric power, but these sensors are exceptions.

2-8. RTUs and MTUs are often provided with UPSs to increase their reliability during power upsets. RTUs depend on electrical power to operate and to allow them to send their messages to the MTU. An uninterruptible power supply (UPS) allows the equipment that it supplies to continue to operate when normal or utility power has failed. This is often the time when the process variables that the RTU is monitoring become most important.

UNIT 3

3-1. Although two-way control and monitoring did exist in limited applications before the 1960s, it was in the early part of that decade that it became a recognized technology.

3-2. The three factors are as follows: (1) The cost of installation is frequently less for radio than it is for the alternative, (2) backhoes and rodents cannot damage a radio signal but can destroy a land line, and (3) radio paths are relatively immune to the condition of the ground between the sites.

3-3. The other reason that electronic computers replaced built-for-purpose MTUs is that the cost of computers became much lower than the cost of the alternative.

3-4. The most profound effect of using inexpensive minicomputers is that it was no longer necessary to be limited to only one MTU. MTUs could be located in the place that made the most sense from a business point of view.

3-5. Like railroads, pipelines and electric transmission lines are linear. This allowed them to be monitored and controlled through control wires, which were the most popular media of communication in the early days of the technology.

3-6. The two operator abilities that SCADA attempts to extend are: (1) the operator's view of the process, in that SCADA presents the process conditions as they are happening as much as 100 miles away, and (2) the operator's reach, in that SCADA allows her/him to adjust process actuators from as far away as 100 miles.

3-7. Analog signals carry a wealth of information about the process. They can convey to the operator the height of sewage in a settling pond within 0.5 cm, or the amount of electrical current in a

The Integration Group of The Americas Ex. 1007-Page 218
SitePro, Inc. v. WaterBridge Resources, LLC, et al

WB_00001271

distribution line within 5 amps. Discrete signals, although not less important, do not carry so much information. A low-level alarm in that same settling pond will use a discrete signal to tell the operator that the level is (1) too low, or (2) not too low. A high-current alarm will tell the operator that the current is (1) too high, or (2) not too high. An analog signal converted to binary form will use perhaps 12 to 16 bits of binary data to move this information. A discrete signal will use only 1 bit of binary data to move its information.

UNIT 4

4-1. a. Adequate. A scan rate of once per hour will identify all significant excursions of the meter.

b. Inadequate. During some scan periods, several customers may fill up, but only the one filling up when the system is scanning will be detected. Many will not be charged for gasoline; one will be overcharged.

4-2. a. A ten-minute scan would work.

b. A one-hour scan would work.

c. A twenty-four-hour scan would be too long, unless the scan were arranged to occur just before the maintenance crew planned its daily activities. Even then, it would catch only those failures that occurred before the start of the day. To be effective, a scan period of one or two hours would be acceptable for failures like this one.

4-3. Nothing. All systems operating with a Master-Slave communications protocol require that the MTU contact and instruct the RTU to respond before the RTU can send a message to the MTU. The RTU will have to wait until it is told to report.

4-4. One RTU in a group of RTUs being scanned can be addressed twice or more in each scan. This will have the effect of scanning that RTU at a higher rate than the others.

4-5. Most SCADA systems communicate between 300 bps and 2400 (bits per second). This is changing as a result of the need by electric utilities and pipelines to scan large numbers of points very quickly. Many new SCADA systems, including but not limited to those used with electric utilities, are using data rates on the order of millions of bits per second.

4-6. The following detract from communications efficiency: communications overhead in the form of RTU addresses included in

WB_00001272

the message, error-detecting and -correcting codes, and radio transmitter settling times. One additional inefficiency for communications paths that are subject to noise is that some messages will be corrupted by the noise and will have to be discarded and resent.

4-7. Refer to Example 4-4. The number of bits of information will be unchanged at 896 per RTU or 17,920 bps. We will assume that the data rate remains unchanged at 1200 bps. So, at 100% efficiency, it would take 17,920/1200 = 14.933 seconds. But now we will use a communications medium that has a 70% efficiency (as compared to the 40% efficiency in Example 4-4.) So it will take 14.933/0.70 = 21.33 seconds. We would probably round this up to 30 seconds if we were doing a first pass scan time check.

4-8. a. If the separator cycle and the scan rate were each exactly two minutes, each scan would occur when the liquid level was at the same height. The level would appear to be static.

b. This would work. The liquid level would be sampled four times throughout its cycle. The operation of the separator could be inferred from this information.

UNIT 5

5-1. Electric wire has long been the preferred medium for moving measurement data and instructions between the process and the facility control room. Other media have been used, for example, compressed air and even mechanical force and motion. Electric signals have the advantage of being clean, flexible, and relatively safe. The preference for electrical media moved to RTU and process connections as an evolutionary step.

5-2. Oil and gas processing, as well as some chemical processes, create the possibility that a process fluid will be released that can form a flammable or explosive mixture with the ambient air. Electrical sensors, switches, etc. must be built in such a way that they cannot ignite such a mixture.

5-3. Marshalling panels have as their primary purpose the termination of cables and wires from the process at some point near the control panel. In addition, they can be used to rearrange or reorder control signals; to mount barriers, fuses, and isolating switches in the control and monitoring circuits; and to mount instruments and indicators between the process and the main control panel.

WB_00001273

5-4. Often, the layout of a process results in a concentration of instruments and/or actuators. Rather than use one small cable to connect each instrument to the distant RTU, the designer will find it less expensive to run a multi-pair cable to a location near the instruments. The way that the instruments are constructed precludes running the multi-pair cable through the instrument. A field termination box serves as the termination for the multi-pair cable, and from there, individual (often single-pair) cables are run to the instruments.

5-5. Engineering charges are higher for SCADA projects because SCADA projects are composed of very large numbers of complex, but not very expensive, elements. The effort to ensure that all the parts go together properly costs a significant amount of money; the purchase and installation of the parts is also expensive, but often not as much as for other capital projects. The result is that for SCADA projects, engineering costs may be as high as 50 percent of the total project cost.

5-6. The four factors are as follows:

- The installation details for each type of device would have to be documented.
- Training would be required for operation and maintenance personnel for each type.
- Spare parts would have to be maintained for each type.
- Checkout and calibration procedures would have to be developed, learned and maintained for each type.

5-7. SCADA installations have many electronic parts and many electrical connections. Both of these types of equipment are subject to high initial failure. Note that when electronic equipment is burned in at the factory, fewer problems should result. With better wire termination techniques, electrical connections should cause fewer problems.

UNIT 6

6-1. Both 4- to 20-mA and 0- to 50-mA signals send the information by changing the amount of current flowing through a wire from the sensor to the RTU. The transmitter is able to control this current very well—except when the wire breaks. Then, since there is 0 mA going through the wire, the 0 to 50 mA signal will just indicate the minimum value that the sensor is capable of putting out. But the 4-

WB_00001274

to 20-mA sensor is not capable of putting out 0 mA, so a 0-mA signal can be interpreted as a broken wire alarm. The broken wire will get fixed faster.

6-2. Each bit increases the precision of the measurement by a factor of 2. So a 1-bit digital measurement has a precision of 1 in 2^1 or 1 in 2. A 4-bit digital measurement has a precision of 1 in 2^4 or 1 in 16. An 8-bit digital measurement has a precision of 1 in 2^8 or 1 in 256, which works out to about 1/2-percent precision.

6-3. Electrical cable is less expensive to buy and to install than metal tubing. Cable takes up less room in field trays and in control and marshalling rooms. Electrical cable is more immune to degradation over time than is metal tubing.

6-4. An instrument connected to an RTU in a star topology system can send a message to the RTU at any time, if there is a single-wire pair connecting each instrument to the RTU, and if the RTU is not talking to the instrument at the time. The RTU will have to dedicate a separate circuit to each instrument for this to happen, but it is the normal way for instruments to talk to RTUs. If instruments in a star topology were using radio on a single frequency to talk to an RTU, the situation would be completely different, because if two instruments transmitted at the same time, they would interfere with each other. In that case, each instrument would have to wait until told by the RTU to speak.

6-5. The HART protocol superimposes a digital signal on an analog 4- to 20-mA signal. It can do this only because the number of positive-going half cycles is equal to the number of negative-going half cycles in the digital frequency pulse that is sent to represent each bit. The positive half cycles cancel out the negative half cycles over a length of time that is short compared to the analog signal but is very long compared to the frequency of the digital signal.

6-6. In serial digital communication, we can send one bit of information down the wire for each clock pulse. There is only one pair of wires.

In parallel digital communication, we can send one bit of information down EACH wire pair for each clock pulse. If we have eight pairs of wire between the transmitter and the receiver, at the same clock pulse rate we can send information eight times as fast as with serial.

6-7. Although IEC 61158 describes eight digital communication standards, the only other one that is mentioned in this text is Fieldbus.

WB_00001275

UNIT 7

7-1. Most RTUs, in addition to gathering discrete signals from electrical switches that show status or alarm conditions, can also accept analog signals that indicate the amount of level or pressure or temperature. They can also count the number of times that (for example) a blade passes a magnetic pickup on a turbine meter. This is called pulse count signaling. And finally, most RTUs are capable of accepting digital serial signals from more complex equipment like chromatographs, burner management controllers, and the like.

7-2. Not surprisingly, the RTU's output capability is very much the same as its input capability. RTUs are nearly all capable of sending discrete messages to motors and solenoids, telling the field devices to turn on or off, open or close. Analog signals can be sent to valve actuators instructing them to open to 65 percent or close to 33 percent. Pulse control outputs, although they are not very popular, can instruct a stepping motor to increase, for example, a valve's openness by 8 steps or to reduce its openness by 17 steps. Finally, serial digital signals can be sent to field devices with more complex instructions.

7-3. Protocol drivers are programs written to instruct a computer about the order of steps that must be taken in order to complete some task. Even such a simple task as receiving a serial digital message has rules that must be followed if the message is to be decoded properly. Changing from the language that one instrument understands to a language that the RTU understands, requires a protocol driver to accomplish.

7-4. The three basic fields of many protocols include "message establishment," "information" or "data," and "message termination."

7-5. Security codes are added to the end of a digital serial message to allow the receiver of the message to check to see if any errors corrupted the message from the time it was sent until the time it was received. Occasionally, noise pulses will look very much like a bit in the message. The security code can tell if such an error occurred.

7-6. Field devices can communicate with RTUs by using serial signals. Since this is a very dense form of communication, much information can be passed in a short time. Often this form of communication is used when talking to relatively complex devices that have complex messages to send.

WB_00001276

7-7. Each bit in a digital message doubles the precision of a word with one fewer bits. A 16-bit word can convey a precision of $1 / 2^{16}$. In percent, this works out to 1 in 64,000 or 0.0016%. There are no valves that can operate to that precision and none that need to, and therefore, it would not be useful to record the numbers to this precision.

7-8. Programmable logic controllers (PLCs) were among the first non-RTU devices that were built with RTU capability. At some sites, most of the calculations are done by a PLC, so adding the functionality of the RTU made sense. At other locations, fluid flow totalizing represents most of the calculation effort; thus, fluid flow totalizers have followed in adding RTU functionality.

UNIT 8

8-1. SCADA, by its very definition, requires two-way communication. Simplex is the definition of a communication system that can talk only in one direction.

8-2. When you turn on a radio transmitter, the power that is fed to parts of the transmitter causes transients that swing both the frequency and the power levels up and down for some short time, perhaps as much as 500 milliseconds. During this time, there is too much distortion for a receiver to understand any message. As a result, the message is not fed to the modulator for a period slightly longer than the expected transient. For a message that is about 100 milliseconds long, this turn-on time is very wasteful of the limited time that is available to send all the messages that must be sent. Turn-on time is one of the major contributors to inefficiency of radio communication.

8-3. Any use of the Internet in a control system exposes that system to public inspection and malicious activity. There are ways to protect your system, but a great deal of attention to the security of the system is necessary.

8-4. The primary disadvantage of UHF is that it cannot reliably send a message to a location that is out of the line of sight. UHF is a high enough frequency that it does not refract well around corners. This is sometimes an advantage, but more often it seems like a disadvantage.

8-5. Low speed SCADA normally uses copper wire, either buried or overhead, or some form of radio to move data between the MTU and its RTUs.

WB_00001277

8-6. The three most common methods of modulation are (1) amplitude modulation, AM; (2) frequency modulation, FM; and (3) phase shift modulation, also called phase-shift keying, PSK.

8-7. Buried telephone lines are available with several choices in the number of wire pairs. Because the cost of the armor, waterproof jacket, shipping, and installation is much higher than the cost of the copper in the wires, it is unusual to bury cable with less than 18 pairs. For connecting large urban centers, cables are available with as many as 2400 pairs of copper wire.

8-8. One of the functions of the modem is to check to ensure that the medium is not being used before it turns on its transmitter.

UNIT 9

9-1. This statement is true for Master-Slave communication.

9-2. The station that has a definition for the entire process is the master terminal unit (MTU).

9-3. Each remote terminal unit (RTU) needs to know about only those things that it directly interfaces with. Interfaces at other RTUs or at the MTU are of no interest to an RTU.

9-4. MTUs communicate with RTUs, with the equipment that forms the human-machine interface, and with other computers, which may include accounting machines, applications engineering workstations, and long-term storage databases.

9-5. For a transmission-line system that has feeder lines going off at points A, B, and C, each one of which is equipped with a remotely controlled switch, the program for operating the switches would look like this.

- If a keyboard entry calling for "Open Switch A" is made, set a flag (put a 1) in the MTU register reserved for the control of this switch. Similar instructions must be made for Switch B and Switch C.
- Each time a scan is ordered, check each of these registers and compare their contents to the contents of registers that tell what the present status of each switch is (1 for open; 0 for closed).
- If the registers are the same, send a message to the operator I/O that says, "Switch A is already open." Go to standby mode.

WB_00001278

- If the registers are different, include an order in this scan telling the RTU at Switch Location A to open the switch.
- At the next scan, check the switch status to determine that the switch did in fact open. If it did, send a message to the I/O that says, "Switch A now open." Go to standby mode.
- If the status registers indicate that the switch did not open, resend the order to open it on the next scan.
- After the next scan, recheck the switch status to determine that the switch did open. If it did, send a message to the I/O that says; "Switch A now open." Go to standby mode.
- If it did not open, send a message to the I/O that says; "Switch A failed to open." Go to standby mode.
- For each of the three switch locations, provide a "Max Current" register in the MTU that will store the maximum allowable current through that feeder line.
- For each of the three switch locations, on each scan, monitor the current being drawn through that line.
- Compare the value detected to the valued in the "Max Current" register. If the value detected is equal to or greater than 90 percent of the value in the "Max Current" register, send a message to the I/O and to the alarm log that says; "Load on Line A is approaching critical." Send the date and time to the alarm log.
- If the value detected is equal to or greater than 100 percent of the value in the "Max Current" register, set the flag to open the appropriate switch, and send a message to the I/O that says, "Switch A has been ordered to open." Send a message to the alarm log that says, "Overcurrent at Feeder Line A." Send the date and time to the alarm log.
- Check the next scan to determine that the switch did open. If it did, send a message to the I/O that says, "Switch A is now open." Go to standby mode. If it did not open, send another message to the RTU telling Switch A to open, and so on.
- Apply similar logic to Switches B and C.

9-6. The ability of the MTU to transfer large amounts of information to a computer that is not directly involved with the day-to-day operation will probably cause much of this information to be stored outside of the MTU. This transfer could be done by hard-wired connections

WB_00001279

between the two computers or by some form of networking—if there is sufficient confidence in the immunity of the network to cyber interference.

9-7. Graphics have the effect of increasing the need for memory for two reasons. First, graphics themselves use a significant amount of memory. Second, the ability of operators to interpret much larger amounts of data makes it beneficial to have much more operating data stored in locations that are accessible to the MTU.

9-8. One of the most important things that the MTU does is to routinely run applications programs. An example of an applications program is the scanning function. Another is the process of determining whether a point is in alarm by comparing the present reading of that point to a selected value that is entered by the operator and stored in the memory registers of the MTU.

UNIT 10

10-1. MTUs can advise the operator by means of the I/O screen or by a hardcopy method such as a printed alarm report. On large SCADA systems, they can also get the attention of the operator by ringing bells or sirens in the MTU control room. If the room is frequently empty, the MTU can be programmed to call the operator on his or her cell phone to advise of an upset.

10-2. Trending allows the pattern recognition part of the human brain to evaluate large amounts of data in a relatively painless way. If a pattern exists, a graphical display like trending will allow it to be found much more easily than will table or list-based displays.

10-3. Clustering similar pieces of data together on I/O screens will also allow the pattern recognition part of the brain to quickly analyze the data.

10-4. Changes in status points at the MTU level do not trigger major reactions. They result in updates to status registers and do not cause interrupts. Alarm point changes result in the same type of register updates, but they also cause interrupts that often involve audible alarms, messages to alarm printer logs, and the need to acknowledge the alarms.

10-5. An alarm log is a hardcopy printout of all alarms, acknowledgements, and returns to normal, complete with their date and time of occurrence. It is automatically generated by a system. It provides an auditable record of the out-of-limits operation of the system.

WB_00001280

10-6. Reporting by exception reduces the load on the operator by filtering out older system responses and reporting only those alarms or status changes that are new and/or unexpected. For example, if an irrigation gate has been open for the last week, there is no need to tell the operator that it was open on the latest scan. The operator should be told only when the gate, after being open for so long, finally closes.

10-7. Several technological tools are making printed maintenance reports unnecessary. Lap-top and palm-top computers, on which the maintenance personnel can store their daily assignments, are one example. With proper communication between the MTU and the maintenance computers, the maintenance workers can call up MTU generated reports as they drive to their work. Cell phones that let a maintenance manager in the office instruct his team of maintenance workers in real time are another example.

10-8. The economic justification for installing a SCADA system comes from increasing the ability of the operator and the maintenance team to get more from the facility. One example is being able to safely push more current through a transmission line because the operator knows that temperature and wind conditions will allow it. Learning more quickly about an irrigation gate left open can reduce the over-watering that would otherwise result.

UNIT 11

11-1. The fact that safety instrumented systems should be independent from control systems is one indication that SCADA, which is a control system, should not be used as part of a safety system. The fact that SCADA systems have many parts—not few parts—is another indication that a SCADA system should not be used as part of a safety instrumented system.

11-2. Yes. Analog signals such as this are frequently monitored by SCADA.

11-3. No. The failure of the displacer would then not only inhibit the operation of the normal control system, it would also cause the protective system to be inoperative.

11-4. Communications systems contain many parts. This in itself does not preclude using them in safety systems; however, communications systems usually exhibit low reliability. Safety instrumented systems should be composed of elements that are known to have high reliability.

WB_00001281

11-5. Yes. This is one of the functions that make SCADA a valuable tool for electric utilities, and it can be thought of as a normal operation.

11-6. Local operating equipment should be installed to protect each section of the line in the event that the remote switches do not work. These local devices constitute the safety instrumented system.

11-7. Some regulatory agencies require that billings for product delivered be backed up by paper or extended memory. Make sure that you check the regulations before you include this function in your SCADA or ensure that you have sufficient memory and/or print outs to meet the regulations.

11-8. Flow totalizers must make provision for changing factors within the algorithm and even for changes to the algorithm itself. Of course, any change to the algorithm or its factors will result in a change in the reported amount of the material being measured. A hard-copy printout can provide an accounting check when an audit of the process is needed.

UNIT 12

12-1. The two divisions of security for a SCADA system are Physical Security and Cyber Security.

12-2. The security team should develop a detailed description, both graphic and narrative, that it can compare to the actual installation to check for weak spots.

12-3. As in any position of responsibility, a person will better fulfill the responsibilities that are assigned if that person can take ownership in the assignment. An Owner should understand the consequences to him/her of success and of failure.

12-4. Old SCADA systems were designed before any concern existed that someone might want to hack into them. On the other hand, old SCADA systems did not connect to other networks, especially the Internet, where potential enemies can find simple entry into the SCADA system.

12-5. Many of the security features of a SCADA system will make it impossible (or nearly so) to install new software. The software manufacturer will often include in the installation instructions a note to turn off one or more of the cyber security features. Unfortunately, they seldom tell the installer to turn the feature back on.

WB_00001282

12-6. The first phase of the project is to analyze the system for security shortfalls and to gather and/or develop solutions for these shortfalls. The listing of these shortfalls and solutions, along with the costs, schedules, and benefits of the solutions, forms a report that is presented to management by the owner. The owner should follow the project to completion, including installation and testing of the recommended solutions after the report has been presented.

UNIT 13

13-1. MTU scanning speed can be important because of the time response needed to address alarm situations.

13-2. If the MTU is in the decision path, it must first learn that there is a problem. That will take one scan period. In most cases, the MTU will wait until the next scan before it sends instructions to the RTU with the problem, telling it what to do. Then it must wait for additional scans before it can tell if the problem has been resolved.

If the issue is very urgent, a special response by the MTU can be programmed to issue orders – outside of the regular scan procedure – to make the correction to the process in less than two scan periods.

13-3. If regulations prevent you from billing using electronically gathered data, you can issue an interim invoice, based on the electronic billing, with the mutual understanding that the final invoice will be based on the auditable paper meter readings.

13-4. The total price of a transferred commodity is the product of the unit price and the number of units.

13-5. Accuracy and security are both important when you are depending on a meter to measure large values' worth of a commodity. The accuracy is obviously important. The security is also important because both sides of the purchase must be satisfied that no one made unauthorized changes to the meter factors that determine how the meter calculates the throughput.

13-6. SCADA systems are an attractive control method for processes that are large, that are relatively simple to control, and that require frequent monitoring and measuring of some variables.

13-7. Because SCADA depends so much on the communications system that ties its various elements together, it is absolutely vital that this communications system works. Keeping track of communication failures will identify weak spots in the system that may be reinforced before total communications failure occurs.

WB_00001283

UNIT 14

14-1. The development of cyber secure communications will make fully automatic SCADA control more attractive. Encryption methods now exist and are starting to be installed even as retrofits in existing SCADA systems where strategic values have been assigned to these processes.

Spread-spectrum radio has allowed secure communication on radios that require so little power that no radio license is required for their operation. These systems will replace wiring in many applications. Spread-spectrum radio also has effective cyber security features.

14-2. Frequency Hopping Spread Spectrum (FHSS) operates by having the transmitter and receiver change their selected frequency according to a secret pattern. This pattern is sufficiently complex that it cannot be broken. In fact, in many cases, it cannot even be detected.

Direct Sequence Spread Spectrum (DSSS) operates by adding a secret coded sequence of ones and zeros to the message before the message is modulated onto the carrier. Again, the code is sufficiently complex that it is nearly impossible to break.

14-3. Whenever you connect SCADA to a network, you are increasing the potential for a person with malicious intent to access your SCADA.

14-4. (1) Cyber security improvements can allay some concerns about intentionally corrupted data. (2) The quality of instrumentation, including its reliability, has improved. (3) The cost of instrumentation has not increased unreasonably. (4) Better application programs are available, including programs that have proven to be reliable over time.

14-5. The use of very wide bandwidths allows reasonable data rates to be communicated at low signal-to-noise ratios. The trading off of high bandwidth for low signal-to-noise requirements is one of the bases of spread-spectrum's technical success. Instruments do not require a very high data rate to be practical.

14-6. Packet data cost can be extremely low because it gets a free ride on the infrastructure that has been put in place for voice cell phones. The data packets are sized to be able to fit between pauses in voice messages. No additional cell or network equipment is required. No additional frequencies need to be reserved.

WB_00001284

UNIT 15

15-1. The two basic factors that make up the economic equation are costs and benefits.

15-2. As long as interest costs exceed 0 percent, the time value of money will be significant. One dollar in your hand today is more valuable to you than the promise of one dollar five years from now.

15-3. Each political area establishes a taxation regime to meet its needs. Within that political area, different industries may be treated differently. Levels of taxation can make the difference between a project being economically positive or negative. Only with good advice on taxation can you accurately determine the after tax economics of a project, which is the value that is really important to your company.

15-4. If money must be spent to do something in the future, resources must be allocated now so that the money will be available when it is needed. These resources can be invested now, and they will grow by an amount that depends on the interest rate they are invested at and the length of time they are invested. The present value of the money is the amount of resources that must be invested now so that the investment grows to equal the amount of money that will be needed at that future date.

15-5. Often this class of benefits is large, and since these benefits occur early in the life of a project, they have a high present value.

15-6. Operations specialists are the best qualified to identify the potential operating savings of a project.

15-7. The time at which the training is scheduled is important. Training should be provided just before the ability is needed. Other considerations involving the location of the training are also important.

15-8. There are many ways that SCADA can improve the effectiveness of a facility. Only by conducting a comparative study, using several different types of specialists, of the way the facility would be operated with and without SCADA, can an estimate be made to quantify the net benefit. Reduced capital cost, reduced operating cost, improved product quality, improved throughput, and improved response to changing conditions are a few of the factors to consider when doing such an evaluation.

WB_00001285

Index

Index

accounting 163, 173, 192, 194–195, 245, 249
actuators 4, 12, 51–53, 58, 60–61, 67, 73–74, 92, 169, 205, 217–218, 238, 241, 243
advisory 229
  applications 200
alarm
  conditions 160
  logs 163
  storms 158
alarming 158, 183, 200
algorithm 4, 23, 34, 36, 63–66, 91, 176, 190, 192–193, 195–196, 229
aliasing 62, 229
AM 115, 128, 229
amplitude
  distortion 115
  modulation 117
analog 11, 21–24, 34, 72
  control 65, 98
  output card 100
  signals 22–23, 64, 73, 76–77, 80, 93, 205, 238, 243, 248
analog-to-digital 80
analog-to-digital converter 82
applications 144, 187, 189, 200, 208
asynchronous 119, 230
automatic control 5, 199–200

bandwidth 119, 128, 132, 206, 251
baud 128, 230
Bell Labs 206
benefits 213
binary message 94
bit 11, 79, 81, 83, 96, 111–112, 114, 118, 143, 230
bits per second 77, 128, 230, 239
bps 230

capital costs 216, 219
CDMA 206
central processing unit 230
code division multiple access 206
communication reports 163
communications 69, 71, 131, 196, 207
  access 61, 147
  interface 92, 137
  system 109, 121, 169, 195, 207, 248, 250
control 21–22, 36, 97–98, 100–101, 167, 199
  functions 17, 52, 162
  screens 162

costs 53, 216, 218–220
  capital 216, 219–221
  maintenance 67, 154, 218–221
  operating 27, 219–220
  training 218
CPU 33, 93, 230
CRC 114
CRT 230
cyber security 179–183, 185, 208, 225, 230
cyclic redundancy code (CRC) 114

data
  rate 113, 115, 118–119, 125, 129, 140, 206, 237, 239, 251
  storage 147
  terminal equipment 109
development from telemetry 24
direct sequence spread spectrum 206, 251
discrete 22–23, 34, 140, 230
  control 97
  signals 101
displacer 175, 230, 248
DSSS 206, 251
duplex systems 125

economics 52, 213, 221–222, 252
EPROM 231
erasable programmable read only memory 231

facility effectiveness 221–222
FHSS 206, 251
flip-flop 79, 83–84, 231
FM 115, 118, 128, 231
frequencies 85, 114–116, 127–129, 251
frequency
  bands 128
  hopping, spread spectrum 206, 251
  modulation 118
frequency-shift keying 115, 128, 231
FSK 116, 128, 231
function 51, 65, 75, 93–94, 110, 112, 121, 162, 193, 195

gas volumes 193
geosynchronous 131–132, 231
graphics 149, 247

half duplex systems 125
hardwired controllers 156

WB_00001287

host computer 12, 137

I/O 12, 153, 231, 245–247
information field 94–95
input/output 12, 153, 231
internal address 112
International Organization for Standardization (ISO) 109, 231
intrusion detection 182–183
iterative 213, 231

Jacobs, Irwin 206

Lamarr, Hedy 206
LAN 137, 231
LCD 230–231, 233
least significant bit 81, 83, 231
limit switch 79
local area network 231
local loop override 171
loop protection 171
LSB 81, 231

maintenance 61, 130
  costs 218
master terminal unit 4, 12, 24, 35, 137, 154, 184, 217, 232, 245
master-slave communication 85, 110, 137, 207, 239
medium 51, 67, 71–72, 74, 85, 113, 128, 207, 232
message
  establishment 94, 243
  termination 94, 243
  terminator field 97
modem 12, 61, 92–93, 109–110, 113, 119, 217
modifier 112
modulation rate 128
most significant bit 81, 83–84, 114, 232
MSB 81, 84, 96, 232
MTU 207

normal control system 168, 248

objectives 6
open systems interconnection (OSI) 109, 111, 232
operating costs 219–220
operator interface 151, 153, 164

paper trail 173–174, 195, 201
parallel operator interface 164
path study 53, 129
phase-shift keying 116, 232, 245
present value 5, 214–215, 252
processes 10
protocol 110
protocol driver 61, 93, 113, 243
PSK 116, 118, 232, 245
pulse control 100
pulse count signals 102

Qualcomm 206

radio
  communication 23, 126, 140, 205, 207–208, 244
  control 206
  technology 130
real-time
  systems 4, 33
reduced capital costs 219
register 34, 79–81, 94, 112, 114, 141, 144, 146, 158, 232, 245–246
regulatory requirements 172
reliability 5, 22, 130, 163, 168, 238, 248
remote address 94, 112
remote control 167, 199
remote terminal unit (RTU) 4, 34, 63, 122, 205, 232, 245
report-by-exception 132, 158
reports 163
risk 170–171, 179–181, 200, 208, 232
risk mitigation 182
RTU 4, 12, 34–36, 51–56, 58–59, 61, 65, 71–73, 76, 78, 85, 91–94, 109, 111, 113, 123, 131–132, 137–138, 141–142, 144, 153, 162, 169, 174, 179, 182, 190–191, 195, 197–198, 206–207, 217, 219, 232

safety instrumented systems 157, 168–170, 248
satellite communication 131
SCADA 7, 132, 165, 167
  elements of 9, 12
  radio systems 121
scan 4, 36, 62, 67, 126, 144–147, 153, 158, 160, 189–192, 197–198, 233, 239–240, 246, 248, 250
  interval 40
scan interval 36–37, 119, 125, 160
scanning 36, 153, 191, 196, 239, 247, 250
seasonal variations 129
security 177, 179, 225
security code 195, 243
sensors 4, 12, 23–24, 34, 51–53, 58, 60–61, 67, 74, 92, 138, 169, 205, 238

WB_00001288

serial 84, 91–92, 232–233, 242–243
control 101
signal 104
Shannon, Claude 206
signals 73, 101–102, 104
signal-to-noise ratio 128, 206, 251
simplex 121, 123-124, 233, 244
solar variations 130
special orders 96, 112
spread-spectrum 206
communications 206
radios 207, 251
standardization 60
study materials 4, 223, 225
supervisory control 9, 121, 156, 233, 237
supervisory control and data acquisition 3, 9–10, 12, 34, 52, 91, 110, 153, 179, 233
sync 94
synchronous 119, 233

tax implications 221
telemetry 24
temperature compensation 130
temperature transmitter 54
thermometer 54
time delay 38
time value of money 214
timing chart 126
totalizer 56, 65, 91, 140–141, 143, 156, 194–195, 233, 244, 249
training costs 218
trending 161
two-way system 17

UHF 119–121, 128–130, 233, 244
uninterruptible power supply 53, 130, 217, 233, 238
UPS 52, 130, 217, 233, 238

wiring 51–52, 55–56, 58, 67, 251

WB_00001289