IEEE Recommended Practice for Master/ Remote Supervisory Control and Data Acquisition (SCADA) Communications

Sponsor
Substations Committee
of the
IEEE Power Engineering Society

Approved June 18, 1992
IEEE Standards Board

Approved January 12, 1993
American National Standards Institute

Abstract: The use of serial digital transmission by supervisory control and data acquisition (SCADA) systems having geographically dispersed terminals is addressed. These types of systems typically utilize dedicated communication channels, such as private microwave channels or leased telephone lines, which are limited to data rates of less than 10,000 bits/s. Wideband local networks used for high-speed data acquisition and control functions are excluded. This standard covers the communication channels, channel interfaces, message format, information field usage, and communication management. A standard message protocol is defined to the octet level, rather than to the bit level; most details at the bit level are left to the manufacturers of SCADA equipment to define and implement.
Keywords: communications, SCADA equipment, SCADA systems, serial digital tranmission

---

The Institute of Electrical and Electronics Engineers, Inc.

345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1993 by the Institute of Electrical and Electronics Engineers, Inc.

All rights reserved. Published 1993. Printed in the United States of America

ISBN 1-55937-228-1

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason IEEE and the members of its technical committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

IEEE Standards documents are adopted by the Institute of Electrical and Electronics Engineers without regard to whether their adoption may involve patents on articles, materials, or processes. Such adoption does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the standards documents.

Foreword

(This foreword is not a part of IEEE Std 999-1992, IEEE Recommended Practice for Master/Remote SCADA Communications.)

Historical Perspective

The work on this recommended practice began in the early 1980s as an attempt to standardize master/remote communications practices. At that time, each manufacturer of Supervisory Control and Data Acquisition (SCADA) systems had developed a proprietary protocol based on the technology of the time. These proprietary protocols exhibited varied message structures, terminal-to-Data Circuit Terminating Equipment (DCE) and DCE-to-channel interfaces, and error detection and recovery schemes.

This recommended practice addresses this non-uniformity among the protocols, provides definitions and terminology for protocols, and simplifies the interfacing of more than one manufacturer's remote terminal units to a master station.

Prior to development of this recommended practice, the use of bit-oriented protocols for this application was analyzed. The message security of certain protocols was judged unsatisfactory for critical SCADA functions, due to the fact that the message length (in bits) is variable because of zero insert/delete actions of the hardware; therefore, the location of the security check bits in the message cannot always be precisely determined in the presence of message errors. The International Electrotechnical Committee (IEC) Telecontrol group[1] has independently reached the same conclusion. Therefore, a message protocol with known message lengths has been developed for this recommended practice.

This recommended practice provides the following benefits:

- Improved immunity to random errors, burst errors, and false synchronization over most existing protocols
- Protection from loss of remote-terminal stored data due to noise or extraneous voltages on the communication channel
- Capability for techniques made possible by microprocessor technology, such as report-by-exception and sequence of events reporting

Relevance to Modern Practices

The trend towards standardization of communications protocols and practices among all elements of computer-based systems has progressed in parallel with the development of this recommended practice. As a result, much of the technology underlying this recommended practice has been supplanted by contemporary technology.

This recommended practice addresses the master/remote protocols and practices in wide use today. The relevance of newer communications technology now being introduced will require additional study. The issues to be addressed in future revisions of this recommended practice include

1) Increased data rates
2) Additional standardization of message fields (for example, standardized function codes and data formats)
3) The initiation of communications by remote terminals ("spontaneous" reporting)
4) Use over communications channels with variable transmission delays (for example, packet switched networks)

The harmonization of this recommended practice with appropriate national and international communications standards, such as the Open System Interconnection (OSI) model promulgated by the International Standards Organization (ISO), the Utility Communication Architecture standard under development by the Electric Power Research Institute (EPRI), and the standards of the IEC Telecontrol group must also be deliberated. This work will begin immediately so that these issues will be resolved in the first revision of this recommended practice.

[1]IEC Technical Committee No. 57: Telecontrol, Teleprotection, and Associated Telecommunications for ElectricPower Systems.

This document defines services and protocol elements that permit the exchange of management information between stations attached to IEEE802 local and metropolitan area networks. The standard includes the specification of managed objects that permit the operation of the protocol elements to be remotely managed.

At the time that this standard was completed, Working Group C3, Electric Network Control Systems Standards of the Data Acquisition, Processing, and Control Systems Subcommittee had the following membership:

Floyd W. Greenway, *Chair*

W. J. Ackerman
G. J. Bartok
J. R. Benckenstein
W. R. Block
D. M. Clark
R. W. Corlew
G. J. Crask
J. G. Cupp
T. L. Doern
J. W. Evans
R. J. Farquharson
J. E. Holladay
D. L. Johnson
D. F. Koenig
R. L. Kreger
T. L. Krummrey
L. W. Kurtz, Jr.
J. D. McDonald
J. S. Oswald
W. B. Prystajecky
S. C. Sciacca
J. Singletary, Jr.
A. R. Skopp
H. L. Smith
R. C. Sodergren
S. R. Sykes
J. T. Tengdin
A. D. Watson

At the time that this standard was complete, the Data Acquisition, Processing, and Control Systems Subcommittee had the following membership:

John D. McDonald, *Chair*

W. J. Ackerman
G. J. Bartok
J. R. Benckenstein
W. R. Block
D. M. Clark
R. W. Corlew
T. L. Doern
J. W. Evans
R. J. Farquharson
F. W. Greenway
J. E. Holladay
K. K. Jackson
D. F. Koenig
R. L. Kreger
T. L. Krummey
L. W. Kurtz, Jr.
C. T. Lindenberg
J. S. Oswald
W. B. Prystajecky
D. G. Rishworth
B. D. Russell
S. C. Sciacca
J. Singletary, Jr.
H. L. Smith
R. C. Sodergren
S. R. Sykes
J. T. Tengdin
W. L. Yeager
A. D. Watson

Special thanks to Jim Oswald, the previous working group chair and the coordinator of this document, who was responsible for all coordination and all drafts.

At the time that it balloted and approved this standard for submission to the IEEE Standards Board, the Substations Committee had the following membership:

W. J. Ackerman
B. Y. Afshar
S. J. Arnot
A. Baker
N. Barbeito
G. J. Bartok
J. D. Betz
K. M. Bevins
K. L. Black
C. J. Blattner
W. Block
S. Boggs
L. N. Ferguson
G. G. Flaig
D. L. Garrett
A. Haban
D. L. Harris
M. A. Hick
J. E. Holladay
M. L. Holm
D. C. Johnson
Z. Kapelina
G. G. Karady
R. P. Keil
J. D. McDonald
T. S. McLenahan
P. R. Nannery
S. P. Meliopoulus
J. T. Orrell
J. S. Oswald
S. G. Patel
R. J. Perina
L. Pettersson
T. A. Pinkham
J. Quinata
D. G. Rishworth
P. C. Bolin
S. D. Brown
J. C. Burke
J. B. Cannon
R. E. Carberry
J. R. Clayton
E. F. Counsel
D. M. Christie
N. Cuk
F. A. Denbrock
W. K. Dick
C. C. Diemond
W. B. Dietzman
T. Doern
F. F. Kluge
D. F. Koenig
T. J. Kolenda
A. Kollar
E. Kolodziej, Jr.
T. L. Krummey
L. W. Kurtz
D. N. Laird
A. A. Liebold
C. T. Lindeberg
P. Lips
W. F. Long
R. Matulic
D. Russell
J. Sabath
D. R. Schafer
F. C. Shainauskas
B. Sodka
R. C. St. Clair
W. K. Switzer
E. R. Taylor, Jr.
C. F. Todd
D. R. Torgerson
L. F. Volf, Jr.
R. J. Wehling
W. M. Werner
B. W. Wray

When the IEEE Standards Board approved this standard on June 18, 1992, it had the following membership:

Marco W. Migliaro, *Chair*
Donald C. Loughry, *Vice Chair*
Andrew G. Salem, *Secretary*

Dennis Bodson
Paul L. Borrill
Clyde Camp
Donald C. Fleckenstein
Jay Forster*
David F. Franklin
Ramiro Garcia
Thomas L. Hannan
Donald N. Heirman
Ben C. Johnson
Walter J. Karplus
Ivor N. Knight
Joseph Koepfinger*
Irving Kolodny
D. N. “Jim” Logothetis
Lawrence V. McCall
T. Don Michael*
John L. Rankine
Wallace S. Read
Ronald H. Reimer
Gary S. Robinson
Martin V. Schneider
Terrance R. Whittemore
Donald W. Zipse

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
James Beall
Richard B. Engelman
David E. Soffrin
Stanley Warshaw

Mary Lynne Nielsen, *IEEE Standards Project Editor*

CLAUSE PAGE

IEEE Recommended Practice for Master/ Remote Supervisory Control and Data Acquisition (SCADA) Communications

1. Scope

This recommended practice applies only to the use of serial digital transmission by supervisory control and data acquisition (SCADA) systems having geographically dispersed terminals. These types of systems typically utilize dedicated communication channels, such as private microwave channels or leased telephone lines, which are limited to data rates of less than 10 000 b/s.

This recommended practice is not applicable to wideband local networks used for high-speed data acquisition and control functions.

This recommended practice generally defines a standard message protocol to the octet level, rather than to the bit level; most details at the bit level are left to the manufacturers of SCADA equipment to define and implement. With the increased use of microprocessors in SCADA equipment, it is expected that decoding at the bit level will employ table look-up techniques rather than use hard-wired logic; therefore, such details need not be specified in order to reach a reasonable degree of compatibility.

This recommended practice supports Sections 5.4 and 7.4 of IEEE Std C37.1-1987 [7].

2. References

This standard shall be used in conjunction with the following publications. When the following publications are superseded by an approved revision, the revision shall apply.

[1] ANSI X3.4-1986, Coded Character Set—7 Bit American National Standard Code for Information Interchange.[1]

[2] ANSI X3.172-1990, American National Standard Dictionary for Information Systems (ANDIS).

[1]ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

Copyright © 1993 IEEE All Rights Reserved

[3] CCITT Blue Book, Vol. VIII.1 (V Series Recommendations), Data Communication Over the Telephone Network, November 1980.[2]

[4] EIA-422-A (Dec. 1978), Electrical Characteristics of Balanced Voltage Digital Interface Circuits.[3]

[5] EIA-423-A (Dec. 1978), Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits.

[6] EIA-449 (Nov. 1977, Reaff. Dec. 1984), General Purpose 37-Position and 9-Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.

[7] IEEE Std C37.1-1987, IEEE Standard Definition, Specification, and Analysis of Systems Used for Supervisory Control, Data Acquisition, and Automatic Control (ANSI).[4]

[8] IEEE Std 100-1992, The New IEEE Standard Dictionary of Electrical and Electronics Terms.

[9] IEEE Std 367-1987, IEEE Recommended Practice for Determining the Electric Power Station Ground Potential Rise and Induced Voltage From a Power Fault (ANSI).

[10] IEEE Std 487-1980, IEEE Guide for the Protection of Wire Line Communications Facilities Serving Electric Power Stations (ANSI).

[11] IEEE Std 643-1980, IEEE Guide for Power-Line Carrier Applications (ANSI).

[12] IEEE Std 776-1987, IEEE Guide for Inductive Coordination of Electric Supply and Communication Lines (ANSI).

3. Definitions

The definitions of terms contained in this recommended practice or in other standards referred to in this recommended practice are not intended to embrace all legitimate meanings of the terms. They are applicable only to the subject treated in this recommended practice.

Master/remote communication is used in equipment defined in accordance with IEEE Std C37.1-1987 [7]. Selected definitions of hardware and system application terms extracted from IEEE Std C37.1-1987 have been included as an aid to the reader and are indicated with a [7]. SCADA systems may use computers. For standard definitions of computer terms, refer to ANSI X3.172-1990 [2].

address: An identifying name, label, or number for a data terminal, source, or storage location calculation.

analog data: Date represented by scalar values [7].

analog signaling: See **signaling, analog.**

bidirectional: Providing for information transfer in both directions between master and remote terminals (of a communication channel).

binary digit: A character used to represent one of the two digits in the binary number system and the basic unit of information in a two-state device. The two states of a binary digit are usually represented by “0” and “1”. *Synonym*: **bit.**

[2]CCITT publications are available from the CCITT General Secretariat, International Telecommunications Union, Sales Section, Place des Nations, CH-1211, Genève 20, Switzerland/Suisse.
[3]EIA publications are available from Global Engineering, 1990 M Street NW, Suite 400, Washington, DC, 20036, USA.
[4]IEEE publications are available from the Institute of Electrical and Electronics Engineers, Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

 Copyright © 1993 IEEE All Rights Reserved

binary signaling: See **signaling, binary**

Bose-Chaudhuri-Hocquenghem (BCH) Code: A class of security code that is relatively simple to implement in hardware and that provides a high degree of immunity to transmission errors for a small reduction in communication efficiency.

broadcast: A mode of information transfer in which a single message is transmitted simultaneously to multiple receivers.

buffer: A device in which data are stored temporarily in the course of transmission from one point to another; used to compensate for a difference in the flow of data, or time of occurrence of events, when transmitting data from one device to another [7].

byte: A group of adjacent binary digits operated on as a unit. Usually 8 b (which is synonymous with **octet).**

carrier detect: A dc electrical signal presented by a modem to its associated terminal equipment when the modem is receiving a modulatory signal.

channel: See **communication channel**

check code: See **security code.**

command: A pulse, signal, or set of signals initiating one step in the performance of a controlled operation.

communication channel: A facility that permits signaling between terminals.

data: Any representation of a digital or analog quantity to which meaning has been assigned [7].

data acquisition: The collection of data [7].

data rate: The rate at which a data path (for example, a communication channel) carries data, measured in bits per second [7].

digital quantity: A variable represented by coded pulses (for example, bits) or states [7].

diagnostic: A process by which hardware malfunctions may be detected.

duplex: A simultaneous, two-way, independent transmission in both directions. *Synonym*: **full duplex.**

error control: Any of a variety of techniques employed to detect and/or correct transmission errors that occur on a communication channel.

error count: The number of detected errors in the operation of some device. For communication channels, separate error counts may be maintained for several different error types, e.g., no response, invalid response, and multiple retries, to simplify determination of the error source(s).

error rate: The probability of an error occurring in the course of data manipulation. For serial binary channels, the error rate is usually expressed as the “bit error rate,” i.e., the probability that an individual bit will be received in error.

field: A group of any number of adjacent binary digits operated on as a unit.

flag: A character that signals the occurrence of some event. Usually a field of 1 b.

frequency division multiplex: See **multiplexing**

half duplex: Transmission over a circuit capable of transmitting in either direction, but only in one direction at a time. *Contrast with*: **duplex.**

interface: A shared boundary between two system components across which information is transferred.

master terminal: See **terminal, master.**

message:

1) In information theory, an ordered series of characters or bits intended to convey information.
2) An arbitrary amount of information whose beginning and end are defined or implied.

Copyright © 1993 IEEE All Rights Reserved

3) For bisync-type devices, the data unit from the beginning of a transmission to the first end-of-text (ETX) characters.
4) A group of characters and control bit sequences transferred as an entity from a data source to a data sink, where the arrangement of characters is determined by the data source.
5) In telecommunications, a combination of characters and symbols transferred from one point to another.

modem: A device that modulates and demodulates signals transmitted over data communication facilities. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities.

multiplexing: The division of a transmission facility into two or more channels, either by splitting the frequency band transmitted by the channel into narrower bands, each of which is used to constitute a distinct channel (frequency division multiplexing) or by allotting this common channel to several different information channels one at a time (time-division multiplexing).

network: A series of points interconnected by communication channels.

octet: A group of eight adjacent binary digits operated on as a unit.

party line: A communication channel that services multiple terminals.

point-to-point: Descriptive of a communication channel that services just two terminals.

power-line carrier: The use of radio frequency energy to transmit information over transmission lines whose primary purpose is the transmission of power.

preconditioning time: The interval of time required by channel equipment (e.g., modems) to ready the channel for data transmission.

protocol: A strict procedure required to initiate and maintain communication [7].

remote terminal: See **terminal, remote.**

response: A pulse, signal, or set of signals indicating a reaction to a preceding transmission.

SCADA: Supervisory Control and Data Acquisition.

scan: The process by which a data acquisition system interrogates remote terminals or points for data [7].

security code: A group of data bits calculated by a transmitting terminal from the information within its message by use of a prearranged algorithm, appended to the transmitted message, and tested by the receiving terminal to determine the validity of the received message.

serial communication: Method of transferring information between devices by transmitting a sequence of individual bits in a prearranged order of significance.

signaling, analog: A means of communicating between devices that uses continuously variable signals.

signaling, binary: A means of communicating between devices that uses two-state signals. Where multiple binary data bits are to be transferred, either multiple signaling paths (“parallel binary”) or a time series of individual data bits (“serial binary”) transmission methods are to be used.

simplex: A communication channel that permits information transfer in one direction only. Duplex channels consist of two simplex channels simultaneously operating in opposing directions.

squelch: Facility incorporated in radio receivers to disable their signal output while the received carrier signal level is less than a preset value.

status codes: Information used to indicate the state or condition of system components.

supervisory control: An arrangement for operator control and supervision of remotely located apparatus using multiplexing techniques over a relatively small number of interconnecting channels.

sync slip: An error condition in serial communication channels in which the receiving terminal incorrectly recognizes the start of a new message.

 Copyright © 1993 IEEE All Rights Reserved

system: Hardware and software collectively organized to achieve an operational objective.

terminal: A master or remote terminal connected to a communication channel.

terminal, master: The entire complement of devices, functional modules, and assemblies that are electrically interconnected to effect the master terminal supervisory functions (of a supervisory system). The equipment includes the interface with the communication channel, but does not include the interconnecting channel [7].

terminal, remote: The entire complement of devices, functional modules, and assemblies that are electrically interconnected to effect the remote terminal supervisory functions (of a supervisory system). The equipment includes the interface with the communication channel, but does not include the connecting channel [7].

transaction: A sequence of messages between cooperating terminals to perform a specific function. Usually a minimum of one message in each direction that is comprised of a command followed by a response.

UHF: Ultra High Frequency. Applies to radio communication between 300 MHz and 3000 MHz.

VHF: Very High Frequency. Applies to radio communication between 30 MHz and 300 MHz.

voice frequency: The analog signal bandwidth of approximately 300–3400 Hz used in telephone circuits.

voice-grade: A channel suitable for the transmission of speech, digital or analog data, or facsimile.

word: A group of adjacent binary digits operated on as a unit. Usually an integral number of octets.

4. Communication Channels

SCADA systems consist of one or more master terminals that acquire data from, and send control commands to, multiple remote terminals by transferring digitally encoded messages between the terminals over serial data communication channels. This section defines the necessary characteristics of these channels. The communication scheme defined in this recommended practice is based on the principle that remote terminal messages are transmitted only in response to master terminal messages that explicitly request such responses.

4.1 Channel Requirements

The necessary communication facility between SCADA system master and remote terminals may be provided by any media capable of supporting serial binary signalling, including cable, radio, and optical fiber channels. The communication facility has to provide bidirectional serial data transfer at low error rates. Both point-to-point channels, each servicing a single remote terminal, and party-line channels, each servicing multiple remote terminals, may be used.

SCADA communication channels should be available to the terminals continuously without changes to message routing to permit achievement of adequate system response times. SCADA system operation over switched networks is not included in this recommended practice. Extension to permit the use of dial-up telephone channels may be implemented where needed for special applications.

4.2 Channel Types

4.2.1 Cable Channels

Either duplex or half-duplex cable channels may be used to provide the necessary bidirectional data transfer capability. Voice frequency analog signalling should be used. Any convenient combination of privately owned and dedicated (nonswitched) leased telephone cable may be used.

Copyright © 1993 IEEE All Rights Reserved

4.2.2 Radio Channels

Either duplex or half-duplex VHF or UHF radio channels may be used. Voice frequency tone signalling is typically used as the basic radio-frequency carrier modulating signal. Radio channels may be used for party-line operation of multiple remote terminals.

4.2.3 Microwave Channels

Either duplex or half-duplex channels may be provided by microwave radio equipment, which typically provides multiple channels by means of multiplexing techniques.

4.2.4 Optical Fiber Channels

Duplex (i.e., two simplex) or half-duplex optical fiber channels may be used with any suitable signalling scheme to provide serial binary data transmission. These channels provide exceptional immunity to interference from unrelated electrical or optical signals and can operate at considerably higher data rates than voice-grade cable channels.

4.2.5 Miscellaneous Channels

Free-space optical, power-line carrier, hybrid combinations of the above, and other specialized channel types, may be used to provide data transfer capabilities equivalent to the channels in 4.2.1 to 4.2.4.

5. Channel Interfaces

This section deals with

1) The physical and electrical connections between the logic equipment of SCADA master and remote terminals and the communication channels defined in Section 4.; and
2) The procedures for control of operation of these channels

5.1 General

Conversion of the electrical signals used by SCADA master and remote terminals to present serial binary data to the signalling format used by the associated communication channel(s) is performed by Data Circuit Terminating Equipment (DCE). The DCE for operation of voice-grade analog channels is commonly referred to as a “modem.” Additional DCE functions should include

1) Electric isolation or neutralization between the remote or master terminal and the communication channel [10].
2) Detection of channel busy and idle states.
3) Detection of degraded signal quality.

SCADA terminals may be arranged either with integral or external DCE. The interface between the terminal equipment and the DCE should meet the requirements of 5.3, and the DCE to channel interface should meet the requirements of 5.4. The procedures for control of the operation of the various types of communication channels are presented in 5.5.

5.2 Data Rates

Master and remote terminals should include a provision for the selection of an operation at any of the following standard data rates:

 Copyright © 1993 IEEE All Rights Reserved

1) 600 b/s
2) 1200 b/s
3) 2400 b/s
4) 4800 b/s

Data rates of 75 b/s, 150 b/s, or 300 b/s may also be used if required for special applications, such as the use of frequency division-multiplex or power-line carrier channels. These lower data rates necessarily limit the SCADA system response times and throughput; their use should be minimized. Operation at 9600 b/s may be used to support large-capacity remote terminals in point-to-point channel configurations. If dedicated fiber optic channels are used, extremely high data rates can be accommodated.

All remote terminals connected to a party line (multipoint) communication channel shall operate at a common data rate. Master terminals that are equipped with multiple channel interfaces should include a provision for the independent selection of the data rate for each such interface.

5.3 Terminal-to-DCE Interface

The interface between a master or remote terminal and its associated DCE should, for stand-alone DCE, meet the signalling, connector, and electrical specifications of EIA-RS-423-A [5], EIA-422-A [4], EIA-449 [6], and CCITT Recommendations V.24 and V.28 [3]. All signal circuits designated as Category 1 in EIA-449 [6] should be implemented as a minimum and should use unbalanced signalling as defined in EIA-423-A [5]. These definitions permit operation, if necessary, with DCE interfaces that only meet the superseded EIA-RS-232C specification.[5]

5.4 DCE-to-Channel Interfaces

The interface between the DCE and the communication channel is currently defined only for voice-grade analog signalling as typically used with cable and radio channels. Corresponding definitions for operation of optical fiber channels will be added to this recommended practice when suitable standards for such channels become available. Channel interfaces for other types of channels, e.g., power-line carrier, are not defined, as these are implementation-specific. Voice-grade channel transmission characteristics are required to be at least equal to those specified for unconditioned voice-grade channels.

The DCE (i.e., modem) to voice-grade channel interface should meet the following specifications:

(1) Terminal Arrangement:	Two-wire or four-wire, selectable
(2) Termination Impedance:	600 Ω ± 10%, isolated and balanced
(3) Transmit Level:	0 dBm nominal, adjustable to −12 dBm in at most 4 dB steps
(4) Receive Level Range:	0 to −30 dBm without adjustment
(5) Modulation Polarity:	Per CCITT Recommendation V.1 [3]
(6) Signalling Standards:	Per CCITT Recommendations:
600 b/s:	CCITT Recommendation V.23 [3] Mode 2 of Section 2.
1200 b/s:	CCITT Recommendation V.23 [3] Mode 2 of Section 2.
2400 b/s:	CCITT Recommendation V.26 [3] Alternative 2 of Section 2.3
4800 b/s:	CCITT Recommendation V.27 bis [3]

[5]Operation of such a DCE requires the use of interface adapters as described in the *EIA Industrial Electronics Bulletin*, Number 12, dated November 1977.

Copyright © 1993 IEEE All Rights Reserved

All CCITT Recommendation V.26 and V.27 modems connected to any one communication channel shall use identical combinations of the various options permitted by these CCITT Recommendations, e.g., CCITT Recommendation V.26 data coding, CCITT Recommendation V.27 turn-on sequence timing, etc. Two modems, when interconnected by a communication channel equivalent to an unconditioned voice-grade channel, should provide an end-to-end random bit error rate of less than 1 in 10^4 b.[6] This performance, in conjunction with the security code and the limited message length defined in Section 6., ensures that the probability of acceptance of messages received in error will be less than 1 in 10^{10}, as specified in the IEEE Std C37.1-1987 [7].

All transmitters shall generate the selected data rate within a tolerance of ± 0.01% in accordance with CCITT Recommendations V.26 and V.27 bis [5] for the two higher data rates above. This data rate tolerance also ensures adequate bit synchronization accuracy for the longest permitted messages when using asynchronous modems at the two lower data rates.

5.5 Channel Control

5.5.1 General

DCE transmitters and receivers should be operated as described in the following subsections for each communication channel configuration. Each transmitter and receiver may assume either of two states, “quiescent” and “active,” which are defined as follows:

Transmitter:	Quiescent if:	Request to Send and Ready for Sending are inactive.
	Active if:	Request to Send or Ready for Sending is active.
Receiver:	Quiescent if:	Received Line Signal Detector is inactive.
	Active if:	Received Line Signal Detector is active.

Each DCE receiver should be arranged to clamp its Received Data output signal to logic “1” while quiescent. Each DCE Transmitted Data input signal should be set at logic “1” except when the terminal is transmitting a message.

Each DCE transmitter should transmit a preconditioning or synchronizing line signal following activation of its Request to Send control signal before activating its Ready for Sending status signal. On external deactivation of the Request to Send input signal, the DCE has to complete transmission of any previously delivered Transmitted Data bits before deactivating its Ready for Sending output signal. The DCE should not respond to a reactivation of its Request to Send signal until any such transmission is completed. Timers within the master or remote terminal (see 5.6) have to accommodate DCE (e.g., modem) delays.

Asynchronous modems in cable channels transmit a preconditioning line signal that consists of a series of logic “1” bits for a minimum time interval of 8 ms (See Table 1). Synchronous modems in cable channels transmit a synchronizing line signal in accordance with the CCITT V Series Recommendations.

[6]The user shall ensure that the communication channel and modems selected for use with this recommended practice provide an end-to-end random bit error rate less than this value.

 Copyright © 1993 IEEE All Rights Reserved

Table 1— Typical DCE (Modem) Response Times

Channel Rate (b/s)	Preconditioning Time (ms)	Turn-Off Time (ms)	Remarks
75–1200	8	2	Two- or four-wire channel
2400	30	10	Two- or four-wire channel
4800	50	25	Four-wire channel
9600	TBS	TBS	Four-wire channel

NOTE — These values reflect minimum times from the CCITT V Series Recommendations [3].
TBS—to be specified.

All master and remote terminals should incorporate provision for extending these preconditioning or synchronizing time intervals, where operation over radio channels is required, to cover the radio receiver carrier detector "squelch" response times, which may be as large as 0.5 s.

Three types of channels are used:

1) Duplex point-to-point channels
2) Duplex party-line channels
3) Half-duplex channels

5.5.2 Duplex Point-to-Point Channels

For this type of channel, the DCE Request to Send signals at both terminals are activated continuously. The DCE transmitters and receivers are both continuously active while the channel is operational, thereby eliminating DCE response time delays.

5.5.3 Duplex Party-Line Channels

The master terminal DCE Request to Send signal is operated as described in 5.5.2. The corresponding signal at any remote terminal is activated only when that terminal responds to a preceding master terminal message and is deactivated immediately following completion of transmission of the response message. A DCE response time delay is encountered at the remote terminal.

5.5.4 Half-Duplex Channels

The DCE Request to Send signals are activated only when the associated terminal initiates transmission of a message and are deactivated immediately on completion of each message transmission. DCE response-time delays are encountered at both master and remote terminals.

5.5.5 Additional DCE Facilities

Remote terminal DCE equipment operating in party-line communication channels should be equipped with means to monitor the length of their output transmissions and to deactivate their DCE transmitter if an excessive length occurs, presumably due to an equipment failure. This feature, commonly known as "anti-streaming protection," minimizes the probability that a failure in one remote terminal will disable communication with other remote terminals that share the channel.

The DCE may also be equipped with means to monitor the quality of the received line signal and to report to the associated terminal when degraded signal conditions occur.

Copyright © 1993 IEEE All Rights Reserved

5.6 Message Transfer Control

5.6.1 Terminal States and State Transitions

The master and remote terminal communication message transfer control equipment, commonly referred to as the Data Terminal Equipment (DTE), operates in one of four mutually exclusive states that are independent of, but related to, the DCE states defined above. The master and/or remote may manage multiple DTEs on multiple channels simultaneously. These DTE states are

Quiescent: The message transmission and reception logic is deactivated or reset or off. Processing of a previously received message may be in progress.

Inactive Receive: The reception logic is awaiting the arrival of an expected message and the transmission logic is deactivated.

Active Receive: The reception logic is receiving a message and the transmission logic is deactivated.

Transmit: The reception logic is deactivated and the transmission logic is controlling the transmission of a message.

Fig 1 illustrates, for both master and remote terminals, the permitted transitions between these DTE states and summarizes their initiating conditions. The DTE activities surrounding each transition depend on the terminal type (master or remote) and the communication channel configuration.

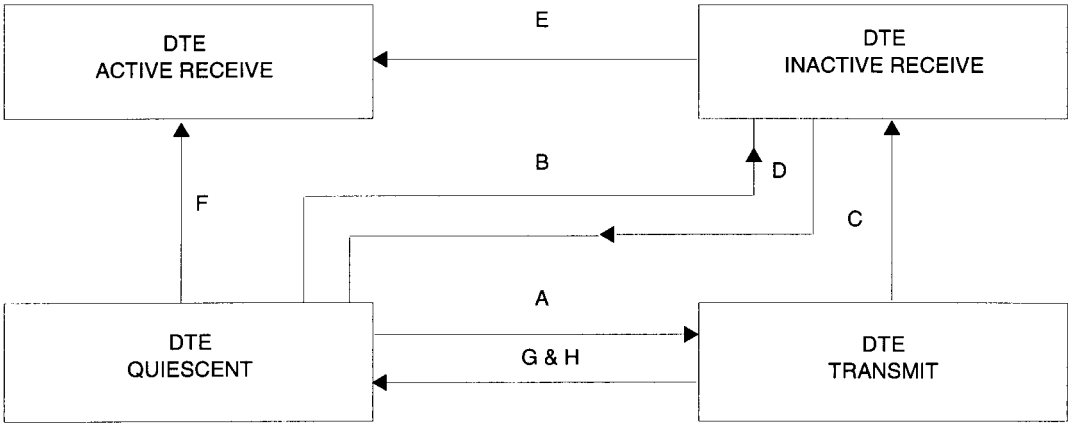
5.6.1.1 Transition A

Terminals in half-duplex channels, and remote terminals in duplex party-line channels, activate the DCE Request to Send signal when their DCE receiver is quiescent and an output message is ready for transmission. All terminals in all channel configurations then transfer the pending message(s) to the DCE Transmitted Data serial input after detection by the DTE of an active DCE Ready for Sending output.

5.6.1.2 Transition B

A remote terminal in any channel configuration performs this transition following receipt and interpretation of any message that does not require a response by that remote terminal or when leaving the reset condition.

 Copyright © 1993 IEEE All Rights Reserved



Transition	Initiating Condition	Applicable Terminal	
		Master	Remote
A	Ouput message(s) ready for transmission	X	X
B	Input message(s) expected		X
C	Output message(s) transmission complete and input message(s) expected	X	X
D	No-Response timer expired	X	
E	Message start detected “110”	X	X
F	Input message(s) complete	X	X
G	Output message(s) transmission complete and deactivate command received		X
H	Output message(s) transmission complete and no response expected	X	

Figure 1— DTE State Diagram

NOTE — For all terminals, Reset (off/on) immediately triggers the quiescent state.

5.6.1.3 Transition C

Master terminals perform this transition following completion of transmission of any message that requests a response. All remote terminals perform this transition following completion of transmission of any response message, except the response associated with the deactivate command. Completion of message transmission is defined as the delivery of the last data bit of a message to the DCE for master terminals in duplex channels and for remote terminals in duplex point-to-point channels. For all other channel configurations, completion of message transmission is defined as the DCE transmitter lowering the Ready for Sending after the DTE deactivates the Request to Send signal.

Copyright © 1993 IEEE All Rights Reserved

5.6.1.4 Transition D

Master terminals perform this transition when an expected response to a previous message has not been received within a preset time limit.

5.6.1.5 Transition E

All terminals perform this transition with the first transition of the DCE Received Data output signal to logic “0” after the receipt of at least 2 b at logic ”1.”

5.6.1.6 Transition F

All terminals perform this transition when a message of the expected length has been received.

5.6.1.7 Transition G

Remote terminals perform this transition under the conditions defined in 8.5.3.

5.6.1.8 Transition H

Master terminals perform this transition when no further output messages are pending following transmission of a “broadcast command” (see 6.2.2).

5.6.2 Quiescent State Timing Considerations

The timing of the DTE quiescent state is subject to the following constraints:

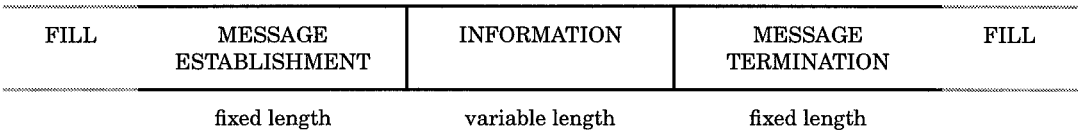
1) Remote terminals operating in duplex channels shall be capable of servicing any master terminal broadcast command message within the time required to receive the Message End Subfield because the master terminal can follow the broadcast message with another message (see 6.4.2). This requirement defines the maximum time available for the remote DTE quiescent state under such conditions.
2) The maximum time required by a remote terminal to prepare a response message implicitly defines the time interval value for the master terminal “No-Response” detector. Efficient operation of the communication channel requires that this value be minimized. All remote terminals operating in duplex channels should be capable of completing preparation, while in the DTE quiescent state, of a response message in no more than 10 ms.
3) Operation of half-duplex channels is defined in 5.6.1 to ensure that all connected DCE receivers reach their quiescent state between messages. This requires that the DTE quiescent state for both master and remote terminals in such channels should be maintained for a minimum of 4 ms with asynchronous modems and 10 ms with synchronous modems. If the DCE receiver remains active, a failure condition on such channels, the remote terminal will remain in the quiescent state.

6. Communication Message Format

This section deals with the basic structure and content of the messages to be transferred between SCADA master and remote terminals via their communication channels.

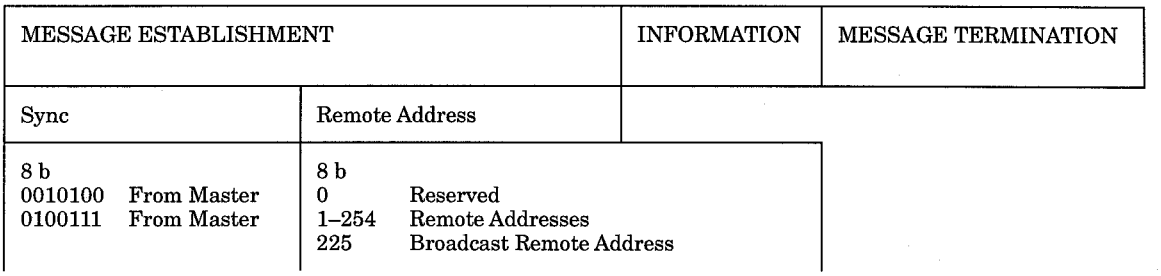
 Copyright © 1993 IEEE All Rights Reserved

6.1 General



The communication channels between master and remote terminals are used to transfer serial binary data messages, each of which consists of three basic fields, respectively; "Message Establishment," "Information," and "Message Termination." The Message Establishment and Message Termination fields have fixed lengths and the Information field a variable length as specified below. Communication management procedures ensure that each receiving terminal is automatically preset for the length of the transmitted Information field.

6.2 Message Establishment Field



This Message Establishment field consists of two subfields, respectively; "Sync" (Synchronizing), and "Remote Address."

6.2.1 Sync Definitions

The Sync subfield consists of 8 b with the following values and with the leftmost bit transmitted first:

Master Terminal Transmissions:	Sync = 00010100
Remote Terminal Transmissions:	Sync = 00100111

Received messages having valid Sync and Security Code (see 6.4) subfields are accepted and interpreted appropriately. All other received messages are ignored. The Sync subfield values enable the remote terminal logic to distinguish between master and remote terminal messages when operating on a party-line communication channel. These Sync subfields both require at least 4 b errors to cause synchronizing errors (known as "sync slip") to convert one into the other. The receiving terminal should, after a user-adjustable interval, reinitiate its search for a sync bit pattern if the received bits do not match the expected pattern following a "110" transition. ["110" defines the start of a message—"11" being the Message End Subfield (see 6.3.2) and "0" being the first bit of a new Sync field.]

6.2.2 Remote Address Definitions

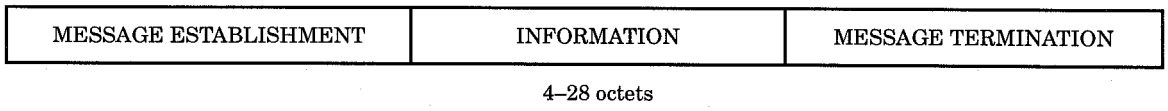
The Remote Address subfield consists of eight binary bits, with the most significant bit transmitted first. Remote terminals should each be assigned a unique address for each channel in the range 1 to 254_{10} and service only those

Copyright © 1993 IEEE All Rights Reserved

master terminal messages which contain either that address or address 255_{10}. The latter is used for "broadcast" commands that all remote terminals accept but to which they do not reply. Remote Address 0 is reserved for future use. Remote terminal response messages include their unique address to allow the master terminal to check that the correct remote terminal is responding.

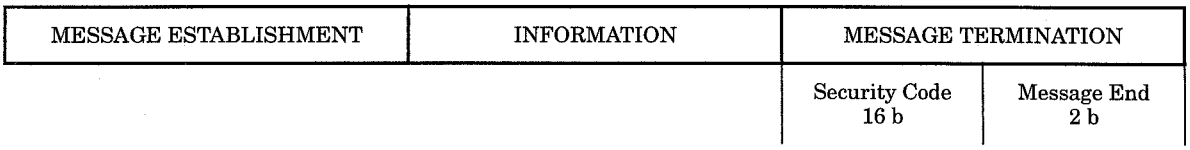
Each communication channel can thus support up to 254 remote terminals. When needed, larger numbers of remote terminals may be supported either by use of multiple channels or by extending the Remote Address subfield with the first bits of the Function Code subfield, which is defined in Section 8.

6.3 Information Field



The Information field consists of 4 or 28 octets for master to remote messages. Remote to master messages may use 4–28 information octets in response to master station requests. Usage of this subfield is described in Section 7.

6.4 Message Termination Field



The Message Termination field consists of two subfields; a 16 b Security Code subfield and a 2 b Message End subfield.

6.4.1 Security Code Subfield

The Security Code used is the (255, 239) Bose-Chaudhuri-Hocquenghem (BCH) code, which is calculated over all preceding message bits with the exception of the first bit, (0), of the 8 b Sync fields. The generator polynomial for the (255, 239) BCH code is:

$$(x^{16} + x^{14} + x^{13} + x^{11} + x^{10} + x^9 + x^8 + x^6 + x^5 + x + 1) \quad (1)$$

The calculated BCH code subfield is logically complemented prior to transmission and again on reception. This process improves the rejection of messages subjected to sync slip.

The maximum-length Information field utilizes the full range of the Security Code (7 Sync subfield + 8 Remote Address subfield + 28×8 Information field), a total of 239 b. The error detection capabilities of the code ensure that the probability of undetected error in a maximum-length message will be about 1×10^{-10} for a communication link bit error rate of 1×10^{-4} as specified in 5.4.

 Copyright © 1993 IEEE All Rights Reserved

6.4.2 Message End Subfield

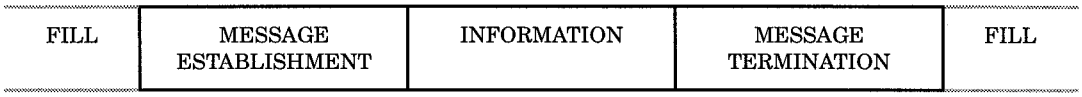
The transmitted Message End subfield consists of at least 2 b at logic “1” to provide a minimum time interval between completion of transmission of the Security Code and termination of transmission. Received messages that satisfy all other format and security checks are accepted irrespective of the received Message End subfield value.

The Message End subfield of any master terminal message that requires no reply from the receiving remote terminal(s) may be followed immediately with the Sync subfield of the next master terminal message, without intervening fill bits, subject to the limitation discussed in 5.6.2. Upon request from the master terminal, a remote terminal may chain a defined set of messages to the master without intervening fill bits.

6.5 Message Format Summary

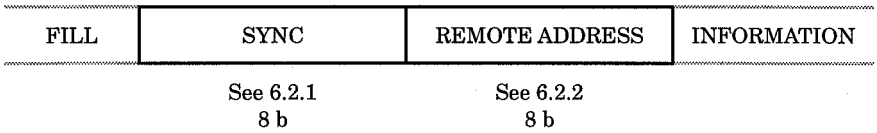
6.5.1 Basic Message Structure

Total length 66 b minimum and 258 b maximum.



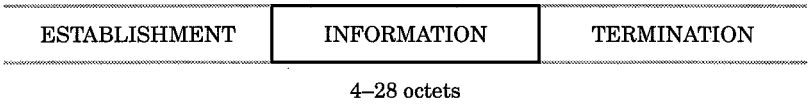
6.5.2 Message Establishment Field

(See 6.2)



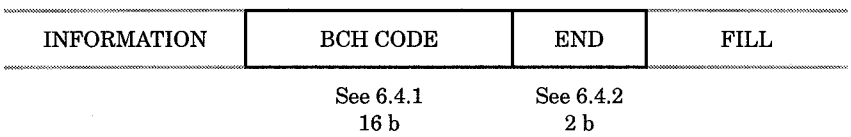
6.5.3 Information Field

(Usage described in Section 7.)



6.5.4 Message Termination Field

(See 6.4)



Copyright © 1993 IEEE All Rights Reserved

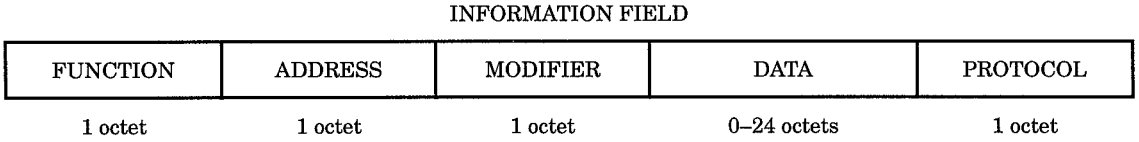
7. Information Field Usage

This section defines the internal formats of the Information field of all messages and the message transaction sequences to be used to transfer information between master and remote terminals.

7.1 Information Field Formats

7.1.1 Master-to-Remote Terminal (M-R) Messages

(M-R) message information fields are arranged as follows:



These subfields are used as follows:

FUNCTION: This octet, which is transmitted first, specifies one of up to 256 predefined data transfer or control message types to be transferred in the response from the remote terminal.

ADDRESS: This octet specifies the internal location of one of up to 256 Data Units for the specified data transfer or control message type.

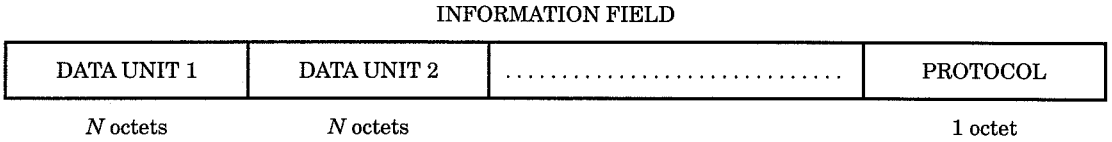
MODIFIER: This octet defines the total number of data octets, or optionally, the total number of Data Units, to be transferred. In either case, Data Units following that defined by the Address octet are identified by successively incrementing the latter until the complete message is assembled.

DATA: This subfield provides for transfer of up to 24 octets of generalized data to the remote terminal.

PROTOCOL: The usage of this octet is defined in 7.2.2.

7.1.2 Remote-to-Master Terminal (R-M) Messages

(R-M) message information fields are arranged as follows:



 Copyright © 1993 IEEE All Rights Reserved

These subfields are used as follows:

DATA UNIT: Data Unit subfields consist of any convenient number of octets that collectively total at least 3 and no more than 27 octets.

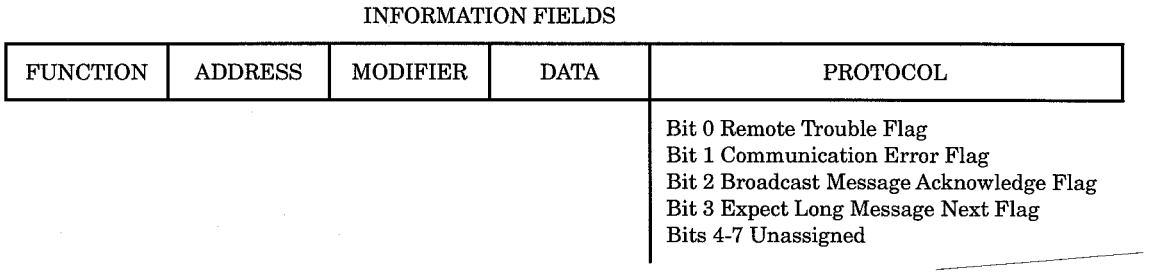
PROTOCOL: The usage of this octet is defined in 7.2.1.

7.2 Protocol Octet Functions

These octets are used for routine transfer of up to 8 b of protocol information between the master terminal and the remote terminal. The remote terminal provides, in each response message, a group of 8 flags that summarize its current operating condition. The master terminal uses its protocol octet to acknowledge receipt of certain of these flags, as described in the following subsections. The master terminal may obtain more detailed information on the reasons for setting these flags using standard data acquisition transactions.

Bits in the protocol octets are numbered sequentially from left to right, i.e., Bit 0 is transmitted first.

7.2.1 Remote Terminal Protocol Octet



The remote terminal should support operation of the following status flags. The master terminal is expected to request supplemental information prior to resetting any flag in the Remote Terminal Protocol Octet.

Bit 0: *Remote Trouble Flag* (reset by the master terminal only). Activation of this flag bit indicates that the remote terminal has either executed a restart or has detected a hardware problem since this flag was previously reset by the master terminal. Remote terminals should restart in the event of

- Interruption of power
- Receipt of a master terminal command to restart
- Receipt of a local manual reset command
- Self-diagnostic reset

Hardware problems may include pending overflow of data buffers or detection by diagnostic procedures that a hardware subsystem is not operating satisfactorily, e.g.,

- Sequence of Events buffer 75% full
- Analog Report by Exception buffer 75% full
- Analog Inputs function check failure
- Control Outputs function check failure

Bit 1: *Communication Error Flag* (reset by the master terminal only). Activation of this flag bit indicates that the remote terminal has detected a communication-oriented problem since this flag was previously reset by the master terminal, e.g.,

- Communication channel signal quality degradation

Copyright © 1993 IEEE All Rights Reserved

Bit 2: *Broadcast Message Acknowledge Flag* (reset by the master terminal only). Activation of this flag bit indicates that the remote terminal has received and executed a broadcast command since this flag was previously reset by the master terminal. Typical uses of this feature include the receipt of

- Analog Freeze command
- Accumulator Freeze command
- Time Synchronization command

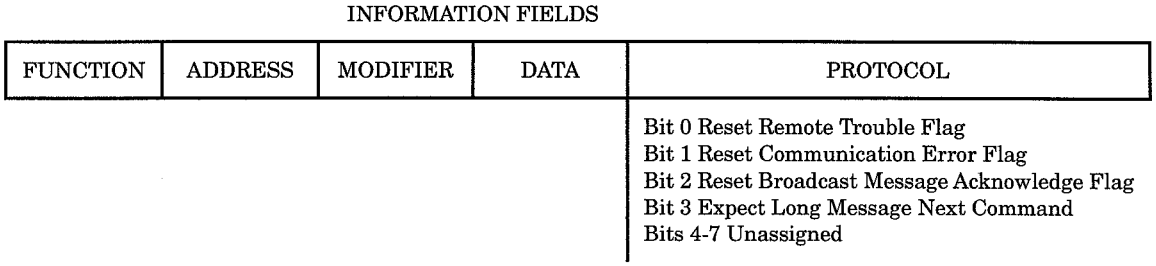
The master terminal is responsible for the proper interpretation of this flag.

Bit 3: *Expect Long Message Next Flag* (set and reset by the remote terminal only). Activation of this flag bit indicates that the remote terminal is expecting a long master-to-remote message. The use of this flag is further defined in 8.5.2.

Bits 4–7: *Unassigned.* These bits may be used individually or collectively to implement up to 15 conditions such as

- Exception data (analog or status) present that has not yet been transferred to the master station.
- Analog Scan Request Flag used to indicate that a total analog scan should be requested.
- Unsolicited Data Flag used to indicate the presence of Sequence of Events data, operator entry data, disturbance data, etc.

7.2.2 Master Terminal Protocol Octet



This octet in each master-to-remote message should be used to command certain actions by the remote terminal. As a minimum, the following four single-bit command functions should be supported.

Bit 0: *Reset Remote Trouble Flag* (set by the master terminal only). Activation of this flag acknowledges receipt by the master terminal of the restart or trouble condition at the remote terminal. The master terminal should reset this flag when the Remote Trouble Flag is reset by the remote.

Bit 1: *Reset Communication Error Flag* (set by the master terminal only). Activation of this flag acknowledges receipt by the master terminal of the communication error condition at the remote terminal. The master terminal should reset this flag when the Communication Error Flag is reset by the remote.

Bit 2: *Reset Broadcast Message Acknowledge Flag* (set by the master terminal only). Activation of this flag acknowledges receipt by the master terminal of the broadcast message acknowledge from the remote terminal. The master terminal should reset this flag when the Broadcast Message Acknowledge Flag is reset by the remote.

Bit 3: *Expect Long Message Next Command* (set by the master terminal only). Activation of this flag bit indicates that the next master-to-remote message will be a long message. The use of this flag is further defined in 8.5.2.

Bits 4–7: *Unassigned.* These bits may optionally be used either individually as additional single-bit commands or collectively to permit implementation of up to 15 coded commands.

 Copyright © 1993 IEEE All Rights Reserved

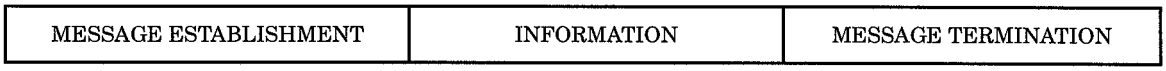
7.3 Transaction Types

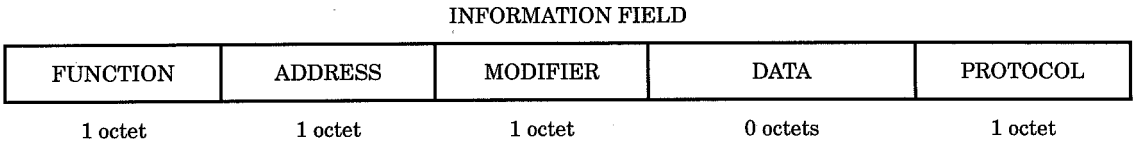
A transaction is an uninterruptible sequence of messages between a master and a remote terminal to complete the transfer of one block of data between the terminals. Three transaction types are currently defined in the following subsections.

7.3.1 Type 1

This transaction type consists of one short (M-R) message that contains Function, Address, and Modifier octets, i.e., a maximum of three “data” octets, together with the protocol octet.

TYPE 1



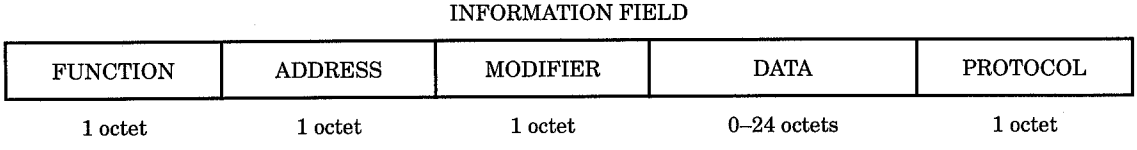


7.3.2 Type 2

This transaction type nominally consists of one (M-R) message followed by one (R-M) message between a master terminal and a specific remote terminal. It is used to transfer up to 27 octets of data between the terminals. This transaction sequence may be extended, when necessary, by retries as described in 8.2.3 and 8.4.

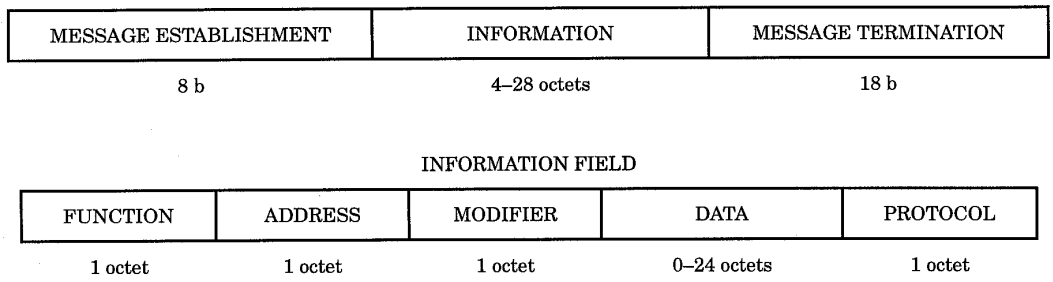
TYPE 2

COMMAND—Master to Remote



Copyright © 1993 IEEE All Rights Reserved

RESPONSE—Remote to Master

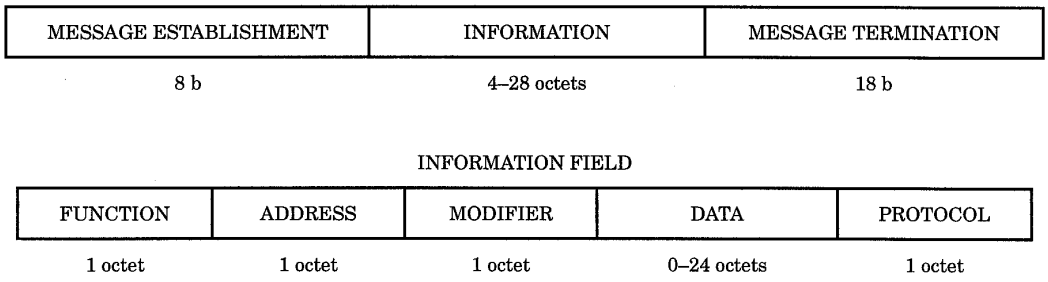


7.3.3 Type 3

This “Select, Check, Execute” transaction type nominally consists of two consecutive Type 2 transactions. It is used to transfer up to 27 octets of data from a master to a specific remote terminal with the highest possible level of immunity to transfer errors. The first master terminal message (“Select”) transfers the data to the addressed remote terminal, which temporarily stores the received data and retransmits it (“Check”) to the master terminal for verification. If the data contained in this first remote terminal message is found to be identical to that previously transmitted, the second master terminal message (“Execute”) instructs the remote terminal to make use of the data previously stored. Valid receipt of the Execute message initiates the second remote terminal message (“Execute Acknowledge”) confirming data acceptance. The Execute message should follow valid receipt of the Check message without interruption by any unrelated master terminal message(s). However, if the data contained in the Check message is incorrect, the Select message should be repeated.

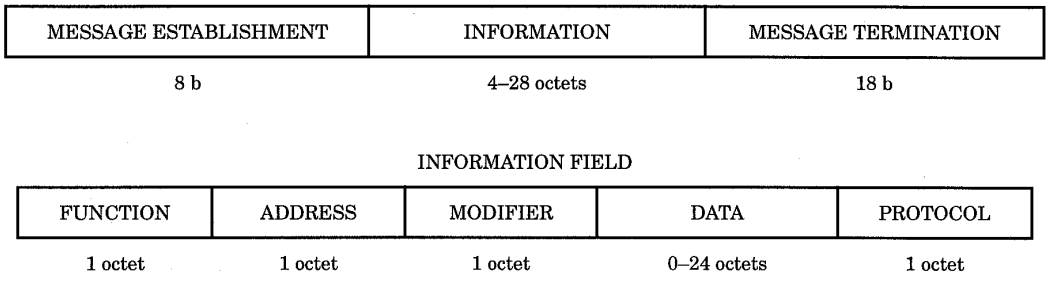
TYPE 3: Select, Checkback, Execute, Execute Acknowledge

SELECT—Master to Remote



CHECKBACK—Remote to Master (similar to Select)

EXECUTE—Master to Remove



EXECUTE ACKNOWLEDGE—Remote to Master (similar to Execute)

 Copyright © 1993 IEEE All Rights Reserved

Select message data stored by the remote terminal should preferably be reassembled by mechanisms that are independent of that involved in the internal transfer to storage so that the master terminal data validation process can detect any errors that may have occurred in the remote terminal data storage and transfer equipment.

7.4 Remote-to-Master Data Transfer

Remote-to-master data transfer uses the Type 2 transaction defined in 7.3. The master terminal message contains the standard 4-octet Information field, as defined in 7.1.1 above.

Each Data Unit may contain any number of octets, but the complete remote terminal message shall contain at least 3, and no more than 27, data octets together with the Remote Terminal Protocol octet defined in 7.2.1. The effective internal address of each transferred Data Unit is implied by its position in the message.

Data types that may be acquired by the master terminal using this procedure include

1) Current condition of binary (status) inputs to the remote terminal.
2) Current values of analog inputs to the remote terminal.
3) Values of analog, binary, or other inputs previously stored at the remote terminal in response to a master terminal “Store Data Type (N)” command. This is commonly referred to as “Data Snapshot Reporting” and is used to minimize time skew between measurements made at multiple remote terminals.
4) Values of analog, binary, or other inputs that have changed significantly since last reported. This is commonly referred to as “Data by Exception Reporting” and is used to minimize the total volume of data to be transferred to the master terminal. Each Data Unit in this case includes both the new value and an identification of its internal address.
5) Sequence of Events Data. Each Data Unit of this type of data contains the internal address identification of a binary input that has changed state since previously reported, a flag defining its new state, and data indicating the time at which the remote terminal detected the state change.
6) Values of accumulators, e.g., input contact cycle counters, which may either be their current values or values previously stored in the remote terminal in response to master terminal or local “Accumulator Freeze” commands.
7) Data values calculated and stored within the remote terminal from combinations of its external inputs.
8) Data values previously transferred to the remote terminal from the master terminal that are being requested for verification purposes.
9) Data values obtained from remote terminal internal diagnostic processes that provide information on the operational performance of the various remote terminal subsystems.

Both Sequence of Events and Data by Exception Reporting involve the transfer of an unknown volume of data to the master terminal. Each master terminal request for the transfer of these data types therefore specifies the transfer of 27 data octets. These requests are normally repeated until the corresponding protocol octet flags are reset by the remote terminal. Unused data octets are set to zero in the last message of a set of these data transfer transactions.

For Data by Exception reporting of analog values, the difference between the current measured value and the value previously reported to the master terminal for each analog input point is compared with a change limit for that point, which is stored at the remote terminal. When this deadband limit is exceeded, the new input signal value and its address identification are added to a table stored for transfer to the master terminal. The new value is then used as the reference value for subsequent tests for significant input signal change.

7.5 Master-to-Remote Data Transfer

Five categories of master-to-remote data transfers are available that use the various transaction types defined in 7.3. They are defined in the following subsections.

Copyright © 1993 IEEE All Rights Reserved

7.5.1 Uncritical Command

This category transfers one or two octets of uncritical data using the Type 1 transaction. It is normally used to deliver simple commands such as “Accumulator Freeze” either to a specific remote terminal or to all remote terminals connected to a party-line communication channel using the “Broadcast” Remote Address 255_{10}.

The Address and Modifier octets are used to convey the required data. The master terminal is responsible for recovery from failure of any remote terminal to accept such commands.

7.5.2 Short Command

This category transfers one or two octets of data using the Type 2 transaction, each message of which contains the standard 4-octet Information field. The remote terminal message Function, Address, and Modifier octets nominally copy the corresponding master terminal message octets.

This category may be used where ultimate data security is unnecessary but where evidence of acceptance by the remote terminal is required, e.g., loading limited quantities of data into operator displays and recorders. The Address and Modifier octets are used to convey the required data.

7.5.3 Long Command

This category transfers 24 octets of data using the Type 2 transaction, in which the master and remote terminal messages contain a 28-octet and a 4-octet Information field, respectively. The remote terminal message Function, Address, and Modifier octets nominally copy the corresponding master terminal message octets.

This category is used for similar applications to those using the Short Command but that require larger volumes of data, e.g., operation of a printer.

7.5.4 Control Command

This category transfers one or two octets of data using the Type 3 transaction, each message of which contains the standard 4-octet Information field. The remote terminal message Function, Address, and Modifier octets nominally copy the corresponding master terminal message octets.

This category is primarily used to provide ultimate security for control of devices external to the remote terminal. The Function octet defines the type of device to be activated or control action to be performed, the Address octet defines the internal address of the specific device, and the Modifier octet provides up to 8 additional data bits if needed. The Function octet values in the Select and Execute commands should differ for highest security. Devices that require between 9 and 16 data bits may be accommodated using the Modifier octets of the Select and Execute messages for the higher- and lower-significance data octets, respectively.

7.5.5 Batch Data Transfer

This category transfers up to 24 octets of data using the Type 3 transaction, each message of which contains the extended 28-octet Information field. The remote terminal message Information fields nominally copy those of the master terminal messages, except for the protocol octets.

Batch data transfer applications include

1) Operating schedules for locally-controlled devices
   a) Voltage/VAR control
   b) Time-oriented activities
2) Contingency sequences for locally controlled devices
   a) Blackout configuration

 Copyright © 1993 IEEE All Rights Reserved

   b) Restoration sequences
3) Parameters for report by exception
   a) Dead band
   b) Alarm limits
   c) Rate of change limits
4) Parameters for internal data processing procedures

8. Communication Management

This section defines the procedures to be used by the master and remote terminals to manage operation of their communication channels.

8.1 General

Operation of dedicated communication channels between master and remote terminals is based on the following principles. These principles may be modified for dial-up telephone networks or dc signalling applications.

1) All terminals connected to one communication channel will use a common data rate and the message formats of this recommended practice only.
2) Remote terminals will transmit only in immediate response to receipt of a valid master terminal message that authorizes such transmission.
3) Master terminal messages will use the standard format defined in Section 6. with either 4 or 28 octets in the Information field.
4) Each remote terminal response transmission will consist of one or more messages with the standard format defined in Section 6. and with any integral number from 4 to 28 octets in the Information field.
5) The master terminal, by requesting a specific response, will be aware of the required number of octets in the remote terminal response, and the master terminal reception logic will be preset to expect that number.
6) Remote terminal reception logic will normally be preset to expect 4 octets in the Information field of master terminal messages. Special command procedures will be used to preset the remote terminal reception logic for master terminal messages containing 28 octets.
7) Master and remote terminals will be distinguished functionally by these rules. However, one subsystem may be arranged, if needed, to behave both as a master and as a remote terminal on different channels or at different times on one channel.

8.2 Master Terminal Channel Control Functions

In addition to supporting the basic communication functions listed in 7.1, the master terminal is required to provide the following channel management functions. In this section, parameters labelled “user alterable” are required to be readily adjustable to permit user tuning of the communication facilities. The system supplier is expected to provide default values for these parameters to support initial field operation.

8.2.1 Message Priorities

The capability to manage the transmissions on each channel based on relative priorities assigned by nonprotocol processes to waiting messages should be supported. The capability to assign different priorities to the various message functional types (e.g., status versus analog data acquisition) should be supported. A priority order based on remote terminal address should be supported for party line remotes. The assignment of priorities should be user alterable.

Copyright © 1993 IEEE All Rights Reserved

8.2.2 Message Queuing

The capability to manage a queue of messages waiting for access to each channel should be supported. The size of each queue shall be user alterable. The capability to establish alarm thresholds indicating imminent queue overflow and excessive queuing time for each queue should be supported. The values of the alarm thresholds should be user alterable.

8.2.3 Message Retransmission

When any master terminal message requiring a response is transmitted, a “No-Response” timer should be started and subsequently reset on receipt of the response. If the user-alterable time-out value is exceeded, the previous master terminal message may be retransmitted. The capability for user-alterable assignment of the permitted maximum number of retries for each message functional type should be supported. Some message types may not require any retries.

8.2.4 Communication Performance

The capability to alarm channels as inoperative or marginal should be supported. The criteria for declaring a channel inoperative or marginal should be user-alterable and be based on measured channel quality parameters and/or error statistics. As a minimum, an error count should be accumulated for a user-defined message count to alarm a channel as inoperative or marginal when the error count exceeds a useralterable limit.

Channel quality parameters may include signal-to-noise ratio, carrier level, etc., which are monitored by communication equipment. Rejection of messages by remote or master terminals may be due to conditions such as a low quality channel, marginal modems, or terminal equipment failure.

8.3 Multiple Channels

8.3.1 Master Terminal

Master terminals should be capable of supporting concurrent and independent operation of multiple communication channels with arbitrary combinations of standard data rates and channel types; e.g., duplex, half-duplex, party line, etc.

8.3.2 Redundant Channels

The use of redundant communication channels should be supported by master and remote terminals to permit improvement, where desired, in the effective channel availability.

The master terminal should be arranged to transmit messages alternately on both channels of an operational redundant pair. The remote terminals should monitor both channels for receipt of valid master terminal messages and transmit necessary responses only on the channel from which each such message is received.

When the master terminal declares one of the two channels of a pair to be inoperative or marginal, it should discontinue its use, issue an appropriate alarm to the local operator, and transmit all subsequent messages on the remaining channel pending repair of the failed channel.

The effective availability of nonredundant channels can also be improved by equipping the master and remote terminals with access to the public switched network via suitable automatic dialers and extended channel-control support procedures. Such extensions should be arranged to permit normal operation of the procedures of this recommended practice following the establishment of the public network link.

 Copyright © 1993 IEEE All Rights Reserved

8.3.3 Multiple Master Terminals

A SCADA system may incorporate more than one master terminal either to obtain improved system reliability or to permit data acquisition and control from more than one geographical location. Such systems may be configured either with multiple independent communication channels to each remote terminal or with each communication channel shared by all master terminals.

In shared communication channel configurations, the master terminals should include suitable procedures to eliminate mutual contention for access to the channels. These procedures should be based on the principle that each connected master terminal monitors channel activity, for example, by operating as a remote terminal except when authorized directly or by default to assume the master terminal role. The operation of system configurations that employ multiple independent communication channels to each remote terminal is beyond the scope of this recommended practice.

8.4 Repeat Last Message

In order to minimize the possibility of loss of data (due to communication channel noise) that had been stored (e.g., device status) at a remote terminal prior to its transmission, both master and remote terminals should support a “Repeat Last Message” function. The Information field of every message transmitted by a remote terminal should be stored in a suitable local buffer. When the master terminal receives an invalid message, it may immediately request the relevant remote terminal to retransmit its preceding response in whole or in part. This procedure can be repeated as necessary until the original data is correctly received at the master terminal or the latter declares the remote terminal inoperative.

8.5 Message Length Control

8.5.1 General

The exceptionally high degree of immunity to transmission errors provided by the 16 b Security Code used is only obtained when the receiving terminal reception logic is correctly preset to the length of the transmitted message. Otherwise, the probability of erroneous acceptance of a message is relatively high, 1 in $2.^{16}$.

8.5.2 Basic Length Control Procedures

Master terminal reception logic is preset to the expected length of the remote terminal response message when each master terminal message is transmitted. Remote terminals normally expect to receive the standard short master terminal message containing a 4 octet Information field. When the master terminal requires to transfer a long message containing a 28 octet Information field to a remote, its preceding message to that remote includes an active command bit that indicates that (only) the next master terminal message to that remote will be extended. The Expect Long Message Next Command of the Master-to-Remote Protocol subfield has been reserved for this notification(see 7.2.2). The response from the remote to this message includes an active status bit to confirm that the remote terminal is expecting a long next message. The Expect Long Message Next Flag of the Remote-to-Master Protocol subfield has been reserved for this notification (see 7.2.1). In the event that this response from the remote is rejected on receipt due to a detected transmission error, the master terminal shall then transmit a long message that requests “Repeat Last Message” or suspends operation on that channel until the remote expecting the long message resets its logic. On receipt of the pending long message command bit, the remote terminal should start a timer. If the long message is not correctly received before the time reaches a predefined value, the remote terminal should automatically reset its logic to expect a short message. A long message from the master terminal may contain the same command bit active, indicating that the next message will also be a long message. The remote terminal response message will contain the long message status bit active to confirm that it is ready for the following long message.

Copyright © 1993 IEEE All Rights Reserved

8.5.3 Extensions for Party-Line Operation

These provisions for presetting remote terminal reception logic require extension where party-line communication channels are used. Long master terminal messages are permitted in such communication channel configurations only if all connected remote terminals support a “Remote Terminal Deactivate” function. The master terminal will then precede any set of long messages directed to one remote terminal by individually commanding all other remote terminals connected to the party line to ignore all received messages, i.e., to assume the quiescent state, defined in 5.5, for a specified time interval sufficient to cover all pending long message transfers. This procedure effectively eliminates any possibility of a remote terminal accepting an apparently valid short message that may be contained in a long message being transferred to another remote terminal.

 Copyright © 1993 IEEE All Rights Reserved

Annex A Transaction Throughput

(Informative)

(These appendixes are not part of IEEE Std 999-1992 , IEEE Recommended Practice for Master/Remote Supervisory Control and Data Acquisition (SCADA) Communications, but are included for information only.)

The transaction throughput capacity of each communication channel shall support the maximum need (e.g., data acquisition during a disturbance). The message standards, protocols, and practice shall not compromise the critical use of the communication channel. Transaction throughput in SCADA systems is constrained by four essentially independent system design choices:

1) *Protocol Efficiency.* Defined in various ways but effectively measured by the ratio of the number of data bits retrieved from a remote terminal to the total number of transmitted bits in the transaction.
2) *Channel Type to Be Used*. Duplex/half-duplex and point-to-point/party line. Selection involves a cost/ performance tradeoff by the user, which is essentially independent of the protocol employed.
3) *Channel Data Capacity.* Typically, channel data capacity for a given protocol efficiency is directly proportional to the data rate used. Again, selection involves a cost/performance tradeoff.
4) *Channel Error Control Procedures.* Channel error rates and error control procedures influence overall transaction throughput through a fundamental protocol design choice, the maximum permitted message length.

These design choices are examined in more detail in the following sections. Discussions of data-by-exception data acquisition techniques and control command response times are also included in this appendix.

A.1 Protocol Efficiency

Each master terminal data request in this recommended practice consists of a 8 octet message, and the resulting response ranges from 8 to 32 octets of which from 3 to 27 are data. The data acquisition efficiency therefore ranges from 3/16 to 27/40, i.e., 18.8% to 67.5%. Corresponding values for the widely used (31, 26) BCH code-based protocol, in which a 31 b master terminal message can request from 1 to 16 31-b responses each containing 24 data bits, are 38.7% to 72.9%. This recommended practice thus provides a data acquisition channel efficiency that is essentially comparable with current industry practice.

A.2 Channel Configuration Selection Considerations

The selection of channel type between master and remote terminals, point-to-point or party line and duplex or half-duplex, typically is a cost/performance tradeoff. Note that this recommended practice suggests the use of a Remote Terminal Deactivate command where long master-to-remote messages are to be implemented (8.5.3) on party-line channels. Note also that if half-duplex party-line channels are used, the remote terminals will attempt to interpret the reply of another remote terminal as a master terminal command. Although the basic security features of this recommended practice minimize the probability of a remote terminal transmission being interpreted as a master terminal command, and the use of half-duplex party-line channels has not been specifically prohibited, their use should be considered acceptable only if no other alternative is available.

A.2.1 Point-to-Point and Party-Line Channels

Point-to-point communication channels provide both the highest data efficiency for a given message protocol and the highest dynamic performance, as the entire channel is available for use by the single remote terminal. They are also generally simpler to set up and to maintain. They represent the highest cost alternative in respect of master terminal channel hardware and support software processing bandwidth.

Copyright © 1993 IEEE All Rights Reserved

Party-line channel configurations are essential where only a limited number of communication channels are accessible, as in systems based on VHF, UHF, or microwave radio facilities.

A.2.2 Duplex and Half-Duplex Channels

The operating cost of some communication channels may be reduced by using half-duplex (two-wire) circuit configurations. The use of half-duplex channels results in a corresponding performance penalty associated with "turnaround" delays at each terminal. These are a minimum of 8 ms plus logic delays at each terminal.

The effects of this turnaround delay on overall channel times are shown in the half-duplex section of Table A.2. They are of greatest proportional significance in the shortest transactions. However, for some system applications, this performance reduction may be of minor significance relative to the channel cost reduction.

A.3 Channel Data Capacity

Transaction throughput is a direct function of the channel signalling rate. To simplify the problem of selecting a channel signalling rate, it may be noted that the average channel utilization may be estimated considering only the data values to be routinely serviced by the channel. This typically includes status and analog data acquisition or only analog data where status-by-exception reporting is implemented (see A.5). Any high-periodicity control commands (such as generator raise/lower actions) should be added to the routine data acquisition utilization.

A second major simplification is effected by limiting the desired channel utilization to 40–60%. This would provide channel resources for low-periodicity data acquisition (such as hourly accumulator scans), operator commanded control actions, and channel error control procedures (see A.4). Where the channel will be subject to large bursts of data acquisition loads (such as during a disturbance where report-by-exception techniques are employed), the lower values of the desired channel utilization range may be appropriate. The user of this recommended practice should verify the simplifications made above for the specific intended system application. If these assumptions prove invalid, the user must construct a valid data volume estimate.

The recommended practice allows a single-message remote terminal reply to include up to 27 octets of data. (Multiple-message remote terminal replies are discussed in A.4.)

Table A.2 presents a chart of transaction times using this recommended practice for a variety of response message lengths. These values ignore channel propagation times, error rates, and resulting retransmissions but include all other necessary times for transmission initiation and termination.

Table A.2 illustrates the reduction in the effective channel data efficiency as the message length is reduced. For example, a duplex point-to-point channel operating at 1200 b/s requires 254 ms of channel time to retrieve 12 16-b data values in one transaction (29 response octets—1 sync octet, 1 remote address octet, 24 data octets, 1 protocol octet, and 2 BCH code octets). If these values are retrieved using three transactions each with four 16 b values, the total channel time required will be $3 \times 147 = 441$ ms.

Table A.2 may then be used to calculate effective channel load factors for various remote terminals and point assignments to each channel, or it may be used to determine the necessary channel data rate for any desired remote terminal and point configuration. Channel transaction times for response message lengths not listed may be obtained by interpolation.

 Copyright © 1993 IEEE All Rights Reserved

Table A.1—Channel Message Times (in ms)

	Number of Octets							
Channel Data Rate (b/s)	**8 (min)**	**9**	**13**	**17**	**21**	**25**	**29**	**32 (max)**
75	880	987	1413	1840	2267	2693	3120	3440
150	440	493	707	920	1133	1347	1560	1720
300	220	247	353	460	567	673	780	860
600	110	123	177	230	283	337	390	430
1200	55	62	88	115	142	168	195	215
2400	28	31	44	58	71	84	98	108
4800	14	15	22	29	35	42	49	54
9600	7	8	11	14	18	21	24	27

NOTE — These times are for single messages (not transactions) and do not consider hardware and channel delays. Table A.2 provides transaction time data.

A.4 Channel Error Control Procedures

Channel error control procedures are those conventions exercised in reaction to a detected transaction error. While error control procedures are not included in this recommended practice, the following material is presented to guide users of this recommended practice in the design of error control procedures.

In today's SCADA systems, channel error control procedures typically include rejection of data received with errors and multiple requests for repeat transactions (transaction "retries") until all data is received without errors. Given a quantity of data values to be acquired by the master terminal, the remote terminal could include one data value in a reply to a master terminal data request, all data values, or a quantity of values greater than one but less than all. Table A.2 illustrates the generally better efficiency (lower channel usage times for a given quantity of data) of longer messages. Longer messages have a greater probability of being received with errors than short messages, however. Channel error control procedures have to balance the need to acquire error-free data during a given data acquisition period against the effect on channel throughput of the basic efficiency of the transaction (varying directly with message length), the probability of an error-free transaction (varying inversely with message length), and the penalties exacted by retrying transactions.

A typical practice in industry is to not retry some data acquisition transactions, typically high-periodicity (1–5 s) transactions. This assumes that previously acquired data will be retained and that the applications using the "old" data will not generate significantly erroneous results without "new" data. This also assumes that the applications will rapidly generate correct results when valid data is acquired on subsequent transactions. Where the receipt of valid data is mandatory during a single data acquisition period, such as for low-periodicity (10 s to 60 min) data, a maximum of three retries (four total attempts) is typical.

Copyright © 1993 IEEE All Rights Reserved

Table A.2 —Channel Transaction Times

Transaction Type	**1**	**2**	**2**	**2**	**2**	**2**	**2**	**2**	**2**
Number of Response Octets	**0**	**8 (min)**	**9**	**13**	**17**	**21**	**25**	**29**	**32 (max)**
Number of 16 b Data Units	**0**	**1+**	**2**	**4**	**6**	**8**	**10**	**12**	**13+**
Channel Data Rate (b/s)	Duplex Point-to Point Channel								
75	882	1764	1871	2297	2724	3151	3577	4004	4324
150	442	884	937	1151	1364	1577	1791	2004	2164
300	222	444	471	577	684	791	897	1004	1084
600	112	224	237	291	344	397	451	504	544
1200	57	114	121	147	174	201	227	254	274
2400	30	59	62	76	89	102	116	129	139
4800	16	32	33	40	47	53	60	67	72
9600	9	18	19	22	25	29	32	35	38
	Duplex Party-Line Channel								
75	882	1774	1881	2307	2734	3161	3587	4014	4334
150	442	894	947	1161	1374	1587	1801	2014	2174
300	222	454	481	587	694	801	907	1014	1094
600	112	234	247	301	354	407	461	514	554
1200	57	124	131	157	184	211	237	264	284
2400	30	99	102	116	129	142	156	169	179
4800	16	107	108	115	122	128	135	142	147
	Half-Duplex Channel								
75	892	1784	1891	2317	2744	3171	3597	4024	4334
150	452	904	957	1171	1384	1597	1811	2024	2184
300	232	464	491	597	704	811	917	1024	1104
600	122	244	257	311	364	417	471	524	564
1200	67	134	141	167	194	221	247	274	294
2400	70	139	142	156	169	182	196	209	219
4800	91	182	183	190	197	203	210	217	222

NOTES:

1 — Master and remote terminal logic equipment response times are assumed to be 2 ms.

2 — Modem preconditioning and turnoff times are as defined in this recommended practice and the CCITT V Series Recommendations.

75 to 1200 b/s8 ms preconditioning and 2 ms turnoff

2400 b/s30 ms preconditioning and 10 ms turnoff

4800 b/s50 ms preconditioning and 25 ms turnoff

3 — 9600 b/s modems are suitable only for duplex point-to-point channels due to their long turnaround times.

4 — 4800 b/s modems are not recommended for half-duplex channels.

This recommended practice limits the length of a message to 27 data octets; this is equivalent to 13.5 16-b data values, 18 12-b data values, or 216 1-b data values. Additional data values can be transmitted in a single transaction by allowing more than one message in the remote terminal reply. This is acceptable within this recommended practice,

 Copyright © 1993 IEEE All Rights Reserved

but multiple message replies increase the probability of an error occurring during the transaction and exact a greater channel utilization penalty when the long transaction must be retried.

Fig A.l charts selected transaction lengths against channel error probabilities and the resulting probability of a successful (error-free) transaction. If the protocol is to realize a 99% success probability on the third retry (fourth attempt) of a transaction, the success probability of an individual transaction should be above 68%. Only a transaction with a single maximum-length reply message will satisfy this criterion under worst-case channel bit error rates. To minimize the channel throughput penalty of transaction retries where multiple message replies are used, the user should consider channel error control procedures to identify the individual message received in error in the master terminal retry message so that the remote terminal need retransmit only those messages received with errors.

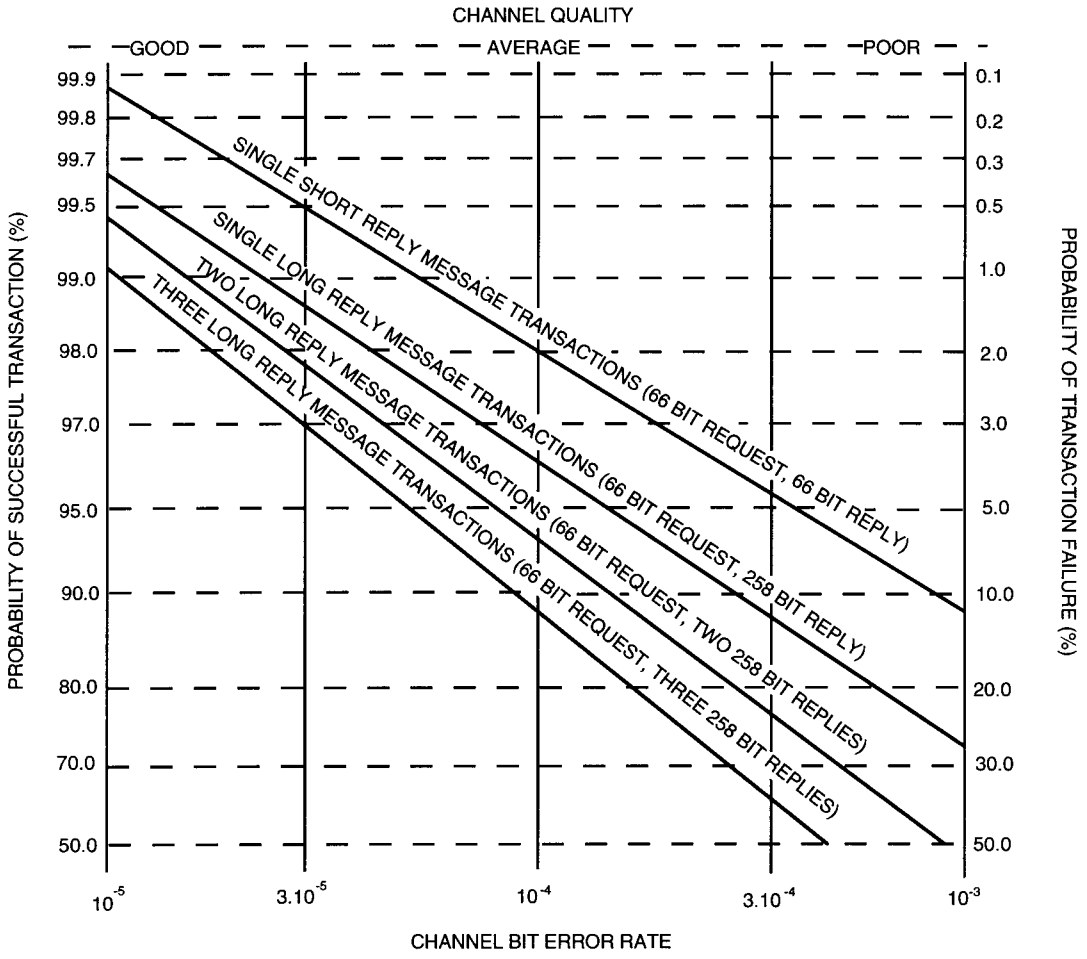


Figure A.1—Transaction Success Probabilities

A.5 Data-By-Exception/Routine Data Scans

One function of SCADA systems is to maintain an up-to-date measurement of all remote terminal signal inputs at the master terminal. If “significant” changes in these signals occur infrequently, then these changes can, in principle, be reported to the master terminal with shorter delays due to communication channel throughput restrictions than if all signals are routinely reported whether unchanged or not.

Copyright © 1993 IEEE All Rights Reserved

Remote terminal status input signals can have this property. By definition, any change in a 1 b input signal is “significant,” and it should be reported to the master terminal as rapidly as possible. Remote terminals typically monitor some tens, or even hundreds, of status input signals, but the probability of any one changing in a time interval of the order of 1 s is very low.For this reason,“status-by-exception” reporting techniques have been widely applied in SCADA systems, and these techniques are supported by this protocol. Exception reporting techniques may also be applicable to analog data values. The definition of a “significant” change in an analog value is less clear than that of a status value, however. The usual criterion for selecting an analog value for transmission is that its latest value measured at the remote terminal differs from the value most recently reported to the master terminal by some adjustable threshold. This threshold should be selected such that any master terminal processing of the value is not degraded by the threshold. Examples of processing that might be degraded by exception reporting are State Estimation and filtered variables.

Exception reporting techniques almost always reduce the efficiency of the data acquisition transactions. For example, practices in use today include transmitting the address of the value reported along with the value, and executing one transaction to determine the presence of data to be reported at the remote terminal followed by a second transaction to acquire the data. Any efficiency degradation should be offset by a reduction in the average number of values transmitted in order to maintain the transaction throughput.

The average channel utilization selected (see A.3) should include a sufficient margin for burst transfer requirements. A need to transmit a large quantity of data values much greater than the average quantity of values transferred might be expected during a disturbance. Since it is during a disturbance that the system users have the greatest need for accurate and timely data, the channel should have the capacity to report the maximum quantity changed data values that could be expected under worst-case conditions at the reduced efficiency of the exception-reporting protocol, or that channel should be capable of switching to a more efficient data transfer method to provide the necessary capacity.

A.6 Control Response Time

Control action response times are mainly constrained by two factors; the channel time required to complete the control procedure with the channel data rate and protocol formats used, and the delay inherent in completing any ongoing transaction at the time of initiating the control action request. Other factors such as software delays in the master terminal or device operation times are outside the scope of this recommended practice.

Table provides for direct assessment of control action response times with this recommended practice. Assuming that all external equipment control actions will be performed using the“Select, Check, Execute” sequence, two Type 2 transactions with a reply message length of 8 octets are required. If the maximum reply message lengths (32 octets) are used during routine data acquisition processes, initiation of control actions may be delayed by the time intervals listed.

For example, if a duplex party-line channel is operated at 1200 b/s, the maximum time interval between initiation of a control action and its completion, ignoring master terminal overhead and hardware response times external to the remote terminal, will be just over 0.5 s, (2×124 ms + 284 ms or 532 ms).

 Copyright © 1993 IEEE All Rights Reserved

Annex B Equipment Compatibility Restrictions

(Informative)

While all equipment manufactured by various suppliers to operate under this protocol will necessarily be basically compatible, it should not be assumed to be completely interchangeable in all respects. The following items provide an indication of some potential inconsistencies that should be considered prior to mixing equipment from different sources:

1) *Data Rate Selection.* Some terminals may not provide facilities for all specified data rates or channel configurations.
2) *Preamble Time.* While a minimum interval of 8 ms is specified, some terminals may also incorporate an upper limit when operating on a party-line channel that could be less than the time used by others. Note that preamble times of up to 250–300 ms may be needed in some radio channels.
3) *Remote Address.* Some remote terminals may not provide for selection of all possible address values.
4) *Functionality.* Remote terminals may vary in the range of functions that can be implemented and in the specific Function Codes and Address values used.
5) *Point Count Modularity.* Remote terminals may vary in respect to point count modularity, which may impact master terminal data base management facilities. Such variations should not, however, affect channel operation since any unimplemented data or control points accessed by the master terminal will result in the correct length remote terminal response.
6) *Remote Terminal Protocol Octet Usage.* Variations in the system significance of these octets will require corresponding changes in the master terminal service procedures for these octets.
7) *Data Units.* The encoding of data and the types of data may differ between different remote terminals.

Copyright © 1993 IEEE All Rights Reserved

Annex C Message and Transaction Security

(Informative)

This appendix describes the message and transaction security features of this recommended practice.

C.1 Sync Pattern Selection

C.1.1 Basic Sync Field Requirements

Each new message transmission shall be prefaced with a standardized preamble condition for a sufficient time to allow any signal carrier switching transients to subside and to permit synchronous modems to acquire bit synchronism. This shall be followed by a predetermined synchronizing field or “sync pattern,” which enables the receiving terminal(s) to recognize correctly the start of the transmitted message. The preamble condition consists of a series of bits at the logic “1” state of the binary channel. The first active bit of the sync pattern shall therefore be a logic “0.”

A sync pattern consisting of a single bit would be unduly susceptible to message framing errors. Any received bit error during the preamble would initiate message reception prematurely. Conversely, if the sync bit were received in error, the start of message reception would be delayed. In principle, as the sync pattern length is increased, the probability of incorrect message framing, known as “sync slip,” can be reduced at the expense of a corresponding reduction in overall message data efficiency.

In accordance with the octet basis of all messages, 8 b are assigned to the Sync field. Use of different sync patterns in master and remote terminal messages can improve communication security in half-duplex party-line channels. The two sync patterns used are selected to minimize the probability of sync slip due to received bit errors prior to and during Sync field reception.

C.1.2 Optimum Sync Patterns

Optimum sync patterns for any sync field length are those that require the largest number of received bit errors to cause sync slip. Consideration of the effects of received bit errors during the preamble shows that an optimum 8 b sync pattern should contain at least 4 logic “0” and 2 logic “1” bits and will be immune to any 3 b received in error.

Ninety-one of the 128 8 b patterns that commence with logic “0” contain 4, 5, or 6 logic “0” bits. The minimum number of bits that have to be received in error to cause sync slip can be found for each of these 91 patterns by comparing the pattern with slipped versions of it. Such comparisons show that 26 of these patterns are immune to any 3 received bit errors.

Selection of the two sync patterns used for master and remote terminal messages from the set of 26 optimum patterns is then based on maximizing the number of received bit errors required to transform one pattern into a slipped version of the other. Two of the 26 patterns require four or more received bit errors for this transformation. These are the two patterns used in this recommended practice. All bits, with the exception of the first bit, of these sync patterns are included in the BCH code.

C.2 Message Security Analysis

C.2.1 Introduction

Serial channels used for data communication are subject to two classes of error: active and passive. Active errors are the result of willful attempts by a third party to alter a transmitted message. Passive errors are the result of the effects of channel noise on the transmitted message. The consequences of both classes of error can be minimized by the use of suitable message coding, encryption for active errors, and security coding for passive errors. The following analysis

 Copyright © 1993 IEEE All Rights Reserved

addresses message security coding only for SCADA data communication applications that are not potentially subject to active interference.

Both random and impulse noise on serial channels can cause the data receiver(s) to misinterpret the received signal and thus misread the transmitted binary message. Random noise results in received data bit errors, all of which are, by definition, independent of each other. Impulse noise results in groups of received data bit errors, termed “burst errors,” in which multiple bit errors occur during the time span of the impulse transient.

The objective of message security coding is to reduce the probability of accepting messages containing passive bit errors to an adequately low level. This probability is the sum, over all possible types of received error, of the product of the probability of each error type occurring and the probability of that error type not being detected by the security code. The first term in each product is a function of the end-to-end error performance of the data channel. The second is defined by the error detection performance of the security code.

The performances of the (255, 239) BCH message security code used in this recommended practice are examined in the following subsections.

C.2.2 Error Detection Performance of BCH Codes

BCH codes are cyclic codes that are relatively simple to implement in hardware (for error detection) and that provide good error detection performances with relatively short code lengths.

Cyclic codes are defined as those for which any cyclic permutation of a valid message block is also a valid message block. These codes have the following error detection capabilities:

1) Each (n, k) cyclic code detects all signal bit errors and all burst errors of length (n - k) bits or less in a block, where n is the total number of bits and k is the number of information bits, in the block. A burst error of r bits is defined as two or more bits in error with the first and last such bits separated by (r – 2) bits.
2) The probability that a burst of length (n - k + 1) will not be detected is $2^{-(n - k + 1)}$.
3) The probability that a longer burst will not be detected is $2^{-(n - k)}$.

An (n, k) BCH code, in which n and k are as defined above, has these additional characteristics:

$n < 2m - 1$ where m is a positive integer, and

$(n - k) = m \times t$ where t is also a positive integer

BCH codes detect all message blocks containing $2t$ or fewer bits in error, in addition to the burst error detection capabilities of cyclic codes. The (255, 239) BCH code selected has:

$n = 255$, $k = 239$, $(n - k) = 16$, $m = 8$, and $t = 2$

It therefore detects:

— All messages containing 1 b, 2 b, 3 b, or 4 b in error
— All messages containing a burst error of 16 or fewer bits
— 99.99695% of all messages containing a burst error of 17 b ($2^{-(n - k - 1)} = 3.05 \times 10^{-5}$
— 99.99847% of all other messages in error ($2^{-(n - k)} = 1.55 \times 10^{-5}$).

C.2.3 Error Characteristics of Serial Channels

Measurement of the overall error rate of any operating serial channel merely involves transmitting known test patterns and counting the number of received bit errors over adequately long periods. Many such tests have been performed on a wide variety of typical SCADA channel types.

Copyright © 1993 IEEE All Rights Reserved

"High" quality channels are obtained using leased point-to-point telephone data circuits with modern synchronous modems operating at 4800 b/s. The typical error rate in such channels is about 3 in 10^6 b.

"Average" quality channels are obtained using multidrop voice-grade unconditioned telephone circuits with asynchronous modems at 1200 b/s. The typical error rate in such channels is about 3 in 10^5 b.

"Low" quality channels are obtained with VHF radio links, power-line carrier links, direct buried cable, etc. The typical error rate in such links is about 3 in 10^4 b.

Each of these "typical" bit error rates is subject to occasional degradation by a factor of three or more under extreme noise conditions or when equipment maintenance is needed. Security code protection against errors can reasonably, therefore, be evaluated for "normal" and "worst case" bit error rate conditions, respectively, of 1 in 10 000 b and 1 in 1000 b. As some channel types (such as the switched telephone network) can occasionally deliver unrelated signals due to crosstalk or switching errors, the error protection provided by the security code when the bit error probability is 0.5 may also be important.

The measured error rates represent the combined effects of both random and burst errors due to channel noise. The relative significance of the two types of error varies widely with channel type and also with time for a given channel. For performance analysis purposes, the total error rate may be assumed to result from either type of error. The error detection performance of a security code can be evaluated directly for any random bit error rate using the procedure of C2.4.

Evaluation of the probability of undetected error due to impulse noise requires evaluation of the probabilities of occurrence of bursts of all possible lengths, since the security code detects only bursts shorter than some limit value. For any practical finite-bandwidth channel, noise bursts of durations much longer or shorter than the reciprocals of the lower and upper cutoff frequencies respectively of the channel have small probabilities of occurrence.

The distribution function of burst length in any channel is determined only by the channel frequency response function and can be calculated directly from it. The channel bit error rate due to burst errors, which represents the combined effects of bursts of all lengths, in conjunction with the burst length distribution function, enables the probability of occurrence of burst that will defeat the security code to be evaluated as shown in C.2.6.

C.2.4 (255,239) BCH Code Random Error Detection Performance

The probability of an undetected message error due to random bit errors using the (255,239) BCH code is evaluated below for the maximum and minimum message block lengths used in this recommended practice, 256 b and 64 b respectively, and for average and worst-case random bit error rates of 1 in 10 000 b and 1 in 1000 b.

Since this code detects all messages in error containing up to 4 b in error, only messages containing five or more error bits may not be detected. The probability of P_R, of a message block of N bits being received with R random bits in error is given by

$$P_R = {}^{N}C_R \times p^R \times (1-p)^{N-R} \tag{C1}$$

where

p = Random bit error rate

$${}^{N}C_R = \frac{N!}{R! \cdot (N-R)!}$$

The approximate values of P_R for the four cases under consideration and when R = 5, 6, and 7 are presented in Table C.1, together with the total probability ($P_5 + P_6 = P_7 + \ldots$) of reception of messages containing more than 4 b in error.

 Copyright © 1993 IEEE All Rights Reserved

Some of these messages will also be detected by the burst error detection capabilities of the code. However, the fractions of 64 b or 256 b messages for which the random error burst length is no more than 16 b are negligible, being about 3% of 64 b messages and 0.01% respectively of all messages in error.

The probability that a message received with 4 b in error will contain an apparently valid security check code 16 b in length is at most 1 in 2^{16}. The probability of undetected message random errors for the (255, 239) BCH code is, therefore, less than 2^{-16} times the probability that more than 4 b will be received in error. These probabilities are listed in Table C.1.)

Table C.1 —Message Random Error Probabilities Versus Message Length

Random Bit Error Rates	1 in 10 000 b		1 in 1000 b	
Message Lengths (b)	**256**	**64**	**256**	**64**
Message Probabilities				
5 b in error	8.6×10^{-11}	7.6×10^{-14}	6.9×10^{-6}	7.2×10^{-9}
6 b in error	3.4×10^{-13}	7.5×10^{-17}	2.9×10^{-7}	7.1×10^{-11}
7 b in error	1.3×10^{-15}	6.2×10^{-20}	1.0×10^{-8}	5.9×10^{-13}
5 or more bits in error	8.6×10^{-11}	7.6×10^{-14}	7.2×10^{-6}	7.3×10^{-9}
Undetected message error	1.3×10^{-15}	1.2×10^{-18}	1.1×10^{-10}	1.1×10^{-13}

C.2.5 (255, 239) BCH Code Severe Error Detection Performance

The probabilities of undetected error listed above assume that the received message is essentially similar to that transmitted and that the receiver correctly detects the message sync pattern. “Severe” errors occur otherwise.

When an active receiver is suddenly presented with arbitrary serial data due, for example, to switching errors in a multichannel communication facility, the message in the course of transmission has a probability of 1 in 2^{16} of being accepted in error. The probability of such errors is, therefore the probability of the event divided by 2^{16}. The event probability is simply the mean time interval between these events divided by the number of transactions in that interval.

The probability of this class of undetected message error is typically small compared with the worst-case values listed in Table . For example, in a channel operating at 1200 b/s with 50% load factor using only maximum-length messages, the undetected message error probability will be less than 1×10^{-10} provided that the mean time between such events exceeds about 10 h. In practice, this interval is likely to be months or years.

The combination of the sync patterns and the (255, 239) BCH code used in this recommended practice detects all messages subjected to a sync slip of up to 16 b and reduces the probability of sync slip in excess of 16 b to a negligible level. For example, to cause premature sync in a remote-to-master transmission, four fill bits have to be inverted to generate the sync pattern. This recommended practice suggests that the interval between completing reception of the master message and initiating transmission of the remote response message should be less than 20 ms, which is a 100 b at 4800 b/s data rate. At a random bit error rate as high as 1 in 1000 b, the probability of generating a spurious sync pattern due to random errors in only 100 b times is less than 1 in 10^{10}. The resulting incorrectly framed message has a probability of 1 in 2^{16} of containing an apparently valid BCH code so that the overall probability of acceptance of such a message is about 1 in 10^{15}.

Copyright © 1993 IEEE All Rights Reserved

C.2.6 (255, 239) BCH Code Burst Error Detection Performance

The burst error detection capabilities of the (255, 239) BCH code are defined in terms of burst lengths in bits. The effects of a given channel noise pulse time, therefore, depends on the data rate in use. The relative probabilities of bursts of all possible lengths can be calculated from the channel frequency response.

For a typical telephone channel, for example, about 98% and 65% respectively of all bursts will be of 16 or fewer bits in length at data rates of 1200 b/s and 4800 b/s. All such bursts are detected by the BCH code. The probability of undetected errors due to longer bursts is 1 in $2.^{16}$ if, for simplicity, the special cases of bursts of exactly 17 b in length are ignored.

The overall probability, P_E, of an undetected message burst error is given by:

$$P_E = 2^{-16} \times P_B \times P_M \tag{C2}$$

where

P_B = Probability of "long" burst
P_M = Probability of a message

P_M is simply the channel message load factor and is typically about 0.5 in SCADA systems. A "long" burst is one exceeding 16 b in time. P_B can be calculated from the channel burst length distribution function combined with an assumed value for the average bit error rate due to bursts of all lengths. The following table presents the results obtained using a burst length distribution function that is typical of leased telephone circuits.

Table C.2 —Message Random Error Probabilities Versus Error Rates

Burst error rates	**1 in 10 000 b**		**1 in 1000 b**	
Channel data rates (b/s)	**4800**	**1200**	**4800**	**1200**
Probabilities				
Long burst (> 16 b)	6.6×10^{-1}	1.7×10^{-5}	6.6×10^{-4}	1.7×10^{4}
Message	0.5	0.5	0.5	0.5
Undetected message burst error	5.1×10^{-10}	1.3×10^{-10}	5.1×10^{-9}	1.3×10^{-9}

C.3 Security Performance Summary

The combination of the 8 b sync field and the (255, 239) BCH security code provides virtually complete immunity to message errors due to sync slip and adequate immunity to channel random and burst errors.

Comparison of the overall message error probabilities that are presented in Table C.1 and Table C.2 suggests that the latter could be serious in some SCADA applications. However, these results are pessimistic, as they assume burst error rates that are excessive for modern 4800 b/s modems and they ignore those long bursts that contain less than 5 b errors and are therefore rejected by the BCH code.

 Copyright © 1993 IEEE All Rights Reserved

Annex D Protocol Performance Comparisons

(Informative)

D.1 Introduction

This appendix compares the performances of the recommended practice protocol with those of others that have been widely used in SCADA and computer-to-computer data communications applications. These protocols are

1) *(31,26) BCH*. This SCADA protocol uses a 31 b basic message block, of which 2 b and 24 b are used respectively for synchronizing and data. The final 5 b are the (31,26) BCH code calculated over the preceding 26 b. Each 31 b master terminal message may elicit from 1 to 16 contiguous 31 b remote terminal response message blocks, i.e., from 3 to 48 data octets.
2) *High-Level Data Link Control (HDLC) [or Synchronous Data Link Control (SDLC]*. These general-purpose bit-oriented data communication protocols provide for messages of any length, up to 32 767 b, and frame each message with at least one "Flag," 01111110. Data transparency is achieved by "stuffing" at the transmitter and "stripping" at the receiver a logic 0 b following each sequence of five consecutive logic 1 b in the data. Security is provided by use of a 16 b cyclic redundancy check code (CRC-CCITT in HDLC and CRC-16 in SDLC).
   For simplicity, these comparisons assume that a duplex point-to-point communication channel is used and that channel and terminal equipment delays are negligible. HDLC data acquisition transactions for SCADA applications are assumed to consist of one Flag framing each message with a master terminal message length of eight octets and a remote terminal message length equal to the number of data octets plus four.

D.2 Data Acquisition Efficiency Comparison

Data acquisition transactions in this recommended practice require the following numbers of octets for *D* data octets in the remote terminal response message:

(D + 13) for D in the range 3 to 27 octets
(D + 18) for D in the range 28 to 54 octets
(D + 23) for D in the range 55 to 72 octets, etc.

The (31,26) BCH protocol uses 31 (1 + D/3) bits in each transaction for D in the range 3 to 48 (and divisible by 3).

HDLC transactions for SCADA applications require 9 octets, including Flags in the master terminal message followed by 6 octets plus the number of data octets in the remote terminal response message. Thus, the HDLC transaction length is (D + 15) octets.

The communication channel data efficiencies for data acquisition transactions are tabulated below for representative values of D in the range from the minimum (3) to maximum (48) values obtainable in all three protocols from one master terminal request message. The data transfer efficiencies of all three protocols are essentially equivalent at message lengths of about 20–24 data octets, which are the most frequently used in modern SCADA systems. The lower efficiency of this recommended practice at the shortest message lengths is of minor significance since few such transactions are used during routine data acquisition processes.

Copyright © 1993 IEEE All Rights Reserved

Table D.1—Channel Data Efficiencies (in percent)

	Number of Data Octets				
	3	**12**	**21**	**27**	**48**
IEEE Std 999-1992	18.75	48.00	61.76	67.50	72.72
(31,26) BCH	38.71	61.94	67.74	69.68	72.87
HDLC	16.67	44.44	58.33	64.29	76.19

D.3 Synchronizing Performance Comparison

The message synchronizing performance of this recommended practice is shown in Appendix C to be excellent.

The probability of undetected sync slip occurring in the (31,26) BCH code is relatively high due to its short sync pattern and its security code of 2 b and 5 b, respectively. If the transmission delay of a remote terminal is less than 5 b times after completion of reception of a master terminal request message, then a premature sync accepted by the master terminal will be subsequently rejected by the security code. However, if the remote terminal delays its response by as little as 20 ms in a channel operating at 1200 b/s with a random error rate of 1 in 10 000 b, then the probability of acceptance by the master terminal of a spurious message due to premature sync will be about 6 in 10^9 messages. This probability is about 60 times larger than the target value for SCADA system immunity to channel errors as specified in IEEE Std C37.1-1987 .

The basic synchronizing performance of HDLC is poor since an error in any transmitted logic 1 b of a Flag converts that Flag into an apparent first octet of a message. However, the minimum message length, combined with the 16 b check code, requires that at least two consecutive Flag characters immediately preceding a message have to contain an error to defeat the message format and security checks. The overall probability of acceptance of a spurious message due to a sync error is HDLC is about 6 in 10^{12} messages at a channel random error rate of 1 in 10 000 b.

D.4 Error Detection Comparisons

The basic error detection performances of the security check codes used in the three protocols are:

	IEEE Std 999-1992	**31,26 BCH**	**HDLC**
Numbers of message error bits detected	1, 2, 3, 4	1, 2	All odd and 2
Maximum message error burst length, bits	16	5	16
Maximum probability of acceptance of message containing errors	2^{-16}	2^{-5}	2^{-16}

These bit and burst error detection capabilities apply only when a message is correctly framed so that the correct group of bits is interpreted as the security code. The undetected error probability applies to an incorrectly framed message and to any correctly framed message that is received with more bits in error, and with a longer burst, than the listed maximum values.

 Copyright © 1993 IEEE All Rights Reserved

The probability of acceptance of a correctly framed 256 b message in error resulting from a random error rate of 1 in 10 000 b is negligible for this recommended practice and for HDLC. The probability of acceptance of a correctly framed 31 b message in error for the (31,26) BCH protocol at the same error rate is about 1.4 in 10^{10}.

The burst error detection capability of this recommended practice is evaluated in Appendix C. HDLC provides virtually equal performance, but that of the (31,26) BCH code is substantially worse. The difference results from the much higher probability of a message error not being detected combined with the larger fraction of channel noise bursts that exceed the detectable burst length. At a channel data rate of 1200 b/s and a burst error rate of 1 in 10 000 b, the probability of undetected message error in this code is about 8 in 10^{7} messages. i.e., 8000 times larger than the target value for message error immunity in SCADA applications as shown in IEEE Std C37.1-1987 .

While the basic error detection capability of the HDLC CRC-CCITT security code is comparable with that of the (255,239) BCH code of this recommended practice, the overall channel error immunity performance of HDLC is several orders of magnitude worse as a result of its bit “stuffing” and “stripping” scheme for data transparency. A single bit error in a message can simulate a premature message end Flag and a single error in the latter can convert it into data. In both cases, an incorrect group of 16 b will be interpreted as the CRC check code.

For a bit error rate of 1 in 10 000 b and a message length of 255 b, the probability of either error is about 6 in 10^{4}. These error conditions have a probability of 1 in $2.^{16}$ that the incorrect 16 b will contain an apparently valid CRC code value. The overall probability of accepting an HDLC message in error for these reasons is thus about 1.8 in 10^{8}, i.e., nearly 200 times the SCADA target value.

D.5 Performance Comparison Summary

D.5.1 Channel Data Transfer Efficiency

The approximate efficiency range for the majority of data acquisition transactions is as follows:

—IEEE Std 999-1992	50–60%
—(31,26) BCH	60–70%
—HDLC	45–60%

D.5.2 Synchronizing Performance

The probability of acceptance of an incorrectly synchronized message with a channel random error rate of 1 in 10 000 b is

—IEEE Std 999-1992	2 in 10^{14}
—(31,26) BCH	6 in 10^{9}
—HDLC	6 in 10^{12}

Copyright © 1993 IEEE All Rights Reserved

D.5.3 Message Error Immunity

The probabilities of acceptance of the longest permitted messages received in error due to channel random and burst errors at an error rate of 1 in 10 000 b are

	Random	**Burst**
— IEEE Std 999-1992	1.3 in 10^{15}	1.3 in 10^{10}
— (31,26) BCH	1.4 in 10^{10}	8.3 in 10^{7}
— HDLC	1.8 in 10^{8}	1.8 in 10^{8}

The probabilities of acceptance of messages subject to framing or other “severe” errors are

— IEEE Std 999-1992	1.5 in 10^{5}
— (31,26) BCH	3.1 in 10^{2}
— HDLC	1.5 in 10^{5}

Copyright © 1993 IEEE All Rights Reserved