

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 transmission

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 group¹ 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.

¹IEC Technical Committee No. 57: Telecontrol, Teleprotection, and Associated Telecommunications for Electric Power 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. Prystajeky
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. Prystajeky

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	P. R. Nannery	D. F. Koenig
B. Y. Afshar	S. P. Meliopoulos	T. J. Kolenda
S. J. Arnot	J. T. Orrell	A. Kollar
A. Baker	J. S. Oswald	E. Kolodziej, Jr.
N. Barbeito	S. G. Patel	T. L. Krummey
G. J. Bartok	R. J. Perina	L. W. Kurtz
J. D. Betz	L. Pettersson	D. N. Laird
K. M. Bevins	T. A. Pinkham	A. A. Liebold
K. L. Black	J. Quinata	C. T. Lindeberg
C. J. Blattner	D. G. Rishworth	P. Lips
W. Block	P. C. Bolin	W. F. Long
S. Boggs	S. D. Brown	R. Matulic
L. N. Ferguson	J. C. Burke	D. Russell
G. G. Flaig	J. B. Cannon	J. Sabath
D. L. Garrett	R. E. Carberry	D. R. Schafer
A. Haban	J. R. Clayton	F. C. Shainauskas
D. L. Harris	E. F. Counsel	B. Sodka
M. A. Hick	D. M. Christie	R. C. St. Clair
J. E. Holladay	N. Cuk	W. K. Switzer
M. L. Holm	F. A. Denbrock	E. R. Taylor, Jr.
D. C. Johnson	W. K. Dick	C. F. Todd
Z. Kapelina	C. C. Diamond	D. R. Torgerson
G. G. Karady	W. B. Dietzman	L. F. Volf, Jr.
R. P. Keil	T. Doern	R. J. Wehling
J. D. McDonald	F. F. Kluge	W. M. Werner
T. S. McLenahan		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	Donald N. Heirman	T. Don Michael*
Paul L. Borrill	Ben C. Johnson	John L. Rankine
Clyde Camp	Walter J. Karplus	Wallace S. Read
Donald C. Fleckenstein	Ivor N. Knight	Ronald H. Reimer
Jay Forster*	Joseph Koepfinger*	Gary S. Robinson
David F. Franklin	Irving Kolodny	Martin V. Schneider
Ramiro Garcia	D. N. "Jim" Logothetis	Terrance R. Whittemore
Thomas L. Hannan	Lawrence V. McCall	Donald W. Zipse

*Member Emeritus

Also included are the following nonvoting IEEE Standards Board liaisons:

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

Mary Lynne Nielsen, *IEEE Standards Project Editor*

CLAUSE	PAGE
1. Scope	1
2. References	1
3. Definitions	2
4. Communication Channels	5
4.1 Channel Requirements	5
4.2 Channel Types	5
5. Channel Interfaces	6
5.1 General	6
5.2 Data Rates	6
5.3 Terminal-to-DCE Interface	7
5.4 DCE-to-Channel Interfaces	7
5.5 Channel Control	8
5.6 Message Transfer Control	10
6. Communication Message Format	12
6.1 General	13
6.2 Message Establishment Field	13
6.3 Information Field	14
6.4 Message Termination Field	14
6.5 Message Format Summary	15
7. Information Field Usage	16
7.1 Information Field Formats	16
7.2 Protocol Octet Functions	17
7.3 Transaction Types	19
7.4 Remote-to-Master Data Transfer	21
7.5 Master-to-Remote Data Transfer	21
8. Communication Management	23
8.1 General	23
8.2 Master Terminal Channel Control Functions	23
8.3 Multiple Channels	24
8.4 Repeat Last Message	25
8.5 Message Length Control	25
Annex A (informative) Transaction Throughput	27
Annex B (informative) Equipment Compatibility Restrictions	33
Annex C (informative) Message and Transaction Security	34
Annex D (informative) Protocol Performance Comparisons	39

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).

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

[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: Data 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**.

²CCITT publications are available from the CCITT General Secretariat, International Telecommunications Union, Sales Section, Place des Nations, CH-1211, Genève 20, Switzerland/Suisse.

³EIA publications are available from Global Engineering, 1990 M Street NW, Suite 400, Washington, DC, 20036, USA.

⁴IEEE 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.

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.

- 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.

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.

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:

- 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 $\Omega \pm 10\%$, 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]

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

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 $1 \text{ in } 10^4$ 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 $1 \text{ in } 10^{10}$, as specified in the IEEE Std C37.1-1987 [7].

All transmitters shall generate the selected data rate within a tolerance of $\pm 0.01\%$ 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.

⁶The 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.

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 “squench” 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.