IEEE Standard for SCADA and Automation Systems

IEEE Power Engineering Society

Sponsored by the
Substations Committee

C37.1™

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

8 May 2008

IEEE Std C37.1™-2007
(Revision of
IEEE Std C37.1-1994)

IEEE Std C37.1™-2007
(Revision of
IEEE Std C37.1-1994)

IEEE Standard for SCADA and Automation Systems

Sponsor
Substations Committee
of the
IEEE Power Engineering Society

Approved 5 December 2007

IEEE-SA Standards Board

Abstract: The requirements for SCADA and automation systems in substations are defined. This standard defines the process of substation integration as the design process that is the foundation for substation automation. Functional and environmental requirements are provided for all IEDs located in the system. Tutorial material is included in the annexes to address common issues with systems without introducing requirements. Information is also presented in the annexes regarding SCADA masters.

Keywords: automatic control, data acquisition, IED, Intelligent Electronic Device, SCADA, substation integration, substation automation, supervisory control

---

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-7381-5378-0 STD95762
Print: ISBN 978-0-7381-5379-7 STDPD95762

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied "**AS IS**."

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.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

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 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 societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

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

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Introduction

This introduction is not part of IEEE Std C37.1-2007, IEEE Standard for SCADA and Automation Systems.

This standard applies to systems used for monitoring, switching, and controlling electric apparatus in unattended or attended stations, generating stations, and power utilization and conversion facilities. It does not apply to equipment designed for the automatic protection of power system apparatus or for switching of communication circuits. The requirements of this standard are in addition to those contained in standards related to the individual devices (e.g., switchgear).

This document is a significant revision of IEEE Std C37.1-1994. This revision reflects current technology that is generally being provided to meet the requirements of utilities. Originally, this standard was a section of ANSI C37.2-1970, which also contained device function numbers. ANSI C37.2-1970 was revised into two standards: IEEE Std C37.1-1979, IEEE Standard Definition, Specification, and Analysis of Manual, Automatic, and Supervisory Station Control and Data Acquisition, and IEEE Std C37.2™-1979, IEEE Electric Power System Device Numbers. Previous editions were approved by the IEEE in 1962, 1956, 1945, and 1937. The original work on this subject was done by the American Institute of Electrical Engineers (now the Institute of Electrical and Electronic Engineers) and published in 1928 as AIEE No 26. The latest revision of the standard on Electrical Power System Device Function Numbers is IEEE Std C37.2-1996 (Reaff 2001) [B11].[a]

This standard applies to rapidly changing technology. It is anticipated that frequent revision may be desirable. This revision was prepared by the Electric Network Control Standards Working Group of the Data Acquisition, Processing, and Control Systems Subcommittee of the IEEE Power Engineering Society Substations Committee. The revision is an attempt to bring the standard up to date and further broaden its applicability with respect to control, supervisory, and telemetry.

IEEE Tutorial Course Text EHO 337-6 PWR referenced in the previous revision of this standard is no longer available from the IEEE service center. In addition, the corresponding Tutorial Video Tape HVO 245-1-POT referenced in the previous revision of this standard has been discontinued by the IEEE. The following special publications and tutorial texts are available from the IEEE service center:

a) IEEE Tutorial “Substation Automation Tutorial” [B17] is recommended for those not familiar with substation automation systems

b) IEEE Tutorial “The Protective Relay IED in the Automation World” [B18]

c) IEEE Tutorial “Adding New Life to Legacy SCADA Systems” [B16]

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

[a] The numbers in brackets correspond to those of the bibliography in Annex I.

Copyrights

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this guide are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE-SA Standards Board for approval, the Electric Network Control Systems Standards Working Group had the following membership:

Craig Preuss, *Chair*

Dennis K. Holstein, *Vice-chair*

Alex Apostolov
William J. Ackerman
Dennis Carr
Mason Clark
Kenneth Cooley
Bob Corlew
Geoff Crask
Steven Dalyai
Michael Dood
James Evans
Ron Farquharson
James Gardner
William Harlow
Marc Lacroix
Greg Luri
Edward Miska
Scott Mix
Peter Raschio
James Recchia
Sam Sciacca
H. Lee Smith
John Tengdin
Michael Thesing
Michel Toupin
Peter Wong

The following members of the balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

William J. Ackerman
Steven Alexanderson
Ali Al Awazi
David Bassett
Thomas Basso
Anne Bosma
Stuart Bouchey
Steven Brockschink
Chris Brooks
Gustavo Brunello
James Case
Danila Chernetsov
Keith Chow
Tommy Cooper
Bob Corlew
James Cornelison
Bostjan K. Derganc
Thomas Dineen
Kevin Donahoe
Michael Dood
Paul Drum
Gary Engmann
Fredric Friend
Keith Gray
Charles Grose
Randall Groves
Ajit Gwal
Rutger A. Heunks
Scott Hietpas
Gary Hoffman
David Horvath
James Huddleston
C. Huntley
James Jones
Lars Juhlin
Innocent Kamwa
Piotr Karocki
Gael Kennedy
Joseph L. Koepfinger
Jim Kulchisky
Marc Lacroix
Chung-Yiu Lam
Raluca Lascu
Albert Livshitz
Federico Lopez
Faramarz Maghsoodlou
Keith N. Malmedal
Omar Mazzoni
John McDonald
Jeffrey Merryman
Charles Morse
Jerry Murphy
Bruce Muschlitz
Arthur Neubauer
Michael S. Newman
T. Olsen
William Petersen
Craig Preuss
Iulian Profir
Peter Raschio
Charles Rogers
Anne-Marie Sahazizian
Bob Saint
Bartien Sayogo
Thomas Schossig
Douglas Seely
Mark Simon
Veselin Skendzic
H. Smith
John Spare
Thomas Starai
Charles Sufana
James Swank
John Tengdin
Joe Uchiyama
John Vergis
Kenneth White
Roland Youngberg
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 5 December 2007, it had the following membership:

Steve M. Mills, *Chair*
Robert M. Grow, *Vice Chair*
Don Wright, *Past Chair*
Judith Gorman, *Secretary*

Richard DeBlasio	Richard H. Hulett	Narayanan Ramachandran
Alex Gelman	Hermann Koch	Greg Ratta
William R. Goldbach	Joseph L. Koepfinger*	Robby Robson
Arnold M. Greenspan	John Kulick	Anne-Marie Sahazizian
Joanna N. Guenin	David J. Law	Virginia C. Sulzberger
Julian Forster*	Glenn Parsons	Malcolm V. Thaden
Kenneth S. Hanus	Ronald C. Petersen	Richard L. Townsend
William B. Hopf	Tom A. Prevost	Howard L. Wolfman

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Satish K. Aggarwal, *NRC Representative*
Alan H. Cookson, *NIST Representativ*e

Michelle D. Turner
IEEE Standards Program Manager, Document Development

Soo H. Kim
IEEE Standards Program Manager, Technical Program Development

Contents

IEEE Standard for SCADA and Automation Systems

IMPORTANT NOTICE: This standard is not intended to assure safety, security, health, or environmental protection in all circumstances. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.

1. Overview

1.1 Scope

This standard applies to, and provides the basis for, the definition, specification, performance analysis, and application of SCADA and automation systems in electric substations, including those associated with generating stations and power utilization and conversion facilities.

1.2 Purpose

The purpose of this standard is to provide guidance to the engineer responsible for the design and specification of SCADA and automation systems.

1.3 Use

The designer/specifier may use this standard in the design, procurement, and implementation of all or a portion of a system. This document is a generic standard for SCADA and Automation Systems. The designer/specifier shall select those portions of this document that are applicable to a specific system. This may include the modification of tables and requirements contained herein.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

ANSI S1.4, Specification for Sound Level Meters-ASA 47.[1]

ANSI S12.10, Acoustics—Measurement of airborne noise emitted by information technology and telecommunications equipment—ISO 7779:1999.

ANSI X3.1, Information Systems—Data Transmission—Synchronous Signaling Rates.[2]

EIA/ECA-310, Cabinets, Racks, Panels, and Associated Equipment.[3]

IEC 60529, Degrees of Protection Provided by Enclosures (IP Code).[4]

IEC 60870-6, Telecontrol Equipment and Systems.

IEC 61131-3, Programmable Controllers—Part 3: Programming Languages.

IEC 654-3, Operating Conditions for Industrial Process Measurement and Control Equipment, Part III, Mechanical Influences.

IEC 61850, Communication Networks and Systems in Substations.

IEEE Std 487™, IEEE Recommended Practice for the Protection of Wire-Line Communication Facilities Serving Electric Supply Locations.[5, 6]

IEEE Std 525™, IEEE Guide for the Design and Installation of Cable Systems in Substations.

IEEE Std 1379™, IEEE Recommended Practice for Data Communications between Intelligent Electronic Devices and Remote Terminal Units in a Substation.

IEEE Std 1588™, IEEE Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

IEEE Std 1590™, IEEE Recommended Practice for the Electrical Protection of Communication Facilities Serving Electric Supply Locations Using Optical Fiber Systems.

IEEE Std 1613™, IEEE Standard Environmental and Testing Requirements for Communications Networking Devices Installed in Electric Power Substations.

IEEE Std 1615™, IEEE Recommended Practice for Network Communication in Electric Power Substations.

IEEE Std 1646™, IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.

---

[1] ANSI publications are available from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[2] ANSI X3.1 was withdrawn in 1997; however, copies can be obtained from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http://www.ansi.org/).

[3] EIA publications are available from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112, USA (http://global.ihs.com/).

[4] IEC publications are available from the Sales Department of the International Electrotechnical Commission, Case Postale 131, 3, rue de Varembé, CH-1211, Genève 20, Switzerland/Suisse (http://www.iec.ch/). IEC publications are also available in the United States from the Sales Department, American National Standards Institute, 25 West 43rd Street, 4th Floor, New York, NY 10036, USA (http:// www.ansi.org/).

[5] IEEE publications are available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).

[6] The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

IEEE Std C37.98™, IEEE Standard Seismic Testing of Relays.

IEEE Std C37.115™, IEEE Standard Test Method for Use in the Evaluation of Message Communications between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System.

IEEE Std C37.118™, IEEE Standard for Synchrophasors for Power Systems.

IEEE Std C37.231™, IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control.

IRIG Standard 200, IRIG Serial Time Code Formats, Telecommunications and Timing Group, Range Commanders Council, U.S. Army White Sands Missile Range.[7]

NEMA 250, Enclosures for Electrical Equipment (1000 Volts Maximum).[8]

TIA-232-F, Interface between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange.[9]

TIA 334-C, Signal Quality at Interface Between Data Terminal Equipment and Synchronous Data Circuit-Terminating Equipment for Serial Data Transmission.

TIA/EIA 404-B, Standard for Start-Stop Signal Quality for Non-Synchronous Data Terminal Equipment.

TIA/EIA 422-B, Electrical Characteristics of Balanced Voltage Digital Interface Circuits.

TIA/EIA 423-B, Electrical Characteristics of Unbalanced Voltage Digital Interface Circuits.

TIA-485-A, Electrical Characteristics of Generators and Receivers for Use in Balanced Digital Multipoint Systems.

TIA-530-A, High Speed 25 Position Interface for Data Terminal Equipment and Data Circuit-Terminating Equipment, Including Alternative 26-Position Connector.

3. Definitions, acronyms, and abbreviations

3.1 Definitions

For the purposes of this standard, the following terms and definitions apply. *The Authoritative Dictionary of IEEE Standards, Seventh Edition* [B10], should be referenced for terms not defined in this clause.

3.1.1 accuracy: The difference between the actual value of a measurement and the indicated value of the measurement.

[7] See https://wsmrc2vger.wsmr.army.mil/rcc/PUBS/pubs.htm
[8] NEMA publications are available from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112, USA (http://global.ihs.com/).
[9] TIA publications are available from Global Engineering Documents, 15 Inverness Way East, Englewood, CO 80112, USA (http://global.ihs.com/).

NOTE—Accuracy is usually expressed in terms of percentage deviation from a reference value, commonly full scale of the measuring device and less commonly the actual value at the input. Note that accuracy for power measurements are expressed with an applicable power factor range. (Real power measured at less than 10% power factor or reactive power measured at greater than 90% power factor tend to have significant errors) Note also that if the "measuring device" is a current transformer, its full scale rating may be significantly larger than the displayed value (e.g., a 3000 ampere 0.3% CT measuring a 300 ampere load current). In this case, its accuracy is 0.3 % × 3000 or ± 90 amps, so the accuracy of a 300 amp load measurement is actually 300 ± 90 amps or ± 30% of the measured value.[10]

3.1.2 availability: Availability (A) is defined in the following as the ratio of uptime to total time (uptime + downtime). It is customary to express availability in percentage, usually as 99.xxx, where xxx are numbers that complete the percentage.

NOTE—See 8.3.

3.1.3 chatter filter: A facility that is used to disable a digital input point if the number of state changes of that point during a defined time interval is excessively high.

3.1.4 clear time: The amount of time that the select relay will continue to operate after the master trip or close has operated. Clear time can also mean operating time.

3.1.5 control arm time-out: The maximum amount of time that a device will wait to receive an execute command after receiving a select or arm command. Refer to select command.

3.1.6 debounce period: The amount of time for which the state of a digital input point shall be detected in a valid "on" or "off" condition before it is considered to be in that position.

3.1.7 diagnostics: Programs executed to check the health of the device on either a periodic or random interval.

3.1.8 double-point status: A pair of digital input points that can assume four different states. States 1 and 2 may be described as NORMAL or VALID states, and states 3 and 4 may be described as TRAVELLING or ABNORMAL or INVALID states. Purpose is to detect complete changes of state (transitions), while ignoring any incomplete transitions.

3.1.9 Form A Counters: A single-point type of digital input that counts rising-edge changes of state (or transitions).

3.1.10 Form C Counters: Also known as KYZ pulses. A pair of digital inputs that count the transitions from one valid state to the next valid state, while ignoring any transitions to invalid states. An increase in the count occurs when both inputs change to the opposite state (one turns on, one turns off).

3.1.12 latency: The time between when sensor outputs are present at the physical interface of a measuring device until its value is available to the first user or program.

3.1.11 local area network (LAN): A LAN is a network normally designed for a limited geographical area, such as a utility substation or an office area. It is generally capable of transmitting data, voice, and image and video information. In most cases a LAN is considered to be an integral part of the facility, and is owned by the facility owner. A substation LAN may have sub-networks or segments to manage information flow and access. Segments may also be added to accommodate passing messages over distances exceeding the basic messaging distance inherent in the media. Serial networks can often be implemented over a LAN by embedding the serial messages in a network protocol.

3.1.13 lock-out period: A parameter that defines the length of time that a device or point will be disabled from operation after exceeding a pre-defined error condition.

[10] Notes in text, tables, and figures are given for information only, and do not contain requirements needed to implement the standard.

3.1.14 pseudo points: System data points generated internally by a software application. They often represent the results of a calculation, or the internal state of a process.

3.1.15 recloser: Abbreviated name for automatic circuit recloser.

3.1.16 resolution: The smallest increment of a value that can be resolved, often expressed as percent of full scale. It is better expressed in engineering units of the measured value.

NOTE—If the resolution of a 1000 full scale value is 0.1% of full scale, then values displayed on a CRT or report should only be whole numbers (no decimal values).

3.1.17 scan (interrogation): The process by which a data acquisition system interrogates intelligent electronic devices (IEDs) for points of data.

3.1.18 scan cycle: The time in seconds required to obtain a collection of data (e.g., all data from one IED, all data from all IEDs, or all data of a particular type from all IEDs).

3.1.19 Scan Enable: A feature that allows or disallows a particular input point to be scanned.

3.1.20 Select Before Operate: Two-part command sequence used to achieve high communications security and hardware verification before the control is actually executed. See Annex D for more information.

3.1.21 single point/multiple point control: The control of a single point versus global control of multiple points.

3.1.22 time skew: The elapsed time between when the first value in a set of measurements is taken until the last value of the same set of measurements is taken. The data set may consist of measurements made in a close proximity, as within a single substation, or across a large geographic area as in the flow measurements for a large transmission network.

3.1.23 unavailability: The ratio downtime/(uptime + downtime). The ratios of downtime to total time (uptime + downtime), or downtime/(uptime + downtime). It is often expressed as a maximum period of time during which the variable is unavailable, e.g., 4 h per month.

3.1.24 update periodicity: The time between updates, sometimes expressed as the rate at which a measurement is updated (frequency).

3.1.26 virtual input/output (I/O): An I/O point such as status, control, or analog that is not physically wired to an IED.

3.1.25 wide area network (WAN): A WAN provides long-distance transmission of data, voice, and image and video information over a large geographical area. A WAN can be owned by a utility or WAN services can be leased from telecommunication providers. WANs connect LANs together. For automating substations, an enterprise WAN connection may become the pathway to link the substation to the enterprise.

3.2 Acronyms and abbreviations

AGA	American Gas Association
API	application programming interface
CPU	central processing unit
CRC16	16-bit cyclic redundancy check
CSMA/CD	collision sensing multiple access/collision detection
CT	current transformer
DISCO	distribution company

DMS	Distribution Management System
DNP/DNP3	Distributed Network Protocol, version 3.0
DPI	double-point information
EMC	electromagnetic compatibility
EMI	electromagnetic interference
EMS	Energy Management System
EPROM	erasable programmable read-only memory
FAT	factory acceptance test
FMEA	failure modes and effect analysis
FPGA	Field Programmable Gate Array
GAL	Generic Array Logic
GENCO	generation company
GPR	ground potential rise
HMI	Human Machine Interface
I/O	inputs/outputs
ICCP	Inter-Control Center Communication Protocol
IED	intelligent electronic device
IRIG-B	Inter Range Instrumentation Group format B
ISA	Instrumentation, Systems, and Automation Society
ISO	Independent System Operator
IT	information technology
ITU	International Telecommunication Union
LAN	local area network
LCD	liquid crystal display
LED	light emitting diode
MTBF	mean time between failure
MTTR	mean time to repair
NERC	North American Electric Reliability Corporation
NIM	network interface module
NTP	Network Time Protocol
ODBC	Open Database Connectivity
PLC	programmable logic controllers
POSIX	Portable Operating System Interface
PROM	programmable read-only memory
PSTN	Public Switched Telephone Network
PT	potential transformer
RAID	redundant array of inexpensive disks or redundant array of independent disks
ROM	read-only memory
RTO	Regional Transmission Organization
RTU	remote terminal unit
SAT	site acceptance test
SCADA	Supervisory Control and Data Acquisition
SNTP	Simple Network Time Protocol
SOE	sequence of events
SPI	single-point information
SQL	structured query language
SWC	surge withstand capability
TASE	Telecontrol Application Service Element
TCP/IP	Transmission Control Protocol/Internet Protocol
TRANSCO	transmission company
UHF	ultra high frequency
UPS	uninterruptible power supply
UTP	Unshielded Twisted Pair
VDU	video display unit
WAN	wide area network

4. System overview

4.1 General

In recent years, network-based substation automation has greatly evolved with the use of IEDs. The processing is now distributed and functions that used to be done at the control center or remote terminal unit (RTU) can now be done by the IED or a group of networked IEDs. Despite the fact that many functions can be moved to the IED, utilities still need a master station for the operation of the power system. Due to the restructuring of the electric industry, traditional vertically integrated electric utilities are replaced by many entities such as: GENCO, TRANSCO, DISCO, ISO, RTO, etc. To fulfill their role, each of these entities needs a master station and/or control center to receive and process data and take appropriate control actions.

4.2 Master station (control center) architecture and functions

Modern Supervisory Control and Data Acquisition (SCADA) master stations have both software and hardware in a distributed architecture. The processing power is distributed among various computers and servers that communicate with each other through a real-time dedicated LAN in the control center.

Distributed systems have many advantages over centralized systems. Since the data processing is shared on the network, the various servers require less processing power than in a centralized system. In this way, the cost of computers can be reduced. It is also easier to upgrade or to add servers if additional processing power is required. Another advantage of distributed systems is that the failure of one server does not necessarily affect the whole system. Figure 1 shows an example SCADA master station system architecture without the inclusion of network security.

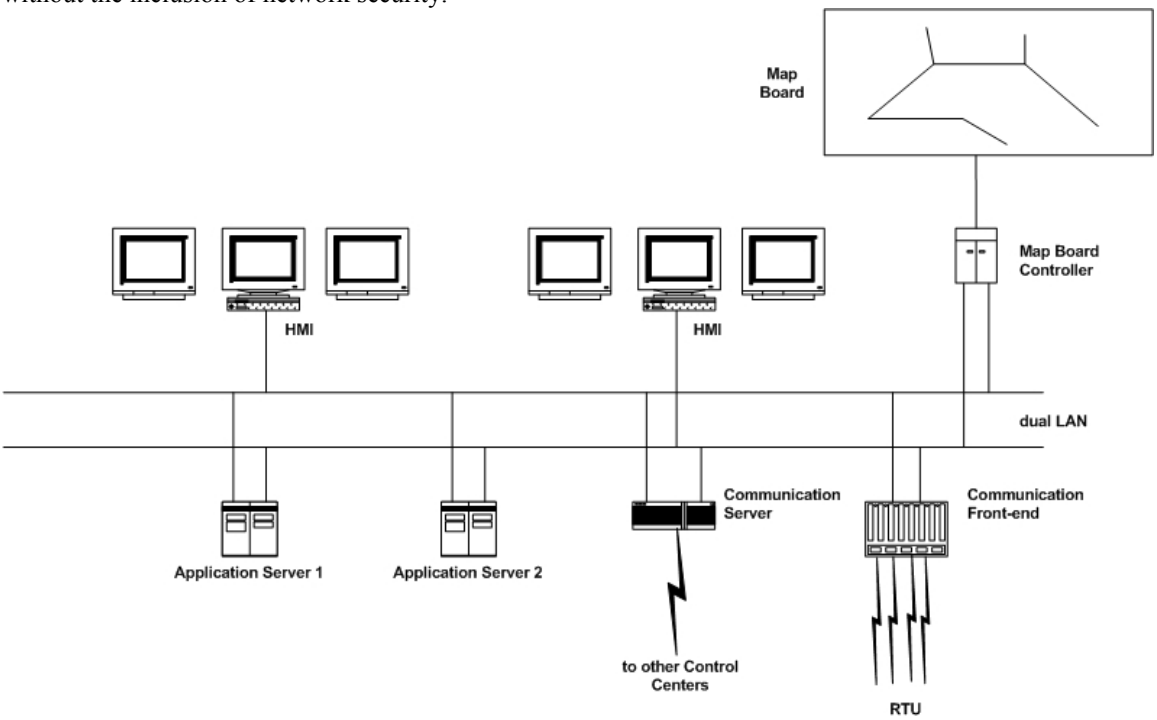

Figure 1—Example SCADA master station system configuration at a control center without network security shown

Modern SCADA master station systems can use open architecture features that support interconnections with other systems. Open system standards also support interfaces with other vendors' products.

To ensure the openness, the system should comply with international standards, such as POSIX®, or industry's de-facto standards such as Microsoft® Windows®, X Window,[11] and related products for the computer applications; IEC 60870-6 (TASE.2)[12] for communications to other control centers; and IEEE Std 1379 for remote terminal unit (RTU) communications. Despite the fact that most vendors offer open systems, they each develop their own application programming interface (API). This API enables software modules to communicate with each other by using common objects and data exchange mechanisms. The IEEE and the IEC are developing appropriate standards to ensure inter-operability at the API level.

The main elements of the SCADA system illustrated in Figure 1 are as follows:

— **Human Machine Interface (HMI):** This interface comprises the mimic board and multi video display unit (VDU) workstations:

  — **Mapboard:** The mapboard (mimic board, or wall board displays an overview of the power system. It shows a simplified representation of the power system preserving as much detail as possible, and is arranged to approximated the geographical orientation of the power system. It is useful in observing major power system disturbances covering a large geographic area. Two different map board technologies are used in control centers.

    The mosaic type mapboard uses small mosaic tiles with the static type information etched or taped on the tiles. Indicators are used for dynamic information such as breaker status. A matrix of light emitting diodes (LEDs) can also be inserted in the mimic board to offer animation capability. If a modification is needed, old tiles are replaced by new ones—a time-consuming activity.

    Today, large screen displays (projection systems, large-scale LCD systems, plasma systems, etc.) are more commonly used in control centers. The system software prepares and sends to the mapboard controller the pictures to be displayed. This type of mapboard requires much less effort when the electric network configuration is modified. A new picture is edited and propagated to the mapboard. It is also significantly easier to ensure consistent display of the electric network configuration across multiple control centers.

    One significant advantage of the mosaic tile mapboard is the fact that the network orientation and topology remains visible to a user even in the event of a total power failure, or a malfunction of the VDU driver or VDU itself.

  — **Multi-VDU Interface:** These are workstations used to view the status of power system devices in more detail. In modern SCADA systems, multi-VDU workstations give operators easy access to a wide variety of application and control functions. These workstations can support four or more physical or virtual VDUs and offer full graphic capability with multi-window techniques such as pan, zoom, pop-up/pull-down menu and "drag and drop." Interactive menu selection speeds up switching between applications.

— **Application servers:** SCADA systems have several different servers, as follows:

  — **Core SCADA subsystems:** This server is used mainly for data processing functions and real-time operational process control.

  — **Database subsystems:** This server supports the historical database and other system databases.

[11] This information is given for the convenience of the users of this standard and does not constitute an endorsement by the IEEE of these products. Equivalent products may be used if they can be shown to lead to the same results.
[12] Information on references can be found in Clause 2.

  - **Advanced application subsystems:** These servers support all Energy Management System (EMS) or Distribution Management System (DMS) applications. The main characteristic of this server is its processing power. More than one server may be used for these applications.
  - **Historical databases:** These servers support the database that contains all historical data. This information can also be used for system studies or operators' training. Data are forecasted or estimated for future values.
  - **Configuration and management:** This server is used for the control, management, and maintenance of the whole SCADA system. From this server, the operation mode of each server can be controlled and system backup functions can be ordered.
- **Communication front-end:** This system is used for data acquisition from RTUs and field equipment. It provides functions such as acquiring the RTU data, protocol conversion, security check, temporary storage of analog and digital data, and detection of analog value and digital state changes.
- **External communication server:** This server provides data exchange with other control centers. A standard protocol, such as IEC 60870-6 (TASE.2) should be used to exchange real-time and archive data. As this server provides a window into the master station, special attention should be paid to protecting unauthorized access via this server, and to the protection of the data residing in the master station database from unauthorized access or modification. See 5.5 for additional security requirements.

4.3 Remote site (substation) control system functions and architecture

Prior to using IEDs as the control and monitoring interface to the power system equipment, the substation RTU was the gathering point for substation data and control circuits. The substation protection and automatic controls provided the basic functions, and the RTU was an overlay to provide remote control and monitoring. With IEDs, the RTU may still be specified as all or as only a part of the substation control and data acquisition system and may still provide the communications interface to the master station. By using substation integration techniques to connect IEDs together using one or more communication networks, the traditional RTU functionality becomes more distributed within the substation with the result that the traditional RTU may not even exist. Once the substation IEDs are integrated together, it is then possible to accomplish substation automation.

The main elements of a substation automation system are similar to those in a SCADA master and should be specified for a substation automation system. The following elements may be contained in a system:

- **HMI:** This hardware interface runs software that creates graphics on a video display that replace the traditional mimic boards, analog displays, control switches, and selector switches. The hardware component usually includes an IEEE Std 1613 substation-hardened computer with a display terminal and keyboard that are mounted in a rack or panel. The HMI hardware may also be a commercially available computer that is appropriately isolated from the substation environment as required.
- **RTU:** The substation RTU may still be a traditional RTU with hard-wired inputs and outputs and communication with one or more SCADA masters. With the proliferation and increasing capabilities of IEDs, however, the RTU may actually combine several different elements into one device. For example, the RTU may provide the substation HMI, the data concentrator, and remote access controller.
- **Data Concentrator:** A data concentrator collects the required data from all substation IEDs, even the RTU as necessary, and provides data exchange with other systems (possibly even other SCADA masters). Different system configurations are possible such that the RTU, HMI, and data concentrator elements are in one device.

— **Remote Access Controller:** This IED enables remote access to the substation IEDs for remote configuration, access, and data retrieval. Different system configurations are possible, such that the remote access controller is the same IED as the data concentrator.

These elements perform at least the following functions in a substation automation system:

a) Measurement

b) Status monitoring

c) Control

d) Ancillary services

e) Time synchronization

f) Programmed logic

Clause 5 contains the specification for these functions and elements that the designer/specifier can use to specify a substation automation system. Many of these elements and functions are combined together into a block diagram, which the designer/specifier may require as part of the substation automation system. Figure 2 is a simplified block diagram taken from IEEE Std C37.115 that does not show any network security. It is an example of a substation automation system with all IEDs on a substation LAN. The example block diagram shows a single LAN and non-redundant IEDs. Other architectures may include redundant IEDs, LANs, and communication channels. IEDs that are not network enabled are typically connected to the substation LAN via a data concentrator or serial device server (serial port server), which is not shown in the figure.

Not shown or included in Figure 2 are separate connections to the maintenance ports of the IEDs for remote access. In the past, these ports were often connected to a port switch and an auto-answer modem connected to a dial-up phone line, providing an additional communications channel into the substation. Many IEDs still support this method of remote access. As IEDs have added network ports, as shown in Figure 2, remote and local access to IEDs can now be accomplished over the substation LAN. In Figure 2, the connection from the substation to the EMS and other users at engineering work stations is through a WAN. The connection from the WAN to the substation LAN is through a router and firewall.

Figure 2 shows a “dedicated channel” from the SCADA master to the RTU, which is not meant to imply either serial or network connectivity, but to convey the concept that substation control systems may have both an interface to a SCADA master (for control by a regional operating center) and to the corporate EMS. The diagram shows two methods of data acquisition and control. One is via IEDs connected to the substation power system equipment and sensors. The other is via direct connections to the substation RTU. In both cases, the data may be stored in a database server or a separate connection to a remote historian or database may be provided (not shown). Depending on the capabilities of the substation HMI, the database server and the HMI may be combined into one device. This reduces the database generation and maintenance effort and simplifies the system design.

Figure 2 does not show any communication message encryption devices for any internal or external communications, although the router could address external encryption and authentication.

Figure 2 does show wiring for a timing signal from an IRIG-B generator, which is typically a GPS satellite clock that distributes a time signal to the substation IEDs using a separate timing wire. Depending on the timing requirements, the timing wire may not be necessary if the IED clocks can be accurately set over the LAN using the NTP, SNTP, or IEEE Std 1588.

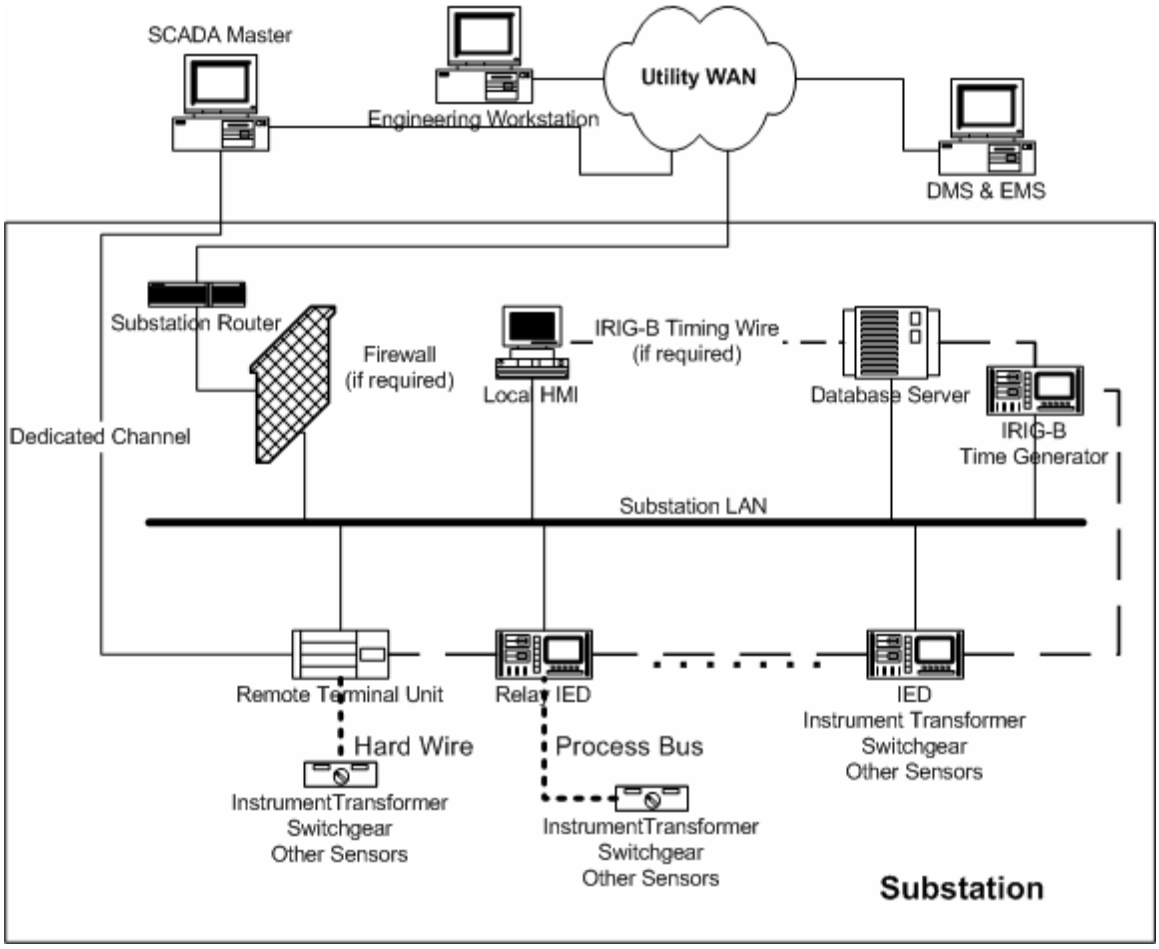

Figure 2—Example substation automation system architecture without security shown

The designer/specifier can use the following sections to specify the elements and functions of the system briefly discussed in 4.3.

5. System design

System design requires multiple steps and will most likely require multiple iterations. First, the designer/specifier should define the near and long-term system functionality. The most benefit from this definition will be obtained by using an analysis from an enterprise level such that corporate standards could be developed. This definition should be based upon the existing or planned electrical infrastructure. This definition should be based on reality. An overly aggressive plan may include components that will not be used or may be obsolete by the time such functions are implemented. The definition of requirements is usually based on perceived current needs and anticipation of future needs, and is therefore somewhat unconstrained. Confining the list to minimum requirements may leave users with unfulfilled requirements and the need for an upgrade sooner than desirable.

Once the functional requirements are defined, then decisions can be made regarding communication protocols (external and internal to the substation), IEDs, architecture, security, and availability. Conversely, selection of components and architectures is usually constrained by various elements such as pre-existing equipment, IED selection by other departments, equipment and procedure standards, costs, etc. Therefore, the system design may redefine previously established requirements, resulting in an iterative process in order to reach a satisfactory compromise.

This clause assumes the designer/specifier has a working knowledge of the functions common to SCADA and automation systems. The annexes of this standard provide important reference information on function implementation. The designer/specifier is encouraged to use these annexes to align the work with known common practices.

5.1 System function definitions

SCADA and Substation Automation systems can be viewed as providing specific key functions, such as the following:

a) Measurements

b) Status monitoring

c) Control

d) Ancillary services

e) Time synchronism

f) Programmed logic functions

The system design needs to include a definition of the required functions. Once the required functions are established, an assessment should be made to define the required performance.

CAUTION

To assist the designer/specifier, tables in this clause provide typical values representing industry consensus for a power transmission network. Requirements for particular transmission, distribution, or generation utilities are likely to be different. The system designer/specifier should determine the actual performance requirements.

These tables include the system functions previously listed. Not all functions require the same data set. The designer/specifier may find it useful to define subsets of measurements, status, and control points that have different performance requirements.

The tables in this clause also include the following typical performance requirements (whose definitions can be found in the definitions and annexes):

— Update periodicity (seconds)

— Accuracy (%)

— Unavailability (hours/month)

— Latency (seconds)

— Resolution (%)

— Time skew (seconds)

Typical is used in these tables to demonstrate that the values shown are for a specific example as previously discussed. If the designer/specifier is using these tables in a specification, then the word “typical” shall be removed from the tables. Where no values are present, no industry consensus was available.

System functions may have differing performance requirements specific to a group of users. These differences depend on the location, function, and needs of the users within the physical and organizational enterprise. It is valuable to group common requirements as requirement tiers within a function list so as to

fully understand how performance issues impact the system design. To recognize the differences, the tables have multiple-tier entries so that different performance requirements from users can be captured. Because of system, IED, or other limitations, implementers may need to use the most stringent requirements, which will impact performance requirements for some users.

The tables in this clause can be used as a basis for evaluating all aspects of system performance. For example, if the requirement is that power measurements be presented to the local substation HMI with only a two-second latency and refresh rate, the requirements for the local communications network and data handling of IEDs are bounded. These requirements may impose unreasonable communications network performance if the same performance is extended to the enterprise operation center or to the support staff workstations. A reasonable solution might be to allow longer, more suitable, latency and refresh for the operations center.

The designer/specifier should ensure that system testing requirements discussed in Clause 9 include confirmation of the performance requirements developed from this clause. The designer/specifier should also note that system alarms, discussed in 6.4.6, will be required in order to track performance requirements.

5.1.1 Measurement services

Table 1 is presented as a means to capture typical performance requirements for measurements.

Table 1—Typical measurement services performance requirements

	Typical measurement services performance requirements							
Enterprise/function	**Example measured elements**	**Update periodicity (s)**	**Accuracy (%)**	**Unavailability (h/mo)**	**Latency (s)**	**Resolution (%)**	**Time skew substation (s)**	**Time skew SCADA (s)**
Tier 1								
Substation operator indications	Voltage, Bus	5	0.3	4	1	0.1	1	1
Switching and tagging	Voltage, Line	5	0.3	4	1	0.1	1	1
End element control	Real and Reactive Power, Line	10	1.0	4	5	0.2	1	1
Low-priority alarm	Real and Reactive Power, Equip	10	1.0	4	5	0.2	1	1
High-priority alarm	Current, Line	5	0.3	4	1	0.1	1	1
System restoration	Current, Equip	5	0.3	4	1	0.1	1	1
	Frequency/Phase Angle	1-5	0.3	4	1	0.1	1	1
	Position, Regulator/valve	10	1.0	4	5	0.2	1	1
	Ancillary value	10	1.0	4	5	0.2	1	1
Tier 2								
Non-System Operator Enterprise User Indication	Voltage, Bus	15	0.3	24	10	0.1	1	1

	Typical measurement services performance requirements							
Enterprise/function	**Example measured elements**	**Update periodicity (s)**	**Accuracy (%)**	**Unavailability (h/mo)**	**Latency (s)**	**Resolution (%)**	**Time skew substation (s)**	**Time skew SCADA (s)**
System Planning	Voltage, Line	15	0.3	24	10	0.1	1	1
	Real and Reactive Power, Line	30	1.0	24	30	0.2	1	1
	Real and Reactive Power, Equip	30	1.0	24	30	0.2	1	1
	Current, Line	15	0.3	24	30	0.1	1	1
	Current, Equip	15	0.3	24	30	0.1	1	1
	Frequency/Phase Angle	30	1.0	24	30	0.2	1	1
	Position, Regulator/valve	30	1.0	24	30	0.2	1	1
	Ancillary value	30	1.0	24	30	0.2	1	1
Tier 3								
Auto Gen Control	Voltage, Bus	2	0.3	2	1	0.1	1	1
Auto restoration	Voltage, Line	2	0.3	2	1	0.1	1	1
Sectionalizing	Real and Reactive Power, Line	2	1.0	2	1	0.2	1	1
	Real and Reactive Power, Equip	2	1.0	2	1	0.2	1	1
	Current, Line	2	0.3	2	1	0.1	1	1
	Current, Equip	2	0.3	2	1	0.1	1	1
	Frequency/Phase Angle	2	1.0	2	1	0.2	1	1
	Position, Regulator/valve	10	1.0	2	1	0.2	1	1
	Ancillary value	10	1.0	2	5	0.2	1	1
Tier 4								
State Estimation	Voltage, Bus	15	0.3	8	30	0.1	1	1
Operator Load Flow	Voltage, Line	15	0.3	8	30	0.1	1	1
Optimal Power Flow	Real and Reactive Power, Line	15	3.0	8	30	0.2	1	1
Contingency Analysis	Real and Reactive Power, Equip	15	3.0	8	30	0.2	1	1
Security Surveillance	Current, Line	15	3.0	8	30	0.1	1	1
	Current, Equip	15	3.0	8	30	0.1	1	1
	Frequency/Phase Angle	30	3.0	8	30	0.2	1	1
	Position, Regulator/valve	30	1.0	8	30	0.2	1	1
	Ancillary value	30	1.0	8	30	0.2	1	1
Tier 5								
Power Quality	Voltage, Bus	ED				0.001		

	Typical measurement services performance requirements							
Enterprise/function	**Example measured elements**	**Update periodicity (s)**	**Accuracy (%)**	**Unavailability (h/mo)**	**Latency (s)**	**Resolution (%)**	**Time skew substation (s)**	**Time skew SCADA (s)**
Intra-Substation Phasor Measurements	Voltage, Line							
Inter-substation/utility Phasor measurements	Real and Reactive Power, Line							
Substation Events	Real and Reactive Power, Equip	OD						
System Events	Current, Line	OD						
	Current, Equip	OD						
	Frequency/Phase Angle	OD						
	Position, Regulator/valve	OD						
	Ancillary value	OD						
Tier 6								
Device configuration data	Configuration Files							
GIS data	Mapping Files							
Electric system topology	Archive Files							
Condition monitoring								
Archive								
Disturbance/Fault data								
Tier 7								
Substation/system time reference								
ED: Event Driven OD: On Demand								

5.1.2 Status monitoring service performance

Table 2 is presented as a means to capture typical performance requirements for status monitoring. Note that accuracy of digital inputs should only be applied when multiple sources are used to calculate the state of the status point.

Table 2—Typical status monitoring performance requirements

	Typical monitoring services performance requirements							
Enterprise/function	**Example measured elements**	**Update periodicity (s)**	**Accuracy (%)**	**Unavailability (h/mo)**	**Latency (s)**	**Resolution (%)**	**Time skew substation (s)**	**Time skew SCADA (s)**
Tier 1								
Substation operator indications	Breaker trip, fire	2	99.9	4.0	0.5	0.1	0.1	0.1
Switching and tagging	Substation HMI control	2	100	4.0	0.5	0.1	0.1	0.1
End element control		2	99.9	4.0	0.5	0.1	0.1	0.1
Substation algorithm		0.5	99.99	4.0	0.5	0.1	0.1	0.1
Tier 2								
Non-system operator enterprise user indication		30	99	12	30	1	1	1
Security surveillance		2–3		1				
Low-priority alarm	Doors, gates, water on floor,	5–10	99	12	60	1	N/A	N/A
High-priority alarm	Breaker trip, fire,	2–5	99	1	2	0.001	N/A	N/A
Substation sequence of events	Device state, time of state change,	OO	TS	8	20	0.001	0.0001	0.0001
System sequence of events	device state, time of state change,	OO	TS	99	20	0.001	0.0001	0.0001

OO: On Occurrence
TS: De-bounce logic, time stamp

5.1.3 Control services performance

Table 3 is presented as a means to capture typical performance requirements for control services. See D.1 regarding the implementation of SBO.

Table 3—Typical control services performance requirements

	Typical control services performance requirements						
Enterprise/function	**Example measured elements**	**Execution time (s)**	**Accuracy %**	**Unavailability (h/mo)**	**Latency (s)**	**Single point /multiple point**	**Feedback sequence**
Tier 1							
Substation operator control	Circuit breaker, capacitor switcher	2	99.99	4.0	1	Single	SBO
Auto-sectionalizing	Substation or field device	2	99.99	4.0	5	Multiple	None
Generation dispatch		2	99.9	4.0	1	Multiple	None
Substation algorithm		0.5	99.99	4.0	Depends	Depends	Depends
Tier 2							
Non-System Operator Enterprise User		15	99	24	N/A	Single	None
Low priority control	Pumps, lighting	15	99	12		Single	

5.1.4 Ancillary services performance

Ancillary services are often specified for a system, which are outside of the real-time services. Table 4 is presented as a means to capture typical performance requirements for ancillary services.

Table 4—Typical ancillary services performance requirements

	Typical ancillary services performance requirements								
Function	**Example measured elements**	**Update periodicity**	**Execution time (s)**	**Accuracy %**	**Unavailability(h/mo)**	**Latency (s)**	**Resolution (s)**	**Time skew substation (s)**	**Time skew SCADA (s)**
Tier 1									
Substation operator reports		N/A	20		4.0				
Non-system operator enterprise user reports		N/A	200		4.0				
State estimation		5	2		4.0				
Operator load flow		OD	0.5		4.0				
Tier 2									
Optimal power flow		OD	2		24				
Contingency analysis		15	900		24				
Tier 3									
Device configuration data		OD	15		24				
Electric system topology		OD	15		24				
System planning		N/A	15		12				
Condition monitoring		N/A	1800						
Archive		N/A	1800						
Disturbance/Fault data		N/A	300						
OD: On demand									

5.1.5 Time synchronism services performance

Table 5 is presented as a means to capture typical performance requirements for time synchronism services.

Table 5—Typical time synchronization services performance requirements

	Typical time synchronization services performance requirements						
Function	**Example measured element**	**Accuracy %**	**Unavailability (h/mo)**	**Latency (s)**	**Resolution (s)**	**Time skew substation (s)**	**Time skew SCADA (s)**
Tier 1							
Substation operator reports	Operating sequence of events logs		4.0	3	0.001	0.010	0.010
Non-system operator enterprise user reports	Non-operating sequence of events logs		4.0	300	0.001	0.010	0.010
Diagnostic task force	Disturbance reports			28 800	0.001	0.010	0.010
Tier 2							
Archive							
Disturbance/fault data			4.0	300	0.001	0.010	0.010
Tier 3							
Synchrophasors							

5.1.6 Programmed logic services performance

Table 6 is presented as a means to capture the typical performance requirements for programmed logic services.

Table 6—Typical programmed logic performance requirements

	Typical programmed logic performance requirements						
Function	**Example measured element**	**Execution time (s)**	**Accuracy %**	**Unavailability (h/mo)**	**Latency (s)**	**Resolution (s)**	**Time skew Substation (s)**
Tier 1							
Automatic generation control	Unit commitment	1.5	2.0	3	0.10		1.0
Switching and tagging	Interlocks	1.0		1	1.0	0.5	1.0
Auto restoration	Transmission line reclosing	5.0		1	5.0	0.1	3.0
Sectionalizing	Feeder sectionalizing						
System restoration							
Tier 2							

5.2 Selection of IEDs

IED selection should begin only after the functional requirements are determined as previously discussed. However, when IEDs are chosen to satisfy certain primary functions, they may impact the system overall design, performance, and architecture. Reconciling the functional and performance requirements with the functions and performance available from the pre-selected IEDs may impose some compromise. The designer/specifier should address the following considerations for both physical, calculated, and virtual I/O.

5.2.1 Common considerations

Some common considerations the designer/specifier should assess for most functional requirements are at least the following:

a) Effects of hardware/software power cycle and restart

b) Effects of equipment maintenance on critical data

c) Provisions to view I/O value and state

d) Provisions to view point mapping

e) Processing time for the parameters present at the IED inputs to be available as a parameter at the communications port. Data processing capabilities shall be defined for each equipment item and all applicable data types.

f) Ease of automated data retrieval and centralized storage for trends, events, disturbances, and faults for IEDs.

g) Input power requirements when IED will be placed on the DC system.

5.2.2 Functional requirements

This subclause contains the functional requirements the designer/specifier should use for system specification.

5.2.2.1 Measurements

The IEDs selected should use an acceptable process to meet the measurement functional requirements. The designer/specifier is advised to assess the impact of at least the following measurement characteristics on their performance expectations:

a) Accuracy over the expected operating range

b) Resolution over the full operating range

c) Instability at or near zero input or some constant value

d) Sample size used to compute the measurement

e) Sampling rate used to compute the measurement

f) Algorithms available for producing “instantaneous” and “time averaged” analog values

g) Time for a step change at the input to be processed

h) Burden on the instrument transformers or sensors

i) Leakage current impacts from shared inputs and outputs

5.2.2.2 Input status monitoring

The IEDs selected should use an acceptable process to meet the input status monitoring functional requirements. The designer/specifier is advised to assess the impact of at least the following input status monitoring characteristics on their performance expectations:

a) Time to recognize a change of state

b) Sampling rate

c) De-bounce options

d) Available counting registers for state changes

e) Available input processing for change of state, e.g., momentary change detect

f) Time tagging capability, resolution, and accuracy

g) Wetting voltage and current for inputs

h) Isolation

i) Support for different input configurations, e.g., form A, form B, form C

5.2.2.3 Control

The IEDs selected should use an acceptable process to meet the control functional requirements. The designer/specifier is advised to assess the impact of at least the following control characteristics on their performance expectations.

a) The time delay to execute control output once a control command has been sent to or received from a communication port

b) Time delay after a control command has been executed before another command can be initiated

c) Support for control of multiple points per command

d) Output interface compatibility with substation control requirements

e) Control output isolation

f) Support for "select-before-operate" control commands

g) Support for momentary and maintained outputs

h) Provisions to block, or "tag," single or multiple outputs for the IED

i) Support for different output configurations, e.g., form A, form B, form C

5.2.2.4 Ancillary services

Most automation systems provide ancillary services over the substation communication network. These include configuration, file transfer, log and data capture, and diagnostic observation. They often involve movement of large blocks of data as well as interaction with IEDs that are serving system users. The designer/specifier should be mindful of the impact their IED selection makes on the system while ancillary services are being performed with regard to at least the following concerns:

a) Additional traffic affecting the performance of the system networks

b) Potential for corrupting system mapping to other functions

c) Potential for injecting "interfering or false" data onto the substation communication network

d) Potential for compromising IED security

e) Potential for interrupting critical communications

5.2.2.5 Time synchronization

IEDs may need to use time in their computation, logging, and reporting functions. The designer/specifier should assess the IED choices with regards to the method(s) used for synchronizing time across the population of IEDs. The IEDs chosen shall share a common method of time synchronization and be capable of maintaining the required synchronism for the system over a suitable period without overly frequent time re-synchronizations. Time synchronization may require a separate time synchronization network to maintain the specified time drift requirements (such as IRIG-B). IED time synchronization should support IEEE Std 1646. If time tagging of events to ± 1 ms is a requirement, then the IED clocks shall be set to ± 0.1 ms. For IEDs computing synchrophasor data, the maximum allowable time error in IEEE Std C37.118, leaving no additional error margin in computing synchrophasor data, is ± 26 μs for a 60 Hz system and ± 31 μs for a 50 Hz system.

5.2.2.6 Programmed logic

Programmed logic is a common feature of automation systems. There are any number of IED platforms upon which logic may be deployed. Some IEDs have programmed internal logic, where their normal function includes protection algorithms. Other IEDs are programmable devices such as PLCs. Selecting the appropriate platform for logic should include at least the following considerations:

a) Process to upload and download programs

b) Support for program de-bugging and troubleshooting

c) Support for IEC 61131-3 programming languages

d) Portability of developed algorithms between devices from the same or different vendors

e) Remote program control support

f) Required performance for the intended task including data acquisition, processing, and delivery

g) Failure and recovery modes

h) Expandability

i) Organizational support for the selected platform and program tasks

j) Behavior of the IED in response to the programmed logic before the IED has initialized all of the logical variables. This includes the methodology utilized to handle variables as they are placed in non-volatile memory and the means of creating the non-volatile memory

k) Self-diagnostics

5.2.2.7 Protection

Protection IEDs shall meet the criteria set for their primary function as specified by the utility protection staff. Protection IEDs used to perform functions secondary to protection should meet the system performance requirements for the primary system functions. As such, these IEDs may have reduced capability for other system functions that may impact integration of the protection IED into an integrated system.

5.2.2.8 Revenue meters

Revenue meter IEDs shall meet the criteria set for their primary function as specified by the utility revenue meter staff. Revenue meter IEDs used to perform functions secondary to revenue metering should meet the system performance requirements for the primary system functions. As such, these IEDs may have reduced capability for other system functions that may impact integration of the protection IED into an integrated system.

5.2.3 IED lifespan

IEDs are microprocessor based devices whose life expectancy, or life cycle, is shorter than that of major substation power equipment and possibly even the project life cycle. IED life cycle includes both hardware and firmware. When selecting IEDs, the designer/specifier should consider the maturity of the IED along its life cycle as indicated as follows:

a) New products may have yet undiscovered deficiencies and pose a challenge to integrate with older devices.

b) Mature devices may be nearing the end of their production life and could go out of production in the near future.

c) IED suppliers should be queried as to the expected production life. A manufacturer should support at least the following phases with advanced notice: cease production of new sales, cease production of spares and replacements, cease availability of full technical support, and cease availability of any support (see IEC 61850-4).

d) IED suppliers should be queried as to their hardware/firmware change notification process (see IEEE Std C37.231).

e) IED suppliers should be queried for the lifespan of standard tools and processes for IED configuration, querying, and integration. Otherwise, some tools and processes will need to be revised whenever an IED is replaced without an exact duplicate.

f) IED components may become impossible to procure if the components are no longer in production.

IED obsolescence is inevitable. The designer/specifier should include as part of their design, provisions for the replacement of an IED. Users should expect to budget replacements of their IEDs, as the substation will likely last several IED lifetimes.

5.3 Human machine interface (HMI)

User interfaces at substations first started out as a switchboard interface. This was an assemblage of instruments, indicators, annunciators, switches and associated hardware placed on the relay panels or switchboard in such a way as to represent the electrical connectivity and operating condition of the substation. They are clearly identifiable by their unique shape and appearance that distinguishes them from functionally similar devices for other industries. These devices are connected directly to control and monitoring circuits of power equipment. The operation of equipment through this interface is generally restricted to operators or their delegate. This switchboard interface has evolved over the decades.

With the introduction of IEDs, the traditional switchboard interface is being replaced by HMI software loaded on computer hardware. The designer/specifier has a wide choice of HMI vendors that support a wide range of functionality. HMI software may be tightly integrated into a hardware platform such that when the HMI is ordered the software is actually an option for the hardware. The designer/specifier should use this section to determine some of the important criteria for both the hardware and software components of an HMI that should be specified for the system.

5.3.1 Hardware

The HMI hardware performs in a substation environment. The most common issue that should be addressed is whether a commercial personal computer, industrial computer, substation hardened computer, or server is required. The choice of any hardware that does not meet IEEE Std 1613 requires that the designer/specifier provide additional system design requirements for at least the following items:

a) Isolation of the computer from the substation battery and AC systems by using an inverter or other device that meets IEEE Std 1613

b) Isolation of the communication ports from interference generated in the substation environment by using fiber optic transceivers or other intermediate device that meets IEEE Std 1613

c) Installation of heating and cooling systems that are remotely monitored and alarmed such that temperatures beyond the computer rating are remotely indicated

As an option, the designer/specifier may determine that the HMI is a “throw away” component providing non-critical functionality that is designed so that it can be “easily” replaced when failure occurs. This approach should not be considered without the designer/specifier completely understanding the HMI functionality and replacement procedures. Some operating systems and HMI software are “keyed” to specific hardware serial numbers or models, making it difficult or impossible to move to a new hardware configuration without the cooperation and consent of the software supplier.

Depending upon the system architecture, the HMI may have other requirements, including but not limited to the following: multiple serial ports, multiple network ports, an IRIG-B port for time synchronization, mounting requirements (rack mount, panel mount, shelf mount, etc), keyboard, mouse, and redundancy.

The computer display device should also be carefully selected with respect to temperature and power supply requirements. Other display specifications typically include requirements for size, mounting, and touch screen.

5.3.2 Software

HMI software can be divided into the following three categories:

a) Operating system software

b) Application software that includes any application loaded on the computer

c) Configuration file(s) for the settings, displays, and database of the HMI application

Note that the HMI computer may have other applications that also have configuration files, but the specification of these applications and files are not included in this standard.

The HMI application typically runs on computers requiring the latest version of Windows, Linux, or some other operating system. Design tradeoffs can occur when certain requirements are made. For example, the designer/specifier may require a certain operating system to meet a corporate standard, which may limit HMI selection.

The behavior of the operating system software during and after power failures may help to prevent unexpected HMI performance and shall be determined prior to deployment.

5.3.3 HMI screens

The HMI application provides a series of screens or windows for the monitoring and control of substation devices. The designer/specifier should specify either all, part, or additional minimum requirements for these windows that include at least the following:

a) A menu system that provides an easy mechanism to move between different windows with no more than three movements such as mouse clicks. This may include a main menu window where all or most windows can be accessed plus a menu bar on each window that provides access to other windows.

b) Alarm annunciator that displays real-time alarms that can be sorted, filtered, individually disabled/enabled, and silenced based upon multiple criteria such as alarm name, group, and time.

c) Substation electrical one-line that overlays a summary of the status and analog points over a representation of the one-line. Control should be possible from the one-line window and easily disabled, if desired. Once disabled, however, the enabling scheme used shall meet any security requirements. The window should display at least the following:

    1) A geographical orientation of physical equipment including the location of manually or electrically operated disconnect and bypass switches, CTs, PTs, breakers, capacitor banks, reactors, and transformers

    2) Status and analog data

    3) Control of devices (if required)

    4) Tags (if required)

5) Colored values/graphics to indicate energized/de-energized status

6) Voltage levels

d) Protection one-line that is usually a simplified electrical single-line diagram. The various protection zones (distance or overcurrent protection, bus and transformer differential protection, transfer-trip schemes, etc.) are indicated. Current and potential transformer connections are shown. Some protection diagrams include supplementary notes that outline the requirements for taking equipment and protective relays out of service.

e) Communication one-line that overlay a summary of the status and analog points related to substation communications over a representation of all system communication connections. Basic communications statistics should be shown, including communication status, number of successful and unsuccessful poll attempts and control attempts on the device level, LAN statistics, and LAN performance, etc.

f) Trending windows that show present and historical analog values (and/or status values) and can be configured by the user to add/delete analog points, change pen colors, and trending start and stop times. A method should be provided that allows this data to be automatically transferred to a central repository, should one be available.

g) Historical alarm display that functions similar to the alarm annunciator window. A method should be provided that allows this data to be automatically transferred to a central repository, should one be available.

h) Substation logging functionality that allows operators to leave notes

Graphics and text shall be large enough and colored to be seen from an ergonomic distance and such that selectable items can be selected via a touch screen or by mouse. The color choices should also be specified by the designer/specifier.

5.3.4 Control capabilities

The HMI application includes the capability of controlling equipment. The designer/specifier shall specify if HMI control is required. When control capabilities are required, they may include a combination of at least the following:

a) Keys and switches (alphanumeric or function, or both)

b) Cursor (mouse, trackball, or key controlled).

c) Poke points (defined display control selection points)

d) Pull-down or pop-up menus

e) Physical switches, meters, lights, etc.

As a minimum, a control action through the HMI shall require two separate steps by the operator to reduce the possibility of inadvertent operations. The first step is to select the field device. A visual confirmation on the HMI is presented that gives a clear indication as to what device has been selected in the system database. The operator should also be presented with the options for the selected device (OPEN/CLOSE, TRIP/CLOSE, RAISE/LOWER, START/STOP, ON/OFF, SET POINT VALUE, etc) as well as the ability to CANCEL the control action. Execution of the desired control action or cancellation option will complete the HMI dialog. It is not required that this action implement full select before operate functionality down to the control device. An appropriate alternative is to prevent the control operation from occurring if the end device is not available to perform the control (polling has stopped, the device is off-line, the device is being tested, etc). See D.1 for more discussion of SBO schemes.

Devices that do not allow control should not allow the control dialog box to be displayed.

The designer/specifier should include tagging requirements, including how many tag types (information, control inhibit, etc), what additional information is required (comments and how many characters), whether

the tagging is replicated in the SCADA master, etc. Placing a tag on a device may also be accomplished by inhibiting a control from occurring by monitoring one or more local/remote switches and possibly even controlling the switch from remote to local.

HMI control actions should be logged in order to uniquely determine who performed the control from the HMI.

5.3.5 Other features

The HMI application will typically provide other features that include report generation from any historical or real-time measurement or status point, log files, links to documentation, help files that are context sensitive, multiple users, multiple security levels, symbol templates, symbol libraries, multiple protocol support, printing, etc.

In addition to the HMI software, the designer/specifier should also consider other software applications to be loaded on the computer. Examples of such applications include software that configures substation devices, monitors network traffic, retrieves data from substation devices, views different files, web browsers, and other applications that may be important to personnel working in the substation. These applications may or may not be directly linked in the HMI application.

The designer/specifier should also consider whether the actual configuration files should have backup files located on the substation computer or if the files should be stored elsewhere. Due to availability, security, and redundancy, this determination may not be trivial and should engage all of the impacted parties.

5.4 Software, firmware, and hardware issues

Patches and updates to all HMI software and firmware will be issued at various times during the life of the system. Coordination of the various updates is essential and may require a maintenance contract or licenses that the designer/specifier should include in the specification. This may increase costs.

The designer/specifier may require that all vendors provide copies of all software and firmware. The designer/specifier should consider whether multiple copies are required, which may increase software costs due to licensing issues.

The designer/specifier should also address process issues that most likely should not be included in the HMI specification. The designer/specifier should specify a version control or change management process that records all software, firmware, and hardware. These records should include compatibility relationships between the various software, firmware, and hardware (which versions inter-operate as a complete system). A backup process should also be put in place.

5.5 Security requirements

Security is an important concept that is beyond the scope of this document. A brief summary of security issues is presented here to acquaint the designer/specifier with security concepts. At least the following security concepts should be addressed:

- **Access control:** Control access to selected devices, information or both to protect against unauthorized interrogation of the device or information.
- **Use control:** Control use of selected devices, information or both to protect against unauthorized operation of the device or use of information.
- **Data integrity:** Ensure the integrity of data on selected communication channels to protect against unauthorized changes.

- **Data confidentiality:** Ensure the confidentiality of data on selected communication channels to protect against eavesdropping.
- **Restrict data flow:** Restrict the flow of data on communication channels to protect against the publication of information to unauthorized sources.
- **Timely response to event:** Respond to security violations by notifying the proper authority, reporting needed forensic evidence of the violation, and automatically taking timely corrective action in mission critical or safety critical situations.
- **Network resource availability:** Ensure the availability of all network resources to protect against denial of service attacks.

Refer to the bibliography for applicable work from other sources for more complete treatment of security. Corporate policy may establish the need for an electronic security perimeter around the system. This policy usually relies on some blend of technology and procedures. System security cannot rely on technology alone. Application of system security requirements should consider at least the following:

- Industry regulations and standards (NERC [B26], IEC [B6]–[B9], IEEE, AGA [B4], ISA [B20]–[B22])
- Government regulations
- Corporate safety, IT, and personnel policies

Using these requirements, the designer/specifier will need to balance security with operations. System design can be so secure that troubleshooting may be difficult or impossible to accomplish. Therefore, consideration should be given to other means of securing such items as:

- Diagnostic and maintenance tools
- Configuration software and files
- Technical manuals and documents
- Password maintenance and access control procedures
- Maintenance access policies for IEDs

Application of these requirements should address both physical and electronic security vulnerabilities. Physical security includes physical access to the automation system network and equipment, but also includes securing network equipment and cables (see IEEE Std 1402 for substation physical and electronic security recommended practices). Electronic security may include items such as encryption, network intrusion detection, authentication, firewalls, and IED access detection to establish an electronic perimeter of the system. Encryption techniques are available for the substation database, IED network communications, and communication links to SCADA, corporate WAN, IED maintenance ports, and other entities that should be considered in establishing a security practice. Note that encryption may make communication diagnostics much more difficult unless every piece of diagnostic equipment is prepared to decrypt the messages.

5.6 Selection of architecture

The designer/specifier shall define or specify the system physical architecture—the physical connectivity between IEDs, servers, and users needed to support the specified functionality. The interconnection of IEDs, servers, workstations, and communications interfaces constitute the integration of the IEDs into a system architecture. The system architecture may include simple point-to-point connections and/or an array of complex interconnected networks, depending on the goals and expectations for the system. Some of the common architectures are illustrated in Annex B.

The designer/specifier may use a specific physical architecture that fits a particular concept, such as an architecture that matches the physical layout of the substation, some other functionality, or process. In addition, developing a suitable architecture often requires that the new and the existing be blended together in a functional accommodation along with a vision toward a future architecture.

This definition stage may uncover the loss of some desired functionality resulting from limitations imposed by connectivity. Resolving these limitations requires an implementation plan to carry the existing architecture forward to a final architecture that supports the goals of the system.

5.6.1 Selection of external communications interfaces

While an automation system may be fully contained within a single substation, few systems are implemented without connections to the utility outside the substation through an external interface. As with other portions of the system, these interfaces need to meet the functional and performance requirements of the users, at whatever location they may reside. The availability of communications technology to support outside connections has both an economic and performance impact on users and the utility. Communications choices should withstand a critical performance weighted cost/benefit analysis. External interfaces also expose the substation to the broader environment and therefore expose the substation to hazards from uncontrollable actions by others as well as unauthorized access or intrusion. The interface between the communications technology and the substation system thus becomes a critical component in meeting the utility expectations.

External communications interfaces serve two distinctly different clients: those that use “real-time” or “near real-time” monitoring and control for utility operation(s) at operation(s) and engineering center(s); and session oriented users performing data retrieval, maintenance, and configuration activities. “Real-time” or “near real-time” monitoring and control interfaces are usually maintained connections, dedicated to a single user and/or purpose such as a SCADA, EMS, and DMS. This interface often maintains compatibility between an existing utility EMS or DMS and the substation. Such an interface may take the following forms:

a) A traditional SCADA RTU with hardwired interfaces to substation equipment

b) An advanced RTU where its interface is more of a communications gateway to IEDs and their network(s)

c) An RTU like function embedded within a substation host or an automation controller

The typical SCADA/EMS/DMS dedicated communications link operates with a serial style protocol (legacy) with low speed communications technology that should be supported at least until system upgrades provide for moving to newer communications technology. With analog pathways giving way to digital communications links such as Frame Relay that incorporate packet-based protocols, support for carrying the legacy messages within these protocols should be required. Network pathways are also capable of supporting legacy messages embedded within TCP/IP protocol links along with other network traffic. This is an obvious migration path and should be included in the growth plan for external interconnections.

Other outside users typically connect through session oriented communications interfaces and links to interact with the substation system and/or its IEDs, on demand. This interface is often to a separate substation network connecting to IED serial “maintenance” ports, isolated from that supporting real-time monitoring and may take the following forms:

— A public or private switched network, “dial-up,” connection to a modem with a port selector mechanism to allow the user to connect to a targeted IEDs.

— A dedicated interface device that serves as a connection point for IEDs and an access point for outside users.

— A dedicated WAN interface access device with enough intelligence to route messages to specific IEDs and perform protocol translation or message “packing” if needed.

— A WAN network connection to an internal substation TCP/IP network that interconnects the IEDs, through a gateway, network switch or firewall.

The configuration of the session oriented user interface is driven by the communications capabilities of the IEDs and the economic justification for supported functionality. The designer/specifier should consider the communications capability of IEDs in selecting them for the system as they may add hardware and software to support the required access. Where the system has a population of serial IEDs, the designer/specifier should develop a plan to accommodate network enabled IEDs as they replace serial IEDs. The designer/specifier should also be aware of the potential security issues posed by providing outside access to IED "maintenance" ports.

Any external interface may suffer from reliability issues related to messaging over long distances. In many instances, such channels pass through media changes that can also impact performance and reliability. The designer/specifier should assess the potential effects of loss of any portion of a pathway to at least the following considerations:

— Loss of power to an interface device

— Unauthorized access to an interface device

— Failure of an interface device (due to fault or other causes)

— Exposure of the channel media to physical damage

— Response of the channel owner to request for repair service

— The consequences of channel owners reconfiguring channels without notification to users

— Return time of the channel after temporary failure

5.6.2 Selection of internal communications interfaces

Communications interfaces internal to the substation are evolving from simple serial connections, to highly complex networked integrations. The selection of internal interface options is driven by two constrains. The functionality of the system will determine what messaging is supported and who the users will be. Often, the IEDs selected for the system will constrain the functionality based on the communications technology they support. Thus, a multi-user wide access architecture concept may be impeded by IEDs that only support serial communication through one or more configurable ports. This will challenge the growth plan for the substation integration.

IEEE Std 1615 provides details on applying network technology to substations and should be used as a reference.

5.6.2.1 Serial interfaces

IED serial interfaces are generally byte oriented although some legacy SCADA protocols are not. Serial messaging may be a one-to-one (point-to-point) connection, or point- to-multipoint.

Generally IEDs provide ports conforming to the EIA-RS-232 standard. The designer/specifier should be aware of at least the following potential issues using these ports:

a) IEDs may not fully support connections to modems or computers that require channel control signals to be available.

b) IEDs may have additional signal and/or power conductors present in the port connector that can be problematic to users.

c) EIA-RS-232 does not specify isolation between the channel pathway and the communications port or UART of the device. Isolation is advisable to maintain the reliability of the channel.

d) EIA-RS-232 does not support multi-drop configurations. Additional hardware will be needed to implement a multi-drop channel.

e) EIA-RS-232 is limited to short distances depending upon the cable quality (capacitance) and baud rate, typically less than ten meters.

IEDs may also support multi-drop communication ports with an TIA-485-A interface. The designer/specifier should be aware of at least the following potential issues using these ports:

— TIA-485-A channel control is generally "master/slave" where one device addresses others one at a time to control traffic. There is no mechanism defined in TIA-485-A to mitigate channel contention or collisions. Some messaging schemes allow the transfer of channel control from one IED to another to provide multiple device access. Here the serial protocol supports addressing for both sender and receiver in each message.

— All devices on a TIA-485-A channel shall use a common protocol.

— Many devices provide for biasing the TIA-485-A twisted pair above ground potential or for establishing a channel ground reference. Only one device per pathway should be configured to supply bias or ground reference. All other devices cannot provide pair biasing (as this adds to the channel loading), unless TIA-485-A current limits are not exceeded.

— TIA-485-A pathways may be terminated with resistors at one end, sized to match the characteristic impedance of the pathway cable used. Many devices provide terminating resistors internally. Only those devices at the end of the pathway should have these resistors connected. When used, internal terminating resistors should be checked to verify they are the correct value for the cable being used.

— TIA-485-A does not specify isolation between the channel pathway and the communications port or UART of the device. Isolation is required to maintain the reliability of the channel and its connected devices.

— A TIA-485-A pathway shall be linear; stubs are not permitted.

— Round-trip travel time for messages in an TIA-485-A network can impact the ability of a master to poll all of the IEDs on the network that supports minimum update times. As the number of IEDs increases, the polling interval decreases. As this situation reaches a critical limit, it is important to configure the master polling time appropriately.

Serial interfaces are supported by a communications process within the IED. This process may be based on terminal emulation (for example, VT100), a proprietary protocol, or standard protocol. The designer/specifier should be aware of at least the following port support characteristics:

— Integrating IEDs with terminal emulation interfaces beyond simple session oriented single user connections requires custom software and some form of communications processing device to extract information and perform controls. The communications processing device emulates the activities of a human with a terminal to interact with the IED. Some IEDs will require the communications processing IED to provide a dedicated port for each connected device. While these devices can be successfully integrated into a "system" this can be an expensive, single product and short-lived solution.

— Protocol based interfaces can be easier to integrate, especially since they tend to support multiple devices per channel (port) and are addressable. If a device specific protocol is based on a common protocol e.g., Modbus, creating the bridge between the system and the devices can be less expensive. Still, a communications processing interface will be needed although the supplier of such a device may only need to configure the bridging software rather that create new software from scratch. Some suppliers have access to a large library of such software and may be able to create the bridge at a reasonable cost. The interface device, however, can become a significant risk

as a single point of failure. This can also be a short-lived solution as the interface software may leave the user with no path to integrate newer version devices without reinventing the interface.

— Standard protocol-based interfaces can have a significant advantage. Some systems can communicate with them directly without an interface device. When an interface is required, creating an interface connection is simplified significantly by the availability of the standard protocol. However, some differing interpretations of the standard may lead to difficulties. It is more likely new devices, or even devices of a different manufacturer can use the interface, therefore it may have a longer useful life.

5.6.2.2 Network-based interface

Network-based systems assemble messages in fixed length packets. Each packet contains the message data bytes in whatever form the sender and receiver understand. To traverse the network, a network protocol "wraps" the message data in an envelope that network devices understand. Network devices do not need to understand the contents of the message. The network protocol may carry data bytes representing any kind of transaction, in any form and of any size. Network devices will use as many packets as necessary to complete the transaction.

While serial messaging connects the sender and receiver directly, network messages may pass through intermediary devices to reach their destination. Moreover, the route taken by packets from sender to receiver may change without changing any parameters at either the sender or receiver.

Network messaging assumes that any device may exchange messages with any other device. Special message handling is required to "route" messages only between specific senders and receivers. This service is performed, not by the devices, but by intermediary devices in the network pathway.

Unlike a serial pathway, networks can support multiple users and devices quasi simultaneously. While only one message packet can traverse the network at a time, the source and destination can be anyone with different sources and destinations interspersed. Messages using multiple packets are not necessarily contiguous.

5.6.2.2.1 Network adapters

It is possible to bridge the gap between network devices and serial devices with a network adapter, often called NIMs, which connect to serial devices on one-port and packet networks on another. They may support multiple serial ports and may have multiple network ports. The NIM communicates with the serial devices and embeds the messaging transaction in a network protocol. It may also convert the serial device messages into a protocol common to other network devices such that they may share data and functionality. Once in a network protocol the messages may be transported across the network to any user authorized to exchange such messages and that can understand their content. When a NIM is considered for a system, the designer/specifier should consider at least the following characteristics:

a) NIMs are a patch put in place to allow non-network-ready devices to become part of a network based system while the long-term plan evolves to replace them with network-enabled devices.

b) The NIM has special functionality and is usually device specific. Therefore, including NIMs in a system design adds significant cost and upkeep to the system. NIMs may require version updates any time there is a software or firmware change in the IED or the network devices.

c) A larger form of NIM is the gateway or data concentrator that supports a number of serial devices and communicates to them in their native protocols. It makes the result of these transactions available to the network in whatever form is compatible with the network. This function may reside in a special processor, sometimes supplied by an IED supplier to bridge the gap in their product offering. Some RTU suppliers offer this function as a natural extension of their RTU product offering. This function is sometimes embedded within a substation processor that may be providing a HMI or data logging service.

5.6.2.2.2 Network standards

There are multiple standards that an automation network can be based upon. IEC 61850, among other things, specifies many levels of protocols needed to support integrated substation automation functionality. IEC 61850 is a very complex and comprehensive standard.

IEC 61850 targets the electric substation and enterprise. On the power generation side of the utility, as well as other utility areas, other standards are being applied. Utilities should evaluate whether they want to have different standards for the different activities of their business.

IEEE Std 1615 provides guidance for incorporating networks into utility communications for automation. The IT standards commonly deployed for the business environment are being adopted to reach to the substation. See IEEE Std 1615 for a discussion for some of the protocols commonly used.

Some utilities have found that they can integrate their substation automation functions using their IT standards and technologies. These utilities use the IT environment to transport messaging to their substation devices and retain their native protocols, embedded within the IT protocol suites.

5.7 Selection of protocols

It is important to recognize that any specific IED may understand a limited number of protocols. If a standard protocol is already in use in a substation, the designer/specifier should select a new IED with the same protocol for connection to the communications channel or network. Conversely, if a proprietary protocol is installed in the substation and new IEDs are to be added, then the following options should be evaluated:

- Upgrade the existing RTUs, IEDs, and master with the standard protocol (preferred)
- Use different protocols but with a translation gateway so that data can be transferred on a common channel
- Order the new IEDs with the old legacy protocol

When making this decision, the designer/specifier should be aware of both technical and economic implications:

a) What is the cost of implementing the substation's existing protocol in the new IED vs. the cost of installing a new network? Is the new IED a one-time device, or will it become a new standard device? Some manufactures may not maintain any specific customization in future product releases and the user may be required to fund the development of the desired customization multiple times.

b) Does the existing protocol have all the capabilities needed to support the required functionality?

c) Will a new protocol meet the performance requirements using the existing communication infrastructure or will that have to upgrade? At what cost?

d) Will it support the interrogation of single data values, sets of data, or the entire stored data on a "report by exception" basis?

e) Will it support unsolicited alarm reporting—analogs out of limits or status changes?

f) Will it support the transfer of large files? If not, and these are important requirements, then the existing protocol may not be suitable at all. In that case, a new network is established using one of the recommended protocols.

g) What is the impact on the long-term life cycle costs, including impacts on future upgrades, additional equipment installations and on-going support?

5.8 Maintaining availability

5.8.1 Define availability requirements

In the process of designing an automation or SCADA system it is important to define the availability requirements for system functions. This is illustrated as a column in the performance requirements shown in Table 1 through Table 6. Some functions can be expected to be critical to the operation of the substation and power system such that their availability is assured at all times. Protection is an example of this requirement. Protection designs generally provide for a contingency loss of a primary protective function by use of a secondary protective function that will adequately cover for the loss.

The loss of some automation system functions may have marginal impact if the outage is not too long. Loss of those functions may delay some tasks or require a less convenient method be used to perform a task, but do not critically impact the enterprise. Collection of planning data might be such a function. Thus, the first step in dealing with availability is to define the availability requirements by function. The second step is then to render a design that meets those requirements with suitable solutions. The designer/specifier should include in the system architecture any alternate pathways and devices as needed to meet availability targets and mitigate single point of failure consequences.

5.8.2 Identifying critical components

Once the availability requirements are defined, the proposed design should be evaluated to identify critical components. A critical component is one that can disable or impair a function such that it no longer meets its performance criteria. A critical component can affect more than one function. For example, if a communications link between a substation and an operations center fails, it will disrupt all messaging that takes place over that link; hence many functions may be affected. While the communications link in this example is a critical component, the analysis needs to look in depth at each component and its pieces. The communications link may share a common cable with other links, which will also be affected, should the failure be the cable itself. The designer/specifier should identify areas where critical components are shared by system functions and treat them as additional system functions.

5.8.3 Limiting risk of failure

The designer/specifier should assess the risk of failure of critical components identified above. Risk may be expressed for analytical purposes in several ways. The most common risk index mean time between failure (MTBF), which is a probabilistically derived estimate of the longevity of the component. Perhaps a more useful evaluation is to assess the exposure of critical components to damage inflicted by the environment or operation, as MTBF primarily focuses on components that have a “wear” mechanism. Many times, protecting the component from damage can substantially reduce the risk of failure. As in the example of a communications cable cited above, installing the cable in protective conduit to limit exposure to physical damage will reduce the risk of its failure. Minimizing its exposure to moisture can also substantially reduce the risk of its failure.

The designer/specifier should refer to standards such as IEEE Std 1613 that can help determine environmental withstand requirements for devices, and define the tests that can help identify weaknesses in components. Selecting components that are resistant to the hazards they are exposed to is another technique for reducing risk. As in the cable example, the water resistance capability of the cable should be a key consideration of its specification if it operates in wet environments. Another risk avoidance measure is to add significant safety factors to the component loadings that are supplied with component specifications. While many electronic components do not perform well at the very low end of their ratings, they also experience life-shortening stress when operated near the upper boundary of their ratings. The designer/specifier should evaluate the expected longevity and stress applied to such components as the design is formulated.

5.8.4 Estimating loss of function time

Using the list of critical components previously identified, the designer/specifier should assess the time required to return the impaired function to usability, taking into account any common failure modes that may exist. This estimate is usually discussed in analysis as MTTR. Since the availability requirements have already been identified, the designer/specifier will be able to compare them to the MTTR times of each component so as to identify those components that have a significant impact on the system functionality. There are many factors that contribute to MTTR times. These include the following:

a) Time for a qualified support person to identify the failure

b) Time for the a replacement component to be delivered to the failure site

c) Time for a qualified support person to repair the failure

d) Time to verify the replacement is functional

Where any of the above significantly impact MTTR, an alternative method to support the function will be required or the function will have to remain unavailable until it is restored.

5.8.5 Providing alternative functional support

There are many ways to provide alternative functional support to achieve a quick “Return To Service”. The designer/specifier may provide for a redundant function to replace the unavailable function when one of its components fails. The designer/specifier may also provide redundant components for those that impact multiple functions. Where redundant components or functions are provided, a means to transfer from one function or component to its alternate may be required because redundant functions may not always be able to co-exist in the active state without conflict. At a minimum, failure alarming of redundant component(s) is/are a requirement to ensure redundant functions are actually available as required. The designer/specifier should evaluate which function should be restored manually, by human intervention considering the implications cited as follows:

a) ***Human initiated.*** A qualified person recognizes that a function is impaired and takes action to disable that function and enable its alternate. This may take place in the substation if it is manned, or the transfer can wait until a person arrives at the substation to perform this task. It is common for a centrally located person to perform function transfers remotely. This is driven by the need to restore the function faster than can be achieved by dispatching a person to the substation, but may suffer some lack of detailed assessment of the conditions existing that caused the function to fail. There is an inherent unknown when transferring functionality remotely.

b) ***Automatic fail-over mechanism.*** Automatic fail-over schemes should have monitor functions to recognize when a function has become impaired and then perform the transfer. Defining the criteria by which a function is declared impaired takes careful scrutiny by the system designer, and may entail some additional monitoring hardware and software. The monitoring criteria should be comprehensive enough to accurately detect impairment under all operating conditions without being prone to false detection. Likewise, the detection mechanism itself should be monitored to ensure that it is active and capable of performing its task.

5.8.6 Operating functions in parallel

In order to assure the continuous availability of system functions, the designer/specifier can configure systems to operate multiple equivalent functions simultaneously. Given the multiplicity of functions available in common substation IEDs, it is possible that duplicate functionality may exist even without being intentionally specified.

In the case of measurements, it is also likely that IED measurements will provide similar but not identical or completely interchangeable values. The designer/specifier should specify which measurement from a

specific IED will be the primary data source and which will be an alternative source. The designer/specifier should specify how the user will know which source is being used at any given time and what the limitations of that source might be, if any. The designer/specifier should also provide a means for the user to know if one of the measurements is unavailable.

Control functions can also be duplicated in multiple IEDs. As with measurements, there may be some performance differences or preferences that will dictate that the designer/specifier specify one IED as the primary controller and another as the alternate. The designer/specifier should provide a means for the user to know, at any given time, which IED is providing the control functions.

5.8.7 Using functional diversity to improve availability

There are perceived advantages to using functional diversity when addressing availability. Many reliability references suggest that primary and secondary components of systems should not be identical, but rather be of different technology, design and manufacture. The logic supporting this concept suggests that the differing technology, design and manufacture will limit the system's exposure to a common failure mode. The designer/specifier should consider this concept as a potential benefit, but that it might be outweighed by additional support and training costs. With the commonality found in IEDs, it is conceivable that diverse systems might share more in common than is outwardly evident as there are a limited number of electronic component suppliers, processors and software tools.

Diversity in the execution of the system design can have real benefits for improving availability. It is important to keep components separated to limit potential physical damage. The better the separation, the more likely key functions will not be lost for the same event. For example, if all the communications facilities to the substation run through a common element like a cable, a duct run, or a telecommunications switching station, the likelihood that a common event will cause the failure of all facilities is higher than if none of those elements were shared.

The designer/specifier should assess the costs, risks, advantages, and disadvantages of separating shared facilities. They should also assess the likelihood of events that compromise shared facilities, and whether the cost to separate these facilities is worth the risk and cost associated with the potential loss of functionality.

6. Interface and processing requirements

The control and data acquisition equipment shall have interfaces and processing requirements for those interfaces as described in this clause.

6.1 Mechanical

The designer/specifier should carefully assess the physical and mechanical needs of the proposed system from the user's perspective. Often, users have special requirements that are rooted in their philosophy or experience base that need to be captured and presented to potential suppliers. While some of these might be classed as "utility specials," many have legitimate reasons to exist.

6.1.1 Enclosures

Equipment enclosures shall be suitable for the proposed environment. Enclosure specifications are found in NEMA 250 and IEC 60529, which typically apply to harsh environments and ANSI/EIA 310-D, which typically applies to controlled environments.

6.1.2 Special requirements

The designer/specifier should assess the requirements for equipment for each specific application and incorporate those requirements into the system specification. These requirements include at least the following considerations:

a) Location and size of access doors

b) Physical security (locking devices and keys)

c) Enclosure mounting

d) Temperature control and ventilation requirements

e) Resistance to moisture, atmospherically born contamination and solar radiation

f) Terminal-block type, location and specific termination layout(s) when required

g) Cable entry locations

h) Special cabling and connector requirements

i) Placement and details for cabinet grounding and bonding

j) Cabinet material, color, and finish considerations

k) Lighting and power outlets

Enclosure selection provides equipment protection from moisture, dust penetration, etc. Once an enclosure is sealed, the equipment is exposed to the environment inside the sealed enclosure. This may result in temperature, condensation, and other impacts on the enclosed equipment that the designer/specifier should account for in equipment selection.

6.2 Grounding

Grounding is required for all equipment. Control and data acquisition equipment shall not ground a floating power source. Care shall be exercised to ensure ground compatibility when grounded power sources are used.

6.2.1 Device ground

Cabinets and device enclosures shall be grounded only at the same point that the electrical service or UPS neutral is grounded. All devices within one cabinet shall be grounded together by means of a ground cable or strap.

6.2.2 Signal or instrumentation circuit ground

The signal or instrumentation circuit ground shall be connected to an external ground at a single point so that ground loop conditions are minimized. The shielded wire, drain wire, and/or ground wire of input/output cables shall be terminated at one ground point in each cabinet or the device shall be insulated from the cabinet. These ground points shall be connected together and connected to the facility ground. Caution shall be used to prevent inadvertent ground paths from apparatus such as convenience outlets, conduit, structural metal, test equipment, and external interfaces.

The manufacturer shall be consulted prior to selection of the cable end to be bonded as the optimal location is dependant upon the manufacturer’s design choices.

A special caution on filtering is worth noting. If the noise is shunted to the signal ground, then it becomes another source of signal reference corruption. Sometimes separate power, noise, digital, and analog ground buses are necessary. However, the NEC [B27] requirement for a single point safety grounding source shall

always be met. A very important design rule is to keep all signal reference voltages, at all frequencies of operation, as close to zero as possible (i.e., at zero voltage signal reference).

6.2.3 Fiber optic signal circuits

Fiber optic circuits require no grounding unless the cable has a conductive element.

6.2.4 Electrical power ground

Where grounding is provided with the power source, safety grounding conductors shall be bundled with the power source conductors, but be insulated from the power conductors and from other equipment and wiring conduit. The ground conductor shall be terminated in the cabinet enclosure, and grounded only at the same point that the source of the electrical service to the cabinet or UPS neutral is grounded.

6.3 Electrical power

This clause defines the ratings of DC and AC control power inputs and allowable ripple on DC supplies.

The electric power interfaces to control and data acquisition equipment shall meet the following requirements:

a) The alternating current source defined below may originate directly from the station source or from a regulating/uninterruptible power supply.

b) Equipment operating on direct current shall not sustain damage if the input voltage declines below the lower limit specified or is reversed in polarity.

The following voltage ratings have been adapted from IEEE Std 1613.

6.3.1 DC power sources

DC power supplies and auxiliary circuits with DC voltage rating shall be able to continuously withstand the maximum design voltage range shown below. Power supplies with a wide DC voltage range (i.e., 12 V to 250 V) are encouraged. Substation equipment shall be capable of operating with one or more of the following source voltage ranges:

a) 12 Vdc nominal (9.6 Vdc to 14 Vdc)

b) 24 Vdc nominal (19.2 Vdc to 28 Vdc)

c) 48 Vdc nominal (38.4 Vdc to 56 Vdc)

d) 110 Vdc nominal (88 Vdc to 123 Vdc)

e) 125 Vdc nominal (100 Vdc to 140 Vdc)

f) 220 Vdc nominal (176 Vdc to 246 Vdc)

g) 250 Vdc nominal (200 Vdc to 280 Vdc)

6.3.1.1 Allowable AC component in DC control voltage supply

All devices shall operate properly with an alternating component (i.e., ripple) of 5% peak or less in the DC control voltage supply, provided the minimum instantaneous voltage is not less than 80% of rated voltage. The ripple content of DC supply expressed as percentage is defined as Equation (1).

$$\frac{(\text{peak value} - \text{DC component})}{(\text{DC component})} \times 100 \quad (1)$$

NOTE—Equation (1) refers to low-frequency ripple as might typically be introduced on the DC control power bus by a battery charger. Higher frequency effects, such as might be introduced by a DC-DC converter within the device or equipment itself, are not included.

6.3.1.2 DC system loading

The addition of automation system devices will increase the loading on a substation or stationary battery system. The designer/specifier should evaluate the load being added to substation and stationary battery system to ensure the battery capacity is sufficient and that the charging system can carry the added load. The utility standard for discharge rate and capacity should be preserved.

6.3.2 AC power sources

AC power supplies and auxiliary circuits with AC voltage ratings shall be capable of operating successfully over a minimum range of 85% to 110% of rated voltage and frequency. The nominal AC voltage rating shall be as follows:

a) 120 V 60 Hz

b) 220–240 V 50 Hz

c) 120–240 V 50–60 Hz

The designer/specifier should consider the requirements for power conditioning and uninterruptible power sources as a means to assure reliability and availability of AC-powered substation automation system equipment.

6.3.3 Redundant power sources

Some devices, typically found in substations or in/near the substation switchyard, may be fitted with power supplies that operate nominally from station AC service but provide internal DC backup supply from the substation DC battery or a dedicated storage battery. Dedicated storage batteries should be given at least the following considerations when they are specified:

a) Duration of backup power operation without battery charging (usually not less than 4 h but normally at least 24 h)

b) Longevity of the battery source as estimated by its shelf life on charge

c) Temperature range over which the battery will maintain required voltage and current capabilities

d) Replacement interval for backup batteries

e) Precautions for possible corrosive material spill/seepage and explosive gas accumulation

f) Recovery time of the backup battery after a full discharge

g) Alarming for failure of either power supply

Whenever non-rechargeable, replaceable batteries are utilized, consideration should be given to providing a means to identify the discharged state of the batteries and providing for remote indication to allow for timely maintenance replacement.

6.3.4 Internal noise

Internal noise generated by devices and appearing on the power supply terminals shall not exceed 1.5% (peak to peak) of the external power source voltage, from 1 kHz to 10 kHz, as measured into an external power source impedance of 0.1 Ω minimum.

6.3.5 Electrical power supply identification

All equipment associated with a substation automation system should be powered from isolated and dedicated electrical supply circuits in order to prevent unintended loss of power to SCADA equipment while other unrelated equipment is being worked on. These circuits may be tagged at the distribution panel as "critical do not disconnect." The circuits, either AC or DC, should be isolated from all other facility loads and alarming should be provided to indicate loss of either source. The circuits should operated only by knowledgeable personnel with suitable training.

6.4 Data and control interfaces

Data and control signal cabling for the substation automation system may reference IEEE Std 525 for design guidelines.

Data and control interfaces consist of electrical interconnections between control and data acquisition equipment and the apparatus being monitored and controlled. Two types of signal paths are defined as follows:

a) Data paths: Inputs to data acquisition or supervisory control equipment

b) Control paths: Outputs from data acquisition or supervisory control equipment

For each input (data) or output (control) path, various signal characteristics shall be defined using the preferred signal characteristics defined in the tables below. If specific characteristics are not included in those tables, the designer/specifier shall specify the applicable characteristics.

6.4.1 Point count

The designer/specifier should specify the number of each point type the system should support. Due to the system architecture, the total point count may be distributed among already existing IEDs as well as new IEDs. When point count limitations of IEDs are taken into consideration, some points may need to be relocated to other IEDs or to a general distributed I/O IED that will specifically handle miscellaneous status points.

The designer/specifier should differentiate between those points that are hardwired into an IED (relay, meter, distributed I/O, RTU, etc.) and those points which are "soft" or "calculated" points provided by IEDs. The characteristics for each data type shall be defined. Ranges of data input, scale factors, rates, and accuracy shall be defined for the data types to be supported such as:

a) Analog inputs

b) Status inputs—two state

c) Status inputs—more than two state with every state defined (more than two state status inputs are usually accomplished by using multiple two state status inputs)

d) Status inputs—with memory

e) Accumulator pulse inputs

f) Sequence-of-events inputs

g) BCD inputs—multi-bit

The capacity (total inputs) and rate of acquisition (inputs per second) for field data interfaced to the RTU equipment and master station shall be defined for all applicable data types.

The modularity (e.g., number of inputs per card) of each data type shall also be specified for the RTU equipment.

6.4.2 Insulation requirements

It is general practice to require all electrical circuitry connected to substation sensors, instrument transformer, and power equipment to meet the specifications for 600-volt class installations. This includes circuitry connected to the station battery or other power sources. Such installations are subject to conductor sizing, spacing considerations between energized conductors, insulation ratings and are subject to test to insure integrity with 1000 V or 2500 V AC to ground insulations test and/or 500 VDC or higher insulations resistance tests. Where interface circuitry can be isolated from station equipment, the designer/specifier may specify less restrictive interface specifications.

6.4.3 Input interface requirements

Inputs to automation controllers and measuring devices shall be compatible with substation and power equipment sensors. The following characteristics are commonly specified to achieve compatibility. Where circumstances cause the designer/specifier to deviate from those listed, the designer/specifier should provide details similar to those shown such that compatibility can be assessed. In addition, the processing requirements for each input are discussed.

6.4.3.1 Analog inputs

Analog data (integer and non-integer) is used to describe a physical quantity (i.e., voltage, current) that normally varies in a continuous manner. The information content of an analog signal is expressed by the value or magnitude of some characteristic of the signal such as amplitude, phase angle, frequency, the amplitude or duration of a pulse, etc.

Table 7—DC analog input signals

Parameter	Specifications	Notes
Nominal input signal range	± 1 mA or 4–20 mA	± 5 V with normalizing resistance less than 5 kΩ is acceptable
Input signal over range without damage	± 2 mA or 3–24 mA	Limited by the transducer to 2 mA
Fully isolated inputs		
Common ground return	None	Electrically isolated
Maximum input signal (non-operating)	200 V peak	DC to 60 Hz, to prevent damage when mis-wired to source outside operating range
Maximum common-mode voltage (operating)	200 V peak	DC to 60 Hz, referred to equipment ground
Signal ground referenced inputs		
Common ground return	Signal ground, 0–1.0 MΩ	Signals may be single-ended referenced to ground at the input or differential with a common-mode reference to signal ground at the input
Maximum input signal (non-operating)	200 V peak	DC to 60 Hz, to prevent damage when mis-wired to source outside operating range
Maximum common-mode voltage (operating)	10 V peak	DC to 60 Hz, referred to equipment ground
Maximum input signal (operating)	10 V peak	DC to 60 Hz
Maximum input signal common or single-ended mode offset	10 V DC	—

Parameter	Specifications	Notes
All DC analog input signals		
Maximum input signal resistance	10 kΩ for ± 1 mA inputs 600 Ω for 4–20 mA inputs	Includes overload protection
Conversion resolution, minimum (with sign)	12 bits, 16 bits, 32 bits	Binary data format (includes sign)
Maximum error at 25 °C	± 0.1%	Percent of nominal input signal range for a single sample
Maximum temperature error[a]	± 0.005%/ °C	Percent nominal input signal range
Minimum common-mode rejection	90 dB	DC to 60 Hz
Minimum differential (normal)—mode rejection	60 dB	At 60 Hz

[a] Associated with the operating temperature.

Table 8—AC analog input signals[a]

Parameter	Specifications	Notes
Nominal input signal range	1 A or 5 A, 6 V, 69 V, or 120 V	rms values, 50/60 Hz
Input signal range	2 A or 10 A, 138 V or 240 V	Continuous rms values, 50/60 Hz
Overload input signal rating	CT–40 × nominal, 1 s PT–2.5 × nominal, 10 s	—
Maximum input signal burden	PT–3 VA CT–1 VA	—
Conversion resolution, minimum (with sign)	12 bits, 16 bits, 32 bits	Binary data format (includes sign)
Maximum error at 25 °C	± 0.1%	Percent of nominal input signal range for a single sample
Maximum temperature error[b]	± 0.005%/ °C	Percent of nominal input signal range
Maximum operating common-mode voltage (CMV)	200 V peak	DC to 60 Hz, referred to equipment ground
Minimum common-mode rejection ratio (CMRR)	90 dB	DC to 60 Hz
Common ground return	None	Electrically isolated
Insulation level	600 V	1500 V rms for 1 min
Anti-aliasing filter	Specify	Cutoff less than one-half A/D sampling rate

[a]600 V insulation class, 1200 V hi pot, all isolated (ungrounded).
[b] Associated with the operating temperature.

Note that ground referenced signals can form “sneak circuits” that cause circulating currents, or even short out a signal. This occurs when multiple devices have internal ground references and are connected to a common analog input card or module.

The analog data processing options to be supported at both the master station and the RTU shall be defined. Particular attention shall be given to input data validity processing (e.g., the validity of the data) and to the interface between the supervisory control function and the analog data processing function.

a) Data input scaling shall give adequate consideration to off-normal operation of the power system (e.g., overvoltage, fault conditions, emergency load limits).

b) Data change detection may be a function included as an alternative to processing every input on every scan. Data change detection is accomplished by testing to see if the new value for each input is within N digital counts (e.g., deadband) of the last stored value for that input. The new value shall replace the last stored value only if the deadband was exceeded and then the input will be further processed as defined below. When the data change detection function is included, the following characteristics shall be defined:

1) Location of processing, RTU or master station, or both
2) Range of N, RTU or master station, or both
3) Definition of N on an RTU, card, or point basis
4) Technique for changing value of N

c) Data filtering for noisy or unstable inputs may be required to smooth data before it is used by other functions. When this function is included, the equation(s) used shall be defined and the time delay(s) introduced by the filtering specified.

d) Data limit checking is typically included to determine if other downstream functions, such as alarm detection, or further processing are required. The number of high or low limits accommodated and associated return-to-normal deadband processing shall be defined. Specific attention shall be given to the procedure for user configuration and revision of limit and deadband values.

e) The data report-by-exception function is used to eliminate communication of unchanged data from the RTU(s) to the master station or sub masters. Its input is received from the change detection function. When the analog data report-by-exception function is included the following characteristics shall be defined:

1) Percent of analog changes per scan that results in the channel load associated with reporting all analog points from the RTU (i.e., how many analog changes per scan will it take for the reporting of analog changes to take the same bandwidth of just reporting all analog values).
2) Description of logic in the master station that can be used to select between using the analog data report-by-exception function or the report-all-analog data functions when acquiring analog data from each RTU.

f) Data conversion to engineering units is typically required before analog data is used by other software, printed, or displayed as output. The mathematical equation(s) used to convert analog values represented by digital counts into the corresponding engineering units shall be defined. Specific attention shall be given to sensor and transducer scale factors that may be provided by the user.

g) Invalid data techniques shall be defined that are used to

1) Detect an open input to an analog channel
2) Identify reasonable values
3) Detect a drifted or faulty A/D converter
4) Automatically calibrate an analog channel

6.4.3.2 Status data

Status data is used to describe a physical quantity (e.g., device position) that has various possible combinations of discrete states. The information content of a digital signal is expressed by discrete states of the signal such as the presence or absence of a voltage, current, or a contact in the open or closed position.

Table 9—Digital electronic input signals

Parameter	Specifications	Notes
Input data format	Specify	Application dependent
Common ground return	Specify	Optical coupler or equivalent
Signal voltage range	0 V to 20 V	—
Signal current range	0 mA to 20 mA	—
Signal data rate	Specify	—
Signal duration	Specify	—

Table 10—Contact (electromechanical) inputs

Parameter	Specifications	Notes
Input data format	Specify	Application dependent
Common ground return	Specify	Optical coupler or equivalent
External contact format	Specify	Dry contact. Form A is typical
Minimum signal voltage	12 Vdc	Minimum for substation power. Station battery may be used subject to surge restrictions
Minimum signal current	10 mA	New equipment may require only 2 mA
Settable debounce time	2–128 ms	Digital filter adjustments
Minimum change detection time	0.5 ms	—
Maximum change detection time	1 ms	—
Maximum contact resistance	100 Ω	Includes cable resistance
Minimum leakage resistance (at operating voltage)	50 kΩ	Includes cable leakage resistance

The status data processing options to be supported at the master station and the RTU shall be defined. This is the responsibility of both the user and supplier. Particular attention shall be given to input data validity processing, and to the interface between the supervisory control function and the status data processing function.

a) Data change detection may be a function included as an alternative to processing every input on every scan. Data change detection is performed by testing to see if the current state is the same as the last stored state for that input. Changed data shall replace the last stored value and the point, or group of inputs, shall be routed to other functions such as data report-by-exception, alarm processing or both. When the data change detection function is included, the following characteristics shall be defined:

   1) Location of processing (RTU or master station)

   2) Quantity of data reported when a single input changes

   3) Minimum signal duration to be considered a change

   4) Minimum current required for detection

   5) Security against loss of change data

b) Data report-by-exception function is used to eliminate unnecessary communication of unchanged data from the RTU(s) to the master station or sub master. Its input is received from the change detection function. When the status data report-by-exception function is included, the following characteristics shall be defined:

   1) Percent of status point changes per scan that result in the channel load associated with reporting all status points from the RTU.

   2) Description of logic in the master station or RTU that can be used to select between using the status report-by-exception or the report all status data function when acquiring status data from each RTU.

c) Status with memory may be a function implemented in the RTU. When this function is included, the number of status changes accommodated and legal bit combinations supported by the design shall be defined.

6.4.3.3 Accumulator data

Accumulator data is used to provide the number of counts for some quantity being represented by digital pulses, usually watt-hours and VAR-hours, but other counts are possible (breaker operations). Accumulator inputs are usually status inputs where the number of changes in counted and processed.

Table 11—Accumulator inputs

Parameter	Specifications	Notes
External contact format	Specify	Dry contact. Form C is typical
Minimum signal voltage	12 Vdc	Station battery may be used subject to EMI restrictions
Minimum signal current	10 mA	In metering AC is normal; new equipment may require only 2 mA
Minimum change detection time	30 ms if electromechanical 1 ms if solid state	—
Counts per contact cycle	Specify	With de-bounce filter
Maximum count rate	10 counts per second	—
Minimum accumulator count range	Specify	~15 min at maximum rate
Accumulator freeze/retrieve command	Specify	—
Non-volatile memory	Specify	—

The following characteristics shall be defined when pulse accumulation and accumulator data processing is included:

a) Input circuit (two or three terminal and how input circuit operates)

b) Sources of freeze command, if any (internal/external)

c) Ranges of values (RTU and master station)

d) Nominal and maximum counting rates

e) Source of memory power

f) Input voltage if externally powered

g) Reset command (if any)

h) Maximum count value

i) Action at maximum count value (saturate or rollover)

6.4.3.4 Sequence of events (SOE) data

The following characteristics shall be defined when SOE data acquisition capability is included:

a) Time resolution

b) Method of system time synchronization

c) Time accuracy between any two substations

d) Number of SOE inputs

e) Size of SOE buffers (number of SOE events that can be stored)

f) Time (minimum/maximum) between successive change(s) of an input

g) Method of indicating that SOE data is available

h) Data filter time constant and accuracy (e.g., contact de-bounce)

i) Data time skew (introduced by de-bounce filters)

j) Number of SOE events that can be transferred in one communications transaction

k) Capability of accepting the time stamp from another IED and/or replacing a received time stamp with its own time stamp

6.4.4 Output interface requirements

Outputs shall be compatible with substation and power equipment that they control. The following characteristics (see Table 12 through Table 15) are commonly specified to achieve compatibility. Where circumstances cause the designer/specifier to deviate from those listed, the designer/specifier should provide details similar to those shown such that compatibility can be assessed. In addition, the processing requirements for each input are discussed.

Table 12—Contact (electromechanical) outputs

Contact (electromechanical) outputs	Contact (electromechanical) outputs	Contact (electromechanical) outputs
Output contact format	Specify	Dry contacts
Contact current rating	10 A	Typical range 1 A to 30 A AC or DC (see Table 15 for typical values)
Contact voltage rating	125 Vdc	Resistive load
Activation time	Adjustable, 0.1 s to 30 s	—
Latched outputs available	Yes	—

Table 13—DC analog output signals

Parameter	Specifications	Notes
Nominal output signal range	± 1 mA or 4–20 mA	Constant current into a burden of 0 to 10 kΩ. ± 5 V range of voltage output is acceptable
Output signal range	± 1.2 mA	—
Maximum output load	10 kΩ 600 Ω	10 kΩ minimum for voltage outputs 600 Ω maximum for current outputs
Maximum error at 25 °C	± 0.1%	Percent of nominal output signal range includes offset, noise scale factor, and calibration error over six-month period
Maximum temperature error [a]	± 0.005%/°C	Percent of nominal output signal range
Conversion resolution, minimum (with sign)	12 bits	Binary data format
Common ground return	None	Electrically isolated
Maximum common-mode voltage (operating)	200 V peak	DC to 60 Hz, referred to equipment ground
Maximum common-mode error	± 0.1%	Percent of nominal output signal range

[a] Associated with the operating temperature

Table 14—Digital electronic output signals

Parameter	Specifications	Notes
Output data format	Specify	Application dependent
Common ground return	None	Optical coupler or equivalent
Signal voltage range	0 V to 30 V	—
Signal current range	0 mA to 50 mA	—
Signal data rate	Specify	—
Signal duration	Specify	—

Table 15—Typical control circuit switching duty

Duty	Make	Carry	Duration	Break	L/R ratio
Breaker tripping	30 A at 125 VDC	30 A	0.5 s	0.0A	0.04 s
Breaker closing	10 A at 125 VDC or 120 VAC	2.0 A	1.0 s	2.0 A	0.04 s for DC 0.4 pf for AC
Switcher tripping	30 A at 125 VDC	30 A	0.5 s	0.0A	0.04 s
Switcher closing	10 A at 125 VDC or 120 VAC	2.0 A	1.0 s	2.0 A	0.04 s for DC 0.4 pf for AC
Pilot duty	0.50 A 125 VDC or 120 VAC	0.50 A	Indefinite	0.50 A	Not applicable

When the capability to remotely control external apparatus and processes is provided, the characteristics of such a control capability shall be defined. Definition of characteristics common to all control interfaces shall include the following:

a) Control sequence description (select before operate, direct/immediate operate, etc.)

b) Type of checkback message, if required (echo or re-encoded)

c) Security of control sequences

d) Broadcast controls

6.4.4.1 Equipment control with relay interface

Control using a relay output shall be defined as follows:

a) Dwell time of relay contacts

b) Number of relays that can be simultaneously energized in each type of RTU

c) Processing actions (e.g., logging and alarm suppression)

d) AC or DC ampere and voltage ratings for relay contacts

6.4.4.2 Equipment control with setpoint interface

Control using a setpoint output shall be defined as follows:

a) Resolution of setpoint value

b) Duration of output value

c) Processing actions (e.g., limit check, equation, and alarms)

d) Electrical interface

6.4.4.3 Equipment/process control with electronic interface

Control using an electronic interface shall be defined as follows:

a) Timing diagram of signals

b) Interface communication protocol

c) Processing actions associated with control

d) Physical interface

6.4.4.4 Automatic control functions

When the capability to automatically control external apparatus is provided the characteristics of such control capabilities shall be defined as follows:

a) Location of automatic control logic
b) Control equation(s)
c) Feedback value and accuracy, if closed loop
d) Frequency of execution
e) User alterable control parameters
f) Associated logging or alarming
g) Method of altering control logic

6.4.5 Computed data

The following characteristics shall be defined when the capability of computing data (which are not directly measured) is included:

a) Location (RTU or master station)
b) Equations supported
c) Resulting data types (numeric or logical, or both)
d) Downstream functions (e.g., limit checking)

6.4.6 Alarm data

The following characteristics shall be defined when the capability to process and report alarm conditions is included:

a) Conditions reported as alarms (calculated or uncalculated)
b) Methods of acknowledgment (single or groups)
c) Methods of highlighting alarms (e.g., flash, tone)
d) Information in alarm messages
e) Hierarchy of alarms (priority level)
f) Size of alarm queue(s)
g) Queue management (e.g., time ordered)
h) Alarm limit(s)
i) Overall alarm management philosophy shall be documented
j) Maximum alarm generation rate
k) Maximum number of standing alarms that can be allowed
l) Alarm filtering

Care should be given to prevent the alarm system from overwhelming the operators with data during an event. Alarms should always be logged, whether or not they are presented to the operators. Filtering should

be used to limit the amount of data that an operator will be required to act upon. In no situation should the operators be provided with more alarm data than they can process and respond to with actions.

6.4.7 Digital fault data

The RTU(s) and their microcomputers are becoming sophisticated enough that they can monitor power waveforms at such a rate as to be able to record high resolution data for pre-fault, fault, and post-fault analysis. The following characteristics shall be defined when the capability to process and report digital fault data is included:

a) Samples per cycle

b) Number of data points per fault

c) Maximum buffer size (total samples to be stored)

d) Sample triggers

e) Number of faults to be reported and stored

f) Means of reporting digital fault data

g) Methods of storing fault data

h) Number of pre-fault and post-fault cycles to be stored

6.4.8 Isolation

The designer/specifier should assess the requirement for isolating inputs and outputs from controllers and devices to the equipment providing the inputs and controls. Inputs may need to be isolated from each other or from common power supplies (both sources and returns) or between the device and the input for testing. Outputs may need to be isolated from each other or from common power supplies (both sources and returns) or between the devices and their outputs for testing. On IEDs that provide contacts which may be field configured as either input or output contacts, special care may be required to prevent input leakage currents from impacting the devices connected to the output contacts. Annex E discusses common output configurations and interfaces as well as methods to disable outputs from controlling equipment. The activity of disabling outputs from controlling equipment is commonly called “Local Disable.”

Isolation can be accomplished through test switches, sliding link terminal blocks, disconnecting terminal blocks, or other appropriate methods. The designer/specifier should specify the means by which the isolation is accomplished.

6.4.9 Surge suppression

Many I/O circuits terminating in the equipment are subject to surge suppression to protect the equipment electronics. Surges typically result from the operations of devices connected to the I/O that generate transient voltages that exceed the nominal operating voltage of the circuits, usually from inductance of the driven device. Surges may also be present from faults, distribution of transient current through the ground mat, and radiating sources within the equipment environment.

It is common practice to provide over-voltage protection devices to clamp the transient voltages and shunt the resulting surge current to ground. Any number of devices may be used for this purpose. They may be internal to IEDs and devices or applied by to circuits externally the users or both. The designer/specifier should be aware that there may be multiple surge suppression devices on any given conductor and that they should coordinate such that they all clamp at the same voltage to prevent creating a “sacrificial” device along the distributed wiring. Surge suppression devices also need to be specified with sufficient energy absorbing capacity so as not to become a reliability issue. Directing the surge currents to ground may also have detrimental effect should a protection device fail in the short-circuited mode and thereby ground the

circuit it is protecting. Location of surge suppression devices with IEDs may impact the reliability of the IED as a whole and should be specified as required.

Operation of control circuits generally produces transient voltages and currents at the beginning and end of the control actuation. The designer/specifier should consider the method to be applied to control such transients and the effects of that method on interface and other devices. Routing transient suppression currents to ground may become a source of reliability concern over time as the failure of suppression devices can

a) Make unintentional control circuits connections to ground
b) Create unintentional circuit paths through ground
c) Allow multiple grounds to create ground "loops"
d) Permit false tripping from unsuppressed transients
e) Induce failure to trip via shorted control conductors

Transient suppression devices are generally not monitored and their failure can go undetected until some unexpected, undesirable, or unexplainable incident points to them as potential contributors.

6.4.10 I/O expansion

The designer/specifier should assess the long-term requirements for system I/O. Depending on the IEDs included in the automation system and the system architecture, the capability to expand point count for future requirements may be limited. The designer/specifier should explore the requirements for future expansion and provide for the reasonable expected expansion.

6.4.11 IED expansion

The designer/specifier should assess the long-term requirements for system IEDs. Depending on the IEDs included in the automation system and the system architecture, the IEDs functioning as a master may have limited capability to expand beyond a certain number of slave IEDs without compromising the performance of the master IED. The designer/specifier should explore the requirements for future expansion and provide for the reasonable expected expansion.

6.5 Communication interfaces

IED network communication interfaces should meet the requirements specified in IEEE Std 1613. While not specifically addressed in IEEE Std 1613, the designer/specifier may apply IEEE Std 1613 to the serial communication interfaces. However, two characteristics are common to internal and external modem interfaces and shall be measured regardless of the configuration utilized:

a) Surge withstand capability measured between data communication equipment and the communication channel is defined in IEEE Std 1613 shall be used in common mode only with the channel connected to the data communication equipment.
b) Channel bit error rate is measured between data communication equipment and control and data acquisition equipment. Due to the variety of channel and modem qualities available and in use, an average value of 1 bit error in 10^4 bits is recommended for design and analysis purposes. For Ethernet network systems, the bit error rate objective should be below 1 bit error in 10^{10} bits for good installations.

6.5.1 Serial ports not connected to external data communication equipment (e.g., modems)

The following are the interface characteristics:

a) *Interface signals.* As a minimum each interface shall satisfy the cabling requirements as defined in TIA-530-A, category 1 according to EIA-422-B or TIA-485-A for balanced voltage digital interface circuits or category 2 according to TIA/EIA 423-B for unbalanced voltage digital interface circuits. Where digital interfaces according to TIA-232-F are utilized, the necessary adapters shall be provided as part of the control and data acquisition equipment.

b) *Signal repetition rate.* All nominal signaling rates in kilobits per second shall be in accordance with ANSI X3.1.

c) *Signal quality.* All signals shall meet TIA/EIA 404-B for asynchronous DCE and TIA 334-C for synchronous DCE.

d) *Noise limits.* These are defined in the references given in item c).

6.5.2 Interface characteristics to internal data communication equipment (e.g., modem) when the modem is provided as an integral part of the control and data acquisition equipment

The following are the interface characteristics:

a) *Signal impedance.* All inputs and outputs shall be balanced 600 Ω ± 10% whenever signal rates require standard voice grade channels.

b) *Signal level.* Input (receive) levels may range down to –45 dBm and output (transmit) levels shall not exceed 0 dBm. The output level and receive sensitivity shall be adjustable in steps of 4 dB or less.

c) *Signal stability.* All inputs and outputs shall be stable within ± 1 dB for at least one month without adjustment.

d) *Signal linearity.* The output (transmit) level shall be linear within ± 1 dB over the output level range and frequency allowed. Input (receive) level linearity and delay distortion are not defined and should be specified for each channel type and data rate required.

e) *Signal distortion.* All input and output signals shall not contain rms harmonics that exceed 2% dBm whenever signal rates require standard voice grade channels.

f) *Signal carrier.* Specify center frequency and bandwidth.

6.5.3 Protocol

The designer/specifier shall specify the protocol(s) required between the following:

— SCADA master(s) and RTU(s)

— RTU and IEDs

IEEE Std 1379 is the recommended practice between the substation RTU and IEDs. The designer/specifier may also apply IEEE Std 1379 to SCADA master communications. In addition to IEEE Std 1379, the designer/specifier may also use IEC 61850 for substation and SCADA master communications. Besides defining the protocols being used, the designer/specifier should also define the following:

a) Number of channels

b) Channel considerations

c) Error detection techniques

d) Channel switching

e) Number of RTUs per channel and/or channels per RTU

f) Number of retries each attempt

g) Time out value(s) by message type

h) Communication error reporting, failure criteria, and recovery

i) Channel quality monitoring (normal and backup)

j) Channel diagnostic/test provisions

k) Equipment interfaces

l) Report-by-exception polling or point scan, or both

Systems with report-by-exception functions shall have the capability to report all data for initialization and periodic update purposes.

The data acquisition capability for each data type used in the protocol shall be defined in terms of the following characteristics:

— Scan groups. Number of scan groups, size of each group, points in each group.

— Scan cycle. Time to complete the acquisition of a scan group from all IEDs on the communication channel.

The communication hardware related performance capabilities used in the calculation of scan cycle shall be defined.

6.5.4 Channel considerations

The routine loading of each serial communication channel by SCADA equipment shall be calculated as described in Annex C to establish the adequacy of the channel configuration. The channel routine load factor is defined as the worst-case fractional channel operating time required to complete all routine (i.e., periodic) data and control transactions between the master station and the attached RTU(s). Where report-by-exception data acquisition techniques are employed, realistic assumptions for the average number and length of exception transactions during the repetition interval shall be made. The repetition interval of SCADA system periodic transactions typically ranges from seconds to hours.

It is recommended that the channel routine load factor, with fully-expanded RTUs, should be less than 0.75. The remaining channel capacity will then be available for occasional retransmissions and for event-driven data and control transactions. To minimize the incidence of message failures due to channel errors, it is also recommended that transaction lengths be limited to about 250 channel bit times. When the channel bit error rate reaches one in 10 000 bits, 2.5% of such transactions will fail. Automatic repetition (retry) of transactions that fail may be implemented but no more than three consecutive retries should be permitted. If the transaction is not completed satisfactorily at the fourth attempt, the relevant RTU, or the channel itself, should be declared at least temporarily inoperative.

6.5.5 Sub-master/slave RTU links

The sub-master/slave RTU links shall consist of at least one communication link to a master station as well as at least one additional link to slave RTUs, or a link to a distributed RTU module of the same RTU, or a link to an IED.

6.5.5.1 Sub-master RTUs

The communications link(s) to the sub-master RTUs are identical to that described in 6.5.5 on SCADA master to RTUs.

6.5.5.2 RTUs

The communication links to slave RTUs is similar to that described in 6.5.5.1, except that the role of the master station is assumed by the sub-master RTU. The protocol used need not be the same as that used between the sub-master RTU and the master station. Indeed, it is usually the case that the protocols are not the same.

6.5.6 Distributed I/O modules

The communications link between the RTU network controller and I/O modules can be a proprietary design of the RTU supplier. When these I/O modules are contained within single or multiple RTU cabinets using a proprietary communication network, the definitions and descriptions of this link are beyond the scope of this standard. When these distributed I/O modules are installed outside the RTU cabinets, outside in the substation yard, or use Ethernet networks, the appropriate serial or network requirements of this standard shall apply.

7. Environmental requirements

This clause contains the definition of the environment in which control and data acquisition equipment is required to operate.

When unusual conditions exist, they shall receive special consideration. Such conditions shall be brought to the attention of those responsible for the application, manufacture, and operation of the equipment. Devices and apparatus for use in such cases may require special construction or protection. The user should specify those special physical requirements that apply to specific locations. Examples are as follows:

a) Damaging fumes or vapors, excessive or abrasive dust, explosive mixtures of dust or gases, steam, salt spray, excessive moisture, or dripping water

b) Abnormal vibration, shocks, or tilting

c) Radiant or conducted heat sources

d) Special transportation or storage conditions

e) Unusual space limitations

f) Unusual operating duty, frequency of operation, difficulty of maintenance

g) Altitude of the operating locations in excess of 2000 m (6600 ft)

h) Abnormal electromagnetic interference

i) Abnormal exposure to ultraviolet light

7.1 Environment

7.1.1 Ambient temperature and humidity conditions

Ambient temperature and humidity are defined as the conditions of the air surrounding the enclosure of the equipment (or the equipment itself, if it uses open rack construction) even if this enclosure is contained in another enclosure or room.

For temperature and humidity parameters by operating location, see Table 16. This table is a guideline to establish five equipment classification groups. Equipment designated to be in a specific group shall meet all conditions set forth in that group.

Equipment subjected to temperature and humidity variations outside of the first four group classifications listed in Table 16 will require special consideration. Methods to resolve these problems include the following:

a) *Low temperature.* A thermostatically controlled heater strip should be used in the cabinet enclosure or use wide temperature range equipment.

b) *High temperature.* A sun shield, some other cooling method, or wide temperature range equipment should be used.

c) *High humidity.* Heater strips or special shelters or dehumidifier should be used.

d) *Low humidity.* A humidifier should be used to maintain acceptable humidity levels.

e) *Temperature restrictions.* If it is necessary to use heating/cooling equipment to meet the parameters set forth in Table 16, the equipment should be so marked by a warning sign and a warning statement in the associated documentation.

f) *Limit alarms.* If critical equipment may be exposed to temperature or humidity conditions that might exceed design limits, consideration should be given to local and/or remote audible and/or visual alarm indications when such limits are reached.

g) *Limit shutdowns.* If critical equipment may be damaged by operation under temperature or humidity conditions that exceed design limits, consideration should be given to automatic shutdown equipments if abnormal conditions exceed pre-specified time limits.

Table 16—Operating temperature and humidity by location

Equipment group	Typical location of the equipment	Humidity operating range (in percent relative humidity)	Temperature operating range (^{o}C)	Allowable rate of change of temperature (^{o}C/h)
(1)(a)	Unspecified	Up to 95% without internal condensation	–40 to +85	Not specified
(1)(b)	Unspecified	Up to 95% without internal condensation	–30 to +65	Not specified
(1)(c)	Unspecified	Up to 95% without internal condensation	–20 to +55	Not specified
(2)(a)	In a building with air-conditioned areas	40 to 60	+20 to +23	5
(2)(b)	In a building with air-conditioned areas	30 to 70	+15 to +30	10
(3)	In a building with heating or cooling but without full air conditioning	10 to 90 without condensation[a]	+5 to +40	10
(4)	In a building or other sheltered area without special environmental control	10 to 95 without condensation[a]	0 to +55	20
(5)	Outdoors or location with wide temperature variations	10 to 95 without condensation[a]	–25 to +60	20
(6)	Extremes outside the above	Specify	Specify	Specify

[a] Maximum wet bulb temperature of 35 ^{o}C

NOTE—Equipment group 1 corresponds to operational and storage temperature ranges specified in IEEE Std 1613 for communications networking devices.

7.1.2 Dust, chemical gas, and moisture

Suppliers shall be made aware of the presence of atmospheric pollutants so that special provisions for protection can be made where necessary.

In groups (2), (3), and (4) of Table 16, all equipment cabinets that are vented shall have dust filters. In groups (4) and (5), equipment that is exposed to moisture, corrosive or explosive gases, or other unusual environmental conditions shall have a special enclosure. Available types of enclosures for various conditions are specified in NEMA 250.

Consideration should be given to possible contamination occurring inside the enclosure during storage and transit, and also when the enclosure is opened for maintenance or repairs. In extreme cases (e.g., possible contamination with explosive gas mixtures), supplemental methods for purging the enclosure should be provided.

7.1.3 Altitude

The equipment shall be suitable for operation at altitudes from –100 m (–330 ft) to up to at least 1500 m relative to mean sea level.

7.1.4 Ultraviolet (UV) light exposure

Suppliers shall be made aware of the expected level of exposure to ultraviolet radiation attributable to sunlight where equipment is to be installed outdoors. Equipment cabinets, paint finishes, and jacket material of any exposed cabling shall be sufficiently treated to resist damage or degradation due to ultraviolet exposure. The designer/specifier shall supply information pertaining to altitude above or below mean sea level and the anticipated average daily hours of direct exposure to sunlight.

7.2 Vibration and shock

7.2.1 Operation

Where control and data acquisition equipment will be subjected to vibration or shock, the designer/specifier shall express the local vibration environment as constant velocity lines to represent vibration severity levels over a specified frequency range.

Five severity classes are listed in Table 17 as examples in typical locations.

Table 17—Vibration and shock severity classes

Class	Velocity v (mm/s)	Frequency range (Hz)	Examples
V.S.1	< 3	1 to 150	Control room and general industrial environment
V.S.2	< 10	1 to 150	Field equipment
V.S.3	< 30	1 to 150	Field equipment
V.S.4	< 300	1 to 150	Field equipment including transportation
V.S.X	> 300	—	To be specified by user
Source: IEC 654-3, Operating Conditions for Industrial Process Measurement and Control Equipment, Part III, Mechanical Influences.			

Shock phenomena that may occur during handling for operation and maintenance of equipment shall be expressed in terms of an equivalent height of fall. This relationship is shown in Table 18.

Table 18—Shock phenomena

Height of fall (mm)	Treatment (hard surface)
25	Light handling
50	Light handling, heavy material (> 10 kg)
100	Normal handling
250	Normal handling, heavy material (> 10 kg)
1000	Rough handling
1500	Rough handling, heavy material (> 10 kg)
Source: IEC 654-3, Operating Conditions for Industrial Process Measurement and Control Equipment, Part III, Mechanical Influences.	

7.2.2 Transportation

The designer/specifier shall assess the requirements for special care to be used in the transportation of equipment. The equipment shall be packaged and braced so as to prevent damage during transit. Items such as swinging panels should be strapped and blocked to minimize stress on the hinges.

All control and data acquisition equipment should show no degradation of mechanical structure, soldered components, plug-in components, or operation after shipping.

7.3 Seismic environment

The purpose of this subclause is to describe the analytical and test criteria for equipment that is required by the designer/specifier to operate in an environment subject to seismic disturbance. The designer/specifier shall supply, during system development, information that will allow the supplier to make a seismic equipment analysis and submit an equipment seismic report (e.g., for relays, see IEEE Std C37.98).

7.3.1 Seismic equipment analysis

The designer/specifier shall supply a response spectrum in the form of frequency vs. amplitude for the location site of the equipment to be installed. Alternately, the designer/specifier may supply information, on which the supplier is to base the analysis, listed in the following:

a) Earthquake reports, which can be obtained from the George Housner Earthquake Engineering Collection, housed in the Sherman Fairchild Library for Engineering and Applied Science at California Institute of Technology, Pasadena, CA

b) Data pertaining to typical foundations and soils

c) A study of the support structures

d) An indication of the seismic zone in which the equipment is to be installed (see the International Building Code or IBC [B19])

7.3.2 Equipment seismic report

The following information is typically required as part of an equipment seismic report:

a) An outline drawing of the equipment locating the centers of gravity, weights of major components, and the location and size of hold-down bolts

b) The maximum vertical and horizontal forces, and the upsetting moments that the foundation shall be capable of resisting

c) The portion of the equipment that requires an integral pad, and the portion(s) that may be mounted on independent foundations

d) An outline drawing of the equipment showing the expected maximum displacement of electrical terminals and other points of interconnection between the apparatus and other equipment

e) The fundamental natural frequencies and sampling data

f) An analysis and description of the probable modes of failure. Maximum working stresses should also be included in the analytical data furnished.

g) The ductility factors used should be indicated in the analytical data furnished

h) Satisfactory connections between isolated and non-isolated apparatus should be proposed

i) A description and results of the dynamic analysis used

j) A description of the test method that has been used to determine the natural frequencies and results of damping of the apparatus together with the static analysis, when a dynamic analysis is not applicable

k) A summary of the results of an explanation of the seismic proof test procedures (see IEEE Std 344 [B15])

7.4 Impulse and switching surge protection

The purpose of this subclause is to describe design criteria and recommend practices that will minimize the adverse consequences of exposure to impulse discharges and switching surges. Effective protection can only be accomplished through a combination of adequate design and proper installation.

7.4.1 Design criteria

The basic design goal for achieving protection from impulse and switching surges shall be that of keeping any abnormal voltage or current, or both, out of the equipment cabinets. The electrical data, power, control, and communication interfaces (e.g., inputs and outputs to an IED, serial ports, IRIG-B ports, Ethernet ports) shall be designed to withstand the surge withstand capability tests and impulse tests as defined in IEEE Std 1613 without IED damage, misoperation, or data corruption.

7.4.1.1 Basic protection

This design criteria requirement applies to equipments mounted in substation yards or control houses. The designer/specifier may waive this requirement if equipment is installed in a protected environment where it will not be exposed to intra-cabinet, inter-cabinet, or external adverse surge conditions.

7.4.1.2 Voltage surges

DC systems experience events that impress voltage disturbances and transients that propagate throughout the system. These are associated with the operation of specific equipments such as circuit breakers, motor operated switches, and auxiliary support systems. The designer/specifier should assess the impact of these events to assure they will not damage or disrupt operation of the automation system. It is likely some DC powered devices will experience voltage excursions in excess of the nominal operating ranges specified above and special consideration should be given to their effects.

Voltage surges can exceed the test limits specified in IEEE Std 1613. Thus, they may enter the cabinet and cause damage despite the SWC protection provided. Equipment failures resulting from such damage shall be fail-safe. Logic designs shall be such as to minimize the possibility of false or improper operation of field devices. Partial failures that do not disable the equipment but can reduce or eliminate security

features, such as error checking in communication circuits, shall be detected and cause the blocking of control outputs to prevent false operations of field devices.

7.4.2 Installation criteria

The basic installation goal for achieving protection from impulse and switching surges shall be to minimize the exposure of all connecting wires and cables.

7.4.2.1 Power, signal, and communication circuits

Power, signal, and communication circuits provide a path through which impulse and switching surges enter equipment. Circuits totally within a protected building can generally be installed without regard to these external effects. See IEEE Std 1615 for Ethernet network cabling recommendations. These circuits may still be subjected to transients generated by the operation of solenoids and control relays within control panels and inside the building. Such transients are described in the fast transient tests in IEEE Std 1613. Circuits that are connected to, or are part of, circuits not within a protected building shall be installed in a manner that minimizes exposure.

7.4.2.2 Installation constraints

When installation constraints result in a high degree of exposure to impulse or switching surges, supplementary protection such as spark gaps or surge limiters should be considered (see IEEE Std 525). IEEE Std 525 provides guidance relating to GPR impact. IEEE Std 487 provides guidance in protecting wire-line facilities serving substations. As an option, fiber optic cable can be used to minimize exposure (see IEEE Std 1590).

7.5 Acoustic interference limitations

The sound level from any equipment at a distance of 3 ft in any direction shall not exceed 55 dB above the standard reference level with the Type “A” weighted network. The measurements and the weighted network shall be in accordance with ANSI S12.10. The sound level measurements shall be made with a sound level meter that meets or exceeds ANSI S1.4.

7.6 EMI and EMC

Manufacturers shall design and test their equipment to ensure that EMI limits are not exceeded, and the designer/specifier shall select, design, and test locations (environments) to ensure that EMC limits are not exceeded.

Computer and microcomputer-based equipment are expected to perform their intended functions in substations even when exposed to transient electromagnetic interference. The designer/specifier should be aware of EMI in substations and either specify the worst-case EMI level for which proper operation shall be guaranteed, or ensure that the risk of misoperation in the presence of EMI is acceptable.

7.6.1 EMI limits

Control and data acquisition equipment shall not generate radiated emissions in excess of (1 V/m)/MHz as measured 1 m from the enclosure. Manufacturers shall mechanically and electrically design equipment to satisfy emission limits by employing attenuation techniques such as isolation, shielding, grounding, gasketing, filtering, and bonding. Copper cables are susceptible to transferring radiated emissions to the connected equipment. If adequate protection cannot be assured, fiber optic cables should be utilized.

7.6.2 EMC limits

Control and data acquisition equipment shall be capable of operating in radiated fields as specified by the designer/specifier. Information available to date indicates that the average field strength in substations may run in the order of (1 V/m)/MHz. The specified value of (1 V/m)/MHz refers to broadband radiated fields due to the station environment, resulting from such things as corona and switching transients. This requirement is not intended to cover narrowband radiated field sources such as electronic test equipment or portable radio transmitters (walkie-talkies). Where such equipment may be used, the field strength is properly expressed as volts per meter at a specified frequency, and different EMC limits may be required (see IEEE Std 1613). The designer/specifier shall utilize fiber optic cable or mechanically and electrically design the equipment location for conducting susceptibility limits by using cable shielding and grounding techniques found in IEEE Std 525.

7.6.2.1 High radiated emissions

Whenever equipment is to be located in an environment and is susceptible to radiated emissions that are higher than those specified in 7.6.2, then either

a) The manufacturer should shield from radiated sources with an enclosure that provides the necessary attenuation, or

b) The user should provide additional structural attenuation

The approach taken should be an economic one that considers the location's configuration, the signal range of interest, and the amount of additional field strength encountered.

When metallic enclosures are used for protection in areas with high radiated emissions, difficulties during maintenance may be created if the enclosure is opened while the source of the emissions is still emitting. When this is the case, suitable signs shall be employed to warn of the risks associated with opening the enclosure in the presence of the radiating emissions.

7.6.2.2 High magnetic fields

Equipment that is sensitive to magnetic fields should be stored and operated in environments that limit magnetic flux density. Typical storage limitations for magnetic tape and disk units are in the range of 50×10^{-4} to 70×10^{-4} Tesla.

8. Characteristics

This clause defines and discusses general characteristics that are required of the control and data acquisition equipment. These characteristics include reliability, maintainability, availability, security of operation, expandability, and changeability.

8.1 Reliability

Mathematically, reliability is the probability that a unit or system will perform its intended function under specified conditions during a specified period of time. For complex equipment, failures will occur on the average at a constant rate throughout the useful life of the equipment. This allows the manufacturer to characterize equipment reliability with MTBF.

The exceptions to this constant failure rate are a higher, decreasing failure rate, early in the equipment's life, called "infant mortality," and a higher, increasing failure rate, that signals the onset of "end-of-life." These phenomena give a typical plot of failure rate vs. time, a shape known as a "bathtub curve." Reliability models and predictions may be made in accordance with MIL-HDBK-217 [B24], or as directed

by the designer/specifier. Software tools (e.g., spreadsheets and programs) are available to facilitate these calculations.

Reliability-related design goals for equipment shall be as follows:

a) Infant mortality be eliminated by the supplier before delivery of the equipment

b) The MTBF of the equipment be above a specified, acceptable, lower limit

c) End-of-life begin only after a specified, acceptable usage period

d) A single hardware or software failure anywhere in the system shall not result in a critical failure (e.g., false operation of an external device)

e) Component failures do not propagate throughout the system, increasing the scope of repair and loss of function

The failure modes of equipment and the effects of these failures shall be formally analyzed by the supplier. The results of these FMEA shall be available for review upon request.

Failure distribution vs. time data for equipment while in the possession of the supplier, and for those field units for which data are available from the users, shall be documented and available upon request.

Manufactured and/or supplier-procured parts and components that can cause a critical or major system failure are subject to these requirements. When these values are not within acceptable limits, redundant systems and/or components should be utilized.

8.2 Maintainability

Control and data acquisition equipment shall be maintainable on-site by trained personnel according to the maintenance strategy specified by the designer/specifier. Requirements for training, documentation, spares, etc., shall take the designer/specifier's organization and geography into account.

The most common repair strategy is for the supplier to train personnel to identify and replace failed modules on-site from a stock of spare modules. These may then be either returned to the supplier for repair or repaired to the component level at a maintenance facility. On-site service by the supplier may be necessary.

The supplier shall, upon request, be required to provide as part of the system proposal, a list of test equipment and quantities of spare parts calculated to be necessary to meet the specified availability and maintainability requirements. In establishing the quantities of spare parts, the supplier shall consider the time required to return a failed component (field and/or factory service) to a serviceable condition.

The maintainability of equipment is reflected in MTTR. The MTTR values used in the supplier's availability computations shall be based to the maximum extent possible upon maintenance experience.

MTTR is the sum of administrative, transport, and repair time:

a) Administrative time is the time interval between detection of a failure and a call for service.

b) Transport time is the time interval between the call for service and on-site arrival of a technician and the necessary replacement parts.

c) Repair time is the time required by a trained technician, having the replacement parts and the recommended test equipment on-site, to restore nominal operation of the failed equipment.

Unless otherwise specified by the designer/specifier, the following values shall be used in availability calculations:

— Administrative time 0.0 h

— Transport time 0.5 h

When insufficient maintenance data has been accumulated to provide MTTR values, then the appropriate segments/procedures as defined in MIL-HDBK-471 [B25] may be used.

Provisions to enhance the maintainability shall include the following:

— Useful training and documentation, directed toward maintenance requirements and techniques

— Equipment self-tests, diagnostics, and trouble shooting procedures to identify failure or malfunction to the optimal field-replaceable module level

— Readily accessible test and/or disconnect points, to facilitate fault isolation. Placement of components on cards shall allow access for test probes and connectors

— Physical provisions to preclude improper mounting of modules, including interchange of modules of a same or similar form that are not interchangeable

— Provisions (e.g., labels) to facilitate identification and proper mounting of units or modules

— Identifying, orienting, and aligning provisions for cable and connectors

— Location and/or guarding of adjustment points such that adjustments will not be disturbed inadvertently

— Location, guarding, and/or labeling of manual controls to avoid dangerous voltages or other hazards

— Provision for connecting external I/O simulation equipment

— Provision of extender cards for card cage mounted circuit cards

8.3 Availability

Availability (A) is defined in Equation (2) as the ratio of uptime to total time (uptime + downtime):

$$A = \frac{\text{uptime}}{(\text{uptime} + \text{downtime})} \times 100\% \quad (2)$$

Downtime normally includes corrective and preventive maintenance. When system expansion activities compromise the user's ability to operate apparatus via the system, this may also be included in downtime.

Typical availabilities achievable by non-redundant commercial grade equipment range from 99.99%, for simple devices, to approximately 97% for complex subsystems. Proper use of redundant configurations with automatic failover can provide an overall availability of primary system functions of 99.9%.

The designer/specifier shall specify the availability level required, and the planned maintenance strategy, requiring suppliers to provide supporting predicted availability calculations in their proposals.

For design analysis, and to determine the prediction of availability for subassemblies and units, Equation (3) for predicted availability (A_P) utilizing MTBF and MTTR shall be used.

$$A_p = \frac{MTBF}{(MTBF + MTTR)} \quad (3)$$

Equations for modeling complex designs shall be formulated by the supplier in accordance with 9.1. Use of the equations associated with parallel redundant components (or subsystems) is valid under the following conditions:

a) Failure of parallel elements is independent. Component failures do not propagate failures of other components.

b) Sufficient repair turnaround and standby replacement parts are available to handle multiple simultaneous failures.

The impact of the outage of each system element or function on the availability of the total system shall be mutually agreed upon between the user and the supplier.

Availability test results shall be calculated separately for major system components. Since these components may have a varying impact on the usefulness of the system as a whole, different definitions of downtime are applicable.

Major component downtime shall be defined to reflect the proportional significance of the equipment that is down. For example, downtime for the data acquisition system could be defined as the sum of the downtime for all RTUs divided by the total number of RTUs. At the master station, downtime should not include malfunctions in peripheral devices that do not detract from the functional capabilities of the master station as a whole (e.g., printers).

8.4 Security of operation

Security of operation is defined as the ability to recognize an inappropriate or undesirable operation or condition in such a fashion that causes an appropriate alarm, a non-operation, or both.

Security of operation considerations are divided into the following three areas:

a) Operating practice and procedures

b) Communication security

c) Hardware and software design

The use of the term “security” in this section is not in the same context as Cyber Security. Historically, “security of operation” has been used to mean “assurance of operation.”

8.4.1 Operating practice and procedures

Security features comprising operating practice and procedures include the use of function and operating checks (manual and/or automatic). The designer/specifier should include which function and operating checks are included in the system:

a) Control function check (loop-back)

b) Scan function check (loop-back)

c) Poll function check

d) Logging function check

e) Queue overflow alarms

f) Diagnostic aids

g) Calibration checks

h) Logging of all operator actions, including whether the equipment completed the requested action

i) Tagging of out-of-service control points at the user interface

j) Use of at least one local/remote switch, with feedback to a status point, to disable control actuators while the system is being serviced

Equipment designed for remote control of power system devices shall use both a select-before-execute user interface sequence and a checkback-before-operate communication sequence for control operations.

The user interface sequence shall provide visual feedback of the selection to the user, so the user can verify the correct interpretation of the selection before executing the control function.

The communication sequence checkback message shall be derived from the systems point selection hardware, and not be just a simple echoing of the received select message. This allows the master station to verify not only that the communication was error free, but also that the systems I/O hardware and software acted correctly in interpreting the selection.

In order to provide maximum security when the designer/specifier states that there is significant risk of random channel noise being interpreted as a select/execute sequence, the following safeguards should be incorporated:

— The communications protocol shall have a very effective redundancy check code (this is necessary, but not sufficient, security)

— There shall be a relatively short timeout between the select and operate steps

— The next master station message following the select shall be the execute

— The complete point identification shall be contained in the select, checkback, and execute messages, which shall be fully compared before the control operation is executed

— If any of the above checks fail, the control sequence shall be reset immediately, and a new select message shall be required to restart it

— Both the master station and substation system shall enforce the above rules.

The communication checkback sequence may be performed either concurrently with the control selection sequence at the master, or after the selection sequence has been completed. When performed concurrently, the selection of a point for control shall cause the select message to be transmitted to the slave. Upon successful receipt, the slave shall arm itself for control, generate the checkback message, and transmit it back to the master station. A valid checkback message shall result in visual selection feedback to the user, who can then choose to either execute or cancel the control function.

This type of operation requires a longer select/execute timeout, and will either violate the execute-next rule, or will stop scanning on that channel until the user responds with an execution or cancellation.

When the user interface sequence and communication sequence are performed sequentially at the master, the selection of a point for control should cause the master station to display a visual indication of that selection for verification.

In this type of operation, the user's verification of selection does not come from the slave, but all other security features may be fully implemented.

The user may then execute the control function. Status and data scanning should then be interrupted at the master, and a select message sent to the slave. The slave shall then arm the control function and return a checkback message. The checkback message shall be checked by the master, and an execute message sent

automatically to the slave. If this execute message is received as valid, the slave shall execute the command and return an acknowledgment that the function has been performed.

8.4.2 Communication message security

The designer/specifier should specify which of the following communication security features shall be included in the system design:

a) The design goal that an error in a message shall not result in a critical failure of the system.

b) Alarming the failure of an RTU to respond to a message within a specified number of automatic retries.

c) Ensuring that communication channel error control, in concert with the communication protocol and line discipline, reduce the probability of acceptance of messages received with errors to less than 1 in 10^{10} when the channel bit error rate is 1 in 10^{4}.

d) Verification of the proper operation of communication channels on a regular basis.

e) Counting, and periodically logging, communication errors on a per-channel basis.

f) Ensuring that no two IEDs with the same address share the same serial multi-drop communication channel.

g) Ensuring that each serial multi-drop RTU communication channel supports only one communication protocol.

8.4.3 Hardware/software security features

The designer/specifier should specify which of the following security features shall be included in the system hardware and software design:

a) Power supply protection—overcurrent, over/undervoltage, surge withstand, etc

b) Automatic initialization and restart

c) Equipment self-check with alarm

d) Watchdog timer(s) with alarm

e) Automatic failover with alarm

f) Fail-safe operation

g) Non-volatile station address retention in RTUs

8.5 Expandability

Expandability is the ease with which new points and/or functions, or both, can be added to the system, and the amount of downtime required to add them to the system.

Expansion point types are defined as spare point, wired point, and space-only as follows:

a) Spare point equipment is equipment that is not being utilized but is fully wired and equipped.

b) Wired point is the capacity for which all common equipment, wiring, and space are provided, but no plug-in point hardware is provided.

c) Space-only point is the capacity for which cabinet-space-only is provided for future addition of equipment and wiring.

The designer/specifier should include an appropriate amount of each type of expansion point types in the system design given that expandability limitations may include, but are not restricted to, the following:

- Available physical space
- Power supply capacity
- Heat dissipation
- Processor throughput and number of processors
- Memory capacity of all types. A requirement of no less than 50% unused main memory and spare disk capacity initially will allow enough expansion for new functions, enhancement of existing functions, and growth of the power system and the equipment that needs to be monitored. System documentation shall also be consulted to determine how much main memory capacity can be expanded over and above the capacity initially installed. As a minimum, it shall be possible to double the initial capacity with the addition of memory modules.
- Point limits of hardware, software, or protocol
- Bus length, loading, and traffic
- Limitations on routines, addresses, labels, or buffers
- Unacceptable extension of scan times by increased data (given bit rate and protocol efficiency)

8.6 Changeability

Changeability is defined as the ease with which system, RTU, and point data base parameters may be changed at both the master station and RTU. Parameters that shall be easy to change include the following:

a) Operating parameters
b) Configuration and setup parameters

The supplier's documentation shall contain the step-by-step process for 9.6.1 through 9.6.3.

8.6.1 Operating parameters

Operating parameters should be easily changed by the system user. They include, but are not limited to the following:

a) RTU on/off-scan
b) Point on/off scan
c) Point tags on/off
d) Manually entered values
e) Point alarm limits
f) Point deadband values
g) IED parameters

8.6.2 Configuration and setup parameters

Configuration and setup parameters should be easily changed and protected through role-based access controls requiring at least a user name and password. These parameters include, but are not limited to the following:

a) Configuration password
b) Major/minor alarm conditions and actions
c) User-definable calculations
d) Definition of a new IEDs or RTUs
e) Communication port and/or station address assignments
f) Addition and/or rearrangement of points
g) Correspondence of status points to control points
h) Point and state descriptions
i) Point scaling factors for conversion of data to engineering units
j) Output relay dwell times

8.6.3 Changeability limitations

Changeability limitations may result from, but are not limited to the following:

a) Inability to make master station and RTU data base changes on-line from the master station
b) Storage of parameters in memory (e.g., ROM) that is not modifiable in-circuit
c) Restrictions caused by data base structure
d) Hardware/software compatibility (e.g., software that is keyed to specific hardware)
e) Hardware limitations
f) Software operating system limitations
g) Restrictions caused by use of IEDs

9. General requirements

Adequate specification of general requirements will help contribute to a successful project. The following subclauses discuss specific requirements to ensure a successful project.

9.1 Project plan

A good project plan provides a central repository of information for the project team that covers at least the following topics:

a) Scope of work
b) Quality plan
c) Management plan
d) Documentation
e) Transition plan
f) Testing plan
g) Training plan
h) Installation plan
i) Tracking plan

The project manager develops the project plan for all project participants (designer/specifier, Vendor(s), integrator(s), and project manager). The project plan should be completed early in the project and maintained throughout the project.

9.1.1 Scope of work

The scope of work describes the project tasks, who is doing what, the roles of each project participant, the deliverables, and project schedule. The scope of work should also define the interfaces between participants and how conflicts are handled.

9.1.2 Quality plan

The quality plan describes the quality procedures to be used in the project. The quality plan should be based on the international standard ISO 9001 [B23]. The quality plan includes a set of procedures and planned work instructions to control the design and implementation process as well as inspection and verification in order to

a) Assure that the design will conform to specified requirements, including performance goals
b) Readily detect and control the disposition of nonconformance and prevent their recurrence

The project manager develops, documents, implements, and maintains the quality plan, which assures that each management action, design project and technical responsibility for quality is integrated and executed effectively. The project manager is responsible for insuring that the requirements of the quality plan are adhered to by all project participants and that major quality tasks are included in the project schedule.

9.1.3 Management plan

The role of project management is very important because of the complexity of the systems being purchased. This role can be provided by multiple sources: the designer/specifier, a vendor, an integrator, a consultant, or other third party. The important point is to define who the project manager is up front and make sure the project manager creates the project plan. The management plan details the project organizational structure. The plan lists the contact information for the persons responsible for different aspects of the project:

a) Project management
b) Project design
c) Drafting
d) Software
e) Hardware
f) Testing
g) Training
h) Installation
i) Support

The management plan also defines the communication channels that are used during project execution:

— The person to contact to submit technical problem descriptions
— The person responsible to organize meetings
— The person responsible for maintaining the project's correspondence files and records

Finally, this plan describes the agreement between parties governing when and where the project management meetings will be held.

9.1.4 Documentation plan

The documentation plan details what documentation is supplied with the project, who is providing the documentation, how the documentation is provided, the review and approval process, and when the documentation is provided. The documentation plan defines the standards applicable to the creation and approval of documentation. The project schedule should include tasks for the initial review, corrections, final review, and delivery. The schedule should include adequate time for all phases of review, with final approved copies being made available a specified time prior to use (i.e., final test plans should be delivered at least two weeks prior to the start of testing).

9.1.5 Transition plan

The transition plan describes the impact of the installation of the new system. The following aspects shall be covered:

a) The impacts on the power system

b) The measures to minimize system impacts

c) The impacts on the existing system and current and future users

d) How to resolve conflicts between current operating requirements and requirements for installation and testing of the new system

The project schedule includes the proposed implementation schedule.

9.1.6 Test plan

The test plan describes how and when tests will be performed. The plan specifies how these tests will be divided (hardware and software etc.) and the various documents to be used during the tests.

The document plan specifies the format of the test plan documents. The project schedule specifies the delivery of the test plan documents for review and approval.

It is recommended that every test plan include an adequate allowance for unstructured testing.

9.1.7 Training plan

The training plan describes the different training sessions to be provided and includes the following information:

a) Who should attend

b) Session contents and goals

c) Location

d) Schedule

e) Prerequisite training and/or experience required for each segment

f) Instructor qualifications

g) The provider of the course material

9.1.8 Project tracking plan

The project tracking plan describes the methods and requirements for the project status reports. The plan identifies who is responsible for creating the progress report. The progress report includes the significant accomplishments to date and potential obstacles. The progress report also includes a project schedule. The project schedule identifies relationships between tasks and provides milestones for project tasks. Use of a comprehensive commercially available project tracking and scheduling software package is recommended.

9.2 Marking

Major components and major subassemblies need to be suitably marked as necessary for safety and identification.

9.2.1 Identification

Identification provides a correlation between devices and the project documentation and depending upon the naming convention can indicate the function or purpose of the device being identified. The identification convention should be uniform throughout the system and includes the use of color coding, labeling, naming conventions, and parts numbering.

9.2.2 Nameplates

Identification marks are permanently affixed to what they identify by using nameplates. Each major component requires a nameplate. Nameplate locations can be located on the front and rear of panels/racks, enclosures, and devices. Nameplate locations shall be such that no disassembly, parts removal, etc., is required to view the nameplate. The type of nameplate to be used can be plastic or tape. Plastic nameplates can be secured using screws or adhesive. Nameplates should include the following information, as applicable to the equipment:

a) Identification as referenced in the documentation
b) Manufacturer’s name
c) Reference to procurement specification and purchase order
d) Rated voltage (AC or DC, or both)
e) Rated continuous current
f) Rated frequency (if necessary)
g) Revision or version level

Nameplates mounted on panels/racks or devices should be legible at a distance of approximately 1 meter. Nameplates can be permanently attached using adhesive or screws, depending upon the location of the nameplate, type of nameplate, and the surface it is to be mounted on. Panel mounted nameplates can be attached using either adhesive or screws.

The designer/specifier needs to define the labeling conventions for all types of devices and equipment, including panels/racks/cabinets that contain more than one type of equipment and/or equipment from more than one manufacturer.

Permanently affixed bar coded labels should be considered, in addition to nameplates, for identifying equipment and subassemblies.

Programmable parts such as programmable read-only memory (PROM), erasable programmable read-only memory (EPROM), Generic Array Logic (GAL), Field Programmable Gate Array (FPGA), and similar

components should be marked by the supplier with a program identifier and version. The designer/specifier is encouraged to acquire programming tools for these components and their programs.

9.2.3 Warning

Warning signs or safety instructions are required where there is a need for general instructions relative to safety measures (e.g., supply circuit, multiple sources, AC and DC sources, etc), and shall be in compliance with all safety codes and standards applicable to the device and its intended use.

9.3 Documentation

Project documentation covers six basic areas as follows:

a) Design

b) Installation

c) Operation

d) Maintenance

e) Testing

f) Reliability

Documentation may be structured in an alternate fashion, but should still cover all six areas. The scope of work defines who provides the documentation provided in each area. The documentation is delivered per the project schedule.

The documentation may be supplied in printed or electronic files. In the latter case, the supplier should either identify or supply the supporting software used to prepare the files. To facilitate knowledge transfer, the designer/specifier should require that all documentation be provided using the designer/specifier's preferred software programs and versions. The designer/specifier should also secure the rights to copy and/or modify any and all documentation for internal use or by support organizations or third parties under defined circumstances. Style, format, and publication requirements are excluded from this standard.

Documentation represents knowledge transfer to the designer/specifier and as such should be subject to review or approval by the designer/specifier. In general, the final documentation reflects the actual equipment as accepted by the designer/specifier. The designer/specifier is responsible for recording all subsequent equipment changes as document revisions.

The following references are recommendations for abbreviations and symbols:

a) ANSI/ISO 5807 Information Processing—Documentation Symbols and Conventions for Data, Program and System Flowcharts, Program Network Charts and System Resources Charts [B2]

b) IEEE Std C37.2™, IEEE Standard Electrical Power System Device Function Numbers and Contact Designations [B11]

c) IEEE Std 91a/91, IEEE Standard for Graphic Symbols for Logic Functions [B12]

d) IEEE Std 280™, IEEE Standard Letter Symbols for Quantities Used in Electrical Science and Electrical Engineering [B13]

e) IEEE Std 315™, IEEE Graphic Symbols for Electrical and Electronics Diagrams [B14]

Content requirements, including suggested practices, for each type of document are defined in subsequent subclauses.

9.3.1 Design

Design documents describe the system design and the implementation of that design. These usually take the form of detailed drawings, configuration files, spreadsheets, calculations, settings files, configuration files, and may also include a design manual.

Fundamental design drawings include block diagrams, panel elevations, schematics, and wiring diagrams. Block diagrams describe overall system architecture, including control and data acquisition equipment and external equipment. Panel elevations, schematics, and wiring drawings should be provided as they further refine the details of the block diagram, but all may not be required. Panel elevations show how equipment is installed in the panels, racks, cubicles, or enclosures. Schematics show the relevant external connections to other system components. Wiring drawings show the specific details of the point-to-point connections defined in the schematics.

The overall system may contain devices from several different vendors that use different software or methods of configuration. These device configuration or settings files should be included in the design documentation, as well as the software used to generate the files. When programmable parts such as PROMs, EPROMs, GALs, FPGAs, and similar components are provided, the designer/specifier should acquire the programming tools for these components as well as their final programs.

A design manual should also provide text, photographs, and illustrative material accompanying the design drawings, containing sufficient detail so that functional performance and design may be readily understood. For example, functional block diagrams and explanatory text are used to describe each major component contained in the system. Documentation for application software may include listings and/or logic diagrams with sufficient annotations and comments to make the software easily understood by the trained programmer. A document describing the communication process between system devices shall be provided (see IEEE Std 1379 for an example). Note that documenting device configuration may not be directly transferable to a standard format, which can increase the documentation costs and introduce design errors. For example, a program may not be capable of providing a configuration file that can be imported into a graphics program, so the logic diagram is manually transferred to the graphics program.

Design drawings and documentation may also be applied to the component level of devices. For example, a card that is added to a computer may need to be separately documented.

9.3.2 Installation

Installation documents include outline drawings, mounting requirement details, customer connection details, environmental requirements, size, weight, and any other information needed for installation, including the following:

a) Electrical power, data, control, and communications interface wiring procedures

b) Floor, rack and shelf mounting, drilling, and bolting methods necessary to secure the equipment

c) Safety precautions or guards

d) Grounding and bonding procedures

e) Clearances for access and ventilation

f) Testing and alignment methods

g) Weatherproofing, dust proofing, and other environmental procedures

h) Shipping splits required to accommodate any physical restrictions on placing equipment in its final location (i.e., assembled equipment distributed across several cabinets may be too wide for door openings, windows, elevator weight and size limits, etc; therefore, the equipment needs to be split into multiple segments whose dimensions and weights will fit the physical constraints)

i) Other procedures needed to properly install the equipment

9.3.3 Operation

Operation documents describe how various personnel will be able to operate the devices provided with the system. This includes a statement of the intended use of each device and the function it performs. Procedural instructions should be provided that state routine and emergency procedures, safety precautions, and quantitative and qualitative limits to be observed in the starting, running, stopping, switching, and shutting down of the device. The documentation should supply adequate illustrative material to identify and locate all control and indicating devices.

Whenever a user interface, such as a console, bench board, indicating/control panel, computer or printing device is involved, the operational documentation also details, in step-by-step fashion, the operational sequences required to use these human interface devices.

9.3.4 Maintenance

Many devices include self-diagnostics that limits the amount of required maintenance and allows repair work to be performed only when required. It is still important that maintenance documentation be provided for personnel of various skill levels, (e.g., electronic technician, relay technician, substation maintenance, substation engineer) that includes performance information, preventative maintenance, and corrective maintenance.

The designer/specifier is responsible for ensuring that the relevant environmental and operating conditions of the System satisfy the conditions described in the technical documentation of the System and its individual products. The customer is obligated to carry out preventive maintenance for service or exchange of repairable parts in accordance with the instructions of the manufacturer. The inspection and regular check of individual products and their inter-related function (e.g., protection—circuit breaker) will be necessary from time to time in accordance with the recommendations of the manufacturer or the customer's standards organization (IEEE, IEC, etc.). Corrective maintenance has to be carried out immediately after detection of defects.

9.3.4.1 Performance information

Performance information includes a condensed description of how each device operates and a block diagram illustrating each major assembly and software program in the configuration. The description also contains the operational sequence of major assemblies and programs using functional block diagrams. Detailed logic diagrams and flowcharts are normally also provided as necessary for troubleshooting analysis and field-repair actions.

If an IED uses a protocol as part of the overall system, then the protocol implementation should be provided such that the messaging can be understood. This information includes message sequences, including data and security formats for each type of message, in the condensed description and illustrated whenever such messages are used.

9.3.4.2 Preventive maintenance instructions

Many of the devices available today are self-diagnostic and require very limited preventative maintenance. However, where appropriate, instructions should be provided for all applicable visual examinations, software and hardware tests and diagnostic routines, and resultant adjustments necessary for periodic maintenance of the provided devices. Instructions on how to load and use any test diagnostic program or any test equipment required, is an integral part of these procedures. Preventative maintenance for batteries and other equipment should also be included as appropriate.

9.3.4.3 Corrective maintenance instructions

Guides for locating malfunctions down to the field-replaceable unit or field-repair level include adequate details for quickly and efficiently locating the cause of an equipment malfunction, and state the probable source(s) of trouble, the symptoms, probable cause, and instructions for correcting the malfunction. These guides usually explain how to use special diagnostic programs, tools, and test equipment. Cautions or warnings, to be observed to protect personnel and equipment, are also normally included. Corrective maintenance instructions need to include an explanation for the repair, adjustment, or replacement of all items. Maintenance documents normally include schematic diagrams of electrical, mechanical, and electronic circuits; parts location illustrations, or other methods of parts location information; and photographs, and exploded and sectional views giving details of mechanical assemblies as necessary to repair or replace equipment.

9.3.4.4 Parts information

Parts information includes the identification of each replaceable or field repairable module. Parts need to be identified on lists or drawings in sufficient detail for procurement of any repairable or replaceable part. These parts should be identified by their specific part numbers and have second source referencing whenever possible. Any equipment that cannot be economically repaired should be identified in the parts list of the maintenance instructions.

9.3.4.5 Expansion information

Expansion information includes the methods that can be used to expand the system, including the addition of new hardware components, assemblies and software programs or tables including descriptive text and illustrations.

9.3.5 Test plans, procedures, and reports

Test documentation normally consists of a system test plan, test procedures, and certified test reports. The test plan states what equipment configuration will be tested, when it will be tested, which tests will be run, and who will conduct and witness the tests. The test procedures should define the operating steps and expected results. The test report records all test results.

The test plan should also provide for tests specified by the designer/specifier, which address user specific concerns.

Test plans should include a reasonable period for unstructured testing by the designer/specifier (i.e., testing to determine “what happens when I do something unexpected”).

9.3.6 Reliability, maintainability, and availability data and calculations

If the designer/specifier chooses to monitor the reliability, maintainability, and availability parameters of the system and its components both operating and maintenance personnel need to collect information on failures and repairs for all devices. This data on operating performance is then periodically reviewed and/or provided to the supplier for subsequent analysis and reporting of system reliability, availability, and maintainability.

9.4 Quality assurance

Quality assurance is a common task of the system integrator/manufacturer and designer/specifier. If two or more parties are involved then the responsibilities of each party needs to be defined in the scope of work.

9.4.1 Quality system

The stages of quality assurance are a responsibility of the manufacturer and system integrator. The designer/specifier may require the system integrator/manufacturer be ISO 9001 [B23] certified. The scope of the quality assurance program should be agreed upon by all parties prior to the start of work.

9.4.2 Test responsibilities

All IEDs have to pass device specific routine tests defined by the manufacturer to ensure quality before the products are released for production and delivery. The manufacturer is responsible for the correct handling of type tests and system tests for individual products.

The designer/specifier may require specific verifications and approvals according to the designer/specifier's philosophy. These tests, along with who performs them, are negotiated between the manufacturer, system integrator, and the designer/specifier as defined in the scope of work.
For example, the system integrator should prepare and carry out these special investigations with individual products and the overall Automation System. Furthermore, the system integrator should prove the fulfillment of the technical requirements, including performance criteria as presented in the system specification. The system integrator should be responsible for ensuring that all functions are jointly tested by the representatives of the system integrator and the designer/specifier during the optional factory acceptance test (FAT) and the mandatory site acceptance test (SAT) with the specific configuration and parameter set provided by the designer/specifier. The successful finishing of the FAT (if required) is the precondition for the equipment delivery and further site acceptance test at the customer's premises. FAT and SAT, as well as their contents, are negotiated between the designer/specifier and system integrator/manufacturer.

9.4.3 Warranty and after sales service

After a system has been successfully delivered per the contractual agreements (successful SAT, beneficial uses, etc), the warranty begins in accordance with the agreed conditions for the following:

a) Hardware

b) Engineering

c) Software

Once the warranty period has ended, the system integrator/ manufacturer may provide the following:

— Spare parts for an agreed period

— Support in diagnosing failures, misoperation, poor system performance, etc.

— Mandatory provision of urgent information to the customers about malfunctions

— Correction of detected software errors and hardware defects

— Offer and installation of software updates

9.5 Diagnostics

The designer/specifier should consider requiring the development of diagnostic tools for the following:

a) Defining failure inside or outside the system

b) Localizing failure inside the system and to a particular device.

c) The diagnostic tools should be designed for remote operation, if appropriate

d) Diagnostic tools that can help in the maintenance of the system

9.6 Testing

Testing of the system follows the logical progression of how the system is put together, as follows:

a) Type test
b) Routine test
c) Conformance test
d) System test
e) Factory acceptance test
f) Site acceptance test

The scope and object of tests, the test procedures and the passing criteria shall be specified in the test documentation. All tests shall be performed in such a way that the results are reproducible, if required. Where possible, all tests should be witnessed by the designer/specifier and/or performed by an independent organization that is qualified for performing the tests. If not possible, the tests can be performed by a manufacturer provided that unbiased completion of the tests can be achieved through witnessed tests.

9.6.1 Type test

The "fitness for use" of any product is proven by a type test. The type test is performed using samples from the manufacturing process. The type test is the check of the product against the technical data, which are specified as follows:

a) Mechanical capability
b) Electromagnetic compatibility
c) Climatic influences
d) Functional correctness and completeness

The type test is carried out by the use of system tested software.

The type test is passed before regular production delivery can be started.

9.6.2 Routine test

The routine test consists of the following special hardware and functionality tests:

a) Burn in
b) Insulation test
c) Function test

The routine tests should be carried out for each product before leaving the manufacturer.

9.6.3 Conformance test

The conformance tests are performed on the communication channels of IEDs and include the check of the communication protocol in accordance with the standard or its parts. Any device supporting a "standard" protocol shall be certified by an organization that is approved to perform testing by the User Group associated with the protocol (i.e., the Modbus-IDA, the DNP Users Group, and UCA International Users Group). This testing is the only way to ensure that the product properly supports the protocol.

9.6.4 FAT and SAT

The FAT provides validation and verification from the point of view of the designer/specifier prior to system deployment at the substation. The FAT is optional. But when required, the scope and objective of the FAT shall be discussed and agreed between all parties involved prior to the start of testing. The FAT documentation shall include a scope and objective. The result of the FAT shall be documented and signed by all representatives witnessing the testing.

The FAT is completed on a system that is not installed at the substation, where it may not be possible to simulate actual installed conditions. The SAT is carried out on the completely installed equipment in the following individual steps:

a) Process—IED level

b) IED level—station control level

c) Station control level—system control center(s)

d) Process—system control center(s)

The stages are carried out according to a commissioning plan, which shall check all information exchanges, controls, and functions. The test procedure has to document the results of each step and confirms that the system can be placed into operation.

System tests that may be performed during the FAT and SAT are as follows:

— Functional test

— System performance tests

— Data acquisition performance

— Control performance

— User interface performance

— Computer and display performance

— Stability test

— Availability test

— Maintainability test

— Expandability test

The designer/specifier should detail which tests listed above or any additional tests are required at the FAT and SAT.

9.6.4.1 Functional test

Initial power-up and subsequent power-up of all system components should be compared against the vendor's normal startup sequence. Self-test failures are monitored and reported to the vendors for repair or replacement. Error logs or other error detection schemes are monitored to determine improper configuration or operation. The power-up test should be performed prior to and after device configuration to ensure that the configuration is retained by the device. Firmware versions should be compared against what versions are required by the system. During the power-up test it is also convenient to check device part numbers against the system bill of material to ensure that all system components that are to be tested are available.

A simple communication test checks whether all devices are communicating as required without significant errors and good communications are being reported as required. Removal of each device from the

communication network (IEDs, Ethernet switches, etc.) and stopping of I/O servers or other software applications providing communication links should also be performed to check that communication trouble is correctly being reported as required.

9.6.4.2 System performance tests

The performance of all critical parameters of the equipment [e.g., communication, IEDs, user interfaces, I/O processing, and central processing unit (CPU)] should be measured under various loading conditions or scenarios. This may be difficult to accomplish during the FAT when the whole system may not be connected and during the SAT when the substation is not placed in service. Loading conditions and scenarios can be difficult to simulate or calculate. If tested as early in a project as possible, system performance tests can identify system weaknesses with enough time to resolve problems in a timely manner. The loading scenarios should simulate the following as practical and applicable:

a) Normal activity—initial system

b) Heavy activity (disturbance loading defined by user)—initial system

c) Normal activity—fully expanded system

d) Heavy activity (disturbance loading defined by user)—fully expanded system

e) Communications failures or high noise conditions, such as high noise on an entire microwave system

The measurements for performance assume that all functions of the system have been individually verified by functional tests and that the total system is ready to be evaluated.

If actual system inputs are not available, they shall be simulated with special hardware or software. For a meaningful test, simulated system inputs can be used such as alarm contacts, power circuit breakers, analog inputs, transformers, current, and potential circuits, etc.

Operation sequences to be performed during tests shall be described in detail to provide a repeatable test scenario and a way to measure improvements in performance (e.g., for a SCADA master, five people requesting one-line diagrams and two people requesting menu displays simultaneously). Test steps should simulate typical operations.

Response performance shall be measured in seconds. All measurements shall be recorded for analysis after the tests.

9.6.4.3 Data acquisition performance

Data acquisition subsystem performance measures the following:

a) The time for a status change or analog change at the RTU to be displayed to the user at the master station and/or local user interface.

b) The time to query all RTUs or IEDs on a per-channel basis

A cyclic status point input of 2.1 times faster than the scan rate can be used to detect a missed scan due to overloading. The status input simulator should be connected to an input of one RTU. The alarm associated with the toggled input shall appear on the logger with a time tag of approximately twice the scan rate. A system overload causing an extension of the scan cycle is obvious from the printout because one or more status changes are missed.

9.6.4.4 Control performance

Control performance measures the elapsed time between a control request by a user at the master station or local user interface and the control output contact closure. When performed in the field with all system components installed, this test will provide more realistic measurements.

9.6.4.5 User interface performance

The user interface performance is a measure of the response time to satisfy user requests for information at the master station or local user interface at the substation. Display response time is the time from when a request is made until the result of the request is completed. Different classes of displays (one-line diagrams, alarm summaries, menus, tabular, etc.) may have different display response times due to the amount of data to be gathered and computations required before a display request can be completed.

9.6.4.6 Computer and disk performance

The performance measuring device should be a computer program temporarily added to the system to operate at the lowest priority. The objective of using a low-priority program is to measure what otherwise is unused or idle capacity.

The impact of various loads on idle capacity is the information that is to be obtained and analyzed. The program should accumulate time for central processor usage. In addition, it should print a time-tagged message every time it is called.

These measurements can help locate software bottlenecks and thus improve system performance.

9.6.4.6.1 Computer CPU and disk utilization

Measurement of computer CPU utilization gives the user an idea of how much spare CPU capacity remains in the system. Monitoring programs from the computer manufacturer, operating system supplier, or even third-party suppliers who specialize in this area can provide these programs to monitor CPU utilization.

Computer CPU utilization, disk spare capacity, and memory usage shall be measured and evaluated during performance tests under varied loading conditions.

9.6.4.6.2 Computer link response time

Computer to computer link response times should be measured and evaluated during performance tests under varied loading conditions.

9.6.4.6.3 LAN response time

LANs that connect application computers together should be measured and evaluated during performance tests under varied loading conditions.

9.6.4.6.4 Reconfiguration, power fail, and restart tests

On systems with redundant equipment, reconfiguration tests should be performed to confirm the ability to properly failover and to switch peripheral equipment to the primary system, the secondary system, or off-line (i.e., out-of-service).

Power fail tests measure the time to recover from a complete or partial power failure until the system is fully operational. Because normal maintenance procedures and equipment failure cause downtime, restart tests are to assure the system will recover in a timely manner. Downtime of the system or parts of the system should be measured during these tests to confirm the length of these outages that can be tolerated.

For some system components, like a SCADA master, the time required to load a system from mass storage and initiate operation (or startup) should be measured. This time should be less than the acceptable system outage time.

9.6.4.7 Stability test

A test to verify stability of the system over a continuous period should be conducted at the FAT. Typical duration of 100 h to 400 h shall suffice. The test shall include periods of unattended operation, operation under normal activity conditions, and operation under heavy activity conditions. All functions shall be operating with simulated inputs throughout the test.

9.6.4.8 Maintainability test

The designer/specifier should require a maintainability test to evaluate the design, documentation, training, and recommended spare parts. Tests to be witnessed should include the following on applicable system components:

a) System generation tests (measure time to complete, and amount of manual intervention required)

b) Database maintenance

   1) Adding an alarm point (time to make operational) should be demonstrated

   2) Deleting or changing text on an alarm point should be demonstrated

   3) Changing an analog scale factor should be demonstrated

c) Display maintenance

   1) A new one-line diagram should be added and linked to the database (a specific example in the specification should be provided)

   2) A line and power circuit breaker bay should be added to an existing one-line diagram including analogs, tags, etc.

d) Equipment maintenance

   1) A display device should be replaced

   2) A communications device (modem, Ethernet switch, etc.) should be replaced

   3) A component of a device should be replaced

9.6.4.9 Expandability tests

Expansion capability of a new system shall be analyzed and may be tested. For example:

a) I/O point expansion (both hardware and software changes required)

b) Master station expansion

   1) Peripherals, disk space, memory

   2) CPU capacity (percent utilization)

   3) User interface (CRT additions, mapboard point expansion)

   4) Database and display expansion

9.6.4.10 Availability test

An availability test should be run after the system is installed and placed in operation. An availability test takes place over a specified length of time during which the system shall operate correctly and reliably for at least a specified percentage of that time. The length of the test shall be sufficient to verify that the equipment can be expected to perform its intended functions reliably and correctly over its intended lifetime.

The availability test shall be run under conditions mutually agreeable to the designer/specifier and supplier. In general, the supplier shall be responsible for making the necessary repairs. Downtime should not include delays over which the supplier has no control.

Availability tests are typically performed over a period of thousands of hours. This is followed by analyzing the number and types of failures, and their effects on system operation. The test time should be selected so that the total number of device operating hours for each type of system-critical device is representative of the predicted MTBF for that device to obtain statistically significant failure data. Specific rules for accumulation of uptime, downtime, maintenance time, and administrative time shall be agreed upon before the test.

9.6.5 Test records

A record of all tests applied to the system and the results of that test should be maintained during all testing phases. Test records should include completed test documentation that includes the names of those applying and witnessing the tests. Should the test result in an unfavorable outcome, a careful description of the results should be attached to the test record. If the test is a repeat of a previous test, the previous test record should be available for the test persons to review before proceeding with the test.

Annex A

(informative)

SCADA master station functions

The master station is the focal point for SCADA, whose traditional use in electric grid operations has greatly expanded. The master station, in a traditional role, performs the supervisory control and data acquisition—along with display, logging, data processing, and archiving functions used mainly for operations. However, the advent of automation and the integration of SCADA into the enterprise-wide information network has ushered in an expanded role. SCADA is no longer an isolated electrical network management system. SCADA serves as a source of important operating data required for the effective management of the utility's business. The introduction of substation IEDs makes a large amount of data available to SCADA. In its expanded role, today's master station may serve as an information gateway to the utility enterprise.

A.1 Architecture

Modern SCADA systems use open architecture features that allow connectivity with other systems and products from a variety of vendors. To ensure openness, the SCADA master station should comply with international standards, such as POSIX and IEC60870-6. To be considered an open system, communications to the substations should also comply with standards such as IEC61850, IEC60870-5, or de-facto standards such as DNP3. Despite the fact that most vendors offer open systems, each vendor develops their own API. This API enables software modules to communicate with each other, by using common objects and data exchange mechanisms. The IEEE and the IEC are developing appropriate standards to ensure inter-operability at the API level.

There are two main physical system architectures for SCADA master stations—centralized and distributed. Which architecture is used depends upon the applications and availability objectives.

A.1.1 Centralized

In traditional systems, the common architectural configuration is a centralized one. Even today, in less complex applications and when cost may be an important consideration, a centralized architecture is an effective approach.

A centralized architecture is a common practice today for less complex applications such as electric distribution network monitoring and control. In a centralized configuration, all the applications are running on a single or redundant hardware platform, including the software that supports the operator displays. Having all the software applications resident on the same computer and running on one operating system makes the development of such a system easier and therefore less costly. The interface between the various software applications also becomes simpler since data exchange between applications is handled by the inter-process communications utility provided by the operating system. Hardware maintenance of a fewer number of computers is less costly.

A.1.2 Distributed

When complex applications require more extensive data processing and availability requirements, a distributed architecture is more appropriate. Distributed systems have many advantages over centralized systems. Since the data processing is shared by multiple servers on the network, the various servers require less processing power than a centralized system. In this way, the cost of the individual hardware platforms

can be reduced. It is also easier to upgrade or to add servers if additional processing power is required. In distributed systems, the failure of one server does not make the whole system inoperative.

There are many reasons for using a distributed architecture. One reason is using different operating systems for different applications: a real-time operating system (UNIX®, VMS) is used for data acquisition and processing while Microsoft Windows is used for a graphical user interface.

Another reason for a distributed architecture is the need to distribute the applications to achieve performance and availability objectives. The most common form of distributed systems shares the load between the data acquisition functions and the user interface functions. In such configurations, the data acquisition and processing applications are resident on a server platform(s) that handle(s) all the communications functions with the substations and other systems as well as most of the data processing. The user interface functions are handled by clients that are connected to the servers via a network. In a more advanced version of a distributed system the applications software may also be running on multiple computing platforms. In such systems, it is important that some form of common information model be utilized to facilitate communications between the distributed applications.

A.2 Backup/emergency control centers

Today there is increased concern about potential damage to control centers as the result of a natural disaster or a terrorist act. In order to prevent the debilitating effect of such an event on system operations, many utilities install a backup master station that can take over system operations without major interruption. Such systems usually duplicate the functionality of the primary control center, although they may provide reduced capacity. The key issue in backup/emergency systems is the continuous synchronization of the backup system database to the primary database and the means to transfer the communications facilities to the field devices from the primary control center to the backup control center.

A.3 Primary and backup systems

Most control center applications are critical enough to warrant provisions for continuous system functioning when there is some form of hardware or software failure. This is normally achieved by providing redundancy for both hardware and software. There are several ways this can be achieved. The most common approach is to utilize a dedicated second or possibly multiple server platforms for dual or up to quad hot standby redundancy. In these configurations, one of the servers is in the active mode and it handles all the system functions while the other(s) are running, but not working online. The backup processor monitors the health of the active or primary system(s) and immediately assumes the primary role upon the failure of the primary system(s). A high-speed data connection between the systems ensures that the database is fully synchronized between the systems and there is no loss of data or functionality when the backup unit takes over.

A.4 Communications

Data exchange between substations and the SCADA master station offer the communication interconnections shown in Annex B and architectures discussed in Annex H. The major consideration with the master station is with the amount of data that can be brought back from the substations. Due to communication channel limitations, there may not be enough bandwidth to support the desired amount of data that is coming back from the substations to the control center. Communication channel analysis should be used as discussed in Annex B.

This section is intended to highlight the various communications interfaces required at a master station. Specific details of the communications requirements and protocol specifications can be found in Annex H.

A.4.1 Substation communications

The primary communications activity of a master station is the acquisition of data from substations. The master station communicates with IEDs such as RTUs, Data Concentrators, and Gateways. In most applications, additional IEDs (such as relays and meters) are connected to one of the other IEDs and do not communicate directly with the master station; however, there may be some IEDs that connect directly.

The performance of the substation communications physical media has a direct effect on the performance of the overall system. The speed and quality of the data acquisition is a primary requirement in the design of a SCADA system that takes into account the selection of the communications physical media. In rural areas where wide band communication facilities are not readily available, careful analysis of physical layer data transmission performance should be performed and protocol efficiency should be taken into consideration. Over the years many proprietary protocols have been developed by various vendors in order to provide the best communications performance in their particular system. A variety of standard protocols are discussed in Annex H.

A.4.2 Inter-control center communications

Control centers are frequently connected together for either synchronizing data used in grid operations or obtaining load data from distribution level systems. It is recommended that a standard protocol be used in order to ensure interoperability and minimize initial configuration effort. There are two recommended approaches as discussed in A.4.2.1 and A.4.2.2.

A.4.2.1 Inter-control center protocol (ICCP)

ICCP or IEC 60870-6 has been specifically developed to provide all the required bidirectional communications functionality for inter-control center communications.

A.4.2.2 Mailbox gateway (RTU)

In less stringent applications where the rich functionality of ICCP is not required, the mailbox approach may be a more cost-effective solution. In this application, the lower-level master is functioning as a slave to the higher-level master and utilizes a master/slave protocol such as DNP3. The higher-level master polls the other as a field device.

A.5 Measurements

Data can come from different sources such as RTUs and other control centers. Each element of information is composed of many data types that form an object. The objects define the format of the element, a quality descriptor, and if necessary, a time tag.

If the data includes a time tag, then only the data changes can be sent to the control center. If the object does not include a time tag, it is then meaningless to send all intermediate status. In this case, an IED should use a change flag to indicate that a state change has occurred and has not been reported since the previous report. Usually, the IED reports the current value of the input and a change flag associated to this input. The flag will be set when

a) An input has transitioned from state “1” to state “0” and returned to state “1” or beyond or

b) An input has transitioned from state “0” to state “1” and returned to state “0” or beyond or

c) An input has transitioned more than two (2) times since last reported

The objects described in A.5.1 through A.5.4 are the most commonly used.

A.5.1 Analog data

Analog values describe a physical quantity (i.e., voltage, current) that normally varies in a continuous manner. The information content of an analog signal is expressed by the value of magnitude of some signal characteristics such as amplitude, phase angle, frequency, etc.

A.5.2 Status data

A.5.2.1 Single-point information (SPI)

This object is used to represent the state of digital inputs and is generally used for alarm status and circuit breaker status. This type of input receives single information, which is either true or false (information lacking). For instance, this object can be used to indicate if a circuit breaker is closed or open.

A.5.2.2 Double-point information (DPI)

This object is used to indicate the status of a device that has one of two steady statuses (i.e., a high-voltage circuit breaker position: tripped or closed). Two bits are used to signal the status for maximum security. In most cases, the input status bits are derived from the “a” and “b” contacts of the physical circuit breaker. Thus, 0/1 DPI status would correspond to an opened circuit breaker while 1/0 status would correspond to a closed circuit breaker. However, if device maneuvering is in progress, or if there is an anomaly, the status of both input bits is the same.

A.5.3 Accumulator data

Accumulators, counters, integrated totals, or pulse accumulators are used for energy transaction, breaker operation counts, etc. Pulses received on status inputs are counted. Usually, accumulator data is acquired by the master station on the hour or on the half-hour, but may also be reported upon demand.

A.5.4 SOE data

SOE data are used to analyze power system events. Each status change is transmitted to the master station with a time tag. Usually, the precision of the time tag is 1 millisecond. The IEDs in the substation should be synchronized to the same time reference in order to correlate events from each substation.

A.6 Bulk data transfer

Bulk data transfer may be use to download IED configuration or firmware to an IED. The communication protocol supported by the master station and IED may offer such capability.

A.7 Digital fault records

This information is used to analyze the behavior of the power system signal after a fault. Data transfer occurs similar to bulk data transfers. This analysis may confirm the correct operation of power system protection equipment.

This information is mainly used by the protection engineer.

A.8 Control

The SCADA master station issues control commands to the substations. These control commands are issued by the operators from any console on which the command has been authorized or by applications through the API.

Automation system messages that result in trip/close control action should be secured against inadvertent operation. This includes the requirement for an efficient message error detection system and a sufficiently robust message coding scheme to reduce the probability of control error to an acceptable level.

A.8.1 Binary outputs

Direct-operate commands are used when erroneous or inadvertent operations have minor or minimal effect on the operation of the power system. Direct operate commands can be used, for instance, for raise/lower actuation. The single message Direct Operate Method is more efficient and responsive than SBO since it requires fewer messages and therefore less communications bandwidth. It also eliminates the need for the operator to constantly re-select a device each time a control command is issued.

A.8.1.1 Single command

This object is used to control the status of an output contact. This contact will be closed when validated and then returns back to "open" (e.g., lower or raise control order).

A.8.1.2 Double command

This object is used to control the toggling of an external device, which may have one of two steady statuses (e.g., a high-voltage circuit breaker tripping/closing order). This type of output normally corresponds to a "0/0" contact pair and becomes validated either "1/0" or "0/1" depending on the toggling direction, and then returns to the normal "0/0" steady status.

A.8.2 Analog outputs

Analog outputs are also referred to as set points. They are utilized to send analog values to an IED and normally follow the same object format as the analog inputs. Typical use of the analog output is for generation control.

A.8.3 Select-before-operate

This type of command has a three-step sequence as follows:

a) Device selection

b) Operation selection

c) Operation execution

This method is used to minimize the possibility of inadvertent operation. SBO commands permit the operator to examine the requested action for security. When the operator selects a control point, an SBO sequence follows, that when satisfied, results in device operation. More information on SBO is contained in Annex D.

A.8.4 Jogging or raise/lower

Jogging refers to the incremental control performed by an operator at the master station. While automatic processes utilize incremental control, the term jogging refers to the action of an operator issuing repeated control execute commands to affect a process at the substation. Typical applications are the control of analog processes such as voltage regulation (tap changer) and generation.

During the control action the operator observes the change in the controlled value, such as the voltage in case of a regulator or megawatt output in case of a generator, and "jogs" the value by manually issuing repeated execute commands. Jogging can utilize either direct operate or SBO type of control, but most applications utilize SBO for added security.

When the point selection is made, an SBO sequence follows. Each subsequent execute triggers the timer again to keep the execute window open for the next command. The communications process scans the substation on a priority basis to acquire and display the controlled value to the operator in real time. The SBO configuration for the response time includes the response time of the controlled device in the substation. The output relays in the substation devices should be the momentary type for jogging control.

A.8.5 Tagging

Tags are used to provide information or warning to operator regarding restrictions or malfunctions of power system devices. The tagging application provides means for adding, modifying, removing and displaying the tags. Tags may be applied to individual network elements or voltage levels within a substation or to all the substations. The method of applying and removing tags should be spelled out in operating procedures that are outside the scope of this standard.

A.8.5.1 Information tags

Operating procedures for substations rely on an information notice system to convey important information to substation equipment operators. Examples of “information notices” include: an equipment function has been disabled, an equipment is out of service pending repair, an equipment function is out of normal and is to be returned to normal following a certain event in the future, etc. Information notices do not have the stature of safety notices. They cannot be confused with protective procedures. Most information “tags” include provisions for a message, a signature of the person writing the notice, and a date. They may also include referral to a person or authority for further information.

A.8.5.2 Safety or protective tags

Operating procedures for substations rely on a system to minimize worker safety risks associated with energized equipment. Many tasks in a substation can only be performed with the equipment de-energized and protected from sources of hazard e.g., electrical voltage, mechanical operation, and stored energy. Protective tags are used to identify devices that should not be remotely controlled.

A.9 User interface

A.9.1 Operator consoles

Most vendors provide an HMI based on X Window or Microsoft Windows. More recent systems are web based using Java. A full windowing environment offers the capability to concurrently display multiple windows of information. Today, such operator consoles are typically provided on PC platforms under a Microsoft Windows operating system running full graphics applications. Each console may have multiple flat screen monitors driven by the appropriate graphic card that allows operators to display multiple windows at full screen or stretch a large display over multiple monitors. The operator consoles typically provide the following functions.

A.9.2 Tabular displays

Tabular displays show listings of application data. For instance, a tabular display can list the substation RTUs and display their actual in/out of service status.

A.9.3 Graphs/trends

Trend displays graphically show the variation in time of power system data. The data to be trended can be selected by the operator.

A.9.4 World map

A world map is a two-dimensional graphical representation of the real world. Each point in a world map is defined by a pair of unique (X,Y) coordinates. The world map is divided into a set of planes referred to as layers. Each plane covers the complete 2-D area with the whole range of the unique world coordinates. Many layers can thus be defined; each one contains different representation of the power system. For example, level 1 shows the entire power system, level 2 the substation state, level 3 the summary state of the main feeders, etc.

A.9.5 Zooming/panning

Panning allows the operator to move the world map window to different positions over the entire world map.

The zooming function changes the magnification of the world map.

The de-cluttering function gives the ability to mask or unmask information while zooming. For instance, a country's map does not show streets and street names; while the city's map, which is another level of information, shows such details.

A.10 Large displays

A large display is intended to give an overview of the entire power system. It shows a simplified representation of the power system while preserving, as much as possible, the geographical orientation of the system. At a glance, the operators can identify conditions that require their actions and then perform the required operation from their consoles. There are several technologies available to provide large displays.

A.10.1 Mosaic tile mapboards

The mosaic type display boards are usually referred to as mapboards and have been the common technology in the past. Such a display board uses small mosaic tiles with the information etched or taped on the tiles for static type information. Indicators are used for dynamic information such as breaker status. A matrix of LEDs can also be inserted in the mimic board to offer animation capability. If a modification is needed, old tiles are replaced by new ones—a time-consuming activity. Mapboards are viewing-only devices and generally do not offer any facility for control.

A.10.2 Projection displays

Today, projected screen displays are commonly used in control centers. A projected screen display is nothing more than a big monitor. These types of displays are typically driven by PC-based controllers that are equipped with multi-headed graphics cards and appropriate software. The system software should prepare and send to the controller the pictures to be displayed. This type of mapboard requires much less effort when the electric network configuration is modified. A new picture is edited and propagated to the display. Depending on the desired display size, there are rear projection units or front projection units. Projection displays operate as large monitors and can be used to execute control in addition to viewing.

A.10.3 Plasma and LCD

LCD and plasma displays are just large monitors and usually utilized in multiple display configurations like the projection units above. Care should be exercised in the configuration of such displays since these projection units are large and they have a resolution limitation that determines the minimum displayable object size.

A.11 Reports

Reports are generated for record and short-term archiving purposes. The primary report used for operating purposes is the event log that lists each system event by device name and provides a time stamp of the occurrence. Other periodic or on demand reports can be defined by utilizing the systems reporting tools provided with the database.

A.12 Security

Security is another important design criteria. Since most of the computers have network communication capabilities, it is important to consider access security. It is also important to have the possibility of defining security categories for data access. Some of the data can be made available to the general public but some other data can have restricted access because of competitive issues or other security concerns.

A.12.1 Access authorization

Different levels of access can be defined for different groups of workers. For instance, operators should have complete access to display and control functions whereas the maintenance staff may only have restrictive access to display functions. Area of responsibility can also be defined. If an operator is responsible for one area of the power system he cannot operate equipment in another area of the power system.

A.12.2 Areas of responsibility (zoning)

Each user has some preferences on the way information is displayed on the screen. These preferences are stored in the user profile and each time a user logs into the system, the display will be adjusted according to the profile.

A.12.3 Logging

For security reasons, it is important to log each access to the master station. Each access should be recorded, including the name of the person accessing the system and logging time.

A.13 Data processing

The function of data processing is to perform data calculation, data combination, and special processing on data retrieved from IEDs and store the result in a database.

The analog values are first converted into engineering units. For each individual analog point, linear or non-linear conversion can be chosen.

The analog value can be compared against predefined limits, and if a limit is violated, an alarm is generated.

A dead-band can also be defined to avoid meaningless alarms when a value close to a limit value is subject to slight variations.

Integrated totals (counters, accumulators, etc.) are normally continuous counters and may not represent current values. In this case, they need a special process so that the last retrieved accumulator value is subtracted from the current reading. The result is stored in the database. At some point the integrated total will “roll over” (i.e., reach its maximum count and start over at zero) and this factor is included in the special process.

Status processing detects the existence of status changes and generates alarms accordingly. If an unauthorized (not commanded by the operator) change is detected, the state of the point is changed in the database and an alarm is generated.

If necessary, the operator can manually replace an analog value or status. This replaced value is stored in the database and used for calculation. During the time a value is manually replaced, it will not be updated with values received from the field.

Any analog or status values can be used in calculating other analog or status values. These calculated values are stored in the database and are processed in the same way as other values such as limit checking, alarming, logging, etc.

A.14 Performance

The most important criteria for SCADA system are availability, maintainability, performance, security, and expandability.

A.14.1 System availability

The availability of a system is measured in terms of the availability of system functions. Availability depends upon hardware and software reliability. Availability is given by Equation (2) in 8.3.

The reliability of the software can be ensured by proper design. Some techniques can be used to detect software malfunctions. For instance, a supervisory software application can monitor each function and take remedial action if one of the functions does not work properly. “Watch Dog” timers can also be used to avoid the possibility that one function takes all computer resources due to a software problem.

Redundancy is also used to ensure high availability and continuous operation of the system. In modern SCADA systems, most of the computers are connected to a redundant LAN and if one computer fails, all communications will switch over the remaining computer. Most critical computers are doubled and if a hardware or software failure occurs, the other will take over the processing. Different redundancy topologies are used.

A.14.2 System maintainability

Maintainability is an important factor to system availability. The repair times following hardware or software failures can be minimized if the system provides good diagnostic tools. It should be possible to perform preventive maintenance, system debugging, corrections, updates, tests, and enhancement without affecting system performance.

A.14.3 System performance

System performance is a major criterion of a SCADA system. Desired response time should be determined for each function of the SCADA system. These response times should comply with power system operation and control procedures.

Response time is the length of time it takes from the instant a function is requested until the instant the outputs from this function are available. In a control center, the response time requirements may be divided into two broad categories corresponding to critical and non-critical functions.

Condition of operation should also be taken into account to specify system performance. A system is considered in **normal state** when the power system is in quasi-steady-state condition. Load and operating constraints are being satisfied. In this condition, the basic control system performances should always be met. A power system is in **emergency state** when the operating constraints are not completely satisfied. In this state, the amount of status changes and measurement variations can be very high. During emergency

mode, the operators' activities augment the computer load, causing an additional burden to the computer system. The response time is then slower, but this situation may be acceptable because the power system operator cannot deal with all the information at the same time. Most control systems are engineered to meet a specified "emergency" condition without degradation. If the actual situation exceeds the defined "emergency" condition the control system performance is allowed to degrade but still retain its basic functionality. For example, alarms and status changes should be correctly time-stamped; but the processing and actual display to the system operator may be slower than real-time.

Table A.1 shows typical quantities of information the computer system should process for different conditions of operation.

Table A.1—Conditions of operation

Event type	Normal state	Emergency state
Analog values variation	1 % of all analog values/5 s	40 % of all analog values/5 s
Status changes	1 change/5 s	15 % of all status indication/5 s
User request	1 request/min each workstation	1 request/15 s each workstation

A.14.4 Expandability

Expandability is the ease with which new points, functions, and/or equipment can be added to the system, and the amount of downtime required.

Expandability limitations may include, but are not restricted to the following:

a) Available physical space
b) Power supply capacity
c) Heat dissipation
d) Processor throughput and number of processors
e) Memory capacity of all types
f) Point limits of hardware, software, or protocol
g) Bus length, loading, and traffic
h) Limitations on routines, addresses, labels, or buffers
i) Unacceptable extension of scan times by increased data (given bit rate and protocol efficiency)

Annex B

(informative)

Master station/substation interconnection diagrams

This annex includes block diagrams of different master station and RTU connections.

B.1 Single master station

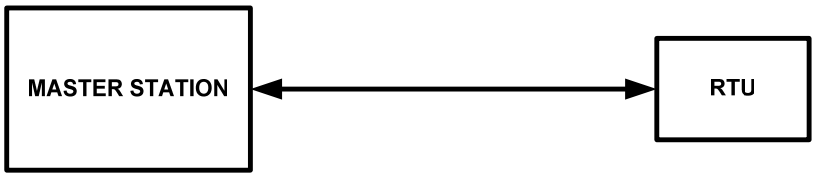

Figure B.1—Single master station, single RTU

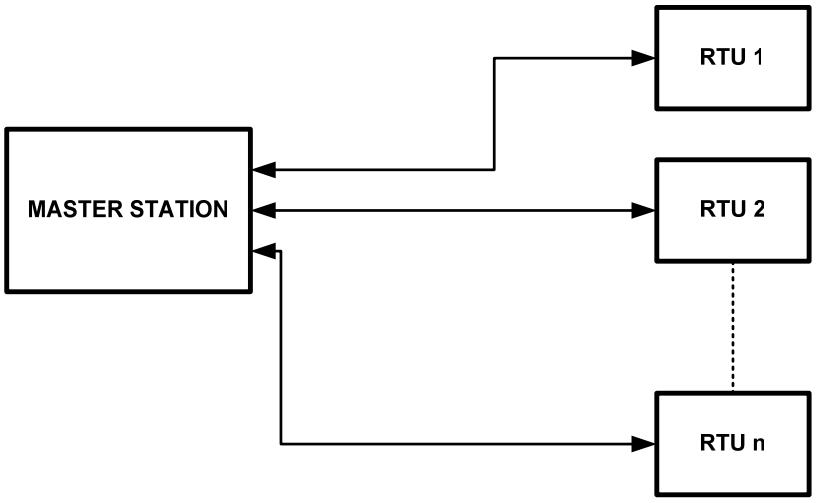

Figure B.2—Single master station, multiple RTU(s), radial circuit

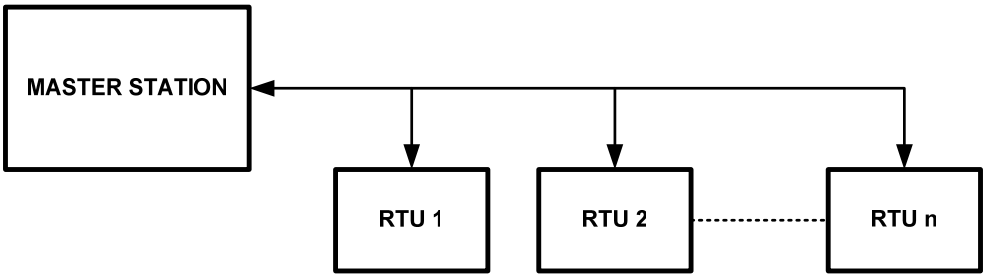

Figure B.3—Single master station, multiple RTU(s) multi-drop circuit

B.2 Multiple master stations

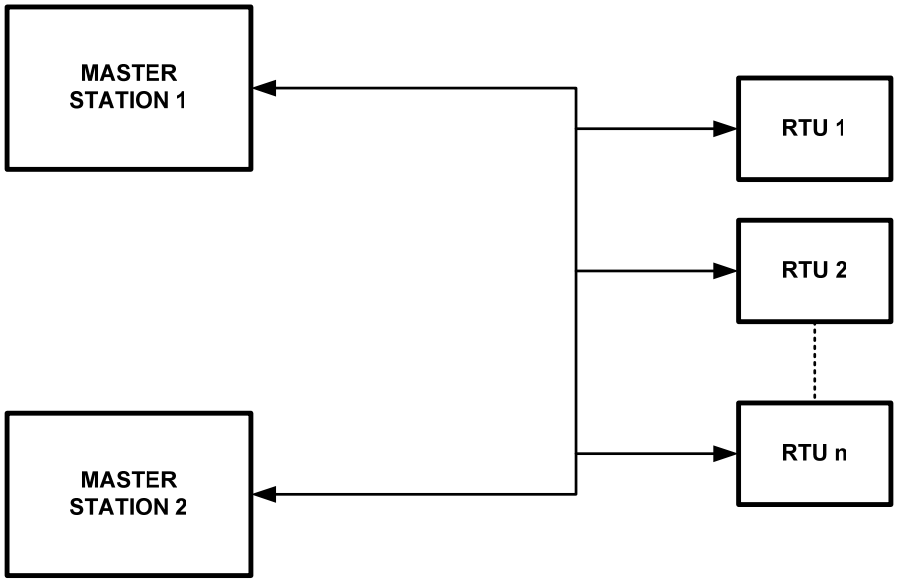

Figure B.4—Dual master stations, multiple RTU(s), multi-drop circuit

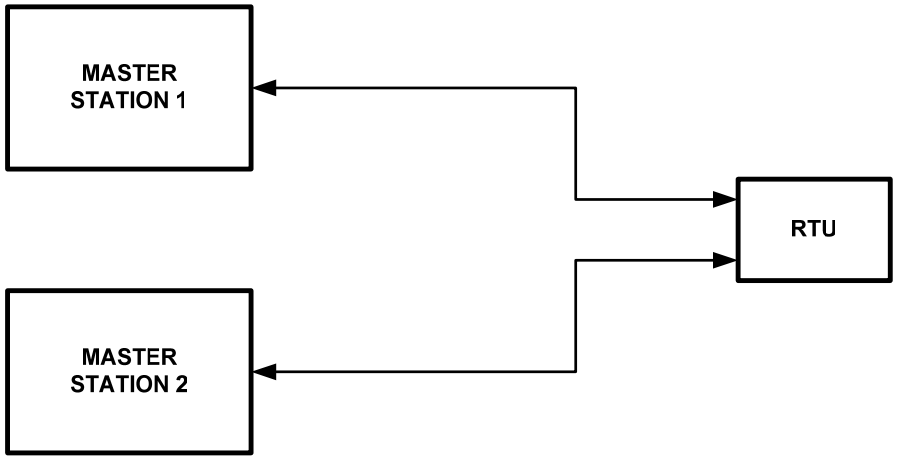

Figure B.5—Master station, single dual ported RTU, radial circuit

B.3 Multiple master stations, multiple RTU(s)

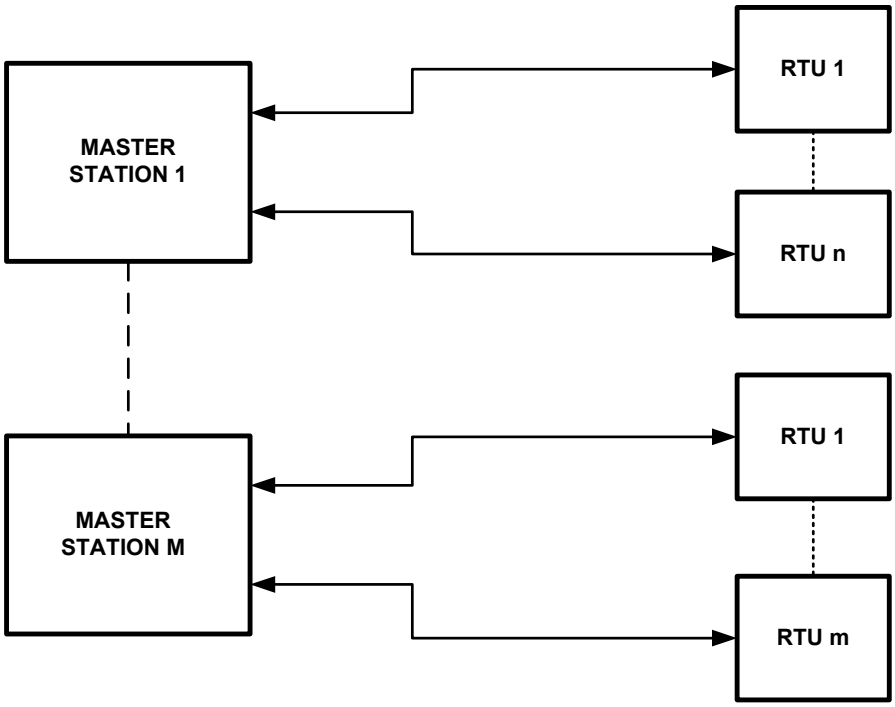

Figure B.6—Multiple master stations, multiple single ported RTU(s)

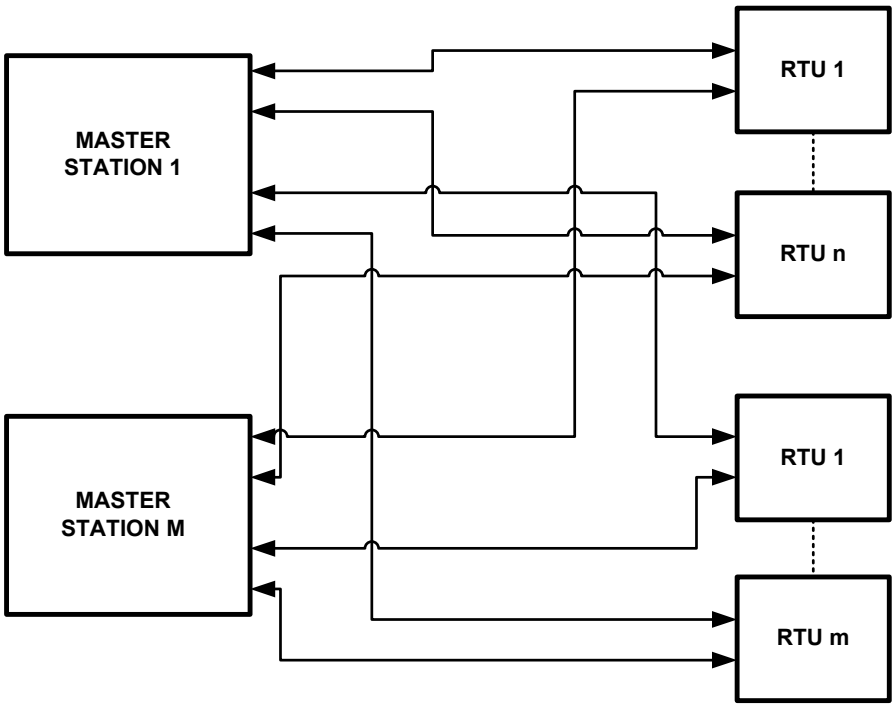

Figure B.7—Multiple master stations, multiple dual ported RTU(s)

B.4 Combination systems

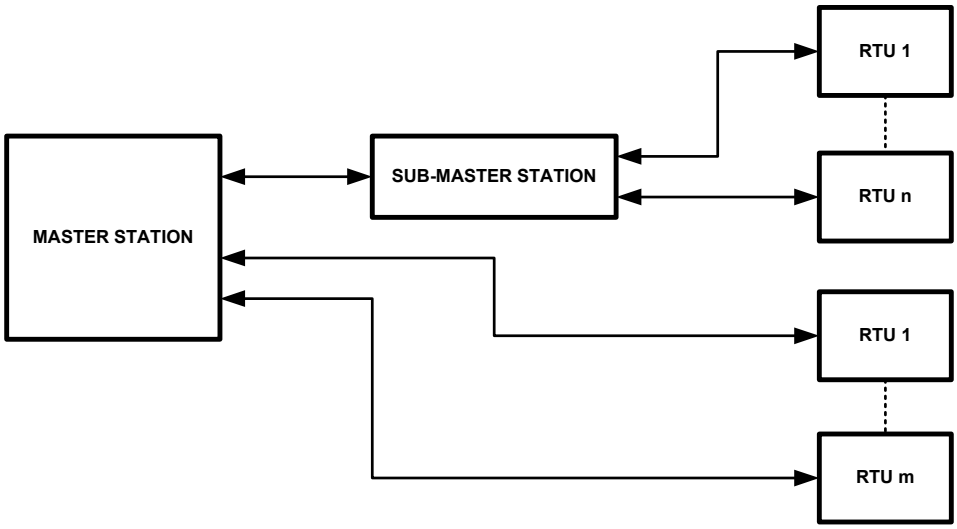

Figure B.8—Single master station, single sub-master station, multiple RTU(s)

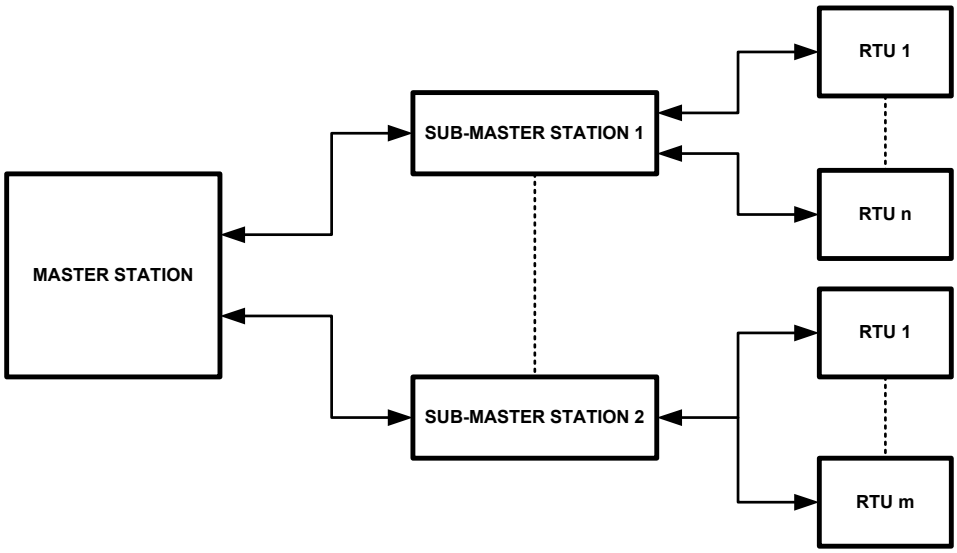

Figure B.9—Single master station, multiple sub-master stations, multiple RTU(s)

B.5 Substation gateway connections (legacy to standard protocols)

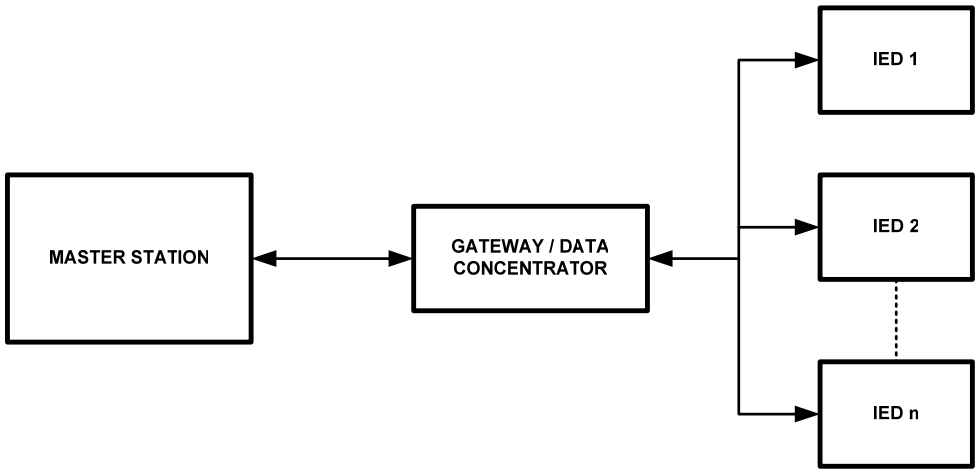

Figure B.10—Single master station, substation gateway/data concentrator

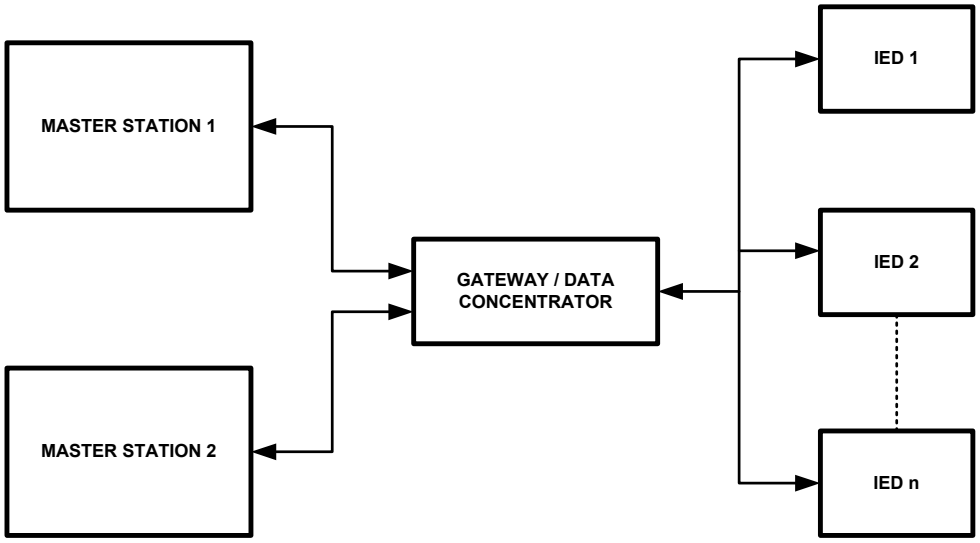

Figure B.11—Dual master station, substation gateway/data concentrator

B.6 Networked systems

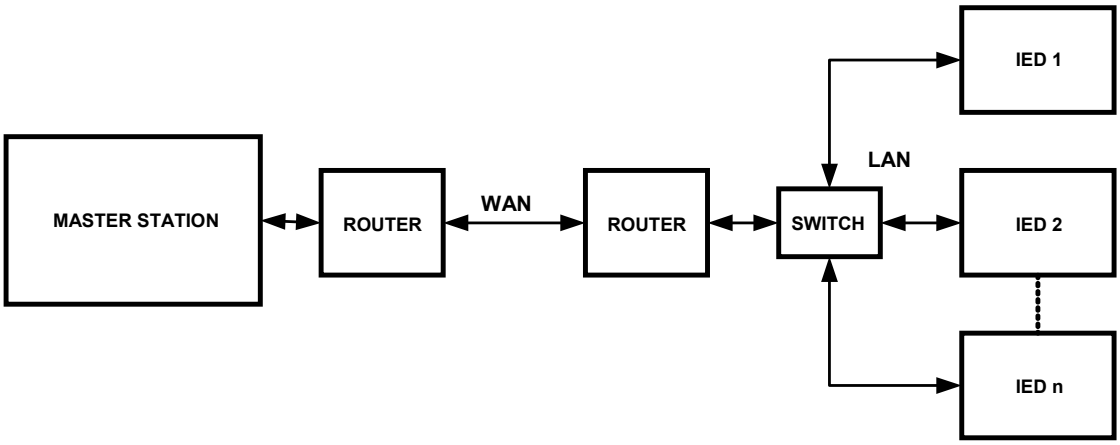

Figure B.12—Single master station, substation WAN/LAN connection via routers (Firewall not shown)

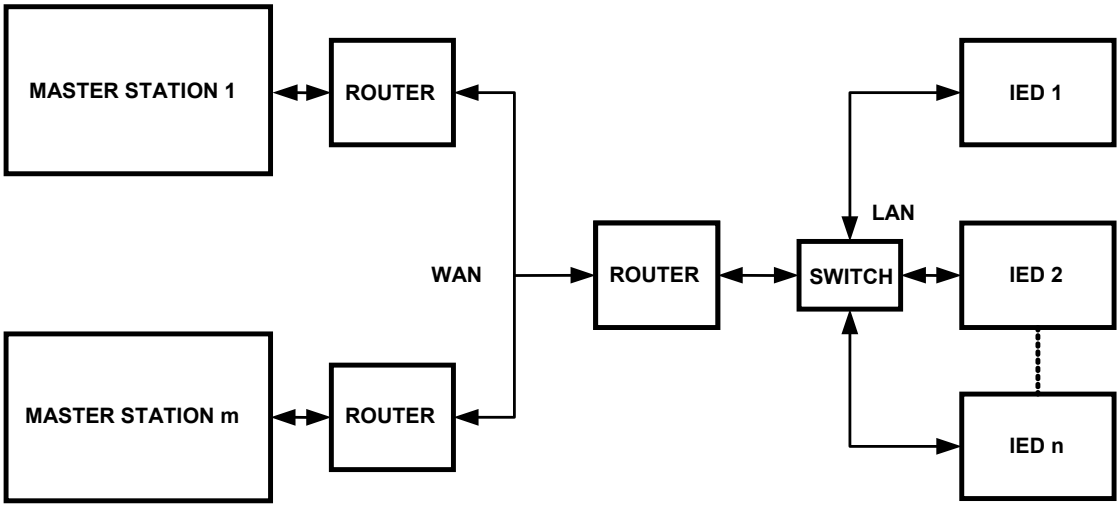

Figure B.13—Multiple master station, substation WAN/LAN connection via routers

Annex C

(informative)

Serial communication channel analysis

C.1 Introduction

The responsiveness of a SCADA system is limited primarily by the data throughput and latency characteristics of the data communication network that connects the master station to its RTUs (and any attached IEDs). It is therefore essential to be able to check that the network design will support acceptable system performances.

This annex describes a two-step procedure to identify any necessary changes either to the network design or to the SCADA system specifications. The procedure addresses only bandwidth and delivery-time issues in the communication network. All other network implementation issues such as connectivity, cost, security, reliability, maintainability and expandability are resolved separately. It applies to any network configuration where one or more RTUs are connected to one master station communication network port.

The required communication performances in terms of the SCADA system data volumes and required update times are document in C.2. Subclause C.3 verifies that the real or virtual data communication channel provided by the communication network between a master station and its connected RTUs can provide the required performances. Finally, C.4 provides an example of the application of this procedure.

C.2 Specify the performance of a master station to RTU communication channel

a) List all required types of master station "on-line" functions that involve data communication with an RTU (and any attached IEDs). These functions include the following:

   1) Remote control of RTU internal and external devices
   2) Reporting of measured and processed data values (status, analogs, counters, etc.) from RTUs and their local IEDs to the master station
   3) Transfer of analog output values from the master station to RTU and IED processors.

   NOTE—Transfers of configuration, event, or other files to and from the RTU and IED processors are considered to be "off-line" or "setup" functions that do not affect the performance of the system.

b) Specify the required repetition (update) interval for every on-line function that is to be executed periodically. Typical values are as follows:

   1) Two, 1,0 and 30 s for acquisition (upload) of measured values
   2) Thirty seconds for delivery (download) of generator automatic control data
   3) Fifteen, 30, and 60 min for upload of counter data (each transaction is typically preceded by a counter control function)
   4) Hourly and daily for transfers of processed data

c) Specify the maximum acceptable execution time limits (referred to as *T* below) for all on-line functions, both periodic and event-driven. Typical values are as follows:

   1) One second for any device control function
   2) One second for upload of any data transferred on demand (for example, status data acquired "by-exception")
   3) Less than 50% of the update interval for periodic functions (some functions may require a lower limit to provide sufficient time for master station processing between data updates)
   4) No specific limit for file transfers

d) List, for each connected RTU and any attached IEDs, the data size in bytes (information bytes exclusive of communication overheads) to be transferred in each update cycle of each periodic function. Allowances should be made for likely future expansions of these units.

C.3 Channel performance analysis procedure

a) Estimate (or measure) the typical time, T_C, required to execute a device control function. This time includes the operating times for all channel equipment while servicing all layers of the communication protocols used, in a channel that is ready, idle, and operating with no communication errors.

b) Check that T_C is much less than the limit value, T, specified in C.2.c).1) above. T is a fundamental network design parameter that limits the worst-case network transport delay. For example, the value of one second listed as typical for T inherently precludes routing any part of the network via a geosynchronous satellite.

c) If T_C exceeds about 25% (a recommended practical limit) of T, the communication subsystem design should be revised to reduce T_C or the specified value of T should be increased. Reducing T_C relative to T increases the channel time available for transfers of other data. Preferably, T_C should be less than about 20% of T. However, T cannot exceed the fraction specified in C.2.c).3) of the shortest periodic update interval specified in C.2.b).1).

d) To meet the limit value T for completing the execution of a device control function, the channel time required to execute any uninterruptible communication function should be less than ($T - T_C$). This time interval is typically too short to support the transfer of the largest files listed in C.2.d). Such files are therefore divided into multiple segments for delivery.

e) Estimate (or measure) the maximum file segment size that can be transferred in time ($T - T_C$) when the channel is open, idle, and error-free.

f) Calculate, from the entries in C.2.d) above, the number of data segments required to be transferred during each execution of each periodic function.

g) Calculate the total number of periodic data segments to be transferred, and thus the required total transfer time for routine data, during any 60-minute period of operation of the RTU communication channel.

h) Check that the total channel time required to transfer all periodic data is less than about 45 min, for a channel loading by routine data of less than a practical target value of about 75%. Unused channel time is then available for other, future, functions.

i) Check that the data transfer processes will meet the execution time requirements of C.2.c).

C.4 Illustrative example

The results of each step in the analysis procedure, when applied to a network servicing one large-capacity RTU, are as follows:

C.3.a) Result: The measured value of T_C is approximately 400 ms in the initial communication network configuration.

C.3.b) Result: The initial value of T_C is about 40% of T.

C.3.c) Result: As the initial value of T_C exceeds 25% of T, network changes were required to reduce data delivery times. These changes reduced the value of T_C to 180 ms.

C.3.d) Result: With T set at 1.0 s, the nominal value of ($T - T_C$) is 820 ms.

C.3.e) Result: The measured value of the maximum file segment size is about 0.2 kB.

C.3.f) Results for the example RTU:

Periodic function	Data segments
2-second measurements (1800 transfers/h):	1
10-second measurements (360 transfers/h):	2
30-second measurements (120 transfers/h):	1
30-second controls (120 operations/h):	1
15-minute counters (4 transfers/h):	1
60-minute processed data in (1 transfer/h):	30
60-minute processed data out (1 transfer/h):	10
24-hour processed data	0

C.3.g) Result: From item f), the total number of data segments to be transferred per hour is:
(1800 + 2 × 360 + 120 + 120 + 4 + 30 + 10), i.e., 2804.

C.3.h) Result: Assuming a convenient data segment transfer rate of one/second, the total channel time required per hour is 2804 s, or nearly 47 min. This calculated channel time represents a channel loading for routine traffic of about 78%. This high value can be accepted as it includes sufficient time (180 msec.) for the execution of one device control function in every one-second interval. It also provides the maximum length of 820 msec for the transfer of every file segment although most will be shorter. In addition, there are 796 (3600 – 2804) unused one-second time slots available during each hour for future functions.

C.3.i) Result: Assuming, for simplicity, that the time required to execute one device control function (180 msec) is reserved in each one-second time slot, then:

The time required to upload any short data file on demand is available in each of the majority of one-second time slots that are not pre-empted by device controls.

Transfers of all two-second measurements can be completed in the first 820 msec of each time slot, i.e., in 41% of their update interval.

Transfers of all 10-second measurements can be completed in 3.82 s, i.e., in 38% of their update interval.

Transfers of all 30-second measurements can be completed in 5.82 s, i.e., in 19% of their update interval.

Transfers of all 30-second generator control commands can be completed in 7.82 s, i.e., in 26% of their update interval.

Transfers of all 15-minute counter data can be completed in 10 s, i.e., in about 1% of their update interval.

Transfers of all 60-minute data can be completed in 400 s, i.e., about 11% of their update interval.

These results show acceptable performance of the example RTU and network configuration.

Annex D

(informative)

Control applications

D.1 Select before operate

A generic SBO requirement may yield uncertain results that may not be immediately discovered and resolved. The designer/specifier should provide the exact implementation of SBO that is required.

SBO is a method to minimize the possibility of inadvertent or incorrect control relay operation. SBO has been implemented in varying aspects of through-system checking and confirmation with the goal of minimizing the potential for operating more than one point, the incorrect point, or a point that is not ready to operate.

In the early days of remote control and SCADA, adopters of the technology wanted a method to assure themselves that a control operation request from the control center would result in the operation of the intended device at the remote location. The technique employed was called "select-before-operate," and was intended to provide a hardware feedback of confirmation that the proper device was about to be operated.

In "one-on-one" systems (precursor to modern SCADA), the control center personnel actuated a "SELECT" pushbutton—in the control room—of the device to be operated. At the device end, one half of the operator coil in the substation was energized by this action. The energizing of the coil half provided an electrical feedback to illuminate the "selected" light on the control panel for that particular control point. Having received confirmation that the correct relay had been selected, the control center personnel then completed the sequence by pushing the "OPERATE" button.

The first vintage of SCADA systems (pre-microprocessor) also followed this philosophy. A control operation required that the master station first send a "SELECT" command to the RTU. This command would energize one half of the RTU interposing relay coil, which would in turn provide an encoded message (generated completely by hardware) back to the master that the correct interposing relay had been energized. Upon receipt of the message, the master station would then send an "OPERATE" command which would complete the sequence. It is important to distinguish the SBO message sequence between the master and the remote hardware with the initiate/confirm sequence of the graphical user interface of the control center master station.

With the advent of microprocessors, byte-oriented communications with error detection, the modular and/or distributed architecture of RTUs, and the move away from direct-wired control systems, SBO as defined above has been made obsolete. In fact, the term SBO is a somewhat imprecise term that can include the following characteristics:

a) No control action can take place until a properly formatted select command is received by the RTU.

b) A select command is sent to the RTU to put the point into "selected" mode. The point stays in this mode until it receives a properly formatted operate command or a "SBO timer" expires. This timer is on the order of a few to several seconds depending on the communication delays.

c) Echo back of the SELECT command by the remote device without actually energizing an interposing relay coil (but only if the remote device accepts remote control (i.e., Local/Remote switch set to Remote).

d) Once the "Operate" command of the SBO sequence has been received by the RTU, it proceeds to operate the control relay as dictated by its control system (hardware and software).

e) The SCADA HMI may employ an initiate/confirm dialog which is separate from the SBO control action. The SBO sequence is generally configured in the communication front end with the specifics dictated by the protocol in use.

It is important to note that in any system architecture that does not employ direct-wired feedback from the hardware, SBO as originally defined will not exist, since the messaging is passed between software applications rather than a hardware check. At most, an RTU can use the SBO command echoes to indicate errors such as incorrect or unavailable points, incompatible hardware, local/remote switch disable, or other warnings related to control point activation.

Utility culture is very difficult to change, and SBO has been specified for many years as a perceived mechanism of ensuring proper remote operation of devices. Ironically, the fact that SBO is not understood by many of those who specify its use actually increases the potential for SBO to create safety problems due to the fact that the actual security it provides may be inconsistent with the user's understanding and/or assumption of the function. If SBO is to be specified, the designer/specifier should clearly communicate his/her expectations of functionality for SBO.

Note that the above comments apply to RTUs that are directly connected (wired) to the trip and close circuits of an end device (i.e., a circuit breaker). If the RTU is instead connected to an IED, which in turn is connected to the trip and close circuits, the traditional SBO loop may not include those IED control circuits.

Within a substation, SBO may also be configured between the substation HMI and the IEDs controlling the end devices (i.e., circuit breakers). IEC 61850 includes the provision for SBO between an HMI and its substation IEDs via the substation Ethernet LAN.

D.2 Multi-coded control messaging

Some communications systems are too slow to satisfy the operator expectation of SBO to the end device and therefore the "select" may only include the communications hub that reaches out to the end device. In this case the communications hub may or may not use SBO methodology. For slow communications channels, a multi-coded control methodology may be employed to provide the required security.

D.2.1 Multiple coded messages

For slow or non-deterministic communications channels a multi-coded control messaging methodology may be employed to provide the required security. This method may also be applied where a large number of commands are issued in a short period of time such that waiting for the command echoes unduly slows the system. These control systems rely on complex control message coding to provide the security for switch and breaker controls. Using this method, a single message transfers the point identity and action required and that message is operated on when received in tact and error free. However, to ensure security, the message contains multiple copies of the point and command information, encoded in different forms. The entire message and all the copies are received error free before the message is executed. Some of the encoding variations include inverting the message character bits, reversing the order of the bits, and/or complimenting the message bits. Secure message error detection schemes, such as 16-bit cyclic redundancy check (CRC16), are also employed.

D.3 Direct operate

Some modern protocols may be sufficiently secure to meet the needs for direct operate control without the added security of SBO or multi-coding. The designer/specifier should ascertain conformance to this requirement.

Direct operate is a control methodology that uses a single message to initiate a control action by an automation system control device. The single message Direct operate method is more efficient and responsive than multiple message systems since it requires fewer messages and therefore less communications bandwidth. In order to minimize inadvertent operations, direct operate message schemes may use multiple selection codes, encoded in differing formats, within the message to reduce the sensitivity to single and multiple bit errors.

This includes the requirement for an efficient message error detection system and a sufficiently robust message coding scheme to reduce the probability of control error to an acceptable level.

D.3.1 Control disable

Control disable prevents the system from operating one or more control points, usually through a local/remote switch. This switch is normally operated by substation operating personnel who wish to ensure that device operation is prevented and is part of tagging procedures. While many control schemes have provisions for technicians to disable a control output during testing, such test switches are not to be confused with the local/remote switch function. While the design of a local/remote scheme may facilitate testing IEDs, the primary consideration is the safety of substation operating personnel and adherence to company tagging procedures.

D.4 Local/remote scheme examples

The following are examples of the more common local/remote schemes with a brief description of the features.

D.4.1 Control power cut-off

This scheme (shown in Figure D.1) uses a local/remote switch to cut-off power from all IED outputs that are used to operate the apparatus. Typically, the switch is located on or near the IED for all control points of the IED. This scheme facilitates tagging, but does not allow a specific apparatus to be put in local/remote without putting all control points in local/remote.

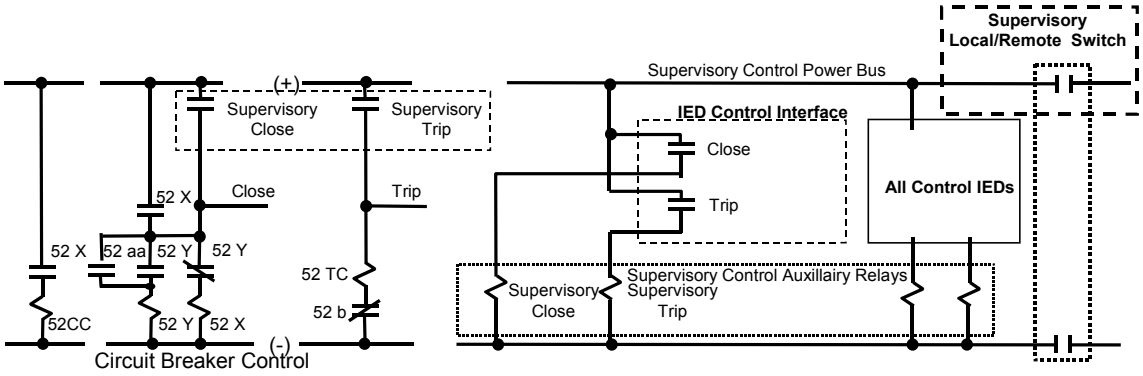

Figure D.1—Control power cutoff local remote switch interrupts power to all IED controls

D.4.2 Individual IED interface cut-off

This scheme (shown in Figure D.2) uses a local/remote switch to interrupt the output of the IED outputs used to operate the apparatus. Typically, the switch is located on or near the apparatus control panel. This scheme facilitates tagging and allows specific apparatus to be put in local/remote without putting all points in local/remote. However, the requirement of one switch for every piece of apparatus greatly increases material and installation costs.

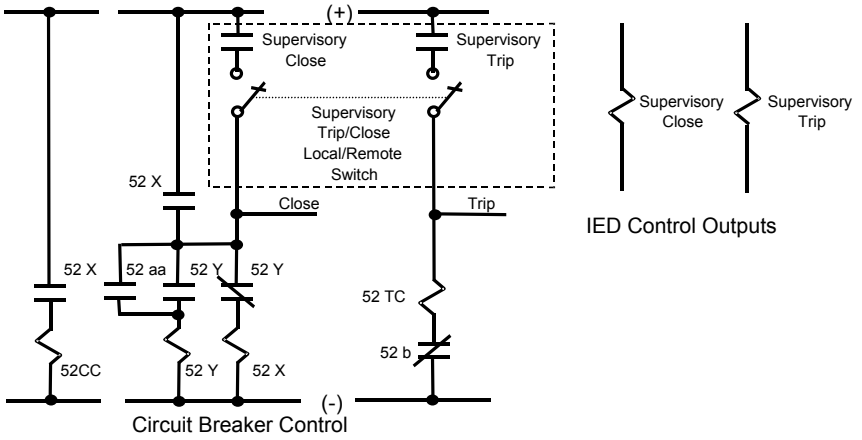

Figure D.2—Apparatus local/remote local remote switch interrupts individual IED control

D.4.3 IED interposing power cut-off

When IEDs do not have contact outputs rated for direct coil operation, interposing relays are utilized. In such cases, a local/remote switch can be installed to interrupt the coil power of the interposing relay. Typically, the switch is located on or near the IED, but may also be on the apparatus control panel if the interposing relays are located there as well. This scheme (shown in Figure D.3) has the advantage that the local/remote switch can be very small and inexpensive due to the low voltage and low current requirements of the interposing relay coil. One issue with this scheme is that the IED control function is disabled for all operations. Therefore, if the IED was also being used for non-SCADA applications (protective relaying, reclosing, etc.) this scheme will not work unless the IED has multiple output contacts for SCADA and non-SCADA applications.

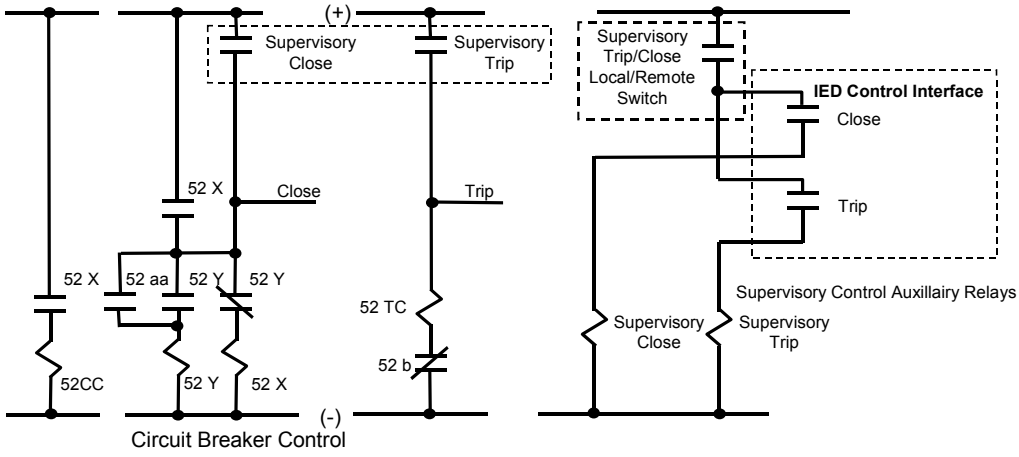

Figure D.3—IED interposing relay coil cutoff

D.4.4 IED logic input

This scheme (shown in Figure D.4) uses a local/remote switch to provide a digital input to the IED. This input is interpreted by the IED as a local/remote request and sets internal logic to prevent SCADA operation. Typically, the switch is located near the IED, but may also be on the apparatus control panel. Depending on the IED features, the local/remote logic can be set so that the non-SCADA applications can

still operate the contacts. In the case of a Data Concentrator, it is possible to employ an IED logic control input local/remote for any or all control outputs in the station connected to the Data Concentrator.

A potential disadvantage of this scheme is that it is internal to the IED. An IED failure or misoperation can result in the switch failing to accomplish its purpose. This failure may not be visible or apparent to the operator.

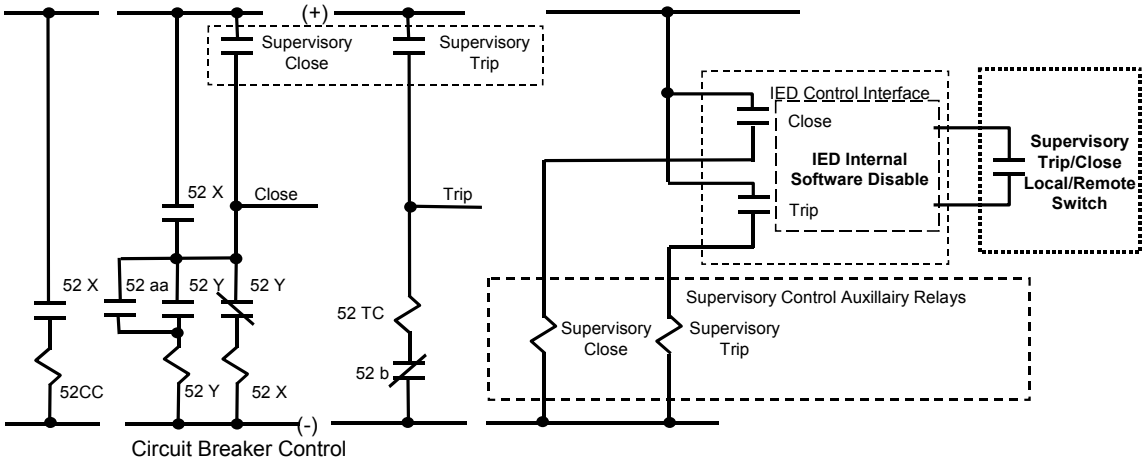

Figure D.4—IED logic input control disable

D.4.5 IED software control disable

This scheme uses a local/remote feature integral to the IED that is set in software, usually through a menu selection or keypad. This setting function sets internal logic to prevent control operation. Depending on the IED features, the local/remote logic can be set so that other applications can still operate the contacts. In the case of a Data Concentrator, it is possible to employ an IED logic control input local/remote for any or all control outputs in the station connected to the Data Concentrator. A drawback to this feature is that it can complicate physical tagging procedures. Also, other precautions should be taken if the local/remote state is lost during IED reset.

A potential disadvantage of this scheme is that it is internal to the IED. An IED failure or misoperation can result in the switch failing to accomplish its purpose. This failure may not be visible or apparent to the operator.

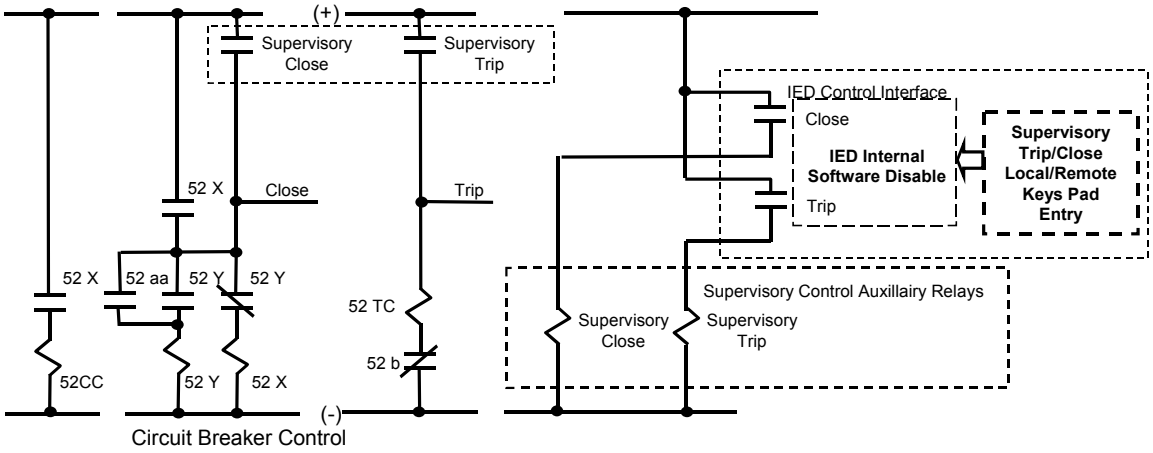

Figure D.5—Software input local/remote

D.5 Summary

It is not uncommon for a utility to actually employ a combination of local/remote schemes for safety reasons and to ensure the reliability of the local/remote feature. While older specifications frequently prohibited the use of software/logic to perform the local/remote function, the growing proliferation of sophisticated microprocessor relays has caused a re-evaluation of these prohibitions, and software/logic local/remote functionality is now being accepted. It is up to the designer/specifier to determine if the software/logic local/remote feature in the IED will satisfy safety, tagging, and operational requirements.

Utilities also find the changing environment a challenge to balance their long-standing "culture" with the realities of new equipment configuration and packaging. Some seemingly simple requirements can be difficult to meet, for example, finding a place to attach a "Do Not Operate" tag such that the tag interferes with operating the tagged device. Overcoming the "culture" issues can be more difficult than harnessing the new technology.

Annex E

(informative)

Database

This annex discusses the different types of databases in a system. Databases are collections of data organized such that a computer program can easily select desired pieces of data. Databases are generally organized by fields, records, and tables. A field is a single piece of information; a record is one complete set of fields; and a table is a collection of records.

Databases are usually categorized according to the data model that they represent: flat, hierarchical, network, relational, dimensional, nested, object, and proprietary.

E.1 Database characteristics

A database is a key component of the system. It is the repository and collector of data that feeds many utility processes. It is an interface between IEDs and users.

E.1.1 Database tools

A database is usually accessible with a standard set of software tools to access data from a database. A database management system is a collection of programs that enables a user to input, edit, organize, select, calculate on, and report data. In many instances, the terms database and database management system are interchangeable.

E.1.2 Storage media

Many different storage devices are available for databases. These include rotating hard disc drives and bulk "static" memories. Their significant characteristics include read/write access speeds and size per unit.

Environmental tolerance is often a key in selecting an appropriate storage media. The operating temperature range and environmental contamination in a substation environment often precludes rotating discs.

E.1.3 Size

The database is sized according to utility needs. Database size is estimated by determining the data sets that will be retained in the server, the number of elements in each data set, the periodicity with which the data sets will be captured and the length of time the data will be retained. This estimate should be considered a bare minimum-sizing requirement as it can be expected to expand in the future. Databases are typically sized 3 to 5 times larger than the initial estimate.

E.1.4 Expandability

The database is configured such that it can be easily expanded with readily available hardware and software. While many databases are implemented on hard disc drives that continually increase in size at diminishing cost per Mbyte, some implementations require static drives that are usually size limited. The designer/specifier should be careful to make expansion requirements very clear in the requirements documents.

E.1.5 Backup

Users should backup the database at regular intervals and before an upgrade. The interval should be based upon a strategy that assesses the consequence of lost data. Normally some data needs to be moved to a secure archive away from the substation site. The backup process can take many forms including: tapes, high-density removable disk, disk mirroring, CD-ROMs, and DVDs. Many utilities prefer the backup process occur without human presence or intervention in order to minimize visits to the substation. The database should be easy to restore such that excessive time and skill is not required to restore lost data.

E.1.6 Compression

Many data sets lose their detail requirements as the data ages. Data compression can reduce storage requirements while retaining key characteristics of the data. For example, feeder flow data can be reduced to retaining daily peak, average, and minimum values instead of the normal ten second or one minute data needed for operations. Retaining "demand" data for planning at slower intervals is often better than retaining snapshots of real-time data sets. There are several archiving and compression software packages that can be used for data compression. Some archiving packages are particularly good at recreating events from archive data.

E.1.7 Archiving

It is important to periodically check that archived data can be retrieved when needed. Technology changes and hardware obsolescence can quickly make data archives virtually useless. For example, consider those users who stored "valuable" information or references using 8.5-inch floppy discs. Today it is virtually impossible to find operational 8.5-inch floppy drives, even in the scrap yards. Unless the stored data was transferred to more modern media, for all practical purposes the data is lost forever. Important data should be reviewed at least every two to three years to ensure it is still important and is still recoverable. If it is still important, consideration should be given to making copies on the latest available hardware technology.

E.1.8 Maintenance tools

The database needs a set of maintenance tools. This includes tools to: create, expand, edit, modify, and remove data sets. Tools are also required to retrieve selected data and modify values. The tool set should also include tools to test and diagnose the database platform and its communications. The maintenance tools need to be easy to use specific to the skill level of those performing maintenance.

E.1.9 Access security

A database usually has some form of access control to manage users of the data. A well-defined security policy is needed to enforce access control. An administrator controls who has access to what sets of data. Often, there are multiple levels of access based on user need and position within the organization.

A database may hold multiple data sets in a partitioning arrangement to limit access. For example, data originating in protective relays may be partitioned from real-time data received from power quality monitors. Partitions coupled with a strong access security policy help to ensure that the data will not be used inappropriately or misinterpreted by users. Selected data items may be mapped in multiple partitions to satisfy the access strategy.

The database should have facilities to control user access that comply with operational security policy. Normally, a user name and password scheme is employed for access control. An administrator controls the access list(s). Access control should allow for multiple levels of access such that authority, granted by access control, enables users to view specific data sets and IEDs.

E.1.10 Connectivity

Databases usually have software database drivers so that application software can use a common API to retrieve the information stored in a database. One commonly used API for relational databases is Open Database Connectivity (ODBC). Users (or programs such as the API) request data from a relational database by sending the database a query written in Structured Query Language (SQL®). Some databases deliver data through web pages such that interaction with the database only requires a standard web browser.

E.2 System databases

Data is the result of measurements, calculations, and monitoring. Access to and distribution of this data may be the function of a database and database server. There are many places where data for the system may reside internally and externally to the substation:

a) IED database

b) Substation database

c) SCADA, EMS, or DMS database

d) Enterprise database

These different databases have characteristics discussed in E.1.

E.2.1 IED database

IEDs make measurements and monitor inputs from substation equipment as data for executing their respective functions. IEDs may also manipulate their data to calculate additional data, which are not direct measurements or conversions. These data are retained within the IED and made available through the communications capability of the IED. The IED data set is specific to each IED and its firmware version. The IED vendor provides the data definition.

E.2.1.1 Real-time values

The IED has a set of values that are updated every 0.1 s to 10.0 s. Multiple samplings may be made to develop an updated value, or the value may correspond to the most recent sampling. These are usually described as “real time” even though the values may be seconds old. As the IED updates the real-time data set, it replaces the previous values. These new values may be accessible via a display provided in the IED. The communication port(s) deliver the most recent set of real-time values on request or as programmed for automatic delivery (unsolicited reporting).

The IED database usually does not provide (directly or indirectly) for manual override of real-time database values in the event that measurements from the field have been determined to be invalid.

E.2.1.2 Calculated values

IEDs may have a set of values that are calculated from the real-time measurements. These calculated values are periodically updated based on the real-time update cycle. The calculated values may be accessible via a display provided in the IED. These values may also be accessible via the IED communication port(s). The IED will deliver the latest set of calculated values on request or as programmed for automatic delivery (unsolicited reporting).

E.2.1.3 Retained values

IEDs may retain a set of real-time and calculated values captured at a specific time. The time may be at a specified time, a programmed interval (e.g., every 5 min), or event triggered (e.g., device position change).

IEDs often provide the data set with a time tag based on its internal clock. The specific values retained and the number of entries retained is IED specific and may be programmable. IEDs have different strategies for dealing with over-flow of their retained value data set, including discarding the oldest values and ignoring the newest until the data set is retrieved and erased. The retained data set may be accessible via the IED display. The retained data set is usually accessible via the communication port(s) on request or as programmed for automatic delivery (unsolicited reporting).

The IED retained data set may be erased on request. It also may be retained with a continuous replacement of the oldest values with new ones (circular buffer). This characteristic may be programmable.

The IED retained data set may or may not be contained in a historical database.

E.2.1.4 Captured data sets

IEDs may have a set of values that differs from the real-time and calculated values and is retained based on an internal or external trigger. The specific data set and number of entries retained, as the result of a trigger event is IED specific and may be user programmable. The time spacing between value sampling may be user programmable and is IED specific. The trigger characteristics may also be user programmable. The captured data set usually includes a time stamp based on the IEDs internal clock. The number of captured data sets is IED specific and may be user programmable. Usually, the size of captured data sets and the number of sets retained are limited by memory; thus the user selects their characteristic and provides a mechanism to unload the captured data sets periodically to fully utilize this capability.

The IED captured data set may be erased on request. It also may be retained with a continuous replacement of the oldest values with new ones. This characteristic may be user programmable and is IED specific.

The captured data sets may be accessible via the IED display. The captured data sets are accessible via the communication port(s) on request or as programmed for automatic delivery (unsolicited reporting).

E.2.1.5 Data retention

IEDs may retain their data sets in either volatile or non-volatile memory or both. Data retained in volatile memory will be lost on a power cycle or software restart. Data stored in non-volatile memory is usually retained during a power cycle or software restart. However, there are many different memory technologies used in IEDs for non-volatile memory. Some may require periodic replacement of their backup power source or the memory module when the backup power is self-contained. In some IEDs, the location of data retention (volatile or non-volatile memory) is programmable.

E.2.1.6 Data access

IEDs usually only provide minimal access to data sets. Typically, access is protocol dependent. One set of data may be accessible via a standard protocol (such as Modbus or DNP3) and a different set of data may be accessible via an IED specific protocol.

The IED may support access control for some data sets and not others. IEDs often support access control with different passwords for different levels. Access control to data sets may not be programmable. Access control to data sets may require custom implementations of protocols that may not be supported by all vendor implementations of that specific protocol. Embedding passwords in protocol messages may pose security risks and problems.

E.2.2 Substation database

Within the substation there may be one or more databases. The substation database may acquire data from IEDs as a client and provide data to other systems as a server. The substation database may acquire all IED data or selected data sets depending on the distribution of functions within the substation and the communications architecture of the IEDs and client/servers within the substation. The substation database

may consist of multiple databases each with a specific purpose. For example, the substation database may retain a set of real-time values to feed a SCADA or EMS system and another set of values for a historical database accessible by enterprise users. Multiple databases may be configured with data sets to satisfy specific needs.

A substation database differs from a gateway or data concentrator in that a database provides more than protocol translations, mapping, and real-time data. A substation database retains data for use at some unspecified time.

E.2.2.1 Real-time database

The real-time database is characterized by fast access and processing. This database is usually proprietary because of performance requirements. It should be capable of handling large volumes of database updates that may be caused by a major event in the substation. In the worst case, every analog and data point can change "simultaneously" and all changes are processed, stored, and updated. "Simultaneous" is not difficult to visualize because every IED connected to the bus voltage (or line/feeder currents) can experience the voltage and current changes caused by a close-in fault or similar incident.

The substation database may provide (directly or indirectly) for manual override of real-time database values in the event that measurements from IEDs have been determined to be invalid. A "manually entered" value should be differentiated from values received from IEDs.

E.2.2.2 Historical database

The historical database is usually separate from the real-time database and can be slower since it is typically made up of samples based on change of status or percent change of analogs. Rapid changes can be stored up and processed into the database as time permits. Relational databases tend to not handle historical data very well, tremendously increasing in size and slowing data retrieval rates. Relational databases will often have real-time extensions to handle historical data. Proprietary databases usually provide smaller database size and shorter access times for historical data and the proprietary databases often have a standard ODBC interface to permit easy retrieval of data.

The historical database should have periodic copies of alarm limits and other items that do not change often. Usually, this is done as an initialization snapshot, then a periodic snapshot and on demand (when something in the limit tables changes.) The same approach can be applied to the message text and alarm text databases if common "fill-in-the-blanks" messaging and alarming is used.

The historical database should provide (directly or indirectly) for manual override of database values in the event that values have been determined invalid. A "manually entered" database value should be differentiated from actual values.

E.2.3 SCADA, EMS, or DMS database

The SCADA, EMS, or DMS database may be a subset of the real-time database, or may just be a table of values extracted from the real-time database upon request.

E.2.4 Enterprise database

Utilities often maintain a database for access by the enterprise. The intent of this database is to provide substation data to users throughout the enterprise without giving these users access to critical substation data or control functions. This database may reside in the substation or may be offsite at an enterprise location. The enterprise database may be a copy of the real-time database, updated on a slower frequency, and/or copies of the historical database or selected portions of both. To the user, the enterprise database is normally read only. The substation database periodically updates the enterprise database.

Some enterprise databases provide a restricted data set to users outside the enterprise. These are typically customers with a contractual obligation or other agreement with the utility.

E.3 Performance guidelines

The database has varied performance requirements based on the clients serviced by the database and the utility needs.

E.3.1 Server requirements

The database provides data to various users inside and outside the substation.

E.3.1.1 SCADA/EMS/DMS

Where the utility control center SCADA/EMS/DMS is supplied real-time data from the database, the database should respond similar to an RTU. Real-time data should be less than 1.0 s old. Responses to data requests should not require more than 5.0 ms from the receipt of request.

E.3.1.1.1 Control timing issues in SCADA/EMS/DMS

Many SCADA/EMS/DMS initiate a “demand” scan of the controlled point within a specified time after a control action has been commanded. This is to check that the control action was successfully executed. As soon as the status change of the controlled point is detected, another demand scan is issued for all status and analog points in a substation. This helps to prevent inconsistencies in data displayed to an operator, such as an indication of an open circuit breaker along with finite values of current and power flows. Likewise, in the other direction, it is not desirable to show an operator a closed circuit breaker with zero values for current and power flows.

A second control timing issue is the time delays that may be involved in retrieving status changes from an IED after a control action. If the time delay exceeds the SCADA/EMS/DMS control timeout period, the operator will receive two alarms. The first will be a ‘control failed’ alarm, indicating that the device did not change state, as it should have in the allowed time interval. Then, when the device change is reported, the “control in action” flag has been reset so the operator receives another alarm, indicating an “un-commanded change of state”. There are two solutions to this problem. One is to lengthen the control timeout period, which is undesirable because the operator waits longer to see if a command has been successful. The second is to ensure that the IED responds to status changes faster than the control timeout period.

E.3.1.1.2 Data timing issues in SCADA/EMS/DMS

An operator might see “false” indications if there are significant differences in the retrieval and transmission of status and analog changes. If there is an un-commanded status change, such as a circuit breaker tripping because of a fault, it is important that all relevant status and analog changes be transmitted to the master station as quickly as possible. Some IEDs may differentiate in the reporting of status and analog changes. This is the major cause of inconsistent data displays.

E.3.1.2 Local HMI

Where the database supplies data to a local HMI in the substation, the real-time data should not be more than 1.0 s old. Data requested to populate local displays should be provided in no more than 1.0 s.

E.3.1.3 Enterprise

Data provided to enterprise users should be provided in accordance with the utility expectation. Utilities should access their needs and data transport capability to provide realistic requirements for data access speeds.

E.3.1.4 Local control processes

The requirements for data supplied to local control processes are closely linked to the functions of the process. The database should support the local process at a rate that fits those requirements

E.3.2 Client requirements

The database is a client to the IEDs that supply data to the database. The communications architecture of the automation system determines the ways the database can acquire IED data and the speed for updating records.

E.3.2.1 Communications

The database may be configured to have multiple communication ports (serial and network) for acquiring IED data. See Annex H for more information on serial communication networks.

Annex F

(informative)

Interlocking

The system design may incorporate interlocks that constrain the operation of control devices or other IED and system functions. Typically, interlocks are specified and configured by the system user and implement a specific operating philosophy. The implementation of interlocks may be dispersed throughout the system or implemented in a specific control device, host, or IED. Interlocks may draw data from any source within the system and effect one or more functions of the system.

F.1 Logical or sequential interlocks

Interlocks that require equipment to be operated in particular sequence are implemented in a number of different devices in the automation system. Interlock logic can also be implemented in a protective device like a breaker monitor relay or reclosing relay. For example, a user may interlock the automatic closing of a circuit breaker with the state of its disconnect switches such that the breaker will not reclose unless its associated disconnects are closed. A PLC may be programmed to perform this task. That logic may rely entirely on the PLC inputs to represent the logical conditions to be met for operation and the PLC output then controls the reclosing device.

Implementers are cautioned to recognize the logical difference of input sensors. Sensors for open and closed should not be taken as simply the inverse of open or closed. Sensors should, as nearly as possible, represent the physical position of the equipment. Interlock logic should check for and resolve conflicts in the logic truths such that sensor states that represent the equipment in an ambiguous, e.g., neither fully open nor fully closed, both alarm and, if suitable, disable.

F.2 Distributed interlocks

In a fully distributed automation system, interlock logic may reside in any number of devices such that sensor input states are messaged to the interlock device and the result of the interlock logic messaged to the equipment controller. In the previous example, the state information of the disconnects may reside in a PLC and the interlock logic in a breaker controlling IED. The IED satisfies its logic requirements by data received from messaging with the PLC that enables or disables automatic reclosing.

The designer/specifier of such a system is cautioned to assess the reliability of the component devices as well as the messaging system. Care should be taken to assure the link between elements of this system are maintained and that a satisfactory state can be reached if the required sensor states are not available or corrupted. The results of altered linking may result in inoperability or catastrophic damage.

F.3 Measured parameter interlocks

An automation system may use measurements of system parameters to modify or enable control actions. These measurements may include voltage, current, real or reactive power flow, phase angle, and/or frequency. The interlocking device may measure these parameters directly or acquire the measurement from another device over a communications system.

The designer/specifier is cautioned to assure the measurement quality suits the action to be performed. Accuracy, resolution, stability, and time lag are all possible sources of performance problems. Likewise, the absence of a measurement or an invalid measurement is resolved within the interlock framework such that the result is satisfactory.

F.4 High speed interlocks

Some applications of interlock lock require high-speed response. The timing requirements of such an application should be assessed to assure the acquisition of input data and the subsequent logical result occur within the expected time frame. Logical alternatives need to be implemented to redirect the process if the timing or data become lost or invalid.

F.5 Operator override

Implementation of interlocks requires the user to recognize the possibility of missing or misleading data and program appropriate interlock logic to react accordingly. Often, an operator "override" is provided to permit intervention with interlocks. Users are advised to monitor the state of the interlock logic for reporting purposes such that they determine if an interlock has performed its intended function or it has failed due to an anomaly. Operator intervention to override an interlock should also be logged.

F.6 Testing interlocks

Once interlocks have been implemented it becomes important to assure the programmed logic meets the desired intent. The designer/specifier is advised to require a means to view and test the interlock logic. Testing is a major concern because being able to block specific messages may be a problem. Disconnecting the communication cable blocks all messages. There should be a way to selectively block specific messages during testing.

Annex G

(informative)

System support tools

This annex describes software elements related to error detection, diagnostics, and troubleshooting that the designer/specifier should include in the system HMI and/or substation computer.

G.1 System tools

There are many software applications that can be used for error detection, diagnostics, and troubleshooting the system:

a) Protocol analyzers
b) Vendor software applications
c) Manuals and documentation for system components, protocols, and IEDs
d) Help files for software applications

Vendor software applications are particularly helpful to maintenance personnel who need to easily view inputs and outputs from any part of the system. Many vendor software tools include the ability to force inputs/outputs, test inputs/outputs, and view raw input/output values.

Depending upon system architecture, the substation computer that normally runs the HMI application may have this software loaded on it. This approach may present issues with software version control, and a more centralized approach may be desired. A centralized approach may require a broadband or high-speed connection out of the substation to the centralized server so the application can be effectively run at a remote location.

G.2 HMI tools

In addition to IED vendor tools, the substation HMI, data concentrator, or RTU may have the capability for custom HMI displays that can help with error detection, diagnostics, and troubleshooting by collecting status and diagnostic data.

G.2.1 System components

Some system components that may be monitored are as follows:

a) Any hardware component for which a device status can be determined, such as
    1) Modems
    2) RTUs
    3) I/O modules
    4) Computers
    5) Printers
    6) Network interface devices (port servers, network switches, and routers, etc)
    7) Communication ports
    8) Other

b) Any software component (functional modules/calculations, applications, services, systems, and subsystems) for which an operating status and internal integrity (logic checks) can be determined (I/O server statistics, etc).

c) Any collection of hardware and software components that can be treated as a single logical device for which a composite device status can be determined:

   1) Communication links

   2) Database servers

   3) View nodes

   4) Master stations

   5) Other

G.2.2 Element tests

To enhance availability, a set of tests are built to determine if a system element is normally operating. The checks or tests fall into the following categories:

a) Collect, maintain, and report performance statistics for selected system components. Watch for degraded internal functions or errors that are likely to lead to serious problems in the future. (monitoring free memory, free CPU cycles, checking that an internal program or task is running on a periodic basis, etc.)

b) Check sensor inputs for analog and/or discrete quantities against the same quantities from another source.

c) Check that the communication link error rate is below some acceptable minimum value.

d) Check for incorrect combinations of status inputs. Incorrect means that they are in states that can never be obtained if the equipment is operating correctly. (A switch has both a normally open and normally closed status for switch position. These two inputs always report opposite of each other.)

G.2.3 Corrective actions

If an element is found to be malfunctioning corrective action may be taken based upon a predefined response, such as starting up a recovery program.

Predefined recovery responses can be as follows:

a) Do nothing.

b) Notify a person or process of the detected condition.

c) Reset or restart the device or software.

d) Switch to an alternate element.

When certain failures occur, the automation system may be able to perform some recovery action in order to restore system operation while alarming the failure event and even abnormal system reconfiguration. For example, redundant networks can be switched from primary to backup when errors are detected; communication drivers can be restarted when communications fail; and devices can be powered down and restarted by using smart power equipment.

G.2.4 Displays

HMI displays may be customized or standardized for some HMIs, RTUs, and data concentrators. Tabular displays are typical and are useful to see the sequence of events. Graphical displays can be useful to determine a root cause (a breaker is reported open because communication failed to an IED, etc). Some examples of displays are as follows:

a) Single element health with an option to view any additional data that comprises the element health. (Element status is normally comprised of hardware component status, memory status, and software status, etc).

b) Network status (port servers, hubs, switches, routers, etc).

c) Master station status including disk space, CPU utilization, RAID status, UPS status, etc.

d) System overall health that shows the health of all system elements in a block diagram.

e) Show performance statistics in addition to health of all system elements in a block diagram.

Annex H

(informative)

Communication fundamentals

The IEDs of an automated substation are tied together by communications internal to and external to the substation. Internal communication passes data and control messages between IEDs to form an integrated control system. The initial reason for extending communications beyond the substation was to provide basic SCADA access. External communications now also enable remote access to the substation IEDs by users throughout the enterprise. In addition, the large amounts of data and functions available from substation IEDs can be accessed from systems of many descriptions and purposes, all to the benefit of the enterprise. This section discusses communication fundamentals to help the designer/specifier understand both internal and external communications.

H.1 Basic communications technology

Communications can be simple point-to-point connections between IEDs or complex networks shared by many IEDs. They can be a mix of technologies, media, protocols, and access methods. The designer/specifier needs to determine the level of communication complexity that is suitable for the proposed system, the cost and complexity of the required communications, and the support requirements for all required communications. This subclause addresses the following basic communications technology:

a) Media
b) Signaling
c) Protocol

H.1.1 Media

IEDs are connected together using some kind of physical media as follows:

a) Copper
    1) Conductors or wires
    2) Coaxial cable
b) Wireless
    1) Radio
    2) Microwave
c) Optical fiber

All these media have special characteristics that make them useful for specific applications.

More than one media can be used to connect devices through the use of media converters that convert messaging signals from one media to another. Some messaging functionality may be media-dependent and may be compromised when crossing between media.

Internal substation communications share many of the same characteristics of external communications. However, the extended distance to reach the enterprise adds constraints such that some techniques suitable for internal communications may not be appropriate because of distances involved.

General media considerations are discussed in more detail in IEEE Std 1615, specifically in relationship to Ethernet.

H.1.2 Electrical characteristics

The electrical characteristic of the message scheme used over the media is important. There are many different methods to send and receive messages over a media as well as parameters to characterize the method. Methods and media that are compatible enable IEDs to communicate.

For example, the TIA-485-A standard specifies as its method a differential voltage polarity between a pair of wires to signify a logical "1" and "0". It also specifies loading on the interconnecting pairs and some other important characteristics. The standard, however, is method-only (it only specifies electrical characteristics).

Other standards may also include some communications requirements such as collision detection used in IEEE Std 802.3. All IEDs connected to a media segment share the same messaging characteristics. These characteristics can be changed only by using a media converter or similar device. In some cases, more than a media converter is needed when messaging techniques change. Here, a translator or a gateway performs the changes.

H.1.3 Protocol

Once IEDs have a common media and media electrical characteristics, there is a set of rules established that define how messages are structured and how they will be interchanged over the media. This is the function of a protocol. (The 26 letters of the alphabet, along with a group of punctuation marks, are the basic elements of written communications. The English language protocol specifies, in great detail, how these elements are to be combined to make up words, sentences, paragraphs, etc., that are required to communicate.) The protocol also implies the methods for packing message data in the form of bits, bytes, blocks, and packets.

These details make up the protocol definitions needed to communicate between devices. Just sharing bits and bytes will not allow devices to successfully communicate. Some situations may require multiple protocols to be run on the same physical media. This is a common situation with a substation LAN.

IEDs know what data values are in the message and where they are placed in the data stream. This is part of the protocol specification that is performed by the software that assembles and disassembles the message stream.

H.2 Proprietary and standards-based protocols and networks

A proprietary network consists of IED connected via some physical media (standard or proprietary) using a vendor specific proprietary protocol that will only interoperate with similar IEDs running the same protocol. Often proprietary protocol networks are intended to be "stand alone". There may be no need or desire for IEDs on these networks to interoperate with IEDs on other networks. A gateway IED is needed to connect a proprietary network to other portions of the substation network should such a connection be desired.

IEDs can typically communicate on a standard serial communications bus by virtue of sharing a common messaging protocol such as Modbus, Modbus Plus, and DNP3. There are a few other protocols that have been implemented by some users with the help of specific suppliers. These IEDs may be compatible but may not interoperate. Often one IED in the network can interoperate with all IEDs and serves as gateway.

IEDs that support Ethernet can be connected on the same Ethernet network even when different protocols are used. This is different from serial and proprietary networks, where all IEDs on the same network use

the same protocol. DNP3 and Modbus are two serial protocols that have network implementations that run on Ethernet networks. IEC 61850 is usually considered a protocol that runs on Ethernet networks.

H.3 Network physical topologies

Network topologies are either logical or physical. A logical topology is the way that data passes over a network from one IED to the next without regard to the physical IED interconnection. The physical topology of a network maps the IEDs of the network and the connections between them. There are two major groups of topologies: point-to-point and point-to-multipoint. Point-to-point connection only connects two IEDs together. Point-to-multipoint networks have several major network topologies for communications.

H.3.1 Point-to-point networks

A point-to-point connection is an individual communication channel between two IEDs. It is the simplest solution to provide data exchange between two IEDs.

Many IEDs may connect point-to-point to a multi-ported controller or data concentrator that serves as the substation automation system communications hub. In early implementations, these connections were simple EIA-RS-232 serial pathways similar to those between a computer and a modem. EIA-RS-232 is one of the first standards used to connect terminal devices to leased wire lines, where the telephone system supplied the interconnecting device—a modem. Figure H.1 illustrates a more modern EIA-RS-232 point-to-point connection.

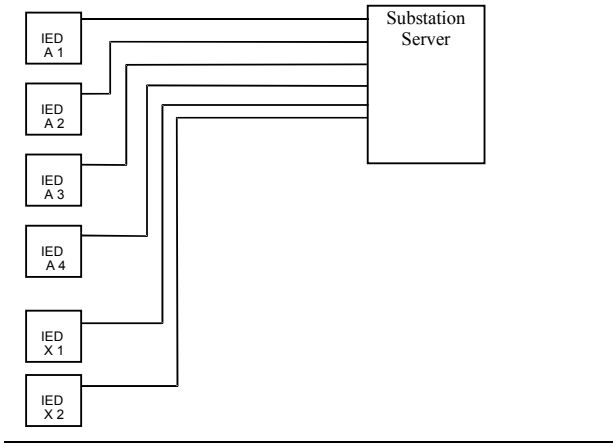

Figure H.1—Point-to-point IED to server connections

EIA-RS-232 does not support multiple IEDs, so IED addresses are not required (unless required by the protocol). When the media is copper, EIA-RS-232 is typically used for short distances, with a limitation of about 50 ft, depending upon the cable quality (capacitance) and baud rate. Cables with lower capacitance allow transmission over longer distances than cables with high capacitance. The longer a cable, the more the capacitance increases and the baud rate decreases. Eventually, the cable will be too long to function even at a very low baud rate. To extend the distance, fiber optic transceivers can be used or EIA-RS-232 to TIA-485-A converters or EIA-RS-232 to TIA-422 converters can be used. To electrically isolate EIA-RS-232 cables in a substation environment, the designer/specifier should use fiber optic transceivers to convert the electrical signal to optical and back again. Other options are to provide a device that provides optical isolation and surge suppression. Some IEDs support a serial EIA-RS-232 or TIA-485-A fiber optic port(s). When using fiber optic transceivers in IEDs, similar transceivers should be used at either end to ensure compatibility.

TIA-422 (formerly EIA-422 and RS-422) is similar to EIA-RS-232 (not addressable, point-to-point) except it is two pairs: one outbound and one inbound. TIA-422 is intended to allow longer distances (up to about 4000 ft, as opposed to EIA-RS-232 which is 50 ft).

H.3.2 Point-to-multipoint networks

Many substation control systems use point-to-multipoint IED connections. IEDs that share a common protocol can usually support the same communications pathway wherein they share the channel.

With a point-to-multipoint topology, many IEDs are connected together on the same physical media. This communication supports only one data exchange at a time and some protocol is needed to allow one IED at the time to use the communication media. In a multi-drop configuration, the master broadcasts a message that is received by all the devices connected to the media. The IED with the address responds and the master waits for the answer before polling the next IED.

H.3.2.1 Bus topology

A bus topology has each IED connected to the same physical media as shown in Figure H.2.

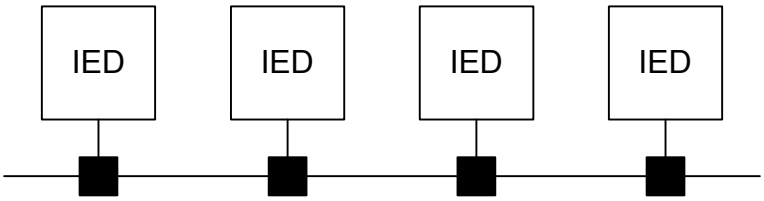

Figure H.2— Bus topology

Figure H.3 illustrates a TIA-485-A communications bus seen in a substation. TIA-485-A is the most common point-to-multipoint bus. It uses a twisted shielded pair copper cable. The TIA-485-A standard states to use termination resistors at both ends of the line that are equal to the characteristic impedance of the cable, typically 120 Ω for twisted shielded pair cable. Termination resistors may not be required for shorter cable runs and baud rates slower than 115kbps. Good TIA-485-A cables have a braided shield, nominal impedance of 120 Ω, and a capacitance of 12 to 16 picofarads per foot. Channel length is typically 4 000 feet maximum. TIA-485-A buses support up to 32 devices on the channel. Repeaters can be added to increase the number of IEDs by 32 devices and cable length by 4000 ft for each repeater. The longer the bus the more likely communications errors will occur because of reflection and noise on the cable. Generally, the longer the bus is the slower the baud rate is. TIA-485-A may run as fast as 1.0 Mbps although most operate closer to 19.2 kbps or slower. The TIA-485-A bus should be linear, end to end. Stubs or taps will cause reflections and communication trouble. TIA-485-A devices are wired in a “daisy chain” arrangement. The channel direction is turned around when each device takes control of the bus while transmitting.

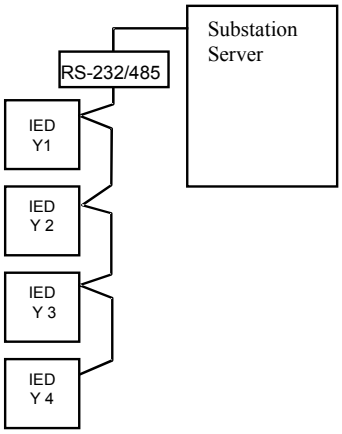

Figure H.3—TIA-485-A IED communications bus with converter

TIA-422 can also be used point-to-multipoint, but only one master is allowed.

Ethernet is typically a logical bus topology now that has a physical star topology.

H.3.2.2 Star topology

In a star topology such as Ethernet, each IED is connected to a special node at the center that can be passive, providing a path for the message to traverse, or active regenerating the electrical signal. Hubs simply repeat any message on all ports. More intelligent hubs are switches, which route a message to the port where the targeted IED is connected. The data exchange on each segment is isolated with full duplex and since separate optical fibers or twisted pair wires are used for data transmitted and received, collisions are avoided. This creates a situation where each IED appears to be on a single "virtual" LAN, so that collision and contention problems are minimized or eliminated.

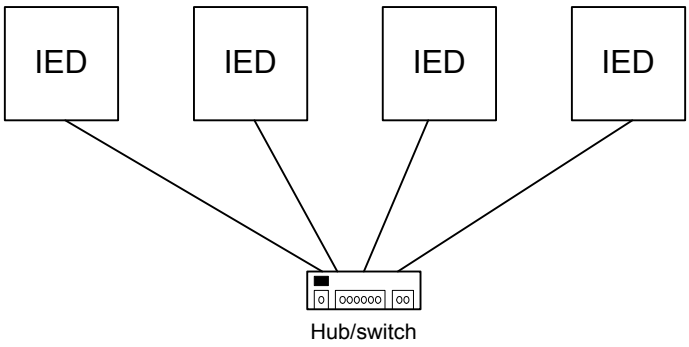

Figure H.4—Star topology

H.3.2.3 Ring topology

In a ring topology, each IED is connected to the next with the entire network forming a closed circle. Each IED is isolated from all, but two, IEDs. Ring networks are less efficient than star networks because data travel through more IEDs before reaching its destination. Ring networks are also less reliable because if one node on the network breaks down, the entire network breaks down because a full ring is required in

order to function. The token ring network is a logical ring topology because it runs on a physical star or bus network.

H.4 Communication relationship models

Network communications can take many different forms, modes, or models. Three of the most popular models are discussed in this section.

H.4.1 Master slave

Master slave communications is when the master controls all of the traffic on the channel. There are two different types of masters—dedicated master and token-passing masters.

Polling schemes involve no network contention because access to the medium is granted in an orderly fashion with every device taking its turn.

H.4.1.1 Centralized

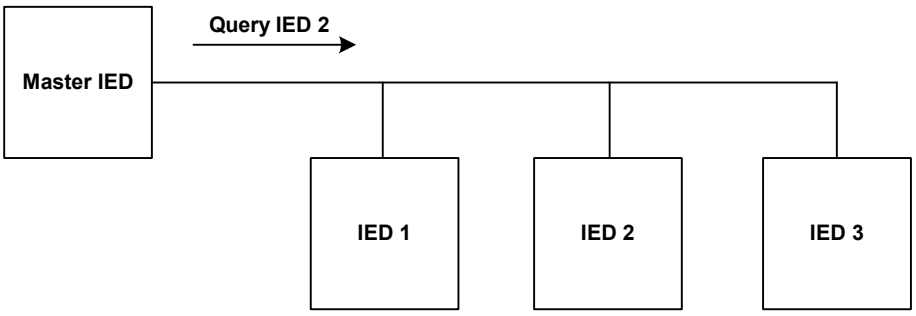

Figure H.5—Centralized polling

With centralized polling, all IEDs are addressable and the master IED will send out messages only addressed to a single slave. Each device has a different address as defined in the protocol being used. The master communicates to each IED one at a time so as to prevent communications collisions.

As shown in the Figure H.6, each IED listens for incoming messages and when it recognizes its address in the incoming message, it processes the information and sends back an answer to the master IED.

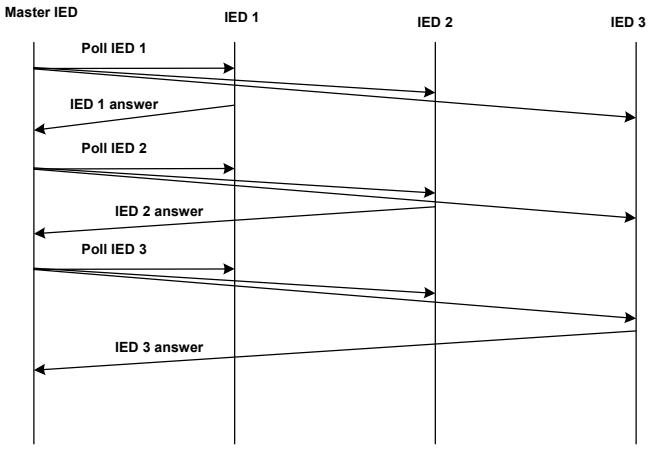

Figure H.6—Centralized polling scheme

H.4.1.2 Token passing

With token passing, each IED acts as a repeater of a message called a token and each IED can be both a master (requesting data from other IEDs) and a slave (sending requested data to other IEDs). The token may contain some data that is copied by the receiver. If the token contains no data, then an IED can use it and fill in its information contained in the token.

PLC communications and some other control systems use token passing schemes to give control to IEDs along the bus. A "token" is passed from IED to IED along the communications bus that gives the IED the authority to transmit messages. While the IED has the "token" it may transmit messages to any other IED on the bus. Different schemes control the amount of access time each "pass" allows. When the "token" is lost or an IED fails, the token is regenerated. Therefore, "token" schemes have a mechanism to recapture order. The most significant advantage of a "token passing" scheme is that it is deterministic. That is, every IED is guaranteed an opportunity to transmit data, and the total time to accumulate a specific amount of data from each device can be calculated. Applications that require timed responses or completion of control sequences will benefit from this determinism.

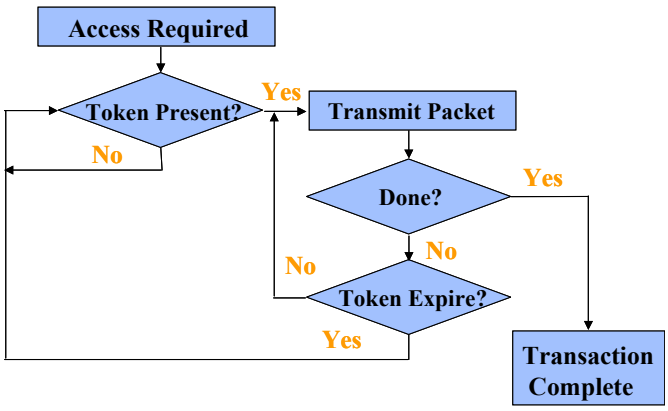

Figure H.7—Token ring access flowchart

H.4.2 Client-server model

This is the most popular model for network application. Each IED on the network is either a client and/or server.

The characteristics of a server are as follows:

- It is passive, similar to the slave in master slave communications
- It waits for requests from clients
- Upon receipt of requests, it processes them and then sends a response

The characteristics of a client are as follows:

- It is active, similar to the master in master slave communications
- It sends requests to servers
- It waits for and receives server replies

Master slave and client server communications are similar. The biggest difference is that generally there is only one master, whereas there can be multiple clients.

H.4.3 Peer-to-peer networks

There is a growing trend in IED communications to support peer-to-peer messaging. Here, each IED has equal access to the physical media and can message any other IED. Thus, each IED is both a client and a server. This is substantially different than master slave communications, even when multiple masters are supported. A peer-to-peer network provides a means to prevent message collisions, or to detect them and mitigate the collision. In this configuration, each IED can communicate to each other in an unsolicited manner.

H.5 Communications stack

Network technology has a set of common standards for defining communication details. They are common knowledge to the network professional but may be foreign to the utility power professional. The common framework for describing communications is the layered communications stack.

In the world of computer systems, the various functions are described as being layers in a stack that are needed to complete the interaction between computers. Normally there are seven layers described.

In the substation, to ensure data exchange between IEDs, a communication system topology is required along with a communication architecture that supports them. The communication architecture is composed of several communication protocols/standards that ensure that data is transmitted between IEDs. A set of protocols/standards are layered over each other, each layer offering a set of services to the layers above and below to enable data transmission from layer to layer. Data starts at the top of the stack and is transferred from layer to layer until it reaches the bottom of the stack, where the data is transferred over the physical media. Once the data is received, the data is again transferred from layer to layer, each layer adding its own information in the message. As shown in Figure H.8, some layers are responsible for data exchange between IEDs, while other layers are responsible for data exchange between application functions.

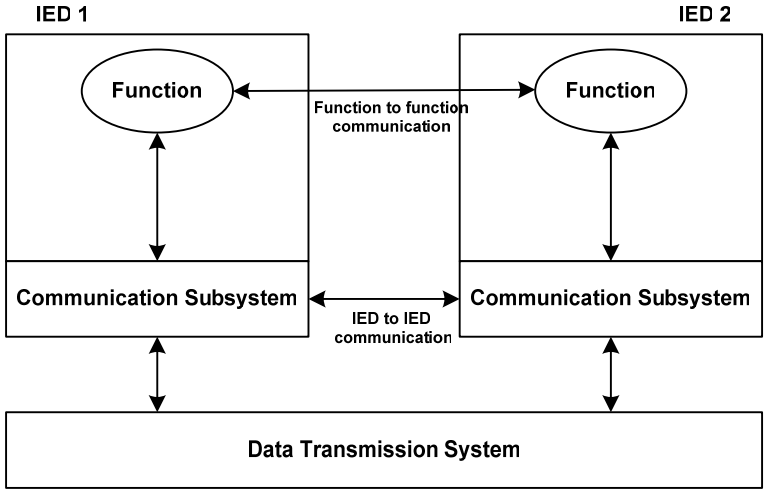

Figure H.8—IED-to-IED communication

A chosen set of protocols forms a stack, where a substation communication network will often use up to four layers. In the simplest implementation with a point-to-point communication, a two-layer stack can be used. More complex systems have additional layers in the stack.

Complex networks often use the Internet stack as shown in Figure H.9.

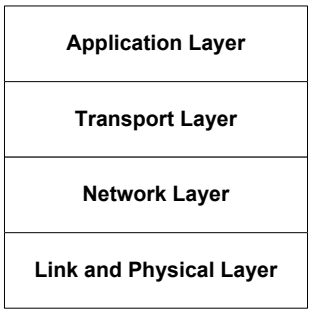

Figure H.9—Internet stack

The data link and physical layer control the transmission/reception of data in a suitable format for the communication media. The specification of the physical layer includes both mechanical and electrical characteristics. This layer also detects some types of errors and notifies the data link layer when such errors are detected. Some examples of physical layer standards are: EIA-RS-232-C, EIA-RS-422, and Ethernet for high-speed networks. The link is in charge of transmitting messages over the physical connection, detecting errors and, in some implementations, correcting some types of errors. It detects frame errors, controls the flow of data between IEDs, and ensures the correct sequence the received message.

The network layer routes messages between nodes that is transparent to the upper layers. The network layer ensures that the data will be transmitted from end-to-end over the network. The network layer also handles network addressing and congestion control.

The transport layer provides a network-independent message transfer facility. The transport layer provides for making connections between messaging partners when a messaging session is opened to connect partners or for transporting messages where a connection-less session is supported.

The application layer offers a set of services and data manipulation for substation automation. This is the segment that is specific to the data transfer and IEDs. This segment determines the inter-operability between IEDs. To be inter-operable, devices understand the specific application layer protocol carried by the network messaging protocols. Examples of utility specific protocols include: DNP3, Modbus, Modbus Plus, and IEC 61850.

Refer to IEEE Std 1615 for additional information on the Internet Protocol Suite communication stack. Refer to IEEE Std 1615 for an overview of the network implementations of IEC 60870-5, DNP3, and IEC 61850. Refer to IEEE Std 1379 for an overview of the serial implementations of IEC 60870-5 and DNP3.

H.6 Networks

Refer to IEEE Std 1615 for additional information on networks.

Networks permit passing messages between end-points over a wide range of distances and provides a messaging service that is independent of the message content. Any number of different media supports network messaging.

Network designers should carefully plan how substation devices connect to a substation network such that the network does not become a performance-limiting element for the system. Network design should also provide for retaining critical functions in the event of a network failure.

H.6.1 Wireless Area Network (WAN)

A WAN provides long-distance transmission of data, voice, image and video information over a large geographical area. A WAN can be owned by a utility or WAN services can be leased from telecommunication providers. WANs permit enterprise access to all nodes on the WAN. Normally, connections to a WAN are made through a router, bridge, or firewall to control access to distant nodes such as substations.

H.6.2 Local Area Network (LAN)

A LAN is normally designed for a limited geographical area, such as a utility substation or an office area. It is generally capable of transmitting data, voice, image and video information. In most cases, a LAN is considered to be an integral part of the facility, and is owned by the facility owner. In a substation, there may be one or more LANs to logically group devices and functions as well as control loading and security.

H.6.2.1 Sub-network

A LAN can be configured with devices and nodes that are shared but retain a degree of isolation from one another. The pieces of network are sub-networks. The devices and nodes could interchanges messages but by virtue of configuration they do not. In effect, the devices do not know of the existence of the other devices. Sub-networks reduce messaging traffic to devices that do not need to interoperate.

H.6.2.2 Segments

There are physical and logic limitations that constrain the size of a LAN. These are managed by defining LAN segments. A segment serves a small geographic area whose center is a device like a switch or router that passes messages within the segment members and to other segments. This limits messages passing the outside and compensates for the distance restriction imposed by the media. Network designers often establish LAN segments to logically group devices together. For example, in a substation one network segment may be configured for relays and another for meters. Or, one segment might be configured for primary relays and another for backup relays. Configuring segments is a technique to manage the risks of a LAN failure.

H.6.3 Messaging across multiple nodes

Network based communication may use a telecommunication system that can provide multiple communication paths between two IEDs as opposed to a simple common bus arrangement. As shown in Figure H.10, communication between A and B can be done through nodes C, D, or E. This provides a more robust pathway that is both fault and loading tolerant.

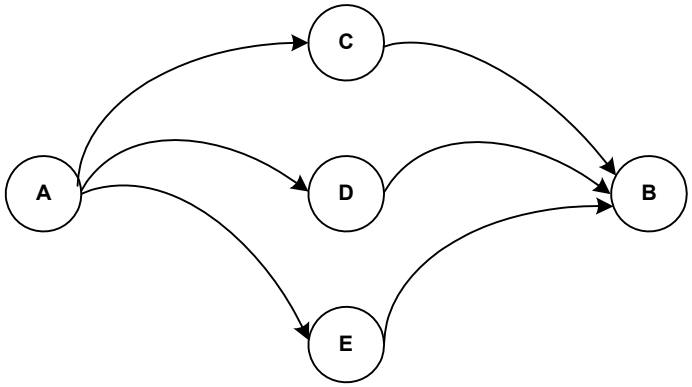

Figure H.10—Message routing between multiple nodes

To allow the data exchange between IEDs on a network, additional information is needed to route the data through the network. Each message contains addressing information used to help nodes to route the message to its destination.

A substation communications system may require many segments and links to make a complete physical media connection between all IEDs. The system may involve media conversion, protocol translation, gateways, and access devices.

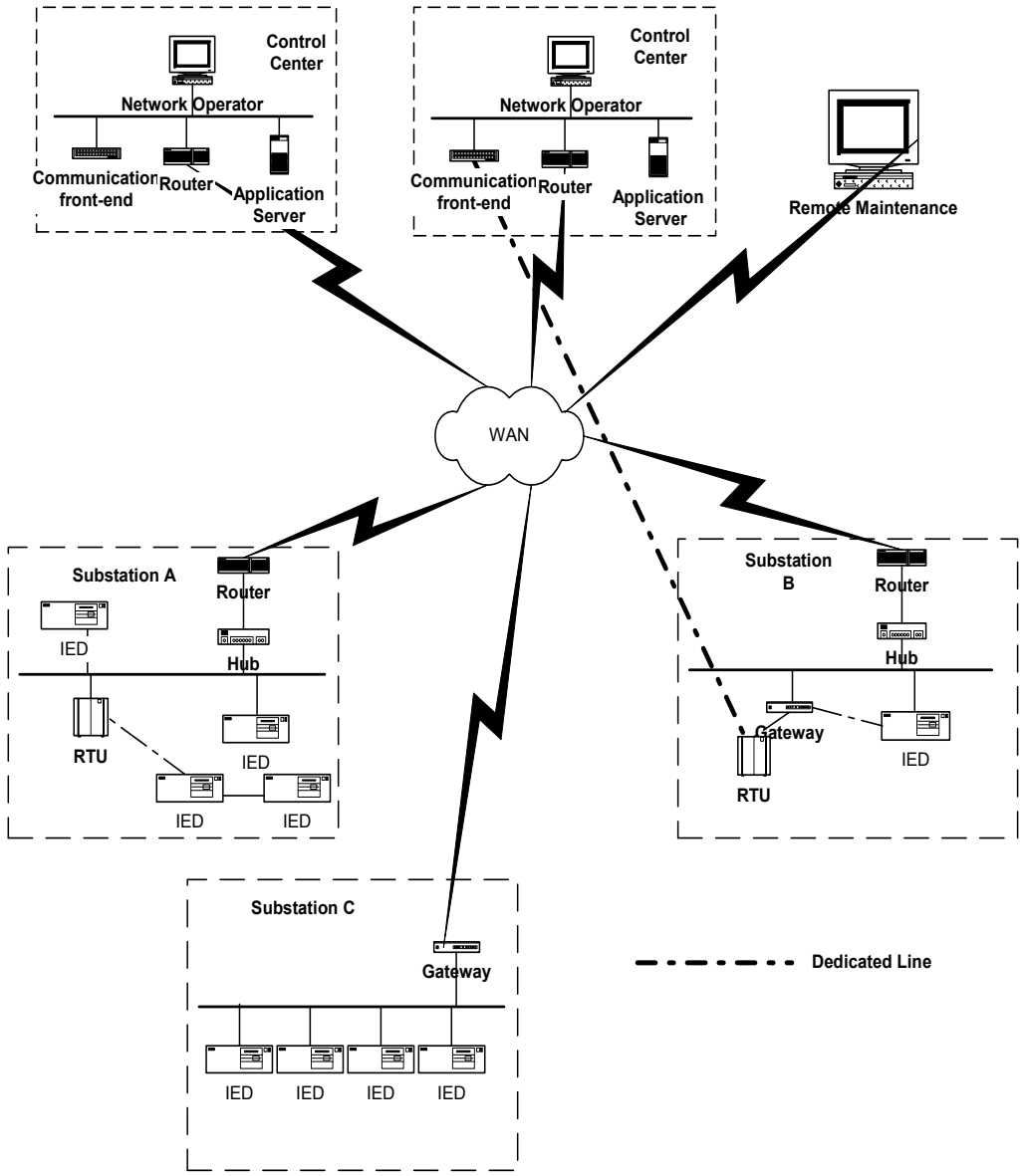

Figure H.11—Enterprise level network example

Figure H.11 illustrates the network implementations at the enterprise level. Figure H.12 illustrates the possible complexity of a substation network.

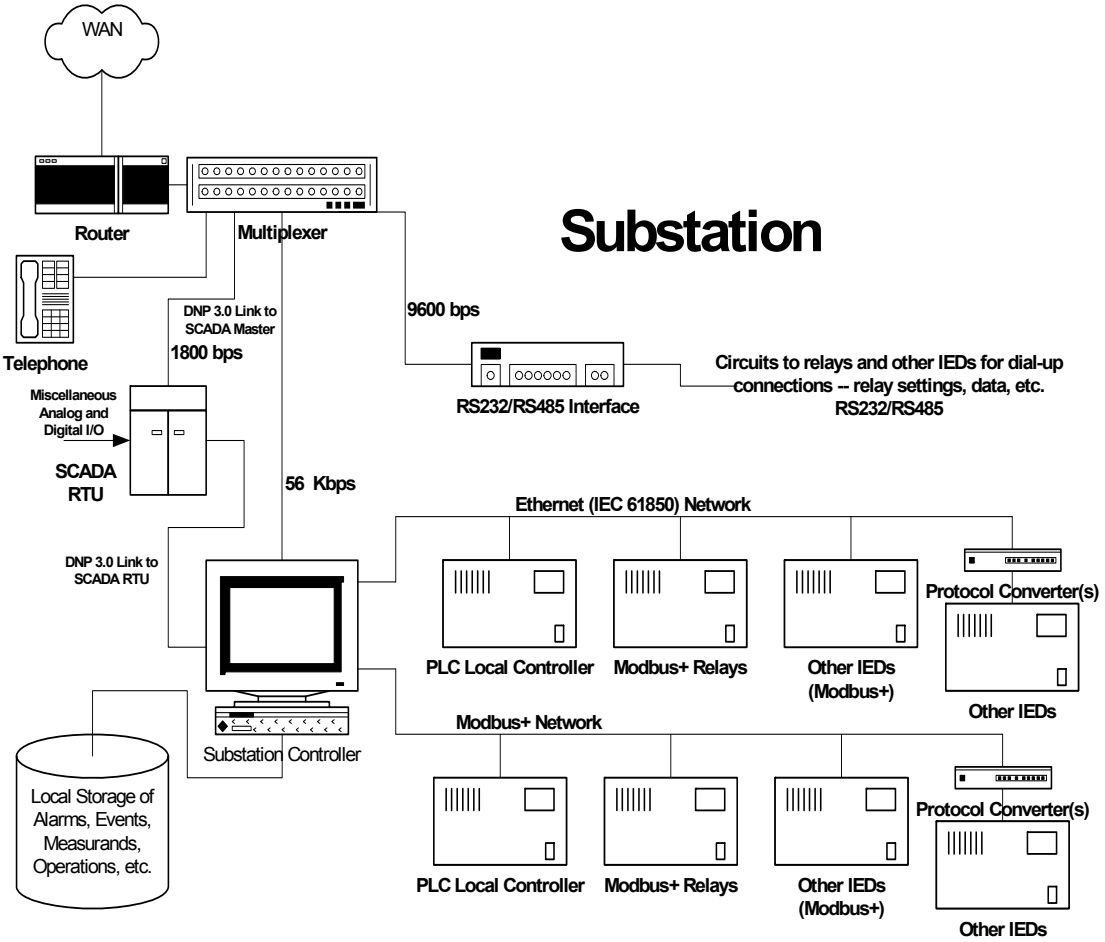

Figure H.12—Substation network example

The communications network connecting IEDs within the substation may also be connected to, or in parallel with, a network to serve enterprise users. While many automation system designers envision a single multi-function network within the substation connected to the enterprise for outside users, it is likely the system will be comprised of networks and sub-networks within the substation and a variety of connection options for enterprise users. The configuration of this assemblage, the network topology, is the "road map" that enables communication. Intersecting points on the map and may require devices to change media, change protocol, extend connection distance and/or control access. There may also be requirements to support legacy devices and systems as well.

Connecting substation IEDs to users dispersed throughout the utility and possibly the outside world imposes a different set of communications requirements. Typically, substation-to-enterprise communications has been a dedicated low-speed pathway used primarily for real-time applications. To add enterprise-wide users requires more connectivity than simple point-to-point pathways. Some solutions to this requirement rely on the PSTN to provide users in diverse locations a means to connect to the substation. A more robust solution for adding remote sites lies in network technology where the substation-to-enterprise traffic is carried over a WAN. Network technology can employ any number of different media including wire-line, optical fiber, UHF and microwave radio and the public telecommunications network to connect enterprise users to substation networks or network servers. Networks afford a high-speed connection more suitable to multiple users and varied applications.

One or more of the elements discussed in H.7 may be present in the final topology.

H.7 Designing a communications network for automation

The design of a communication system for substation automation includes the following steps:

a) Define messaging system endpoints (internal or external to the substation, or both)

b) Develop the communication system topology

c) Determine device interoperability requirements

d) Choose the communication media

e) Define the communication architecture

f) Determine the protocols and physical interfaces supported by EVERY IED to be interfaced

g) Determine the minimum protocols and physical interfaces that are required

h) Determine if it is more cost effective to provide protocol and media converters or establish dedicated networks for each combination, or a combination of approaches.

Each of these steps is related to each other. For instance, some topologies may be supported by only a few types of communication media. Also, the communication topology may restrict the choice of communication protocol or protocols. In a network-based communication system, a set of protocols is chosen.

H.7.1 Functional requirements

The basic functional requirement of any communications system is that it supports the various communications methods that may be required or desired. If an "all new" installation is specified, a study should be undertaken to determine the following:

a) All data sources and destinations

b) Expected routing for above including alternate routes where required

c) Delivery and refresh time for all data sets and control messages

d) Expected flow in the short and long term for normal and out of normal power system conditions

e) Appropriate media and technologies

f) Electrical and physical isolation requirements

g) Estimate of preliminary cost

h) Requirements for continuity of service

i) Assess privacy, security and access control requirements

j) Requirements for electrical isolation

k) Requirements for environmental withstand

If the communications system incorporates any part of an existing system, such as existing communications interfaces built into existing facilities, microwave systems, wire line systems or optical fiber systems, the functional requirements include detailed descriptions of these "pre-existing" conditions. They also define how any pre-existing facilities are to be integrated into the communications system.

Regardless of what the final system may look like, a complete description of the functional requirements of the system should be written along with a plan to get from existing to final configuration.

H.7.1.1 Reliability

It cannot be assumed that any given stream of bits to be sent between IEDs will be delivered without error to the output at all times. A communications channel consists of an assembly of wires and cables, electronic equipment, power supplies, terminations, towers, and other apparatus. Each individual communications channel should be reviewed from end to end with a list of all equipment that is involved. Take into account possible redundant paths and a combination of series and parallel-connected equipment. If there is any AC-dependent equipment in series with the channel, it should be assumed the channel will not function in the event of a power failure or "blackout".

Reliability calculations can be complicated when public facilities are involved. Many telephone systems include significant redundancy in common equipment. However, very few, if any, public telephone systems are designed for 100% service. Dial-up circuits are particularly vulnerable to overloading (access denial) during emergency situations. Dedicated virtual private networks can be more reliable, but there is no guarantee that a higher priority user (government or public safety, for example) will not preempt the virtual network. Very few public network facilities are AC independent.

In the reliability assessment, identify points in the network that represent a single point of failure. The assessment should include how each element (or its function) is mitigated if its failure impedes critical functions. Consider duplicating sensitive items with functional equivalents, but consider using different suppliers so that a weakness in one device does not propagate to the redundant device. If an identified failure impedes performance, determine if that impediment is tolerable or if replicating the equivalent performance is not economically justifiable.

Consider segregation of pathways. The network can become vulnerable to failure if all communications passes through a single device (e.g., communications isolator) or in routed through a common space such as an exit cable, cable duct, communications tower or even an equipment room. Segregating network cabling within the substation may also afford some protection for accidental damage or a disaster. Segregating pathways external to the substation reduces the system's exposure to natural and manmade disasters.

Segregate LANs and WANs by critical function. It is important that critical functions be maintained under all reasonable circumstances, while secondary functions may be compromised without undue affect on the users. Times of stress on the utility system can bring significant traffic in secondary data transfers that could slow the delivery of critical functions. The added expense to assure critical functions is often money well spent during times of stress.

H.7.1.2 Performance

The system relies on the performance of the communications links to satisfy the requirements for data and control both inside and outside of the substation. Assess the data flow over the network elements during normal and stressed conditions of the power system. A network may be robust enough to handle normal condition traffic but may bog down or "crash" during periods of high activity. Note that some systems rely on abbreviated messaging techniques such as change reporting to lower traffic and thereby lower cost, but even these techniques are vulnerable to overload during stress on the power system when many parameters are changing very rapidly. This condition needs thorough evaluation in the design stage.

H.7.1.3 Establishing priority pathways

The most common measure of performance is the bit error rate. A bit error rate of 1×10^{-5} is typical of an unconditioned voice grade channel, and it is recommended that this be the worst possible bit error rate that is acceptable. This means that on average one bit out of 10 000 transmitted bits will be in error. If this were an evenly spaced distribution, it would not be that great a problem and it would be fairly easy to develop an error correcting code that would compensate for the errors. However, errors in communications circuits tend to occur in bursts; so most communications protocols contain techniques to at least detect errors and initiate a re-transmission. Extended outages of communications channels due to weather or other conditions are usually better analyzed under the category of reliability.

H.7.1.4 Security

A communications channel should be immune to unauthorized access. Unauthorized access includes such activities as taps, eavesdropping, bit substitution, spoofing, etc., or just random interference. A detailed analysis of each channel is required to ensure immunity. Inadvertent access is a common cause of communications problems. Channel connections can appear in many locations, such as patch and connection boxes, main frames, etc. A technician using probes to discover a noisy pair, or unused pair, can often cause problems as the probes are run down the terminal blocks. Most often it is impossible to ensure that the communications channel is highly secure. The security function is therefore usually applied to the protocol(s) used on the communications channel.

Annex I

(informative)

Bibliography

[B1] ANSI/ISA 50.00.1, Compatibility of Analog Signals for Electronic Industrial Process Instruments.

[B2] ANSI/ISO 5807, Information Processing—Documentation Symbols and Conventions for Data, Program and System Flowcharts, Program Network Charts and System Resources Charts.

[B3] ANSI/NEMA ICS 6, Industrial Control and Systems: Enclosures.

[B4] "Cryptographic Protection of SCADA Communications—General Recommendations," American Gas Association, September 7, 2005.

[B5] "Cyber-Security for Utility Operations," NETL Project M63SNL34, Sandia National Laboratories Final Report, May 2005.

[B6] IEC 62351-3: Communication Network and System Security – Profiles Including TCP/IP.

[B7] IEC 62351-4: Communication Network and System Security – Profiles Including MMS.

[B8] IEC 62351-5: Data and Communication Security—Security for IEC 60870-5 and Derivatives.

[B9] IEC 62351-6: Data and Communication Security—Security for IEC 61850 Profiles.

[B10] IEEE 100, *The Authoritative Dictionary of IEEE Standards Terms,* Seventh Edition.

[B11] IEEE Std C37.2, IEEE Standard Electrical Power System Device Function Numbers and Contact Designations.

[B12] IEEE Std 91a/91, IEEE Standard for Graphic Symbols for Logic Functions.

[B13] IEEE Std 280, IEEE Standard Letter Symbols for Quantities Used in Electrical Science and Electrical Engineering.

[B14] IEEE Std 315, IEEE Graphic Symbols for Electrical and Electronics Diagrams.

[B15] IEEE Std 344, IEEE Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations.

[B16] IEEE Tutorial "Adding New Life to Legacy SCADA Systems," IEEE Std product number 03TP163.

[B17] IEEE Tutorial "Substation Automation Tutorial" IEEE Std product number 03TP166 is recommended for those not familiar with substation automation systems.

[B18] IEEE Tutorial "The Protective Relay IED in the Automation World," IEEE Std product number 03TP162.

[B19] International Building Code (IBC).[13]

[B20] ISA-99 "Manufacturing and Control System Security."

[B21] ISA-TR-99-001 "Security Technologies for Manufacturing and Control Systems."

[B22] ISA-TR-99-002 "Integrating Electronic Security into the Manufacturing and Control Systems Environment."

[B23] ISO 9001, "Quality management systems—Requirements."

[B24] MIL-HDBK-217, *Reliability Prediction of Electronic Equipment.*

[B25] MIL-HDBK-471, *Designing and Developing Maintainable Products and Systems*.

[B26] NERC CIP-002 to CIP-009.[14]

[B27] NFPA 70, National Electrical Code® (NEC®).[15]

[13] The IBC is published by the Internation Code Council whose headquarters are 500 New Jersey Avenue, NW, 6th Floor, Washington, DC 20001-2070.

[14] NERC CIP standards are published by the North American Reliability Corporation whose main office is in Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5721.The documents are available online from www.nerc.com, presently at http://www.nerc.com/~filez/standards/Reliability_Standards.html#Critical_Infrastructure_Protection.

[15] The NEC is published by the National Fire Protection Association, Batterymarch Park, Quincy, MA 02269, USA (http://www.nfpa.org). Copies are also available from the Institute of Electrical and Electronics Engineers, Inc., 445 Hoes Lane, Piscataway, NJ 08854, USA (http://standards.ieee.org/).