

IEEE PC37.1™/D1.9

Draft Standard for SCADA and Automation Systems

Prepared by the Electric Network Control Systems Standards Working Group of the
Substations Committee

Copyright © 2006 by the Institute of Electrical and Electronics Engineers, Inc.
Three Park Avenue
New York, New York 10016-5997, USA
All rights reserved.

This document is an unapproved draft of a proposed IEEE Standard. As such, this document is subject to change. **USE AT YOUR OWN RISK!** Because this is an unapproved draft, this document must not be utilized for any conformance/compliance purposes. Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of IEEE standardization activities only. Prior to submitting this document to another standards development organization for standardization activities, permission must first be obtained from the Manager, Standards Licensing and Contracts, IEEE Standards Activities Department. Other entities seeking permission to reproduce this document, in whole or in part, must obtain permission from the Manager, Standards Licensing and Contracts, IEEE Standards Activities Department.

IEEE Standards Activities Department
Standards Licensing and Contracts
445 Hoes Lane, P.O. Box 1331
Piscataway, NJ 08855-1331, USA

Abstract: <Select this text and type or paste Abstract—contents of the Scope may be used>

Keywords: <Select this text and type or paste keywords>

1. Overview	1
1.1 Scope	1
1.2 Purpose	1
2. References	1
3. Definitions	1
35. Function Overview	1
35.1 General	1
35.2 Master station (control center) Architecture and Functions.....	1
35.3 Remote site (substation) control system functions and architecture.....	1
36. System Design.....	1
36.1 System Function Definition Requirements.....	1
36.2 Selection of IEDs.....	1
36.3 Security Requirements.....	1
36.4 Selection of Architecture	1
36.5 Selection of Protocols.....	1
36.6 Maintaining Availability.....	1
37. Interface Requirements.....	1
37.1 Mechanical.....	1
37.2 Grounding.....	1
37.3 Electrical Power.....	1
37.4 Data and Control Interfaces.....	1
37.5 IED Communication Interfaces	1
38. Environmental Requirements	1
38.1 Environment	1
38.2 Surge Withstand Capability (SWC).....	1
38.3 Vibration and shock.....	1
38.4 Seismic environment	1
38.5 Impulse and switching surge protection	1
38.6 Acoustic interference limitations	1
38.7 Electromagnetic interference (EMI) and electromagnetic compatibility (EMC).....	1
39. General Requirements	1
39.1 Project Plan.....	1
39.2 Marking	1
39.3 Documentation.....	1
39.6 Testing	1
Annex A (informative) Bibliography	1

Annex B (informative) Control Center Functions	1
B.1 Architecture.....	1
B.2 Communications	1
B.3 Measurements	1
Annex C (informative) Master Station/Substation Interconnections	1
C.1 Single Master Station	1
C.2 Multiple Master Stations.....	1
C.3 Multiple master stations, multiple RTU(s).....	1
C.4 Combination systems	1
C.5 Substation gateway connections (legacy to standard protocols)	1
C.6 Networked systems	1
Annex D (informative) Serial Communication Channel Analysis	1
D.1 Introduction	1
Annex E (informative) Annex E Control Applications	1
E.1 Select Before Operate (SBO)	1
E.2 Multi-coded Control Messaging.....	1
E.3 Direct Operate	1
Annex F (informative) Control Disable.....	1
F.1 Control Disable (Local – Remote) Scheme Examples	1
F.2 Control Power Cut-Off	1
F.3 Individual IED Interface Cut-Off	1
F.4 IED Interposing Power Cut-Off	1
F.5 IED Logic Input.....	1
F.6 IED Software Control Disable.....	1
F.7 Summary	1
Annex G (informative) Communications System Security	1
G.1 Authentication and authorization	1
G.2 Data integrity and confidentiality	1
G.3 Forensics	1
Annex H (informative) Database, Database Server.....	1
H.1 IED database.....	1
H.2 Substation database client/server	1
H.3 SCADA, EMS or DMS database	1
H.4 Enterprise accessible database	1
Annex I (informative) Interlocking	1
I.1 Logical or Sequential Interlocks.....	1
I.2 Distributed Interlocks	1
Annex J (informative) System Support Tools	1

J.1 Software Tools	1
J.2 Health Check.....	1
Annex K (informative) Communication Fundamentals	1
K.1 Basic Communications technology.....	1
K.2 Introduction to the communications stack	1
K.3 Communications Topologies	1
K.4 Designing A Communications Network for Automation	1
Annex L (informative) Communication Topologies	1
L.1 Point to point networks	1
L.2 Point to multi-point networks.....	1
L.3 Peer to peer networks	1
L.4 Multiple pathways	1
L.5 Networks	1
Annex M (informative) Protocols.....	1
M.1 Application (utility specific protocol)	1
M.2 Description of communication protocol used in legacy systems.....	1
M.3 Some protocol notes.....	1
M.4 Protocol Characteristics (look at 1525 1379).....	1
Annex N (informative) Integrated Substation Human Machine Interface.....	1
N.1 Users	1
N.2 Intelligent Electronic Device Human Interface.....	1
N.3 Integrated Station Level HMI	1
N.4 Software Specification	1
N.5 Functions	1
N.6 Graphics Display	1
N.7 Report Generation.....	1
N.8 System Diagrams	1
N.9 Client/server functions.....	1
N.10 Log Files	1
N.11 Availability	1
N.12 Maintenance.....	1
N.13 Software Issues	1
Annex O (informative) Integration of legacy devices in substation automation project (or modernization) .	1
Annex P Communication Protocol Profile	1
P.1 Network Configuration.....	1
P.2 Physical Layer	1
P.3 Network Based Communication.....	1
P.4 Link Layer	1
P.5 Transport Layer	1
P.6 Application Layer.....	1

Introduction

(This introduction is not part of IEEE PC37.1/D1.9, Draft Standard for SCADA and Automation Systems.)

This document is not designed to serve as a standard for all possible users. When applicable, the user may use this standard as a guideline in the design or specification of all or a portion of a system. 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 37.2, which also contained device function numbers. ANSI C37.2-1970 was revised into two standards: IEEE C37.1-1979, Standard Definition, Specification, and Analysis of Manual, Automatic, and Supervisory Station Control and Data Acquisition, and IEEE Std C37.2-1979, Electric Power System Device Numbers. Previous editions were approved by the IEEE Standards Institute 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 C37.2..

This standard applies to a 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, for greater use in many industries.

IEEE Tutorial Course Text EHO 337-6 PWR [Bxy] is recommended for those not familiar with Supervisory Systems. In addition, the corresponding Tutorial Video Tape HVO 245-1-POT [BXY] is also recommended. Both are available from the IEEE Service Center.

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 shall not be responsible for identifying patents or patent applications for which a license may be required to implement an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Participants

At the time this draft standard was completed, the Electric Network Control Systems Standards Working Group had the following membership:

John Tengdin, *Chair*

Dennis K. Holstein, *Vice-chair*

Alex Apostolov
William Ackerman
Mason Clark
Kenneth Cooley
Geoff Crask

Steven Dalyai
Michael Dood
James Evans
James Gardner
William Harlow

Dennis Holstein
Marc Lacroix
Edward Miska
Scott Mix
Craig Preuss

Peter Raschio
James Recchia

H. Lee Smith
Michel Toupin

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

(to be supplied by IEEE)

Draft Standard for SCADA and Automation Systems

Introduction

Participants

At the time this draft standard was completed, the Electric Network Control Systems Standards Working Group had the following membership:

John Tengdin, *Chair*

Dennis K. Holstein, *Vice-chair*

Alex Apostolov
William Ackerman
Mason Clark
Kenneth Cooley
Geoff Crask
Steven Dalyai
Michael Dood

James Evans
James Gardner
William Harlow
Dennis Holstein
Marc Lacroix
Edward Miska
Scott Mix

Craig Preuss
Peter Raschio
James Recchia
H. Lee Smith
Michel Toupin

Draft Standard for SCADA and Automation Systems

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.

2. References

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

IEC 60870-6, Telecontrol Equipment and Systems

IEC 61850, Communication Networks and Systems in Substations

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

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

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

IEEE 1646, Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation
IEEE-1379 Recommended Practice for communications between IED and RTUs

IEEE C37.115, 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 C37.90.1, Standard Surge Withstand Capability (SWC) Tests for Relays and Relay Systems Associated with Electric Power Apparatus

3. Definitions

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

3.1)Accuracy: The difference between the actual value of a measurement and the indicated value of the measurement.

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 must be expressed with a 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 $0.3\% \times 3000$ or ± 90 amps, so the accuracy of a 300 amp load measurement is actually 300 ± 90 amps or $\pm 30\%$ of the measured value.

3.2)Availability: The measure of time a parameter measurement is available to users and algorithms. It is customary to express availability in percentage, usually as 99.xxx where xxx is an expressed fraction of a percentage point. It is sometimes more useful to express unavailability as a maximum period of time during which the variable is unavailable, e.g. 4 hrs per month. Availability = uptime/(uptime + downtime).

3.3)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.

3.4)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.

3.5)Clear Time: The amount of time that the select relay will operate after the master trip or close has operated.

3.6)Control Arm Time-out: The maximum amount of time that a device will wait to receive an execute command after receiving an arm command. Refer to Select Command.

3.7)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.

3.8)Diagnostics: Programs automatically executed at predetermined intervals to check the health of the device.

3.9)Double-point Accumulator: 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 ABNORMAL or INVALID states. Purpose is to detect and count complete changes of state (transitions), while ignoring any incomplete transitions.

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

3.11)Form C Counters: A pair of digital inputs that counts the transitions from one valid state to the next valid state, while ignoring any transitions to invalid states. 2 inputs, counts when both change to the opposite state (1 on, 1 off).

3.12)Host Name: On an IP network, an arbitrary name used as an alias for a network device's address.

3.13)Host Table: A table maintained in a network device that lists all host names on the IP network.

3.14)IP Network:

3.15)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.

3.16)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.

3.17)PING: Acronym for Packet Internet Groper, a utility that can test the "reach ability" of destinations on an IP network. It uses an ICMP echo request, and waits for its reply.

3.18)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.

3.19)Recloser: Abbreviated name for automatic circuit recloser.

3.20)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).

3.21)Scan (interrogation): The process by which a data acquisition system interrogates RTUs for points of data. See also polling (data request).

3.22)Scan cycle: The time in seconds required to obtain a collection of data (e.g. all data from one RTU, all data from all RTUs, or all data of a particular type from all RTUs).

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

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

3.25)Single point/multiple point: Control of a single point versus global control of multiple points.

3.26)Software Debouncing: A method used to determine whether a digital input has actually changed state, or whether a perceived change of state was actually contact bounce or other line

3.27)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.

3.28)Unavailability: The ratios of downtime to uptime, or downtime/(uptime + downtime).

3.29)Update Periodicity: The unit time between updates, sometimes expressed as the rate at which a measurement is updated (frequency).

3.30)Local Area Network (LAN): A LAN is a general-purpose technology 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.

3.31)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.

4. Function Overview

References Annex XX Security.

4.1 General

In recent years, network based automation has greatly evolved with the use of Intelligent Electronic Devices (IED) in substations and power stations. The processing is now distributed and functions that used to be done at the control center can now be done by the IED. 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 (Generation Company), TRANSCO (Transmission Company), DISCO (Distribution Company), ISO (Independent System Operator), RTO (Regional Transmission Organization) etc. To fulfill their role, each of these entities needs a Control Center to receive and process data and take appropriate control actions.

4.2 Master station (control center) Architecture and Functions

Modern 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 Local Area Network (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 a typical SCADA master station system architecture.

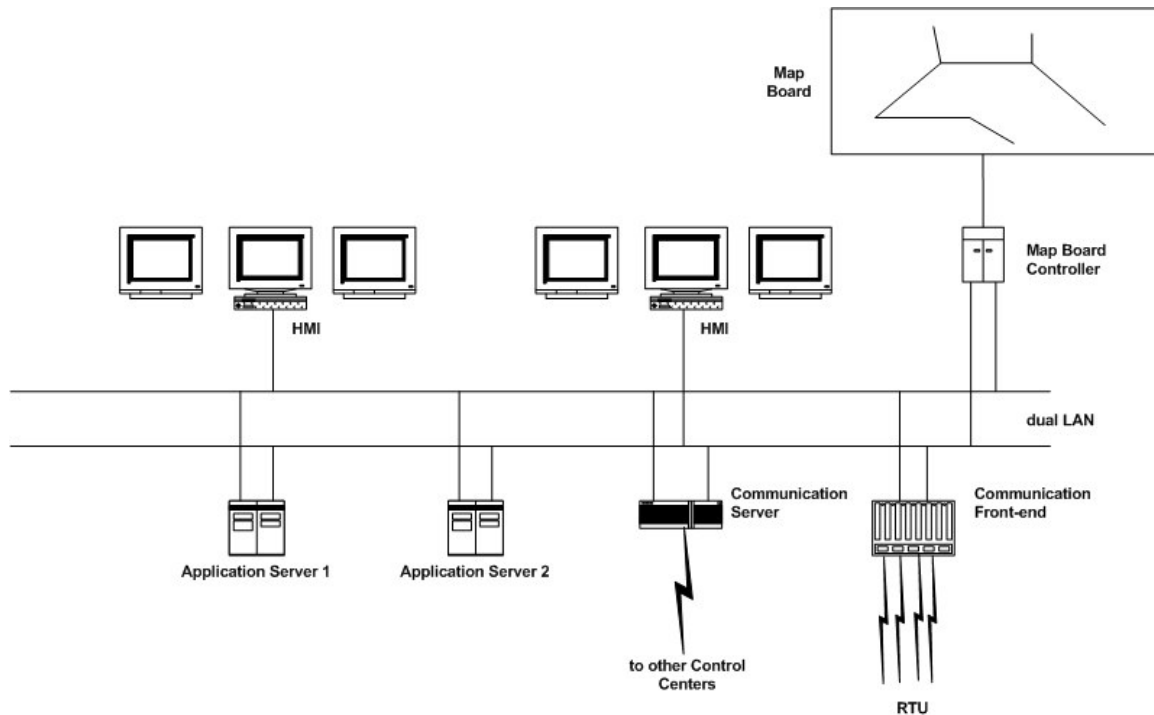


Figure 1—Typical SCADA master station system configuration at a control center

Modern SCADA master station systems 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-Windows, and related products for the computer applications, IEC-60870-6 (TASE.2) for communications to other control centers, and IEEE 1379 for RTU communications. Despite the fact that most vendors offer open systems, they each develop their own API (Application Programming Interface). 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 insure inter-operability at the API level.

The main elements of the SCADA system illustrated in Figure 4-1 are:

- **Human-Machine Interface (HMI):** This interface comprises the mimic board and multi VDU (Video Display Unit) workstations:
 - **Mapboard:** The map board (or mimic board) is intended to give an overview of the power system. It shows a simplified representation of the power system preserving as much detail as possible with the geographical orientation of the system. Two different map board technologies are used in control centers. The mosaic type mimic board 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 LEDs can also be inserted in the mimic board to offer animation capability. If a modification is needed, tiles must be removed and 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 should prepare and send 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.

The main reason given for preferring 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:** Workstations that are 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 4 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:
 - **Core SCADA subsystems:** This server is used mainly for data processing functions and real-time database storage.
 - **Database subsystems:** This server supports the historical database.
 - **Advanced Application subsystems:** These servers support all EMS or DMS applications. The main characteristic of this server is its processing power. More than one server may be used for these applications.
 - **Historical and future 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 administration:** 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 Remote Terminal Units (RTUs) and field equipment. It provides functions such as control and monitoring of the RTU data, protocol conversion, security check, storage of analog and digital data, and detection of analog value and switch 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 section XX for additional security requirements.

4.3 Remote site (substation) control system functions and architecture

Prior to using IEDs (Intelligent Electronic Devices) 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. The RTU may still be specified as all or a part of the substation control and data acquisition system and to provide the communications interface to the master station. With the advent of IEDs that provide protective relaying as well as data acquisition and control functions, a different control system architecture may be required. Figure 2 is taken from IEEE C37.115 and is an example reference architecture of a substation automation system with a substation local area network (LAN).

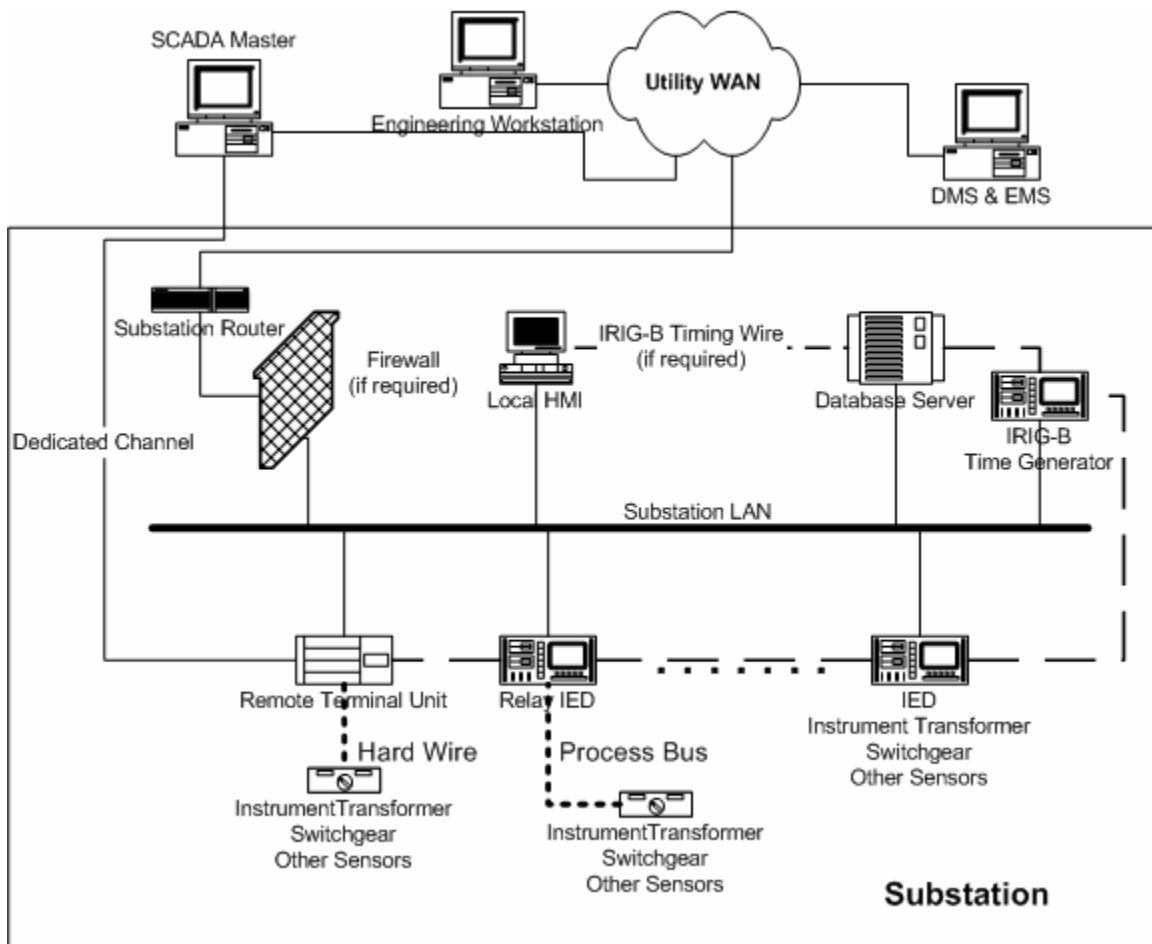


Figure 2— Substation Automation System Architecture

In this figure, the connection from the substation to the EMS and other users at engineering work stations is through the corporate WAN. The connection from the WAN to the substation LAN is through a router and firewall, if this access control is required. Also shown is a “dedicated channel” to the RTU 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. Communication message encryption (not shown) may be required on these external connections. 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 is stored in a database server. 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.

The timing wire shown connecting the timing source (shown as an IRIG-B receiver) to the IEDs is not required if the clocks in the IEDs can be accurately set over the LAN, such as by using IEEE 1588. If time tagging of events to ± 1 ms is a requirement, then the IED clocks must be set to ± 0.1 ms. For IEDs computing synchrophasor data, the time error requirement in IEEE C37.118 “IEEE Standard for Synchrophasors for Power Systems” is ± 26 μ s for a 60 Hz system and ± 31 μ s for a 50 Hz system.

The functions performed by a substation automation system include at least the following:

- Measurement
- Status (static) Monitoring
- Control

- Protection
- Ancillary services
- Time synchronization
- Database maintenance
- Human machine interface (HMI)
- Remote access to the database and controls
- Programmable logic controller

Not shown or included are connections to the maintenance ports of the IEDs. These ports are 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. This channel may be required to meet the security standard requirements, check with your organizations security policies. Security is discussed in more detail in section XX.

The example diagram shows a single LAN and non-redundant IEDs. Other architectures may include redundant IEDs, LANs, and communication channels. These and other architectures are discussed in section XX.

5. System Design

The Designer/Specifier should define the near and long term system functionality. 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 that 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), IEDs, security, availability, and architecture. Conversely, selection of components and architectures is usually constrained by various elements such as pre-existing equipment, IED selection by others, 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. However, the annexes of this document 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 Definition Requirements

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

- Measurements
- Status monitoring
- Control
- Protection
- Ancillary services

- Time synchronism
- Programmed logic functions

The SCADA or substation automation 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.

To assist the Designer/Specifier, tables in this section show industry consensus for a power transmission network. Requirements for systems for 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 section also include typical performance requirements:

- Update Periodicity (Seconds)
- Accuracy (%)
- Availability (Hours/month)
- Latency (Seconds)
- Resolution (%)
- Time skew (Seconds)

The definition of these performance requirements can be found in the Definitions and Annexes.

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 section 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 2-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.

5.1.1 Measurement Services

The following table is presented as a means to capture the requirements for measurements.

Table 1—Typical Measurement Services

Enterprise / Function	Typical Measurement Performance Requirements							
	Example Measured Elements	Update Periodicity (Sec)	Accuracy (%)	Availability (Hrs/mo)	Latency (Sec)	Resolution (%)	Time skew Substation (Sec)	Time skew SCADA (sec)
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 & Reactive Power, Line	10	1.0	4	5	0.2	1	1
Low priority alarm	Real & 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	10	1.0	4	5	0.2	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
System Planning	Voltage, Line	15	0.3	24	10	0.1	1	1
	Real & Reactive Power, Line	30	1.0	24	30	0.2	1	1
	Real & 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 & Reactive Power, Line	2	1.0	2	1	0.2	1	1
	Real & 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

Typical Measurement Performance Requirements								
Enterprise / Function	Example Measured Elements	Update Periodicity (Sec)	Accuracy (%)	Availability (Hrs/mo)	Latency (Sec)	Resolution (%)	Time skew Substation (Sec)	Time skew SCADA (sec)
	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 & Reactive Power, Line	15	3.0	8	30	0.2	1	1
Contingency Analysis	Real & 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							
Intra-Substation Phasor Measurements	Voltage, Line							
Inter-substation/utility Phasor measurements	Real & Reactive Power, Line							
Substation Events	Real & Reactive Power, Equip							
System Events	Current, Line							
	Current, Equip							
	Frequency/Phase Angle							
	Position, Regulator/valve							
	Ancillary value							
Tier 6								
Device configuration data	Configuration Files							
GIS data	Mapping Files							
Electric system topology	Archive Files							
Condition monitoring								
Archive								
Disturbance/Fault data								

		Typical Measurement Performance Requirements						
Enterprise / Function	Example Measured Elements	Update Periodicity (Sec)	Accuracy (%)	Availability (Hrs/mo)	Latency (Sec)	Resolution (%)	Time skew Substation (Sec)	Time skew SCADA (sec)
Tier 7								
Substation/system time reference								

5.1.2 Status Monitoring Service Performance

The following table is presented as a means to capture the requirements for status monitoring.

Table 2—Typical Status Monitoring Performance Requirements

		Typical Monitoring Performance Requirements						
Enterprise / Function	Example Measured Elements	Update Periodicity (Sec)	Accuracy (%)	Availability (Hrs/mo)	Latency (Sec)	Resolution (%)	Time skew Substation (Sec)	Time skew SCADA (Sec)
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	99.9	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		5						
Security Surveillance								

Typical Monitoring Performance Requirements								
Enterprise / Function	Example Measured Elements	Update Periodicity (Sec)	Accuracy (%)	Availability (Hrs/mo)	Latency (Sec)	Resolution (%)	Time skew Substation (Sec)	Time skew SCADA (Sec)
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

The following table is presented as a means to capture the requirements for control services.

Table 3—Example Control Services Performance Requirements

Enterprise / Function	Typical Control Performance Requirements						
	Example Measured Elements	Execution Time (Sec)	Accuracy %	Unavailability (Hrs/mo)	Latency (Sec)	Single Point / Multiple Point	Feedback Sequence
Tier 1							
Substation Operator Control	Circuit breaker, capacitor switcher	2	99.99	4.0		Single	SBO
Auto-sectionalizing	Substation or Field device	2	99.99	4.0		Multiple	None
Generation Dispatch		2	99.9	4.0		Multiple	None
Substation algorithm		0.5	99.99	4.0			
Tier 2							
Non-System Operator Enterprise User		15		24		Single	
Low priority control	Pumps, lighting	15	99	12		Single	

5.1.4 Ancillary Services Performance

Ancillary services are often specified for a SCADA/Automation system, which are outside of the real-time services. The following table is presented as a means to capture the requirements for ancillary services.

Table 4—Example Ancillary Performance Requirements

Function	Typical Ancillary Performance Requirements								
	Example Measured Elements	Update Periodicity	Execution Time (Sec)	Accuracy %	Unavailability(Hrs/mo)	Latency (Sec)	Resolution (Sec)	Time skew Substation (Sec)	Time skew SCADA (Sec)
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

The following table is presented as a means to capture the requirements for time synchronism services.

Table 5—Example Time Synchronization Performance Requirements

		Typical Time Synchronization Performance Requirements					
Function	Example Measured Element	Accuracy %	Unavailability (Hrs/mo)	Latency (Sec)	Resolution (Sec)	Time skew Substation (Sec)	Time skew SCADA (Sec)
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			28800	0.001	0.010	0.010
Tier 2							
Archive							
Disturbance/Fault data			4.0	300	0.001	0.010	0.010

5.1.6 Programmed Logic Services Performance

The following table is presented as a means to capture the requirements for programmed logic services.

Table 6—Example Programmed Logic Performance Requirements

Function	Typical Programmed Logic Performance Requirements						
	Example Measured Element	Execution Time (Sec)	Accuracy %	Unavailability (Hrs/mo)	Latency (Sec)	Resolution (Sec)	Time skew Substation (Sec)
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:

- Effects of hardware/software power cycle and restart
- Provisions to view I/O value and state
- Provisions to view point mapping
- Processing time for the parameters present at the device terminal to be available as a parameter at the communications port

5.2.2 Measurements

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

- Accuracy over the expected operating range
- Resolution over the full operating range
- Instability at or near zero input or some constant value
- Sample size used to compute the measurement
- Sampling rate used to compute the measurement
- Algorithms available for producing “instantaneous” and “time averaged”
- Time for a step change at the input to be processed
- Burden on the instrument transformers or sensors

5.2.3 Input Status Monitoring

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

- Time to recognize a change of state
- Sampling rate
- De-bounce options
- Available counting registers for state changes
- Available input processing for change of state, e.g. momentary change detect
- Time tagging capability, resolution, and accuracy
- Wetting voltage and current for inputs
- Isolation
- Support for different input configurations, e.g. form a, form b, form c

5.2.4 Control

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

- The time delay to execute control output once a control command has been sent to or received from a communication port
- Time delay after a control command has been executed before another command can be initiated
- Support for control of multiple points per command
- Output interface compatibility with substation control requirements
- Control output isolation
- Support for “select-before-operate” control commands
- Support for momentary and maintained outputs
- Provisions to block, or “tag”, single or multiple outputs for the IED

- Support for different output configurations, e.g. form a, form b, form c

5.2.5 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:

- Additional traffic affecting the performance of the system networks
- Potential for corrupting system mapping to other functions
- Potential for injecting “interfering or false” data onto the substation communication network

5.2.6 Time Synchronization

IEDs may need to use time in their computation or logging functions. Designer/Specifiers should assess the IED choices with regards to the method(s) that they plan to deploy for synchronizing time across the population of IEDs. The IEDs chosen should 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. IED time synchronization should support IEEE 1646 “IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation”.

5.2.7 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 logic internal, where their normal function includes protection algorithms while others are blank programmable devices such as programmable logic controllers. Selecting the appropriate platform for logic should include at least the following considerations:

- Process to upload and download programs
- Support for program de-bugging and troubleshooting
- Support for IEC-61131 programming logic
- Portability of developed algorithms between devices from the same or different vendors
- Remote program control support
- Required performance for the intended task including data acquisition, processing, and delivery
- Failure and recovery modes
- Expandability
- Organizational support for the selected platform and program tasks

5.2.8 Protection

Protection IEDs must 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 those system functions.

5.2.9 Revenue Meters

Revenue meter IEDs must 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 those system functions.

5.2.10 IED Lifespan

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

- New products may have yet undiscovered deficiencies and pose a challenge to integrate with older devices.
- Mature devices may be nearing the end of their production life and could go out of production in the near future.
- IED suppliers should be queried as to the expected production life.
- IED suppliers should be queried as to their hardware/firmware change notification process (see IEEE C37.231)

IED obsolescence is inevitable. Designers 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 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 specifier with security concepts. Refer to the bibliography for applicable work from other sources for more complete treatment of security. Corporate policy should establish an electronic security perimeter around the system. This policy usually relies on some blend of technology and procedures. System security should not rely on technology alone. Application of system security requirements should consider:

- Industry regulations and standards
- Government regulations
- Corporate safety, IT, and personnel policies
- Other (the bibliography identifies a few documents on security and the annex includes more information on security)

Using these requirements, the 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. 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/EMS, corporate WAN, IED maintenance ports, and other entities that should be considered in establishing a security practice.

5.4 Selection of Architecture

The interconnection of IEDs, servers, workstations, and communications interfaces constitute the architecture of the system. 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 XX.

System designers often have a specific architecture in mind that fits their particular concept for automation. That architecture may fit a specific logical configuration to support power equipment or some functionality or process. However, developing a suitable architecture often requires that new and existing be blended together in a functional accommodation along with a vision toward a future architecture. To reach this architecture requires the designer to define the connectivity between IEDs, servers and users needed to support the functionality specified. The designer should also provide alternate pathways and devices as needed to meet availability targets and mitigate single point of failure consequences. 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.

5.4.1 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 which 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, Energy Management (EMS) or Distribution Management System (DMS). This interface often must maintain compatibility between an existing utility EMS or DMS and the substation. Such an interface may take several forms:

- A traditional SCADA remote terminal unit (RTU) with hardwired interfaces to substation equipment
- An advanced RTU where its interface is more of a communications gateway to IEDs and their network(s)
- 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 several forms such as:

- 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 devices. Designer/specifiers should also be aware of the potential security issues posed by providing outside access to IED “maintenance” ports.

More details of internal “maintenance” port networks are discussed in section 5.4.2.

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. Designer/Specifiers 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
- Exposure of the channel media to physical damage
- Response of the channel owner to request for repair service
- The consequences of channel owners to reconfiguring channels without notification to users

5.4.2 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 must be 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 1615 “Recommended Practice for Network Communication in Electric Power Substations” provides details on applying network technology to substations and should be used as a reference.

5.4.2.1 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. Designers should be aware of at least the following potential issues using these ports:

- IEDs may not fully support connections to modems or computers that require channel control signals to be available.
- IEDs may have additional signal and/or power conductors present in the port connector that can be problematic to users.
- 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.
- EIA-RS-232 does not support multi-drop configurations. Additional hardware will be needed to implement a multi-drop channel.
- EIA-RS-232 is limited to short distances, typically less than ten meters.

IEDs may also support multi-drop communication ports with an EIA-RS-485 interface. Designers should be aware of at least the following potential issues using these ports.

- EIA-RS-485 channel control is generally “master – slave” where one device addresses others one at a time to control traffic. There is no mechanism defined in EIA-485 to mitigate channel contention or collisions. Some messaging schemes allow the transfer of channel control from one device to another to provide multiple device access. Here the serial protocol must support addressing for both sender and receiver in each message.
- All devices must on an EIA-RS-485 channel must use a common protocol
- Many devices provide for biasing the EIA-RS-485 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 must not provide pair biasing as this adds to the channel loading.
- EIA-RS-485 pathways must be terminated with resistors at each end, sized 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.
- EIA-RS-485 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.
- An EIA-RS-485 pathway must be linear, stubs are not permitted.

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

- Integrating devices 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 must emulate the activities of a human with a terminal to interact with the IED. Some IEDs will require the communications processor 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 than 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 re-inventing 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.

5.4.2.2 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.

5.4.2.2.1 Network Adapters

It is possible to bridge the gap between network devices and serial devices with a network adapter, often called a Network Interface Module (NIM). NIMs 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 characteristic:

- 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.
- 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.
- 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.

5.4.2.2.2 Network Standards

There are multiple standards based upon which an automation network can be built. The newest of these is IEC 61850 “Communication Networks and Systems in Substations”. Among other things, this standard specifies many levels of protocols needed to support integrated substation automation functionality. IEC 61850 is a very complex and comprehensive standard. Some utilities will find that it is more than is needed to accomplish their task and could add significant overhead cost.

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

IEEE-1615 (insert title) provides guidance for incorporating networks into utility communications for automation.

The Information Technology (IT) standards commonly deployed for the business environment are being adopted to reach to the substation. These include:

- TCP/IP
- SMTP
- SMS
- More

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

5.5 Selection of Protocols

It is important to recognize that any specific IED may understand only one protocol. If a standard protocol is already in use in a substation, Designer/Specifiers 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:

- 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?
- Does the existing protocol have all the capabilities needed to support the required functionality?
- Will a new protocol meet the performance requirements using the existing communication infrastructure or will that have to upgrade? At what cost?

- Will it support the interrogation of single data values, sets of data, or the entire stored data on a “report by exception” basis?
- Will it support unsolicited alarm reporting – analogs out of limits or status changes?
- 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 must be established using one of the recommended protocols.
- What is the impact on the long-term life cycle costs must be considered including impacts on future upgrades, additional equipment installations and on-going support?

5.6 Maintaining Availability

5.6.1 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 Tables 5.1.1 through 5.1.6. Some functions can be expected to be critical to the operation of the substation and power system such that their availability must be 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 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 requirements by function. The second step is then to render a design that meets those requirements with suitable solutions.

5.6.2 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 system designer should identify areas where critical components are shared by system functions and treat them as additional system functions.

5.6.3 Limiting Risk of Failure

The system designer 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 is Mean Time Between Failure (MTBF) which is a probabilistically derived estimate of the longevity of the component. Refer to Appendix XX for a discussion on deriving MTBF. 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. Designer/Specifier should refer to standards such as IEEE 1613 and C37.90 which can help the designer 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 to which they are exposed 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 must operate 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. Designers should evaluate the expected longevity and stress applied to such components as they formulate their designs.

5.6.4 Estimating Loss of Function Time

Using the list of critical components previously identified, the designer should assess the time required to return the impaired function to usability. This estimate is usually discussed in analysis as Mean Time To Repair (MTTR)¹ and is discussed in Appendix XX. Since the availability requirements have already been identified, the designer 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:

- Time for a qualified support person to identify the failure
- Time for the a replacement component to be delivered to the failure site
- Time for a qualified support person to repair the failure
- 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.

5.6.5 Providing Alternative Functional Support

There are many ways to provide alternative functional support to achieve a quick "Return To Service". The designer may provide for a redundant function to replace the unavailable function when one of its components fails. The designer 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. The Designer/Specifier should evaluate which function should be restored manually, by human intervention considering the implications cited below.

- 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.
- Automatic fail-over mechanism. Automatic fail-over schemes must monitor functions and recognize a function has become impaired, 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 must 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.

¹ IEEE 100 defines mean time to repair (MTTR) as "The time interval (hours) that may be expected to return failed equipment to proper operation."

5.6.6 Operating Functions in Parallel

In order to assure the continuous availability of system functions, 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 should specify which measurement from a specific IED will be the primary data source and which will be an alternative source. The designer must 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 must 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 which will dictate that the designer specify one IED as the primary controller and another as the alternate. The designer must provide a means for the user to know, at any given time, which IED is providing the control functions.

5.6.7 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. SA system designers 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.

System designers must assess the cost of separating shared facilities as a cost of obtaining availability. They must 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 Requirements

The control and data acquisition equipment shall have interfaces as described in this clause. The interfaces described consist of those illustrated in [Figure 5](#).

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 250-2003 and IEC 60529, which typically apply to harsh environments and ANSI/EIA 310-D-1992, 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:

- Location of access doors
- Physical security (locking devices and keys)
- Enclosure mounting
- Temperature control and ventilation requirements
- Resistance to moisture, atmospherically born contamination and solar radiation
- Terminal-block type, location and specific termination layout(s) when required
- Cable entry locations
- Special cabling and connector requirements
- Placement and details for cabinet grounding and bonding
- Cabinet material, color, and finish considerations
- Lighting and power outlets

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 device 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.

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 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 DC voltage ratings have been adapted from IEEE 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 to 14 Vdc)
- b) 24 Vdc nominal (19.2 to 28 Vdc)
- c) 48 Vdc nominal (38.4 to 56 Vdc)
- d) 110 Vdc nominal (88 to 123 Vdc)
- e) 125 Vdc nominal (100 to 140 Vdc)
- f) 220 Vdc nominal (176 to 246 Vdc)
- g) 250 Vdc nominal (200 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 (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 insure 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 AC voltage rating shall be 120 V 60 Hz, 240 V 50 Hz, or 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 back-up 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 back-up power operation without battery charging (usually not less than 4 hours but normally at least 24 hours)
- 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 back-up batteries
- e) Precautions for possible corrosive material spill/seepage and explosive gas accumulation
- f) Recovery time of the back-up battery after a full discharge

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 to 10 kHz, as measured into an external power source impedance of 0.1 ohms 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. 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.

6.4 Data and Control Interfaces

Data and control signal cabling for the substation automation system may reference IEEE 525 “IEEE Guide for the Design and Installation of Cable Systems in Substations” 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. Point count limitations of IEDs should be taken into consideration, as 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.

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 or 2500 volt 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 Typical Input Interface Requirements

Inputs to automation controllers and measuring devices must 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 here such that compatibility can be assessed.

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 kOhms 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 miswired 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	

Parameter	Specifications	Notes
Common ground return	Signal Ground, 0 – 1.0 megohms	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 miswired 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	
Maximum input signal resistance	10 kOhms for ± 1 mA inputs 600 Ohms for 4–20 mA inputs	Includes overload protection
Conversion resolution, minimum (with sign)	12 bits	Binary data format (includes sign)
Maximum error at 25 °C	$\pm 0.1\%$	Percent of nominal input signal range for a single sample
Maximum temperature error*	$\pm 0.005\%/^{\circ}\text{C}$	Percent nominal input signal range (2 mA)
Minimum common-mode rejection	90 dB	dc to 60 Hz
Minimum differential (normal)—mode rejection	60 dB	At 60 Hz
* Associated with the operating temperature		

Table 8—AC Analog Input Signals*

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 x nominal, 1 s PT – 2.5 x nominal, 10 s	—
Maximum input signal burden	PT - 3 VA CT – 1 VA	—
Conversion resolution, minimum (with sign)	12 bits	Binary data format (includes sign)
Maximum error at 25 °C	$\pm 0.1\%$	Percent of nominal input signal range for a single sample
Maximum temperature error **	$\pm 0.005\%/^{\circ}\text{C}$	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 Vrms for 1 min
Anti-aliasing filter	Specify	Cutoff less than one-half A/D sampling rate

Parameter	Specifications	Notes
* 600 V insulation class, 1200 V hi pot, all isolated (ungrounded).		
** Associated with the operating temperature		

Table 9—Digital Electronic Input Signals

Parameter	Specifications	Notes
Input data format	Specify	Application dependent
Common ground return	No	Optical coupler or equivalent
Signal voltage range	0 to 20 V	—
Signal current range	0 to 20 mA	—
Signal data rate	Specify	—
Signal duration	Specify	—

Table 10—Contact (Electromechanical) Inputs

Parameter	Specifications	Notes
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 Ohms	Includes cable resistance
Minimum leakage resistance (at operating voltage)	50 kOhms	Includes cable leakage resistance

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	9999	~15 min at maximum rate
Accumulator freeze/retrieve command	Specify	—
Non-volatile memory	Specify	—

6.4.3.1 Isolation

The Designer/Specifier should assess the requirement for isolating inputs to controllers and devices. 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. Annex XX discusses common input configurations.

6.4.4 Output Interface Requirements

Outputs must be compatible with substation and power equipment that they control. 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 here such that compatibility can be assessed.

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
Contact voltage rating	125 Vdc	Resistive load
Activation time	Adjustable, 0.1 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 kOhms. ± 5 V range of voltage output is acceptable
Output signal range	± 1.2 mA	—
Maximum output load	10 kOhms 600 Ohms	10 kOhms minimum for voltage outputs 600 Ohms maximum for current outputs
Maximum error at 25 °C	$\pm 0.1\%$	Percent of nominal output signal range (2 mA) includes offset, noise scale factor, and calibration error over six-month period
Maximum temperature error *	$\pm 0.005\%/^{\circ}\text{C}$	Percent of nominal output signal range (2 mA)
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	$\pm 0.1\%$	Percent of nominal output signal range (2 mA)
* 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 to 30 V	—
Signal current range	0 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	30A at 125 VDC	30 A	0.5 Sec	0.0A	
Breaker Closing	10A @ at 125 VDC or	2.0 A	1.0 sec	2.0 A	

	120 VAC				
Switcher Control	Same as breaker controls				
Pilot Duty	0.50 A 125 VDC or 120 VAC	0.50 A	Indefinite	0.50 A	

6.4.4.1 Isolation For Outputs

The Designer/Specifier should assess the requirement for isolating outputs from controllers and devices to controlled equipment. 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. Annex XX 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”.

6.4.5 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.

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 undesirable or unexplainable incident points to them as potential contributors.

(We need a reference to a transient suppression guide, here)

6.4.6 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 reasonable expected expansion.

6.5 IED Communication Interfaces

IED network communication interfaces should meet the requirements specified in IEEE 1613. While not specifically addressed in IEEE 1613, the Designer/Specifier may apply IEEE 1613 to the serial communication interfaces.

7. Environmental Requirements

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

There are unusual conditions that, where they exist, 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:

- 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) Electrostatic discharge
- j) 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 15. 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 15 will require special consideration. Methods to resolve these problems include

- 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 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 15, 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 (°C)	Allowable rate of change of temperature (°C/h)
(1)(a)	unspecified	up to 95% without internal condensation	-40 to +70	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*	+ 5 to +40	10
(4)	In a building or other sheltered area without special environmental control	10 to 95 without condensation*	0 to +55	20
(5)	Outdoors or location with wide temperature variations	10 to 95 without condensation*	- 25 to + 60	20
(6)	Extremes outside the above	User to specify (see 7.1.1)	User to specify (see 7.1.1)	User to specify (see 7.1.1)
* Maximum wet bulb temperature of 35 °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 15, 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 2000 m (6600 ft) 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 UV 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 Surge Withstand Capability (SWC)

The electrical data, power, and control interfaces (e.g., inputs and outputs to the RTU, IED or similar device) shall be designed to withstand the surge withstand capability tests as defined in IEEE 1613 without RTU damage, mis-operation, or data corruption.

7.3 Vibration and shock

7.3.1 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 the following table as examples in typical locations.

Table 17—Operating Temperature and Humidity by Location

Class	Velocity (mm/s)	v	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 the following table.

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.	

7.3.2 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.

7.4 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 C37.98](#) Standard Seismic Testing of Relays).

7.4.1 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 furnished by the California Institute of Technology, Earthquake Engineering Laboratory, 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 Uniform Building Code UBC-1988).

7.4.2 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 **ANSI Z24.21** Method For Specifying The Characteristics Of Pickups For Shock And Vibration Measurement and **IEEE 344** Recommended Practice for Seismic Qualification of Class 1E Equipment for Nuclear Power Generating Stations)

7.5 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.

7.5.1 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.

7.5.1.1 Basic protection

All inputs and outputs are required to meet the oscillatory and fast transient surge withstand capability (SWC) tests, as defined in IEEE 1613. This requirement applies to equipments mounted in substation yards or control houses. Consideration may be given to waiving this requirement if equipment is installed in a protected environment where they will not be exposed to intra-cabinet, inter-cabinet or external adverse environmental conditions.

7.5.1.2 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, auxiliary support systems and the like. 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 1613. Thus they may enter the cabinet and cause damage despite the SWC protection provided on inputs and outputs. 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.

7.5.2 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.

7.5.2.1 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. 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 1613. Circuits that are connected to, or are part of, circuits not within a protected building shall be installed in a manner that will minimize exposure.

7.5.2.2 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 1613 provides guidance relating to Ground Potential Rise (GPR) impact.

7.6 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](#).

7.7 Electromagnetic interference (EMI) and electromagnetic compatibility (EMC)

Manufacturers shall design and test their equipment to ensure that EMI limits are not exceeded, and Designer/Specifiers 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 insure that the risk of mis-operation in the presence of EMI is acceptable.

7.7.1 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 [in accordance with IEC XX](#). Manufacturers shall mechanically and electrically design equipment to satisfy emission limits by employing attenuation techniques such as isolation, shielding, grounding, gasketing, filtering, and bonding.

7.7.2 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 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 1613**). Should the field strength of a proposed installation exceed this value, the Designer/Specifier shall mechanically and electrically design the equipment location for conducting susceptibility limits by using cable shielding and grounding techniques found in

- l) **IEEE Std 525** for substations
- m) The equipment manufacturer's guide for site preparation and installation shall be followed at other locations.

7.7.2.1 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 **7.7.2**, 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.

7.7.2.2 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. General Requirements

Adequate specification of general requirements will help contribute to a successful project. The following sections discuss specific requirements to insure a successful project. For more information on this section refer to IEC standard 61850-4.

8.1 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.

8.1.1 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.

8.1.2 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. 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.

8.1.3 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:

- a) The person to contact to submit technical problem descriptions
- b) The person responsible to organize meetings
- c) 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.

8.1.4 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).

8.1.5 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.

8.1.6 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.

8.1.7 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

8.1.8 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.

8.2 Marking

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

8.2.1 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 must be uniform throughout the system and includes the use of color coding, labeling, naming conventions, and parts numbering.

8.2.2 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 PROMs, EPROM, GALs, FPGAs and similar components should be marked by the supplier with a program identifier and version. Users are encouraged to acquire programming tools for these components and their programs.

8.2.3 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 must be in compliance with all safety codes and standards applicable to the device and its intended use.

8.3 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 alternate fashion, but must 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 must 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:

- **ANSI/ISO 5807** Information Processing - Documentation Symbols and Conventions for Data, Program and System Flowcharts, Program Network Charts and System Resources Charts
- **IEEE Std C37.2** Standard Electrical Power System Device Function Numbers and Contact Designations
- **IEEE Std 91a/91** IEEE Standard for Graphic Symbols for Logic Functions
- **IEEE Std 280** Standard Letter Symbols for Quantities Used in Electrical Science and Electrical Engineering
- **IEEE Std 315** Graphic Symbols for Electrical and Electronics Diagrams

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

8.3.1 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, EPROM, 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 1379-2000](#) 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 must be 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.

8.3.2 Installation

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

- 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., door openings, windows, elevator weight and size limits, etc.).
- i) Other procedures needed to properly install the equipment

8.3.3 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.

8.3.4 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, etc) 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 Automation 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.

8.3.4.1 Performance information

Performance information includes a condensed description of how each device operates (derived from [8.3.1](#)) 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 a device 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 between stations, or locally at a station.

8.3.4.2 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.

8.3.4.3 Corrective maintenance instructions

Guides for locating malfunctions down to the field-replaceable unit (FRU) 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.

8.3.4.4 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 which cannot be economically repaired should be identified in the parts list of the maintenance instructions.

8.3.4.5 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.

8.3.5 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”).

8.3.6 Reliability 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.

8.4 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.

8.4.1 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 certified. The scope of the quality assurance program should be agreed upon by all parties prior to the start of work.

8.4.2 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 must prepare and carry out these special investigations with individual products and the overall Automation System. Furthermore, the system integrator must prove the fulfillment of the technical requirements, including performance criteria as presented in the system specification. The system integrator must 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.

8.4.3 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:

- a) Hardware
- b) Engineering
- c) Software

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

- a) Spare parts for an agreed period
- b) Support in diagnosing failures, mis-operation, poor system performance, etc
- c) Mandatory provision of urgent information to the customers about malfunctions
- d) Correction of detected software errors and hardware defects
- e) Offer and installation of software updates.

8.5 Diagnostics

The Designer/Specifier should consider requiring the development of diagnostic tools for:

- 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

8.6 Testing

Testing of the system follows the logical progression of how the system is put together. First, individual components are tested by the manufacturers to meet the standards that the components are manufactured to. These are typically called type tests. Then the interoperation of devices is tested to the standard to which

they are to interoperate. Finally, the whole system is tested as a whole against the standards to which the whole system must perform.

The scope and object of tests, the test procedures and the passing criteria must be specified in the test documentation. All tests must 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 performed by an independent organization that is qualified for performing the tests. If not possible, tests can be performed by a manufacturer provided that unbiased completion of the tests can be achieved through witnessed tests.

8.6.1 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:

- 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.

8.6.2 Routine test

The routine test consists of 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.

8.6.3 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 needs to be certified by an organization that is approved to perform testing by the User Group associated with the protocol (i.e., the Modbus Users Group, the DNP Users Group, and UCA International Users Group). This testing is the only way to ensure that the product properly supports the protocol.

8.6.4 System test

The system test is the proof of correct functionality and performance of each IED under different application conditions (different configuration and parameters) and in cooperation with other IEDs of the overall Automation System including all tools, for example for configuration and diagnostics.

8.6.5 FAT and SAT

The FAT provides validation and verification from the Designer/Specifier’s point of view. The FAT is sometimes optional. The scope and object of the FAT have to be discussed and agreed between all parties involved in the project and are included as part of the test documentation. The result of the FAT should be documented and signed by all representatives witnessing the testing.

The SAT is carried out on the completely installed equipment in 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 must check all information exchanges, controls, and functions. The SAT procedure has to document the results of each step and confirms that the system can be placed into operation.

8.6.6 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)

Bibliography

- [B1] CIP-002 to CIP-009
- [B2] “Cryptographic Protection of SCADA Communications - General Recommendations”, American Gas Association, September 7, 2005.
- [B3] “Cyber-Security for Utility Operations”, NETL Project M63SNL34, Sandia National Laboratories Final Report, May 2005
- [B4] ISA-99 “Manufacturing and Control System Security”
- [B5] ISA-TR-99-001 “Security Technologies for Manufacturing and Control Systems”
- [B6] ISA-TR-99-002 “Integrating Electronic Security into the Manufacturing and Control Systems Environment”
- [B7] IEC 62351-3: Communication Network and System Security – Profiles Including TCP/IP
- [B8] IEC 62351-4: Communication Network and System Security – Profiles Including MMS
- [B9] IEC 62351-5: Data and Communication Security – Security for IEC 60870-5 and Derivatives
- [B10] IEC 62351-6: Data and Communication Security – Security for IEC 61850 Profiles
- [B11] ANSI C2, National Electrical Safety Code (NESC).
- [B12] ANSI/ISA 50.00.1, Compatibility of Analog Signals for Electronic Industrial Process Instruments.
- [B13] ANSI/NEMA ICS 6, Industrial Control and Systems:Enclosures.
- [B14] EIA EMC B2, EMC Specifications, Standards and Bibliography.
- [B15] EIA EMC B3, Testing and Measurement Techniques for Electronic Equipment.
- [B16] EIA EMC B4, Designers Guide on Electromagnetic System Design of Electric Equipment.
- [B17] EIA EMC B5, Bonding of Electronic Equipment.
- [B18] EIA EMC B6, Grounding of Electronic Equipment.
- [B19] EIA EMC B10, Enclosures of Electronic Equipment.
- [B20] EIA EMC B8, Cabling of Electronic Equipment.
- [B21] EIA EMC B9, Filtering of Electronic Equipment.
- [B22] EIA EMC B10, Electromagnetic Susceptibility.

- [B23] EIA RS-422-A, Electrical Characteristics of Balanced Voltage Digital Interface Circuits.
- [B24] FCC Code of Federal Regulations (CFR) Title 47, FCC Rules Part 15, Subparts A and B: clause 15.3—Definitions; clause 15.101—Equipment Authorization of Unintended Radiators; clause 15.103—Exempted Devices; clause 15.107—Conducted Limits; clause 15.109—Radiated Limits.
- [B25] Gaushell, D. J., Frisbie, W. L., and Kuchefski, M. H., “Analysis of Analog Data Dynamics for Supervisory Control and Data Acquisition System,” IEEE Paper 82 SM 304-4.
- [B26] IEC 68-2-6, Test Fc and Guidance: Vibration (sinusoidal).
- [B27] IEEE Std 4, IEEE Standard Techniques for High-Voltage.
- [B28] IEEE Std 518, IEEE Guide for the Installation of Electrical Equipment to Minimize Noise Inputs to Controllers from External Sources (ANSI).
- [B29] IEEE C62.45, IEEE Guide on Surge Testing for Equipment Connected to Low-Voltage AC Power Circuits (ANSI).
- [B30] IEEE Tutorial Course Text 91 EHO 337-6 PWR, “Fundamentals of Supervisory Systems.”
- [B31] IEEE Tutorial Video Tape HVO 245-1-POT, “Fundamentals of Supervisory Systems.”
- [B32] Koenig, D. F., “In Service Availability of the AEP System Control Center,” IEEE Paper 87 WM 059-9.
- [B33] Lloyd and Lipow. Reliability, Management, Methods, and Mathematics. Englewood Cliffs, NJ: Prentice-Hall, 1962.
- [B34] OSHA FR vol. 37, Occupational Safety and Health Standards, Oct. 18, 1972.17
- [B35] Uniform Building Code (UBC)-1988.18

Annex B

(informative)

Control Center Functions

B.1 Architecture

[ALREADY COVERED IN NEW SECTION 5]

B.1.1 Centralized

B.1.2 Distributed

B.1.3 Hierarchical

B.1.4 Split Systems

B.1.5 Backup/Emergency

B.2 Communications

B.2.1 Substation

B.2.2 Enterprise/Intranet

B.2.3 Internet

B.2.4 Operator workstations

B.2.5 Dial-up

B.2.6 Inter Control Center

B.3 Measurements

Data exchange between IEDs and the control center may be performed using different procedures. In a master/slave (or unbalanced) procedure, the control center controls the data traffic by polling IEDs sequentially. In this case, the control center is the master that initiates all message transfers while the IEDs are slave stations that may transmit only when polled.

In peer-to-peer (or balanced) transmission procedures, each IED may initiate a message transfer. In case of major power system disturbances, large amount of data may be sent at the same time to the control center, causing data overflow.

To minimize the amount of information to be exchanged, IEDs may report only those objects that have change status or analog values that go beyond a dead-band value. This mode is called report by exception. To make sure that no status change has been missed, the control center periodically scans all the data in the IED. This is called integrity scan.

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, for different types of information, the format of the element, the quality descriptor and if necessary a time tag. The following objects are the most commonly used.

B.3.1 Analog data

Measured values are 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 of magnitude of some signal characteristics such as amplitude, phase angle, frequency, etc.

B.3.2 Status data

B.3.2.1 Single-Point Information (SPI):

This object is used to represent the state of digital input state. An SPI signal is generally used for alarm status. This type of input receives single information, which is true or false (information lacking). For instance, this object can be used to indicate if a line switch is closed or open.

If an SPI object includes a time tag, then all the status changes shall be sent to the control center. If the object does not include a time tag, it is then meaningless to send all intermediate status. The IED uses 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:

- an input has transitioned from state “1” to state “0” and returned to state “1” or beyond or
- an input has transitioned from state “0” to state “1” and returned to state “0” or beyond or
- an input has transitioned more than two (2) times since last reported

B.3.2.2 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 statuses of both input bits will be the same.

B.3.3 Accumulator data

Integrated totals (or Pulse Accumulators) are used for energy transaction. Pulses received from energy transducers are counted.

B.3.3.1 SOE data

B.3.3.2 Acquisition time

B.3.3.3 Methods

B.3.3.4 Quality codes

B.3.4 Bulk Data Transfer

B.3.4.1 SOE

B.3.4.2 Power Quality

B.3.4.3 Configuration

B.3.4.4 Digital Fault Records

B.3.4.5 IED historical data**B.3.4.6 Disturbance data****B.3.4.7 Method (how do we do it?)****B.3.5 Control**

Supervisory control is the SCADA function used to issue control commands to field equipments under the supervision of the IED. 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 must 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.

B.3.5.1 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.

B.3.5.1.1 Single Command (SC):

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).

B.3.5.1.2 Double Command (DC):

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.

B.3.5.2 Analog Outputs**B.3.5.3 Select-Before-Operate**

This type of command has a three-step sequence:

- 1) Device selection
- 2) Operation selection
- 3) 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 device, he waits for confirmation of device selection and if he is satisfied he can request its operation. SBO controls are timed. If the delay between device selection and device operation is too long, then the control sequence will be aborted and the selection will be cancelled.

B.3.5.4 Set-point

This object is used to send analog values to control devices such as generating unit controller.

B.3.5.5 Raise/Lower

B.3.5.6 Jogging

B.3.5.7 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.

B.3.5.7.1 Information Tags

Operating procedures for substations rely on an information notices 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 certain event in the future, etc. Information notices do not have the stature of safety notices. They must not 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.

B.3.5.7.2 Safety or Protective tags

Operating procedures for substations rely on a system to assure workers' safety from 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.

B.3.6 Alarms

B.3.6.1 Conditions

B.3.7 Database

B.3.7.1 Real-time

B.3.8 User Interface

B.3.8.1 Definitions

Most vendors provide HMI based on X Windows or Microsoft Windows. A full windowing environment offers the capability to concurrently display multiple windows of information. HMI includes the following functions.

B.3.8.2 Graphical displays

B.3.8.3 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.

B.3.8.4 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.

B.3.8.5 Summary displays

B.3.8.6 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. 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 1 the substation state, level 3 the summary state of the main feeders etc.

B.3.8.7 Browsers

B.3.8.8 Tools and builders

B.3.8.9 Large Displays

B.3.8.9.1 Mosaic tile

B.3.8.9.2 LCD

B.3.8.9.3 Plasma

B.3.8.9.4 Projection

B.3.8.10 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 streets' name while the city's map, which is another level of information, shows such details.

B.3.9 Logging

B.3.10 Reports

B.3.11 Security

B.3.11.1 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.

B.3.11.2 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.

B.3.11.3 Communications

B.3.12 Time Synchronization

B.3.13 Operator Messaging

B.3.14 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 are normally continuous counters and do not represent current values. 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 Totals will 'roll over' (i.e., reach its maximum count and start over at zero) and this factor must also be 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.

B.3.15 Fault Recovery

B.3.15.1 Cold standby

B.3.15.2 Warm standby

B.3.15.3 Hot standby

B.3.16 Performance

The most important criteria for SCADA system are availability, maintainability, performance, security, and expandability.

B.3.16.1 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:

$$\text{Availability} = \frac{\text{Total time of satisfactory operation}}{\text{Reference period}}$$

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.

B.3.16.1.1 Hot Standby Redundancy

In this configuration, two servers are dedicated to the same purpose. One of the servers is in active mode while the other is in standby mode. Both servers process in parallel, each one receiving the same information. If the server in standby mode detects a failure of the active one, it will take over process control and change its mode to active. The failover is very fast and no data is lost.

Spare redundancy

In this configuration, a pool of spare servers is provided to cover the event of a failure of one or more active server. A spare server can act as a spare to more than one server. All data and programs must reside on the spare server. The failover can be long and may require the attention of a computer operator.

B.3.16.2 System Maintainability

Maintainability is an important factor to system availability. The repair times following hardware or software failures can be minimised 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.

B.3.16.3 System Performance

System performance is a major criteria 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 must be correctly time-stamped; but the processing and actual display to the system operator may be slower than real-time.

Table B.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

Table B.1 shows typical quantities of information the computer system should process for different conditions of operation.

B.3.16.4 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:

- Available physical space
- Power supply capacity
- Heat dissipation
- Processor throughput and number of processors
- Memory capacity of all types
- 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)

B.3.16.5 Security

Security is another important design criteria. Since most of the computers and IED 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.

B.3.17 System Maintenance

Annex C

(informative)

Master Station/Substation Interconnection Diagrams

C.1 Single Master Station

Figure C.1—Single master station, single RTU

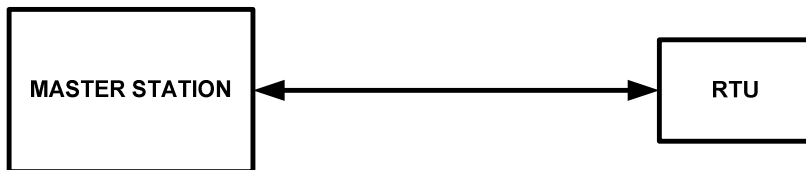


Figure C.2—Single master station, multiple RTU(s), radial circuit

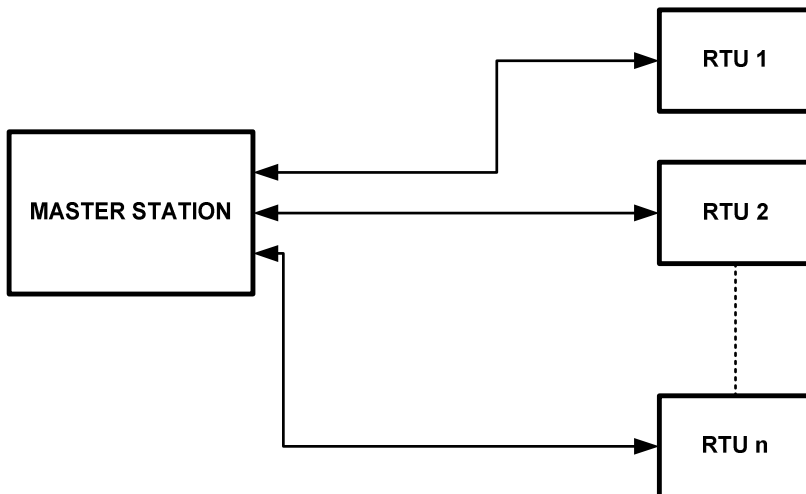
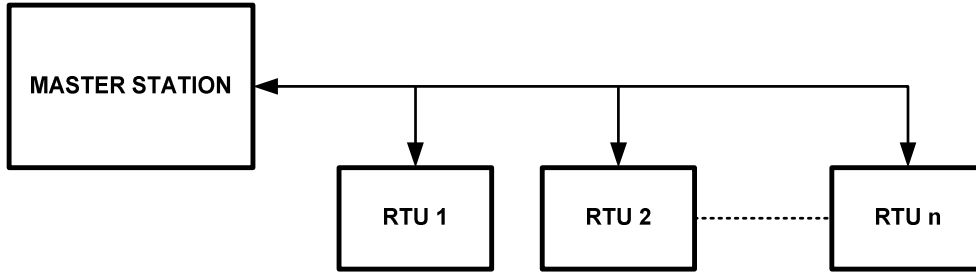


Figure C.3—Single master station, multiple RTU(s) multi-drop circuit



C.2 Multiple Master Stations

Figure C.4—Dual master stations, multiple RTU(s), multi-drop circuit

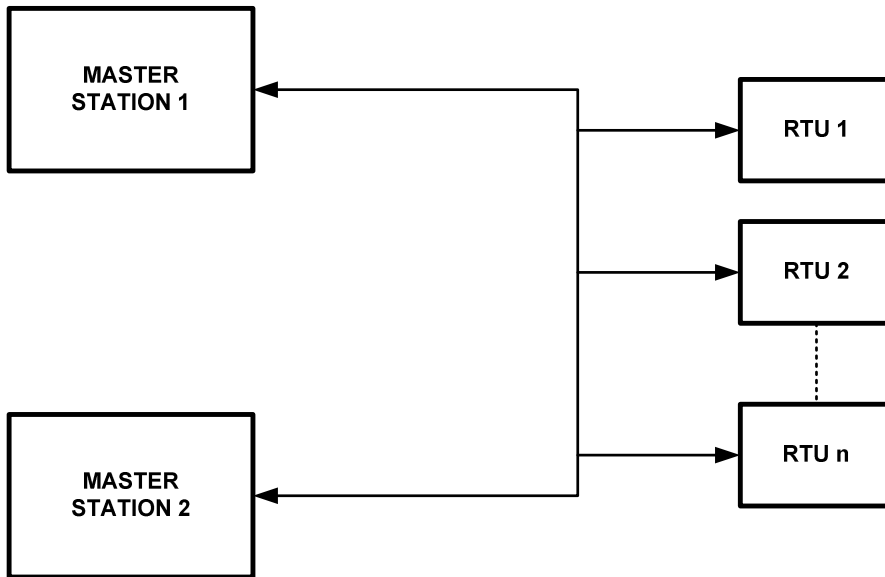
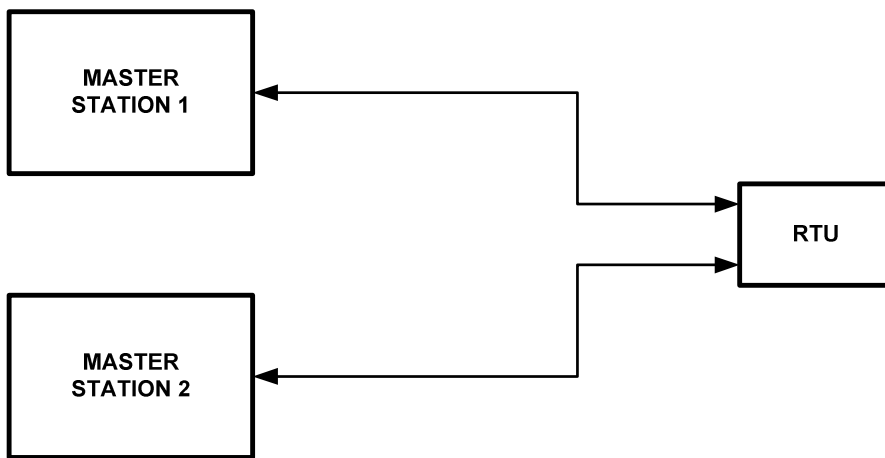


Figure C.5—master station, single dual ported RTU, radial circuit



C.3 Multiple master stations, multiple RTU(s)

Figure C.6—Multiple master stations, multiple single ported RTU(s)

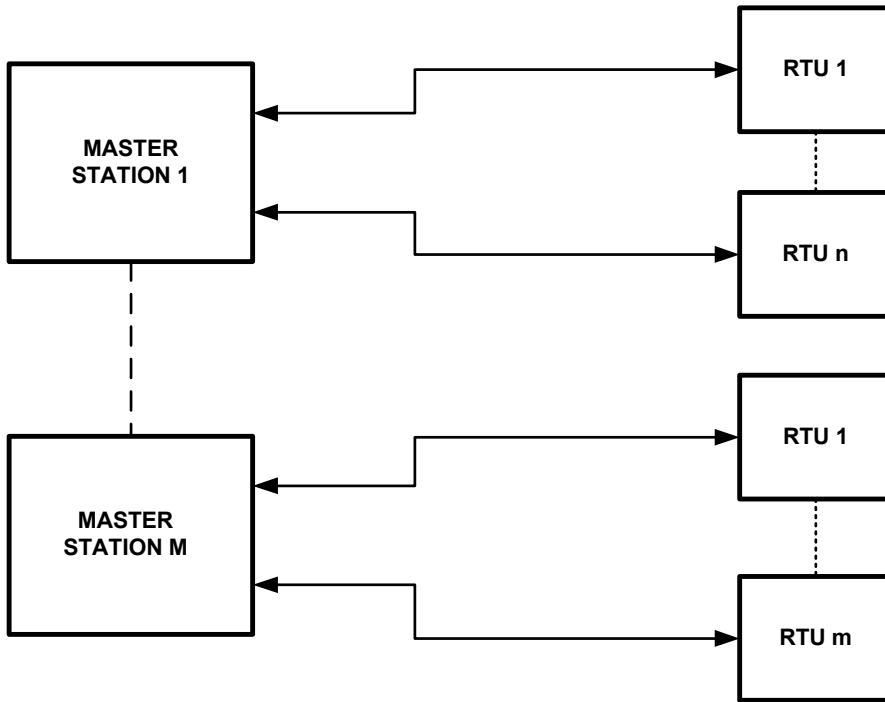
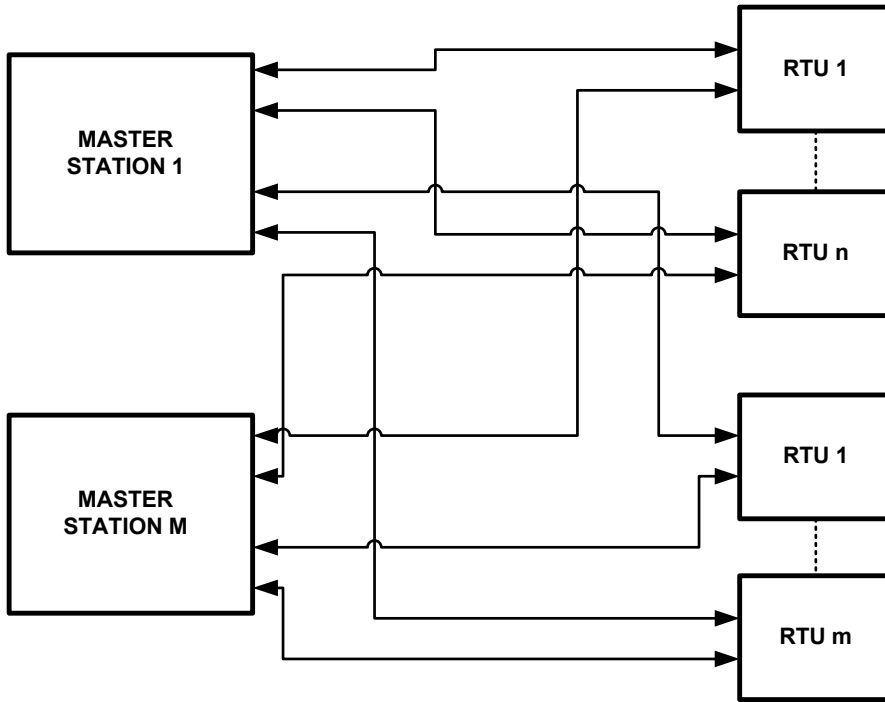


Figure C.7—Multiple master stations, multiple dual ported RTU(s)



C.4 Combination systems

Figure C.8—Single master station, single sub-master station, multiple RTU(s)

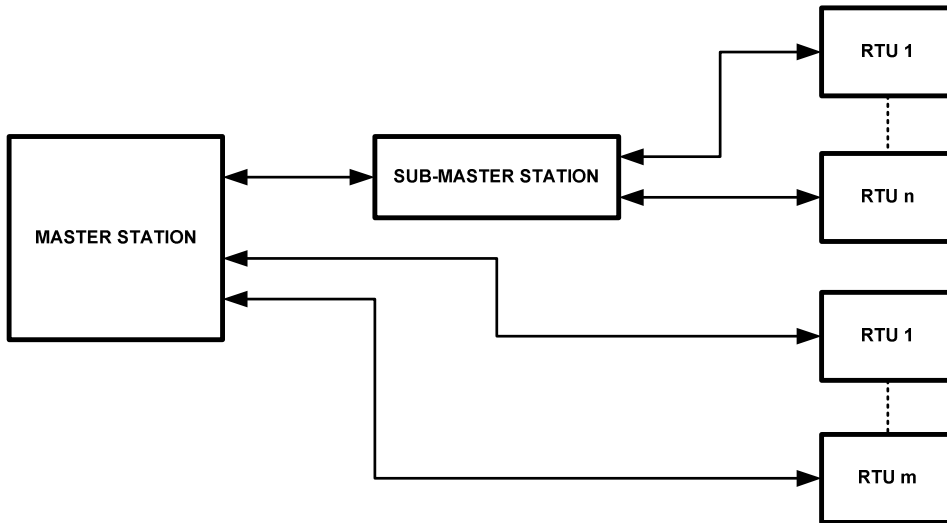
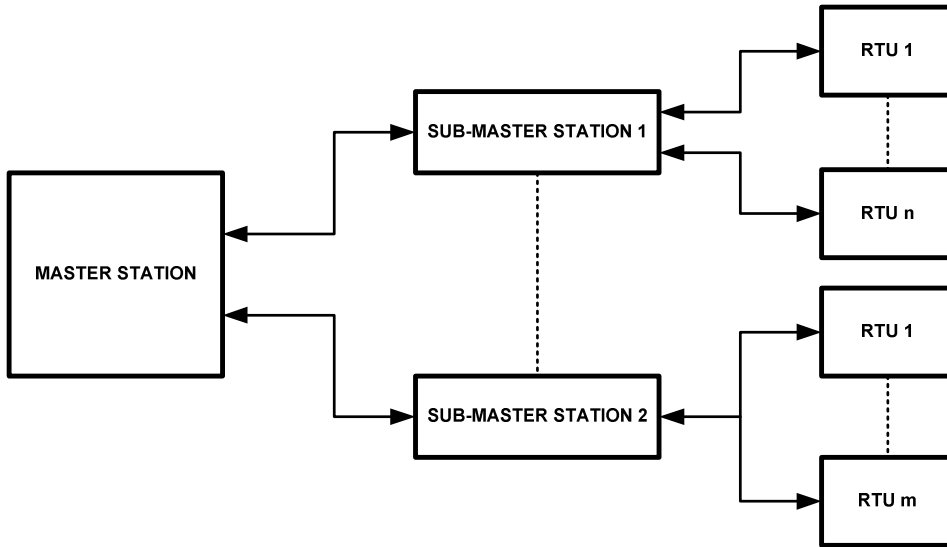


Figure C.9—Single master station, multiple sub-master stations, multiple RTU(s)



C.5 Substation gateway connections (legacy to standard protocols)

Figure C.10—Single master station, substation gateway/data concentrator

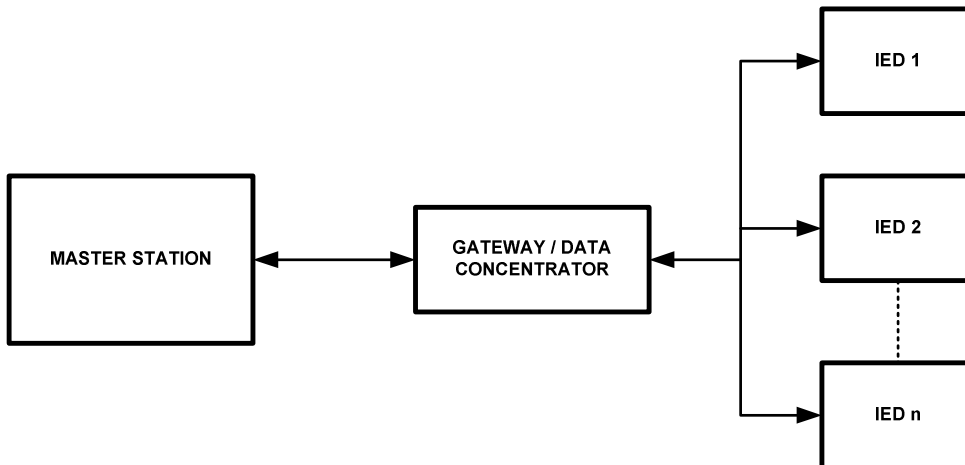
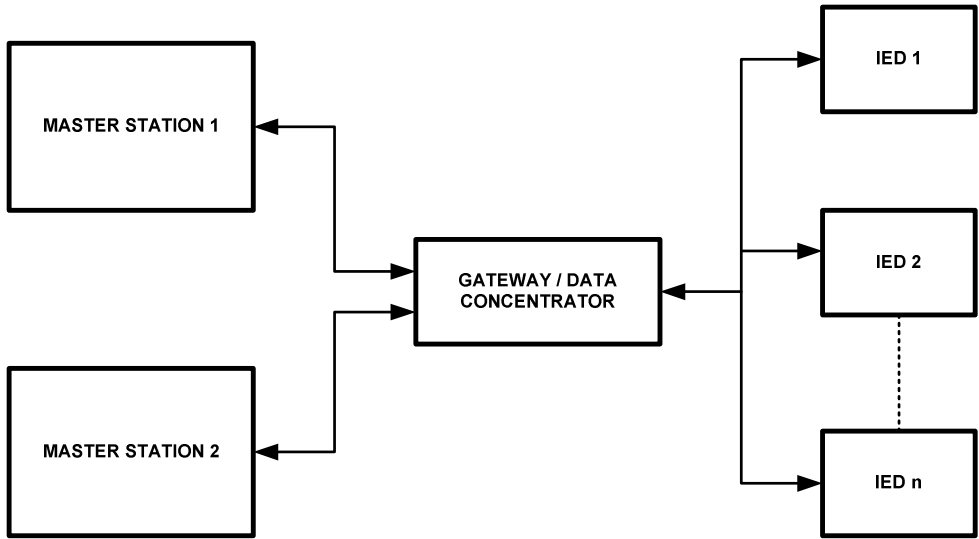


Figure C.11—Dual master station, substation gateway/data concentrator



C.6 Networked systems

Figure C.12—Single master station, substation WAN/LAN connection via routers (Firewall not shown)

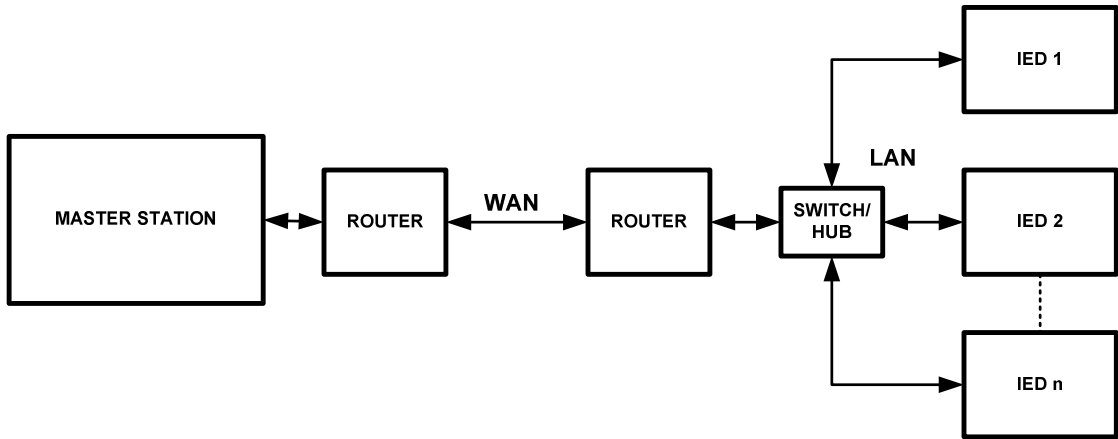
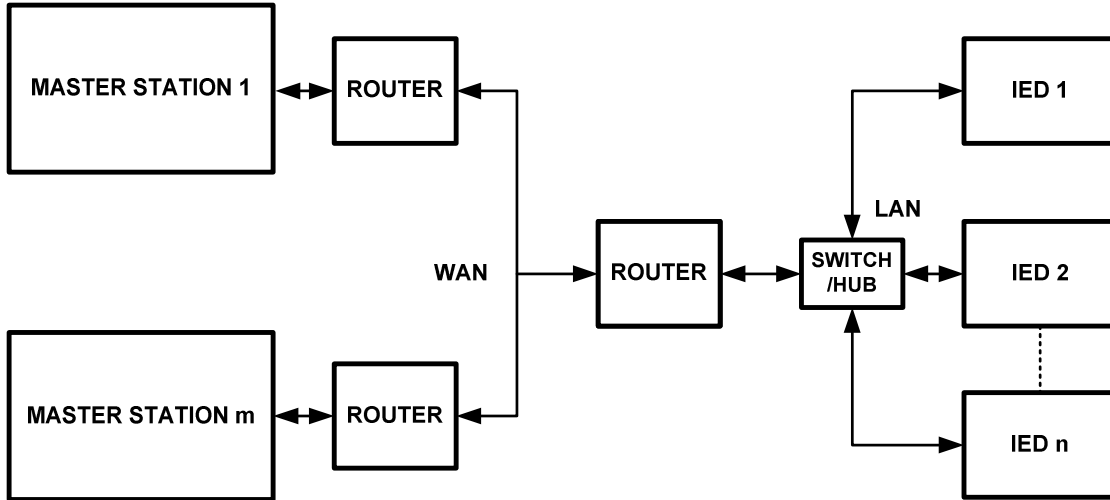


Figure C.13—Multiple master station, substation WAN/LAN connection via routers



Annex D

(informative)

Serial Communication Channel Analysis

D.1 Introduction

The responsiveness of any automation system is limited primarily by the data throughput and latency characteristics of the serial communication facilities that connect the master station to its RTUs. It is therefore essential to check that a planned communication subsystem design will support adequate system performances. This Annex provides a simple procedure for such checks that can identify any necessary changes either to the network design (or, equivalently, to the specifications of the automation system). This procedure addresses only bandwidth and delivery time issues in the data communication network. It assumes that all other network implementation issues such as connectivity, cost, security, reliability, maintainability and expandability have been resolved.

D.1.1 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. These typically include:
 - i) Remote control of RTU internal and external devices
 - ii) Upload of data files (i.e., data acquisition) from the RTU and its local IEDs
 - iii) Download of data files (i.e., remote parameter adjustment) to RTU and IED processors.

NOTE—Transfers of program files to and from 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:
 - i) Two, 10 and 30 seconds for upload of measurement data
 - ii) Thirty seconds for download of generator automatic control data
 - iii) Fifteen, 30 and 60 minutes for upload of counter data. (Each transaction is typically preceded by a counter control function.)
 - iv) Hourly and daily for transfers of processed data files.
- c) Specify the maximum acceptable execution time for all on-line functions, both periodic and event-driven. Typical values are:
 - i) One second for any device control function
 - ii) One second for upload of any data transferred on demand (For example, status data acquired “by-exception”)
 - iii) Less than 50% of the update interval for periodic functions. (Some functions may require a lower limit to provide time for master station processing.)
 - iv) No limit for file downloads.

- d) Specify the maximum file size (information bytes exclusive of all communication overheads) to be transferred in each update cycle of each periodic function. These dimensions must be sufficient to support the largest-capacity RTUs and their associated IEDs.

D.1.2 Channel Performance Analysis Procedure

For illustrative purposes only, typical results for each step in the following procedure are shown in italics.

- a) Estimate (or measure) the total channel time, *T*, required to execute a device control function. This time must include the operating times for all channel equipment while servicing all layers of the communication protocols to be used, in a link that is open, idle, and operating with no communication errors.

Result: The initial measured value of *T* is approximately 400 msec.

- b) Check that *T* is (much) less than the limit value, *L*, specified in (**Error! Reference source not found. c.i**) above. *L* is a fundamental design parameter that limits the worst-case network transport delay. For example, the value of one second listed as typical for *L* inherently precludes routing any part of the network via a geosynchronous satellite.

Result: *T* is less (though not much less) than *L* (one second).

- c) If *T* exceeds about 25% of *L*, either change the communication subsystem design to reduce *T* or increase the specified value of *L*. Reducing *T* relative to *L* increases the channel time available for transfers of other data. *T* should preferably be less than about 20% of *L*. Also, *L* cannot exceed the fraction specified in (**Error! Reference source not found. c.iii**) of the shortest periodic update interval specified in (**Error! Reference source not found. b.i**).

Result: As the initial value of *T* exceeds 25% of *L*., network changes were made to reduce data delivery times. These led to a revised value of 180 msec.

- d) To meet the limit value *L* for completing the execution of a device control function, the channel time required to execute any other communication function must be less than (*L* - *T*). This time interval is typically too short to support the transfer of the largest files listed in (**Error! Reference source not found. d**). Such files must therefore be divided into multiple segments and delivered in a series of transfers.

Result: The nominal value of (*L* - *T*) is 820 msec.

- e) Estimate (or measure) the maximum file segment size that can be transferred in the time (*L* - *T*), under the conditions of (2.a) above.

Result: The measured value of the maximum file segment size is about 2 kB.

- f) Calculate, from the entries in (D.1.2 d) above, the minimum number of file segments required to be transferred during each execution of each periodic function.

Results:

2-second measurements (1,800 transfers/hour): one
 10-second measurements (360 transfers/hour): two
 30-second measurements (120 transfers/hour): one
 30-second controls (120 operations/hour): one
 15-minute counters (4 transfers/hour): one
 60-minute processed data in (1 transfer/hour): 30
 60-minute processed data out (1 transfer/hour): 10

- g) Calculate the total number of periodic file segments to be transferred, and thus the required total transfer time for routine data, during any 60-minute period of operation of the largest-capacity RTU.

Result: From (f), the total number of file segments to be transferred per hour is: $(1,800 + 2 \times 360 + 120 + 120 + 4 + 30 + 10)$, i.e., 2,804.

- h) Check that the total channel time required to transfer all periodic data is less than about 45 minutes, for a channel loading by routine data of less than 75%. Unused channel time is then available for other, future, functions.

Result: Assuming a convenient file segment transfer rate of one/second, the total channel time required per hour is 2,804 seconds, or nearly 47 minutes. 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. In addition, there are 796 unused one-second time slots available during each hour for future functions

- i) Check that the assumed data transfer process will meet the execution time requirements of **(Error! Reference source not found. c)** above.

Result: The time required to execute one device control function (180 msec.) is reserved in each one-second-time slot.

The time required to upload any short data file on demand is available in each one-second time slot not pre-empted by device control.

Transfers of all 2-second measurements are completed in one time slot, i.e., in 50% of their update interval.

Transfers of all 10-second measurements are completed in four seconds, i.e., in 40% of their update interval.

Transfers of all 30-second measurements are completed in six seconds, i.e., in 20% of their update interval.

Transfers of all 30-second generator control commands are completed in 8 seconds, i.e., in 27% of their update interval.

Transfers of all 15-minute counter data are completed in 10 seconds, i.e., in about 1% of their update interval.

Transfers of all 60-minute data are completed in 400 seconds, i.e., about 11% of their update interval.

Annex E

(informative)

Annex E Control Applications

E.1 Select Before Operate (SBO)

Select before Operate (SBO) is a method to minimize the possibility of inadvertent operation. SBO has been implemented with varying degrees 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. SBO uses a feed back mechanism which includes the system operator in the loop.

E.1.1 SBO Sequences

SBO control requires a control originator to transmit a “select” message to the automation system control device which contains a coded action and point identity to establish connection to the end interface being selected. An error free “select” is returned by the automation system control device to the originator along with the selection codes. If the end interface device is successfully selected. Upon receipt of the returned select message the originator will send a execute or activate message to the automation system control device. Upon receipt of the an error free execute or activate message the automation system control device will operate its selected interface. The automation system control device will return an error free execute message to the originator as a signal that control is activated. Any errors in the message stream will cause the automation system control device to ignore the message to return an error message. An error in the process cancels the control sequence. If the messaging does not take place completely within a time window the control process is also canceled. Once an end point is selected, it will hold in select mode for the originator and reject all other select requests until Select Mode self cancels on “time -out”, or is canceled or executed by the Originator.

Refer to Informative Annex # for a discussion of Select Before Operate Control methodology. [Sam Sciacca has written a good SBO - Why we do it or Shouldn't do it annex].

E.1.2 SBO Implementation Variations

The common expectation of SBO is for it to verify the select action through the system to the end device and provide a successful select indication to the Operator. The operator becomes part of the control loop and responds to the select with an additional action to either activate (execute) or cancel.

In some systems the operator select and activate sequence is part of the HMI and messaging to the end device does not occur until the operator dialog is completed. Then, the system performs the select and activate messaging associated with the control message sequence. The system may provide operator feed back with error messages to indicate the select messaging failed due to an error or end device problem.

When control message must pass through a data concentrator or substation host, it may not be possible to “select” all the way to the end device and the SBO dialog may only include the data concentrator. This occurs where the end device does not support SBO.

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.

E.2 Multi-coded Control Messaging

Some control systems rely on a complex control message coding to provide the security for switch and breaker controls.

E.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 must be 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 when received in tact and error free. However, to insure security, the message contains multiple copies of the point and command information, encoded in different forms. The entire message and all the copies must be 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. A secure message error detection scheme such as CRC16 is also employed.

E.2.2 Protocol Selection

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 Specifier must ascertain conformance to this requirement.

E.3 Direct Operate

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 a 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.

Annex F

(informative)

Control Disable

The Control Disable (Local-Remote Switch) provides the functionality to disable the ability of the SCADA/Automation System to operate a control point, or group of control points. This switch would normally be operated by station personnel who wish to ensure that SCADA/Automation operation is prevented. While many IEDs and substation control schemes have provisions to disable a control output to allow RTU and IED technicians to perform IED testing, such switches are not to be confused with the LOCAL/REMOTE switch function that would be used by substation operating personnel and be a part of the tagging procedures. The design of a Local/Remote scheme may facilitate testing IEDs, but the primary consideration must be the safety of station operating personnel and adherence to company tagging procedures.

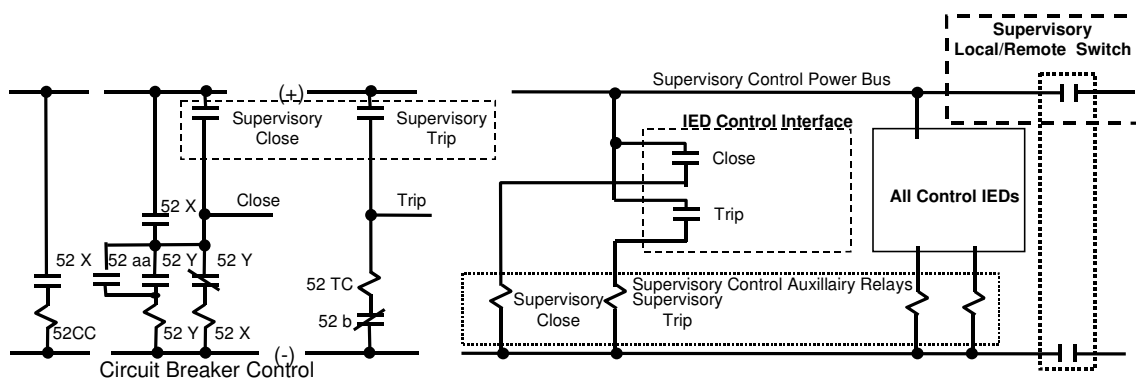
F.1 Control Disable (Local – Remote) Scheme Examples

The following are examples of the more common Local/Remote arrangements with a brief description of the features of each.

F.2 Control Power Cut-Off

This scheme uses a L/R switch to remove power from all IED contactors 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 points in local/remote.

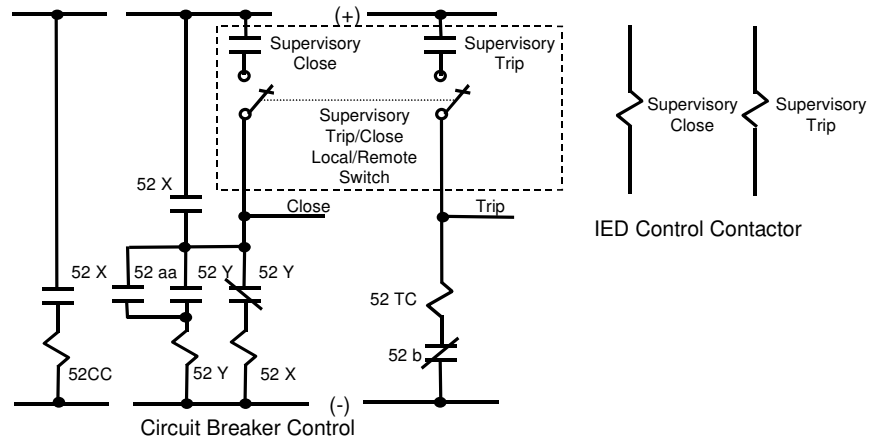
Figure F.1— Control Power Cutoff Local Remote Switch Interrupts Power to All IED Controls



F.3 Individual IED Interface Cut-Off

This scheme uses a L/R switch to interrupt the output of the IED contactors 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.

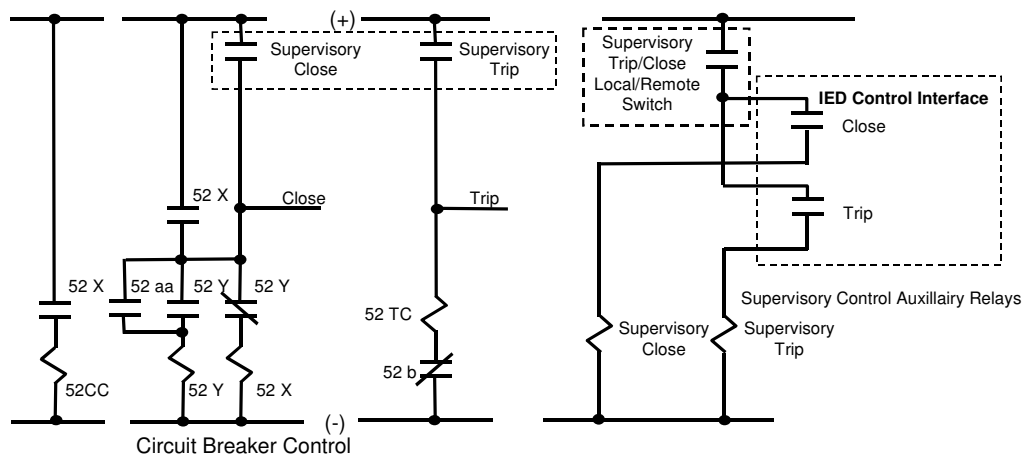
Figure F.2— Apparatus Local/Remote Local Remote Switch Interrupts Individual IED Control



F.4 IED Interposing Power Cut-Off

A number of IEDs do not have contact outputs rated for direct coil operation, and interposing relays are utilized. In such cases, a L/R 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 has the advantage that the L/R 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 F.3— IED Interposing Relay Coil Cutoff



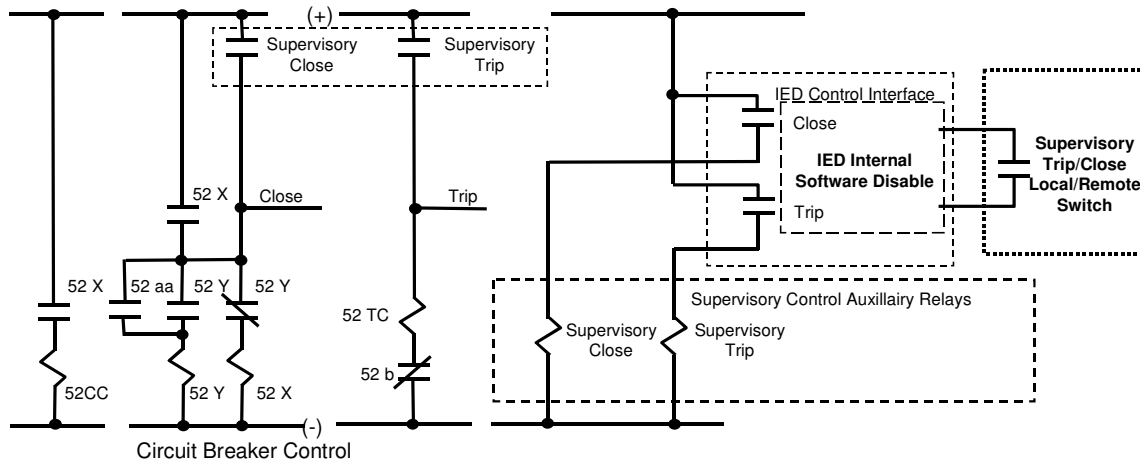
F.5 IED Logic Input

This scheme uses a L/R switch to provide a digital input to the IED. This input is interpreted by the IED as a L/R 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 L/R 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 L/R for any or all control outputs in the station connected to the Data Concentrator.

A potential disadvantage of this scheme is that is internal to the IED; and 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 F.4— IED Logic Input Control Disable

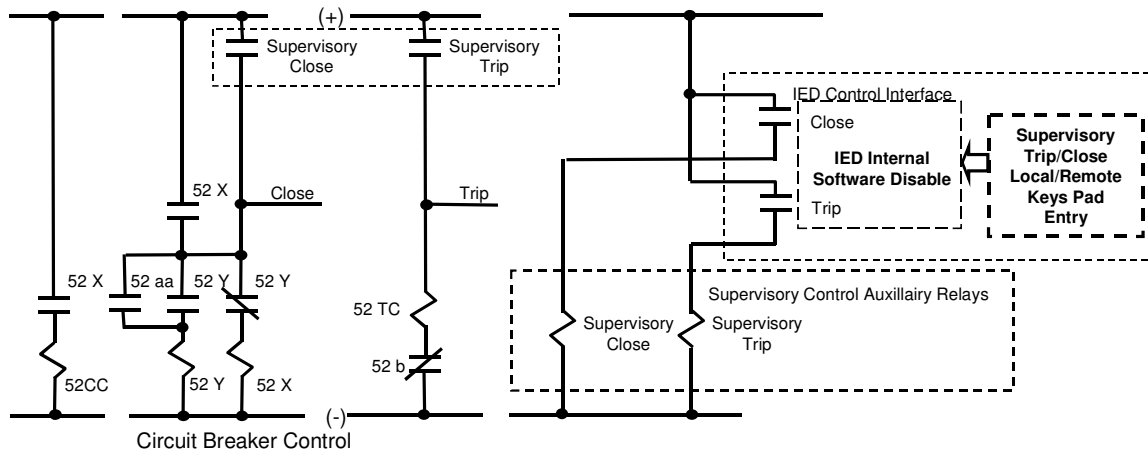


F.6 IED Software Control Disable

This scheme uses a L/R 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 SCADA/Automation operation. Depending on the IED features, the L/R logic can be set so that the non-SCADA/Automation applications can still operate the contacts. In the case of a Data Concentrator, it is possible to employ an IED logic control input L/R 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 must be taken if the L/R state is lost during IED reset.

A potential disadvantage of this scheme is that is internal to the IED; and 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 F.5—Software Input L/R



F.7 Summary

It is not uncommon for a utility to actually employ a combination of L/R philosophies to ensure the safety and reliability of the L/R feature. While older specifications frequently prohibited the use of software/logic to perform the L/R function, the growing proliferation of sophisticated microprocessor relays has caused a re-evaluation of these prohibitions, and software/logic L/R functionality is now being accepted. It is up to the individual user to determine if the software/logic L/R 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 G

(informative)

Communications System Security

Requirements for communication system security must be tailored to the utility's operational security policy. The security policy provides the operational guidance that dictates the level of security required; ensuring that users are properly authenticated and authorized to operate the system, that mechanisms are provided to ensure the integrity and confidentiality of the data passed over the communication networks, and the forensics needed to audit who access the system and what actions were taken. Forensics also includes the requirements for procuring an intrusion detection system.

In addition to the security policy, the utility's protection profile should be used to identify communication system counter measures that address the threats and vulnerabilities identified in the security policy.

G.1 Authentication and authorization

SCADA communication security requires strong authentication. Simple password protection, including multiple-level password protection, is probably not sufficient. Strong authentication requires that the user be authenticated by two factors, something known such as a password and something possessed such as a physical token. Smart cards or authentication keys should be required to access any IED in the substation.

G.2 Data integrity and confidentiality

Data integrity may require cryptographic mechanism to ensure that the data has not been corrupted. It is very important that a national standards body recognize the cryptographic mechanism selected. For the United States, FIPS (Federal Information Processing Standard) Publication 140-2-Annex A with some amendments is recommended for SCADA and substation automation systems.

Most SCADA communications today is over asynchronous serial communications. Affordable retrofit to add security is available using certified commercial products. There is also some SCADA communications over Internet Protocol networks today, and this trend is growing. IEEE C37.1 addresses both.

G.2.1 Cryptographic algorithms

Because all cryptographic algorithms do not serve the same purpose, IEEE C37.1 recommends that algorithms be selected from the following candidates:

- a) Encryption: 3DES, AES; bit length of 128 minimum
- b) Digital Signing: RSA (1024 bit minimum), ECDSA (160 bit minimum)
- c) Integrity hashing: SHA-1
- d) Key exchange: X9.44, IKE
- e) All signing and key exchange keys must be generated in hardware
- f) All long-use encryption keys must be escrowed
- g) All secure cryptographic functions require multiple operators

G.2.2 Cryptographic security modules

SCADA cryptographic security modules must comply with FIPS 140-2 (or 140-1) Level 1 or higher, and must be validated by a CMVP(Cryptographic Module Verification Program) Partner. Validation requires the following:

- a) A demonstration that shows tamper evidence
- b) Assurance that key materials are properly handled
- c) The capability to handle multiple levels of user authentication

SCADA security requires modules that provide onboard key generation with bit lengths of at least 1024 bits. Dual serial ports are needed for communications and a trusted path for local maintenance.

G.2.3 Data integrity over IP networks

SCADA and substation automated systems operating over IP networks should use IPSec. IPSec may be implemented in substation IEDs or on security gateways such as routers and firewalls. This is typically done by directly modifying the IP stack to support IPSec natively. When access to the IP stack is not possible, the functional equivalent of IPSec shall be implemented as a “Bump in the Stack” (BITS) or “Bump in the Wire” (BITW). The former is typically a shim that extracts and inserts packets from the IP stack. The latter is typically an external, dedicated crypto device that may be independently addressable.

G.2.3.1 Security association

To properly encapsulate and decapsulate IPSec packets a Security Association (SA) shall be implemented to associate security services and a key, with the traffic to be protected, and the remote peer with whom IPSec traffic is being exchanged. SA is unidirectional. It defines security services for one direction, either inbound for packets received by a substation IED, or outbound, for packets that are secured and sent by the substation IED. They shall be identified by a Security Parameter Index (SPI), which exists in IPSec protocol headers, the IPSec value, and the destination address to which the SA applies (which dictates the direction).

SAs generated manually or dynamically shall reside in the Security Association Database (SADB).

- a) When generated manually, an SA shall have no lifetime. It exists until it is manually deleted.
- b) When created dynamically, an SA may have a lifetime associated with it. This lifetime shall be negotiated between the IPSec peers by the key management protocol.

G.2.3.2 IP security policy

The IPSec architecture defines the granularity by which a user defines security policy. This allows for certain traffic to be identified coarsely and have one level of security applied while allowing other traffic to be identified more finely and have a completely different level of security applied.

IPSec policy shall be maintained in a Security Policy Database (SPD). Each entry of the SPD shall define the traffic to be protected, how to protect it, and with whom the protection is shared.

For each packet entering or leaving the IP stack, the SPD shall be consulted for the possible application of security. An SPD entry shall define three actions to take upon traffic match.

- 1) Discard: do not let this packet in or out.
- 2) Bypass: do not apply security services to an outbound packet and do not expect security on and inbound packet.

- 3) **Apply:** apply security service on outbound packets and require inbound packets to have security services apply. SPD entries that define an action of “apply” shall point to an SA or bundle of SAs to apply to the packets.

Selectors that identify some component of traffic and may be either coarse or fine shall map IPSec traffic to IPSec policy. IPSec selectors are: destination IP address, source IP address, name, upper-layer protocol, source and destination ports, and a data sensitivity level (if IPSec provides for flow security).

The values of these selectors shall be specific entities, ranges, or “opaque”. A selector in a policy specification may be opaque because that information may not be available to the system at that time. Opaque shall be used as a wild card, indicating the selector applies to any value.

If an SPD entry defines apply as an action and does not point to any existing SAs in the SADB, those SAs shall be created before any traffic may pass. If this rule is for inbound traffic and the SA does not exist, the IPSec Architecture requires the packets to be dropped; if this rule is for outbound traffic the SAs shall be created dynamically using the Internet Key Exchange (IKE).

G.2.3.3 Internet key exchange

Security associations shall be used with IPSec to define the processing done on a specific IP packet. If there is no SA that instantiates the policy from the SPD, the Internet Key Exchange (IKE) defined in RFC2409 shall be used to establish shared security parameters and authenticated keys between IPSec peers. In addition to the IKE specification, compliant IKE requires adherence to the base Internet Security and Key Association Management Protocol (ISAKMP) specification defined in RFC2408, and the Domain of Interpretation (DOM) for IPSec defined in RFC 2407.

G.3 Forensics

SCADA and substation automation systems are components of the critical infrastructure. IEEE C37.1 recommends that high value substations integrate an intrusion detection system (IDS) to detect cyber attacks and record the information needed to legally prosecute the attacker. A fundamental tool for intrusion detection is the audit record. C37.1 recommends two plans to record the outgoing activity by users as input to IDS:

- a) **Native audit records:** Virtually all multi-user operating systems include accounting software that collects information on user activity. The advantage of using this information is that no additional collection software is needed. The disadvantage is that the native audit records may not contain the needed information or may not contain it in a convenient form.
- b) **Detection-specific audit records:** A collection facility can be implemented that generates audit records containing only that information required by IDS. One advantage of such an approach is that it could be made vendor independent and ported to a variety of systems. The disadvantage is the extra overhead involved in having, in effect, two accounting packages running on a machine.

Procurement needs to incorporate the requirements derived from the utility’s firewall filtering policy into the intrusion detection filters for operation’s SCADA and substation automation networks.

C37.1 recommends a “deny-everything-not-specifically-allowed” for this network. The deny-everything policy makes intrusion detection easy: Just set an alarm for violations.

Annex H

(informative)

Database, Database Server

There are many places where data for an Automation System may reside within and external to the substation. Data is the result of measurements, calculations and monitoring by IEDs. Access to and distribution of this data is the function of the database and database server.

H.1 IED database

IEDs make measurements and monitor inputs from substation equipment as data for executing their respective functions. They 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 software version. The IED supplier provides the definition of this information.

H.1.1 Real-time values

The IED has a set of values, which are updated with a periodicity that is typically 0.1 to 10.0 seconds. 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”. As the IED updates its real time data set it replaces the previous values. These values may be accessible via a display provided in the IED. The communication port(s) will deliver its most recent set of real time values on request or as programmed for automatic delivery.

H.1.2 Calculated values

IEDs may have a set of values that are calculated from its real time measurements. They are periodically updated based on the IED's real time update cycle. These 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.

H.1.3 Retained Values

IEDs may retain a set of real-time and calculated values captured at specific time. The time may be pre-specified (time of day), a programmed interval (e.g., every 5 minutes), or event triggered (e.g., device position change). IEDs often provide the data set with a time tag based on its internal clock. For precise timing, some IEDs rely on a common timing signal supplied from a time generator. The specific values retained and the number of entries retained is IED specific and may be user programmable. IEDs have different strategies for dealing with over-flow of their retained value data set, which include 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.

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 user programmable and is IED specific.

H.1.4 Captured data sets

IEDs may have a set of values which differs from the real-time and calculated values and that are 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 memory limited, thus the user must select their characteristic and provide 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.

H.1.5 IED 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 should the IED experience a power cycle or software re-start. Data stored in non-volatile memory is usually retained during a power cycle or software re-start. However, there are many different memory technologies used in IEDs for non-volatile memory. Some may require periodic replacement of their back-up power source or the memory module when the back-up power is self-contained. In some IEDs, the location of data retention (volatile or non-volatile memory) is programmable.

H.1.6 IED data access control

IEDs usually only provide minimal access control to data sets. Typically, access is protocol dependent. One suite of data sets may be accessible via a standard protocol (such as Modbus or DNP3.0) that is not access controlled; and a different suite of data sets may be accessible via an IED specific protocol. The IED specific protocol often supports access control with password and occasionally multiple passwords and authorization levels. The IED specific protocol usually supports configuration of the IED in addition to other functions.

H.2 Substation database client/server

Within the substation, an automation system may have one or more database client/servers (D-C/S). A D-C/S acquires data from IEDs as a client and provides data to users and other systems as a server. It 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. A D-C/S may consist of multiple databases each with a specific purpose. For example, A D-C/S 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 D-C/Ss may be configured with data sets to satisfy specific needs.

A D-C/S differs from a gateway or data concentrator in that it provides more than protocol translations and mapping. A D-C/S retains data for client's use at some unspecified time.

H.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 must be capable of handling large volumes of database updates that may be caused by a major upset in the substation. In the worst case, every analog and data point can change 'simultaneously' and all changes must be processed, stored, 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 D-C/S must 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" data base value should be differentiated from live values being received from IEDs.

H.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. The historical database is often relational, or uses a standard relational database such as Access or Oracle to permit easy retrieval of data.

The historical value 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, etc. 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 must provide (directly or indirectly) for manual override of database values in the event that values have been determined invalid. A "manually entered" data base value should be differentiated from live values.

H.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 to be extracted from the real-time database upon SCADA request.

H.4 Enterprise accessible database

Utilities often maintain a database for access by the enterprise. The intent of the 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 in 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 D-C/Ss 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.

H.4.1 Database tools

Because the enterprise database is an open resource for the enterprise, it is usually accessible with standard software tools, easy to use by enterprise user. These might include standard query language (SQL) support for desktop applications like Microsoft Access, Excel, Lotus and other. Some enterprise databases deliver data through web pages such that the user need only have a standard Internet browser.

H.4.1.1 Database access control

The enterprise 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 and to what sets of data. Often, there are multiple levels of access based on user need and position within the organization.

H.4.1.2 Database partitions

The enterprise 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 insure that the data will not be used inappropriately or misinterpreted by users. Selected data items may be mapped in multiple partitions to satisfy the agreed access strategy.

H.4.2 Functional requirements

The D-C/S is a key component of the automation system. It is the repository and collector of data that feeds the many utility processes. It is an interface between IEDs and users.

H.4.2.1 Storage media

Many different storage devices are available for implementing the D-C/S. 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 often precludes rotating discs, as does environment contamination.

H.4.2.2 Size requirement

The D-C/S needs to be sized according to the utility needs. The utility can estimate the D-C/S size requirements 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. D-C/Ss are typically sized 3 – 5 times larger than the initial estimate.

H.4.2.3 Expandability

The D-C/S should be configured such that it can be easily expanded with readily available hardware and software. While many D-C/Ss are implemented on hard disc drives which are continually increasing in size at diminishing cost per Mbyte, some implementations require static drives that are usually size limited. The specification writer should be careful to make expansion requirements very clear in the requirements documents.

H.4.2.4 Data back-up

The data in the D-C/S needs to be backed up based on a strategy that suits the utility. The utility must assess the consequence of lost data and take appropriate care to make recovery possible as required. Normally some data needs to be moved to a secure archive away from the substation site. The back-up process can take many forms including; tapes, high-density removable disc, shadow disc and CD-ROM's. Many utilities prefer that the back-up process occur without human presence or intervention in order to minimize visits to the substation. The D-C/S should be easy to restore such that excessive time and skill is not required to restore lost data.

H.4.2.5 Data 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 operation. 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.

H.4.2.6 Maintenance tools

The D-C/S 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 D-C/S platform and its communications. The maintenance tools need to be easy to use specific to the skill level of those performing maintenance.

H.4.2.7 Archiving cautions

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 as the medium. 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 it is lost forever. Important data should be reviewed at least every two to three years to insure 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.

H.4.3 Performance requirements

The D-C/S has varied performance requirements based on the clients serviced by the D-C/S and the utility needs.

H.4.3.1 Server requirements

The D-C/S provides data to various users inside and outside the substation. The follow requirements are provided as a guide.

H.4.3.1.1 SCADA/EMS/DMS

Where the utility control center SCADA/EMS/DMS is supplied real-time data from the D-C/S, the D-C/S must respond similar to an RTU. Real-time data should be less than 1.0 seconds old. Responses to data requests should not require more than 5.0 milliseconds from the receipt of request.

H.4.3.1.1.1 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 must wait longer to see if a command has been successful. The second is to insure that the IED responds to status changes faster than the control timeout period.

H.4.3.1.1.2 Data Timing Issues in SCADA/EMS/DMS

Section 4.8.2.6.1.1.1 refers to the ‘false’ indications that an operator might see 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.

H.4.3.1.2 Local HMI

Where the D-C/S supplies data to a local HMI in the substation, the real-time data should not be more than 1.0 second old. Data requested to populate local displays should be provided in not more than 1.0 seconds.

H.4.3.1.3 Enterprise

Data provided to enterprise users should be provided in accordance with the utility expectation. Utilities must access their needs and data transport capability to provide realistic requirements for data access speeds.

H.4.3.1.4 Local control processes

The requirements for data supplied to local control processes is closely linked to the functions of the process. The D-C/S must support the local process at a rate that fits those requirements

H.4.3.2 D-C/S requirements as a client

The D-C/S is a client to the IEDs that supply data to the D-C/S database. The communications architecture of the automation system determines the ways the D-C/S can acquire IED data and the speed for updating records.

H.4.3.2.1 Port networks

The D-C/S may be configured to have multiple ports for acquiring IED data. The ports may be simple direct EIA-RS-232 point-to-point connections to individual IEDs or a EIA-RS-485 port to multi-port arrangement with IEDs sharing a common communications bus connected to a D-C/S port. The rate at which the D-C/S can access and retrieve data from IEDs is dependent on the channel speed, the volume of data to be retrieved and processing time for the D-C/S communications processor to decode the IED protocol and store the data. The delay inherent to the IED response to a data request is also a factor. Large volumes of data on relatively slow channels can extend the time required to refresh the D-C/S database.

H.4.3.2.2 LAN Networks

The D-C/S may acquire data from IEDs using a local area network in the substation. The time to acquire data from IEDs on a network is usually shorter than using serial channels as above because the network speed is much faster. However, if the network is heavily loaded, update times may be effected. The individual IEDs may also slow the update rates based on the speed at which they can supply data from their process processor to their communications processor. Ultimately, if the IED services its data request as a secondary function update time may be substantially affected. Collision Detecting/Multiple Access (CS/MA) networks such as Ethernet are particularly sensitive to heavy traffic loads. The peak design load on such networks should never exceed 50%, with 25% or 30% peak loading being preferred.

H.4.3.3 Access security

The D-C/S must have facilities to control user access that comply with operational security policy. Normally, a user ID 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.

Annex I

(informative)

Interlocking

An Automation System 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 their 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 information from any source within the system and effect one or more functions of the system.

I.1 Logical or Sequential Interlocks

Interlocks that require equipment to be operated in particular sequence can be implemented in a number of different devices in the automations 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. Sensor 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 which represent the equipment as in a state that is ambiguous, e.g. neither fully open nor fully closed, both alarm and, if suitable, disable.

I.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 information received from messaging with the PLC to thereby enable or disable automatic reclosing.

The specifier of such a system is cautioned to assess the reliability of the component devices as well as the messaging system. Care must 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.

I.2.1 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. An implementer is cautioned to assure the quality of the measurements suits to action to be performed. Accuracy, resolution, stability and time lag are all possible sources of performance problems. Likewise, the absence of a measurement or a measurement that is out of bounds must be resolved within the interlock framework such that the result is satisfactory.

I.2.2 High Speed Interlocks

Some applications of interlock lock require high-speed response. The timing requirements of such an application must 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 becomes lost.

I.2.3 Operator Over-Ride

Implementation of interlocks requires the user recognize the possibility of missing or misleading data and program appropriate interlock logic to react accordingly. Often, an operator "over - ride" must 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 over-ride an interlock should also be logged.

I.2.4 Testing Interlocks

Once interlocks have been implemented it becomes important to assure the programmed logic is meets the desired intent. Users are advised to provide a means to view and test their interlock logic.

Annex J

(informative)

System Support Tools

This section describes software elements related to error detection, diagnostics and troubleshooting.

J.1 Software Tools

Maintenance personnel need a mechanism to easily check inputs and outputs. This includes the ability to simulate real control outputs and look directly at input values. Some systems also have numerous status messages and/or diagnostic programs.

J.2 Health Check

To enhance availability a set of software tests are built into the system to monitor the status of elements of a control system for correct internal functionality and/or operation. For the most part the results are oriented to maintenance personnel and therefore may include statistical data. The checks or tests fall into several categories:

- 1) Watch for degraded internal functions or errors that are likely to lead to serious problems in the future. [examples: monitoring free memory, free CPU cycles, check internal program or task running on a periodic basis.]
- 2) Sensor inputs for analog quantities can be checked against similar quantities from another close by source or second transducer. [If voltage, current, and MW values are all input, each of the other two can be calculated from the remaining two.
- 3) Communication link error rate
- 4) Incorrect combinations of status inputs. Incorrect in that they are states that can never be obtained if the equipment is operating correctly. [an example in powerhouse status is the main breaker which has both a normally open and normally closed status for breaker position. These two inputs must always report opposite of each other.]
- 5) 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. In addition to monitor and recovery functions, the health check may collect, maintain, and report performance statistics for selected elements.

An element of the control system can be:

- a) Any hardware component for which a device status can be determined. Examples include: each node, modems, RTUs, I/O modules, PCs, printers, and network interface devices like port servers, network switches, and routers, network links.
- 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. Examples include: statistics on communications links (message and protocol errors), reports.
- 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. Examples include: communication links, database servers, view nodes, and master stations.

Predefined recovery responses can be:

- 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.

Examples:

- 1) Master Station multi-tasking system. Tell me if a program is running and has a heartbeat.
- 2) Tell me if my view stations are alive and well.
- 3) Tell me if the remote control communication has errors (how many and what kind).
- 4) Monitor an RTU, collect statistics (master station communications timeouts, communications faults, I/O faults, etc.), and notify the operator if it fails to a predetermined level.

An RTU is considered “alive” if it is running the base operating system, is connected to the master station such that it can be detected (e.g., responds to ping requests), and is able to produce a heartbeat. A RTU is considered “well” if it can gather and report error statistics. The health check monitor will respond to requests for monitoring services and information queries (story #1). A health check monitor client will notify the health check monitor that a RTU requests monitoring services. In addition, an RTU will collect and report error statistics to the health check monitor. The health check monitor will detect the presence of the specified RTU and record if it subsequently fails the “alive and well” check after initial detection.

J.2.1 Show the present overall status of all system elements that are being monitored.

Display the present status of all monitored GDACS system elements on a user interface. The health check system may use monitored elements to display GDACS system status (i.e., may use Intellution Dynamics Workspace to graphically display the health check status). However, the health check monitor must continue to be fully functional, including failure event notification, even if the display system fails.

J.2.2 Show me network interface device statuses (port servers, hubs, switches, routers).

We need to know if a network interface device is alive and be able to display the present status on a graphical user interface. A network interface device is considered “alive” if it is connected to the GDACS operational network such that it can be detected (e.g., responds to ping requests). The health check monitor will respond to requests for monitoring services and information queries (story #1). A health check monitor client will notify the health check monitor that a network interface device requests monitoring services. The health check monitor will detect the presence of the specified network interface device and record if it subsequently fails the “alive” check after initial detection. The client will collect and report error statistics to the health check monitor. Statistics will be able to be reset by a user request. The present status of network interface devices reported by the health check monitor will be displayed on a user interface.

J.2.3 Show me the master station status including disk space, CPU utilization, RAID status, UPS status, etc.

First we need to know if a master station is alive and well. A master station is a server class PC running a standard server operating system, Intellution iFIX, GDACS, and possibly other systems such as the Oracle database server. A master station is considered “alive” if the PC is running the base operating system, is connected to the GDACS operational network such that it can be detected (e.g., responds to ping requests), and has the health check monitor running. A master station is considered “well” if it has some complement (TBD) of the GDACS software running and reporting an operational status. The master station health check monitor will collect statistics on local disk space usage, CPU utilization, RAID status, UPS status, etc. It will detect the presence of the other master stations, respond to “alive and well” check

communications with them, exchange statistics, and record if they subsequently fail an “alive and well” check after initial detection. Local device statistics will be able to be reset by a user request. The present status of the master station reported by the health check monitor will be displayed on a user interface.

J.2.4 Show a display the whole system including I/O, RTU, network links and switches, view stations, printers, master stations, communication links, and software subsystems.

Graphically display on a user interface the present status and statistics of all monitored GDACS system elements including MTL I/O, RTU, network links and switches, view stations, printers, master stations, DAGC communication links, and software subsystems. Include linked multi-page layouts, “system details”, and “system at a glance” views. The health check system may use monitored elements to display GDACS system status (i.e., may use Intellution Dynamics Workspace to graphically display the health check status). However, the health check monitor must continue to be fully functional, including failure event notification, even if the display system fails.

J.2.5 Show me performance statistics.

Add monitored element performance statistics as available.

Add smart recovery action when failure events are detected.

Annex K

(informative)

Communication Fundamentals

The IEDs of an automated substation are tied together by communications within the substation, which enables the passing of information between components. Substation communication systems also enable passing control messages between components to form integrated control systems. Communications external to the substation enable the substation IEDs to be accessed by users throughout the enterprise. The initial reason for extending communications beyond the substation was to provide basic SCADA access. By extending substation communications beyond a basic SCADA real-time connection the large amounts of data and functions available in substation IEDs can be accessed from systems of many descriptions and purposes, all to the benefit of the enterprise.

K.1 Basic Communications technology

Internal substation communications can be simple point-to-point connections between devices or complex networks shared by many devices. They can be a mix of technologies, media, protocols and methods. The specifier of an automation system needs to determine the level of networking complexity that is suitable for the proposed system, the cost and complexity of the required networks, and the support requirements for all required networks.

Devices are connected with a physical media: a pair of copper wires, coaxial cable, strands of optical fiber, or a wireless radio or microwave signal. 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. Media considerations are discussed in section 6.XXXX.

Once media pathways have been selected for connecting devices, the electrical (optical, RF) characteristic of the message scheme used over the media becomes 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 must be compatible to enable devices to communicate. For example, EIA standard EIA-RS-485 specifies a differential voltage polarity between a pair of wires to signify message logical “1”s and “0”s. It also specifies loading on the interconnecting pairs and some other important characteristics. Another way to send messages over a copper pair is to use a signal whose waveform changes according to the transmission of logic “1”s and “0”s in some manner. CCITT standard 212T specifies such a system. The media and methods may also include some communications requirements such as collision detection as in IEEE Standard 802.3. All devices connected to a media segment must 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.

Once devices have a common media and media electrical characteristics there must be a set of rules established which define how messages are structured and how they will be interchanged over the pathway. 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 complete the communications pathway. Some situations may require multiple protocols when complex message transactions take place. This is a common situation with

substation local area networks based on the Internet messaging scheme. This area of communications is often referred to as the “data link”.

Devices must know what data values are in the message and where they are placed in the data stream. This is the function of the software that assembles and disassembles the message stream at each device. These functions are related to the software application. Fundamentally, it is the applications that are trying to pass information between each other. The other elements previously discussed are necessary to get that task completed. (There are other functions that must take place when two computers interact to make up a system. These are not described here, as the focus of an automation system network is to enable the passing of information between devices in the substations rather than link two computer and their users together.)

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 (7) layers described. Section 6.0.2 further describes the layered stack concept.

Communicating beyond the substation shares many of the same requirements as communicating within the substation. 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.

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 public switched telephone network (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 Wide Area Network (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.

Network technology has a set of common standards for defining the details of the pathways. They are common knowledge to the network professional but may be foreign to the utility power professional. The common framework for describing networks is the layered communications stack introduced in the following section.

K.2 Introduction to the communications stack

To insure data exchange between functions offered by IEDs, a designer must choose a communication system topology and select a communication architecture that supports them. The communication architecture is composed of several communication protocols/standards that ensure that information will be transmitted between IEDs and functions. The designer must select a set of protocols that are layered over each other. Each layer offers a set of services to the layers above and below to enable data transmission from layer to layer. Data start at the top of the stack and is transferred from layer to layer until it reaches the bottom of the stack at which point it is transferred over the communication network media. As data is transferred from layer to layer, each layer adds its own information in the message. As shown in the following figure, some layers are responsible for data exchange between IEDs while other layers are responsible for data exchange between functions. The designer must verify the compatibility between each layer. (Appendix *** shows the application of a layered stack to a post office activity.)

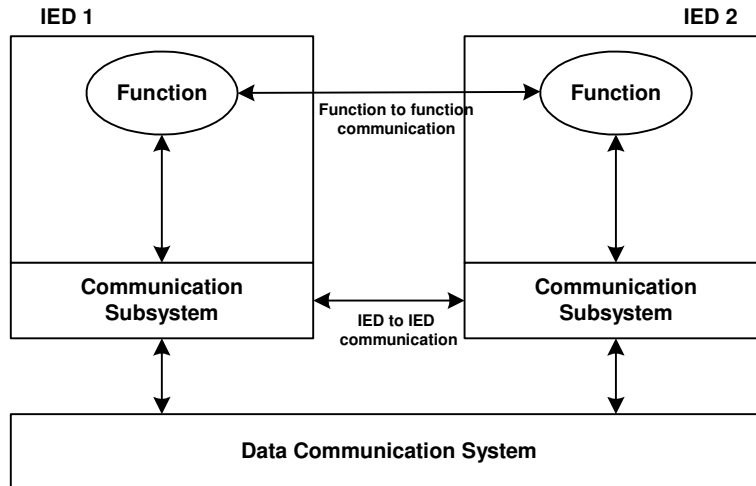


Figure K.1—Untitled

The chosen sets of protocols form a stack. For an automation system, up to 4 layers are often used. In its simplest implementation, for point-to-point communication, a two-level communication stack can be used. More complex systems may be modeled with additional layers in the stack.

Complex networks for data exchange based on networking technology often use the Internet stack as shown in Figure 6-2.

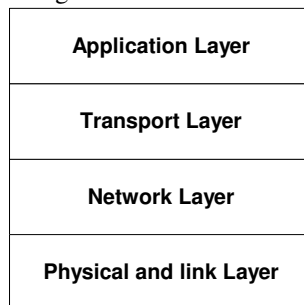


Figure 6-2

The lower layer controls 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, RS-422 for simple networks or the physical specification in IEEE 802.3 or 802.4 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 insures the correct sequence the received message.

The role of the network layer is to route messages between nodes in a way that is transparent to upper layers. It is used for network-based communication. This layer insures that the data will be transmitted from end-to-end over the network. It also handles addressing of IEDs in the network and congestion control.

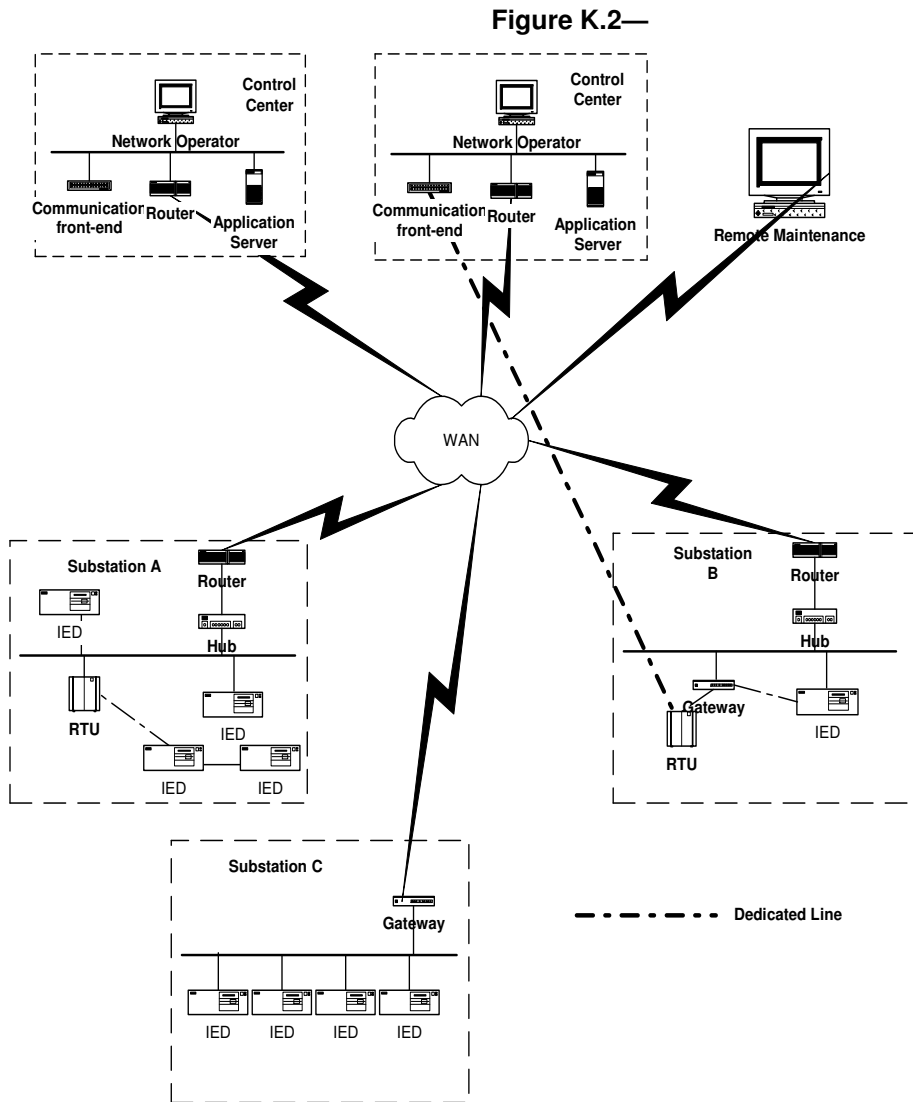
The transport layer provides a network-independent message transfer facility. It provides for making connections between messaging partners when a messaging session must be opened to connect partners or for transporting messages where a connection-less session is supported.

The fourth layer, the utility specific protocol, 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 devices. To be inter-operable, devices must understand the utility specific

protocol carried by the network messaging protocols. Example of utility specific protocols include: DNP3, Modbus, Modbus Plus, IEC 61850, and UCA-2.0. Refer to Appendix XX for a more detailed discussion of protocols.

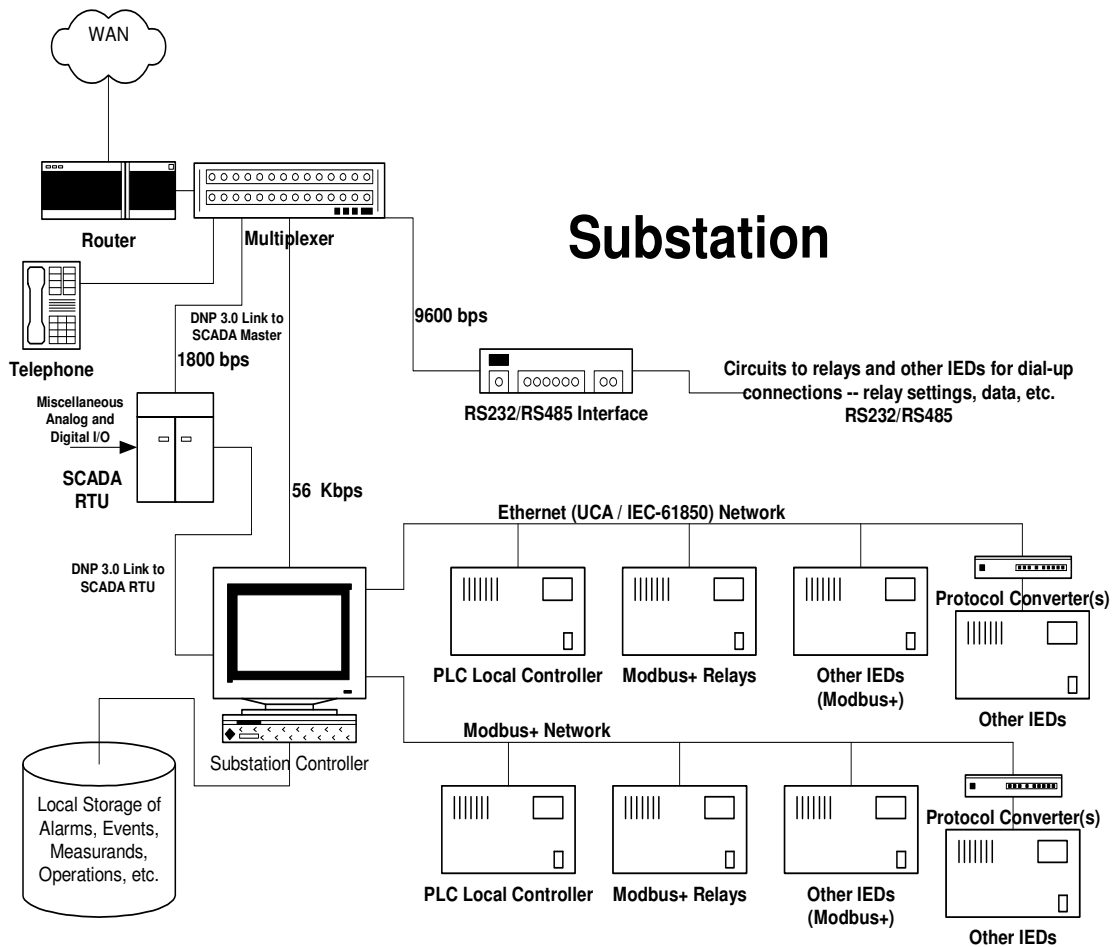
K.3 Communications Topologies

A communications system for automated substations may require many segments and links to make a complete pathway between end-points. It may involve media conversion, protocol translation, gateways and access devices.



The diagram below illustrates the network implementations at the enterprise level. The following diagram illustrates the possible complexity of a network inside a substation.

Figure K.3—Substation Automation



The communications network which connects devices within the substation may 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 automation 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. One or more of the following elements may be present in the final topology.

K.3.1 Proprietary Network

A proprietary network consists of devices connected via a media operating with a vendor specific protocol that will only interoperate with similar devices in that environment. Often proprietary networks are intended to be “stand alone”. There may be no need or desire for these devices to interoperate with others devices by virtue of their functionality. A gateway device is needed to connect this network to other portions of the substation network should such a connection be desired. Enterprise access to the proprietary network is often restricted to specific users equipped with the vendor-specific communications package.

K.3.2 Standards based serial IED Network

More IEDs are can communicate on a common communications bus by virtue of sharing a common messaging protocol such as Modbus, Modbus Plus, DNP3. There are a few other protocols that have been

implemented by some users with the help of specific suppliers. These devices may be compatible but may not interoperate. Often one device in the network can interoperate with all devices and serves as gateway.

K.4 Designing A Communications Network for Automation

The design of a communication system for substation automation includes the following steps:

- e) Define messaging system endpoints
- f) Develop the communication system topology
- g) Determine device interoperability requirements
- h) Choose the communication media
- i) Define the communication architecture
- j) Determine the protocols and physical interfaces supported by EVERY IED to be interfaced
- k) Determine the minimum protocols and physical interfaces that must be provided
- l) 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 must be chosen.

The following sections will describe each of these steps and present the different options that can be used.

K.4.1 Functional requirements

The basic functional requirement of any communications system is that it must support the various communications methods that may be required or desired. If an “all new” installation will be specified, a study should be undertaken to determine:

- 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 isolation from “ground rise”

If the communications system must incorporate 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 must include detailed descriptions of these 'pre-existing' conditions. They must 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.

K.4.1.1 Reliability

A communications systems designer cannot assume that any given stream of bits presented to the input of a communications system will be delivered without error to the output. A communications system 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 the facilities of the public telephone network 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 the designer should identify points in the network that represent a single point of failure. The assessment should include how each element (or its function) will be mitigated if its failure impedes critical functions. Designers should consider duplicating sensitive items with functional equivalents, but designers should consider using different suppliers so that a weakness in one device doesn't propagate to the redundant device. If an identified failure will impede performance, the designer should determine if that impediment will be tolerable by users or if replicating the equivalent performance is not economically justifiable.

Segregation of pathways should also be considered. The network can become vulnerable to failure if all communications passes through a single device, e.g. communications isolator, or is 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.

Communications and control systems designers should 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.

K.4.1.2 Performance

The automation system will rely on the performance of the communications links to satisfy the requirements for data and control both inside and outside of the substation. The designer needs to 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 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 stages.

K.4.1.3 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 can be accepted. 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.

K.4.1.4 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 insure 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 insure that the communications channel is highly secure. The security function is therefore applied to the protocol(s) used on the communications channel.

See Appendix XX for more information on security.

Annex L

(informative)

Communication Topologies

The topology is the physical structure of a network.

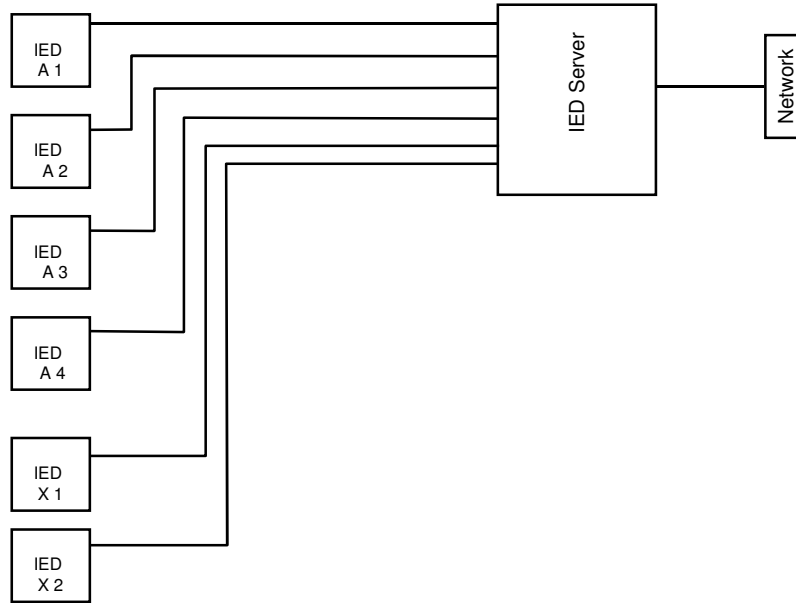
L.1 Point to point networks

A point to point connection is an individual communication channel between two IEDs. It is the simplest solution to provide data exchange between two devices. The two devices are directly connected through a communication media that can be:

- a) Copper wire (direct connection or with a modem)
- b) Fiber Optic
- c) Radio system

The communications link from an IED to the SA system may be a simple point-to-point connection where the IED connects directly to a SA controller. Many IEDs may connect point-to-point to a multi-ported controller or data concentrator that serves as the SA 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 6-x illustrates an EIA-RS-232 point-to-point connection. EIA-RS-232 does not support multiple devices on a pathway, and some IEDs do not have a protocol that supports addressing which is required for communicating on a party line. When the media is copper, EIA-RS-232 is typically used for short distances, with a limitation of about 50 feet. Most EIA-RS-232 connections are also direct device-to-device. Isolating EIA-RS-232 paths requires special hardware. Often, utilities use point-to-point optical fiber links to connect EIA-RS-232 ports together to insure isolation and allow an increased distance between devices.

Figure L.1—Point to Point IED to Server Connections



L.2 Point to multi-point networks

Many substation control systems employ point-to-multi-point connections for IEDs. IEDs that share a common protocol can usually support a “party line” communications pathway wherein they share the channel. A SA controller may use this as a “master - slave” communications bus where the SA controller controls the traffic on the channel. All devices on a common bus must be addressable and the master device must insure that only one device communicates at a time. These devices must also be set to a common baud rate. The SA controller communicates to each device one at a time so as to prevent communications collisions. “Party line” channels can also be set up to support multiple “masters” by using a control passing message from one device to another; giving the receiving device authority to take control of the channel as a “master”.

EIA EIA-RS-485 is the most common point-to-multi-point bus. It is a shielded twisted copper pair, terminated at each end of the bus with a termination resistor equal to the characteristic impedance of the bus cable. EIA-RS-485 buses support up to 32 devices on the channel. Channel length is typically 4000 feet maximum in length. The longer the bus the more likely communications errors will occur because of reflection on the transmission line therefore the longer the bus the slower it normally runs. EIA-RS-485 may run as fast as 1.0 megabits per second although most operate closer to 19.2 kbps or slower. The EIA-RS-485 bus must be linear, end to end. Stubs or taps will cause reflections. EIA-RS-485 devices are wired in a “daisy chain” arrangement. RS-422 is similar to EIA-RS-232 (Not addressable, point-to-point) except it is two pairs: one outbound and one inbound. RS-422 is intended to allow longer distances (up to about 4000 feet, as opposed to EIA-RS-232 which is 50 feet). The channel direction is turned around when each device takes control of the bus while transmitting. Figure 6-y illustrates an EIA-RS-485 communications bus.

Figure L.2—RS-485 IED Communications Bus

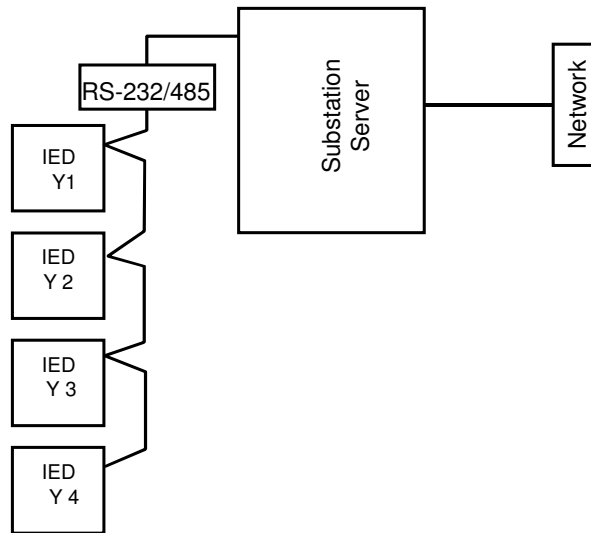
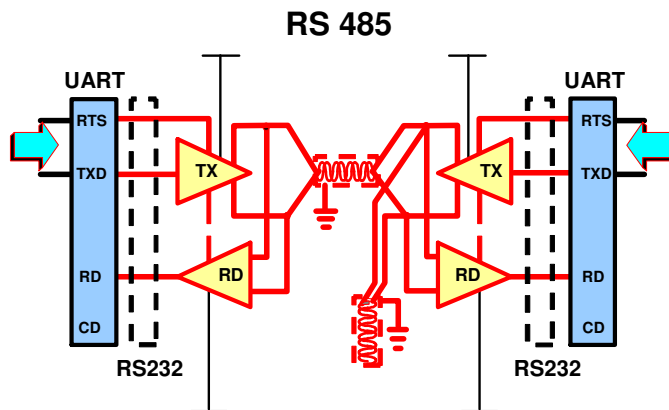


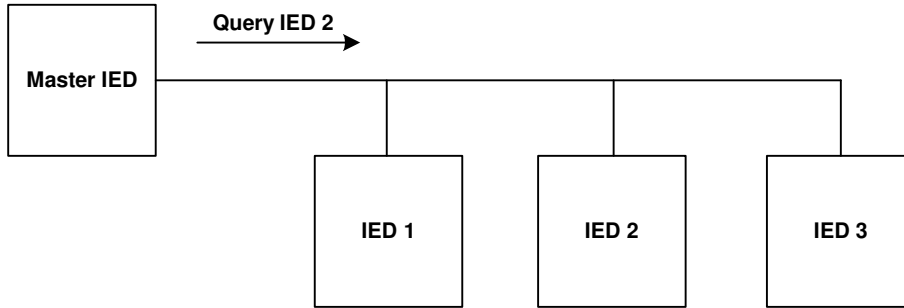
Figure L.3—Detailed EIA-RS-485 Communications Bus



In this topology, many devices are connected together on the same communication media. This communication support only one data exchange at the time and some protocol is needed to allow one device at the time to use the communication media. In multi-drop configuration, a master IED polls one IED at the time and wait for answer before polling the next device. It broadcasts a message that is received by all the devices connected to the media. Addressing information in the message indicates the intended destination device.

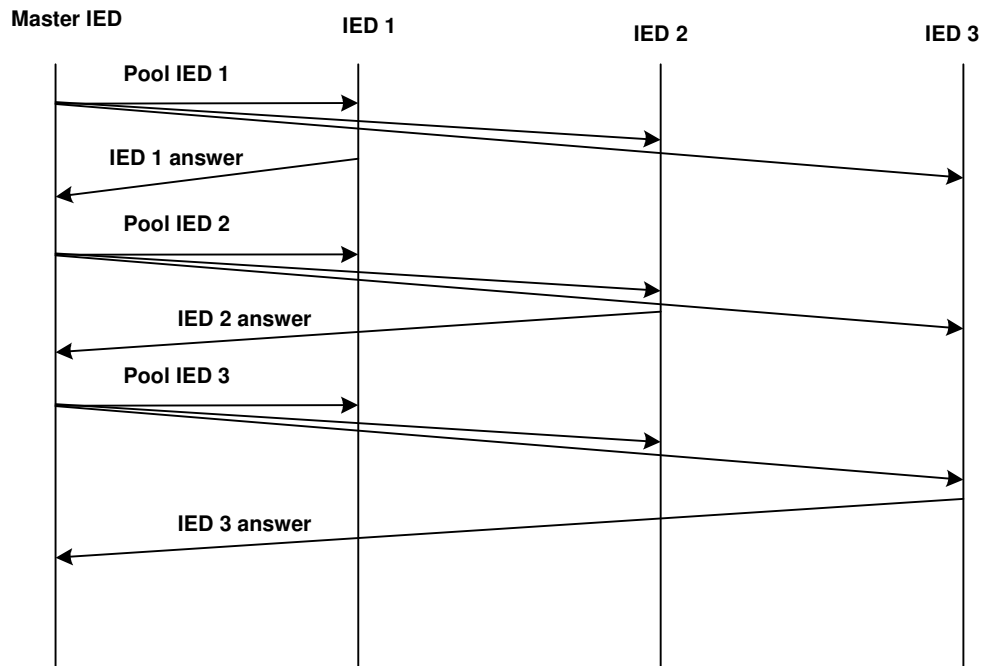
L.2.1 Access method: Centralized polling

Figure L.4—Centralized Polling



Each device has a different address that is used in data communication. As shown in the following figure, each IED always listen to the 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 L.5—Centralized Polling Scheme

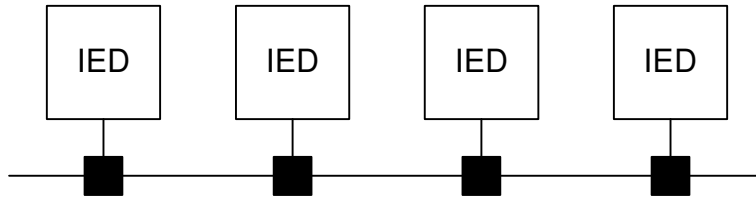


To improve reliability, a ring topology can be used in point to multi-point communication. If the loop breaks in one point, then the communication can be resumed in the other direction. In addition, some IEDs can be accessed in one direction and the others in the other direction.

L.2.2 Bus Topology

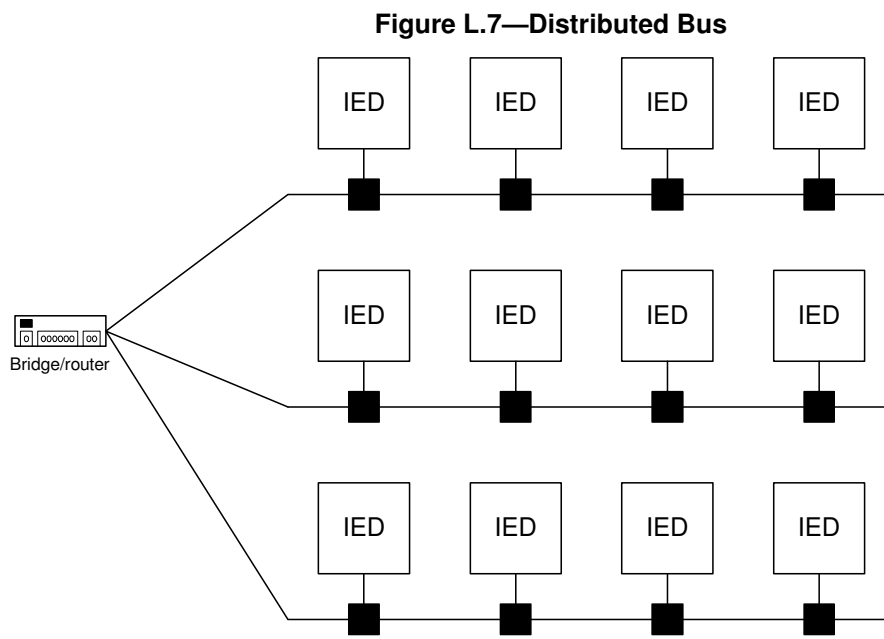
Ethernet or 802.3 is based on a bus topology. Each IED is connected to the same media. Each node or IED can thus use the LAN at the same time. The access method is a contention-based access.

Figure L.6— Bus Topology



L.2.2.1 Performance

Performance depends on the number of IEDs on a particular segment. When the number of IEDs is too large, the number of collision increases affecting then the performance. To improve the performance, the IEDs should be distributed on many segments. Routers or bridges can be used to allow data exchange between segments.



L.2.2.2 Reliability

L.2.2.2.1 Bridge

A Bridge is a device that connects two systems using the similar or identical data link layer protocols. A bridge will filter, forward, or flood an incoming frame based on the MAC (Medium Access Control) address of that frame. Bridges isolate collision domains but create only one broadcast domain.

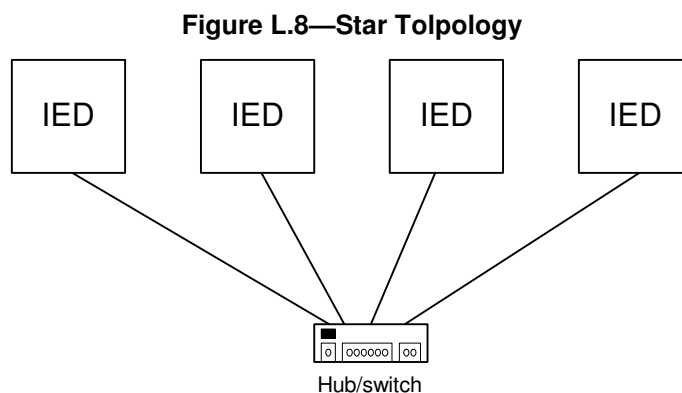
L.2.2.2.2 Router

A Router is a network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer (level 3 of OSI model) information. Occasionally called a gateway, this definition of gateway is becoming increasingly outdated.

L.2.3 Star Topology

In a star topology, each IED is connected to a special node at the center called a hub. The hub can be passive, providing a path for the message to traverse, or active regenerating the electrical signal. Hubs are now more intelligent and they are able to route the message to the port to which the targeted IED is connected.

While 10BaseT and 10BaseFO are using Ethernet type bus technology, each node or IED is directly connected to a switch or hub in a star topology. The data exchange on each segment is isolated and since separate optical fibers or twisted pair wires are used for data transmitted and received, collisions are avoided.



A LAN Switch is similar to a hub, the difference being that the switch will filter messages so that only messages to the appropriate IED are passed on. Messages to other IEDs are blocked. 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.

L.2.4 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. Each IED acts as a repeater of the signal passing a message called a token. This token may contain some data and will be emptied by the receiver. If the token contains no data, then an IED can use it and fill in the information to be transmitted to another IED.

L.2.4.1 Client-server model

This is the most popular model for network application. This model involves functions (servers) offering services to other functions (client) that can reside on the same IED or on different IEDs.

Master/slave: In this configuration, the master controls the data exchange. The slave answers only when it recognizes its address.

L.2.4.2 Peer-to-peer

In this configuration, each IED can communicate to each other in an unsolicited manner, provided that the token is present. Some mechanism is required to avoid channel overload or excessive burden to other IEDs. Note that token ring techniques are deterministic; in that the maximum token rotation time and data transfer time can be calculated. In addition, unless the ring is broken, delivery of the data in the calculated time is assured.

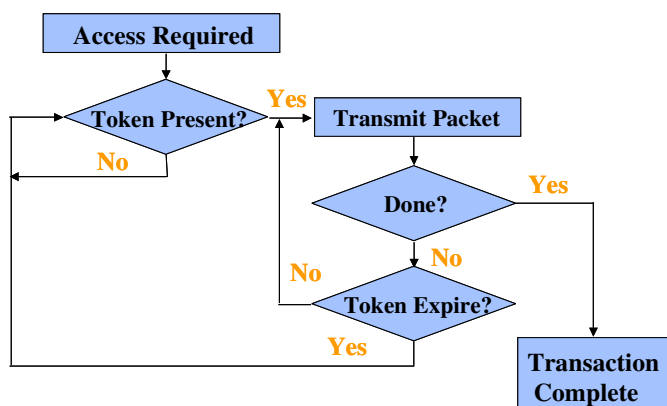
L.3 Peer to peer networks

There is a growing trend in IEDs communications to support peer-to-peer messaging. Here, each device has equal access to the communications bus and can message any other device. This is substantially different than a master - slave environment even where multiple masters are supported. A peer-to-peer network must provide a means to prevent message collisions, or to detect them and mitigate the collision.

L.3.1 Token ring

Programmable Logic Controller (PLC) communications and some other control systems use a token passing scheme to give control to devices along the bus. This is called “Token Ring”. A message is passed from device to device along the communications bus that gives the device authority to transmit messages. While the device has the “Token” it may transmit messages to any other device on the bus. Different schemes control the amount of access time each “pass” allows. These busses may be EIA-RS-485 or higher speed coaxial cable arrangements. When the “token” is lost or a device fails, the bus must restart. Therefore, “token ring” schemes must have a mechanism to recapture order. The most significant advantage of a Token Ring is that it is deterministic. That is, every device 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, completion of control sequences, etc. will benefit from this ability to calculate performance.

Figure L.9—Token Ring Access Flowchart

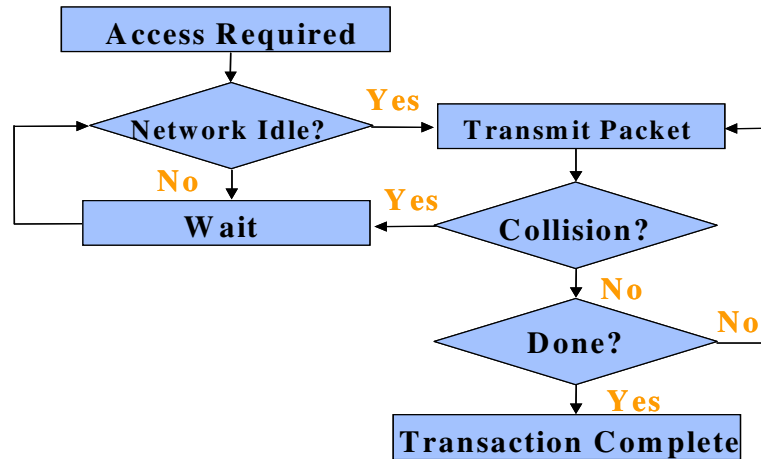


L.3.2 Ethernet (CSMA/CD)

Another way to share a common bus as peers is to use a Carrier Sense Multiple Access with Collision Detection (CSMA/CD) scheme. Ethernet, IEEE Standard 802.3, is such a scheme. Ethernet is widely used in the information technology environment and is finding its way into substations. Ethernet can be coaxial cable or twisted pair cabling. Unshielded twisted pair (UTP) cable for high-speed Ethernet, Category 5, 5E or 6 (CAT 5, 5E, 6), is widely used to wire Ethernet local area networks (LANs). Some utilities are extending their wide area networks (WAN) to substations where it becomes both an enterprise pathway and a pathway for IED and Automation. Some utilities are using local area networks (LAN) within the substation to connect IEDs together. A growing number of IEDs support Ethernet communication over LANs. Where IEDs cannot support Ethernet some suppliers offer network interface modules (NIMs) to make the transition. A number of different communications protocols are appearing on substation LANs embedded in a general purpose networking protocol such as TCP/IP. The most common protocols over networks include DNP3, Modbus, MMS (UCA2 and IEC 61850). Since messages can be delayed by collision mitigation, determination of the time required for a message to pass from device A to device B is a statistical concept which takes into account the network utilization (i.e., bits-per-second loading). In other words, the communications is non-deterministic. This can complicate SCADA communications where the

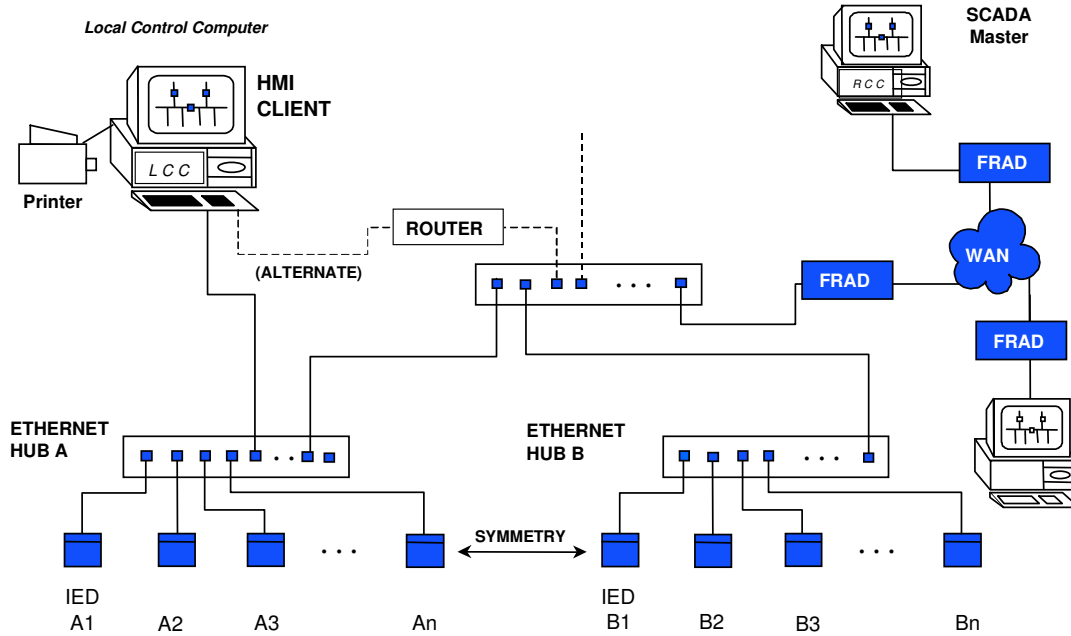
traditional messaging time is controlled by the master or communications gateway where message timing is deterministic.

Figure L.10—Ethernet (CSMA/CD) Flowchart



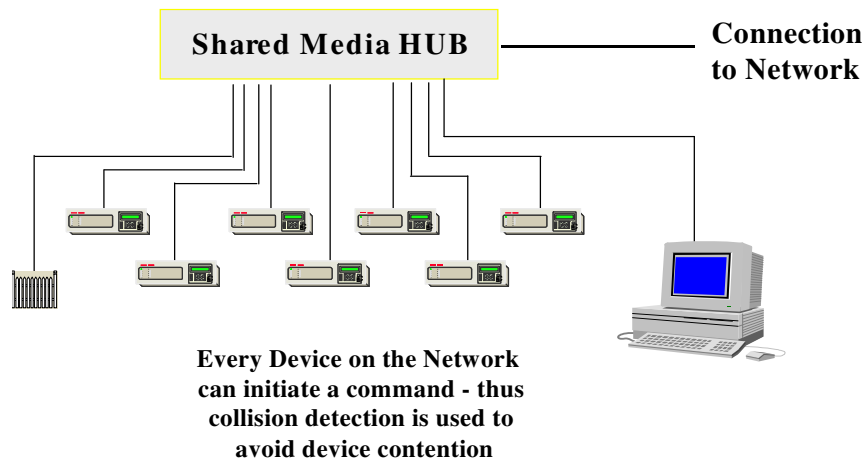
While Ethernet can be a “daisy chained” device to device network like RS-485, it is more common to connect devices to a hub or router. Each device has a “home run” connection to the hub. In the hub the outbound path of each device connects to the inbound path of all other devices connected to the hub. All devices hear a message from one device. Figure **6-w** illustrates devices connected together with a hub. Hubs can also acquire intelligence and perform a switching service. A switched hub “learns” which devices are connected to its ports and passes outbound messages only to the intended recipient. That allows more messages to pass through without busying all devices with the task of figuring out for whom the message is intended. Routers connect segments of LANs and WANs together to get messages in the right place and to provide security and access control. Hubs and routers require operating power and therefore must be provided with a high reliability power source in order to function during interruptions in the substation. It should be noted that Ethernet and similar networks are statistical. Performance can be calculated and determined to very high probability of success. However, there is no absolute guarantee. Compensation, such as multiple transmissions, verification of receipt, etc., for this fact is often built in to various protocols. The communication system provides a mechanism to transfer data between IEDs. The communication medium forms the communication path between two nodes. A node can be an IED or an intermediate communication processor such as switches, bridges or routers.

Figure L.11—Devices Connected With Shared Hubs



L.4 Multiple pathways

Figure L.12—Multiple Pathways



L.5 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 support network messaging.

C37.1 recommends network designers 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.

L.5.1 Wide Area Network (WAN)

A Wide Area Network (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 permits enterprise access to all nodes on the WAN. Normally, connections to a WAN are made through a bridge or firewall to control access to distant nodes such as substations.

L.5.2 Local Area Network

A Local Area Network (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.

L.5.3 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 interchange 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.

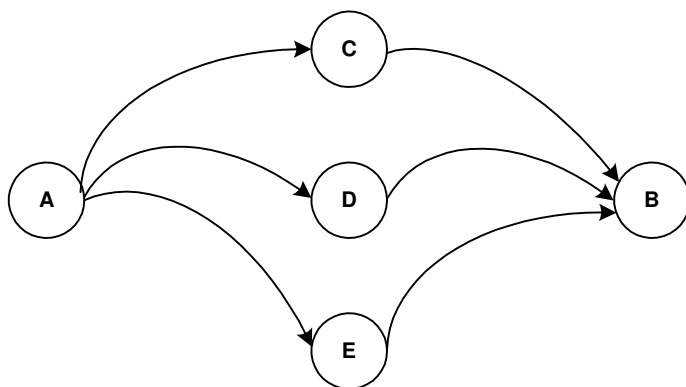
L.5.4 Segments

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 switched hub 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 a group of protective devices and another for measuring devices. Or, one segment might be configured for primary protective devices and another for back-up devices. Configuring segments is a technique to manage the risks of a LAN failure.

L.5.5 Messaging Across Multiply 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 the following figure, 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 L.13—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 must contain addressing information used to help nodes to route the message to its destination.

Annex M

(informative)

Protocols

M.1 Application (utility specific protocol)

The data communication between master station and RTU shall utilize an orderly communication protocol defined in terms of message standards. Message standards shall be defined in accordance with the general format described below. There are a number of supplier-specific and industry standard protocols available that may be suitable. The user and the supplier must agree on the protocol to be used. The following message format segments apply to both fixed and variable length message standards:

- d) The message establishment segment includes signals required to synchronize data communication equipment and address station equipment.
- e) The information segment includes signals associated with point addresses, point data values, commands, and other codes that are used by station equipment.
- f) The message termination segment includes signals used for message security and end-of-message purposes by station equipment.

The order of data transmission (least or most significant bit first), the signal states (mark, center, space), and the state values (mark = 0 or 1) shall be specifically defined.

To exchange data, one station sends a message to another station, which in turn responds with an appropriate message. If an error is detected in either message, that part of the message, or the message sequence, may be repeated one or more times. A message transaction is complete when both the initial message and reply message have been received without error.

M.2 Description of communication protocol used in legacy systems.

There are many types of IEDs used in the substation including relays, RTUs, meters, equipment monitoring IEDs etc. Data from all these IEDs must be efficiently and securely communicated to designated users and software applications. Data exchange is governed by protocols.

A communications protocol can be thought of as the computer “language” used to send and receive data, alarms, set points, and commands. A protocol must be clear and unambiguous. It should be in the public domain, well documented and supported yet with no requirement to pay a royalty or user fee. Not all protocols have the same capabilities. C37.1 recognizes several that are in common use in successful projects. They include: one of two protocols in IEEE Standard 1379 (DNP3 or IEC 60870-5-101) which is well suited to monitoring devices and systems, Modbus and Modbus Plus which are widely used in the PLC and process environment, and IEC 61850 (which incorporates much of the UCA™ 2.0 work) which is seeing application in heavily integrated systems. Each has its own strengths and limitations.

M.2.1 The Role and Requirements of a Protocol

The two recommended protocols in IEEE 1379 operate effectively in a master/slave mode. One IED (for example, a monitoring device) is the slave and another IED, typically the RTU or substation computer, is the master. The master might also be a computer at a remote site. The master requests data over the communications channel and the slave then responds by sending all requested data. Since sending full data sets can use a considerable portion of channel bandwidth in some cases, change reporting which sends only data that has changed since the last report makes more efficient use of the channel. An even more efficient

reporting method is called “unsolicited report by exception” where an IED initiates communications only when it has a change or event to report. The recommended protocols have the capability of requesting all data, specified subsets of data, or single data points with or without “report by exception”, as well as “unsolicited report by exception”. IEC-61580 provides additional functions and services. It is “object oriented” and offers “self description” which can be useful. It also carries significantly more overhead.

There are many existing proprietary and “legacy” protocols in use today that serve their intended purpose efficiently. Modbus is only one example where its simplicity makes it easy to implement and configure by users. A system implementation may require these protocols be allowed to continue their role while automation overtakes them in the future.

System Designers/Specifiers should be especially careful to incorporate protocols that fit the capabilities of the communications channels over which they will run. More sophisticated protocols will probably require upgrades in communications through-put, support staff training and specialty tools for trouble shooting and analysis.

M.2.2 Additional Protocol Requirements

- g) Data integrity: Correct data transmission is required in the presence of harsh environmental conditions such as electromagnetic interference and other sources of disturbance and noise incident on the communications channel. The probability of an undetected error must be extremely low.
- h) Efficient data transfer: Short transfer times are needed particularly for event-initiated messages carried over a variety of channels (e.g., twisted pair, fiber optics, radio) that have varying bandwidth and uncertain noise and interference characteristics.
- i) Flexible data transmission: No restrictions on IED data should be imposed. The protocol shall accept and transmit a wide variety of data types and structures including large event files.
- j) Criticality and Priority: Supports varying treatment of data depending on the need for reliability or speed.
- k) Flexible polling schemes: Including standard polling, report by exception and unsolicited report by exception.
- l) Media independent: The protocol shall be able to operate over physical layers of wire, coax, radio, and fiber optic media.
- m) Addressable: The protocol shall support a large number of addresses of nodes and/or devices over a common channel. In addition, protocol messages should include both sender and recipient addresses for future peer-to-peer type messaging over a network.
- n) OSI model-compliant: The protocol shall adhere to the layer structure of the OSI model for at least layers 1, 2, and 7. Protocols adhering to this structure can more easily be implemented over standard local area networks such as Ethernet.
- o) Standards: Protocol should make maximum use of international/national standards wherever possible.

M.3 Some protocol notes

The current IEEE recommended practice for RTU to IED communications in a substation is to use either DNP3 or IEC 60870-5-101. DNP is most commonly used in North and South America, Australia, and the UK while IEC 60870-5-101 is most commonly used in Western Europe and the Middle East. IEC 61850 will see increasing acceptance in the future and IEC 61850-compliant protocols may well become the protocols of choice.

M.3.1 Distributed Network Protocol (DNP3)

The development of DNP was a comprehensive effort to achieve open, standards-based interoperability among substation computers, RTUs, IEDs and master stations (except inter-master station communications) for the electric utility industry.

DNP defines one protocol profile each for serial and for LAN applications. This maximizes compatibility and reduces complexity for the utility staff. DNP is based on the IEC 60870-5 standard with alterations needed to meet new requirements such as large file transfer.

M.3.2 IEC 60870-5 Protocol

IEC 60870-5 does not define one particular protocol profile but specifies a number of protocol options that may be provided at different layers. This can impact compatibility between different implementations. IEC 60870-5 (like DNP) is based on a three-layer Enhanced Performance Architecture (EPA) reference model for efficient implementation within RTUs, meters, relays, and other IEDs. Additionally, IEC 60870-5 defines basic application functionality for a user layer, which is situated between the OSI Application Layer and the application program. This user layer adds interoperability for such functions as clock synchronization and file transfers.

Another document included in this standard is the “101 profile document” that contains definitions specific for telecontrol applications of IEDs and RTUs. The IEEE Std 1379 specifies the use of this profile.

M.3.3 Substation LAN Protocol Development

The Electric Power Research Institute (EPRI) has been developing industry consensus on the requirements for communications within a substation – specifically for an integrated protection, control and monitoring system using LAN technology. A key objective has been to define a system that allows interoperability and peer to peer communications between substation IEDs from different manufacturers. One important difference from the two recommended protocols is that the data in the IEDs will be represented as device oriented data objects that can be discovered by a query. A very comprehensive list of these data objects has been developed, and are known as Generic Object Models for Substation and Feeder Equipment (GOMSFE). This EPRI work, referred to as UCA™ 2.0, has been turned over to Working Groups 10, 11, & 12 of IEC Technical Committee 57 as input to their development of IEC standard 61850 for this application. The intent is to use Ethernet technology with either twisted pair copper wire or fiber optic cable as the physical layer. IEC 61850 will become an adopted international standard in 2004.

In addition, work has been completed by the DNP Users Group to provide a recommended practice for the use of the DNP3 protocol over local and wide area networks using Ethernet. This work was completed in 1998 and has been implemented by multiple vendors. The Users Group is also investigating a means to support the GOMSFE models using DNP.

M.4 Protocol Characteristics (look at 1525 1379)

Table M.1—Main characteristics of mostly used communication protocols

Communication Protocol	Synchronous/Asynchronous			
DNP 3.0				
IEC 60870-5-101				
Modbus				
Etc				

Annex N

(informative)

Integrated Substation Human Machine Interface

There are many diverse users of a substation automation system. Each user often has different needs and requirements for their interface to the system or its components. Likewise, users may interface with the system at different levels. For example, one user may have an interface through an IED while another does not while yet another user may have system wide interface and another only partial interface (This last sentence needs revising).

The characteristic of a substation user interface can be dependent on the usage the interface is expected see over its life span. Most substations are not attended and therefore the HMI is only needed when there is somebody in the substation. The presentation of data through an HMI should recognize that most of the time; no one is there to see its presentation or to react to its discoveries. Note that the device that is performing the HMI function may also be performing other functions such as online, real-time, data collection and processing.

N.1 Users

The substation control and monitoring system is used by a number of different persons who perform different tasks and function within the utility. These differences form the basis for interface requirements.

N.1.1 Operations

A substation operator has the authority and responsibility for operating the equipment within the substation. Usually, equipment operation that affects the electrical network of the utility is coordinated through a central responsibility at an operation center. The operator energizes and shuts down power equipment, re-configures equipment and provides for the safety of people in the substation. The operator may also be responsible for reporting the condition of the substation and its equipment to an oversight organization at the enterprise level.

N.1.2 Engineering

The design and operating characteristics of the substation are usually the responsibility of an Engineering body. The Engineering body may be within one enterprise organizational unit or be spread across several units. For example, a utility may have a Protection Engineering group responsible for the protective functions, an Equipment Engineering group which assumes the responsibility for the power equipment and Planning Engineering group responsibly for the substation characteristics as they effect the flow of energy through the substation and network. These groups may share a common management hierarchy or be diversely distributed throughout the organization. In a small utility, they may be only a few people.

N.1.3 Technical Support

The support of the substation equipment is the responsibility of Technical Support. Technical support works under the direction of Operations and Engineering to install, test, maintain and update systems within the substations.

N.1.4 Technical Trades

The installation, modification assembly, and disassembly of substation components and structures are the responsibility of Technical Trades. Technical Trades may include a number of different crafts such as electrical, mechanic, ironworker, plumber, and others. Technical trades may be a utility workforce or contractors.

N.1.5 Switchboard Interface

An assemblage of instruments, indicators, switches and associated hardware make up a switchboard. The physical arrangement of switchboards within the substation is utility specific and suits a requirement and philosophy developed over the history of the utility. Switchboards are the mounting structure for protection and control devices and the interface point for the substation operator.

N.1.6 Traditional Operator Interface

The traditional operator interface for substation operators is a configuration of specialty switches and instruments that have evolved over decades. 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.

N.1.7 Integrated Substation Interface

The substation interface can become integrated such that many interfaces previously distributed throughout the substation, can be integrated into a single interface. Section 4.5.4 describes the requirements of such an interface. The many access points within an integrated substation control and monitoring system reached through this interface must meet the requirement of the different users, thus, some form of partitioning is required to assure only authorized users gain access to their portion of the system.

N.1.8 Access to operating and historical data available from anywhere in the network

need words here

N.2 Intelligent Electronic Device Human Interface

Most IEDs include an HMI for the user to gain access to the device and for the device to provide information to the user. The interface may take many forms, however indicating LEDs, a keypad and alphanumeric display are the most common. The display provides information specific to the IED function and the state of the process it monitors or controls. It also serves as the selection map for accessing the IED. The keypad and display provide for scroll, branching and selection for functions nested in IED menus.

N.2.1 Display Characteristics

IEDs have a number of different ways of presenting information to the user. Most IEDs include some form of display for this purpose.

N.2.1.1 General Requirements

The display should conform to the requirements of its application. For operating purposes, it should be readable at a distance of 1.0 to 1.5 M in the user specified environment. It should not be effected by high or low ambient temperatures. The character set should be unambiguous; for example, characters such as letter "O" and number "0" or letters "L" or "I" and number "1" should be clearly distinguishable to avoid confusion. Operator displays should be intuitive and use symbols and nomenclature that are common

usage to the utility (refer to IEEE symbol standard?). For example, phase designations should conform to the common usage at the utility whether it is “A, B, C” or “X, Y, Z” or “1, 2, 3”. Likewise, numeric values should be displayed in scales common to the utility, for example, engineering units, secondary units, or “meter” units. Hierarchical display structures are most common. Displays should present the most frequently needed information first with lesser-used information deeper in the page structure. In some instances, utilities should consider customizing displays or limiting access to seldom used or potentially confusing information to avoid additional burden on the operating staff.

IED displays for the sole use of Technical Support or Engineering may use smaller characters in order to provide more information per screen provided they are acceptable to the user. The use of characters with special significance may be considered in order to expand the information available to the user. Technical support displays may show important configuration data and therefore might need a means to restrict access to some pages.

(These general requirements also apply to section 4.5.4, Integrated Station Level HMI. Maybe it should be moved up one level and address both IED and station level HMIs.)

N.2.1.2 Display Power Requirements

IED displays can add to the overall power requirement of the IED from the station power source. With a proliferation of IEDs, each with a display, the power requirements can become significant. A method to limit the power consumption by the displays in the quiescent mode should be provided.

N.2.1.3 Display Lifespan

IED displays may be subject to a life span limitation under continuous use. Users are cautioned to understand the impact of display life span should they choose to use an IED display for extended periods. Some displays fade with continued use and become un-readable.

N.2.1.4 Indicating LEDs

It is common for IEDs to have LEDs which provide information to the user. These LEDs may also be part of a lighted push button or control switch. The significance of the state of the light (on, off, blinking, color change) should be clearly defined and should be consistent throughout the system. Critical indications such as the presence of power or processor reset should be obvious and intuitive. Indications of lesser importance may use more subjective indications such as flashing, flashing pattern or color change.

N.2.1.5 Graphic Panel Displays

Some IEDs have adopted graphic panel displays for user interfaces. Graphic panels can provide information in a more flexible format than alphanumeric displays. Graphic panels are capable of graphs and images that are useful to the viewer. Often, graphic panels can be programmed either by the vendor or the user to customize the presentation of information. Custom displays allow different images to be provided to different classes of users. This feature can be useful for providing operators with a standard set of data tailored to their needs while providing more complex displays such as phasor diagrams to support other users.

N.2.2 IED Keypads

IEDs are provided with keypads for navigating through the display pages and for entering configuration parameters. The size and tactile feel of keypads should be considered in light of their intended use. Keypads that are used frequently for operations should be large enough to allow operations with large fingers or gloved hands such that a pointing object such as a pencil is not needed to depress the keys. Key covers should be durable and sealed from dust and moisture. The function of the keys should be clearly

marked and intuitive. Where keypads are not needed for operations, their design should be suitable for the intended purpose.

Keypads are often used for data entry to the IED. They may provide a set of numeric keys, 0 – 9 and some special character for data entry or a set of keys to move a “cursor” across the display and to increment or decrement the display character. The user is urged to evaluate the “touch and feel” before committing to a specific IED.

N.2.3 Touch Screen Controls

N.2.4 IED Controls

IEDs may be equipped with switches, keys or buttons to control pieces of equipment through the IED interface. Such devices should be suitable for their intended purpose. They may need:

- 1) Locking or tagging details
- 2) Accidental operation deterrents such as “pull to toggle” or guard rings
- 3) Specific colors keyed to their operations such as green to “open” and red to “close”
- 4) A specific shape or configuration to meet the utility “culture”
- 5) Sized to fit a “gloved” operator.

N.3 Integrated Station Level HMI

A Human Machine Interface (HMI) may be provided that supports user access to the control and data acquisition equipment integrated in to the substation system.

N.3.1 General Characteristics

A HMI typically consists of a COTS computer (e.g. PC, industrial or server class) a COTS operating system (e.g. Microsoft Windows 2000, Linux) and a software application, which provides a series of screens for monitoring and control of substation devices. The HMI will typically provide other features, such as historical trending of data to the computer's hard drive, viewing of historical data, report generation, and configuration of substation devices.

N.3.2 Communications Interfaces

The substation HMI has communication interfaces to substation IEDs via a local IED network or to the substation controller to which the IEDs are connected. It may also have connections to a remote network accessible to the enterprise or a portion thereof. Refer to section XX for a discussion of local substation communication interfaces. Refer to section XX for a discussion of remote substation communication interfaces.

N.3.3 Control Capabilities

The HMI may provide capabilities for operator input at the user interface for controlling equipment within the substation. The control capabilities may include a combination of:

- Keys and switches (alphanumeric or function, or both)
- Cursor (mouse, trackball, or key controlled).

- Poke points (defined CRT displayed control selection points)
- Pull-down or pop-up menus
- Physical switches, meters, lights, etc.

N.3.4 HMI Control Dialog

As a minimum, control action dialog through an HMI must require two separate steps by the operator to reduce the possibility of inadvertent operations. The first step must select the field device to be controlled. A visual confirmation on the HMI must be presented giving a clear indication as to which 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. Placing a tag or information note on a device can also be defined as a control function, with the appropriate poke points in the control dialog.

The user's input to the HMI shall be processed, control action completed, and appropriate feedback displayed within in an acceptable amount of time (i.e. 1-2 seconds).

N.3.4.1 Push Buttons

When labeled function push buttons are included in control and data acquisition equipment, the labels shall be legible from a distance of approximately 1m in the user specified environment. When lighted push buttons are included, the significance of the state of the light (on, off, blinking) shall be clearly defined and shall be consistent throughout the system.

Control push buttons (e.g. raise, lower, trip, open, and close) shall be within convenient viewing distance of the information display that will be used during the control operation.

Control push buttons should be placed at a convenient height for visibility and for human operation. Buttons should never require reaching above eye level, or below the waist.

N.3.4.2 Control Feedback

The selection of a point for a user control action shall result in a visual feedback at the user interface. This positive feedback to the user shall signify that the control and data acquisition equipment is ready to accept a control action. The results of the control action (select-before-operate or direct-operate) shall be displayed only after a status change has been received from the RTU equipment.

N.3.4.3 Control Color Codes

The standard meanings for colors (e.g., CRT displays, status lights) used at the HMI to highlight the condition of apparatus monitored and controlled through control and data acquisition equipment should be defined by users to suit common usage within the utility.

The significance of colors should be consistent throughout the system.

The color status of an apparatus under operator control should only change to its new state, which may include attributes such as color and shape change, flashing, etc. after the status of the apparatus has changed.

N.3.4.4 Interactive Dialog

The activity at the HMI during operational use of control and data acquisition equipment shall be intuitive and shall be consistent throughout the system.

N.3.5 Alarms

When alarm conditions detected by control and data acquisition equipment are first interfaced to the user, both an audible (voice, tone, or bell) and visual (flashing light or symbol) annunciation shall be presented. It shall be possible to silence the audible alarm without affecting the visual annunciation. The visual indication of each alarm condition shall remain as long as the alarm condition exists.

N.3.6 HMI Activity Logs

All operator or user activity on the HMI should be entered into an operations or event log which includes the date, time, operator identification, function performed, final state.

N.3.7 HMI Hardware Option

N.3.7.1 Display options

There are many options suitable for operator displays for the HMI. These include:

- Standard LCD (If the HMI display is not in constant operation 24/7 then this may be an acceptable option.)
- Industrial LCD (This is more important for LCD's that are always on.)
- Industrial CRT
- Standard CRT

Note that CRTs can be affected by magnetic fields in a substation. This will cause color distortion and possible character distortion. CRTs should be shielded against magnetic fields and/or include degaussing facilities to restore the image to its proper appearance.

N.3.7.2 Power Supplies/Power

N.3.7.3 Processor Selection

Industrial PC vs. COTS PC vs. COTS server

N.3.7.4 Embedded Systems (e.g. QuickPanel)

N.3.7.5 Equipment Mounting

Rack Mount Equipment/Physical Size
System Components should meet

N.3.7.6 Pointing Device Options

A display based HMI usually provide the operator with a pointing device with which to interact with the displays. The following point devices may be used in a substation:

- Keyboard
- Mouse

- Trackball
- Touch Screen
- Light pen

N.4 Software Specification

A substation HMI requires software in addition to the hardware to make up a system. The following characteristics should be considered:

N.4.1 Operating System Specification

N.4.2 Licensing Issues Key control

N.4.3 I/O Server

N.4.4 DDE

N.4.5 OPC

N.4.6 HMI application Specification

N.4.6.1 I/O Point (tags) Counts

N.4.6.2 Operating Modes

N.4.6.3 Runtime versus development

N.4.6.4 Key control/licensing

N.4.6.5 I/O server compatibility with substation devices

N.4.6.6 Users Programs

N.4.6.6.1 Scripting/macro capabilities

N.4.6.6.2 Libraries

N.4.6.7 Graphics symbols

N.4.6.8 Screens

N.4.6.8.1 Hardware, Control Panel Issues

N.4.6.8.2 Digital Transducers with Displays

N.4.6.8.3 Local Manual Control Switches

N.4.6.8.4 Supervisory Cutout Switches

See previous sections

N.5 Functions

N.5.1 Maintenance Interface

N.5.1.1 Enable/Disable

N.5.1.2 Set Point Adjustments

N.5.1.3 IED configuration

N.5.1.4 HMI Display Development

N.5.2 Alarm Annunciation

N.5.2.1 Current

N.5.2.2 Historical

N.5.2.3 Alarm Acknowledgement

N.5.2.4 Searching

N.5.2.5 Sorting

N.5.3 User Action Log

N.5.3.1 Current

N.5.3.2 Historical

N.5.3.3 Searching

N.5.3.4 Sorting

N.5.4 Sequence of Events Interface

N.5.4.1 Searching

N.5.4.2 Sorting

N.5.5 Station One-lines

N.5.5.1 Station Analogs

N.5.5.2 Breaker/Recloser/MOD Status

N.5.5.3 Tap Changer Status

N.5.5.4 GIS Quality

N.5.5.5 Local Control

N.5.5.6 Breaker/Recloser/MOD Status (Trip/Close)

N.5.5.6.1 SBO

N.5.5.7 Transformer LTC Control (Raise/Lower)

N.5.5.8 Tagging, Lockout, Cutout, Remote/Local Coordination

N.6 Graphics Display

N.6.1 User-configurable

N.6.2 Adequate Resolution

N.6.3 Adequate number of screens

N.6.4 Graphics Import from drawing packages or image files

N.6.5 Animation of graphics and text

N.7 Report Generation

N.7.1 Data Logging (storage)

N.7.2 Standard database application

N.7.3 Flat file data storage

N.7.4 Trend charts

N.7.5 Network Alarming

Centralized alarm, trend and report processing-data available from anywhere in the network

N.8 System Diagrams

Single-line diagrams are a basic element of any substation HMI. The diagram presents information about the electrical connectivity of the substation and provides the initial display for performing data requests and control actions. Common elements of a single-line diagram can include the following:

- Geographical orientation of physical equipment
- Telemetered or manually-entered status data
- Remote control or manual operation
- Safety tags
- Information notes
- Telemetered or manually-entered power system data
- Color-tracing to indicate energized/de-energized status
- Voltage levels

- Location of manually or electrically operated disconnect and bypass switches

N.8.1 Protection System One-Line

The protection system one-line is usually 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. For example, the procedures to be followed when taking elements of a bus differential scheme out of service.

N.8.2 Communication system/device monitoring functions

A communications system diagram is a desired tool for monitoring and trouble-shooting the communications connectivity of the equipment in the substation. Basic communications statistics such as number of successful and unsuccessful poll attempts and control attempts on the device level, LAN statistics and LAN performance, etc. The modern substation is very dependent upon digital communications media and multiple tools should be provided to aid in trouble-shooting the network, locating failed or failing equipment and otherwise restoring the LAN to correct operation.

N.9 Client/server functions

Diagrams should be provided showing the sources and sinks for all data. The diagrams should include appropriate indications when backup devices are in use or are the source of data elements.

N.10 Log Files

Log files refer to activities taking place on the HMI system, and do not include data logging activities (see 4.5.4.xx.yy). Log files are usually divided into at least three categories although the user can specify different names or additional categories.

There is no standard assignment of the various alarms to different log files. The user should be able to assign any 'message' to any or all log files or sub-categories.

N.10.1 Alarm Logs

Alarm logs are records of all abnormal events relating to data and events being monitored by the system. Common entries include limit violations, failed commands, return to normal messages, etc. Larger systems can further refine log contents by assigning different categories to alarms, grouping by areas of responsibility, groupings by geographical or substation categories, etc.

N.10.2 Operation Logs

Operation logs comprise all activities that take place in the normal use and operation of the system. This includes at least the following elements:

- Operator entry of data, notes, etc.
- Operator commands and the results
- Operations or events relating to substation equipment, whether commanded or not.
- Operator log-on and log-off

The data recorded in each log entry must include date and time as well as all relevant information regarding the activity. For example, an operator data entry should include the original data before the entry and then

the new data value. (i.e., date—time—operator name or id—point id—old value—new value) A record of both the before and after values makes it easier to recover from mistakes.

N.10.3 System Event Logs

System event logs normally consist of all other records that are not included in the Alarm Logs or Operations Logs files.

Event logs can include abnormal hardware events, communications activities, invalid logon attempts, etc.

N.11 Availability

Availability is the ratio of operational time divided by total time. Critical applications frequently require an availability of 99.99% or better. An availability of 99.99% implies a maximum downtime slightly less than one hour per year.

The first step in specifying a system is to make a realistic determination of required availability, and the time period in which the availability requirement applies. (A rocket launch computer system must have a 100% availability, but only for the launch phase or about 10 minutes. An automobile should have an availability of 99% for an extended period, which allows about 87 hours per year of downtime for routine maintenance, etc., for as long as the automobile is owned.) The more stringent the availability requirement, the greater the cost of the system.

The following elements are some of the factors that determine the availability requirements for a HMI system:

- The substation is normally unmanned, and the HMI system is shut down when not in actual use.
- The HMI system is part of the substation automation system and is involved in the RTU function of sending data to a SCADA system.
- The required response and repair time for any substation event. (A remote distribution substation may have a standard response time of four hours, while a high-priority transmission substation may have a standard response time of less than one hour.)

If the HMI system includes an RTU function, the availability of the communications channel may be the determining factor.

Appropriate selection and application of hardware and software can usually meet availability requirements up to about 99% without requiring redundancy.

N.11.1 Redundancy

Availability requirements greater than 99% will require the use of redundancy in hardware and software.

N.11.1.1 Computer

Redundancy in the computer system implies a complete duplication of the computer hardware or selected portions of the computer system. Experience indicates that most failures in computer hardware will occur in rotating equipment (such as hard drives or cooling fans) or elements that require a high voltage for operation (such as a CRT).

N.11.1.2 Specific Hardware

Application of redundancy requirements to specific portions of the computer system can reduce costs at little or no decrease in availability. For example, the use of arrays of inexpensive disks (RAID technology) can prevent a disk failure from taking the system down. Likewise, multiple on-line CRTs provide adequate

backup for the user interface. On-line duplication of other hardware items such as network interface modules, etc., further increase availability at a modest cost penalty.

N.11.1.3 Failover Issues

Availability requirements in excess of 99.9% usually require on-line redundancy with automatic failover. The redundant computer system adds slightly more than 100% of the cost of the non-redundant system. The greatest increase in cost is associated with the additional software that is required to insure a smooth and complete automatic transition between the on-line and backup system. Such transitions require attention to the following elements:

- Transfer of periodic updates of the complete on-line database to the backup system.
- Immediate transfer of operator-entered data from the on-line system to the backup system.
- Proper handling and recovery if a failover event occurs during the execution of a control command.
- Ability to manually control failover events (such as reversion to the previous configuration after the cause of the failover has been remedied).

The availability of backup hardware and software can permit the use of manual replacement or failover actions without drastically decreasing the system's availability.

N.12 Maintenance

N.12.1 Back-up

N.12.1.1 Hardware Backup

There should be backup equipment for all hardware items. One method is to have a complete second set of equipment (i.e., a duplicate computer). The rapid changes in hardware design require that the user constantly monitor parts availability and insure that an 'adequate' supply of spares is maintained.

There can be subtle interactions between hardware, operating system software and application software. This creates a situation where two functionally equal items (such as an IBM personal computer and an HP personal computer) are not necessarily interchangeable. The user must be aware of any constraints on hardware backup and parts availability and interchangeability. Informed decisions can then be made regarding the stocking of spare parts. Note that some equipment can 'deteriorate on the shelf in that capacitors dry out, etc. Therefore, some hardware should be maintained in an energized state.

Hard drive failures can be a major problem. A spare hard drive, even if loaded with the system software, may not be adequate. Some software systems are internally coded to a specific hardware item (to prevent copying or unauthorized use of proprietary software). If this situation exists, the user will have to contact the original vendor to obtain the necessary keys or passwords to implement the transfer.

N.12.1.2 Operating system software backup

Backup copies of operating system software must be maintained. These copies should be on installation or recovery disks so that in case of necessity a complete re-installation can be performed.

N.12.1.3 Application software backup

Backup copies of application software must be maintained. These copies should be on installation or recovery disks so that in case of necessity a complete re-installation can be performed.

N.12.1.4 Operational data backup

HMI equipment is used to place tags or information notes on equipment, change alarm limits, etc. Some method of backing up and restoring this information is mandatory as there may be safety issues involved.

Some HMI systems include tools to make display and database changes on line. These tools can include the addition of additional data points, extensions to single line diagrams, etc. Specific documentation procedures should be implemented to insure that all changes could be reproduced if necessary. In addition, after any such changes a new backup software copy should be made.

N.12.2 Historical data database

Periodic copies of the historical database should be made on bulk storage media (magnetic tape, CD-ROM, etc.) so that historical data is not lost due to over-writing of old data or a disk problem.

N.12.3 Backup copy retention

It is desirable to maintain a library of backup copies that span at least 3 to 5 backups. This library will allow reversion to a previous version if that becomes necessary.

N.12.4 Disk Maintenance

Computer disks tend to become fragmented over time. Fragmentation can impact performance, and reduce the apparent available disk space. The degree of disk fragmentation should be monitored and the disk should be de-fragmented when necessary. There are also defragmentation software packages available that run in the background and automatically de-fragment the disk.

N.13 Software Issues

N.13.1 Software runtime/development

Runtime and development copies of all software should be maintained. The runtime copy is the version that is installed in the on-line system. The development copy should be installed on a backup system and used for all maintenance and development work. When changes to the development copy have been completed and tested, the development copy should be switched to be the runtime copy; and a new copy generated for additional development work. Before and after backup copies should be made any time a switch is made between runtime and development software.

N.13.1.1 Software version control

HMI software can be divided into three categories: Operating System Software, Application Software, and Operations Software (the current display, database, records, etc. software that is applicable to the current operation of the HMI). Version control records for all software modules are mandatory. These records must include compatibility (which versions inter-operate as a complete HMI system) relationships between the various modules. Whenever a backup copy of any software module is made, it should be noted in the version control document. It may be a desirable practice that whenever a backup copy of a particular module is installed, the compatible versions of all other software modules are also installed.

N.13.1.2 Vendor supplied software maintenance updates

Operating system (OS) software is normally a standard package such as Microsoft Windows, LINUX, QNX, etc which is purchased from an OS supplier. The HMI system supplier selects one of these operating systems and then adds the application software. The user normally supplies the Operations Software (database, displays, etc.) although the initial version may be generated by the HMI supplier.

Patches and updates to all three modules are issued at various times during the life of the system. Coordination of the various updates is essential. For example, any new patches or updates to the operating system must be checked to insure that they do not adversely impact the application software. In most cases the HMI supplier is the best source for such compatibility verification. The HMI system supplier should include compatibility verification in the system warranty. The user should purchase compatibility verification services after the expiration of the warranty period.

N.13.2 Physical Attributes

N.13.2.1 Readability

HMI screen readability is a function of brightness, resolution and character size. All three parameters must be specified to insure user acceptance. In general, the greater the resolution, the better the appearance of the screen. Brightness and character size are discussed in the following paragraphs.

N.13.2.2 Ambient light

HMI screens can be either CRT or flat panel technology if they are always going to be used in subdued or artificial light. Simple flat panel technology tends to 'wash out' in high ambient light or bright sunlight. The user should verify that the selected technology can be viewed in all possible lighting conditions.

N.13.2.3 Text character size

If the user is always within a 50 cm or so from the screen, a 12-point character size is generally acceptable. To accommodate personnel with eyesight problems (such as near-sightedness), a larger character size can be used. For maximum flexibility, provisions can be made for each user to select the character size that is most readable.

N.13.2.4 Viewing angle

In general, CRT-oriented display equipment provides a wider viewing angle than does flat-panel technology. Some flat-panel devices claim a very wide viewing angle; although they tend to be more expensive. If the user is normally situated in front of the screen, either technology will provide adequate viewing. However, if a user must be able to see the screen from an angle (such as when manually operating something on a panelboard), the viewing angle must be determined and an appropriate technology selected. It may be necessary to allow the HMI screen to pivot to insure adequate viewing.

N.13.2.5 Display height

HMI equipment is usually mounted semi-permanently to insure it remains in the substation. If the HMI equipment is rack-mounted, a decision must be made whether the display screens, keyboard and mouse-trackball are to be mounted at a convenient height when the user is standing or when the user is sitting. If the HMI equipment is table-mounted, the screen and data entry equipment must be placed at a convenient height to insure readability and simple data entry activities without strain. This may require a keyboard drawer or pullout to achieve the proper height.

N.13.2.6 Accessibility

HMI screens, keyboard and cursor positioning devices must be easily accessible to the user. The keyboard must be mounted at a convenient height, and can be in a pull-out drawer if desired. A horizontal surface must be provided for the use of a mouse or a trackball. Some pull-out drawers provide space for mouse movement or mounting of a trackball with appropriate buttons.

N.13.3 Touch Screen Issues

Touch screens are based on CRT or Flat Panel technology. Identification of the area being ‘touched’ is accomplished by a matrix consisting of Light-emitting diodes (LEDs) along the horizontal and vertical sides of the screen frame, and light-sensing diodes along the opposite sides. A decoding process is used to determine the x and y coordinates where the light path has been interrupted by a blocking device—usually a finger. These coordinates are then passed to the HMI software which, in turn, determines the action to take.

N.13.3.1 Advantages of Touch Screens

- Direct access, no need for mouse, trackball or light pen
- Use is intuitive
- Adapts well to menu-driven displays
- Displays tend to be large and easy to read --- mostly to correspond with the requirement for large ‘poke’ areas.

N.13.3.2 Disadvantages of Touch Screens

- Requires large “poke” area: 1 to 2 cm. square area for bare fingers, 2 to 4 cm. square when gloves are being worn
- Finger marks and dirt on screen
- Dirt build-up along edges of frame can block light path and create false input calculations
- May require a pressure-sensitive screen to initiate a location decoding sequence. That is, the x and y coordinates of a touch are calculated and passed to the HMI software only when there is a positive input from the pressure-sensing or “z” coordinate.

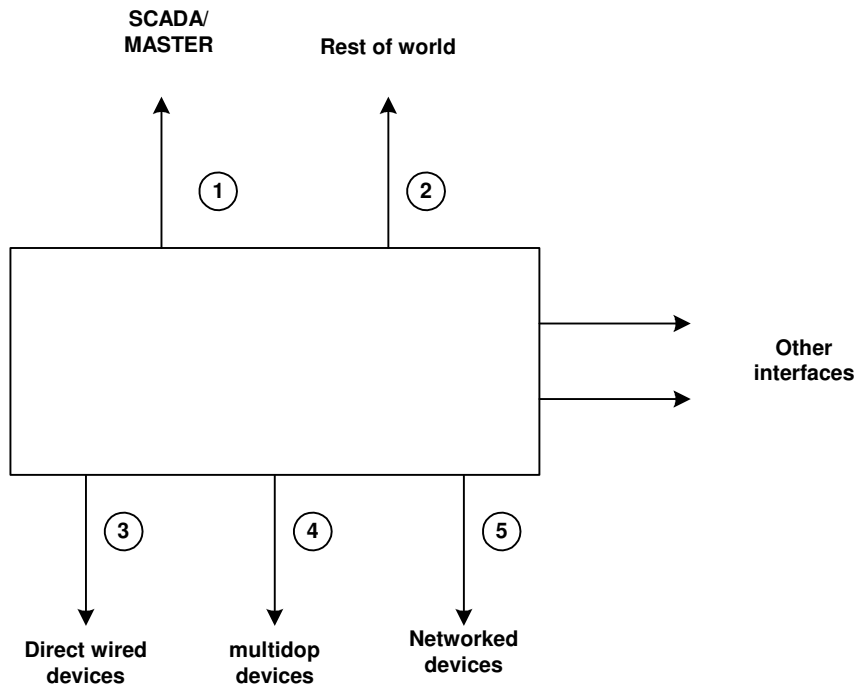
Annex O

(informative)

Integration of legacy devices in substation automation project (or modernization)

The following figure illustrates the different type of communication interface an IED may have to connect. In substation modernization, the user may face the problem of finding a way to connect a legacy device with the new IEDs. The legacy device may have communication interface that can not be connected to new devices.

Figure O.1—IED Communication Interfaces



In the preceding figure, the different possible communication interfaces are numbered. The following table identifies for each type of interface the different possibilities to be connected or adapted to other interface and some precaution.

New IEDs

	1	2	3	4	5
	The two control centers must have the same communication protocol				
			6) The two devices must have the same electrical interface (RS232, RS485). 7) The two devices must have the same communication protocols. 8) Caution in the options pertaining to the protocol	9) The legacy device must have a protocol that supports multi-drop. 10) An adapter must be added to be interfaced to the multi-drop communication link. 11) Caution in the options pertaining to the protocol	The legacy device must be connected to a gateway that will convert its protocol to a network based protocol.
Legacy Device	-	-	-	-	Are the new IEDs used unicast or multicast? What is the protocol used for transportation and networking?

Annex P Communication Protocol Profile

P.1 Network Configuration

<input type="checkbox"/>	Point-to-Point	<input type="checkbox"/>	Multipoint-Party line
<input type="checkbox"/>	Multiple Point-to-Point	<input type="checkbox"/>	Multipoint-Star
<input type="checkbox"/>	Token Ring	<input type="checkbox"/>	Star

P.2 Physical Layer

P.2.1 Point-to-point Communication

P.2.2 Transmission Speed (Control direction)

Unbalanced interchange
Circuit V.24/V.28
Standard

- | | | |
|--------------------------|------------|--------------------------|
| <input type="checkbox"/> | 100 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 200 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 300 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 600 bit/s | |
| <input type="checkbox"/> | 1200 bit/s | |

Unbalanced Interchange
Circuit V.24/V.28
Recommended if > 1200 bit/s

- | | | |
|--------------------------|------------|--------------------------|
| <input type="checkbox"/> | 2400 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 4800 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 9600 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | | <input type="checkbox"/> |
| <input type="checkbox"/> | | <input type="checkbox"/> |

Balanced interchange
Circuit X.24/X.27

- | | | | |
|--------------------------|-------------|--------------------------|-------------|
| <input type="checkbox"/> | 2400 bit/s | <input type="checkbox"/> | 56000 bit/s |
| <input type="checkbox"/> | 4800 bit/s | <input type="checkbox"/> | 64000 bit/s |
| <input type="checkbox"/> | 9600 bit/s | | |
| <input type="checkbox"/> | 19200 bit/s | | |
| <input type="checkbox"/> | 38400 bit/s | | |

P.2.3 Transmission Speed (Monitor direction)

Unbalanced interchange
Circuit V.24/V.28
Standard

- | | | |
|--------------------------|------------|--------------------------|
| <input type="checkbox"/> | 100 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 200 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 300 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 600 bit/s | |
| <input type="checkbox"/> | 1200 bit/s | |

Unbalanced Interchange
Circuit V.24/V.28
Recommended if > 1200 bit/s

- | | | |
|--------------------------|------------|--------------------------|
| <input type="checkbox"/> | 2400 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 4800 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | 9600 bit/s | <input type="checkbox"/> |
| <input type="checkbox"/> | | <input type="checkbox"/> |
| <input type="checkbox"/> | | <input type="checkbox"/> |

Balanced Interchange
Circuit X.24/X.27

- | | | | |
|--------------------------|-------------|--------------------------|-------------|
| <input type="checkbox"/> | 2400 bit/s | <input type="checkbox"/> | 56000 bit/s |
| <input type="checkbox"/> | 4800 bit/s | <input type="checkbox"/> | 64000 bit/s |
| <input type="checkbox"/> | 9600 bit/s | | |
| <input type="checkbox"/> | 19200 bit/s | | |
| <input type="checkbox"/> | 38400 bit/s | | |

P.3 Network Based Communication

- | | | | | | |
|--------------------------|---------|--------------------------|------------|--------------------------|--------------------------|
| <input type="checkbox"/> | 10BaseT | <input type="checkbox"/> | IEEE 802.3 | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | 10Base | <input type="checkbox"/> | IEEE 802.4 | <input type="checkbox"/> | <input type="checkbox"/> |

<input type="checkbox"/>		IEEE	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	802.11a	<input type="checkbox"/>
<input type="checkbox"/>			<input type="checkbox"/>

P.4 Link Layer

P.4.1 Point-to-Point Communication

<input type="checkbox"/>	Balanced Transmission	<input type="checkbox"/>	Not present (Balanced Transmission only)
<input type="checkbox"/>	Unbalanced Transmission	<input type="checkbox"/>	1 Octet
		<input type="checkbox"/>	2 Octets
<input type="checkbox"/>	Max. Length L (configurable)	<input type="checkbox"/>	Structured
		<input type="checkbox"/>	Unstructured

P.4.2 Network based Communication

<input type="checkbox"/>	IP	<input type="checkbox"/>
<input type="checkbox"/>		<input type="checkbox"/>

P.5 Transport Layer

P.5.1 Point-to-Point Communication

Not applicable

P.5.2 Network based communication

<input type="checkbox"/>	Connection oriented	<input type="checkbox"/>
<input type="checkbox"/>	Connection-less	<input type="checkbox"/>

P.6 Application Layer

P.6.1 Protocol

<input type="checkbox"/>	DNP3	UCA/61850
<input type="checkbox"/>	IEC-60870-5-101	

P.6.2 Options specific to a protocol

