TM 5-601

TECHNICAL MANUAL

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

HEADQUARTERS, DEPARTMENT OF THE ARMY
21 JANUARY 2006

REPRODUCTION AUTHORIZATION/RESTRICTIONS

Technical Manual
No. 5-601

HEADQUARTERS
DEPARTMENT OF THE ARMY
Washington, DC, 21 January 2006

APPROVED FOR PUBLIC RELEASE: DISTRIBUTION IS UNLIMITED

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) SYSTEMS FOR COMMAND, CONTROL, COMMUNICATIONS, COMPUTER, INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE (C4ISR) FACILITIES

CONTENTS

CONTENTS

CONTENTS

CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1-1. Purpose

The purpose of this publication is to provide guidance for facilities managers and engineers in selection, design, installation, commissioning, and operation and maintenance of supervisory control and data acquisition (SCADA) systems for command, control, communications, computer, intelligence, surveillance and reconnaissance (C4ISR) facilities. SCADA systems provide control and monitoring of the mechanical and electrical utility systems serving the mission critical loads. Although this technical manual (TM) is written primarily for C4ISR facilities and reflects the high reliability required for those facilities, it may also be used a reference for similar systems in other facility types.

1-2. Scope

The fundamental concepts of control systems, including industry standards and definitions are presented as an introduction to the subject. Topics covered include system architecture, network communication methods, reliability considerations, operator interfaces, and commissioning. Control system architecture review and recommended SCADA configurations for typical small, medium, and large facilities are presented. Special reliability and threat-resistance considerations governing SCADA systems are discussed. Operational issues including commissioning, maintenance practices and requirements for SCADA system documentation are also presented.

1-3. References

A complete list of references with citations is included in appendix A. Selection, design, installation, and commissioning of SCADA systems should always be based on the most current relevant edition of the standards listed in the references. Where the recommendations of this manual and the referenced standards differ, the more stringent requirement should be followed.

1-4. Currency

Because SCADA systems make extensive use of electronic technology, the technology cycle can be very short, and recommendations regarding specific types of hardware, software, communications protocols, etc. in this TM may no longer represent the state of the art several years following publication. Selection of SCADA systems should consider the advantages obtained from application of advanced technologies, but must assure that the newer technologies considered comply with the principles identified in this TM for reliability and threat-resistance and have a demonstrated history in field service adequate to assure the attainment of design reliability criteria.

CHAPTER 2
FUNDAMENTALS OF CONTROL

2-1. General control

Control consists of monitoring the state of a critical parameter, detecting when it varies from the desired state, and taking action to restore it. Control can be discrete or analog, manual or automatic, and periodic or continuous. Some terms that are commonly used in describing control systems are defined below. Additional terms are included in the glossary in appendix B:

a. The *process variable* is the parameter that is to be controlled. Examples of process variables in C4ISR systems are the temperature in a given space, the pressure produced by a cooling water pumping system, or the voltage maintained by a standby generator. To be controlled, the process variable must be capable of being measured and that measurement converted into a signal that can be acted on by the controller.

b. Devices that measure process variables are *transducers* or *sensors.* Examples are a pressure switch that closes a set of contacts when air pressure in a supply line drops below a set value, or a watt transducer that converts a measurement of the electrical power produced by a generator into a low current signal proportional to power. In many cases, the process variable sensor consists of a direct measurement device, called an *element* and a separate signal processor called a *transmitter*. An example of this would be temperature measurement using a resistive temperature detector, or RTD, as the element and a temperature transmitter, which converts the varying resistance value of the RTD into a current or voltage proportional to the temperature.

c. The *setpoint* is the desired value of the process variable, normally preset into the control system by an operator, or derived as an output of another control calculation. The *error signal* is the difference between the process variable and the setpoint, and is the basis for control action. The controller is the device that processes the error signal, determines the required control action, and provides a *control output* to the process.

d. The control output usually must act on the system through another device to effect the desired control action, such as varying the position of a valve, the speed of a motor, or the current through a heating element. The device that converts the control output into control action is the *actuator*.

2-2. Discrete control

Discrete control deals with systems in which each element can only exist in certain defined states. An example of discrete control would be starting an exhaust fan when the temperature in a space exceeds a preset value and stopping the fan when the temperature falls below a lower preset value. The temperature (process variable) is either within the acceptable range, or outside of it. The fan control relay (actuator) is either on or off. This type of control is implemented with logic diagrams and circuits. In discrete control, even though some of the parameters actually have a continuous range of values, the only information used by the control system is whether their value is greater than, less than, or equal to some desired value. A block diagram of a simple discrete control system is shown in figure 2-1. The devices used to sense system conditions in discrete control are typically electrical switches, with contacts that are open when the variable is in one state and closed when it is in the other. Similarly, the control action is typically produced by control relays, which open or close contacts in the control circuits of motors, valve actuators, or other devices.

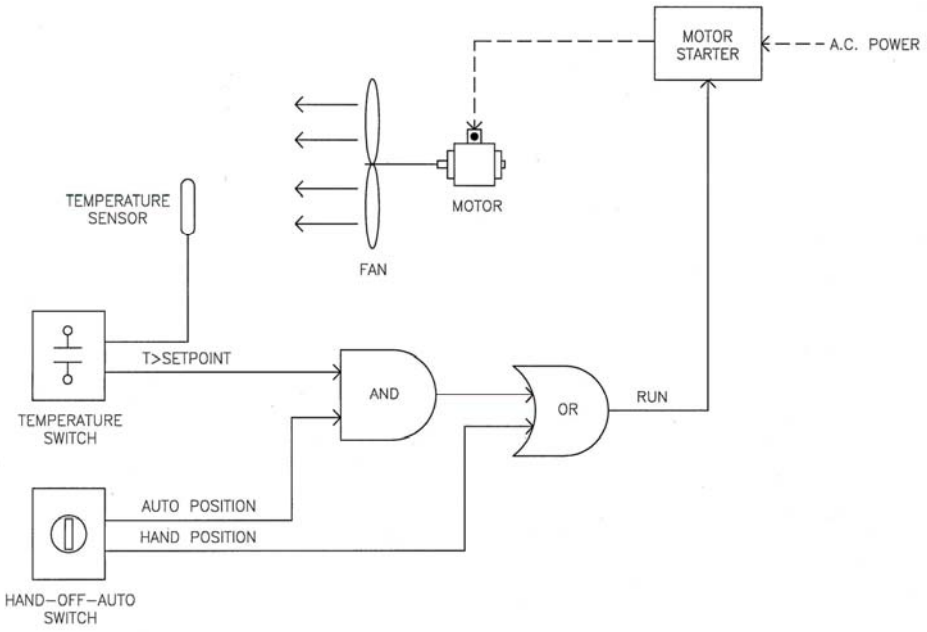


Figure 2-1. Discrete control system block diagram

2-3. Analog control

Analog control deals with systems in which variables can have a continuous range of values, rather than simply discrete states. Basic analog control consists of the process of measuring the actual output of a system, comparing it to the desired value of that output, and taking control action based on the difference to cause the output to return to the desired value. This process can be as simple as the driver of an automobile comparing the speedometer reading (process variable) to the speed limit (setpoint) and adjusting the position of the accelerator pedal (control action) to speed up or slow down the vehicle accordingly. In most systems we are concerned with, this type of control action is performed automatically by electronic processors, which receive signals from sensors, process them, and provide signals to pumps, valves, motors, or other devices to effect control action. Figure 2-2 shows a block diagram of a basic analog control system.

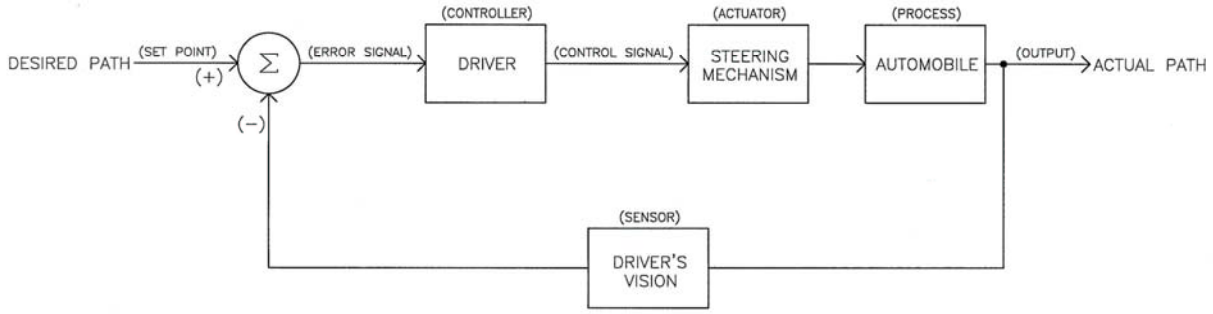


Figure 2-2. Analog control system block diagram

2-4. Classes of analog controllers

Analog controllers can be classified by the relationship between the error signal input to them and the control action they produce:

a. *Proportional* (P) controllers produce an output that is directly proportional to the error signal. A defining characteristic of P control is that the error signal must always be non-zero to produce a control action; therefore, proportional control alone cannot return the process to setpoint following an external disturbance. This non-zero error signal that is characteristic of P controllers is the *steady-state offset*. The adjustable value of the proportionality constant of a P controller is the *gain*. The higher the gain, the greater the control action for a given error signal and the faster the response. An example of a P controller is a governor on an engine-generator operating in droop mode, in which the governor opens the fuel valve proportionately to the difference between the desired revolutions per minute (RPM) setpoint and actual RPM; as load on the generator increases, RPM decreases and the governor increases the fuel flow to allow the engine to carry the additional load. Similarly, as load decreases, RPM increases and the governor responds by reducing fuel flow to match the new load condition. For any condition other than no-load, the actual RPM will be slightly different from the setpoint RPM (steady-state offset).

b. *Proportional plus Integral* (PI) controllers produce a control action that is proportional to the error signal plus the integral of the error signal. The addition of the integrator allows the controller to eliminate the steady state offset, and return the process variable to the setpoint value. The adjustable value of the integration constant of the PI controller is called the *reset*, because it has the effect of resetting the error signal to zero. An engine governor operating in isochronous mode, in which constant RPM is maintained over the full load range, uses PI control to accomplish this.

c. *Proportional plus Integral plus Derivative* (PID) controllers add a component of control action that is proportional to the derivative of the error signal, or the rate at which the error signal is changing. This mode of control allows the controller to anticipate changes in the process variable by increasing control action for rapid changes, making it useful for systems that require very fast response times, or are inherently unstable without the controller. The adjustable value of the derivative constant in a PID controller is the *rate*.

2-5. Control loops

The complete control scheme required to control a single process variable or a group of related process variables is called a control loop. The control loop includes the relevant part of the process, the process variable sensor and associated transmitter(s), the input signals, the controller, the control output signal, and the actuator. Once defined, the control loop serves as the basis for both labeling of devices and documentation of wiring and control strategy (refer to chapter 10). The process of adjusting the gain, reset, and rate parameters to obtain effective and stable response of the system to changes in the setpoint or external disturbances is called *loop tuning*, and is an essential aspect of control system startup and commissioning.

2-6. Types of controllers

Control can be implemented using either individual standalone controllers, known as *single-loop controllers*, or by combining multiple control loops into a larger controller. Single-loop controllers have provisions for a process variable input signal, a control output signal, setpoint adjustment, tuning of the PID control parameters, and typically include some type of display of the value of the process variable and the setpoint. They are compact, panel mounted devices that may be used effectively when only a small number of control loops is involved. With some exceptions, single-loop controllers are not typically used in C4ISR SCADA systems. The basic controller used in C4ISR SCADA systems should be programmable logic controllers (PLCs), which are microprocessor-based systems having provisions for multiple inputs and outputs, both discrete and analog control capability, advanced human-machine interfaces (HMIs), and network communications capability. These controllers are in more detail in chapter 3.

CHAPTER 3
SYSTEM ARCHITECTURE

3-1. General

Control system architecture can range from simple local control to highly redundant distributed control. SCADA systems, by definition, apply to facilities that are large enough that a central control system is necessary. Reliability criteria for C4ISR facilities dictate the application of redundant or distributed central control systems.

3-2. Local control

Figure 3-1 describes a system architecture in which sensors, controller, and controlled equipment are within close proximity and the scope of each controller is limited to a specific system or subsystem. Local controllers are typically capable of accepting inputs from a supervisory controller to initiate or terminate locally-controlled automatic sequences, or to adjust control setpoints, but the control action itself is determined in the local controller. Required operator interfaces and displays are also local. This provides a significant advantage for an operator troubleshooting a problem with the system, but requires the operator to move around the facility to monitor systems or respond to system contingencies. Examples of local control are the packaged control panels furnished with chillers or skid-mounted pump packages.

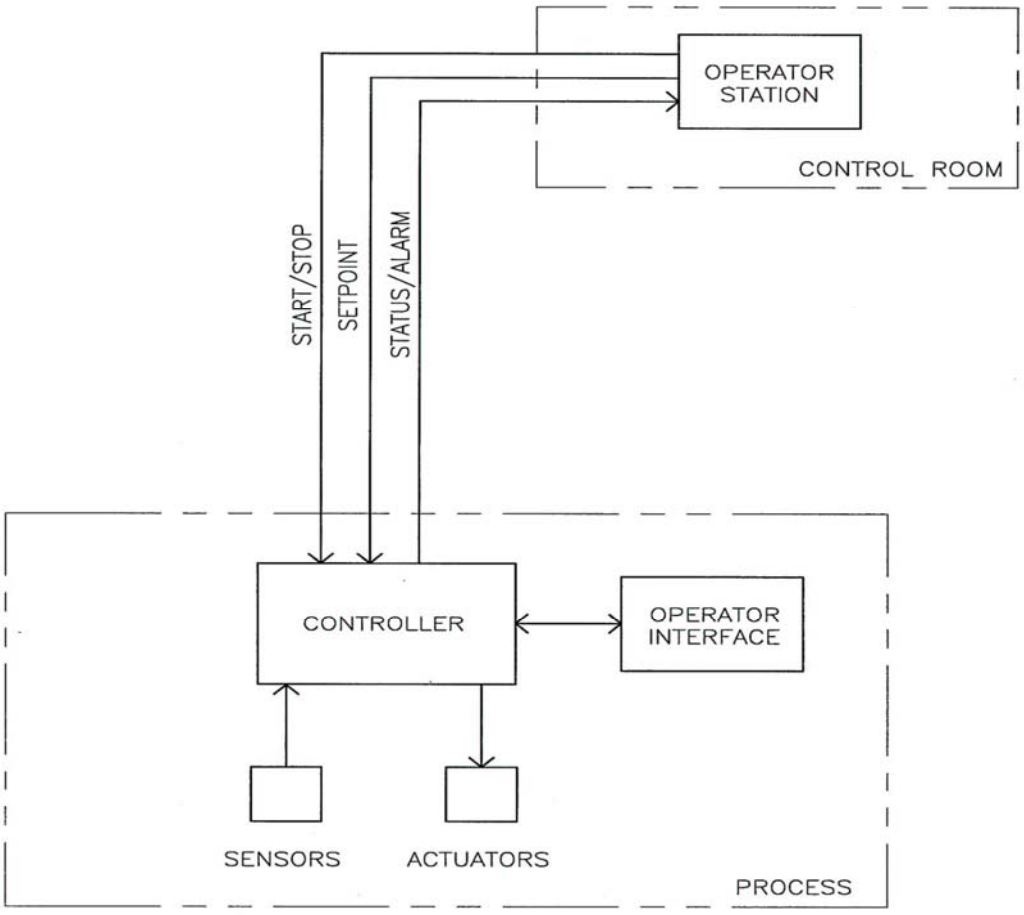


Figure 3-1. Local control system architecture

3-3. Centralized control

Centralized control describes a system in which all sensors, actuators, and other equipment within the facility are connected to a single controller or group of controllers located in a common control room. Locating all controls, operator interfaces and indicators in a single control room improves operator knowledge of system conditions and speeds response to contingencies. This type of system architecture was common for power plants and other facilities using single-loop controllers or early digital controls in the past, but it has now been largely supplanted by distributed control because of the high cost associated with routing and installing all control system wiring to a central location. Centralized control systems should only be considered for small C4ISR facilities and if used, must have fully redundant processors. Where redundancy is provided in a centralized control system segregated wiring pathways must be provided to assure that control signals to and from equipment or systems that are redundant are not subject to common failure from electrical fault, physical or environmental threats (figure 3-2).

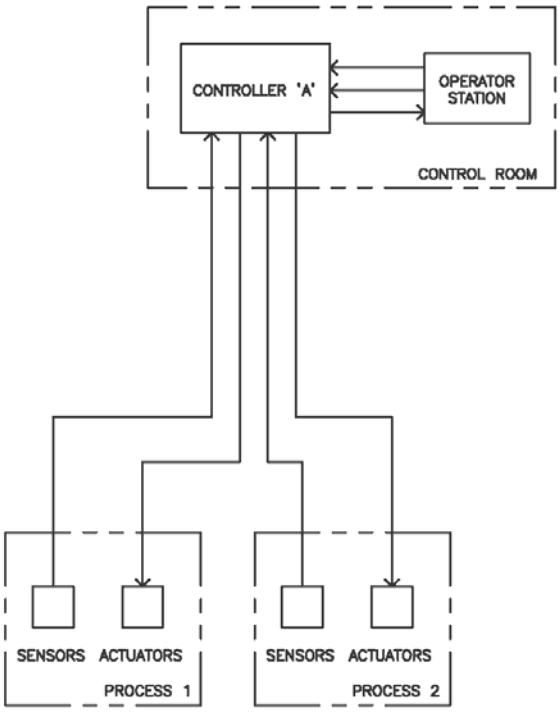


Figure 3-2. Centralized control system architecture

3-4. Distributed control

Distributed control system architecture (figure 3-3) offers the best features of both local control and centralized control. In a distributed control system, controllers are provided locally to systems or groups of equipment, but networked to one or more operator stations in a central location through a digital communication circuit. Control action for each system or subsystem takes place in the local controller, but the central operator station has complete visibility of the status of all systems and the input and output data in each controller, as well as the ability to intervene in the control logic of the local controllers if necessary.

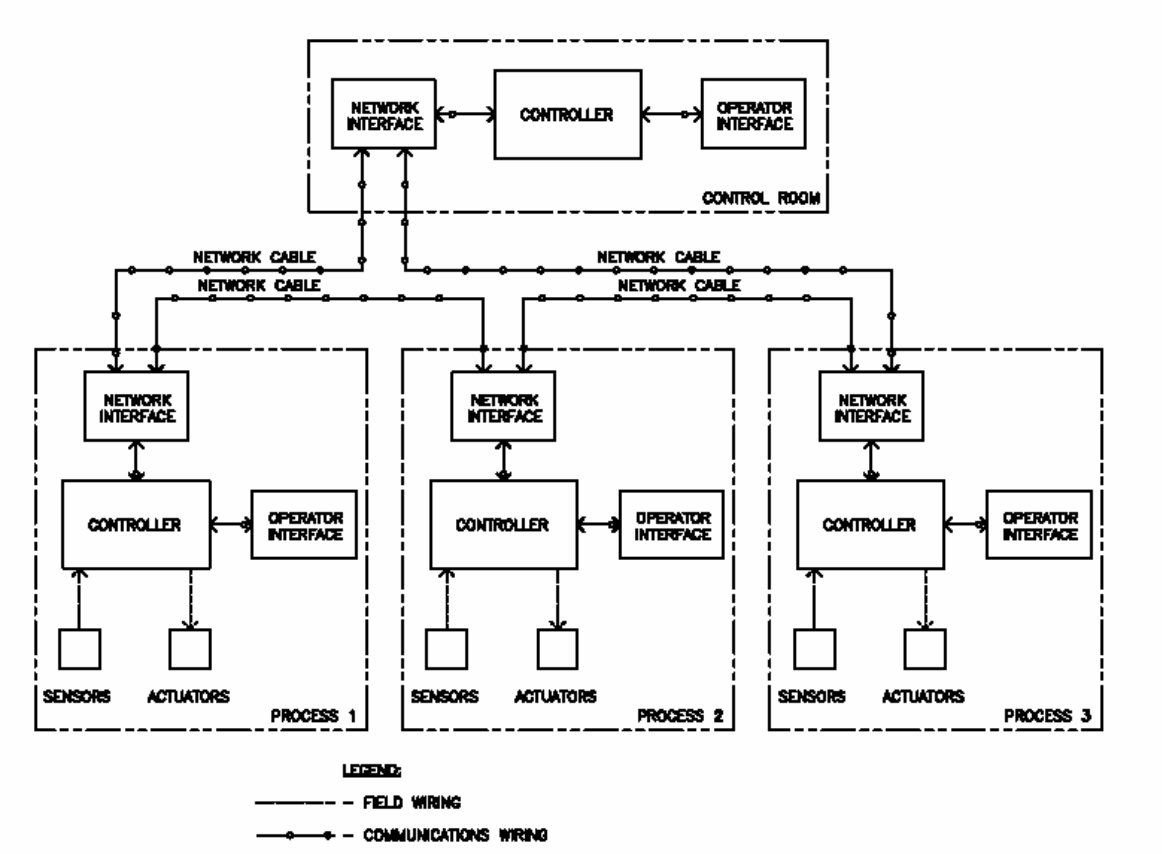


Figure 3-3. Distributed control system architecture

a. There are a number of characteristics of distributed control architecture which enhance reliability:

(1) Input and output wiring runs are short and less vulnerable to physical disruption or electromagnetic interference.

(2) A catastrophic environmental failure in one area of the facility will not affect controllers or wiring located in another area.

(3) Each local controller can function on its own upon loss of communication with the central controller.

b. There are also specific threats introduced by distributed control architecture that must be addressed in the design of the system:

(1) Networks used for communication may become electronically compromised from outside the facility.

(2) Interconnection of controllers in different locations can produce ground loop and surge voltage problems.

(3) If the central controller is provided with the ability to directly drive the output of local controllers for purposes of operator intervention, software glitches in the central controller have the potential to affect multiple local controllers, compromising system redundancy.

(4) Distributed control system architecture redundancy must mirror the redundancy designed into the mechanical and electrical systems of the facility. Where redundant mechanical or electrical systems are provided, they should be provided with dedicated controllers, such that failure of a single controller cannot affect more than one system. Equipment or systems that are common to multiple redundant subsystems or pathways, (such as generator paralleling switchgear) should be provided with redundant controllers.

3-5. Types of distributed control systems

a. Plant distributed control system (DCS): While the term DCS applies in general to any system in which controllers are distributed rather than centralized, in the power generation and petrochemical process industries it has come to refer to a specific type of control system able to execute complex analog process control algorithms at high speed, as well as provide routine monitoring, reporting and data logging functions. In most applications, the input and output modules of the system are distributed throughout the facility, but the control processors themselves are centrally located in proximity to the control room. These systems typically use proprietary hardware, software and communication protocols, requiring that both replacement parts and technical support be obtained from the original vendor.

b. Direct digital control (DDC): DDC systems are used in the commercial building heating, ventilation and air conditioning (HVAC) industry to monitor and maintain environmental conditions. They consist of local controllers connected to a network with a personal computer (PC) based central station which provides monitoring, reporting, data storage and programming capabilities. The controllers are optimized for economical HVAC system control, which generally does not require fast execution speeds. Their hardware and control software are proprietary, with either proprietary or open protocols used for network communication.

c. Remote terminal unit (RTU) based SCADA: RTU-based systems are common in the electric, gas and water distribution industries where monitoring and control must take place across large geographical distances. The RTUs were developed primarily to provide monitoring and control capability at unattended sites such as substations, metering stations, pump stations, and water towers. They communicate with a central station over telephone lines, fiber-optics, radio or microwave transmission. Monitored sites tend to be relatively small, with the RTU typically used mainly for monitoring and only limited control. Hardware and software are proprietary, with either proprietary or open protocols used for data transmission to the central station.

d. Programmable logic controller (PLC) based systems: PLCs, which are described in greater detail in the next section, can be networked together to share data as well as provide centralized monitoring and control capability. Control systems consisting of networked PLCs are supplanting both the plant DCS and the RTU-based systems in many industries. They were developed for factory automation and have traditionally excelled at high speed discrete control, but have now been provided with analog control capability as well. Hardware for these systems is proprietary, but both control software and network communication protocols are open, allowing system configuration, programming and technical support for a particular manufacturer’s equipment to be obtained from many sources.

3-6. Programmable logic controllers

The recommended controller for SCADA systems is the programmable logic controller (PLC). PLCs are general-purpose microprocessor based controllers that provide logic, timing, counting, and analog control with network communications capability.

a. PLCs are recommended for the following reasons:

(1) They were developed for the factory floor and have demonstrated high reliability and tolerance for heat, vibration, and electromagnetic interference.

(2) Their widespread market penetration means that parts are readily available and programming and technical support services are available from a large number of control system integrators.

(3) They provide high speed processing, which is important in generator and switchgear control applications.

(4) They support hot standby and triple-redundant configurations for high reliability applications.

b. A PLC consists of the required quantities of the following types of modules or *cards*, mounted on a common physical support and electrical interconnection structure known as a *rack*. A typical PLC rack configuration is shown in figure 3-4.

(1) Power supply: The power supply converts facility electrical distribution voltage, such as 120 VAC or 125 VDC to signal level voltage used by the processor and other modules.

(2) Processor: The processor module contains the microprocessor that performs control functions and computations, as well as the memory required to store the program.

(3) Input/Output (I/O): These modules provide the means of connecting the processor to the field devices.

(4) Communications: Communications modules are available for a wide range of industry-standard communication network connections. These allow digital data transfer between PLCs and to other systems within the facility. Some PLCs have communications capability built-in to the processor, rather than using separate modules.

(5) Communication Media and Protocols: The most common communication media used are copper-wire, coaxial, fiber-optics, and wireless. The most common “open” communication protocols are Ethernet, Ethernet/IP, and DeviceNet. “Open” systems generally provide “plug and play” features in which the system software automatically recognizes and communicates to any compatible device that is connected to it. Other widely accepted open protocols are Modbus, Profibus, and ControlNet.

(6) Redundancy: Many PLCs are capable of being configured for redundant operation in which one processor backs up another. This arrangement often requires the addition of a redundancy module, which provides status confirmation and control assertion between the processors. In addition, signal wiring to redundant racks is an option.

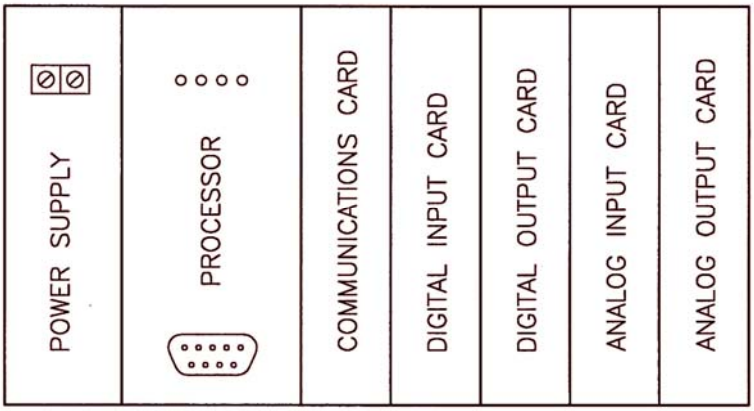


Figure 3-4. Typical PLC rack

c. All software and programming required for the PLC to operate as a standalone controller is maintained on-board in the processor. PLCs are programmed with one of the following standard programming languages:

(1) Ladder Diagrams: Used primarily for logic (Boolean) operations and is easily understood by electricians and control technicians. This is the most commonly used language in the United States and is supported by all PLC suppliers.

(2) Function Block Diagrams: Used primarily for intensive analog control (PID) operations and is available only in "high-end" PLC's. It is more commonly used outside the United States.

(3) Sequential Function Chart: Used primarily for batch control operations and is available only in "high-end" PLC's.

(4) Structured Text: Used primarily by PLC programmers with a computer language background and is supported only in "high-end" PLC's.

d. SCADA PLCs should be specified to be programmed using ladder diagrams. This language is very common, and duplicates in format traditional electrical schematics, making it largely understandable by electricians and technicians without specific PLC training. The ladder logic functions the same as equivalent hard-wired relays. The PLCs in a SCADA system will be networked to one or more central personal computer (PC) workstations, which provide the normal means of human machine interface (HMI) to the system. These PCs will be provided with Windows-based HMI software that provides a graphical user interface (GUI) to the control system in which information is presented to the operator on graphic screens that are custom-configured to match the facility systems. For example, the electrical system status may be shown on a one-line diagram graphic in which open circuit breakers are colored green, closed breakers are colored red, and voltage and current values are displayed adjacent to each bus or circuit breaker.

3-7. Redundant PLCs

Where redundant PLC Systems are required, they may utilize a warm standby, hot standby, or voting configuration. Figure 3-5 shows a typical system configuration for redundant PLCs in either warm or hot standby. Both processors have continuous access to the I/O over redundant buses or networks, and register data and status information are exchanged over a dedicated fiber optic link. In warm standby configu-

ration, the primary processor is running the program and controlling the output states. Upon failure of the primary processor, the standby processor takes over and begins to run the program. In a hot standby configuration, both processors are running continuously with their program scans synchronized over the fiber optic link. If one processor fails, the other takes control with a “bumpless” transfer in which the outputs do not change state. The hot standby configuration is recommended for most SCADA applications. For highly critical applications, a triple-redundant voting scheme, shown in figure 3-6, may be used. In this configuration three processors run continuously with synchronized scans, using either shared input data or independent input data from redundant sensors. The outputs of the processors pass through a two-out-of-three (2oo3) voter to select the control value to the process. A spare voter prevents this from becoming an opportunity for a single point of failure.

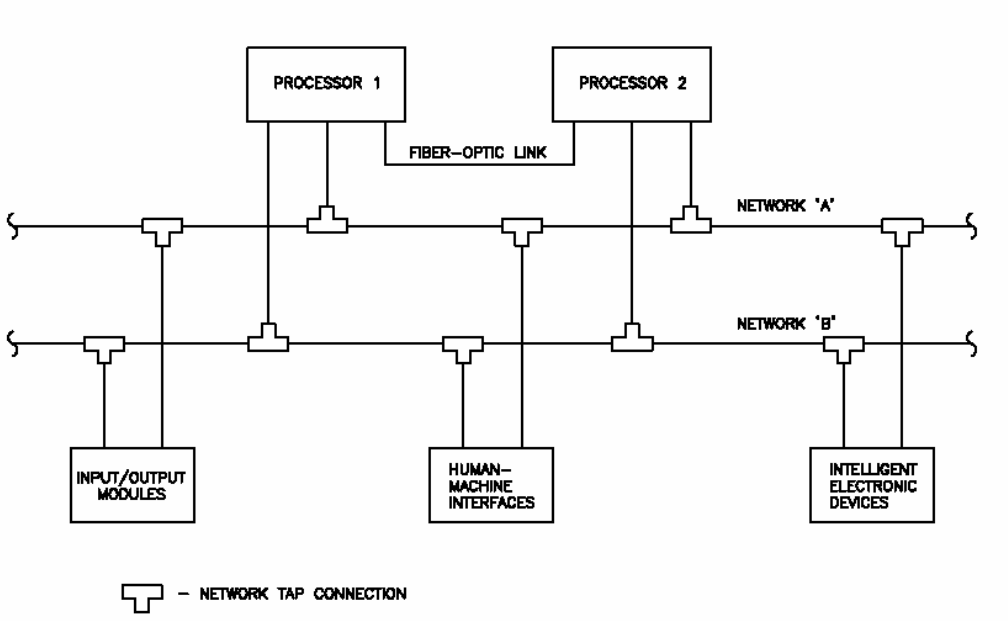


Figure 3-5. Typical redundant PLC configuration

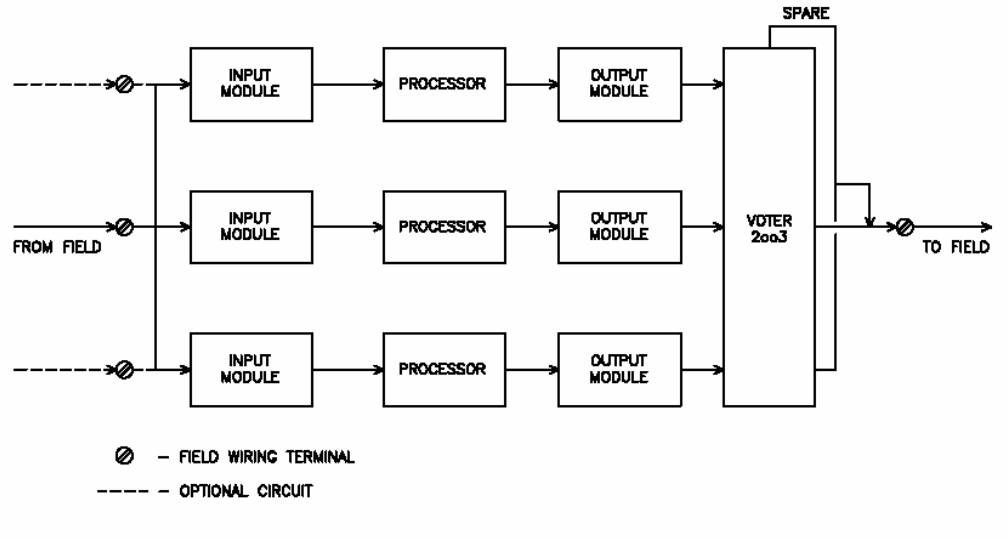


Figure 3-6. Triple-redundant PLC configuration

3-8. Safety PLCs

A recommended means of assuring that PLC hardware and software meet specified reliability criteria is through specification of PLCs that are certified for use in Safety Instrumented Systems according to IEC 61508. This standard, while intended for application to protective systems used in manufacturing, chemical, and nuclear facilities, represents the only independently verified criteria for PLC reliability and diagnostic capability. PLCs meeting the requirements of this standard must have diagnostic coverage for failure of the power supply, processor and input and output modules. They must also have been shown to provide a minimum reliability level defined in terms of probability of failure on demand (PFD), or probability of failure per hour (PFPH). Safety integrity level (SIL) target reliability indices for PLCs in low-demand operation modes (such as controlling a standby power system) are given in table 3-1. For PLCs in continuous operation (such as controlling a base load power plant), the corresponding SIL levels are given in table 3-2. These values can be used in conjunction with the reliability analysis techniques described in chapter 5 to determine the required SIL for a specific application.

Table 3-1. Safety integrity levels – low demand operation

Safety Integrity Level (SIL)	Probability of Failure on Demand (PFD)
4	$\geq 10^{-5}$ to $<10^{-4}$
3	$\geq 10^{-4}$ to $<10^{-3}$
2	$\geq 10^{-3}$ to $<10^{-2}$
1	$\geq 10^{-2}$ to $<10^{-1}$

Table 3-2. Safety integrity levels – continuous operation

Safety Integrity Level (SIL)	Probability of Failure Per Hour
4	$\geq 10^{-9}$ to $<10^{-8}$
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

3-9. Recommended configurations

Three levels of SCADA system architecture are recommended to support C4ISR facilities. These vary in configuration to correspond to the size, criticality, and amount of mechanical and electrical equipment installed in the facility as noted.

a. The small system is recommended to support a remote data and/or telephone switch site. Such a facility would generally include a single service transformer and a single standby diesel generator. Equipment inside would consist of a small rectifier for a 48 VDC bus, a small inverter, and two or more stand-alone direct-expansion cooling units. Systems for these facilities may not achieve the reliability/availability criteria specified for larger facilities. The level of SCADA system redundancy should reflect the mechanical/electrical system redundancy. See figure 3-7 for a suggested configuration.

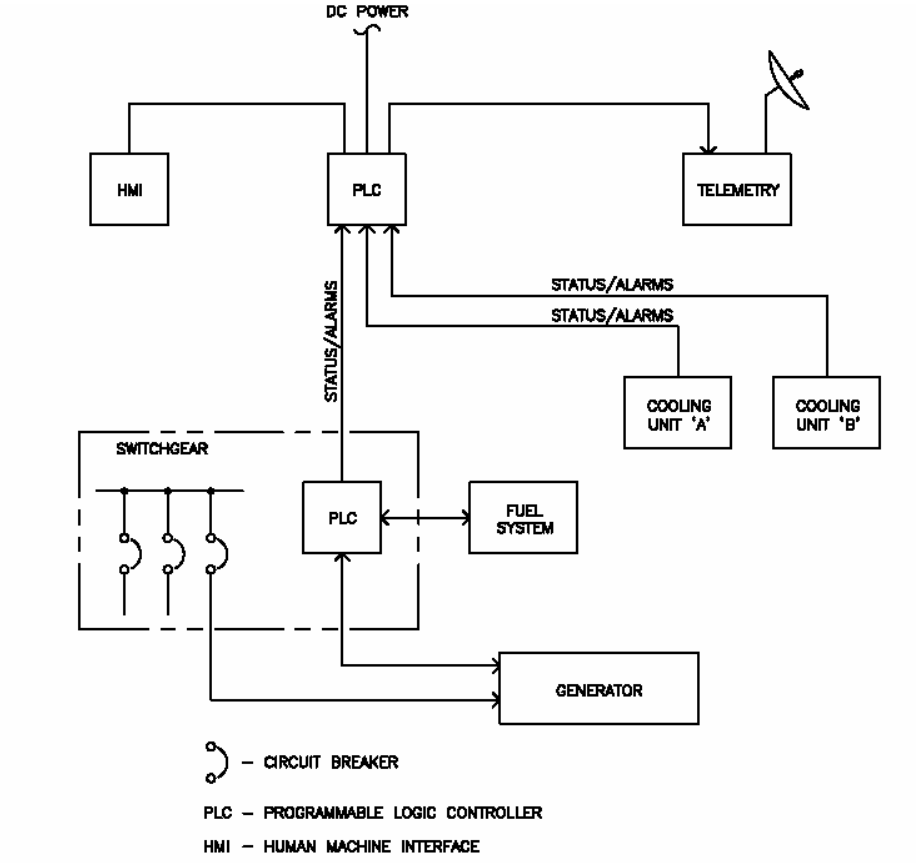


Figure 3-7. Small facility SCADA system

b. The medium system is recommended to support a main computer facility, which would include multiple service transformers and standby generators with paralleling switchgear, one or two large UPS systems, and multiple refrigeration machines with associated auxiliary equipment. SCADA systems for this size facility should utilize redundant distributed control architecture. The level of PLC redundancy should be selected based on the design of the mechanical and electrical systems. Two options and suggested SCADA configurations are provided.

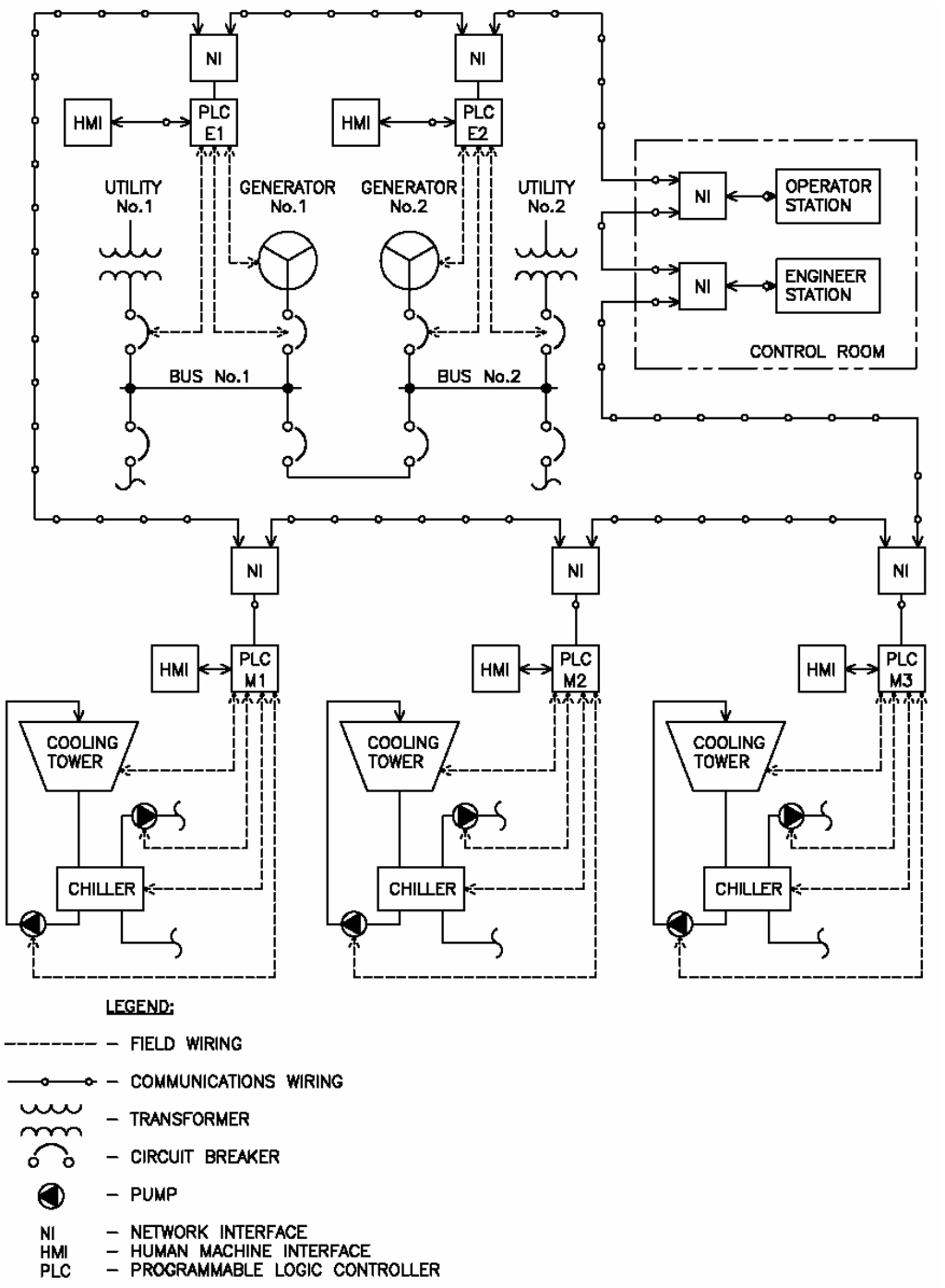


Figure 3-8. Medium facility SCADA system – redundant M/E systems

c. Figure 3-8 presents a suggested SCADA configuration applicable to a facility with mechanical and electrical systems designed to provide redundancy through segregated systems. In this case, PLCs controlling individual systems must have a reliability level adequate to maintain the required availability at the system they serve, but do not necessarily have to be redundant, as redundancy is provided through the N+X system approach. Failure of a single PLC will affect only the system it controls and the remaining systems continue to meet the mission-critical load.

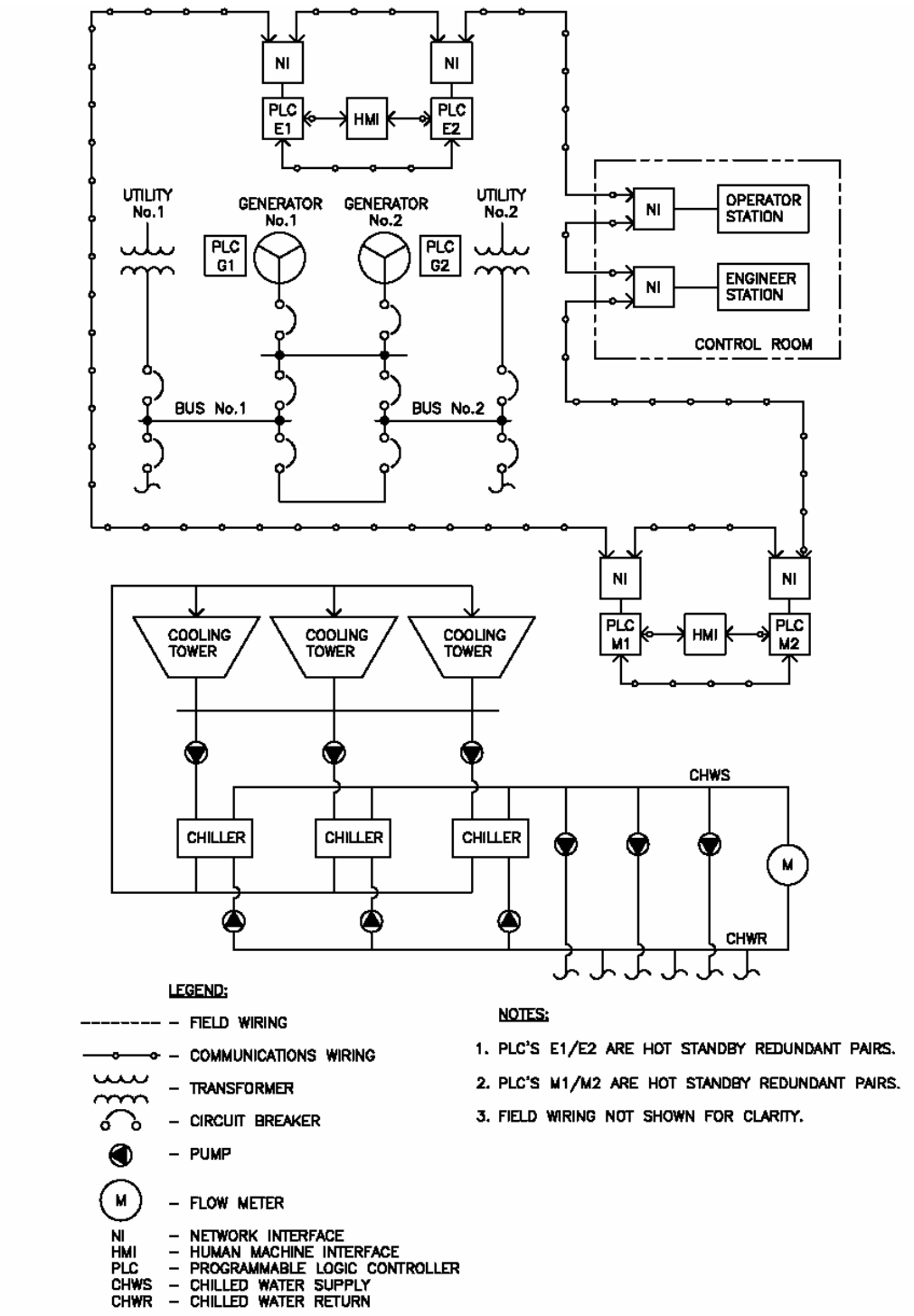


Figure 3-9. Medium facility SCADA system – redundant M/E components

d. Figure 3-9 presents a suggested SCADA configuration for a similarly sized facility in which mechanical and electrical systems utilize redundant components in a manifold configuration. In this design, any combination of components can be selected to serve the load. This provides greater flexibility than segregating components into redundant systems, but requires common control of all components, making

the PLC a potential single point of failure. In this configuration, system-level PLCs must have redundancy adequate to meet the required availability of the system.

e. A large system serving a multi-facility site consisting of several installations will require a central supervisory control room networked to distributed control within the individual buildings appropriate to the mission and reliability criteria of each facility. A control room will typically be located in each central power plant that is required for such a facility and the system can also be accessed from other locations distributed along the network. Redundant and segregated pathways are recommended for the on-site communication network. See figure 3-10 for a suggested configuration.

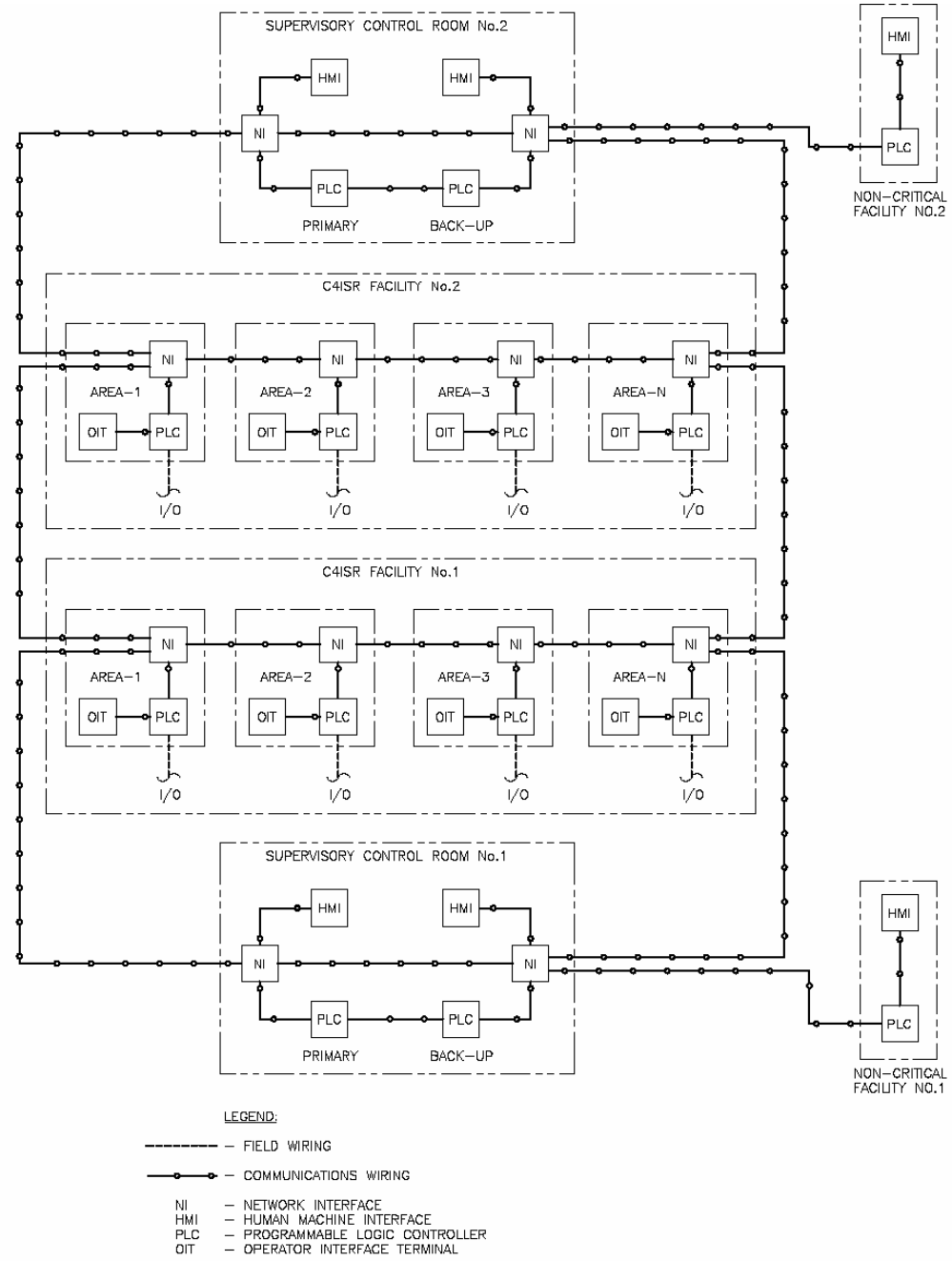


Figure 3-10. Large Facility SCADA system

CHAPTER 4
COMMUNICATION TECHNOLOGY

4-1. General communications

Communication networks may be used in SCADA systems to pass data between field devices and PLCs, between different PLCs, or between PLCs and personal computers used for operator interface, data processing and storage, or management information. Although a communications circuit can involve only two pieces of equipment with a circuit between them, the term *network* typically refers to connecting many devices together to permit sharing of data between devices over a single (or redundant) circuits. Data is transmitted over a network using *serial communication*, in which words of data called *bytes* consisting of individual logical zeros and ones (*bits*) are transmitted sequentially from one device to another. The collection of data in a single transmission is often called a *packet*. The rate at which data can be transmitted over a network is defined in bits-per-second or bps, but typically expressed in thousands (*Kbps*) or millions (*Mbps*).

a. In large SCADA systems, there is usually a communications network of some type connecting the individual PLCs to the operator interface equipment at the central control room. There may also be networks used at lower levels in the control system architecture, for communications between different PLCs in the same subsystem or facility, as well as for communications between field devices and individual PLCs. Figure 4-1 shows the various levels of network communications in a typical large SCADA system.

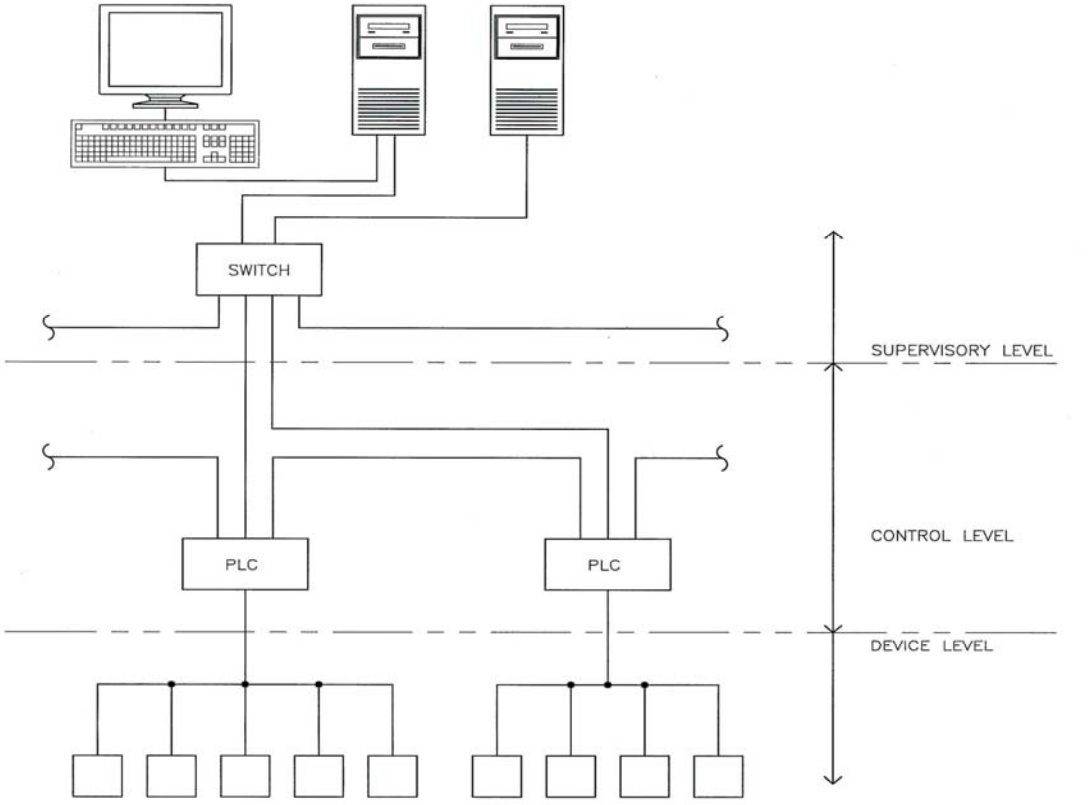


Figure 4-1. Typical SCADA network levels

b. Although not widely applied to SCADA systems, two terms that are commonly used with respect to management information systems communication are *local area network (LAN)* and *wide area network (WAN)*. A LAN consists of all of the devices, typically PCs and servers within a particular facility or site. A WAN is created by providing a connection between LANs, typically over a long geographic distance using telecommunications facilities. Large SCADA systems may be required to interface to LANs or WANs to provide data transfer to management information systems or to permit internet access to SCADA system data.

4-2. Physical media

All communications networks utilize one of two media to transmit data signals between devices: Electrical conductors such as copper wire or optical conductors such as fiber optic cable (wireless communication via radio or microwave radiation does not require an intervening medium). The point on a device at which the circuit is connected is referred to as a *communications port*; the physical and electrical characteristics of the communications port must match the media to be used for the network.

a. Copper media will support either point-to-point or tapped network configurations. Copper-based networks may be used between devices and PLCs or between PLCs, but should not be installed over long distances, or across a facility boundary. All copper network cables should be of shielded construction. For copper-based networks, three basic types of copper conductors are used.

(1) Shielded twisted pair (STP), in which individual pairs of insulated conductors are twisted together to reduce inductively coupled interference and covered with a continuous metallic foil shield to reduce capacitive coupled interference. Individual pairs or multiple pairs are then assembled into a cable within an overall jacket that provides environmental protection.

(2) Unshielded twisted pair (UTP), have individual pairs of insulated conductors that are twisted together to reduce inductively coupled interference. Individual pairs or multiple pairs are then assembled into a cable with an overall jacket to provide environmental protection.

(3) Coaxial cable (COAX) has a single conductor that is surrounded by an annular layer of dielectric material that is then covered with a metallic braided shield and then an overall jacket. Configurations are available with multiple coaxial cables within a common overall jacket; these are often referred to as twin-ax (2 cables) or tri-ax (3 cables). Coaxial cable construction is inherently shielded.

b. In fiber-based networks, optical fibers transmit data in the form of pulses of light, which are produced by a light emitting diode (LED) or laser transmitter and detected by a photodiode or phototransistor receiver at the other end of the fiber. In addition to these photoelectric components, fiber optic transceivers contain the circuitry required to convert electronic data into pulses of light and the reverse. Each optical fiber consists of a glass fiber core with another layer of glass over the core called cladding. The core and cladding have different indexes of refraction, causing light waves that enter the core to be continuously reflected from the interface and not dispersed outside the core. Cable sizes are typically defined by the outside diameters of the core and cladding in microns, such as 62.5/125. Optical fiber is available in two types:

(1) Single Mode Fiber, consisting of a single core strand having a single transmission path, provides very high data transmission rates over long distances, but is costly. This type of cable is used for long-distance telecommunications and video application.

(2) Multi-Mode Fiber, consisting of multiple core strands, provides multiple signal paths which result in some distortion of the signal and is therefore restricted to shorter lengths, but is more economical. This is the type of cable commonly used in SCADA system and data processing networks.

c. SCADA networks operating between facilities on large sites, over long distances, or outside of the facility HEMP shield should be fiber-based. Fiber-based networks have some significant advantages for SCADA application, including the following.

(1) They provide very high signal quality.

(2) As no electric voltage or current is used, they are completely free of RFI and EMI interference.

(3) When used over long distances or between buildings they eliminate problems with ground potential differences, ground loops, and transient voltages.

(4) They provide enhanced security since point-to-point communications cannot be tapped or daisy chained.

4-3. Media standards

Industry standards for communications media define both the physical and electrical (or optical) characteristics of both the conductors and the connectors used to mate them to communications ports. Some common network conductor physical standards and their characteristics are listed in table 4-1.

Table 4-1. Common network communication media

Standard Designation	Conductor Type	Connection	Transmission Speed	Maximum Distance	Typical Application
RS-232	Copper M/C with 9-pin connectors	Point-to-Point	265 kbps	15 m	Laptop computer to PLC
RS-485	Copper UTP or STP	Multi-drop	10 Mbps	1000m	PLC to field devices
CAT 5	Copper UTP or STP	Multi-drop	100 Mbps	Depends on Protocol	PLC to PLC
RG6	Copper Coax	Multi-Drop	5Mbps	1000m	PLC to PLC, Video
	Single-Mode Fiber	Point-to-Point	>1Gbps	50 kM	Long-distance telecommunications (No typical SCADA application)
	Multi-Mode Fiber	Point-to-Point	>1 Gbps	1000m	PLC to Control Room and PLC to PLC

4-4. Communication protocols

Communication protocols define the “rules” by which devices on a network are able to communicate. They define the structure of data packets that are transmitted on the network as well as other necessary information such as how individual devices are uniquely addressed, what signals the beginning and end of a data message, and how each message is checked for transmission errors by the receiving device. A par-

ticular communication protocol may be implemented using more than one type of physical media. For example, Ethernet may operate on UTP, coaxial cable or fiber, but the data structure is the same on any of these media. The protocol used may impose limitations on the media such as maximum data transmission rate (Mbps) or maximum circuit length between devices.

a. Protocols may be either *proprietary* or *open.* Proprietary protocols are those developed by vendors for use with their own systems and for which application information is not made publicly available for use by other vendors. Open protocols are those for which all application information is in the public domain, permitting any vendor to develop devices and software that can use the protocol. Most of the open protocols used today originated with specific vendors. However, they have been made accessible by those vendors to increase the number of devices that are compatible with their systems, making them more marketable. Table 4-2 shows common open network communication protocols.

b. SCADA systems for C4ISR facilities should use open protocols for a number of reasons:

(1) There is substantial published data regarding their reliability and performance characteristics.

(2) Technical support is available from multiple sources.

(3) There are larger numbers of competing compatible devices to select from.

(4) Systems may be modified or expanded without requiring sole-source proprietary contracts.

Table 4-2. Common open network communication protocols

Protocol	Level	Common Applications
ModBus	Device	Manufacturing, Electric Utility
Profibus	Device	Process Industry
DeviceNet	Device	Manufacturing
DNP 3.0	Device	Electric Utility SCADA
BACNet	Control	HVAC Control, Building Automation
ControlNet	Control	Manufacturing
ARCNet	Supervisory	Office Automation, Gaming
Ethernet/IP	Supervisory	Office Automation, Internet

4-5. Network topologies

Commonly used network topologies include star, ring and tapped configurations. A *logical network* is defined as a group of interconnected devices that are communicating together with the same protocol. Different logical networks may be interconnected by using protocol converters or translators.

a. In a star topology, each device on the network is connected to a central hub by a single communications circuit, as shown in figure 4-2. The hub performs the function of passing messages between devices. Types of devices that may serve as the hub of a star network include repeaters, switches and routers. The most common example of this topology is the Ethernet LAN used to interconnect all of the personal computers within an office environment. In this case, a dedicated cable is routed from the Ethernet port on each PC back to a switch or router somewhere in the office building. In a star network, loss of a single communication circuit affects only the single device at the end of that circuit, although loss of a hub device obviously affects the entire network. The star network has the highest installation cost per device.

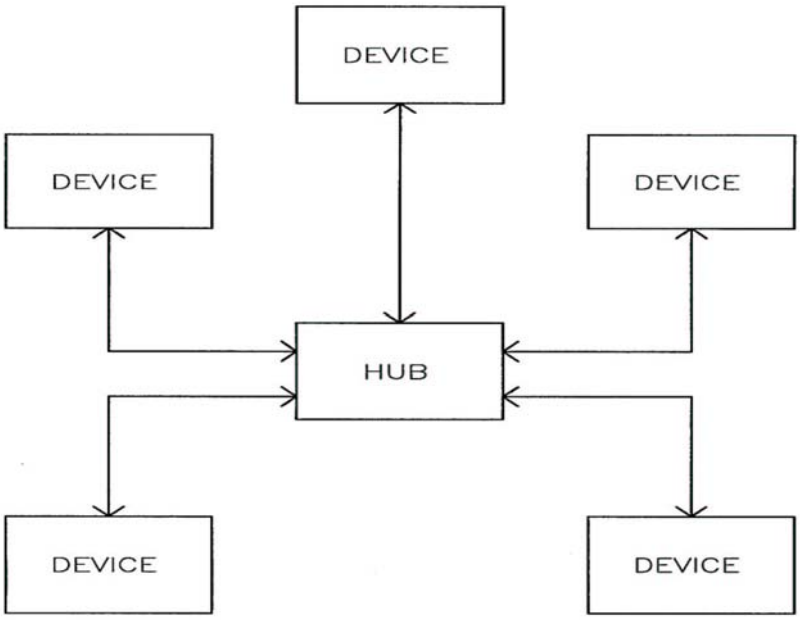


Figure 4-2. Star network topology

b. In a ring topology, two communication ports are provided on each device and the network circuit makes a loop through all of the devices, with an open point, as shown in figure 4-3. Two-way communication allows messages to pass in either direction along the network. Messages must be passed through the communication ports of each device on the network, making it vulnerable to a break if a single device fails or is removed. If a means is provided to bridge the open point on failure of a particular device or circuit segment, this configuration can have high reliability at relatively low cost.

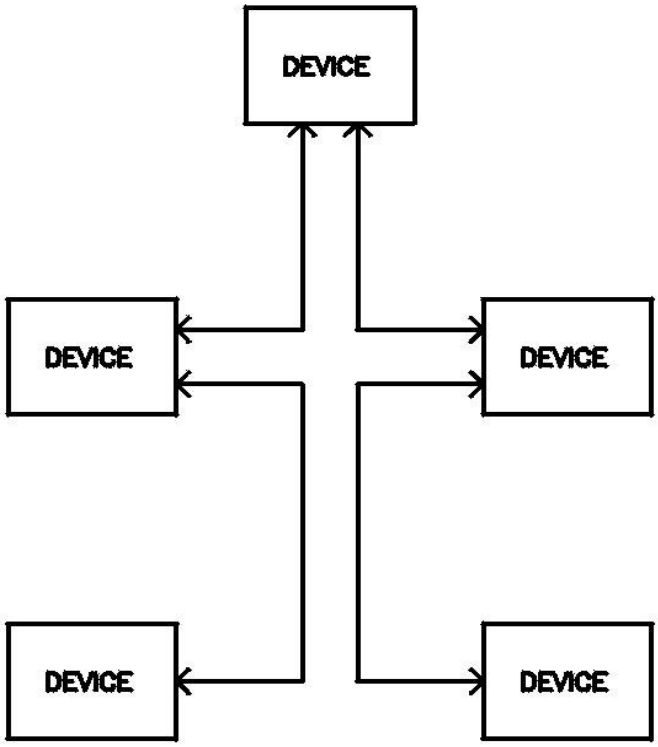


Figure 4-3. Ring network topology

c. In a tapped (or multi-drop) network the communications circuit is tapped to be connected to each device so that the communication ports of the various devices are effectively electrically in parallel. Tapped connections are applicable only to copper-based media; fiber optic circuits are limited to point-to-point operation. The configuration in figure 4-4 typically represents the lowest installed cost per device. This configuration is commonly used for field device communications; a common example is a fire detection system with addressable devices, in which a UTP network is T-tapped at each device.

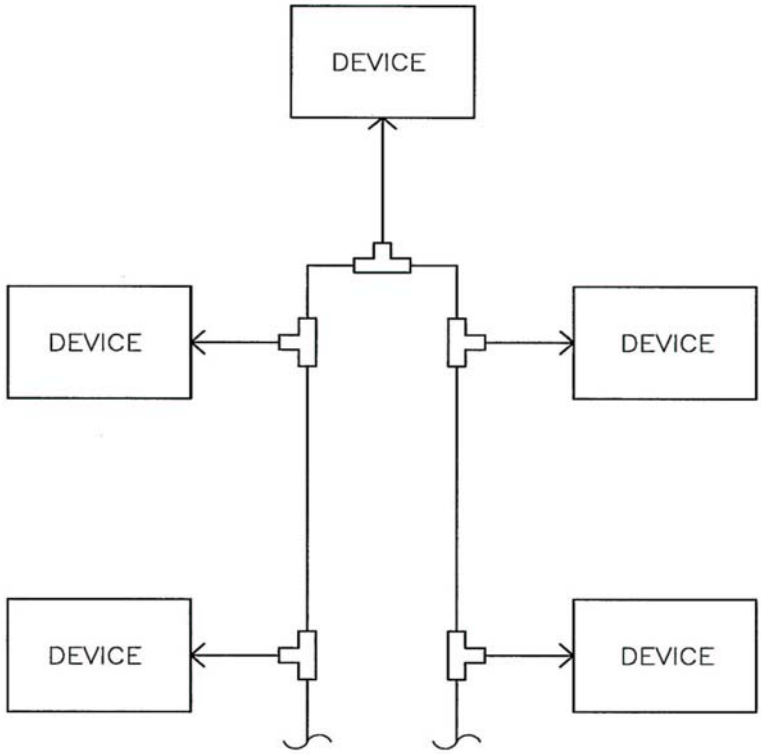


Figure 4-4. Tapped network topology

4-6. Network redundancy

The need for network redundancy in a SCADA system is dependent on the robustness and vulnerabilities of the type of network used as well as the criticality of the control or reporting functions that rely on the network. In a system where the network serves only to pass management information reporting or trending of data to a central location, and all automatic control and operator interface functions are fully present with the network out of service, a non-redundant configuration is acceptable. If a network serves only a single redundant component of a system, such as the point-to-point communication circuit between a generator PLC located in the control room and the local engine control panel, network redundancy is also not required. Any network, however, that is required for system operation, or whose failure could affect multiple redundant sub-systems or components, must be redundant. For example, a communications network used to pass information (such as generator start signals) between all of the generator PLCs and the system master PLC must provide redundancy.

a. In a either a star or a tapped network, redundancy requires complete duplication of the network, including communication ports at each device, communication circuits, and the hub equipment. Figure 4-5 presents an example of a fully redundant network configuration. In this configuration, one network serves as the primary with all devices using it for communication. If any (or all devices) sense loss of communications with the primary network, they automatically transfer to the backup network. This provides protection both against loss of the entire primary network and loss of an individual device connection. A bridge is required between the two networks to allow a device that has transferred to the backup network to communicate to those remaining on the primary network. An advantage of this configuration is that each device requires only a single address, as it only communicates with one network at a time.

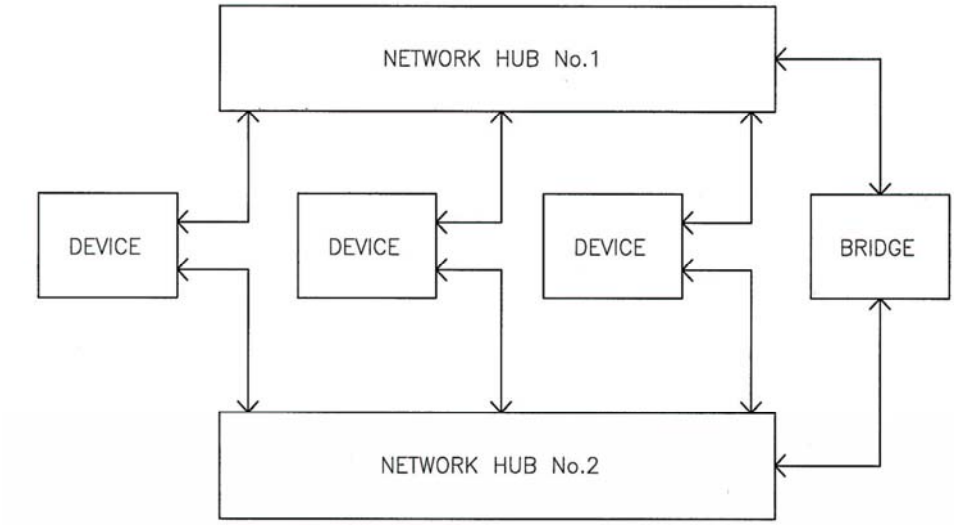


Figure 4-5. Fully redundant network

b. The reliability of a ring network can be increased by providing an automatic switching device at the open point. The switching device periodically polls the other devices on the network and detects an open point due to device or communication circuit failure by the lack of response from particular devices. The switch is then automatically closed, restoring communications between all devices. This is referred to as a "self-healing" ring as shown in figure 4-6. This provides a network that is more reliable than any of the non-redundant configurations, at less cost than a fully redundant configuration, and may be acceptable for facilities with lower RAM criteria.

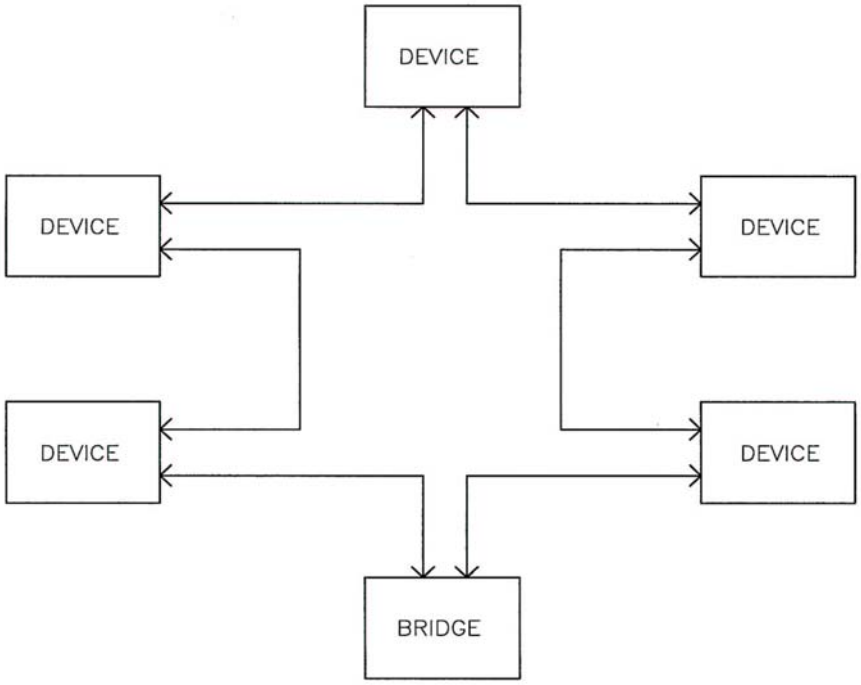


Figure 4-6. Self-healing ring network

4-7. Network speed

The speed at which information can be transmitted on a communications network depends upon the protocol, the physical media, the number of devices on the network and the level of message traffic. Traditionally, the networks associated with SCADA systems have provided adequate speed for alarm and status reporting and operator control, but were not fast enough for critical functions like protective relay tripping or under frequency load shedding. Advances in electrical utility substation automation have led to testing and qualification of some network systems to speeds adequate for protective relay trip functions (4 milliseconds) under specified traffic levels. However, before considering a SCADA system that relies upon the network for critical control and protection functions, the user must verify that the hardware and software to be used has been tested and demonstrated the required speed under worst-case traffic conditions.

CHAPTER 5
RELIABILITY CONSIDERATIONS

5-1. Reliability criteria

Mechanical and electrical support systems for C4ISR facilities are required to be designed to attain a reliability/availability (R/A) of 0.999999. SCADA systems are integral to the function of the mechanical and electrical support systems and must therefore be designed to support this R/A goal. A mechanical/electrical system configuration that meets this criterion based on analysis of the process flow diagram or the electrical one-line will not achieve it if the control system compromises the reliability/availability designed into the process.

a. *Reliability* defines the probability of a system serving its function or being able to perform its mission over a certain fixed period of time. A system having a reliability of 0.999999 for a specific mission time has a 99.9999% chance of functioning without failure over that period.

b. *Availability* defines the long-term fraction of time that a system is functioning properly or able to perform its mission. A system with availability of 0.999999 will have an average downtime of only 31 seconds per calendar year. This does NOT mean that the average outage of the system will last 31 seconds; it only means that the number of expected failures per year multiplied by the average outage length equals 31 seconds per year. For example, a probability of a failure occurring once every 40 years, with an average duration of 20 minutes, would be more typical of a facility with an availability of 0.999999. Given their continuous operation and lack of a defined mission time, availability is generally a more appropriate design criterion than reliability for SCADA systems.

5-2. Reliability calculations

If the time, t, over which a system must operate and the underlying distributions of failures for its constituent elements are known, then the system reliability can be calculated by taking the integral (essentially the area under the curve defined by the failure distribution) from t to infinity, as shown in equation 5-1.

$$R(t) = \int_t^{\infty} f(t)\, dt \qquad \text{(Equation 5-1)}$$

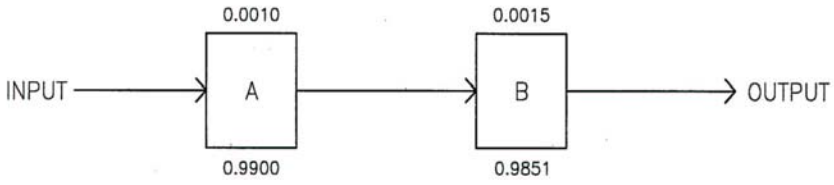
a. *Exponential distribution*. If the underlying failure distribution is exponential, a common, but only approximate, assumption for mechanical and electrical systems, equation 5-1 becomes equation 5-2. If the underlying distribution for each element is exponential and the failure rates, λ_i, for each element are known, then the reliability of the system can be calculated using equation 5-2.

$$R(t) = e^{-\lambda t} \qquad \text{(Equation 5-2)}$$

where:

λ is the failure rate
t is the length of time the system must function
e is the base of natural logarithms
R(t) is reliability over time *t*

b. *Series reliability*. Consider the system represented by the reliability block diagram (RBD) in figure 5-1.



NOTES:

1. THE NUMBER ABOVE EACH BLOCK IS THE FAILURE RATE IN FAILURES PER HOUR.
2. THE NUMBER BELOW EACH BLOCK IS THE RELIABILITY CALCULATED USING EQUATION 5-2 WITH T = 10 HOURS (EXPONENTIAL DISTRIBUTION ASSUMED).

Figure 5-1. Reliability block diagram.

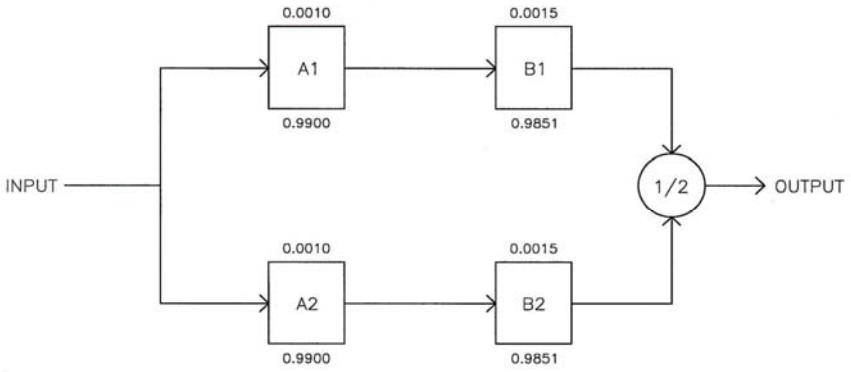
(1) *Series configuration - the weakest link*. A and B in figure 5-1 are said to be in series, which means all must operate for the system to operate. Since the system can be no more reliable than the least reliable component, this configuration is often referred to as the weakest link configuration. An analogy would be a chain; the strength of the chain is determined by its weakest link.

(2) *Series calculation method 1*. Since the components are in series, the system reliability can be found by adding together the failure rates of the components and substituting the result in equation 5-2. The system failure rate is 0.001000 + 0.001500 = 0.002500. The reliability is:

$$R(t) = e^{-0.0025x10} = 0.9753 \qquad \text{(Equation 5-3)}$$

(3) *Series calculation method 2*. Alternatively, we could find the system reliability by multiplying the reliabilities of the two components as follows: 0.9900 x 0.9851 = 0.9753.

c. *Reliability with Redundancy*. Now consider the RBD shown in figure 5-2.



NOTES:

3. THE NUMBER ABOVE EACH BLOCK IS THE FAILURE RATE IN FAILURES PER HOUR.

4. THE NUMBER BELOW EACH BLOCK IS THE RELIABILITY CALCULATED USING EQUATION 5-2 WITH T = 10 HOURS (EXPONENTIAL DISTRIBUTION ASSUMED).

Figure 5-2. RBD of a system with redundant components.

(1) *The redundant or parallel configuration.* The system represented by the RBD in figure 5-2 has the same components (A and B) used in figure 5-1, but two of each component are used in a configuration referred to as redundant or parallel. Two paths of operation are possible. The paths are top A-B and bottom A-B. If either of two paths is intact, the system can operate. The reliability of the system is most easily calculated by finding the probability of failure (1 - R (t)) for each path, multiplying the probabilities of failure (which gives the probability of both paths failing), and then subtracting the result from 1. The reliability of each path was found in the previous example. Next, the probability of a path failing is found by subtracting its reliability from 1. Thus, the probability of either path failing is 1 - 0.9753 = 0.0247. The probability that both paths will fail is 0.0247 x 0.0247 = 0.0006. Finally, the reliability of the system is 1 - 0.0006 = 0.9994, about a 2.5% improvement over the series-configured system.

(2) *Types of redundancy*. Two components in parallel (redundant) may always be on and in operation (hot standby) or one may be off or not in the "circuit" (cold standby). In the latter case, failure of the primary component must be sensed and the standby component turned on or switched into the circuit. Standby redundancy may be necessary to avoid interference between the redundant components and, if the redundant component is normally off, reduces the time over which the redundant component will be used (it's only used from the time when the primary component fails to the end of the mission). Of course, more than two components can be in parallel. Both types of standby redundancy are available in PLC systems

5-3. Redundancy terminology

Redundant configurations of systems and equipment are commonly referred to using mathematical formulas based on the parameter "N", such as "N + 1" or "2N". In this convention, N is the number of systems or pieces of equipment which must be operational to meet the load or accomplish the mission.

a. N + X redundancy refers to a system configuration in which the total number of units provided is equal to the number needed to meet the load, N, plus some number of spare units, X. For example, if a cooling system requires 300 gallons per minute (gpm) of flow, and five 100 gpm pumps are provided, the system would be described as N + 2, where N = 3.

b. XN redundancy refers to a system configuration in which the total number of units provided is some multiple, X, of the number required to meet the load. For example, if the same cooling system were provided with two 300 gpm pumps, it would be described as 2N, where N = 1.

Further information on redundant system configurations can be obtained from TM 5-698-1 – Reliability/Availability of Electrical and Mechanical Systems for Command, Control, Computer, Communications, Intelligence, Surveillance and Reconnaissance (C4ISR) Facilities.

5-4. Availability calculations

a. Once an expected failure rate, λ, is known for a component or a system, the associated availability can be calculated from the failure rate and the repair time, *r* as in equation 5-4.

$$A = \frac{8760 - \lambda r}{8760} \qquad \text{(Equation 5-4)}$$

λ = failure rate, per year
r = repair time, hours

b. Availability can also be calculated from published or tested Mean Time Between Failure (MTBF) and Mean Time To Repair (MTTR) data using equation 5-5:

$$A_i = \frac{MTBF}{MTBF + MTTR} \times 100\% \qquad \text{(Equation 5-5)}$$

Availability calculated on this basis is also termed *inherent availability,* A_i, as it is based only on the inherent failure characteristics of the system and does not account for unavailability for scheduled maintenance or overhauls. *Operational availability*, A_o, is availability calculated including the effects of scheduled downtime based on Mean Time Between Maintenance (MTBM) and Mean Down Time (MDT) as shown in Equation 5-6. As SCADA systems and components rarely require extended shutdowns for maintenance, inherent availability is an appropriate design and performance criteria.

$$A_o = \frac{MTBM}{MTBM + MDT} \times 100\% \qquad \text{(Equation 5-6)}$$

5-5. Component reliability

The components used to assemble SCADA systems are typically industrial- or utility-grade sensors, controllers, relays and actuators, which are mass-produced in large numbers for the commercial market and generally are not designed to Military Specifications (MilSpec) or to documented reliability criteria. Where available, SCADA systems should use components meeting the applicable MilSpec designations. For those applications where such components are not available, components should comply with other applicable industry standards that address reliability, maintainability, environmental protection, seismic withstand, surge withstand, etc.

a. Reliability of non-Milspec components should be enhanced by specifying heavy-duty components or overrating of devices, where such overrating does not interfere with the operation or function of the component. Examples include:

(1) Use of 600V rated wire for all control circuits operating above 50 V.

(2) Use of relays with contact ratings exceeding circuit voltage and current ratings in power circuits.

(3) Derating of devices to operate below a specified fraction (often 80%) of their capability.

b. Reliability data for electrical components used in the power supply circuits for SCADA systems can be obtained from IEEE 493, also known as “The Gold Book” or from the PREP Equipment Reliability Database.

5-6. Systems reliability

Reliability of a SCADA system can be calculated from the known indices of the components or subsystems as described above. From a qualitative standpoint, however, there are two primary considerations in developing a reliable SCADA system: Providing segregation and redundancy corresponding to that specified for the supported mechanical and electrical systems; and keeping the configuration, control sequences, and programming as simple as is consistent with the required functionality. The tendency to design control sequences to account on an automatic basis for every conceivable contingency or to provide sustained service to the load after the third or fourth contingency failure often results in systems that are unwieldy to operate and makes it difficult for operators to retain knowledge of the system. Because of the critical role of humans in the function of SCADA systems (see chapter 6), complex configurations and sequences that provide very high calculated reliability/availability indices may actually produce significantly lower real-world availability than simpler systems due to the effects of human action.

a. It is said that *software* neither fails randomly nor wears out, and thus all software failures must be designed into the system, and simply remain dormant until the right combination of input conditions, timing and logic cause them to show up. SCADA software should incorporate self-diagnostic features including flow control, watchdog timers, and reasonableness checking. Failure of a self-diagnostic check should result in an alarm report to the supervisory system, driving all outputs to a defined fail-safe state, and transfer of control to the redundant processor, where provided. Comprehensive commissioning testing, as described in chapter 8, can significantly reduce the likelihood of undiscovered software errors.

b. System reliability can be enhanced by anticipating likely *field device* failure modes and providing program logic to detect them. For example, monitoring the position of a critical circuit breaker using only

a single normally open or normally closed auxiliary contact leaves the control system vulnerable to false information in the event of a short or open on the input circuit. If both contacts are used, they must always agree on the state of the breaker, or a faulted input circuit is declared and automatic operation of that breaker suspended.

5-7. Power supply sources

The preferred power supply for SCADA systems is the direct current (DC) station battery system supplying the equipment controlled by the SCADA. DC Station battery systems can be inherently more reliable than alternating current (AC) uninterruptible power supply (UPS) systems, because they rely on electronic components only to maintain the batteries in a charged state, and not to deliver energy to the load. PLCs are available with DC power supplies rated at voltages between 24 VDC and 125 VDC, and DC-DC converters are available to supply lower voltage components from higher voltage systems.

a. Station battery banks provide voltage over a range limited on the lower end by the specified end-of-discharge voltage, which is typically 1.75 volts per cell (VPC) for lead-acid batteries and 1.14 VPC for nickel cadmium batteries and on the upper end by charging voltage required to periodically equalize the batteries, typically 2.38 VPC for lead-acid and 1.70 VPC for nickel cadmium. SCADA components must be rated to operate properly over this range, or must be provided with DC-DC converters that are rated for this input range.

b. The level of redundancy in power supply circuits should correspond to the redundancy criteria of the PLC. For example, in multiple generator paralleling switchgear applications where reliability is attained through an N+X generator configuration, it is common for each generator to be provided with a single PLC supplied from the DC control voltage source of that generator, which is typically the starting battery. A redundant power circuit to the generator PLC would add no benefit as the generator cannot start without local control power anyway. The master controller associated with the paralleling switchgear, however, is typically a redundant PLC configuration. It should be provided with redundant DC supplies from separate station battery banks.

c. Diode-based “best battery” selection systems, as shown in figure 5-3 may be used to increase system availability by supplying non-redundant pieces of switchgear or SCADA system equipment from two or more DC power sources. This arrangement provides automatic protection against low voltage or complete loss of one source, as the diode pair with the highest voltage is always conducting and the “failed” source is isolated from the load by the other diode pair that is in a reverse-biased blocking state. This source selection scheme must only be used at the branch circuit level, as it does not provide isolation of the sources for short circuits on the load side of the diodes. Such a short circuit will cause both diodes to conduct, clearing the fuses or tripping the circuit breakers on both DC circuits. For this reason, individual sets of diodes should be provided for each PLC cabinet, circuit breaker, etc. to limit the outage to the affected unit.

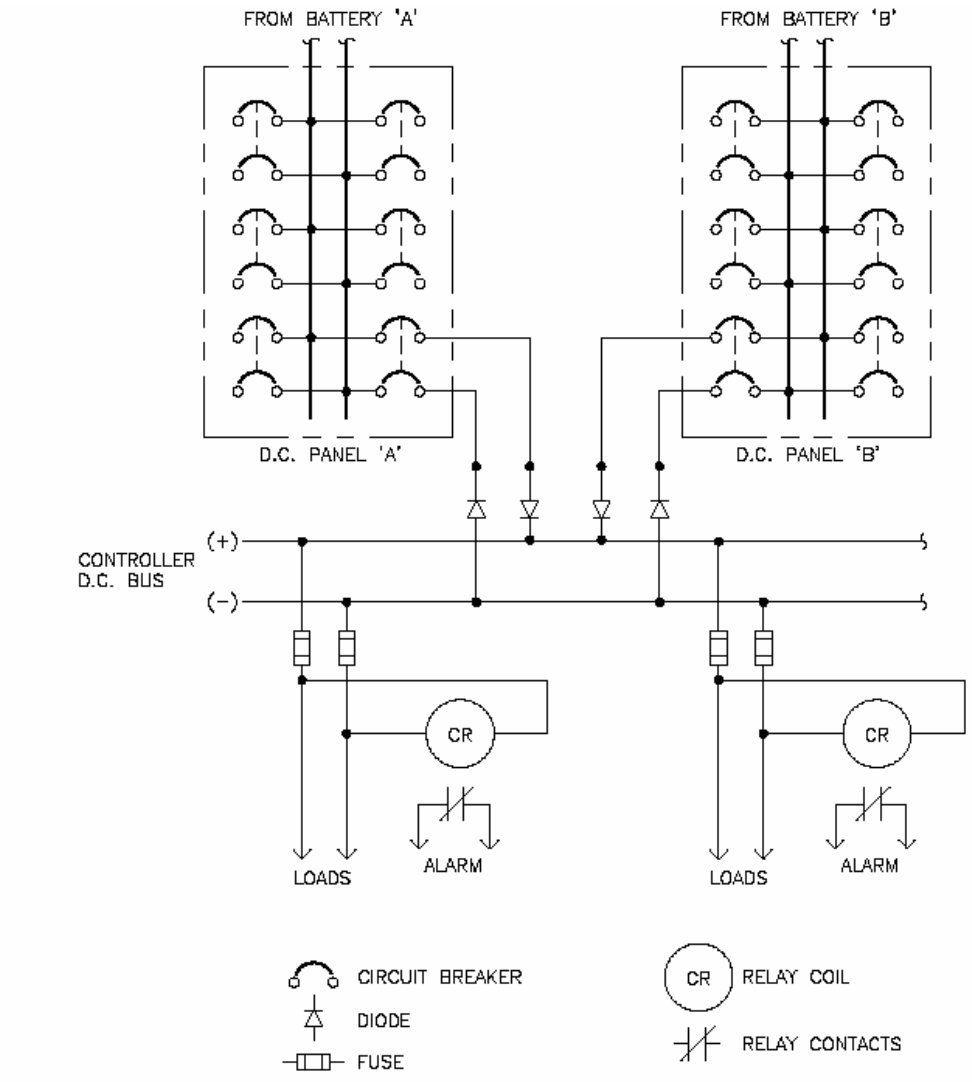


Figure 5-3. Diode-based "best-battery" selector circuit

d. Every branch of a control power circuit should be provided with a voltage relay or other means of supervision to verify continuously the presence of control power. This supervision should be provided on the load side of all fuses, circuit breakers, diodes and transfer switches. Failure of any control power branch circuit should initiate local and central alarms.

e. Where UPS systems must be used to supply SCADA equipment that requires AC power, they should be of the on-line, or reverse transfer type, in which the rectifier-inverter combination is normally supplying the load while float-charging the battery and provided with quarter-cycle static switching to the AC line upon inverter failure. UPS systems should be selected in compliance with TM 5-693, Uninterruptible Power Supply System Selection, Installation, and Maintenance for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities.

f. SCADA power supplies must be provided with overcurrent protective devices (fuses or circuit breakers) whose ratings and settings have been determined to provide selectively coordinated protection. Selective coordination is defined as opening the protective device closest to the point of the fault without opening upstream devices, thus limiting the associated outage to the faulted circuit or equipment. Guidelines for selective coordination can be found in IEEE 242 – Protection and Coordination of Industrial Power Systems.

5-8. Segregation

Redundant components and subsystems should be segregated electrically and physically to reduce the probability of common mode failure from electrical, environmental, or physical threats.

CHAPTER 6
OPERATOR INTERFACES

6-1. General interfaces

Operator interfaces, or human machine interface (HMI) for SCADA systems provide the functions of status indication, alarm reporting, operator intervention in control action, and data storage and programming. Several levels or layers of operator interfaces are required to provide a reliable and maintainable system: equipment level, controller level, and supervisory level. At the controller and supervisory level, HMI may also provide capability to modify the controller program.

6-2. Equipment level

Equipment level HMI should consist at minimum of the control switches and indicators necessary to permit an operator to manually control the equipment in the absence of communications from the controller or for maintenance purposes. Examples of this level of control are hand-auto-off switches and indicator lights at motor starters; local-remote switches, potentiometers and meters at variable frequency drives; and circuit breaker control switches, meters and indicator lights at switchgear. Table 6-1 lists minimum manual control capabilities to be provided for mechanical and electrical system components:

Table 6-1. Minimum manual control capability

Function Identification	Function Description
	Standby Generation
G-1	Generator Set Start/Stop
G-2	Speed/Frequency Adjust
G-3	Synchronizing to Bus
G-4	Emergency Stop
G-5	Fuel Oil Pumps Start/Stop
G-6	Alarm Acknowledge/Reset
	Switchgear
S-1	Circuit Breaker Close (W/Sync-Check)
S-2	Circuit Breaker Trip
S-3	Lockout Relay Reset
S-4	Alarm Acknowledge/Reset
	Cooling Systems
C-1	Chiller Start/Stop
C-2	Pump Start/Stop
C-3	Fan Start/Stop
C-4	Setpoint Adjust
C-5	Valve Open/Close
C-6	Alarm Acknowledge/Reset
	Auxiliary Systems
A-1	Air Compressor Start/Stop
A-2	Sump Pump Start/Stop
A-3	Alarm Acknowledge/Reset

a. Manual control substitutes the facility operator for the automatic control system in the feedback loop, and leads to the risk of system or equipment mis-operation due to human error. Safety interlocks, such as motor overload, high-high pressure switches, fire detection, etc. should therefore be hard-wired into the control circuit such that they are active in both manual and automatic control modes. Switchgear protective relaying required for fault protection should always be hard-wired in the circuit breaker trip circuit and not dependent upon the controller.

b. In some cases, hard-wired manual controls for entire facilities have been centrally located in a control panel or benchboard at the control room. Although this simplifies operator intervention upon complete failure of the automatic control system, it is not recommended as the lack of physical segregation compromises reliability. A catastrophic structural or environmental failure at the control room would disable both automatic and manual control capability.

6-3. Controller level HMI

At the controller level, the primary HMI device should be a graphical display/keypad combination providing access to input and output data, timer and register settings, and alarm and status screens. These devices are commonly panel-mounted in the door of the PLC cabinet, and are available in enclosures suitable for hostile environments. With password-protected access control the controller level HMI may also provide a means of accessing and modifying the controller program logic. Table 6-2 lists the minimum recommended functionality of controller level HMI.

Table 6-2. Required controller level HMI functionality

Access Level[(1)]	Function Description
1	Alarm and Status Displays
1	Alarm Acknowledge
1	Initiate Pre-Programmed Control Sequence
2	Adjust Control Setpoints
2	Individual Device Start/Stop, Open/Close
2	Setup Data Trending/Reporting
3	Adjust Alarm Setpoints
3	Adjust Control Setpoint Ranges
3	Modify Controller Parameters
3	Modify Control Logic

[(1)] Increasing numbers indicate more restricted levels of operator access. Access levels are typically password-protected. Each access level includes the functionality of those below it.

6-4. Supervisory level HMI

Supervisory level HMI devices are typically personal computer workstations located in the central control room and/or management and engineering offices. The quantity and function of these workstations depends on the size and complexity of the facility. Simple facilities may be provided with a single workstation, which may be located in the main electrical or mechanical space in the absence of a central control room. Large or complex facilities should be provided with a minimum of two workstations in the

control room to permit operators to back one another up, plus the additional workstations required for engineering use, management overview, or data storage and reporting, as determined by the facility manager. Multiple-building campuses should be provided with workstations in the mechanical/electrical space of each major building to permit operations staff to obtain status and alarm information for the entire facility from any building.

a. Supervisory level HMI uses graphical screens displayed on the computer monitor to communicate system status and alarm conditions. Screens should be configured for facility overview, system overview, subsystem, and equipment screens for all major components of the facility. Remote manual control and supervisory control is typically performed at the supervisory level HMI under security access control. (See 7-3.)

b. Trending and data storage capability should be included in all SCADA systems to provide a permanent log of facility performance. All critical system parameters, such as temperature, humidity, voltage, current, should be stored every 15 minutes (or other specified preset time interval). The system should have the capability to record critical signal values more frequently at an operator-selected rate when prompted from the HMI or by a signal from operating equipment. The system should automatically return to its primary trending when system operation returns to normal. Data storage should utilize a separate server or drive from that used for the primary system control software and should be periodically backed up. Records should be maintained on-site for a minimum of 5 years.

6-5. Human factors

Design of HMI for SCADA systems must include consideration of Human Factors Engineering (HFE). It is estimated that 50 percent or more of all loss of load events in mission-critical facilities involve human action. A commonly reported scenario begins with a single component failure and correct response by the automatic control system to isolate the failure and maintain service to the load, however resulting in an off-normal system condition. Incorrect human intervention in attempting to restore the system to normal conditions then results in loss of service to the load. Consideration of HFE in the layout of operator controls can help prevent these occurrences.

a. Labeling: All control devices must be clearly labeled with letters that are large enough and provide high contrast with the background to be clearly legible in a hurry at a full arms length. The primary designation should be the functional description of the device, ex: “Generator No. 1 Speed Control”. The label should also carry the tag number of the device, ex: “43GS-1” that corresponds to the system documentation, but this information is secondary in emphasis and size to the primary designation.

b. Layout: Controls should be arranged and grouped in an intuitive and logical manner. Some of the many techniques that may be used to design intuitive layouts include:

(1) Grouping controls associated with individual pieces of equipment such as a chiller or a generator with substantial separation between groups.

(2) Placing control switches left-to-right, or top-to-bottom in the sequential order in which they are operated during a normal startup or shutdown.

(3) Spacing devices far enough apart so that labels are clearly associated with their device and an operator’s hand does not obscure the labels on adjacent devices.

(4) Arranging controls in the physical or electrical order of the process, using a mimic diagram or mimic bus.

(5) Color-coding control devices by function; ex: green start buttons, red stop buttons, yellow lamp test buttons, etc.

(6) Colored backgrounds or borders to emphasize grouping of controls on large control panels.

c. Color schemes: Color schemes used for controls and for graphic screens may duplicate color coding used within the process, such as piping color codes or system color codes, or may be developed strictly for the HMI. In all cases, colors should be selected to provide high levels of contrast without eye fatigue. Some rules for use of color in HMI displays are given in table 6-3.

Table 6-3. Rules for HMI colors schemes

Use colors with gray scale contrast ratios of approximately 3:7.
Use neutral background colors, such as light gray.
Limit the number of colors to seven, unless more are required, as for trend graphs.
Sixteen colors are sufficient for 95 percent of all applications.
Use the standard Windows® interface colors listed in table 6-4.
Observe industry standard color conventions; red for breaker closed, green for breaker open, etc.
Use color consistently between screens.

d. Select-before-operate: HMI software should be programmed such that an operator must select the device to be controlled by point-and-click or other means and then select the operation to be performed. This two-step requirement for manual control can reduce errors resulting from selection of the incorrect device. Selection of a device to be controlled should result in highlighting that device on the screen, providing the operator a visual verification of correct selection.

Table 6-4. RGB values for standard colors

Color	Red Tint	Green Tint	Blue Tint
Black	0	0	0
White	255	255	255
Dark Grey	128	128	128
Light Grey	192	192	192
Dark Red	128	0	0
Bright Red	255	0	0
Amber	255	202	0
Bright Yellow	255	255	0
Dark Green	0	128	64
Bright Green	0	255	0
Dark Cyan	0	128	128
Cyan	0	255	255
Dark Blue	0	0	125
Bright Blue	0	0	255
Purple	128	0	128
Magenta	255	0	255

CHAPTER 7
SECURITY CONSIDERATIONS

7-1. Environmental threats

SCADA equipment installed in C4ISR facilities must be of such design or otherwise protected to withstand seismic effects as well as shock (ground motion) and overpressure effects of weapons. A detailed dynamic analysis should be made of the supporting structure(s) of the equipment enclosures to evaluate the magnitude of motion and acceleration established at the mounting points for each piece of SCADA equipment. Where accelerations exceed the allowable limits of equipment available, the equipment should be mounted on shock isolation platforms.

a. SCADA equipment should be protected from the effects of dust, dirt, water, corrosive agents, other fluids and contamination by appropriate location within the facility or by specifying enclosures appropriate for the environment. Care should be taken that installation methods and conduit and tubing penetrations do not compromise enclosure integrity.

b. Central computer or control rooms should be provided with dry agent fire protection systems or double-interlocked pre-action sprinkler systems using cross-zoned detection, to minimize the threat of accidental water discharge onto unprotected equipment.

c. Sensors, actuators, controllers, HMI, UPS and other SCADA equipment located throughout the facility should utilize enclosures with a minimum environmental protection level of IP66 per EN 60529 or Type 4 per NEMA 250. Where thermal management issues or other equipment requirements prevent use of such enclosures, alternate means should be provided to protect the equipment from environmental contaminants.

d. Facility design must ensure that any facility chemical, biological, radiological, nuclear or explosive (CBRNE) protection warning, alert, or protection systems also protect SCADA systems and utility equipment areas if the mission requires the facility to remain operational in a CBRNE environment. Appropriate coordination and systems integration must occur between SCADA and CBRNE protection systems so that appropriate facility environmental conditions are maintained if the facility experiences a CBRNE attack or incident.

7-2. Electronic threats

Electronic threats to SCADA systems include voltage transients, radio-frequency (RF) interference (RFI), RF weapons, ground potential difference and electromagnetic pulse (EMP). These threats can all be largely mitigated by proper design of the systems

a. SCADA controllers and field devices are vulnerable to voltage transients coupled through the facility power system from atmospheric (thunderstorm and lightning) effects, transmission and distribution system switching events, and switching of capacitors or inductive loads within the facility. Transient voltage surge suppression (TVSS) should be provided on the power supply circuits to all SCADA equipment and TVSS or optical isolation should be provided on all metallic control and communication circuits transiting between buildings. To avoid the effects of voltage transients, fiber optic cable should be used for all circuits entering or leaving a facility. Fiber media are available for most network applications at the supervisory and control levels (see paragraph 4-1). Field devices typically require metallic conduc-

tors, and where these must be run outside or between facilities, they should be provided with TVSS where they cross the facility perimeter.

(1) TVSS should be specified to comply with the testing requirements of ANSI C62.34 and should be installed in accordance with IEEE 1100. Selection of TVSS locations and connections should consider that it is most effective when connected directly to the terminals of the device to be protected and provided with a direct low-impedance path to the facility ground system. Incorrect installation methods can readily render TVSS protection ineffective. Protected and unprotected circuits should be physically segregated to avoid capacitive and inductive coupling that may bypass the TVSS. See figure 7-1 for an example of correct TVSS installation.

(2) Network surge protectors should be provided at all device connections, between the equipment port and the tap.

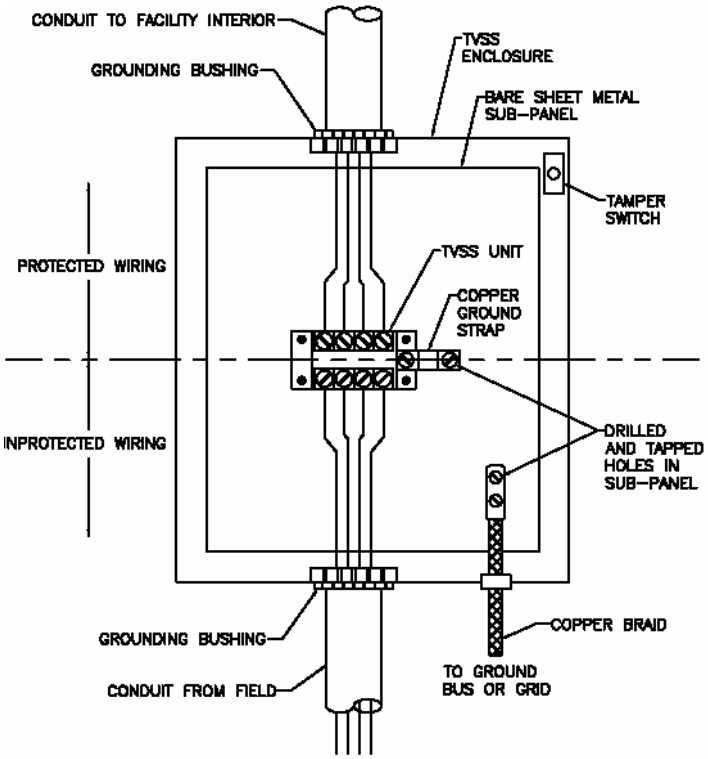


Figure 7-1. Signal level TVSS installation

b. C4ISR facilities often contain powerful radio frequency sources which may interfere with control system operation if coupled into control circuits. Other ambient sources of RFI may also exist including commercial signals, electronic counter measures (ECM), and radiated RFI from other equipment within the facility. Design and operation of SCADA systems should address measures to protect against RFI, including:

(1) Use of shielded twisted pair or twisted triple conductors for low-level signals.

(2) Installation of SCADA wiring in continuous metallic conduit systems.

(3) Use of metallic controller enclosures with RFI-gasketed doors.

(4) RFI-shielded control rooms and computer rooms.

(5) Maintenance practices that maintain the integrity of enclosures.

c. Effective shielding to limit RFI to within the required limits for C4ISR facilities is dependent upon the grounding and bonding practices required to provide a unified facility ground. The grounding practices for the earth electrode system, the building structure, the lightning protection system, the power system, and the signal reference system must be integrated to achieve a unified ground system. The particular grounding practices for each of these subsystems are illustrated in MIL-HDBK-419A, Grounding, Bonding, and Shielding for Electronic Equipment and Facilities. Additionally, specifications and installation designs for new equipment should include requirements to assure electromagnetic compatibility (EMC) between the equipment and the operating environment. These requirements should serve to minimize the susceptibility of the new equipment to EMI that may be present in the operating environment as well as to limit radiated emissions by the equipment to the environment and to existing equipment.

(1) Ground potential differences within a facility that may affect SCADA systems are mitigated by proper connection of equipment to the unified grounding system that is required to be provided for all C4ISR facilities. This system ties the electrical service, lightning protection, and all other facility grounds together into a single low-impedance ground grid. Additional grounding requirements for C4ISR facilities may be found in TM 5-690, Grounding and Bonding in C4ISR facilities.

(2) Each electrical room within the C4ISR facility which contains electrical equipment should be provided with a ground bus, connected to the unified ground system. SCADA equipment enclosures and internal ground buses should be connected directly to this ground bus, and should not rely solely on an equipment grounding conductor installed with the power supply circuit.

(3) All exterior metallic components which penetrate the building, such as metal piping, conduits, and ducts, should be grounded at the point of penetration. All conductive SCADA circuits entering the facility from outside should be provided with TVSS, effectively grounded to the ground grid at the point of entry.

(4) Low-voltage shielded cables must be installed to avoid ground loops, which can induce interfering currents on the signal common conductor. Unless otherwise dictated by the equipment manufacturer, cable shields should be grounded at the controller end only, with the instrument end left floating and insulated.

(5) On large multi-facility sites potential differences between the different facilities' ground systems caused by atmospheric electrical activity and electrical system faults can not be prevented, in spite of their common connection through the facility primary electrical distribution grounding system. SCADA circuits installed between facilities on these sites should always utilize fiber optic cables or optical signal isolation at the facility perimeter.

d. EMP protection requires magnetically continuous ferrous shielding which is not provided by the enclosures of typical SCADA sensors, controllers and actuators. For this reason, all electronic SCADA components must be assumed vulnerable to EMP and must be protected by location, external shielding, or replacement with pneumatic components.

(1) Whenever possible, all SCADA components should be located inside the C4ISR HEMP shield. Components that must be located outside the shield, such as sensors at an external fuel storage tank, may

be provided with a local HEMP-shielded enclosure and circuits routed back to the facility within a shielded conduit system or using pneumatic lines or optical fiber cable.

(2) EMP protection for non-conductive penetrations of the facility shield such as pneumatic tubing and fiber optic bundles uses the principle of "waveguide below cutoff" in which the lines penetrate the facility shield through a high aspect-ratio cylinder or waveguide. The waveguide must be made of a conductive material and must be continuously welded or soldered to the primary EMP shield so that current flowing on the waveguide can be discharged to the primary EMP shield.

(3) The maximum inside diameter of a penetration must be 4 inches or less to achieve a cutoff frequency of 1.47 GHz for a rectangular penetration and 1.73 GHz for a cylindrical penetration. The unbroken length of conducting material adjacent to the penetration must be a minimum of five times the diameter of the conducting material (i.e., pipe, duct) to attenuate by at least 100 dB at the required frequencies.

(4) The wave guide filter will be specified in terms of the attenuation over a specified range of frequencies in accordance with TM 5-858-5, Designing Facilities to Resist Nuclear Weapons Effects: Air Entrainment, Fasteners, Penetration Protection, Hydraulic Surge Protection Devices, and EMP Protective Devices.

e. Equipment located in electrical substations or other areas where electrical systems over 600V exist may be subject to particularly harsh transient voltage and transient electrical field conditions associated with power system faults, lightning strikes, and switching surges. This equipment should be qualified to the industry standards applicable to the withstand capability of protective relays, ANSI C37.90.1, C37.90.2 and C37.90.3, which apply to surge voltage, radiated EMI and ESD, respectively. Testing has shown that both STP and coaxial network communications circuits are subject to communications errors in high transient electric field conditions. For this reason, all network communication within the substation environment should be over fiber optic circuits. Even with a fiber communication circuit, the network equipment connected to the fiber may be susceptible to radiated fields or to conducted interference at the power supply. This equipment should be qualified to IEEE 1613, which requires automatic recovery from transient-induced communications disruptions with no false operation and no human intervention.

f. Portable RF weapons of van size down to brief-case size are now commercially available. Many of the above factors will also provide varying levels of protection against this emerging threat. For example, a HEMP shield should provide protections from RF Weapons external to the shield. However, it will provide no protection from an RF Weapon inside the shield. Thus, a critical aspect of protection from this threat is ensuring physical security protection plans, measures, and procedures recognize this threat and mitigate it. Examples of this are to insure that facility guards or security personnel are trained on this threat, are able to recognize RF Weapons, and that procedures are instituted for random or mandatory checks of all items entering the facility.

7-3. Physical security

In general, SCADA system equipment should be located inside secured areas having the same degree of security deemed appropriate for the supported systems. However, the electronic nature of these systems provides opportunities for compromise from both inside and outside the secured area that must be addressed.

a. HMI devices for controllers that provide access to the entire SCADA system shall use password-protected screen access with multiple levels of access control, and automatic logout routines with short

time settings. Password policies for screen savers shall be in compliance with established DoD policies (CJCSI 6510.01D).

b. Equipment enclosures and pull and junction boxes should be kept locked or secured with tamper-resistant hardware. Doors and covers should be provided with tamper switches or other means of detecting attempted intrusion, connected to the site security system. Tamper detection devices should be designed to detect the initial stages of access such as removal of fasteners, unlatching of doors, etc.

c. Raceways and enclosures for SCADA circuits external to the secured area should be designed to resist entry by unauthorized persons. Access to field wiring circuit conductors can potentially provide "back-door" entry to controllers for damaging over-voltages or transients. Outside raceways should consist of rigid steel conduits with threaded and welded joints and cast junction boxes with threaded hubs and tamper proof covers.

d. Conduits exiting the secured area should also be sealed to prevent them from being used to introduce hazardous or damaging gases or fluids into enclosures within the secured area.

7-4. Communication and information networks

Connections from SCADA systems to networks extending beyond the C4ISR facility or between facilities on a common site introduce the threat of attacks.

a. These attacks are of several types:

(1) Unauthorized user access (hacking).

(2) Eavesdropping; recording of transmitted data.

(3) Data interception, alteration, re-transmission.

(4) Replay of intercepted and recorded data.

(5) Denial of Service; flooding the network with traffic.

b. The best defense against these threats is to entirely avoid network connections with other networks within or external to the facility. If they must be used, data encryption techniques should be applied to all network traffic. The following additional means of enhancing security should also be considered:

(1) Physically disconnect when not in use; applicable to dial-up connections for vendor service.

(2) Use fiber optic media which cannot be tapped or intercepted without loss of signal at the receiving end.

(3) One-way traffic; alarm and status transmission only with no control permitted.

7-5. Software management and documentation

With the modern complexity and exposure to intentional software damage that can occur in modern industrial controls systems, it is a good practice to implement a Software Management and Documentation System (SMDS).

a. A SMDS system is software which resides on a dedicated computer on the plant network that monitors all activities of the control system. Such a system should be required for the control system in an important and complex military facility. It allows the facility administrator to do the following:

(1) Control who may use any SCADA application software and what actions can be performed

(2) Maintain a system-wide repository for historical storage of the application configuration files

(3) Identify exactly who has modified a control system configuration or application parameter, what they changed, where they changed it from, and when the change was made

(4) Assure that the control system configuration thought to be running the facility actually is

(5) Support application restoration following a catastrophic event

(6) Generate views into the Software Management System for more detailed analysis of configuration changes

b. Software Management and Documentation systems are available now from the major suppliers of industrial control systems. Having such a system provides the following additional benefits:

(1) Avoids maintaining incorrect or incompatible software versions

(2) Assures that there are not multiple versions of software on file

(3) Prevents multiple users from causing a conflict somewhere on the system

(4) Prevents legitimate changes from being reversed or overwritten

(5) Supports the availability of the system at its maximum

c. Among the specific software that such a system would secure are:

(1) PLC programs

(2) HMI screens

(3) SCADA configurations

(4) CAD drawings

(5) Standard Operating Procedures (SOP’s)

(6) Network Configurations

CHAPTER 8
COMMISSIONING/VALIDATION

8-1. General commissioning

Commissioning is the formal process of verifying and documenting that the installed SCADA system complies with and performs in accordance with the design intent, as defined in the design documentation described in chapter 10. Commissioning should be identified as a specific activity requiring its own planning, scheduling, management and monitoring during the design and construction process. A commissioning team should be assembled including representatives of all involved parties.

a. Those represented should include as a minimum:

(1) Government project management

(2) Facility operations

(3) Design engineer

(4) General contractor

(5) Mechanical subcontractor

(6) Electrical subcontractor

(7) System integrator

(8) Installation subcontractor

(9) Major equipment vendors

(10)Reliability engineer

b. Roles and responsibilities of the various parties within the commissioning process may vary with the agency and the type of project. In some cases, an independent engineer may be brought in to coordinate and oversee the commissioning process. If an independent engineer is not used, the design engineer should be retained to oversee the commissioning process. In either case, certain key components of the program that must be included for a successful outcome:

(1) A clear definition of the process and the parties' roles and responsibilities (Commissioning Plan).

(2) Integration of commissioning activities into the overall project schedule.

(3) An organized system of commissioning documentation.

(4) Development of written testing and verification procedures for every critical aspect of system performance.

(5) Review of these procedures by all affected parties prior to testing.

(6) Clear definition prior to testing of the criteria for acceptance.

(7) Procedures for correction and retesting in the case of failure.

c. Projects completed through the Military Construction (Mil Con) process automatically include commissioning. Facility managers must assure that commissioning is included in the scope of site-initiated projects.

8-2. Factory acceptance testing

A factory acceptance test and demonstration should be required in which the controller(s), I/O, and HMI hardware and software are verified to the extent possible without the actual field devices.

a. This test should demonstrate the following:

(1) Simulation of all inputs

(2) Operation of all outputs with dummy load

(3) Loop operation

(4) Control sequences

(5) Network communications

(6) HMI screens, displays, and alarms

(7) Operator control functions

(8) Physical and information security measures

b. PLC systems providing control of standby generators and paralleling switchgear should be factory-tested with the switchgear to demonstrate actual operation of the breakers and other controls with simulated utility and generator voltage and frequency sources.

8-3. Integrity testing

Pneumatic lines should be pressure tested per ISA RP 7.1 and checked for obstructions. Electrical conductors should be tested for continuity and insulation resistance according to industry standards for their voltage ratings.

8-4. Calibration

Instrument and actuator calibration should be completed prior to loop checkout or startup of systems. The calibration program should include the following:

a. All sensors, elements, indicators, transmitters and actuators should be calibrated from NIST-traceable standards according to the manufacturer’s instructions.

b. All calibration equipment should have current independent certification of accuracy.

c. Stroke actuators and verify control action, limits, and end switches.

d. Each calibrated instrument should be field-marked with a waterproof calibration tag bearing the range, setpoint, date and calibrator's initials.

e. An Instrument Certification sheet should be completed for each instrument and included in the system documentation. A detailed description is described in paragraph 8-9.

f. A Final Control Element Certification sheet should be completed for each control valve and included in the system documentation. A detailed description is described in paragraph 8-10.

8-5. Loop verification

The wiring of each control loop should be physically verified from the field device terminals to the controller. Cable, conductor, terminal board and terminal designations should be verified and marked off as such on a copy of the loop diagram or equivalent schematic or wiring diagram. Verification should be by signal tracing, continuity verification, or "ringing out". Tags and labels placed during construction should not be considered adequate verification.

a. Each control loop should be verified by injection of an appropriate pressure, voltage, or current signal. Use actual signals where available.

(1) Closely observe controllers, recorders, alarm and trip units, remote setpoints, ratio systems, and other control components. Make corrections as required. Following any corrections, retest the loop as before.

(2) Stroke all control valves, cylinders, drives and connecting linkages from the local control station and from the control room operator interface.

(3) Check all interlocks to the maximum extent possible. In addition to any other as-recorded documents, record all setpoint and calibration changes on all system documentation.

b. All analog loops should be tuned for optimum response using a closed-loop tuning method and the resulting gain, reset and rate recorded on the loop checkout sheet.

c. A Control Loop Checkout sheet should be completed for each loop. A detailed description is described in paragraph 8-11.

8-6. Functional performance testing

Performance testing of all systems should be performed to verify compliance with the specified sequences of operations and control diagrams. Functional performance testing consists of executing written step-by-step procedures in which a condition is initiated or simulated and the response of the system is noted and compared to the specified response. Functional performance tests must verify the following:

a. Manual and automatic control modes.

b. Normal system conditions and modes of operation.

c. Contingency conditions and modes of operation.

d. Effect of all operator controls.

e. Operation of all interlocks and permissives.

f. Confirmation of failure state of all outputs.

g. Physical and information security measures.

8-7. Software integrity

It is common for PLC programming errors to be identified during functional performance testing of SCADA systems. Typically these are easily corrected by revising the program logic via a laptop computer and testing is then continued. It is also common for unforeseen circumstances to dictate that a change be made to the specified sequence of operation in the field, again easily implemented by changing the PLC logic. These common startup processes contain the serious risk that a change made to correct misoperation at one point in the PLC control sequence may inadvertently affect the performance of other control sequences that have already been tested and accepted.

8-8. Re-commissioning

Whenever all or part of a SCADA system is modified, repaired or replaced, re-commissioning is required to verify that the portions of the system affected function correctly and that the work has not affected other portions of the system. The extent of re-commissioning required should be determined from the extent of the modifications.

a. For work that affects only devices and wiring external to the controller, the affected loops should be verified and functionally tested.

b. For changes to controller program logic or settings, the entire process or subsystem supported by that controller should be functionally tested, and the interface to the supervisory level HMI verified.

c. More extensive modifications may require re-commissioning of the complete SCADA system.

d. Functional performance testing for system certification must take place without operator intervention in the processor from beginning to end of the test. For this reason it is highly recommended that a complete pre-test be conducted, using the full functional performance test procedure, prior to undertaking the certification test.

8-9. Instrument certification sheet

Prior to functional performance testing, all sensors and instruments should be calibrated and documented using an Instrument Certification Sheet. Each Instrument Certification Sheet should include four sections:

a. Description of the Instrument such as Tag Number and Description;

b. A table to record the calibration of Transmitters and Indicators;

c. A table to record the calibration of Process Switches;

d. A list of the Calibration equipment used.

e. Instrument Description: The Instrument Description section should include the following information:

(1) Project name

(2) Project location

(3) Project number

(4) Certifier's name

(5) Certification date

(6) Control loop number

(7) Drawing references (such as P&ID, wiring diagram, etc.)

(8) Instrument tag number

(9) Instrument Description

(10) Instrument location

(11) Instrument manufacturer

(12) Instrument model number

(13) Instrument serial number, if applicable

(14) Instrument range

(15) Instrument setpoint and deadband (for switches)

f. A record of the transmitters and indicators calibration should contain the following data for both increasing and decreasing input signals at 0, 25, 50, 75 and 100 percent of span.

(1) Input value

(2) Output value

(3) Error

g. A record of the process switches calibration should contain the following data for both increasing and decreasing inputs at all setpoints:

(1) Setpoint value

(2) Operate value

(3) Error

h. Calibration equipment: The certification sheet should include the following information on the calibration equipment used.

(1) Type of Device

(2) Manufacturer and Model Number

(3) Accuracy

(4) NIST Traceability (Yes/No)

i. Definitions:

(1) Input: the process value

(2) Output: the measured value of the switch actuation point

(3) Span: the difference between the Maximum and Minimum value of the instrument

(4) Error: [(Output – Input) / Span] x 100%

8-10. Final control element certification sheet

Valve actuators and other final control elements should also be calibrated and documented. A final control element certification sheet should include four sections:

a. Description of the final control element such as tag number and description

b. A table to record the calibration of the I/P (current to pneumatic) converter, if applicable

c. A table to record the calibration of the final control element

d. A list of the calibration equipment used

e. The final control element description section should include the following information.

(1) Project Name

(2) Project Location

(3) Project Number

(4) Certifier's Name

(5) Certification Date

(6) Control Loop Number

(7) Drawing References (such as P&ID, Wiring Diagram, etc.)

(8) Control Valve Tag Number

(9) Control Valve Description

(10) Control Valve Location

(11) Control Valve Manufacturer

(12) Control Valve Model Number

(13) Control Valve Serial Number, if applicable

(14) Control Valve Actuator (Pneumatic or Electric)

(15) Control Valve Positioner (Direct or Reverse), if applicable

(16) Control Valve Positioner Input and Output Signal, if applicable

(17) Control Valve I/P Converter Input and Output Signal, if applicable

(18) Control Valve Failure Mode (open or close) on air failure, if applicable

(19) Control Valve Failure Mode (open or close) on power failure, if applicable

f. A record of the I/P (current to pneumatic) converter calibration should contain the following data for both increasing and decreasing inputs at 0, 25, 50, 75 and 100 percent of span:

(1) Input value

(2) Output value

(3) Error

g. A record of the final control element calibration should contain the following data for both increasing and decreasing signals at 0, 25, 50, 75 and 100 percent span:

(1) Input value

(2) Output travel (position)

(3) Error

h. The certification sheet should include the following information on the calibration equipment used.

(1) Type of Device

(2) Manufacturer and Model Number

(3) Accuracy

(4) NIST Traceability (Yes/No)

i. Definitions:

(1) Input: the control signal from the controller (PLC)

(2) Output: the measured value of the valve controller to the valve

(3) Travel: the valve percent open (not all valves are linear)

(4) Error: [(Output – Input) / Span] x 100%

8-11. Control loop checkout sheet

The control system integrator should perform loop checkouts for each control loop in the system and provide suitable documentation certifying that the loop is tuned and operating properly. The control loop checkout sheet should have a section verifying each of the six steps described below. When this has been verified and signed off, the functional performance testing (FPT) can be started.

a. Verify Mechanical Field Installation; that are no leaks;

(1) Motors and Pumps

(2) Valves and Dampers

b. Verify that all instruments are calibrated correctly for the specified ranges and setpoints;

(1) Pressure instruments

(2) Flow instruments

(3) Level instruments

(4) Temperature instruments

(5) Analysis instruments

c. Verify Electrical power wiring;

(1) Incoming power sources for proper voltage

(2) Field cables properly installed and identified

(3) Circuit breakers sized and operating correctly

(4) Fuses sized correctly inside control panels

d. Verify control system Input and Output wiring;

(1) Digital (switch) inputs

(2) Digital (on/off) outputs

(3) Analog (transmitters) inputs

(4) Analog (VFD's, valves, and meters) outputs

e. Verify software logic is complete;

(1) Correct programs are loaded

(2) Factory Acceptance Test (FAT) thoroughly completed

(3) Software Management Practices in place

f. Verify HMI (or OIT) points and displays are complete;

(1) Graphic screens and screen navigation

(2) Alarm screens and operator actions

(3) Trend Displays and Data Archiving configured properly

g. The software logic and HMI/OIT should have been verified during the factory acceptance test.

h. The Control Loop Checkout Sheet should have a section verifying each of the steps describe above. When this has been verified and signed off, the Functional Performance Testing can be started.

CHAPTER 9
MAINTENANCE PRACTICES

9-1. General maintenance

A comprehensive maintenance program is critical to attaining long-term reliable performance of SCADA systems. Periodic device calibration, preventive maintenance, and testing allow potential problems to be identified before they can cause mission failure. Prompt corrective maintenance assures reliability by minimizing downtime of redundant components.

9-2. Preventive maintenance

The SCADA system should be part of the overall preventive maintenance (PM) program for the facility. Table 9-1 provides a list of recommended maintenance activities and frequencies for SCADA systems and their components. Preventive maintenance schedules for SCADA components and subsystems should be coordinated with those for the mechanical/electrical systems they serve to minimize overall scheduled downtime.

Table 9.1 Recommended maintenance activities.

Activity	Frequency
Pneumatic Systems/Components	
Check Regulators and Filters	Monthly
Inspect Tubing and Piping	Monthly
Actuate Pressure Switches	6 Months
Actuate (Stroke) Valves and Actuators	6 Months
Calibrate Switches and Sensors	Yearly
Calibrate Pressure Gauges	Yearly
Calibrate Thermometors	Yearly
Electrical/Electronic Systems	
Lamp Test/Verify Indicators	Monthly
Inspect Enclosures for Dirt, Water, Heat	Monthly
Actuate (Stroke) Valves and Actuators	6 Months
Actuate Switches	6 Months
Run PLC Diagnostics	6 Months
Calibrate Sensors and Transmitters	Yearly
Calibrate Meters	Yearly
Calibrate Actuators	Yearly
Test Batteries	6 Months
Test Automatic control Sequences	Yearly
Verify Alarms	Yearly
Software Maintenance and Patching	2 Months
Anti-virus Definition Updates	Monthly
Inspect Wire, Cable and Connections	Monthly

a. Many components of SCADA systems, such as dead-bus relays, are not required to function under normal system operating modes. For this reason the system should be tested periodically under actual or simulated contingency conditions. These tests should approach as closely as possible the actual off-

normal conditions in which the system must operate. For example, SCADA for standby generator plants should be tested by interrupting the utility source as far upstream of the normal service as possible.

b. Periodic system testing procedures can duplicate or be derived from the functional performance testing procedures discussed in chapter 8.

c. The SCADA software maintenance should include timely updates of any new versions from the supplier and testing to verify proper installation on the SCADA computer. In addition, software anti-virus updates should be maintained. This should be performed any time after the computer is connected to the Internet. Normal operation requires that the SCADA computer not be connected to the Internet.

d. Electrical power systems, both AC and DC, serving SCADA systems should be maintained in accord with the requirements of TM 5-692-1 and NFPA 70B.

9-3. Concurrent maintenance

Concurrent maintenance is defined as testing, troubleshooting, repair or replacement of a component or subsystem while redundant component(s) or subsystem(s) are serving the load. The ability to perform concurrent maintenance is critical to attaining the specified reliability/availability criteria for C4ISR facilities and must be designed into the SCADA system. Where SCADA components are associated with equipment that has redundancy and therefore are not themselves redundant, their maintenance should be scheduled to occur during maintenance of the associated equipment. SCADA components and controllers that are redundant must be capable of being taken out of service, repaired or replaced and tested without interfering with the operation of the redundant component.

9-4. Reliability centered maintenance

Reliability-Centered Maintenance (RCM) is an approach for developing an effective and efficient maintenance program based on the reliability characteristics of the constituent parts and subsystems, economics, and safety. RCM provides a logical, structured framework for determining the optimum mix of applicable and effective maintenance activities needed to sustain the operational reliability of systems and equipment while ensuring their safe and economical operation and support. RCM has changed the approach to preventive maintenance, and can be considered the “next step” in moving from a trial and error based approach to establishing PM frequencies to an intelligent approach to maintenance planning. A significant byproduct of the application of SCADA systems to the control of C4ISR facilities is the large amount of operational data made available through the trending and data storage features of the SCADA. This operational data can be used for automated performance monitoring of mechanical and electrical systems that can support a RCM approach. Detailed information about the application of RCM to C4ISR facilities can be found in Chapter 3 of TM 5-698-1, and in TM 5-698-2.

9-5. Operations and maintenance documentation

The design agency should perform an O&M analysis to determine the O&M data required to support maintenance of the SCADA system by the using government agency. This analysis should be coordinated with the using government agency to determine maintenance parameters and O&M data that are available to the using government agency. Typical O&M data requirements include the following items:

a. System documentation as defined in chapter 10.

b. Minimum spare parts list.

c. Recommended spare parts list.

d. Recommended onsite test equipment.

e. Recommended O&M training.

f. Recommended O&M to be performed by contract.

9-6. Spare parts stocking

An adequate on-site stock of spare parts is essential to obtaining high availability of SCADA systems. Reliability calculations demonstrating compliance with “six nines” criteria typically use repair times based on “replace with spare” which are shorter than those for “repair failed component”. If on-site stocks are inadequate, actual availabilities will be significantly less than these calculated values.

a. Minimum recommended stocking levels include the following. These quantities may need to be increased for components which are used in large numbers in the facility:

(1) Manufacturer’s recommended spare parts list.

(2) One each of all line replaceable boards or modules.

(3) Six each power and control fuses used in the system.

(4) Tools required to terminate coaxial on fiber optic cables.

b. Specifications should also require that the following be furnished with each system:

(1) Laptop computer loaded with software required to access controllers.

(2) Licenses for all software installed on the system.

(3) Permission to modify program code.

(4) Spare cables for connecting computer to controllers.

9-7. Technical support

The design agency should specify functional areas of the operating system and/or equipment where a technical representative will be furnished by the manufacturer for training, test, checkout, validation, or pre-operational exercises. Ongoing O&M of SCADA system software may require technical support from the system vendor or from agency technical personnel not located at the facility. Commercial SCADA software typically has provisions for remote modem access that permit this type of support from the vendor’s location or an agency central engineering group. Such remote access provisions represent a vulnerability to “hacking” and must be used with great caution. They should be monitored when in use and physically disconnected when not in use. PLC suppliers have indicated that they are unable to provide a firewall that will protect the controller program in the event of unauthorized access to the HMI processor. Password protection policies for all SCADA systems, including PLC’s, shall be in compliance with established DoD policies. The DoD policy is established by the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01 D, Information Assurance (AI) and Computer Network Defense (CND).

These policies require that the default password that came from the control supplier be changed when placed into operation at the facility.

CHAPTER 10
DOCUMENTATION AND CHANGE CONTROL

10-1. General

Complete and accurate documentation is critical to the commissioning and ongoing maintenance and operation of a SCADA system and should be a high priority of design contract administration.

a. SCADA system documentation provided by the system designer and/or system integrator should include the following:

(1) One-line diagrams

(2) Process and instrumentation diagrams (P&IDs)

(3) Sequences of operation

(4) Instrument data sheets

(5) Points list

(6) Loop diagrams or I/O wiring diagrams

(7) Binary logic diagrams

(8) Control schematics

(9) PLC program listing

(10) HMI description (screen prints and database)

(11) Software configuration management documentation

(12) Facility physical and information security policies

b. All SCADA documentation should be furnished in both hard copy and appropriate electronic format. Electronic format should be capable of revision; i.e. scanned documents or portable document format (pdf) files are not acceptable, although pdfs may be submitted as archive copies in addition to revisable files.

c. All system documentation for C4ISR facilities should be treated as sensitive and this applies to SCADA system diagrams and documentation as well. At a minimum, document security measures should include:

(1) Marking all documents For Official Use Only (FOUO)

(2) Controlling access to documents

(3) Properly destroying outdated or unused documents

10-2. Symbols and identification

Individual control loops should be identified by loop number following the convention established by ISA S5.1. Each instrument, actuator and control point should have a unique tag number incorporating the loop number and identification letters per table 1 of ISA S5.1. All equipment and instruments should be consistently identified by their complete tag number on all drawings and points lists.

10-3. Process and Instrumentation Diagram (P&ID)

P&IDs should be provided for all mechanical systems. P&IDs should depict all components of mechanical systems including vessels, pumps, compressors, chillers, heat exchangers, piping, valves and instruments and the control relationships between them. Symbols used should comply with ISA S5.1 - Instrumentation Symbols and Identification and ISA 5.3 - Graphic Symbols for Distributed Control/Shared Display Instrumentation, Logic and Computer Systems.

10-4. Sequences of operation

Written sequences of operation should be provided for all control loops.

a. Sequences of operation should include the following minimum information:

   (1) Manual and automatic control modes;

   (2) Normal system conditions and modes of operation;

   (3) Contingency conditions and modes of operation;

   (4) Effect of all operator controls;

   (5) Description of all interlocks and permissives;

   (6) Identification of failure state of all outputs.

10-5. Instrument data sheets

Instrument data sheets should be provided per ISA S20

10-6. Points list

A points list should be provided that includes all real and virtual input, output and control points.

a. Provide the following information, where applicable, for each point:

   (1) System

   (2) Equipment

   (3) Loop number

   (4) Tag number

(5) Controller, rack and slot

(6) Point type

(7) Field location

(8) Range

(9) Failure state

b. A points list is located in appendix D.

10-7. Loop diagrams

Loop diagrams define the physical wiring for each loop from each instrument or actuator to the controller. All field devices, terminal boards, junction boxes, etc. are depicted along with the signal type and range. These drawings are the basis for verification of all SCADA system field wiring, instrument calibration, and loop tuning. All devices, terminals, cables and conductors must be completely identified on the loop diagrams per ISA S5.4 – Instrument Loop Diagrams. A loop diagram is located on page D-2.

10-8. Binary logic diagrams

Binary logic diagrams are flowcharts that depict all discrete logic using Boolean logic symbols. Logic diagrams should comply with ISA S5.3 – Binary Logic Diagrams. A binary logic diagram is located on page D-3.

10-9. Control schematics

Control schematics show the interface between the SCADA system and the internal wiring of related equipment such as motor starters, pump control panels, generator control panels, etc. Proper development of control schematics requires a significant effort on the part of the SCADA system integrator because the standard drawings provided by manufacturers of these related system drawings are typically inconsistent in format, symbols and content, requiring that they be redrafted by the integrator to provide an integrated documentation package. Symbols used on control schematics should comply with the previously referenced ISA standards and ANSI Y14.15. – Electrical and Electronic Diagrams.

10-10. PLC program listing

A documented listing of the complete program of each PLC should be provided. Documentation should consist of an English-language description of the function of each logic rung inserted into the listing.

10-11. Change control

All SCADA documentation should include creation date, issue date, revision data, and revision history in a format that is consistent across all documents. A document database or spreadsheet should be maintained that provides a current listing of all documents and their revision status.

a. The database should include the following:

(1) Document Type

(2) Document Number

(3) Page Number

(4) Sheet Number

(5) Title

(6) Current Revision

(7) Revision Date

b. Each submittal of SCADA documentation should include an updated submittal of the document database. The database should be provided in electronic format and maintained on an ongoing basis by the facility manager after system commissioning. All changes made to the system should be promptly reflected by revising the documentation and the database and distributing copies of the revised documentation and updated database to the field.

CHAPTER 11
PROJECT PLANNING AND IMPLEMENTATION

11-1. General planning

This chapter has two objectives: to outline the basic process and key issues in planning, design, construction and commissioning of a SCADA project; and to summarize key points from the rest of the technical manual in a way that can serve as a checklist for the facility manager during the implementation process. References to other chapters of this TM are given in parentheses. The implementation process may be considered to include the following six stages. Each of these stages contains key milestones that must be met and issues that must be addressed and resolved before moving on to the next stage.

a. Project team selection

b. Project initiation

c. Requirements definition

d. System design

e. Construction

f. Commissioning

11-2. Project team selection

The following key personnel or their representatives make up the recommended project implementation team. Although time commitment and degree of involvement will vary with the stage of the project, all team members should be involved from the planning stage and remain in the communications loop throughout the duration of the project. It is a mistake to delay the involvement of maintenance staff or the commissioning agent until the end of the design stage or the construction stage; making changes at this late stage based on their input will undoubtedly impact schedule and cost. If the procurement method used allows it, involving the installing contractor(s) from the start is also beneficial.

a. Project manager

b. Facility manager

c. Operations and maintenance manager

d. Controls technician

e. Mission commander

f. Utility system designer(s)

g. SCADA system designer

h. Physical security specialist

i. Information security specialist

j. Reliability analyst

k. Commissioning agent

11-3. Project initiation

The objective of the project initiation stage is to assemble the team, focus them on the objectives of the project as a common mission, and put in place the tools necessary for the team to accomplish that mission. Specific tasks that must be accomplished for the project to move forward effectively include:

a. Define the project scope and schedule.

b. Establish the communication processes to be followed.

c. Establish a document management system.

d. Establish a process for tracking issues and documenting their resolution.

11-4. Requirements definition

The objective of the requirements definition stage is to clearly define the criteria which will serve as the basis for design of the system. The result should be a written design basis document against which the design can be verified as it progresses. Meeting the criteria defined in this stage becomes the primary measure of the technical success of the project.

a. Top level criteria:

(1) Reliability, Availability, Maintainability (RAM) criteria matched to mission chapter 5.

(2) Configuration and level of redundancy matched to M/E system design (paragraph 3-9).

(3) Type of HMI and extent of manual control capability matched to staffing levels and qualifications (chapter 6).

(4) Established design standards for C4ISR facilities (appendix A).

(5) Physical security policies (paragraph 7-3).

(6) Information/network security policies (paragraph 7-4).

b. Detail level criteria:

(1) M/E systems sequence of operations/control strategy clearly defined (paragraph 10-4).

(2) Required failure states of all valves and other equipment identified (paragraph 10-4).

(3) Define all contingency conditions to be protected against (paragraph 10-4).

(4) Determine data presentation format, number of screens, etc. (chapter 6).

(5) Physical security provisions defined (paragraph 7-3).

(6) Information/network security provisions defined (paragraph 7-4).

11-5. Design

The objective of the design stage is to translate the design basis document into a system design and document the design clearly and completely so that it can be constructed properly, commissioned completely, and operated and maintained reliably and efficiently. The primary criteria for design documents should be completeness of detail and clarity of design intent. The system should be fully designed during this stage, where careful review can take place, rather than leaving details to be "worked out" in the field during construction and commissioning.

a. Key issues to be addressed in this stage include:

(1) Develop a system architecture schematic or block-diagram drawing (chapter 3).

(2) Select network communications media (fiber optic, etc.) appropriate to the physical and electrical environments (paragraph 4-2).

(3) Analyze the proposed architecture to verify it meets the RAM criteria (chapter 4 and paragraph 5-2).

(4) Select system vendor(s) and hardware considering;

(a) In-service history

(b) Vendor support

(c) RAM data

(d) Staff experience

b Detailed design documents should be formally reviewed by all team members at established points in the design process. The number of review submittals may vary with the size and complexity of the project, but a minimum of two submittals prior to completion is recommended. These reviews should verify the following:

(1) All symbols, abbreviations and line types are clearly defined (paragraph 10-2).

(2) A complete and consistent equipment and cable identification (tag number) scheme is used (paragraph 10-2).

(3) Loop and Binary Logic Diagrams or Descriptions are provided (paragraphs 10-7 and 10-8).

(4) A complete input/output points list has been provided (paragraph 10-6).

(5) Open protocols and readily available hardware are specified (paragraphs 3-6 and 4-4).

(6) Design has been analyzed for reliability, availability and maintainability criteria (chapter 5).

(7) Power supplies match system RAM and redundancy levels (paragraph 5-6).

(8) Physical segregation exists between redundant components and paths (paragraph 3-9 and 5-7).

(9) Layout of operator controls and indicators and HMI screens has been clearly specified for human factors considerations (paragraph 6-5).

(10) Environmental protection level of devices and enclosures is clearly specified and appropriate for their location (paragraph 7-1).

(11) The design of the grounding and surge protection system is clearly detailed and specified (paragraph 7-2).

(12) Control equipment is located within secure spaces (paragraph 7-3).

(13) External communication links are secure (paragraph 7-4).

(14) The design includes all test and measurement provisions needed for commissioning (chapter 8).

(15) All components can be tested and maintained without interrupting the mission (paragraph 9-3).

(16) Physical security provisions are clearly defined (paragraph 7-3).

(17) Information/network security provisions are clearly defined (paragraph 7-4).

11-6. Construction

The objective of the construction stage is to install and place into operation the SCADA system hardware and software in compliance with the design documents. This stage should utilize standard construction management tools and techniques for managing schedule, cost, contract changes, etc. However, for a SCADA project, there are some additional considerations that must be addressed:

a. A change management process should be established assuring that all field issues receive appropriate technical review (paragraph 10-11).

b. All changes should be documented on an ongoing basis, and design documents kept current, rather than leaving this to an end-of-project “as-built drawings” task (paragraph 10-11).

c. Operations and maintenance data should be assembled and reviewed during the construction process and must be complete prior to commissioning (paragraph 9-5).

11-7. Commissioning

The objective of the commissioning stage is to obtain formal verification that the installed SCADA system complies with and performs in accordance with the design intent as defined in the Design Basis and the detailed design documents. Key aspects of commissioning include:

a. Preparation of a commissioning plan (paragraph 8-1).

b. Factory acceptance testing of PLC hardware and software (paragraph 8-2).

c. Integrity testing of installed devices and conductors (paragraph 8-3).

d. Instrument calibration and loop verification (paragraphs 8-4 and 8-5).

e. Preparation and review of test procedures (paragraphs 8-2, 8-3 and 8-6).

f. Functional performance testing (paragraph 8-6).

g. Verification of physical and information/network security provisions (paragraphs 7-3 and 7-5).

h. Verification of complete system documentation (chapter 10)

APPENDIX A

REFERENCES

REQUIRED PUBLICATIONS

Government Publications

Department of the Army:

CJCSI 6510.01D
Information Assurance (IA) and Computer Network Defense (CND) dated 15 June 2004 [cited in paragraphs 7-3a and 9-7].

MIL-HDBK-419A
Grounding, Bonding, and Shielding for Electronic Equipment and Facilities [cited in paragraph 7-2c]

TM 5-690
Grounding and Bonding in Command, Control, Communication, Computer, Intelligence Surveillance and Reconnaissance (C4ISR) Facilities [cited in paragraph 7-2c(1)]

TM 5-692-1
Maintenance of Mechanical and Electrical Equipment at Command, Control, Communications, Intelligence, Surveillance and Reconnaissance (C4 ISR) Facilities – Recommended Maintenance Practices [cited in paragraph 9-2c]

TM 5-693
Uninterruptible Power Supply System Selection, Installation, and Maintenance for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities [cited in paragraph 5-6e]

TM 5-698-1
Reliability/Availability of Electrical & Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities [cited in paragraph 9-4]

TM 5-698-2
Reliability Centered Maintenance for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities [cited in paragraph 9-4]

TM 5-858-5
Designing Facilities to Resist Nuclear Weapons Effects: Air Entrainment, Fasteners, Penetration Protection, Hydraulic Surge Protection Devices, and EMP Protective Devices [cited in paragraph 7-2d4]

Non-Government Publications

American National Standards Institute
1819 L Street, NW
Washington, DC 20036

ANSI C37.90.1
Guide for Surge Withstand Capability Tests [cited in paragraph 7-2e]

ANSI C37.90.2
Withstand Capability of Relay Systems to Radiated Electro-Magnetic Interference from Transceivers [cited in paragraph 7-2e]

ANSI C37.90.3
Electrostatic Discharge tests for Protective Relays [cited in paragraph 7-2e]

ANSI C62.34
Standard for Performance of Low Voltage Surge Protective Devices (Secondary Arrestors) [cited in paragraph 7-2a(1)]

ANSI Y14.15
Electrical and Electronic Diagrams [cited in paragraph 10-9]

International Electrotechnical Commission

IEC/EN 60529
Degrees of Protection Provided by Enclosures (IP Code) [cited in paragraph 7-1c]

IEC 61508
Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems [cited in paragraph 3-8]

Institute of Electrical and Electronic Engineers
445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855-1331

IEEE 242
Recommended Practice for Protection and Coordination of Industrial and Commercial Power Systems [cited in paragraph 5-6f]

IEEE 493
Recommended Practice for Design of Reliable Industrial and Commercial Power Systems [cited in paragraph 5-4b]

IEEE 1100
IEEE Recommended Practice for Powering and Grounding Sensitive Electronic Equipment [cited in paragraph 7-2a(1)]

IEEE 1613
Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations [cited in paragraph 7-2e]

Instrumentation, Systems, and Automation Society
67 Alexander Drive, Research Triangle Park, NC 27709

ISA RP7.1
Pneumatic Control Circuit Pressure Test [cited in paragraph 8-3]

ISA S5.1
Instrumentation Symbols and Identification [cited in paragraphs 10-2, 10-3, and 10-9]

ISA S5.2
Binary Logic Diagrams for Process Controls [cited in paragraphs 10-8 and 10-9]

ISA S5.3
Graphic Symbols for Distributed Control/Shared Display Instrumentation, Logic and Computer Systems [cited in paragraphs 10-3, 10-8 and 10-9]

ISA S5.4
Instrument Loop Diagrams [cited in paragraphs 10-7 and 10-9]

ISA S20
Form Templates [cited in paragraph 10-5]

National Electrical Manufacturers Association
1300 North 17th Street, Suite1847, Rosslyn, VA 22209

NEMA 250
Enclosures for Electrical Equipment (1000 Volts Maximum) [cited in paragraph 7-1c]

National Fire Protection Association
One Batterymarch Park, PO Box 9101, Quincy, MA 02269-9101

NFPA 70B
Recommended Practice for Electrical Equipment Maintenance [cited in paragraph 9-2c]

RELATED PUBLICATIONS

Government Publications

Department of the Army:

TM 5-691
Utility Systems Design Requirements for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities

TM 5-694
Commissioning of Electrical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities

TM 5-697 Commissioning of Mechanical Systems for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities

TM 5-698-3
Reliability Primer for Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR) Facilities

TM 5-858-7
Designing Facilities to Resist Nuclear Weapon Effects - Facility Support Systems

Non-Government Publications

Institute of Electrical and Electronic Engineers
445 Hoes Lane, PO Box 1331, Piscataway, NJ 08855-1331

IEEE 485
IEEE Recommended Practice for Sizing Load-Acid Batteries for Stationary Applications (1997)

Instrumentation, Systems, and Automation Society
67 Alexander Drive, Research Triangle Park, NC 27709

ISA S5.5
Graphic Symbols for Process Displays

ISA S51.1
Process Instrumentation Terminology

ISA S7.0.01
Quality Standard for Instrument Air

ISA 84.01
Application of Safety Instrumented Systems for the Process Industries

Reliability Analysis Center
201 Mill Street, Rome, NY 13440-6916

NPRD 95
Non Electronic Parts Reliability Data

"Design and Implementation of a UCA-based Substation Control System" by Mark Adamiak, Ashish Kulshretha, presented at MYPSYCON 2003, November 6, 2003, Minneapolis, Minnesota

"Whats Your Color? – Human Influence in Screen Design", by S. Hall, K. Cockerham and D. Rhodes, IEEE Industry Applications Magazine, March/April 2002.

APPENDIX B

GLOSSARY

1. Glossary

-A-

ALTERNATING CURRENT (AC). Refers to an electrical system in which the supply voltage, and thus the current flowing is a load, alternates polarity at a specified frequency. Alternating current systems are typically supplied from rotating electrical generators.

AVAILABILITY. A measure of the degree to which an item is in an operable and commitable state at the start of a mission when the mission is called for at an unknown (random) time. (Item state at start of a mission includes the combined effects of the readiness-related system reliability and maintainability parameters, but excludes mission time.) (MIL-STD-721C, now canceled). In its simplest definition, availability is uptime divided by downtime. In terms of reliability (MTBF or and maintainability (Mean Time to Repair or Mean Downtime), inherent and operational availability are defined as:

A_o. Operational Availability. The percentage of time that a system is available for use based on its operational reliability and maintainability, and logistics factors, such as delay times. Usually defined by the following steady-state equation:

$$A_o = \frac{MTBM}{MTBM + MDT}$$

A_i. Inherent Availability. The percentage of time that a system is available for use based only on its inherent reliability and maintainability characteristics. Usually defined by the following steady-state equation:

$$A_i = \frac{MTBF}{MTBF + MTTR}$$

-C-

COAXIAL CABLE (COAX). A cable construction in which a single copper conductor is insulated and then covered with a concentric braided copper shield which also serves as a current carrying conductor.

COMMISSIONING. The process of verifying and documenting that systems or equipment perform in accordance with their specifications and design intent.

CONTROL SELECTIVITY. The degree to which a control can be manipulated without accidentally activating other controls. A common problem is to position buttons or keys too closely, leading to the wrong button being pressed.

-D-

DIRECT CURRENT (DC). Refers to an electrical system in which the supply voltage, and thus the current flowing in a load, is fixed in polarity. Direct current systems are typically supplied from storage batteries.

DIRECT DIGITAL CONTROL (DDC).A control system used for electronic measurement and control of building HVAC systems.

-E-

ELECTROMAGNETIC COMPATIBILITY (EMC). The extent to which a piece of hardware will tolerate electrical interference from other equipment and will interfere with other equipment.

ELECTROMAGNETIC INTERFERENCE (EMI). Any spurious effect produced in the circuits or element of the device by external electromagnetic fields.

ELECTROMAGNETIC PULSE (EMP). Electromagnetic radiation from a nuclear explosion. The resulting electric and magnetic fields may couple with electrical/electronic systems to produce damaging current and voltage surges.

ELECTROSTATIC DISCHARGE (ESD). A transfer of electric charge between bodies at different electrostatic potentials caused by direct contact or induced by an electrostatic field.

ENERGY MANAGEMENT SYSTEM (EMS). In the commercial building industry, a control system designed to monitor and maintain environmental conditions by controlling heating, ventilation and air conditioning systems. In the electric utility industry, a control system designed to monitor and control power generation and transmission facilities.

ERROR. The algebraic difference between the indicated value and the true value.

EUROPEAN NORM (EN). A standard that has been adopted by the countries of the European Union.

-F-

FAILURE. The event, or inoperable state, in which any item or part of an item does not, or would not, perform as previously specified.

-G-

GRAPHICAL USER INTERFACE (GUI). A user interface based on graphics (icons, pictures, menus) instead of text; uses a mouse as well as keyboard, as an input device.

-H-

HEATING VENTILATING AND AIR CONDITIONING (HVAC). Refers to the systems and equipment used to maintain environmental conditions of temperature and humidity within specified ranges.

HIGH ALTITUDE ELECTROMAGNETIC PULSE (HEMP). A strong electromagnetic field of short duration produced by detonation of a nuclear warhead in the atmosphere.

HUMAN-MACHINE INTERFACE (HMI). Human-machine interface between user and terminal system that consists of a physical section and a logical section dealing with functional operation states.

-I-

INHERENT AVAILABILITY (A_i). A measure of availability that includes only the effects of an item design and its application, and does not account for effects of the operational and support environment.

INHERENT AVAILABILITY (A_i). A measure of availability that includes only the effects of an item design and its application, and does not account for effects of the operational and support environment. Sometimes referred to as "intrinsic" availability.

INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS (IEEE). An international professional organization of electrical and electronics engineers which develops standards and recommended practices for the design, operation and maintenance of facility electrical systems.

INSTRUMENTATION, SYSTEMS AND AUTOMATION SOCIETY (ISA). A professional organization that develops standards for the design and documentation of control and automation systems.

-L-

LOCAL AREA NETWORK (LAN). A network operated within a single facility or group of facilities in close physical proximity.

-M-

MEAN DOWN TIME (MDT). The average time a system is unavailable for use due to maintenance.

MEAN TIME BETWEEN FAILURE (MTBF). A basic measure of reliability for repairable items. The mean number of life units during which all parts of the item perform within their specified limits, during a particular measurement interval under stated conditions.

MEAN TIME BETWEEN MAINTENANCE. The mean time between all maintenance activities.

MEAN TIME TO REPAIR (MTTR). A basic measure of maintainability. The sum of corrective maintenance times at any specific level of repair, divided by the total number of failures within an item repaired at that level, during a particular interval under stated conditions.

-N-

NATIONAL FIRE PROTECTION ASSOCIATION (NFPA). A codes and standards producing organization concerned with protection of life and property. Commonly used NFPA standards include 101-Life Safety Code, and 70-National Electrical Code.

NATIONAL INSTITUE OF STANDARDS AND TECHNOLOGY (NIST). An organization that establishes and maintains standard quantities used for calibration of measurement devices.

NETWORK. A system, typically using physical transmission media, to allow communication between multiple electronic devices.

-P-

PACKET. A group of data assembled for transmission on a network.

P CONTROLLER. A controller having only proportional control action (see paragraph 2-4).

PREVENTIVE MAINTENANCE. The practice of periodically performing maintenance activities on a system or equipment with the intended purpose of preventing unscheduled outages of the equipment due to component failure.

PI CONTROLLER. A controller having proportional and integral control action (See paragraph 2-4).

PID CONTROLLER. A controller having proportional, integral and derivative control action (see paragraph 2-4).

POINT. A single variable within a control system. This term usually refers to the inputs and outputs of the system, but can also be applied to variables that exist only within the internal logic of the processor, which may be called virtual points or control points.

POINTS LIST. A tabulation of all the system points that includes relevant data for each point. See Appendix D-1.

PROCESS VARIABLE. The quantity in a process or system that is to be controlled to a desired value.

PROGRAMMABLE LOGIC CONTROLLER (PLC). A microprocessor based controller capable of accepting input signals, performing pre-programmed digital control logic or analog control action, and providing output signals.

PROTOCOL. A set of rules for assembling and transmitting data over a network.

-R-

RADIO FREQUENCY INTERFERENCE (RFI). Electromagnetic radiation which is emitted by electrical circuits carrying rapidly changing signals, as a by-product of their normal operation and which causes unwanted signals (interference or noise) to be induced in other circuits.

RANDOM ACCESS MEMORY (RAM). The most common computer memory which can be used by programs to perform necessary tasks while the computer is on; an integrated circuit memory chip allows information to be stored or accessed in any order and all storage locations are equally accessible.

REDUNDANCY. The existence of more than one means for accomplishing a given function. Each means of accomplishing the function need not necessarily be identical.

a. N+X Redundancy: N is the number of units required to meet the load. X additional (redundant) units are provided for a total quantity of N+X units. Common configurations are N+1 and N+2.

b. X times N or XN Redundancy: N is the number of units required to meet the load. The total number of units installed is a multiple X of that number. A common configuration is 2N.

RELIABILITY. (1) The duration or probability of failure-free performance under stated conditions. (2) The probability that an item can perform its intended function for a specified interval under stated conditions.

RELIABILITY-CENTERED MAINTENANCE (RCM). A disciplined logic or methodology used to identify preventive and corrective maintenance tasks to realize the inherent reliability of equipment at a minimum expenditure of resources.

RESISTANCE TEMPERATURE DETECTOR (RTD). A device whose electrical resistance varies predictably with temperature, used as a temperature sensor in automatic control systems.

-S-

SELECT-BEFORE-OPERATE. Refers to a program requirement that a particular device, such as a valve, to be controlled be selected by pointing at and clicking on a screen icon or other means before an operation such as open or close may be selected to apply to that device. This reduces errors by requiring a two-step process for manual control.

SENSOR. See transducer.

SHIELDED TWISTED PAIR (STP). A cable construction consisting of two copper conductors, twisted together to reduce inductive coupling and covered with an electrically continuous metallic foil or tape shield to reduce capacitive coupling.

SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA). An electronic system that provides for monitoring and controlling systems or processes remotely.

-T-

TRANSDUCER. An element or device which receives information in the form of one quantity and converts it to information in the form of the same or a different quantity.

TRANSMITTER. A transducer which responds to a measured variable by means of a sensing element, and converts it to a standardized transmission signal which is a function of only the measured variable.

TRANSIENT VOLTAGE SURGE SUPPRESSION (TVSS). A protective device for limiting transient voltages by diverting or limiting surge current; it also prevents continued flow of follow current while remaining capable of repeating these functions.

-U-

UNINTERRUPTIBLE POWER SUPPLY (UPS). A device that is inserted between a primary source and the primary power input of equipment to be protected for the purpose of eliminating the effects of transient anomalies or temporary outages.

UNSHIELDED TWISTED PAIR (UTP). A cable construction consisting of two copper conductors, twisted together to reduce inductive coupling.

-V-

VARIABLE FREQUENCY DRIVE (VFD). A device which allows the speed of an electric motor to be controlled by varying the frequency of alternating current (AC) voltage applied to the motor.

VOLTS PER CELL (VPC). The chemical voltage of a battery produced by a single electrochemical cell. The total voltage of a battery is the VPC times the number of cells connected in series.

-W-

WIDE AREA NETWORK (WAN). A network operated between facilities separated by large distances.

WINDOWS. A common personal computer operating system, produced and marketed by Microsoft Corporation.

APPENDIX C

LIST OF ABBREVIATIONS

2oo3	Two Out of Three
AC	Alternating Current
ANSI	American National Standards Institute
C4ISR	Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance
CAD	Computer-Aided Drafting
CBRNE	Chemical, Biological, Radiological, Nuclear and Explosive
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CND	Computer Network Defense
COAX	Coaxial
DC	Direct Current
DCS	Distributed Control System
DDC	Direct Digital Control
DOD	Department of Defense
ECM	Electronic Counter Measures
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EMP	Electromagnetic Pulse
EN	European Norm
ESD	Electrostatic Discharge
FAT	Factory Acceptance Test
FOUO	For Official Use Only
FPT	Functional Performance Testing

GHz	Gigahertz
GUI	Graphical User Interface
HEMP	High Altitude Electromagnetic Pulse
HFE	Human Factors Engineering
HMI	Human Machine Interface
HVAC	Heating, Ventilation and Air Conditioning
I/O	Input/Output
I/P	Current to Pneumatic Signal Converter
IA	Information Assurance
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISA	Instrumentation, Systems and Automation Society
Kbps	Thousand bits per second
LAN	Local Area Network
LED	Light Emitting Diode
M/E	Mechanical/Electrical
Mbps	Million bits per second
M/C	Multi-conductor
MDT	Mean Down Time
MilCon	Military Construction
MilSpec	Military Specification
MTBF	Mean Time Between Failures
MTBM	Mean Time Between Maintenance
MTTM	Mean Time to Maintain
MTTR	Mean Time to Repair

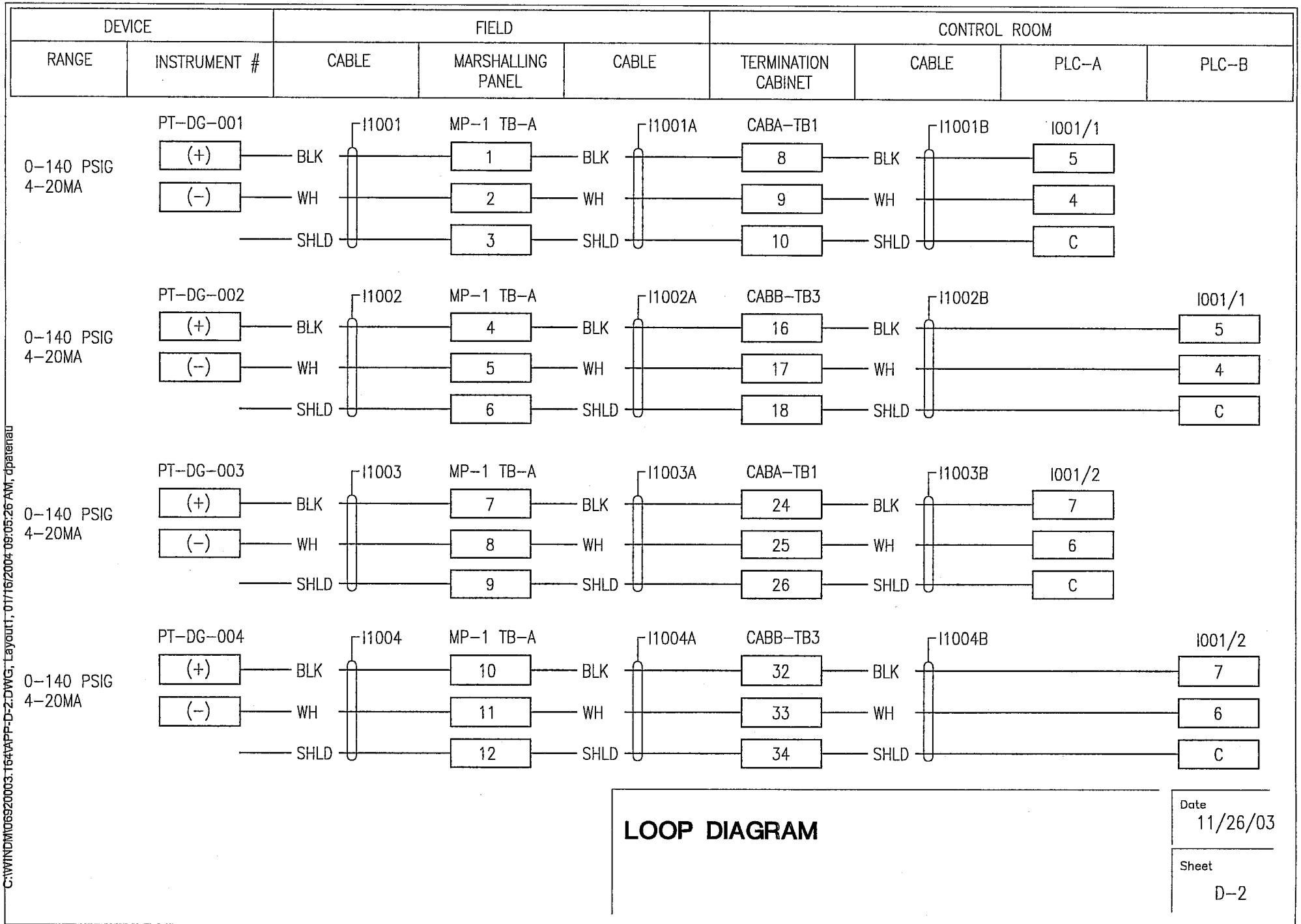
NEMA	National Electrical Manufacturer's Association
NFPA	National Fire Protection Association
NI	Network Interface
NIST	National Institute of Standards and Technology
O&M	Operation and Maintenance
OIT	Operator Interface Terminal
P	Proportional
P&ID	Process and Instrumentation Drawing
PC	Personal Computer
PFD	Probability of Failure on Demand
PFPH	Probability of Failure Per Hour
PI	Proportional – Integral
PID	Proportional-Integral-Derivative
PLC	Programmable Logic Controller
PM	Preventive Maintenance
PREP	Power Reliability Enhancement Program
R/A	Reliability/Availability
RAM	Reliability, Availability and Maintainability
RBD	Reliability Block Diagram
RCM	Reliability Centered Maintenance
RF	Radio Frequency
RFI	Radio Frequency Interference
RGB	Red Green Blue
RPM	Revolutions per Minute
RTD	Resistance Temperature Detector

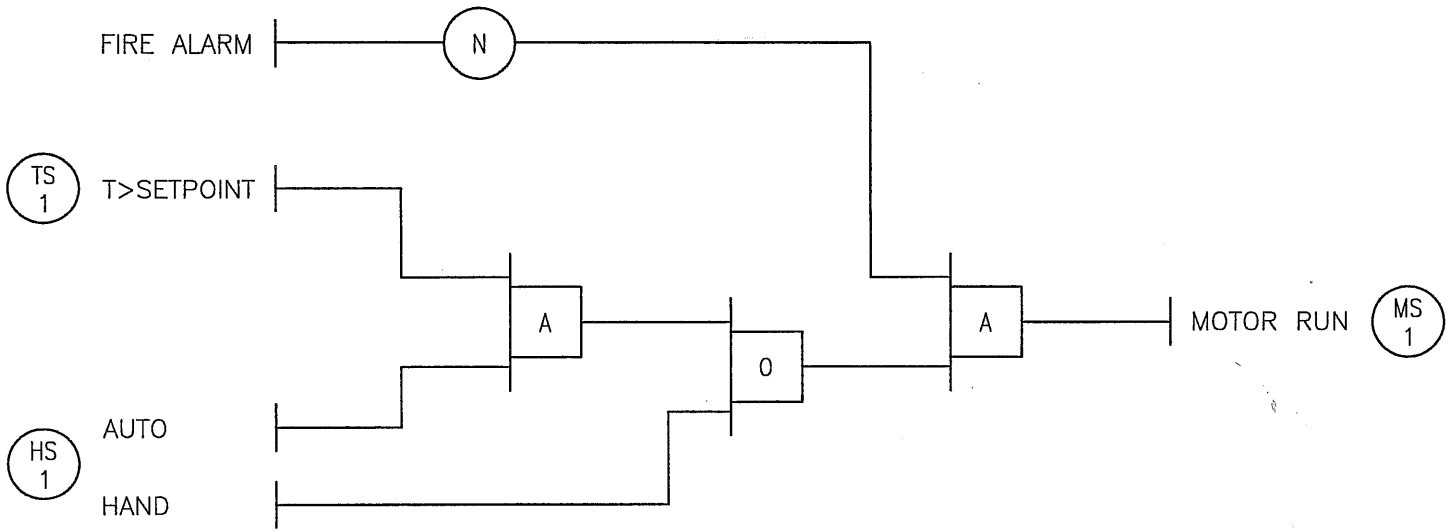
RTU	Remote Terminal Unit
SCADA	Supervisory Control And Data Acquisition
SIL	Safety Integrity Level
SMDS	Software Management and Documentation System
STP	Shielded Twisted Pair
TM	Technical Manual
TVSS	Transient Voltage Surge Suppression
UPS	Uninterruptible Power Supply
UTP	Unshielded Twisted Pair
VAC	Volts Alternating Current
VDC	Volts Direct Current
VFD	Variable Frequency Drive
VPC	Volts per Cell
WAN	Wide Area Network

APPENDIX D – POINTS LIST

System	Tag Number	Description	Type	Location	Field Device	Drawing
GEN 1	TSH - 1001	Coolant High Temperature Alarm Switch	DI	PLC-G1	Gen Control Panel	E-01
GEN 1	TSHH - 1002	Coolant High Temperature Shutdown Switch	DI	PLC-G1	Gen Control Panel	E-01
GEN 1	PSL - 1003	Lube Oil Low Pressure Alarm Switch	DI	PLC-G1	Gen Control Panel	E-01
GEN 1	PSLL - 1003	Lube Oil Low Pressure Shutdown Switch	DI	PLC-G1	Gen Control Panel	E-01
GEN 1	YSX-1101	Generator Circuit Breaker Trip	DO	PLC-G1	52-G1	E-02
GEN 1	YSX-1102	Generator Circuit Breaker Close	DO	PLC-G1	52-G1	E-02
GEN 1	YSX-1103	Generator Circuit Breaker Closed	DI	PLC-G1	52-G1/a	E-02
GEN 1	YSX-1103	Generator Circuit Breaker Open	DI	PLC-G1	52-G1/b	E-02
GEN 1	YSX-1103	Generator Circuit Breaker Drawn-out	DI	PLC-G1	52-G1/TOC	E-02
GEN 1	YSX-1103	Generator Lockout Relay Tripped	DI	PLC-G1	86G1	E-02
SWGR A	YSX-1101	Utility Circuit Breaker Trip	DO	PLC-E1	52-U1	E-03
SWGR A	YSX-1102	Utility Circuit Breaker Close	DO	PLC-E1	52-U1	E-03
SWGR A	YSX-1103	Utility Circuit Breaker Closed	DI	PLC-E1	52-U1/a	E-03
SWGR A	YSX-1103	Utility Circuit Breaker Open	DI	PLC-E1	52-U1/b	E-03
SWGR A	YSX-1103	Utility Circuit Breaker Drawn-out	DI	PLC-E1	52-U1/TOC	E-03
SWGR A	YSX-1103	Utility Lockout Relay Tripped	DI	PLC-E1	86U1	E-03
SWGR A	EIT-1201	Utility Average Phase-to-Phase Voltage	AI	PLC-E1	Utility Protection Relay	E-03
SWGR A	JIT-1202	Utility Real Power, kW	AI	PLC-E1	Utility Protection Relay	E-03
SWGR A	JIT-1203	Utility Reactive Power, kVAR	AI	PLC-E1	Utility Protection Relay	E-03
SWGR A	FIT-1204	Utility Frequency	AI	PLC-E1	FT-1204	E-03
AHU 1	TIT-2001	Discharge Air Temperature	AI	PLC-M1	TE-2001	M-02
AHU 1	FCV-2001	Chilled Water Valve Position	AO	PLC-M1	V-2001	M-02
AHU 1	YSX-2002	Supply Fan Run	DO	PLC-M1	VFD SF1	M-02
AHU-1	PIT-2003	Supply Fan Discharge Pressure	AI	PLC-M1	PE-2003	M-02
AHU 1	YSX-2003	Supply Fan Speed Setting	AO	PLC-M1	VFD SF1	M-02
AHU 1	IIT-2004	Supply Fan Motor Amps	AI	PLC-M1	VFD SF 1	M-02
AHU 1	YSX-2005	VFD Fault	DI	PLC-M1	VFD SF 1	M-02

Type Legend: DI – Digital Input
DO – Digital Output
AI – Analog Input
AO – Analog Output





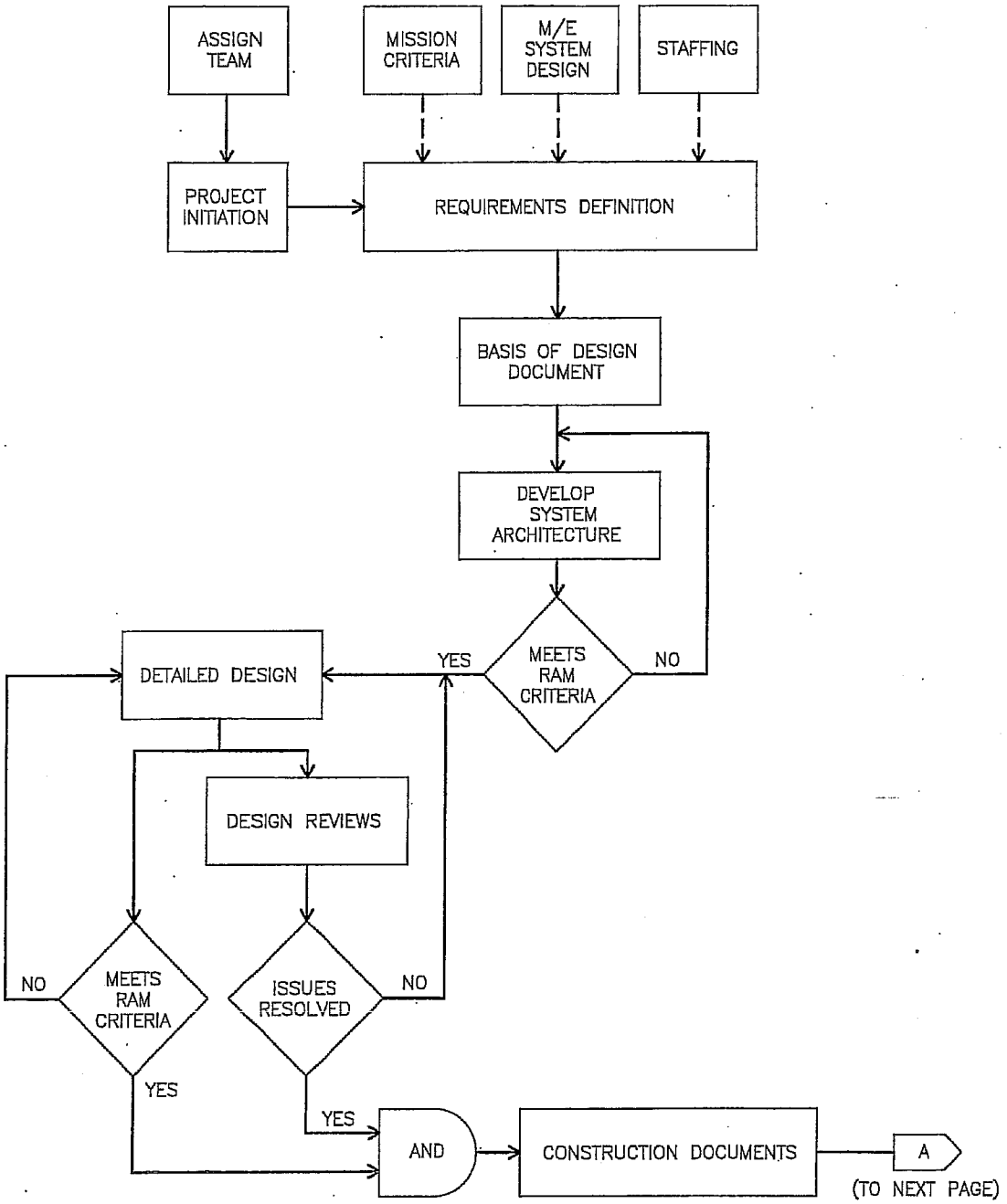
LEGEND:

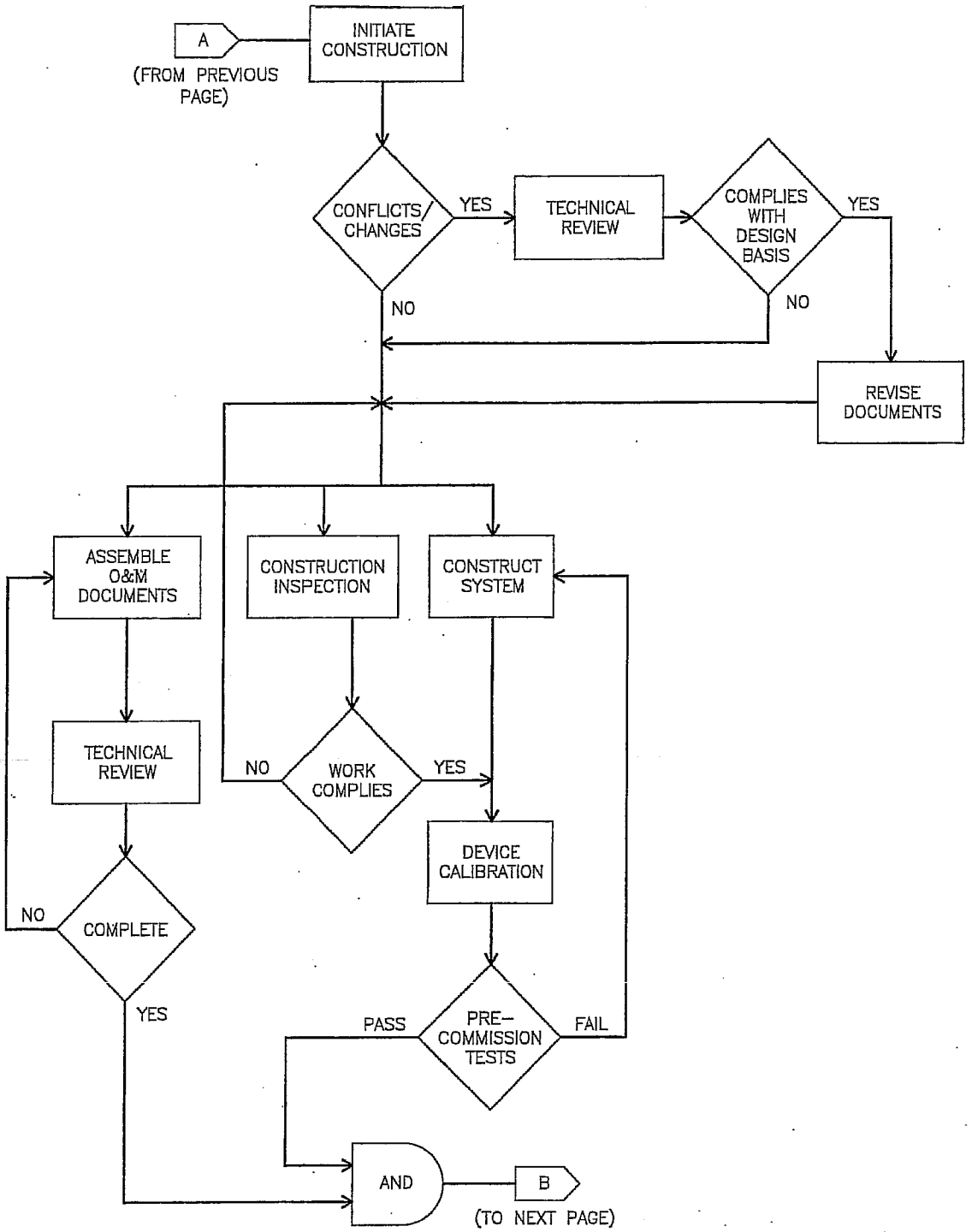
- MS 1 — MOTOR STARTER
- TS 1 — TEMPERATURE SWITCH
- HS 1 — HAND SWITCH
- N — SIGNAL INVERTER (NOT GATE)
- A — AND GATE
- O — OR GATE

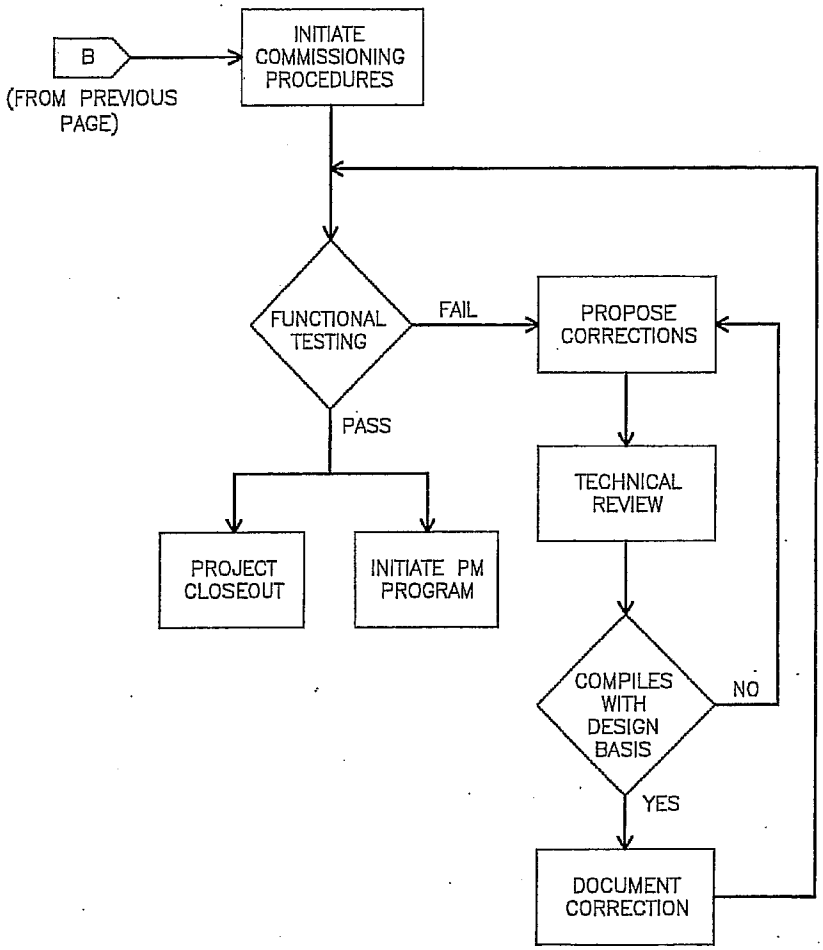
BINARY LOGIC DIAGRAM

Date 6/24/05

Sheet D-3


ASSIGN TEAM
MISSION CRITERIA
M/E SYSTEM DESIGN
STAFFING
PROJECT INITIATION
REQUIREMENTS DEFINITION
BASIS OF DESIGN DOCUMENT
DEVELOP SYSTEM ARCHITECTURE
MEETS RAM CRITERIA
YES
NO
DETAILED DESIGN
DESIGN REVIEWS
MEETS RAM CRITERIA
NO
ISSUES RESOLVED
NO
YES
YES
AND
CONSTRUCTION DOCUMENTS
A
(TO NEXT PAGE)


A
(FROM PREVIOUS PAGE)
INITIATE CONSTRUCTION
CONFLICTS/ CHANGES
YES
TECHNICAL REVIEW
COMPLIES WITH DESIGN BASIS
YES
NO
NO
REVISE DOCUMENTS
ASSEMBLE O&M DOCUMENTS
CONSTRUCTION INSPECTION
CONSTRUCT SYSTEM
TECHNICAL REVIEW
NO
WORK COMPLIES
YES
DEVICE CALIBRATION
NO
COMPLETE
YES
PASS
PRE-COMMISSION TESTS
FAIL
AND
B
(TO NEXT PAGE)


B
(FROM PREVIOUS PAGE)
INITIATE COMMISSIONING PROCEDURES
FUNCTIONAL TESTING
FAIL
PROPOSE CORRECTIONS
PASS
TECHNICAL REVIEW
PROJECT CLOSEOUT
INITIATE PM PROGRAM
COMPILES WITH DESIGN BASIS
NO
YES
DOCUMENT CORRECTION

The proponent agency of this publication is the Chief of Engineers, United States Army. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to HQUSACE, (ATTN: CEMP-OS-P), Washington, DC 20314-1000.

By Order of the Secretary of the Army:

PETER J. SCHOOMAKER
General, United States Army
Chief of Staff

Official:

SANDRA R. RILEY
Administrative Assistant to the Secretary of the Army

Distribution:

To be distributed in accordance with Initial Distribution Number (IDN) 344776, requirements for non-equipment TM 5-601.