4.14 DCS: System Architecture

**Analog Inputs:** Single-ended (reference to signal common) or isolated, channel to ground — 600 V RMS
Intrinsically safe (field circuit Class 1 Division 1, Zone 1, Zone 0) and redundancy options

**Analog Input Ranges:** 4 to 20 mA, 1 to 5 volts with optional digital communications (HART) Thermocouple, RTD
Input resolution 12 bits (1 part in 4000) to 16 bits (1 part in 64,000)

**Analog Outputs:** 4 to 20 mA into a 700 ohm load
Intrinsically safe (field circuit Class 1 Division 1, Zone 1, Zone 0) and redundancy options
Resolution: 10 to 12 bits

**Digital Inputs and Outputs:** 24 or 48 volts DC; 120 or 230 volts AC; optically isolated
Simplex or redundant

**Fieldbus:** AS-Interface, DeviceNet, Foundation Fieldbus, Profibus

**Other I/O Types:** RS232, RS422/485 half duplex, RS 422/485 full duplex serial communication ports, binary coded decimal (BCD), pulse count input, pulse duration output, sequence of events

**Number of Loops of Control:** 8 to 30,000

**Display Interface:** CRT or LCD monitor, 19 in diagonal measure

**Normal Operating Limits:** Temperature: 0 to 60°C
Relative humidity: 5 to 95%, noncondensing
Power supply: 115/220 VAC

**Network:** IEEE 802.3 (Ethernet) 10BaseT or dual-speed 10/100BaseT network, depending on the hubs or switches; shielded twisted-pair cable connects each node to the hub or switch; maximum cable length from the hub/switch to a node is 100 m. For longer distances, use a fiber-optic solution.

**Cycle Times:** Sample interval cycle times range from 0.02 to 0.2 sec/cycle for dedicated loop controllers and from 0.1 to 1 sec/cycle for multiloop unit operations controllers. Scan periods can be fixed or individually specified for each loop.

**Partial List of DCS Suppliers:**
- ABB (www.abb.com)
- Emerson (www.EasyDeltaV.com)
- Honeywell (www.honeywell.com)
- Invensys (www.invensys.com)
- Siemens (www.siemens.com)
- Yokogawa (www.yokogawa.com/us)
INTRODUCTION

The instrumentation used to implement automatic process control has gone through an evolutionary process and is still evolving today. In the beginning, plants used local, large-case pneumatic controllers; these later became miniaturized and centralized onto control panels and consoles. Their appearance changed very little when analog electronic instruments were introduced. The first applications of process control computers resulted in a mix of the traditional analog and the newer direct digital control (DDC) equipment located in the same control room. This mix of equipment was not only cumbersome but also rather inflexible because of the changing of control configurations necessitated changes in the routing of wires. This arrangement gave way in the 1970s to the distributed control system (DCS).

The DCS offered many advantages over its predecessors. For starters, the DCS distributed major control functions, such as controllers, I/O, operator stations, historians, and configuration stations onto different boxes. The key system functions were designed to be redundant. As such the DCS tended to support redundant data highways, redundant controllers, redundant I/O and I/O networks, and in some cases redundant fault-tolerant workstations. In such configurations, if any part of the DCS fails the plant can continue to operate.

Much of this change has been driven by the ever-increasing performance/price ratio of the associated hardware. The evolution of communication technology and of the supporting components has dramatically altered the fundamental structure of the control system. Communication technology such as Ethernet and TCP/UDP/IP combined with standards such as OPC allowed third-party applications to be integrated into the control system. Also, the general acceptance of object-oriented design, software component design, and supporting tools for implementation has facilitated the development of better user interfaces and the implementation of reusable software.

Major DCS suppliers introduced a new generation of process control systems based on these developments. These systems incorporate commercially available hardware, software, and communications. They fully integrate I/O Bus technology such as Fieldbus and Profibus into the system. Batch technology, advanced control, and safety system-oriented software packages are also being included as embedded technologies within the DCS system, although some suppliers might charge extra for some of that software.

These new systems are the foundation for the instrumentation and control implemented in new grass-roots plants. Also, because of the significant operational improvements, including such advanced features as abnormal situation prevention, which may be achieved with such systems, they are quickly replacing the early DCS systems.

More recently, some of the control functions have begun to move into the field. This move to further distribute control and functionality has opened the door to hybrid controllers available from most of the DCS suppliers.

These newer controllers are also being used as linking devices—interfacing with and integrating multiple I/O buses such as Fieldbus, DeviceNet, AS-Interface, HART, and conventional I/O into a single system, as is illustrated in Figure 4.14a.

DCS control, which has dominated the process control industry for years, has improved its performance and reliability. Over the years the DCS design has become more modular and, due to the reduction in the cost of its hardware, has penetrated even some of the smaller installations—especially where advanced capabilities such as alarm management, batch, and advanced control are needed. Installations consisting of only a single controller, one workstation, a bus arrangement such as AS-Interface and Fieldbus, and a small number of I/O are not uncommon.

A review of the nature of analog and DDC is useful in understanding why the DCS has been so successful.

Analog Control

Operators often receive large amounts of information concurrently. This information arrives in the form of alarms and value updates. The operator needs to be able to focus on critical information when an issue arrives, but at the same time, operators should be able to freely move about displays displaying the key aspects of their process. For these reasons, panel arrangements in the past proved to be unsatisfactory, particularly when handling a plant upset or emergency.

The DCS addressed these problems by assigning priorities to issues. Alarming features such as alarm prioritization, acknowledgement, suppression, and filtering play an important part in plant operations. Alarms are associated with control items so that a user in a single click can move from the alarm directly to the appropriate display or faceplate.

Analog instrument panel designs of the past consumed too much expensive space. Issues included recording instruments whose charts were filed in equally expensive storage locations, fixed instrument arrangements on the panel, and the fact that the panels do not easily permit the relocation of associated devices so that they can be observed as a unit. The requirement to run individual electric wiring from every transmitter and final control device to the control room also increased the cost of a project.

Other costs include the cost of real estate for the control room, the cost of the instrument panel, and the cost of utilities necessary to provide a clean and comfortable environment for the instruments. The DCS addressed this need by including trending directly into the operator workstations. Specific process conditions to be monitored were added directly into the displays. Other related items can be placed on the same trend or on a graphic display along with the trend.

More recently the cost of running individual pairs of wires from transmitters and to valves has been reduced by substituting the use of networks and I/O buses such as Fieldbus and Profibus.
 DIRECT DIGITAL CONTROL

Direct digital control (DDC) and supervisory control of analog systems by computers are two other control options. In DDC a digital computer develops control signals that directly operate the control devices (DDC is rarely used in current DCS installations). In supervisory control, a digital computer generates signals used as reference (set-point) values for conventional analog controllers. Both options were offered by earlier generations of the DCS. Even with DCS systems this is still a problem to be reckoned with because each installation is different and requires a separate programming effort; however, the availability of standardized and tested DCS software packages for the more routine functions reduces this problem.

 DISTRIBUTED CONTROL SYSTEM

The major components that make up a DCS process control system are illustrated in Figure 4.14b. The operator interface to the process is typically made up of standard off-the-shelf personal computers (PCs), standard keyboards, mice, and CRT or LCD monitors.

The use of custom keyboards and furniture for the operator interface is often not a viable option because of the associated cost and restrictions on operation. Initial fears that operators would not accept a standard keyboard and mouse have been proven wrong by successful installations on a variety of processes. To provide a wider view and range of control, dual or quad monitor arrangements are often included as part of the operator station.

Similarly, the speed, memory, and disk capacity of personal computers have proven sufficient to address the requirements of the engineering stations that are utilized for system configuration and diagnostics. Also, the price-performance of PCs has driven their adaptation as application stations for the integration of third-party software into the control system. Standard operating systems such as Windows NT and XP are often preferred because of the broad support available to manufacturers.

Equipment that the operator uses to monitor process conditions and to manipulate the set points of the process operation is located in a central control room or distributed on the plant floor close to the equipment. From these locations the operator can (1) view information transmitted from the processing area and displayed an operator display and (2) change control conditions from an input device. The controlling portions of the system, which are distributed at various locations throughout the process area, perform two functions at each location: the measurement of analog variable and discrete inputs and the generation of output signals to actuators that can change process conditions.

Input and output signals can be both analog and discrete. By means of electrical transmission, information is communicated between the central location and the remotely located controller locations. The communication path is either a cable from each remote location to the central station or a single
cable data highway interfacing all the remote stations. The cable in some cases can be a wireless connection via radio, microwave, or satellite.

**Functional Components**

Distributed control systems are made of several components including workstations, controllers, I/O cards, I/O buses, a control network, control technology, and software. The controllers are connected to field devices via analog, digital, or combined analog/digital buses. The field devices, such as valves, valve positioners, switches, and transmitters or direct sensors, are located in the field.

Smart field devices, if they are designed to conform the bus protocols for the I/O, can communicate on the buses while locally performing control calculations, alarming functions, and other control functions. Control strategies that reside in field-mounted controllers send their signals over the communication lines to the final control elements, which they control.

The main components of a process control system are illustrated in Figure 4.14c.

Information from the field devices and the controller can be made available over a control network to the operator workstations, data historians, report generators, centralized databases, etc. These nodes run applications that enable the operator to perform a variety of operations. An operator may change settings, modify control modules within the controller or within the field devices, view the current state of the process, or access alarms that are generated by field devices and controllers. The system may support process simulation for the purpose of training personnel or testing the process control software, plus keep and update a configuration database.

DCS control systems are always sold as packages. Suppliers do not sell only the remote portions or only the centrally located portion. This is because the parts function together as a system; they must be completely integrated and tested as a system. Because the components of the system communicate over a shared data highway, no change is required to the wiring when the process and its control system are modified (Figure 4.14d).

**DCS Control Network**

The communication link from the controller and from the PCs supports the workstations for the operator, engineering, and applications of the DCS system. For process alarms and values needed by the operation, earlier DCS systems utilized customer communication interfaces. These have been replaced in most process control systems by less expensive Ethernet interfaces operating at communication rates of 10 or 100 Mbit.

With twisted pair wiring, the maximum distance between hub and workstations is limited, but this distance limitation can be overcome by using fiber-optic cables. For example, at a rate of 100 Mbit per second, the distance limitation for twisted pair of wiring is 300 ft (100 m), while with fiber-optic cable it is 6000 ft (2000 m). For the distance capabilities and relative features of various cable designs refer to Figure 4.14e and Table 4.14f.

Uncertainty in communications due to packet collisions can be eliminated by using full-duplex switches rather than hubs because each interface has its own channel on which to transmit. By designing the PC communication interface to utilize two Ethernet interface cards, it is possible to provide fully redundant communications.

As was shown in Figures 4.14b and 4.14c, the operators’ console in the control room can be connected through a shared communications facility (e.g., area control network consisting of Ethernet hubs, switches, and CAT5 cable) to
4.14 DCS: System Architecture

**FIG. 4.14c**
The main components of a DCS system, shown from the perspective of its main functional components.

**FIG. 4.14d**
DCS communications are over area control network. In some cases switches may be used to manage the flow of traffic on specific network segments.

**FIG. 4.14e**
The capabilities of data highways made of twisted pairs, coaxial cables, or fiber-optic cables. (From M. P. Lukas, Distributed Control Systems, Van Nostrand Reinhold, 1986.)
several distributed system components. These components can be located either in rooms adjacent to the control room or out in the field.

These distributed control units, which can be remotely located controllers, intelligent fieldbus devices, or remote I/O modules, can in some cases also provide a limited amount of display capability (low-level operator’s interface, LLOI). An example of this is a local panel connected to a serial device using a MODBUS protocol.

A specific DCS for a particular plant is configured from standard building blocks marketed by most DCS suppliers. Figure 4.14b illustrates the categories of components that are available to configure various DCS systems. These components include the operator consoles in the central control room, controllers, I/O cards, communications components, and serial cards serving the interconnections with other digital systems such as PLCs and supervisory computers. The components also include bus cards interfacing to Fieldbus, Profibus, DeviceNet, AS-Interface, and other buses.

The process I/O signals are connected to I/O cards, which can fail. For all control loops that should continue functioning if the central processor or the data highway fails, the I/O should be directly connected to the location where the control is executing.

The preferred approach of control system layout is to keep all the I/O and all the associated controllers for a particular unit operation of the process (chemical reactor, distillation column, etc.) in the same physical controller. If this approach is implemented, the process will remain under control as long as the controller is functioning.

In critical applications, the controller and I/O modules can be made redundant.

Operator Console

The viewing applications, which may run on one or more operator workstations, receive data from the controller application via the control network and display this data to process control engineers, operators, or users of user interfaces, and may provide any of a number of different views, such as an operator’s view, an engineer’s view, and a technician’s view.

Operator display applications are typically implemented on a systemwide basis in one or more of the workstations and provide preconfigured displays to the operator or maintenance people regarding the operating state of the control system or the devices within the plant. Alarm displays receive alarm signals generated by controllers or other devices within the process plant, control displays indicating the operating state of the controllers and other devices within the process plant, maintenance displays indicating the operating state of the devices within the process plant, etc.

These displays are generally preconfigured to display, in known manners, information or data received from the control modules or the devices within the process plant. Often displays are created through the use of objects that have a graphic that is associated with a physical or logical element and that is tied to the physical or logical element to receive data about the element. The object may animate the graphic on the display screen based on the received data to illustrate, for example, that a tank is half full or to illustrate the flow measured by a flow sensor.
Although the information needed for the displays is sent from the devices or configuration database within the process plant, that information is used only to provide a display to the user containing that information. As a result, all information and programming that is used to generate alarms, detect problems within the plant, etc., must be generated by and configured within the different devices associated with the plant, such as controllers and field devices, during configuration of the process plant control system.

Although error detection and other programming are useful for detecting conditions, errors, and alarms associated with control loops running on different controllers and problems within the individual devices, it is difficult to program the process plant to recognize system-level conditions or errors that must be detected by analyzing data from different devices within the process plant.

New control systems provide various levels of support for alarm management. In some cases control logic must be built into the control strategies. In other cases smart objects or agents are configured on top of the control strategy to detect abnormal conditions.

**Core Architectural Components**

The core architectural components of the DCS are:

- System configuration
- Communications
- Control
- Alarms and events
- Diagnostics
- Redundancy
- Historical data
- Security
- Integration

**System Configuration**

Like any computer, distributed control equipment must be told what to do. Programming the process control system instructions is called configuring. There are several aspects to the configuration—the physical configuration and the control strategy configuration. These two activities are generally run in parallel and brought together as the project is engineered.

The configuration database enables users to create and modify control strategies and download these strategies via the control network to distributed controllers, consoles, and devices. Typically, the control strategies are made up of interconnected function blocks, sequential function charts (SFC), and equipment and units representations, which perform functions within the control scheme based on inputs and which provide outputs to other function blocks and/or I/O within the control scheme.

The configuration application also allows a designer to create or change operator interfaces, which are used by a viewing application to display data to an operator and to enable the operator to change settings within the process control system. Each controller and, in some cases, field devices too, stores and executes controller applications that run the control modules assigned and downloaded to implement actual process control functionality. The general configuration items are illustrated in Figure 4.14g.

For regulated and highly critical applications, such as those requiring Food and Drug Administration (FDA) certification, a record can be kept of any changes that are made to the control system configuration. Such an “audit trail” records all changes that were made, the names of people who made the changes, and the time and date when the changes were made. Provisions are also provided to automatically or manually undo any changes that are made in the control system.

**FIG. 4.14g**

DCS system function configuration, showing the process display and a listing of alarms and other key events.
**Physical Configuration**  The physical configuration requires configuring the nodes, cards, and devices. In many systems, this activity is greatly simplified using auto-sense capabilities. The physical configuration of part of the system is illustrated in Figure 4.14h.

**Logical or Control Strategies**  A distributed control system must have a consistent means of representing and referencing information. Ideally, such reference can be made independent of the physical device that holds this information. A common way to divide data within the control system is according to identifier tag numbers.

The S88 batch standard defines such logical grouping of measurement, calculation, or control as a module. When a control system follows this convention, then each module is assigned a tag that is unique within the control system. Based on this tag and the structure of the components in the module, it is possible for applications in the control system to reference any piece of information. For example, consider the module of an instrument with the tag number 200FI102 (which represents flow indicator No. 102 in area 200 of the plant). In the module, a calculation identified as CALC1 is made using inputs AI1 and AI2 and generating an output as shown in Figure 4.14i.

Based on the module tag number and unique function block names within the module, the output of the calculation block is identified as 200FI102/CALC1/OUT.

DCS Systems support multiple control languages. The control languages include function block diagrams, sequential function charts, and structured text and may also include ladder diagrams and instruction lists. Some systems may be IEC 61131-3 compliant. Most control systems also include interlocking and batch capability — in most cases supporting S88. Some systems also support embedded advanced control and safety functions. The control strategies can often be mixed. Strategies can reference I/O as well as local and remote parameters.

An important feature of DCS systems is their ability under certain conditions to be upgraded online. In case of failure, most systems have extensive support for holding the last value, using a default value, or moving to some known state.

One of the features that make distributed control systems so powerful is their function library, which is available and can be used just by calling for it. This availability simplifies the task of the process control engineer, if he or she is familiar with the particular vendor’s practices. Such a function library list of one supplier is shown in Table 4.14j.

What distinguishes some DCS suppliers from most PLC manufacturers and what distinguishes the various DCS suppliers from each other is the size and quality of the algorithm library that is embedded and freely available with their basic control system.
packages. When it comes to implementing some of the more advanced control strategies, it makes all the difference whether the algorithm library includes the algorithms that the particular project requires.

Some of these are analog inputs, sample and hold for dead time processes, dead band control for fast processes, set-point filtering, error squared, integral squared, dead time PID, set-point and process variable characterizers for nonlinear processes, decoupling of interactions, linear dynamic compensation of lead/lag blocks for feedforward, external feedback for antireset windup, self-tuning, and nonlinear adaptive controls, not to mention the more demanding algorithms for optimization, statistical process control, fuzzy logic, model-based optimization, sampled data control, sliding mode control, neural networks, and state-space controls.

Configuration of the control strategy often makes use of libraries of prebuilt control logic. The prebuilt control logic can be linked into final control strategies, in which case changes to the library can be automatically propagated to each control item. Alternatively, the prebuilt control logic can be embedded or unlinked so that individual control strategies are unaffected by changes in the library.

Batch and larger continuous projects, following the suggestions of S88, define strategies as a set of class-based items that can come together as a complete class-based strategy. If the required elements are offered by the DCS supplier, creating a control strategy from a class-based library can result in a significant set of configurations. Binding these configurations to actual I/O, loops, and equipment can become a “fill in the table” exercise.

**Input/Output** The requirements for redundancy and interfacing for I/O processing dictate that the process controller be of custom hardware design. Multiple processors are often used to address the communication and I/O processing and control execution. Also, a real-time operating system for embedded applications is often used to provide deterministic scheduling and execution of control. A large variety of I/O cards are normally provided to address a variety of field measurements and actuators:

- Analog Input (isolated) 1 to 5 volt DC, 4 to 20 mA
- Analog Output 4 to 20 mA
- Isolated RTD input (2, 3, 4 wire) and Thermocouple Input (B, E, J, K, N, R, S, T)
- Discrete Input 24 VDC, 120/230 VAC
- Discrete Output 24 VDC, 120/230VAC
- Pulse Count Input
- Pulse Duration Output

Since digital transmitters and actuators that utilize a variety of communication protocols and physical interfaces are available, many manufacturers offer interfaces to the most common buses. Also, serial interface cards are often supported for interfacing to supporting systems. Examples of these communication interface cards are:

- HART AI-Card, 4 to 20 mA
- HART AO Card, 4 to 20 mA Series
- DeviceNet (Baud rate 125 250 500 kbit/sec)
- FOUNDATION Fieldbus
- AS-Interface
- Profibus DP Baud rate (9.6 19.2 93.75 187.5 500 1500 kbit/sec)
- Serial Interface (MODBUS or Allen-Bradley’s Data Highway Plus protocol)

In addition, some manufacturers may offer I/O cards to meet special requirements. For example, sequence of events (SOE) input cards are used to capture process-upset events coming directly from devices in the field. Because events are captured and temporarily stored locally—on the SOE input card itself—faster recording for each of the channels on the card is possible. For example, events captured by an SOE input card are time stamped using a 1/4-millisecond resolution.

Input and output terminations are made at terminals that are either part of the electronic mounting frames or on separate terminal boards. In the latter case there will usually be a cable connection between the terminal board and the electronic controller file. Connections are usually made from the front of the cabinet. An alternate method is to use a separate termination cabinet, filled with rows of terminal strips. This requires extra wiring from the termination cabinet over to the
terminals in the remote controller cabinet, but it has the advantage that field wiring can be completed before the distributed control housings are delivered and installed.

**Conventional I/O** Analog input and output signals will usually be carried on shielded, twisted pairs of copper wire. Digital inputs and outputs, either 120-volt AC or 24-volt DC, can be carried on twisted pairs, which do not, however, have to be shielded. Analog signals should never be run in proximity to alternating current wiring. The controller files operate almost universally on 1- to 5-volt signals, so the most common input is a 4- to 20-mA current signal, developing a 1- to 5-volt input across a 250-ohm resistor mounted on the input terminal board. Most distributed control systems can accept low-level signals from RTDs and thermocouples, performing the signal amplification in their input electronic circuitry. A few systems can accept pulse input with frequencies sufficiently high to allow signals from turbine flow meters to be used directly.

Most suppliers offer some conditioning of signals. Providing square root extraction, linearizing thermocouples, and resistance thermometers and dampening noisy inputs can be selected by configuration. Some input/output boards provide terminals with fused 24-volt DC power that can be used to supply a positive voltage to two-wire transmitters.

Separate terminal boards may also be supplied for digital input and output signals. Usually, optical isolation is provided. A DC input signal (or a rectified AC input signal) causes a light-emitting diode (LED) in the isolating relay to be energized. A photoelectric device energized from the LED actuates a transistor in transistor–transistor logic (TTL) input circuitry to signal a digital input. A digital output signal is similarly isolated to actuate a transistor driver circuit for DC outputs or a triac for AC outputs. The solid-state relay from which the output is generated functions like a dry contact, and the output must be powered from a separate power source.

**Diagnostics** Integrated diagnostics is an important feature of the DCS. The diagnostics cover the hardware, redundancy, communications, control, and to some extent, the software that makes up the DCS.

**Redundancy** Redundancy is an important requirement for any critical process control application using DSC systems. These systems must have redundant communications, redundant controllers, redundant I/O cards, and redundant I/O communications. It is also possible to take redundant or preferably two out of three voting measurements and discard the defective or inaccurate one during control execution.

One advantage of redundancy is the ability to upgrade components online in the control system, but on critical processes this has to be very carefully planned so that safety will not be compromised.

**Historical Data** The DCS usually includes the ability to collect batch, continuous, and event data. A centrally defined history database is available for the storage of historical data. The value of any attribute, alarm, or any control strategy, alert, or process condition can be recorded in the history database along with its status. In modern control systems the data values are collected as an integrated feature of the system. Events are collected and time-stamped at their source—in some cases down to a few millisecond resolution.

Users and layered applications can retrieve the batch, continuous, and event data in a time-ordered fashion. For security reasons values cannot be edited without leaving behind an audit trail.

**Security** Security is essential in process control. The DCS system must be able to limit the access to the various parts of the control system to authorized people only. This is done by user, plant area, and workstation. Layered applications have to form a session before they are allowed access into the system. There are several aspects to security as summarized below:

- **Authentication.** Access to the DCS for human users and layered applications users will be controlled through the use of password-protected user accounts.
- **User.** A human user of the DCS must have a user account on the system in order to gain access. All user accounts are named. User accounts have unique names within the scope of a site. All user accounts have a password, which must be provided in conjunction with the account name in order to start a DCS session.
- **Plant area security.** A user account can be permitted or denied access to make changes within zero or more plant areas within a site.

For each plant area where access is permitted, access can be restricted at runtime according to the classification of the runtime attribute data. For each plant area where access is permitted, the ability to make configuration changes can be restricted.

A user account can be permitted or denied access to view or modify user account and privilege information.

In some systems it is also possible to enable authorization. In these cases the user, or in some cases several users, will need to confirm by password the changing of certain parameters, starting/stopping a batch, etc.

**Integration** When a new plant area is added or expanded, the operators of the new area may need some information about the existing plant to provide a coordinated operation. Similarly, the operators of the existing plant may need to have feedback from the new process area in making decisions on how best to run the balance of the plant. In most cases, only a small fraction of the information in either system must be communicated to support such coordination between these areas. Several techniques are used to integrate systems.

The OPC Foundation has defined an industry standard for accessing information within a control system. Thus, many control systems provide OPC server capability in workstations designed for interfacing to the plant local area network (LAN).
OPC client applications in this station or on the network may access information using the path convention supported by the control system.

**International Fieldbus Standards**

The adoption of the IEC1158-2 Fieldbus standard by the major DCS manufacturers has ushered in the next generation of control and automation products and systems. Based on this standard, fieldbus capability may be integrated into a DCS system to provide:

- Advanced function added to field instruments
- Expanded view for the operator
- Reduced wiring and installation costs
- Reduced I/O equipment by one half or more
- Increased information flow to enable automation of engineering, maintenance, and support functions

Similarly, the Ethernet and OPC industry standards have provided DCS manufacturers a defined means for other applications to access information in a process control system. Through the active use of control system data in a plant information system, the operation benefits that may be achieved are:

- Improvement in production scheduling
- Better inventory control
- Consolidation of maintenance and operation information from multiple sites

**DATA HIGHWAY DESIGNS**

DCS systems today range in size from a single stand-alone laptop for the purpose of plant design and simulation to full-scale systems covering a whole plant. The systems come complete with integrated Web services for plant integration — often supporting a variety of open standards, such as OPC, for communicating with outside data sources.

**Control Network**

The communication infrastructure on the area control network supports the following:

- **Connections.** Connection between nodes in the system.
- **Unsolicited communications.** Transferring real-time information as data changes.
- **Synchronous and asynchronous read/writes.** Reads and writes block/don’t block during the transaction.
- **Passthrough messages.** Transfer of hosted messages across control network to device, serial, or other network.
- **Configuration downloads.** Transfer of configuration from engineering node to controller and devices.
- **Auto-sensing.** Automatic detection of controllers, workstations, I/O cards, devices.
- **Diagnostics.** Diagnosis of system components, control strategies, etc.
- **Debugging.** Debugging of control strategies.
- **Directory services.** Location services to find nodes, cards, control strategies, devices, and other items in the system.
- **Online upgrades.** Upgrading a system that is in operation.
- **Hot/warm/cold restart.** Restarting a control strategy from backup.
- **Secure and unsecured access.** Security required to access information in the system.
- **Alarms and events.** Alarms and events are generated by the control strategy and system.
- **Device alerts.** Device alerts are generated by devices and equipment in the control system.
- **Time synchronization.** Time synchronized across nodes, devices, and sometimes I/O (e.g., sequence of events recording).

The data highway is the communication device that allows a distributed control system to live up to its name, permitting distribution of the controlling function throughout a large plant area. Data highways vary in length as a function of traffic capability and speed of transmission.

The most popular medium is Ethernet CAT5 cable. Several suppliers still offer twisted and shielded coax cables. In situations where noise is extensive, either fiber optics or wireless may be used — with fiberglass cable being the most prevalent. This is used most commonly for point-to-point connection between switches and hubs. Fiber optics is attractive for use as a data highway because it eliminates problems of electromagnetic and radio frequency interference, ground loops, and common mode voltages; it is safe in explosive or flammable environments; it can carry more information than copper conductors; it is inert to most chemicals; and it is lighter and easier to handle than coaxial cable. For more details on fiber-optic transmission refer to Section 3.7.

**Ethernet Configuration**

Hubs and switches can be used for 10 or 100 Mbit and even 1 Gbit per second networks. With Ethernet switches, each port auto-senses the speed of the attached workstation or controller and then operates at that speed. Standard DCS architectures operate at 100 Mbit per second speed.

Figure 4.14k illustrates a Class II repeater network where the maximum distance between workstation A and workstation B (the furthest points) can be up to 672.6 feet (205 meters) when up to two of the dual speed hubs are daisy-chained with twisted pair link segments. Each port on the switch can support up to 328 feet (100 meters) of twisted pair cable; however, only 672.6 feet (205 meters) is allowed end to end. This leaves 16.4 feet (5 meters) for the twisted pair link segment between the hubs.
An alternative is to use shorter-length cables (less than 328 feet [100 meters]) from workstation or controller to hub and allow a longer cable between hubs. Any combination will work as long as the total of all cable lengths does not exceed 672.6 feet (205 meters). It is a good practice to use a 16.4-foot (5-meter) or shorter cable between the hubs to avoid problems later if a new cable needs to be attached to the hub. This is to avoid a situation in which the 672.6-foot (205-meter) maximum length is exceeded because the length of the intra-repeater link is not known and an assumption is made that all ports can have a 328-foot (100-meter) cable.

Operators can also suppress and filter alarms. Alarm suppression is typically used to temporarily remove alarms from the system for which some condition exists that the operator knows about (e.g., a piece of equipment has been shut down). Alarm filtering provides a way for the operator to view collections of alarms.

The following paragraphs describe alarm processing and alarm management and conclude with a discussion of higher-level applications built on top of the overall alarm processing and management system.

**Alert Processing**

In 1996 the SP50 committee finally finished its standards, including field-testing, and made the standards available in the form of a commercial product.

As part of SP50 alarms and events, collectively known as alerts, were included as part of the function block efforts of Foundation Fieldbus and IEC 61804. In these standards, alarms and alerts represent state changes within function block applications. Resources each have an alert notifier responsible for reporting their alert occurrences. Alerts objects are used to communicate the event to other devices.

An alert notifier examines the results of function block executions to determine whether any of a defined set of alert states has been entered. When an alert occurrence has been detected, the alert notifier builds a report message, referred to as an event notification, and publishes it onto the network. The time at which the alert state was detected is included as a time stamp in the alert message. The reporting of alerts may be individually suppressed.

A reply is required that confirms receipt of the notification. If the reply is not received within a time-out period, the alert may be retransmitted.

Alerts may also be acknowledged. Acknowledgment indicates that the alert has been processed by an interface device to satisfy operational interface requirements.

An alert notifier examines the results of function block executions to determine whether any of a defined set of alert states has been entered. When an alert occurrence has been detected, the alert notifier builds a report message, referred
to as an event notification, and publishes it onto the network through the alert object.

Based on the type of alarm and event information, which may be reported by blocks contained in a resource, up to three classes of alerts may be defined in the resource:

1. Analog alert. Alert used to report alarms or events whose associated value is floating point
2. Discrete alert. Alert used to report alarms or events whose associated value is discrete
3. Update alert. Alert used to report a change in the static data of the block

A reply is required from one interface device that confirms receipt of the notification. If the reply is not received within a time-out period, the alert notifier will retransmit the notification. This method ensures that alert messages are not lost.

The following alarms are supported by Foundation Fieldbus devices:

- 0 = Discrete alarm
- 1 = High high alarm
- 2 = High alarm
- 3 = Low low alarm
- 4 = Low alarm
- 5 = Deviation high alarm
- 6 = Deviation low alarm
- 7 = Block alarm

Associated with each alarm is a time stamp that indicates the time when evaluation of the function block was started and a change in alarm state was detected that is unreported. The time-stamp value will be maintained constant until alert confirmation has been received, even if another change of state occurs. Also, the value of the associated parameter at the time the alert was detected is reported.

A function block must detect the alarm condition. The alarm must be transported to the responsible entity, e.g., interface device supporting human interface. The entity must confirm that the transport was successful. The alarm may require that a plant operator acknowledge that the alarm has been noticed, even if the condition has cleared.

Every occurrence of an alarm must be balanced by a notification that the alarm has cleared or that the same alarm has occurred again before the clear could be reported. An alarm will also be cleared in a device when 1) an alarm that is active is disabled or 2) a block containing an active alarm is placed in out-of-service mode. In these cases, specific alarm-clear messages should be generated, to allow remote alarm summaries to clear the alarm information for this block.

Each alarm and event parameter may have an associated priority parameter. The alert priority enumeration value is:

- 0 = The associated alert may clear when the priority is changed to 0, but it will never occur.
- 1 = The associated alert is not sent as a notification. If the priority is above 1, then the alert must be reported.
- 2 = Reserved for alerts that do not require the attention of a plant operator, e.g., diagnostic and system alerts. Block alarm, error alarm, and update events have a fixed priority of 2.
- 3 to 7 = Increasing higher priorities; advisory alarms.
- 8 to 15 = Increasing higher priority; critical alarms.

The alert object allows block alarms and events to be reported to a device responsible for alarm management.

The alert object contains information from an alarm or update event object, which is to be sent in the notification message. The alert object will be invoked by the alert notification task. If multiple alarms or event parameters are unreported, then the one with the highest priority or the oldest of equal priority will be selected by the alert notification task. The selected alert object is sent in a message at the first opportunity—less than the alert confirm time. If a confirmation from an interface device is not received by the alarm notification routine in the field device within a time determined by the resource block confirm time parameter, then the alert will be considered unreported so it may be considered for selection.

Figure 4.14 illustrates the transport of an alert.

### Alarm Management

Operator consoles maintain a list of active alarms in the system:

- Consoles register an interest in alarms/events (by plant area) in all other nodes in the system.
- The alarm state change events are routed to the software that maintains the active alarm list.
- Active alarms may be regenerated in order to build the active alarm list in workstations starting up, or when additional plant areas are required.
- In the background, alarms are resynchronized to keep the active alarm lists accurate (in particular, remove “dead” active alarm list items for alarm parameters/modules/nodes that are no longer out there and communicating (and did not get a message out before they went away).

Workstations select which alarms are eligible for inclusion in the workstation alarm list:

- Must be in workstation’s “alarm scope” (set of plant areas).
- Must be in current user’s “alarm scope” (set of plant areas that user has one or more security keys for).
- Area level alarm filtering (per workstation) must be set to enable alarms from that area.

© 2006 by Béla Lipták
Unit level alarm filtering (per workstation) must be set so if the alarm is associated with a unit, that unit does not have the alarm turned off.

The workstation alarm list maintains the list in order of importance:

- Unack ahead of acked
  - Then: Higher priority ahead of lower priority
  - Then: Condition still active ahead of condition cleared (latched)
  - Then: more recent “went active” time ahead of older alarms

When alarms and alerts arrive at the operator console they are first classified. Alarms and alerts can be classified into process alarms, device/equipment alarms, and hardware alarms.

Process alarms cover “traditional” process alarms: HI, LO, HI-HI, LO-LO, DEV, etc. They are highly configurable:

- User-configurable alarm (parameter) names
- User-configurable alarm types (alarm words, category, message content)
- User-configurable alarm condition (with arbitrarily complex logic to arrive at the alarm condition)
- User-configurable priority
- Unlimited number per containing module

Device alarms are from instruments, transmitters, valves, and equipment attached to the DCS. Relatively little configuration is needed:

- Limited/fixed number of distinct alarms:
  - FAILED
  - MAINT
  - ADVISE
- Alarm conditions have “fixed” mapping to the alarms.
- User-configurable priority, and whether or not alarm should be enabled.

Hardware alarms are triggered by the hardware components of the DCS (controllers, I/O cards, remote I/O communication links, redundant hardware, etc.). Relatively little configuration is required.

Operators usually interact with the alarm system through alarm banners and alarm summary displays.

**DCS ATTRIBUTES**

The DCS has a number of advantages over other control approaches. If the client and design engineering firm are highly experienced, distributed control can reduce overall installation, configuration, and commissioning costs. Less wiring is required when information is transmitted over bus networks.
From the point of view of the operator, the interface with the process is improved. Integrated alarming and diagnostics substantially improve the operator’s ability to identify the causes of upsets and to bring the process back under control.

Configuration capabilities allow for prebuilding portions of the control system configuration, which can be reused on other projects. There is great potential for extensive standardization of control systems.

The distributed control system is flexible and relatively easy to expand.

**Reliability**

Digital computers are more reliable today than when they were first introduced, but the possibility of failure of a single piece of electronic equipment causing the shutdown of an entire production facility still raises concerns that cannot be ignored. How does distributed control satisfy the requirement for continuous production?

Most suppliers subject their equipment to extensive periods of cycling at temperatures exceeding the extremes listed in equipment specifications. This weeds out the components most likely to fail. Failures of marginally operational parts will usually show up in the first few weeks of operation. Once past that period, electronic equipment seems to operate indefinitely, so long as limits of temperature and atmospheric cleanliness are observed. The advent of large-scale integration (LSI) has fostered this reliability. As size has been reduced, so has heat generation.

Nevertheless, failures will inevitably occur. Consequently, suppliers provide redundancy in their design, as well as backup. Some suppliers simply build two of everything and supply it as standard. Others offer redundancy on an optional basis. Power supplies, data highways, traffic directors, and remote controller electronics are important links in the communications chain and should be considered as candidates for redundancy. The operator station itself, with its video terminal, will not shut the system down if it fails, but it will leave the operator blind to the condition of the process, and so it is another candidate for redundancy.

There should be automatic transfer between redundant parts, so that if one fails the other takes over with no disturbance of the operation or output. At the same time, there must be some sort of alarm to alert the operator to the fact that a failure has occurred. How much redundancy is provided must depend on how much loss of production will cost. If continuous production is absolutely necessary, no expense cutting is justified.

Another form of redundancy, available from most suppliers, is controller backup. A complete modular file is mounted in the same remote location as others that are considered important enough to require backup protection. Some suppliers back up one complete set of electronics with another complete set, updating the database of the backup unit as that of the primary is changed. The two are cabled together, and on failure of the primary, the secondary takes over automatically.

Another supplier backs up eight controller files with a single backup file, and if any of the eight fails, its place will be taken by the backup unit. Still another supplier, in addition to supplying one-for-one backup, allows portions of the backup file to back up portions of the primary controller file, freeing the unused portions of the backup file for additional control tasks.

**Mean Time between Failure**

High availability is as important as reliability. Defining availability as the ratio of mean time between failure (MTBF) to mean time between failure plus mean time to repair (MTBF + MTTR), it is clear that a system will be most available when it is very reliable (high MTBF) and can be quickly repaired (low MTTR). Since distributed control equipment is highly modular and contains many printed circuit cards, time to repair can be very short if sufficient spare parts are available.

Most systems make good use of diagnostics; internal failures are reported on the CRT screen, indicating where in the system a failure has been detected and providing some clue to the cause. Substitution of printed circuit cards can often restore operation, and this can be done quickly by a service technician who knows where to look for the trouble and has spare parts for making the substitution. The failed card can then be returned to the supplier for replacement.

High-availability process control systems are essential in case of large continuous processes such as a cracking unit in a petroleum refinery. Such units can be designed to run with no shutdown for 5 to 6 years while running 24 hours a day 7 days a week. Some parts of the system can be made redundant so that automatic switchover might occur in case of a failure. Other parts of the system can be provided with automatic fault diagnosis and identification for rapid repair.

For such applications obviously one would hope and aim to design a system that allows the failed unit to be replaced while the process continues without interruption, but in the real world Murphy’s Law often comes true.

The high diagnostic coverage and rapid replacement capabilities of the controller and I/O assemblies allow the user to decide how much redundancy is really needed for an application. A customer may choose to use simplex I/O and possibly even simplex controllers, where failure events are not significant as long as the failures are automatically diagnosed and reported and the repair steps are simple.

To address this, built-in diagnostics that identify the majority of assembly failures are provided by some suppliers. In addition, all of these assemblies are “hot pluggable” (a “computerize” buzzword for testing while in operation) so that an I/O assembly can be diagnosed and repaired efficiently. Some controllers are also able to check whether a new card is the proper type when replacement of a failed card is needed.
Some manufacturers also have extensive diagnostics on their bus cards such as Fieldbus Foundation H1 Fieldbus IO cards and HART analog input and analog output cards. Some conventional cards, such as discrete input and output cards, also support automatic short-circuit and open-circuit detection on discrete sensors and actuators.

### PRICING

Utilizing PCs and standard monitors and keyboards for operator and engineering stations and the use of standard Ethernet for communication have reduced the cost of DCS system hardware. Also, the introduction of fieldbus devices has dramatically impacted the cost and space required for controller I/O.

In the cost information provided here, the cost of services associated with system configuration, factory acceptance, installation, simulation, testing, commissioning and startup are not included. Similarly excluded is any software not embedded in the DCS supplier’s standard package. This usually excludes control and simulation or modeling algorithms that are unique to the particular process, interfacing with software or hardware of other suppliers that the DCS vendor does not support with embedded software, and the configuration of most graphics that are specific to the particular project.

A sample price list for DCS hardware components is shown in Table 4.14m. This price list basically covers the cost of DCS control system hardware. Most of the software costs are not included in the list.

As an example, Table 4.14m lists the cost of the DCS hardware (and the licenses for some basic software) for a project that requires 256 analog and 961 on/off I/O as follows:

- **25% Fieldbus Analog (64 I/O—12 fieldbus devices per segment)**
- **75% Non-Fieldbus I/O (192 I/O, redundancy for 5% of analog I/O)**
- **10% Fieldbus Discrete (96 I/O—8 discrete fieldbus devices)**
- **90% Non-Fieldbus Discrete (865 I/O, redundancy for 10% of discrete I/O)**

Based on the above scope definition, the cost of the package has been estimated using typical list prices for the components, as shown in Table 4.14.

After the hardware components of the DCS have been manufactured, the system must be integrated and made fully operational before it can be tested. If the user wants to have a complete estimate for the whole DCS project, including factory acceptance test and startup, it is advisable to include all the software development, integration, and training tasks in the initial specifications for the DCS bid package, when it is sent out for competitive bidding. Following system integration, a factory acceptance test (FAT) is normally conducted.

<table>
<thead>
<tr>
<th>Description</th>
<th>Price Range ($US)</th>
<th>Typical ($US)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HARDWARE W/SOFTWARE LICENSE</td>
<td>5300 to 6600</td>
<td>5500</td>
</tr>
<tr>
<td>Control unit, w/carrier, power supply</td>
<td>11,700 to 14,300</td>
<td>13,000</td>
</tr>
<tr>
<td>Operator’s console w/21” monitor (1200 I/O)</td>
<td>9,800 to 10,300</td>
<td>10,000</td>
</tr>
<tr>
<td>Engineer’s station w/21” monitor (1200 I/O)</td>
<td>20,000 to 22,000</td>
<td>21,000</td>
</tr>
<tr>
<td>Analog input (AI) card, 8 channel w/HART</td>
<td>1400 to 1800</td>
<td>1500</td>
</tr>
<tr>
<td>Analog input (AI) card, 8 channel w/HART redundant</td>
<td>2500 to 3000</td>
<td>2800</td>
</tr>
<tr>
<td>Analog output, 4 to 20 mA, 8 channel w/HART</td>
<td>1700 to 1900</td>
<td>1800</td>
</tr>
<tr>
<td>Analog output, 4 to 20 mA, 8 channel w/HART, redundant</td>
<td>2700 to 3300</td>
<td>3000</td>
</tr>
<tr>
<td>Foundation Fieldbus interface card w/2 segments</td>
<td>2200 to 2900</td>
<td>2500</td>
</tr>
<tr>
<td>Discrete input, 24 Vdc, 8 channel</td>
<td>520 to 630</td>
<td>550</td>
</tr>
<tr>
<td>Discrete output, 24 Vdc, 8 channel</td>
<td>1000 to 1150</td>
<td>1100</td>
</tr>
<tr>
<td>Discrete input, 24 Vdc, 8 channel as fieldbus I/O</td>
<td>820 to 930</td>
<td>850</td>
</tr>
<tr>
<td>Discrete output, 24 Vdc, 8 channel as fieldbus I/O</td>
<td>1000 to 1150</td>
<td>1000</td>
</tr>
<tr>
<td>Discrete input, 24 Vdc, dry contact, 8 channel, redundant</td>
<td>1000 to 1200</td>
<td>1100</td>
</tr>
<tr>
<td>Discrete output, 24 Vdc, hi-side, 8 channel, redundant</td>
<td>1500 to 1700</td>
<td>1600</td>
</tr>
<tr>
<td>Carrier for 8 cards</td>
<td>600 to 800</td>
<td>700</td>
</tr>
<tr>
<td>Bulk power supply</td>
<td>900 to 1200</td>
<td>1000</td>
</tr>
</tbody>
</table>
If an engineering firm or system integrator performs some of the software development, simulation, training, and commissioning tasks, the initial bid package should clearly define the areas of responsibilities that are to be met by the DCS supplier.

**Bibliography**


Williams, T. J., “Hierarchical Distributed Control,” InTech, March 1983.

