CONTROLINC

Digital Network Controls
Modbus RTU

Supplying Non-Proprietary Digital Control Networks
Since 1985 - Suitable for Interfacing with Other Manufacturer’s Products
Introduction:

Controlinc is EIM’s generic name for the range of integrated digital control networks first introduced by EIM in 1985. The controller is specifically designed for valve control applications, either block valve or proportional valve (modulating) control. With auto-calibrating analog inputs as a standard feature, it automatically learns and adapts to any valve size and speed of operation.

EIM’s digital control networks have always incorporated standard non-proprietary protocols in the communication module in the actuator so that the customer has the guarantee of installing actuators from other manufacturers in the same network in the future, if so desired. EIM have never used proprietary protocols since this would restrict the customer in the selection of alternative manufacturer’s products in the future, resulting in higher costs and often poor performance, especially from current-based proprietary systems that have slow response times and severe restrictions on the length of network cabling.

The first protocol used by EIM in 1985 was Modbus RTU and this is still the most popular solution for digital control networks since it is a de facto standard around the world and has been used frequently by all experienced systems integrators. It is an efficient protocol, inherently noise-resistant and capable of being used over long distances with fast communication rates in excess of 9600 baud without degradation of the performance.

Some of the proprietary, current-based protocols have significant restrictions when long cable lengths need to be installed, resulting in very slow communication rates (sometimes as low as 110 baud) and subsequent lengthening of the response times and general degradation of the performance that is expected from modern DCS or computer-controlled process plants.

More recently, other protocols have been produced in order to provide the user with added benefits and more flexibility in satisfying the requirements of modern process control and the provision of on-line calibration and diagnostics. One of the main objectives of these protocols has been to offer true interchangeability and inter-operability between the products of different manufacturers since this affords the user the benefit of always being able to obtain competitive prices from a selection of suppliers. It also enables the user to quickly replace a faulty item of equipment with another without a lot of interface or calibration problems, regardless of the manufacturer.

Controlinc digital control networks can interface with several different network protocols through the use of a Communication Adaptor Module (CAM) and, currently, there are four protocols that are provided and fully supported by EIM, these being:

- **Modbus RTU** - CAM-205
- **DeviceNet** - CAM-207
- **Foundation Fieldbus H1** - CAM-208
- **Profibus DP** - CAM-210
Benefits of Digital Network Controls

- **Reduced Installation Costs**
  - Up to 60% saving in cost of cable since a single twisted pair, shielded cable is used instead of the multi-core cable used in conventional control
  - Reduced installation costs since less cable trays/ducting required and less time to install the cable and terminate each core at the actuator
  - Simplified engineering design and cable scheduling due to simplicity of network topology and standardized termination of twisted-pair cable
  - Reduced interfacing equipment in the control room compared to a conventional multi-core cabling system
  - Reduced time to commission and trouble-shoot the system since less cables to be terminated and all actuators can be communicated with direct from the control room via the network

- **Improved Efficiency**
  - Real-time diagnostics provides information that can be used to rectify equipment problems occurring on the plant or enable the planning of preventive maintenance programs, thus reducing downtime and lost production
  - Real-time alarming reduces hazards and process upsets, thus increasing the productivity of the plant
  - Increased visibility of the entire plant enables the operators to manage the process more effectively

- **Ease of Expansion**
  - Additional actuators can easily be incorporated in the control network during future upgrades or extensions to the plant without major changes to the existing network cabling
  - Additional actuators are given the next sequential node address and configured from the control room via the network or non-intrusively at the actuator
  - Changes to the configuration of the existing actuators can be performed easily from the control room via the network or non-intrusively at the actuator

- **Consistent Reliability of Communication**
  - Network cabling is inherently noise-resistant
  - All communication modules incorporate a high level of surge protection, comprising gas discharge tubes and transorbs, to protect against noisy environments and lightning
  - Network cabling is optically isolated at the communication module to prevent a single cable fault, such as a short-circuit or a ground fault, causing loss of communication with any actuator
  - Redundant ring topology of the network is possible in certain cases (Modbus E>Net ring) in order to prevent a single open-circuit in the network cabling causing loss of communication with any actuator
  - Double-sealed terminal compartment prevents ingress of moisture or dust in to the control compartment while cable terminations to the unit are being made, thereby preventing damage and/or corrosion to the unit
  - The communication protocols employed by EIM are entirely secure
  - Dual-redundant (Hot Standby) network masters are available for Modbus networks in order to provide two data paths to each actuator in case of equipment failure or damage to the network cable
MODBUS RTU Networks

The standard protocol, in use since 1985, is Modbus RTU. All the standard Modbus function codes are fully supported including the ‘Report by Exception’ command which enables the status of up to 100 actuators to be updated in less than 2 seconds. Up to 254 actuators can be installed in a single network and the overall length of the network cabling can be extremely long, without degrading the performance or response time of the network. The length of cable between each actuator, or between the controller and the first actuator in the network can be up to 1500 meters (5000 ft). There is no need to use separate repeaters.

Fully redundant networks comprising a serial loop topology are a standard feature and no single cable fault, open-circuit, short-circuit or ground fault, will cause a loss of communication to any actuator. Hot-standby, Redundant Network Masters are a standard option.

Network Master Station or Direct-to-Host

Controlinc Modbus Networks may be interfaced with the Supervisory Controller (DCS, PC, PLC, etc.) either utilising a Network Master Station, provided by EIM, or connected Direct-to-Host. The choice will depend partly on the type of application and the systems integration skills available to the customer: there are benefits to either of the two alternatives.

![Modbus Network Master](image1)

![Modbus Direct-to-Host](image2)
The major purpose of the Network Master is to act as a data concentrator; routinely polling all the devices on the network, storing current status and alarm data in it's memory and performing CRC (Cyclic Redundancy Checking) error detection on all the Modbus messages that are handled by it. It also controls all the network activity; processing commands received from the controller, formatting messages to send to the devices and controlling access to all the data paths. If a cable fault occurs, or if communication is lost to any of the devices on the network, then the Network Master automatically tries to access the non-communicating device(s) by switching communication from Port ‘A’ to Port ‘B’. It remembers which port has access to each device and switches backwards and forwards automatically, extremely quickly, to enable it to maintain communication with all devices on the network. After a pre-determined number of polls, the Network Master retries the original data path for that device so, as soon as the fault is cleared, it regains communication with all devices on Port ‘A’. Even if there has been no loss of communication with a device on Port ‘A’, the Network Master automatically forces communication with Port ‘B’ after every 800 polls of the network in order to check the integrity of the complete redundant network.

Commands received from the host controller are always given priority and routine polling is interrupted while these are processed and issued to the designated device. Commands are infrequent in most applications but, once a command has been issued, the operator needs to see status updates as quickly as possible in order to achieve full visibility of the plant. Special functions are included in the application software that is loaded in the Network Master in order to speed up the polling process. The first of these is “Report-by-Exception” polling which is a standard Modbus feature that ensures that only those devices that have had a change of status since the last poll are requested to give a full response to a status request from the Network Master, otherwise they are bypassed. Other features include the ability to set a different level of priority for individual devices so that some are polled more frequently than others, and devices that are transmitting (e.g. a valve that is moving in mid-travel) are automatically given priority so that they are polled frequently until they reach their desired state.

A keypad and LCD panel are recommended options for the Network Master since these provide the operator or maintenance personnel with the ability to control all the devices on the network in the case of failure of the host controller, assist with the commissioning of the network or to view alarms or status of individual devices.

The Controlinc Network Master is supplied, as standard, with two communication ports for connection to both ends of our recommended E>Net ring topology since this provides a redundant network automatically and two data paths to each device on the network. Dual-redundant, hot-standby Network Masters are a standard option when a higher level of integrity is required for a particularly important process/installation. In all instances, each port is fitted with surge suppression/isolation modules to protect the Network Master and higher level host controllers from surges/spikes emanating from the network cabling due to lightning strikes, etc.

This option is available for those users who want to configure/program their own host controller so that it communicates directly with the devices on the network, thus obviating the need for an intermediate device which may be viewed as a potential ‘point of failure’ even though the MTBF for the Controlinc Network Master is in the order of 15 years.

The host controller must be able to act as a Modbus Master that supports Modbus RTU protocol and have a RS485 serial interface operating at 9.6Kbaud (or higher), or use a RS232/RS485 converter if the controller only has a RS232 serial interface port. Ideally it should have two
communication ports so that a serial E>Net ring topology can be installed, along with surge suppression/isolation modules to prevent surges/spikes reaching the host controller from the network cabling. The user will need to configure/program the controller so that it issues commands to the devices, polls the devices on a frequent basis to retrieve current status and alarm data from them, and performs CRC error checking on all communication that is occurring.

This option may be attractive to users that have software engineers who are skilled with Modbus protocol, have only a few devices to control on each network, need to configure a quantity of similar installations (such as water filtration plants), and do not need a standby operator interface such as that offered with the Controlinc Network Master.

**Serial (E>Net Ring) or Bus (Multi-drop) Network Topology**
Network Master - Model M124 – Mini-Master

The M124 Mini-Master may be supplied in a weatherproof enclosure (IP65/NEMA 4) suitable for wall/bulkhead mounting or in an EIA 19” rack mount enclosure that conforms to EIA RS-310, IEC 297-1 and DIN 41 494, Part 1 standards.

- Includes field-proven application software and supplied fully engineered and ready to “plug-and-play”
- Control functions pre-configured
- Supports Controlinc E>Net Ring – Redundant Loop Topology
- System Setup and Configuration performed via host network using EIM CCU software – available free on the EIM website
- Modbus Host Link with RS232 and RS422/485 selectable, using Modbus RTU protocol
- Communicates with supervisory controller at high baud rate – 1200 to 115.2k bits/sec. Standard is 9600 baud
- Processes commands received from the Controller and format messages to send to the valves or other field devices
- Performs CRC error checking
- Communicates with the field devices at a minimum of 9600 baud
- Controls network activity and access to all data paths – ensures no loss of communication to any device in event of a single cable fault
- Network ports include isolation and surge suppression to protect against noise and spikes emanating in the field cabling
- Acts as data concentrator by routinely polling all field devices on the network
- Priority Polling for Commands and other instructions
- Priority Scanning of Moving MOVs ensures fast status updates
- Supports “Report-by-Exception” polling for faster status updates of valves in motion
- Supports up to 124 devices per network – option available for up to 254 devices (Model NM320)
- Provides fault management of actuator and monitors cable in case of short- or open-circuit, or ground fault
- Includes user-friendly keypad and LCD display
- Complete network may be commissioned from Network Master independently of Supervisory Controller
- Control the process with valve sequencing, interlocking, scheduling and PID closed loop control
- Ethernet (TCP/IP) wired or fiber optic host links available as standard options
- Hot-Standby redundancy option

Figure No. 3
Redundant Network

Controlinc offers true redundancy for the network because the Network Master is supplied with an electronic switching module and appropriate software to enable communication to be maintained with both ends of the looped network (E>Net Ring) that we recommend for the cabling topology. This ensures, together with opto-coupling of the network connections at the communication module, that communication is not lost to any MOV in the network due to a single cable fault (short-circuit, open-circuit or ground-fault).

Each Controlinc valve actuator has a network Port A and Port B connection on its communication module. When a message is received on either port, it is conditioned by hardware and transmitted at the other port. If a message is received on Port A, it is transmitted at Port B, and vice versa. Messages on the network are conditioned and transmitted in both directions without the intervention of microprocessor software. As the message passes through the communication module of the valve actuator, it is received by the microprocessor and, if the message address matches the module (actuator) address, the command is processed and the valve actuator responds to the host command. When the actuator responds, it transmits on both Ports A and B: therefore both communication channels of the network master receive messages returned from the field.

Network Interface Module (NIM)

All Controlinc Network Masters include two Network Interface Modules, one for each end of the E>Net Ring. These interface modules convert the RS232 signal of the Network Master to the RS485 signal that is required to achieve good communication over long distances in the field network: they also provide isolation and transient protection in order to prevent damage being caused to the Network Master in the event of voltage surges, spikes, noise, etc. occurring in the network cabling.

Network Length

EIM has designed special features into the Controlinc Network Master and field communication modules to ensure that there are virtually no restrictions to the length of cable that may be installed in an E>Net Ring network on a typical plant. Furthermore, the length of the cable has no affect on the communication rate (baud rate) of the Modbus messages being transmitted in the network: the customer can always rely on the baud rate being 9600 bits/second or higher, and a guaranteed response time to commands and feedback of status and/or alarm data. This approach has considerable benefits over proprietary current-based protocols that typically communicate very slowly and are significantly debased when longer loop distances are installed. Customers using these digital current networks can only determine the response and scan times of their system after the installation has been completed: so much depends on the resistance and capacitance of the cabling and the resistance of the connections through the terminals and junction boxes. From a maximum baud rate of 2400 that is typical of such networks, this figure can very quickly diminish down to 110, with the subsequent deterioration in response times and visibility of the various actuators installed in the plant.

On all Controlinc E>Net Ring networks the length of cable installed between the Network Master and the first actuator in the network may be up to 1500 meters, and between each subsequent actuator it may also be up to 1500 meters. Although this is unlikely to occur in practice, a network exceeding 150 km in length could be constructed if 100 actuators were each spaced 1500 meters apart, but this distance capability ensures that the customer is unlikely to encounter any problems when installing a Controlinc E>Net Ring network. Please refer to Fig. 4 on page 6.

This exceptional performance is achieved by incorporating special hardware in each field communication module that conditions the digital signal as it passes through, thereby ensuring
that the amplitude of the signal, the squareness of the waveform and the correct number of bytes are contained in the message. The digital signal being transmitted out of the communication module is as strong as when it left the Network Master. This is achieved without the need for repeaters, either in the communication module or elsewhere in the network.

Should customers elect to install a Controlinc network with a multi-drop topology; the total length of the cable that may be installed is limited to 1200 meters for up to 32 actuators: this is a requirement of the Modbus Standard and applies to all suppliers of Modbus-compliant devices. If longer lengths of cable or a larger number of actuators need to be installed, then a repeater must be installed in the network for each additional 1200 meters of cable or 32 actuators. Please refer to Fig. 5 on page 6.

Digital Communication Module (DCM)

The DCM is enclosed within the electronic control package contained in the actuator and is powered from the control transformer: no additional power supply is required. Each DCM has a Port A and a Port B, both ports having opto-isolation and surge suppression hardware to protect the internal electronics from damage due to noise or spikes that might occur in the network cabling. It also ensures that communication is maintained with the actuator via the other port should there be a short-circuit or ground-fault in the network cabling connected to the other port: this is applicable for E>Net loop topology only, not for multi-drop bus topology.

The DCM is designed in such a way that, when a message is received on Port A, it is conditioned by hardware and then re-transmitted automatically at Port B, and vice-versa; this signal conditioning and bi-directional transmission being achieved without the intervention of microprocessor software. As the message passes through the communication module, it is received by the microprocessor and, if the message address matches the module (actuator) address, the command is processed and the valve actuator responds to the host command. When the actuator responds, it transmits on both Ports A and B: therefore both communication channels of the network master receive messages returned from the field.

Scan Times

Scan times in a Controlinc network can be estimated quite accurately prior to system start-up because the baud rate is fixed at 9600 regardless of the length of the network cabling, providing our recommendations are adhered to. The variables that affect scan times include the number of commands that are being sent by the host, the number of valves that are in transition and the activity of operators in the plant itself. In a typical installation, valves are operated infrequently so there will be no status updates to report because they will not have changed position: there will be more activity if some of the valves are modulating duty.

As stated elsewhere in this document, the Controlinc Network Master utilizes the Modbus Function Code 07 to retrieve data from the actuators by report-by-exception polling of the
network. The time taken to communicate with an individual actuator by this method, and receive a response, is in the order of 18mS.

The time taken to obtain a complete status update from an actuator will be 26mS, excluding data processing by the Network Master, or 38mS when data processing is included.

Network Fault Detection

Whenever the Network Master gains access to the network it performs a network test: it transmits a message from Port A and verifies that it is received through the network at Port B, then it transmits from Port B and checks that the message is received at Port A. If the message is not received on either port after three attempts, it then sets the network fault alarm. It then polls from Port A around the ring in the order of slave address from the scan list for the total number of actuators configured. The module records the last address that responded as the fault location ‘low’ address. The module then polls the network from Port B, starting with the last configured address in the scan list and decrementing to the first address in the scan list, and records the last address to respond as the fault location ‘high’ address. The network fault is located between the ‘low’ address and the ‘high’ address and this information is available to the host in dedicated Modbus registers. Each time the module finishes five (5) complete poll cycles of all network addresses, it repeats the network fault test.

If a network fault is detected, the module polls the accessible addresses around the ring in one direction from Port A and then polls around the ring in the opposite direction from Port B: this function is performed automatically by the software installed in the Network Master and, since the switching is performed electronically, there is no time delay in the module accessing all available actuators on both sides of the network.

Under network fault conditions, the module polls one address from the scan list higher than the last address to respond, i.e. it polls one address past the fault location. If the address past the fault responds, the network fault alarm is reset and normal polling resumes.

Polling Process

The Network Master module gets the slave address for each actuator on the network from a scan list located in the global data that is loaded into it from the database at power up; the database having been prepared prior to shipment of the Network Master. For optimum efficiency in the location of network faults or actuators that are not responding, this database should include the address of the actuator, the Tag Number of the valve that it is attached to and the physical position of the actuator in the network. Otherwise, there is no need for the addresses of the actuators to proceed sequentially around the network.

If a valid address is the next address in the poll sequence, the actuator is polled and received data is stored in the global database by address sequence, not scan list sequence. If an actuator does not return data for three poll cycles, the module sets the COM alarm bit for that slave address but only when both network paths have failed, meaning both Port A and Port B of the module have lost access to the actuator. The COM alarm bit is reset when either port regains access to the actuator.

Report-by-Exception Polling

Controlinc Network Masters use Modbus Function Code 07 for report-by-exception (RBE) polling and this process speeds up the system throughput by a factor of four to six times due to the small amount of data being transferred over the network. Throughput is also increased due to the fact that no data is processed into the database, the most time-consuming activity, until data has changed.
The module normally polls all actuators with Function Code 07 and, if an individual actuator does not have any changes in status, alarms or analog values since the last request from the Network Master, it returns ‘00’ in the Function 07-processor status field, and the module simply moves on to the next address in the scan list. If data has changed since the last poll, the actuator returns ‘FF’ in the processor status field to indicate an exception, in which case the module now polls the same address using Modbus Function Code 03 and requests a full status update, in one block of data, that is then processed into the database. To ensure that the host system always has an accurate database, the valve actuators automatically force an exception after every 200 poll cycles.

**Priority Scan**

In order to increase the visibility of the plant to the operator, when a command is received from the host to operate a valve, the Network Master module issues the command to the actuator and then puts the actuator’s address in priority scan. If a valve transition status (opening or closing) is received from an actuator, it’s address is also put in priority scan. The module then polls the actuators that are in priority scan first, before proceeding with the next address in the scan list, continuing with this pattern of interlace scanning of moving valves between non-moving valves. This ensures a fast update of moving valves to the host system: an unlimited number of addresses may be in priority scan at any one time but, as soon as the opening or closing transition has ended, the address is automatically removed from the priority scan.

In addition to the automatic priority polling of MOVs that are still in transition, the Network Master may also be configured to give weighted priority to the most important MOVs on the network: these will be polled on every scan cycle whereas less important MOVs will be polled only on every 2nd or 3rd scan cycle.

**Commands**

Commands received from the host automatically have priority over the scanning routine for status updates: the Network Master interrupts the scan and immediately sends the command to the designated address. When commands are received at the Network Master, they are stored in the global database and an interrupt to the central CPU is set. The CPU then writes the commands to the Network Master module which, in turn, generates an interrupt to the module and causes immediate processing of the commands. The module decodes the commands, determines which slave address is to receive the command and then, providing the address is in the scan list, transmits the command to the appropriate actuator. The module then waits for an acknowledgement from the actuator and, if this is not received within the time-out period, the command is retransmitted up to three times on Port A and three times on Port B. If, after these further transmission attempts, an acknowledgement is still not received the COM alarm bit for this address is set in the module, which in turn is reported back to the host when it next polls the Network Master.

The host may send commands for multiple valves at the same time and, when this happens, the module will decode each command in the order of the slave address and transmit each in turn. The time taken to decode each command and transmit it to the valve is in the 100mS, so the interruption to the normal scan causes a very short delay in updating the host with the status of all the valves on the network.

The command signals available are:

<table>
<thead>
<tr>
<th>Digital Control</th>
<th>OPEN / STOP / CLOSE / ESD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analog Control</td>
<td>SET POSITION 0-100%</td>
</tr>
</tbody>
</table>
The Controlinc Network Master has a standard option of a Keypad and LCD display which allows configuration and local diagnostics to be performed from it and status information to be determined. This is a significant feature that has major benefits in the commissioning of a network and then as a backup controller in case of the failure of the Host Controller in the Control Room, in which case it may be used to control all the MOVs in the network.

**LCD Keypad Terminal**

- **Valve Status Lights**: Displays the valve status.
- **Display Mode Key**: Selects Valve Status or Alarm Display.
- **Up/Down Arrow Keys**: Increments Alarms when Alarm Display Selected.
- **Valve Control Keys**: Used to select valve.
- **Selector Switch**: Auto / Off / Manual.
- **Network Station Address**: User Designated.
- **Valve Tag Number**: Displayed when any alarm(s) are present.
- **Valve Position**: 0 – 100%.
- **LCS Display**: Valve Status.

**Figure No. 5**
LCD Message Center displays the node address of the valve being interrogated, the valve tag number, the position of the valve 0-100% Open, whether the actuator is in ‘Manual’, ‘Off’ or ‘Auto’ mode and an “Alarms” message to indicate that a fault exists in one of the devices on the network.

Valve Status Lights provide position status of the valve – CLOSE, STOP & OPEN. If the valve is in transition, either the CLOSE light or the OPEN light will flash to indicate the direction of travel.

Valve Control Keys enable an individual valve to be operated – CLOSE, STOP & OPEN.

Display Mode Key enables the LCD display to be switched between “Status” mode or “Alarm” Mode. Valves may be controlled only when “Status” mode is selected.

Next Alarm Key that increments the alarm messages when there are faults on the network, only operative after the “Alarm” mode has been selected.

ESD Command Emergency shutdown (ESD) command may be sent to all valves from the control keys by pressing both CLOSE and NEXT ALARM keys at the same time. When the command is executed, the message *** ESD *** will be displayed.

Special Features

Enable/Disable Valve Control from LCD Terminal & Keypad

Valve control from the LCD terminal may be enabled or disabled, using a passcode provided by EIM, thus preventing unauthorized personnel from operating valves and endangering the correct functioning of the plant. Unless instructed otherwise, the system is shipped with the passcode disabled and the LCD valve control function enabled at all times.

Switch Active Master to Hot-Standby Master

On hot-standby installations, the active Network Master may be switched to go to hot-standby mode and allow the Network Master currently on standby to switch to the active role. This allows the two masters to be toggled between active and standby modes thereby enabling their operation to be checked or maintenance to be carried out.
Single Network Master and Redundant Loop Network Topology

- All actuators installed in E>Net Ring – Redundant Loop topology
- Single or Dual Serial Interface to Supervisory Controller may be RS-232, RS-485 or RS-422
- 2 Data Paths from Network Master to each device on the network
- Open-circuit, short-circuit and ground-fault Protected
- No loss of communication with any actuator in event of a single cable fault
- Long cable distances may be installed
  - Upto 1500 meters (5000 ft) between Network Master and 1st actuator/device in network
  - Upto 1500 meters (5000 ft) between each subsequent actuator/device
- Minimum 9600 baud rate regardless of loop cable length or number of actuators on the network
- Up to 124 devices on a single network – Model M124N
- Up to 254 devices on a single network – Model NM320

Single Network Master and Multi-drop Network Topology

- May be either one Data Path (as shown) or two Data Paths (Loop topology) to each device from Network Master
- No short-circuit or ground-fault protection in the network
- If only one Data Path there is open-circuit protection only to the first cable fault
- Redundancy included only if loop topology installed
- Maximum network cable length is 1200 meters (4000 ft)
- Maximum number of valves in network is 32
- Repeaters required to extend the network. Repeater should be installed in the network cabling for each additional 32 valves and/or 1200 meters (4000 ft) of cable extension
Direct-to-Host Interface with Supervisory Controller

- Host must support Modbus RTU protocol and be configured to act as a Modbus Master
- Host must be programmed to issue commands and retrieve status & alarm data from all actuators, or other devices, by polling the network at frequent intervals
- Host should perform CRC error checking to network and status or diagnostic data received from it
- Host should communicate via RS485 signal or include a RS232/RS485 converter since network operates with a RS-485 electrical signal and Modbus RTU protocol
- To ensure redundancy of Data Paths, Host should have two ports to enable it to communicate with both ends of an E>Net ring network
- Network topology may be E>Net ring or multi-drop but E>Net ring provides more redundancy

Figure No. 8
Dual-Redundant Hot-Standby Network Master

The above illustration shows three networks arranged in a fully redundant architecture, with two hosts linked to each of the dual-redundant, hot-standby Network Masters via a RS485 bus. Each individual actuator may be accessed via two (2) data paths, thereby ensuring that no single cable fault or failure of one of the Network Masters will cause a loss of communication with any of the actuators.

The redundant Network Masters are pre-configured so that one of them is the ‘Active’ master and the other the ‘Standby’ master: on power-up, the ‘Standby’ master delays polling by 2 seconds to allow the ‘Active’ master to take control of the network. This forces the ‘Standby’ unit to remain in the ‘Hot Standby’ mode for as long as the ‘Active’ master is communicating on the same network. The functioning of the dual-redundant Network Masters and the changeover from ‘Active’ to ‘Standby’ is handled automatically, without the intervention of the operator, by the application software loaded into each device. After power-up, both masters listen to the network to which they are connected for 500mS: if no activity is detected (quiet line) then the module designated as the ‘Active’ master checks the status of the host links to both masters. If one of the masters is not present then the other will proceed to take control of the network, providing it has a good host link. If network activity is detected during this process, the timer is reset to 200mS and the whole process begins again. If, at any time during the listening process, the ‘Standby’ master detects a quiet line, it will begin the polling process and thus take over control of the network, but only if a good host link is detected. During the polling process, if another master’s message is received (since it is operating as the ‘Active’ master), this master will go into Hot Standby mode and begin listening to the network again. This process requires less than 1 second to complete whereas the normal listening process takes up to 2 seconds to fail over.

In the case of redundant host links, if all host links to the ‘Active’ master are bad, the module will check the status of the host links to the ‘Standby’ master. If those links are good then the listen mode will be repeated, thus allowing the ‘Standby’ master to take control. Each master resets its
own watchdog timer when valid data is received from the network but it also checks the status of its watchdog timer on every poll cycle. If the watchdog timer times out, the master goes to the listen mode and turns the network over to the ‘Standby’ master. Also included is a feature which makes the masters count the number of responses from the slave addresses: if the number of no responses exceeds the number of connected devices - plus ten (10), without receiving good data, then the ‘Active’ master goes into listen mode and releases the network to the ‘Standby’ master. Normal failover time is 800mS for problems other than host link failures whereas it may be up to six seconds for host link failures from the time the host stops polling the master.

**Control or Collect Data from other Devices**

All DCMs have spare inputs and outputs that may be used to control other devices or collect data from them: the devices would be hard-wired to the dedicated terminals in the actuator.

**Control Ancillary Devices**

- Start/Stop pumps, fans, mixers, etc.
- Operate pneumatic actuators via solenoid valve control
- Control analog devices via 4-20mA signal

**Collect & Transmit Data**

- Collect digital data from switches, alarm contacts, etc.
- Collect analog data from transmitters, transducers, flowmeters, etc.
- Transmit data to host controller

**Field Network Wiring – E>Net Ring**

- The network ports should be wired as shown opposite, taking care to maintain the correct polarity throughout the network.
- The shield of each twisted-pair cable should be connected at each DCM, as shown, ensuring that continuity of the shield is maintained throughout the network or each section of the network.
- The shield should be grounded at only one point in the network, or in each section of the network, in order to avoid circulating currents occurring in the cable shielding.
- Ensure that all connections are fully tightened in order to avoid poor continuity in the future.
- Ensure that all cable terminations are completed correctly and without damage to the insulation that might cause short-circuiting of the cable cores.
Field Network Wiring – Multi-Drop

- The network ports should be wired as shown opposite, taking care to maintain the correct polarity throughout the network
- The shield of each twisted-pair cable should be connected at each DCM, as shown, ensuring that continuity of the shield is maintained throughout the network or each section of the network
- The shield should be grounded at only one point in the network, or in each section of the network, in order to avoid circulating currents occurring in the cable shielding
- Ensure that all connections are fully tightened in order to avoid poor continuity in the future
- Ensure that all cable terminations are completed correctly and without damage to the insulation that might cause short-circuiting of the cable cores

Status & Alarm Reporting

A wide range of status and alarm data is stored in the communication module of each actuator and may be retrieved for control, display and diagnostic purposes: the following status information is stored in contiguous registers and may be incorporated into the host controller as required by the systems integrator:

1. OPEN limit switch - Valve Fully Open
2. CLOSE limit switch - Valve Fully Close
3. Transition Opening - Valve is Moving in Open Direction
4. Transition Closing - Valve is Moving in Close Direction
5. Local Mode - Selector Switch in LOCAL Position
6. Remote Mode - Selector Switch in REMOTE Position
7. OPEN Torque Alarm - Torque Overload in OPEN Direction
8. CLOSE Torque Alarm - Torque Overload in CLOSE Direction
9. Valve Stall Alarm - Valve Failed to Move
10. Power Monitor Alarm - Loss of Control Voltage
11. Motor Overload Alarm - Motor Overload Relay Tripped
12. Phase Monitor Alarm - Incoming 3-Phase Power is Reverse-Phased
13. Local ESD Alarm - Local ESD Input Activated
14. Actuator Fail Alarm - Failed Self-Diagnostics
15. Com No-Response Alarm - Communication Failure on Both Ports
16. Unit Alarm - General Alarm if one or more alarms 7 through 13 are Active

Other status information available, depending on configuration of actuator:

1. Valve Position 0-100% - Analog Position in 1% increments
2. Torque Profile - Torque Readout at 10% increments throughout Valve Travel
Hard-wired Local Controls

All EIM electric actuators that are suitable for network control have local controls that are hard-wired and bypass the micro-processors in the electronic control package, thereby enabling the valve to be operated locally in the unlikely event of a failure of the communication module in the actuator. There is also a dedicated ESD input that is hard-wired: this ensures that the valve can always be stopped in it’s last position or prevented from moving by the application of a single contact from a remote stayput pushbutton, configurable as normally open or normally close.

Modbus Function Codes Supported

<table>
<thead>
<tr>
<th>Host Beginning</th>
<th>Register</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>Read Coil Status 00001</td>
</tr>
<tr>
<td>02</td>
<td>Read Input Status 10001</td>
</tr>
<tr>
<td>03</td>
<td>Read Holding Register 40001</td>
</tr>
<tr>
<td>04</td>
<td>Read Input Register 30001</td>
</tr>
<tr>
<td>05</td>
<td>Force Single Coil 00001</td>
</tr>
<tr>
<td>06</td>
<td>Preset Single Register 40001</td>
</tr>
<tr>
<td>07</td>
<td>Read Exception Status</td>
</tr>
<tr>
<td>08</td>
<td>Loopback Diagnostic Test</td>
</tr>
<tr>
<td>15</td>
<td>Force Multiple Coils 00001</td>
</tr>
<tr>
<td>16</td>
<td>Preset Multiple Coils 40001</td>
</tr>
<tr>
<td>17</td>
<td>Report Slave I.D.</td>
</tr>
</tbody>
</table>

Control Selector Inhibit (Local / Off / Remote)

User relay 1 is a programmable relay that can be energized / de-energized by a network command. To inhibit unit operation the internal user relay 1 is wired in the STM terminal compartment to the Open & Close Inhibit terminal and programmed to monitor the Local / Remote selector switch. If there is a change of status of the selector switch then the User relay 1 will be energized and inhibit and operation from local and remote commands. The DCS will need to monitor the status of the Selector switch for a change in status and issue an alarm if an unauthorized change is made.

The selector switch change can be validated by controlling the status of User relay 1 and can then release the unit for control locally and remotely.
Technical Data

Network Masters

Dimensions

EIA 19” Rack Mounting Enclosure

This enclosure conforms to EIA RS-310, IEC 297-1 and DIN 41 494 (Part 1) standards, with rear terminals and connectors, and applies to the following Network Masters:

Model M124N Mini-Master – Dual Redundant Type
Model NM320A-L Master – Single Type

Note:
Model NM320A-L Master – Dual Redundant Type will be contained in two (2) 19” Rack Mounting enclosures but the Standby Master will not contain the LCD & keypad.
The rack in which the enclosure is mounted must allow a minimum of 508mm (20") depth, allowing space for cable connections.

Cabinet for Wall/Bulkhead Mounting

This cabinet has a weatherproof enclosure (IP65/NEMA 4) that is suitable for bulkhead or wall-mounting using the internal mounting holes, or an external mounting bracket: it is supplied with five compression-type cable entry hubs on the base, and applies to the following Network Masters:

Model M124N Mini-Master – Dual Redundant Type
Model NM320A-L Master – Dual Redundant Type

Depth of enclosure: 190mm (7.5")
Cable Entries: (5) cable entries provided, spaced 63mm (2.5") apart

Environmental

- Storage temperature: -20°C to +70°C
- Ambient operating temperature: 0°C to +55°C
- Ambient humidity: 5% to 95% (non-condensing)
- Vibration resistance: MIL STD 810C, Method 514.2
- Shock resistance: MIL STD 810C, Method 516.2

Electrical
Supply voltage: 100 to 240 VAC (specify with order)
Other options available
Total power consumption: 25 VA nominal (includes LCD/keypad)
Isolation resistance: >10 MΩ @ 500 VDC
Dielectric withstand voltage: 1500 VAC @ 1 minute

Host Communications

Each Network Master has two Modbus RTU communication ports
May be configured as: RS232 full duplex, RS422 (4-wire) or RS485 (2-wire) half duplex

LCD Panel

Display type: 2-Lines x 16-Character LCD, LED Status lights
Enclosure: IP65 (NEMA 4)
Input voltage: 8-32 VDC
Power consumption: 5 VA @ 24 VDC
Operating temperature: 0°C to 50°C

Keypad Controls

Numeric keypad
Up/Down arrow keys, Enter & Cancel Entry keys
Open/Stop/Close keys
Display Mode & Next Alarm keys

Password Protection

Password protection, to prevent unauthorized operation of the keypad, is a standard feature.
Password protection may be enabled/disabled by the user.

Cable Recommendations

For optimum performance, Controlinc networks should be installed using twisted pair and shielded cable with a characteristic impedance between 50 and 120 ohms: the capacitance between conductors must be less than 98 pF/m (30 pF/ft): shielding may be aluminum foil with drain wire. Only cables with stranded conductors are recommended since this significantly reduces the risk of cable breaks. The insulation and outer jacket materials should be selected to suit the application environment.

The following are acceptable Belden cables (1-pair) for most network applications but equivalent cables are available from other manufacturers:

<table>
<thead>
<tr>
<th>AWG</th>
<th>Belden 8162</th>
<th>78 pF/m</th>
<th>24 pF/ft</th>
<th>Belden 8762</th>
<th>88 pF/m</th>
<th>27 pF/ft</th>
<th>Belden 8760</th>
<th>78 pF/m</th>
<th>24 pF/ft</th>
<th>Belden 8719</th>
<th>75 pF/m</th>
<th>23 pF/ft</th>
<th>Belden 8720</th>
<th>78 pF/m</th>
<th>24 pF/ft</th>
</tr>
</thead>
<tbody>
<tr>
<td>24AWG</td>
<td>Belden 9841</td>
<td>42 pF/m</td>
<td>12.8 pF/ft</td>
<td>22AWG</td>
<td>Belden 8761</td>
<td>78 pF/m</td>
<td>24 pF/ft</td>
<td>20AWG</td>
<td>Belden 8762</td>
<td>88 pF/m</td>
<td>27 pF/ft</td>
<td>18AWG</td>
<td>Belden 8760</td>
<td>78 pF/m</td>
<td>24 pF/ft</td>
</tr>
<tr>
<td>16AWG</td>
<td>Belden 8719</td>
<td>75 pF/m</td>
<td>23 pF/ft</td>
<td>14AWG</td>
<td>Belden 8720</td>
<td>78 pF/m</td>
<td>24 pF/ft</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Belden 8162, 9729 and 9842 are suitable 2-pair, 24AWG cables with capacitance <42 pF/m (12.8 pF/ft).
Data Line Termination

There are a number of manufacturers of cables suitable for network, typical cable types manufactured by Belden with conductor sizes of, 18 awg (0.823mm²), 22 awg (0.326mm²) and 24 awg (0.205mm²).

A termination must be used to interface the data line to the terminal screw in the termination compartment of the TEC2000 actuator. It is important to use the correct terminal lug for the wire size, and crimped using the manufacturers recommended tool. Using the incorrect terminal lug or tool to crimp to the conductor will result in a poor connection and will eventually fail.

Signal Cable Installation

The signal cable used on Controlinc systems frequently contains 24awg twisted pair shielded wires. The signal shield of this cable must be grounded at one end. This shield, when properly grounded, provides protection against high electric fields caused by a high voltage in the vicinity. This protection is accomplished by providing a discharge path for the charge induced by the electric field. The ground connection also provides a discharge path for the surge protection devices that protect the electronics from high voltage spikes.

Very rarely is there a suitable earth ground rod at each valve actuator. In general, the safety ground (the fourth wire of the three-phase power cable) is used to provide the grounding connection back to the power system earth ground connection. Of course, the shield must be grounded only at one end in order to avoid ground loops. Section 6 provides some data on noise injection caused by improper grounding. For the moment we'll assume the ground connection is adequate.

For a redundant system there will be two cables entering the terminal compartment of the valve actuator, channel A and channel B. The EIM TEC2000 valve actuator terminal compartment is illustrated showing the wiring terminals.
Consider the first valve actuator or Unit No. 1 in the loop. The signal cable coming from the control room to Unit No. 1 is connected to Channel A+ (terminal #39) and to Channel A- (terminal #41). The control cable going from Unit No. 1 to the next valve actuator or Unit No. 2 in the loop is connected to Channel B+ (terminal #43) and to Channel B- (terminal #44).

When connecting a braided shield and/or its drain wire cover with insulation so that it cannot touch any part of the housing. Signal cables must be in their own conduit and is kept at a distance from the power cable. Also, note that both signal in and signal out cables will be identical in appearance which makes it impossible to determine (except where connected on the terminal block) which cable comes from the control room and which cable goes to the next valve actuator down the line. The channels on the Controlinc are unidirectional in that what is received on a channel is automatically transmitted out to the next valve actuator. However, if the signal cables are reversed, it is a good possibility that the shields are improperly connected.

The TEC2000 valve actuator option compartment with CAM 205 Modbus module.

The following procedure will insure that the signal cables and their shields are connected properly. This procedure will determine whether:

a) the signal lines are connected with the correct polarity.

b) the shields are connected to ground only at one point.

c) the control room is around the same ground as the valve actuator ground, or are the valve actuator grounds the same between valve actuators.

The polarity checking procedure to determine the correct polarity connection is the simplest.....

1) Insure that a cover exists over the power terminals in the valve actuator since this procedure is performed at the valve actuator with power applied.

2) Insure that the Master Controller (if not Direct-to-host) is powered up and that the Master Controller is not transmitting signals. This latter requirement is accomplished by disconnecting the network connection from the Master Controller. This will avoid any transmitted signals from reaching the converter and still allow the DC bias voltage to be applied and easily read without the RS485 signal masking the bias voltage.

3) Insure that the valve actuator being checked is powered up (power to the valve actuator can be disconnected after the signal line polarity is checked).

4) Using a high impedance digital voltmeter, the voltage from A(+) to A(-) or from B(+) to B(-) should be a minimum of +0.25 VDC. Terminal 39 and/or terminal 43 are positive. A voltage greater than 0.2 VDC will activate the receiver. With the correct bias, the receiver (when in the idle state) is forced continuously on. If there is a reversal of polarity between one valve actuator and the next, the DC bias voltage is reduced to approximately zero. In this condition, a very slight noise generated voltage will incorrectly turn on and off the receiver at the valve actuator and will be interpreted as an incoming signal. This could effectively block a true incoming signal from being received.

The recommended colour coding of white for A(+) or B(+) and Blue for A(-) or B(-). A consistency of colour
coding will reduce the possibility of incorrect polarity connection.

The following procedure is to insure that the shield is connected to ground at only one point:

1) Temporarily disconnect the shield from the ground. This should be the cable coming from the previous valve actuator or Master Station. The wire numbers inside the shield should be A1 and A1*. For the purpose of this discussion, we will assume the shield ground is the same as the safety or equipment ground.

2) Selecting the incoming signal cable and, using an ohmmeter, measure the resistance from the disconnected shield to the ground connection. The resistance should be infinite since we have disconnected the single point ground. If the ohmmeter indicates low resistance, a bare portion of the shield is touching the equipment somewhere in the conduit. Or the signal cables have been reversed and this cable is going to the next valve actuator away from the control room and not to the previous valve actuator. Correct the problem and connect the proper shield to its ground.

3) Now select the outgoing signal cable and, using an ohmmeter, measure the resistance from the unconnected shield. Touch the other ohmmeter probe to the equipment ground. The resistance should be the resistance of the shield.

The circuit is through the shield to the equipment ground at the next valve actuator, then return through the common equipment ground.

The shield resistance will vary from less than one ohm to several ohms depending on how many feet of shield is involved. The common equipment ground will have much less than one-ohm resistance.

If Belden 9841 cable is used, the shield resistance is 3.35 ohms per 1000 ft or 11.0 ohms per kilometre.

If the resistance measured is high or is infinite, either

a) the shield is not connected, at the opposite end of the cable.......or

b) the equipment ground at the opposite end of the cable (usually the control room) is not the same ground as the equipment ground at the valve actuator.

The problem is easily corrected if a) is the cause. It usually means that the incoming and the outgoing cables have been reversed. The solution is more complicated if b) is the cause. This is addressed in the following paragraph.

When the equipment ground is not the same ground at the two ends of the signal cable.

1) When the opposite end of the signal cable resides in a valve actuator and the two equipment grounds are not connected, the solution must be reported to the user or the contractor. Equipment grounds are also used as safety grounds and must be at the same ground potential; this means that they must be connected together.

2) When the opposite end of the signal cable resides in the control room, it is quite likely that the equipment ground (usually the instrument ground) in the control room is different from the equipment ground at the valve actuator. Do not connect the two equipment grounds together. This could possibly inject noise from the valve actuator safety ground into the control room instrument ground. Let us assume for the moment that this is the only point where the equipment grounds at the two ends of the signal cable are different.

If the control room is within 100 feet of the first valve actuator, it will not matter which end of the shield is grounded as long as only one end of the shield is grounded!

If the control room is far from the first valve actuator, leave the ground connected to the shield in the control room. If poor communication results, remove the shield ground from the control room end of the signal cable and connect the shield to the equipment ground in the first valve actuator. This will mean, in the first valve actuator only, that the shields of both cables will be connected to the equipment ground at that first valve actuator. The balance of the valve actuators will conform to the standard procedure, which insures that the shield is connected to ground at only one point as described above. If poor communication still occurs, disconnect the cable going from the first valve actuator to the second valve actuator. This will determine if the problem is with the shielding to the first valve actuator. If poor communication still exists, the paragraph below must be followed. If the poor communication is eliminated, the problem is with valve actuators further down the line.
The problem is serious if the equipment ground between valve actuators is not a 'low resistance' solid wire connection. This means that the user is depending on the mechanical connection between valve actuators (usually the pipeline) for the equipment ground. This is rarely acceptable for the safety ground, and is not suitable for the shield ground. The preferable solution is to run a heavy ground wire (sometimes called a drain wire) in the conduit with the signal cable. This ground wire will be grounded at one point and serve as the shield ground where necessary as well as the electronic circuit ground for the network surge protection.

However, by the time that the lack of a good common equipment ground is discovered, the field wiring is installed and the additional wire for the common ground cannot be added. In this case, the only choice is to ground the shield in the control room and connect, at each valve actuator, the shield of the incoming cable to the shield of the outgoing cable. Do not connect the shield to any of the equipment grounding. Connect the network surge protection ground (terminal) to the equipment ground stud. Divide the valve actuators into two equal parts. Ground the shield in the control room for signal cables going to each group of valve actuators. One valve actuator in the middle of the loop will have the shields not connected. At this valve actuator, the incoming cable will have its shield grounded at the control room on channel A1. The outgoing cable will have its shield grounded at the control room on channel A2. The two shields will not be connected to each other only in this valve actuator.

Noise Tolerance on Data Lines

Common mode noise is (in our case) that unplanned voltage, which appears between the receiver common and both of the RS485 receivers signal inputs. Because the RS485 receiver senses the voltage difference between the two signal inputs, common mode noise cannot cause false signals. This is to say that the receiver receives only differential mode signals. However, common mode noise can cause damage to the RS485 receiver. The receivers used in the Controlinc are rated at +12 volts maximum above receiver common and -7 volts maximum below receiver common. The common mode over voltage protection is two 6.2 Vdc Zener diodes and two 10 Vdc Zener diodes. The Zener diodes can absorb 500 milliwatt of power. A continuous common mode voltage in excess of +10 volts peak or -6.2 volts peak could possibly cause a Zener diode to fail and then subsequently damage the RS485 receivers.

Having said all of the above, the common mode noise voltage is very difficult to measure due to the fact that (on the TEC2000 actuator) the receiver common is not available at the customer terminal block. A noise voltage can be measured from the surge ground or from the shield ground (on one signal cable, these two points are the same) to any of the signal lines (A(+), B(+), A(-) or B(-)). This is not the common mode voltage that was discussed in the paragraph above. A noise voltage greater than 3 volts RMS or 4.2 volts peak appearing between the surge common and any of the data lines, or between the shield and any of the data lines. This is an indication that common mode noise is perhaps being injected onto the data lines and returned through the capacitive coupling between the signal receiver common and the shield common or surge common.

Noise voltage can easily be separated from the signal voltage with an oscilloscope. The signal voltage is regular square wave signals; the noise voltages are random which are rarely square waves. If no oscilloscope is available, disconnect the RS232 signal at the signal converter in the control room and use a high impedance digital voltmeter. If a voltage of greater than 31 volts RMS is observed between the shield and any data line, this indicates that there is a noise voltage on the shield.

If the frequency of the noise voltage between shield and data line is the same as the power line frequency, then the equipment ground probably causes noise voltage. This being the power safety ground and the power safety ground having a current flow due to an unbalanced three-phase load. You should bring this matter to the attention of the user or contractor. There is a possibility that this voltage will cause no communication difficulty or damage, but the only assurance is to open up the valve actuator and place an oscilloscope between the receiver common and either data line. This should be done only by a EIM trained serviceman or representative.

If the frequency of the noise voltage is a high frequency (only detectable with an oscilloscope), this voltage is from an external source. A variable frequency drive will generate 6-14 kilohertz noise on the power line. This can also appear on the power neutral or common and usually the signal cable shield is connected to the power line neutral or common. This is particularly true when
the power line neutral is also the equipment safety ground.

The best solution for eliminating either power line frequency noise or external high frequency noise is to find a different shield ground. Try using one of the solutions discussed in section 3.

**Differential Mode Noise** is unplanned voltage which appears between the two signal lines. It is the unplanned voltage between A(+) and A(-) or between B(+) and B(-). Differential mode noise will disrupt communications. This type of noise is generated from magnetic varying fields. The signal lines in all signal cable are twisted to avoid this type of noise.

Check the data lines as they exit from the signal cable. Insure that the twist remains between the two data lines for the full distance between the exit point and the termination point. Differential mode noise of power line frequency can be coupled into the data lines if the two data lines are not twisted as they pass in the vicinity of the power wires. When differential mode noise is of a high frequency, an oscilloscope is needed. If high frequency noise is present, look for the source. A variable frequency drive again can be the source of this noise. If variable frequency drives are injecting high frequency noise onto the power lines, the best solution is to either place reactors in the feed to the variable frequency drive (this is expensive) or to switch the valve actuators to another power source (may be difficult to accomplish). The only other solution is to find the point where the high frequency noise is being injected into the electronics or onto the data lines and then filter out the noise at this point.

Simply said: "**Differential mode noise cannot be allowed to remain on the data lines.**"

---

**Signal Isolators**

It has been experienced by manufacturers and suppliers of networking systems that the use of isolators increases the ‘point-of-failure’ within a system.

Example 1 opposite shows the standard connections with only 4 possible points-of-failure.

Example 2, is connected via an isolator, this involves extra wiring and connections, which increases the point-of-failure per field unit to 12 points. Also, the contacts can increase resistance in the wiring loop over a period of time. Typically, a system with 60 field units with standard wiring would have 240 resistance/failure points. With isolators, there would be 720 resistance/failure points, which directly influences to reliability of the system.

It should be noted that the field unit would become transparent to the system if the power supply were de-energised to an actuator. This means that in normal circumstances no wiring changes would be necessary unless the actuator is physically removed. If this is the case then a temporary, simple cost effective explosion or weatherproof junction/link box can be used to connect the network wires together (Example 3).
© Signal Cable

Signal cable must be a twisted pair shielded signal conductor. The normal impedance @ 1 MHz must be 120Ω (±10%). These three typical network cable types manufactured by Belden.

<table>
<thead>
<tr>
<th>Catalogue Number</th>
<th>Conductor AWG</th>
<th>Nominal Impedance @ 1MHz</th>
<th>Nominal Capacitance between conductors @ 1kHz</th>
<th>Nominal DC Resistance @ 20°C</th>
<th>Temperature Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>9841</td>
<td>24</td>
<td>120Ω</td>
<td>12.8 pf per foot</td>
<td>24.0Ω per 1000ft</td>
<td>-30 to +80°C</td>
</tr>
<tr>
<td>3105A</td>
<td>22</td>
<td>120Ω</td>
<td>11.0 pf per foot</td>
<td>17.5Ω per 1000ft</td>
<td>-20 to +60°C</td>
</tr>
<tr>
<td>3074F</td>
<td>18</td>
<td>124Ω</td>
<td>14.0 pf per foot</td>
<td>6.92Ω per 1000ft</td>
<td>+75°C</td>
</tr>
</tbody>
</table>

Table 1.

© Comparison of AWG & Area of wire in mm²

AWG is based on a geometrical progression of 38 sizes between two defined sizes of wire. The ratio between any two diameters of successive sizes is constant. The two defined sizes or numbers are: a) number 4/0 wire (the maximum diameter) is defined as a wire having a diameter of 0.4600 inches, and b) number 36 wire (the minimum diameter) is defined as a wire having a diameter of 0.0050 inches. The constant for the ratio between two diameters of successive sizes is the 39th root (there are 39 steps between the maximum and the minimum diameter) of the ratio of the maximum to the minimum diameter. The equation is expressed as:

\[ \frac{0.460}{0.005} = 39 \sqrt{92} \]

For example, 24 AWG is 12 steps from 36 AWG. Thus, 24 AWG diameter is defined by: 0.0050 inches times \((1.12293219653228)^{12} \approx 0.020\) inches

Table 2 shows the typical AWG sizes with their equivalent area in mm².

<table>
<thead>
<tr>
<th>AWG</th>
<th>Step No.</th>
<th>Dia. (Inch)</th>
<th>Dia. (mm)</th>
<th>Area (mm²)</th>
</tr>
</thead>
<tbody>
<tr>
<td>36</td>
<td>0</td>
<td>0.005</td>
<td>0.127</td>
<td>0.013</td>
</tr>
<tr>
<td>24</td>
<td>12</td>
<td>0.020</td>
<td>0.511</td>
<td>0.205</td>
</tr>
<tr>
<td>22</td>
<td>14</td>
<td>0.025</td>
<td>0.644</td>
<td>0.326</td>
</tr>
<tr>
<td>20</td>
<td>16</td>
<td>0.032</td>
<td>0.812</td>
<td>0.518</td>
</tr>
<tr>
<td>18</td>
<td>18</td>
<td>0.040</td>
<td>1.024</td>
<td>0.823</td>
</tr>
<tr>
<td>16</td>
<td>20</td>
<td>0.051</td>
<td>1.291</td>
<td>1.309</td>
</tr>
<tr>
<td>14</td>
<td>22</td>
<td>0.064</td>
<td>1.628</td>
<td>2.081</td>
</tr>
<tr>
<td>12</td>
<td>24</td>
<td>0.081</td>
<td>2.053</td>
<td>3.309</td>
</tr>
<tr>
<td>10</td>
<td>26</td>
<td>0.102</td>
<td>2.588</td>
<td>5.261</td>
</tr>
<tr>
<td>4/0</td>
<td>39</td>
<td>0.460</td>
<td>11.684</td>
<td>107.21</td>
</tr>
</tbody>
</table>

Table 2.
Important

Most site communication problems are a result of faulty cabling and/or terminations. EIM cannot accept responsibility for systems incorrectly wired.

Remember….

The network cable is a signal carrying cable. It is individually shielded and inherently noise resistant but should not be run in conduit or cable trays with power cables. Running it in conduit with high current carrying cables may induce unwanted noise into the system. It may, however, be run in conduit with other signal carrying cable, e.g. 4-20 mA signalling, etc.

Placing network cables into conduit or cable trays with power carrying cable may result in noise being induced into the control system. This practice may cause the control signals to be partially interrupted leading to poor or erratic operation of the system.

Basic rules.

Routing Cables Away from Noise Sources

The user is advised to take every precaution when laying out the control system to keep signal cables separate from noise generating sources. These noise sources may be motors, contactor operated devices, transformers, or other devices that contain or switch high currents.

Separation by space, use of metallic conduit, and proper grounding of the network cable shields are some of the best ways to prevent noise from entering the control system.

Quality of Field Unit Connections

It is very important to the correct operation of the control system in terms of network cabling, the quality of the connection to the field unit is possibly more important. Standard instrumentation practices apply to field unit connection.
Information in this publication is believed to be accurate. EIM reserves the right to modify published information to reflect product improvements or changes.