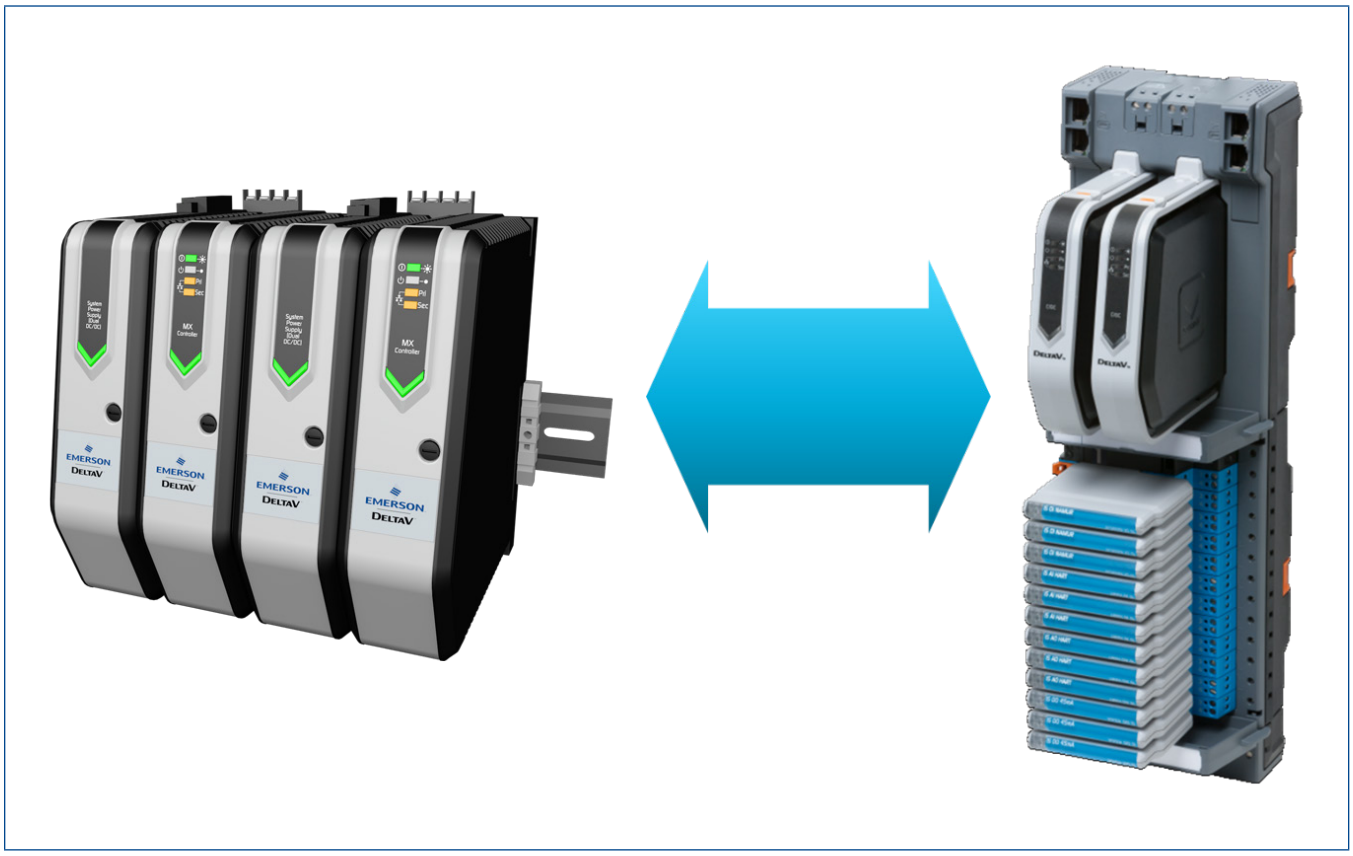
White Paper
October 2022

Network Considerations for M-series with Electronic Marshalling

This white paper provides information about important network requirements to consider when assigning Electronic Marshalling (CHARM I/O Cards) to M-series Controllers on a DeltaV™ system v14.3 or higher.



DeltaV™

EMERSON™

www.emerson.com/deltav

Table of Contents

Introduction

In DeltaV™ v14.3 a new feature has been introduced that allows CHARM I/O Cards (CIOC) to be assigned to M-series Controllers. This new feature expands the options to experience Electronic Marshalling, and at the same time simplifies the implementation of CHARMs if you only have M-series controllers on your DeltaV system.

With Electronic Marshalling, you have options to address common project issues such as: inflexible and more aggressive schedules, late changes due to delays in the I&C data approvals, unexpected changes, installations in “hard-to-staff” locations, among others. Please refer to the white paper “Electronic Marshalling Overview” for additional information about the benefits of using CHARMs in your DeltaV system.

An essential part of Electronic Marshalling is the communication between DeltaV Controllers and the CIOC. What used to be only managed at the rail-bus level with the traditional I/O cards, now runs across the DeltaV Area Control Network (ACN), and with that came requirements to allow high-speed redundant communications between these nodes. Emerson released a portfolio of DeltaV Smart Switches that are specially configured to support Electronic Marshalling. They are required to provide full support for such type of DeltaV network implementation.

The same Electronic Marshalling network requirements apply when CIOCs are assigned to M-series Controllers. This white paper provides a summary of information already available in Books-OnLine and Knowledge Base Articles to help you determine which topologies and network equipment to use with Electronic Marshalling that is compatible with M-series Controllers in DeltaV systems version 14.3 and higher.

DeltaV Control Network Description and Specification

The DeltaV Control Network can be physically connected as a star or cascade (daisy-chain) topology. Other network configurations are possible, such as a combination of a star and cascade topology – Emerson does not support network ring topologies for DeltaV systems.

Refer to the latest DeltaV system installation and planning manuals for details of network layouts and network cable shielding requirements and power and grounding requirements for the overall DeltaV distributed control system (DCS). The DeltaV control network can use one or more Ethernet switches for communication connections.

The maximum twisted-pair cable length for the DeltaV control network for any Ethernet-connected device is 100 meters (328 feet). If longer cable distances are needed for any type of connection, there are various fiber optic cables, transceivers and unmanaged switches/media converters available from Emerson as part of a standard supported solution. For special network designs that go beyond the supported diagrams shown in the DeltaV installation and planning manuals, consult with the Emerson services team.

The DeltaV ACN supports the use of auto-negotiated 10-half, 100-half, 10-full, and 100-full duplex communications where the industry standard auto-negotiation process determines the highest speed at which two devices will communicate with each other. The latest DeltaV network products make use of gigabit (Gbps) Ethernet for certain connections and can support long distances (100+ Km) using standard product fiber optic communications.

The DeltaV workstations and embedded devices contain two Ethernet ports to provide the recommended redundant communications. Early models of DeltaV Controllers supported 10 megabit (Mbps) Ethernet at half-duplex only. The latest DeltaV Controllers auto-negotiate to any speed and duplex from 10-half to 100-full, depending on what the controller is attached to. The workstations do the same: they auto-negotiate to the highest speed and duplex available from their attached device.

Emerson recommends the use of Category 5e Screened Twisted Pair (CAT5e ScTP) cable for the 10/100/1000 BaseTX control network. Fiber optic cables do not conduct electricity; therefore they should be used in connections between buildings or in plant areas where electromagnetic interference is present. Fiber optic cabling should also be used where wire runs are longer than 100 meters (328 feet).

Supported Network Equipment in the DeltaV Area Control Network

DeltaV Smart Switches are required for systems with Electronic Marshalling and this same requirement applies to DeltaV systems that now allow CIOCs to be assigned to M-series Controllers. The same network equipment that can be used today to build DeltaV networks can also be used if CIOCs are assigned to Controllers, and the network equipment would include:

- DeltaV Smart Switches
- DeltaV Unmanaged switches and DeltaV Media Converters
- DeltaV Firewall-IPD
- Specific Cisco switches sold by Emerson (available with an Emerson part number with licensed/approved firmware)

DeltaV Smart Switches provide the complete protection and data handling that addresses the DeltaV communication needs. They provide plug-n-play functionality on a DeltaV network and are delivered with storm protection and loop prevention enabled by default. DeltaV Smart Switches can also be locked down by you to further protect the DeltaV networks against unauthorized access.

The DeltaV Unmanaged Switches as well as the DeltaV Media Converters must be used in combination with DeltaV Smart Switches to support Electronic Marshalling – networks with existing and/or unmanaged switches only (no DeltaV Smart Switches) should not be used with Electronic Marshalling. Emerson does not provide support to DeltaV networks that are not implemented per the provided recommendations.

The DeltaV Firewall-IPD is highly recommended by Emerson to protect the DeltaV embedded nodes against Denial-of-Service attacks or unauthorized access for troubleshooting. This recommendation is even more important with Electronic Marshalling as you can segment the DeltaV ACN into two security zones. One of the zones (the trusted side) is dedicated to DeltaV embedded devices which will be protected from a network flood in case the other zone (dedicated to DeltaV workstations) is compromised.

If you are upgrading your DeltaV system and you are using Cisco switches in the DeltaV ACN, you can continue to use them provided they are running the supported firmware version and configuration available in Guardian Support Portal. Emerson provides support to Cisco switches that are acquired from Emerson (specific Emerson part number). Cisco switches running Emerson's custom configuration tailored for DeltaV systems have a similar storm protection algorithm to the DeltaV Smart Switches, as well as loop prevention, but cannot be locked down using the Network Device Command Center. The supported Cisco switches are sold only as spares or to expansions on systems where Cisco switches were originally implemented. Please refer to the white paper "Use of Cisco Switches on the DeltaV Area Control Network" for additional information about the support and purchase limitations.

DeltaV ACN Topologies for Electronic Marshalling Support

The recommended network architecture for Electronic Marshalling includes DeltaV Smart Switches. Figure 1 reflects the ideal configuration where DeltaV Smart Switches are considered in every network layer within the DeltaV ACN. Figure 1 also indicates that storm protection, loop prevention and port lockdown are available throughout the network.

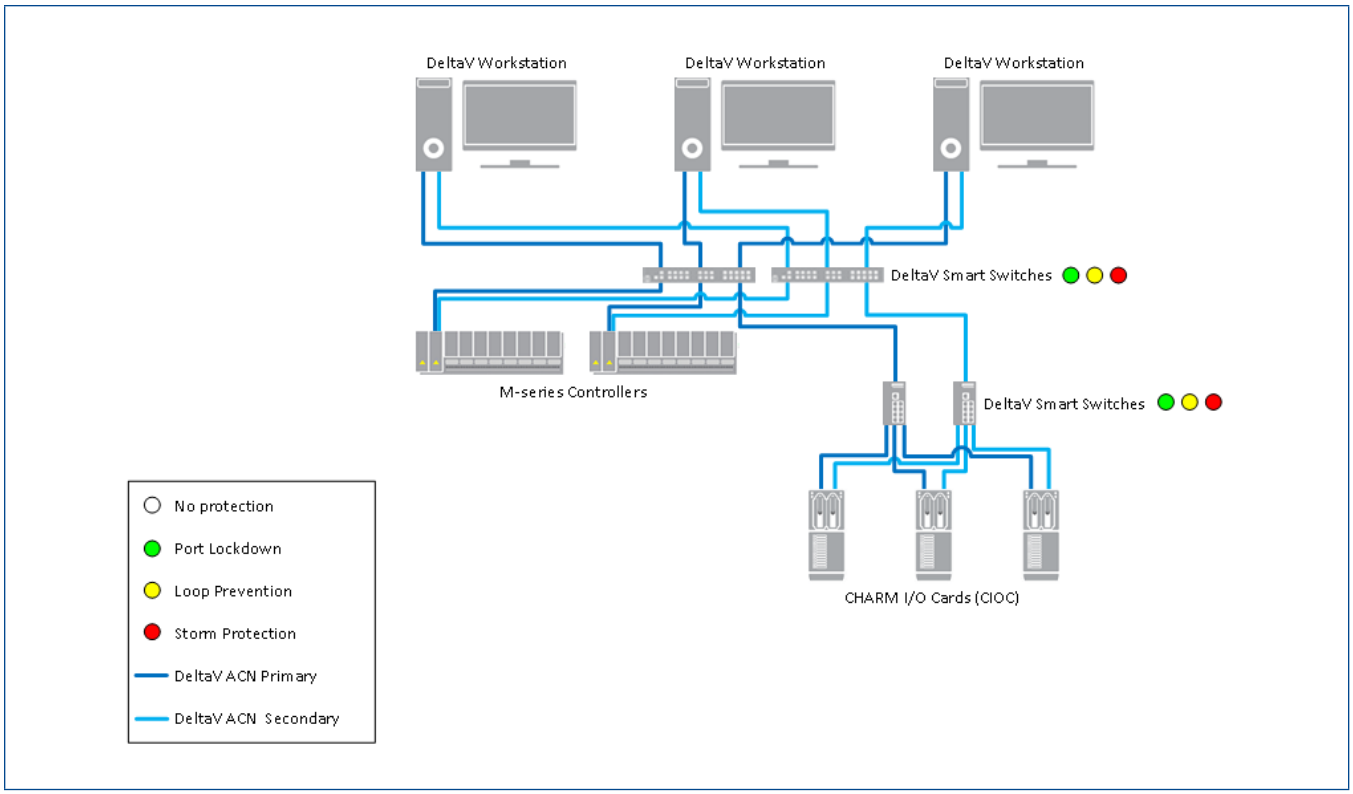


Figure 1. *M-series and CIOCs on a network with DeltaV Smart Switches.*

Optionally you can combine DeltaV Smart Switches with DeltaV Unmanaged Switches and/or Media Converters even when Electronic Marshalling is added to the architecture. Figures 2 and 3 illustrate this use case – Figure 2 shows DeltaV Media Converters directly connected to the network backbone formed by DeltaV Smart Switches, and Figure 3 shows a daisy-chain of DeltaV Unmanaged Switches also connected to the network backbone formed by DeltaV Smart Switches.

Note that for the DeltaV Unmanaged Switches and DeltaV Media Converters the diagrams highlight that no protection is available as these switches do not provide storm protection, loop prevention nor can be locked down.

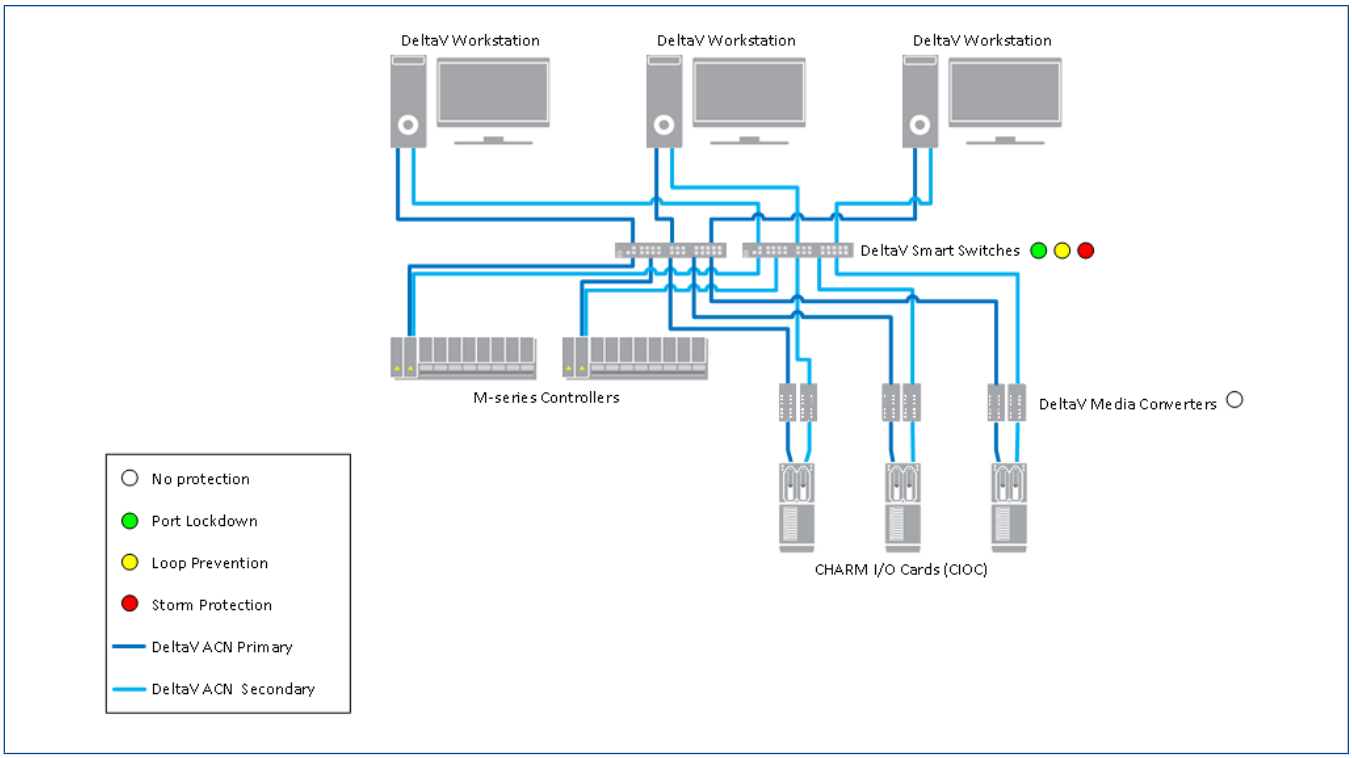


Figure 2. *M-series and CIOCs on a network with DeltaV Media Converters connected to the network backbone (DeltaV Smart Switches).*

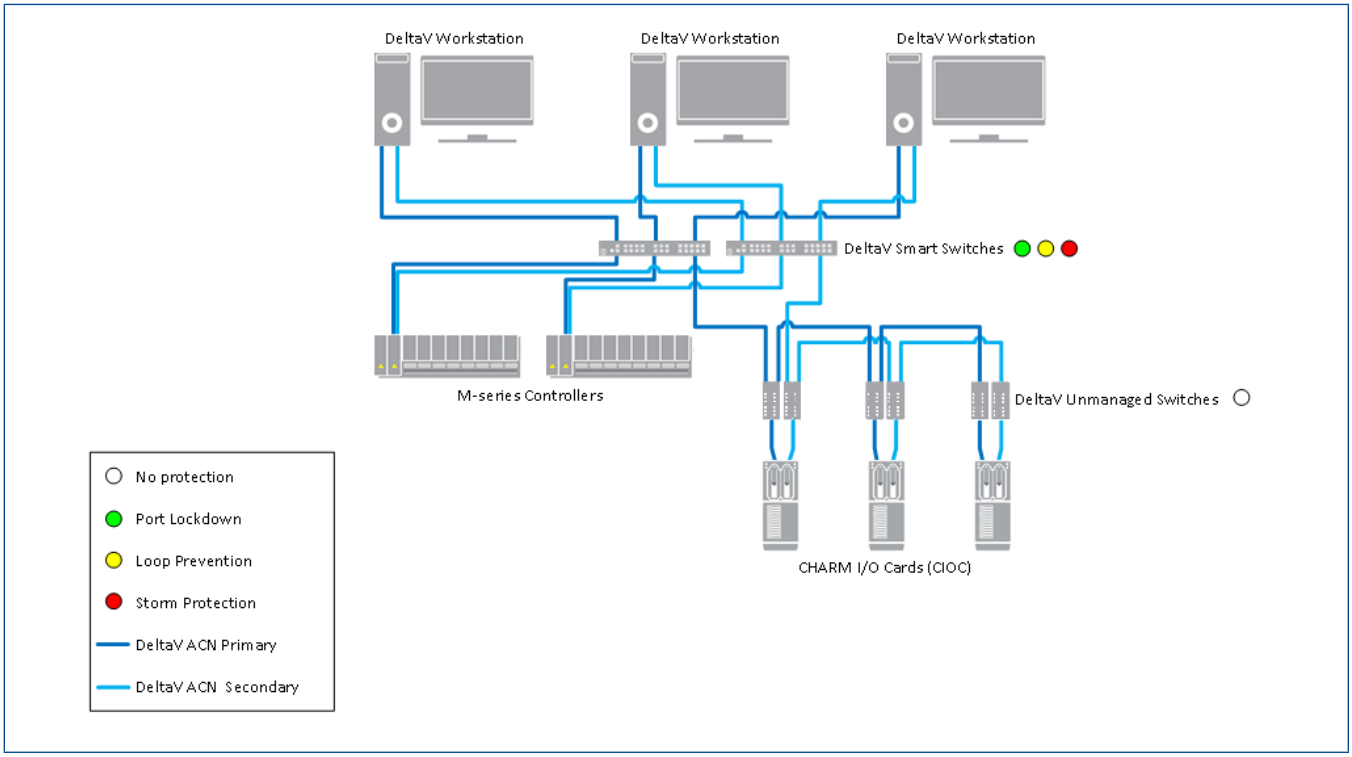


Figure 3. *M-series and CIOCs on a network with DeltaV Unmanaged Switches connected to the network backbone (DeltaV Smart Switches).*

It is also acceptable to expand existing DeltaV networks that have a backbone formed by other types of switches (not DeltaV Smart Switches) and to include Electronic Marshalling. In these cases, Controllers and CIOCs will need to be connected to DeltaV Smart Switches, meaning that an extension of the DeltaV ACN is implemented with DeltaV Smart Switches. This specific topology is highlighted in Figure 4 reinforcing that CIOCs shall not be assigned to Controllers which are not connected to DeltaV Smart Switches.

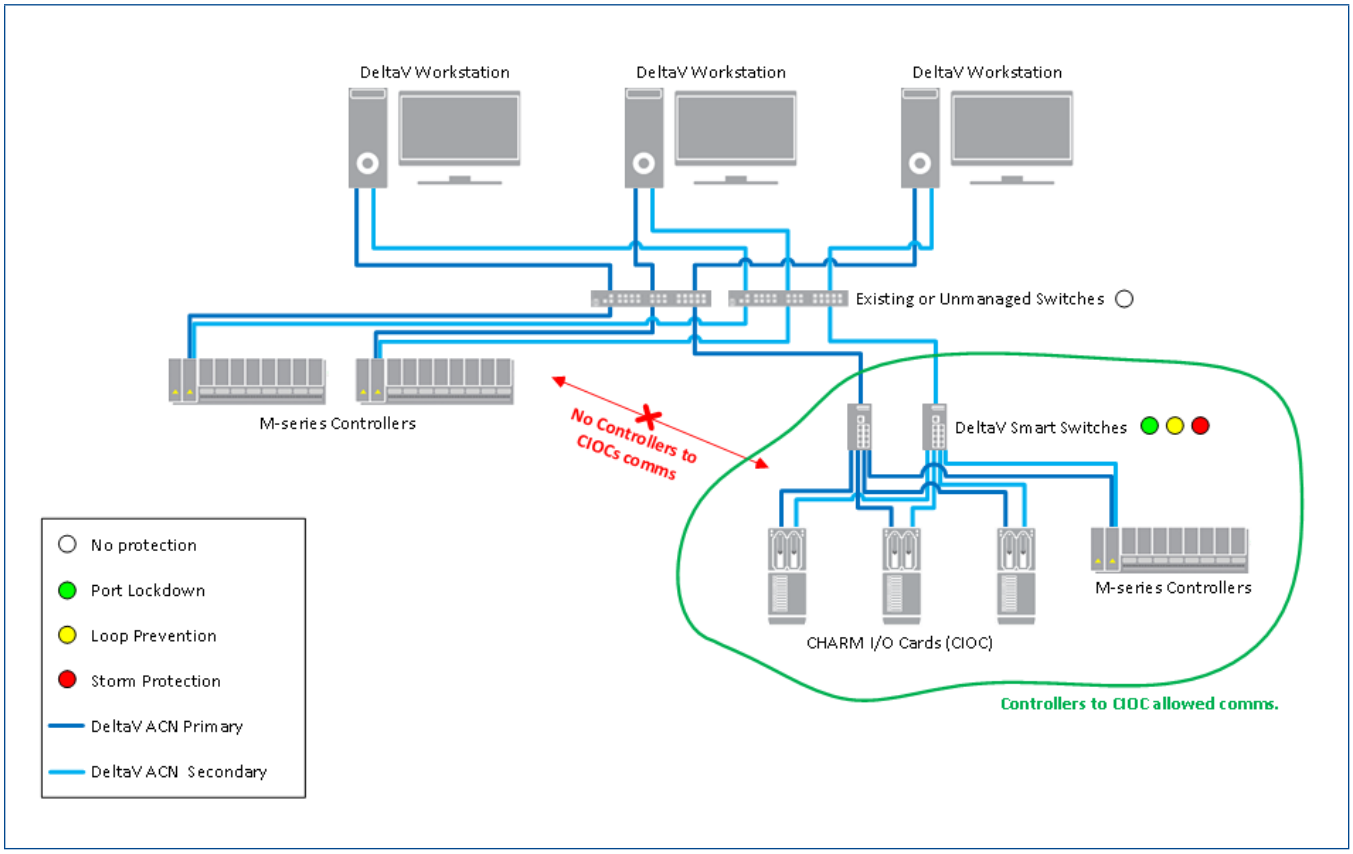


Figure 4. *M-series and CIOCs on a sub-segment of the DeltaV ACN with DeltaV Smart Switches.*

Note: The DeltaV Smart Switches port lockdown mechanism has been enhanced in the switches' firmware v9.0.12. The new algorithm detects when DeltaV Smart Switches are connected to each other (uplink ports) and lock any other port than uplink ones with whichever number or type of devices connected to it. This enhanced port lockdown also prevents new devices to communicate across the DeltaV ACN if the backbone is implemented with DeltaV Smart Switches, and at the remote ends with either DeltaV Unmanaged Switches or DeltaV Media Converters – the remote end switches/converters would still be unprotected (unlocked) though.

DeltaV LOCK Command and Firewall-IPD

In DeltaV v13.3.1 a new LOCK command was introduced and it applies to all DeltaV embedded devices connected to the DeltaV ACN (including the DeltaV SZ Controller). When LOCKED, the DeltaV embedded devices do not accept downloads, decommissioning commands, access for troubleshooting (privileged access) and firmware upgrades. You can enforce physical presence to unlock the embedded devices by adding the DeltaV Firewall-IPD in the network – you will need to put the Firewall- IPD in bypass mode to allow devices to be unlocked and this is done either accessing the local pushbutton on the firewall or sending a pulse signal to the firewall's discrete input. The Firewall-IPD also segments the DeltaV ACN which then protects the embedded devices from Denial-of-Service attacks.

Up to eight redundant DeltaV Controllers (and assigned CIOCs) are connected to the trusted side of the Firewall-IPD (switches are required as the firewall has a single Ethernet port for embedded devices connections, and a single Ethernet port for workstations). DeltaV Controllers and CIOCs that communicate among themselves must be in the same side of the same firewall – no Controller to CIOC communications shall go across the Firewall-IPD.

Emerson highly recommends the use of the DeltaV Firewall-IPD on any DeltaV network, and this is especially true with Electronic Marshalling. Figure 5 illustrates the ideal network design with the Firewall-IPD as part of the architecture.

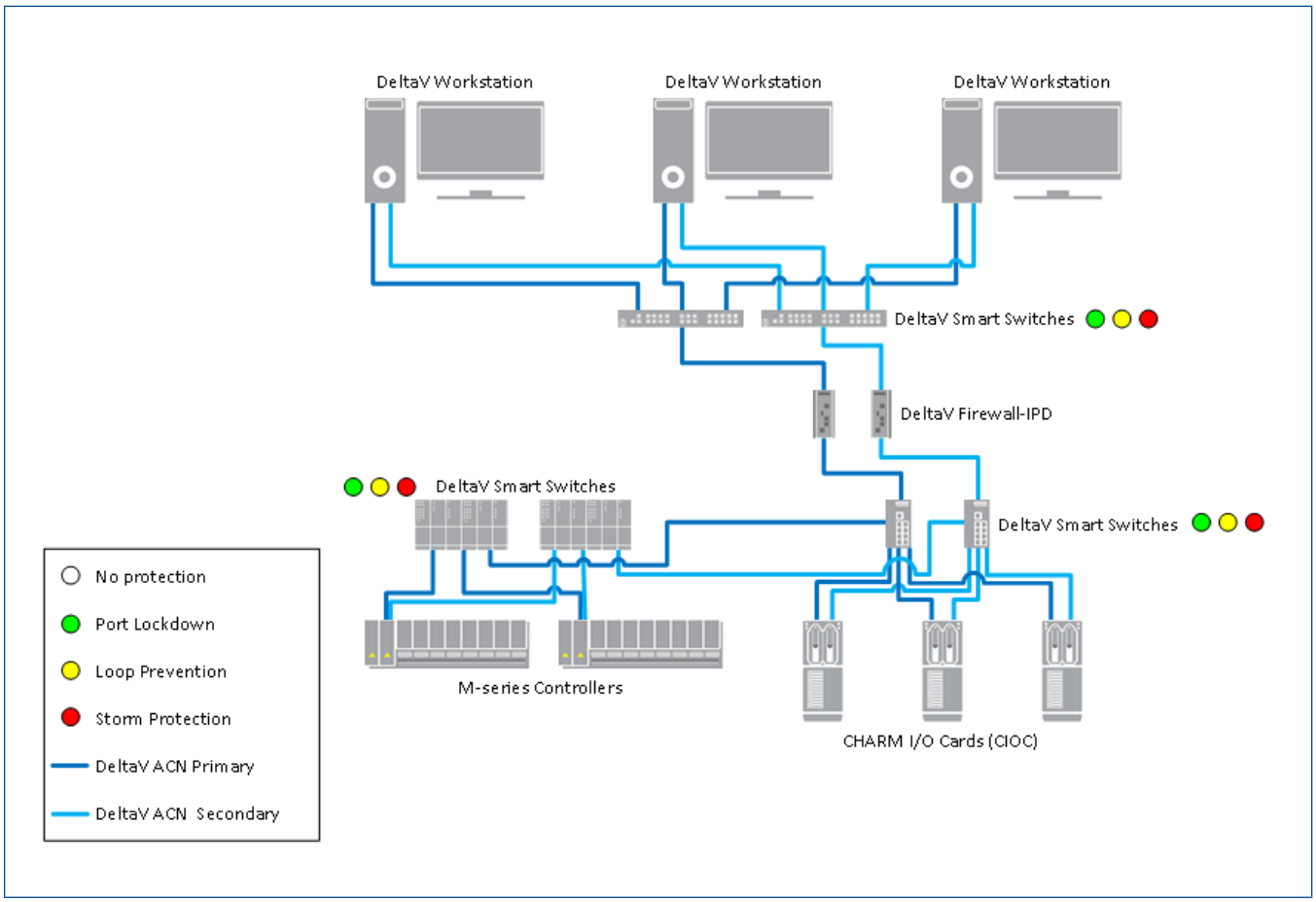


Figure 5. *Network architecture with M-series Controllers, CIOC and the Firewall-IPD.*

Conclusion

Extending the Electronic Marshalling benefi ts to the M-series deployments allow fl exibility which also needs to be designed and planned accordingly. This white paper provides examples of network topologies and equipment that can be used to allow a supported network infrastructure for CIOCs to M-series Controllers communications. Please reach out to your Emerson local sales offi ce for support. You can also fi nd additional information about the topics referenced in this white paper on the following online documentation:

- Web page: DeltaV DCS M-series Hardware
- Product data sheet: DeltaV Electronic Marshalling
- Product data sheet: DeltaV Smart Switches
- Product data sheet: DeltaV Control Network Hardware
- Products data sheet: DeltaV Firewall-IPD
- White paper: Use of Cisco Switches on the DeltaV Area Control Network
- White paper: Electronic Marshalling Overview

Contact Us
www.emerson.com/contactus

EMERSON